Πλαίσιο Ανίχνευσης και Αντιμετώπισης Περιστατικών Ασφαλείας σε Συστήματα Διαδικτυακής Τηλεφωνίας

Η Διδακτορική Διατριβή
παρουσιάστηκε ενώπιον
της συμβουλευτικής & εξεταστικής επιτροπής

Σε Μερική Εκπλήρωση
των Απαιτήσεων για την απόκτηση του Διδακτορικού Διπλώματος
του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

του
Γενειατάκη Δημήτρη

Η ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΕΠΙΤΡΟΠΗ
ΤΗΣ ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗΣ
ΤΟΥ ΓΕΝΕΙΑΤΑΚΗ ΔΗΜΗΤΡΗ:

Λαμπρινουδάκης Κωνσταντίνος — Επιβλέπων
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Γκρίτζαλης Στέφανος — Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Καμπουράκης Γεώργιος — Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Ιούνιος 2008

Η ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ
ΤΗΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ
ΤΟΥ ΓΕΝΕΙΑΤΑΚΗ ΔΗΜΗΤΡΗ:

Σωκράτης Κάτσικας

Καθηγητής Πανεπιστημίου Πειραιώς

Σπυρίδων Λυκοθανάσης

Καθηγητής Πανεπιστημίου Πατρών

Νικήτας Νικητάκος

Καθηγητής Πανεπιστημίου Αιγαίου

Στέφανος Γκρίτζαλης

Αναπληρωτής Καθηγητής Πανεπιστημίου Αιγαίου

Κωνσταντίνος Λαμπρινουδάκης

Επίκουρος Καθηγητής Πανεπιστημίου Αιγαίου

Καμπουράκης Γεώργιος

Λέκτορας Πανεπιστημίου Αιγαίου

Δημήτρης Λέκκας

Λέκτορας Πανεπιστημίου Αιγαίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Ιούνιος 2008

ΕΥΧΑΡΙΣΤΙΕΣ

Κατά τη διάρκεια εκπόνησης της διδακτορικής διατριβής μου δεν ήταν λίγοι εκείνοι που με βοήθησαν, ο καθένας με το δικό του τρόπο, ώστε να φτάσω στο σημερινό τελικό αποτέλεσμα. Το σίγουρο είναι ότι θέλω να τους ευχαριστήσω όλους μαζί και τον καθένα ξεχωριστά για την υπομονή που επέδειξαν όλα αυτά τα χρόνια.

Όπως είθισται, οι ευχαριστίες σε όλες σχεδόν τις διδακτορικές διατριβές ξεκινούν ευχαριστώντας τον επιβλέποντα, και εγώ σε αυτή την περίπτωση δεν θα πράξω διαφορετικά όχι λόγω εθιμοτυπίας αλλά λόγω της αμέριστης υποστήριξης που μου παρείχε όλο αυτό το χρονικό διάστημα. Θα ήθελα να του εκφράσω τη βαθιά μου ευγνωμοσύνη για όλα όσα μου έχει προσφέρει όλα αυτά τα χρόνια, τόσο γιατί μου έδωσε την ευκαιρία για τρίτη φορά να συνεργαστώ ακαδημαϊκά μαζί του, όσο και για τις συμβουλές, την καθοδήγηση και τις παροτρύνσεις που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης της διδακτορικής αυτής διατριβής.

Επίσης θα ήθελα να ευχαριστήσω τα υπόλοιπα μέλη της τριμελούς επιτροπής τα οποία συνέβαλαν σε μεγάλο βαθμό στην επίτευξη του τελικού στόχου. Ειδικότερα, ευχαριστώ θερμά τόσο το Δρ. Καμπουράκη Γεώργιο για τα εποικοδομητικά του σχόλια και τις συμβουλές του, όσο και τον Καθηγητή Γκρίτζαλη Στέφανο για τις επισημάνσεις και τις οδηγίες του, με σκοπό την επίτευξη του καλύτερου δυνατού αποτελέσματος. Επιπλέον, θα ήθελα να ευχαριστήσω το Δρ. Νταγιούκλα Αναστάσιο για τις αρχικές οδηγίες που μου παρείχε στα πλαίσια του ερευνητικού έργου SNOCER.

Πέρα από την τριμελή επιτροπή θα ήθελα να ευχαριστήσω το Λεουτσάκο Θεόδωρο, τη Δούμα Αναστασία και την Παριανού Αγγελική τόσο για την υποστήριξη τους, διατηρώντας με στον πραγματικό κόσμο όλα αυτά τα χρόνια, όσο και για τη βοήθεια τους σε τεχνικά ζητήματα ως μέλη της υπηρεσίας πληροφορικής της Σχολής Θετικών Επιστημών. Ξεχωριστά από τους παραπάνω ευχαριστώ τον Κεχαγιά Σταμάτη για τις αμέτρητες «πέρδικες» που σκοτώσαμε.

Από τις ευχαριστίες δεν θα μπορούσαν να λείπουν δύο εκλεκτοί συνάδελφοι με τους οποίους πορευτήκαμε μαζί όλα αυτά τα χρόνια. Αναφέρομαι στον κ. Καρόπουλο και τον κ. Ευδωρίδη. Τους ευχαριστώ, για τις αναρίθμητες συζητήσεις, επισημάνσεις και πλάκες που κάναμε όλά αυτά τα χρόνια, και σίγουρα αποτελούν ένα αναπόσπαστο μέρος του διδακτορικού αυτού.

Φθάνοντας προς το τέλος, θα ήθελα να ευχαριστήσω ιδιαιτέρως ένα παιδικό μου φίλο το Θεόδωρο Καραλάκη, που όλα αυτά τα χρόνια όχι μόνο δεν με ξέχασε αλλά μου πρόσφερε ανιδιοτελώς τις επαγγελματικές του υπηρεσίες.

Σε αυτό το σημείο θα ήθελα να εκφράσω τις ευχαριστίες μου στην «επιστήμονα» (ως μαθηματικό) Παπαναγιώτου Ευαγγελία για τα μαθηματικά της σχόλια και για τις παροτρύνσεις που μου έδινε κατά τη διάρκεια της διδακτορικής διατριβής.

Κλείνοντας, ένα μεγάλο ευχαριστώ στους γονείς μου και στον αδερφό μου, που χωρίς την υποστήριξη τους σίγουρα δεν θα ήταν δυνατή η εκπόνηση της διδακτορικής αυτής διατριβής.

ΠΕΡΙΛΗΨΗ

Η παροχή υπηρεσιών φωνής μέσω του διαδικτύου προσφέρει σε όλες τις εμπλεκόμενες οντότητες μια σειρά από πλεονεκτήματα, όπως χαμηλό κόστος παροχής της υπηρεσίας, δυνατότητα ανάπτυξης νέων εξελιγμένων υπηρεσιών, ευκολία διαχείρισης και άλλα πολλά. Βέβαια, πέρα από τα πλεονεκτήματα και τους νέους ορίζοντες που δημιουργούνται στις υπηρεσίες τηλεφωνίας, θα πρέπει να αντιμετωπιστούν τόσο τα προβλήματα αξιόπιστης μετάδοσης των δεδομένων, όσο και αυτά της ασφαλείας των υπηρεσιών φωνής. Τα συγκεκριμένα προβλήματα είναι ιδιαίτερα έντονα λόγω των χαρακτηριστικών των δημόσιων δικτύων ανοικτών προδιαγραφών, όπως είναι το διαδίκτυο, που αξιοποιούνται για την παροχή των υπηρεσιών.

Τα προβλήματα αξιόπιστης μετάδοσης, κυρίως για τα δεδομένα φωνής, ήταν αυτά που προσέλκυσαν το ενδιαφέρον της επιστημονικής κοινότητας, δεδομένου ότι η αξιοπιστία μετάδοσης είναι αδιαπραγμάτευτο προαπαιτούμενο για την παροχή υπηρεσιών τηλεφωνίας. Σήμερα, υπάρχουν ικανοποιητικές λύσεις για τα περισσότερα από τα προβλήματα που έχουν εντοπιστεί οι οποίες βασίζονται στους κατάλληλους μηχανισμούς κωδικοποίησης.

Από την άλλη πλευρά, το ενδιαφέρον για τα ζητήματα ασφαλείας των υπηρεσιών ήταν σχετικά περιορισμένο, παρά το γεγονός ότι η παροχή υπηρεσιών μέσω δημόσιων δικτύων ανοικτών προδιαγραφών προσφέρει πληθώρα δυνατοτήτων εκδήλωσης κακόβουλων ενεργειών. Το διαδίκτυο, ως το πλέον αντιπροσωπευτικό παράδειγμα δικτύου ανοικτής αρχιτεκτονικής, κινδυνεύει τόσο από τα πολυάριθμα γνωστά προβλήματα ασφαλείας, όσο και από νέες ευπάθειες που μπορεί να προκύψουν από τη συνεχή διαδικασία αναζήτησης κενών ασφαλείας σε υπηρεσίες και πρωτόκολλα. Συνεπώς, οι υπηρεσίες που παρέχονται μέσω του διαδικτύου, μη εξαιρουμένων των υπηρεσιών φωνής, κληρονομούν όλες τις εγγενείς ευπάθειες του. Επιπλέον, η εισαγωγή νέων πρωτοκόλλων για την εγκαθίδρυση και διαχείριση συνόδων, όπως το Session Initiation Protocol (SIP), δημιουργεί πληθώρα νέων απειλών που, λόγω της διασυνδεσιμότητας των υπηρεσιών, καθιστούν ολόκληρο το τηλεφωνικό δίκτυο ευπαθές σε επιθέσεις.

Η παρούσα διδακτορική διατριβή επικεντρώνεται σε ζητήματα ασφαλείας που αφορούν το πρωτόκολλο σηματοδοσίας SIP. Συγκεκριμένα, αναλύονται όλες οι πιθανές ευπάθειες που μπορεί να ‘αξιοποιηθούν’ για την εκδήλωση επιθέσεων κατά τη διαδικασία εγκαθίδρυσης συνόδων SIP. Στη συνέχεια παρουσιάζονται και αξιολογούνται, ως προς την αποτελεσματικότητα τους, οι μηχανισμοί ασφαλείας που προδιαγράφονται στο πρότυπο του SIP. Τα κενά ασφάλειας που παραμένουν αντιμετωπίζονται μέσω νέων μηχανισμών ασφάλειας που προτείνονται και οι οποίοι δρουν συμπληρωματικά με τα υπάρχοντα μέτρα ασφαλείας. Οι προτεινόμενοι μηχανισμοί έχουν υλοποιηθεί και αξιολογηθεί ως προς την αποτελεσματικότητα και την απόδοση τους μέσω πειραματικού περιβάλλοντος που αναπτύχθηκε.

Συνολικά, για την αποτελεσματική αντιμετώπιση των προβλημάτων ασφαλείας στις υπηρεσίες διαδικτυακής τηλεφωνίας, προτείνεται μια αρχιτεκτονική τριών επιπέδων στην οποία εντάσσονται τα κατάλληλα προληπτικά, αναγνωριστικά και ανασταλτικά μέτρα ασφαλείας. Στο πρώτο επίπεδο κατατάσσονται οι κατάλληλοι μηχανισμοί πρόληψης για την αντιμετώπιση περιστατικών μη εξουσιοδοτημένης τροποποίησης των δεδομένων σηματοδοσίας. Στο δεύτερο επίπεδο αναπτύσσονται αυστηρές πολιτικές και μηχανισμοί ελέγχου που βασίζονται στις προδιαγραφές των αξιοποιούμενων πρωτοκόλλων σηματοδοσίας, όπως το SIP, προκειμένου να αποτρέπεται η επεξεργασία μη συμβατών μηνυμάτων από τους αναλυτές μηνυμάτων των υπηρεσιών. Στο τελευταίο επίπεδο άμυνας,

υλοποιούνται μηχανισμοί για την άμεση αναγνώριση επιθέσεων πλημμύρας. Η προτεινόμενη αρχιτεκτονική συμπληρώνει τους υπάρχοντες μηχανισμούς ασφαλείας και αποτελεί μια εύκολα κλιμακούμενη αρχιτεκτονική.

Οι πάροχοι υπηρεσιών διαδικτυακής τηλεφωνίας, εκτός από την έγκαιρη ανίχνευση και την αντιμετώπιση των επιθέσεων που μπορεί να εκδηλωθούν κατά των υπηρεσιών που προσφέρουν, θα πρέπει να διαθέτουν τη δυνατότητα αποτύπωσης των περιστατικών ασφαλείας μέσω κάποιας κοινής σημασιολογικής περιγραφής. Με τον τρόπο αυτό θα καταστεί δυνατή η ανάπτυξη μιας ενιαίας αρχιτεκτονικής ασφαλείας και προστασίας. Προς την κατεύθυνση αυτή, και συγκεκριμένα για τη δημιουργία ενός ενιαίου τυπικού μοντέλου ασφαλείας για τις υπηρεσίες διαδικτυακής τηλεφωνίας, αποφασίστηκε να αξιοποιηθούν οντολογίες για την ανάπτυξη μίας κοινής «βάσης ασφαλείας» μέσω της οποίας προωθείται η συνεργασία των παρόχων διαδικτυακής τηλεφωνίας στα πλαίσια ενός ασφαλούς περιβάλλοντος παροχής υπηρεσιών τηλεφωνίας. Η οντολογία που αναπτύχθηκε, αναπαραστάθηκε σε κατηγορηματική λογική και εφαρμόστηκε σε πειραματικό περιβάλλον.

ABSTRACT

Voice service provision over the internet offers many advantages to all entities involved, like reduced cost, opportunities for new services, ease of management and many more. However, together with the advantages and the new opportunities, it is necessary to ensure the reliability of data transmission, as well as to address all remaining security problems. These problems mainly originate from the characteristics of the public, open architecture, networks, like the internet, utilised for the provision of the services.

The problems related to the reliability during data transmission are the ones that have attracted most of the interest of the scientific community, mainly due to the fact that reliability is a prerequisite for the provision of voice services. Today most of the identified problems are satisfactorily addressed.

On the other hand, the interest for other security issues that may affect the voice services is not too high, eventhough the provision of the services over public networks offers many opportunities to malicious users to launch an attack. The internet, which is an indicative example of open architecture networks, faces all the threats originating from the existing vulnerabilities, as well as from the new vulnerabilities that may be identified by attackers trying to harm the new services and protocols. Therefore, the services offered through internet, including the voice services, inherit all its security gaps. On top of that, the introduction of new protocols for session management, like the Session Initiation Protocol (SIP), gives birth to numerous new threats which, due the interoperability of the services, make the entire voice network susceptible to attacks.

This thesis focuses on the security issues of the signalling protocol SIP. More specifically it analyses all its vulnerabilities that may be utilised for launching an attack during the establishment of a session. Then the security measures proposed by the SIP standard are presented and evaluated in terms of their effectiveness. The remaining security problems are addressed through new security mechanisms that are proposed. The effectiveness and performance of the proposed mechanisms have been evaluated through an experimental environment that was developed for that purpose.

In order to achieve effective protection of the internet based voice services, the thesis proposes a three layer security architecture that incorporates all the necessary preventive and detection security measures. In the first layer there are preventive mechanisms that address cases of unauthorized modification of signalling data. In the second layer there are strict security policies and access control mechanisms that have been based on the specifications of the signalling protocols, like SIP, in order to protect parsers from processing not compatible messages. In the last layer, there are mechanisms for the detection of flooding attacks.

Service providers, in addition to the early detection of and protection against all potential attacks that can be launched against the services that they offer, should be able to represent any security incident in a formal way. This will allow the development of a common security and protection architecture. To this direction, ontologies have been utilised for developing a common “security data base” through which service providers can cooparate in order to achieve ‘a secure environment for the provision of the voice services’. The ontology developed was represented in first order logic and was applied in an experimental environment.

Γενειατάκης Δημήτρης
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
© 2008

Γλωσσάρι Όρων

Αγγλικός Όρος	Απόδοση
Public Switch Telephone Network	Δημόσιο Τηλεφωνικό Δίκτυο Μεταγωγής
Throughput	Διεκπεραιωτική Ικανότητα
In-band Signalling Systems	Εσωζωνικά Συστήματα Σηματοδοσίας
Out-of-band Signalling Systems	Εξωζωνικά Συστήματα Σηματοδοσίας
Signalling System 7	Σύστημα Σηματοδοσίας 7
Internet Protocol	Πρωτόκολλο Διαδικτύου
Voice over IP	Υπηρεσία Φωνής μέσω IP Δικτύων
Internet	Διαδίκτυο
Internet Providers	Πάροχοι Διαδικτυακών Συνδέσεων
Wiretapping	Υποκλοπές Συνδιαλέξεων
Local Exchange Center	Τοπικό Τηλεφωνικό Κέντρο
Multimedia Sessions	Πολυμεσική Σύνοδος
IP Multimedia Subsystem	Υποσύστημα Πολυμέσων IP
Next Generation Networks	Δίκτυα Επόμενης Γενεάς
Denial of Service	Άρνηση Παροχής Υπηρεσίας
Billing Service	Υπηρεσία Χρεώσεων
Switching Techniques	Τεχνικές Μεταγωγής
Circuit Switching	Μεταγωγή Κυκλώματος
Packet Switching	Μεταγωγή Πακέτων
Sharing	Διαμοιρασμό
Utilization	Ποσοστό Χρήσης
Virtual Circuit	Ιδεατή Σύνδεση
Connectionless	Ασυνδεσμική
Trunk	Διαθέσιμη Γραμμή
Signalling network	Δίκτυο Σηματοδοσίας
Monitoring	Έλεγχος-Επίβλεψη
Signalling Transfer Point	Σημείο Μεταφοράς Σηματοδοσίας
Service Control Point	Σημείο Ελέγχου Υπηρεσίας
Open Systems Interconnection Standard	Πρότυπο Διασύνδεσης Ανοικτών Συστημάτων
Physical Level	Φυσικό Επίπεδο
Data-Link Level	Επίπεδο Ζεύξης Δεδομένων
Network Level	Επίπεδο Δικτύου
Application Level	Επίπεδο Εφαρμογών-Υπηρεσιών
Message Transfer Part Level	Μεταφοράς Μηνύματος Επιπέδου
Flow Control	Έλεγχος Ροής
Request-for-Service	Αίτηση για Χρήση της Υπηρεσία
Dial Tone	Τόνος Κλήσης
Ringing Tone	Τόνος Κωδωνισμού
Answer Signal	Σήμα Απάντησης Κλήσης
Encapsulation	Ενθυλάκωση
Header	Κεφαλίδες
Real-Time Data	Δεδομένα Πραγματικού Χρόνου

Αγγλικός Όρος	Απόδοση
Signalling Protocols	Πρωτόκολλα Σηματοδοσίας
Multimedia Protocols	Πρωτόκολλα Πολυμέσων
Address Name Resolution Service	Υπηρεσία Επίλυσης Ονομάτων
Peer-to-Peer Model	Μοντέλο Διότιμης Επικοινωνία
Request	Αίτηση
Client	Πελάτης
Server	Εξυπηρέτης
Response	Απόκριση
Start- Line	Αρχική Γραμμή
Message Body	Κύριο Μέρος Μηνύματος
Request-Line	Γραμμή Αίτησης
Status-Line	Γραμμή Κατάστασης
Contact Address	Διευθύνσεων Επαφής
Uniform Resource Locator	Μηχανισμός Ομοιόμορφου Εντοπιστή Πόρων
User Agents	Πράκτορες Χρήστη
Registrar	Εξυπηρέτης Εγγραφής
Proxy	Πληρεξούσιος Εξυπηρέτης
Redirect	Εξυπηρέτης Ανακατεύθυνσης
Gateway	Εξυπηρέτης Πύλη
Stateless Mode	Κατάσταση Χωρίς Μνήμη
Stateful Mode	Κατάσταση με Μνήμη
Transactional Protocol	Πρωτόκολλο Δοσοληψίας
Transactional Level	Επίπεδο Δοσοληψιών
Finish State Machine	Μηχανή Πεπερασμένης Κατάστασης
Message Parsing	Συντακτική Ανάλυση Μηνύματος
Gatekeeper	Εξυπηρέτης Θυρωρός
Multipoint Control Unit	Πολυσημειακή Μονάδα Ελέγχου
Multicast Address	Διεύθυνση Πολυεκπομπής
Gatekeeper Confirmation Message	Μήνυμα Επιβεβαίωσης Θυρωρού
Registration Confirmation Message	Μήνυμα Επιβεβαίωσης Εγγραφής
Call Admission Request	Αίτηση Αποδοχής Κλήσης
Admission Confirmation Message	Μήνυμα Επιβεβαίωσης Αποδοχής Κλήσης
Negotiation	Διαπραγμάτευση
Codec	Κωδικοποιητής
Media Gateway Control Protocol	Πρωτόκολλο Ελέγχου Πολυμεσικών Πυλών
Media Gateway Servers	Εξυπηρέτες Πύλες Πολυμέσων
Real Time Data	Δεδομένα Πραγματικού Χρόνου
End-to-End Delivery	Παράδοση από Άκρο σε Άκρο
Domain	Τομέας
Unauthorized Access	Μη Εξουσιοδοτημένη Πρόσβαση
Toll Frauds Call	Απάτη Χρέωσης Κλήσης
Impersonation	Πλαστοπροσωπία
Eavesdropping	Υποκλοπή Επικοινωνίας
Confidentiality	Εμπιστευτικότητα

Αγγλικός Όρος	Απόδοση
Out-of-Sequence Messages	Μηνυμάτων που Λαμβάνονται εκτός της Προκαθορισμένης Διαδικασίας
Green Houses	Εναλλακτικοί Πάροχοι Τηλεφωνίας
Malformed Messages	Μη Συμβατά Μηνύματα
Integrity	Ακεραιότητα
Authenticity	Αυθεντικότητα
Client impersonation	Πλαστοπροσωπία Πελάτη
Service impersonation	Πλαστοπροσωπία Υπηρεσίας
Text Based	Μηνύματα Κειμένου
Traffic Analysis	Ανάλυση Κίνησης
Injection Code Attacks	Επιθέσεις Έγχυσης Κώδικα
Buffer Overflow	Υπερχείλιση Καταχωρητή
Credentials	Διαπιστευτήρια
Accounting	Χρέωση Λογαριασμού
Modules	Δομοστοιχεία
Special Characters	Ειδικοί Χαρακτήρες
Application Programming Interface	Διεπαφή Προγραμματισμού Εφαρμογής
Man-in-the-Middle Attack	Επιθέσεις Ενδιάμεσου
Flooding Attacks	Επιθέσεις Πλημμύρας
Reflection Flooding Attack	Επιθέσεις Πλημμύρας Τύπου Ανάκλασης
Irresolvable Address	Μη Επιλύσιμη Διεύθυνση
Three Way Handshake	Τριμερής Διαδικασία Χειραψίας
Signalling Attacks	Επιθέσεις Σηματοδοσίας
Termination	Τερματισμό
Cancellation	Ακύρωση
Redirection	Ανακατεύθυνση
Challenge-Response	Πρόκληση-Απάντηση
Spoofing	Απόκρυψη Ταυτότητας
Session Hijacking	Υποκλοπή Συνόδου
Data Origin Authentication	Γνησιότητα Προέλευσης Δεδομένων
Secure IP	Ασφαλές IP
Transport Layer Security	Πρωτόκολλο Ασφαλούς Μεταφοράς
Tunneling Integrity and Authentication	Δίοδος Ακεραιότητας και Αυθεντικοποίησης
One-way Message Authentication	Μονοκατευθυντική Γνησιότητα Μηνυμάτων
Known Plaintext Attacks	Επιθέσεις Αποκρυπτογράφησης με Γνωστό Κείμενο
Prearrange Trust	Προ-Εγκατεστημένος Δεσμός Εμπιστοσύνης
Signalling Path	Μονοπάτι Σηματοδοσίας
Detection Mechanism	Μηχανισμός Αναγνώρισης
Cross Protocol	Συσχετισμός Πρωτοκόλλων
False Positive Alarms	Λανθασμένος Θετικός Συναγερμός
Colored Hierarchical Petri Net	Χρωματιστά Ιεραρχικών Δίκτυα Petri
Misuse detection	Μοντέλα Ανίχνευσης μη Ορθής Χρήσης
Authentication Token	Αδειοπλαισίο Αυθεντικοποίησης

Αγγλικός Όρος	Απόδοση
Elliptic Curve Cryptography	Κρυπτογραφία Ελλειπτικών Καμπυλών
Cumulative Sum	Προοδευτικό Άθροισμα
Threshold	Επιτρεπτό Όριο
Honeypot	Παγίδα Ασφαλείας
Keyed Hash Functions	Συνάρτηση Σύνοψης Κλειδιού
Brute force attack	Επίθεση Εξαντλητικής Αναζήτησης
Cryptographic Space	Κρυπτογραφικό Διάστημα
Alert	Συναγερμός
Firewall	Ανάχωμα Ασφαλείας
Monitoring System	Σύστημα Καταγραφής-Ελέγχου
Call-Agent	Πράκτορας Κλήσεων
Clear Forward	Σήμα Εμπροσθαπόλυσης
Clear Back	Σήμα Οπισθόδρομης Απόλυσης
Port	Θύρα
Format	Μορφότυπος
Configuration	Διαμόρφωση
Null Value	Κενή Τιμή
Replay Attack	Επίθεση Επανάληψης

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: Εισαγωγή

1.1 Γενικά

Στις μέρες μας μεγάλο μέρος των τηλεφωνικών κλήσεων πραγματοποιούνται μέσω του δημόσιου τηλεφωνικού δικτύου μεταγωγής (Public Switch Telephone Network– (PSTN)). Για την πραγματοποίηση μιας κλήσης απαιτείται η δέσμευση όλων των απαραίτητων πόρων καθ'όλη τη χρονική διάρκεια της επικοινωνίας, με αποτέλεσμα να γίνεται αξιοποίηση των δεσμευμένων πόρων μόλις κατά το 10-25% [1] και να υπάρχει (έμμεσα) αυξημένο κόστος παροχής της υπηρεσίας. Ταυτόχρονα, οι δυνατότητες για παροχή νέων υπηρεσιών είναι περιορισμένες. Για το λόγο αυτό, οι τηλεπικοινωνιακοί πάροχοι (telecommunication providers) καταβάλουν συνεχείς προσπάθειες για καλύτερη διαχείριση/αξιοποίηση των διαθέσιμων πόρων, με στόχο τόσο τη μείωση του κόστους όσο και τη βελτίωση των παρεχόμενων υπηρεσιών, με απώτερο σκοπό την προσέλκυση νέων πελατών. Προϋπόθεση όμως για την καλύτερη διαχείριση των διαθέσιμων πόρων είναι η βελτίωση των βασικών υποσυστημάτων που απαρτίζουν το τηλεφωνικό δίκτυο και συγκεκριμένα των υποσυστημάτων σηματοδοσίας και επεξεργασίας φωνής.

Το υποσύστημα σηματοδοσίας είναι υπεύθυνο για τη διαχείριση των κλήσεων, δηλαδή για την αποκατάσταση, την ανανέωση των παραμέτρων και τον τερματισμό κάθε κλήσης, καθώς και για την παροχή εξειδικευμένων υπηρεσιών. Από την άλλη πλευρά το υποσύστημα επεξεργασίας φωνής είναι υπεύθυνο για την επεξεργασία και μετάδοση των δεδομένων φωνής μεταξύ των τηλεφωνικών κέντρων μέχρι τον τελικό βρόγχο, δημιουργώντας την κύρια κίνηση ενός τηλεφωνικού δικτύου με βάση τις παραμέτρους που έχουν προσδιοριστεί από το σύστημα σηματοδοσίας, κατά τη διαδικασία αποκατάστασης της κλήσης. Άρα η βελτιστοποίηση των υποσυστημάτων αυτών, θα δημιουργήσει καλύτερες υπηρεσίες μειώνοντας, ταυτόχρονα, το κόστος παροχής των. Για παράδειγμα, η αξιοποίηση του καναλιού επικοινωνίας από άλλες κλήσεις, όσο χρόνο αυτό παραμένει ανενεργό, βελτιώνει την διεκπεραιωτική (throughput) ικανότητα του συστήματος, με άμεση μείωση του κόστους. Επιπλέον, θα πρέπει να τονιστεί ότι όσο πιο πολύπλοκη είναι η διαχείριση των κλήσεων τόσο μεγαλύτερό είναι το κόστος παροχής των, ενώ ακόμα μεγαλύτερο είναι στις περιπτώσεις ανάπτυξης εξειδικευμένων υπηρεσιών.

Είναι λοιπόν ξεκάθαρο ότι η εξέλιξη των υποσυστημάτων σηματοδοσίας συνδέεται άμεσα με τη μείωση του κόστους (άμεσου ή έμμεσου) παροχής τηλεφωνικών υπηρεσιών καθώς και με το σχεδιασμό και ανάπτυξη νέων υπηρεσιών για το ευρύ κοινό. Οι κλασικές εσωζωνικές (in-band) μέθοδοι σηματοδοσίας που αξιοποιούσαν τα συστήματα τηλεφωνίας μέχρι τη δεκαετία του 1970 αντικαταστάθηκαν από εξωζωνικά (out-of-band) συστήματα σηματοδοσίας. Ο κύριος αντιπρόσωπος των συστημάτων αυτών είναι το σύστημα σηματοδοσίας 7 (Signalling System 7–(SS7)). Το συγκεκριμένο σύστημα είναι ένα σύνολο από πρωτόκολλα και προδιαγραφές που απαιτείται να ακολουθούνται και να εφαρμόζονται για την ορθή λειτουργία ενός τηλεφωνικού συστήματος και αποτελεί ουσιαστικά την απαρχή μιας νέας γενιάς τηλεφωνικών συστημάτων με μεγάλες δυνατότητες υποστήριξης νέων υπηρεσιών. Παρ' όλα αυτά, δεν καταφέρνει να απαγκιστρωθεί από την πάγια απαίτηση αξιοποίησης δικτύων, προτύπων και εξοπλισμού κλειστής αρχιτεκτονικής, γεγονός που έχει σαν αποτέλεσμα το αυξημένο κόστος ανάπτυξης νέων εξειδικευμένων υπηρεσιών.

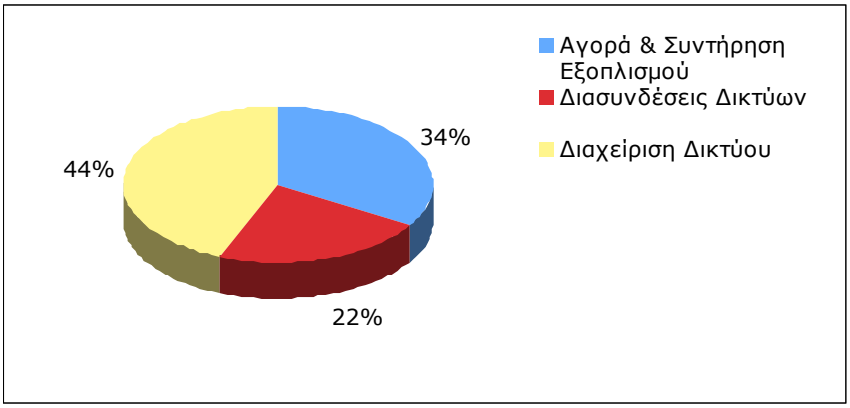
Για το λόγο αυτό αναζητήθηκαν εναλλακτικοί τρόποι παροχής υπηρεσιών τηλεφωνίας που θα χρησιμοποιούσαν ανοικτά συστήματα. Σε αυτούς εντάσσονται οι αρχικές προτάσεις που πραγματοποιήθηκαν στις αρχές της δεκαετίας του 1970 για την μετάδοση φωνής μέσω δικτύων δεδομένων [2] οι οποίες βέβαια δε μπορούσαν να υποστηριχθούν με αξιόπιστο τρόπο

με την τότε υπάρχουσα τεχνολογία. Οι πρώτες επιτυχημένες προσπάθειες για τη μετάδοση φωνής μέσω ανοικτών δικτύων δεδομένων πραγματοποιήθηκαν στις αρχές της δεκαετίας του 1990. Ο κορμός του δικτύου αυτού, όπως και σήμερα, βασιζόταν στο πρωτόκολλο Διαδικτύου (Internet Protocol–(IP))[3], ενώ η υπηρεσία της μετάδοσης της φωνής μέσω τέτοιων δικτύων είναι ευρέως γνωστή ως Υπηρεσία Φωνής μέσω IP Δικτύων (Voice over IP–(VoIP)) ή εναλλακτικά IP Τηλεφωνία.

Στο μεσοδιάστημα, υπήρχε μια συνεχής βελτίωση των PSTN συστημάτων που βασιζόταν τόσο στην τεχνογνωσία και στην εμπειρία των προηγούμενων δεκαετιών όσο και στην αξιοποίηση των τεχνολογικών καινοτομιών, κάτι που είχε σαν αποτέλεσμα να επιτευχθούν πολύ υψηλά επίπεδα ποιότητας, αξιοπιστίας, διαθεσιμότητας και ασφάλειας. Αυτό αντικατοπτρίζεται στο γεγονός ότι οποιαδήποτε στιγμή ένας χρήστης θελήσει να πραγματοποιήσει μια τηλεφωνική κλήση μπορεί να το κάνει με σχεδόν απόλυτη βεβαιότητα ότι δε θα αντιμετωπίσει κάποιο πρόβλημα. Το επίπεδο της αξιοπιστίας και διαθεσιμότητας της υπηρεσίας φωνής στη μονάδα χρόνου λειτουργίας που παρέχεται η υπηρεσία, ποσοτικοποιείται από τους τηλεπικοινωνιακούς παρόχους σε ποσοστό 99,999% (γνωστό ως πέντε 9 (five nines)) [4].

Ταυτόχρονα με τη δημιουργία ενός αξιόπιστου δικτύου τηλεφωνίας, το διαδίκτυο καθιερώνεται ως de-facto επικοινωνιακό-πληροφοριακό μέσο, γεγονός στο οποίο συνέβαλε και η ραγδαία εξέλιξη των δικτύων δεδομένων. Η εξέλιξη αυτή δημιούργησε και νέες επιχειρηματικές δραστηριότητες αφού εκτός των παρόχων σύνδεσης στο διαδίκτυο (Internet Providers), εμφανίστηκαν πάροχοι διαφόρων υπηρεσιών μέσω του διαδικτύου όπως οργάνωση ταξιδιών, αναζήτηση πληροφοριών, ηλεκτρονικό ταχυδρομείο, άμεσα μηνύματα, τηλεφωνία και άλλων πολλών. Γενικότερα, προς τα τέλη της δεκαετίας του 1990 παρατηρήθηκε ένα είδος μετάβασης όλων των υπαρχόντων, κλασικών υπηρεσιών στο περιβάλλον του διαδικτύου.

Από αυτή τη γενικότερη τάση δε θα ήταν δυνατόν να λείψει η υπηρεσία της τηλεφωνίας, η οποία ουσιαστικά εισέρχεται σε μια νέα εποχή. Οι πάροχοι μπορούν πλέον να αναπτύσσουν και να προσφέρουν νέες υπηρεσίες χαμηλού κόστους αξιοποιώντας ένα ενιαίο παγκόσμιο δίκτυο όπως αυτό του διαδικτύου για την παροχή τηλεπικοινωνιακών υπηρεσιών. Η δυνατότητα παροχής υπηρεσιών χαμηλού κόστους οφείλεται κυρίως στην μείωση των εξόδων των τηλεπικοινωνιακών παρόχων. Πιο συγκεκριμένα, σύμφωνα με το [4] υπάρχει μείωση του κόστους κατά 44 % αναφορικά με τη διαχείριση του δικτύου, 34% αναφορικά με τον εξοπλισμό και τη συντήρηση του και 22% αναφορικά με τις διασυνδέσεις με το δίκτυο κορμού και άλλα εναλλακτικά δίκτυα (βλέπε Σχήμα 1–1). Βασικό στοιχείο της ανάπτυξης των υπηρεσιών τηλεφωνίας μέσω του διαδικτύου είναι και το χαμηλό κόστος πρόσβασης που παρέχεται στους χρήστες μέσω των ευρυζωνικών συνδέσεων. Επιπροσθέτως, χαρακτηριστικό της δυναμικής που εμφανίζει η αγορά στο συγκεκριμένο χώρο είναι το γεγονός ότι αν και μέχρι σήμερα οι χρήστες υπηρεσιών IP τηλεφωνίας δεν ξεπερνούν το ένα εκατομμύριο, αναμένεται ότι το 2012 θα ξεπερνούν τα δώδεκα εκατομμύρια [5].



Σχήμα 1–1. Μείωση τηλεπικοινωνιακών δαπανών με την αξιοποίηση του διαδικτύου

Η υπηρεσία της τηλεφωνίας, με την αξιοποίηση του διαδικτύου ως δικτύου κορμού εισέρχεται σε μια νέα εποχή όπως προαναφέρθηκε, με το ενδιαφέρον των τηλεπικοινωνιακών οργανισμών για την αξιοποίηση της συγκεκριμένης λύσης να αυξάνεται συνεχώς. Πέρα από τη δυναμική που εμφανίζει η IP τηλεφωνία, το PSTN καθ' όλη τη διάρκεια λειτουργίας του έχει αποδείξει ότι μπορεί να υποστηρίξει υπηρεσίες με υψηλές απαιτήσεις αξιοπιστίας, διαθεσιμότητας και ασφάλειας, κερδίζοντας έτσι την εμπιστοσύνη της πλειοψηφίας των χρηστών. Συνεπώς, για την καθιέρωση της IP τηλεφωνίας ως de-facto επικοινωνιακού μέσου, θα πρέπει, μεταξύ των άλλων, να εξασφαλιστούν αντίστοιχα επίπεδα αξιοπιστίας, διαθεσιμότητας και ασφάλειας. Αυτό είναι ιδιαίτερα σημαντικό για το περιβάλλον του διαδικτύου αφού θεωρείται ένα μη «φιλικό» δίκτυο με γνωστές απειλές και ευπάθειες που μεταφέρονται αυτόματα σε όλες τις υπηρεσίες που το αξιοποιούν ως μέσο παροχής υπηρεσιών.

1.2 Ερευνητική Περιοχή

Έχει παρατηρηθεί ότι πάρα πολλές φορές κατά τη διαδικασία σχεδίασης ενός πληροφοριακού συστήματος τα θέματα ασφαλείας δε λαμβάνονται υπόψη. Το ίδιο συμβαίνει και κατά τη σχεδίαση των συστημάτων τηλεφωνίας, ανεξαρτήτως αν πρόκειται για υπηρεσίες βασισμένες στο PSTN ή στο IP. Η κύρια διαφορά μεταξύ τους εντοπίζεται στην αξιοποίηση συστημάτων κλειστής (PSTN) ή ανοιχτής (IP τηλεφωνία) αρχιτεκτονικής για την παροχή των υπηρεσιών φωνής, με τα όποια πλεονεκτήματα και μειονεκτήματα της κάθε λύσης.

Η αξιοπιστία και ασφάλεια που σήμερα προσφέρει το PSTN βασίζεται στη χρήση των κλειστών αρχιτεκτονικών και συστημάτων [6]. Μεταξύ των πιο γνωστών περιστατικών ανασφάλειας που έχουν καταγραφεί σε δίκτυα σταθερής τηλεφωνίας είναι οι υποκλοπές συνδιαλέξεων (wiretapping), οι οποίες απαιτούν φυσική πρόσβαση στον εξοπλισμό του PSTN, καθώς και οι κλήσεις χωρίς χρέωση οι οποίες εμφανίστηκαν στα εσωζωνικά συστήματα σηματοδοσίας όπου ο επιτιθέμενος έστελνε στο τοπικό τηλεφωνικό κέντρο (Local Exchange Center–(LEC)) συγκεκριμένους τόνους σηματοδοσίας προσποιούμενος ότι η κλήση έχει τερματιστεί ενώ στην πραγματικότητα ο χρήστης συνέχιζε την ομιλία του χωρίς χρέωση [7]. Παρ' όλα αυτά, σε γενικές γραμμές θα μπορούσε να επισημανθεί ότι στο PSTN η συμπεριφορά των χρηστών είναι ελεγχόμενη και καλά προκαθορισμένη.

Από την άλλη πλευρά στα δίκτυα ανοικτής αρχιτεκτονικής οι πιθανές συμπεριφορές των χρηστών δεν είναι πάντα προβλέψιμες, ενώ υπάρχει μεγαλύτερη πολυπλοκότητα και δυσκολία στον έλεγχο των. Επιπροσθέτως, τα δίκτυα αυτά, όπως για παράδειγμα το διαδίκτυο, υποφέρουν τόσο από προβλήματα αξιοπιστίας κατά την μετάδοση των δεδομένων όσο και από ένα πλήθος άλλων ευρέως γνωστών προβλημάτων ασφαλείας. Όλα αυτά τα

προβλήματα κληρονομούνται από οποιαδήποτε υπηρεσία αξιοποιεί το διαδίκτυο, ενώ γίνονται ιδιαιτέρως αισθητά σε υπηρεσίες πραγματικού χρόνου όπως αυτή της τηλεφωνίας. Επιπλέον, οι επιτιθέμενοι αναζητώντας νέους τομείς εξερεύνησης ελκύονται από ανερχόμενες τεχνολογίες ανακαλύπτοντας νέα κενά ασφαλείας τα οποία δεν είχαν εμφανιστεί σε προγενέστερες υπηρεσίες.

Κατά συνέπεια, κατά τον σχεδιασμό συστημάτων IP τηλεφωνίας θα πρέπει να ληφθούν υπόψη όλα τα πιθανά τρωτά σημεία που είναι δυνατόν να δημιουργήσουν προβλήματα αξιοπιστίας και διαθεσιμότητας, με στόχο το σχεδιασμό των κατάλληλων μηχανισμών που θα είναι σε θέση να αντιμετωπίσουν τα αντίστοιχα προβλήματα ασφαλείας σε δίκτυα ανοιχτής αρχιτεκτονικής, όπως το διαδίκτυο, λαμβάνοντας πάντα υπόψη τις ιδιαιτερότητες της IP τηλεφωνίας. Θα πρέπει να τονιστεί ότι η αξιοποίηση υπαρχόντων μηχανισμών ασφαλείας στην αρχιτεκτονική της IP τηλεφωνίας απαιτεί, πρώτα, μελέτη για τη διερεύνηση της καταλληλότητας εφαρμογής των. Υπό το πρίσμα αυτό μελετώνται, αναλύονται και αξιολογούνται μηχανισμοί ασφαλείας που χρησιμοποιούνται στην IP τηλεφωνία, ενώ σε όσες περιπτώσεις απαιτείται, προτείνονται εναλλακτικοί ή/και επιπρόσθετοι μηχανισμοί για την περαιτέρω βελτίωση της ρωμαλεότητας των υπηρεσιών αυτής της κατηγορίας.

1.3 Περιγραφή του Προβλήματος

Τα αρχικά συστήματα IP τηλεφωνίας ήταν κλειστά δίκτυα και αξιοποιούσαν το εξωζωνικό σύστημα σηματοδοσίας SS7, το οποίο σχεδιάστηκε για χρήση σε τέτοιου τύπου δίκτυα και παράλληλα χρησιμοποιήθηκε για τη δημιουργία υποβοηθητικών υπηρεσιών σε συνδυασμό με άλλα πρωτόκολλα ώστε να είναι δυνατή η ενοποίηση διαφορετικών τμημάτων του δικτύου τηλεφωνίας. Η μεταφορά του SS7 σε δίκτυα ανοικτής αρχιτεκτονικής, όπως αυτή του διαδικτύου, δημιούργησε αρκετό προβληματισμό καθώς απαιτεί αξιόπιστη μετάδοση μηνυμάτων χωρίς καθυστερήσεις. Τα πρωτόκολλά που είχαν σχεδιαστεί για το διαδίκτυο δε μπορούσαν να καλύψουν τις ανάγκες αυτές και για το λόγο αυτό σχεδιάστηκε ένα νέο πρωτόκολλο μεταφοράς, συγκεκριμένα το Stream Control Transport Protocol (SCTP) [8], ώστε να καταστεί δυνατή η χρήση του SS7 στο διαδίκτυο. Παρ' όλα αυτά, μέχρι πρότινος το SCTP δεν υλοποιείται ως μέρος του λειτουργικού συστήματος, όπως το Transport Control Protocol (TCP) [9], μη παρέχοντας έτσι τη δυνατότητα δημιουργίας τηλεφώνων που θα βασίζονται στο IP αξιοποιώντας το SS7. Η λύση αυτή θεωρείται κατάλληλη κυρίως για διασυνδέσεις μεταξύ τηλεφωνικών κέντρων μέσω IP δικτύων.

Ως εκ τούτου εναλλακτικά πρωτόκολλα σηματοδοσίας τα οποία θα επικεντρώνονται στις ιδιαιτερότητες του διαδικτύου, παρέχοντας ταυτόχρονα αντίστοιχες υπηρεσίες με αυτές του SS7, θεωρήθηκαν αναγκαία. Μεταξύ των διαφορετικών πρωτοκόλλων που προτάθηκαν, τα δύο επικρατέστερα είναι το H.323 [10] και το Session Initiation Protocol (SIP) [11]. Πιο συγκεκριμένα, το H.323 σχεδιάστηκε από την ITU-T και δεν αποτελεί ένα απλό πρωτόκολλο, αλλά ένα σύνολο πρωτοκόλλων, όμοιο του SS7, σχεδιασμένο με γνώμονα όχι μόνο την αρχιτεκτονική του διαδικτύου αλλά και το σταθερό τηλεφωνικό δίκτυο ώστε να είναι δυνατή η παροχή νέων υπηρεσιών με την αξιοποίηση του διαδικτύου ή ενός IP δικτύου. Το H.323 [10] ουσιαστικά αποτελεί ένα ολοκληρωμένο «οριζόντιο» σύστημα. Αυτό δημιουργεί αρκετά μεγάλη δυσκολία στην εφαρμογή του σε αρχιτεκτονικές πλην αυτής που έχει σχεδιαστεί, καθώς και στην ανάπτυξη νέων υπηρεσιών.

Από την άλλη πλευρά το SIP [11] σχεδιάστηκε από την Internet Engineering Task Force (IETF) και χρησιμοποιεί μια εντελώς διαφορετική προσέγγιση σε ότι αφορά τον τρόπο σηματοδοσίας στο διαδίκτυο. Η διαφορετικότητα αυτή οφείλεται κυρίως στα στοιχεία που κληρονομεί το SIP [11] από πρωτόκολλα που έχουν αξιοποιηθεί επιτυχώς στο διαδίκτυο όπως το Hyper Text Transport Protocol (HTTP) [12]. Το γεγονός αυτό το καθιστά πολύ πιο

απλό όχι μόνο στη διαχείριση πολυμεσικών συνόδων (multimedia sessions) αλλά και στη δημιουργία νέων υπηρεσιών τηλεφωνίας. Ουσιαστικά το SIP, σε αντίθεση με το H.323, αποτελεί ένα από τα δομικά στοιχεία των υπηρεσιών IP τηλεφωνίας παρέχοντας δυνατότητες αξιοποίησης του σε συνδυασμό με άλλα πρωτόκολλα ανοιχτών προδιαγραφών που μπορούν να εφαρμοστούν ή εφαρμόζονται στο διαδίκτυο. Εξαιτίας της ευελιξίας αυτής και της απλότητας ανάπτυξης νέων υπηρεσιών που βασίζονται στο SIP, φαίνεται ότι κυριαρχεί έναντι του H.323. Επιπλέον έχει ενσωματωθεί ως πρωτόκολλο σηματοδοσίας στην αρχιτεκτονική της 3^{ης} γενεάς κινητών επικοινωνιών στο υποσύστημα πολυμέσων IP (IP Multimedia Subsystem (IMS)) το οποίο το καθιστά ως κυρίαρχο πρωτόκολλο σηματοδοσίας για τα δίκτυα επόμενης γενεάς (Next Generation Networks-(NGNs)) . Εκτενής σύγκριση μεταξύ αυτών των δύο πρωτοκόλλων σηματοδοσίας παρουσιάζεται στις εργασίες [13],[14].

Η έλευση των διαδικτυακών πρωτοκόλλων σηματοδοσίας έδωσε νέα ώθηση στις υπηρεσίες τηλεφωνίας και επέτρεψε την ανάπτυξη εξελιγμένων υπηρεσιών [15] όπως κλήσεις μέσω διαδικτυακών ιστοτόπων, τηλεσυνδιάσκεψης κτλ., ταυτόχρονα όμως δημιούργησε νέα προβλήματα κυρίως κατά την μετάδοση της φωνής, όπως ηχώ (echo), καθυστέρηση μετάδοσης (delay), ποιότητα προσφερόμενης υπηρεσίας (Quality of Service) που απαιτούν λύσεις [16]. Τα προβλήματα αυτά παρουσιάζονται κυρίως λόγω της αναξιόπιστης μετάδοσης, παράδοσης και παραλαβής, που υπάρχει στο διαδίκτυο. Τα συγκεκριμένα προβλήματα αντιμετωπίστηκαν με επιτυχία αναπτύσσοντας εναλλακτικά συστήματα κωδικοποίησης φωνής [16]. Στη συνέχεια όμως, άρχισαν να εμφανίζονται σοβαρά προβλήματα ασφαλείας τα οποία είναι άμεσα συσχετισμένα με τη χρήση ανοικτών – μη ασφαλών επικοινωνιακών υποδομών και τα οποία μέχρι και σήμερα διερευνώνται από την επιστημονική κοινότητα.

Το διαδίκτυο, ως το πλέον αντιπροσωπευτικό παράδειγμα δικτύου ανοιχτής αρχιτεκτονικής, δημιουργεί ένα μη έμπιστο περιβάλλον το οποίο πέραν των πολλών προβλημάτων ασφαλείας, προσφέρει και νέες δυνατότητες εκδήλωσης επιθέσεων από κακόβουλους χρήστες. Είναι λοιπόν βέβαιο ότι η IP τηλεφωνία κληρονομεί όλα τα γνωστά προβλήματα ασφαλείας και όλες τις ευπάθειες που υπάρχουν στο διαδίκτυο, ενώ παράλληλα δημιουργεί νέες ευπάθειες σε ολόκληρο το τηλεφωνικό δίκτυο.

Σε αντίθεση με το PSTN, στο διαδίκτυο η μη εξουσιοδοτημένη πρόσβαση στα διακινούμενα δεδομένα (ανεξαρτήτως του τύπου) είναι άμεση και χωρίς συγκεκριμένους περιορισμούς κάτι που έχει σαν αποτέλεσμα την εύκολη και χωρίς ιδιαίτερα υψηλό κόστος αποκάλυψη ή τροποποίηση των δεδομένων αυτών. Κακόβουλοι χρήστες μπορούν να αξιοποιήσουν διάφορα εργαλεία ανοιχτού κώδικα [17] για να δημιουργήσουν ποικίλα προβλήματα στην προσφερόμενη υπηρεσία. Για παράδειγμα, κάποιος κακόβουλος χρήστης είναι δυνατόν να προσπαθήσει να εκμεταλλευτεί κάποια λανθασμένη διαμόρφωση (configuration) του διαδικτυακού τηλεφωνικού δικτύου, προκειμένου να επιτύχει μη εξουσιοδοτημένη πρόσβαση σε αυτό [18]. Εναλλακτικά μπορεί να δημιουργήσει αναρίθμητες αιτήσεις κλήσεων με στόχο να προκαλέσει πρόβλημα στον εξυπηρέτη που επεξεργάζεται τα αιτήματα κλήσεων και να επιτύχει άρνηση παροχής υπηρεσίας (Denial of Service). Είναι σκόπιμο να επισημανθεί ότι τέτοιου είδους προβλήματα μεταφέρονται αυτόματα και στην κλασική υπηρεσία τηλεφωνίας καθώς πλέον τα συστήματα είναι διασυνδεδεμένα μεταξύ τους.

1.4 Σημαντικότητα του Προβλήματος

Η εύκολη πρόσβαση σ’ ένα IP δίκτυο καταλύει σε μεγάλο βαθμό την έννοια της εμπιστευτικότητας των κλήσεων που διεκπεραιώνονται μέσω διαδικτύου. Για παράδειγμα όλα τα δεδομένα σηματοδοσίας αποστέλλονται σε καθαρή μορφή (clear text) με αποτέλεσμα ένας επιτιθέμενος να μπορεί να γνωρίζει τόσο τις οντότητες που επικοινωνούν μεταξύ τους,

όσο και τις παραμέτρους μιας συνόδου. Οι παράμετροι αυτοί είναι δυνατόν να αξιοποιηθούν για την υλοποίηση μια άλλης επίθεσης. Επιπλέον, η κατάλυση της ακεραιότητας των μηνυμάτων σηματοδοσίας οδηγεί είτε σε αδυναμία αποκατάστασης μιας συνόδου μεταξύ δύο ή περισσότερων οντοτήτων, είτε στη δρομολόγηση των συνόδων σε μη εξουσιοδοτημένες οντότητες. Αντιστοίχως, η εξάντληση των υπολογιστικών πόρων της παρεχόμενης υπηρεσίας, λόγω απρόσμενης κίνησης, μπορεί να δημιουργήσει προβλήματα αδυναμίας αποκατάστασης συνόδων.

Αξίζει να σημειωθεί ότι η άρνηση παροχής υπηρεσιών θεωρείται σήμερα ως μη αποδεκτή από τους χρήστες, δεδομένης της σχεδόν μόνιμα διαθέσιμης συμβατικής τηλεφωνικής υποδομής. Επιπροσθέτως, η αξιοποίηση των ιδίων πρωτοκόλλων και συστημάτων στα δίκτυα κινητής τηλεφωνίας 3ής γενεάς (3G) καθώς και η γενικότερη ενοποίηση των δικτύων, καθιστούν επιτακτική την ανάγκη εντοπισμού και αντιμετώπισης περιστατικών ανασφάλειας που θα εμφανιστούν στην IP τηλεφωνία καθώς έχουν άμεσα αντίκτυπο στη διαθεσιμότητα και αξιοπιστία των προσφερόμενων υπηρεσιών και κατ' επέκταση στην εμπιστοσύνη που αναπτύσσουν προς τις υπηρεσίες αυτές οι χρήστες, ενώ σε πολλές περιπτώσεις βάλλονται περιφερειακές υπηρεσίες, όπως η υπηρεσία χρεώσεων (billing service), ή ακόμα και οι τελικοί χρήστες.

1.5 Στόχος της Διδακτορικής Διατριβής

Στόχος της διδακτορικής αυτής διατριβής είναι η δημιουργία ενός ενιαίου πλαισίου ασφαλείας το οποίο θα μπορεί να αξιοποιηθεί για την ανίχνευση, αποτροπή και αντιμετώπιση επιθέσεων σε υπηρεσίες διαδικτυακής τηλεφωνίας. Συγκεκριμένα, οι επιμέρους στόχοι είναι:

Α) Ο εντοπισμός ευπαθειών και δυνητικών επιθέσεων κατά των υπηρεσιών IP τηλεφωνίας.

Β) Η αποτίμηση των ήδη υπαρχόντων μηχανισμών ασφαλείας κατά την εφαρμογή τους σε υπηρεσίες IP τηλεφωνίας.

Γ) Ο σχεδιασμός, η υλοποίηση και η αξιολόγηση αντιμέτρων για περιπτώσεις που οι ήδη υπάρχοντες μηχανισμοί ασφαλείας δεν καλύπτουν τις ιδιαίτερες απαιτήσεις των υπηρεσιών IP τηλεφωνίας.

Δ) Η εξασφάλιση διαλειτουργικότητας, σε θέματα ασφαλείας, μεταξύ διαφορετικών παρόχων IP τηλεφωνίας.

1.6 Συνεισφορά στο Ερευνητικό Πεδίο

Η κύρια ερευνητική συνεισφορά της διατριβής είναι η ανάπτυξη ενός ολοκληρωμένου πλαισίου ασφαλείας για υπηρεσίες IP τηλεφωνίας. Βέβαια, τα επιμέρους αποτελέσματα που έχουν προκύψει δεν αξιοποιούνται μόνο στον σχεδιασμό, υλοποίηση και αποτίμηση του προτεινόμενου πλαισίου, αλλά συμβάλουν και στην ενημέρωση της επιστημονικής κοινότητας και του ευρύτερου κοινού, αναφορικά με τα ακόλουθα:

- Προβλήματα ασφαλείας, απειλές, ευπάθειες και επιθέσεις που άπτονται των υπηρεσιών IP τηλεφωνίας. Περιγράφονται και αναλύονται λεπτομερώς οι τρόποι με τους οποίους ένας κακόβουλος χρήστης θα μπορούσε να:
  - υποκλέψει ιδιωτικές πληροφορίες σχετικά με τις οντότητες που επικοινωνούν.
  - τροποποιήσει τα δεδομένα των χρηστών που αποθηκεύονται από τον πάροχο της υπηρεσίας,

  - πραγματοποιεί κλήσεις χωρίς χρέωση.
  - τερματίσει κλήσεις χωρίς εξουσιοδότηση.
  - δημιουργήσει καταστάσεις άρνησης παροχής υπηρεσιών.
- Αποτίμηση των ήδη εφαρμοζόμενων μηχανισμών ασφαλείας σε υπηρεσίες IP τηλεφωνίας.
- Μέθοδοι ανίχνευσης – αντιμετώπισης προβλημάτων ασφαλείας σε υπηρεσίες IP τηλεφωνίας.
- Χρήση οντολογιών για την ενιαία αναπαράσταση των απαιτήσεων ασφαλείας.

Πιο συγκεκριμένα, αρχικά διερευνώνται τα τρωτά σημεία των υπηρεσιών IP τηλεφωνίας κατά τη διαδικασία αποκατάστασης συνόδων [19]. Ταυτόχρονα μελετάται η αποτελεσματικότητα των μηχανισμών ασφάλειας που είναι σήμερα διαθέσιμοι [20]. Στη συνέχεια πραγματοποιείται εξομοίωση γνωστών επιθέσεων κατά υπηρεσιών IP τηλεφωνίας, αναπτύσσοντας ένα εξειδικευμένο εργαλείο στα πλαίσια του ερευνητικού έργου SNOCER [21], με στόχο να διαπιστωθεί η εφικτότητα τους. Ακολούθως αφού έχουν καταγραφεί οι πιθανές επιθέσεις και έχουν προσδιοριστεί οι βασικοί λόγοι εμφάνισης τους, προτείνεται μια σειρά από νέες τεχνικές,[22]–[27] για την αντιμετώπιση τους. Επιπροσθέτως αξιοποιούνται οντολογίες για να επιτευχθεί μια ενιαία περιγραφή των προβλημάτων και απαιτήσεων ασφαλείας της IP τηλεφωνίας, με απώτερο σκοπό την ανάπτυξη ενός ομοιόμορφου συνεργατικού περιβάλλοντος ασφαλείας [28],[29] μεταξύ διαφορετικών παρόχων υπηρεσιών IP τηλεφωνίας.

Ο Πίνακας 1–1 αποτυπώνει συνοπτικά την ερευνητική συνεισφορά της διατριβής, με βάση τους στόχους που παρουσιάστηκαν στην ενότητα 1.5.

Στόχος	Σύντομη περιγραφή	Συνεισφορά
Α	Εντοπισμός ευπαθειών και δυνητικών επιθέσεων σε υπηρεσίες IP τηλεφωνίας.	[19]
Β	Αποτίμηση υπαρχόντων μηχανισμών ασφαλείας.	[20]
Γ	Σχεδιασμός, υλοποίηση και αξιολόγηση κατάλληλων αντιμέτρων για την προστασία των υπηρεσιών IP τηλεφωνίας.	[22]–[27]
Δ	Παροχή υπηρεσιών διαλειτουργικότητας σε θέματα ασφάλειας μεταξύ διαφορετικών παρόχων IP τηλεφωνίας.	[28],[29]

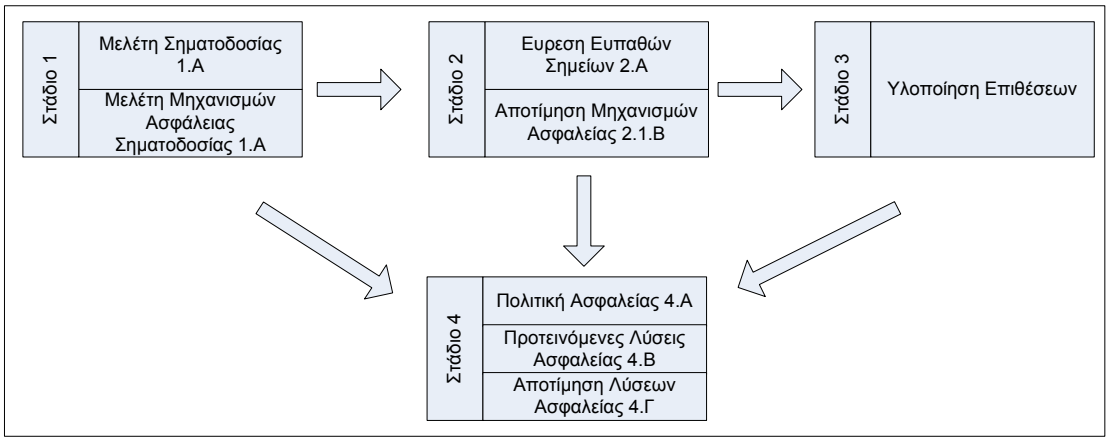
Πίνακας 1–1. Συνοπτική Παρουσίαση Ερευνητικών Αποτελεσμάτων

Τονίζεται ότι η ερευνητική εργασία που παρουσιάζεται στην παρούσα διατριβή εστιάζει στο πρωτόκολλο σηματοδοσίας SIP. Η επιλογή αυτή έχει βασιστεί στο γεγονός ότι το συγκεκριμένο πρωτόκολλο έχει καθιερωθεί ως το de-facto πρωτόκολλο για την διαδικτυακή τηλεφωνία ενώ θεωρείται το πρωτόκολλο σηματοδοσίας της Επόμενης Γενεάς Δικτύων. Βέβαια αντίστοιχα προβλήματα ασφάλειας, ίσως με μικρές διαφοροποιήσεις, εντοπίζονται και στα άλλα πρωτόκολλα σηματοδοσίας κάτι που σημαίνει ότι η αξιοποίηση των αποτελεσμάτων της παρούσας δεν περιορίζεται στο πρωτόκολλο SIP.

1.7 Μεθοδολογία Προσέγγισης του Προβλήματος

Για την επίτευξη των προαναφερόμενων στόχων η ερευνητική μας εργασία εκπονήθηκε σε τέσσερα διακριτά στάδια. Στο πρώτο στάδιο μελετήθηκαν διεξοδικά τα πρωτόκολλα

σηματοδοσίας και οι αξιοποιούμενοι μηχανισμοί ασφαλείας για υπηρεσίες IP τηλεφωνίας. Στη συνέχεια διερευνήθηκε η ύπαρξη νέων ευπαθειών που θα επέτρεπαν την εμφάνιση νέων τύπων επιθέσεων με στόχο να πλήξουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των παρεχόμενων υπηρεσιών. Ταυτόχρονα, στο δεύτερο αυτό στάδιο, γίνεται και η αποτίμηση της αποτελεσματικότητας των μηχανισμών ασφαλείας που είχαν καταγραφεί στο πρώτο στάδιο. Στο τρίτο στάδιο υλοποιούνται οι επιθέσεις που εντοπίστηκαν κατά το δεύτερο στάδιο, με στόχο να γίνει δυνατή η ακριβέστερη και λεπτομερέστερη ανάλυση των ευπαθειών που επιτρέπουν την εκδήλωση των συγκεκριμένων επιθέσεων. Στο τέταρτο και τελευταίο στάδιο σχεδιάζονται, υλοποιούνται και αποτιμώνται οι εναλλακτικές λύσεις που προτείνονται, υπό το πρίσμα μια ενιαίας και ομοιόμορφης περιγραφής, για την ανίχνευση, αντιμετώπιση ή / και αποτροπή πιθανών κακόβουλων ενεργειών. Η προαναφερόμενη διαδικασία αποτυπώνεται στο Σχήμα 1–2.



Σχήμα 1–2. Μεθοδολογική Προσέγγιση

1.8 Δομή της Διατριβής

Εκτός του παρόντος εισαγωγικού κεφαλαίου, η διατριβή υποστηρίζεται με τη συγγραφή άλλων οκτώ κεφαλαίων. Στο Κεφάλαιο που ακολουθεί γίνεται επισκόπηση των υπαρχόντων τηλεφωνικών υποδομών και υπηρεσιών. Στο Κεφάλαιο 3 πραγματοποιείται εκτενής παρουσίαση των υπηρεσιών διαδικτυακής τηλεφωνίας με ιδιαίτερη έμφαση στο πρωτόκολλο σηματοδοσίας SIP. Στο Κεφάλαιο 4 περιγράφονται αναλυτικά οι απειλές και οι επιθέσεις που δύναται να εκδηλωθούν προς τις υπηρεσίες που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP. Στο Κεφάλαιο 5 προσδιορίζονται οι απαιτήσεις ασφαλείας που θα πρέπει να καλύπτονται από τις υπηρεσίες διαδικτυακής τηλεφωνίας και αξιολογούνται οι μηχανισμοί ασφαλείας που προτείνονται από τις προδιαγραφές του SIP. Στο Κεφάλαιο 6 παρουσιάζονται οι συμπληρωματικοί μηχανισμοί που έχουν προταθεί για την ενδυνάμωση των υπηρεσιών ασφαλείας και του επιπέδου προστασίας της διαδικτυακής τηλεφωνίας. Ακολούθως, στο Κεφάλαιο 7, περιγράφεται και αξιολογείται μια ολοκληρωμένη αρχιτεκτονική για την εφαρμογή των κατάλληλων προληπτικών, ανασταλτικών και αναγνωριστικών μηχανισμών ασφαλείας για τις υπηρεσίες διαδικτυακής τηλεφωνίας. Εν συνεχεία, στο Κεφάλαιο 8, αξιοποιούνται οντολογίες για την αναπαράσταση, υπό το πρίσμα ενός ενιαίου τυπικού μοντέλου ασφάλειας, των επιθέσεων που μπορεί να εκδηλωθούν κατά των υπηρεσιών διαδικτυακής τηλεφωνίας, με απώτερο σκοπό την επίτευξη διαλειτουργικότητας μεταξύ διαφορετικών παρόχων.

ΚΕΦΑΛΑΙΟ 2: Υπάρχουσα Υποδομή Τηλεφωνικών Δικτύων & Υπηρεσιών

2.1 Γενικά

Οι εξελίξεις στον τομέα των τηλεπικοινωνιών επηρέασε σε μεγάλο βαθμό τον τρόπο και το είδος των τηλεφωνικών υπηρεσιών που παρέχονται από τους τηλεπικοινωνιακούς παρόχους. Από τα πρώτα τηλεφωνικά συστήματα στα τέλη τις δεκαετίας του 1880, τα οποία ήταν γεωγραφικά περιορισμένα σε περιοχές της Αμερικής, φτάνουμε στις σημερινές ευρυζωνικές συνδέσεις, οι οποίες αξιοποιούνται παγκοσμίως για μεταφορά όχι μονό φωνής (voice) αλλά και δεδομένων (data). Σε αυτό το γεγονός συμβάλει σημαντικά η ραγδαία ανάπτυξη των υπολογιστικών συστημάτων η οποία έφερε στο προσκήνιο την ανάγκη της μεταξύ των αδιάλειπτης επικοινωνίας. Η έλευση των τοπικών δικτύων έδωσε ακόμη περισσότερη ώθηση στις τεχνικές διασύνδεσης, η οποία κατά ένα μέρος ολοκληρώνεται με την καθιέρωση του διαδικτύου ως τηλεπικοινωνιακού μέσου. Το διαδίκτυο αποτελεί ουσιαστικά το εργαλείο που μπορεί να αξιοποιηθεί για χαμηλού κόστους αδιάλειπτη επικοινωνία [30] μεταξύ διαφορετικών δικτύων για την παροχή ολοκληρωμένων υπηρεσιών.

Στη συνέχεια του κεφαλαίου αυτού παρουσιάζονται οι βασικές αρχές μεταγωγής που αξιοποιούνται από τα τηλεπικοινωνιακά συστήματα σήμερα, καθώς ο τρόπος λειτουργίας των τηλεφωνικών συστημάτων επηρεάζεται σε μεγάλο βαθμό από αυτές. Ακολούθως πραγματοποιείται σύντομη επισκόπηση των διαφορετικών αρχιτεκτονικών και των δομικών στοιχείων που αξιοποιούνται, τόσο στο PSTN όσο και στο διαδίκτυο, για την παροχή υπηρεσιών φωνής.

2.2 Βασικές Έννοιες Μεταγωγής

2.2.1 Τεχνικές Μεταγωγής Δεδομένων

Τα τηλεπικοινωνιακά δίκτυα μπορούν να κατηγοριοποιηθούν, μεταξύ των άλλων, με βάση τις τεχνικές προώθησης των δεδομένων, ή εναλλακτικά των τεχνικών μεταγωγής (Switching Techniques), που αξιοποιούνται τόσο για την ορθή δρομολόγηση από ένα τερματικό κόμβο προς ένα άλλο όσο και για τον καλύτερο διαμοιρασμό (sharing) των τηλεπικοινωνιακών καναλιών μεταξύ των χρηστών. Οι πλέον ευρέως γνωστές τεχνικές μεταγωγής δεδομένων είναι οι ακόλουθες:

- Μεταγωγή κυκλώματος (circuit switching)
- Μεταγωγή πακέτων (packet switching)

2.2.1.1 Μεταγωγή Κυκλώματος

Η μεταγωγή κυκλώματος θεωρείται η πιο διαδεδομένη τεχνική μεταγωγής καθώς αξιοποιείται στο PSTN. Στην τεχνική αυτή το επικοινωνιακό κανάλι, που απαιτείται για τη μετάδοση των δεδομένων μεταξύ δύο ή περισσότερων οντοτήτων, δεσμεύεται αποκλειστικά για τη συγκεκριμένη επικοινωνία, χωρίς να υπάρχει η δυνατότητα διαμοιρασμού του από άλλες οντότητες, ανεξαρτήτως του ποσοστού χρήσης (utilization) του καθ' όλη τη διάρκεια της επικοινωνίας.

2.2.1.2 Μεταγωγή πακέτων

Η μεταγωγή πακέτων αξιοποιείται ευρέως στα δίκτυα δεδομένων. Στην τεχνική αυτή το κάθε μήνυμα κατακερματίζεται σε μικρότερα τμήματα (πακέτα), τα οποία μεταδίδονται είτε μετά την αποκατάσταση μιας ιδεατής σύνδεσης (virtual circuit), είτε με την ασυνδεσμική (connectionless) μετάδοση κάθε πακέτου, δηλαδή χωρίς να απαιτείται η προ-εγκατάσταση σύνδεσης για τη δρομολόγηση του, όπως στις ιδεατές συνδέσεις. Στις περιπτώσεις που χρησιμοποιείται ιδεατή σύνδεση τα δεδομένα δρομολογούνται πάντα μέσω της ίδιας διαδρομής. Αντιθέτως, στην ασυνδεσμική μετάδοση τα πακέτα δρομολογούνται αυτόνομα, χωρίς να αξιοποιείται απαραίτητα η ίδια διαδρομή.

Για την αποφυγή 'συγχύσεων' μεταξύ ιδεατού καναλιού και μεταγωγής κυκλώματος, θα πρέπει να διευκρινιστεί ότι στην πρώτη περίπτωση το κάθε πακέτο επεξεργάζεται και αποθηκεύεται προσωρινά σε κάθε κόμβο πριν αποσταλεί στον επόμενο κόμβο, επιλέγοντας το ίδιο μονοπάτι δρομολόγησης, ενώ στη δεύτερη περίπτωση η μετάδοση πραγματοποιείται άμεσα μεταξύ των επικοινωνούντων κόμβων χωρίς να πραγματοποιείται επεξεργασία από τους ενδιάμεσους.

2.3 Το Δημόσιο Τηλεφωνικό Δικτύο Μεταγωγής – PSTN

Το PSTN θεωρείται ως το μεγαλύτερο αναπτυγμένο τηλεπικοινωνιακό δίκτυο παγκοσμίως. Για την επικοινωνία μεταξύ δύο ή περισσότερων χρηστών απαιτείται η δέσμευση μίας διαθέσιμης γραμμής (trunk) καθ' όλη τη χρονική διάρκεια της επικοινωνίας είτε αυτό αξιοποιείται είτε όχι (μεταγωγή κυκλώματος). Αποτέλεσμα αυτής της μεθόδου μετάδοσης των δεδομένων είναι η αξιοποίηση (utilization) του δεσμευμένου καναλιού μόνο κατά το 10-25% του συνολικού όγκου των δεδομένων που μπορούν να μεταδοθούν μέσω αυτού [1].

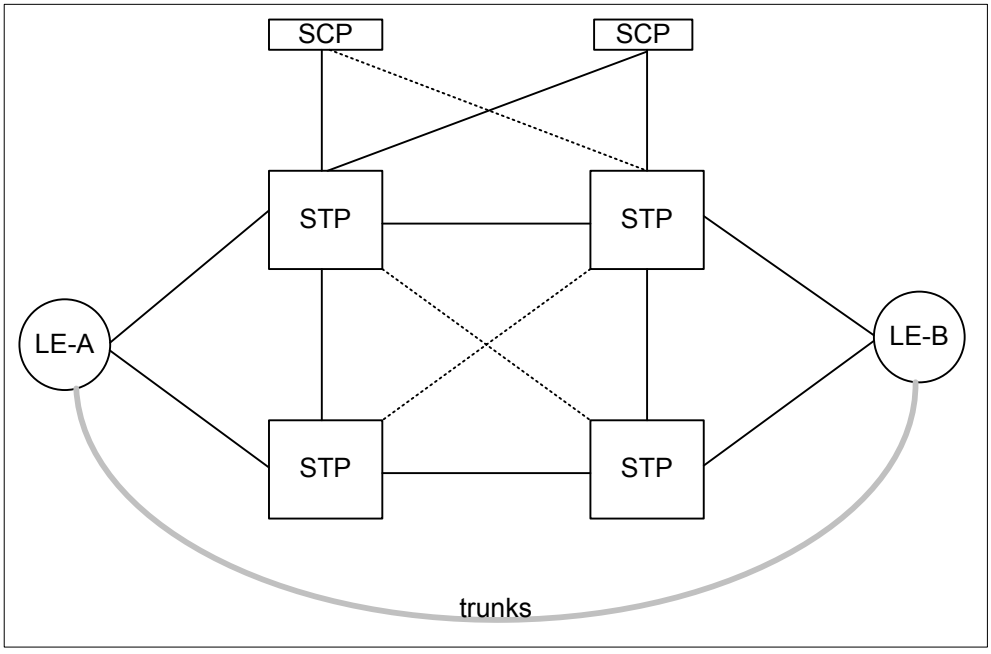
Για την αποκατάσταση μίας σύνδεσης και συνεπώς τη δέσμευση της γραμμής απαιτείται η αξιοποίηση των κατάλληλων συστημάτων σηματοδοσίας. Αρχικά χρησιμοποιήθηκαν εσωζωνικά σύστημα όπου απαιτούσαν την αρχική δέσμευση του καναλιού και όλων των απαραίτητων πόρων για την πραγματοποίηση της επικοινωνίας μεταξύ των χρηστών, ανεξαρτήτως της διαθεσιμότητας του καλούμενου. Σε αυτά τα συστήματα όλες οι πληροφορίες σηματοδοσίας μεταδιδόταν μέσω του δεσμευμένου καναλιού. Εξαιτίας όμως της αναξιοπιστίας αυτών των συστημάτων αλλά και των προβλημάτων ασφαλείας που παρουσιάστηκαν μετέπειτα σε αυτά [31], προτάθηκε η αξιοποίηση ενός διαφορετικού δικτύου για τη μετάδοση των δεδομένων σηματοδοσίας. Ουσιαστικά, προτάθηκε η εξωζωνική μετάδοση των δεδομένων σηματοδοσίας, δηλαδή η χρήση διαφορετικού καναλιού και όχι μέσω του καναλιού μετάδοσης φωνής.

Πιο συγκεκριμένα, σε αυτή την περίπτωση δεν απαιτείται η αρχική δέσμευση του καναλιού, αλλά το δίκτυο σηματοδοσίας (signalling network) είναι επιφορτισμένο για τον εντοπισμό του καλούμενου και εφόσον είναι διαθέσιμος πραγματοποιείται η δέσμευση του καναλιού για την επίτευξη της επικοινωνίας. Με τη μέθοδο αυτή δε βελτιώθηκαν μόνο ο χρόνος αποκατάστασης των συνδέσεων, αλλά και ο έλεγχος-επίβλεψη (monitoring) των κλήσεων. Ταυτόχρονα όμως, είναι δυνατή η παροχή επιπρόσθετων υπηρεσιών όπως αναμονή κλήσης, προώθηση κλήσης κ.α. Αξιοσημείωτο είναι το γεγονός ότι για κανάλι σηματοδοσίας με ταχύτητα μετάδοσης 2400bits/sec είναι δυνατή η επίβλεψη μέχρι και 3000 καναλιών [31], σε αντίθεση με την αξιοποίηση των εσωζωνικών μεθόδων όπου για την επίβλεψη του καναλιού αξιοποιείται το ίδιο το κανάλι.

2.3.1 Γενική Αρχιτεκτονική Δικτύου Σηματοδοσίας

Στο Σχήμα 2–1 απεικονίζονται τα βασικά δικτυακά στοιχεία ενός εξωζωνικού συστήματος σηματοδοσίας, συγκεκριμένα του SS7, όπως αυτό υλοποιείται σήμερα στα πλαίσια της διασύνδεσης δύο διαφορετικών γεωγραφικών περιοχών. Συγκεκριμένα, το δίκτυο αυτό απαρτίζεται από τα ακόλουθα στοιχεία:

- Τοπικό Τηλεφωνικό Κέντρο (Local Exchange Center–(LEC)): Τα τοπικά τηλεφωνικά κέντρα επιφορτίζονται με τη διαχείριση των τελικών χρηστών μιας συγκεκριμένης γεωγραφικής περιοχής και αποτελούν την κύρια διεπαφή των χρηστών με τον κορμό του τηλεφωνικού δικτύου.
- Σημείο Μεταφοράς Σηματοδοσίας (Signaling Transfer Point–(STP)): Η οντότητα αυτή είναι ουσιαστικά υπεύθυνη για τη διαχείριση (επεξεργασία, δρομολόγηση, μετάδοση) των μηνυμάτων σηματοδοσίας. Η μετάδοση-δρομολόγηση των δεδομένων σηματοδοσίας πραγματοποιείται με την αξιοποίηση των συνδέσεων μεταξύ των διαφορετικών STPs. Για την επίτευξη αυξημένης αξιοπιστίας του δικτύου σηματοδοσίας οι οντότητες αυτές υλοποιούν ένα δίκτυο πλέγματος.
- Σημείο Ελέγχου Υπηρεσίας (Service Control Point–(SCP)): Η οντότητα αυτή επιφορτίζεται με την παροχή επιπρόσθετων υπηρεσιών, όπως ενδεικτικά είναι:
  - Πληροφορίες προ-πληρωμένων καρτών.
  - Κλήσεις χωρίς χρέωση.
  - Φραγές και προωθήσεις κλήσεων.
  - Τηλέ-διασκέψεις, χρεώσεις καλούμενου κ.α.
- Γραμμή Επικοινωνίας (Trunk): Οι γραμμές επικοινωνίας ουσιαστικά αντιστοιχούν στο διαθέσιμο εύρος ζώνης που χρησιμοποιείται για τη μετάδοση δεδομένων φωνής μεταξύ των χρηστών υπηρεσιών τηλεφωνίας.



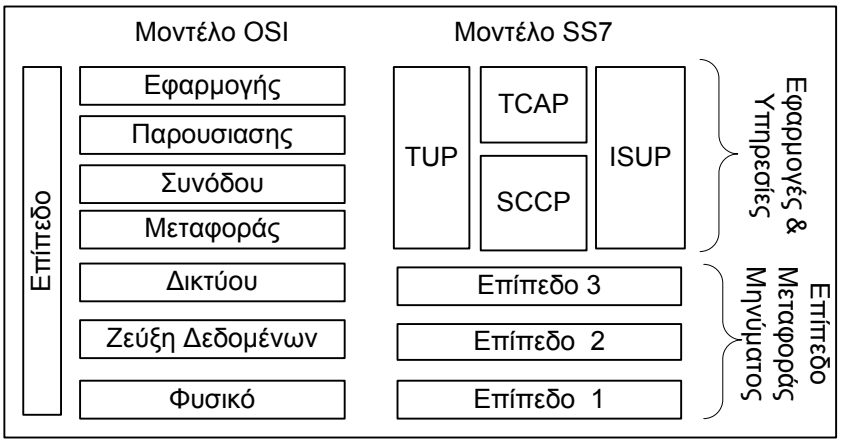
Σχήμα 2–1. Γενική Αρχιτεκτονική Δικτύου Σηματοδοσίας στο PSTN

2.3.2 Συστήματα Σηματοδοσίας στο PSTN

Όπως προαναφέρθηκε το κυρίαρχο σύστημα σηματοδοσίας το οποίο αξιοποιείται στο PSTN είναι το SS7 [31]. Οι βασικές λειτουργίες που διεκπεραιώνονται είναι:

1. Διαχείριση κλήσεων (αποκατάσταση, ανανέωση και τερματισμός).
2. Φορητότητα τηλεφωνικών αριθμών.
3. Υπηρεσίες κλήσεων χωρίς χρέωση (800x) και ειδικές υπηρεσίες (900x).
4. Υπηρεσίες προώθησης κλήσεων (call forwarding).
5. Υπηρεσίες αναγνώρισης κλήσεων κ.α.

Το SS7 δεν αποτελεί ένα απλό πρωτόκολλο αλλά ένα σύνολο από προδιαγραφές και διαφορετικά πρωτόκολλα τα οποία απαιτούνται για την ορθή λειτουργία ενός τηλεφωνικού συστήματος όπως αυτό του PSTN. Πιο συγκεκριμένα το SS7, σε αντιστοιχία με το πρότυπο Διασύνδεσης Ανοικτών Συστημάτων (Open Systems Interconnection–(OSI)) [32], διαχωρίζεται σε τέσσερα επίπεδα[1]: το φυσικό επίπεδο (physical level), το επίπεδο ζεύξης δεδομένων (data-link level), το επίπεδο δικτύου (network level) και το επίπεδο εφαρμογών-υπηρεσιών (application level) όπως απεικονίζεται στο Σχήμα 2–2.



Σχήμα 2–2. Συσχέτιση της Στοίβας Πρωτοκόλλων SS7 με το Μοντέλο Αναφοράς OSI

2.3.2.1 Φυσικό Επίπεδο

Το φυσικό επίπεδο στο SS7, γνωστό ως Τμήμα Μεταφοράς Μηνύματος Επιπέδου 1 (Message Transfer Part Level 1), προσδιορίζει τις προδιαγραφές των φυσικών συνδέσεων που πρέπει να χρησιμοποιούνται σε ένα δίκτυο SS7. Σε αυτές συμπεριλαμβάνονται τα πρότυπα E-1 (2048 kb/s με 32 κανάλια των 64 kb/s), DS-1 (1544 kb/s, με 24 κανάλια των 64kb/s), V.35 (64 kb/s), DS-0 (64 kb/s) και DS-0A (56 kb/s).

2.3.2.2 Ζεύξης Δεδομένων

Το επίπεδο ζεύξης δεδομένων στο SS7, γνωστό ως Τμήμα Μεταφοράς Μηνύματος Επιπέδου 2 (Message Transfer Part Level 2), εξασφαλίζει την ορθή μετάδοση των μηνυμάτων σηματοδοσίας μεταξύ δύο κόμβων παρέχοντας υπηρεσίες ελέγχου ροής (flow control),

[1] Οι υπηρεσίες επιπέδων 1-3 στην αντιστοιχία με το OSI παρέχονται από το Τμήμα Μεταφοράς Μηνύματος (Message Transfer Part) για λόγους συμβατότητας με το OSI έγινε η κατάτμηση του σε 3 επίπεδα όπως απεικονίζεται στο Σχήμα 2-2.

ελέγχου λαθών και ακολουθίας μηνυμάτων. Σε περιπτώσεις εσφαλμένης μετάδοσης το μήνυμα επανεκπέμπεται.

2.3.2.3 Επίπεδο Δικτύου

Το επίπεδο δικτύου, γνωστό ως Τμήμα Μεταφοράς Μηνύματος Επιπέδου 3 (Message Transfer Part Level 3), προσφέρει υπηρεσίες για την ορθή δρομολόγηση των μηνυμάτων σηματοδοσίας.

2.3.2.4 Επίπεδο Εφαρμογών & Υπηρεσιών

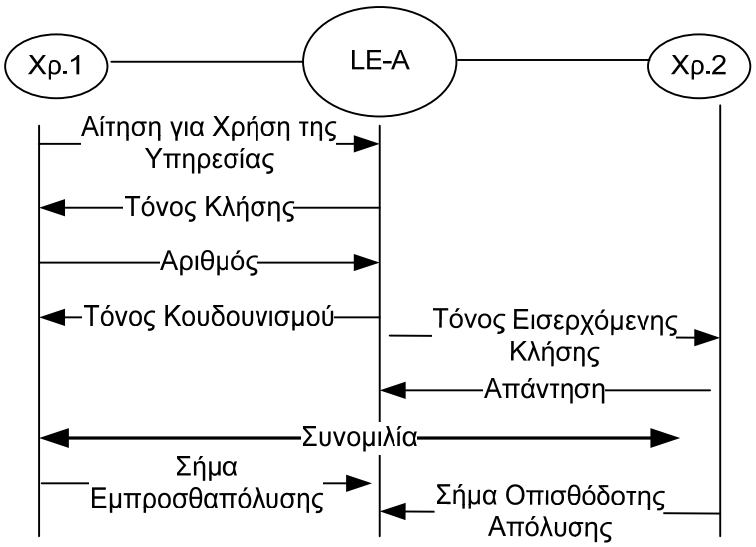
Το επίπεδο εφαρμογών και υπηρεσιών στο SS7 αποτελείται από διαφορετικά πρωτόκολλα για τη διαχείριση των κλήσεων και την παροχή επιπρόσθετων υπηρεσιών όπως το ISDN User Part (ISUP), το Telephone User Part (TUP) και το Transaction Capabilities Applications Part (TCAP).

2.3.3 Μοντέλο Λειτουργίας Υπηρεσιών Τηλεφωνίας στο PSTN

Για την «απλοποίηση» της περιγραφής της διαδικασίας αποκατάστασης κλήσης μεταξύ δύο χρηστών, στο PSTN θεωρείται ότι οι χρήστες βρίσκονται συνδεδεμένοι στο ίδιο τηλεφωνικό κέντρο, για παράδειγμα στο LE-A όπως απεικονίζεται στο Σχήμα 2–1. Αναλυτικότερα, όταν ένας χρήστης (καλών) επιθυμεί να πραγματοποιήσει μια κλήση σε έναν άλλον (καλούμενος) ακολουθείται η παρακάτω διαδικασία:

1. Ο καλών σηκώνει (hang-off) το τηλέφωνο. Η κίνηση αυτή ερμηνεύεται αυτόματα από το τοπικό τηλεφωνικό κέντρο ως αίτηση για χρήση της υπηρεσία (request-for-service), με αποτέλεσμα να στέλνει ως απάντηση της αίτησης αυτής, τον τόνο κλήσης (dial-tone), δείχνοντας ότι υπάρχει η δυνατότητα παροχής της υπηρεσίας και αναμένοντας να λάβει τον αριθμό του καλούμενου για να πραγματοποιήσει την εγκατάσταση της σύνδεσης.
2. Ο καλών προσδιορίζει τον αριθμό του καλούμενου και τον αποστέλλει στο τοπικό τηλεφωνικό κέντρο.
3. Το τοπικό τηλεφωνικό κέντρο μόλις λάβει τον αριθμό του καλούμενου ελέγχει τη διαθεσιμότητα του. Στην περίπτωση που είναι διαθέσιμος (δεν είναι κατειλημμένος) όλοι οι απαραίτητοι πόροι δεσμεύονται και ο καλούμενος ενημερώνεται για την ύπαρξη εισερχόμενης κλήσης με τη λήψη του σήματος εισερχόμενης κλήσης, ενώ ο καλών 'ενημερώνεται' για την πρόοδο της κλήσης με τη λήψη του τόνου κωδωνισμού (ringing tone).
4. Μόλις ο καλούμενος απαντήσει δημιουργείται σήμα απάντησης κλήσης (answer signal) και όλοι οι επιπρόσθετοι απαραίτητοι πόροι για την τελική αποκατάσταση της κλήσης δεσμεύονται και οι δύο χρήστες είναι πλέον σε θέση να επικοινωνήσουν μεταξύ τους.
5. Στο τέλος της κλήσης και εφόσον ο καλών και ο καλούμενος «κατεβάσουν» (hang-on) τα ακουστικά τους, αποστέλλουν στο τοπικό τηλεφωνικό κέντρο σήμα εμπροσθαπόλυσης (clear-forward) και οπισθόδρομης απόλυσης (clear-back) αντιστοίχως για την τελική αποδέσμευση των δεσμευμένων πόρων.

Η παραπάνω διαδικασία παρουσιάζεται στο Σχήμα 2–3. Στην περίπτωση που οι χρήστες δε βρίσκονται στην ίδια γεωγραφική περιοχή θα πρέπει τα τοπικά τηλεφωνικά κέντρα να πραγματοποιήσουν τις απαραίτητες συνδέσεις μεταξύ τους (αξιοποιώντας τα κατάλληλα STPs) ώστε να προωθήσουν την κλήση στον καλούμενο.



Σχήμα 2–3. Διαδικασία Αποκατάστασης Σύνδεσης Μεταξύ Δύο Χρηστών που Βρίσκονται στην Ίδια Γεωγραφική Περιοχή.

2.4 Η Υπηρεσία της IP Τηλεφωνίας

2.4.1 Η Αρχιτεκτονική Διαδικτύου

Η αρχιτεκτονική του διαδικτύου, όπως έχει καθιερωθεί σήμερα, είναι αποτέλεσμα μακροχρόνιας έρευνας, η οποία ξεκίνησε από το αμερικανικό υπουργείο άμυνας και συγκεκριμένα από το Defense Advanced Research Projects Agency (DARPA). Η αρχιτεκτονική αυτή στρωματοποιείται σε τέσσερα επίπεδα: το φυσικό, διαδικτύου, μεταφοράς, και εφαρμογής αντιστοίχως. Η στρωματοποίηση αυτή βρίσκεται σε αντιστοιχία με το μοντέλο αναφοράς OSI **[32]** όπως απεικονίζεται στο Σχήμα 2–4.

2.4.1.1 Φυσικό επίπεδο (Physical Network)

Το φυσικό επίπεδο αποτελεί το χαμηλότερο επίπεδο στη διαστρωμάτωση των πρωτοκόλλων του διαδικτύου και επιφορτίζεται με τη διαχείριση της φυσικής διεπαφής μεταξύ συσκευής και επικοινωνιακού μέσου. Μεταξύ των πιο γνωστών πρωτοκόλλων που αξιοποιούνται σε αυτό το επίπεδο είναι (α) το Ethernet (β) το IEEE 802.11 (γ) το V.90 σε συνδυασμό με το Point to Point Protocol.

2.4.1.2 Επίπεδο Διαδικτύου (Internet Layer)

Το επίπεδο διαδικτύου αποτελεί τον πυρήνα της διαδικτυακής αρχιτεκτονικής. Το επίπεδο αυτό επιφορτίζεται με τη δρομολόγηση των δεδομένων, ανεξαρτήτως της τοποθεσίας που βρίσκεται η πηγή και ο αποδέκτης αυτών. Η διαφανής αυτή διασύνδεση επιτυγχάνεται με την αξιοποίηση του ασυνδεσμικού πρωτοκόλλου Διαδικτύου [3]. Τα δεδομένα (των υψηλότερων επίπεδων) ενθυλακώνονται (encapsulated) σε πακέτα IP και δρομολογούνται-αποστέλλονται με βάση τη διεύθυνση προορισμού IP (κάθε διαδικτυακή οντότητα προσδιορίζεται μοναδικά από αυτή τη διεύθυνση) που περιέχεται στις κεφαλίδες (header) των IP μηνυμάτων.

2.4.1.3 Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς επιφορτίζεται με τη μεταφορά των μηνυμάτων, ανεξαρτήτως του υποκείμενου δικτύου, αξιοποιώντας είτε πρωτόκολλα ιδεατών συνδέσεων όπως το TCP [9]

και SCTP [8] είτε ασυνδεσμικά όπως το UDP [33]. Ουσιαστικά, στο διαδίκτυο αξιοποιείται μεταγωγή πακέτων σε αντίθεση με το PSTN που αξιοποιείται μεταγωγή κυκλώματος.

2.4.1.4 Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής περιλαμβάνει όλα τα πρωτόκολλα που απαιτούνται για την πλήρη υποστήριξη των εφαρμογών των χρηστών. Μέσω των πρωτοκόλλων αυτών προσδιορίζονται οι διαδικασίες που ακολουθούν οι εφαρμογές-υπηρεσίες. Παραδείγματα τέτοιων εφαρμογών-υπηρεσιών αποτελούν (α) το εικονικό τερματικό (TELNET), (β) η μεταφορά αρχείων (FTP), (γ) το ηλεκτρονικό ταχυδρομείο (SMTP), (δ) το σύστημα ονομάτων περιοχών (DNS) και άλλα.

Σχήμα 2–4. Συσχέτιση της Στοίβας Πρωτοκόλλων Διαδικτύου με το Μοντέλο Αναφοράς OSI

2.4.2 Αρχιτεκτονική IP Τηλεφωνίας

Το διαδίκτυο δεν είχε εξ αρχής σχεδιαστεί για μεταφορά δεδομένων σε πραγματικό χρόνο (real-time data), κάτι που αντικατοπτρίζεται στο γεγονός ότι κατά την αρχική του ανάπτυξη-εξέλιξη στηρίχθηκε κυρίως σε εφαρμογές που δεν ήταν ευαίσθητες σε χρονικές καθυστερήσεις, όπως το ηλεκτρονικό ταχυδρομείο(e-mail) και η μεταφορά αρχείων (FTP). Ο λόγος ήταν ότι η μετάδοση δεδομένων μέσω αυτού δεν μπορούσε να χαρακτηριστεί αξιόπιστη. Παρ' όλα αυτά με την πάροδο του χρόνου η αξιοπιστία μετάδοσης βελτιώθηκε και συνεχίζει να βελτιώνεται, με αποτέλεσμα την υλοποίηση και παροχή πολυμεσικών υπηρεσιών μέσω του διαδικτύου, με πρώτη εξ αυτών την τηλεφωνία.

Πιθανότατα κάποιος θα μπορούσε να υποστηρίξει ότι το SS7, ή τμήματα αυτού, είναι δυνατόν να αξιοποιηθούν στην αρχιτεκτονική της IP τηλεφωνίας. Παρ' όλα αυτά είναι ξεκάθαρο ότι η πλήρης εφαρμογή του SS7 στο διαδίκτυο δεν είναι εφικτή αφού τα πρωτόκολλα των κατωτέρων επιπέδων δεν είναι συμβατά με τα αντίστοιχα του διαδικτύου. Συνεπώς, είναι δυνατή μόνο η μερική εφαρμογή του SS7 και συγκεκριμένα των πρωτοκόλλων του επιπέδου εφαρμογής. Ακόμα όμως και η εφαρμογή αυτών υπόκειται σε περιορισμούς. Συγκεκριμένα, απαιτούν αξιόπιστη μετάδοση μηνυμάτων χωρίς καθυστερήσεις κάνοντας χρήση πρωτοκόλλων μεταφοράς τα οποία είναι προσανατολισμένα σε μετάδοση μηνυμάτων (message oriented protocols) και όχι πακέτων, όπως είναι τα πρωτόκολλα μεταφοράς που αξιοποιούνται στο διαδίκτυο. Για την κάλυψη των ειδικών αυτών αναγκών σχεδιάστηκε ένα νέο πρωτόκολλο μεταφοράς το SCTP [8] ώστε να είναι δυνατή η χρήση του SS7 στο διαδίκτυο. Παρ' όλα αυτά, μέχρι πρότινος το SCTP δεν υλοποιείται ως μέρος του λειτουργικού συστήματος όπως το TCP [9], με αποτέλεσμα να μην είναι δυνατή η δημιουργία τηλεφώνων βασισμένων στο IP που αξιοποιούν ως μοναδική λύση τα πρωτόκολλα επιπέδου εφαρμογής του SS7. Πέραν όμως των συστημάτων σηματοδοσίας, στο διαδίκτυο δεν υπάρχει αφιερωμένο κανάλι για την μετάδοση των δεδομένων φωνής. Η φωνή μεταδίδεται μέσω του δικτύου δεδομένων που όμως είναι μη αξιόπιστο για τη μετάδοση δεδομένων πραγματικού χρόνου, με αποτέλεσμα να απαιτούνται διαφορετικοί μηχανισμοί μετάδοσης. Επιπλέον θα

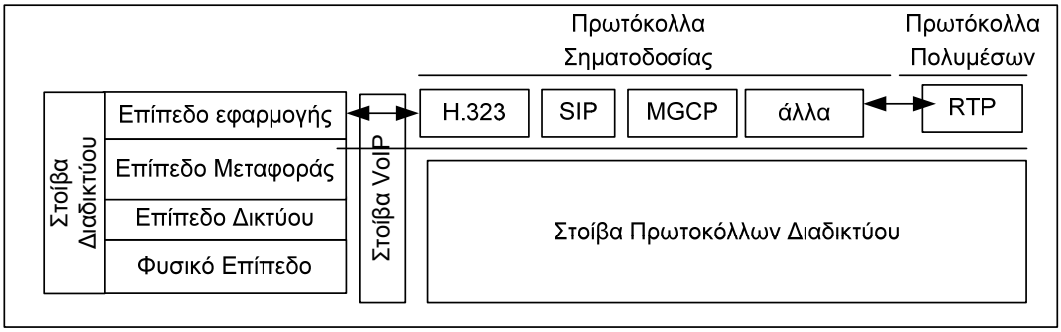
πρέπει να σημειωθεί ότι η αρχιτεκτονική του διαδικτύου θεωρείται δεδομένη και ως εκ' τούτου, τροποποιήσεις σε αυτή είναι σχεδόν ανέφικτές. Όλοι οι επιπρόσθετοι μηχανισμοί που απαιτούνται για την κάλυψη των αναγκών της IP τηλεφωνίας πρέπει να ενσωματώνονται στο επίπεδο εφαρμογής.

Συνεπώς, για την εξέλιξη της IP τηλεφωνίας η ανάπτυξη νέων πρωτοκόλλων τόσο για τη διαχείριση των κλήσεων όσο και για τη μεταφορά των πολυμεσικών δεδομένων (φωνής και εικόνας) θεωρείται αναγκαία. Στο Σχήμα 2–5 απεικονίζονται τα διαφορετικά πρωτόκολλα που χρησιμοποιούνται στην IP τηλεφωνία και τα οποία εντάσσονται στις παρακάτω κατηγορίες:

Πρωτόκολλα Σηματοδοσίας: Τα πρωτόκολλα σηματοδοσίας αναλαμβάνουν τη διαχείριση των κλήσεων (εγκατάσταση, τροποποίηση, τερματισμός) μεταξύ των επικοινωνούντων οντοτήτων. Για τη διαχείριση των κλήσεων στην IP τηλεφωνία έχουν σχεδιαστεί και υλοποιηθεί πρωτόκολλα διαφορετικής αρχιτεκτονικής, μεταξύ των οποίων είναι το H.323 [10] και το SIP [11]. Το SIP όμως φαίνεται να κυριαρχεί έναντι των άλλων καθώς καθιερώνεται ως de-facto πρωτόκολλο σηματοδοσίας συστημάτων IP τηλεφωνίας και γενικότερα των πολυμεσικών επικοινωνιών. Σε αυτό έχει συμβάλει και το γεγονός ότι το SIP αξιοποιείται στο υποσύστημα πολυμέσων IP των συστημάτων 3ής γενεάς κινητών επικοινωνιών. Λεπτομερέστερη παρουσίαση των πρωτοκόλλων σηματοδοσίας πραγματοποιείται στο κεφάλαιο 3 (βλέπε ενότητες 3.2-3.4)

Πρωτόκολλα Πολυμέσων: Τα πρωτόκολλα πολυμέσων αξιοποιούνται κυρίως για τη μετάδοση των (πολυμεσικών) δεδομένων μεταξύ των οντοτήτων που έχουν ήδη εγκαταστήσει ένα κανάλι επικοινωνίας μεταξύ τους. Για τη μετάδοση των πολυμεσικών δεδομένων αξιοποιείται κυρίως το Real Transport Protocol [34] (RTP). Λεπτομερέστερη παρουσίαση των πολυμεσικών πρωτοκόλλων πραγματοποιείται στο κεφάλαιο 3 (βλέπε ενότητα 3.6)

Βοηθητικά Πρωτόκολλα: Βοηθητικά πρωτόκολλα θεωρούνται όλα εκείνα τα οποία αξιοποιούνται ήδη επιτυχώς στις υπηρεσίες του διαδικτύου και ενσωματώνονται στην αρχιτεκτονική της IP τηλεφωνίας, για την παροχή ολοκληρωμένων υπηρεσιών. Παραδείγματα τέτοιων πρωτοκόλλων είναι το DNS [35] και το DHCP [36] για την παροχή υπηρεσιών επίλυσης ονομάτων (address name resolution) και τη δυναμική διαμόρφωση των τερματικών συσκευών αντιστοίχως. Λεπτομερέστερη παρουσίαση των βοηθητικών πρωτοκόλλων πραγματοποιείται στο κεφάλαιο 3 (βλέπε ενότητα 3.7).



Σχήμα 2–5. Η Στοίβα Πρωτοκόλλων Διαδικτυακής Τηλεφωνίας

2.4.3 Μοντέλο Λειτουργίας Υπηρεσιών Διαδικτυακής Τηλεφωνίας

Για την ανάπτυξη εφαρμογών και υπηρεσιών σε περιβάλλον διαδικτύου χρησιμοποιούνται κυρίως δύο μοντέλα:

1. Πελάτη-Εξυπηρέτη (Client-Server) [37], και
2. Διότιμης Επικοινωνίας (Peer-to-Peer) [38]

Η εφαρμογή της τηλεφωνίας στο διαδίκτυο μπορεί να θεωρηθεί συνδυασμός των δύο αυτών μοντέλων. Όμοια με τη λειτουργία του PSTN, η διαδικασία επικοινωνίας μεταξύ δύο οντοτήτων χωρίζεται σε δύο φάσεις. Στη φάση αποκατάστασης συνόδου, όπου διαμεσολαβεί ο κατάλληλος εξυπηρέτης μεταξύ των επικοινωνούντων οντοτήτων, και στη φάση των δεδομένων όπου υπάρχει διότιμη επικοινωνία των οντοτήτων.

2.5 Συμπεράσματα

Το PSTN είναι ένα κεντρικοποιημένο σύστημα που βασίζεται σ' ένα κλειστό δίκτυο. Αξιοποιώντας την κατάλληλη αρχιτεκτονική και πρωτόκολλα που είναι προσανατολισμένα στις ανάγκες του SS7, επιτυγχάνει μεγάλο βαθμό αξιοπιστίας, διαθεσιμότητας και ασφάλειας. Από την άλλη πλευρά, η IP τηλεφωνία αξιοποιεί ανοικτά πρότυπα και χρησιμοποιεί ως δίκτυο 'κορμού' το διαδίκτυο, κληρονομώντας τόσο τα πλεονεκτήματα όσο και τα μειονεκτήματα αυτού και όλων των (κατανεμημένων) υποδομών που το υποστηρίζουν.

ΚΕΦΑΛΑΙΟ 3: Πρωτόκολλα και Αρχιτεκτονική Συστημάτων Διαδικτυακής Τηλεφωνίας

3.1 Γενικά

Το PSTN είναι ένα κεντρικοποιημένο σύστημα κλειστής αρχιτεκτονικής μέσω του οποίου διενεργείται τόσο η μεταφορά των δεδομένων όσο και η συνολική διαχείριση των συνόδων. Να επισημανθεί ότι στις περιπτώσεις που η διαχείριση των συνόδων διενεργείται με ευθύνη του δικτύου, οποιοδήποτε πρόβλημα ή αποτυχία του δικτύου επηρεάζει άμεσα τη διαχείριση των συνόδων και συνεπώς τη διαθεσιμότητα και αξιοπιστία των παρεχόμενων υπηρεσιών [30]. Το διαδίκτυο είναι ένα κατανεμημένο σύστημα ανοικτής αρχιτεκτονικής του οποίου βασική σχεδιαστική αρχή αποτελεί το γεγονός ότι επιφορτίζεται αποκλειστικά και μόνο με τη μετάδοση των δεδομένων και όχι με τη διαχείριση των συνόδων που πραγματοποιούνται μέσω αυτού [39]. Ως εκ τούτου έχει επιλεγεί η διαχείριση των συνόδων να πραγματοποιείται από τις τερματικές συσκευές ή εναλλακτικά από άλλα υποστηρικτικά συστήματα (για παράδειγμα ο εξυπηρετής της προσφερόμενης υπηρεσίας) [30]. Η σχεδιαστική αυτή αρχή ενσωματώνεται πλέον στα περισσότερα πρωτόκολλα που αναπτύσσονται για παροχή υπηρεσιών στο διαδίκτυο, συμπεριλαμβανομένων και των πρωτοκόλλων διαχείρισης-σηματοδοσίας πολυμεσικών συνόδων.

Για την παροχή ολοκληρωμένων υπηρεσιών IP τηλεφωνίας απαιτείται η χρήση διαφορετικών πρωτοκόλλων (βλέπε Σχήμα 2–5). Διαφορετικά πρωτόκολλα έχουν ήδη αναπτυχθεί τόσο για τη διαχείριση των κλήσεων όπως το H.323 [10] και το SIP [11], όσο και για τη διαχείριση των πολυμεσικών δεδομένων για την επίτευξη διαλειτουργικότητας μεταξύ διαφορετικών αρχιτεκτονικών, όπως το Media Gateway Control Protocol–(MGCP) [40]. Πέρα από τα πρωτόκολλα σηματοδοσίας βασική υποδομή των υπηρεσιών διαδικτυακής τηλεφωνίας αποτελεί η μεταφορά των πολυμεσικών δεδομένων που πραγματοποιείται κυρίως με την χρήση Real Transport Protocol–(RTP)[34]. Μεταξύ των πρωτοκόλλων διαχείρισης σηματοδοσίας το επικρατέστερο είναι το SIP καθώς εξειδικεύεται στην αρχιτεκτονική του διαδικτύου και έχει ενσωματωθεί ως πρωτόκολλο σηματοδοσίας στην αρχιτεκτονική της 3ης γενεάς κινητών επικοινωνιών στο υποσύστημα πολυμέσων IP (Multimedia Subsystem IP–(IMS)). Για τη διασύνδεση των διαφορετικών αρχιτεκτονικών μετάδοσης των πολυμεσικών δεδομένων το επικρατέστερο είναι το MGCP [40].

Στη συνέχεια του παρόντος κεφαλαίου περιγράφονται τα προαναφερόμενα πρωτόκολλα και ο τρόπος αξιοποίησης τους στη διαδικτυακή τηλεφωνία. Έμφαση δίνεται στην περιγραφή του πρωτοκόλλου SIP καθώς, όπως προαναφέρθηκε, είναι το κυρίαρχο πρωτόκολλο σηματοδοσίας και αναμένεται να χρησιμοποιηθεί ευρέως στις επόμενες γενεές δικτύων. Επιπροσθέτως, πραγματοποιείται συνοπτική περιγραφή τόσο των διαφορετικών τοπολογιών που δημιουργούνται με την έλευση της διαδικτυακής τηλεφωνίας, όσο και των βοηθητικών πρωτοκόλλων που απαιτείται για την παροχή ολοκληρωμένων υπηρεσιών τηλεφωνίας μέσω του διαδικτύου.

3.2 Το Πρωτόκολλο Σηματοδοσίας SIP

3.2.1 Βασικές Λειτουργίες του SIP

Το SIP [11] είναι ένα πρωτόκολλο σηματοδοσίας, επιπέδου εφαρμογής, για τη διαχείριση (εγκατάσταση, τροποποίηση παραμέτρων και τερματισμό) πολυμεσικών συνόδων. Τέτοιου

είδους σύνοδοι θεωρούνται και οι τηλεφωνικές κλήσεις που πραγματοποιούνται μέσω IP δικτύων για τις οποίες, άλλωστε, έγινε ο αρχικός σχεδιασμός του SIP.

Το SIP χαρακτηρίζεται από απλότητα και ευπροσαρμοστικότητα παρέχοντας τη δυνατότητα εφαρμογής του παράλληλα με άλλα πρωτόκολλα και υπηρεσίες του διαδικτύου. Σε αυτό συντελεί και το γεγονός ότι μια από τις βασικές απαιτήσεις κατά τον αρχικό σχεδιασμό του αποτελούσε η εφαρμογή του στην αρχιτεκτονική του διαδικτύου, κάτι που είχε ως αποτέλεσμα να ενσωματωθούν μηχανισμοί και πρωτόκολλά που είχαν εφαρμοσθεί με επιτυχία στο διαδίκτυο, όπως το HTTP [12]και το SMTP [41]. Σε γενικές γραμμές το SIP έχει ως στόχο την ανάπτυξη και υποστήριξη υπηρεσιών τηλεφωνίας στο διαδίκτύο, παρά να προσφέρει μια ολοκληρωμένη λύση πρωτοκόλλων όπως για παράδειγμα το H.323 [10] και το SS7. Ο Πίνακας 3–1 αποτυπώνει συνοπτικά τις βασικές υπηρεσίες που υποστηρίζει το SIP.

Λειτουργικότητα	Σύντομη Περιγραφή
Εντοπισμός χρήστη	Προσδιορισμός της τελικής θέσης-διεύθυνσης του τελικού χρήστη η οποία θα αξιοποιηθεί για την εγκατάσταση της συνόδου.
Διαθεσιμότητα χρήστη	Ο χρήστης προσδιορίζει την επιθυμία συμμετοχής του σε μια συγκεκριμένη σύνοδο.
Δυνατότητες συσκευής χρήστη	Προσδιορισμός των πολυμεσικών παραμέτρων και δεδομένων που υποστηρίζουν οι συσκευές που χρησιμοποιούνται για την επικοινωνία μεταξύ των χρηστών.
Διαχείριση Συνόδου	Προσδιορισμός όλων των απαραίτητων παραμέτρων που απαιτούνται για την εγκατάσταση, ανανέωση και τον τερματισμό μιας κλήσης.

Πίνακας 3–1. Οι Βασικές Υπηρεσίες που Υποστηρίζει το SIP

Είναι αναγκαίο να σημειωθεί ότι, σε αντίθεση με την αρχιτεκτονική του PSTN όπου οι τερματικές συσκευές δεν ενσωματώνουν καμία λειτουργικότητα, στην αρχιτεκτονική του SIP ένα μεγάλο μέρος της απαιτούμενης λειτουργικότητας ενσωματώνεται στις τερματικές συσκευές, υποστηρίζοντας έτσι τη δυνατότητα ανάπτυξης νέων υπηρεσιών με βάση τον χρήστη.

3.2.2 Δομή Μηνυμάτων στο SIP

Ένα από τα βασικά στοιχεία που κληρονομεί το SIP από τα πρωτόκολλα του διαδικτύου, όπως το HTTP [12] και το SMTP [41], είναι η δομή και η σύνταξη των μηνυμάτων που αξιοποιούνται. Πιο συγκεκριμένα, τα μηνύματα στο SIP κωδικοποιούνται σε μορφή κειμένου (text based) και διαχωρίζονται σε δύο κατηγορίες:

1. Αιτήσεις (requests) οι οποίες αποστέλλονται από τους πελάτες (clients) στους εξυπηρέτες (servers).
2. Αποκρίσεις (responses) οι οποίες αποστέλλονται από τους εξυπηρέτες στους πελάτες ως απαντήσεις στις αντίστοιχες αιτήσεις.

Τόσο στις αιτήσεις όσο και στις αποκρίσεις γίνεται χρήση της ίδιας γενικής σύνταξης (βλέπε Σχήμα 3–1). Κάθε μήνυμα αποτελείται από την αρχική γραμμή (start-line) ακολουθούμενη από μια ή περισσότερες κεφαλίδες (headers) και προαιρετικά, ανάλογα με τον τύπο του μηνύματος γίνεται χρήση ή μη του ‘κύριου μέρους’ του μηνύματος (message body).

```
Generic-Message=start-line message_header CRLF [message body]
Start-line= Request-line|Response-line
```

Σχήμα 3–1. Γενική Δομή SIP Μηνυμάτων

3.2.2.1 SIP Αιτήσεις (Requests)

Κάθε SIP αίτηση (request) αποτελείται από τη γραμμή αίτησης (request-line) η οποία βρίσκεται στην πρώτη γραμμή του μηνύματος, ακολουθούμενη από τις κατάλληλες κεφαλίδες που περιγράφουν το μήνυμα και, προαιρετικά, από το κύριο μέρος του μηνύματος (message body) ανάλογα με τα οριζόμενα στις προδιαγραφές του SIP. Στο Σχήμα 3–2 απεικονίζεται ένα παράδειγμα μιας SIP αίτησης.

```
INVITE(METHOD) sip:dgentele.com (resource) SIP/2.0 (version) (REQUEST LINE)
From: <sip:3400001586@dgentele.com;user=phone>;tag=3199572059
To: <sip:3400001587@dgenele.com;user=phone>
Call-ID: 3021094946@81.0.7.124
CSeq: 1 INVITE
Contact: sip:195.251.166.73>;
content-Type: application/sdp

v=0
o=Tesla 2890844526 IN IP4 sip.lab.aegean.gr
c=IN IP4 195.251.166.73
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

HEADERS

Msg Body

Σχήμα 3–2. Παράδειγμα SIP Αίτησης (*SIP INVITE*)

Η γραμμή αίτησης περιέχει το όνομα της μεθόδου, τη διεύθυνση του πόρου που αιτείται ο χρήστης και την έκδοση του SIP πού χρησιμοποιείται, ακολουθούμενη από τις κατάλληλες κεφαλίδες και το κύριο μέρος του μηνύματος.

Ουσιαστικά, μια SIP αίτηση περιγράφει την «ενέργεια» που επιθυμεί ο χρήστης να εκτελέσει και οι κεφαλίδες δίνουν τις απαραίτητες επιπρόσθετες πληροφορίες που απαιτούνται για τη διαχείριση και επεξεργασία του συγκεκριμένου μηνύματος όπως, για παράδειγμα, πληροφορίες που σχετίζονται με τη δρομολόγηση του μηνύματος. Στο κύριο μέρος του μηνύματος περιγράφονται επιπρόσθετοι παράμετροι που απαιτούνται για την επιτυχή ολοκλήρωση της επικοινωνίας.

Οι επιτρεπτές «ενέργειες» προσδιορίζονται μέσω των μεθόδων και ορίζονται στις προδιαγραφές του SIP. Ο Πίνακας 3–2 αποτυπώνει τις βασικές μεθόδους που αξιοποιούνται στο SIP.

Όνομα Μεθόδου	Σύντομη Περιγραφή
INVITE	Εγκατάσταση συνόδου.
ACK	Επιβεβαίωση μιας απόκρισης που δημιουργήθηκε από μια αίτηση INVITE.
BYE	Τερματισμός μιας συνόδου.
REGISTER	Εγγραφή του χρήστη στην υπηρεσία καθορίζοντας τη διεύθυνση επαφής του.
CANCEL	Τερματισμός μιας συνόδου που δεν έχει ολοκληρωθεί.
OPTION	"Ανίχνευση" των μεθόδων που υποστηρίζει ένα τερματικό SIP.

Πίνακας 3–2. Βασικές Μέθοδοι στο SIP

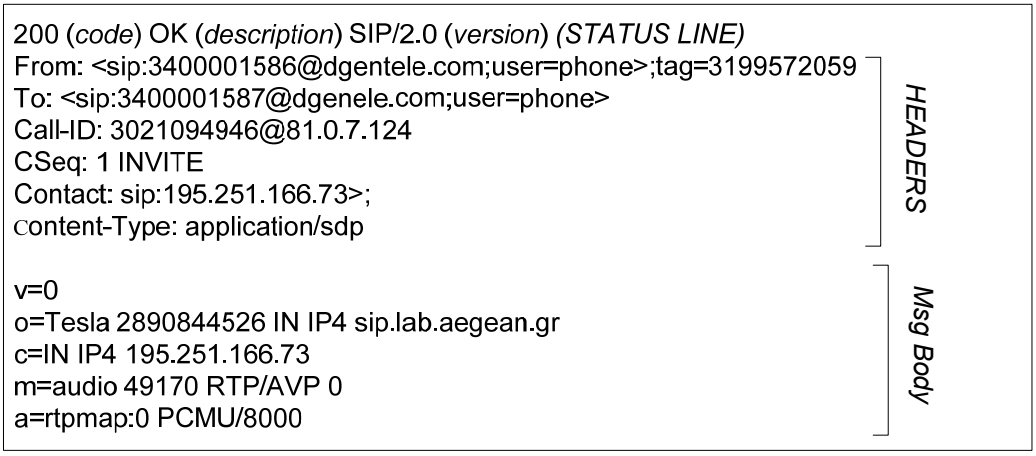
Εκτός των προαναφερόμενων βασικών SIP μεθόδων έχουν προταθεί διάφορες επιπρόσθετες μέθοδοι [42]-[44] με στόχο τον εμπλουτισμό των υπαρχόντων λειτουργιών. Ο Πίνακας 3–3 παρουσιάζει συνοπτικά αυτές τις μεθόδους.

Όνομα Μεθόδου	Σύντομη Περιγραφή
SUBSCRIBE	Αίτηση για πληροφόρηση σχετικά με την κατάστασης στην οποία βρίσκεται ένας χρήστης.
NOTIFY	Απόκριση στην αίτηση κατάστασης που βρίσκεται ένας χρήστης.
MESSAGE	Μεταφορά αυτόνομων μηνυμάτων (instant messaging) μεταξύ δύο επικοινωνούντων οντοτήτων.
UPDATE	Ανανέωση των παραμέτρων μιας συνόδου.

Πίνακας 3–3. Επιπρόσθετοι Μέθοδοι στο SIP

3.2.2.2 SIP Αποκρίσεις (Responses)

Οι αποκρίσεις (responses) είναι μηνύματα απαντήσεις στις αντίστοιχες αιτήσεις. Οι αποκρίσεις μπορεί να περιέχουν επιπρόσθετες πληροφορίες που πρέπει να γνωρίζει ο αιτών για να ολοκληρώσει με επιτυχία τη δοσοληψία, ή τους λόγους αποτυχίας αυτής. Η διαφορά μεταξύ αποκρίσεων και αιτήσεων στο SIP, όπως απεικονίζεται και στο Σχήμα 3–1, εντοπίζεται στο γεγονός ότι η γραμμή αίτησης που υπάρχει στα μηνύματα αιτήσεων αντικαθίσταται από τη γραμμή κατάστασης (status-line). Οι κεφαλίδες και το σώμα του μηνύματος παραμένουν ακριβώς όπως εμφανίζονται στην SIP αίτηση. Για παράδειγμα στο Σχήμα 3–3 απεικονίζεται η απόκριση που αντιστοιχεί στην αίτηση του Σχήμα 3–2.



Σχήμα 3–3. Παράδειγμα SIP Απόκρισης (SIP OK)

Πιο συγκεκριμένα, η γραμμή κατάστασης περιλαμβάνει τον κωδικό κατάστασης, την περιγραφή του αντίστοιχου κωδικού και την έκδοση του SIP που χρησιμοποιείται από την οντότητα δημιουργίας-επεξεργασίας της απόκρισης. Οι κωδικοί κατάστασης αντιστοιχούν είτε στην ενέργεια που πραγματοποίησε ο εξυπηρέτης που επεξεργάστηκε την αίτηση, είτε σε αυτή που πραγματοποίησε ο τελικός αποδέκτης αυτής. Τα μηνύματα των αποκρίσεων, σύμφωνα με τις προδιαγραφές του SIP, διαχωρίζονται σε έξι γενικές κατηγορίες όπως απεικονίζει ο Πίνακας 3–4.

Κωδ.	Τύπος	Σύντομη Περιγραφή
1xx	Πληροφοριακά(Informational)	Προσδιορίζει την κατάσταση στην οποία βρίσκεται μια μη ολοκληρωμένη κλήση.
2xx	Επιτυχίας (Success)	Σηματοδοτεί την επιτυχή διεκπεραίωση της αίτησης.
3xx	Ανακατεύθυνσης (Redirection)	Προσδιορίζει εναλλακτικές τοποθεσίες στις οποίες ο αιτών θα πρέπει να αποστείλει την αίτηση του.
4xx	Σφάλμα τελικού χρήστη (Client error)	Σηματοδοτεί το γεγονός ότι η επεξεργασία της αίτησης απέτυχε λόγω σφάλματος στον τελικό χρήστη. Η αίτηση θα πρέπει να αποσταλεί ξανά.
5xx	Σφάλμα Εξυπηρέτη (Server failure)	Σηματοδοτεί το γεγονός ότι η επεξεργασία της αίτησης απέτυχε λόγω σφάλματος στον εξυπηρέτη. Η αίτηση μπορεί να αποσταλεί σε εναλλακτικό εξυπηρέτη.
6xx	Γενικό Σφάλμα (Global failure)	Σηματοδοτεί το γεγονός ότι η επεξεργασία της αίτησης απέτυχε και δεν επιτρέπεται να υποβληθεί ξανά η αίτηση αυτή.

Πίνακας 3–4. Κατηγορίες SIP Αποκρίσεων

3.2.2.3 Μέθοδοι Διευθυνσιοδότησης στο SIP

Σε όλα τα μηνύματα αιτήσεων και αποκρίσεων απαιτείται ο προσδιορισμός των διευθύνσεων επαφής (contact address) των οντοτήτων που επικοινωνούν. Είναι φανερό ότι αν δεν καθοριστούν οι προαναφερόμενες διευθύνσεις η επικοινωνία μεταξύ των οντοτήτων δεν είναι εφικτή.

Στο διαδίκτυο για τον προσδιορισμό της διεύθυνσης ενός διαθέσιμου πόρου αξιοποιείται ο μηχανισμός ομοιόμορφου εντοπιστή πόρων (Uniform Resource Locator–(URL)) [45]. Πιο συγκεκριμένα, η διεύθυνση ακολουθεί την μορφή «scheme:resource». Για παράδειγμα η διεύθυνση «http://www.samos.aegean.gr/index.html» προσδιορίζει τον πόρο index.html που βρίσκεται αποθηκευμένος στο διαδικτυακό εξυπηρέτη με διεύθυνση «www.samos.aegean.gr» ενώ το «σχήμα»-πρωτόκολλο που αξιοποιείται για την προσπέλαση του πόρου αυτού είναι το «http». Ακριβώς αντίστοιχος είναι ο τρόπος προσδιορισμού των διευθύνσεων στην διαδικτυακή τηλεφωνία και συγκεκριμένα είναι της ακόλουθης μορφής:

«scheme:user:password@host:port;uri-parameters?header»

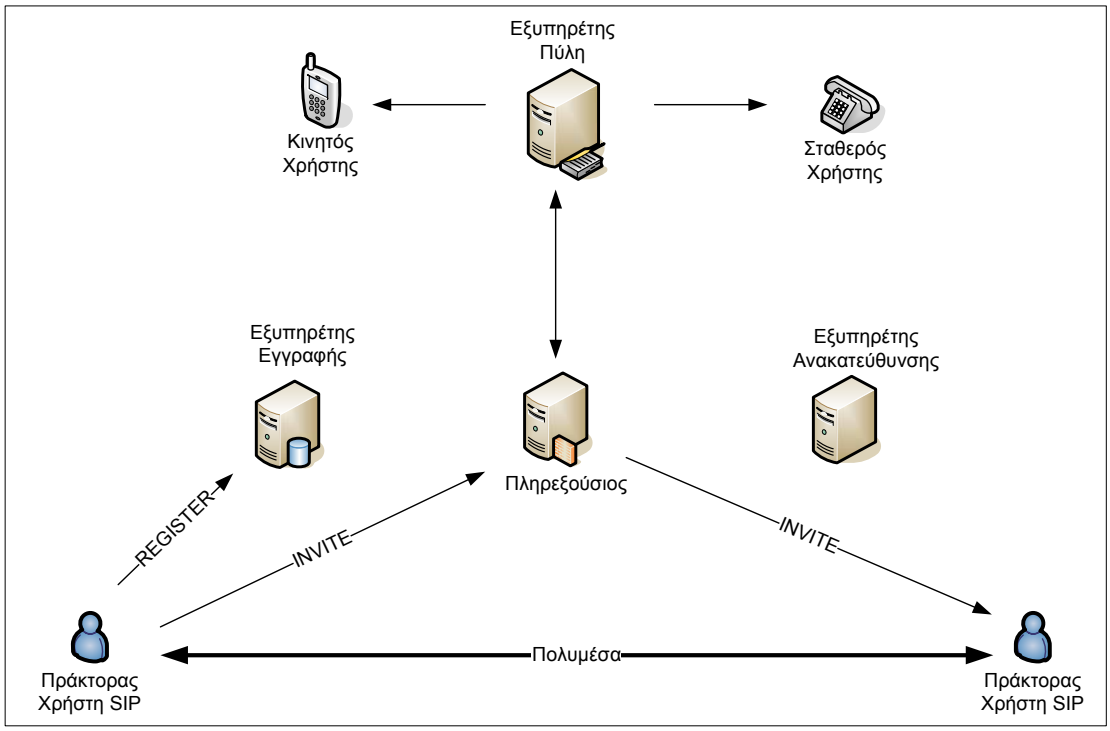
Η βασική διαφορά εντοπίζεται στη χρήση εναλλακτικών σχημάτων διευθυνσιοδότησης όπως για παράδειγμα το SIP, Secure SIP, Tel, κ.α. Θα πρέπει να σημειωθεί ότι ο τρόπος συγγραφής των διευθύνσεων αλλάζει σύμφωνα με τις προδιαγραφές που προσδιορίζονται από την εκάστοτε υπηρεσία. Στο Σχήμα 3–4 παρουσιάζονται παραδείγματα διευθυνσιοδότησης στο SIP που αφορούν τόσο τον προσδιορισμό των διευθύνσεων των τελικών χρηστών όσο και των επιπρόσθετων υπηρεσιών που παρέχονται σε αυτούς.

```
sip:alice:secretword@atlanta.com;transport=tcp
sips:alice@atlanta.com?subject=project%20x&priority=uent
sip:+1-212-555-212:1234@gateway.com;user=phonesips:1212@gateway.com
sip:alice@192.0.2.4
sip:atlanta.com;method=REGISTER?to=alice%40atlanta.comtel:411;phone-context=+1314
sip:411%3Bphone-context%3D+1314@gateway.example.com
Tel:+302273082247
```

Σχήμα 3–4. Εναλλακτικοί Τρόποι Διευθυνσιοδότησης στο SIP

3.2.3 Η Αρχιτεκτονική του SIP

Οι οντότητες που απαρτίζουν ένα δίκτυο SIP, όπως απεικονίζεται στο Σχήμα 3–5, είναι οι πράκτορες χρήστη (User Agents) και οι εξυπηρέτες (Servers).



Σχήμα 3–5. Βασική Δικτυακή Αρχιτεκτονική του SIP

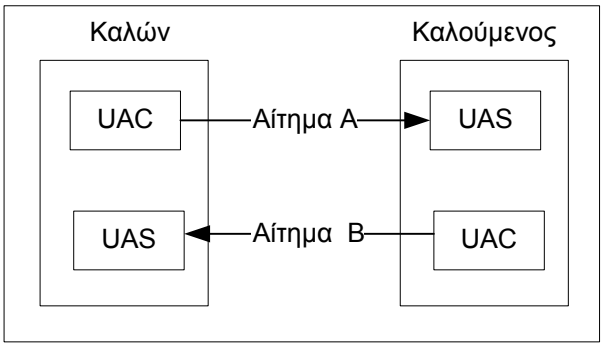
3.2.3.1 Πράκτορες Χρήστη (User Agents)

Οι πράκτορες χρήστη (User Agents-UA) ενσωματώνονται στις τελικές συσκευές των χρηστών ενός SIP δικτύου και λειτουργούν για λογαριασμό τους, διεκπεραιώνοντας τα αιτήματα τους. Κάθε UA διαχωρίζεται, με βάση τις λειτουργίες που εκτελεί, στα ακόλουθα τμήματα:

1. UA Πελάτης (Client) (UAC): Ο UAC επιφορτίζεται με τη δημιουργία των αιτημάτων του χρήστη.
2. UA Εξυπηρέτης (Server) (UAS): Ο UAS επιφορτίζεται με την επεξεργασία των εισερχόμενων αιτημάτων δημιουργώντας την κατάλληλη απόκριση για κάθε αίτηση που λαμβάνει.

Θα πρέπει να σημειωθεί ότι και οι δύο προαναφερόμενες οντότητες ενσωματώνονται στη SIP συσκευή τελικού χρήστη, σε αντίθεση με τις κλασικές υπηρεσίες του διαδικτύου όπως το

WWW όπου η συσκευή του τελικού χρήστη ενσωματώνει μόνο το τμήμα του πελάτη. Στο Σχήμα 3–6 παρουσιάζεται το επικοινωνιακό μοντέλο μεταξύ δύο πρακτόρων χρηστών SIP .



Σχήμα 3–6. Επικοινωνία μεταξύ Δύο SIP Πρακτόρων Χρήστη

3.2.3.2 Εξυπηρέτες (Servers)

Οι εξυπηρέτες στην αρχιτεκτονική του SIP είναι ενδιάμεσες οντότητες (διαμεσολαβητές) που παρέχουν επιπρόσθετες υπηρεσίες για την παροχή ολοκληρωμένων λύσεων και υπηρεσιών τηλεφωνίας στο διαδίκτυο. Οι εξυπηρέτες που αξιοποιούνται στην αρχιτεκτονική του SIP (βλέπε Σχήμα 3–5) είναι οι ακόλουθοι:

1. Εξυπηρέτης Εγγραφής (Registrar)
2. Πληρεξούσιος Εξυπηρέτης (Proxy)
3. Εξυπηρέτης Ανακατεύθυνσης (Redirect)
4. Εξυπηρέτης Πύλη (Gateway)

3.2.3.2.1 Εξυπηρέτης Εγγραφής (Registrar)

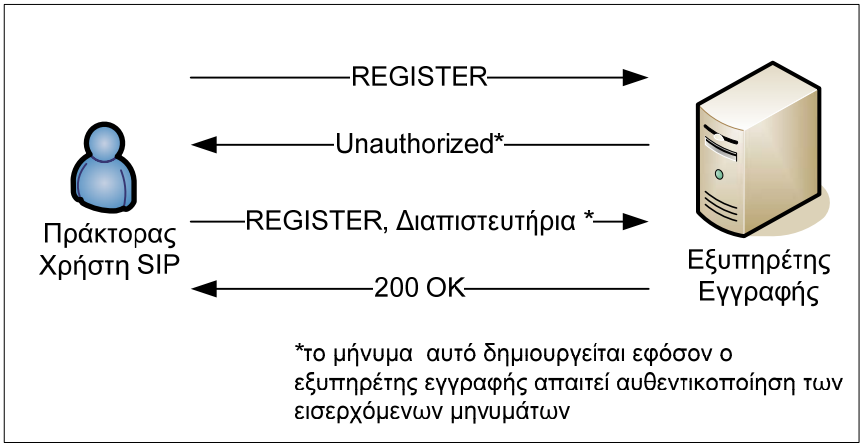
Ο εξυπηρέτης εγγραφής επιφορτίζεται με τη διαχείριση/επεξεργασία αιτήσεων εγγραφής (SIP REGISTER). Οι αιτήσεις εγγραφής περιέχουν τις πληροφορίες που απαιτούνται για να είναι δυνατός ο εντοπισμός της θέσης του χρήστη για την προώθηση των αιτημάτων και των αποκρίσεων που απευθύνονται σε αυτόν. Η πληροφορία εντοπισμού θέσης αποθηκεύεται σε κάποια βάση δεδομένων και έχει συγκεκριμένη διάρκεια ζωής με βάση τις προτιμήσεις του χρήστη. Με το πέρας αυτής, είναι απαραίτητο να αποσταλεί νέα αίτηση εγγραφής. Σε περίπτωση που ο χρήστης αλλάξει (για οποιοδήποτε λόγο) θέση εντοπισμού απαιτείται η ενημέρωση του εξυπηρέτη εγγραφής με την αποστολή νέας αίτησης (εγγραφής).

Στο Σχήμα 3–7 απεικονίζεται ένα παράδειγμα αίτησης εγγραφής που έχει δημιουργηθεί από το χρήστη με διεύθυνση «34000001586@dgentele.gr». Ο συγκεκριμένος χρήστης προσδιορίζει τη θέση εντοπισμού του στην κεφαλίδα «Contact», με χρονική ισχύ 300 δευτερολέπτων. Με το πέρας του χρονικού αυτού ορίου, όπως προαναφέρθηκε, θα πρέπει να ενημερώσει τον εξυπηρέτη εγγραφής για τη νέα θέση εντοπισμού του. Οι τιμές των κεφαλίδων «From» και «To» περιέχουν διαφορετικές τιμές όταν ένας εξουσιοδοτημένος χρήστης λειτουργεί για λογαριασμό κάποιου άλλου.

```
REGISTER sip:dgentele.com SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: <sip:3400001586@dgentele.com;user=phone>;tag=3199572059
To: <sip:3400001586@dgenele.com;user=phone>
Call-ID: 3021094946@81.0.7.124
CSeq: 2 REGISTER
Contact: sip:3400001586@81.0.7.124:5070;user=phone;transport=udp>;
expires=300
User-Agent: Cisco ATA 186  v3.1.0 atasip (040211A)
Authorization: Digest username="3400001586",realm="dgentele.com",
            nonce="426302039afdf717c6687e28f6c7d39c4fdb9f08",
            uri="sip:dgentele.com",response="af0d725596c8f06f370f8c80ade67b05"
Content-Length: 0
```

Σχήμα 3–7. Παράδειγμα Μηνύματος Εγγραφής (SIP REGISTER)

Ο χρήστης «34000001586@dgentele.gr» μόλις δημιουργήσει την αίτηση εγγραφής (βλέπε Σχήμα 3–7) την αποστέλλει στον κατάλληλο εξυπηρέτη και εφόσον αυτός την αποδεχτεί αποκρίνεται με το μήνυμα «200 OK». Η διαδικασία αυτή απεικονίζεται στο Σχήμα 3–8.



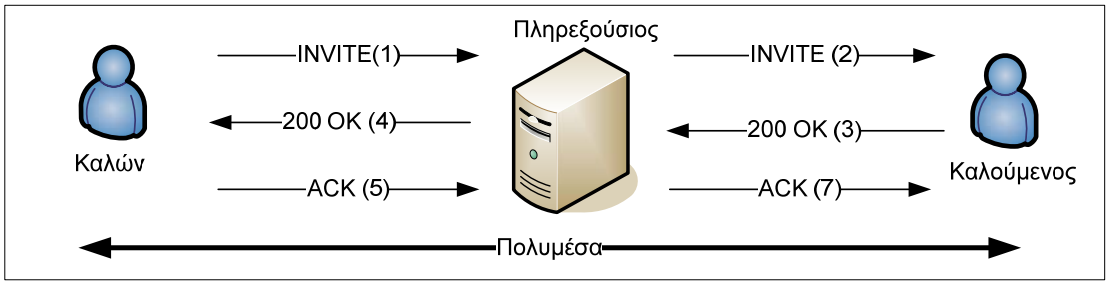
Σχήμα 3–8. Διαδικασία Εγγραφής στο SIP

3.2.3.2.2 Πληρεξούσιος (Proxy) Εξυπηρέτης

Ο Πληρεξούσιος εξυπηρέτης επιφορτίζεται με τη διαχείριση, επεξεργασία και προώθηση όλων των αιτήσεων (εκτός αιτήσεων εγγραφής) και των αντίστοιχων αποκρίσεων στους παραλήπτες τους. Για παράδειγμα στην περίπτωση όπου ένας χρήστης (καλών) επιθυμεί να επικοινωνήσει με κάποιον άλλο χρήστη (καλούμενος), θα στείλει την αίτηση κλήσης SIP INVITE (βλέπε Σχήμα 3–2) στον κατάλληλο πληρεξούσιο εξυπηρέτη ο οποίος αφού την επεξεργαστεί την προωθεί στον αποδέκτη του, ενημερώνοντας ταυτόχρονα τον καλούντα για την κατάσταση-εξέλιξη στην οποία βρίσκεται η κλήση που πραγματοποίησε. Η διαδικασία αυτή παρουσιάζεται στο Σχήμα 3–9. Αντίστοιχη είναι η διαδικασία που ακολουθείται και για τις άλλες μεθόδους-αιτήσεις.

Αξίζει να σημειωθεί ότι οι πληρεξούσιοι εξυπηρέτες λειτουργούν είτε σε «κατάσταση χωρίς μνήμη (stateless mode)», όπου απλά επεξεργάζονται ένα αντίγραφο του αρχικού μηνύματος μέχρι την αποστολή του στους κατάλληλους αποδέκτες, είτε σε «κατάσταση μνήμης (stateful mode)», όπου πέρα από το αντίγραφο του αρχικού μηνύματος πρέπει να διαχειριστούν την κατάσταση της κλήσης πραγματοποιώντας τον αντίστοιχο συσχετισμό μεταξύ των αιτημάτων και αποκρίσεων. Με τον τρόπο αυτό δεν υπάρχουν άσκοπες επανεκπομπές μηνυμάτων αλλά δημιουργούνται επιπρόσθετες απαιτήσεις μνήμης και

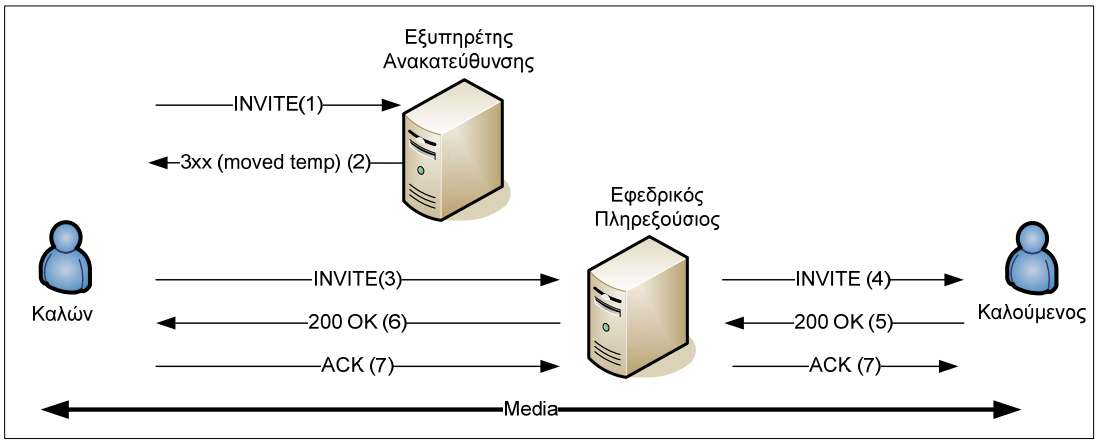
επεξεργαστικής ισχύος. Έχει υπολογιστεί ότι για τη διαχείριση κατάστασης κάθε κλήσης απαιτούνται περίπου 3kbytes μνήμης για χρονικό διάστημα λίγων δευτερολέπτων έως μερικών λεπτών, ανάλογα με τη διαμόρφωση του πληρεξούσιου και την υλοποίηση του.



Σχήμα 3–9. Παράδειγμα Διαδικασίας Αποκατάσταση Σύνδεσης

3.2.3.2.3 Εξυπηρέτης Ανακατεύθυνσης (Redirect)

Οι εξυπηρέτες ανακατεύθυνσης επιφορτίζονται με τη διαδικασία ενημέρωσης των χρηστών για τη χρήση εναλλακτικών συστημάτων για τη διεκπεραίωση των αιτημάτων τους. Ουσιαστικά, σε όλες τις αιτήσεις που λαμβάνουν αποκρίνονται με τους εναλλακτικούς προορισμούς στους οποίους μπορούν να αποστείλουν την αίτηση τους οι χρήστες της υπηρεσίας. Για παράδειγμα, ας υποθέσουμε ότι η διαδικασία εγκατάστασης κλήσης, όπως περιγράφτηκε στην ενότητα 3.2.3.2.2, μπορεί να μην είναι δυνατόν να πραγματοποιηθεί μέσω του προκαθορισμένου πληρεξούσιου εξυπηρέτη (π.χ λόγω αναβάθμισης του). Σε αυτή την περίπτωση ο εξυπηρέτης ανακατεύθυνσης αναλαμβάνει να ενημερώσει τον καλούντα για τους εναλλακτικούς πληρεξούσιους εξυπηρέτες που είναι διαθέσιμοι για την επεξεργασία της αίτησης. Μόλις ο καλών λάβει τη συγκεκριμένη πληροφορία, δύναται να δημιουργήσει μια νέα αίτηση και να την αποστείλει σ' έναν από τους εναλλακτικούς προορισμούς που περιείχε η απόκριση που έλαβε από τον εξυπηρέτη ανακατεύθυνσης. Η διαδικασία αυτή απεικονίζεται στο Σχήμα 3–10.



Σχήμα 3–10. Παράδειγμα Διαδικασίας Ανακατεύθυνσης

3.2.3.2.4 Εξυπηρέτης Πύλη (Gateway)

Οι εξυπηρέτες πύλες επιφορτίζονται με τη διασυνδεσιμότητα συστημάτων τηλεφωνίας που αξιοποιούν διαφορετικά πρωτόκολλα σηματοδοσίας. Στην αρχιτεκτονική του SIP ένας εξυπηρέτης πύλη αποτελεί ένα ειδικό πράκτορα χρήστη που λειτουργεί για λογαριασμό ενός πρωτοκόλλου και όχι κάποιου χρήστη. Η λειτουργία του είναι είτε να ενθυλακώνει (encapsulation) τη σηματοδοσία σε μηνύματα SIP, αξιοποιώντας το μηχανισμό Multipurpose Internet Mail Extensions (MIME) [46] στο κύριο μέρος του μηνύματος, είτε να μετατρέπει τη

σηματοδοσία από το ένα σύστημα στο άλλο και αντιστρόφως [47], με βάση συγκεκριμένους κανόνες. Σε περίπτωση όπου οι τελικοί χρήστες δεν έχουν δυνατότητα επεξεργασίας των δεδομένων φωνής, απαιτείται η χρήση των κατάλληλων πυλών πολυμέσων οι οποίες ενσωματώνουν και δυνατότητες μετατροπής της σηματοδοσίας από το ένα σύστημα στο άλλο. Για περισσότερες λεπτομέρειες βλέπε ενότητα 3.6.

3.2.4 Διασφάλιση της Αξιοπιστίας των Αιτήσεων στο SIP

Το SIP είναι ένα πρωτόκολλο δοσοληψίας (transactional protocol) στο οποίο πραγματοποιούνται αλληλεπιδράσεις μεταξύ των δικτυακών οντοτήτων με την ανταλλαγή μιας σειράς μηνυμάτων. Κάθε δοσοληψία στο SIP απαρτίζεται από την αρχική SIP αίτηση και όλες τις αποκρίσεις που σχετίζονται με αυτή.

Για τη διαχείριση των δοσοληψιών το SIP ορίζει ένα επίπεδο επιπλέον αυτών που ορίζονται σύμφωνα με την αρχιτεκτονική του διαδικτύου, γνωστό ως επίπεδο δοσοληψιών (transactional level). Το επίπεδο αυτό βρίσκεται μεταξύ του επιπέδου μεταφοράς και του επιπέδου εφαρμογής (βλέπε Σχήμα 3–11) και αξιοποιείται σε περιπτώσεις χρήσης πρωτοκόλλων μεταφοράς που δεν υποστηρίζουν μηχανισμούς για την αξιόπιστη μετάδοση των δεδομένων, όπως το πρωτόκολλο UDP το οποίο για παράδειγμα δεν υποστηρίζει μηχανισμό επιβεβαίωσης αποστολής / λήψης μηνυμάτων.

Επίπεδο Εφαρμογής	UAC	UAS	Πληρεξούσιος με μνήμη	Πληρεξούσιος χωρίς μνήμη
Επίπεδο Δοσοληψιών	Δοσ. Πελάτη	Δοσ. Εξηπυρέτη	Δοσολ. Πελ. & Εξυπ.	
Επίπεδο Μεταφοράς	UDP			

Σχήμα 3–11. Επίπεδο Δοσοληψίας στο SIP

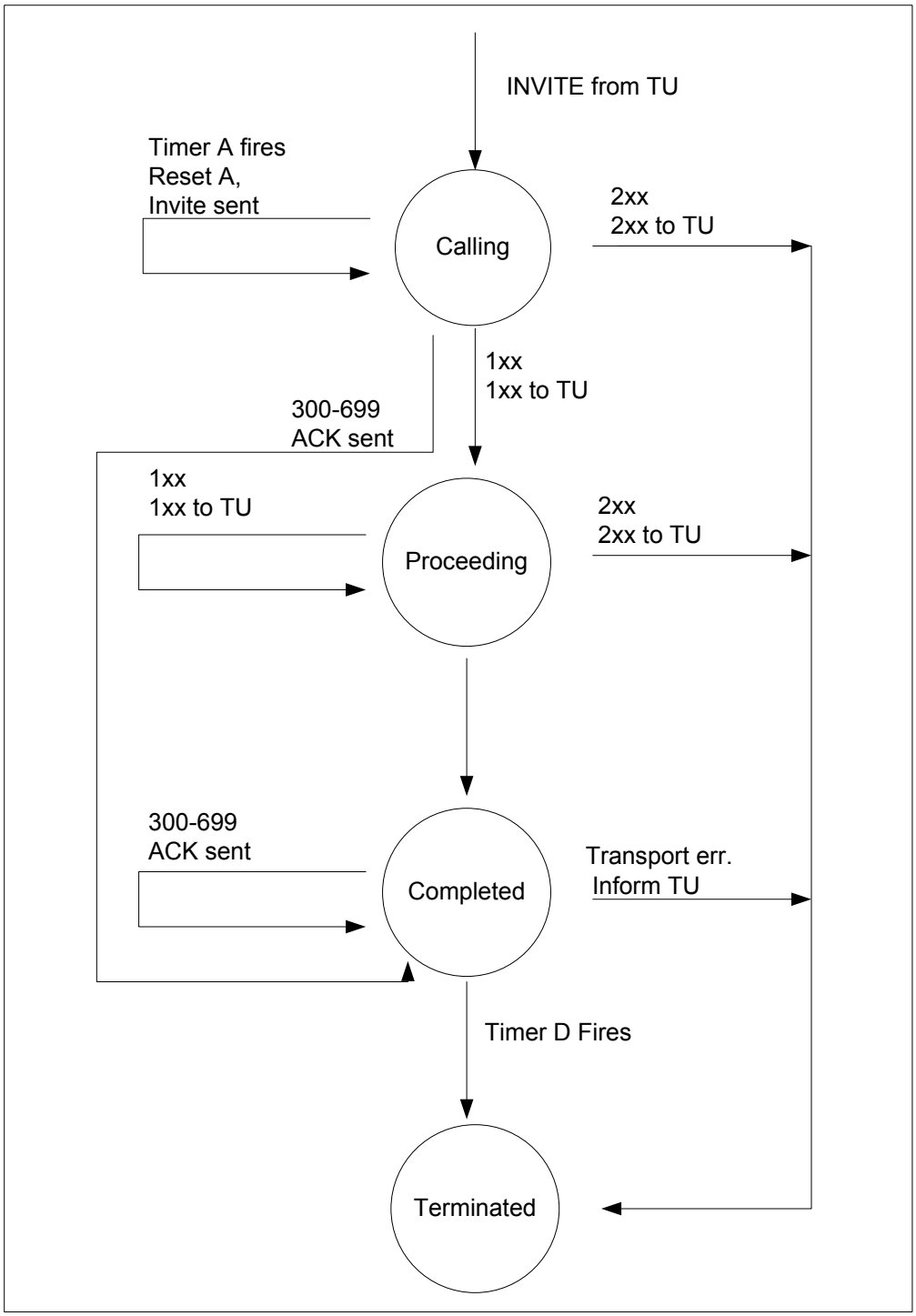
Συγκεκριμένα, μέσω του επιπέδου δοσοληψιών, το SIP προσδιορίζει δύο κατηγορίες δοσοληψιών:

1. Δοσοληψίες Πελάτη (Client transaction) και
2. Δοσοληψίες Εξυπηρέτη (Server Transaction).

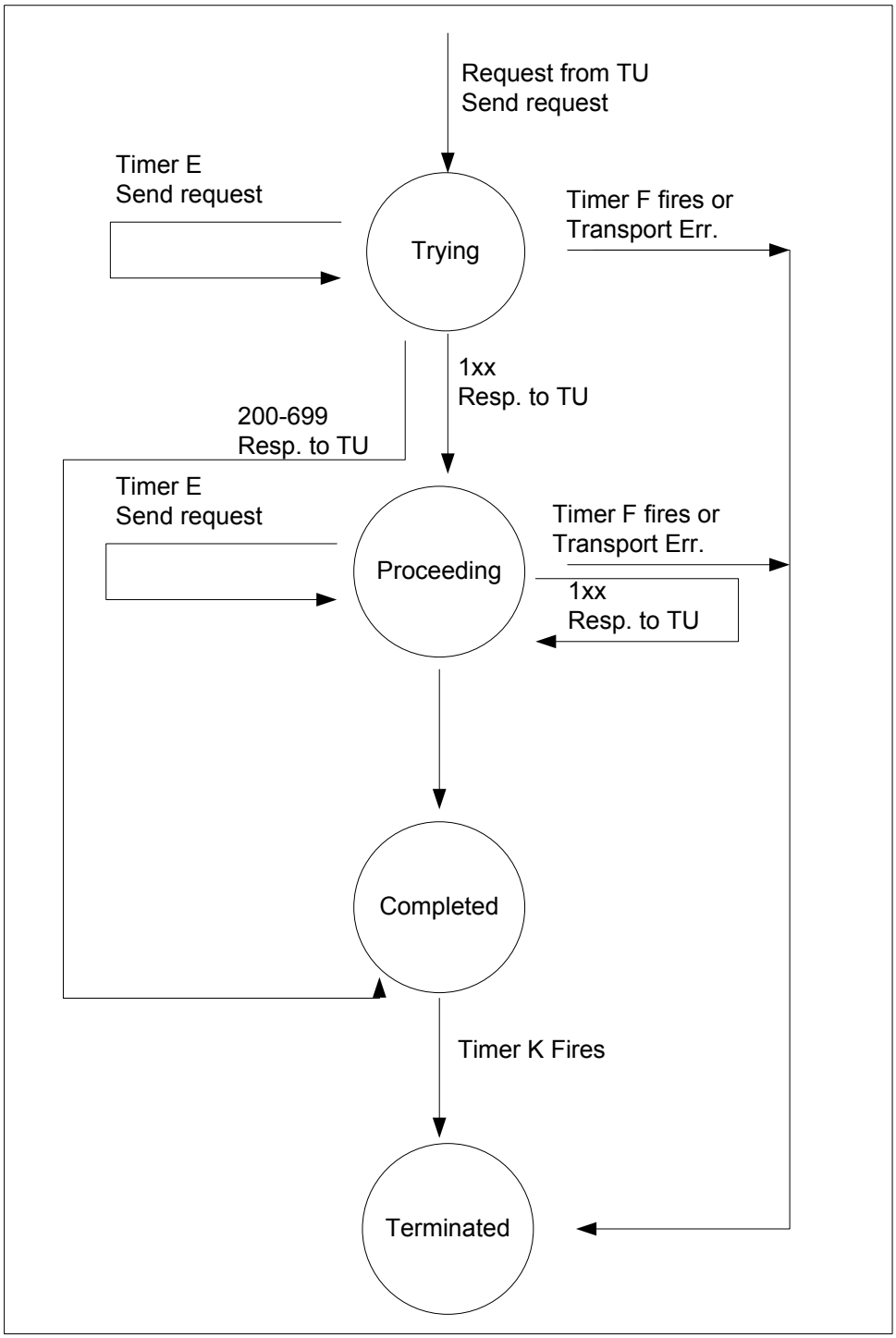
Κάθε μία από τις παραπάνω κατηγορίες διαχειρίζεται τα μηνύματα με ξεχωριστό τρόπο, ανάλογα με τον τύπο του μηνύματος (όπως εμφανίζει ο Πίνακας 3–5). Για κάθε κατηγορία δοσοληψίας το SIP δημιουργεί μια διαφορετική μηχανή πεπερασμένης κατάστασης (Finish State Machine–(FSM)) η οποία και αποτελεί τον πυρήνα διαχείρισης των αντίστοιχων μηνυμάτων (βλέπε Σχήμα 3–12 έως Σχήμα 3–15). Περισσότερες λεπτομέρειες αναφέρονται στις προδιαγραφές του SIP [11]. Αξίζει να σημειωθεί ότι ο διαχωρισμός των δοσοληψιών σε INVITE και μη-INVITE πραγματοποιείται λόγω των διαφορετικών διαδικασιών που ακολουθούνται για τη διαχείριση μιας συνόδου. Συγκεκριμένα, η εγκαθίδρυση (SIP INVITE) μιας συνόδου αξιοποιεί μια τριμερή διαδικασία, ενώ οι υπόλοιπες υπηρεσίες που παρέχονται στο SIP αξιοποιούν το γενικότερο μοντέλο αιτήματος-απόκρισης.

Κατηγορία	Τύπος Αίτησης	Σύντομη Περιγραφή
Δοσοληψίες Πελάτη	INVITE	Αφορά τη δημιουργία μηχανής πεπερασμένης κατάστασης ως αποτέλεσμα αποστολής αίτησης SIP INVITE από ένα πελάτη δοσοληψιών (βλέπε Σχήμα 3–12)
	μη-INVITE	Αφορά τη δημιουργία μηχανής πεπερασμένης κατάστασης ως αποτέλεσμα αποστολής μηνυμάτων πέρα του SIP INVITE (βλέπε Σχήμα 3–13)
Δοσοληψίες Εξυπηρέτη	INVITE	Αφορά τη δημιουργία μηχανής πεπερασμένης κατάστασης ως αποτέλεσμα της λήψης SIP INVITE αίτησης από ένα εξυπηρέτη δοσοληψιών (βλέπε Σχήμα 3–14)
	μη -INVITE	Αφορά τη δημιουργία μηχανής πεπερασμένης κατάστασης ως αποτέλεσμα της λήψης πέρα του SIP INVITE (βλέπε Σχήμα 3–15)

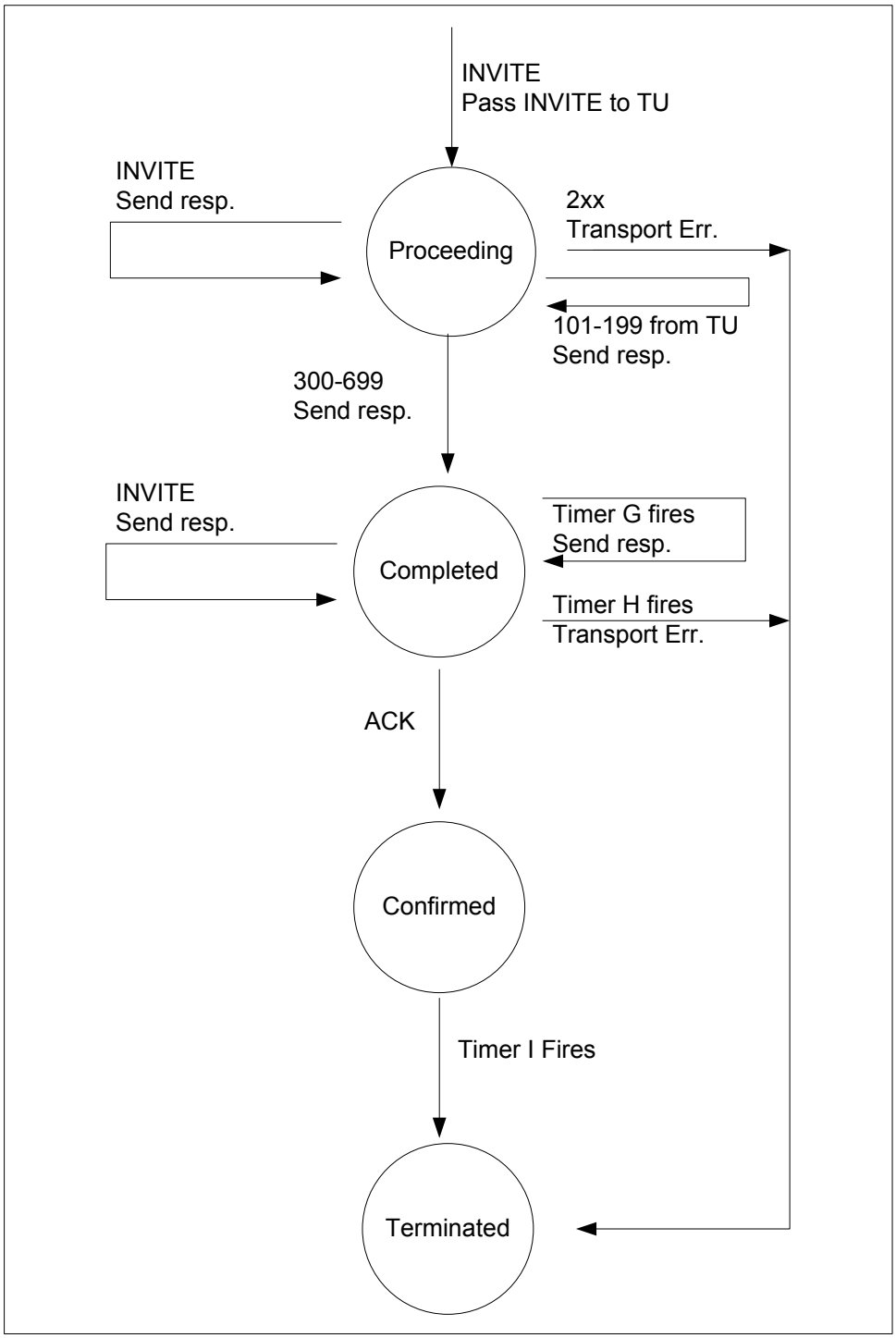
Πίνακας 3–5. Κατηγορίες Δοσοληψιών στο SIP



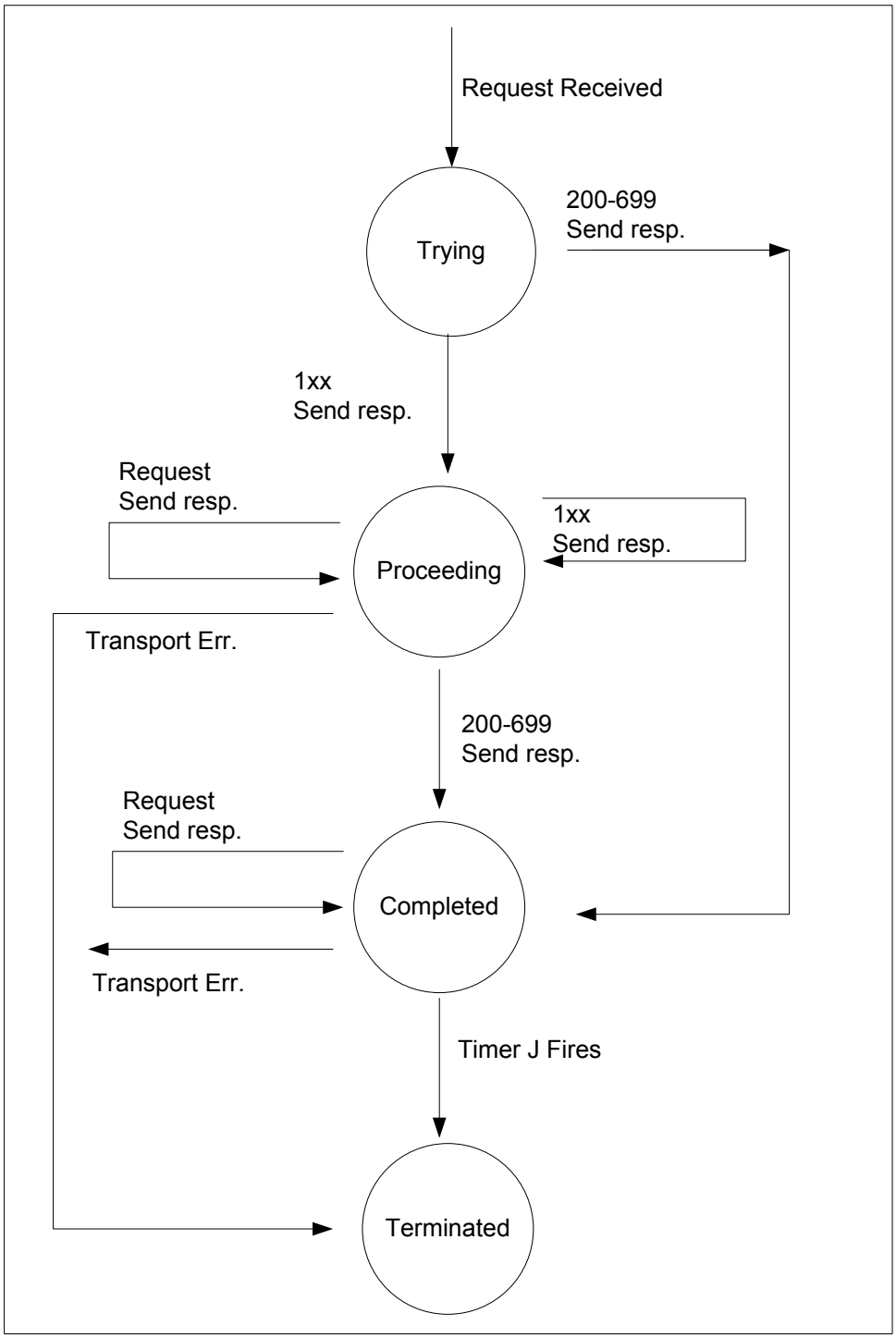
Σχήμα 3–12. Μηχανή Πεπερασμένης Κατάστασης για INVITE σε Δοσοληψίες Πελάτη



Σχήμα 3–13. Μηχανή Πεπερασμένης Κατάστασης για μη - INVITE σε Δοσοληψίες Πελάτη



Σχήμα 3–14. Μηχανή Πεπερασμένης Κατάστασης για INVITE σε Δοσοληψίες Εξυπηρέτη

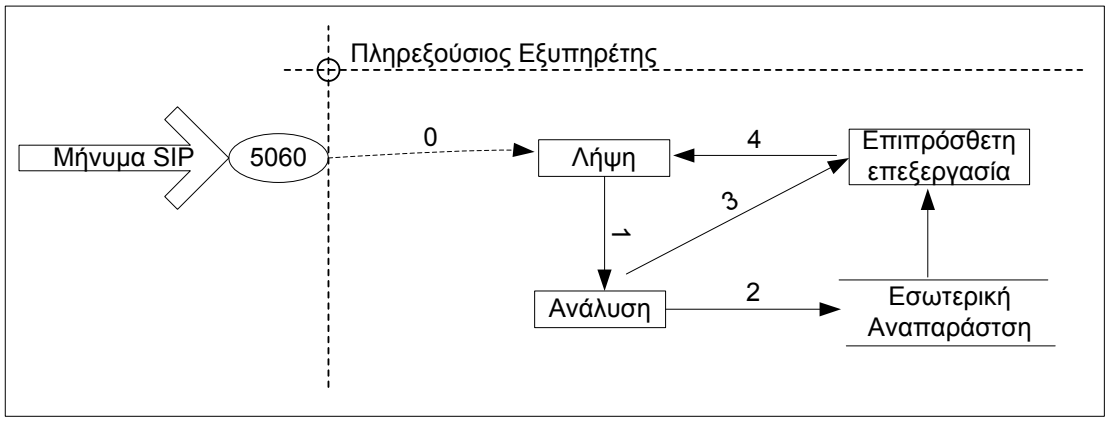


Σχήμα 3–15. Μηχανή Πεπερασμένης Κατάστασης για μη - INVITE σε Δοσοληψίες Εξυπηρέτη

3.2.5 Γενικό Μοντέλο Λειτουργίας SIP Οντοτήτων

Κάθε εισερχόμενο μήνυμα που λαμβάνεται από κάποια δικτυακή οντότητα SIP, θα πρέπει να αναλυθεί συντακτικά (message parsing), ώστε να αναπαρασταθεί στην εσωτερική δομή που αξιοποιείται από τη συγκεκριμένη οντότητα, και στη συνέχεια να δημιουργηθεί η κατάλληλη μηχανή πεπερασμένης κατάστασης (σύμφωνα με τον τύπο τους αιτήματος - βλέπε ενότητα 3.2.4) για να διασφαλιστεί η αξιόπιστη μετάδοση του αιτήματος. Στο Σχήμα 3–16 απεικονίζεται η γενική προσέγγιση που ακολουθείται για την επεξεργασία των SIP

μηνυμάτων από τις διάφορες οντότητες του SIP. Αξίζει να σημειωθεί ότι η διαδικασία αυτή πιθανόν να διαφοροποιείται ελαφρώς με βάση τον κατασκευαστή της SIP οντότητας. Αναλυτικότερα μια SIP οντότητα λαμβάνει τα SIP μηνύματα στην προκαθορισμένη θύρα (port) 5060, εκτός και εάν έχει ορισθεί διαφορετική θύρα από το διαχειριστή της υπηρεσίας. Αμέσως μόλις ένα μήνυμα παραληφθεί προωθείται στον αναλυτή μηνυμάτων ώστε να αναπαρασταθεί στην εσωτερική δομή που αξιοποιεί η SIP οντότητα και να δημιουργηθεί, εάν απαιτείται, η κατάλληλη μηχανή πεπερασμένης κατάστασης.



Σχήμα 3–16. Γενική Μέθοδος Επεξεργασίας SIP Μηνυμάτων

3.3 Το πρωτόκολλο Σηματοδοσίας H.323

Το H.323 [10], όπως και το SS7, είναι μια σουίτα προδιαγραφών και πρωτοκόλλων (ο Πίνακας 3–6 αποτυπώνει συνοπτικά τα διαφορετικά πρωτόκολλα που αξιοποιούνται σε αυτό) που αποτελεί μια ολοκληρωμένη λύση για την παροχή υπηρεσιών τηλεφωνίας. Το H.323 δεν έχει σχεδιαστεί αποκλειστικά και μόνο για χρήση στο διαδίκτυο αλλά και για εφαρμογή του σε δίκτυα όπως το ATM και το PSTN. Επιπλέον, για λόγους συμβατότητας με το σύστημα σηματοδοσίας SS7, ακολουθείται η ίδια δομή για τη σύνταξη μηνυμάτων (η οποία βασίζεται στο σύστημα ASN.1 [48]).

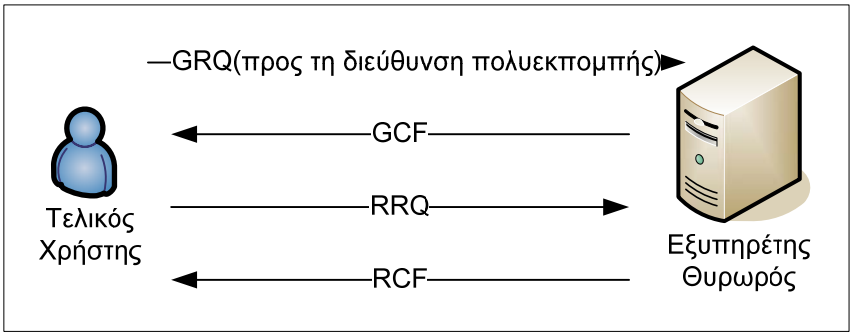
Όπως στο SIP έτσι και στο H.323, για να υποστηριχθούν υπηρεσίες τηλεφωνίας απαιτούνται οι παρακάτω δικτυακές οντότητες:

- Τερματικοί Σταθμοί.
- Οι εξυπηρέτες θυρωροί (Gatekeepers), οι οποίοι παρέχουν υπηρεσίες σηματοδοσίας.
- Οι εξυπηρέτες πύλες (Gateways), οι οποίοι παρέχουν διασυνδεσιμότητα με άλλα συστήματα τηλεφωνίας.
- Πολυσημειακές Μονάδες Ελέγχου (Multipoint control units MCUs), οι οποίες παρέχουν υπηρεσίες τηλε-συνδιάσκεψης.

Πρωτόκολλο	Σύντομη Περιγραφή
H.225	Προσδιορίζει τις προδιαγραφές για την εγγραφή-εισαγωγή των χρηστών στην υπηρεσία, τον έλεγχο εξουσιοδότησης στους πόρους της υπηρεσίας και τον έλεγχο διαθεσιμότητας των απαιτούμενων πόρων για την αποκατάσταση μιας σύνδεσης.
H.245	Προσδιορίζει τις προδιαγραφές για τη διαχείριση των πολυμεσικών δεδομένων όπως η διαπραγμάτευση (α) των χρησιμοποιούμενων κωδικοποιητών, μεταξύ των τερματικών, (β) των απαραίτητων παραμέτρων για την ολοκλήρωση μιας συνόδου, κ.α.
H.235	Προσδιορίζει τους μηχανισμούς ασφάλειας που μπορούν να αξιοποιηθούν σε μια σύνοδο.
G.7xx	Προσδιορίζει τις προδιαγραφές ήχου που μπορούν να αξιοποιηθούν σε μια σύνοδο.
H.26x	Προσδιορίζει τις προδιαγραφές εικόνας που μπορούν να αξιοποιηθούν σε μια σύνοδο.
H.450	Προσδιορίζει τις προδιαγραφές για επιπρόσθετες υπηρεσίες.

Πίνακας 3–6. Η Σουίτα Πρωτοκόλλων H.323

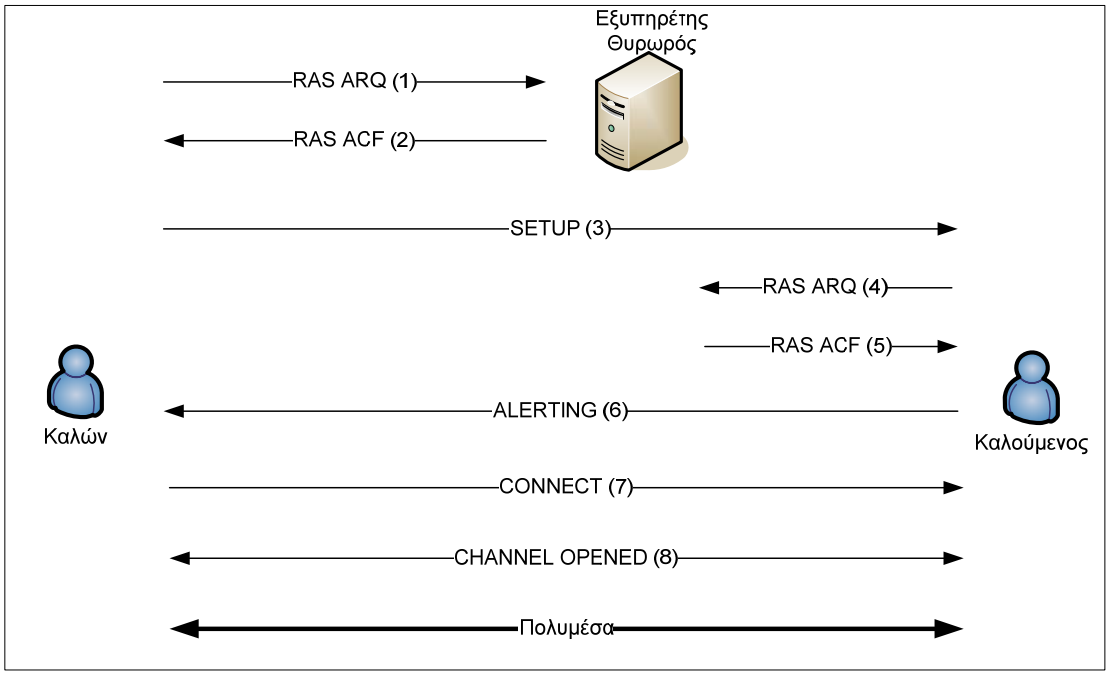
Για τη χρήση μιας υπηρεσίας τηλεφωνίας που αξιοποιεί το H.323 απαιτείται η εγγραφή του χρήστη (Registration) σε αυτή μέσω του εξυπηρέτη θυρωρού. Σε περίπτωση που ο χρήστης δε γνωρίζει τη διεύθυνση του εξυπηρέτη θυρωρού, θα πρέπει να αποστείλει σχετικό αίτημα στη διεύθυνση πολυεκπομπής (multicast address). Ο υπεύθυνος θυρωρός επεξεργάζεται την αίτηση και αποκρίνεται με ένα μήνυμα επιβεβαίωσης θυρωρού (Gatekeeper Confirmation–(GCF)), ενημερώνοντας με τον τρόπο αυτό το χρήστη για τη δικτυακή του διεύθυνση. Στη συνέχεια ο χρήστης μπορεί να εγγραφεί στην υπηρεσία δημιουργώντας μια αίτηση εγγραφής προς τον εξυπηρέτη θυρωρό, οποίος σε περίπτωση αποδοχής της, αποκρίνεται με ένα μήνυμα επιβεβαίωσης εγγραφής (Registration Confirmation–(RCF)). Η διαδικασία αυτή απεικονίζεται στο Σχήμα 3–17.



Σχήμα 3–17. Παράδειγμα Διαδικασία Εγγραφής στο H.323

Με τον επιτυχή τερματισμό της διαδικασίας εγγραφής ο χρήστης είναι σε θέση να διεκπεραιώσει κλήσεις προς τους αριθμούς που επιθυμεί, μέσω του εξυπηρέτη θυρωρού. Ο εγγεγραμμένος χρήστης (καλών) θα πρέπει αρχικά να αποστείλει προς τον εξυπηρέτη Θυρωρό μια αίτηση αποδοχής κλήσης (Admission Request–(ARQ)). Αυτός με τη σειρά του ελέγχει τα δικαιώματα κλήσης του καλούντα και την ύπαρξη των διαθέσιμων πόρων για τη διεκπεραίωση της κλήσης, οπότε και αποκρίνεται με ένα μήνυμα επιβεβαίωσης αποδοχής κλήσης (Admission Confirmation–(ACF)), εφόσον οι έλεγχοι έχουν ολοκληρωθεί επιτυχώς. Στο προαναφερόμενο μήνυμα προσδιορίζονται οι βασικές παράμετροι (π.χ διαθέσιμο εύρος ζώνης, διευθύνσεις μεταφοράς κτλ) για την αποκατάσταση της κλήσης. Στη συνέχεια ο

καλών δημιουργεί ένα μήνυμα αποκατάστασης συνόδου (SETUP) το οποίο και αποστέλλει στον καλούμενο. Μόλις η τερματική συσκευή του καλούμενου λάβει την εισερχόμενη κλήση «ενημερώνει» σχετικά τον καλούμενο και αποστέλλει ένα μήνυμα ειδοποίησης (ALERTING) προς τον καλούντα. Υποθέτοντας ότι ο καλούμενος αποδέχεται την κλήση θα στείλει ένα μήνυμα σύνδεσης (CONNECT), επιτρέποντας στη συνέχεια τη διαπραγμάτευση (negotiation) των κωδικοποιητών (codecs) που θα χρησιμοποιηθούν, ώστε οι χρήστες να είναι δυνατόν να επικοινωνήσουν επιτυχώς. Η προαναφερόμενη διαδικασία απεικονίζεται στο Σχήμα 3–18



Σχήμα 3–18. Παράδειγμα Διαδικασίας Αποκατάστασης Κλήσης στο H.323

Αντιστοίχως, για τον τερματισμό της επικοινωνίας είτε ο καλών είτε ο καλούμενος στέλνει το κατάλληλο μήνυμα προς τον εξυπηρέτη θυρωρό ο οποίος και το προωθεί στην άλλη οντότητα, ενώ ταυτόχρονα απελευθερώνει όλους τους πόρους που σχετίζονται με τη σύνοδο των δύο συγκεκριμένων χρηστών.

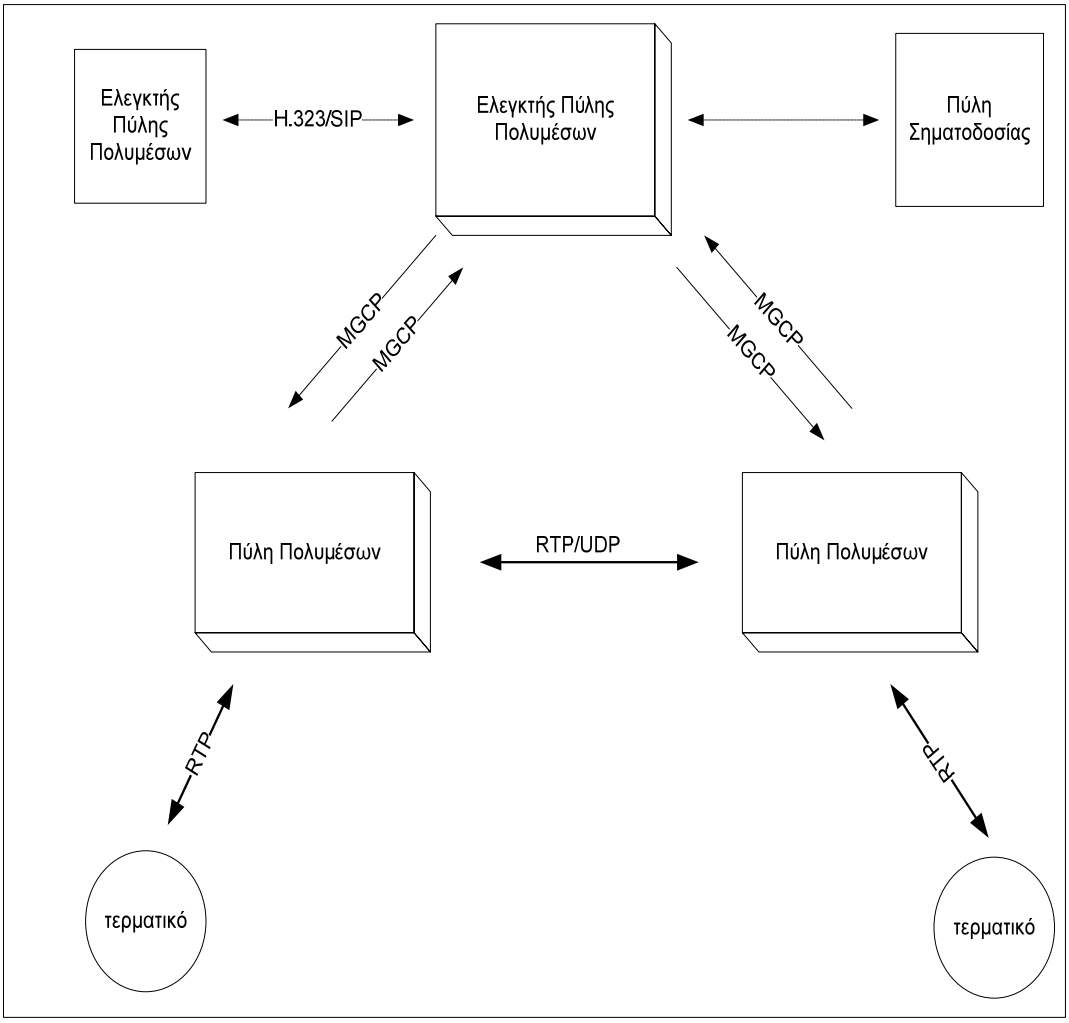
3.4 Το Πρωτόκολλο Ελέγχου Πολυμεσικών Πυλών (Media Gateway Control Protocol)

Οι εξυπηρέτες πύλες πολυμέσων (media gateway servers) υποστηρίζουν την απαραίτητη διασυνδεσιμότητα μεταξύ PSTN και IP δικτύων, μετατρέποντας τα πακέτα RTP σε μορφή κατάλληλη για μετάδοση στο PSTN και αντιστρόφως. Τέτοιες δικτυακές οντότητες εντοπίζονται στην «περιφέρεια» ενός δικτύου τηλεφωνίας για την τροποποίηση-μετάφραση των δεδομένων φωνής από το ένα σύστημα στο άλλο. Το Πρωτόκολλο Ελέγχου Πολυμεσικών Πυλών (Media Gateway Control Protocol– (MGCP)) [40] αποτελεί ίσως το πιο χαρακτηριστικό παράδειγμα τέτοιων πρωτοκόλλων και εμπλέκει δύο βασικές οντότητες:

1. Τον ελεγκτή πύλης πολυμέσων (Controller Media Gateway) γνωστό και ως Πράκτορα Κλήσεων (Call Agent), και
2. Την Πύλη Πολυμέσων.

Όπως φαίνεται και στο Σχήμα 3–19 ο ελεγκτής πύλης πολυμέσων έχει τον κεντρικό έλεγχο των πυλών πολυμέσων. Σε αντίθεση με το H.323 και το SIP, το MGCP είναι ένα πρωτόκολλο τύπου κυρίου-υπηρέτη (master-slave) και συνεπώς οι υπηρέτες-συσκευές μπορούν να

μεταδώσουν πληροφορίες ή να εκτελέσουν εντολές μόνο μετά από σχετικό αίτημα της κύριας οντότητας. Προκύπτει λοιπόν ότι εξαιτίας της αρχιτεκτονικής του το MGCP δεν είναι δυνατόν να αξιοποιηθεί για την επικοινωνία των ελεγκτών και για το λόγο αυτό είναι απαραίτητη η χρήση ενός εκ των πρωτοκόλλων σηματοδοσίας SIP/H.323.



Σχήμα 3–19. Η Βασική Αρχιτεκτονική του MGCP

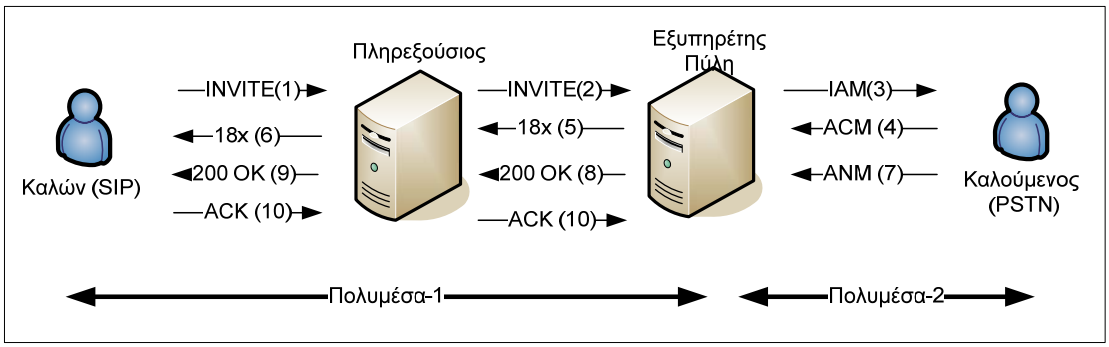
3.5 Τοπολογίες Διαδικτυακής Τηλεφωνίας

Τα συστήματα διαδικτυακής τηλεφωνίας[2] μπορούν να αξιοποιηθούν για τη διαχείριση κλήσεων μεταξύ χρηστών που βρίσκονται:

1. Μόνο σε IP δίκτυα: Σε αυτή την περίπτωση οι επικοινωνούντες οντότητες (καλών και καλούμενος) βρίσκονται σε κάποιο IP δίκτυο και η επικοινωνία πραγματοποιείται με την διαμεσολάβηση των κατάλληλων εξυπηρετών (βλέπε Σχήμα 3–9)
2. Σε IP και PSTN δίκτυα: Σε αυτή την περίπτωση οι επικοινωνούντες οντότητες (καλών και καλούμενος) βρίσκονται σε διαφορετικά δίκτυα (IP και PSTN ή αντιστρόφως). Ανεξάρτητα από την οντότητα (IP ή PSTN) που αρχικοποίησε την κλήση, αυτή θα πρέπει να δρομολογηθεί μεταξύ PSTN, πύλης (gateway), πληρεξούσιου (proxy) και αντιστρόφως. Η διαδικασία αποκατάστασης μίας κλήσης

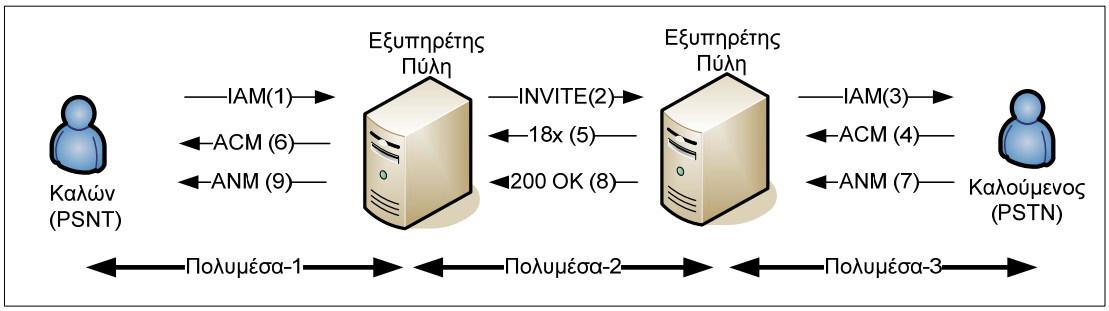
[2] Στη παρούσα ενότητα γίνεται ενδεικτική αναφορά στο πρωτόκολλο SIP, αν και τα αναγραφόμενα ισχύουν και για τα υπόλοιπα πρωτόκολλα

που αρχικοποιήθηκε από ένα IP τερματικό και τερματίζεται σε ένα PSTN τερματικό απεικονίζεται στο Σχήμα 3–20. Αντίστοιχη διαδικασία ακολουθείται και στην περίπτωση που ο καλών είναι χρήστης PSTN.



Σχήμα 3–20. Παράδειγμα Κλήσης μεταξύ IP και PSTN

3. Μόνο σε PSTN δίκτυα (μέσω IP δικτύων): Σε αυτή την περίπτωση οι επικοινωνούντες οντότητες βρίσκονται στο PSTN με τη διαφορά ότι η κλήση δε δρομολογείται μέσω του PSTN αλλά μέσω του IP δικτύου των παρόχων αξιοποιώντας τους κατάλληλους εξυπηρέτες πύλες (gateways).



Σχήμα 3–21. Παράδειγμα Κλήσης PSTN προς PSTN μέσω IP δικτύων

Περισσότερες λεπτομέρειες για τις τοπολογίες τηλεφωνίας στο SIP αναφέρονται στην εργασία [47].

3.6 Πρωτόκολλα Μεταφοράς Φωνής και Πολυμεσικών Δεδομένων

Το πρωτόκολλο Real-Time Transport Protocol (RTP) [34] όπως απεικονίζεται και στο Σχήμα 2–5 στρωματοποιείται στο επίπεδο εφαρμογής και αναπτύχθηκε με σκοπό την μετάδοση, μεταξύ δύο ή περισσοτέρων χρηστών, δεδομένων πραγματικού χρόνου (real time data) μέσω δικτύων IP. Όλες οι απαραίτητοι παράμετροι επικοινωνίας έχουν προσδιοριστεί κατά τη διαδικασία αποκατάστασης της σύνδεσης (βλέπε Σχήμα 3–9).

Τα δεδομένα πραγματικού χρόνου και συγκεκριμένα τα δεδομένα φωνής, απαιτούν την ικανοποίηση συγκεκριμένων απαιτήσεων για παράδοση από άκρο σε άκρο (end-to-end delivery), αφού οποιαδήποτε χρονική επιβάρυνση επηρεάζει (αρνητικά) την ποιότητα της παρεχόμενης υπηρεσίας. Για το λόγο αυτό το συγκεκριμένο πρωτόκολλο υποστηρίζει επιπρόσθετες υπηρεσίες, όπως ανίχνευση απωλειών, λήψη εκτός σειράς (out of sequence) κτλ, για την καλύτερη διαχείριση και τη βελτίωση ποιότητας των παρεχόμενων υπηρεσιών.

3.7 Βοηθητικά Πρωτόκολλα

Για την παροχή ολοκληρωμένων υπηρεσιών τηλεφωνίας μέσω διαδικτύου, όπως αναφέρεται ήδη στο Κεφάλαιο 2, αξιοποιούνται είτε τα υπάρχοντα πρωτόκολλα εφαρμογής, είτε νέα πρωτόκολλα που αναπτύσσονται για να καλύψουν τις επιπρόσθετες απαιτήσεις που έχουν προκύψει από τις συγκεκριμένες υπηρεσίες. Τα κυριότερα βοηθητικά πρωτόκολλα είναι τα ακόλουθα:

1. Dynamic Host Configuration Protocol (DHCP) [36]: Το DHCP αξιοποιείται κυρίως κατά την σύνδεση και αρχικοποίηση της διαδκτυακής τηλεφωνικής συσκευής του χρήστη σε ένα IP δίκτυο, για την αυτόματη λήψη των ρυθμίσεων που απαιτούνται για την ορθή λειτουργία της.
2. Domain Name System (DNS) [35]: Το DNS αξιοποιείται για την επίλυση συμβολικών ονομάτων στην αντίστοιχη IP διεύθυνση και αντιστρόφως (σε όποιες περιπτώσεις απαιτείται).
3. Telephone Number Mapping (ENUM) [49]: Το ENUM αξιοποιείται για τη διασύνδεση μεταξύ συστημάτων τηλεφωνίας PSTN και IP, αντιστοιχίζοντας τους τηλεφωνικούς αριθμούς με διαδικτυακές διευθύνσεις και αντιστρόφως. Οι διευθύνσεις αυτές αποθηκεύονται στον κατάλληλο DNS με τη μορφή εγγραφών Naming Authority Pointer (NAPTR) [50].

3.7.1 Χρήσεις Βοηθητικών Πρωτοκόλλων

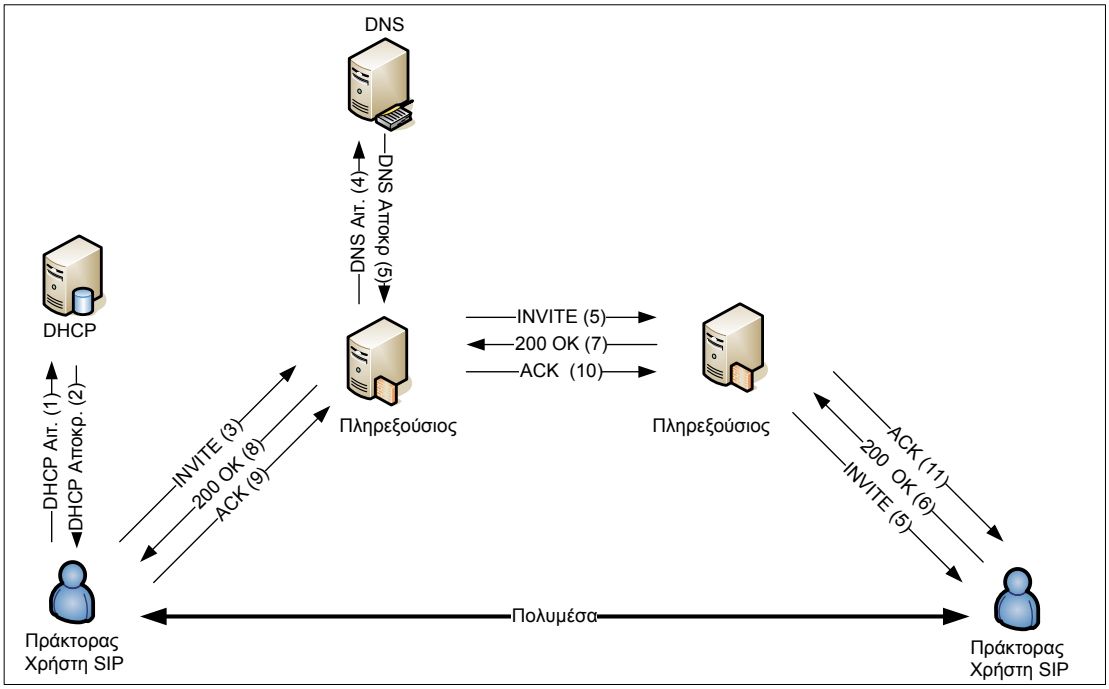
Κατά τη σύνδεση ενός IP τηλεφώνου στο δίκτυο απαιτείται η αρχικοποίηση του με τις απαραίτητες ρυθμίσεις, όπως για παράδειγμα ανάθεση IP διεύθυνσης, τη διεύθυνση του DNS εξυπηρέτη κτλ. Οι ρυθμίσεις αυτές γίνονται αυτόματα μέσω του πρωτοκόλλου DHCP. Στη συνέχεια ο χρήστης δύναται:

1. να πραγματοποιεί κλήσεις αξιοποιώντας είτε τηλεφωνικά νούμερα είτε τα αντίστοιχα URI.
2. να δέχεται κλήσεις είτε στο URI ή στο τηλεφωνικό νούμερο που του έχει δώσει ο πάροχος της υπηρεσίας.

Στην περίπτωση κατά την οποία ένας χρήστης (καλών) επιθυμεί να καλέσει κάποιον άλλο χρήστη (καλούμενος) κάνοντας χρήση του URI, θα πρέπει να δημιουργήσει το κατάλληλο αίτημα και να το προωθήσει στον πληρεξούσιο ή θυρωρό εξυπηρέτη. Ο υπεύθυνος εξυπηρέτης με τη σειρά του, θα αναζητήσει τον κατάλληλο εξυπηρέτη που είναι υπεύθυνος για τη διαχείριση αιτημάτων του τομέα (domain) που περιγράφεται στο URI της αίτησης που δημιούργησε ο καλών.

Η αναζήτηση αυτή πραγματοποιείται μέσω του DNS εξυπηρέτη. Μόλις ο πληρεξούσιος λάβει την απάντηση από το DNS προωθεί την αίτηση του χρήστη στον κατάλληλο πληρεξούσιο και αυτός με τη σειρά του εντοπίζει το χρήστη που προσδιορίζεται στο URI.

Η παραπάνω διαδικασία για το πρωτόκολλο σηματοδοσίας SIP απεικονίζεται στο Σχήμα 3–22. Αντίστοιχη διαδικασία ακολουθείται και στην περίπτωση χρήσης τηλεφωνικών αριθμών αντί διευθύνσεων URI, με μοναδική διαφορά ότι απαιτείται η ύπαρξη των κατάλληλων NAPTR εγγραφών στον DNS, όπως καθορίζεται από το πρωτόκολλο ENUM.



Σχήμα 3–22. Αξιοποίηση Βοηθητικών Πρωτοκόλλων στο SIP

3.8 Συμπεράσματα

Η υπηρεσία διαδικτυακής τηλεφωνίας είναι ένα πολύπλοκο σύστημα που αξιοποιεί διαφορετικά πρωτόκολλα σηματοδοσίας και διαφορετικά συστήματα μετάδοσης φωνής. Με στόχο τη δημιουργία ενός ενιαίου και αξιόπιστου δικτύου τηλεφωνίας, όπως αυτό του PSTN, είναι απαραίτητο να διασφαλιστεί η μεταξύ των διασυνδεσιμότητα.

Σε αντίθεση με το PSTN η υπηρεσία διαδικτυακής τηλεφωνίας βασίζεται κυρίως σε πρότυπα ανοικτών προδιαγραφών τα οποία εφαρμόζονται επιτυχώς σε κατανεμημένες αρχιτεκτονικές όπως αυτή του διαδικτύου. Διαφορετικές οντότητες (φυσικές και λογικές) ανεξαρτήτου θέσης επιφορτίζονται με την παροχή των επί μέρους υπηρεσιών που απαιτούνται για την επιτυχή λειτουργία της τηλεφωνικής υπηρεσίας στο διαδικτύο.

Η ανοικτή αυτή αρχιτεκτονική παρέχει ένα νέο σύνολο δυνατοτήτων για την παροχή εξελιγμένων τηλεφωνικών υπηρεσιών, κάτι που στο PSTN δεν ήταν δυνατόν να επιτευχθεί με χαμηλό κόστος για όλους τους χρήστες. Βέβαια η υπηρεσία διαδικτυακής τηλεφωνίας εισάγει νέα προβλήματα ασφαλείας, τα οποία κληρονομούνται από το διαδίκτυο και τα οποία πρέπει να αντιμετωπιστούν ιδιαίτερα αφού δεν είχαν εφαρμογή στο κλειστό περιβάλλον του PSTN.

ΚΕΦΑΛΑΙΟ 4: Προβλήματα Ασφάλειας Στα Συστήματα Διαδικτυακής Τηλεφωνία

4.1 Γενικά

Η προστασία των τηλεπικοινωνιακών πόρων αποτελεί ακρογωνιαίο λίθο για την αδιάλειπτη παροχή αξιόπιστων υπηρεσιών, ιδιαίτερα σε υπηρεσίες πραγματικού χρόνου όπως αυτή της τηλεφωνίας όπου οι χρήστες αναζητούν πέραν της αξιοπιστίας και την ασφάλεια των υπηρεσιών. Για το λόγο αυτό πριν από τη σχεδίαση και ανάπτυξη μιας υπηρεσίας είναι απαραίτητο να προσδιορίζονται οι πιθανές απειλές και ευπάθειες της υπηρεσίας ώστε να υιοθετούνται τα κατάλληλα μέτρα ασφαλείας, με στόχο την ελαχιστοποίηση της πιθανότητας εμφάνισης μιας απειλής ως επίθεση. Είναι ιδιαίτερα σημαντικό πριν την εφαρμογή οποιουδήποτε μέτρου ασφάλειας, να γνωρίζεις τους πιθανούς κινδύνους από τους οποίους πρέπει να προστατευθείς [51]. Για παράδειγμα σ' ένα κλειστό δίκτυο μπορείς να εμπιστευτείς κάποιο συγκεκριμένο χρήστη για το διαμοιρασμό των δεδομένων σου, ενώ σ' ένα ανοικτό δίκτυο αυτό μπορεί να επιτευχθεί μόνο μέσω της χρήσης των κατάλληλων μηχανισμών ασφαλείας οι οποίοι εξασφαλίζουν το επιθυμητό επίπεδο εμπιστοσύνης μεταξύ των δικτυακών οντοτήτων.

Το PSTN, αποτελεί ένα παράδειγμα της πρώτης κατηγορίας, δηλαδή βασίζεται σ' ένα κλειστό δίκτυο, όπου οι απειλές είναι περιορισμένες ενώ οποιαδήποτε παραβίαση μπορεί εύκολα να ανιχνευθεί [52]. Από την άλλη μεριά η διαδικτυακή τηλεφωνία, ανήκει στη δεύτερη κατηγορία, δηλαδή βασίζεται σ' ένα δίκτυο ανοικτής αρχιτεκτονικής, όπως αυτό του διαδικτύου, με διαφόρων τύπων προβλήματα ασφαλείας. Συνεπώς, οι πάροχοι υπηρεσιών διαδικτυακής τηλεφωνίας θα πρέπει να λάβουν υπόψη τους τις νέες απειλές που προκύπτουν από τη χρήση του διαδικτύου. Επιπροσθέτως, η διασυνδεσιμότητα που απαιτείται μεταξύ υπηρεσιών διαδικτυακής τηλεφωνίας και PSTN καθιστά το τελευταίο όμοια ευπαθές στις νέες απειλές.

Στις υπό-ενότητες που ακολουθούν πραγματοποιείται σύντομη επισκόπηση των προβλημάτων ασφαλείας που έχουν εμφανιστεί στο PSTN, καθώς όλες οι απειλές που παρουσιάζονται σε αυτό μεταφέρονται στην υπηρεσία της διαδικτυακής τηλεφωνίας. Στη συνέχεια γίνεται λεπτομερής ανάλυση των απειλών, των ευπαθειών και των επιθέσεων που μπορούν να πραγματοποιηθούν στην περίπτωση της διαδικτυακής τηλεφωνίας, δίνοντας κυρίως έμφαση στις υπηρεσίες που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP.

4.2 Επισκόπηση Προβλημάτων Ασφάλειας στο PSTN

Παρά το γεγονός ότι το PSTN έχει διάρκεια ζωής περισσότερο από 100 χρόνια, ελάχιστα μέτρα έχουν ληφθεί για την προστασία των δεδομένων που μεταδίδονται μέσω αυτού. Αυτό οφείλεται κυρίως στο γεγονός ότι βασίζεται σ' ένα κλειστό δίκτυο, στο οποίο υπάρχει περιορισμένη πρόσβαση και όλες οι οντότητες που συνδέονται σε αυτό θεωρούνται έμπιστες. Ακόμα όμως και σε αυτή τη περίπτωση (χρήση ενός κλειστού δικτύου) διάφορα προβλήματα ασφαλείας[3] έχουν αναφερθεί [53]-[58], που εκμεταλλεύονται είτε την έλλειψη των απαραίτητων μηχανισμών ασφαλείας, είτε τη μη ορθή διαχείριση των μηνυμάτων σηματοδοσίας.

[3] Θα πρέπει να σημειωθεί ότι οι επιθέσεις και τα προβλήματα ασφαλείας που παρουσιάζονται στους τηλεπικοινωνιακούς παρόχους, στις περισσότερες των περιπτώσεων δεν γίνονται ευρέως γνωστά, καθώς η δημοσιοποίηση τέτοιων γεγονότων επηρεάζουν (αρνητικά) σε μεγάλο βαθμό την εμπιστοσύνη των χρηστών στις παρεχόμενες υπηρεσίες, με αποτέλεσμα οι πηγές γύρω από το συγκεκριμένο θέμα να είναι αρκετά περιορισμένες.

Μεταξύ των πιο διαδεδομένων απειλών για τα επικοινωνιακά συστήματα είναι:

1. Η μη εξουσιοδοτημένη πρόσβαση (unauthorized access) στα δεδομένα σηματοδοσίας και φωνής.
2. Η διεκπεραίωση κλήσεων χωρίς χρέωση (toll frauds calls).
3. Η μεταμφίεση-πλαστοπροσωπία (impersonation).
4. Η άρνηση παροχής υπηρεσίας (denial of service).

Όλες οι προαναφερόμενες απειλές εκτός των απειλών μεταμφίεσης έχουν εκδηλωθεί ως επιθέσεις στο PSTN, καθώς ο κάθε χρήστης στο PSTN προσδιορίζεται από τη φυσική του σύνδεση.

Τα πρώτα προβλήματα ασφαλείας που εμφανίσθηκαν στο PSTN σχετίζονται τόσο με τη διεκπεραίωση κλήσεων χωρίς χρέωση [53] (κυρίως σε συστήματα σηματοδοσίας που αξιοποιούσαν εσωζωνικές τεχνικές), όσο και με τις υποκλοπές (eavesdropping) επικοινωνιών [54]. Τα παραπάνω προβλήματα ασφαλείας παρουσιάζονται στη μεν πρώτη περίπτωση λόγω μη ορθής διαχείρισης των μηνυμάτων που λαμβάνονται εκτός της προκαθορισμένης διαδικασίας (out-of-sequence messages), ενώ στη δεύτερη λόγω της έλλειψης μηχανισμών εμπιστευτικότητας (confidentiality) ή παραβίασης αυτών. Παρ' όλα αυτά, θα πρέπει να σημειωθεί ότι οι υποκλοπές κλήσεων παρουσιάζουν μεγάλο βαθμό δυσκολίας αφού απαιτείται φυσική πρόσβαση στο δίκτυο του PSTN, το οποίο είναι ένα κλειστό δίκτυο.

Επιπροσθέτως, με την εξέλιξη των συστημάτων σηματοδοσίας το τηλεφωνικό δίκτυο αποκτά μεγαλύτερη πολυπλοκότητα δημιουργώντας ταυτόχρονα νέες ευπάθειες. Κάτι τέτοιο παρατηρήθηκε κυρίως στις αρχές τις δεκαετίας του 1990, οπότε και είχαν αναφερθεί αρκετές προσπάθειες παραβίασης [55], επιδιώκοντας κατά κύριο λόγο να εκμεταλλευθούν «λάθη» στο λογισμικό των συστημάτων σηματοδοσίας. Επιπροσθέτως, με την απελευθέρωση των επικοινωνιών, εναλλακτικοί πάροχοι τηλεφωνίας (green houses) συνδέονται στον κύριο κορμό του τηλεφωνικού δικτύου, δημιουργώντας νέα πιθανά σημεία παραβίασης του [56]. Για παράδειγμα, ένας επιτιθέμενος μπορεί, μέσω ενός εναλλακτικού παρόχου τηλεφωνίας, να τροποποιήσει τα δεδομένα που αποθηκεύονται στο SCP (βλέπε ενότητα 2.3.1), ώστε οι κλήσεις ενός συγκεκριμένου χρήστη να δρομολογούνται όχι μόνο σε αυτόν αλλά ταυτοχρόνως και σε κάποια άλλη οντότητα. Χαρακτηριστικό παράδειγμα τέτοιας επίθεσης είναι οι υποκλοπές που πραγματοποιήθηκαν το 2004 στις συνδιαλέξεις μελών της Ελληνικής κυβέρνησης. Εναλλακτικά, ο επιτιθέμενος θα μπορούσε να δημιουργήσει προβλήματα διαθεσιμότητας στα αντίστοιχα SCP ώστε να μην είναι δυνατή η δρομολόγηση των κλήσεων, είτε δημιουργώντας μεγάλο πλήθος αιτήσεων προς αυτά, είτε αποστέλλοντας μηνύματα τα οποία δεν είναι βασισμένα στις αντίστοιχες προδιαγραφές (malformed messages). Θα πρέπει να σημειωθεί ότι σε πολλές περιπτώσεις επιθέσεων στο PSTN απαιτείται η συνεργασία με εσωτερικούς χρήστες για την επιτυχή περάτωση τους. Τα προβλήματα ασφάλειας που εντοπίζονται στο PSTN παρουσιάζονται αναλυτικά στις εργασίες [53]-[56].

Συμπερασματικά, τα προβλήματα ασφαλείας που εμφανίζονται στο PSTN οφείλονται:

1. Στην έλλειψη μηχανισμών ασφαλείας για την παροχή υπηρεσιών εμπιστευτικότητας (confidentiality), ακεραιότητας (integrity) και αυθεντικότητας (authenticity),
2. Στη μη ορθή διαχείριση των δεδομένων που υφίστανται επεξεργασία στο PSTN,
3. Καθώς και στη βοήθεια - συνεργασία που μπορεί να προσφέρουν εσωτερικοί χρήστες σε κάποιον επιτιθέμενο.

Παρ' όλα αυτά δεν υπάρχει συχνή εμφάνιση επιθέσεων [6] και αυτό οφείλεται στην κλειστή αρχιτεκτονική του δικτύου.

4.3 Απειλές και Ευπάθειες στη Διαδικτυακή Τηλεφωνία

Σε γενικές γραμμές οι απειλές που εμφανίζονται στα τηλεπικοινωνιακά συστήματα είναι παρόμοιες. Η κυριότερη διαφοροποίηση εντοπίζεται στον τρόπο εκδήλωσης μιας επίθεσης καθώς η αξιοποίηση διαφορετικών υποδομών για την παροχή της υπηρεσίας δημιουργεί διαφορετικά σημεία ευπάθειας τα οποία προσπαθούν να εκμεταλλευτούν οι επιτιθέμενοι για την εκδήλωση της επίθεσης. Πιο συγκεκριμένα, η υπηρεσία της τηλεφωνίας στο PSTN αξιοποιεί ένα κλειστό δίκτυο, ενώ στο διαδικτύο γίνεται χρήση ενός ανοικτού δικτύου. Όπως είναι φανερό δεν υπάρχει καμία απολύτως διαφοροποίηση της υπηρεσία της τηλεφωνίας αυτής καθαυτής. Αυτό που διαφοροποιείται είναι η υποδομή που αξιοποιείται για την παροχή της υπηρεσίας. Κατά συνέπεια, στην περίπτωση της διαδικτυακής τηλεφωνίας, είναι η εκδήλωση επιθέσεων που σχετίζονται τόσο με απειλές που εμφανίζονται στο PSTN όσο και με αυτές που εμφανίζονται στο διαδίκτυο.

Σε αντίθεση με το PSTN όπου η μη εξουσιοδοτημένη πρόσβαση για την υποκλοπή δεδομένων φωνής προϋποθέτει τη φυσική πρόσβαση σ' ένα κλειστό δίκτυο, στη διαδικτυακή τηλεφωνία η πρόσβαση στο δίκτυο είναι άμεση με αποτέλεσμα η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα των υπηρεσιών τηλεφωνίας (φωνής και σηματοδοσίας) να μην παρουσιάζει καμία ιδιαίτερη δυσκολία. Σε αυτό το σημείο θα πρέπει να επισημανθεί ότι η εφαρμογή μηχανισμών εμπιστευτικότητας, τουλάχιστον αναφορικά με τα δεδομένα σηματοδοσίας, υπάγεται σε αρκετούς περιορισμούς καθώς τα δεδομένα σηματοδοσίας θα πρέπει να δρομολογηθούν μέσω ενός ή περισσότερων εξυπηρετών τηλεφωνίας που απαιτούν να έχουν πρόσβαση σε αυτά για την ορθή αποστολή τους στον τελικό χρήστη (για περισσότερες λεπτομέρειες βλέπε ενότητα 5.2.5). Ο περιορισμός αυτός δεν ισχύει στην περίπτωση των δεδομένων φωνής, καθώς αυτά μεταδίδονται από χρήστη σε χρήστη (end-to-end) και δεν υπόκεινται σε επεξεργασία από ενδιάμεσους εξυπηρέτες όπως τα δεδομένα σηματοδοσίας. Επιπλέον, στη διαδικτυακή τηλεφωνία, όμοια με τις άλλες υπηρεσίες που παρέχονται μέσω διαδικτύου, παρέχονται οι κατάλληλες ευκαιρίες σε οποιαδήποτε οντότητα να τροποποιήσει τόσο τα δεδομένα φωνής όσο και της σηματοδοσίας. Σε αυτό το γεγονός συμβάλει και η μη εφαρμογή των κατάλληλων μηχανισμών διαφύλαξης της ακεραιότητας.

Μια απειλή που δεν αφορά το PSTN, αλλά εμφανίζεται στη διαδικτυακή τηλεφωνία είναι αυτή της πλαστοπροσωπίας, αφού ο χρήστης προσδιορίζεται από ένα αναγνωριστικό και όχι από κάποια φυσική διεύθυνση. Κατά συνέπεια, ένας επιτιθέμενος μπορεί να επιχειρήσει να στείλει κάποιο αίτημα προς τον πάροχο της διαδικτυακής τηλεφωνίας χρησιμοποιώντας το αναγνωριστικό κάποιου άλλου εξουσιοδοτημένου χρήστη (client impersonation) με στόχο, για παράδειγμα, την αποφυγή της χρέωσης του δικού του λογαριασμού. Εκτός αυτού, ο επιτιθέμενος είναι δυνατόν να προσπαθήσει να λειτουργήσει εκ μέρους της υπηρεσίας ή κάποιου εξυπηρέτη (service impersonation) αυτής, εκμεταλλευόμενος κυρίως το γεγονός ότι η πλευρά του δικτύου δεν αυθεντικοποιείται προς τους τελικούς χρήστες.

Μια άλλη σημαντική κατηγορία απειλών για τις υπηρεσίες τηλεφωνίας αφορούν απάτες χρεώσεων (toll frauds). Ενώ στο PSTN δεν υπάρχει η δυνατότητα χρεώσεων άλλων λογαριασμών παρά μόνο η πραγματοποίηση κλήσεων χωρίς χρέωση, στη διαδικτυακή τηλεφωνία, λόγω της ύπαρξης της απειλής πλαστοπροσωπίας χρήστη, και οι δύο προαναφερόμενες κατηγορίες απάτης είναι πιθανές. Για παράδειγμα, ένας κακόβουλος χρήστης μπορεί να στείλει στον πάροχο της διαδικτυακής τηλεφωνίας ένα μήνυμα στο οποίο θα υπάρχει ενσωματωμένος ο κατάλληλος κώδικας είτε για την τροποποίηση των χρεώσεων του είτε για τη χρέωση κάποιου τρίτου.

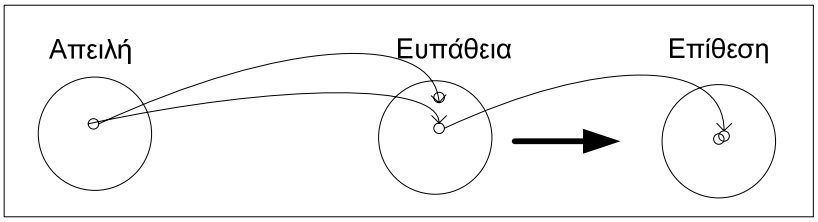
Ένα επιπρόσθετο χαρακτηριστικό το οποίο θα πρέπει να διασφαλίζουν οι υπηρεσίες διαδικτυακής τηλεφωνίας είναι η αδιάλειπτη λειτουργία τους. Η άρνηση παροχή υπηρεσίας θεωρείται ως από τις πλέον σοβαρές απειλές που εμφανίζονται στο διαδίκτυο, πόσο μάλλον για υπηρεσίες πραγματικού χρόνου όπως αυτή της διαδικτυακής τηλεφωνίας. Ένας επιτιθέμενος θα προσπαθήσει να δημιουργήσει μεγάλο πλήθος αιτημάτων προς την υπηρεσία, με αποτέλεσμα τη δημιουργία μεγάλου υπολογιστικού ή/και δικτυακού φόρτου ώστε να μην είναι δυνατή η επεξεργασία επιπρόσθετων αιτήσεων. Εναλλακτικά, μπορεί να επιτύχει την άρνηση παροχής μέσω της δημιουργίας και αποστολής των κατάλληλων μηνυμάτων σηματοδοσίας. Ο Πίνακας 4–1 παρουσιάζει συνοπτικά τη σύγκριση των απειλών που εμφανίζονται στο PSTN και στην υπηρεσία διαδικτυακής τηλεφωνίας. Μπορεί να γίνει άμεσα αντιληπτό ότι η υπηρεσία της διαδικτυακής τηλεφωνίας θα αποτελέσει ένα σημαντικό πόλο έλξης επιτιθέμενων.

Απειλή	**Εμφάνιση στο PSTN**	**Εμφάνιση στη διαδικτυακή τηλεφωνία**
Μη εξουσιοδοτημένη Πρόσβαση	Ναι[4]	Ναι
Μη Εξουσιοδοτημένη Τροποποίηση	Όχι	Ναι
Πλαστοπροσωπία Χρήστη	Όχι	Ναι
Πλαστοπροσωπία Υπηρεσίας	Όχι	Ναι
Απάτες Χρέωσης Πάροχων	Όχι	Ναι
Απάτες Χρέωσης Χρηστών	Όχι	Ναι
Διακοπή Λειτουργίας Υπηρεσίας	Ναι	Ναι

Πίνακας 4–1. Εμφάνιση Απειλών στο PSTN & στη Διαδικτυκιακή Τηλεφωνία

4.4 Επιθέσεις στη Διαδικτυακή Τηλεφωνία

Σύμφωνα με το λεξικό του διαδικτύου [59] ο όρος «επίθεση» μπορεί να ορισθεί ως «οποιαδήποτε προσπάθεια παραβίασης των υπηρεσιών ασφάλειας ενός πληροφοριακού συστήματος ώστε να επιτευχθεί ένας συγκεκριμένος στόχος». Για την πραγμάτωση ενός περιστατικού ασφαλείας γνωστό ως επίθεσης απαιτείται η ύπαρξη των κατάλληλων ευπαθειών (vulnerability) τις οποίες εκμεταλλεύεται (exploit) μια απειλή ώστε να δημιουργήσει συγκεκριμένες επιπτώσεις στο σύστημα στόχο (βλέπε Σχήμα 4–1).



Σχήμα 4–1. Συσχετισμός Απειλών Ευπαθειών και Επιθέσεων

Η αποτελεσματικότητα των επιθέσεων ή ο ρυθμός (rate) επιτυχίας αυτών, εξαρτάται από τρεις βασικούς παράγοντες:

1. Τη ρωμαλεότητα (robustness) των μηχανισμών ασφαλείας που έχουν αναπτυχθεί για την προστασία των υπολογιστικών πόρων.
2. Την ύπαρξη συγκεκριμένων ευπαθειών.

[4] Κυρίως στα δεδομένα φωνής

3. Τις ικανότητες των κακόβουλων χρηστών και των εργαλείων που χρησιμοποιούν για την πραγμάτωση μιας επίθεσης.

Παρόλο, που οι απειλές στη διαδικτυακή τηλεφωνία δεν έχουν εκδηλωθεί ως επιθέσεις σε ευρεία κλίμακα, διάφορες ερευνητικές εργασίες [19],[20],[60]–[64], επισημαίνουν την πιθανότητα εμφάνισης αυτών, εξομοιώνοντας τέτοιου είδους περιστατικά σε εργαστηριακό περιβάλλον.

Στη συνέχεια αυτής της ενότητας γίνεται αναλυτική περιγραφή των πιθανών επιθέσεων που μπορούν να εμφανιστούν στη διαδικτυακή τηλεφωνία, δίνοντας έμφαση κυρίως στις υπηρεσίες που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP. Θα πρέπει να σημειωθεί ότι δεν μελετώνται περιπτώσεις επιθέσεων που προέρχονται από τις βασικές υποδομές του διαδικτύου αλλά αυτές που δημιουργούνται κυρίως από τα πρωτόκολλα που χρησιμοποιούνται στη διαδικτυακή τηλεφωνία (έμμεσα ή άμεσα). Αντίστοιχες επιθέσεις, ίσως με μικρές διαφοροποιήσει είναι δυνατόν να εμφανισθούν και σε δίκτυα-υπηρεσίες τηλεφωνίας που αξιοποιούν εναλλακτικά πρωτόκολλα σηματοδοσίας.

4.4.1 Υποκλοπές Κλήσεων στη Διαδικτυακή Τηλεφωνίας

Μια από τις πιο γνωστές επιθέσεις που εκδηλώνεται σχεδόν σε όλα τα τηλεπικοινωνιακά συστήματα που υποστηρίζουν υπηρεσίες τηλεφωνίας είναι η υποκλοπή συνδιαλέξεων-κλήσεων (eavesdropping). Σε αντίθεση με το PSTN, όπου μόνο τα δεδομένα φωνής είναι υποκείμενο αυτών των επιθέσεων, στη διαδικτυακή τηλεφωνία αφορά και τα δεδομένα σηματοδοσίας.

Όλα τα μηνύματα σηματοδοσίας εμπεριέχουν πληροφορίες σχετικά με τα αναγνωριστικά των χρηστών, τις διευθύνσεις επαφής, κλειδιά ασφαλείας, καθώς και όλες τις βασικές παραμέτρους που απαιτούνται για την αποκατάσταση συνδέσεων μεταξύ δύο ή περισσότερων χρηστών. Όλες οι προαναφερόμενες πληροφορίες θα πρέπει να τηρούνται εμπιστευτικές. Παρ' όλα αυτά, η εύκολη πρόσβαση στο μέσο μετάδοσης, η ύπαρξη διαφόρων ειδών εργαλείων υποκλοπής δεδομένων στο διαδίκτυο (όπως για παράδειγμα το Wireshark–www.wireshark.org), σε συνδυασμό με τα μηνύματα κειμένου (text based) που χρησιμοποιούνται στο SIP, καθιστά την διαδικασία υποκλοπής κλήσεων σχετικά απλή. Επιπρόσθετα, θα πρέπει να επαναλάβουμε ότι η εφαρμογή μηχανισμών εμπιστευτικότητας, από χρήστη σε χρήστη (end-to-end), στα μηνύματα σηματοδοσίας θεωρείται ανέφικτη [19],[20] καθώς τα μηνύματα δρομολογούνται μέσω διαφορετικών πληρεξούσιων εξυπηρετών που απαιτούν πρόσβαση σε συγκεκριμένα τμήματα του μηνύματος για την ορθή δρομολόγηση του στον τελικό παραλήπτη.

Ας υποθέσουμε, για παράδειγμα, ότι κατά τη διάρκεια μιας επίθεσης υποκλοπής κλήσεων, ο επιτιθέμενος υποκλέπτει ένα μήνυμα SIP REGISTER (βλέπε Σχήμα 3–7) με αποτέλεσμα να γίνεται άμεσα γνώστης όλων των παραμέτρων που χρησιμοποιεί για την επικοινωνία του ο αποστολέας του συγκεκριμένου μηνύματος. Πέραν τούτου, αν ο επιτιθέμενος συλλέξει ένα σύνολο από τέτοια μηνύματα μπορεί να πραγματοποιήσει ανάλυση κίνησης (traffic analysis) [65] σε μια προσπάθεια να μαντέψει το συνθηματικό του χρήστη. Στην ανάλυση αυτή χρησιμοποιούνται τα δεδομένα που περιέχονται στην κεφαλίδα «Authorization» κάθε SIP μηνύματος.

Αξίζει να σημειωθεί ότι ακόμα και εάν τα δεδομένα σηματοδοσίας είναι προστατευμένα μέσω κατάλληλων μηχανισμών εμπιστευτικότητας, είναι σχεδόν βέβαιο ότι ο επιτιθέμενος θα προσπαθήσει να αποκαλύψει τα αντίστοιχα κρυπτογραφικά κλειδιά ώστε να εξασφαλίσει πρόσβαση στα δεδομένα σηματοδοσίας, παραβιάζοντας σε κάθε περίπτωση την εμπιστευτικότητα των.

Οι επιθέσεις της συγκεκριμένης κατηγορίας εμμέσως παραβιάζουν και άλλες υπηρεσίες ασφαλείας (ακεραιότητα, διαθεσιμότητα) αφού αποτελούν τα αρχικά βήματα άλλου τύπου επιθέσεων στη διαδικτυακή τηλεφωνία (βλέπε ενότητα 4.4.5).

4.4.2 Επιθέσεις προς Αναλυτές Μηνυμάτων

Το γεγονός ότι τα SIP μηνύματα έχουν τη μορφή κειμένου σε συνδυασμό με το μεγάλο βαθμό ελευθερίας στη σύνταξη τους απαιτεί τη δημιουργία ενός αξιόπιστου και αποδοτικού αναλυτή (parser) για την ορθή επεξεργασία τους. Αξίζει να σημειωθεί ότι υπάρχουν περιπτώσεις επιθέσεων προς τους αναλυτές που αξιοποιούν μηνύματα πλήρως συμβατά με τις προδιαγραφές, για να προκαλέσουν προβλήματα αστάθειας ή ακόμα και να επιτύχουν άρνηση παροχής υπηρεσίας. Στις ακόλουθες υπό-ενότητες εξετάζονται οι διαφορετικές περιπτώσεις επιθέσεων που μπορούν να εκδηλωθούν προς τους αναλυτές μηνυμάτων.

4.4.2.1 Επιθέσεις που Αξιοποιούν Μη Συμβατά Μηνύματα

Είναι γνωστό ότι οι υλοποιήσεις πρωτοκόλλων και δικτυακών εφαρμογών σε πολλές περιπτώσεις δεν συμμορφώνονται πλήρως με τις προδιαγραφές που έχουν τεθεί ή εμπεριέχουν λάθη, τα οποία μπορεί να προκαλέσουν την αποστολή μη ορθών μηνυμάτων. Στο TCP, για παράδειγμα, έχουν αναφερθεί περιστατικά που οφείλονται σε προβλήματα υλοποίησης [66]. Αντίστοιχα περιστατικά έχουν αναφερθεί και για υπηρεσίες που προσφέρονται μέσω του διαδικτύου [67],[68]. Είναι λοιπόν αναμενόμενο ότι και η υπηρεσία της διαδικτυακής τηλεφωνίας έχει να αντιμετωπίσει αντίστοιχες επιθέσεις, γεγονός που επιβεβαιώνεται από τις ήδη υπάρχουσες αναφορές [69]–[71].

Η επεξεργασία και ανάλυση των SIP μηνυμάτων είναι υψηλής σημασίας καθώς αποτελεί αναπόσπαστό τμήμα όλων των δικτυακών οντοτήτων του SIP. Η γενική αρχιτεκτονική ενός αναλυτή SIP μηνυμάτων έχει παρουσιασθεί ήδη στην ενότητα 3.2.5. Όπως, εντοπίζεται και στην εργασία [64] οι περισσότεροι αναλυτές μηνυμάτων στο SIP έχουν σχεδιαστεί για την επεξεργασία μηνυμάτων που είναι απόλυτα συμβατά με τις προδιαγραφές του. Σε ελάχιστες περιπτώσεις είναι δυνατόν να διαχειρισθούν κακόβουλα μηνύματα που δε συμμορφώνονται με τη γραμματική του SIP, απορρίπτοντας τα σε αρχικό στάδιο της επεξεργασίας. Η περαιτέρω επεξεργασία τέτοιων μηνυμάτων οδηγεί την αντίστοιχη SIP δικτυακή οντότητα σε μια από τις ακόλουθες μη επιθυμητές καταστάσεις :

1. Άρνηση παροχής υπηρεσίας (Denial of Service)-(DoS)
2. Μη σταθερή λειτουργία (Unstable operation)
3. Μη εξουσιοδοτημένη πρόσβαση (unauthorized access)

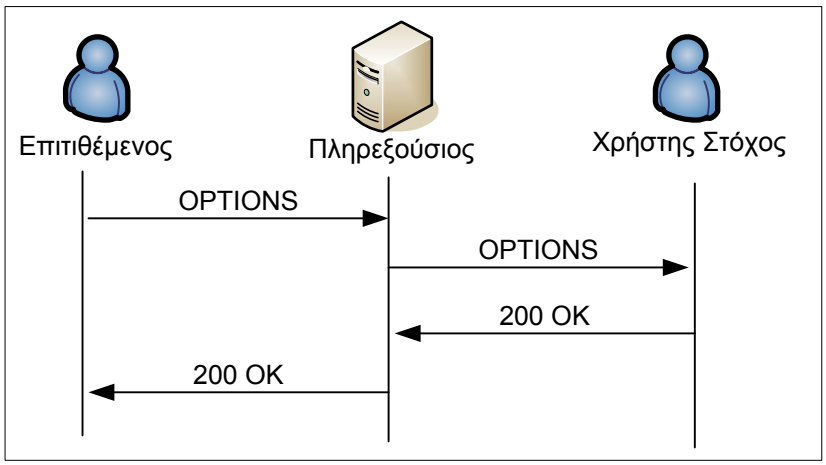
Η μορφή κειμένου που αξιοποιείται από τα SIP μηνύματα προσελκύει περισσότερους επιτιθέμενους που αναζητούν διαφορετικούς τρόπους για να προκαλέσουν μια εκ των προαναφερόμενων καταστάσεων. Για παράδειγμα, ένας επιτιθέμενος αντί να στείλει ένα SIP REGISTER μήνυμα βασισμένο στις προδιαγραφές του SIP (βλέπε Σχήμα 3–7) μπορεί να αποστείλει το SIP REGISTER που παρουσιάζεται στο Σχήμα 4–2. Το μήνυμα αυτό δεν είναι έγκυρο καθώς σύμφωνα με τη γραμματική του SIP μετά τη μέθοδο πρέπει να ακολουθεί το αντίστοιχο URI. Επιπλέον οι κεφαλίδες «From, To» δεν συμπεριλαμβάνουν δεδομένα και αυτό μπορεί να δημιουργήσει πρόβλημα στον αναλυτή που επεξεργάζεται το μήνυμα καθώς σύμφωνα με τις προδιαγραφές του SIP τα δεδομένα για αυτές τις κεφαλίδες είναι υποχρεωτικά.

```
REGISTER I am trying to crash a sip proxy SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: NULL
To: NULL
Call-ID: 3021094946@81.0.7.124
CSeq: 2 REGISTER
```

Σχήμα 4–2. Παράδειγμα Μηνύματος που δεν Συμμορφώνεται με τις Προδιαγραφές

Τα μηνύματα αυτού του είδους που δύναται ένας επιτιθέμενος να δημιουργήσει είναι αναρίθμητα. Για παράδειγμα, ο επιτιθέμενος μπορεί να ακολουθήσει τη μέθοδο εξαντλητικής αναζήτησης δημιουργώντας διαφορετικούς συνδυασμούς κακόβουλων μηνυμάτων για να αποκτήσει πρόσβαση στη διαδικτυακή οντότητα στόχο. Εναλλακτικά, ο επιτιθέμενος μπορεί να ελέγξει τη ρωμαλεότητα ενός SIP αναλυτή εντοπίζοντας τα μηνύματα τα οποία δεν υποστηρίζει, αποστέλλοντας του μη υποστηριζόμενα, μη συμβατά μηνύματα για τον έλεγχο της απόκρισης του σε αυτές τις περιπτώσεις.

Τα μηνύματα που υποστηρίζονται από μια δικτυακή SIP οντότητα εμπεριέχονται τόσο στα SIP REGISTER όσο και στα SIP OPTIONS μηνύματα. Συνεπώς, κάποιος επιτιθέμενος είτε θα υποκλέψει (βλέπε ενότητα 4.4.1) το SIP REGISTER κατά την αρχική διαδικασία εγγραφής του χρήστη στόχου, είτε θα αποστείλει στη συσκευή στόχο ένα μήνυμα SIP OPTIONS (βλέπε Σχήμα 4–3), όπου στην απάντηση που θα παραλάβει θα υπάρχουν, μεταξύ των άλλων, και όλα τα υποστηριζόμενα μηνύματα.



Σχήμα 4–3. Διαδικασία Εύρεσης Υποστηριζόμενων SIP μηνυμάτων

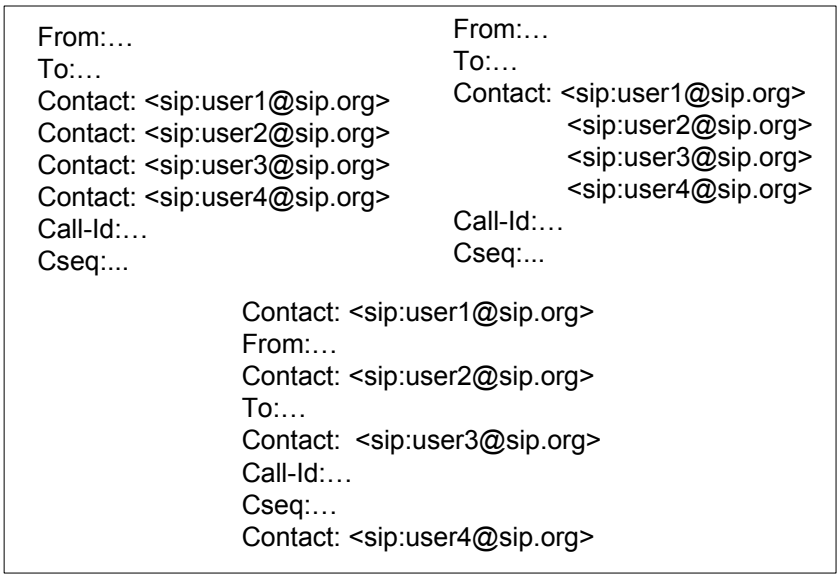
4.4.2.2 Επιθέσεις που Αξιοποιούν Συμβατά SIP Μηνύματα

Σύμφωνα με την εργασία [62] ακόμα και ένα απολύτως συμβατό με τις προδιαγραφές του SIP μήνυμα μπορεί να δημιουργήσει προβλήματα αστάθειας στις δικτυακές οντότητες που το επεξεργάζονται. Πιο συγκεκριμένα, ο επιτιθέμενος μπορεί να δημιουργήσει μηνύματα μεγάλου μήκους προσθέτοντας κεφαλίδες οι οποίες δεν είναι αναγκαίες για την επεξεργασία του συγκεκριμένου αιτήματος ή/και συμπεριλαμβάνοντας πολλά μη αναγκαία δεδομένα στο κύριο σώμα του μηνύματος. Εναλλακτικά, ο επιτιθέμενος δύναται να δημιουργήσει μηνύματα τα οποία έχουν πολλαπλές τιμές (multiple values) οι οποίες διαχωρίζονται αντιστοίχως σε πολλαπλές κεφαλίδες, κάθε μία από τις οποίες περιέχει μια μοναδική τιμή (παράδειγμα τέτοιου μηνύματος με πολλαπλές τιμές στην κεφαλίδα Contact, απεικονίζεται στο Σχήμα 4–4). Τέτοια μηνύματα είναι απολύτως συμβατά με τις προδιαγραφές του SIP. Αντίστοιχες περιπτώσεις μπορεί να δημιουργηθούν κάνοντας χρήση των κεφαλίδων: *Accept-Encoding, Accept-Language, Alert-Info, Allow, Authentication-Info, Call-Info, Contact, Content-*

Encoding, Content-Language, Error-Info, In-Reply-To, Proxy-Require, Record-Route, Require, Route, Supported, Unsupported, User-Agent, Via, and Warning.

Αξίζει να σημειωθεί ότι συγκεκριμένες κεφαλίδες περιέχουν πληροφορίες που αφορούν τη δρομολόγηση του μηνύματος (όπως για παράδειγμα οι κεφαλίδες *Via* και *Route*). Στην περίπτωση που οι κεφαλίδες αυτές τοποθετούνται στο τέλος του μηνύματος είναι ξεκάθαρο ότι προκαλούν μεγαλύτερη επεξεργαστική πολυπλοκότητα, αφού οι απαραίτητες πληροφορίες για την ορθή δρομολόγηση του μηνύματος αναζητούνται στις αρχικές κεφαλίδες.

Όλες οι προαναφερόμενες περιπτώσεις μηνυμάτων εκτός της αυξημένης κίνησης στο δίκτυο (λόγω του μήκους τους), προκαλούν επιπρόσθετη επεξεργαστική επιβάρυνση και μεγαλύτερη κατανάλωση μνήμης εξαιτίας της πολυπλοκότητας που έχει εισαχθεί για τη συντακτική τους ανάλυση.



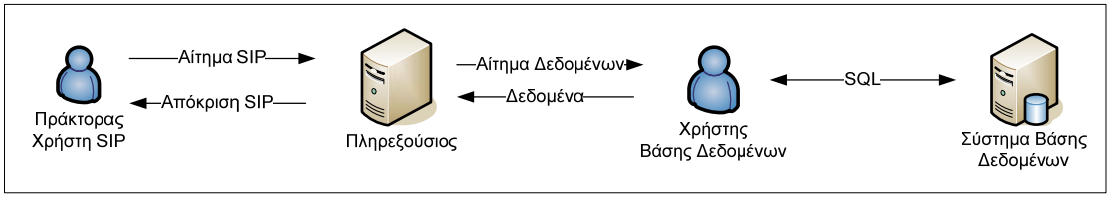
Σχήμα 4–4. Παραδείγματα Σύνταξης SIP Μηνυμάτων με Πολλαπλές Κεφαλίδες «Contact»

4.4.3 Επιθέσεις Έγχυσης Κώδικα σε SIP μηνύματα

Οι επιθέσεις έγχυσης κώδικα (injection code attacks) στις υπηρεσίες του διαδικτύου μπορούν να πραγματοποιηθούν κάνοντας χρήση διαφόρων μεθόδων, όπως για παράδειγμα με την υπερχείλιση καταχωρητών (buffer overflows) [72], την εισαγωγή κακόβουλου κώδικα σε περιγραφή σεναρίων (scripts) που ενσωματώνονται σε ιστοσελίδες [73] ή σε HTTP αιτήματα [74],[75]. Μεταξύ των πιο χαρακτηριστικών παραδειγμάτων εισαγωγής κακόβουλου κώδικα σε HTTP αιτήματα, είναι η εισαγωγή SQL εντολών [74],[76] που έχουν ως στόχο τη μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση δεδομένων που βρίσκονται αποθηκευμένα στη βάση δεδομένων του αντίστοιχου ιστοτόπου. Εξαιτίας του ότι η διεπαφή που αξιοποιείται για την επικοινωνία με τη βάση δεδομένων σε κάθε περίπτωση είναι ανεξάρτητη από τη προσφερόμενη υπηρεσία, αντίστοιχες επιθέσεις δύναται να πραγματοποιηθούν σε οποιαδήποτε υπηρεσία αξιοποιεί βάσεις δεδομένων στο διαδίκτυο.

Προκύπτει, λοιπόν ότι οι υπηρεσίες διαδικτυακής τηλεφωνίας είναι ευπαθείς σε επιθέσεις τέτοιου τύπου, καθώς για τη διαχείριση των δεδομένων των χρηστών, όπως διαπιστευτήρια (credentials), χρεώσεις λογαριασμών (accounting) κ.α, αξιοποιούνται βάσεις δεδομένων όπως MySQL, Postgress, Oracle κτλ. Συγκεκριμένα, οι υπάρχουσες υλοποιήσεις πληρεξούσιων

εξυπηρετών, όπως ο SIP Express Router (SER) [77], και ο αντίστοιχος που προσφέρεται από τη VoVida [78], παρέχουν τα κατάλληλα δομοστοιχεία (modules) για τη διασφάλιση της επικοινωνίας με τις αντίστοιχες βάσεις δεδομένων για την κάλυψη των διαχειριστικών αναγκών των υπηρεσιών διαδικτυακής τηλεφωνίας, αξιοποιώντας την αρχιτεκτονική που απεικονίζεται στο Σχήμα 4–5.



Σχήμα 4–5. Αρχιτεκτονική Διασυνεδεσιμότητας μεταξύ Πληρεξούσιου & Βάσης Δεδομένων

Οι επιθέσεις έγχυσης κώδικα SQL στη διαδικτυακή τηλεφωνία μπορούν να πραγματοποιηθούν σε κάθε περίπτωση όπου γίνεται επικοινωνία με τη βάση δεδομένων. Στην περίπτωση του SIP, τέτοιου είδους επικοινωνία πραγματοποιείται κατά κύριο λόγο όταν γίνεται αυθεντικοποίηση ενός αιτήματος (βλέπε Σχήμα 3–8). Σε αυτή τη περίπτωση ο κακόβουλος χρήστης εκτός των δεδομένων αυθεντικοποίησης-διαπιστευτήρια (credentials) θα μπορούσε να ενσωματώσει και τον κώδικα SQL που παρουσιάζεται στο Σχήμα 4–6 με έντονα στοιχεία.

```
REGISTER sip:dgentele.com SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: <sip:3400001586@dgentele.com;user=phone>;tag=3199572059
To: <sip:3400001586@dgentele.com;user=phone>
Call-ID: 3021094946@81.0.7.124
CSeq: 2 REGISTER
Contact: <sip:3400001586@81.0.7.124:5070;user=phone;transport=udp>;expires=300
User-Agent: Cisco ATA 186  v3.1.0 atasip (040211A)
Authorization: Digest username="3400001586'; UPDATE accounting set duration='200'
                        where username ='340001586';--",
                       realm="dgentele.com",
                       nonce="426302039afdf717c6687e28f6c7d39c4fdb9f08",
                       uri="sip:voztele.com",response="af0d725596c8f06f370f8c80ade67b05"
Content-Length: 0
```

Σχήμα 4–6. Παράδειγμα Έγχυσης Κώδικας SQL σε μήνυμα SIP Register

Η επεξεργασία του παραπάνω μηνύματος από τον αντίστοιχο πληρεξούσιο εξυπηρέτη θα έχει σαν αποτέλεσμα τη δημιουργία και εκτέλεση των παρακάτω εντολών SQL:

(1) Select password From subscriber where username ='3400001586';

(2) Update accounting set duration=200 where username= '3400001586'; --

Όπως μπορεί να παρατηρηθεί, το αποτέλεσμα της εκτέλεσης των SQL εντολών, και συγκεκριμένα της 2^{ης} SQL εντολής, είναι η μη εξουσιοδοτημένη τροποποίηση της διάρκειας των κλήσεων που έχει πραγματοποιήσει ο χρήστης με αναγνωριστικό «340001586» στη τιμή «200». Η δυνατότητα εκτέλεσης της δεύτερης εντολής οφείλεται στο γεγονός ότι τα δεδομένα που βρίσκονται στο πεδίο «username» της κεφαλίδας «Authorization» αν και εκλαμβάνονται ως το πλήρες αναγνωριστικό του χρήστη, έχουν κατατμηθεί από τον επιτιθέμενο σε δύο τμήματα κάνοντας χρήση των χαρακτήρων «**';**». Οι χαρακτήρες αυτοί είναι ειδικοί χαρακτήρες (special characters) για τη γλώσσα SQL. Ο πρώτος χρησιμοποιείται για τον τερματισμό των αλφαριθμητικών σε όλες τις SQL εντολές, με αποτέλεσμα στο

προαναφερόμενο παράδειγμα να τερματίζει το «usernmame» του χρήστη που αξιοποιείται στην εντολή SQL Select (βλέπε εντολή 1). Ο δεύτερος χαρακτήρας ουσιαστικά ολοκληρώνει την εκτέλεση της αρχικής εντολής, παρέχοντας με αυτό τον τρόπο τη δυνατότητα εκτέλεσης της δεύτερης εντολής. Ότι ακολουθεί μετά από τους χαρακτήρες «--» θεωρείται σχόλιο. Έτσι ακόμα και στην περίπτωση όπου η αρχική SQL εντολή (βλέπε εντολή 1) μετά το πεδίο «username» είχε και άλλες συνθήκες, αυτές παραλείπονται και η εκτέλεση των εντολών SQL ολοκληρώνεται.

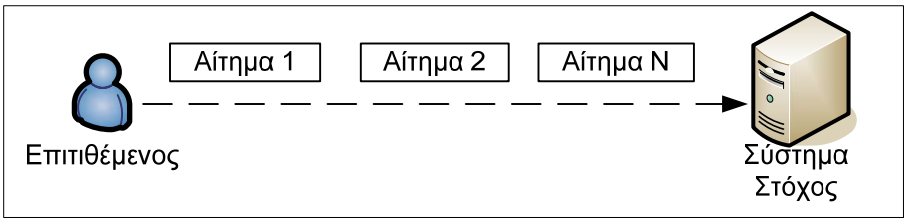
Αξίζει να σημειωθεί ότι οι επιθέσεις έγχυσης SQL κώδικα, όπως και στην περίπτωση των άλλων υπηρεσιών που προσφέρονται στο διαδίκτυο, είναι ανεξάρτητες από τη βάση δεδομένων και την αντίστοιχη υλοποίηση του πληρεξούσιου εξυπηρέτη διαδικτυακής τηλεφωνίας. Ο μοναδικός περιορισμός εντοπίζεται στην αξιοποιούμενη κάθε φορά διεπαφή προγραμματισμού εφαρμογής (Application Programming Interface–(API)) που χρησιμοποιείται για την επικοινωνία με τη βάση δεδομένων. Για παράδειγμα η διεπαφή που παρέχεται από τη MySQL (μέχρι και την έκδοση 4.1) για τη γλώσσα προγραμματισμού C επιτρέπει την εκτέλεση μιας μόνο εντολής SQL σε κάθε κλήση της διεπαφής. Επιπλέον, σε περιπτώσεις όπου εκτελούνται εντολές ενημέρωσης SQL όπως UPDATE, DELETE ο χρήστης της βάσης δεδομένων που ενεργεί εκ μέρους της υπηρεσίας απαιτείται να έχει τα αντίστοιχα δικαιώματα. Βέβαια πρέπει να σημειωθεί ότι ακόμα και εάν ο χρήστης της βάσης δεδομένων έχει τα ελάχιστα δικαιώματα, παρέχει τη δυνατότητα στο κακόβουλο χρήστη (κατ' ελάχιστων) να αυθεντικοποιηθεί ως ένας άλλος χρήστης αξιοποιώντας την κατάλληλη εντολή SQL.

Τελευταίο αλλά ιδιαίτερα σημαντικό είναι το γεγονός ότι οι επιθέσεις έγχυσης κώδικα και συγκεκριμένα SQL σε μηνύματα SIP δεν εκμεταλλεύονται κάποια συγκεκριμένη ευπάθεια αλλά το τρόπο διασύνδεσης της υπηρεσίας διαδικτυακής τηλεφωνίας με τη βάση δεδομένων. Βέβαια, η έλλειψη μηχανισμών διασφάλισης της ακεραιότητας των δεδομένων, προσφέρει στους επιτιθέμενους τη δυνατότητα να λειτουργούν χωρίς κανένα απολύτως έλεγχο αναφορικά με τα δεδομένα τα οποία αποστέλλουν στους εξυπηρέτες διαδικτυακής τηλεφωνίας ενώ είναι ευεπίφορα και σε επιθέσεις ενδιάμεσου (man-in-the-middle attacks) [51]. Για παράδειγμα ένας κακόβουλος χρήστης μπορεί να τροποποιήσει κάποιο μήνυμα εισάγοντας ότι κώδικα επιθυμεί.

4.4.4 Επιθέσεις Πλημμύρας

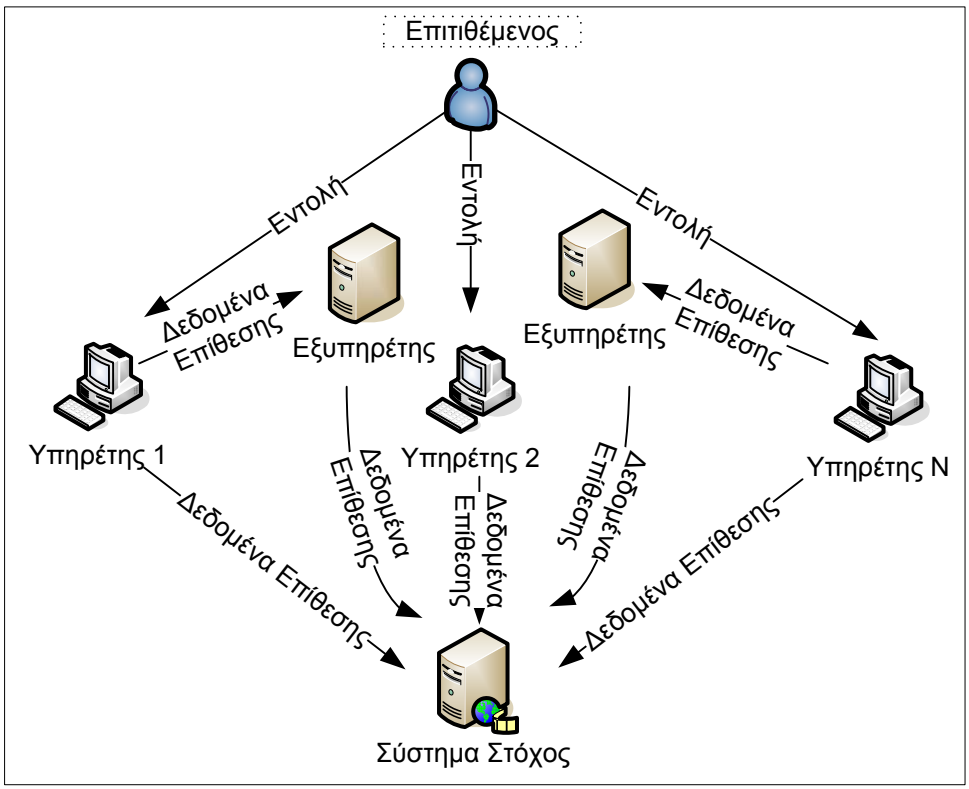
Οι επιθέσεις πλημμύρας (flooding attacks) στο διαδίκτυο θεωρούνται, από τους παρόχους υπηρεσιών, ως οι πλέον καταστροφικές καθώς έχουν στόχο την εξάντληση των υπολογιστικών και επικοινωνιακών πόρων, καθιστώντας την υπηρεσία μη διαθέσιμη (άρνηση παροχή υπηρεσίας). Επιπλέον ο διαχωρισμός μεταξύ φυσιολογικής και επιτιθέμενης κίνησης είναι αρκετά δύσκολος, αφού και στις δύο περιπτώσεις εμπλέκονται μηνύματα που είναι συμβατά με τις προδιαγραφές του SIP.

Στη γενική περίπτωση μιας επίθεσης πλημμύρας, ο επιτιθέμενος αποστέλλει ένα μεγάλο αριθμό αιτημάτων, συμβατών με τις προδιαγραφές του πρωτοκόλλου που χρησιμοποιείται, προς το σύστημα στόχο [79]. Για την πραγμάτωση της επίθεσης συνήθως αξιοποιούνται δύο ειδών αρχιτεκτονικές. Στην πρώτη, ο επιτιθέμενος κάνει χρήση ενός απλού γεννήτορα μηνυμάτων (βλέπε Σχήμα 4–7), ενώ στη δεύτερη χρησιμοποιούνται πολλαπλοί γεννήτορες για τη δημιουργία ακόμα μεγαλύτερης κίνησης, οι οποίοι συντονίζονται από κάποιο κεντρικό σύστημα, ώστε να επιτευχθεί άμεση εξάντληση των υπολογιστικών πόρων (βλέπε Σχήμα 4–8). Οι πολλαπλοί αυτοί γεννήτορες είναι συστήματα που τις περισσότερες φορές συμμετέχουν στην επίθεση χωρίς να το επιθυμούν – γνωρίζουν.



Σχήμα 4–7. Παράδειγμα Αρχιτεκτονικής Επιθέσεων Πλημμύρας Ενός Γεννήτορα

Στο διαδίκτυο έχουν ήδη δημοσιευθεί αρκετά περιστατικά επιθέσεων πλημμύρας [79],[80],[81]. Στην αρχή η πλειονότητα των περιστατικών αφορούσε επιθέσεις πλημμύρας ενός γεννήτορα, καθώς οι υπολογιστικοί πόροι και το εύρος ζώνης ήταν αρκετά περιορισμένα. Με την αύξηση της επεξεργαστικής ισχύος και την ύπαρξη μεγάλου εύρους ζώνης για τη μετάδοση των δεδομένων, οι επιτιθέμενοι αξιοποίησαν πιο «αποτελεσματικές» αρχιτεκτονικές, όπως αυτή των πολλαπλών γεννητόρων, για την εκδήλωση επιθέσεων πλημμύρας. Μεταξύ των πιο χαρακτηριστικών επιθέσεων που αξιοποιούν τη συγκεκριμένη αρχιτεκτονική είναι οι επιθέσεις πλημμύρας τύπου SYN [82],[83] και οι επιθέσεις πλημμύρας τύπου ανάκλασης (Reflection DoS) [84].



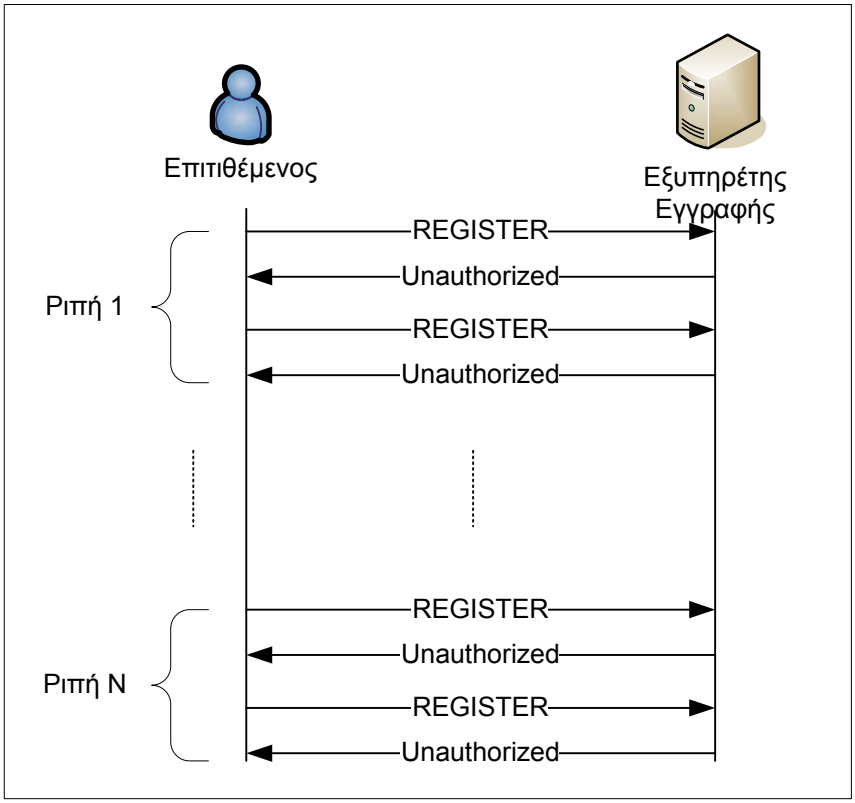
Σχήμα 4–8. Παράδειγμα Αρχιτεκτονικής Επιθέσεων Πλημμύρας Πολλαπλών Γεννητόρων

Τέτοιες επιθέσεις είναι δυνατόν να πραγματοποιηθούν για να προκαλέσουν άρνηση παροχής υπηρεσίας στη διαδικτυακή τηλεφωνία. Είναι ξεκάθαρο ότι όλες οι δικτυακές οντότητες που εμπλέκονται στις υπηρεσίες διαδικτυακής τηλεφωνίας είναι ευπαθείς σε επιθέσεις πλημμύρας. Αυτό προκύπτει από το γεγονός ότι οποιοσδήποτε χρήστης, αυθεντικοποιημένος ή μη, ηθελημένα ή μη, εσωτερικός ή εξωτερικός, είναι σε θέση να δημιουργήσει πληθώρα αιτήσεων και να τις αποστείλει προς την οντότητα στόχο χωρίς να απαιτείται η εκμετάλλευση κάποιας συγκεκριμένης ευπάθειας.

4.4.4.1 Επιθέσεις Πλημμύρας προς Εξυπηρέτες Εγγραφής

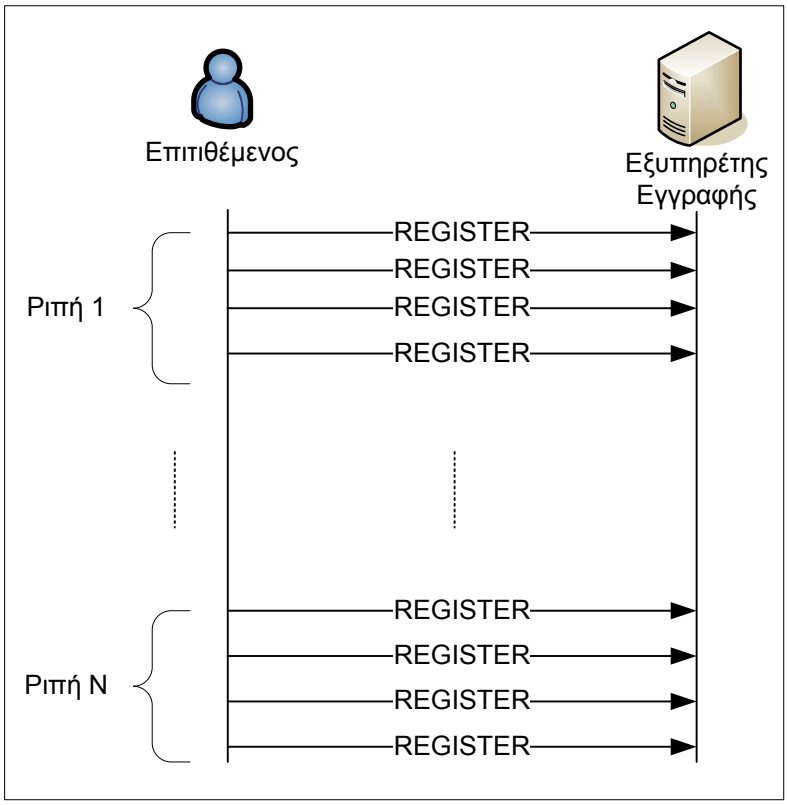
Στις επιθέσεις πλημμύρας προς τους εξυπηρέτες εγγραφής, ο επιτιθέμενος προσπαθεί να προκαλέσει άρνηση παροχής υπηρεσίας αποστέλλοντας μεγάλο αριθμό SIP REGISTER αιτήσεων και συνεπώς εξαναγκάζοντας τον εξυπηρέτη εγγραφής να εκτελεί πλήθος κρυπτογραφικών διαδικασιών με υψηλό υπολογιστικό φόρτο για την αυθεντικοποίηση των χρηστών. Όπως παρουσιάστηκε στην ενότητα 3.2.3.2.1, για την εγγραφή στην προσφερόμενη υπηρεσία, ο χρήστης δημιουργεί μια αίτηση SIP REGISTER παρέχοντας μια ή περισσότερες διευθύνσεις στις οποίες θα είναι διαθέσιμος. Κατά τη διαδικασία εγγραφής ο χρήστης κάνει χρήση του μηχανισμού αυθεντικοποίησης HTTP Digest [85] (βλέπε επίσης ενότητα 5.3.1) για τον υπολογισμό των απαραίτητων διαπιστευτηρίων. Κατά συνέπεια, όταν ένας επιτιθέμενος εκτελεί μια επίθεση πλημμύρας προς τον αντίστοιχο εξυπηρέτη εγγραφής, δημιουργώντας μεγάλο αριθμό αιτήσεων εγγραφής, έχει ως στόχο είτε την εύρεση του κωδικού ενός χρήστη, είτε την πρόκληση άρνησης παροχής υπηρεσίας στην υπηρεσία εγγραφής.

Στο Σχήμα 4–9 παρουσιάζεται ένα σενάριο επίθεσης πλημμύρας προς τον εξυπηρέτη εγγραφής το οποίο μπορεί να αξιοποιηθεί τόσο σε αρχιτεκτονική ενός γεννήτορα όσο και σε αρχιτεκτονική πολλαπλών γεννητόρων. Τα μηνύματα που αποστέλλει ο χρήστης κάθε φορά δεν είναι απαραίτητο να είναι ακριβώς τα ίδια, καθώς τροποποιώντας μερικές παραμέτρους του αρχικού μηνύματος (π.χ τα δεδομένα της κεφαλίδας «call-id») μπορεί να δημιουργήσει διαφορετικό μήνυμα.



Σχήμα 4–9. Παράδειγμα Επίθεσης Πλημμύρας προς τον Εξυπηρέτη Εγγραφής

Ένα εναλλακτικό σενάριο που μπορεί να ακολουθήσει ο επιτιθέμενος είναι η αποστολή πολλαπλών SIP REGISTER μηνυμάτων χωρίς να απαντά στις αποκρίσεις που δημιουργούνται από τον εξυπηρέτη εγγραφής όπως απεικονίζεται στο Σχήμα 4–10.



Σχήμα 4–10. Εναλλακτικό Παράδειγμα Επίθεσης προς τον Εξυπηρέτη Εγγραφής

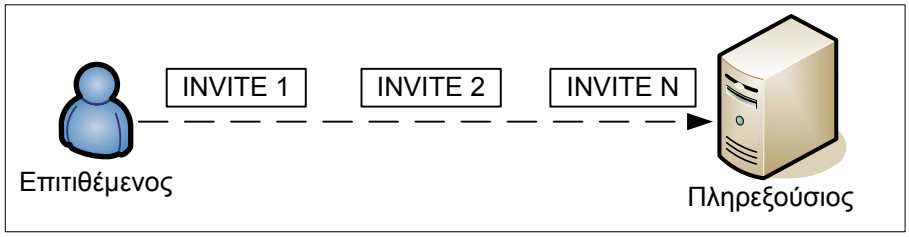
4.4.4.2 Επιθέσεις Πλημμύρας προς Πληρεξούσιους

Οι πληρεξούσιοι εξυπηρέτες είναι υπεύθυνοι για τη διαχείριση και επεξεργασία όλων των μηνυμάτων, εκτός των μηνυμάτων εγγραφής. Όπως έχει ήδη αναφερθεί στην ενότητα 3.2.3.2.2, οι πληρεξούσιοι εξυπηρέτες είναι δυνατόν να λειτουργούν είτε σε κατάσταση χωρίς μνήμη, είτε με μνήμη. Σε όσες περιπτώσεις λειτουργούν σε κατάσταση μνήμης απαιτούν επιπρόσθετη επεξεργαστική ισχύ για τη διαχείριση των μηνυμάτων, αφού για κάθε νέο εισερχόμενο μήνυμα δημιουργούν την αντίστοιχη μηχανή πεπερασμένης κατάστασης (βλέπε ενότητα 3.2.4) για την επεξεργασία και τον έλεγχο της κατάστασης της συνόδου. Η μηχανή πεπερασμένης κατάστασης και ένα αντίγραφο του αρχικού μηνύματος πρέπει να διατηρούνται ενεργά για χρονικό διάστημα έως και μερικών λεπτών, ανάλογα με τη διαμόρφωση του συστήματος. Το γεγονός αυτό καθιστά τους πληρεξούσιους εξυπηρέτες που λειτουργούν σε κατάσταση μνήμης περισσότερο ευπαθείς σε επιθέσεις πλημμύρας, σε σχέση με τις υπόλοιπες δικτυακές οντότητες του SIP. Αυτό σε καμία περίπτωση δε σημαίνει ότι οι εξυπηρέτες που λειτουργούν σε κατάσταση χωρίς μνήμη δεν είναι δυνατόν να αποτελέσουν πιθανό στόχο επίθεση πλημμύρας.

Δεδομένου ότι το μήνυμα SIP INVITE είναι αυτό που αξιοποιείται περισσότερο από οποιοδήποτε άλλο στην αρχιτεκτονική του SIP, στη συνέχεια της ανάλυσης των επιθέσεων πλημμύρας προς τους πληρεξούσιους εξυπηρέτες θα χρησιμοποιηθούν παραδείγματα με τα συγκεκριμένα μηνύματα. Τονίζεται ότι αντίστοιχες επιθέσεις μπορούν να πραγματοποιηθούν με τη χρήση και των υπόλοιπων μηνυμάτων.

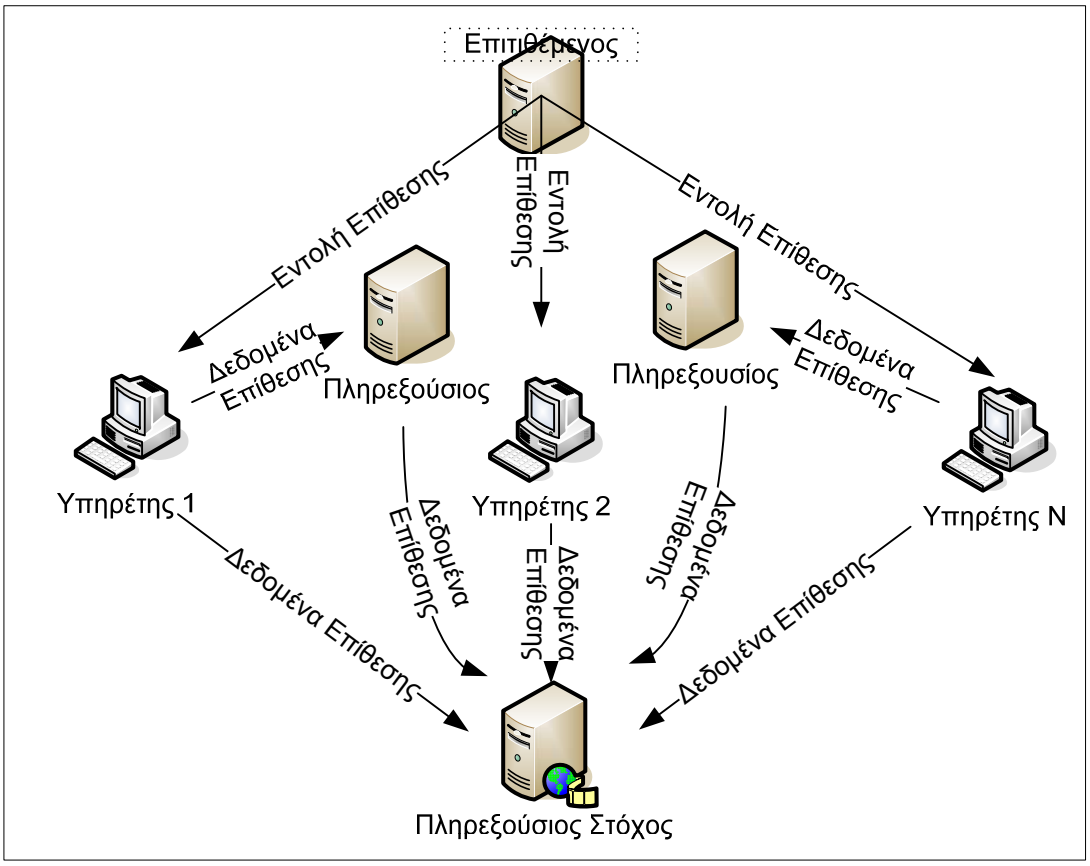
Ίσως η πιο απλή περίπτωση δημιουργίας μιας επίθεσης πλημμύρας προς ένα πληρεξούσιο είναι η δημιουργία διαφορετικών SIP INVITE μηνυμάτων τα οποία αντιστοιχούν σε διαφορετικές συνόδους και τα οποία αποστέλλονται από τον επιτιθέμενο προς τον πληρεξούσιο στόχο αξιοποιώντας την αρχιτεκτονική ενός γεννήτορα (βλέπε Σχήμα 4–11).

Αυτό μπορεί να επιτευχθεί εάν ο γεννήτορας των SIP INVITE μηνυμάτων δημιουργεί διαφορετικά αναγνωριστικά κλήσεων («call id») ή/και διαφορετικά αναγνωριστικά καλουμένων. Για κάθε τέτοιο νέο αίτημα που λαμβάνει ο πληρεξούσιος εξυπηρέτης θα πρέπει να εκχωρήσει τους απαραίτητους πόρους, οι οποίοι αποδεσμεύονται μόλις ληφθεί η τελική απάντηση του αιτήματος ή τερματιστεί η σύνοδος αυτόματα λόγω εκπνοής του χρόνου επεξεργασίας που ορίζεται από τις προδιαγραφές του SIP.



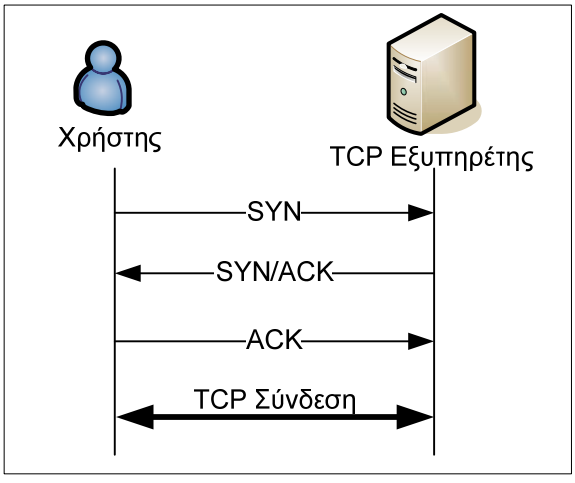
Σχήμα 4–11. Παράδειγμα Επίθεσης Πλημμύρας προς Πληρεξούσιο Εξυπηρέτη SIP με τη Χρήση ενός Γεννήτορα

Για τη δημιουργία μεγαλύτερής κίνησης, η οποία θα έχει ως στόχο την άμεση εξάντληση των υπολογιστικών πόρων, ο επιτιθέμενος μπορεί να αξιοποιήσει μια αρχιτεκτονική πολλαπλών γεννητόρων (βλέπε Σχήμα 4–8). Πιο συγκεκριμένα, ο επιτιθέμενος θα προσπαθήσει να δημιουργήσει ένα δίκτυο επίθεσης SIP (βλέπε Σχήμα 4–12) παραβιάζοντας την ασφάλεια των πληρεξούσιων εξυπηρετών και αξιοποιώντας τους ως φορείς της επίθεσης, δηλαδή προωθώντας την κίνηση της επίθεσης προς τον εξυπηρέτη στόχο χωρίς βέβαια αυτό να γίνεται άμεσα αντιληπτό από αυτούς. Ένας εναλλακτικός τρόπος αξιοποίησης της συγκεκριμένης αρχιτεκτονικής για τη δημιουργία επίθεσης πλημμύρας είναι η χρήση μη επιλύσιμων διευθύνσεων (irresolvable address) στα μηνύματα SIP INVITE, καθώς ο πληρεξούσιος εξυπηρέτης πρέπει να περιμένει την απάντηση από τον αντίστοιχο DNS εξυπηρέτη για να δημιουργήσει και να αποστείλει την κατάλληλη SIP απάντηση. Περισσότερες λεπτομέρειες για τις επιθέσεις μη επιλύσιμων διευθύνσεων στο SIP μπορούν να βρεθούν στις εργασίες [62],[86].



Σχήμα 4–12. Παράδειγμα Επίθεσης Πλημμύρας Πολλαπλών Γεννητόρων προς Πληρεξούσιο Εξυπηρέτη SIP

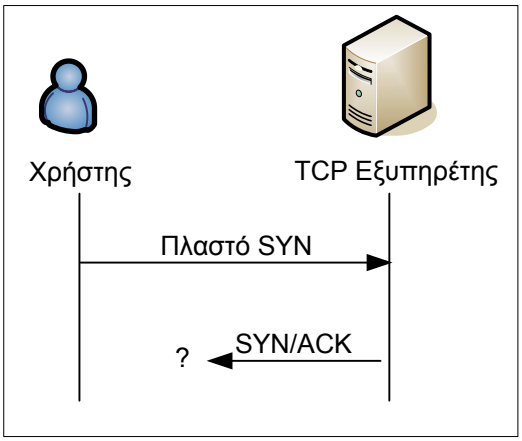
Δεδομένου ότι ο τρόπος λειτουργίας του SIP είναι παρόμοιος με αυτόν του TCP [9], κυρίως λόγω των ομοιοτήτων που παρουσιάζουν κατά την διαδικασία αποκατάστασης συνόδων, είναι πιθανόν στο SIP να εμφανιστούν επιθέσεις πλημμύρας παρόμοιες με αυτές του TCP, όπως αναφέρεται και στην εργασία **[27]**. Για την αποκατάσταση μιας σύνδεσης σε επίπεδο μεταφοράς με τη χρήση του TCP, απαιτείται μια τριμερής διαδικασία χειραψίας (three way handshake) όπως απεικονίζεται στο Σχήμα 4–13.



Σχήμα 4–13. Τυπική Τριμερής Διαδικασία για την Αποκατάσταση Σύνδεσης στο TCP

Παρά το γεγονός ότι το TCP χρησιμοποιείται για τη δημιουργία καναλιών επικοινωνίας, έχει εντοπισθεί από επιτιθέμενους μια σημαντική ευπάθεια στην υλοποίηση του, η οποία μπορεί να οδηγήσει στην εξάντληση της μνήμης ενός εξυπηρέτη TCP και συνεπώς σε

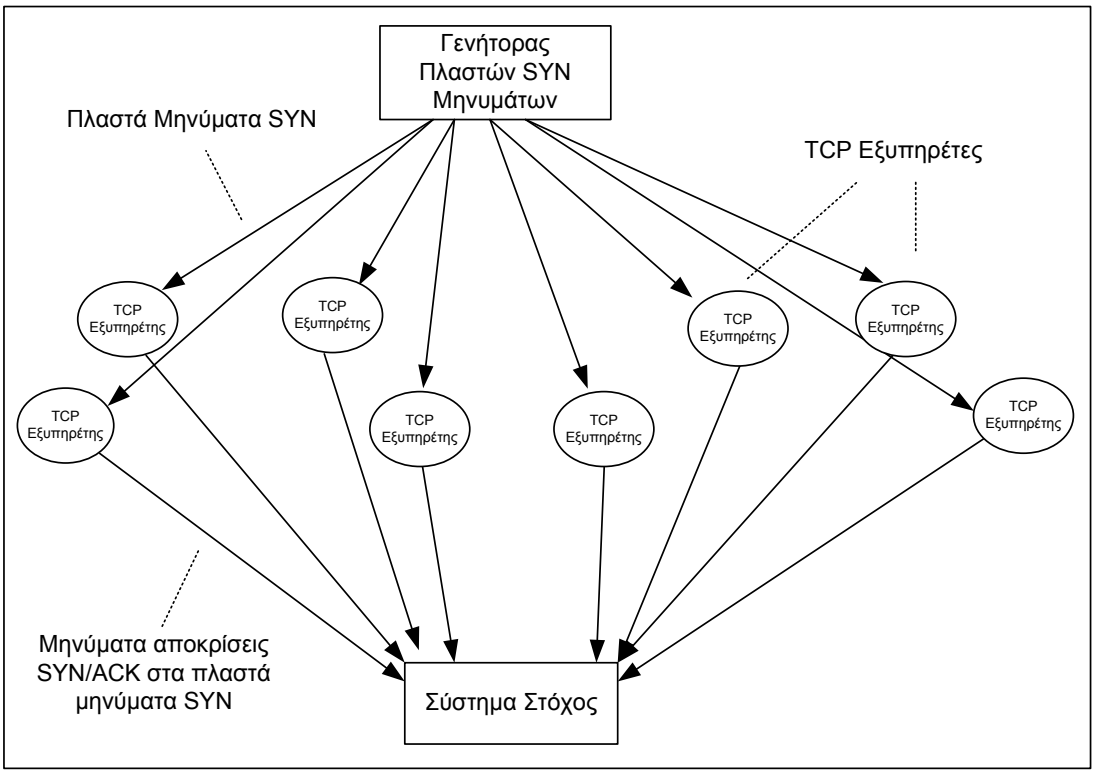
άρνηση παροχής υπηρεσίας. Ο επιτιθέμενος αποστέλλει προς τον TCP εξυπηρέτη ένα μεγάλο αριθμό από SYN αιτήσεις οι οποίες περιλαμβάνουν πλαστή ταυτότητα αποστολέα. Για κάθε μια από τις αιτήσεις αυτές ο εξυπηρέτης δεσμεύει την απαραίτητη για τη διαχείριση της σύνδεσης μνήμη και αποστέλλει πίσω στο πελάτη το αντίστοιχο SYN/ACK μήνυμα. Επειδή όμως οι αρχικές αιτήσεις περιλαμβάνουν πλαστή ταυτότητα αποστολέα, ο εξυπηρέτης αναγκάζεται να διατηρεί δεσμευμένους τους πόρους μέχρι η διαδικασία να τερματιστεί όπως ορίζουν οι προδιαγραφές του TCP. Η ιδέα της επίθεσης TCP-SYN παρουσιάζεται στο Σχήμα 4–14.



Σχήμα 4–14. Η Επίθεση TCP-SYN

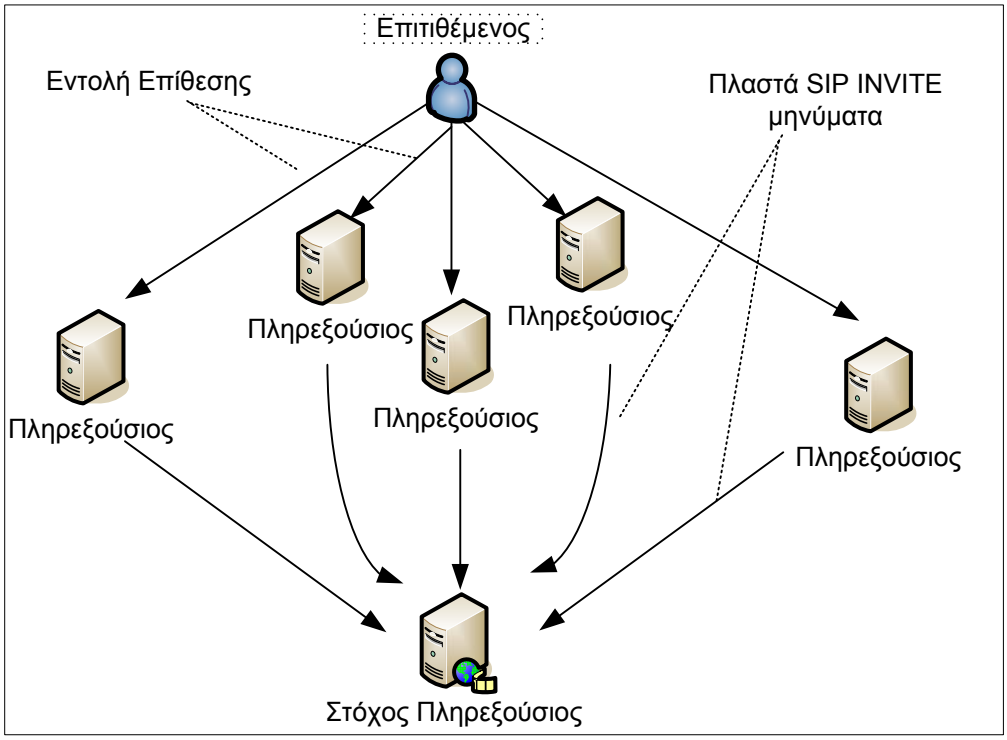
Σύμφωνα με την εργασία **[27]** αντίστοιχη επίθεση θα μπορούσε να πραγματοποιηθεί και στο SIP, γνωστή ως το σύνδρομο SYN επίθεσης. Πιο συγκεκριμένα, στην περίπτωση αυτή ο επιτιθέμενος δημιουργεί ένα SIP INVITE μήνυμα που περιέχει πλαστή ταυτότητα αποστολέα. Ο πληρεξούσιος εξυπηρέτης που λαμβάνει το μήνυμα δεσμεύει τους απαραίτητους πόρους για τη διαχείριση της συνόδου και αποστέλλει την αίτηση στον αποδέκτη (καλούμενος). Υποθέτοντας ότι ο καλούμενος είναι διαθέσιμος και αποδέχεται την κλήση, δημιουργεί μια απάντηση «200 OK» την οποία και προωθεί στον πληρεξούσιο εξυπηρέτη. Ο πληρεξούσιος εξυπηρέτης με τη σειρά του θα προσπαθήσει να αποστείλει την απόκριση του καλούμενου προς τον επιτιθέμενο, χωρίς επιτυχία όμως αφού έχει χρησιμοποιηθεί πλαστή ταυτότητα. Σύμφωνα με τις προδιαγραφές του SIP ο εξυπηρέτης θα διατηρεί την κλήση και θα κάνει συνεχείς προσπάθειες επανεκπομπής της απόκρισης, μέχρι να τερματιστεί η διαδικασία σύμφωνα με τις προδιαγραφές του SIP. Με τον τρόπο αυτό ένας επιτιθέμενος μπορεί να αποστείλει ένα μεγάλο αριθμό μηνυμάτων με στόχο την υλοποίηση επίθεσης πλημμύρας.

Μια παραλλαγή της TCP-SYN επίθεσης, πραγματοποιήθηκε την 11^{η} Ιανουαρίου του 2002. Στην επίθεση αυτή [84] αξιοποιήθηκε η αρχιτεκτονική πολλαπλών γεννητόρων (βλέπε Σχήμα 4–8) στην οποία όμως οι TCP εξυπηρέτες λειτουργούν ως ανακλαστήρες-προωθητές SYN/ACK μηνυμάτων προς το σύστημα στόχο. Συγκεκριμένα οι TCP εξυπηρέτες λάμβαναν TCP SYN αιτήσεις στις οποίες όμως υπήρχε η ταυτότητα του συστήματος στόχου. Το αποτέλεσμα ήταν όλη η κίνηση να προωθηθεί στο δίκτυο του συστήματος στόχου καταναλώνοντας τους υπολογιστικούς πόρους του δικτύου αυτού.



Σχήμα 4–15. Αρχιτεκτονική Επίθεσης Πλημμύρας τύπου Ανάκλασης

Ανάλογη επίθεση πλημμύρας τύπου ανάκλασης είναι δυνατόν να δημιουργηθεί και προς τους πληρεξούσιους εξυπηρέτες SIP. Συγκεκριμένα ο επιτιθέμενος θα δημιουργήσει μια πληθώρα από μηνύματα SIP INVITE τα οποία θα έχουν στην ταυτότητα αποστολέα τη διεύθυνση του συστήματος στόχου, με αποτέλεσμα όλες οι απαντήσεις να προωθούνται στο σύστημα στόχο. Παράδειγμα τέτοιας επίθεσης απεικονίζεται στο Σχήμα 4–16.

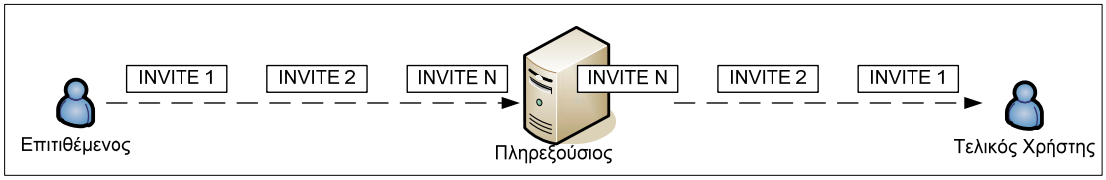


Σχήμα 4–16. Επίθεση Πλημμύρας προς Πληρεξούσιους Εξυπηρέτες τύπου Ανάκλασης

4.4.4.3 Επιθέσεις Πλημμύρας προς Τελικούς Χρήστες

Οι επιθέσεις πλημμύρας συνήθως έχουν ως στόχο κάποιο εξυπηρέτη. Υπάρχουν όμως και περιπτώσεις που ο στόχος είναι κάποιος τελικός χρήστης. Είναι γνωστό ότι οι συσκευές των τελικών χρηστών έχουν σχεδιαστεί κυρίως για να αποκρίνονται κάτω από συνηθισμένες καταστάσεις εισερχόμενης κίνησης, γεγονός που μεταφράζεται ως περιορισμένη δυνατότητα επεξεργασίας πολλαπλών εισερχόμενων αιτήσεων από τις τερματικές συσκευές. Συνεπώς, μόλις ο αριθμός των εισερχόμενων αιτήσεων υπερβεί κάποιο όριο η τερματική συσκευή δεν μπορεί να ανταποκριθεί προκαλώντας άρνηση παροχής υπηρεσίας στον τελικό χρήστη.

Οι επιθέσεις πλημμύρας που πραγματοποιούνται προς τερματικές συσκευές χρηστών είναι αντίστοιχες με αυτές που εμφανίζονται προς τους πληρεξούσιους με τη διαφορά ότι όλα τα δημιουργούμενα SIP INVITE μηνύματα έχουν τον ίδιο προορισμό (ίδιο URI), ενώ ο ρυθμός αποστολής είναι αρκετά μικρότερος συγκρινόμενος με την περίπτωση των επιθέσεων πλημμύρας προς ένα πληρεξούσιο εξυπηρέτη. Ο πληρεξούσιος σε αυτή την περίπτωση δρα ως φορέας της επίθεσης. Στο Σχήμα 4–17 παρουσιάζεται ένα παράδειγμα επίθεσης πλημμύρας προς ένα χρήστη.



Σχήμα 4–17. Παράδειγμα Επίθεσης Πλημμύρας προς Τελικό Χρήστη

4.4.5 Επιθέσεις Σηματοδοσίας

Το πρωτόκολλο SIP ορίζει ένα σύνολο μεθόδων για τον τερματισμό (termination), την ακύρωση (cancellation), την ενημέρωση και την ανακατεύθυνση (redirection) μιας συνόδου. Σύμφωνά με τις εργασίες [19],[20] ένας κακόβουλος χρήστης είναι σχεδόν βέβαιο ότι θα προσπαθήσει να τροποποιήσει ή να αποστείλει κάποιο από τα προαναφερόμενα μηνύματα για να προκαλέσει άρνηση παροχής υπηρεσίας ή μη εξουσιοδοτημένη πρόσβαση στην προσφερόμενη υπηρεσία. Συνεπώς, μια επίθεση σηματοδοσίας ορίζεται ως: *οποιαδήποτε μη εξουσιοδοτημένη προσπάθεια για τροποποίηση ή αποστολή μηνυμάτων σηματοδοσίας που οδηγεί είτε σε μη εξουσιοδοτημένη πρόσβαση στην υπηρεσία ή σε άρνηση παροχής υπηρεσίας σε έναν ή περισσότερους εξουσιοδοτημένους χρήστης που συμμετέχουν σε μία σύνοδο.*

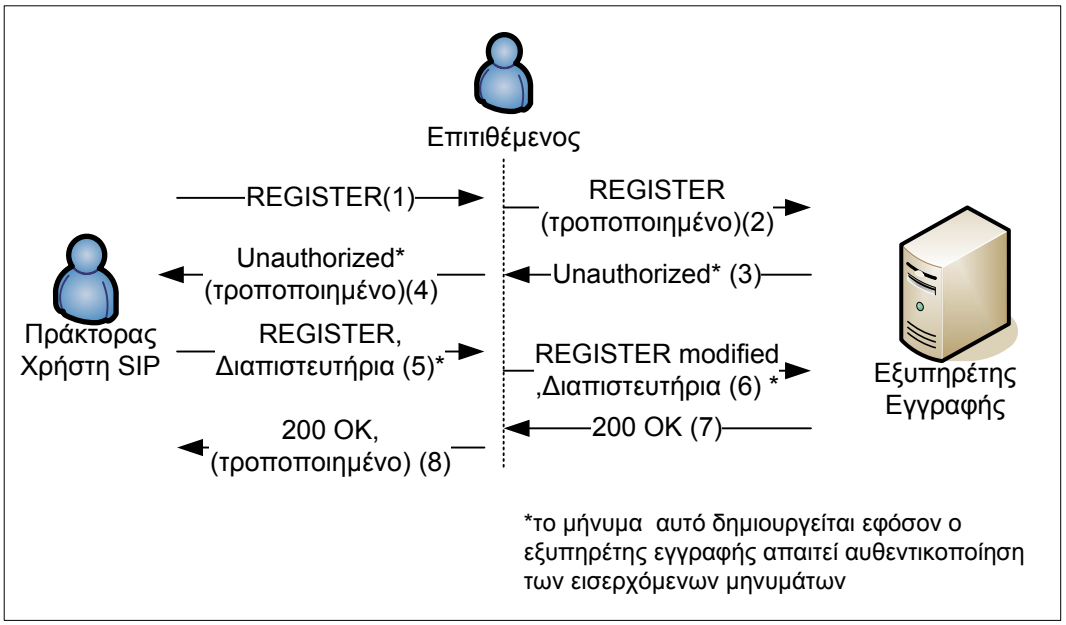
Οι επιθέσεις σηματοδοσίας συνδέονται άμεσα με απειλές όπως απάτες χρεώσεων, πλαστοπροσωπίας χρήστη και εξυπηρέτη, και άρνησης παροχής υπηρεσίας. Οι κύριες αιτίες εμφάνισης των επιθέσεων σηματοδοσίας είναι:

1. Η μη ορθή χρήση-εφαρμογή των μηχανισμών αυθεντικοποίησης στα μηνύματα σηματοδοσίας.
2. Η έλλειψη μηχανισμών διασφάλισης της ακεραιότητας των μηνυμάτων σηματοδοσίας.

Χαρακτηριστικό είναι το γεγονός ότι στις προδιαγραφές του SIP η χρήση μηχανισμών αυθεντικοποίησης δεν είναι υποχρεωτική για όλες τις μεθόδους, ενώ σε ορισμένες περιπτώσεις δεν είναι καν δυνατή η εφαρμογή των προτεινόμενων μηχανισμών λόγω περιορισμών που υφίστανται από τις ίδιες τις προδιαγραφές του SIP (βλέπε ενότητα 5.2.5). Επιπλέον δεν προτείνεται η χρήση μηχανισμών ακεραιότητας, προσφέροντας έτσι ευκαιρίες για εκδήλωση επιθέσεων ενδιάμεσου.

4.4.5.1 Επιθέσεις Σηματοδοσίας Κατά τη Διαδικασία Εγγραφής

Η υπηρεσία εγγραφής είναι το αρχικό σημείο αναζήτησης ευπαθειών που δυνητικά θα μπορούσαν κάποιοι να εκμεταλλευτούν για να εκδηλώσουν επιθέσεις σηματοδοσίας. Ο πρώτος στόχος του επιτιθέμενου είναι να προσποιηθεί επιτυχώς κάποιον εξουσιοδοτημένο χρήστη. Προς αυτή την κατεύθυνση, είτε θα πραγματοποιήσει κάποια επίθεση ενδιάμεσου κατά τη διαδικασία εγγραφής, είτε θα υποκλέψει κάποιο μήνυμα εγγραφής με στόχο να το αξιοποιήσει μελλοντικά. Στην περίπτωση επίθεσης ενδιάμεσου ο επιτιθέμενος είτε θα τροποποιήσει τη διεύθυνση επαφής του αρχικού μηνύματος, με στόχο οι κλήσεις να λαμβάνονται από τον επιτιθέμενο, ή θα τροποποιήσει τα δεδομένα της κεφαλίδας λήξης εγγραφής στη τιμή μηδέν με αποτέλεσμα ο εξουσιοδοτημένος χρήστης να μην εγγραφεί στην υπηρεσία (τα μηνύματα SIP REGISTER με μηδενική τιμή στην κεφαλίδα λήξη εγγραφής μεταφράζονται από την υπηρεσία ως τερματισμός σύνδεσης με αυτή). Παράδειγμα τέτοιας επίθεσης παρουσιάζεται στο Σχήμα 4–18. Αξίζει να σημειωθεί ότι ο επιτιθέμενος μπορεί να οδηγήσει τον εξουσιοδοτημένο χρήστη στη δημιουργία του κατάλληλου μηνύματος εγγραφής, συμπεριλαμβανομένων των αντίστοιχων διαπιστευτηρίων (εξαρτάται από τον τρόπο υλοποίησης του αντίστοιχου πελάτη SIP), προωθώντας του το «Unauthorized» μήνυμα που δημιουργήθηκε μετά από αίτηση του επιτιθέμενου. Η διαδικασία που ακολουθείται στην περίπτωση αυτή είναι αντίστοιχη με αυτή που παρουσιάζεται στο Σχήμα 4–18. Η μοναδική διαφορά είναι ότι απουσιάζει το αρχικό SIP REGISTER μήνυμα που αποστέλλεται από τον εξουσιοδοτημένο χρήστη.



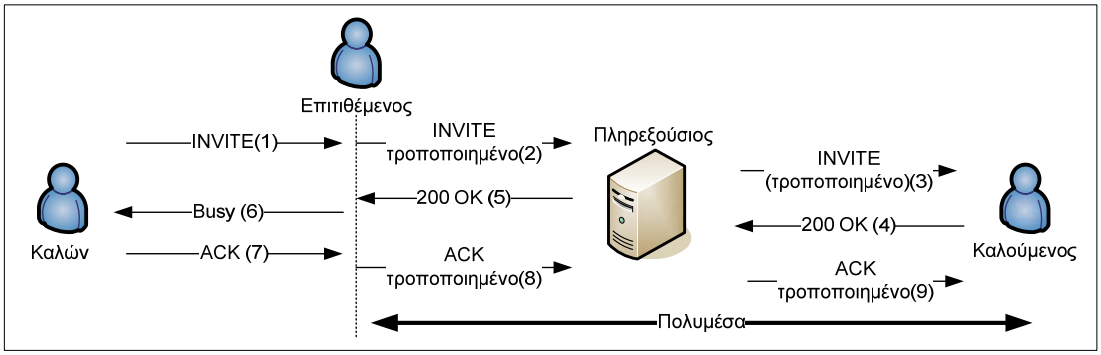
Σχήμα 4–18. Παράδειγμα Επίθεσης Ενδιάμεσου κατά τη Διαδικασία Εγγραφής

Στη δεύτερη περίπτωση (όπου γίνεται χρήση μηνύματος υποκλοπής) ουσιαστικά ο επιτιθέμενος θα πραγματοποιήσει μια επίθεση επανάληψης (replay attack), καθώς έχει ένα έγκυρο μήνυμα εγγραφής ενός εξουσιοδοτημένου χρήστη με διαπιστευτήρια που έχουν υπολογισθεί σε προηγούμενη σύνδεση. Εάν η υπηρεσία εγγραφής κατά το σχεδιασμό της δεν έχει λάβει υπόψη επιθέσεις επανάληψης, ο επιτιθέμενος με την αποστολή του μηνύματος εγγραφής θα έχει πρόσβαση στις υπηρεσίες που παρέχονται στον εξουσιοδοτημένο χρήστη χωρίς αυτό να γίνει αντιληπτό από την υπηρεσία αλλά ούτε και από τον εξουσιοδοτημένο χρήστη.

4.4.5.2 Επιθέσεις Σηματοδοσίας κατά τη Διαδικασία Αποκατάστασης Συνόδου

Αντίστοιχα βήματα με αυτά της επίθεσης ενδιάμεσου κατά της υπηρεσίας εγγραφής, μπορεί να ακολουθήσει ένας επιτιθέμενος κατά τη διαδικασία αποκατάστασης μιας συνόδου. Συγκεκριμένα, σε αυτό το σενάριο ο επιτιθέμενος τροποποιεί το αρχικό μήνυμα SIP INVITE, που έχει δημιουργήσει ο εξουσιοδοτημένος χρήστης, και συγκεκριμένα τη διεύθυνση επαφής, προωθώντας το στον υπεύθυνο πληρεξούσιο εξυπηρέτη. Ο πληρεξούσιος εξυπηρέτης, με τη σειρά του, το προωθεί στον καλούμενο ο οποίος, υποθέτουμε ότι δέχεται την κλήση και συνεπώς αποκρίνεται με ένα μήνυμα «200 OK». Μέσω του πληρεξούσιου εξυπηρέτη το μήνυμα αυτό προωθείται στον επιτιθέμενο. Μόλις ο επιτιθέμενος λάβει τη συγκεκριμένη απάντηση δεν την προωθεί στον τελικό χρήστη αλλά την αντικαθιστά με ένα μήνυμα απασχολημένος (busy), το οποίο και τελικώς αποστέλλει στον εξουσιοδοτημένο χρήστη. Ο τελευταίος αποκρίνεται με το αντίστοιχο μήνυμα επιβεβαίωσης (SIP ACK) και τερματίζει την αρχική σύνοδο θεωρώντας ότι η σύνδεση δεν έχει αποκατασταθεί. Στην πραγματικότητα όμως η σύνδεση έχει αποκατασταθεί μεταξύ επιτιθέμενου και καλούμενου, χωρίς αυτό να γίνεται αντιληπτό ούτε από τον καλούντα αλλά ούτε από την υπηρεσία. Η παραπάνω διαδικασία απεικονίζεται στο Σχήμα 4–19.

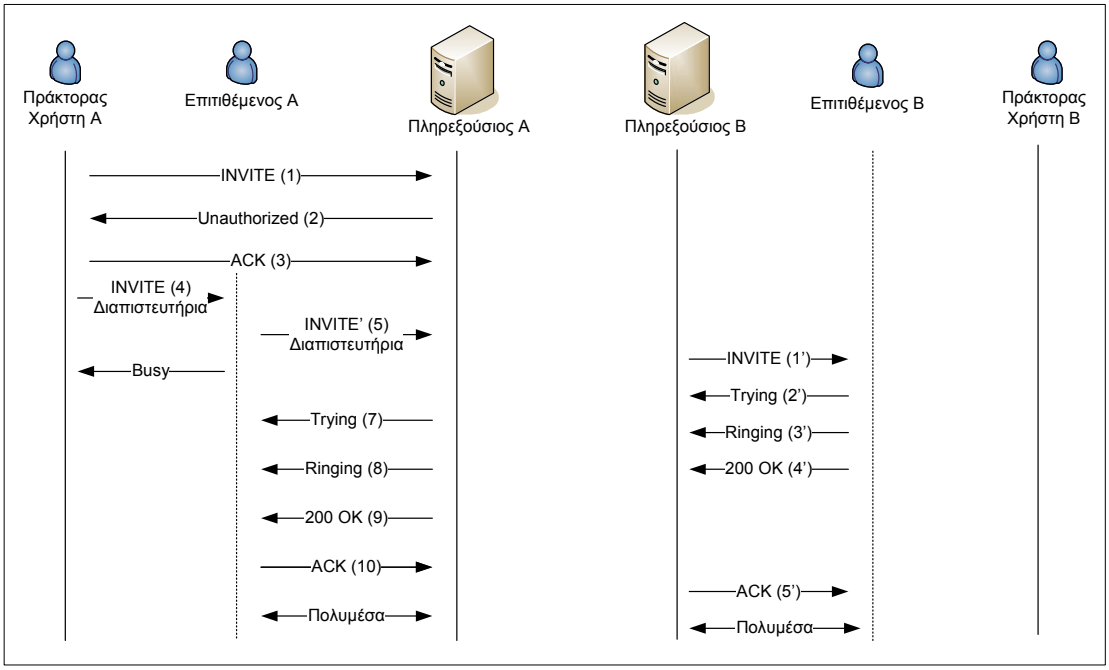
Με τον ίδιο ακριβώς τρόπο ένας επιτιθέμενος που υλοποιεί μια επίθεση ενδιάμεσου μπορεί να μιμηθεί την υπηρεσία ανακατεύθυνσης, αναγκάζοντας έτσι τους εξουσιοδοτημένους χρήστες της υπηρεσίας να αποστέλλουν τα δεδομένα τους μέσω μη εξουσιοδοτημένων εξυπηρετών.



Σχήμα 4–19. Παράδειγμα Επίθεσης Ενδιάμεσου κατά τη Διαδικασία Αποκατάστασης Συνόδου

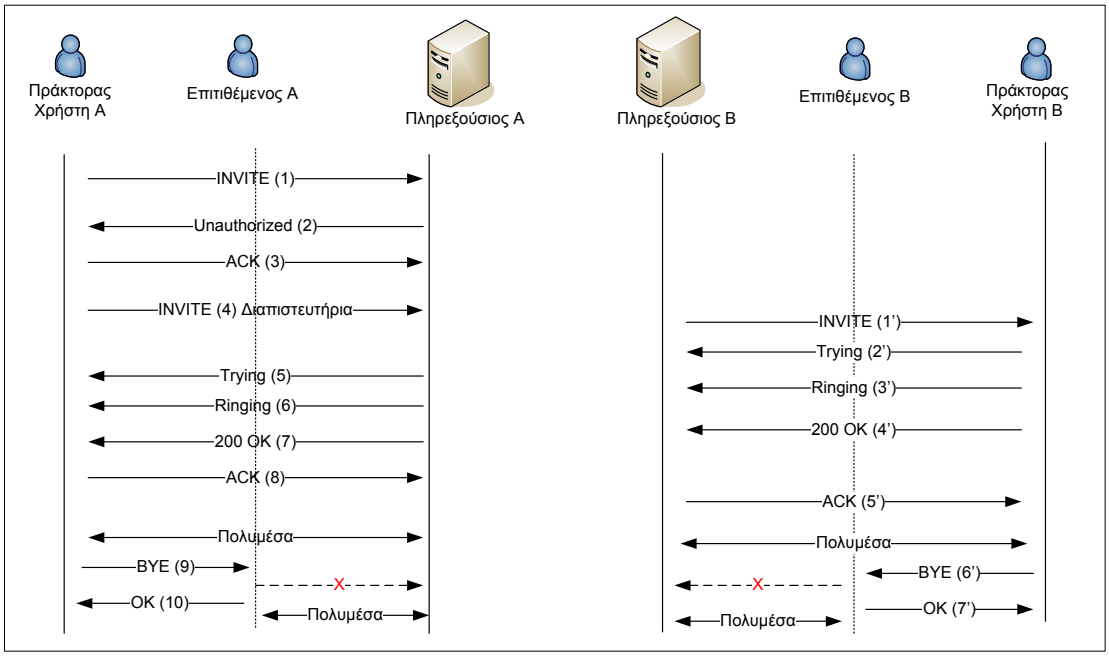
4.4.5.3 Επιθέσεις Απάτης Χρεώσεων

Παρόμοια διαδικασία ακολουθείται σε επιθέσεις απάτης χρεώσεων γνωστές ως «FakeBusy, ByeDelay, ByeDrop, InviteReplay» [63]. Η βασική διαφορά μεταξύ της επίθεσης ενδιάμεσου κατά την αποκατάσταση μιας συνόδου και της επίθεσης «FakeBusy» εντοπίζεται στην ύπαρξη ενός ακόμα επιτιθέμενου που λειτουργεί για λογαριασμό του καλούμενου. Ο επιτιθέμενος που βρίσκεται στη μεριά του καλούντα τροποποιεί το αρχικό μήνυμα SIP INVITE όπως ακριβώς και στην προηγούμενη περίπτωση, ενημερώνοντας τον καλούντα ότι ο καλούμενος είναι απασχολημένος. Ο επιτιθέμενος που βρίσκεται στη μεριά του καλούμενου παρεμποδίζει την προώθηση των μηνυμάτων στον καλούμενο προσδιορίζοντας τη δική του διεύθυνση επαφής στα μηνύματα απόκρισης, με αποτέλεσμα να γίνεται αποκατάσταση κλήσης μεταξύ των δύο κακόβουλων χρηστών, χωρίς αυτό να γίνεται αντιληπτό από καμία οντότητα. Η προαναφερόμενη διαδικασία απεικονίζεται στο Σχήμα 4–20.



Σχήμα 4–20. Η Περίπτωση Επίθεσης FakeBusy

Αναφορικά με τις επιθέσεις «ByeDelay» και «ByeDrop» υπάρχουν αντιστοίχως δύο ενδιάμεσοι, όπως και στην περίπτωση του «FakeBusy», που παρεμποδίζουν την προώθηση των SIP BYE μηνυμάτων στον κατάλληλο πληρεξούσιο εξυπηρέτη και στη συνέχεια στον άλλο εξουσιοδοτημένο χρήστη. Δημιουργούν όμως την κατάλληλη απόκριση επιτυχούς τερματισμού της κλήσης, δίνοντας έτσι την εντύπωση ότι η κλήση έχει τερματιστεί επιτυχώς ενώ ο επιτιθέμενος αξιοποιεί τις αρχικές παραμέτρους επικοινωνίας για τη μετάδοση δεδομένων φωνής με τον επιτιθέμενο που βρίσκεται στην άλλη μεριά (βλέπε Σχήμα 4–21). Όλη η χρέωση γίνεται στον εξουσιοδοτημένο χρήστη που αρχικοποίησε τη συνομιλία.



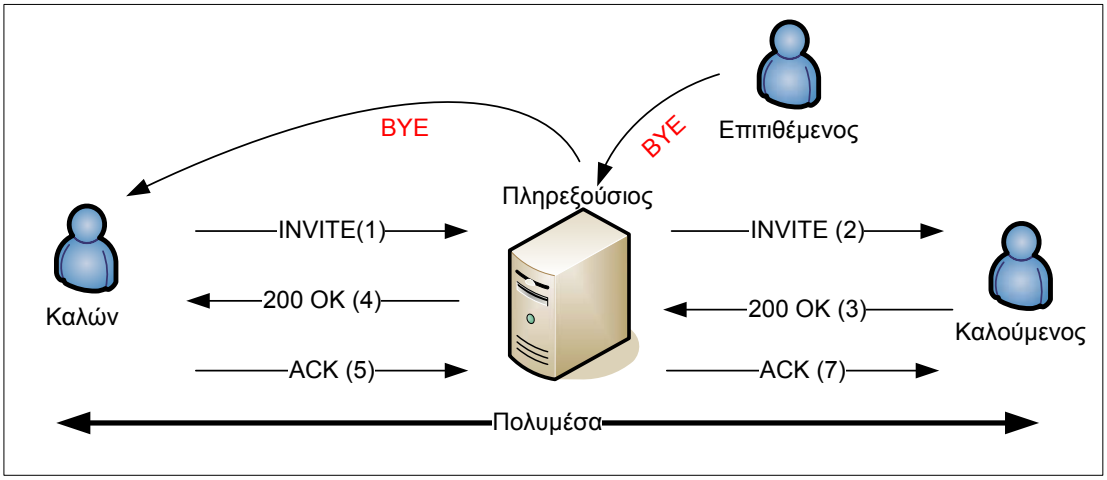
Σχήμα 4–21. Οι Περιπτώσεις Επιθέσεων ByeDelay & ByeDrop

Η επίθεση «InviteReplay» είναι αντίστοιχη με την επίθεση επανάληψης κατά τη διαδικασία εγγραφής. Συγκεκριμένα, ένας επιτιθέμενος που έχει υποκλέψει κάποιο SIP INVITE μήνυμα,

το οποίο συμπεριλαμβάνει τα αντίστοιχα διαπιστευτήρια, (εφόσον τα μηνύματα SIP INVITE αυθεντικοποιούνται από την υπηρεσία), μπορεί να το αξιοποιήσει μελλοντικά για την αποκατάσταση συνόδου με οποιοδήποτε χρήστη επιθυμεί, χρεώνοντας το λογαριασμό του εξουσιοδοτημένου χρήστη που δημιούργησε το μήνυμα αυτό.

4.4.5.4 Επιθέσεις Σηματοδοσίας Τερματισμού Κλήσεων

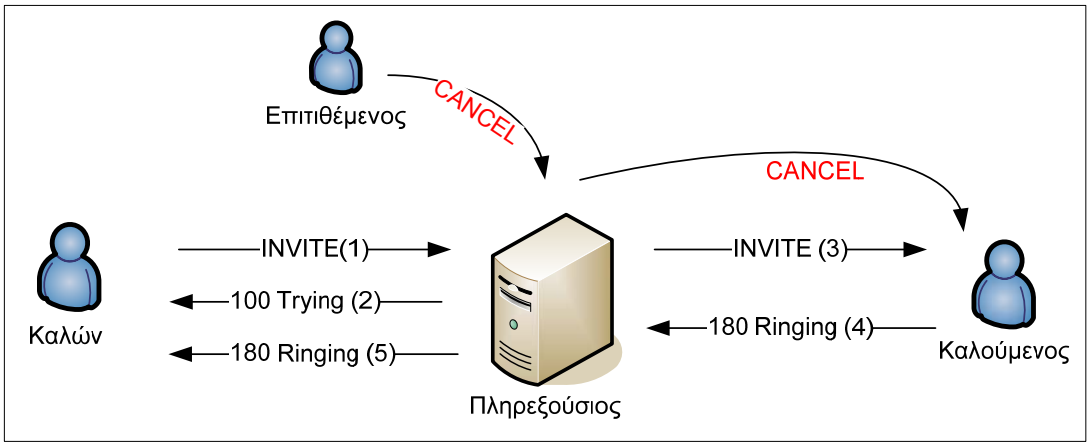
Εκτός όμως των επιθέσεων τύπου ενδιάμεσου, ένας επιτιθέμενος είναι σε θέση να εισάγει κάποια μηνύματα σηματοδοσίας προκειμένου να προκαλέσει άρνηση παροχής υπηρεσίας σε συγκεκριμένους χρήστες. Για παράδειγμα, η εισαγωγή ενός μηνύματος SIP BYE, το οποίο αντιστοιχεί σε μία συγκεκριμένη σύνοδο, προκαλεί τη μη εξουσιοδοτημένη λήξη της συγκεκριμένης συνόδου. Παράδειγμα μιας τέτοιας επίθεσης απεικονίζεται στο Σχήμα 4–22. Να σημειωθεί ότι για τη δημιουργία του κατάλληλου μηνύματος SIP BYE απαιτείται η γνώση των παραμέτρων της συνόδου. Αυτό μπορεί να επιτευχθεί με την υποκλοπή των αρχικών μηνυμάτων που αντιστοιχούν στη συγκεκριμένη σύνοδο και εμπεριέχουν τις παραμέτρους της συνόδου.



Σχήμα 4–22. Παράδειγμα Επίθεσης Σηματοδοσίας BYE

Αντιστοίχως, ο επιτιθέμενος θα μπορούσε να αξιοποιήσει το μήνυμα SIP CANCEL για την ακύρωση μιας αίτησης που βρίσκεται σε εξέλιξη, όπως παρουσιάζεται στο Σχήμα 4–23. Εναλλακτικά, ο επιτιθέμενος μπορεί να προσπαθήσει να πραγματοποιήσει τροποποίηση των παραμέτρων μιας συνόδου, αποστέλλοντας είτε ένα SIP re-INITE, είτε ένα SIP UPDATE μήνυμα, με στόχο είτε την ανακατεύθυνση των δεδομένων, είτε την υποβάθμιση της ποιότητας της υπηρεσίας και συνεπώς την αδυναμία επικοινωνίας των χρηστών.

Μια τελευταία, αλλά εξ' ίσου σημαντική, περίπτωση επίθεσης σηματοδοσίας μπορεί να πραγματοποιηθεί όταν τροποποιούνται δεδομένα σηματοδοσίας PSTN που μεταδίδονται μέσω ενός SIP δικτύου με στόχο την ανακατεύθυνσης της κλήσης, την άρνηση παροχής υπηρεσίας και πολλά άλλα.



Σχήμα 4–23. Παράδειγμα Επίθεσης Σηματοδοσίας CANCEL

4.4.6 Επιθέσεις Κοινωνικής Μηχανικής

Η «Κοινωνική Μηχανική» αποτελεί έναν όρο δανειζόμενο από τη φιλοσοφία ο οποίος αξιοποιείται για να αποτυπώσει συγκεκριμένες μεθόδους που χρησιμοποιούν κακόβουλοι χρήστες για την εξαπάτηση και παραπλάνηση χρηστών που, στις περισσότερες των περιπτώσεων, δεν έχουν τις απαραίτητες γνώσεις για την κατανόηση των προθέσεων των επιτιθέμενων. Χαρακτηριστικό παράδειγμα τέτοιων επιθέσεων αποτελεί η ηλεκτρονική αλληλογραφία που προτρέπει τους χρήστες να υποβάλουν εμπιστευτικές πληροφορίες όπως αριθμό πιστωτικής κάρτας και τον προσωπικό τους αριθμό αναγνώρισης γιατί έχει εντοπισθεί κάποιο πρόβλημα στην κάρτα τους.

Αντίστοιχα σενάρια μπορούν να εμφανισθούν και στη διαδικτυακή τηλεφωνία. Συγκεκριμένα στην εργασία [87] επιδεικνύεται μια τέτοια επίθεση, κατά την οποία ο εξουσιοδοτημένος χρήστης οδηγείται σε ένα συγκεκριμένο ιστοτόπο ο οποίος περιλαμβάνει αιτήματα HTTP προς τη δικτυακή διεπαφή ενός τηλεφώνου, που ουσιαστικά δημιουργούν κλήσεις προς άλλους προορισμούς χωρίς αυτό να γίνεται αντιληπτό από τους εξουσιοδοτημένους χρήστες.

4.5 Συμπεράσματα

Στη διαδικτυακή τηλεφωνία εμφανίζονται απειλές που δεν υπήρχαν στο PSTN. Ταυτόχρονα, τα σημεία ευπάθειας της διαδικτυακής τηλεφωνίας και η μη εφαρμογή των κατάλληλων μηχανισμών ασφάλειας, σε συνδυασμό με την ανοιχτή αρχιτεκτονική του διαδικτύου, προσφέρουν τις κατάλληλες ευκαιρίες σε κακόβουλους χρήστες να εκδηλώσουν επιθέσεις εκμεταλλευόμενοι τις αντίστοιχες ευπάθειες. Ο Πίνακας 4–2 που ακολουθεί παρουσιάζει συνοπτικά τη συσχέτιση μεταξύ απειλών, ευπαθειών και επιθέσεων, όπως αυτή έχει προκύψει από την ανάλυση που έγινε στο κεφάλαιο αυτό. Γίνεται αντιληπτό ότι ο κύριος λόγος εμφάνισης των επιθέσεων στη διαδικτυακή τηλεφωνία οφείλεται στην έλλειψη των κατάλληλων μηχανισμών ασφαλείας που ουσιαστικά είναι συνέπεια της μη λεπτομερούς καταγραφής των απαιτήσεων ασφάλειας (αφού ληφθούν υπόψη οι πιθανές απειλές και ευπάθειες) κατά τον αρχικό σχεδιασμό των υπηρεσιών.

Απειλή	Ευπάθεια	Κατηγορία Επίθεσης	Επιπτώσεις
Μη Εξουσιοδοτημένη Πρόσβαση	Έλλειψη μηχανισμών Εμπιστευτικότητας Εύκολη πρόσβαση στο μέσο μετάδοσης	Υποκλοπές μηνυμάτων σηματοδοσίας & φωνής	Παραβίαση Εμπιστευτικότητας
Μη Εξουσιοδοτημένη Τροποποίηση	Έλλειψη μηχανισμών Εμπιστευτικότητας Εύκολη Πρόσβαση στο μέσο μετάδοσης	Επιθέσεις Σηματοδοσίας Επιθέσεις προς τους αναλυτές μηνυμάτων Επιθέσεις έγχυσης κώδικα	Παραβίαση Ακεραιότητας & Διαθεσιμότητας
Πλαστοπροσωπία χρήστη	Χρήση μη κατάλληλων μηχανισμών αυθεντικοποίησης	Επιθέσεις Σηματοδοσίας Επιθέσεις Ενδιάμεσου	Παραβίαση Εμπιστευτικότητας & Αυθεντικότητας
Πλαστοπροσωπία εξυπηρέτη	Έλλειψη μηχανισμών αυθεντικοποίσης εξυπηρετών	Επιθέσεις Ενδιάμεσου	Παραβίαση Αυθεντικότητας & Ακεραιότητας
Απάτες Χρεώσεων Παρόχων-Χρηστών	Χρήση μη κατάλληλων μηχανισμών αυθεντικόποίησης & έλλειψη μηχανισμών ακεραιότητας	Επιθέσεις Σηματοδοσίας Επιθέσεις έγχυσης κώδικα	Παραβίαση Αυθεντικότητας & Ακεραιότητας
Άρνηση Παροχής Υπηρεσίας	Μη ορθή υλοποίηση των αναλυτών μηνυμάτων	Επιθέσεις προς τους αναλυτές μηνυμάτων	Παραβίαση Διαθεσιμότητας υπηρεσίας
	–	Επιθέσεις Πλημμύρας	
	Χρήση μη κατάλληλων μηχανισμών αυθεντικόποίησης & έλλειψη μηχανισμών ακεραιότητας	Επιθέσεις Σηματοδοσίας	
Εξαπάτησης	Έλλειψη εκπαίδευσης των χρηστών	Επιθέσεις κοινωνικής μηχανικής	Παραβίαση Εμπιστευτηκότητας & Αυθεντικότητας

Πίνακας 4–2. Συσχετισμός Απειλών–Ευπαθειών και Επιθέσεων στη Διαδικτυακή Τηλεφωνία

ΚΕΦΑΛΑΙΟ 5: Απαιτήσεις και Υπάρχοντες Μηχανισμοί Ασφαλείας στη Διαδικτυακή Τηλεφωνία

5.1 Γενικά

Η προστασία των δεδομένων και των υπολογιστικών πόρων καθώς και η αδιάλειπτη παροχή των προσφερόμενων υπηρεσιών πρέπει να αποτελούν τις βασικές σχεδιαστικές αρχές οποιουδήποτε πληροφοριακού συστήματος. Οι λειτουργικές και μη λειτουργικές απαιτήσεις που προκύπτουν είναι απαραίτητο να εξειδικεύονται κατά περίπτωση, λαμβάνοντας υπόψη τις πιθανές απειλές και ευπάθειες του συστήματος, με στόχο την ελαχιστοποίηση της εκδήλωσης επίθεσης. Η παραπάνω διαδικασία καθορισμού απαιτήσεων, είναι απαραίτητη και στην περίπτωση της διαδικτυακής τηλεφωνίας η οποία και θεωρείται υπηρεσία υψηλής κρισιμότητας. Οι χρήστες των υπηρεσιών τηλεφωνίας απαιτούν, πέρα από αξιοπιστία και διαθεσιμότητα, υψηλό επίπεδο ασφαλείας που θα είναι τουλάχιστον αντίστοιχο με αυτό του PSTN.

Ως εκ τούτου, για την ανάπτυξη ασφαλών και αξιόπιστων υπηρεσιών τηλεφωνίας στο διαδίκτυο πρέπει να προσδιοριστούν οι απαιτήσεις ασφαλείας, ώστε στη συνέχεια να επιλεγούν και να ενσωματωθούν στις παρεχόμενες υπηρεσίες οι κατάλληλοι μηχανισμοί ασφαλείας. Κατά τη διαδικασία αυτή είναι απαραίτητο να ληφθούν υπόψη τόσο τα πιθανά προβλήματα ασφαλείας που μπορεί να εμφανιστούν, όσο και οι περιορισμοί που προκύπτουν από τα πρωτόκολλα που αξιοποιούνται.

Στο Κεφάλαιο αυτό προσδιορίζονται οι απαιτήσεις ασφαλείας που πρέπει να ικανοποιούνται από τις υπηρεσίες διδιακτυακής τηλεφωνίας που βασίζονται στο πρωτόκολλο σηματοδοσίας SIP. Ακολούθως περιγράφονται οι υπάρχοντες μηχανισμοί ασφαλείας, για την προστασία του πρωτοκόλλου σηματοδοσίας SIP, με στόχο να αξιολογηθούν και συνεπώς να εντοπισθούν περιπτώσεις (εφόσον υπάρχουν) που οι υπάρχοντες μηχανισμοί δεν είναι επαρκείς ή δεν λαμβάνουν υπόψη τους περιορισμούς που θέτουν τα αξιοποιούμενα πρωτόκολλα.

5.2 Απαιτήσεις Ασφάλειας στη Διαδικτυακή Τηλεφωνία

Οι απαιτήσεις ασφάλειας που πρέπει κατ' ελάχιστον να ικανοποιούνται [88], τόσο για τα δεδομένα φωνής όσο και για τα δεδομένα σηματοδοσίας, είναι οι ακόλουθες:

1. Εμπιστευτικότητα (Confidentiality)
2. Ακεραιότητα (Integrity)
3. Διαθεσιμότητα (Availability)

Στην περίπτωση των υπηρεσιών διαδικτυακής τηλεφωνίας, πέραν των προαναφερόμενων απαιτήσεων θα πρέπει να εξασφαλίζεται και η Αυθεντικότητα (Authenticity) των δεδομένων–μηνυμάτων που ανταλλάσσονται. Η αναγκαιότητα ενσωμάτωσης της αυθεντικότητας ως επιπρόσθετης, ρητής απαίτησης ασφαλείας προκύπτει από τη σοβαρότητα των επιπτώσεων που θα υποστεί ο χρήστης ή/και ο πάροχος της υπηρεσίας σε περίπτωση επιτυχών επιθέσεων που βασίζονται στην αδυναμία ελέγχου της αυθεντικότητας των δεδομένων (Πίνακας 4–2).

Στη συνέχεια προσδιορίζονται οι απαιτήσεις ασφαλείας που πρέπει να ικανοποιούνται από τις υπηρεσίες διδιακτυακής τηλεφωνίας που βασίζονται στο πρωτόκολλο σηματοδοσίας SIP.

5.2.1 Απαίτηση Ασφάλειας 1: Εμπιστευτικότητα

Οι υπηρεσίες εμπιστευτικότητας, στα πλαίσια παροχής υπηρεσιών ασφαλείας, διασφαλίζουν τη μη αποκάλυψη των δεδομένων, που χρησιμοποιούνται για την διεκπεραίωση των λειτουργιών της υπηρεσίας, σε μη εξουσιοδοτημένες οντότητες [88].

Υπό το πρίσμα της διαδικτυακής τηλεφωνίας, ο παραπάνω ορισμός δεν διαφοροποιείται παρά μόνο εξειδικεύεται ως ακολούθως:

1. Μόνο εξουσιοδοτημένοι πληρεξούσιοι εξυπηρέτες έχουν πρόσβαση στα μηνύματα (μη συμπεριλαμβανομένων των μηνυμάτων εγγραφής) που απαιτούνται για τη διαχείριση μιας συνόδου, με δικαίωμα τροποποίησης μόνο στις περιπτώσεις που ορίζει το SIP.
2. Μόνο οι εξουσιοδοτημένοι εξυπηρέτες εγγραφής έχουν πρόσβαση (χωρίς δικαίωμα ώματα τροποποίησης) στα μηνύματα εγγραφής.
3. Μόνο οι εξουσιοδοτημένοι τελικοί χρήστες και εξυπηρέτες έχουν πλήρη πρόσβαση στα δεδομένα σηματοδοσίας (χωρίς δικαίωμα τροποποίησης).

5.2.2 Απαίτηση Ασφάλειας 2: Ακεραιότητα

Οι υπηρεσίες ακεραιότητας, στα πλαίσια παροχής υπηρεσιών ασφάλειας, διασφαλίζουν τη μη εξουσιοδοτημένη τροποποίηση των δεδομένων που απαιτούνται για τη διεκπεραίωση μιας συναλλαγής [88].

Στις υπηρεσίες διαδικτυακής τηλεφωνίας, υπάρχουν περιπτώσεις που οι πληρεξούσιοι εξυπηρέτες πρέπει να τροποποιήσουν τα μηνύματα που προωθούν, εισάγοντας κάποιες επιπρόσθετες κεφαλίδες. Συνεπώς, οι υπηρεσίες ακεραιότητας πρέπει να διασφαλίζουν την ακεραιότητα των μηνυμάτων σηματοδοσίας τόσο μεταξύ πληρεξούσιων εξυπηρετών, όσο και από άκρο σε άκρο.

5.2.3 Απαίτηση Ασφάλειας 3: Διαθεσιμότητα

Οι υπηρεσίες διαθεσιμότητας, στα πλαίσια παροχής υπηρεσιών ασφάλειας, διασφαλίζουν την προσβασιμότητα στην υπηρεσία οποιαδήποτε χρονική στιγμή μια εξουσιοδοτημένη οντότητα αιτηθεί πρόσβαση σε αυτή [88].

Αντίστοιχα, στην περίπτωση της διαδικτυακής τηλεφωνίας οι υπηρεσίες διαθεσιμότητας θα πρέπει να εξασφαλίζουν την πρόσβαση στην υπηρεσία σε επίπεδα παρόμοια με αυτά που επιτυγχάνονται στο PSTN.

5.2.4 Απαίτηση Ασφάλειας 4: Αυθεντικότητα

Οι υπηρεσίες αυθεντικότητας διασφαλίζουν τη γνησιότητα τόσο της ταυτότητας των χρηστών, όσο και της πηγής δημιουργίας των δεδομένων [88].

Αντίστοιχα, στην περίπτωση των υπηρεσιών διαδικτυακής τηλεφωνίας απαιτείται τόσο η διασφάλιση της αυθεντικότητας της ταυτότητας των χρηστών, όσο και της πηγής δημιουργίας των δεδομένων είτε αυτή είναι κάποιος τελικός χρήστης ή κάποια άλλη δικτυακή οντότητα.

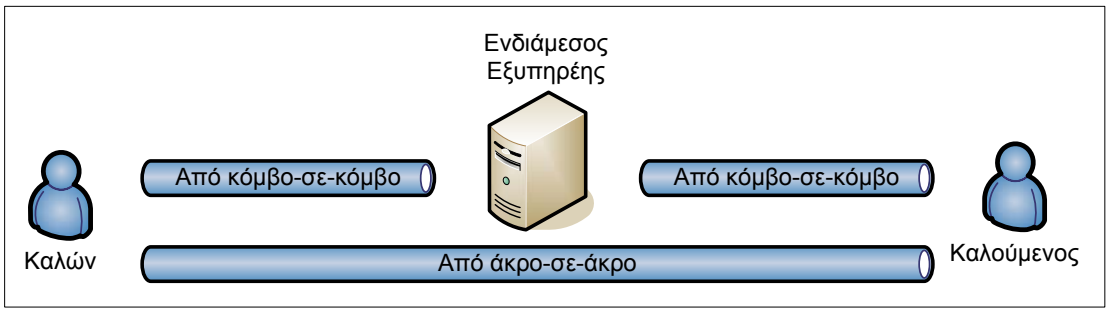
5.2.5 Περιορισμοί που Προκύπτουν από το SIP

Για το σχεδιασμό των κατάλληλων μέτρων ασφαλείας των υπηρεσιών διαδικτυακής τηλεφωνίας, πέραν των προαναφερόμενων απαιτήσεων ασφάλειας, θα πρέπει να λαμβάνονται υπόψιν οι ακόλουθοι περιορισμοί που προκύπτουν από τις προδιαγραφές του SIP:

1. Οι ενδιάμεσες οντότητες (κυρίως οι πληρεξούσιοι εξυπηρέτες) απαιτούν πρόσβαση σε συγκεκριμένες κεφαλίδες για την επεξεργασία και τη δρομολόγηση των αιτημάτων που λαμβάνουν, με αποτέλεσμα να μην είναι δυνατή η πλήρης κρυπτογράφηση των μηνυμάτων σηματοδοσίας.
2. Τα μηνύματα SIP CANCEL, SIP ACK καθώς και οι SIP αποκρίσεις, σύμφωνα με τις προδιαγραφές του SIP δεν είναι δυνατόν να «προκληθούν» για αυθεντικοποίηση, καθώς δεν είναι επιτρεπτή η εκ νέου υποβολή των μηνυμάτων αυτών.

5.3 Προτεινόμενοι Μηχανισμοί Ασφάλειας στο SIP

Σύμφωνα με τις προδιαγραφές του SIP [11], τα προτεινόμενα μέτρα προστασίας βασίζονται σε μηχανισμούς ασφαλείας που έχουν εφαρμοσθεί με επιτυχία σε άλλες υπηρεσίες του διαδικτύου. Όπως απεικονίζεται στο Σχήμα 5–1., οι μηχανισμοί αυτοί παρέχουν υπηρεσίες ασφάλειας είτε από άκρο σε άκρο (end-to-end) είτε από κόμβο σε κόμβο (hop-by-hop).



Σχήμα 5–1. Προτεινόμενοι Μηχανισμοί Ασφαλείας στο SIP

Πιο συγκεκριμένα, προτείνεται η αξιοποίηση των παρακάτω μηχανισμών:

1. HTTP Digest [85]
2. IP Security [89]
3. Transport Layer Security (TLS) [90]
4. SIP Secure (SIPS) [11]
5. Secure MIME (S/MIME) [91]

5.3.1 HTTP Digest

Η πλέον ευρέως εφαρμοζόμενη μέθοδος αυθεντικοποιήσης χρηστών στο SIP βασίζεται στο HTTP Digest [85]. Το πρωτόκολλο αυτό αξιοποιεί την τεχνική πρόκλησης-απάντησης (challenge-response) ενώ απαιτεί την προκαθορισμένη εμπιστοσύνη μεταξύ πελάτη και υπηρεσίας για το διαμοιρασμό των απαραίτητων συνθηματικών και την αποθήκευση τους στον πάροχο της υπηρεσίας.

Για κάθε αίτημα που απαιτείται αυθεντικοποίηση, ακολουθείται η παρακάτω διαδικασία:

1. Αρχικά ο χρήστης στέλνει ένα SIP αίτημα (π.χ SIP REGISTER) προς τον κατάλληλο πληρεξούσιο.
2. Ο πληρεξούσιος απαιτεί αυθεντικοποίηση του μηνύματος, με αποτέλεσμα να δημιουργεί και να αποστέλλει προς τον τελικό χρήστη μια απόκριση «401 unauthorized», η οποία περιλαμβάνει τα δεδομένα που θα χρησιμοποιήσει ο χρήστης για τη δημιουργία των διαπιστευτηρίων.

3. Μόλις ο χρήστης λάβει την παραπάνω απόκριση, δημιουργεί ένα νέο αίτημα στο οποίο συμπεριλαμβάνει την κεφαλίδα «authorization» με τα διαπιστευτήρια τα οποία δημιούργησε βασισμένος στα δεδομένα που του έστειλε ο πληρεξούσιος εξυπηρέτης μέσω του μηνύματος απόκρισης. Το νέο αυτό αίτημα προωθείται στον εξυπηρέτη για την επιβεβαίωση της γνησιότητας / ορθότητας του.
4. Ο πληρεξούσιος εξυπηρέτης, με τη σειρά του, υπολογίζει τα διαπιστευτήρια και εφόσον ταιριάζουν με αυτά που συμπεριλαμβάνει ο χρήστης στην κεφαλίδα «authorization» αποστέλλει ένα μήνυμα επιτυχίας «200 OK».

Η αξιοποίηση του προαναφερόμενου μηχανισμού μπορεί να γίνει για οποιοδήποτε SIP αίτημα, εκτός του SIP CANCEL και SIP ACK όπου, όπως ορίζεται στις προδιαγραφές του SIP, απαιτείται εξειδικευμένος τρόπος διαχείρισης. Παράδειγμα της εφαρμογής της διαδικασίας αυθεντικοποίησης HTTP Digest στο SIP υπάρχει στο Σχήμα 3–8. Περισσότερες λεπτομέρειες για τον μηχανισμό HTTP digest και τον υπολογισμό των διαπιστευτηρίων μπορούν να βρεθούν στο [85].

5.3.2 Ασφαλές IP

Το πρωτόκολλο IP αποτελεί τη βασική δικτυακή υποδομή για οποιαδήποτε επικοινωνία πραγματοποιείται στο διαδίκτύο. Διάφορες έρευνες αναφέρουν ότι το IP πρωτόκολλο είναι ευπαθές σε επιθέσεις όπως απόκρυψη ταυτότητας (Spoofing), υποκλοπή συνόδου (Session Hijacking), ανάλυση κίνησης (traffic analysis) και πολλές άλλες [79]. Για την αντιμετώπιση των προβλημάτων αυτών αλλά και για την παροχή επιπρόσθετων υπηρεσιών ασφάλειας (στο επίπεδο IP), όπως υπηρεσίες εμπιστευτικότητας, γνησιότητας προέλευσης δεοδομένων (data origin authentication) και ακεραιότητας, αναπτύχθηκε το ασφαλές πρωτόκολλο (IP Security–(IPsec)) [89]. Οι υπηρεσίες αυτές προσφέρονται με την αξιοποίηση των μηχανισμών *Encapsulating Security Payload (ESP)* και *Authentication Header (AH)*.

Η εισαγωγή του IPSec στην αρχιτεκτονική του SIP προστατεύει, μέσω ασφαλών διόδων, τη μετάδοση τόσο της σηματοδοσίας, όσο και δεδομένων που προέρχονται από διαφορετικούς τομείς (domains). Πριν την επικοινωνία έχουν δημιουργηθεί δεσμοί αμοιβαίας εμπιστοσύνης για το διαμοιρασμό των απαιτούμενων κλειδιών, πιστοποιητικών κτλ. Ίσως το πιο χαρακτηριστικό παράδειγμα εφαρμογής του IPSec σε συστήματα σηματοδοσίας είναι η χρήση του στο UMTS έκδοση 5, για την προστασία της SIP σηματοδοσίας μεταξύ της συσκευής χρήστη και του αντίστοιχου εξυπηρέτη.

5.3.3 Πρωτόκολλο Ασφαλούς Μεταφοράς

Ένας εναλλακτικός μηχανισμός για την προστασία των μεταδιδόμενων μηνυμάτων αποτελεί η χρήση του Πρωτοκόλλου Ασφαλούς Μεταφοράς (Transport Layer Security–(TLS)) [90]. Αντίστοιχα με το IPSec, το TLS παρέχει υπηρεσίες αυθεντικοποίησης (πελάτη και εξυπηρέτη), ακεραιότητας και εμπιστευτικότητας μεταξύ των δικτυακών οντοτήτων του SIP, χωρίς όμως να προ-απαιτούνται δεσμοί αμοιβαίας εμπιστοσύνης μεταξύ των επικοινωνούντων οντοτήτων.

Επίσης, στα πλαίσια του SIP, το TLS χρησιμοποιείται για την υποστήριξη του "*Ασφαλούς SIP* (*SIP Secure*– (SIPS))" που ουσιαστικά διασφαλίζει την εφαρμογή του TLS από άκρο σε άκρο (end-to-end) του μονοπατιού σηματοδοσίας.

5.3.4 Secure Multipurpose Internet Mail Extension

Το Ασφαλές MIME (Secure MIME–(S/MIME)) [91] θεωρείται ένας από τους πιο ολοκληρωμένους μηχανισμούς ασφαλείας για χρήση στο επίπεδο εφαρμογής της διαδικτυακής αρχιτεκτονικής, υποστηρίζοντας υπηρεσίες ασφάλειας για αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα και μη αποποίησης αποστολέα, κάνοντας χρήση των κατάλληλων υποδομών δημοσίου κλειδιού.

Σύμφωνα με τις προδιαγραφές του SIP μπορούν να δημιουργηθούν μηνύματα τα οποία στο κύριο μέρος να συμπεριλαμβάνουν επιπρόσθετα MIME μηνύματα τα οποία μεταξύ των άλλων δύναται να χρησιμοποιούνται για την προστασία των μηνυμάτων SIP. Αυτό σημαίνει ότι το τμήμα του μηνύματος το οποίο πρέπει να είναι προστατευμένο επισυνάπτεται στο MIME τμήμα του μηνύματος που ενσωματώνεται στο κύριο μέρος του SIP μηνύματος, στο οποίο και εφαρμόζονται οι υπηρεσίες ασφάλειας που επιθυμεί ο χρήστης.

Το S/MIME στην αρχιτεκτονική του SIP μπορεί να αξιοποιηθεί είτε ως Δίοδος Ακεραιότητας και αυθεντικοποίησης (Tunneling Integrity and Authentication) είτε ως Δίοδος Κρυπτογράφησης.

5.3.4.1 Δίοδος Ακεραιότητας και Αυθεντικοποίησης

Στις περιπτώσεις όπου ο αποστολέας ενός μηνύματος επιθυμεί τη διασφάλιση της ακεραιότητας του, το SIP μήνυμα (ολόκληρο ή τμήματα αυτού) ενσωματώνεται στο MIME τμήμα του SIP μηνύματος το οποίο ο αποστολέας υπογράφει ψηφιακά κάνοντας χρήση του ιδιωτικού κλειδιού του. Η ψηφιακή υπογραφή επισυνάπτεται στο κύριο μέρος του μηνύματος μαζί με το MIME τμήμα.

5.3.4.2 Δίοδος Κρυπτογράφησης

Στις περιπτώσεις όπου ο χρήστης επιθυμεί τη διασφάλιση της εμπιστευτικότητας των SIP μηνυμάτων που έχει δημιουργήσει, συμπεριλαμβάνει στο κύριο μέρος MIME του μηνύματος τα τμήματα εκείνα που χρήζουν προστασίας. Τα συγκεκριμένα δεδομένα δεν παρουσιάζονται στις κεφαλίδες του μηνύματος, ενώ ακόμα και στην περίπτωση που η εμφάνιση τους είναι υποχρεωτική εμφανίζονται ανωνυμοποιημένα, όπως για παράδειγμα η ακόλουθη κεφαλίδα «From:anonymoys@sip.gr». Το Σχήμα 5–2, αποτυπώνει ένα μήνυμα SIP στο οποίο εφαρμόζεται η δίοδος κρυπτογράφησης, όπου το τμήμα του μηνύματος που βρίσκεται στην περιοχή με τα αστεράκια είναι κρυπτογραφημένο.

```
REGISTER sip:dgentele.com SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: <sip:3400001586@dgentele.com;user=phone>;tag=3199572059
To: <sip:3400001586@dgentele.com;user=phone>
Call-ID: 3021094946@81.0.7.124
CSeq: 2 REGISTER
Contact: <sip:3400001586@81.0.7.124:5070;user=phone;transport=udp>;expires=300
User-Agent: Cisco ATA 186  v3.1.0 atasip (040211A)
Authorization: Digest username="3400001586"  realm="dgentele.com",
                        nonce="426302039afdf717c6687e28f6c7d39c4fdb9f08",
                        uri="sip:voztele.com",response="af0d725596c8f06f370f8c80ade67b05"
Content-type: application/pkcs7-mime;s-mime-type=envelope-data
Content-Length: 500
**********************************Κρυπτογραφημένο Τμήμα ***************************************
REGISTER sip:dgentele.com SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: <sip:3400001586@dgentele.com;user=phone>;tag=3199572059
To: <sip:3400001586@dgentele.com;user=phone>
Call-ID: 3021094946@81.0.7.124
CSeq: 2 REGISTER
Contact: <sip:3400001586@81.0.7.124:5070;user=phone;transport=udp>;expires=300
User-Agent: Cisco ATA 186  v3.1.0 atasip (040211A)
Authorization: Digest username="3400001586"  realm="dgentele.com",
                        nonce="426302039afdf717c6687e28f6c7d39c4fdb9f08",
                        uri="sip:voztele.com",response="af0d725596c8f06f370f8c80ade67b05"
*************************************************************************************************************
```

Σχήμα 5–2. Παράδειγμα SIP μηνύματος με Κρυπτογραφημένο το Κύριος Μέρος του

5.4 Ανάλυση Υπαρχόντων Μηχανισμών Ασφαλείας στο SIP

Ο μηχανισμός αυθεντικοποίησης HTTP digest παρέχει μονοκατευθυντική γνησιότητα μηνυμάτων πελάτη (one-way message authentication) και προστασία από επιθέσεις επανεκπομπής, από κόμβο σε κόμβο. Να τονιστεί ότι δεν παρέχει αυθεντικοποίηση του χρήστη, καθώς δεν λαμβάνονται υπόψη τα δεδομένα που υπάρχουν στην κεφαλίδα «From» που ουσιαστικά αντιστοιχούν στην ταυτότητα του. Επίσης δεν προσφέρει υπηρεσίες ακεραιότητας για προστασία από μη εξουσιοδοτημένη τροποποίηση των μηνυμάτων και επιθέσεις τύπου ενδιάμεσου, ενώ δεν καλύπτει περιπτώσεις επανάληψης υποβολής μηνυμάτων όπως το SIP CANCEL, δημιουργώντας έτσι ευκαιρίες για επιθέσεις σηματοδοσίας.

Πέρα όμως από τα προαναφερόμενα το HTTP digest είναι ευπαθές σε επιθέσεις τύπου αποκρυπτογράφησης με γνωστό κείμενο (known plaintext attacks) [51], εξαιτίας του γεγονότος ότι τόσο τα δεδομένα που χρησιμοποιούνται για τον υπολογισμό των διαπιστευτηρίων, όσο και τα ίδια τα διαπιστευτήρια μπορεί να υποκλαπούν από ένα επιτιθέμενο, καθώς μεταδίδονται με την υποβολή του νέου αυθεντικοποιημένου μηνύματος. Αποτέλεσμα μιας τέτοιας επίθεσης είναι η πιθανή αποκάλυψη του συνθηματικού που χρησιμοποιεί ένας εξουσιοδοτημένος χρήστης, με όποιες άμεσες ή έμμεσες συνέπειες προκύπτουν. Επιπροσθέτως για την ορθή λειτουργία-εφαρμογή του HTTP digest απαιτείται η αμοιβαία εμπιστοσύνη μεταξύ υπηρεσίας και πελάτη για το διαμοιρασμό των συνθηματικών αλλά και για την αποθήκευση-διατήρηση τους από την υπηρεσία. Η αποθήκευση αυτή μπορεί να είναι είτε σε μορφή κειμένου (μη κρυπτογραφημένη) είτε σε κρυπτογραφημένη μορφή που όμως δεν προσφέρει κανένα επιπρόσθετο επίπεδο ασφάλειας λόγω του τρόπου υπολογισμού των διαπιστευτηρίων.

Το IPSec παρέχει υπηρεσίες ακεραιότητας, εμπιστευτικότητας και αυθεντικότητας δεδομένων, από κόμβο σε κόμβο, χωρίς να παρουσιάζει τα μειονεκτήματα του HTTP Digest. Παρ' όλα αυτά, όπως και το HTTP Digest, απαιτεί την ύπαρξη προ-εγκατεστημένων δεσμών αμοιβαίας εμπιστοσύνης μεταξύ των επικοινωνούντων μερών. Ο βασικός περιορισμός του συγκεκριμένου μηχανισμού εντοπίζεται στο γεγονός ότι υλοποιείται ως μέρος του λειτουργικού συστήματος με αποτέλεσμα οι τερματικές συσκευές των χρηστών να μην το υποστηρίζουν, ενώ υπάρχει έλλειψη περιγραφής του πλαισίου διαχείρισης κλειδιών που απαιτούνται για την ορθή εφαρμογή του IPSec στην αρχιτεκτονική του SIP.

Από την άλλη πλευρά, ο μηχανισμός TLS δεν απαιτεί κανένα είδος προ-εγκατεστημένου δεσμού εμπιστοσύνης (prearrange trust) μεταξύ των οντοτήτων που επικοινωνούν για την παροχή υπηρεσιών ακεραιότητας, εμπιστευτικότητας και αυθεντικότητας από κόμβο σε κόμβο, και υπό προϋποθέσεις από άκρο σε άκρο (SIP Secure – (SIPS)) [11]. Εξαιτίας, όμως της έλλειψης του κατάλληλου πλαισίου διασφάλισης της εφαρμογής του TLS κατά μήκος όλου του μονοπατιού σηματοδοσίας (signalling path) δεν έχει εφαρμοσθεί μέχρι τώρα. Επιπροσθέτως, το γεγονός ότι δεν υποστηρίζει ασυνδεσμικά πρωτόκολλα όπως το UDP, στο οποίο βασίζεται κατά κύριο λόγο η μεταφορά δεδομένων στη διαδικτυακή τηλεφωνία, έχει ως αποτέλεσμα να μη μπορεί να θεωρηθεί ως ιδιαίτερα αποδοτικός και επιτυχημένος μηχανισμός ασφαλείας για τη διαδικτυακή τηλεφωνία. Τέλος οι συνδέσεις που δημιουργεί προκαλούν αυξημένο υπολογιστικό φόρτο καθώς και επιπρόσθετη καθυστέρηση στην επεξεργασία των δεδομένων σηματοδοσίας [92].

Ένας ακόμα περιορισμός για την ορθή εφαρμογή του TLS στην αρχιτεκτονική της διαδικτυακής τηλεφωνίας αποτελεί η έλλειψη ενιαίας υποδομής δημοσίου κλειδιού. Αξίζει να σημειωθεί ότι μέχρι πρότινος ελάχιστες τερματικές συσκευές υποστήριζαν το TLS, οι πιο γνωστές από τις οποίες είναι το KPhone (www.kphone.org), το Minisip(*www.minisip.org*), και το Snom (*www.snom.com*).

Αν και ο μοναδικός μηχανισμός για προστασία εμπιστευτικότητας και ακεραιότητας που μπορεί να εφαρμοσθεί από άκρο σε άκρο παρέχεται από το S/MIME, η αξιοποίηση του σε όλα τα δεδομένα ενός SIP μηνύματος θεωρείται σχεδόν ανέφικτη. Αυτό οφείλεται στο γεγονός ότι για τη σωστή διαχείριση των εισερχόμενων μηνυμάτων όλοι οι ενδιάμεσοι πληρεξούσιοι εξυπηρέτες απαιτούν πρόσβαση, με δικαιώματα τροποποίησης, σε συγκεκριμένες κεφαλίδες. Συνεπώς, όσες κεφαλίδες μπορεί να τροποποιηθούν δεν μπορούν / πρέπει να καλύπτονται από τις υπηρεσίες ακεραιότητας. Αντίστοιχα, όσες κεφαλίδες εξυπηρετούν τη δρομολόγηση του μηνύματος δεν μπορούν να καλύπτονται από τις υπηρεσίες εμπιστευτικότητας. Ο Πίνακας 5–1 αποτυπώνει συνοπτικά τον τύπο πρόσβασης στις διαφορετικές κεφαλίδες που απαιτείται για την ορθή δρομολόγηση ενός SIP μηνύματος.

Κεφαλίδα	**Request URI**	**From**	**To**	**Via**	**Record Route**	**Record**	**Call Id**	**Cseq**
Τύπος Πρόσβασης (T)ροποποίηση (A)νάγνωση	(T)	(A)	(A)	(T)	(T)	(T)	(A)	(A)

Πίνακας 5–1. Επιτρεπόμενοι Τύποι Πρόσβασης στις Κεφαλίδες ενός SIP Μηνύματος από Πληρεξούσιους Εξυπηρέτες

Επιπλέον, βασικό μειονέκτημα, όπως και στην περίπτωση του TLS, είναι η έλλειψη ενιαίας υποδομής δημοσίου κλειδιού, το επιπρόσθετο υπολογιστικό κόστος που δημιουργείται από τη χρήση της κρυπτογραφίας δημόσιου κλειδιού και η δικτυακή επιβάρυνση που οφείλεται στη ενσωμάτωση των MIME μηνυμάτων στο κύριο μέρος των SIP μηνυμάτων. Τέλος πρέπει να

τονιστεί ότι μέχρι σήμερα δεν υπάρχει SIP τερματική συσκευή που να υποστηρίζει το συγκεκριμένο μηχανισμό.

5.5 Ασφάλεια Πολυμέσων

Το πρώτο επίπεδο παροχής υπηρεσιών ασφαλείας στα συστήματα διαδικτυακής τηλεφωνίας εφαρμόζεται στα δεδομένα σηματοδοσίας, καθώς μέσω αυτών πραγματοποιείται η αποκατάσταση του καναλιού και της κλήσης για τη μετέπειτα μετάδοση των πολυμεσικών δεδομένων. Το δεύτερο επίπεδο παροχής υπηρεσιών ασφάλειας αφορά την προστασία των πολυμεσικών δεδομένων. Όμως, ο μηχανισμός RTP για τη μετάδοση πολυμεσικών δεδομένων δεν υποστηρίζει υπηρεσίες ασφαλείας. Για το λόγο αυτό αρχικά προτάθηκε, όπως και στο SIP, η εφαρμογή μηχανισμών που έχουν αξιοποιηθεί με επιτυχία στο διαδίκτυο, όπως το IPSec, TLS κτλ. Εξαιτίας όμως των κρυπτογραφικών λειτουργιών που εκτελούν και των επιπρόσθετων κεφαλίδων που ενσωματώνουν στα μεταδιδόμενα μηνύματα, προκαλούν μη αποδεκτές καθυστερήσεις για την παράδοση από άκρο σε άκρο, με αποτέλεσμα η επικοινωνία να εμφανίζει προβλήματα [93],[94].

Με στόχο την αντιμετώπιση των προβλημάτων αυτών σχεδιάστηκε και αναπτύχθηκε το Ασφαλές (Secure) RTP (SRTP) [95], το οποίο ουσιαστικά αποτελεί μια επέκταση του RTP για την παροχή υπηρεσιών εμπιστευτικότητας, αυθεντικότητας και ακεραιότητας χωρίς να εισάγει σημαντικό επιπρόσθετο φόρτο [93],[94] συγκρινόμενο με το IPSec και το TLS . Για την υποστήριξη των υπηρεσιών αυτών το SRTP αξιοποιεί τεχνικές συμμετρικής κρυπτογραφίας αν και δεν παρέχει κανένα μηχανισμό για τη διαχείριση και δημιουργία των κλειδιών που θα χρησιμοποιηθούν. Αντιθέτως αξιοποιούνται «εξωτερικοί» μηχανισμοί διαχείρισης-δημιουργίας κλειδιών όπως είναι το πρωτόκολλο Multimedia Internet Keying (MIKEY) [96].

Πρέπει να επισημανθεί για μια ακόμα φορά ότι οι προαναφερόμενες υπηρεσίες ασφαλείας θεωρούνται απόλυτα αναγκαίες στις υπηρεσίες διαδικτυακής τηλεφωνίας καθώς η πιθανότητα υποκλοπής κλήσεων στη διαδικτυακή τηλεφωνία είναι σημαντικά μεγαλύτερη και ευκολότερη από αυτή στο PSTN. Η χρήση του SRTP είναι δυνατόν να προσφέρει ικανοποιητικό επίπεδο προστασίας στα πολυμεσικά δεδομένα.

5.6 Συμπεράσματα

Για την παροχή ασφαλών υπηρεσιών διαδικτυακής τηλεφωνίας θα πρέπει να ικανοποιούνται οι βασικές απαιτήσεις ασφάλειας τόσο για τα δεδομένα σηματοδοσίας όσο και για τα δεδομένα φωνής.

Αναφορικά με την προστασία των δεδομένων σηματοδοσίας, τα οποία και προηγούνται των δεδομένων φωνής, οι μηχανισμοί ασφαλείας που προτείνονται στις προδιαγραφές του SIP (βλέπε Πίνακας 5–2) κρίνονται ανεπαρκείς για την κάλυψη των απαιτήσεων ασφαλείας τόσο από άκρο σε άκρο, όσο και από κόμβο σε κόμβο. Βεβαίως, το κύριο μειονέκτημα είναι η αδυναμία προστασίας των δεδομένων από άκρο σε άκρο, καθώς και η έλλειψη μηχανισμών εξασφάλισης διαθεσιμότητας.

	HTTP Digest	**IPSec**	**TLS**	**S/MIME**
Εμπιστευτικότητα	Όχι	Από κόμβο σε κόμβο	Από κόμβο σε κόμβο	Από άκρο σε άκρο (μερικώς)
Ακεραιότητα	Όχι	Από κόμβο σε κόμβο	Από κόμβο σε κόμβο	Από άκρο σε άκρο (μερικώς)
Αυθεντικότητα	Μονοκατευθυντική	Από κόμβο σε κόμβο	Από κόμβο σε κόμβο	Από άκρο σε άκρο
Διαθεσιμότητα	Όχι	Όχι	Όχι	Όχι

Πίνακας 5–2. Υποστηριζόμενες Υπηρεσίες Ασφάλειας από τους Μηχανισμούς Ασφάλειας που Προτείνονται στο SIP

Η απουσία ενός ολοκληρωμένου πλαισίου παροχής υπηρεσιών ασφάλειας για τη διαδικτυακή τηλεφωνία έχει σαν αποτέλεσμα την αδυναμία προστασίας από όλες τις πιθανές επιθέσεις που μπορεί να εκδηλωθούν εναντίον της υπηρεσίας.

	HTTP Digest	**IPSec**	**TLS**	**S/MIME**
Υποκλοπές	Όχι	Ναι	Ναι	Ναι
Επιθέσεις Σηματοδοσίας	Όχι	Όχι	Όχι	Όχι
Επιθέσεις προς τους αναλυτές μηνυμάτων	Όχι	Όχι	Όχι	Όχι
Επιθέσεις έγχυσης κώδικα	Όχι	Όχι	Όχι	Όχι
Επιθέσεις Πλημμύρας	Όχι	Όχι	Όχι	Όχι
Επιθέσεις επαναλήψεων	Ναι	Ναι	Ναι	Όχι

Πίνακας 5–3. Δυνατότητα Αντιμετώπισης Επιθέσεων από των Μηχανισμών Ασφάλειας που Προτείνονται στο SIP

Είναι σημαντικό να τονίσουμε ότι παρόλα τα προβλήματα και τους περιορισμούς που μπορεί να παρουσιάζουν οι προτεινόμενοι, από τις προδιαγραφές του SIP, μηχανισμοί ασφάλειας, η εφαρμογή τους θα πρέπει να είναι υποχρεωτική. Στην περίπτωση που οι συγκεκριμένοι μηχανισμοί ασφαλείας δεν είναι επαρκείς για να εξασφαλίσουν το επιθυμητό επίπεδο που επιθυμεί κάθε τηλεπικοινωνιακός οργανισμός, θα πρέπει να αναζητούνται νέες λύσεις που θα ενδυναμώνουν την ασφάλεια των παρεχόμενων υπηρεσιών «δρώντας» συμπληρωματικά των υπαρχόντων. Ίσως το πιο χαρακτηριστικό παράδειγμα αυτής της αναγκαιότητας είναι η αναφορά που γίνεται στις προδιαγραφές του SIP: *«Protective measure above and beyond those provided services by HTTP Digest need to be taken to prevent active attackers from modifying SIP requests and responses»*

Για τα δεδομένα φωνής οι μηχανισμοί ασφαλείας που υποστηρίζει το SRTP επιτυγχάνουν ένα ικανοποιητικό επίπεδο προστασίας, ειδικά στη διασφάλιση της εμπιστευτικότητας των κλήσεων που είναι και το κύριο ζητούμενο από τους χρήστες.

ΚΕΦΑΛΑΙΟ 6: Δημοσιευμένο Έργο Σχετικό με την Προστασία Συστημάτων Διαδικτυακής Τηλεφωνίας

6.1 Γενικά

Τα τελευταία χρόνια τα θέματα ασφαλείας των υπηρεσιών διαδικτυακής τηλεφωνίας προσελκύουν όλο και περισσότερο το επιστημονικό ενδιαφέρον, λόγω του ότι:

1. Η διαδικτυακή τηλεφωνία αναμένεται να αντικαταστήσει την υπηρεσία τηλεφωνίας που σήμερα προσφέρεται μέσω του PSTN.
2. Οι χρήστες επιθυμούν υπηρεσίες τηλεφωνίας με επίπεδα ασφαλείας και αξιοπιστίας αντίστοιχα με αυτά των υπηρεσιών που προσφέρονται από το PSTN.

Αρκετοί εναλλακτικοί μηχανισμοί ασφαλείας έχουν προταθεί για την προστασία των υπηρεσιών διαδικτυακής τηλεφωνίας και συγκεκριμένα για την κάλυψη των κενών ασφαλείας που έχουν εντοπιστεί στους μηχανισμούς ασφάλειας που προτείνονται στις προδιαγραφές του SIP. Στόχος είναι η προστασία από τις επιθέσεις που μπορεί να εκδηλωθούν προς μια υπηρεσία διαδικτυακής τηλεφωνίας (όπως παρουσιάζει συνοπτικά ο Πίνακας 5–3). Ο Πίνακας 6–1 αποτυπώνει τους προτεινόμενους στη βιβλιογραφία εναλλακτικούς μηχανισμούς, οι οποίοι παρουσιάζονται στη συνέχεια του παρόντος κεφαλαίου.

6.2 Προστασία από Επιθέσεις Υποκλοπών

Δεν υπάρχουν συγκεκριμένοι επιπρόσθετοι μηχανισμοί που να έχουν προταθεί για την προστασία από επιθέσεις υποκλοπών. Αυτό συμβαίνει κυρίως λόγω του ότι η ορθή εφαρμογή των υπαρχόντων μηχανισμών ασφάλειας επιτυγχάνει ένα ικανοποιητικό επίπεδο εμπιστευτικότητας. Με στόχο, λοιπόν, την ορθή εφαρμογή των υπαρχόντων μηχανισμών ασφαλείας προσδιορίστηκαν οι απαιτήσεις που πρέπει να ικανοποιούνται σε κάθε περίπτωση [97], όπως περιγράφονται στη συνέχεια:

- *Απαίτηση-Εμπιστευτικότητας 1*: Οι υιοθετούμενοι μηχανισμοί εμπιστευτικότητας πρέπει να επιτρέπουν την αποκάλυψη δεδομένων σηματοδοσίας (απαραίτητων) σηματοδοσίας σε όλες τις ενδιάμεσες οντότητες οποτεδήποτε ο αποστολέας το επιθυμεί.
- *Απαίτηση-Εμπιστευτικότητας 2*: Στις περιπτώσεις που δεν απαιτείται πρόσβαση στα δεδομένα σηματοδοσίας από τις ενδιάμεσες οντότητες, δεν θα πρέπει να είναι δυνατή η παραβίαση της εμπιστευτικότητας των δεδομένων.
- *Απαίτηση-Εμπιστευτικότητας 3*: Συνίσταται ο αποστολέας να δύναται να εκχωρήσει σε όλες ή σε ορισμένες ενδιάμεσες οντότητες δικαίωμα ανάγνωσης συγκεκριμένων δεδομένων σηματοδοσίας, όπως για παράδειγμα το κύριο μέρος του μηνύματος, όποτε αυτό απαιτείται για την ορθή δρομολόγηση και επεξεργασία του αιτήματος.
- *Απαίτηση-Εμπιστευτικότητας 4*: Θα πρέπει ο παραλήπτης ενός μηνύματος να έχει τη δυνατότητα αποκάλυψης εμπιστευτικών δεδομένων σηματοδοσίας σε ενδιάμεσες οντότητες που επεξεργάστηκαν το συγκεκριμένο μήνυμα, εφόσον βέβαια του έχει εκχωρηθεί το δικαίωμα αυτό από τον αποστολέα.

Να σημειωθεί ότι οι προαναφερόμενες απαιτήσεις εμπιστευτικότητας προκύπτουν στο σύνολο τους και από τον ορισμό της εμπιστευτικότητας που έχει δοθεί στην ενότητα 5.2.

		Προστασία από Επιθέσεις				
		Υποκλοπών	Σηματοδοσίας	Συντακτικών Αναλυτών	Έγχυσης κώδικα	Πλημμύρας
Εναλλακτικές Λύσεις	[97]	√	X	X	X	X
	[98]	X	√	X	X	X
	[99]	X	√	X	X	X
	[100]	X	√	X	X	X
	[101]	X	√	X	X	√
	[86]	X	X	X	X	√
	[102]	X	X	X	X	√
	[103]	X	X	X	X	√
	[104]	X	X	X	X	√
	[105]	X	√	X	X	√
	[106]	X	X	X	X	√
	[107]	X	√	X	X	X
	[108]	X	√	X	X	X
	[109]	X	√	X	X	X
	[110]	X	√	X	X	X
	[111]	X	√	X	X	X
	[112]	X	X	√	X	√
	[113]	X	√	X	X	√

Πίνακας 6–1. Προστασία από Επιθέσεις μέσω Εναλλακτικών Μηχανισμών Ασφαλείας που έχουν Προταθεί

6.3 Προστασία από Επιθέσεις Σηματοδοσίας & Ενδιάμεσου

Η προστασία από τις επιθέσεις σηματοδοσίας που εκδηλώνονται στη διαδικτυακή τηλεφωνία θεωρείται από τους τηλεπικοινωνιακούς πάροχους περισσότερο από επιτακτική, καθώς επηρεάζει την αξιοπιστία και τη διαθεσιμότητα των συνόδων που αποκαθίστανται μεταξύ δύο ή περισσότερων οντοτήτων. Οι επιθέσεις αυτές δεν οφείλονται αποκλειστικά και μόνο στην έλλειψη υπηρεσιών διασφάλισης της ακεραιότητας των δεδομένων σηματοδοσίας, αλλά και στη μη εφαρμογή των κατάλληλων μηχανισμών αυθεντικοποίησης. Διαφορετικές λύσεις έχουν προταθεί από την επιστημονική κοινότητα για τη διασφάλιση των δεδομένων σηματοδοσίας ([98]–[100], [101], [105], [107], [108], [110], [111], [113]). Σε όλες τις περιπτώσεις ο στόχος είναι η ελαχιστοποίηση της εμφάνισης επιθέσεων, είτε προσδιορίζοντας νέα σχήματα αυθεντικοποίησης είτε αναπτύσσοντας μηχανισμούς αναγνώρισης επιθέσεων σηματοδοσίας.

6.3.1 Μηχανισμοί Αναγνώρισης Επιθέσεων Σηματοδοσίας

Ξεκινώντας από την κατηγορία των μηχανισμών αναγνώρισης επιθέσεων σηματοδοσίας, στην εργασία [100] προτείνεται ο βασικός μηχανισμός αναγνώρισης (detection mechanism) για ο οποίος στηρίζεται στην αρχιτεκτονική συσχετισμού πρωτοκόλλων (cross protocol). Πιο συγκεκριμένα, ο προαναφερόμενος μηχανισμός αναγνώρισης αντιμετωπίζει επιθέσεις σηματοδοσίας στις οποίες γίνεται χρήση του μηνύματος τερματισμού SIP BYE. Η συγκεκριμένη επίθεση έχει πραγματοποιηθεί όταν μηνύματα RTP συνεχίζουν να μεταδίδονται και μετά την αποστολή του μηνύματος τερματισμού SIP BYE. Βασικό μειονέκτημα του προτεινόμενου μηχανισμού είναι ότι δε μπορεί να αξιοποιηθεί για την αναγνώριση επιθέσεων σηματοδοσίας που επιφέρουν τον τερματισμό συνόδων. Επιπλέον, ένας επιτιθέμενος μπορεί να μεταδώσει πλαστά (spoof) RTP μηνύματα, προκαλώντας έτσι λανθασμένους θετικούς συναγερμούς (false positive alarms) ή ακόμα, για να εμποδίσει την αναγνώριση της επίθεσης, μπορεί να θέσει εκτός λειτουργίας μία από τις οντότητες που συμμετέχουν στην επικοινωνία με σκοπό να αποστείλει ένα πλαστό μήνυμα SIP BYE για λογαριασμό της εξουσιοδοτημένης οντότητας. Στην περίπτωση αυτή η σύνοδος θα τερματιστεί επιτυχώς χωρίς να είναι δυνατή η αναγνώριση της επίθεσης. Παρ' όλα τα μειονεκτήματα του συγκεκριμένου μηχανισμού αναγνώρισης επιθέσεων σηματοδοσίας, αντίστοιχες λύσεις με χρήση διαφορετικών μοντέλων παρουσιάζονται στις εργασίες [101], [105] και [113].

Αναλυτικότερα, στην εργασία [113] προτείνεται η αναγνώριση επιθέσεων σηματοδοσίας που κάνουν χρήση του μηνύματος SIP BYE να γίνεται με την αντιστοίχηση γεγονότων. Αρχικά γίνεται συσχετισμός ενός εισερχόμενου μηνύματος SIP BYE με την κατάλληλη σύνοδο (session dialog). Σε περίπτωση επιτυχούς αντιστοίχησης ελέγχεται, για κάποιο προκαθορισμένο χρονικό διάστημα, η ύπαρξη νέων εισερχόμενων μηνυμάτων RTP που αντιστοιχούν στην προηγούμενη σύνοδο. Εφόσον ο έλεγχος είναι θετικός σημαίνει ότι έχει εκδηλωθεί επίθεση σηματοδοσίας SIP BYE.

Παρόμοια είναι και η λύση που παρουσιάζεται στην εργασία [105] που όμως βασίζεται στην αξιοποίηση δύο μηχανών πεπερασμένης κατάστασης (finite state machine), συμβατές με τις προδιαγραφές του SIP και του RTP αντιστοίχως. Με την επιτυχή αποκατάσταση μιας συνόδου η Μηχανή Πεπερασμένης Κατάστασης (ΜΠΚ) που αποτυπώνει την κατάσταση της συνόδου, μεταβαίνει σε κατάσταση «αποκατάσταση κλήσης». Η ΜΠΚ που αποτυπώνει την κατάσταση των πολυμεσικών δεδομένων RTP, μεταβαίνει σε κατάσταση «λήψης». Με τη λήψη ενός μηνύματος τερματισμού SIP BYE, η ΜΠΚ της συνόδου μεταβαίνει σε κατάσταση «τερματισμού κλήσης» ενώ, ταυτόχρονα, με ένα μήνυμα συγχρονισμού ενημερώνει τη ΜΠΚ του RTP για τη λήψη μηνύματος τερματισμού SIP BYE. Σε συνέχεια του μηνύματος αυτού, η ΜΠΚ του RTP μεταβαίνει σε κατάσταση «λήψη RTP κατά τη διάρκεια τερματισμού της συνόδου» για ένα προκαθορισμένο χρονικό διάστημα *t* κατά το οποίο επιτρέπεται η λήψη μηνυμάτων RTP. Μετά το πέρας του χρονικού διαστήματος *t*, η λήψη μηνυμάτων RTP αποτελεί ένδειξη εκδήλωσης επίθεσης σηματοδοσίας SIP BYE.

Στην εργασία [101] προτείνεται η χρήση των χρωματιστών ιεραρχικών δικτύων Petri [114] (colored hierarchical Petri Net) για τη μοντελοποίηση της συμπεριφοράς ενός πράκτορα χρήστη συμβατού με τις προδιαγραφές του SIP, αντί της χρήσης μηχανών πεπερασμένων καταστάσεων που προτείνεται στην εργασία [105]. Το μοντέλο αυτό συνδυάζεται με μοντέλα ανίχνευσης μη ορθής χρήσης (misuse detection) και της αρχιτεκτονικής συσχετισμού πρωτοκόλλων για την αναγνώριση επιθέσεων σηματοδοσίας.

6.3.2 Εναλλακτικά Σχήματα Αυθεντικοποίησης

Ο αντίλογος στους προαναφερόμενους μηχανισμούς αναγνώρισης είναι ότι δεν προσφέρουν «προληπτική προστασία» από τις επιθέσεις σηματοδοσίας. Με τον όρο «προληπτική προστασία» νοείται η εξασφάλιση των προϋποθέσεων εκείνων που θα έχουν σαν αποτέλεσμα τη μη δυνατότητα εκτέλεσης επιθέσεων, δηλαδή την ανάπτυξη και εφαρμογή των απαραίτητων υπηρεσιών ακεραιότητας και αυθεντικότητας στα δεδομένων σηματοδοσίας. Υπό το πρίσμα αυτό, μια σειρά διαφορετικών λύσεων για τη διασφάλιση της γνησιότητας και αυθεντικότητας των μηνυμάτων (αιτήσεων και αποκρίσεων) προτείνεται στις εργασίες [98], [99], [107],[108], [110], [111].

Η λύση που περιγράφεται στην εργασία [98] εστιάζει στην προστασία των αποκρίσεων που δημιουργούνται στα πλαίσια μιας συνόδου. Η τεχνική αυτή είναι αποδοτική κυρίως στις περιπτώσεις όπου ένας πληρεξούσιος εξυπηρέτης πραγματοποιεί επιθέσεις ενδιάμεσου, δημιουργώντας πλαστές αποκρίσεις ώστε να ανακατευθύνει τη σύνοδο σε μη εξουσιοδοτημένους χρήστες ή να δημιουργήσει άρνηση παροχής υπηρεσίας. Παρά ταύτα, η προτεινόμενη μέθοδος δεν είναι δυνατόν να αξιοποιηθεί στην περίπτωση επιθέσεων σηματοδοσίας που εκδηλώνονται από τον καλούντα και που κάνουν χρήση μηνυμάτων SIP CANCEL, SIP BYE κτλ, καθώς δεν ελέγχεται η γνησιότητα της ταυτότητας του καλούντα. Το γεγονός αυτό παρέχει τη δυνατότητα σε ένα επιτιθέμενο να δημιουργήσει πλαστά μηνύματα SIP CANCEL, SIP BYE, κτλ εκδηλώνοντας επιθέσεις σηματοδοσίας και προκαλώντας άρνησης παροχής υπηρεσίας.

Μια εναλλακτική λύση η οποία στηρίζεται στην αμοιβαία αυθεντικοποίση εξυπηρέτη-πελάτη, τόσο για τα αιτήματα όσο και για τις αποκρίσεις, προτείνεται στην εργασία [99]. Ουσιαστικά αξιοποιείται μια παραλλαγή του σχήματος ανταλλαγής κλειδιών Diffe-Helman [115], αφού για τον υπολογισμό του κοινού αδειοπλαισίου αυθεντικοποίησης (authentication token) τόσο ο εξυπηρέτης όσο και ο πελάτης διαμοιράζονται ένα κοινό συνθηματικό το οποίο χρησιμοποιείται κατά τη διαδικασία ανταλλαγής κλειδιών για την αυθεντικοποίηση των δύο πλευρών. Ο μηχανισμός αυτός δεν είναι δυνατόν να εφαρμοστεί σε μηνύματα για τα οποία δεν επιτρέπεται η επανάληψη υποβολής (resubmission) των, όπως για παράδειγμα το μήνυμα SIP CANCEL. Επιπλέον, η μη παροχή υπηρεσιών ακεραιότητας προσφέρει στους επιτιθέμενους ευκαιρίες μη εξουσιοδοτημένης τροποποίησης των δεδομένων σηματοδοσίας. Για παράδειγμα, ένας επιτιθέμενος δύναται να τροποποιήσει τα δεδομένα εγγραφής, κατά την αποστολή ενός μηνύματος SIP REGISTER από κάποιο εξουσιοδοτημένο χρήστη, για να λαμβάνει τις κλήσεις για λογαριασμό του τελευταίου (για περισσότερες λεπτομέρειες βλέπε ενότητα 4.4). Βέβαια τα προαναφερόμενα μειονεκτήματα θα μπορούσαν να έχουν αποφευχθεί εάν ο προτεινόμενος μηχανισμός ελάμβανε υπόψη του τις ιδιαιτερότητες του SIP για την παροχή υπηρεσιών ασφαλείας (για περισσότερες βλέπε ενότητα 5.2).

Αντίστοιχος μηχανισμός παρουσιάζεται και στην εργασία [107]. Η κύρια διαφοροποίηση από τον προηγούμενο είναι ότι βασίζεται στη χρήση κρυπτογραφίας ελλειπτικών καμπυλών (elliptic curve cryptography). Επιπλέον στα πλεονεκτήματα του μηχανισμού αυτού συμπεριλαμβάνεται η υποστήριξη υπηρεσιών ακεραιότητας, επιτυγχάνοντας έτσι ένα ικανοποιητικό επίπεδο προστασίας από επιθέσεις σηματοδοσίας.

Μια εναλλακτική πρόταση για αμοιβαία αυθεντικοποίηση χρήστη-εξυπηρέτη, με τη χρήση προ-συμφωνημένων συμμετρικών κλειδιών, περιγράφεται στην εργασία [110]. Μεταξύ των μειονεκτημάτων της λύσης αυτής είναι ο διαμοιρασμός των συμμετρικών κλειδιών αλλά και η μη δυνατότητα εφαρμογής της, στις περιπτώσεις μηνυμάτων για τα οποία δεν επιτρέπεται η επανάληψη υποβολής τους. Μια άλλη λύση αμοιβαίας αυθεντικοποίησης χρήστη-εξυπηρέτη, η οποία βασίζεται σε ένα υβριδικό σχήμα υποδομής δημοσίου κλειδιού και συνθηματικών

μιας χρήσης (one-time passwords), προτείνεται στην εργασία [109]. Τα συνθηματικά μιας χρήσης δημιουργούνται από την υπηρεσία και αποστέλλονται στον χρήστη σε καθαρή μορφή, καθιστώντας τα έτσι όχι μόνο ευεπίφορα σε επιθέσεις υποκλοπής αλλά και πλαστοπροσωπίας του εξουσιοδοτημένου χρήστη. Αντίστοιχα, λόγω του τρόπου υπολογισμού του αδειοπλαισίου αυθεντικοποίησης για την επικύρωση γνησιότητας της ταυτότητας του εξυπηρέτη, είναι δυνατή η αποκάλυψη του συνθηματικού μιας χρήσης που αξιοποιείται από τον εξυπηρέτη, με αποτέλεσμα στη συνέχεια ο επιτιθέμενος να μπορεί να λειτουργήσει για λογαριασμό της υπηρεσίας πραγματοποιώντας κάποια επίθεση ενδιάμεσου.

Στην εργασία [108] αναλύεται ένας μηχανισμός για προστασία από επιθέσεις σηματοδοσίας που πραγματοποιούνται κατά τη διαδικασία εγγραφής. Ο μηχανισμός αυτός κάνει χρήση συνθηματικών μιας χρήσης τα οποία δημιουργούνται από το χρήστη και όχι από τον εξυπηρέτη. Ο εξυπηρέτης υπολογίζει τα διαπιστευτήρια για ένα μήνυμα που λαμβάνει κάνοντας χρήση των διαπιστευτηρίων που επισυνάπτονται στο ακριβώς προηγούμενο μήνυμα. Το βασικό μειονέκτημα της μεθόδου αυτής εντοπίζεται στον τρόπο παράδοσης των αρχικών διαπιστευτηρίων που θα αξιοποιηθούν για την αυθεντικοποίηση του πρώτου μηνύματος σηματοδοσίας. Ενώ η αποστολή των αρχικών διαπιστευτηρίων θα αναμενόταν να γίνεται μέσω ενός ασφαλούς καναλιού επικοινωνίας, στον προτεινόμενο μηχανισμό αποστέλλονται σε καθαρή μορφή με αποτέλεσμα ένας επιτιθέμενος να έχει τη δυνατότητα υποκλοπής των αρχικών διαπιστευτηρίων και συνεπώς να δύναται να λειτουργήσει για λογαριασμό του εξουσιοδοτημένου εξυπηρέτη.

Μια άκρως ενδιαφέρουσα προσέγγιση για την προστασία τόσο των δεδομένων σηματοδοσίας όσο και των δεδομένων φωνής πραγματεύεται η εργασία [111]. Συγκεκριμένα, προτείνεται η εφαρμογή ενός σχήματος υδατογραφίας στα δεδομένα φωνής για την παροχή υπηρεσιών αυθεντικοποίησης και ακεραιότητας. Ο μηχανισμός αυτός παρέχει προστασία από επιθέσεις σηματοδοσίας τύπου SIP BYE, αλλά δεν μπορεί να αντιμετωπίσει περιπτώσεις επιθέσεων σηματοδοσίας που εκδηλώνονται πριν την αποκατάσταση της συνόδου.

6.4 Προστασία από Επιθέσεις κατά των Αναλυτών Μηνυμάτων

Ελάχιστες είναι οι λύσεις που έχουν προταθεί για την προστασία των αναλυτών μηνυμάτων. Συγκεκριμένα, στην εργασία [112] αναφέρεται ότι μεταξύ των ελέγχων που πραγματοποιούνται για τον εντοπισμό πιθανών επιθέσεων εκτελείται και έλεγχος ορθότητας των SIP μηνυμάτων μέσω της βιβλιοθήκη oSIP [116]. Σύμφωνα με την τεκμηρίωση της συγκεκριμένης βιβλιοθήκης, τα εισερχόμενα μηνύματα που δεν είναι συμβατά με τις προδιαγραφές του SIP απορρίπτονται, χωρίς όμως να γίνεται περιγραφή της τεχνικής που αξιοποιείται για την πραγμάτωση των ελέγχων και την αποδοτικότητα αναγνώρισης μη συμβατών μηνυμάτων. Αξίζει πάντως να σημειωθεί, ότι για την προστασία από επιθέσεις μη συμβατών μηνυμάτων μπορούν να αξιοποιηθούν και οι μηχανισμοί των υπηρεσιών ακεραιότητας και αυθεντικότητας, «απωθώντας» με αυτό το τρόπο τους επιτιθέμενους να εκτελέσουν τέτοιου τύπου επιθέσεις. Σε καμία βέβαια περίπτωση από μόνες τους οι λύσεις αυτές δεν είναι δυνατόν να προσφέρουν ολοκληρωμένη προστασία από επιθέσεις μη συμβατών μηνυμάτων.

6.5 Προστασία από Επιθέσεις Πλημμύρας

Μια ακόμα κατηγορία επιθέσεων που πρέπει να ληφθεί πολύ σοβαρά υπόψη, κυρίως λόγω των προβλημάτων διαθεσιμότητας που μπορεί να προκαλέσουν, από τους παρόχους υπηρεσιών διαδικτυακής τηλεφωνίας, είναι οι επιθέσεις πλημμύρας. Για το λόγο αυτό η επιστημονική κοινότητα έχει επικεντρώσει το ενδιαφέρον της στην ανάπτυξη λύσεων και

αρχιτεκτονικών υψηλής διαθεσιμότητας για την προστασία των υπολογιστικών πόρων από επιθέσεις πλημμύρας, για υπηρεσίες οι οποίες βασίζονται στο πρωτόκολλο σηματοδοσίας SIP [86], [106], [112], [113]. Οι περισσότερες από τις λύσεις αυτές εστιάζουν στις περιπτώσεις πλημμύρας που προκαλούνται με τη χρήση μηνυμάτων SIP INVITE, καθώς το συγκεκριμένο μήνυμα θεωρείται ως ένα από τα πλέον αξιοποιούμενα μηνύματα στην αρχιτεκτονική του SIP το οποίο μάλιστα απαιτεί για τη διαχείριση του επιπρόσθετους υπολογιστικούς πόρους σε σχέση με τα υπόλοιπα SIP μηνύματα. Βέβαια δεν θα πρέπει σε καμία περίπτωση να θεωρηθεί ότι επιθέσεις πλημμύρας με τη χρήση μηνυμάτων άλλων, εκτός του SIP INVITE, δεν είναι πιθανές.

Αναλυτικότερα, στην εργασία [102] περιγράφεται ένας μηχανισμός ανίχνευσης επιθέσεων πλημμύρας, ο οποίος βασίζεται στη μέθοδο προοδευτικού αθροίσματος (cumulative sum) [117] των συνόδων που βρίσκονται σε εξέλιξη (δεν έχει πραγματοποιηθεί αποκατάσταση της σύνδεσης) για κάποιο προκαθορισμένο χρονικό διάστημα T, συσχετίζοντας τα SIP INVITE μηνύματα και τις αποκρίσεις «200 OK». Στην περίπτωση που το προοδευτικό άθροισμα υπερβεί ένα συγκεκριμένο επιτρεπτό όριο (threshold), στο προκαθορισμένο χρονικό διάστημα T, θεωρείται ότι έχει εκδηλωθεί επίθεση πλημμύρας. Μια αντίστοιχη αλλά βελτιωμένη λύση για την αναγνώριση επιθέσεων πλημμύρας προτείνεται στην εργασία [103]. Πιο συγκεκριμένα, στον υπολογισμό των συνόδων που βρίσκονται σε εξέλιξη συμπεριλαμβάνονται τόσο τα μηνύματα επιβεβαίωσης (SIP ACK) όσο και τα μηνύματα τερματισμού SIP BYE, εφαρμόζοντας σε αυτά την απόσταση Hellinger [118]. Όπως και στην προηγούμενη λύση, σε περίπτωση όπου η απόσταση Hellinger υπερβεί ένα προκαθορισμένο επιτρεπτό όριο, θεωρείται ότι έχει εκδηλωθεί επίθεση πλημμύρας.

Ένας εναλλακτικός μηχανισμός για την αναγνώριση επιθέσεων πλημμύρας μπορεί να επιτευχθεί με τη χρήση παγίδων ασφαλείας (honeypot) [119], όπως προτείνεται στην εργασία [113]. Όμοια με τους δύο προηγούμενους μηχανισμούς πραγματοποιείται υπολογισμός των συνόδων που βρίσκονται σε εξέλιξη, συσχετίζοντας τα μηνύματα SIP INVITE, τις αποκρίσεις «200 OK» και τα μηνύματα επιβεβαίωσης SIP ACK. Σε περίπτωση όπου ο αριθμός των συνόδων υπερβαίνει ένα συγκεκριμένο επιτρεπτό όριο, τότε δημιουργείται συναγερμός επίθεσης πλημμύρας.

Ομοίως, ο μηχανισμός που προτείνεται στην εργασία [112], μεταξύ των άλλων, πραγματοποιεί ελέγχους για τον εντοπισμό επιθέσεων πλημμύρας. Πιο συγκεκριμένα, καταγράφεται το πλήθος των SIP INVITE, SIP BYE και SIP ACK μηνυμάτων που λαμβάνονται και κατευθύνονται προς ένα συγκεκριμένο προορισμό. Ανά τακτά χρονικά διαστήματα ελέγχεται εάν το πλήθος των ληφθέντων αυτών μηνυμάτων βρίσκεται σε συμφωνία με τις προδιαγραφές του SIP και δεν υπερβαίνει τα προκαθορισμένα επιτρεπτά όρια, σε διαφορετική περίπτωση θεωρείται ότι έχει εκδηλωθεί επίθεση πλημμύρας.

Δύο διαφορετικές προσεγγίσεις, οι οποίες βασίζονται στην αξιοποίηση των μηχανών πεπερασμένης κατάστασης (ΜΠΚ) που δημιουργούνται στα πλαίσια διαχείρισης μιας νέας εισερχόμενης αίτησης --συμβατές με τις προδιαγραφές του SIP (βλέπε ενότητα 3.2.4)-- παρουσιάζονται στις εργασίες [104], [105]. Στην πρώτη [104] από τις δύο προσεγγίσεις, κατά τη λήψη ενός νέου εισερχόμενου μηνύματος, για παράδειγμα SIP INVITE, δημιουργείται μια απλοποιημένη ΜΠΚ απαριθμώντας όλα τα εισερχόμενα INVITE κατά τη διάρκεια ενός αυστηρά προσδιορισμένου χρονικού διαστήματος. Σε περίπτωση που το πλήθος των εισερχόμενων SIP INVITE μηνυμάτων, όπως και στις τεχνικές που παρουσιάστηκαν παραπάνω, υπερβεί ένα προκαθορισμένο όριο τιμών σηματοδοτεί επίθεση πλημμύρας. Βέβαια θα πρέπει επισημανθεί ότι στην περίπτωση που τα SIP INVITE μηνύματα αποσταλούν ταυτόχρονα προς διαφορετικούς χρήστες, με σκοπό την πρόκληση άρνησης παροχής υπηρεσίας σε κάποιο εξουσιοδοτημένο πληρεξούσιο, δεν θα ανιχνευθεί η

επίθεση αφού όλες οι μηχανές πεπερασμένης κατάστασης θα βρίσκονται κάτω από το όριο ένδειξης πλημμύρας. Αντίστοιχη είναι και η λύση που ακολουθείται στη δεύτερη προσέγγιση [105]. Η βασική διαφορά είναι ότι λαμβάνονται υπόψη και οι αποκρίσεις που αντιστοιχούν σε συγκεκριμένες συνόδους, ενώ για την αναγνώριση εκδήλωσης επιθέσεων πλημμύρας προσδιορίζονται διαφορετικά όρια τιμών για το επιτρεπόμενο, στη μονάδα του χρόνου, πλήθος συναλλαγών ανά πελάτη, σφαλμάτων ανά συναλλαγή καθώς και προκαθορισμένος ρυθμός μετάδοσης μηνυμάτων ανά συναλλαγή.

Ένας ελαφρά διαφοροποιημένος μηχανισμός για την αναγνώριση, μεταξύ άλλων, επιθέσεων πλημμύρας, περιγράφεται στην εργασία [101]. Ο μηχανισμός αυτός βασίζεται στα χρωματιστά δίκτυα Petri [114] για τη μοντελοποίηση της συμπεριφοράς ενός πράκτορα χρήστη συμβατού με τις προδιαγραφές του SIP, αντί της χρήσης μηχανών πεπερασμένων καταστάσεων. Πιο συγκεκριμένα, ελέγχεται τόσο το πλήθος των μηνυμάτων SIP INVITE που λαμβάνονται σε ένα συγκεκριμένο χρονικό διάστημα, όσο και η διαφορά των μηνυμάτων SIP INVITE κατά το χρονικό διάστημα μεταξύ της προηγούμενης χρονικής στιγμής και της τρέχουσας. Σε περίπτωση υπέρβασης των επιτρεπτών ορίων σηματοδοτείται επίθεση πλημμύρας.

Πρέπει να τονιστεί ότι όλες οι προαναφερόμενες λύσεις εστιάζουν στον αλγόριθμο αναγνώρισης επιθέσεων πλημμύρας χωρίς να δίνουν ιδιαίτερη έμφαση σε θέματα απόδοσης. Για το λόγο αυτό στην εργασία [106] προτείνεται μια αρχιτεκτονική υψηλής κλιμάκωσης για την αναγνώριση επιθέσεων πλημμύρας και την παροχή επιπρόσθετων υπηρεσιών ασφαλείας, με δυνατότητα επεξεργασίας περισσότερων από 50.000 αιτήσεις ανά δευτερόλεπτο.

Ιδιαίτερα σημαντική είναι και η προστασία των περιφερειακών συστημάτων που αξιοποιούνται από τις υπηρεσίες διαδικτυακής τηλεφωνίας από επιθέσεις πλημμύρας, καθώς επηρεάζουν έμμεσα τη διαθεσιμότητα της υπηρεσίας. Ένα τέτοιο παράδειγμα αποτελεί η υπηρεσία επίλυσης ονομάτων (Domain Name System-(DNS)). Πιο συγκεκριμένα, ένας επιτιθέμενος μπορεί να αποστείλει μια σειρά από αιτήσεις οι οποίες συμπεριλαμβάνουν μη επιλύσημες διευθύνσεις, με αποτέλεσμα ο εξουσιοδοτημένος εξυπηρέτης να επιβαρύνεται με περισσότερο υπολογιστικό φορτίο καθώς αναμένει την απάντηση από τον κατάλληλο DNS εξυπηρέτη για την δημιουργία της τελικής απόκρισης. Μια αποδοτική λύση για την προστασία του πληρεξούσιου εξυπηρέτη από τέτοιου είδους περιστατικά προτείνεται στην εργασία [86].

6.6 Συμπεράσματα

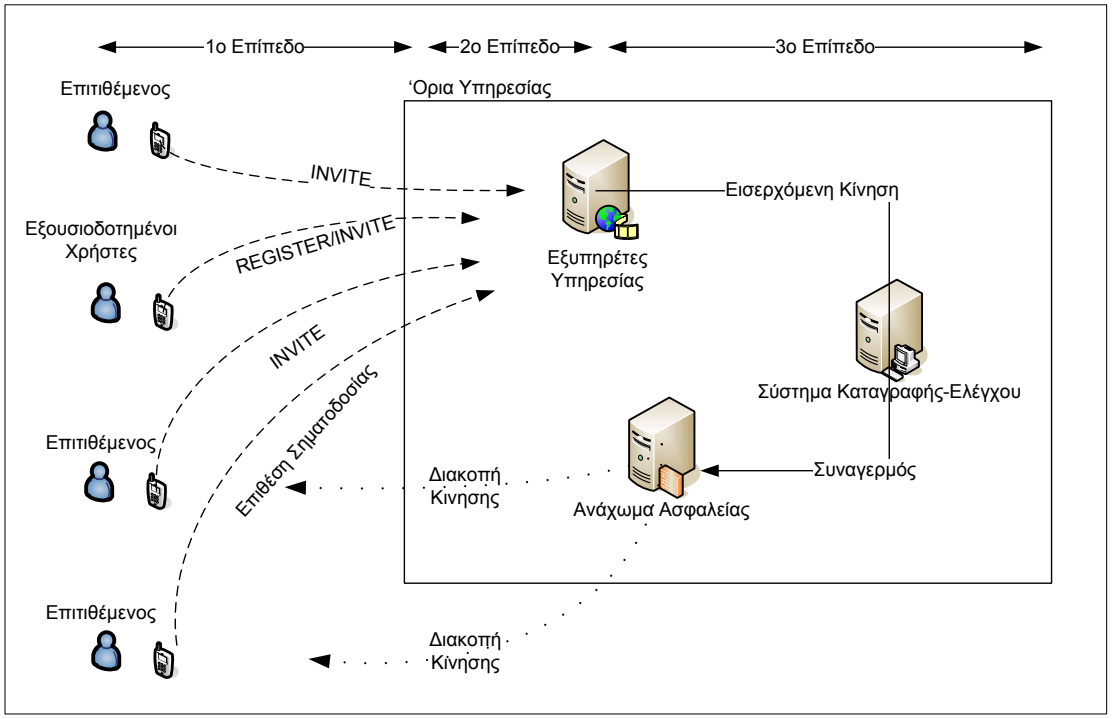
Όπως γίνεται αντιληπτό από τις ερευνητικές προσπάθειες που παρουσιάστηκαν στο κεφάλαιο αυτό, η παροχή υπηρεσιών ασφαλείας και η προστασία των υπολογιστικών πόρων των υπηρεσιών διαδικτυακής τηλεφωνίας δεν μπορεί σε καμία περίπτωση να θεωρηθεί τετριμμένη διαδικασία. Η προσπάθεια εστιάζεται στην εξασφάλιση αυξημένων επιπέδων διαθεσιμότητας και αξιοπιστίας των υπηρεσιών διαδικτυακής τηλεφωνίας, αναπτύσσοντας λύσεις και αρχιτεκτονικές για την αντιμετώπιση επιθέσεων σηματοδοσίας και πλημμύρας.

ΚΕΦΑΛΑΙΟ 7: Προτεινόμενη Αρχιτεκτονική Ασφαλείας για την Προστασία των Υπηρεσιών Διαδικτυακής Τηλεφωνίας

7.1 Γενικά

Λαμβάνοντας υπόψη τη διαφορετικότητα των προβλημάτων ασφαλείας που έχουν εντοπιστεί στις υπηρεσίες διαδικτυακής τηλεφωνίας ή των επιθέσεων που μπορεί να εκδηλωθούν εναντίον τους, γίνεται κατανοητό ότι η δημιουργία ενός ασφαλούς και αξιόπιστου περιβάλλοντος απαιτεί το συνδυασμό προληπτικών, αναγνωριστικών και ανασταλτικών μηχανισμών. Ο ισχυρισμός αυτός ενισχύεται από το γεγονός ότι κανένας από τους εναλλακτικούς μηχανισμούς ασφαλείας που έχουν προταθεί μέχρι σήμερα (βλέπε Κεφάλαιο 6) δεν είναι δυνατόν να αντιμετωπίσει αποτελεσματικά όλες τις πιθανές (γνωστές) επιθέσεις κατά των υπηρεσιών διαδικτυακής τηλεφωνίας. Για τους προαναφερόμενους λόγους, προτείνεται η ανάπτυξη της αρχιτεκτονικής ασφαλείας που παρουσιάζεται στο Σχήμα 7–2. Μέσω της αρχιτεκτονικής αυτής είναι δυνατόν να εφαρμοστούν όλα τα προληπτικά, αναγνωριστικά και ανασταλτικά μέτρα που απαιτούνται για την επίτευξη ενός ιδιαίτερα υψηλού επιπέδου ασφαλείας για τις υπηρεσίες διαδικτυακής τηλεφωνίας.

Όπως μπορεί να διαπιστωθεί, τα μέτρα ασφαλείας υλοποιούνται σε τρία διαφορετικά επίπεδα προστασίας. Στο πρώτο επίπεδο εφαρμόζονται οι απαραίτητοι προληπτικοί μηχανισμοί για την αντιμετώπιση περιστατικών μη εξουσιοδοτημένης τροποποίησης των δεδομένων σηματοδοσίας, με στόχο την αντιμετώπιση επιθέσεων σηματοδοσίας. Στο δεύτερο επίπεδο πραγματοποιούνται οι απαραίτητοι έλεγχοι για την ορθότητα των εισερχόμενων-εξερχόμενων μηνυμάτων σηματοδοσίας, με στόχο την αντιμετώπιση επιθέσεων μη συμβατών μηνυμάτων. Στο τρίτο επίπεδο υλοποιούνται οι απαραίτητοι μηχανισμοί για την αναγνώριση επιθέσεων πλημμύρας.



Σχήμα 7–1. Προτεινόμενη Αρχιτεκτονική Ασφάλειας για την Προστασία των Υπηρεσιών Διαδικτυακής Τηλεφωνίας.

Στη συνέχεια του κεφαλαίου γίνεται αναλυτική περιγραφή των τριών επιπέδων προστασίας της προτεινόμενης αρχιτεκτονικής ασφάλειας.

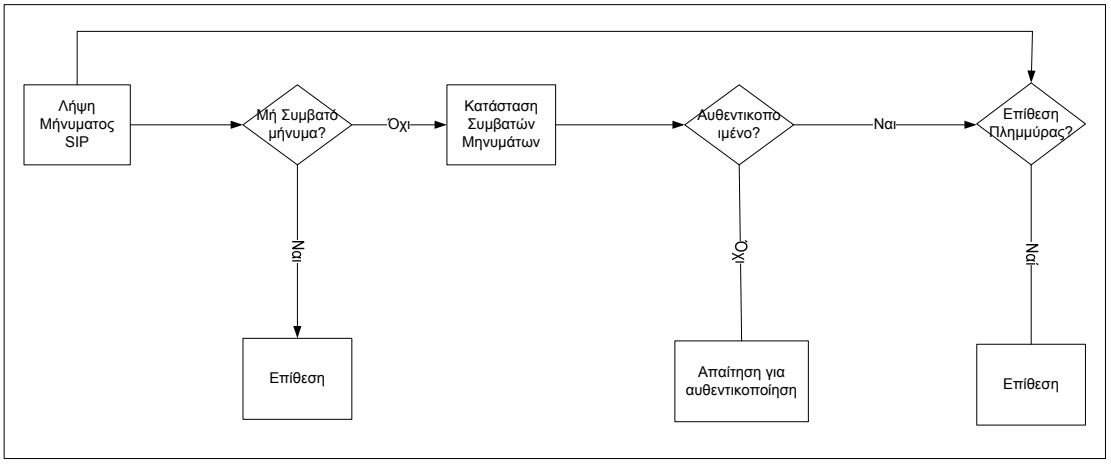
7.2 Συνοπτική Περιγραφή της Προτεινόμενης Αρχιτεκτονικής Ασφαλείας

Όπως παρουσιάζεται στο Σχήμα 7–1, η προτεινόμενη αρχιτεκτονική ασφαλείας απαρτίζεται από τρία διαφορετικά επίπεδα προστασίας. Στο πρώτο επίπεδο προτείνεται η εφαρμογή, σε όλα τα ενεργά δικτυακά στοιχεία των υπηρεσιών διαδικτυακής τηλεφωνίας, ενός μηχανισμού διασφάλισης της ακεραιότητας και αυθεντικότητας των μηνυμάτων σηματοδοσίας. Ο συγκεκριμένος μηχανισμός αξιοποιεί μια ελαφρά τροποποιημένη έκδοση κρυπτογραφικών συναρτήσεων σύνοψης κλειδιού (keyed hash functions) και έχει ως στόχο να αποτρέψει τις επιθέσεις σηματοδοσίας. Να επισημανθεί ότι η απλή αναγνώριση των επιθέσεων σηματοδοσίας δεν προσφέρει ικανοποιητική προστασία αφού πιθανή εκδήλωση της επίθεσης έχει ως άμεσο αποτέλεσμα τον τερματισμό ή την τροποποίηση βασικών παραμέτρων των συνόδων, προκαλώντας άρνηση παροχή υπηρεσίας.

Στο δεύτερο επίπεδο πραγματοποιείται έλεγχος της ορθότητας (συμβατότητας με τις προδιαγραφές του SIP) των εισερχόμενων-εξερχόμενων μηνυμάτων, ώστε να αποφευχθούν τα όποια προβλήματα μπορεί να δημιουργηθούν από την περαιτέρω επεξεργασία μη συμβατών μηνυμάτων. Για τον έλεγχο των μηνυμάτων αξιοποιούνται κατάλληλες *υπογραφές επιθέσεων* οι οποίες βασίζονται στις προδιαγραφές του πρωτοκόλλου σηματοδοσίας SIP.

Τέλος, στο τρίτο επίπεδο προστασίας προτείνεται ένας μηχανισμός για την άμεση αναγνώριση επιθέσεων πλημμύρας. Ο συγκεκριμένος μηχανισμός αξιοποιεί ένα Bloom φίλτρο σε συνδυασμό με τα κατάλληλα όρια τιμών. Το τρίτο επίπεδο άμυνας μπορεί να εφαρμοσθεί «παράλληλα» με τα άλλα δύο επίπεδα χωρίς να επηρεάζει τη λειτουργία τους.

Στο Σχήμα 7–2 απεικονίζεται συγκεντρωτικά η ροή των ελέγχων που πραγματοποιούνται, μέσω της προτεινόμενης αρχιτεκτονικής, από την υπηρεσία διαδικτυακής τηλεφωνίας κατά τη λήψη ενός νέου μηνύματος, με στόχο την αναγνώριση πιθανής επίθεσης. Στο διάγραμμα αυτό μπορεί να παρατηρηθεί ότι οι έλεγχοι για μη συμβατά μηνύματα προηγούνται των ελέγχων αυθεντικοποίησης και ακεραιότητας. Ο λόγος είναι ότι τα αυθεντικοποιήμενα μηνύματα μπορεί να είναι μη συμβατά μηνύματα και συνεπώς η επεξεργασία τους να δημιουργήσει προβλήματα αστάθειας ή ακόμα και να οδηγήσει σε άρνηση παροχής υπηρεσίας.



Σχήμα 7–2. Διάγραμμα Ροής Ελέγχων για την Αναγνώριση και Αντιμετώπιση Επιθέσεων προς τις Υπηρεσίες Διαδικτυακής Τηλεφωνίας

Επιπλέον, σύμφωνα με το διάγραμμα ροής ελέγχων (Σχήμα 7–2), κάποιος θα μπορούσε να ισχυριστεί ότι η προστασία από επιθέσεις σηματοδοσίας βρίσκεται στη δεύτερη γραμμή άμυνας και όχι στην πρώτη όπως αρχικά αποτυπώνεται στην αρχιτεκτονική. Ο συγκεκριμένος ισχυρισμός δεν ισχύει αφού για την αντιμετώπιση των επιθέσεων σηματοδοσίας απαιτείται η ενεργή συμμετοχή των τελικών δικτυακών στοιχείων, που είναι και ο κύριος λόγος που αποτυπώνεται ως πρώτη γραμμή άμυνας στην προτεινόμενη αρχιτεκτονική.

7.3 Προστασία από Επιθέσεις Σηματοδοσίας

7.3.1 Περιγραφή Μηχανισμού Προστασίας

Για την ενίσχυση του παρεχόμενου επιπέδου ασφαλείας των υπηρεσιών διαδικτυακής τηλεφωνίας πρέπει, σύμφωνα και με τις προδιαγραφές του SIP [11], εκτός της εφαρμογής του μηχανισμού αυθεντικοποίησης HTTP Digest [87], να υλοποιηθούν και επιπρόσθετα μέτρα ασφαλείας που θα έχουν ως στόχο την αποτροπή της μη εξουσιοδοτημένης τροποποίησης των μηνυμάτων σηματοδοσίας από κακόβουλους χρήστες. Άλλωστε, όπως προκύπτει τόσο από την ανάλυση των προβλημάτων ασφαλείας (Κεφάλαιο 4) όσο και των μηχανισμών ασφαλείας που προτείνονται από τις προδιαγραφές του SIP [11] (Κεφάλαιο 5), μια από τις κύριες αιτίες εκδήλωσης επιθέσεων σηματοδοσίας είναι η μη εφαρμογή των κατάλληλων μηχανισμών αυθεντικότητας και ακεραιότητας στα μηνύματα σηματοδοσίας. Έχοντας υπόψιν τα προαναφερόμενα αλλά και τις ειδικές απαιτήσεις ασφαλείας που πρέπει να ικανοποιούνται από τις υπηρεσίες διαδικτυακής τηλεφωνίας (βλέπε Ενότητα 5.2), προτείνεται ένας μηχανισμός διασφάλισης της ακεραιότητας και αυθεντικότητας των μηνυμάτων σηματοδοσίας βασισμένος σε μια ελαφρά παραλλαγή του τρόπου δημιουργίας του κώδικα επαλήθευσης μηνυμάτων με την χρήση κρυπτογραφικών συναρτήσεων σύνοψης κλειδιού [120]. Είναι ιδιαίτερα σημαντικό να τονιστεί ότι ο προτεινόμενος μηχανισμός δεν επηρεάζει τη βασική λειτουργικότητα του SIP αλλά ούτε και την υπάρχουσα υποδομή αυθεντικοποίησης με χρήση συνθηματικών.

Η μοναδική προϋπόθεση για την εφαρμογή του προτεινόμενου μηχανισμού είναι η εισαγωγή μιας νέας κεφαλίδας που έχει ονομαστεί «*Integrity-Auth*». Μπορεί στο σημείο αυτό να δημιουργηθεί η εντύπωση ότι η εισαγωγή μιας νέας κεφαλίδας όχι μόνο απαιτεί την τροποποίηση των υποδομών του SIP αλλά και ότι η εφαρμογή ενός τέτοιου μηχανισμού δεν είναι εφικτή σε πραγματικές αρχιτεκτονικές. Κάτι τέτοιο δεν ισχύει και μάλιστα είναι σε πλήρη αντιδιαστολή με την φιλοσοφία του SIP [11] σύμφωνα με την οποία η βελτίωση των παρεχόμενων υπηρεσιών προτρέπει στην εισαγωγή νέων κεφαλίδων και παραμέτρων. Ίσως το πιο χαρακτηριστικό παράδειγμα αποτελούν οι διαφορετικές προτάσεις για εισαγωγή νέων κεφαλίδων [98],[121]–[124] για τη βελτίωση των λειτουργιών που παρέχονται από το SIP.

Στο Σχήμα 7–3 απεικονίζεται η γραμματική της προτεινόμενης κεφαλίδας «*Integrity-Auth*», η οποία συμμορφώνεται πλήρως με τις προδιαγραφές του SIP [11]. Η νέα αυτή κεφαλίδα θα πρέπει να αξιοποιείται-εφαρμόζεται σε όλα τα μηνύματα SIP, ανεξαρτήτως τύπου (αίτηση ή απόκριση).

```
Integrity-Auth=”Integrity-Auth” HCOLON integrity-auth-value
integrity-auth-value= credentials-value;algrotithm;nonce
algorithm=”algorithm” EQUAL alg-value
alg-value=”MD5|SHA1"
credentials-value=quoted-string
```

Σχήμα 7–3. Η Γραμματική για την Κεφαλίδα Integrity-Auth

Η τιμή των διαπιστευτηρίων (Integrity-Auth Credential Value) θα υπολογίζεται μέσω του τύπου που απεικονίζεται στο Σχήμα 7–4, ο οποίος αποτελεί όπως προαναφέρθηκε μια ελαφρά παραλλαγή του τρόπου δημιουργίας του κώδικα επαλήθευσης μηνυμάτων με την χρήση κρυπτογραφικών συναρτήσεων σύνοψης κλειδιού [120]. Συγκεκριμένα, η τιμή της κεφαλίδας «*Integrity-Auth*» θα είναι το αποτέλεσμα της εφαρμογής μιας μονόδρομης συνάρτησης σύνοψης στα παρακάτω δεδομένα:

1. Στο μήνυμα σηματοδοσίας συνδυαζόμενο με ένα τυχαίο αριθμό (random number)
2. Στο αποτέλεσμα της εφαρμογής μιας μονόδρομης συνάρτησης σύνοψης στο αποτέλεσμα της πράξης "αποκλειστικού Η" (exclusive OR) μεταξύ του συνθηματικού του χρήστη και του τυχαίου αριθμού.

$$Integrity\_Auth=Hash((SIP\_Message:Random),\ Hash(Passwd) \oplus Random))$$

Σχήμα 7–4. Φόρμουλα Υπολογισμού της Τιμής της Κεφαλίδας Integrity-Auth

Ουσιαστικά, η εφαρμογή του προαναφερόμενου μηχανισμού προσφέρει τη δυνατότητα παροχής υπηρεσιών ακεραιότητας και αυθεντικότητας. Συγκεκριμένα, οι υπηρεσίες ακεραιότητας παρέχονται μέσω της χρήσης της συνάρτησης κρυπτογραφικής σύνοψης ενώ η αυθεντικότητα διασφαλίζεται με την προσθήκη του συνθηματικού στο αποτέλεσμα της κρυπτογραφικής σύνοψης. Επιπλέον, η χρήση των τυχαίων αριθμών παρέχει προστασία από επιθέσεις επανάληψης. Περισσότερες λεπτομέρειες για τον προτεινόμενο μηχανισμό δίνονται στην ενότητα 7.3.3.

Όσον αναφορά την υπολογιστική επιβάρυνση που εισάγεται από τον προτεινόμενο μηχανισμό, θεωρείται ελάχιστη λαμβάνοντας υπόψη την υπολογιστική επιβάρυνση που προκαλούν οι συναρτήσεις σύνοψης [125]. Αμελητέο επίσης θεωρείται και το επιπρόσθετο μήκος του μηνύματος αφού η τιμή της κεφαλίδας «*Integrity-Auth*» δε μπορεί να ξεπεράσει τα 160 bits, ανάλογα με τον αλγόριθμο κρυπτογραφικής σύνοψης που εφαρμόζεται σε κάθε περίπτωση. Περισσότερες, λεπτομέρειες για την αποδοτικότητα του προτεινόμενου μηχανισμού δίνονται στην ενότητα 7.3.4.

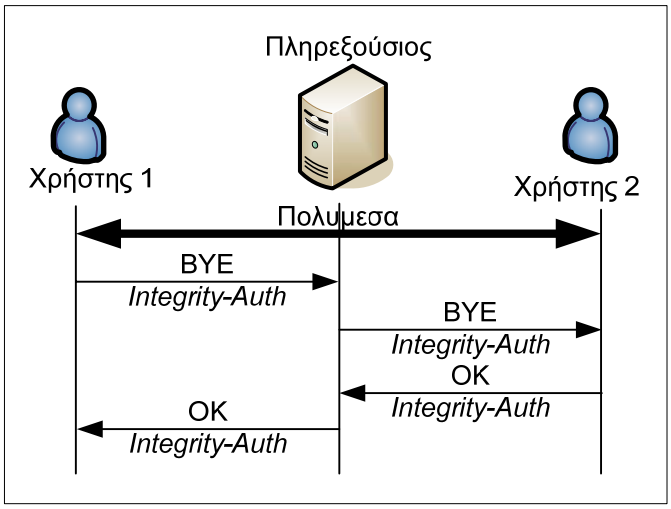
Τέλος, σύμφωνα με το RFC 2104 [120], ο μηχανισμός υπολογισμού του κώδικα επαλήθευσης μηνυμάτων, με τη χρήση κρυπτογραφικών συναρτήσεων σύνοψης κλειδιού, είναι ανεξάρτητος από την υλοποίηση του αλγορίθμου που αξιοποιείται και ως εκ τούτου στο προτεινόμενο μηχανισμό μπορεί να αξιοποιηθεί οποιαδήποτε συνάρτηση κρυπτογραφικής σύνοψης θεωρείται ασφαλής.

7.3.2 Εφαρμογή του Μηχανισμού Integrity-Auth: Η Περίπτωση της Επίθεσης Σηματοδοσίας τύπου BYE

Στην περίπτωση μιας επίθεσης σηματοδοσίας τύπου SIP BYE, ο επιτιθέμενος αρχικά θα υποκλέψει τις παραμέτρους που χρειάζεται για να δημιουργήσει, στη συνέχεια, ένα πλαστό μήνυμα SIP BYE και να επιτύχει τον τερματισμό μιας συνόδου (βλέπε Ενότητα 4.4.5). Η εφαρμογή του προτεινόμενου μηχανισμού είναι δυνατόν να αποτρέψει τη συγκεκριμένη επίθεση. Συγκεκριμένα, ο εξουσιοδοτημένος χρήστης που συμμετέχει σε μία σύνοδο και επιθυμεί τον τερματισμό της, δημιουργεί ένα μήνυμα SIP BYE στο οποίο συμπεριλαμβάνεται η κεφαλίδα *Integrity-Auth*. Σύμφωνα με τον τύπο στο Σχήμα 7–4, η τιμή της *Integrity-Auth* κεφαλίδας θα είναι η ακόλουθη:

$$Integrity\_Auth=Hash((SIP\_Message:Random),\ Hash(PWD_{USER} \oplus Random))$$

Μόλις ο χρήστης δημιουργήσει το μήνυμα SIP BYE το προωθεί στον εξουσιοδοτημένο πληρεξούσιο εξυπηρέτη, ο οποίος ανακτά το συνθηματικό του χρήστη (PWDuser) από την αντίστοιχη βάση δεδομένων και ελέγχει την εγκυρότητα του μηνύματος υπολογίζοντας εκ νέου την τιμή της κεφαλίδας «*Integrity-Auth*» . Στην περίπτωση που η τιμή της κεφαλίδας «*Integrity-Auth*» του αρχικού μηνύματος είναι ίδια με αυτή που μόλις υπολογίστηκε η επαλήθευση θεωρείται επιτυχής και ο πληρεξούσιος εξυπηρέτης προωθεί το μήνυμα τερματισμού SIP BYE στον άλλο χρήστη. Πριν την προώθηση του μηνύματος ο πληρεξούσιος εξυπηρέτης τροποποιεί το αρχικό μήνυμα, αντικαθιστώντας την κεφαλίδα «*Integrity-Auth*» με μια νέα που βασίζεται στο συνθηματικό του άλλου χρήστη. Μόλις ο άλλος χρήστης λάβει το μήνυμα τερματισμού SIP BYE, ελέγχει την εγκυρότητα του ακολουθώντας αντίστοιχη διαδικασία με αυτή που προαναφέρθηκε για τον πληρεξούσιο εξυπηρέτη. Εφόσον, η επαλήθευση είναι επιτυχής αποκρίνεται με ένα μήνυμα «200 OK», στο οποίο και εφαρμόζεται ο προτεινόμενος μηχανισμός για προστασία από μη εξουσιοδοτημένη τροποποίηση. Η συνολική διαδικασία απεικονίζεται στο Σχήμα 7–5.



Σχήμα 7–5. Ροή Μηνυμάτων για την Εφαρμογή του Προτεινόμενου Μηχανισμού στο Μήνυμα Τερματισμού SIP BYE

Ο μηχανισμός που μόλις περιγράφηκε μπορεί να αξιοποιηθεί για την προστασία από όλες τις επιθέσεις σηματοδοσίας ή μη εξουσιοδοτημένης τροποποίησης.

7.3.3 Ανάλυση Ασφαλείας του Προτεινόμενου Μηχανισμού

Η εφαρμογή του προτεινόμενου μηχανισμού, όπως παρουσιάστηκε στις προηγούμενες ενότητες, διασφαλίζει την ακεραιότητα και αυθεντικότητα των μηνυμάτων σηματοδοσίας, παρέχοντας ταυτόχρονα προστασία από επιθέσεις σηματοδοσίας. Για την περαιτέρω ανάλυση της αξιοπιστίας του, υλοποιήθηκαν διαφορετικά σενάρια χρήσης μέσω των οποίων και αναδείχθηκαν τα πλεονεκτήματα - μειονεκτήματα του προτεινόμενου μηχανισμού. Σε όλα τα σενάρια γίνεται η υπόθεση ότι εφαρμόζεται ο προτεινόμενος μηχανισμός.

Αρχικά εξετάζεται το ενδεχόμενο ενός κακόβουλου χρήστη που προσπαθεί να παρακάμψει τον προτεινόμενο μηχανισμό και να πραγματοποιήσει κάποια επίθεση σηματοδοσίας. Ο μοναδικός τρόπος για να επιτύχει κάτι τέτοιο είναι να υποδυθεί έναν εξουσιοδοτημένο χρήστη ή ένα πληρεξούσιο εξυπηρέτη. Στην πρώτη περίπτωση ο κακόβουλος χρήστης πρέπει να δημιουργήσει ένα πλαστό μήνυμα SIP BYE και να το προωθήσει στον αντίστοιχο εξυπηρέτη. Ο εξυπηρέτης που θα λάβει το πλαστό αυτό μήνυμα θα προσπαθήσει να επικυρώσει τη γνησιότητα του, σύμφωνα με όσα περιγράφηκαν στην ενότητα 7.3.1. Βασιζόμενοι στο γεγονός ότι ο κακόβουλος χρήστης δε γνωρίζει το συνθηματικό του

εξουσιοδοτημένου χρήστη, ο πληρεξούσιος εξυπηρέτης δεν είναι δυνατόν να επικυρώσει τη γνησιότητα του μηνύματος καθώς η τιμή της κεφαλίδας «*Integrity-Auth*» που υπολογίζεται από αυτόν δεν είναι ίδια με την τιμή που έχει συμπεριλάβει ο κακόβουλος χρήστης στο μήνυμα τερματισμού SIP BYE. Ακόμα και στην περίπτωση που ο κακόβουλος χρήστης είναι κάποιος εξουσιοδοτημένος χρήστης και αξιοποιήσει το δικό του συνθηματικό κατά τον υπολογισμό της τιμής της κεφαλίδας «*Integrity-Auth*», ο πληρεξούσιος εξυπηρέτης θα απορρίψει το μήνυμα αφού τα συνθηματικά του κακόβουλου και του εξουσιοδοτημένου χρήστη δεν ταυτίζονται και ως εκ τούτου, όπως και στην προηγούμενη περίπτωση, η τιμή που υπολογίζει ο πληρεξούσιος εξυπηρέτης δεν ταυτίζεται με αυτή που συμπεριλαμβάνεται στο πλαστό μήνυμα SIP BYE.

Στην περίπτωση που ο κακόβουλος χρήστης επιχειρήσει να λειτουργήσει για λογαριασμό του εξουσιοδοτημένου πληρεξούσιου, όλες οι οντότητες (χρήστες) που συμμετέχουν στη σύνοδο είναι δυνατόν να το εντοπίσουν, αφού ο επιτιθέμενος δε γνωρίζει τα συνθηματικά των με αποτέλεσμα τα μηνύματα που δημιουργεί να μην αντιστοιχούν με αυτά που παράγουν οι εξουσιοδοτημένες οντότητες. Επιπροσθέτως, το προτεινόμενο σχήμα παρέχει και προστασία από επιθέσεις επανάληψης αφού στον υπολογισμό της τιμής της κεφαλίδας «*Integrity-Auth*» συμπεριλαμβάνεται κάθε φορά ένα διαφορετικός τυχαίος αριθμός. Βέβαια θα πρέπει να τονιστεί ότι απαιτείται ορθή διαχείριση των τυχαίων αριθμών εκ μέρους των εξυπηρετών της υπηρεσίας.

Κάποιος θα μπορούσε να ισχυριστεί ότι το προτεινόμενο σχήμα είναι ευπαθές σε επιθέσεις τύπου εξαντλητικής αναζήτησης (brute force attacks) συνθηματικών. Συγκεκριμένα, ο επιτιθέμενος μπορεί να υποκλέψει ένα μήνυμα SIP, στο οποίο συμπεριλαμβάνονται τόσο ο τυχαίος αριθμός όσο και η τιμή της κεφαλίδας «*Integrity-Auth*», και στη συνέχεια να πραγματοποιήσει επίθεση εξαντλητικής αναζήτησης του συνθηματικού αξιοποιώντας τη μέθοδο που παρουσιάζεται στο Σχήμα 7–6.

Για κάθε πιθανό συνθηματικό *PWDi* εκτέλεσε:
brute_force_value=*Hash(SIP_MESSAGE:Random,Hash(PWDi⊕Random))*
If(brute_force_value==τιμή_υποκλοπής)
τότε συνθηματικό=*PWDi*

Σχήμα 7–6. Επίθεση Εξαντλητικής Αναζήτησης Συνθηματικού

Όμως, επιθέσεις τέτοιου τύπου είναι πρακτικά εφικτές μόνο σε περιπτώσεις που τα συνθηματικά των χρηστών ανήκουν σε μικρό κρυπτογραφικό διάστημα (small cryptographic space)[126]. Συνεπώς, ο βασικότερος περιορισμός του προτεινόμενου μηχανισμού προέρχεται από τη χρήση «κοινών» συνθηματικών μεταξύ χρήστη και υπηρεσίας. Βέβαια ο προτεινόμενος μηχανισμός μπορεί να συνδυαστεί και με άλλα σχήματα ασφαλείας που αξιοποιούν κατάλληλους μηχανισμούς για την παραγωγή των κρυπτογραφικών κλειδιών μιας συνόδου, όπως περιγράφεται στην εργασία [99].

Ένα άλλο ερώτημα είναι το κατά πόσο αντίστοιχες υπηρεσίες θα μπορούσαν να υλοποιηθούν αξιοποιώντας το HTTP Digest [87]. Η απάντηση είναι ότι αυτό δεν είναι εφικτό αφού για κάθε μήνυμα που αυθεντικοποιείται το HTTP digest απαιτεί τη χρήση τριών επιπρόσθετων μηνυμάτων. Επιπλέον, δεν είναι δυνατόν να εφαρμοσθεί σε περιπτώσεις που η επανυποβολή ενός μηνύματος δεν είναι εφικτή. Περισσότερες λεπτομέρειες σχετικά με τους περιορισμούς του HTTP Digest υπάρχουν στην Ενότητα 5.4.

Ο Πίνακας 7–1 παρουσιάζει συνοπτικά τις υπηρεσίες ασφαλείας που υποστηρίζονται από τον προτεινόμενο μηχανισμό και γίνεται σύγκριση με τις αντίστοιχες υπηρεσίες που υποστηρίζουν οι προτεινόμενοι από το SIP μηχανισμοί. Από την άλλη πλευρά ο Πίνακας 7–2

παρουσιάζει μια αντίστοιχη σύγκριση αναφορικά με την αντιμετώπιση συγκεκριμένων τύπων επιθέσεων.

	HTTP Digest	**SSL**	**Προτεινόμενος Μηχανισμός**
Ακεραιότητα	Όχι	Ναι	Ναι
Αυθεντικότητα Χρήστη	Ναι	Ναι	Ναι
Εμπιστευτικότητα	Όχι	Ναι	Όχι
Μη-αποποίηση	Όχι	Όχι	Όχι
Αμοιβαία Αυθεντικοποίηση	Όχι	Ναι	Ναι

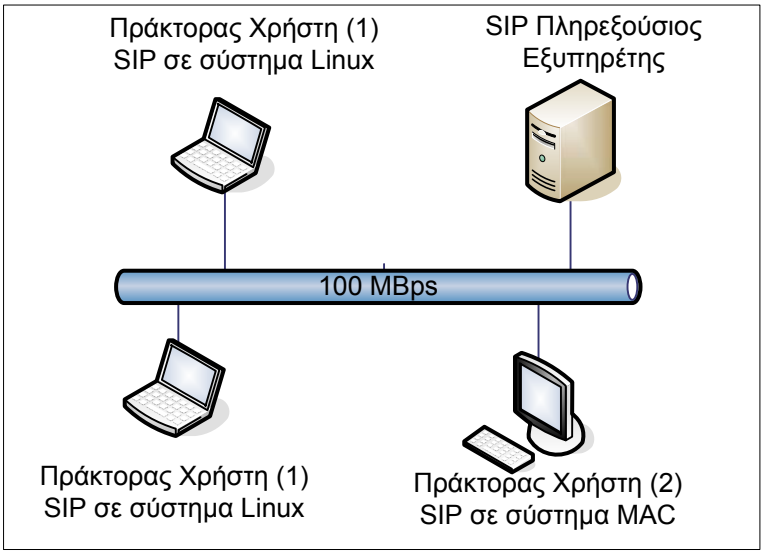
Πίνακας 7–1. Σύγκριση Υποστηριζόμενων Υπηρεσιών Ασφάλειας

	HTTP Digest	**SSL**	**Προτεινόμενος Μηχανισμός**
Επιθέσεις Επανάληψης	Ναι	Ναι	Ναι
Επιθέσεις Σηματοδοσίας	Όχι	Όχι	Όχι
Επιθέσεις Ενδιάμεσου	Όχι	Όχι	NAI

Πίνακας 7–2. Σύγκριση της Ικανότητας Αντιμετώπισης Επιθέσεων

7.3.4 Αποτίμηση Απόδοσης

Για την αξιολόγηση της απόδοσης του προτεινόμενου μηχανισμού, σε πρώτη φάση ενσωματώθηκε σ' ένα πελάτη SIP, βασισμένο στο pjsip [127], και στον «SIP Express Router (SER)» [77] που είναι ένας εξυπηρέτης τύπου πληρεξούσιου. Οι απαραίτητες κρυπτογραφικές λειτουργίες υλοποιήθηκαν με τη χρήση της βιβλιοθήκης «OpenSSL» [128]. Στη συνέχεια αναπτύχθηκε η αρχιτεκτονική που απεικονίζεται στο Σχήμα 7–7, η οποία και αξιοποιήθηκε για την αποτίμηση του μηχανισμού με τη χρήση των κατάλληλων σεναρίων. Ο Πίνακας 7–3 αποτυπώνει τα κύρια χαρακτηριστικά των δικτυακών στοιχείων της αρχιτεκτονικής αυτής.



Σχήμα 7–7. Αρχιτεκτονική Αξιολόγησης του Μηχανισμού Προστασίας από Επιθέσεις Σηματοδοσίας

Δικτυακή Οντότητα	Χαρακτηριστικά Συστήματος		
	Λειτουργικό Σύστημα	Επεξεργαστής	Μνήμη
Πληρεξούσιος Εξυπηρέτης	Fedora Core 8	Pentium 4 2.8 GHhz	512 MB
Πράκτορας Χρήστη 1 SIP	Fedora Core 8	Pentium 4 2.8 GHhz	512 MB
Πράκτορας Χρήστη 2 SIP	Mac OS X 10.4.11	Intel Core 2 Duo 2 GHz	1GB

Πίνακας 7–3. Χαρακτηριστικά των Υπολογιστικών Συστημάτων που Αξιοποιήθηκαν για την Υλοποίηση των Σεναρίων Αξιολόγησης

Πιο συγκεκριμένα, για την αξιολόγηση του προτεινόμενου μηχανισμού υλοποιήθηκαν τα ακόλουθα σενάρια:

1. Ο SIP πελάτης αποστέλλει, στον πληρεξούσιο εξυπηρέτη, μια αίτηση νέας κλήσης ανά δευτερόλεπτο, χωρίς καμία επιπρόσθετη κίνηση (Σ1).
2. Ο SIP πελάτης αποστέλλει, στον πληρεξούσιο εξυπηρέτη, μια αίτηση νέας κλήσης ανά δευτερόλεπτο, υποθέτοντας την ύπαρξη επιπρόσθετης κίνησης 200 κλήσεων ανά δευτερόλεπτο (Σ2).
3. Ο SIP πελάτης αποστέλλει, στον πληρεξούσιο εξυπηρέτη, μια αίτηση νέας κλήσης ανά δευτερόλεπτο, υποθέτοντας την ύπαρξη επιπρόσθετης κίνησης 400 κλήσεων ανά δευτερόλεπτο(Σ3).

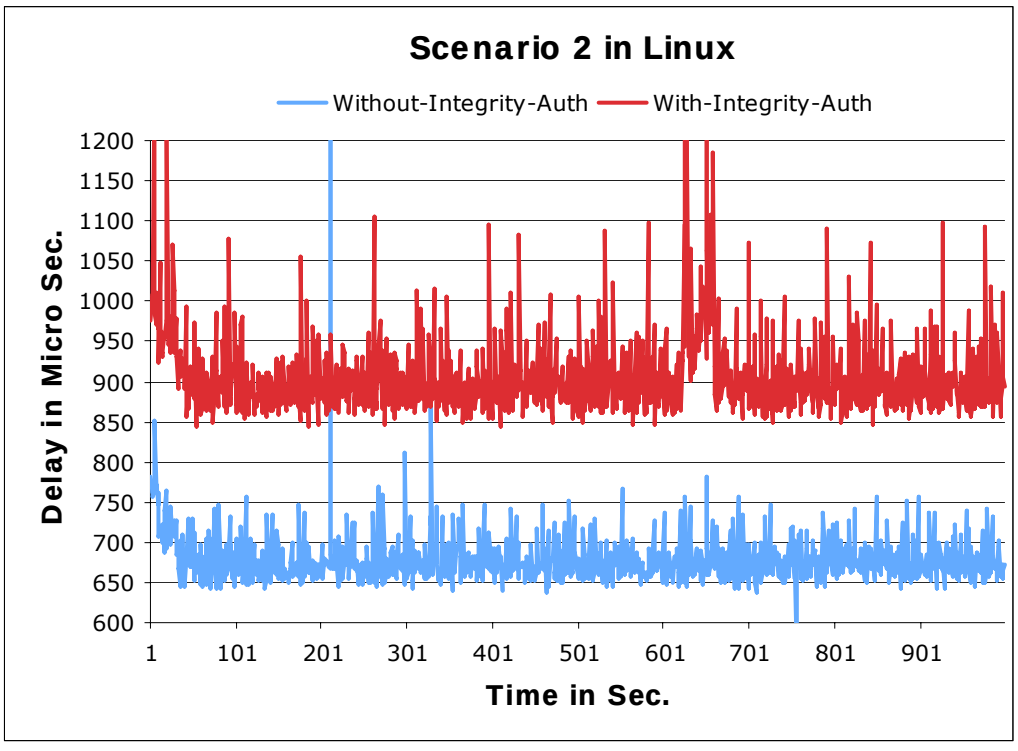
Στα σενάρια αυτά έγινε καταγραφή των παρακάτω ‘επεξεργαστικών χρόνων’:

- Συνολικός χρόνος μέχρι τη λήψη της αρχικής απόκρισης από τον SIP πελάτη.
- Οι επιμέρους χρόνοι για όλες τις ενδιάμεσες διαδικασίες. Συγκεκριμένα:
  - Χρόνος δημιουργίας και αποστολής της αίτησης από τον SIP πελάτη προς τον πληρεξούσιο εξυπηρέτη.

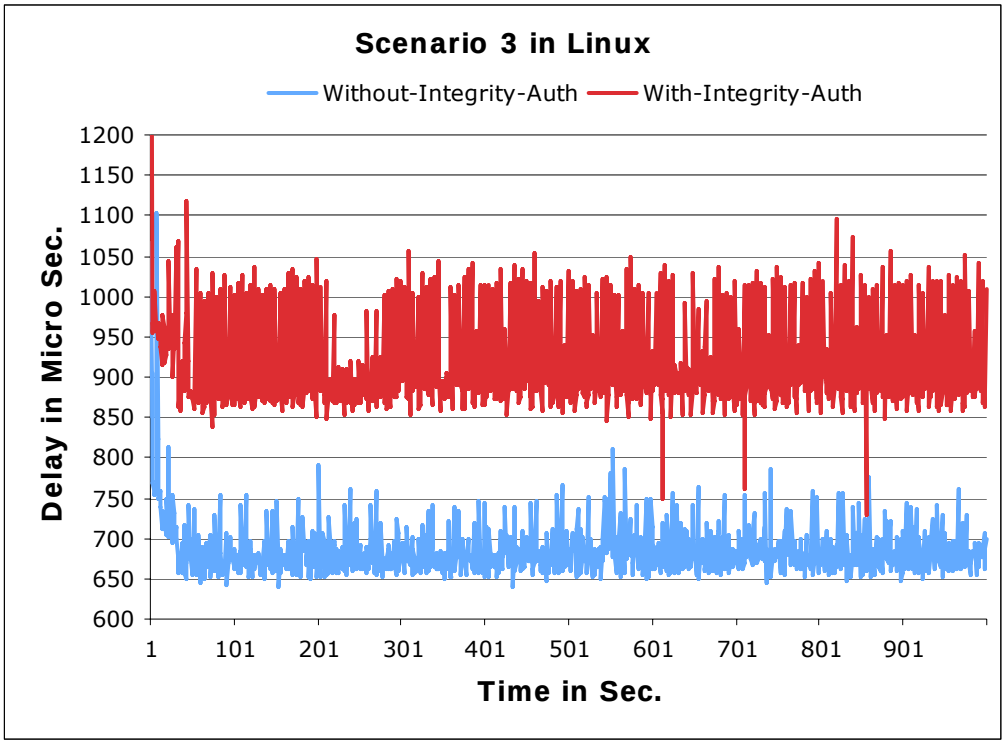
- Χρόνος επαλήθευσης της αίτησης από τον πληρεξούσιο εξυπηρέτη.
- Χρόνος δημιουργίας και αποστολής της απόκρισης από τον πληρεξούσιο εξυπηρέτη.
- Χρόνος επαλήθευσης της απόκρισης από τον SIP πελάτη.

Για να εντοπιστούν πιθανές διαφοροποιήσεις στο χρόνο επεξεργασίας που απαιτούν διαφορετικά υπολογιστικά συστήματα, ο SIP πελάτης που αξιοποιήθηκε για τις παραπάνω μετρήσεις εγκαταστάθηκε σε δύο διαφορετικά συστήματα και συγκεκριμένα σ' ένα φορητό MacBook και σ' ένα προσωπικό υπολογιστή (περισσότερες λεπτομέρειες αναφέρονται στον Πίνακας 7–3). Επίσης, όλα τα σενάρια υλοποιήθηκαν τόσο κάνοντας χρήση του SIP πελάτη που ενσωματώνει τον προτεινόμενο μηχανισμό προστασίας, όσο και κάνοντας χρήση του SIP πελάτη χωρίς το μηχανισμό προστασίας. Με τον τρόπο αυτό είναι εφικτός ο προσδιορισμός της συνολικής επεξεργαστικής επιβάρυνσης που προκαλείται από την εισαγωγή του προτεινόμενου μηχανισμού.

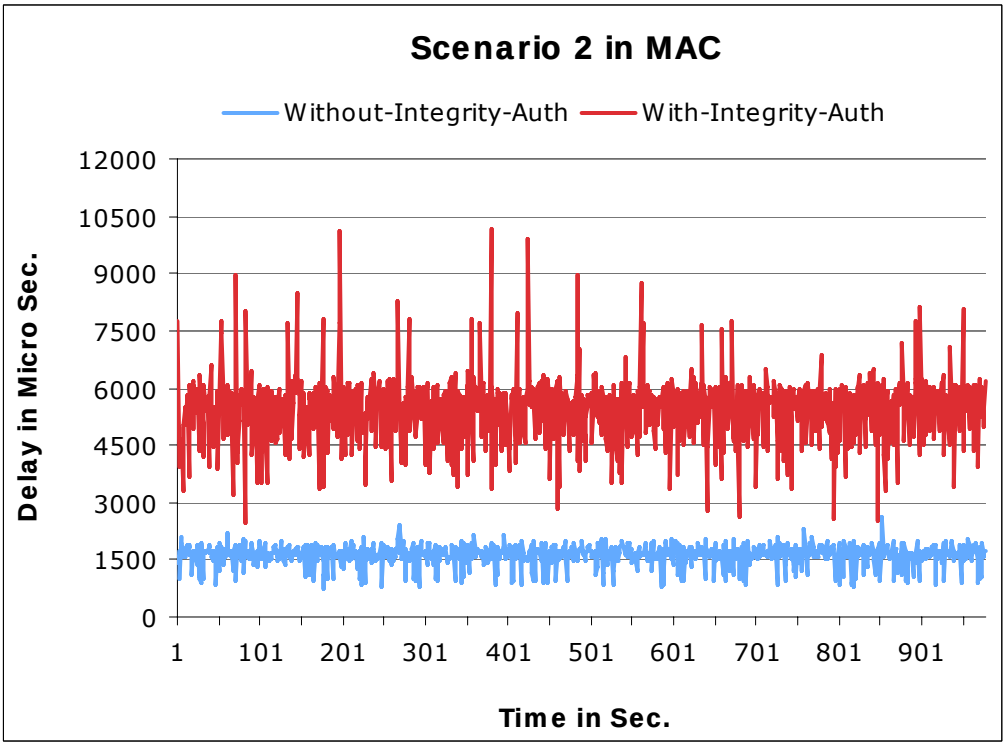
Από το Σχήμα 7–8 έως και το Σχήμα 7–11 απεικονίζονται ενδεικτικά τα αποτελέσματα των μετρήσεων που έγιναν για τα σενάρια 2 και 3, τόσο για την περίπτωση που ο SIP πελάτης ήταν εγκατεστημένος στο σύστημα Linux, όσο και για την περίπτωση που ήταν στο MacBook. Οι αντίστοιχες μετρήσεις για το σενάριο 1 δεν παρουσιάζονται καθώς είναι σχεδόν ταυτόσημες με αυτές του σεναρίου 2. Αντίστοιχα, ο Πίνακας 7–4 μέχρι και ο Πίνακας 7–7, παρουσιάζουν τα στατιστικά χαρακτηριστικά (μέγιστο, ελάχιστο, μέση τιμή και τυπική απόκλιση) όλων των σεναρίων που υλοποιήθηκαν.



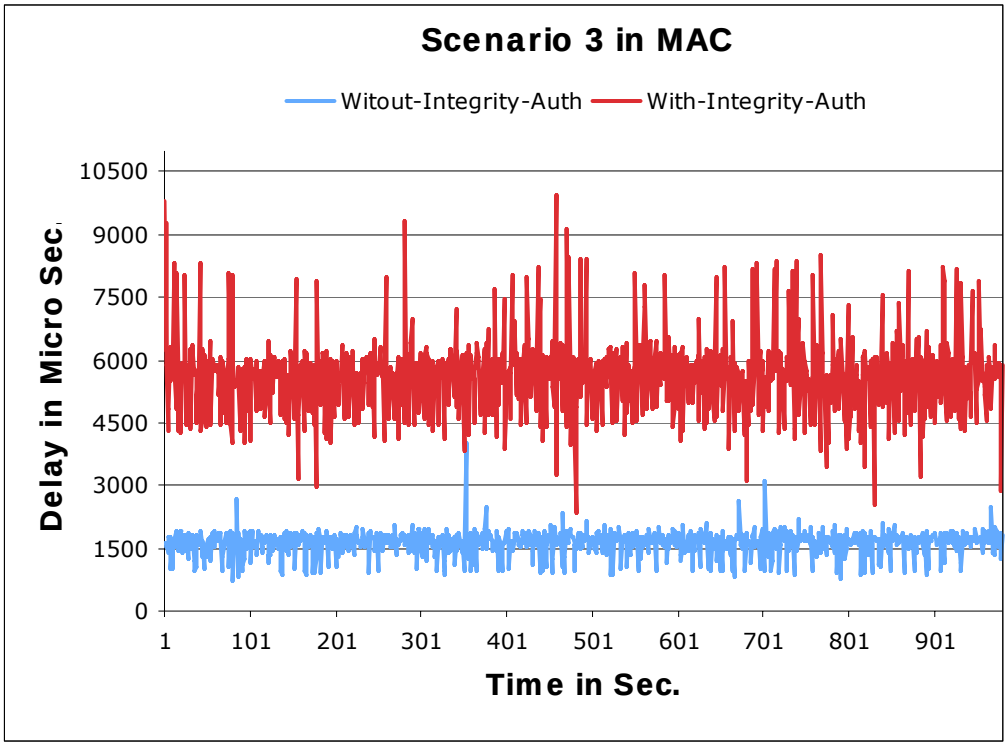
Σχήμα 7–8. Απεικόνιση της Συνολικής Καθυστέρησης που Εισάγεται στον SIP Πελάτη στο Σύστημα Linux για το Σενάριο 2



Σχήμα 7–9. Απεικόνιση της Συνολικής Καθυστέρησης που Εισάγεται στον SIP Πελάτη στο Σύστημα Linux για το Σενάριο 3



Σχήμα 7–10. Απεικόνιση της Συνολικής Καθυστέρησης που Εισάγεται στον SIP Πελάτη στο Σύστημα MAC για το Σενάριο 2



Σχήμα 7–11. Απεικόνιση της Συνολικής Καθυστέρησης που Εισάγεται στον SIP Πελάτη στο Σύστημα MAC για το Σενάριο 3

Τύπος SIP Πελάτη	Σ1	Σ2	Σ3
Linux-χωρίς-τον προτεινόμενο μηχανισμό	672.70	679.34	684.87
Linux-με-τον προτεινόμενο μηχανισμό	908.51	907.78	910.91
Mac- χωρίς-τον προτεινόμενο μηχανισμό	1624.66	1622.88	1635.22
Mac- με-τον προτεινόμενο μηχανισμό	5538.36	5461.17	5641.22

Πίνακας 7–4. Μέση Τιμή Καθυστέρησης σε μικρο-δευτερόλεπτα για τα Σενάρια 1-3

Τύπος SIP Πελάτη	Σ1	Σ2	Σ3
Linux- χωρίς-τον προτεινόμενο μηχανισμό	827.00	1375.00	1104.00
Linux- με-τον προτεινόμενο μηχανισμό	1193.00	2223.00	1933.00
Mac- χωρίς-τον προτεινόμενο μηχανισμό	2593.00	2641.00	4023.00
Mac- με-τον προτεινόμενο μηχανισμό	10157.00	10192.00	9927.00

Πίνακας 7–5. Μέγιστη Τιμή σε μικρο-δευτερόλεπτα Καθυστέρησης για τα Σενάρια 1-3

Τύπος SIP Πελάτη	Σ1	Σ2	Σ3
Linux-χωρίς-τον προτεινόμενο μηχανισμό	635.00	557.00	639.00
Linux-με-τον προτεινόμενο μηχανισμό	789.00	844.00	729.00
Mac-χωρίς-τον προτεινόμενο μηχανισμό	751.00	752.00	741.00
Mac-με-τον προτεινόμενο μηχανισμό	2014.00	2481.00	2358.00

Πίνακας 7–6. Ελάχιστη τιμή Καθυστέρησης σε μικρο-δευτερόλεπτα για τα Σενάρια 1-3

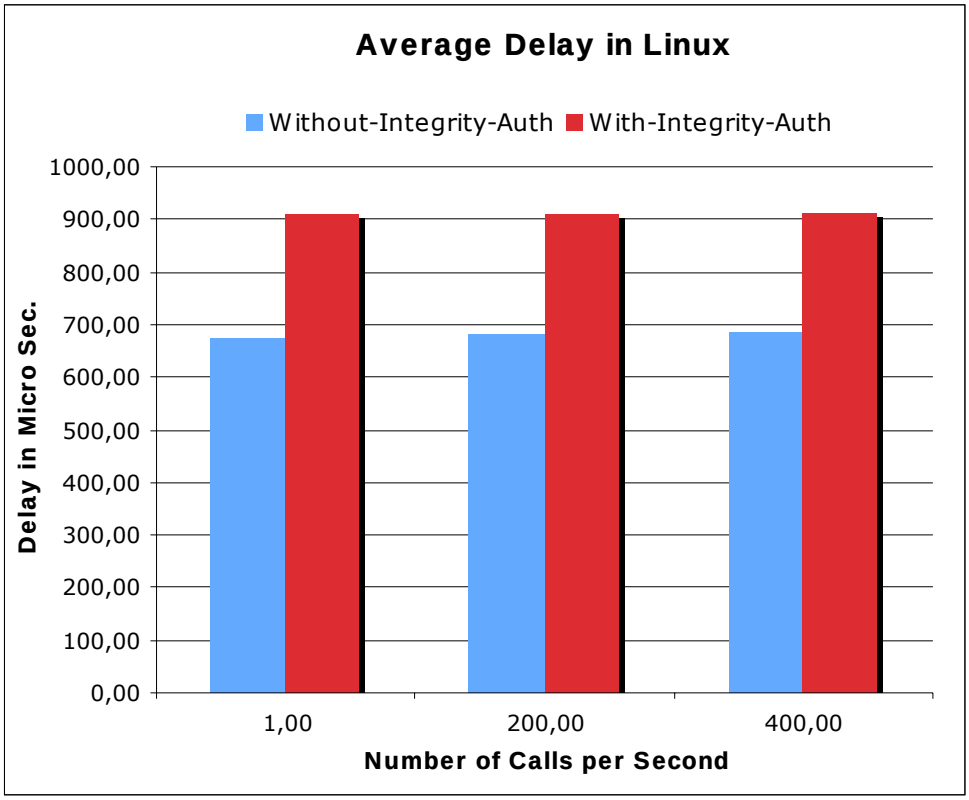
Τύπος SIP Πελάτη	Σ1	Σ2	Σ3
Linux-χωρίς-τον προτεινόμενο μηχανισμό	19.30	34.72	33.28
Linux-με-τον προτεινόμενο μηχανισμό	49.64	66.98	62.68
Mac-χωρίς-τον προτεινόμενο μηχανισμό	252.91	273.98	877.14
Mac-με-τον προτεινόμενο μηχανισμό	831.48	852.15	285.35

Πίνακας 7–7. Τυπική Απόκλιση Καθυστέρησης σε μικρο-δευτερόλεπτα για τα Σενάρια 1-3

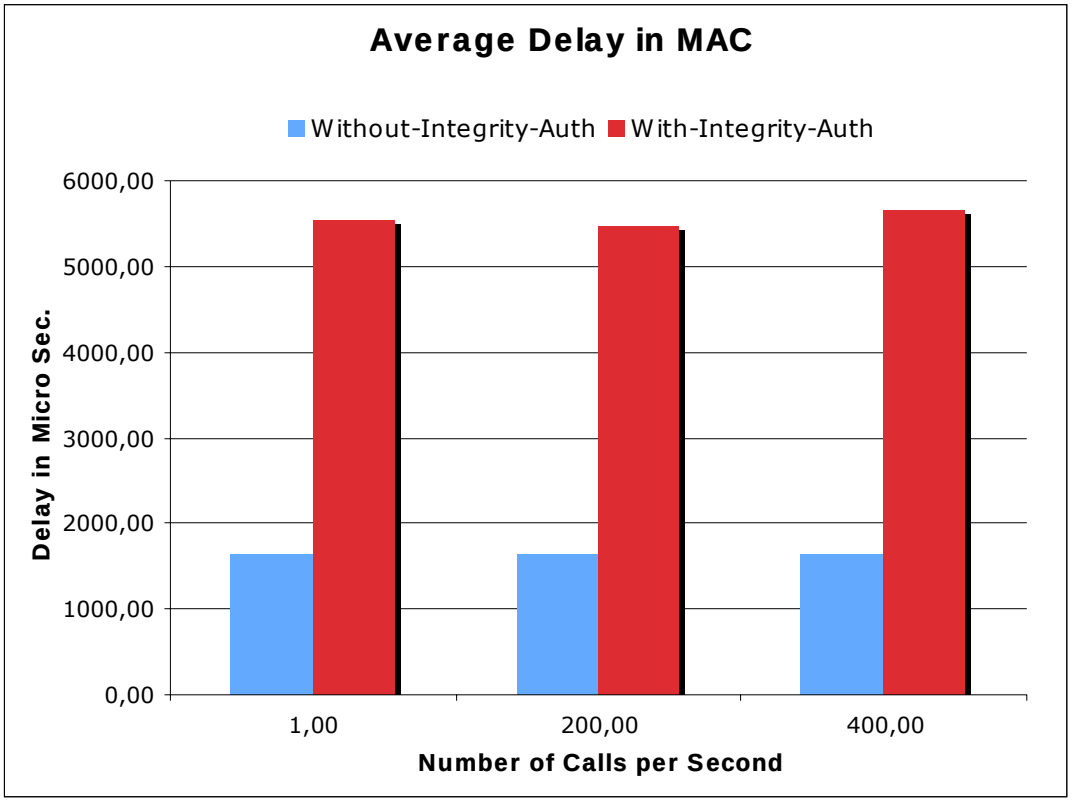
Παρατηρώντας τους χρόνους που έχουν καταγραφεί μπορεί να παρατηρηθεί ότι η μέση επεξεργαστική επιβάρυνση, στην περίπτωση που ο SIP πελάτης είχε εγκατασταθεί στο σύστημα Linux, ήταν της τάξης των 230 μικρο-δευτερολέπτων, ενώ στην περίπτωση που ο SIP πελάτης είχε εγκατασταθεί στο σύστημα MAC, ήταν της τάξης των 5000 μικρο-δευτερολέπτων (βλέπε Σχήμα 7–12 και Σχήμα 7–13 αντιστοίχως).

Δεδομένου ότι δεν υπήρξε καμία τροποποίηση των παραμέτρων των σεναρίων, η διαφορά που παρατηρήθηκε στους χρόνους οφείλεται αποκλειστικά και μόνο στα διαφορετικά χαρακτηριστικά (λειτουργικό σύστημα και επεξεργαστική ισχύ) των δύο συστημάτων. Επιπλέον, οι προγραμματίστηκες διεπαφές «pjsip» και «OpenSSL» που χρησιμοποιήθηκαν είναι βελτιστοποιημένες για συστήματα Linux, επηρεάζοντας (αρνητικά) την γενικότερη απόδοση του λογισμικού όταν χρησιμοποιείται σε άλλα συστήματα.

Σε ότι αφορά στους χρόνους επεξεργασίας που μετρήθηκαν για τα ενδιάμεσα στάδια, όπως αναμενόταν, διαφοροποιούνται και πάλι μεταξύ των δύο συστημάτων. Στην περίπτωση του Linux συστήματος ο μέσος χρόνος δημιουργίας ενός αιτήματος και επικύρωσης της απόκρισης είναι 120 και 100 μικρο-δευτερόλεπτα αντίστοιχα. Οι αντίστοιχοι ενδιάμεσοι χρόνοι στην περίπτωση του MAC συστήματος είναι 230 και 290 μικρο-δευτερόλεπτα, δηλαδή σχεδόν διπλάσιοι. Τα στατιστικά χαρακτηριστικά των μετρήσεων στα δύο διαφορετικά συστήματα παρουσιάζει ο Πίνακας 7–8 έως και ο Πίνακας 7–11 αντιστοίχως.



Σχήμα 7–12. Μέση Τιμή Καθυστέρησης που Εισάγεται στον SIP Πελάτη στο Σύστημα Linux



Σχήμα 7–13. Μέση Τιμή Καθυστέρησης που Εισάγεται στον SIP Πελάτη στο Σύστημα MAC

Στατιστική Παράμετρος	Σ1	Σ2	Σ3
Μέγιστο	183.00	317.00	407.00
Ελάχιστο	102.00	103.00	101.00
Μέση Τιμή	119.33	120.70	117.87
Τυπική Απόκλιση	9.15	10.95	11.65

Πίνακας 7–8. Στατιστικά Χαρακτηριστικά του SIP Πελάτη (στο Linux) για τη Δημιουργία Ενός Αιτήματος, για τα Σενάρια 1-3

Στατιστική Παράμετρος	Σ1	Σ2	Σ3
Μέγιστο	1363	154.00	259.00
Ελάχιστο	95.00	93.00	93.00
Μέση Τιμή	109.26	105.55	107.18
Τυπική Απόκλιση	40.88	7.13	18.10

Πίνακας 7–9. Στατιστικά Χαρακτηριστικά του SIP Πελάτη (στο Linux) για την Επικύρωση μιας Απόκρισης, για τα Σενάρια 1-3

Στατιστική Παράμετρος	Σ1	Σ2	Σ3
Μέγιστο	621.00	494.00	5741.00
Ελάχιστο	174.00	113.00	173.00
Μέση Τιμή	225.11	221.62	241.72
Τυπική Απόκλιση	42.02	37.00	182.69

Πίνακας 7–10. Στατιστικά Χαρακτηριστικά του SIP Πελάτη (στο MAC) για τη Δημιουργία Ενός Αιτήματος, για τα Σενάρια 1-3

Στατιστική Παράμετρος	Σ1	Σ2	Σ3
Μέγιστο	6632.00	3495.00	3934.00
Ελάχιστο	117.00	116.00	118.00
Μέση Τιμή	334.69	274.13	283.92
Τυπική Απόκλιση	594.76	345.11	402.97

Πίνακας 7–11. Στατιστικά Χαρακτηριστικά του SIP Πελάτη (στο Linux) για την Επικύρωση μιας Απόκρισης, για τα Σενάρια 1-3

Η επιβάρυνση που δέχονται οι εξυπηρέτες και, συνεπώς, η καθυστέρηση που εισάγουν στη διαδικασία, θεωρείται ελάχιστη αφού ο μέσος συνολικός χρόνος που απαιτείται για την επαλήθευση του αιτήματος και τη δημιουργία της απόκρισης είναι περίπου 120 μικρο-δευτερόλεπτα. Επιπλέον, δεδομένου ότι οι πληρεξούσιοι εξυπηρέτες είναι αφιερωμένα συστήματα συμπεραίνουμε ότι η καθυστέρηση που εισάγεται από τον εξυπηρέτη σε πραγματικά συστήματα θα είναι ακόμα μικρότερη.

Ο Πίνακας 7–12 και ο Πίνακας 7–13 απεικονίζουν τα στατιστικά χαρακτηριστικά, αναφορικά με την επιβάρυνση η οποία εισάγεται από τους πληρεξούσιους εξυπηρέτες, για την επικύρωση των αιτήσεων και την δημιουργία των αποκρίσεων.

Στατιστική Παράμετρος	Σ1	Σ2	Σ3
Μέγιστο	289	54	452
Ελάχιστο	54	39	37
Μέση Τιμή	64.40	46.50	44.15
Τυπική Απόκλιση	18.37	8.10	21.70

Πίνακας 7–12. Στατιστικά Χαρακτηριστικά του SIP Πληρεξούσιου Εξυπηρέτη για την Επικύρωση μιας Αίτησης

Στατιστική Παράμετρος	Σ1	Σ2	Σ3
Μέγιστο	293.00	63.92	237.00
Ελάχιστο	54.00	47.39	40.00
Μέση Τιμή	64.41	55.75	45.27
Τυπική Απόκλιση	13.45	8.72	10.75

Πίνακας 7–13. Στατιστικά Χαρακτηριστικά του SIP Πληρεξούσιου Εξυπηρέτη για την Δημιουργία μιας Απόκρισης

Συνοψίζοντας, ο προτεινόμενος μηχανισμός αποδεικνύεται μια αποδοτική λύση για την προστασία των υπηρεσιών διαδικτυακής τηλεφωνίας από επιθέσεις σηματοδοσίας, ακόμα και σε περιπτώσεις SIP πελατών που δεν αποδίδουν αποτελεσματικά σε συγκεκριμένα συστήματα. Ως τέτοια περίπτωση μπορεί να θεωρηθεί ο SIP πελάτης που εγκαταστάθηκε στο MAC σύστημα. Θεωρώντας την απόδοση του συγκεκριμένου συστήματος ως τη χειρότερη δυνατή, ο συνολικός χρόνος δεν αναμένεται να ξεπερνά τα 5.000 μικρο-δευτερόλεπτα. Να σημειωθεί ότι σε όλες τις μετρήσεις που παρουσιάστηκαν συμπεριλαμβάνεται, αναπόφευκτα, η επεξεργαστική επιβάρυνση που προκαλεί η διαδικασία καταγραφής.

7.3.5 Σύγκριση με εναλλακτικούς μηχανισμούς προστασίας

Στην ενότητα 6.3 παρουσιάστηκαν δυο εναλλακτικές προσεγγίσεις για την αντιμετώπιση των επιθέσεων σηματοδοσίας. Η μια αφορούσε μηχανισμούς που έχουν τη δυνατότητα αναγνώρισης επιθέσεων σηματοδοσίας, ενώ η δεύτερη νέα εναλλακτικά σχήματα αυθεντικοποίησης τα οποία, μεταξύ των άλλων, παρέχουν υπηρεσίες προστασίας από επιθέσεις σηματοδοσίας. Ο Πίνακας 7–14 καθώς και ο Πίνακας 7–15 αντιστοίχως συνοψίζουν και συγκρίνουν τις παρεχόμενες υπηρεσίες ασφάλειας και την ικανότητα προστασίας από επιθέσεις, του προτεινόμενου και άλλων σχετικών μηχανισμών (λεπτομέρειες αναφορικά με τον τρόπο λειτουργίας του κάθε μηχανισμού παρατίθενται στην ενότητα 6.3).

	Σχετικοί Μηχανισμοί									
Υπηρεσίας-Ασφάλειας	[100]	[101]	[113]	[105]	[98]	[99]	[107]	[110]	[111]	Προτεινόμενος
Ακεραιότητα	Όχι	Όχι	Όχι	Όχι	Μερικώς[5]	Όχι	Ναι	Όχι	Μερικώς	Ναι
Αυθεντικότητα	Όχι	Όχι	Όχι	Όχι	Μερικώς	Ναι	Ναι	Ναι	Ναι	Ναι
Εμπιστευτηκότητα	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι	Όχι	Ναι	Όχι	Όχι
Μη αποποίηση	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
Αμοιβαία Αυθεντικοποίηση	Όχι	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι

Πίνακας 7–14. Σύγκριση με τις Υποστηριζόμενες Υπηρεσίες Ασφάλειας Σχετικών Μηχανισμών

	Σχετικοί Μηχανισμοί									
	[100]	[101]	[113]	[105]	[98]	[99]	[107]	[110]	[111]	Προτεινόμενος
Επιθέσεις Επανάληψης	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Όχι	Ναι
Επιθέσεις Σηματοδοσίας	Μερικώς	Μερικώς	Μερικώς	Μερικώς	Μερικώς	Μερικώς	Ναι	Μερικώς	Όχι	Ναι
Επιθέσεις Ενδιάμεσου	Όχι	Όχι	Όχι	Όχι	Μερικώς	Μερικώς	Ναι	Μερικώς	Όχι	Ναι

Πίνακας 7–15. Σύγκριση με την Ικανότητα Αντιμετώπισης Επιθέσεων Σχετικών Μηχανισμών

[5] Με τον όρο "Μερικώς" καλύπτονται περιπτώσεις κατά τις οποίες δεν παρέχονται ολοκληρωμένες υπηρεσίες ασφάλειας και προστασίας (π.χ προστασία μόνο των αποκρίσεων από μη εξουσιοδοτημένη τροποποίησης).

Παρατηρώντας τους δύο παραπάνω πίνακες διαπιστώνεται ότι ο μοναδικός μηχανισμός, πέραν του προτεινόμενου, που παρέχει πλήρη προστασία από επιθέσεις σηματοδοσίας περιγράφεται στην εργασία [107]. Βέβαια, δεδομένου ότι για το συγκεκριμένο μηχανισμό δεν έχει γίνει κάποια πειραματική υλοποίηση, δεν είναι εφικτή η σύγκριση της αποδοτικότητας του με αυτή του προτεινόμενου μηχανισμού.

Τέλος, είναι σημαντικό να τονιστεί ότι ο μοναδικός μηχανισμός που μελετήθηκε σε πειραματικό περιβάλλον και μετρήθηκε η επιβάρυνση που εισάγει στην υπηρεσία, είναι αυτός που περιγράφεται στην εργασία [110]. Ο μέσος χρόνος μέχρι τη λήψη της αρχικής απόκρισης είναι της τάξης των 110 μιλι-δευτερολέπτων, ο οποίος είναι πολύ μεγαλύτερος της αντίστοιχης μέσης απόδοσης του προτεινόμενου μηχανισμού.

7.4 Προστασία από επιθέσεις μη συμβατών μηνυμάτων

Η επεξεργασία μη ορθών συντακτικά μηνυμάτων (δηλαδή μηνυμάτων μη συμβατών με την οριζόμενη από το SIP γραμματική) μπορεί να οδηγήσει, όπως αναλύεται λεπτομερώς στην ενότητα 4.4.2, στις παρακάτω μη επιθυμητές καταστάσεις:

1. Μη σταθερή λειτουργία.
2. Μη εξουσιοδοτημένη πρόσβαση.
3. Άρνηση παροχής υπηρεσίας.

Για να διασφαλιστεί η αξιοπιστία της παρεχόμενης υπηρεσίας όλα τα εισερχόμενα μηνύματα θα πρέπει να ελέγχονται ως προς την ορθότητα τους.

7.4.1 Περιγραφή Μηχανισμού Προστασίας

Η βασική ιδέα για την ανάπτυξη του κατάλληλου μηχανισμού προστασίας των αναλυτών μηνυμάτων (parsers) από μη συμβατά μηνύματα, προέρχεται από τη γραμματική του πρωτοκόλλου σηματοδοσίας SIP. Παρ' όλα αυτά, ανάλογες περιγραφές είναι δυνατόν να αναπτυχθούν και για τα άλλα πρωτόκολλα σηματοδοσίας που αξιοποιούνται στη διαδικτυακή τηλεφωνία.

Οποιοδήποτε εισερχόμενο-εξερχόμενο μήνυμα δεν συμμορφώνεται με την γραμματική του SIP [11] θα πρέπει να χαρακτηρίζεται ως μη συμβατό και να απορρίπτεται. Εξαιτίας του ότι ο χαρακτηρισμός αυτός βασίζεται στην γραμματική του πρωτοκόλλου σηματοδοσίας, η οποία ακολουθεί μια αυστηρά προκαθορισμένη δομή, οι επιθέσεις αυτού του τύπου μπορούν να αναγνωριστούν αξιοποιώντας κατάλληλες υπογραφές επιθέσεων (attack signatures). Οι υπογραφές αυτές, στη περίπτωση του SIP, αποτελούνται από δύο επίπεδα. Στο πρώτο επίπεδο πραγματοποιούνται γενικοί έλεγχοι, οι οποίοι εφαρμόζονται σε οποιοδήποτε μήνυμα σηματοδοσίας ανεξαρτήτως της μεθόδου που αξιοποιεί. Στο δεύτερο επίπεδο καθορίζονται επιπρόσθετοι κανόνες οι οποίοι εφαρμόζονται σε συγκεκριμένα μηνύματα, ανάλογα με τη μέθοδο που αξιοποιείται. Η γενική δομή των υπογραφών αυτών απεικονίζεται στο Σχήμα 7–14.

```
SIP_METHOD SIP-URI | SIPS-URI MESSAGE HEADER+
[MESSAGE_BODY]

Επιπρόσθετοι Κανόνες (additional rules)
SIP_METHOD!=NULL
MESSAGE_HEADER!=NULL
size_of(SIP_METHOD)>%constant% e.g 50 bytes
size_of(MESSAGE_BODY)>%constant%
```

Σχήμα 7–14. Γενική Δομή Υπογραφών Επιθέσεων μη Συμβατών Μηνυμάτων

Οι πρώτες δύο γραμμές της υπογραφής του παραπάνω σχήματος, αντιστοιχούν στο πρώτο επίπεδο. Εδώ προσδιορίζεται η γενική μορφή ενός SIP μηνύματος, δηλαδή ότι ένα μήνυμα αποτελείται από τη μέθοδο ακολουθούμενη από τον αντίστοιχο προσδιοριστή του αιτούμενου πόρου και τις υποχρεωτικές κεφαλίδες όπως αυτές ορίζονται στις προδιαγραφές του SIP [11]. Η ύπαρξη σώματος μηνύματος είναι προαιρετική και η χρήση της εξαρτάται κάθε φορά από τη μέθοδο του μηνύματος. Το υπόλοιπο τμήμα της υπογραφής αντιστοιχεί στο δεύτερο επίπεδο. Εδώ περιγράφονται οι επιπρόσθετοι κανόνες για τον εντοπισμό μη συμβατών μηνυμάτων. Πιο συγκεκριμένα, σύμφωνα με το Σχήμα 7–14, οι επιπρόσθετοι κανόνες περιγράφουν τους ακόλουθους περιορισμούς:

- Κανένα SIP μήνυμα δεν πρέπει να έχει τα πεδία μεθόδου και κεφαλίδων με κενές τιμές (null values).
- Το μήκος του μηνύματος δεν θα πρέπει να υπερβαίνει ένα προκαθορισμένο όριο.

Η χρήση των υπογραφών επιθέσεων για την αναγνώριση μη συμβατών SIP μηνυμάτων παρέχουν τη δυνατότητα ενσωμάτωσης του προτεινόμενου μηχανισμού στην υπάρχουσα υποδομή του SIP. Εναλλακτικά, σε περίπτωση που αυτό δεν είναι εφικτό, θα μπορούσαν να συμπεριληφθούν σε κάποιο σύστημα αναγνώρισης επιθέσεων όπως το SNORT [129], BRO [136] και άλλα, χωρίς να απαιτείται καμία μετατροπή στην αρχιτεκτονική του SIP.

Υπάρχουν περιπτώσεις μη συμβατών μηνυμάτων τα οποία λόγω του ότι είναι «ορθώς» δομημένα δεν είναι δυνατόν να ανιχνευθούν μέσω των γενικών υπογραφών. Για το λόγω αυτό θα πρέπει να αναπτυχθούν ειδικές υπογραφές για κάθε SIP μέθοδο. Για παράδειγμα, σύμφωνα με τις προδιαγραφές του SIP ένα μήνυμα SIP INVITE πρέπει να συμπεριλαμβάνει εκτός από τις υποχρεωτικές κεφαλίδες (From,To, κτλ) κάποιες επιπρόσθετες, όπως το «Content-Type», οι οποίες όμως δεν απαιτούνται σε όλα τα μηνύματα. Σε περίπτωση λοιπόν, όπου ένα εισερχόμενο SIP INVITE μήνυμα δεν συμπεριλαμβάνει την κεφαλίδα Content-Type θα πρέπει να χαρακτηρισθεί ως μη συμβατό και να απορριφθεί πριν πραγματοποιηθεί οποιαδήποτε περαιτέρω επεξεργασία του. Σε διαφορετική περίπτωση, ο αναλυτής μηνυμάτων θα προσπαθήσει να εντοπίσει τις προαναφερόμενες κεφαλίδες, που όμως δεν υπάρχουν, οδηγώντας τον σε πιθανή κατάρρευση (crash). Ένα τέτοιο παράδειγμα υπογραφής για ένα SIP INVITE μήνυμα απεικονίζεται στο Σχήμα 7–15.

```
INVITE_METHOD SIP-URI | SIPS-URI MESSAGE HEADER+
MESSAGE HEADER =Via | Max-Forwards | From* |To* | Call-Id*
                        CSeq* | Contact* |User-agent
                                |Authorization |Event |Content-Length*
                        |Content-type*|Record-Route
INVITE_METHOD="INVITE" | %x49.4E.56.49.54.45
MESSAGE_BODY
Επιπρόσθετοι κανόνες (additionall rules)
%Content-Length% >0
%Content-Length%==size_of(MESSAGE_BODY)
(*)Υποχρεωτικά πεδία (mandatory fields)
```

Σχήμα 7–15. Παράδειγμα Υπογραφής INVITE Μηνύματος

Με τον ίδιο ακριβώς τρόπο μπορούν να προσδιοριστούν εξειδικευμένες υπογραφές για όλα τα μηνύματα του SIP. Για παράδειγμα, σε αντίθεση με τα μηνύματα SIP INVITE τα μηνύματα SIP REGISTER δεν απαιτούν την χρήση της κεφαλίδα «Content-Type».

Σε ειδικές περιπτώσεις, όπως στην επίθεση έγχυσης κώδικα SQL (βλέπε ενότητα 4.4.3), δεν απαιτείται μόνο ο έλεγχος της σύνταξης του μηνύματος αλλά και η εξέταση των δεδομένων που συμπεριλαμβάνονται σε κάποιες κεφαλίδες. Αναλυτικότερα, στις περιπτώσεις αυτές τα δεδομένα που μεταφέρονται στην κεφαλίδα «Authorization» θα πρέπει να ελέγχονται ως προς το περιεχόμενο τους. Υπό αυτό το πρίσμα, οι υπογραφές επιθέσεων μη συμβατών μηνυμάτων θα πρέπει να επεκταθούν ώστε να πραγματοποιούνται οι κατάλληλοι έλεγχοι και στα δεδομένα της κεφαλίδας «Authorization». Μια τέτοιου τύπου υπογραφή θα ελέγχει τόσο την ορθότητα της σύνταξης της κεφαλίδας όσο και των δεδομένων της. Συγκεκριμένα, για να εντοπιστούν επιθέσεις έγχυσης κώδικα SQL θα πρέπει να ελέγχονται τα πεδία «όνομα χρήστη» (user-name) και «τομέας» (realm). Στο Σχήμα 7–16. απεικονίζεται η αντίστοιχη υπογραφή.

```
INVITE_METHOD SIP-URI | SIPS-URI MESSAGE HEADER+
MESSAGE HEADER =Via | Max-Forwards | From* |To* | Call-Id*
                        CSeq* | Contact* |User-agent
                                |Authorization |Event |Content-Length*
                        |Content-type*|Record-Route
INVITE_METHOD="INVITE" | %x49.4E.56.49.54.45
MESSAGE_BODY
Επιπρόσθετοι κανόνες (additionall rules)
%Content-Length% >0
%Content-Length%==size_of(MESSAGE_BODY)
(*)Υποχρεωτικά πεδία (mandatory fields)
```

Σχήμα 7–16. Περιγραφή Υπογραφής για Ανίχνευση Επίθεσης Έγχυσης Κώδικα SQL

7.4.2 Βελτιώνοντας τη Ρωμαλεότητα των Αναλυτών Μηνυμάτων στο SIP

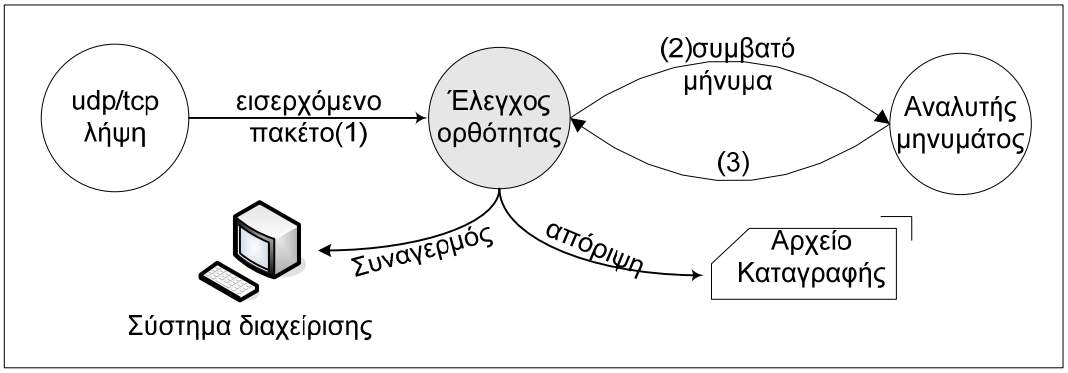
Για να ενισχυθεί, λοιπόν, η αξιοπιστία και ρωμαλεότητα των SIP εξυπηρετών, θα πρέπει να αναπτυχθεί ο κατάλληλος μηχανισμός για την ενσωμάτωση των προαναφερόμενων (βλέπε ενότητα 7.4.1) «υπογραφών επιθέσεων». Όπως αναφέρεται στις προδιαγραφές του SIP [11], η συντακτική εγκυρότητα των μηνυμάτων θα πρέπει να προηγείται οποιασδήποτε επεξεργασίας. Συγκεκριμένα, αναφέρονται τα ακόλουθα: *«The request MUST be well-formed enough to be handled with a server transaction. Any components involved in the remainder of these Request Validation steps or the Request Forwarding section MUST be well-formed. Any*

other components, well-formed or not, SHOULD be ignored and remain unchanged when the message is forwarded».

Όμως, όπως παρουσιάζεται αναλυτικά και στην ενότητα 4.4.2, οι προβλεπόμενοι έλεγχοι δεν είναι αρκετοί, καθιστώντας τους SIP εξυπηρέτες ευεπίφορους σε επιθέσεις μη συμβατών μηνυμάτων. Για το λόγο αυτό είναι απαραίτητο η ορθότητα του μηνύματος να ελέγχεται πριν αυτό προωθηθεί για περαιτέρω επεξεργασία. Στην περίπτωση που κάποιο μήνυμα ταυτίζεται με κάποια από τις προσδιοριζόμενες υπογραφές, θεωρείται μη συμβατό και απορρίπτεται.

Στο Σχήμα 7–17 απεικονίζονται οι τροποποιήσεις, σε σχέση με το αρχικό σύστημα επεξεργασίας (βλέπε ενότητα 3.2), που πρέπει να πραγματοποιηθούν στους εξυπηρέτες SIP. Το προτεινόμενο φίλτρο προστασίας από μη συμβατά μηνύματα μπορεί να ενσωματωθεί σε κάποιο ανάχωμα ασφαλείας (firewall) που αναγνωρίζει το πρωτόκολλο σηματοδοσίας SIP. Ανεξάρτητα από τον τύπο του συστήματος που θα ενσωματώνει το φίλτρο ελέγχου, αυτό θα πρέπει να «γνωρίζει» τις υπογραφές που παρουσιάστηκαν στην ενότητα 7.4.1 και οι οποίες βασίζονται σε κανονικές εκφράσεις (regular expressions). Οι έλεγχοι που διενεργούνται από το προτεινόμενο φίλτρο χωρίζονται σε τρεις διαφορετικές φάσεις:

1. Φάση Ελέγχων Πρώτης Γραμμής.
2. Φάση Ελέγχων Κεφαλίδων.
3. Φάση Εξειδικευμένων Ελέγχων.



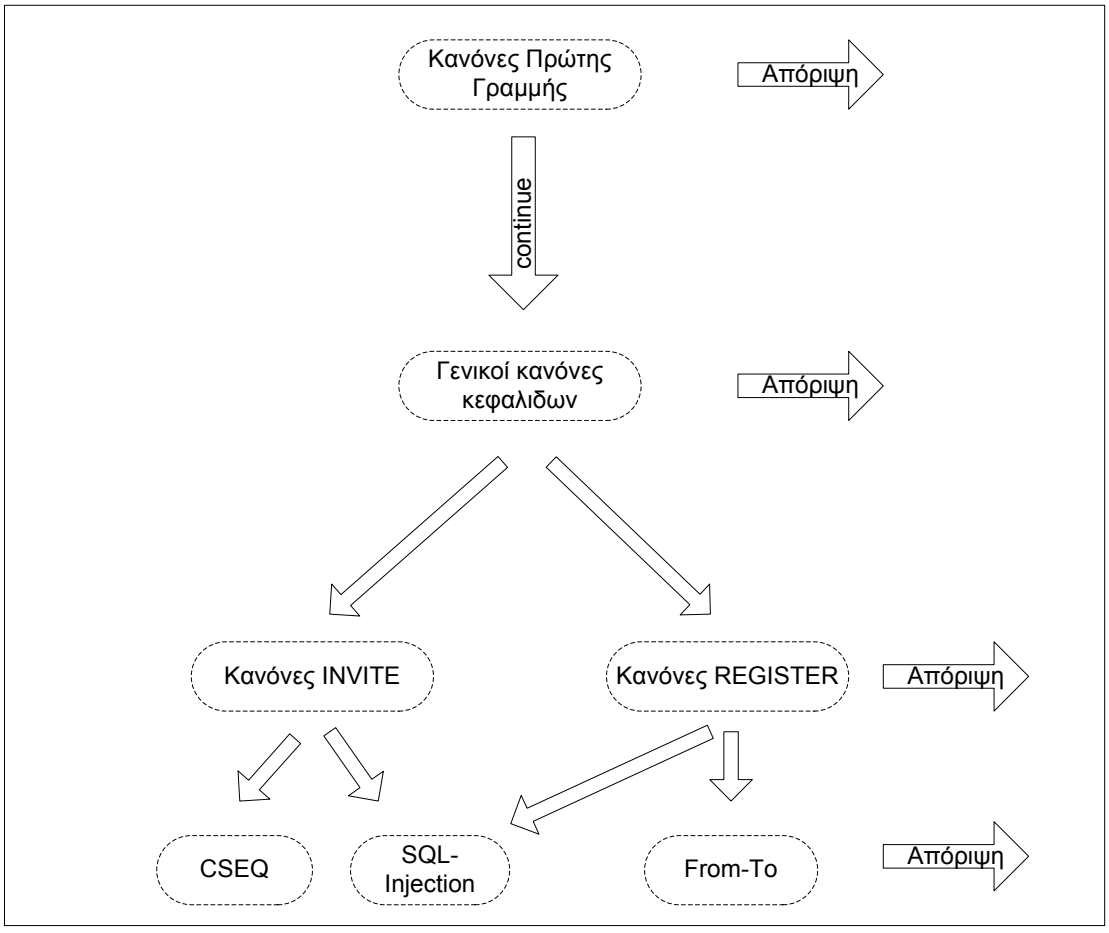
Σχήμα 7–17. Αρχιτεκτονική Τροποποιημένου SIP Αναλυτή Μηνυμάτων

Οι δύο πρώτες φάσεις αντιστοιχούν στο πρώτο επίπεδο υπογραφών επιθέσεων, ενώ η τρίτη φάση αντιστοιχεί στο δεύτερο επίπεδο. Σε οποιαδήποτε φάση των ελέγχων αναγνωριστεί ένα μήνυμα ως μη συμβατό, απορρίπτεται και η επεξεργασία του τερματίζεται. Θα πρέπει να σημειωθεί ότι στους εξειδικευμένους ελέγχους, μεταξύ των άλλων, πραγματοποιούνται και έλεγχοι που αξιοποιούν αποτελέσματα των δύο πρώτων φάσεων, όπως περιγράφεται παρακάτω.

Κάθε εισερχόμενο μήνυμα αρχικά ελέγχεται για την ορθότητα της πρώτης γραμμής του. Σε περίπτωση που το μήνυμα βρεθεί να είναι συμβατό ελέγχεται η ορθότητα των κεφαλίδων. Αν και αυτοί οι έλεγχοι ολοκληρωθούν επιτυχώς, πραγματοποιούνται οι έλεγχοι της τρίτης φάσης κατά τη διάρκεια των οποίων εφαρμόζονται οι κανόνες που αφορούν στο συγκεκριμένο τύπο του μηνύματος, όπως αυτός έχει αναγνωριστεί στην πρώτη φάση. Για παράδειγμα, τα μηνύματα SIP INVITE και SIP REGISTER διαφοροποιούνται σε ότι αφορά το σώμα μηνύματος. Συγκεκριμένα, τα μηνύματα SIP INVITE συμπεριλαμβάνουν σώμα μηνύματος, ενώ τα SIP REGISTER όχι. Συνεπώς, σε περίπτωση που εντοπισθεί ένα μήνυμα SIP REGISTER με σώμα μηνύματος θα πρέπει να χαρακτηριστεί ως μη συμβατό και να απορριφθεί.

Επιπλέον, στη φάση των εξειδικευμένων ελέγχων εντοπίζονται πιθανά λογικά λάθη. Με τον όρο «λογικά λάθη» νοούνται περιπτώσεις πλήρως συμβατών μηνυμάτων τα οποία όμως περιέχουν μη ορθές αναφορές. Για παράδειγμα, όταν ληφθεί ένα μήνυμα SIP INVITE, σύμφωνα με τις προδιαγραφές του SIP η κεφαλίδα CSEQ πρέπει να έχει την ακόλουθη σύνταξη: «CSEQ προσδιοριστής INVITE». Υπό το πρίσμα αυτό ένας κακόβουλος χρήστης μπορεί να αποστείλει ένα μήνυμα SIP INVITE στο οποίο η κεφαλίδα CSEQ να έχει τη μορφή: «CSEQ προσδιοριστής REGISTER». Αν και τα δεδομένα που συμπεριλαμβάνονται στη συγκεκριμένη κεφαλίδα είναι συντακτικά ορθά, στο μήνυμα υπάρχει μη λογική αναφορά αφού στη θέση του REGISTER θα έπρεπε να υπάρχει INVITE. Δεδομένου ότι η περαιτέρω επεξεργασία ενός τέτοιου μηνύματος μπορεί να δημιουργήσει αστάθειες στη λειτουργία του αναλυτή μηνυμάτων, θα πρέπει να απορριφθεί. Τέλος, εξίσου σημαντικοί είναι και οι έλεγχοι που πραγματοποιούνται για τον εντοπισμό κακόβουλου κώδικα στα δεδομένα των μηνυμάτων.

Εν συντομία η παραπάνω διαδικασία ελέγχων αποτυπώνεται στο Σχήμα 7–18.



Σχήμα 7–18. Διαδικασία Ελέγχων για τον Εντοπισμό μη Συμβατών SIP Μηνυμάτων

7.4.3 Θέματα Υλοποίησης του Προτεινόμενου Μηχανισμού Αναγνώρισης Μη Συμβατών Μηνυμάτων

Στα κλασικά συστήματα ανίχνευσης, όπως για παράδειγμα αυτό του SNORT [129], η αναγνώριση και αντιμετώπιση των περιστατικών ασφαλείας προϋποθέτει την περιγραφή τους υπό μορφή «υπογραφών επιθέσεων». Για παράδειγμα, στην περίπτωση επιθέσεων μη συμβατών μηνυμάτων, θα πρέπει να γίνει ακριβής καταγραφή όλων των μηνυμάτων που μπορεί να αποστείλει ένας κακόβουλος χρήστης. Κάτι τέτοιο θεωρείται ανέφικτο, αφού οι

πιθανοί συνδυασμοί μη συμβατών μηνυμάτων είναι άπειροι. Κατά συνέπεια ο προτεινόμενος μηχανισμός ακολουθεί την ακριβώς αντίθετη προσέγγιση, δηλαδή ότι: οποιοδήποτε μήνυμα δεν συμμορφώνεται με τη γενική γραμματική του SIP θα πρέπει να απορρίπτεται. Συνεπώς, κατά την εφαρμογή του προτεινόμενου μηχανισμού δεν απαιτείται η περιγραφή όλων των πιθανών μη συμβατών μηνυμάτων, αλλά μόνο η γενική περιγραφή των συμβατών μηνυμάτων.

Οι υπογραφές που προσδιορίζονται από το διαχειριστή μιας υπηρεσίας διαδικτυακής τηλεφωνίας, αποθηκεύονται σε κάποια βάση δεδομένων στην οποία πρόσβαση έχουν όλες οι εμπλεκόμενες δικτυακές οντότητες SIP. Η αναπαράσταση των υπογραφών γίνεται μέσω κανονικών εκφράσεων που ακολουθούν τη σύνταξη Perl Compiled Regular Expression (PCRE) [130]. Για την αποφυγή περαιτέρω επιβάρυνσης κατά τη διάρκεια της επεξεργασίας των εισερχόμενων μηνυμάτων, αναπτύχθηκαν κανονικές εκφράσεις για την πρώτη γραμμή (*FIRST LINE*) καθώς και για τις περισσότερο συχνά εμφανιζόμενες κεφαλίδες (*CSEQ, FROM, TO, VIA, CONTACT ,AUTHORIZATION*). Η αναπαράσταση για την πρώτη γραμμή απεικονίζεται στο Σχήμα 7–19, η οποία και συμπεριλαμβάνει τις περισσότερο συχνές μεθόδους SIP όπως *INVITE, SUBSCRIBE, OPTIONS, CANCEL, ACK* και *REGISTER*. Στην περίπτωση που ο διαχειριστής της παρεχόμενης υπηρεσίας χρειάζεται να εισάγει μια νέα μέθοδο μπορεί εύκολα να ενημερώσει την αντίστοιχη υπογραφή προσθέτοντας το όνομα της νέας μεθόδου.

```
^\s*(INVITE|SUBSCRIBE|OPTIONS|CANCEL|ACK|REGISTER)\s+
((((\d{1,3}[.]){3,3}\d{1,3}(\:\d{1,5}))|((sip:){1}\s*\w+@(\w+[.])+\w+)|
((sip:){1}\s*(\w+[.])+\w+)))\s+(SIP[/]\d[.]\d)\s*
```

Σχήμα 7–19. Υπογραφή Αναγνώρισης SIP Μηνυμάτων με Συμβατή την Πρώτη Γραμμή

Όσον αφορά τους αντίστοιχους ελέγχους που πραγματοποιούνται για τις κεφαλίδες των μηνυμάτων, οι κανονικές εκφράσεις που υλοποιήθηκαν παρουσιάζονται στο Σχήμα 7–20.

```
CSEQ: ^\s*(CSeq:)\s*\d+\s+\b($utilized_method)\b\s*$

Authorization:^\s*(Authorization:)\s*((Digest\s+username[=]\s*["](\w|\s|['][;])+["]\s*[,]))\s+
                    (realm[=]\s*["]((\w+[.])+\w+)["])(.*)(\w|\S|\s)+(update|insert|delete|union)(.*)

FROM:^\s*(From:)\s*(["]*(\w+\s*\w*)*["]*\s+((<)*(sip:)((\w+@(\w+[.])+\w+)|(((\d{1,3}[.]){3,3}\d{1,3}))(>)*))\s*

TO:^\s*(TO:)\s*(["]*(\w+\s*\w*)*["]*\s+((<)*(sip:)((\w+@(\w+[.])+\w+)|(((\d{1,3}[.]){3,3}\d{1,3}))(>)*))\s*

Via:^\s*(Via:)\s*(SIP[/]\s*\d[.]\d\s*[/]\s*(\w+)\s+(\w+[.])+\w+((\s*[:]\d+)*)(\s*[;]\s*\w+[=]\w+)*)\s*

Contact:^\s*(Contact:)\s*(["]*(\w+\s*\w*)*["]*\s+((<)*(sip:)((\w+@(\w+[.])+\w+)|
                (((\d{1,3}[.]){3,3}\d{1,3}):\d{1,5}))(>)*)).+\s*
```

Σχήμα 7–20. Υπογραφές Αναγνώρισης SIP Μηνυμάτων με Συμβατές Κεφαλίδες

7.4.4 Αξιολόγηση Απόδοσης του Προτεινόμενου Μηχανισμού Αναγνώρισης Μη Συμβατών SIP Μηνυμάτων

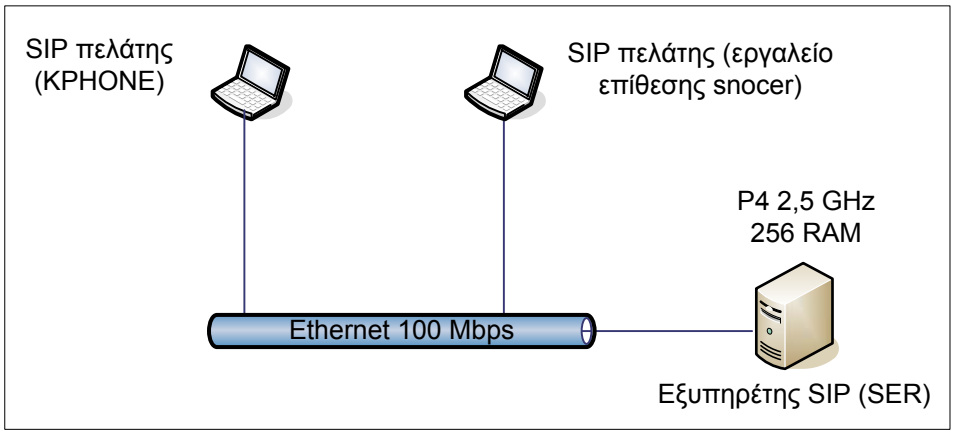
Στο Σχήμα 7–21 απεικονίζεται το πειραματικό περιβάλλον που αναπτύχθηκε για την αξιολόγηση του προτεινόμενου μηχανισμού αναγνώρισης μη συμβατών μηνυμάτων. Συγκεκριμένα η αρχιτεκτονική απαρτίζεται από τις ακόλουθες οντότητες:

- SIP Πελάτες:
  1. KPHONE [131].

2. SIPBobmer [132], γεννήτορας μη συμβατών μηνυμάτων βασισμένος στο σύστημα ελέγχων PROTOS [64].
3. Εξειδικευμένος γεννήτορας πολύπλοκών μη συμβατών μηνυμάτων [21].

- SIP Εξυπηρέτες:
  1. SIP Express Router (SER) [77].

Για την αναγνώριση των μη συμβατών μηνυμάτων τροποποιήθηκε ο πυρήνας του SIP εξυπηρέτη (SER) έτσι ώστε να μπορεί να αξιοποιήσει τις διαθέσιμες υπογραφές. Ο εξυπηρέτης διέθετε επεξεργαστή Pentium 4 στα 2.5 GHz, 256 MB μνήμης RAM και δικτυακή σύνδεση με ονομαστική ταχύτητα 100Mbps.



Σχήμα 7–21. Πειραματικό Περιβάλλον που Αξιοποιήθηκε για την Αξιολόγηση του Προτεινόμενου Μηχανισμού Προστασίας από Μη Συμβατά Μηνύματα

Το παραπάνω πειραματικό περιβάλλον αξιοποιήθηκε τόσο για τον έλεγχο της αποτελεσματικότητας του προτεινόμενου μηχανισμού, όσο και για την αξιολόγηση της απόδοσης του, αναφορικά με την επεξεργαστική επιβάρυνση που εισάγει. Να τονιστεί ότι όλοι οι χρόνοι που παρουσιάζονται στην ενότητα αυτή αποτυπώνουν πάντα τη χειρότερη δυνατή κατάσταση αφού, σκόπιμα, τα μηνύματα δεν απορρίπτονται μόλις εντοπιστεί κάποιο λάθος. Αντίθετα, συνεχίζεται η επεξεργασία τους μέχρι την ολοκλήρωση όλων των ελέγχων, όπως συμβαίνει στην περίπτωση των συμβατών μηνυμάτων.

Ο Πίνακας 7–16 περιγράφει συνοπτικά τα σενάρια που υλοποιήθηκαν για τον πειραματικό έλεγχο του μηχανισμού. Ο ρυθμός δημιουργίας/αποστολής αιτήσεων για το σενάριο 1 ήταν δύο αιτήσεις ανά δευτερόλεπτο, ενώ για όλα τα υπόλοιπα σενάρια ο ρυθμός ήταν 20 αιτήσεις ανά δευτερόλεπτο.

Θα πρέπει να σημειωθεί ότι στα σενάρια 1 έως 4 δε συμπεριλαμβάνονται έλεγχοι για την ορθότητα της κεφαλίδας «Authorization» και συνεπώς δεν αναγνωρίζονται επιθέσεις έγχυσης κώδικα SQL, σε αντίθεση με τα υπόλοιπα που συμπεριλαμβάνουν το σύνολο των απαραίτητων ελέγχων. Η παραπάνω διαφοροποίηση έχει γίνει για να εκτιμηθεί η επεξεργαστική επιβάρυνση που εισάγεται από τους επιπρόσθετους αυτούς ελέγχους. Όλα τα σενάρια, εκτός των ελέγχων για τη συντακτική ορθότητα των μηνυμάτων, ελέγχουν την ύπαρξη λογικών λαθών αλλά και τη μοναδικότητα συγκεκριμένων κεφαλίδων όπως «From, To».

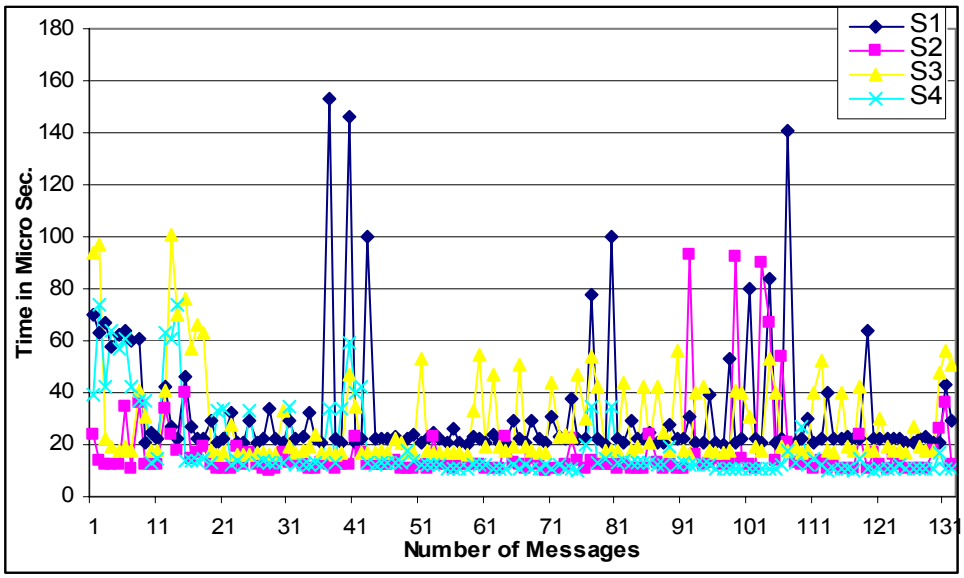
Αναφορικά με την αποτίμηση της αποτελεσματικότητας του προτεινόμενου μηχανισμού, σε κανένα από τα σενάρια που πραγματοποιήθηκαν δεν παρουσιάστηκαν λανθασμένοι συναγερμοί (false alarm). Συγκεκριμένα, όλα τα εισερχόμενα μη συμβατά SIP μηνύματα ανιχνεύθηκαν επιτυχώς, ενώ κανένα συμβατό μήνυμα δεν χαρακτηρίσθηκε, λανθασμένα, ως

μη συμβατό. Η μη ύπαρξη λανθασμένων θετικών συναγερμών (false positives alarms) οφείλεται στο γεγονός ότι το KPHONE [131] που αξιοποιήθηκε για τη δημιουργία συμβατών μηνυμάτων συμμορφώνεται πλήρως με τις προδιαγραφές του RFC 3261 [11]. Βέβαια, υπάρχει πάντα η πιθανότητα ένα συμβατό μήνυμα να χαρακτηρισθεί λανθασμένα ως μη συμβατό. Για παράδειγμα, αν ένας SIP πελάτης εισάγει στα μηνύματα που δημιουργεί κάποιο ιδιαίτερο χαρακτηριστικό που δε συμπεριλαμβάνεται στις υπογραφές, τα μηνύματα του θα χαρακτηρίζονται ως μη συμβατά. Τέτοιες περιπτώσεις μπορούν να καλυφθούν ενημερώνοντας τη βάση υπογραφών. Βέβαια, θα πρέπει να σημειωθεί ότι τα μηνύματα αυτά δεν συμμορφώνονται πλήρως με τις προδιαγραφές του SIP.

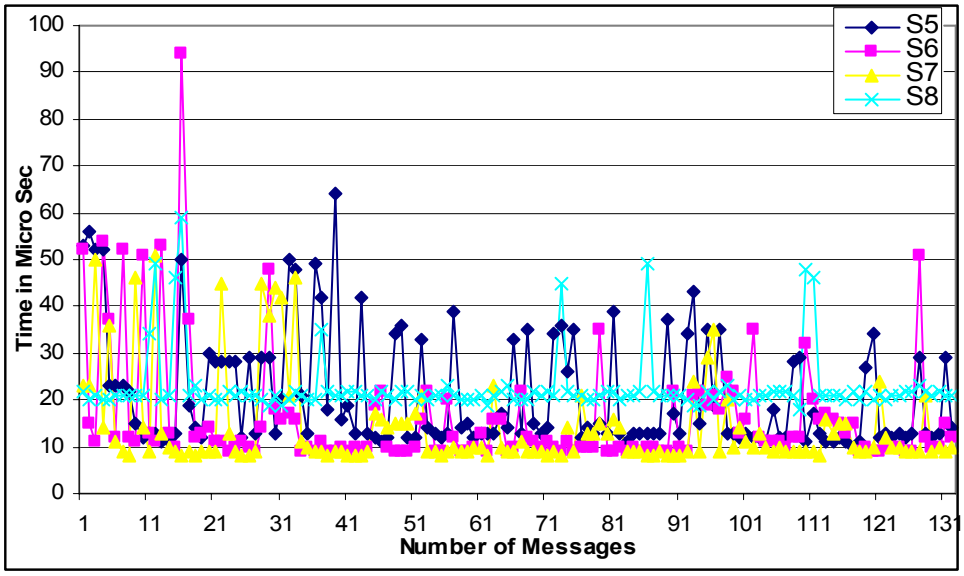
Αριθμός Σεναρίου	**Περιγραφή Σεναρίου**
Σενάριο 1 (S1)	Σε αυτό το σενάριο αξιοποιήθηκε ο γεννήτορας μη συμβατών μηνυμάτων SIPBomber, αποστέλλοντας δύο μηνύματα ανά δευτερόλεπτο.
Σενάριο 2 (S2)	Σε αυτό το σενάριο αξιοποιήθηκε ο εξειδικευμένος γεννήτορας, για τη δημιουργία (μη συμβατών) μηνυμάτων με λάθη σε μία μόνο κεφαλίδα και μόνο
Σενάριο 3 (S3)	Σε αυτό το σενάριο αξιοποιήθηκε ο εξειδικευμένος γεννήτορας για τη δημιουργία (μη συμβατών) μηνυμάτων με λάθη στην πρώτη γραμμή και μόνο.
Σενάριο 4 (S4)	Σε αυτό το σενάριο αξιοποιήθηκε το *KPHONE* για τη δημιουργία συμβατών μηνυμάτων.
Σενάριο 5 (S5)	Σε αυτό το σενάριο αξιοποιήθηκε ο εξειδικευμένος γεννήτορας για τη δημιουργία συμβατών μηνυμάτων.
Σενάριο 6 (S6)	Σε αυτό το σενάριο αξιοποιήθηκε ο εξειδικευμένος γεννήτορας για τη δημιουργία (μη συμβατών) μηνυμάτων με λάθη σε μια από τις ακόλουθες κεφαλίδες: *From, To, Via, CSeq*.
Σενάριο 7 (S7)	Το σενάριο αυτό είναι αντίστοιχο με το Σενάριο 6, με τη διαφορά ότι η κεφαλίδα authorization εμπεριέχει κώδικα SQL.
Σενάριο 8 (S8)	Στο σενάριο αυτό αξιοποιήθηκε ο εξειδικευμένος γεννήτορας για τη δημιουργία συμβατών μηνυμάτων, τα οποία συμπεριλαμβάνουν την κεφαλίδα *Authorization*.

Πίνακας 7–16. Σενάρια που Υλοποιήθηκαν για την Αξιολόγηση του Μηχανισμού Αναγνώρισης Μη Συμβατών Μηνυμάτων

Όσον αφορά την αξιολόγηση της απόδοσης του συγκεκριμένου μηχανισμού προστασίας, δηλαδή την επεξεργαστική επιβάρυνση που εισάγει, από τα αποτελέσματα που καταγράφηκαν προκύπτει ότι είναι αμελητέα. Στο Σχήμα 7–22 και στο Σχήμα 7–23 αποτυπώνονται ενδεικτικές μετρήσεις για την επιβάρυνση που εισάγουν οι έλεγχοι πρώτης γραμμής. Ο Πίνακας 7–17 παρουσιάζει τα αντίστοιχα στατιστικά χαρακτηριστικά, αναφορικά με το ελάχιστο, μέγιστο, μέση τιμή και τυπική διακύμανση.



Σχήμα 7–22. Επεξεργαστική Επιβάρυνση που Εισάγουν οι Έλεγχοι Πρώτης Γραμμής για τα Σενάρια 1-4

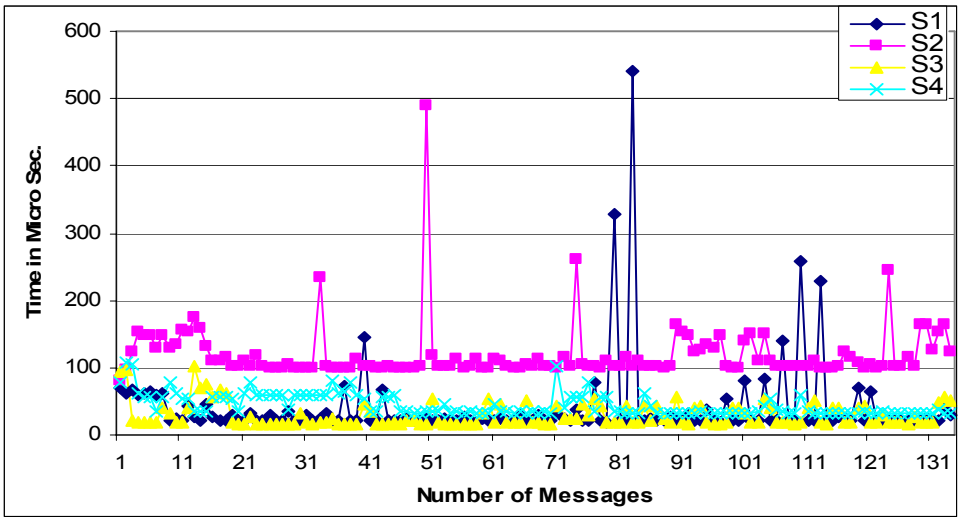


Σχήμα 7–23. Επεξεργαστική Επιβάρυνση που Εισάγουν οι Έλεγχοι Πρώτης Γραμμής για τα Σενάρια 5-8

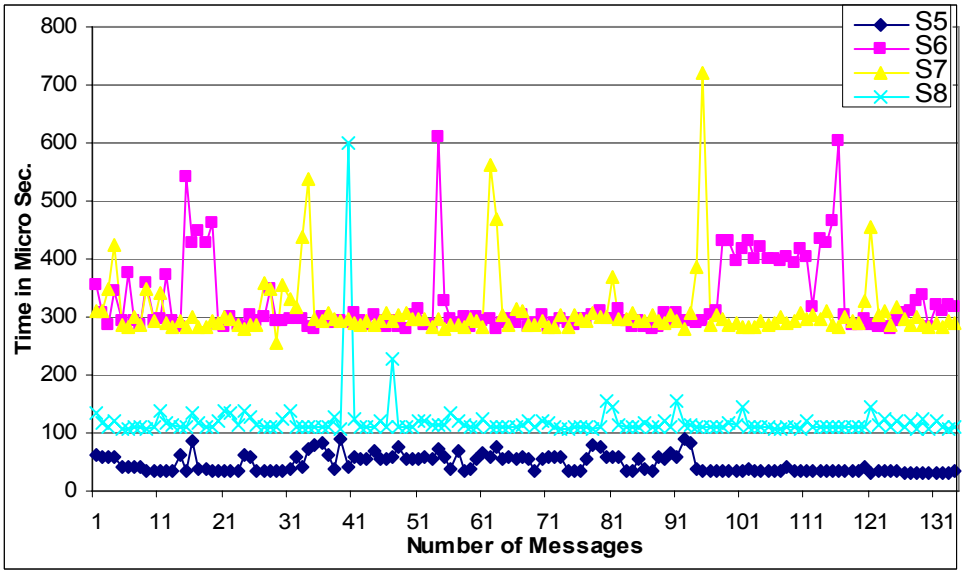
Στατιστική Παράμετρος	S1	S2	S3	S4	S5	S6	S7	S8
Μέγιστο	153.00	93.00	101.00	74.00	64.00	94.00	51.00	59.00
Ελάχιστο	20.00	10.00	16.00	10.00	10.00	09.00	08.00	18.00
Μέση Τιμή	32.08	16.71	28.59	18.37	21.07	15.86	14.07	22.63
Τυπική Απόκλιση	24.01	13.98	17.66	14.25	12.33	12.45	09.92	06.59

Πίνακας 7–17. Στατιστικά Χαρακτηριστικά για την Επεξεργαστική Επιβάρυνση που Εισάγουν οι Έλεγχοι Πρώτης Γραμμής

Αντιστοίχως, στο Σχήμα 7–24 και το Σχήμα 7–25 αποτυπώνονται ενδεικτικές μετρήσεις για την επιβάρυνση που εισάγουν οι έλεγχοι ορθότητας των κεφαλίδων των μηνυμάτων. Ο Πίνακας 7–18 παρουσιάζει τα αντίστοιχα στατιστικά χαρακτηριστικά.



Σχήμα 7–24. Επεξεργαστική Επιβάρυνση που Εισάγουν οι Έλεγχοι Κεφαλίδων για τα Σενάρια 1-4



Σχήμα 7–25. Επεξεργαστική Επιβάρυνση που Εισάγουν οι Έλεγχοι Κεφαλίδων για τα Σενάρια 5-8

Στατιστική Παράμετρος	S1	S2	S3	S4	S5	S6	S7	S8
Μέγιστο	541.00	489.00	101.00	107.00	88.00	657.00	719.00	600.00
Ελάχιστο	20.00	80.00	16.00	31.00	31.00	280.00	255.00	107.00
Μέση Τιμή	40.10	118.98	28.77	44.26	46.84	324.54	309.23	119.96
Τυπική Απόκλιση	60.32	42.54	17.59	16.31	15.32	64.38	56.36	44.03

Πίνακας 7–18. Στατιστικά Χαρακτηριστικά για την Επεξεργαστική Επιβάρυνση που Εισάγουν οι Έλεγχοι Κεφαλίδων

Παρατηρώντας λεπτομερέστερα την καθυστέρηση που εισάγουν οι έλεγχοι, προκύπτει ότι είναι μικρότερη από 35 μικρο-δευτερόλεπτα για τους ελέγχους πρώτης γραμμής και 120 μικρο-δευτερόλεπτα για τους ελέγχους κεφαλίδων. Να σημειωθεί ότι η μεγάλη ομοιότητα των γραφικών παραστάσεων για τους ελέγχους πρώτης γραμμής (βλέπε Σχήμα 7–22 και Σχήμα 7–23) οφείλεται στο γεγονός ότι η μόνη διαφοροποίηση μεταξύ των σεναρίων που αξιοποιήθηκαν αφορούσε στο μήκος των μηνυμάτων και σε κάποιες παραλλαγές των δεδομένων πρώτης γραμμής. Η υψηλή τιμή της τυπικής απόκλισης, ειδικά για το σενάριο 1, μπορεί να αποδοθεί στο γεγονός ότι τα μηνύματα του σεναρίου 1 ήταν μηνύματα με μεγάλη απόκλιση σε ότι αφορά το μέγεθος τους.

Αναφορικά με τους χρόνους επεξεργασίας των κεφαλίδων, παρατειρείται ιδιαίτερα αυξημένη επιβάρυνση στα σενάρια 6 και 7. Το γεγονός αυτό οφείλεται στο ότι τα σενάρια αυτά αξιοποιούν μηνύματα με περισσότερα από ένα λάθη σε κάθε μήνυμα. Συγκεκριμένα, στο σενάριο 6 τα μηνύματα έχουν 4 λάθη στις κεφαλίδες, ενώ στο σενάριο 7 τα μηνύματα έχουν τα ίδια λάθη στις κεφαλίδες και ταυτόχρονα υλοποιούν επίθεση τύπου έγχυσης κώδικα SQL. Τα δύο αυτά σενάρια (S6, S7) υλοποιήθηκαν κυρίως για τον προσδιορισμό της «χειρότερης περίπτωσης» επιβάρυνσης και δεν παρουσιάζουν κάποια πρακτική αξία, καθώς σε περίπτωση εφαρμογής του προτεινόμενου μηχανισμού σε πραγματικό περιβάλλον το μήνυμα θα απορριφθεί αμέσως μόλις εντοπισθεί το πρώτο λάθος.

Ιδιαίτερη σημασία έχει η επιβάρυνση που εισάγεται, από τον προτεινόμενο μηχανισμό προστασίας, κατά την επεξεργασία συμβατών μηνυμάτων. Ο λόγος είναι ότι τα συγκεκριμένα μηνύματα αξιοποιούνται για τη διαχείριση της κλήσης και συνεπώς η καθυστέρηση θα πρέπει να είναι η ελάχιστη δυνατή. Όπως αποτυπώνεται στο σενάριο 8 η συνολική καθυστέρηση που εισάγει ο προτεινόμενος μηχανισμός (κατά την επεξεργασία συμβατών μηνυμάτων) είναι των 150 μικρο-δευτερολέπτων, χρόνος που θεωρείται αμελητέος. Ο επιπρόσθετος χρόνος επεξεργασίας των μη συμβατών μηνυμάτων είναι ουσιαστικά αδιάφορος αφού τα συγκεκριμένα μηνύματα θα απορριφθούν.

Για το γενικότερο έλεγχο της αξιοπιστίας του μηχανισμού υλοποιήθηκε επίθεση πλημμύρας, με χρήση μη συμβατών μηνυμάτων, όπου παρατηρήθηκε ότι όταν ο προτεινόμενος μηχανισμός προστασίας ήταν απενεργοποιημένος ο SIP εξυπηρέτης ετίθετο εκτός λειτουργίας σε μερικά δευτερόλεπτα. Αντίθετα, με τον μηχανισμό ενεργοποιημένο ο SIP εξυπηρέτης συνέχιζε την λειτουργία του χωρίς κάποιο ιδιαίτερο πρόβλημα.

Τέλος, η εισαγωγή του προτεινόμενου μηχανισμού στον εξυπηρέτη SER είχε ως αποτέλεσμα τη αύξηση του μεγέθους του κατά 0,005% (το μέγεθος του SER χωρίς τον μηχανισμό είναι 1,205kbytes ενώ με την ενσωμάτωση του γίνεται 1,212kbytes). Το γεγονός αυτό, συνδυαζόμενο με τα στοιχεία αποτελεσματικότητας και απόδοσης που παρουσιάστηκαν στην ενότητα αυτή, υποδηλώνουν ότι η πρακτική εφαρμογή του προτεινόμενου μηχανισμού είναι εφικτή και ταυτόχρονα αποδοτική αφού μπορεί να βελτιώσει σημαντικά την αξιοπιστία και τη διαθεσιμότητα της παρεχόμενης υπηρεσίας.

7.4.5 Σύγκριση με Εναλλακτικούς Μηχανισμούς

Όπως έχει αναφερθεί και στο Κεφάλαιο 6, μέχρι σήμερα δεν έχουν προταθεί μηχανισμοί για την προστασία από επιθέσεις μη συμβατών μηνυμάτων.

7.5 Προστασία από Επιθέσεις Πλημμύρας

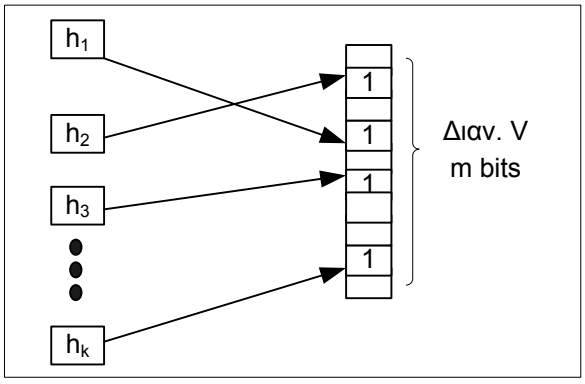
7.5.1 Γενική Περιγραφή

Εκτός από τις επιθέσεις σηματοδοσίας και μη συμβατών μηνυμάτων, ένας επιτιθέμενος μπορεί να αποστείλει προς μια υπηρεσία ένα πολύ μεγάλο αριθμό (συμβατών) αιτήσεων, υπερφορτώνοντας είτε την παρεχόμενη υπηρεσία, είτε το δίκτυο που αυτή αξιοποιεί. Με τον τρόπο αυτό μπορεί να εξαντλήσει τους διαθέσιμους υπολογιστικούς πόρους και, τελικά, να επιτύχει άρνηση παροχής υπηρεσίας. Οι επιθέσεις αυτές θεωρούνται ιδιαίτερα σημαντικές από τους πάροχους καθώς είναι εξαιρετικά δύσκολο να ανιχνευθούν στα αρχικά στάδια εκδήλωσης των, αφού η κίνηση που δημιουργούν είναι πανομοιότυπη με τη φυσιολογική κίνηση που δέχεται η υπηρεσία.

Είναι λοιπόν επιθυμητό οι επιθέσεις πλημμύρας εναντίον κρίσιμων υπηρεσιών, όπως αυτή της διαδικτυακής τηλεφωνίας, να εντοπίζονται το συντομότερο δυνατόν ώστε να λαμβάνονται τα κατάλληλα μέτρα αντιμετώπισης και να ελαχιστοποιούνται τα προβλήματα διαθεσιμότητας που μπορεί να προκαλέσουν. Στη συνέχεια προτείνεται ένας μηχανισμός αναγνώρισης επιθέσεων πλημμύρας σε υπηρεσίες διαδικτυακής τηλεφωνίας που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP. Ο μηχανισμός αυτός υλοποιεί ένα σύστημα καταγραφής της εισερχόμενης κίνησης που βασίζεται στη λειτουργία ενός Bloom φίλτρου [133].

7.5.2 Σύντομη Περιγραφή του Bloom Φίλτρου

Το Bloom φίλτρο [133] αποτελεί μια δομή δεδομένων που αξιοποιείται για την καταγραφή των στοιχείων ενός συνόλου και το μετέπειτα έλεγχο της παρουσίας ή όχι ενός συγκεκριμένου στοιχείου (του συνόλου) στη δομή αυτή. Το χαρακτηριστικό του είναι η πολύ μικρή πιθανότητα λανθασμένης αναγνώρισης της παρουσίας ενός στοιχείου. Πιο συγκεκριμένα, η δομή δεδομένων του Bloom Φίλτρου απαρτίζεται από ένα διάνυσμα V, μήκους m bits, στο οποίο καταγράφονται τα στοιχεία ενός συνόλου A={α1,α2, ...αν}. Αρχικά, όλα τα στοιχεία του διανύσματος V (m bits) αρχικοποιούνται στην τιμή μηδέν. Στη συνέχεια, στα στοιχεία του συνόλου για τα οποία απαιτείται καταγραφή στο φίλτρο, εφαρμόζονται k συναρτήσεις σύνοψης. Το αποτέλεσμα της εφαρμογής των k συναρτήσεων σύνοψης αξιοποιείται ως δείκτης θέσης στο διάνυσμα V, του οποίου η τιμή, στη συγκεκριμένη θέση, θα τεθεί στη μονάδα (βλέπε Σχήμα 7–26).



Σχήμα 7–26. Γενική Δομή του *Bloom* Φίλτρου

Στην περίπτωση κατά την οποία απαιτείται ο έλεγχος παρουσίας ή όχι ενός συγκεκριμένου στοιχείου (π.χ {α3}) στο φίλτρο Bloom, θα πρέπει να εφαρμοσθούν οι k συναρτήσεις σύνοψης στο στοιχείο {α3}. Εάν κάποιο από τα στοιχεία του διανύσματος (με βάση τους δείκτες θέσης που παράγονται από την εφαρμογή των k συναρτήσεων σύνοψης) είναι μηδέν,

τότε το συγκεκριμένο στοιχείο δεν υπάρχει στο φίλτρο με βεβαιότητα ίση με τη μονάδα. Σε αντίθετη περίπτωση, το στοιχείο a3 υπάρχει στο φίλτρο με βεβαιότητα (περίπτωση λανθασμένου εντοπισμού) που προκύπτει από τον παρακάτω τύπο:

$$\left(1-\left(1-\frac{1}{m}\right)^{kn}\right)^{k} \approx \left(1-e^{-kn/m}\right)^{k}$$

Μια τροποποιημένη έκδοση του φίλτρου προτείνεται στην εργασία [134], όπου το διάνυσμα των m bits αντικαθίσταται από ένα νέο διάνυσμα V' από m απαριθμητές (counters). Σε αυτή την έκδοση του φίλτρου, αντί να τροποποιείται -από 0 σε 1- η τιμή ενός στοιχείου του διανύσματος, ο αντίστοιχος απαριθμητής αυξάνεται ή μειώνεται ανάλογα με τη χρήση του φίλτρου. Ο τύπος του φίλτρου αυτού έχει αξιοποιηθεί ήδη για την ανίχνευση επιθέσεων πλημμύρας σε εξυπηρέτες TCP [135].

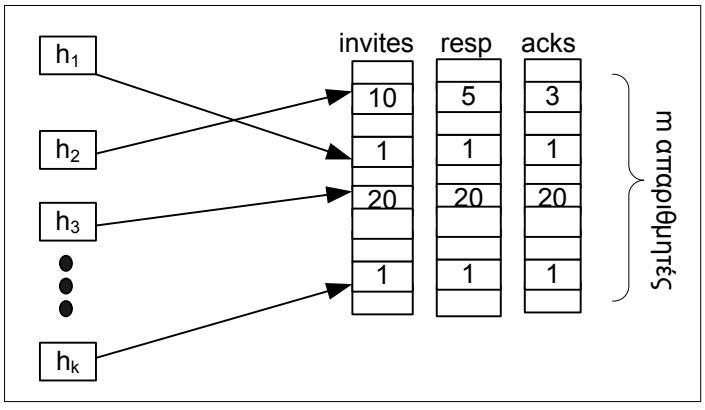
7.5.3 Σύστημα Καταγραφής

Το προτεινόμενο σύστημα αναγνώρισης επιθέσεων πλημμύρας, καταγράφει τα εισερχόμενα μηνύματα μέσω του τροποποιημένου Bloom φίλτρου με τους απαριθμητές. Ο μηχανισμός καταγραφής, ο οποίος και αποτελεί τη βάση για την αναγνώριση επιθέσεων τέτοιου τύπου, αποτελείται από δύο τμήματα.

Στο πρώτο τμήμα καταγράφεται, σε τρία Bloom φίλτρα, όλη η εισερχόμενη, προς την υπηρεσία, κίνηση δηλαδή:

1. οι αιτήσεις INVITE.
2. οι αντίστοιχες αποκρίσεις.
3. τα τελικά μηνύματα ACK.

Ως είσοδος στις συναρτήσεις σύνοψης χρησιμοποιούνται οι κεφαλίδες «From» και «call-id» των μηνυμάτων, αφού οι συγκεκριμένες κεφαλίδες προσδιορίζουν μοναδικά κάθε σύνοδο. Στο Σχήμα 7–27 απεικονίζεται ένα στιγμιότυπο του συστήματος καταγραφής σε συγκεκριμένη χρονική στιγμή. Αντίστοιχα στο Σχήμα 7–28 απεικονίζεται ο αλγόριθμος καταγραφής για το πρώτο τμήμα του φίλτρου.



Σχήμα 7–27. Το πρώτο Τμήμα του Συστήματος Καταγραφής Εισερχόμενης Κίνησης

```
Για κάθε incoming_message ελέγχεται ο τύπος
Εαν ο τύπος είναι αίτημα
  ελέγξε τη μέθοδο
     εάν μεθοδος INVITE
        ενημέρωση invite_bloom_filter
      διαφορετικά εαν η μέθοδος είναι ACK
        ενημέρωση ack_bloom_filter
Έαν ο τύπος είναι τελική απόκριση
    ενημέρωση response_bloom_filter
```

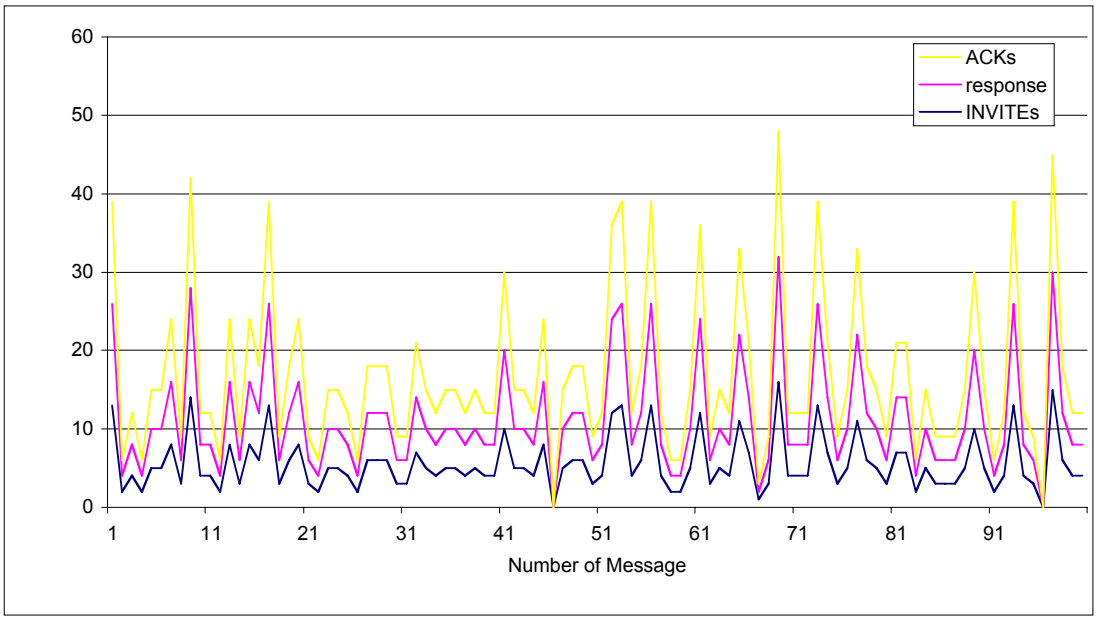
Σχήμα 7–28. Αλγόριθμος Καταγραφής της Εισερχόμενης Κίνησης

Στο δεύτερο τμήμα καταγράφεται, σε ένα Bloom φίλτρο, η κίνηση που προωθείται προς τους τελικούς χρήστες. Οι βασικές διαφορές από το πρώτο τμήμα του συστήματος είναι ότι:

1. Χρησιμοποιείται μόνο το αντίστοιχο φίλτρο "INVITE" του αρχικού τμήματος καταγραφής (βλέπε Σχήμα 7–27)
2. Ως είσοδος στις k συναρτήσεις σύνοψης αξιοποιούνται μόνο τα δεδομένα της κεφαλίδας «To».
3. Για κάθε εισερχόμενο μήνυμα SIP INVITE, τα αντίστοιχα πεδία του φίλτρου αυξάνονται κατά ένα.

7.5.4 Μέθοδος Αναγνώρισης

Στη γενική περίπτωση, οι επιθέσεις πλημμύρας σχετίζονται με ένα μεγάλο αριθμό μη ολοκληρωμένων συνόδων που διατηρούνται για παρατεταμένο χρονικό διάστημα στη μνήμη του υπολογιστικού συστήματος της υπηρεσίας. Από την άλλη πλευρά, σύμφωνα με τις προδιαγραφές του SIP, για κάθε έγκυρη σύνοδο που αποκαθίσταται, υπάρχει μια μοναδική αντιστοίχηση μεταξύ των αιτημάτων (SIP INVITE), των αντίστοιχων αποκρίσεων και των επιβεβαιώσεων (SIP ACK). Στο Σχήμα 7–29 απεικονίζεται μια τέτοια αντιστοίχηση για ένα δείγμα της εισερχόμενης κίνησης προς την υπηρεσία διαδικτυακής τηλεφωνίας, όπου οι αποκρίσεις και τα αντίστοιχα SIP ACK μηνύματα ακολουθούν χρονικά τα μηνύματα SIP INVITE.



Σχήμα 7–29. Απεικόνιση Συσχέτισης SIP INVITE –Αποκρίσεων – SIP ACK

Βασιζόμενοι στα προαναφερθέντα, εισάγουμε μια νέα μετρική ονομαζόμενη απόσταση συνόδου (session distance) η οποία υπολογίζεται σύμφωνα με τον παρακάτω τύπο:

dist=Num of INVITEs - 0,5*(Num of OKs + Num of ACKs)

Υπό φυσιολογικές συνθήκες, η μετρική αυτή για κάθε σύνοδο που έχει αποκατασταθεί επιτυχώς είναι ίση με μηδέν. Ως εκ' τούτου, η ύπαρξη επίθεσης πλημμύρας μπορεί να αναγνωριστεί υπολογίζοντας σε τακτά χρονικά διαστήματα το άθροισμα της μετρικής «απόσταση συνόδου» για όλες τις εγγραφές του πρώτου τμήματος καταγραφής (βλέπε ενότητα 7.5.3). Σε περίπτωση που η υπολογιζόμενη τιμή αποκλίνει σημαντικά από κάποιο προκαθορισμένο όριο τιμών, τότε υπάρχει σοβαρή πιθανότητα να έχει εκδηλωθεί επίθεση πλημμύρας και θα πρέπει να ενεργοποιηθεί ο κατάλληλος συναγερμός. Η συχνότητα των ελέγχων αυτών εξαρτάται, μεταξύ των άλλων, και από τις δυνατότητες του συστήματος (system capabilities) που παρέχει την υπηρεσία.

Αναφορικά με τα κατάλληλα όρια τιμών, αυτά διαφοροποιούνται από σύστημα σε σύστημα και για το λόγο αυτό προτείνεται να προσδιορίζονται με βάση τη μέση τιμή της μετρικής «απόσταση συνόδου» κατά τη διάρκεια ενός συγκεκριμένου χρονικού διαστήματος, όπου το σύστημα βρίσκεται κάτω από φυσιολογικές συνθήκες κίνησης (βλέπε Σχήμα 7–30).

Για κάθε στοιχείο του συστήματος καταγραφής εκτέλεσε:
$session\_distance_i = num\_of\_invite_i - 0{,}5*(num\_of\_resp_i + num\_of\_ack_i)$
$threhsold\_value = +session\_distance_i$

Σχήμα 7–30. Αλγόριθμος Προσδιορισμού των Ορίων Τιμών της Μετρικής «Απόσταση Συνόδου»

Η παραπάνω διαδικασία για τον προσδιορισμό των κατάλληλων ορίων τιμών πρέπει να εκληφθεί ως «περίοδος εκπαίδευσης» του συστήματος, ενώ, για τον τελικό προσδιορισμό των θα πρέπει να λαμβάνονται υπόψη και τα ακόλουθα:

1. Η μέση καθυστέρηση του Δικτύου (*Nd*).
2. Ο μέσος χρόνος απόκρισης των χρηστών (*URT*).

Για παράδειγμα, ας υποθέσουμε ότι κάποιος διαχειριστής καταγράφει την εισερχόμενη κίνηση υπολογίζοντας το άθροισμα των μέσων τιμών της μετρικής «απόσταση συνόδου» για όλες τις εγγραφές του φίλτρου, T_{sd1}, και ότι η καθυστέρηση του δικτύου είναι Nd_1, και ο χρόνος απόκρισης των χρηστών είναι URT_1. Το όριο, T_{alarm}, για την αναγνώριση επίθεσης πλημμύρας υπολογίζεται σύμφωνα με τον παρακάτω τύπο:

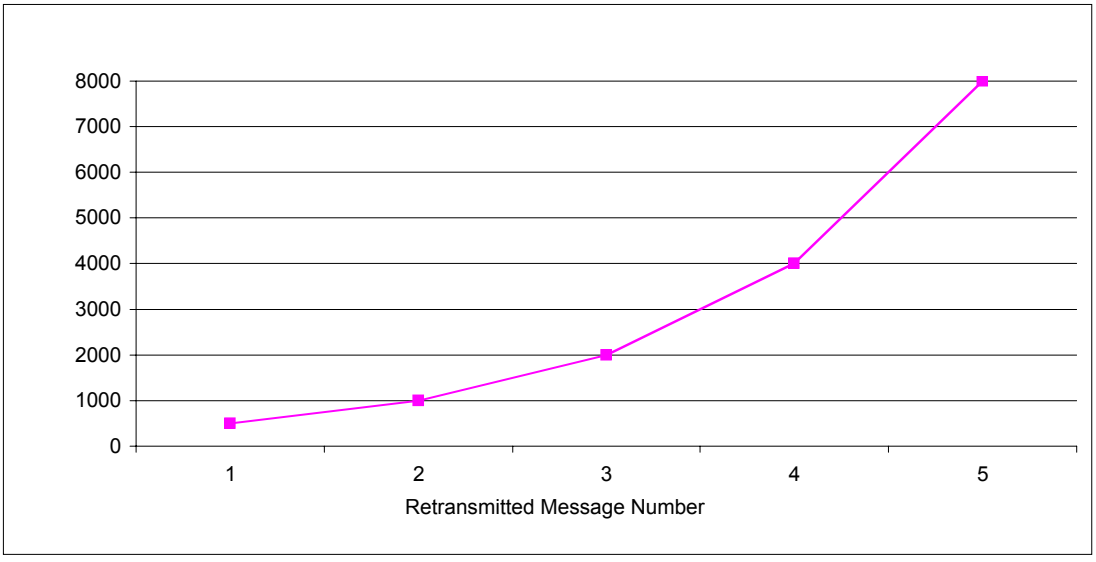
$$T_{alarm} = T_{sd1} + Nd_1 + URT_1 + \delta$$

Η παράμετρος δ αποτυπώνει τις υπολογιστικές δυνατότητες του συστήματος. Όταν η τιμή που υπολογίζεται για τη μετρική «απόσταση συνόδου» υπερβαίνει το T_{alarm}, αποτελεί ένδειξη ότι έχει εκδηλωθεί επίθεση πλημμύρας.

Στη μέχρι τώρα περιγραφή για την αναγνώριση επιθέσεων πλημμύρας έχει γίνει η υπόθεση ότι ο επιτιθέμενος αξιοποιεί διαφορετικά μηνύματα. Παρ' όλα αυτά το πρώτο τμήμα του συστήματος καταγραφής μπορεί να αξιοποιηθεί και για την αναγνώριση επιθέσεων πλημμύρας, προς πληρεξούσιους εξυπηρέτες ή τελικούς χρήστες, που χρησιμοποιούν το ίδιο μήνυμα. Στις περισσότερες περιπτώσεις οι συγκεκριμένες επιθέσεις στοχεύουν στη δημιουργία άρνησης παροχής υπηρεσίας για κάποιο τελικό χρήστη (βλέπε ενότητα 4.4.4.3). Κατά την εκδήλωση μιας τέτοιας επίθεσης θα αυξάνονται συνεχώς μόνο κάποια συγκεκριμένα στοιχεία του φίλτρου που αντιστοιχούν στο μήνυμα που χρησιμοποιείται για την εκδήλωση της επίθεσης. Ως εκ τούτου, αν και η τιμή της απόστασης συνόδου θα αυξάνεται, για ένα αρκετά μεγάλο χρονικό διάστημα θα υπολείπεται της τιμής T_{alarm}. Βέβαια,

σε αυτό το χρονικό διάστημα μπορεί να έχει ήδη προκληθεί άρνηση παροχής υπηρεσίας στον τελικό χρήστη λόγω της περιορισμένης επεξεργαστικής ικανότητας του. Για την αντιμετώπιση τέτοιων περιστατικών είναι απαραίτητη η εισαγωγή μιας δεύτερης τιμής ορίου, $T_{Single1}$. Οποτεδήποτε η υπολογιζόμενη τιμή μιας συγκεκριμένης εγγραφής του φίλτρου υπερβεί την τιμή $T_{signle1}$ αποτελεί ένδειξη ότι έχει εκδηλωθεί επίθεση πλημμύρας, είτε προς κάποιον τελικό χρήστη, είτε προς τον εξυπηρέτη της υπηρεσίας, που αξιοποιεί το ίδιο μήνυμα.

Στην περίπτωση που ο επιτιθέμενος αξιοποιήσει διαφορετικά μηνύματα για την εκδήλωση επίθεσης πλημμύρας προς ένα οποιοδήποτε τελικό χρήστη, τα εισερχόμενα SIP INVITE μηνύματα θα διαμοιράζονται ομοιόμορφα στις εγγραφές του φίλτρου και οι αντίστοιχες αποστάσεις συνόδων θα παραμένουν κάτω από τα όρια των τιμών συναγερμού T_{alarm} και $T_{Single1}$ αντιστοίχως, με αποτέλεσμα να μην είναι δυνατή η αναγνώριση της επίθεσης. Βέβαια το κύριο χαρακτηριστικό των μηνυμάτων αυτών είναι ότι η κεφαλίδα «To» θα παραμένει σταθερή, αφού όλα τα μηνύματα προωθούνται στον ίδιο τελικό χρήστη. Για το λόγο αυτό αξιοποιείται το δεύτερο τμήμα του συστήματος καταγραφής, όπου συγκεκριμένα στοιχεία του φίλτρου αντιστοιχούν στην κίνηση που προωθείται προς ένα συγκεκριμένο τελικό χρήστη. Εάν οποιαδήποτε εγγραφή του δεύτερου τμήματος καταγραφής υπερβεί μια τιμή κατώφλι τότε θα πρέπει να ενεργοποιείται ο αντίστοιχος συναγερμός. Τα συγκεκριμένα στοιχεία του φίλτρου θα πρέπει να ελέγχονται κάθε *T1* δευτερόλεπτα, αφού σύμφωνα με το RFC 3261 [11], ως *T1* ορίζεται ο χρόνος επαναμετάδοσης ενός μηνύματος SIP INVITE, μέχρι ο πελάτης να λάβει την αρχική απάντηση. Η προκαθορισμένη τιμή του *T1* είναι 0.5 δευτερόλεπτα και ο ρυθμός επαναμετάδοσης ενός μηνύματος υπολογίζεται από το τύπο *T1=2*T1*. Το Σχήμα 7–31 αποτυπώνει το μοντέλο επανεμετάδοσης ενός SIP INVITE μηνύματος.



Σχήμα 7–31. Μοντέλο Επαναμετάδοσης INVITE Μηνυμάτων Σύμφωνα με τις Προδιαγραφές του SIP

Δεδομένου ότι ο επιτρεπόμενος αριθμός επανεκπομπών είναι οκτώ, σύμφωνα με τον προαναφερόμενο τύπο, η χρονική διάρκεια όλης της διαδικασίας δεν μπορεί να υπερβαίνει τα τριάντα δύο δευτερόλεπτα. Συνεπώς, ο αριθμός των οχτώ μηνυμάτων, από την ίδια πηγή, σε χρονικό διάστημα τριάντα δύο δευτερολέπτων μπορεί να θεωρηθεί ως ασφαλές κατώφλι για την ανίχνευση τέτοιων περιστατικών.

Όπως συμβαίνει με όλους τους μηχανισμούς αναγνώρισης επιθέσεων, η αποτελεσματικότητα τους εξαρτάται τόσο από τον ρυθμό των λανθασμένων συναγερμών που προκαλούνται, όσο και από το χρόνο που απαιτείται για την αναγνώριση της επίθεσης. Στο προτεινόμενο σύστημα οι λανθασμένοι συναγερμοί εξαρτώνται κυρίως από τις τιμές ορίων που υιοθετούνται αλλά και από τις τιμές των παραμέτρων m, k του φίλτρου για την ύπαρξη ή όχι ενός συγκεκριμένου στοιχείου στο σύστημα καταγραφής (για περισσότερες λεπτομέρειες βλέπε [133]). Για το λόγο αυτό η φάση της εκπαίδευσης του μηχανισμού είναι κρίσιμη και πρέπει να πραγματοποιείται σε χρονικές στιγμές που το σύστημα βρίσκεται κάτω από διαφορετικές συνθήκες κίνησης. Ο χρόνος αναγνώρισης μιας επίθεσης εξαρτάται αποκλειστικά και μόνο από το χρόνο εκτέλεσης των συναρτήσεων σύνοψης που αξιοποιούνται σε κάθε περίπτωση. Τέλος, θα πρέπει να επισημανθεί ότι το φίλτρο Bloom υλοποιείται σε υλικό και ως εκ' τούτου η επιπρόσθετη επιβάρυνση που εισάγει θεωρείται αμελητέα.

7.5.5 Σύγκριση Με Εναλλακτικούς Μηχανισμούς Προστασίας από Επιθέσεις Πλημμύρας

Στην ενότητα 6.5 παρουσιάζονται οι εναλλακτικοί μηχανισμοί που έχουν προταθεί για προστασία από επιθέσεις πλημμύρας. Η τεχνική που υιοθετείται, από το σύνολο των μηχανισμών, για την ανίχνευση των επιθέσεων βασίζεται στη συμβατότητα των εμπλεκομένων οντοτήτων με τις προδιαγραφές του SIP, στη χρήση καλά ορισμένων μετρικών (όπως για παράδειγμα η απόσταση Hellinger*)* και στον προσδιορισμό των κατάλληλων ορίων τιμών. Αντίστοιχα στοιχεία αξιοποιούνται και από τον προτεινόμενο μηχανισμό εστιάζοντας περισσότερο στις ιδιαιτερότητες του SIP για τον ορισμό μιας κατάλληλης μετρικής συνδυάζοντας την με ένα ιδιαίτερα αποτελεσματικό μηχανισμό καταγραφής βασισμένο στο Bloom φίλτρο.

7.6 Συμπεράσματα

Για την επίτευξη ενός ικανοποιητικού επιπέδου ασφάλειας και προστασίας από επιθέσεις στις υπηρεσίες διαδικτυακής τηλεφωνίας, είναι απαραίτητο να συνδυαστούν διαφορετικές λύσεις. Στο κεφάλαιο αυτό παρουσιάστηκαν λύσεις και τεχνικές για την προστασία των υπηρεσιών διαδικτυακής τηλεφωνίας (που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP) από διαφορετικούς τύπους επιθέσεων, καθώς και για την ενδυνάμωση των υποστηριζόμενων υπηρεσιών ασφαλείας. Οι προτεινόμενες τεχνικές αξιολογήθηκαν μέσω πειραματικής αρχιτεκτονικής που υλοποιήθηκε. Τα αποτελέσματα που προέκυψαν μπορούν να αξιοποιηθούν για να τεκμηριώσουν τόσο την ορθότητα και αποτελεσματικότητα των προτεινόμενων μηχανισμών προστασίας, όσο και την εφικτότητα της πρακτικής υλοποίησης των, αφού η επεξεργαστική επιβάρυνση που εισάγουν είναι ελάχιστη.

ΚΕΦΑΛΑΙΟ 8: Ολοκληρωμένη Αναπαράσταση της Προτεινόμενης Αρχιτεκτονικής Ασφαλείας με Χρήση Οντολογιών

8.1 Γενικά

Οι πάροχοι υπηρεσιών διαδικτυακής τηλεφωνίας, πέρα από την έγκαιρη ανίχνευση και την αντιμετώπιση των επιθέσεων που μπορεί να εκδηλωθούν κατά των υπηρεσιών που προσφέρουν, θα πρέπει να αποκτήσουν τη δυνατότητα αποτύπωσης των περιστατικών ασφαλείας μέσω κάποιας κοινής σημασιολογικής περιγραφής. Με τον τρόπο αυτό θα καταστεί δυνατή η ανάπτυξη μιας ενιαίας, μεταξύ όλων των παρόχων υπηρεσιών διαδικτυακής τηλεφωνίας, αρχιτεκτονικής ασφαλείας και προστασίας. Τα υπάρχοντα συστήματα αναγνώρισης και αντιμετώπισης περιστατικών ασφάλειας δεν υποστηρίζουν κανενός τύπου ομοιομορφία σε ότι αφορά την περιγραφή των περιστατικών ασφαλείας. Για παράδειγμα, τα συστήματα ανίχνευσης SNORT[129] και BRO[136] μπορούν να αξιοποιηθούν για την ανίχνευση επιθέσεων, όμως η περιγραφή ενός περιστατικού στο SNORT δεν μπορεί να μεταφερθεί αυτομάτως στο BRO και αντιστρόφως. Επίσης, οι γλώσσες περιγραφής που αξιοποιούνται από τα συστήματα αυτά δεν είναι εύκολα επεκτάσιμες και η τυπική σημασιολογία τους είναι συνήθως ελλιπής.

Για τη δημιουργία ενός ενιαίου τυπικού μοντέλου ασφαλείας, το οποίο θα προσφέρει τα απαραίτητα μέτρα προστασίας για τις υπηρεσίες διαδικτυακής τηλεφωνίας, επιλέχθηκε η χρήση οντολογιών. Ο λόγος ήταν ότι οι οντολογίες υποστηρίζουν τη δυνατότητα τυπικής φορμαλιστικής περιγραφής κάποιου συγκεκριμένου τομέα, στον οποίο συμπεριλαμβάνονται οι ορισμοί των όρων, οι συσχετίσεις μεταξύ τους και η ερμηνεία στο αντίστοιχο υπολογιστικό σύστημα. Επίσης, όπως χαρακτηριστικά αναφέρεται στην εργασία [137], ένας από τους στόχους των οντολογιών είναι η διάχυση της κοινής ερμηνείας των εννοιών ενός συγκεκριμένου τομέα, μεταξύ διαφορετικών οντοτήτων. Συνεπώς, οι οντολογίες επιτρέπουν τη δημιουργία μίας κοινής «*βάσης ασφαλείας*», μέσω της οποίας προωθείται η συνεργασία των παρόχων διαδικτυακής τηλεφωνίας, ανεξάρτητα των ιδιαίτερων χαρακτηριστικών της κάθε υπηρεσίας, με απώτερο στόχο τη δημιουργία ενός ασφαλούς περιβάλλοντος παροχής υπηρεσιών τηλεφωνίας.

Στη συνέχεια του παρόντος κεφαλαίου υπάρχει αναλυτική περιγραφή της οντολογίας, της τυπικής αναπαράστασης της σε κατηγορηματική λογική, καθώς και παραδείγματα της εφαρμογής της σε πραγματικό περιβάλλον.

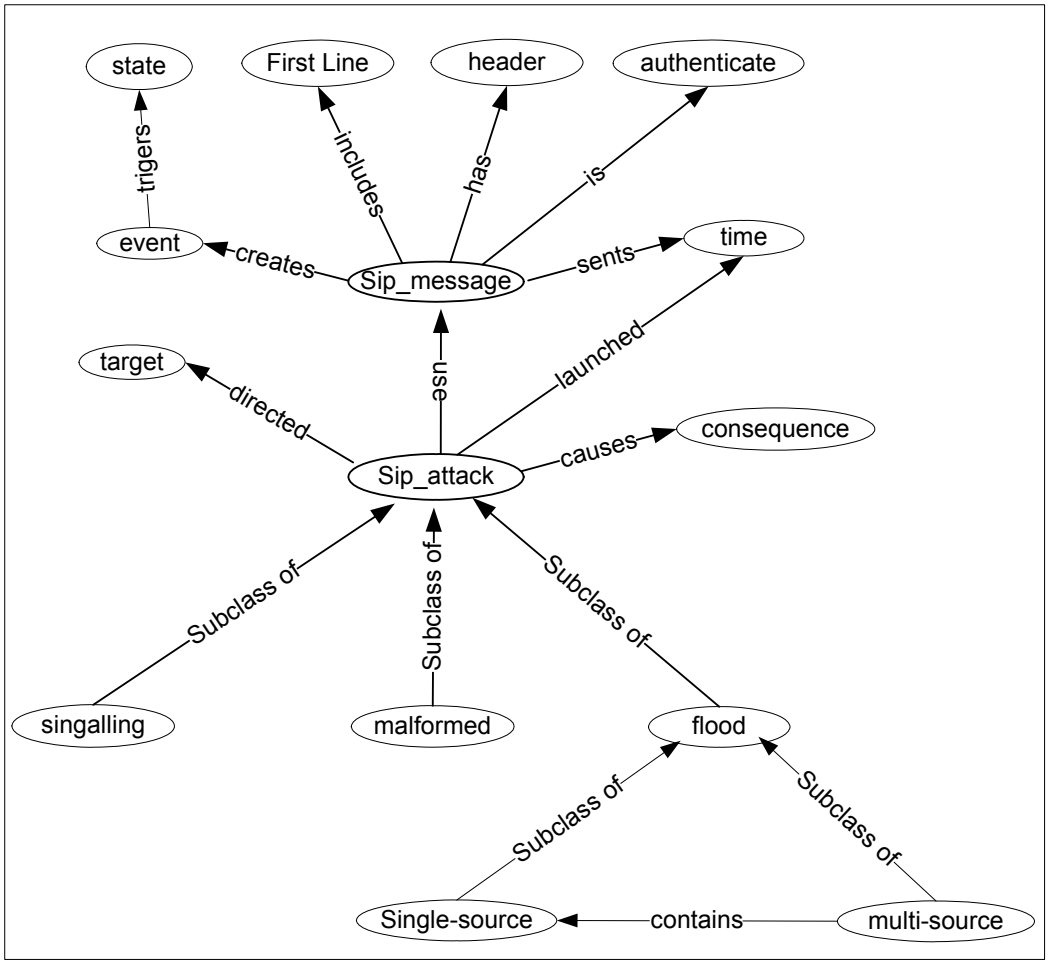
8.2 Οντολογική Αναπαράσταση

Οποιαδήποτε επίθεση εκδηλώνεται κατά ενός πληροφοριακού συστήματος, επιχειρεί να εκμεταλλευτεί αδυναμίες των αξιοποιούμενων πρωτοκόλλων με απώτερο σκοπό να προκαλέσει συγκεκριμένες συνέπειες στο υπολογιστικό σύστημα στόχο. Η συγκεκριμένη φιλοσοφία, σε συνδυασμό με τις καταγεγραμμένες ευπάθειες (Κεφάλαιο 4) των υπηρεσιών διαδικτυακής τηλεφωνίας, έχει αξιοποιηθεί ως ‘οδηγός’ κατά τη διαδικασία σχεδίασης της οντολογίας για την περιγραφή των προβλημάτων ασφαλείας στη διαδικτυακή τηλεφωνία.

Το Σχήμα 8–1 απεικονίζει τη γενική δομή της προτεινόμενης οντολογίας. Όπως έχει προαναφερθεί, και ταυτόχρονα αποτυπώνεται στο προαναφερόμενο σχήμα, οποιαδήποτε επίθεση εκδηλώνεται κατά μιας υπηρεσίας διαδικτυακής τηλεφωνίας που αξιοποιεί το πρωτόκολλο SIP, χρησιμοποιεί κάποιο SIP μήνυμα το οποίο προωθείται προς ένα

συγκεκριμένο κόμβο (στόχο) με σκοπό τη δημιουργία συγκεκριμένων προβλημάτων. Η οντολογία αποτελείται από δύο βασικές κλάσεις:

1. Την κλάση μηνυμάτων SIP.
2. Την κλάση επιθέσεων SIP.



Σχήμα 8–1. Οντολογική Αναπαράσταση των Επιθέσεων κατά των Υπηρεσιών Διαδικτυακής Τηλεφωνίας που Αξιοποιούν το Πρωτόκολλο SIP

8.2.1 Οντολογική Αναπαράσταση των SIP μηνυμάτων

Η προτεινόμενη οντολογία (Σχήμα 8–1) αποτυπώνει καθαρά το γεγονός ότι ένα μήνυμα SIP αποτελείται από την πρώτη γραμμή (first line) και τις αντίστοιχες κεφαλίδες. Ουσιαστικά το τμήμα αυτό της οντολογίας αξιοποιείται για τον έλεγχο συμμόρφωσης των SIP μηνυμάτων με τις προδιαγραφές του RFC 3261 [11], παρέχοντας τους αντίστοιχους κανόνες. Πιο συγκεκριμένα, το τμήμα της οντολογίας για την αναπαράσταση των SIP μηνυμάτων, απαρτίζεται από τις παρακάτω κλάσεις:

1. First Line: Η κλάση αυτή αναπαριστά την πρώτη γραμμή των SIP μηνυμάτων (αποκρίσεων/αιτήσεων). Κάθε "πρώτη-γραμμή" εμπεριέχει τη μέθοδο ή τον κωδικό απόκρισης και την περιγραφή της (ανάλογα με τον τύπο του μηνύματος απόκρισης-αίτησης), καθώς και τον κανόνα που θα πρέπει να εφαρμόσει οποιαδήποτε SIP οντότητα για να ελέγξει την ορθότητα του εισερχόμενου μηνύματος.
2. Header*:* Η κλάση αυτή αναπαριστά τις κεφαλίδες που πρέπει να συμπεριλαμβάνονται σ' ένα SIP μήνυμα, παρέχοντας επιπλέον την περιγραφή της

γραμματικής τους. Συγκεκριμένα υπάρχει το όνομα της κεφαλίδας και ο αντίστοιχος κανόνας για τον έλεγχο της εγκυρότητας της κεφαλίδας, όμοια με τους κανόνες που αξιοποιούνται για τους ελέγχους της πρώτης γραμμής.

3. Authenticate: Η κλάση αυτή αναπαριστά τη μέθοδο που αξιοποιείται για την αυθεντικοποίηση των SIP μηνυμάτων.
4. Event: Η κλάση αυτή αναπαριστά το αποτέλεσμα της επεξεργασίας ενός SIP μηνύματος.
5. Time: Η κλάση αυτή αναπαριστά τη χρονική στιγμή κατά την οποία έγινε η επεξεργασία ενός SIP μηνύματος.

8.2.2 Οντολογική Αναπαράσταση Επιθέσεων

Η οντολογική αναπαράσταση των επιθέσεων που μπορεί να εκδηλωθούν κατά της υπηρεσίας διαδικτυακής τηλεφωνίας αποτελείται από τις ακόλουθες κλάσεις:

1. Malformed: Η κλάση αυτή αναπαριστά επιθέσεις που αξιοποιούν μηνύματα που δεν συμμορφώνονται με τις προδιαγραφές του πρωτοκόλλου SIP. Η περιγραφή αυτή δεν απαιτεί κάποια επιπρόσθετη αναπαράσταση καθώς κάθε μη συμβατό μήνυμα μπορεί να θεωρηθεί ως το συμπλήρωμα των συμβατών μηνυμάτων.
2. Signalling: Η κλάση σηματοδοσίας αναπαριστά τις επιθέσεις κατά τις οποίες κακόβουλες (μη εξουσιοδοτημένες) οντότητες χρησιμοποιούν μηνύματα όπως το SIP BYE ή το SIP CANCEL για τον τερματισμό κάποιας συνόδου.
3. Flood: Η κλάση αυτή αναπαριστά τις επιθέσεις πλημμύρας. Όπως απεικονίζεται στο Σχήμα 8–1 οι επιθέσεις πλημμύρας διαχωρίζονται σε απλής (single) και πολλαπλής (multiple) πηγής.
4. Target: Η κλάση αυτή αντιστοιχεί στις διαθέσιμες δικτυακές οντότητες που αξιοποιούνται για την παροχή των υπηρεσιών διαδικτυακής τηλεφωνίας και αποτελούν πιθανούς στόχους επιθέσεων.
5. Consequence: Η κλάση αυτή αναπαριστά τις επιπτώσεις που προκαλούνται από την εκδήλωση επιθέσεων προς μια SIP οντότητα.

8.2.3 Ανάπτυξη της Οντολογίας

Για τον προσδιορισμό των στοιχείων και της σημασιολογίας μιας οντολογίας απαιτείται η χρήση της κατάλληλης γλώσσας για την περιγραφή των κλάσεων, των αντικειμένων και των συσχετισμών μεταξύ αυτών. Ως εκ' τούτου, για την αξιοποίηση της προτεινόμενης οντολογίας σε πραγματικά συστήματα διαδικτυακής τηλεφωνίας απαιτείται, σε πρώτη φάση, η περιγραφή της αξιοποιώντας την κατάλληλη γλώσσα.

Για την περιγραφή της προτεινόμενης οντολογίας επελέγη η γλώσσα DAML+OIL [138]. Η συγκεκριμένη γλώσσα δεν παρέχει μόνο δυνατότητα αναπαράστασης τους σχήματος της οντολογίας, αλλά ενσωματώνει και τους αντίστοιχους σημασιολογικούς κανόνες, παρέχοντας έτσι τον περαιτέρω τυπικό φορμαλισμό της. Επιπροσθέτως, παρέχεται η δυνατότητα αξιοποίησης της οντολογίας από διαφορετικές οντότητες, κάτω από ένα ενιαίο πλαίσιο. Σημειώνεται ότι η προτεινόμενη οντολογία είναι δυνατόν να περιγραφεί και με άλλες οντολογικές γλώσσες, όπως για παράδειγμα η OWL[139], οι οποίες βασίζονται στο σχήμα RDF [140]. Η αναπαράσταση της οντολογίας σε DAML+OIL παρατίθεται στο Παράρτημα Ι.

8.2.4 Παράδειγμα Αξιοποίησης της Οντολογίας

Ας θεωρήσουμε ότι για την αναγνώριση μη συμβατών SIP REGISTER μηνυμάτων, αξιοποιώντας την προτεινόμενη οντολογία, ο διαχειριστής μιας υπηρεσίας διαδικτυακής τηλεφωνίας αναπτύσσει την περιγραφή που αποτυπώνεται στο Σχήμα 8–2.

```
<Malformed id=”Register-Malformed”’>
        <sip_message rdf:resource=”sip_register”/>
        <target rdf:resource=”registrar”/>
</Malformed>

<target id=”registrar”>
        <ip>195.251.145.3</ip>
        <port>5060</port>
</target>
```

Σχήμα 8–2. Παράδειγμα Περιγραφής Μη Συμβατών Μηνυμάτων

Σύμφωνα με τις προδιαγραφές της οντολογίας, ο διαχειριστής θα πρέπει να προσδιορίσει όλους τους πόρους που εμπλέκονται στην συγκεκριμένη περιγραφή. Δηλαδή, θα πρέπει να περιγραφούν οι πόροι «sip_register» και «registrar». Ο πόρος «registrar» αναπαριστά τον πιθανό στόχο της επίθεσης και περιγράφεται ήδη στο Σχήμα 8–2, αφού προσδιορίζεται η IP του και η θύρα (port) στην οποία λαμβάνει τα SIP μηνύματα. Όσον αναφορά τον πόρο «sip_register», ο διαχειριστής θα πρέπει να προσδιορίσει τα στοιχεία εκείνα του SIP μηνύματος τα οποία επιθυμεί να ελέγχει για κάθε εισερχόμενο SIP REGISTER μήνυμα. Για παράδειγμα ας υποθέσουμε ότι ο διαχειριστής επιθυμεί να ελέγχει την πρώτη γραμμή του μηνύματος και τις κεφαλίδες «CSEQ», «FROM» και «TO». Για να το κάνει αυτό αναπτύσσει την οντολογική περιγραφή «sip_register» που απεικονίζεται στο Σχήμα 8–3.

```
<sip_message id="sip_register">
        <first_line rdf:resource="#REGISTER" id="1"/>
        <header rdf:resource="#CSEQ"/>
        <header rdf:resource="#from"/>
        <header rdf:resource="#to"/>
</sip_message>
```

Σχήμα 8–3. Παράδειγμα Οντολογικής Περιγραφής ενός SIP REGISTER Μηνύματος

Αντίστοιχα, όλοι οι επιπρόσθετοι πόροι που εμπλέκονται στην οντολογική περιγραφή που απεικονίζει το Σχήμα 8–3, θα πρέπει να περιγράφονται σύμφωνα με τις προδιαγραφές της οντολογίας. Δηλαδή οι πόροι «Register, CSeq, From, To» θα πρέπει να συμπεριλαμβάνονται στην περιγραφή της οντολογίας όπως αποτυπώνεται στο Σχήμα 8–4 και στο Σχήμα 8–5 αντιστοίχως.

```
<first_line ID="REGISTER">
        <method rdf:resource="#REGISTER"/>
<rule>
\s+((((\d{1,3}[.]){3,3}\d{1,3}(:\d{1,5}))
(;transport[=].+)*\s+(SIP[/]\d[.]\d))|((SIP[/]\d[.]\d)\s+(\d{3})\s+.+)\s*
</rule>
</first_line>
```

Σχήμα 8–4.Οντολογική Αναπαράσταση της Πρώτης Γραμμής για τον πόρο “REGISTER”

```
sip_message_headers rdf:id="to">
        <name>#to</name>
        <rule>\s*((["]*(\w+\s*\w*)*["]*)*\s+
        ((<)*(sip:)((\w+@(\w+[.])+\w+)
        |((\d{1,3}[.]){3,3}\d{1,3}))(>)*))(\s*;tag=.+)*\s*
        </rule>
</sip_message_headers>
<sip_message_headers rdf:id="from">
        <name>
        #from
        </name>
        <rule>\s*(["]*(\w+\s*\w*)*["]*\s+
        ((<)*(sip:)((\w+@(\w+[.])+\w+)|
        (((\d{1,3}[.]){3,3}\d{1,3}))(>)*))(\s*;tag=\w+)*(.+)*\s*
        </rule>
</sip_message_headers>
<sip_message_headers rdf:id="CSEQ">
        <name>
        #CSEQ
        </name>
        <rule>
        ^\s*(CSeq:)\s*\d+\s+\b(register)\b\s*</rule>
</sip_message_headers>
```

Σχήμα 8–5. Οντολογική Αναπαράσταση των Κεφαλίδων: *From,To,CSEQ*

8.3 Αναπαράσταση της Οντολογίας σε Κατηγορηματική Λογική

Λαμβάνοντας υπόψη ότι οι γλώσσες όπως η DAML+OIL [138] και η OWL[139] βασίζονται στην κατηγορηματική λογική, προχωράμε στον μετασχηματισμό της προτεινόμενης οντολογίας σε κατηγορηματική λογική. Η αναπαράσταση αυτή ουσιαστικά ενοποιεί την οντολογία με υπάρχοντα εργαλεία συμπερασμού όπως το RACER [141], παρέχοντας ταυτόχρονα ένα ισχυρό τυπικό φορμαλισμό για τον προσδιορισμό περιγραφών ασφαλείας για τις υπηρεσίες διαδικτυακής τηλεφωνίας. Ο μετασχηματισμός της οντολογίας σε κατηγορηματική λογική πραγματοποιείται σύμφωνα με τις οδηγίες που παρουσιάζονται στην εργασία [142].

8.3.1 Περιγραφή της Οντολογικής Αναπαράστασης των SIP Μηνυμάτων σε Κατηγορηματική Λογική

Όπως επεξηγήθηκε κατά την περιγραφή της οντολογικής αναπαράστασης των SIP μηνυμάτων στην ενότητα 8.2.1, κάθε SIP μήνυμα αποτελείται από την πρώτη γραμμή και από τις αντίστοιχες κεφαλίδες (ανάλογα με τον τύπο του μηνύματος). Οι τύποι 1 έως 5, που ακολουθούν, αντιστοιχούν στην αναπαράσταση κατηγορηματικής λογικής των SIP μηνυμάτων, ενώ οι υπόλοιποι (6 έως 15) αντιστοιχούν στις συσχετίσεις μεταξύ των στοιχείων που απαρτίζουν ένα SIP μήνυμα.

$$\forall x\ SIP\_Message\ (x) \Leftrightarrow \exists f\ FirstLine\ (f)$$
$$\wedge \exists^{\geq 3}\ h\ \ has\_header\ (h)\ (1)$$
$$\forall f\ FirstLine\ (f) \Rightarrow \text{Re}\ quest\ (f) \vee \text{Re}\ sponse\ (f)\ (2)$$
$$\forall x\ \text{Re}\ quest\ (x) \Rightarrow \neg \text{Re}\ sponse\ (x)\ (3)$$
$$\forall r\ \text{Re}\ quest\ (r) \Leftrightarrow \exists m\ Method\ (m) \wedge \exists rs\ \ \text{Re}\ source\ (rs)\ (4)$$
$$\forall m\ Method\ (m) = \{\ INVITE\ \vee REGISTER\ \vee OPTIONS\ \}\ (5)$$
$$\forall m1, a1\ is\_auth\ (m1, a1) \Rightarrow authenticate\ \ (a1)\ (6)$$
$$\forall m1, a1\ is\_auth\ (m1, a1) \Rightarrow SIP\_message\ (m1)\ (7)$$
$$\forall m1, t1\ message\ \_sent\ (m1, t1) \Rightarrow SIP\_message\ (m1)\ (8)$$
$$\forall m1, t1\ message\ \_sent\ (m1, t1) \Rightarrow time\ (t1)\ (9)$$
$$\forall m1, e1\ create\ (m1, e1) \Rightarrow SIP\_message\ (m1)\ (10)$$
$$\forall m1, e1\ create\ (m1, e1) \Rightarrow \ \ Event\ (e1)\ (11)$$
$$\forall m, h\ has\_header\ (m, h) \Rightarrow SIP\_message\ (m)\ (12)$$
$$\forall m, h\ has\_header\ (m, h) \Rightarrow header\ (h)\ (13)$$
$$\forall m, f\ inc\_first\ \ln(m, h) \Rightarrow SIP\_message\ (m)\ (14)$$
$$\forall m, f\ inc\_first\ \ln(m, h) \Rightarrow SIP\_message\ (m)\ (15)$$

8.3.2 Περιγραφή της Οντολογικής Αναπαράστασης των SIP Επιθέσεων σε Κατηγορηματική Λογική

Όσον αφορά το μετασχηματισμό της οντολογικής περιγραφής των επιθέσεων (βλέπε ενότητα 8.2.2) που μπορεί να εκδηλωθούν κατά των υπηρεσιών διαδικτυακής τηλεφωνίας σε κατηγορηματική λογική, ακολουθείται ακριβώς ο ίδιος τρόπος με αυτόν που αξιοποιήθηκε για το μετασχηματισμό της περιγραφής των SIP μηνυμάτων (βλέπε ενότητα 8.3.1). Συγκεκριμένα, σύμφωνα με την οντολογική αναπαράσταση (βλέπε Σχήμα 8–1) αλλά και τις περιγραφές του Κεφαλαίου 4, μια επίθεση μπορεί να ενταχθεί σε κάποια από τις παρακάτω κατηγορίες:

1. Επίθεση Μη Συμβατών Μηνυμάτων
2. Επίθεση Σηματοδοσίας
3. Επίθεση Πλημμύρας

Οι παραπάνω κατηγορίες επιθέσεων περιγράφονται σε κατηγορηματική λογική μέσω των τύπων 16 έως 22. Επιπροσθέτως, όπως έχει ήδη αναφερθεί στην ενότητα 8.2.2, ένα μη συμβατό μήνυμα είναι το συμπλήρωμα ενός συμβατού όπως περιγράφεται και στην αντίστοιχη αναπαράσταση κατηγορηματικής λογικής (βλέπε τύπο 23).

Οι επιθέσεις σηματοδοσίας, ανάλογα με την πολιτική ασφάλειας που ακολουθείται, μπορούν να αναπαρασταθούν με δύο τρόπους:

1. με την ύπαρξη δύο ή περισσοτέρων ίδιων SIP μηνυμάτων (σε διαφορετικές χρονικές στιγμές) (βλέπε τύπο 24).
2. με την ύπαρξη οποιουδήποτε μη αυθεντικοποιημένου SIP μηνύματος (βλέπε τύπο 25).

Επίσης οι επιθέσεις πλημμύρας μπορεί να είναι απλής πηγής ή πολλαπλών πηγών (βλέπε τύπο 26). Ως απλής πηγής χαρακτηρίζεται μια επίθεση πλημμύρας στην περίπτωση που ένας υπολογιστικός κόμβος κατά τη διάρκεια ενός συγκεκριμένου χρονικού διαστήματος υπερβεί

ένα προκαθορισμένο όριο απεσταλμένων SIP μηνυμάτων (βλέπε τύπο 27) ή ως πολλαπλής πηγής εάν πραγματοποιούνται ταυτόχρονα πολλές επιθέσεις πλημμύρας απλής πυγής (βλέπε τύπο 28). Οι υπόλοιποι τύποι (29 έως 39) αντιστοιχούν στις συσχετίσεις μεταξύ των στοιχείων της οντολογίας SIP επιθέσεων.

$$\forall m\ SIP\_Attack\ (m) \Leftrightarrow Malformed\ (m) \vee Signalling\ (m) \vee Flood\ (m) \quad (16)$$

$$\forall m\ Malformed\ (m) \Rightarrow \neg Singalling\ (m) \quad (17)$$

$$\forall m\ Malformed\ (m) \Rightarrow \neg Flood\ (m) \quad (18)$$

$$\forall m\ Flood\ (m) \Rightarrow \neg Singalling\ (m) \quad (19)$$

$$\forall m\ Flood\ (m) \Rightarrow \neg Malformed\ (m) \quad (20)$$

$$\forall m\ Signalling\ (m) \Rightarrow \neg Flood\ (m) \quad (21)$$

$$\forall m\ Signalling\ (m) \Rightarrow \neg Malformed\ (22)$$

$$\forall m\ \neg SIP\_Message\ (m) \Leftrightarrow Malformed\ (m) \quad (23)$$

$$\forall m1, m2\ SIP\_Message\ (m1) \wedge SIP\_Message\ (m2) \wedge SameAs\ (m1, m2) \Leftrightarrow Signalling\ (m1) \quad (24)$$

$$\forall m\ SIP\_Message\ (m) \wedge \neg Authenticate\ (m) \Leftrightarrow Singalling\ (m) \quad (25)$$

$$\forall m\ Single\ (m) \vee Multi\ (m) \Leftrightarrow Flood\ (m) \quad (26)$$

$$\forall m\ Single\ (m) \Leftrightarrow Number\_of\ (m) > thrshlds \wedge directed\ (m, t) \wedge source\_is\ (m, s) \quad (27)$$

$$\forall m\ Multi\ (m) \Leftrightarrow Number\ (Single\ (m)) > thrhsldm \quad (28)$$

$$\forall m\ Malformed\ (m) \Rightarrow SIP\_Attack\ (m) \quad (29)$$

$$\forall m\ Signalling\ (m) \Rightarrow SIP\_Attack\ (m) \quad (30)$$

$$\forall m\ Flood\ (m) \Rightarrow SIP\_Attack\ (m) \quad (31)$$

$$\forall m\ Single\ (m) \Rightarrow Flood\ (m) \quad (32)$$

$$\forall m\ Multi\ (m) \Rightarrow Flood\ (m) \quad (33)$$

$$\forall a, m\ Attack\_utilize\ (a, m) \Rightarrow SIP\_Attack\ (a) \quad (34)$$

$$\forall a, m\ Attack\_utilize\ (a, m) \Rightarrow SIP\_message\ (m) \quad (35)$$

$$\forall a, t\ attack\_t\ \arg et\ (a, t) \Rightarrow SIP\_Attack\ (a) \quad (36)$$

$$\forall a, t\ attack\_t\ \arg et\ (a, t) \Rightarrow t\ \arg et\ (t) \quad (37)$$

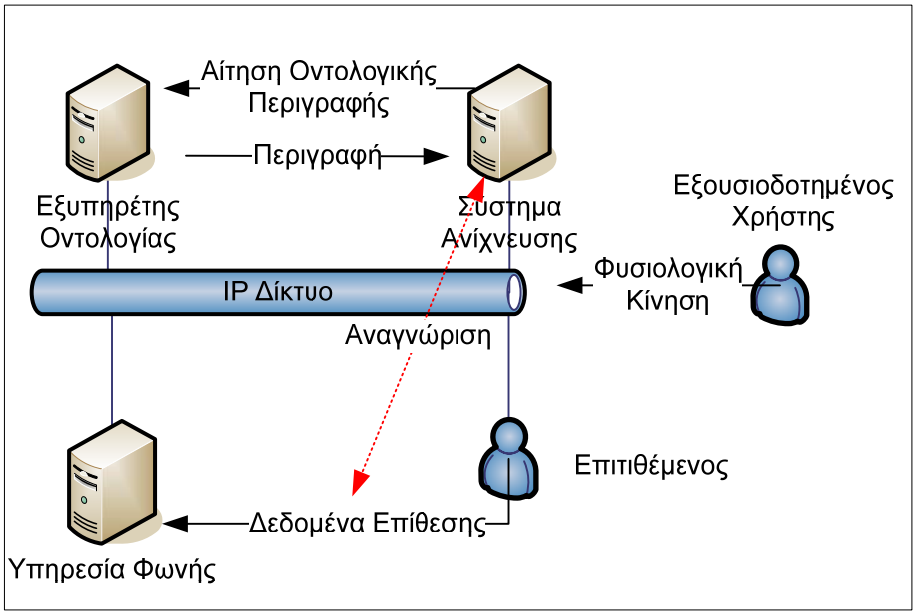
$$\forall a1, c1\ attack\_cause\ (a1, c1) \Rightarrow SIP\_Attack\ (a1) \quad (38)$$

$$\forall a1, c1\ attack\_cause\ (a1, c1) \Rightarrow consequence\ (c1) \quad (39)$$

8.4 Πρακτική Εφαρμογή της Οντολογικής Αναπαράστασης σε Πειραματικό Περιβάλλον

Η προτεινόμενη οντολογία μπορεί να εφαρμοσθεί σε πραγματικό περιβάλλον υπηρεσιών διαδικτυακής τηλεφωνίας είτε για την υλοποίηση των ελέγχων ασφαλείας που πρέπει να πραγματοποιηθούν στην υπηρεσία, είτε για την αναγνώριση επιθέσεων. Στο Σχήμα 8–6 απεικονίζεται η αρχιτεκτονική ενός συστήματος αναγνώρισης επιθέσεων προς υπηρεσίες διαδικτυακής τηλεφωνίας που αξιοποιεί την προτεινόμενη οντολογία. Τα βασικά στοιχεία που απαρτίζουν τη συγκεκριμένη αρχιτεκτονική είναι τα ακόλουθα:

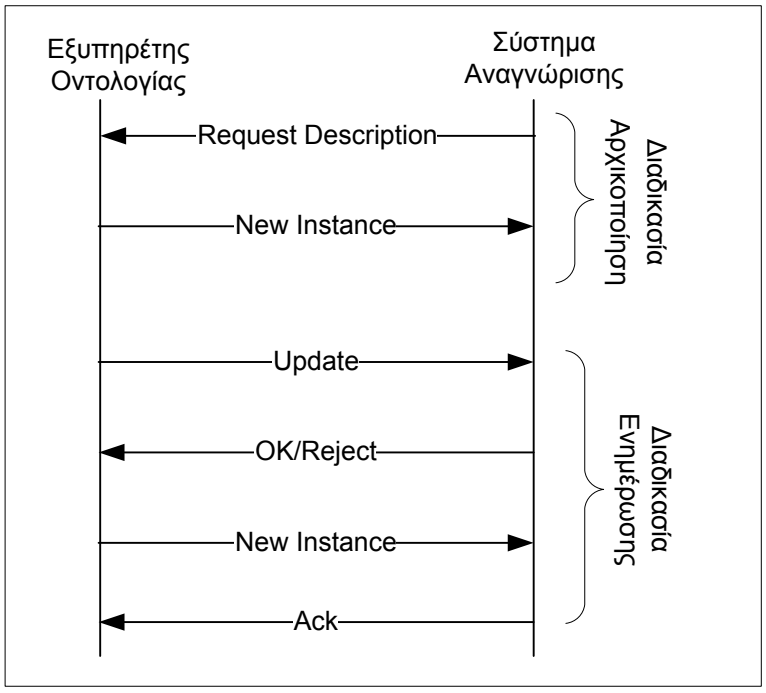
1. Ο Εξυπηρέτης Οντολογίας: Η οντότητα αυτή είναι υπεύθυνη για την αποθήκευση και τη δημοσιοποίηση της οντολογικής περιγραφής.
2. Ο Εξυπηρέτης Αναγνώρισης Προβλημάτων Ασφαλείας (ΕΑΠΑ): Η οντότητα αυτή είναι υπεύθυνη για την αναγνώριση επιθέσεων αξιοποιώντας την αντίστοιχη οντολογική περιγραφή.
3. Ο Πληρεξούσιος Εξυπηρέτης: Η οντότητα αυτή είναι υπεύθυνη για τη διαχείριση των πολυμεσικών κλήσεων.



Σχήμα 8–6. Αρχιτεκτονική Συστήματος Αναγνώρισης Επιθέσεων Διαδικτυακής Τηλεφωνίας με Αξιοποίηση της Προτεινόμενης Οντολογικής Περιγραφής

Αναφορικά με τη λειτουργία του συστήματος, οποτεδήποτε ο ΕΑΠΑ αρχικοποιείται δημιουργεί ένα αίτημα, προς τον «εξυπηρέτη οντολογίας», για την ανάκτηση της οντολογικής περιγραφής την οποία θα αξιοποιήσει για την αναγνώριση πιθανών εισβολών. Ο «εξυπηρέτης οντολογίας» αποκρίνεται στην αίτηση με την αντίστοιχη περιγραφή. Να σημειωθεί ότι υπάρχει η δυνατότητα ασύγχρονης ενημέρωσης του ΕΑΠΑ με νεότερες εκδόσεις της οντολογικής περιγραφής από τον «εξυπηρέτη οντολογίας».

Για την αποφυγή περιπτώσεων μη εξουσιοδοτημένης τροποποίησης της οντολογικής περιγραφής κατά τη μετάδοση της, για την επικοινωνία των δύο εξυπηρετών υιοθετείται είτε το TLS [90] είτε το IPSec [89]. Η παραπάνω διαδικασία απεικονίζεται συνοπτικά στο Σχήμα 8–7.



Σχήμα 8–7. Διαδικασία Ανάκτησης της Οντολογικής Περιγραφής

Ας υποθέσουμε ότι ο διαχειριστής της υπηρεσίας διαδικτυακής τηλεφωνίας επιθυμεί την αναγνώριση των μη συμβατών SIP REGISTER μηνυμάτων και, συνεπώς, έχει αναπτύξει την περιγραφή που έχει ήδη παρουσιαστεί στο Σχήμα 8–2.

Για να είναι εφικτή η επεξεργασία των εισερχόμενων SIP μηνυμάτων είναι απαραίτητο να μετασχηματιστούν στον κατάλληλο μορφότυπο (format). Για παράδειγμα, ας υποθέσουμε ότι μεταξύ των εισερχόμενων SIP μηνυμάτων υπάρχει το ακόλουθο μήνυμα:

"REGISTER AAAAA SIP/2.0"

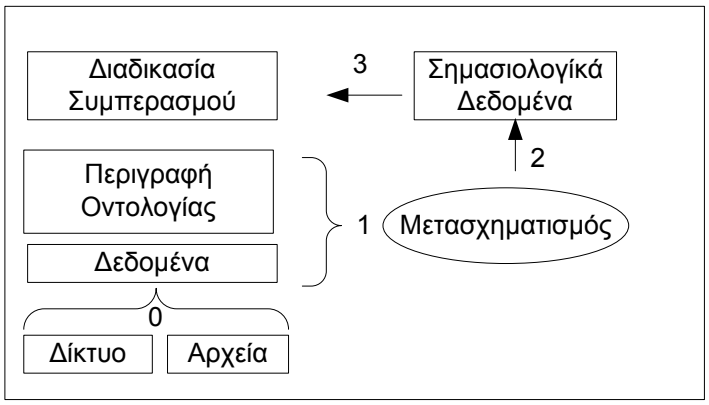
Ο απαραίτητος (σύμφωνα με τις προδιαγραφές της οντολογίας) μετασχηματισμός του μηνύματος αυτού παράγει το αποτέλεσμα που απεικονίζεται στο Σχήμα 8–8.

```
<sip_message id="register-11">
        <first_line rdf:resource="register11-fl"/>
</sip_message>
<first_line id="register11-fl>
        <method rdf:resource="#REGISTER"/>
        <uri>AAAAA</uri>
</first_line>
```

Σχήμα 8–8. Παράδειγμα Μετασχηματισμού Εισερχόμενου SIP Μηνύματος στο Μορφότυπο της Οντολογίας

Στη συνέχεια, η δομή που έχει προκύψει από το μετασχηματισμό του μηνύματος χρησιμοποιείται ως είσοδος στο εργαλείο συμπερασμού για τον έλεγχο της συμβατότητας του μηνύματος με τη γραμματική του SIP. Η διαδικασία αυτή πραγματοποιείται αξιοποιώντας την οντολογική περιγραφή (βλέπε Σχήμα 8–2) συνδυαζόμενη με τους αντίστοιχους τύπους που προσδιορίζουν την ύπαρξη ή όχι κάποια επίθεσης. Αναλυτικότερα, το εργαλείο συμπερασμού εφαρμόζει τους κανόνες που ορίζονται στο τμήμα «rule» του πόρου REGISTER (βλέπε Σχήμα 8–4) στο τμήμα του μετασχηματισμένου μηνύματος «uri» (βλέπε Σχήμα 8–8), συνάγοντας ότι το εισερχόμενο αυτό μήνυμα δεν είναι συμβατό με τις προδιαγραφές του SIP. Ταυτόχρονα ενεργοποιούνται οι τύποι 23 και 16, γεγονός που

δηλώνει ότι το συγκεκριμένο μήνυμα «συμμετέχει» σε επίθεση μη συμβατών μηνυμάτων. Η παραπάνω διαδικασία αναγνώρισης επιθέσεων αναπαρίσταται στο Σχήμα 8–9.



Σχήμα 8–9. Διαδικασία Συμπερασμού Ύπαρξης Επίθεσης σε Υπηρεσίες Διαδικτυακής Τηλεφωνίας με την χρήση της Προτεινόμενης Οντολογίας

8.5 Συμπεράσματα

Η τυπική αναπαράσταση της δομής και λειτουργίας του πρωτοκόλλου σηματοδοσίας που αξιοποιεί μια υπηρεσία διαδικτυακής τηλεφωνίας μπορεί να αποτελέσει ένα σημαντικό εργαλείο τόσο για τον έλεγχο του επιπέδου ασφαλείας της παρεχόμενης υπηρεσίας όσο και για την αναγνώριση πιθανών επιθέσεων κατά της υπηρεσίας.

Στην κεφάλαιο αυτό αξιοποιήθηκαν οντολογίες για να επιτευχθεί ο τυπικός φορμαλισμός του πρωτοκόλλου σηματοδοσίας SIP και των αντίστοιχων προβλημάτων ασφάλειας – επιθέσεων κατά των υπηρεσιών τηλεφωνίας που αξιοποιούν το συγκεκριμένο πρωτόκολλο. Η αναπαράσταση αυτή δεν παρέχει μόνο τη δυνατότητα δημιουργίας διαλειτουργικών υπηρεσιών ασφαλείας αλλά, επιπροσθέτως, δίνει τη δυνατότητα μετάβασης σε ένα τυπικό φορμαλιστικό μοντέλο καθώς βασίζεται στην κατηγορηματική λογική. Το αποτέλεσμα είναι ότι οι επιθέσεις που πραγματοποιούνται προς την παρεχόμενη υπηρεσία διαδικτυακής τηλεφωνίας μπορούν να αναγνωριστούν με ακρίβεια. Επίσης, υποστηρίζεται η δυνατότητα ανάπτυξης ενός ενιαίου περιβάλλοντος ασφάλειας, με κοινή σημασιολογία, μεταξύ διαφορετικών παρόχων υπηρεσιών διαδικτυακής τηλεφωνίας.

ΚΕΦΑΛΑΙΟ 9: Συμπεράσματα και Μελλοντικές Εργασίες

9.1 Συμπεράσματα

Η ασφάλεια των υπηρεσιών διαδικτυακής τηλεφωνίας αποτελεί ακρογωνιαίο λίθο για την αποδοχή τους από το ευρύ κοινό, καθώς επηρεάζει σε πολύ μεγάλο βαθμό την αξιοπιστία και τη διαθεσιμότητα τους. Η αξιοποίηση δικτύων ανοιχτής αρχιτεκτονικής δημιουργεί νέες ευκαιρίες επιθέσεων και παραβίασης της ασφάλειας των παρεχόμενων υπηρεσιών με αποτέλεσμα, πολλές φορές, οι χρήστες να είναι διστακτικοί στη χρήση τους. Είναι λοιπόν απαραίτητο, να υλοποιηθούν μέτρα ασφαλείας που στοχεύουν στη βελτίωση της αξιοπιστίας και διαθεσιμότητας των υπηρεσιών διαδικτυακής τηλεφωνίας, προσελκύοντας ταυτόχρονα την εμπιστοσύνη των χρηστών προς τις υπηρεσίες αυτές. Θα πρέπει να σημειωθεί ότι η ανάπτυξη υπηρεσιών ασφαλείας για τις υπηρεσίες διαδικτυακής τηλεφωνίας διαφοροποιείται σε μεγάλο βαθμό από τις αυτές του συμβατικού τηλεφωνικού δικτύου αφού το τελευταίο βασίζεται σε ένα δίκτυο κλειστής αρχιτεκτονικής όπου η πρόσβαση, φυσική και ιδεατή, είναι περιορισμένη. Διαφορετικές λύσεις έχουν ήδη προταθεί για την προστασία των υπηρεσιών διαδικτυακής τηλεφωνίας, παρ' όλα αυτά, σε ελάχιστες περιπτώσεις λαμβάνονται υπόψη οι ιδιαίτερες απαιτήσεις που παρουσιάζουν οι υπηρεσίες του τύπου αυτού.

Στη διδακτορική αυτή διατριβή παρουσιάζονται αναλυτικά οι απειλές και οι ευπάθειες που προσπαθούν να εκμεταλλευτούν κακόβουλοι χρήστες για την εκδήλωση επιθέσεων, ενώ ταυτόχρονα προτείνονται οι κατάλληλοι μηχανισμοί για την αναγνώριση και αντιμετώπιση των περιστατικών αυτών. Οι προτάσεις αυτές εστιάζουν στις υπηρεσίες διαδικτυακής τηλεφωνίας που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP. Παράλληλα τα αντίμετρα αυτά αξιολογούνται σε ότι αφορά την αποτελεσματικότητα και αποδοτικότητα τους σε πειραματικό περιβάλλον. Πιο συγκεκριμένα, αναπτύσσεται μια αρχιτεκτονική τριών επιπέδων η οποία μπορεί να αντιμετωπίσει επιτυχώς επιθέσεις μη συμβατών μηνυμάτων, σηματοδοσίας και πλημμύρας.

Στο πρώτο επίπεδο εφαρμόζεται ένα προληπτικός μηχανισμός που διασφαλίζει την αυθεντικότητα και την ακεραιότητα των μηνυμάτων σηματοδοσίας, προστατεύοντας ταυτόχρονα από επιθέσεις σηματοδοσίας. Στο δεύτερο επίπεδο, πραγματοποιούνται οι κατάλληλοι έλεγχοι για την ανίχνευση μη συμβατών μηνυμάτων. Οι έλεγχοι αυτοί βασίζονται στις προδιαγραφές του πρωτοκόλλου σηματοδοσίας SIP. Επιπλέον στο επίπεδο αυτό πραγματοποιούνται εκτεταμένοι έλεγχοι για τον εντοπισμό περιπτώσεων εισαγωγής κακόβουλου κώδικα στα μηνύματα σηματοδοσίας. Στο τρίτο επίπεδο, που ουσιαστικά λειτουργεί παράλληλα με τα άλλα δύο επίπεδα, εφαρμόζεται ένα μηχανισμός αναγνώρισης επιθέσεων πλημμύρας. Ο μηχανισμός αυτός βασίζεται σ' ένα σύστημα καταγραφής της εισερχόμενης κίνησης που αξιοποιεί Bloom φίλτρα. Στα πλαίσια του συγκεκριμένου συστήματος έχει ορισθεί μια νέα μετρική, η «απόσταση συνόδου», η οποία, σε συνδυασμό με κάποια όρια επιτρεπτών τιμών που προσδιορίζονται, αξιοποιείται για να εντοπιστούν περιπτώσεις που ο υπολογιστικό φόρτος που ένας πάροχος καλείται να αντιμετωπίσει είναι μεγαλύτερος από αυτόν που μπορεί να υποστηρίξει.

Από την αξιολόγηση των προτεινόμενων μέτρων προστασίας σε πειραματικό περιβάλλον προκύπτει ότι η μέση καθυστέρηση που εισάγεται δεν υπερβαίνει το 1 μιλι-δευτερόλεπτο, γεγονός που αποδεικνύει την εφικτότητα της πρακτικής εφαρμογής της προτεινόμενης αρχιτεκτονικής.

Πέρα και πάνω από τους μηχανισμούς αυτούς η ανάπτυξης μιας ομοιόμορφης περιγραφής κοινής σημασιολογίας είναι δυνατόν να αποτελέσει τον οδηγό προς ένα ενιαίο περιβάλλον

αντιμετώπισης των προβλημάτων ασφαλείας μεταξύ διαφορετικών παρόχων. Για το λόγο αυτό πραγματοποιείται ο φορμαλισμός των δομικών στοιχείων του πρωτοκόλλου σηματοδοσίας SIP και των πιθανών προβλημάτων ασφάλειας με την χρήση οντολογιών ώστε να είναι δυνατή τόσο η δημιουργία πραγματικών υπηρεσιών ασφάλειας βασισμένες σε αυτές όσο και η τυπική αναπαράσταση τους σε κατηγορηματική λογική.

9.2 Προοπτικές Περαιτέρω Έρευνας

Οι τεχνολογικές εξελίξεις των σταθερών και κινητών δικτύων καθώς και η καθιέρωση του διαδικτύου ως δίκτυο κορμού για την παροχή οποιασδήποτε υπηρεσίας, αποτελούν ισχυρές ενδείξεις ότι το διαδίκτυο θα αποτελέσει το βασικό φορέα παροχής φωνητικών υπηρεσιών (υπηρεσίες τηλεφωνίας). Στο γεγονός αυτό συμβάλει και η ενσωμάτωση των πρωτοκόλλων σηματοδοσίας που αξιοποιούνται στο διαδίκτυο, όπως το SIP, στα συστήματα κινητών επικοινωνιών 3ης γενεάς, που ουσιαστικά οδηγεί στην ενοποίηση των παρεχόμενων υπηρεσιών τηλεφωνίας.

Ως εκ’ τούτου οι πάροχοι υπηρεσιών τηλεφωνίας (των επόμενων γενεών δικτύων) μεταξύ των άλλων θα πρέπει να διερευνήσουν και να αντιμετωπίσουν τις απειλές και τις επιθέσεις που δημιουργούνται από την ανάπτυξη υπηρεσιών τηλεφωνίας (βασισμένων στο διαδίκτυο) σε ασύρματα δίκτυα, μελετώντας ταυτόχρονα τις επιπτώσεις που μπορεί να προκύψουν από την εκδήλωση κάθε επίθεσης. Επιπλέον, υπό το πρίσμα ενός ενιαίου περιβάλλοντος θα πρέπει να μελετηθεί η εφαρμογή και ανάπτυξη ενός συστήματος νόμιμης παρακολούθησης των υπηρεσιών τηλεφωνίας, με στόχο την αποφυγή αξιοποίησης των υπηρεσιών για μη θεμιτούς σκοπούς. Τέλος, η μαθηματική μοντελοποίηση των υπηρεσιών ασφαλείας διαδικτυακής τηλεφωνίας είναι βέβαιο ότι θα αποτελέσει ένα σημαντικό εργαλείο για την ανάπτυξη αξιόπιστων υπηρεσιών.

ΚΕΦΑΛΑΙΟ 10: Βιβλιογραφικές Αναφορές

[1] Bates, R. J, "*Broadband Telecommunications Handbook*", McGraw-Hill Professional, Second Edition, 2002.

[2] Schulzrinne, H., "Converging on internet telephony," *Internet Computing, IEEE ,* vol.3, no.3, pp.40-43, May/Jun 1999.

[3] Darpa Internet Program Protocol Specification, "Internet Protocol", *RFC 791*, September 1981.

[4] John Q Wlaker, Jeffrey T. Hicks, "*Taking charge of your VoIP Project*", Cisco Press, September 2005.

[5] VoIP IP Telephony, available on line: http://snapvoip.blogspot.com/2007/03/virtual-voip-carriers-vvcs-will-grow-to.html

[6] Sicker, D. C.; Lookabaugh, T., "VoIP Security: Not An Afterthough", vol. 6, no.2 *Queue ACM*, September 2004.

[7] Shannon M.L., "Phone Book: The Latest High-Tech Techniques And Equipment For Preventing Electronic Eavesdropping, Recording Phone Calls, Ending Harassing Calls, And Stopping Toll Fraud", Paladin Press, July 1998.

[8] Stewart ,R., Xie, Q., Morneault K. Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla M., Zhang L., Paxson V., "Stream Control Transmission Protocol", *RFC 2960*, October 2000.

[9] Darpa Internet Program Protocol Specification, "Transmission Control Protocol", *RFC 793*, September 1981

[10] International Telecommunications Union, "Recommendation H.323", available on line http://www.itu.int/rec/T-REC-H.323/e

[11] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Spark, R., Handley, M, Schooler, E.m "Session Initiation Protocol", *RFC 3261*, June 2002.

[12] Fielding,R., Mogul, J., Gettys, J., Masinter,L., Frystyk, H., Leach, P., Berners-Lee, T., Hypertext Transfer Protocol (HTTP/1.1), *RFC 2616*, June 1999

[13] Schulzrinne, H.; and Rosenberg, J., "A Comparison of SIP and H.323 for Internet Telephony", *in the proceedings of Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, Cambridge, 1998.

[14] Dalgica,I., Fangb H., "*Comparison of H.323 and SIP for IP Telephony Signaling*" available on line: http://www.cs.columbia.edu/~hgs/papers/ others/1999/Dalg9909_Comparison.pdf

[15] Varshney, U., Snow, A., McGivern, M., and Howard, C. "Voice over IP", *Communications of the ACM,* January 2002.

[16] Hersent, O., Petit, J-P., Gurle D., "Beyond VoIP Protocols: Understanding Voice Technology and Networking Techniques for IP Telephony ", Wiley, March 2005.

[17] VoIP SA, "*VoIP Security Tool List*", available on line http://www.voipsa.org/Resources/tools.php

[18] Ofir, A., "The Trivial Cisco IP Phones Compromise Security analysis of the implications of deploying Cisco Systems' SIP-based IP Phones model 7960", available on line http://www.sys-security.com/html/projects/VoIP.html

[19] Geneiatakis D., Dagiouklas A., Kambourakis G., Lambrinoudakis C., Gritzalis S., Ehlert S., Sisalem D., "Survey of Security Vulnerabilities in Session Initiation Protocol", *IEEE Communications Surveys and Tutorials*, Vo. 8, No. 3, pp. 68-81, IEEE Press, 2006.

[20] Geneiatakis D., Kambourakis G., Dagiouklas A., Lambrinoudakis C., Gritzalis S., "Session Initiation Protocol Security Mechanisms: A state-of-the-art review", *in the proceedings of Fifth International Network Conference*, S. Furnell, S. K. Katsikas (Eds.), pp. 147-156, , Samos, Greece, Ziti Pubs, July 2005.

[21] Dagiuklas T., Geneiatakis D., Kambourakis G., Sisalem D, Ehlert S., Fiedler J. Markl, J., Rokos, M., Botron, O., Rodriguez J., and Liu, J., "*General Reliability and Security Framework for VoIP Infrastructures*", available on line http://www.snocer.org, 2005.

[22] Geneiatakis, D., Kambourakis G., Dagiouklas, A., Lambrinoudakis, C., Gritzalis S., "A Framework for Detecting Malformed Messages in SIP Networks", *in the proceeding of 14th IEEE International Workshop on Local and Metropolitan Area Networks*, Chania, Greece, IEEE Press, September 2005.

[23] Geneiatakis D., Kambourakis, G., Lambrinoudakis, C., Dagiouklas, A., Gritzalis S., "SIP Message Tampering: THE SQL code INJECTION attack", *in the proceeding of 13th IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM '05)*, N. Rozic et al. (Eds.), pp. 176-181, Split, Croatia, September 2005

[24] Geneiatakis D., Dagiouklas, A., , Lambrinoudakis, C., Kambourakis, G., Gritzalis S.,"Novel Protecting Mechanism for SIP-Based Infrastructure against Malformed Message Attacks: Performance Evaluation Study*", in the proceedings of 5th International Conference on Communication Systems, Networks and Digital Signal Processing (CSNDSP '06*), M. Logothetis et al. (Eds.), Patras, Greece, July 2006

[25] Geneiatakis D., Kambourakis, G., Lambrinoudakis, C., Dagiouklas, A., Gritzalis S., "A framework for protecting SIP-based infrastructure against Malformed Message Attacks", *Computer Networks*, Vo. 51, No. 10, pp. 2580-2593, 2007, Elsevier

[26] Geneiatakis D., Lamrinoudakis C., "A Lightweight Protection Mechanism against Signaling Attacks in a SIP-Based VoIP Environment", *Telecommunication Systems*, Vo 36, No 4, pp. 153-159, Springer, February 2008,

[27] Geneiatakis D., Lamrinoudakis C. "Utilizing Bloom Filters for Detecting Flooding Attacks against SIP Based Services" Submitted for publication in *Computer and Security*, Elsevier,

[28] Geneiatakis D., Lamrinoudakis C, "An Ontology Description for SIP Security Flaws, ", *Computer Communication*, Vo. 30, No. 6, pp. 1367-1374, Elsevier 2007

[29] Geneiatakis, D., Lambrinoudakis, C., Kambourakis, G., "An Ontology Based-Policy for Deploying Secure SIP- based VoIP Services" Submitted to publication in Computer and Security, Elsevier

[30] Carpenter, B., "Architectural Principles of the Internet", *RFC 1958*, June 1996.

[31] Bosse, J., "*Signaling in Telecommunication Networks*" Wiley-Interscience, January 1997.

[32] ISO/IEC 7498, Information Processing Systems – Open Systems Interconnection Reference Model.

[33] Postel, J., "User Datagram Protocol (UDP) ", *RFC 768*, August 1980.

[34] Schulzrinne, H., Casner, S., Frederick R., Jacobson V., "RTP: A Transport Protocol for Real-Time Applications", *RFC 3550*, July 2003.

[35] Mockapetris P., Domain Names- Implementation and Specification, *RFC 1035*, November 1987.

[36] Droms, R., "Dynamic Host Configuration Protocol", *RFC 2131*, March 1997.

[37] Tanenbaum Andrew S., "*Computer Networks*", Prentice Hall, 1996

[38] Androutsellis-Theotokis, S. and Spinellis, D. "A survey of peer-to-peer content distribution technologies", *ACM Computing Surveys,* Vol 36, Iss. 4, December 2004.

[39] Saltzer, J. H., Reed, D. P., and Clark, D. D., "End-to-end arguments in system design", *ACM Transactions on Computer Systems* Vol. 2, Iss. 4, November 1984.

[40] Andreasen ,F., Foster, B., "Media Gateway Control Protocol (MGCP) ", *RFC 3435*, January 2003.

[41] Klessin J., "Simple Mail Transfer Protocol", *RFC 2821*, April 2001.

[42] Rosenberg J., "The Session Initiation Protocol (SIP) UPDATE Method", *RFC 3311*, September 2002.

[43] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., Gurle D., "Session Initiation Protocol (SIP) Extension for Instant Messaging", *RFC 3428*, December 2002.

[44] Roach, A.B., "Session Initiation Protocol (SIP)-Specific Event Notification", *RFC 3265*, June 2002.

[45] Berners-Lee, T., Masinter L., "Uniform Resource Identifier (URI): Generic Syntax", *RFC 2396*, January 2005.

[46] Borenstein, N., Freed, N., "Multipurpose Internet Mail Extensions Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", *RFC 1521*, September 1993.

[47] Vemuri, A., Peterson J., "Session Initiation Protocol for Telephony", *RFC 3372*, September 2002.

[48] International Telecommunication Unit, "Recommendation X.680, Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation" available online http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf

[49] Faltstrom P., Mealing, M., "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", *RFC 3761*, April 2004

[50] Mealing, M., Daniel R., "The Naming Authority Pointer NAPTR DNS Resource Record", *RFC 2915,* September 2000.

[51] Ferguson, N., Schneier, B., "*Practical Cryptography*", John Wiley & Sons, 2003.

[52] Bates, R. J, "*Broadband Telecommunications Handbook*", McGraw-Hill Professional, Second Edition, 2002.

[53] Wikipedia, "Phreaking" available on-line http://en.wikipedia.org/wiki/Phreaking

[54] Wikipedia, "Telephone Tapping" http://en.wikipedia.org/wiki/Telephone_tapping

[55] Henry (Hank) M. Kluepfel, "Securing a Global Village and its Resources: Base line Security for Inter connected Signaling System # 7 Telecommunications Networks", *in the proceedings of the 1st ACM conference on Computer and communications security*,1993.
[56] Moore, T., Kosloff, T., Keller, J., Manes, G., Shenoi, S., "Signaling System 7 (SS7) Network Security", *in the proceeding of 45th Midwest Symposium on Circuits and Systems*, 2002
[57] G.Lorenz, T. Moore, G. Manes, J. Hale, S. Shenoi., "Securing SS7 Telecommunications Networks", *in the proceeding of the 2001 IEEE Workshop on Information Assurance and Security*, 2001.
[58] Sengar, H., Wijesekera, D., Jajodia, S., "Authentication and integrity in telecommunication signaling network," *in the proceedings of 12th IEEE International Conference and Workshops on the Engineering of Computer-based Systems*, April 2005
[59] Oxford Reference Online Premium, available on line http://www.oxfordreference.com/
[60] Butcher, D., Li, X., Guo , J., "Security Challenge and Defense in VoIP Infrastructures," *IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews*, , vol.37, no.6, pp.1152-1162, November 2007.
[61] VOIPSA, "VoIP Security and Privacy Threat Taxonomy" available on line http://www.voipsa.org/Activities/taxonomy.php, October 2005
[62] Sisalem, D., Kuthan, J., Ehlert, S., "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," *Network, IEEE* , vol.20, no.5pp. 26- 31, 2006.
[63] Ruishan, Xinyuan Wang, Xiaohui Yang, Xuxian Jiang, "Billing Attacks on SIP-Based VoIP Systems", *in the proceedings of first USENIX workshop on offensive technologies*, August, 2007.
[64] Wieser., C., Laakso, M., Schulzrinne, H., "Security Testing of SIP Implementations", Available on line: http://compose.labri.fr/documentation/sip/Documentation/Papers/Security/Papers/462.pdf
[65] Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao, "Active Traffic Analysis Attacks and Countermeasures", Available on line : http://students.cs.tamu.edu/xinwenfu/paper/ICCNMC03_Fu.pdf
[66] Paxson V., Auman M., Dawson S., Fenner W., Griner J., Heavens J., Labey K., Semke J., and B.Volt ., "Known TCP implementation problems", *RFC 2525*, March 1999.
[67] CERT-In Advisory CIAD-2003-09, "Buffer Overrun In RPC Interface Could Allow Code Execution and Denial of Service", August 2003.
[68] Fontana J., "Exchange Server 5.5 Bug Could Be Exploited for Attacks", available online http://www.pcworld.com/resource/article/0,aid,33882,00.asp , November 2000.
[69] "Asterisk SIP Implementation Issue", available online http://www.atstake.com/research/advisories/2003/a090403-1.txt, August 2003.
[70] CERT Advisory CA-2004-01, "Multiple H.323 Message Vulnerabilities", available online http://www.cert.org/advisories/CA-2004-01.html, April 2004.
[71] CERT Advisory CA-2003-06, "Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP) ", available online http://www.cert.org/advisories/CA-2003-06.html February 2003.
[72] Wagner D., Foster J. S., Brewer E. A., Aiken A., "A First Step towards Automated Detection of Buffer Overrun Vulnerabilities", *in the Proceedings of the ISOC Symposium on Network and Distributed System Security (SNDSS)*, February 2000.
[73] CERT Advisory CA-2000-02, "Malicious HTML Tags Embedded in Client Web Requests", available online http://www.cert.org/advisories/CA-2000-02.html
[74] CERT Vulnerability Note, "VU#282403", available online http://www.kb.cert.org/vuls/id/282403
[75] CERT Vulnerability, "Note VU#496064", available online http://www.kb.cert.org/vuls/id/496064
[76] Anley, C., "Advanced SQL Injection In SQL Server Applications", An NGSSoftware Insight Security Research (NISR) Publication, 2002.
[77] "SIP Express Router", http://www.iptel.org/ser
[78] http://vovida.org
[79] Mirkovic J., Dietrich S., Dittrich D., Reiher P., "*Internet Denial of Service: Attack and Defense Mechanisms*", Prentice Hall, 2005.
[80] Carl, G., Kesidis, G., Brooks, R.R., Suresh, Rai.,, "Denial-of-service attack-detection techniques", *Internet Computing IEEE*, Vol.10, Iss.1, 2006
[81] Peng, T., Leckie, C., Ramamohanarao, K., "Survey of network-based defense mechanisms countering the DoS and DDoS problems", *ACM Computing Surveys*, Vol.39, Iss.1, April 2007.

[82] CERT, Advisory CA-1996-21, "TCP SYN Flooding and IP Spoofing Attacks", available online http://www.cert.org/advisories/CA-1996-21.html, September 1996
[83] Eddy, W., "TCP SYN Flooding Attacks and Common Mitigations", *RFC 4987*, August 2007.
[84] Gibson, S., "DRDoS Distributed Reflection Denial of Service", available online http://grc.com/dos/drdos.htm, 2002.
[85] Franks, J., Hallam-Baker P., Hostetler J. Lawrence S., Leach P., Luotonen A., Stewart L., , "HTTP Authentication: Basic and Digest Access Authentication", *RFC 2617*, June 1999.
[86] Zhang, G., Ehlert S., Magedanz, T., Sisalem D., "Denial of Service Attack and Prevention on SIP VoIP Infrastructures Using DNS Flooding", in the proceeding of *Principles, Systems and Applications of IP Telecommunications (IPTComm2007) Conference,* July 2007.
[87] Call Jacking: Phreaking the BT Home Hub, available online http://www.gnucitizen.org/blog/call-jacking
[88] Stamp, M., "Information Security: Principles and Practice", Wiley-Interscience , 2005
[89] Thayer, R., Doraswamy, N., Glenn R., "IP Security Document Roadmap", *RFC 2411*, November 1998.
[90] Dierks T., Rescoral, E., "The Transport Layer Security (TLS) Protocol Version 1.1", *RFC 4346*, April 2006.
[91] B. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", *RFC 3851*, July 2004.
[92] Salsano, S.; Veltri, L.; Papalilo, D., "SIP security issues: the SIP authentication procedure and its processing load," *Network, IEEE* , vol.16, no.6, 2002.
[93] Bilien, J., Eliasson, E., Orrblad, J-O. Vatn, J., "Secure VoIP: call establishment and media protection", *in the proceedings of 2nd Workshop on Securing Voice over IP*, June 2004.
[94] Hong, K., Jung, S., Iacono L. Lo., Ruland C., "Impacts of Security Protocols on Real-Time Multimedia Communications" *in the proceeding of 5th International Workshop on Information Security Applications*, 2004.
[95] Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman K., "The Secure Real-time Transport Protocol (SRTP)", *RFC 3711*, March 2004.
[96] Arkko, J., Carrara, E., Lindholm F., Naslund, M., Norrman K., "MIKEY: Multimedia Internet KEYing", *RFC 3840*, August 2004.
[97] Ono, K., Tachimoto, S., "Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP)", *RFC 4189*, October 2005.
[98] Cao, F., Jennings, C., "Providing response identity and authentication in IP telephony", *in the proceedings of The First International Conference on Availability, Reliability and Security*, April 2006
[99] Yang, Chou-Chen., Wang, Ren-Chiun., Liu, Wei-Ting., "Secure authentication scheme for session initiation protocol", *Computers & Security*, Vol.24, Iss.5, August 2005.
[100] Wu, Yu-Sung., Bagchi, S., Garg, S., Singh, N., "SCIDIVE: a stateful and cross protocol intrusion detection architecture for voice-over-IP environments", *in the proceedings of International Conference on Dependable Systems and Networks*, June 2004.
[101] Ding, Yanlan., Su, Guiping., "Intrusion detection system for signal based SIP attacks through timed HCPN", *in the proceedings of Second International Conference on Availability, Reliability and Security*, April 2007.
[102] Reynolds, B., Ghosal D., "Secure IP Telephony using Multi-layered Protection", *in the proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2003.
[103] Sengar, H., Haining Wang, Wijesekera, D., Jajodia, S., "Fast Detection of Denial-of-Service Attacks on IP Telephony", *in the proceeding of 14th IEEE International Workshop on Quality of Service*, June 2006.
[104] Chen, E.Y., "Detecting DoS attacks on SIP systems", in the proceedings of 1st IEEE Workshop on VoIP Management and Security, April 2006.
[105] Sengar, H., Wijesekera D., Haining, Wang., Jajodia, S., "VoIP Intrusion Detection Through Interacting Protocol State Machines," *in the proceedings of International Conference on Dependable Systems and Networks*, 2006.
[106] Fiedler, J., Kupka, T., Ehlert, S., Magedanz, T., Sisalem, D., "VoIP Defender: Highly Scalable SIP-based Security Architecture", *in the proceeding of Principles, Systems and Applications of IP Telecommunications (IPTComm2007) Conference*, July 2007.
[107] Liufei Wu, Yuqing Zhang, Fengjiao Wang, "A New Provably Secure Authentication and Key Agreement Protocol for SIP Using ECC", *Computer Standards & Interfaces*, accepted for publication, January 2008.

[108] Bremler-Barr, A., Halachmi-Bekel, R., Kangasharju, J., "Unregister Attacks in SIP," *in the proceeding of 2nd IEEE Workshop on Secure Network Protocols*, November 2006.
[109] Srinivasan, R., Vaidehi, V., Harish, K., LakshmiNarasimhan, K., LokeshwerBabu, S., Srikanth, V., "Authentication of Signaling in VoIP Applications," *in the proceeding of Asia-Pacific Conference on Communications*, October 2005.
[110] Chia-Chen Chang, Yung-Feng Lu, Ai-Chun Pang,Tei-Wei Kuo, "Design and Implementation of SIP Security", *in the proceedings of Information Networking Convergence in Broadband and Mobile Networking*, February 2005.
[111] Wojciech Mazurczyk, Zbigniew Kotulski, "New VoIP Traffic Security with Digital Watermarking", *in the proceedings of 25th International Conference on Computer Safety, Reliability, and Security*, September 2006.
[112] Niccolini, S., Garroppo, R.G., Giordano, S., Risi, G., Ventura, S., "SIP intrusion detection and prevention: recommendations and prototype implementation", *in the proceedings of 1st IEEE Workshop on VoIP Management and Security*, April 2006.
[113] Nassar, M., Niccolini, S., State, R., Ewald, T., "Holistic VoIP intrusion detection and prevention system", *in the proceeding of Principles, Systems and Applications of IP Telecommunications (IPTComm2007) Conference*, July 2007.
[114] Christensen, S., Jørgensen, J. B., *"Teaching Coloured Petri Nets: Examples of Courses and Lessons Learned"*, Lectures on Concurrency and Petri Nets, Lectures on Concurrency and Petri Nets, Springer, July 2004.
[115] Diffie W., Hellman, M. E., "New Directions in Cryptology", *IEEE Transactions on Information Theory*, vol. IT-22, November 1976.
[116] Moizard A., "The GNU oSIP library", availabe online http://www.gnu.org/software/osip/osip.html
[117] Brodsky, B.E, Darkhovsky B.S., *"Nonparametric Methods in Changepoint Problems"*, Kluwer Academic Publisher 1993.
[118] "Hellinger Distance", available online http://eom.springer.de/h/h046890.htm
[119] Provos, N., "A Virtual Honeypot Framework", *in the Proceedings of the 13th USENIX Security Symposium*, August 2004.
[120] Krawczyk, H., Bellare, M., Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", *RFC 2104*, February 1997.
[121] Schulzrinne, H., Oran, D., Camarillo G., "The Reason Header Field for the Session Initiation Protocol", *RFC 3326,* December 2002.
[122] Niccolini S., Tartarelli S., Stiemerling M., Srivastava S., "SIP Extensions for SPIT identification", work in progress available on http://tools.ietf.org/html/draft-niccolini-sipping-feedback-spit-03.
[123] Willis, D., Hoeneisen, B., "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", *RFC 3327*, December 2002.
[124] Garcia-Martin, M., Henrikson E., Mills D. "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP) ", *RFC 3455*, January 2003.
[125] Rescorla, E., "SSL and TLS – Designing and Building Secure Systems", Addison Wesley, October, 2000.
[126] Jablon D. P., "Strong Password-Only Authenticated Key Exchange", *ACM SIGCOMM Computer Communication Review*, Vol. 26 Iss 5, October 1996.
[127] "PJSIP, Open Source SIP Stack", available online http://www.pjsip.org/
[128] "OpenSSL Library", available online http://www.openssl.org
[129] "SNORT, - The de facto standard for intrusion detection-prevention", available online http://www.snort.org
[130] "Perl Compatible Regular Expressions", available online http://www.pcre.org
[131] "An Open Source Soft Phone - KPhone", available online http://www.kphone.org
[132] "SIPBobmer", available online http://www.metalinkltd.com/downloads.php
[133] Bloom, B. H. "Space/time trade-offs in hash coding with allowable errors", *Communications of the ACM*, Vol. 13 Iss. 7, July 1970
[134] Li, Fan., Pei, Cao., Almeida, J., Broder, A.Z., "Summary cache: a scalable wide-area Web cache sharing protocol" IEEE/ACM Transactions on Networking, Vol.8, Iss.3, June 2000.
[135] Xiao, B., Chen, W., He, Y., "A novel approach to detecting DDoS Attacks at an Early Stage", *The Journal of Supercomputing*, Vol.36, Iss.3, June 2006.
[136] "Bro Intrusion Detection System", available online http://bro-ids.org/

[137] Gruber, T. R., "Towards principles for the design of ontologies used for knowledge sharing", *International Journal of Human-Computer Studies*, Vol.43, Iss. 5-6, 1995.
[138] McGuinness D.L., Fikes. R., Hendler J., Stein, L.A., "DAML+OIL: an ontology language for the Semantic Web," *Intelligent Systems IEEE*, vol.17, no.5, 2002.
[139] "OWL WEb Ontology Language Guide" available online: http://www.w3.org/TR/owl-guide/
[140] "Resource Description Framework (RDF) ", http://www.w3.org/RDF/
[141] "Renamed Abox and Concept Expression Reasoner (RACER)", Available on line: http://www.sts.tu-harburg.de/~r.f.moeller/racer/
[142] Grosof, B. N.; Horrocks, I.; Volz, R.; Decker, S., "Description logic programs: combining logic programs with description logic", *in the Proceedings of 12th International Conference on World Wide Web*, May 2003.

Παράρτημα Ι

Part A: SIP-Message Sub-ontology

```
<daml:Class rdf:ID=SIP_MESSAGE>
                        <daml:subclassof>
                                <daml:Restriction>
                                        <daml:onProperty rdf:resource="first_line"/>
                                        <daml:hasClass rdf:resource="sip_ first_line"/>
                                </daml:Restriction>
                        </dam:subclassof>
                        <daml:subclassof>
                                <daml:Restriction>
                                        <daml:onProperty rdf:resource="first_line"/>
                                        <daml:cardinality>1</daml:cardinality>
                                </daml:Restriction>
                        </daml:subclassof>
                        <daml:subclassof>
                                <daml:Restriction>
                                        <daml:onProperty rdf:resource="headers">
                                        <daml:mincardinality>3</daml:cardinality>
                                </daml:Restriction>
                        </daml:subclassof>
                        <daml:subclassof>
                                <daml:Restriction>
                                        <daml:onProperty rdf:resource="headers">
                                        <daml:range rdf:resource="sip_headers">
                                </daml:Restriction>
                        </daml:subclassof>
</daml>

<daml:Class rdf:ID=sip_first_line>
                        <daml:disjointUnionOf parseType="daml:collection">
                                <daml:Class rdf:about="request"/>
                                <daml:Class rdf:about="responses"/>
```

```
                    </daml:disjointUnionOf>
</daml>

<daml:DatatypeProperty rdf:ID="uri">
                    <daml:domain rdf:resource="#sip_first_line"/>
                    <rdf:range rdf:Resource="string"/>
</daml:DatatypeProperty>

<daml:Class rdf:ID="request">
</daml:Class>

<daml:objectProperty ref:ID="used_method">
                    <daml:domain resource="#request"/>
                    <daml:range rdf:resource="#methods"/>
</daml:objectProperty>

<daml:Class rdf:ID=sip_headers>
</daml>
<daml:DatatypeProperty rdf:ID="header_name">
                    <daml:domain rdf:resource="#sip_headers"/>
                    <rdf:range rdf:Resource="string"/>
</daml>
<daml:DatatypeProperty rdf:ID="rule">
                    <daml:domain rdf:resource="#sip_ headers"/>
                    <rdf:range rdf:Resource="string"/>
</daml>

<daml:Class rdf:ID="methods">
                    <daml:oneOf ref:parseType="Collection">
                        <daml:Thing rdf:about="REGISTER">
                        <daml:Thing rdf:about="INVITE">
                        <daml:Thing rdf:about="SUBSCRIBE">
                        <daml:Thing rdf:about="BYE">
                        <daml:Thing rdf:about="ACK">
                        <daml:Thing rdf:about="CANCEL">
```

```
                        <daml:Thing rdf:about="OPTIONS">
                    </daml:oneof>
</daml>
```

Part B: SIP-Attack Sub-ontology

```
<daml:Class rdf:ID=attack>
</daml:Class>
<daml:ObjectProperty rdf:ID="attack_utilize">
                    <daml:domain rdf:resource="#attack"/>
                    <rdf:range rdf:Resource="#SIP_MESSAGE"/>
</daml:ObjectProperty>
<daml:ObjectProperty rdf:ID="attack_target">
                    <daml:domain rdf:resource="#attack"/>
                    <rdf:range rdf:Resource="#target"/>
</daml:ObjectProperty>

<daml:Class rdf:ID="malformed">
                    <rdfs:subclassof resource="#attack"/>
                    <rdfs:subclassof>
                        <daml:complementof>
                            <daml:Class rdf:resource=#sip_message/>
                        </daml:complementof>
                    </rdfs:subclassof>
</daml:Class>

 <daml:Class rdf:ID="flood">
                    <rdfs:subclassof resource="attack"/>
</daml:Class>

<daml:Class rdf:ID="single-source">
                    <rdfs:subclassof resource="flood"/>
</daml:Class>

<daml:DatatypeProperty rdf:ID="source-ip">
```

```
                    <daml:domain rdf:resource="#single-source">
                    <rdf:range rdf:Resource="string"  />
</daml:DatatypeProperty>

<daml:DatatypeProperty rdf:ID="threshold">
                    <daml:domain rdf:resource="#single-source">
                    <rdf:range rdf:Resource="number"  />
</daml:DatatypeProperty>

<daml:Class rdf:ID="same-req">
                    <rdfs:subclassof resource="single-source"/>
</daml:Class>

<daml:DatatypeProperty rdf:ID="session-id">
                    <daml:domain rdf:resource="#same-req">
                    <rdf:range rdf:Resource="string"  />
</daml:DatatypeProperty>

<daml:DatatypeProperty rdf:ID="session-to">
                    <daml:domain rdf:resource="#same-req">
                    <rdf:range rdf:Resource="string"  />
</daml:DatatypeProperty>

<daml:Class rdf:ID="new-req">
                    <rdfs:subclassof resource="single-source"/>
</daml:Class>

<daml:DatatypeProperty rdf:ID="session-id">
                    <daml:domain rdf:resource="#new-req"/>
                    <rdf:range rdf:Resource="string"  />
</daml:DatatypeProperty>

<daml:Class rdf:ID="multi-source">
                    <rdfs:subclassof resource="flood"/>
</daml:Class>
```

```
<daml:ObjectProperty rdf:ID="contains">
                        <daml:domain rdf:resource="multi-source"/>
                        <daml:range rdf:resource=" single-source" />
</daml:ObjectProperty>

<daml:DatatypeProperty rdf:ID="memoryconsumption">
                        <daml:domain rdf:resource="multi-source">
                        <rdf:range rdf:Resource="number"  />
</daml:DatatypeProperty>

<daml:DatatypeProperty rdf:ID="threshold">
                        <daml:domain rdf:resource="multi-source">
                        <rdf:range rdf:Resource="number"  />
</daml:DatatypeProperty>

<daml:Class rdf:ID="SYN-syndrome">
                        <rdfs:subclassof resource="multi-source"/>
</daml:Class>

<daml:DatatypeProperty: ID= "without-answered">
                        <daml:domain rdf:resource="SYN-syndrome"/>
                        <rdf:range rdf:Resource="number"  />
</daml:DatatypeProperty>

<daml:Class rdf:ID="REF-syndrome">
                        <rdfs:subclassof resource="multi-source"/>
</daml:Class>

<daml:DatatypeProperty: ID= "without-invite">
                        <daml:domain rdf:resource="REF-syndrome"/>
                        <rdf:range rdf:Resource="number"  />
</daml:DatatypeProperty>

<daml:Class rdf:ID="event">
```

```
</daml:Class>

<daml:ObjectProperty rdf:ID="event-uses">
                        <daml:domain rdf:resource="event"/>
                        <daml:range rdf:resource=" sip-message" />
</daml:ObjectProperty>

<daml:DatatypeProperty rdf:ID="event-time">
                        <daml:domain rdf:resource="event"/>
                        <rdf:Range rdf:Resource="string"/>
</daml:DatatypeProperty>

<daml:Class rdf:ID="state">
                        <daml:oneOf ref:parseType="Collection">
                                <daml:Thing rdf:about="No-state">
                                <daml:Thing rdf:about="calling">
                                <daml:Thing rdf:about="proceeding">
                                <daml:Thing rdf:about="established">
                                <daml:Thing rdf:about="terminating">
                        </daml:oneof>
</daml:Class>

<daml:Class rdf:ID="singalling-attack">
                        <rdfs:subclassof resource="attack"/>
                        <rdfs:subclassof>
                                <daml:Restriction>
                                  <daml:onPropertyrdf:resource="has_sip_message">
                                        <daml:toClass rdf:resource="SIP_Message">
                                </daml:Restriction>
                        </rdfs:subclassof>
                        <daml:intersectionof rdf:ParseTpe="Collection">
                                <daml:Class>
                                        <daml:complementof>
                                                <damlClass rdf:resource="Authenticate"/>
                                        </daml:complementof>
```

```
                    </daml:Class>
                    <daml:Restriction>
                        <daml:onProperty rdf:resource="singalling-uses">
                        <daml:Cardinality>2</daml:cardinality>
                    </daml:Restriction>
                </daml:intersectionof>
</daml:Class>

<daml:ObjectProperty rdf:ID="singalling-uses">
                <daml:domain rdf:resource="singalling-attack"/>
                <daml:range rdf:resource=" sip-message" />
</daml:ObjectProperty>
```