ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΑΣΥΡΜΑΤΩΝ ΕΥΡΥΖΩΝΙΚΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ 4ΗΣ ΓΕΝΙΑΣ

Διδακτορική Διατριβή

Χρήστου Κ. Δημητριάδη

Πειραιάς Ιούνιος 2007

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τριμελής Συμβουλευτική Επιτροπή

Επιβλέπων:
Νικόλαος Αλεξανδρής
Καθηγητής
Πανεπιστημίου Πειραιώς

Μέλη:
Χρήστος Δουληγέρης
Αναπλ. Καθηγητής
Πανεπιστημίου Πειραιώς

Βασίλειος Χρυσικόπουλος
Καθηγητής
Ιονίου Πανεπιστημίου

Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διατριβή
Για την απόκτηση Διδακτορικού Διπλώματος του Τμήματος Πληροφορικής

Χρήστου Κ. Δημητριάδη

«ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΑΣΥΡΜΑΤΩΝ ΕΥΡΥΖΩΝΙΚΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ 4ης ΓΕΝΙΑΣ»

Επταμελής Εξεταστική Επιτροπή

Πρόεδρος:
Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:
Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Χρήστος Δουληγέρης
Αναπλ. Καθηγητής Πανεπιστημίου Πειραιώς

Δημήτριος Κουτσούρης
Καθηγητής Ε.Μ.Π.

Γεώργιος Στασινόπουλος
Καθηγητής Ε.Μ.Π.

Δημήτριος Γκρίτζαλης
Αναπλ. Καθηγητής Οικονομικού Πανεπιστημίου Αθηνών

Δέσποινα Πολέμη
Λέκτορας Πανεπιστημίου Πειραιώς

Ευχαριστίες

Η εκπόνηση μιας διδακτορικής διατριβής προϋποθέτει εκτός από την προσωπική εργασία, την υποστήριξη από ανθρώπους με πείρα στο αντικείμενο, ώστε η προσπάθεια του υποψήφιου διδάκτορα να ευθυγραμμιστεί προς την σωστή κατεύθυνση και να αποφευχθούν λάθη τα οποία κοστίζουν σε χρόνο και ενέργεια. Στο πλαίσιο αυτό, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Ν. Αλεξανδρή για την υπομονή, κατανόηση και τη συμβουλές που μου έδωσε σε όλη τη διάρκεια εκπόνησης της διατριβής, μοιραζόμενος μαζί μου τη σημαντική και πολύχρονη εμπειρία του στον ακαδημαϊκό χώρο. Επίσης, θα ήθελα να ευχαριστήσω τον καθηγητή κ. Χ. Δουληγέρη για τις κατευθύνσεις που μου παρείχε στη συγγραφή εργασιών, τη σημαντική του συμβολή στη διόρθωση και βελτίωση του κειμένου της διατριβής, αλλά και τη δυνατότητα που μου παρείχε να συνεργαστώ μαζί του σε επιστημονικά γεγονότα σε Ελλάδα και Ευρώπη. Συνεχίζοντας θα ήθελα να ευχαριστήσω τον καθηγητή κ. Β. Χρυσικόπουλο για τη συμβολή του σε καίρια σημεία της εκπόνησης της διδακτορικής διατριβής, με σημαντικότερο αυτό της ενδιάμεσης κρίσης, όπου με την παροχή των καταλλήλων κατευθύνσεων με βοήθησε να κερδίσω χρόνο και να αποφύγω λάθη.

Στο σημείο αυτό, αισθάνομαι την ανάγκη να ευχαριστήσω το άτομο που με δίδαξε την τέχνη της επιστημονικής γραφής, με βοήθησε να επιλέξω το θέμα της διατριβής, μου έδωσε τις κατευθύνσεις για σωστές επιλογές και μοιράστηκε μαζί μου εξειδικευμένη γνώση σε θέματα ασφάλειας πληροφοριακών συστημάτων. Η λέκτορας Δ. Πολέμη, λειτούργησε ως ιδιαίτερα σημαντικός παράγοντας επιτυχίας, ο οποίος μου έδωσε την ευκαιρία να γνωρίσω την επιστημονική κοινότητα της ασφάλειας σε Ευρώπη και Αμερική και με καθοδήγησε μέσα από την εμπειρία της υποδεικνύοντας ένα διαφορετικό τρόπο σκέψης που επικεντρώνεται στη λύση του προβλήματος και όχι στην επιτευξιμότητα αυτής, τονίζοντας έτσι τη σημασία ύπαρξης οράματος στο πλαίσιο επιδίωξης υψηλών στόχων.

Ιδιαίτερα ευχαριστώ τον καθηγητή κ. Δ. Κουτσούρη για τις πολύτιμες συμβουλές, την καθοδήγηση που μου παρείχε αλλά και την εμπιστοσύνη του. Ο κ. Δ. Κουτσούρης συνέβαλε καθοριστικά στην μέχρι τώρα πορεία μου στον επιστημονικό χώρο, με εισήγαγε στην έννοια

της ακαδημαϊκής προοπτικής και μου έδωσε σημαντικές συμβουλές και ευκαιρίες από τα πρώτα μου βήματα και την επιλογή της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ ως τη σημερινή ερευνητική μου δραστηριότητα.

Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου και το φιλικό μου περιβάλλον για την πολύτιμη υποστήριξη που μου παρέχει.

Πίνακας Περιεχομένων

Ευρετήριο σχημάτων

Ευρετήριο Πινάκων

ΚΕΦΑΛΑΙΟ 1: ΣΥΝΟΨΗ ΔΙΑΤΡΙΒΗΣ

1.1 Εισαγωγη

1.1.1 Ερευνητικο πεδιο αναφορας

Οι νέες τάσεις στον τομέα της τεχνολογίας της πληροφορίας κινούνται προς μία νέα γενιά τεχνολογιών οι οποίες υπόσχονται παροχή ηλεκτρονικών υπηρεσιών σε οποιαδήποτε περιοχή, με υψηλές ταχύτητες, εύκολα και οικονομικά. Οι νέες αυτές τάσεις είναι εμφανείς σε παγκόσμιο επίπεδο. Στις Ηνωμένες Πολιτείες, χαρακτηριστική είναι η πρωτοβουλία του διεθνούς φήμης Ινστιτούτου Τεχνολογίας της Μασαχουσέτης (Massachusetts Institute of Technology - MIT), το οποίο μέσα από το έργο Oxygen[1], συνδυάζει σχεδόν όλους τους τομείς της επιστήμης των υπολογιστών, στοχεύοντας στην αποκαλούμενη γενιά των **διεισδυτικών, ανθρωποκεντρικών υπολογιστικών συστημάτων**. Τα συστήματα αυτά, περιγράφονται ως διεισδυτικά, από την άποψη ότι είναι παντού, ενσωματωμένα στο περιβάλλον του χρήστη αλληλεπιδρώντας με αυτό, νομαδικά, παρέχοντας πλήρη ελευθερία κινήσεων, ευπροσάρμοστα στις συνθήκες κάθε εφαρμογής, δυνατά και αποτελεσματικά, διαθέσιμα ανά πάσα χρονική στιγμή και έξυπνα, κάνοντας τις πιο συμφέρουσες για το χρήστη επιλογές. Σε Ευρωπαϊκό επίπεδο έχουν περιγραφεί ανάλογα συστήματα έξυπνων ηλεκτρονικών υπηρεσιών στις οποίες ο χρήστης έχει πρόσβαση μέσω μιας ενοποιημένης συσκευής, τα χαρακτηριστικά των οποίων αποτελούν κατευθυντήριες γραμμές για την σχετική έρευνα που χρηματοδοτεί η Ευρωπαϊκή Ένωση. Χαρακτηριστικό παράδειγμα αποτελεί η έκθεση "Σενάρια νοημοσύνης περιβάλλοντος χώρου ως το 2010" [1], της συμβουλευτικής ομάδας ISTAG του τμήματος "Τεχνολογίες της Κοινωνίας της Πληροφορίας (Information Society Technologies - IST)" που αφορά σε δραστηριότητες έρευνας και ανάπτυξης της Γενικής Διεύθυνσης "Κοινωνία της Πληροφορίας" της Ευρωπαϊκής Επιτροπής.

Ένα από τα βασικότερα πεδία έρευνας για την υλοποίηση των παραπάνω στόχων αφορά στην μετάδοση της πληροφορίας πάνω από **ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα** εξασφαλίζοντας τόσο την ευρυζωνικότητα, δηλαδή την *"αδιάλειπτη παροχή*

[1] http://oxygen.lcs.mit.edu/

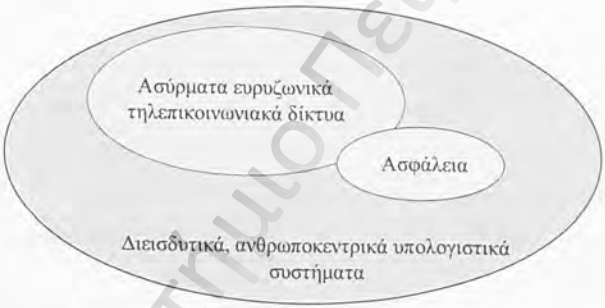
ηλεκτρονικών υπηρεσιών με υψηλής ταχύτητας μετάδοση πληροφορίας"[2], όσο και τη μέγιστη δυνατή ελευθερία κίνησης του χρήστη. Η Τρίτη Γενιά (3rd Generation – 3G) τηλεπικοινωνιακών δικτύων κινητής τηλεφωνίας υλοποιεί την παροχή οικονομικότερων και σημαντικά αναβαθμισμένων υπηρεσιών στους χρήστες, με υψηλότερους ρυθμούς μετάδοσης δεδομένων, πλουσιότερο ψηφιακό περιεχόμενο και υποστήριξη ποικίλων εφαρμογών πολυμέσων, σε σχέση με τα συστήματα της προηγούμενης γενιάς (2nd Generation – 2G). Ένα άλλο είδος ασύρματων δικτύων, το οποίο έχει γνωρίσει μεγάλη άνθιση, είναι τα ασύρματα τοπικά δίκτυα (Wireless Local Area Networks – WLAN). Τα WLAN εξαπλώθηκαν ραγδαία, κυρίως λόγω του χαμηλού κόστους τους, της μεγάλης ευχρηστίας τους και του υψηλού, σε σχέση με τα 3ης γενιάς δίκτυα, ρυθμού μετάδοσης δεδομένων, με μεγάλο αριθμό εφαρμογών σε αεροδρόμια, συνεδριακούς χώρους, πανεπιστήμια, ξενοδοχεία και επιχειρήσεις, λύνοντας τα προβλήματα ελεύθερης μετακίνησης του χρήστη, που δημιουργούσαν τα ενσύρματα μέσα.

Οδεύοντας προς το στόχο της **ασύρματης ευρυζωνικής δικτύωσης**, γρήγορα αναγνωρίστηκε η ανάγκη συνδυασμού της υψηλής γεωγραφικής κάλυψης που προσφέρουν τα δίκτυα 3ης γενιάς, με τους υψηλούς ρυθμούς μετάδοσης δεδομένων των WLANs, με σκοπό την παροχή αδιάλειπτων ευρείας κάλυψης εξελιγμένων υπηρεσιών στους χρήστες. Ο συνδυασμός 3G/WLAN επιτρέπει, εκτός των άλλων, την αποφόρτιση των δικτύων κινητής τηλεφωνίας σε περιοχές υψηλής πυκνότητας χρηστών, με μεταφορά της κίνησης σε σημεία πρόσβασης ασύρματων τοπικών δικτύων. Ο συνδυασμός 3G/WLAN, αποτελεί ένα χαρακτηριστικό βήμα προς την τέταρτη γενιά δικτύων (4G/4Γ), κύριος στόχος των οποίων είναι η υλοποίηση της ασύρματης ευρυζωνικής δικτύωσης μέσα από τη συνένωση ετερογενών ασύρματων τηλεπικοινωνιακών τεχνολογιών [42].

Οι ασύρματες τεχνολογίες τηλεπικοινωνιών, πέρα από τα σημαντικά πλεονεκτήματα τους, είναι ευαίσθητες στον τομέα της ασφάλειας, έναν καθοριστικής σημασίας για την εξέλιξή τους τομέα, κυρίως λόγω της φύσης του μέσου μετάδοσης που επιτρέπει άμεση πρόσβαση στο εκπεμπόμενο σήμα σε αντίθεση με τα ενσύρματα μέσα. Τα περιστατικά ασφάλειας στο χώρο των ασύρματων τηλεπικοινωνιών ήταν πολλά και σημαντικά τα τελευταία χρόνια, τόσο για τα δίκτυα κινητής τηλεφωνίας, όσο και για τα WLAN, γεγονός που υπογραμμίζεται στην Εθνική Στρατηγική Ασφάλειας Κυβερνοχώρου των Ηνωμένων

Πολιτειών της Αμερικής[2]. Οι ανάγκες βελτίωσης των ευρυζωνικών δικτύων, αλλά και της ασφάλειας αυτών, αναγνωρίστηκαν και από το Ευρωπαϊκό Συμβούλιο της Βαρκελώνης, το οποίο κάλεσε την Ευρωπαϊκή Επιτροπή να καταρτίσει το σχέδιο δράσης eEurope [2] –το οποίο σήμερα πλέον ονομάζεται i2010 - εστιάζοντας μεταξύ άλλων, στην εκτεταμένη διάθεση και χρήση των ευρυζωνικών δικτύων (συμπεριλαμβανομένων των δικτύων 3ης γενιάς) σε ολόκληρη την Ευρωπαϊκή Ένωση, καθώς και στην ασφάλεια των δικτύων και των πληροφοριών, την ηλεκτρονική διακυβέρνηση, την ηλεκτρονική μάθηση, την ηλεκτρονική υγεία και το ηλεκτρονικό εμπόριο.

Η παρούσα διδακτορική διατριβή πραγματεύεται θέματα από το χώρο της ασφάλειας των διεισδυτικών, ανθρωποκεντρικών υπολογιστικών συστημάτων. Το Σχήμα 1, παρουσιάζει το ερευνητικό πεδίο αναφοράς της διατριβής.



Σχήμα 1: Ερευνητικό Πεδίο Αναφοράς

Συγκεκριμένα η διδακτορική διατριβή προσδιορίζει ανοικτά προβλήματα και προτείνει λύσεις στο χώρο των νέων ασύρματων ευρυζωνικών τηλεπικοινωνιακών δικτύων και των προσπαθειών υλοποίησης αυτών μέσα από τεχνολογίες 3ης και 4ης γενιάς.

[2] http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

1.1.2 Ορισμοι Εννοιων

Η παρούσα παράγραφος, συνοψίζει τις βασικές έννοιες της διδακτορικής διατριβής και τις ορίζει με ακρίβεια βάσει της διεθνούς βιβλιογραφίας.

Η ασφάλεια πληροφοριακών συστημάτων, ορίζεται ως συνιστάμενη των ακόλουθων ιδιοτήτων, όσον αφορά στην πληροφορία [10]:

- Ακεραιότητα (Integrity): Η διασφάλιση ότι η πληροφορία παραμένει ανέπαφη.
- Εμπιστευτικότητα (Confidentiality): Η διαδικασία εξασφάλισης ότι η πληροφορία παραμένει μυστική σε εκείνους που δεν πρέπει να τη γνωρίζουν.
- Διαθεσιμότητα (Availability): Η εξασφάλιση ότι η πληροφορία και οι υπηρεσίες που παρέχει το σύστημα είναι διαθέσιμες κάθε στιγμή.

και συμπληρώνεται από την ικανοποίηση των παρακάτω θεμελιωδών αναγκών που αφορούν στις εμπλεκόμενες οντότητες:

- Αναγνώριση (Identification): Η διαδικασία αναγνώρισης μιας συγκεκριμένης οντότητας από το σύστημα.
- Πιστοποίηση ταυτότητας (Authentication): Η διαδικασία απόδειξης της ταυτότητας μιας συγκεκριμένης οντότητας στο σύστημα.
- Εξουσιοδότηση (Authorization): Η εξασφάλιση ότι κάθε οντότητα έχει πρόσβαση σε επιτρεπτούς πόρους του συστήματος.
- Μη αποποίηση (Non-repudiation): Η εξασφάλιση ότι μια συγκεκριμένη οντότητα δεν μπορεί να αρνηθεί την ευθύνη για μία ενέργειά της.

Το σύνολο των εννοιών της αναγνώρισης, πιστοποίησης ταυτότητας και εξουσιοδότησης ορίζουν την έννοια της **Διαχείρισης Ταυτότητας** (Identity Management). Ο επίσημος ορισμός της βιβλιογραφίας για τη διαχείριση ταυτότητας είναι ο ακόλουθος: *η αναγνώριση χρηστών σε ένα σύστημα και ο έλεγχος της πρόσβασης αυτών στους πόρους του συστήματος μέσω της συσχέτισης των δικαιωμάτων τους και των περιορισμών τους με μία ορισμένη ταυτότητα* [85].

Τα **βιομετρικά συστήματα**, υλοποιούν ισχυρή αναγνώριση ή πιστοποίηση ταυτότητας και ορίζονται ως *συστήματα αναγνώρισης ή πιστοποίησης ταυτότητας ατόμου μέσω της αυτοματοποιημένης μέτρησης χαρακτηριστικών της φυσιολογίας ή της συμπεριφοράς του* [147].

Ως **ασύρματα ευρυζωνικά** τηλεπικοινωνιακά δίκτυα ορίζονται τα τηλεπικοινωνιακά δίκτυα τα οποία παρέχουν *"αδιάλειπτα ηλεκτρονικές υπηρεσίες με υψηλής ταχύτητας μετάδοση πληροφορίας πάνω από ασύρματα μέσα"* [2].

Τα δίκτυα **τέταρτης γενιάς (4G/4Γ)**, ορίζονται ως ασύρματα ευρυζωνικά δίκτυα που προκύπτουν μέσα από τη συνένωση ετερογενών ασύρματων τηλεπικοινωνιακών τεχνολογιών [38]. Ο συνδυασμός 3G/WLAN [37], αποτελεί ένα χαρακτηριστικό βήμα προς την τέταρτη γενιά δικτύων.

Στο χώρο των τηλεπικοινωνιακών συστημάτων και των δικτύων δεδομένων, η ασφάλεια υλοποιείται ως η συνισταμένη των ακόλουθων τριών τεχνολογικών αντιμέτρων [24]:

- Προληπτικά: ενδεικτικά, στην κατηγορία αυτή συγκαταλέγονται τα αναχώματα ασφάλειας (firewalls), η ορθή παραμετροποίηση των δικτυακών συσκευών για αποτελεσματικό φιλτράρισμα της δικτυακής κίνησης, οι πολιτικές και διαδικασίες λειτουργίας του προσωπικού και τα συστήματα ελέγχου πρόσβασης.
- Ανιχνευτικά: στην κατηγορία αυτή συγκαταλέγονται κυρίως τα συστήματα ανίχνευσης εισβολών (intrusion detection systems) και τα συστήματα ανίχνευσης ιομορφικού λογισμικού.
- Αντιδραστικά: ενδεικτικά, στην κατηγορία αυτή συγκαταλέγονται τα συστήματα αναχαίτισης εισβολών (intrusion prevention systems) και οι διαδικασίες και στρατηγικές αντίδρασης σε περιστατικά ασφάλειας, όπως η εναλλαγή σε εφεδρικά συστήματα.

Τα **συστήματα παγίδευσης εισβολέων (Honeynets)** ορίζονται ως εξελιγμένα συστήματα δικτυακής ασφάλειας, τα οποία συνδυάζουν προληπτικά, ανιχνευτικά και αντιδραστικά αντίμετρα με στόχο την εξαπάτηση και την παγίδευση εισβολέων, των οποίων η χρησιμότητα έγκειται στην παραβίαση αυτών, για τη μελέτη τακτικών εισβολής [171].

1.1.3 Συμβολη διατριβης – Κοινωνικη Διασταση

Επιχειρώντας μια άμεση προσέγγιση οικονομικού προσδιορισμού της ασφάλειας, αξίζει να αναφερθεί ότι οι απώλειες κατά το έτος 2005 στις ΗΠΑ από περιστατικά ασφάλειας έφθασαν τα 130 εκατομμύρια δολάρια[3], ενώ ο προϋπολογισμός για την υλοποίηση έρευνας στο χώρο της ασφάλειας πληροφοριακών συστημάτων έχει προταθεί από την αρμόδια συμβουλευτική επιτροπή της προεδρίας των ΗΠΑ, να αυξάνεται κατά 90 εκατομμύρια δολάρια ετησίως [33]. Στην Ευρώπη, το μέσο κόστος ενός περιστατικού ασφάλειας, σύμφωνα με έρευνα της εταιρίας PriceWaterhouseCoopers για το 2006, κυμαίνεται από 8.000-17.000 λίρες Αγγλίας, ενώ για μεγάλες επιχειρήσεις, από 65.000-130.000 λίρες Αγγλίας.

Θεωρώντας δεδομένο ότι τα **ασύρματα τηλεπικοινωνιακά δίκτυα** έχουν ανάγκες ασφάλειας, μια πιο έμμεση προσέγγιση προσδιορισμού της σπουδαιότητας της ασφάλειας, επιτυγχάνεται μέσω της μελέτης της έκτασης των ίδιων των ασύρματων δικτύων σε παγκόσμια κλίμακα. Εκτός από την ευρεία εξάπλωση των κινητών τηλεπικοινωνιακών συστημάτων **2ης γενιάς και 3ης γενιάς**, χαρακτηριστικό είναι ότι στη Νέα Υόρκη υπάρχουν εγκατεστημένα πάνω από 1000 δημόσια σημεία πρόσβασης σε **WLAN**. Στην Κορέα έχει προγραμματιστεί η εγκατάσταση 10.000 σημείων πρόσβασης από ιδιωτικό φορέα παροχής υπηρεσιών, ενώ σε παγκόσμιο επίπεδο υπολογίζεται ότι υπάρχουν περί τα 70.000 σημεία πρόσβασης. Στην Ευρώπη, σύμφωνα με τη βάση δεδομένων των Κόμβων της Ασύρματης Κοινότητας[4], υπάρχουν εγκατεστημένοι 12689 κόμβοι ασύρματης πρόσβασης σε 711 σημεία. Στην Ελλάδα, οι υπηρεσίες WLAN παρέχονται ήδη στο διεθνή αερολιμένα Ελευθέριος Βενιζέλος. Στους ολυμπιακούς αγώνες οι ασύρματες τεχνολογίες μέρος τον οποίων θα είναι WLANs, είχαν πρωταγωνιστικό ρόλο, ενώ το Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών[5] (ένας μή κερδοσκοπικού χαρακτήρα σύλλογος ο οποίος ασχολείται με τις ασύρματες ψηφιακές ευρυζωνικές επικοινωνίες) μετρά 2557 ασύρματους κόμβους πρόσβασης στην

[3] Έρευνα του Computer Security Institute / Federal Bureau of Investigations (CSI/FBI): http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

[4] http://www.nodedb.com/europe/index.php

[5] http://www.awmn.gr

περιοχή του λεκανοπεδίου Αττικής. Τα παραπάνω μεγέθη, σε συνδυασμό με την τεράστια εξάπλωση των δικτύων κινητής τηλεφωνίας στην υφήλιο, δίνουν μια πρώτη εικόνα της ευρείας εξάπλωσης των ασύρματων τηλεπικοινωνιακών τεχνολογιών. Σε χώρες μάλιστα όπως η Κορέα, η διείσδυση των τεχνολογιών είναι ιδιαίτερα υψηλή [51], ενώ η εξέλιξη της τεχνολογίας οδεύει προς ενσωματωμένες φορητές συσκευές [31, 32] οι οποίες παρέχουν αδιάλειπτη τηλεπικοινωνιακή κάλυψη μέσω συνδυασμού ετερογενών δικτύων [40].

Σε κοινωνικό επίπεδο, η αντιμετώπιση θεμάτων ασφάλειας στις ασύρματες τηλεπικοινωνίες θα ανοίξει νέους ορίζοντες για την εξάπλωση των τεχνολογιών, κάνοντας ένα βήμα προς την απόκτηση της εμπιστοσύνης του πολίτη στη χρήση τους. Συγκεκριμένα, προστατεύονται τα προσωπικά δεδομένα των πολιτών και επιτυγχάνεται το απόρρητο των τηλεπικοινωνιακών συναλλαγών. Ο πολίτης απολαμβάνει εξελιγμένες υπηρεσίες που διευκολύνουν την καθημερινότητά του, χωρίς την αυξημένη ανασφάλεια που προκαλούν τα σημερινά ευπαθή συστήματα. Υπηρεσίες όπως το ηλεκτρονικό εμπόριο και η ηλεκτρονική διακυβέρνηση θα αποκτήσουν περισσότερους χρήστες, διευκολύνοντας τις συναλλαγές του πολίτη με δημόσιους και ιδιωτικούς φορείς, σε ένα πλαίσιο ασφάλειας και εμπιστοσύνης. Οι στόχοι αυτοί είναι συμβατοί και με τις προσδοκίες των ευρωπαίων πολιτών, οι οποίοι σύμφωνα με το <<επιστημονικό ευρωβαρόμετρο>> το οποίο δημοσιεύθηκε τον Ιούνιο του 2005, προσδοκούν κατά 69% η επικείμενη τεχνολογική πρόοδος να κάνει ποιο ενδιαφέρουσα την εργασία του ευρωπαίου πολίτη, κατά 64% ότι η οικονομία θα γίνει περισσότερο ανταγωνιστική βάσει των τεχνολογικών εξελίξεων και κατά 85% ότι θα βελτιώσουν την ποιότητα ζωής στην Ευρώπη [36].

Τεχνολογικά, η διδακτορική διατριβή, στοχεύει στην εξέλιξη της τεχνογνωσίας σε θέματα ασφάλειας νέων τεχνολογιών 3ης και 4ης γενιάς. Πιο συγκεκριμένα, στοχεύει στην αναζήτηση ανοιχτών θεμάτων ασφάλειας και στην πρόταση καινοτόμων λύσεων για την αντιμετώπιση αυτών.

1.2 Ορθολογικη Βαση – Συνοπτικη Αναφορα Προβληματων

Στην παρούσα ενότητα περιγράφονται εν συντομία τα ανοικτά προβλήματα για τα οποία η διδακτορική διατριβή προτείνει λύσεις. Περισσότερες λεπτομέρειες, καθώς και σαφής προσδιορισμός των προβλημάτων αυτών, δίδονται στο επόμενο κεφάλαιο.

1.2.1 Συνοψη προβληματων

1.2.1.1 Διαχείριση Ταυτότητας Χρήστη

Η διαχείριση ταυτότητας χρήστη, όπως ορίσθηκε νωρίτερα, υλοποιεί τρεις από τις θεμελιώδεις αρχές ασφάλειας ενός πληροφοριακού συστήματος. Στο πλαίσιο της διδακτορικής διατριβής, διακρίνουμε δύο είδη διαχείρισης ταυτότητας, έχοντας ως κριτήριο τις οντότητες-άκρα που επικοινωνούν στο πλαίσιο μίας εφαρμογής πάνω από δίκτυα 3ης και 4ης γενιάς:

- Διαχείριση ταυτότητας χρήστη για την παροχή ασύρματων ευρυζωνικών τηλεπικοινωνιακών δικτύων 3ης και 4ης γενιάς. Το είδος αυτό αφορά στην αναγνώριση, πιστοποίηση ταυτότητας και εξουσιοδότηση χρήστη σε ένα φορέα παροχής κινητών τηλεπικοινωνιακών υπηρεσιών 3ης και 4ης γενιάς.
- Διαχείριση ταυτότητας χρήστη για την παροχή υπηρεσιών στο διαδίκτυο πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς. Το είδος αυτό αφορά στην αναγνώριση, πιστοποίηση ταυτότητας και εξουσιοδότηση χρήστη σε ένα φορέα παροχής υπηρεσιών στο Διαδίκτυο, πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς.

1.2.1.1.1 Διαχείριση ταυτότητας χρήστη – υπηρεσίες ασύρματων ευρυζωνικών τηλεπικοινωνιακών δικτύων 3ης και 4ης γενιάς

Η πιστοποίηση ταυτότητας χρήστη βασίζεται συνήθως σε ευπαθείς μηχανισμούς ενός κριτηρίου, όπως η χρήση συνθηματικών, ή το πολύ δύο κριτηρίων, όπως η επιπλέον χρήση

μιας έξυπνης κάρτας. Τα συστήματα ενός και δύο κριτηρίων έχουν αδυναμίες που οφείλονται στο γεγονός ότι τόσο η γνώση, όσο και η κατοχή τεκμηρίων δεν χαρακτηρίζουν μοναδικά το χρήστη [141].

Στο χώρο των υπηρεσιών 3ης και 4ης γενιάς, η πιστοποίηση της ταυτότητας του χρήστη, γίνεται με τη χρήση ενός αναγνωριστικού, το οποίο ονομάζεται Personal Identification Number (PIN) [77]. Από τη στιγμή που ο χρήστης πιστοποιεί την ταυτότητά του στη συσκευή, η περαιτέρω πιστοποίηση ταυτότητας από απομακρυσμένες οντότητες πραγματοποιείται με χρήση προ-αποθηκευμένων αναγνωριστικών ή μυστικών κλειδιών [76]. Αυτό ισχύει για την πρόσβαση στο δίκτυο 3ης και 4ης γενιάς (επίπεδο 2 του μοντέλου αναφοράς Open Systems Interconnection – OSI), όπου ουσιαστικά ο χρήστης αναγνωρίζεται από τον μοναδικό αριθμό International Mobile Subscriber Identity (IMSI) της κάρτας UMTS[6] Subscriber Identity Module (USIM) και πιστοποιείται μέσω ενός προσυμφωνημένου συμμετρικού κλειδιού (K). Επιπροσθέτως, έχουν δημοσιευθεί ερευνητικές εργασίες με αντικείμενο την παραβίαση της ασφάλειας του PIN [70], τονίζοντας την ανάγκη για ισχυρότερους μηχανισμούς πιστοποίησης ταυτότητας χρήστη.

Η ανάγκη για ισχυρή πραγματική πιστοποίηση του χρήστη από άκρο σε άκρο είναι ιδιαίτερα αισθητή, καθώς η σημερινή αλυσίδα ασφάλειας, η οποία στηρίζει όλο το μηχανισμό πιστοποίησης σε ένα PIN, είναι επισφαλής. Την απάντηση στο παραπάνω πρόβλημα φιλοδοξούν να δώσουν τα βιομετρικά συστήματα, εισάγοντας το τρίτο κριτήριο στη διαδικασία, δηλαδή την απόδειξη μέσω ενός ανθρώπινου χαρακτηριστικού. Παρόλα αυτά, ο σχεδιασμός μιας αρχιτεκτονικής ασφάλειας που βασίζεται σε βιομετρικά είναι αρκετά σύνθετος και απαιτητικός τόσο σε θέματα ασφάλειας, όσο και σε θέματα προστασίας των προσωπικών δεδομένων του χρήστη απαιτώντας ειδική μελέτη απαιτήσεων και προδιαγραφών ανάλογα με την εφαρμογή [143]. Ειδικά μάλιστα στο χώρο των εφαρμογών πάνω από δίκτυα 3ης και 4ης γενιάς, η απαιτούμενη μελέτη είναι ιδιαίτερη σημαντική, λαμβάνοντας υπόψη την ιδιαιτερότητα του μέσου μετάδοσης (ασύρματο) των προσωπικών

[6] Αφορά στο πρότυπο τηλεπικοινωνιακών δικτύων 3ης γενιάς Universal Mobile Telecommunications System, στοιχεία του οποίου περιγράφονται στο Κεφάλαιο 2

δεδομένων των χρηστών, κάτι που αποτελεί διαπίστωση που εκφράζεται με ειδική μνεία στις σχετικές κυβερνητικές πολιτικές, τόσο των Ηνωμένων Πολιτειών της Αμερικής όσο και της Ευρωπαϊκής Ένωσης [1,2].

1.2.1.1.2 Διαχείριση ταυτότητας χρήστη – υπηρεσίες στο διαδίκτυο πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς

Ειδικά για φορείς παροχής ηλεκτρονικών υπηρεσιών στο διαδίκτυο, η διαχείριση ταυτότητας αποτελεί σοβαρή πρόκληση, καθώς είναι υποχρεωμένοι να υλοποιήσουν ασφαλείς και φιλικούς προς το χρήστη μηχανισμούς για να ελέγξουν την πρόσβαση ετερογενών, ποικιλόμορφων και διεσπαρμένων γεωγραφικά ομάδων πληθυσμού στους πόρους τους [84]. Η ανάγκη διαχείρισης ταυτότητας για υπηρεσίες που παρέχονται στο διαδίκτυο οδήγησε στη δημιουργία πρωτοκόλλων, όπως το Microsoft .Net Passport[7], καθώς και των συστάσεων-πρωτοκόλλων του Liberty Alliance[8], μιας συμμαχίας από 150 εταιρίες, μη κερδοσκοπικούς οργανισμούς και κυβερνητικές οντότητες. Τα πρότυπα αυτά επεκτείνουν τη γλώσσα OASIS's Security Assertions Markup Language (SAML)[9], η οποία βασίζεται στην Extensible Markup Language (XML) και αφορά στην ανταλλαγή πληροφοριών πιστοποίησης. Οι προδιαγραφές τόσο των προτύπων, όσο και η σχετική βιβλιογραφία, ορίζουν τις παρακάτω βασικές απαιτήσεις για ένα πρωτόκολλο διαχείρισης ταυτότητας:

- Να είναι διαφανές στο χρήστη.
- Να υποστηρίζει πολλαπλές ταυτότητες για κάθε χρήστη.
- Να είναι ελαφρύ.
- Να προστατεύει τα προσωπικά δεδομένα του χρήστη.
- Να είναι διαλειτουργικό.
- Να είναι ασφαλές.

[7] http://www.passport.net

[8] http://www.projectliberty.org/

[9] http://www.oasis-open.org

- Να υλοποιεί επαρκώς ισχυρή πιστοποίηση ταυτότητας χρήστη.
- Να συνδέει ασφαλώς τις έννοιες της αναγνώρισης, της πιστοποίησης και της εξουσιοδότησης.

Οι υπάρχουσες λύσεις, όπως το Microsoft .Net Passport και οι συστάσεις-πρωτόκολλα του Liberty Alliance, ορίζουν μια έμπιστη τρίτη οντότητα μεταξύ του χρήστη και του φορέα παροχής υπηρεσιών στο Διαδίκτυο, η οποία λειτουργεί ως διαμεσολαβητής στην πιστοποίηση της ταυτότητας του χρήστη παρέχοντας τα κατάλληλα τεκμήρια.

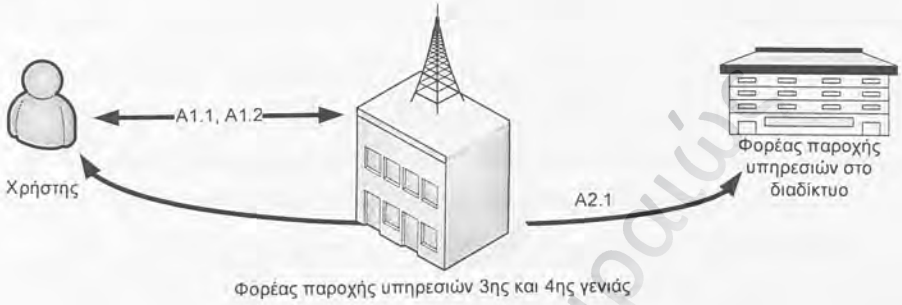
Οι συνδρομητές υπηρεσιών 3ης και 4ης γενιάς, οι οποίοι θέλουν πραγματοποιήσουν αμοιβαία πιστοποίηση ταυτότητας με φορείς παροχής ηλεκτρονικών υπηρεσιών στο διαδίκτυο, μπορούν να χρησιμοποιήσουν τις υπάρχουσες λύσεις διαχείρισης ταυτότητας, με την εγγραφή τους σε μία έμπιστη τρίτη οντότητα παροχής υπηρεσιών ταυτότητας. Παρόλα αυτά, κατά την προσέγγιση αυτή δεν λαμβάνεται υπόψη η σχέση εμπιστοσύνης του συνδρομητή υπηρεσιών 3ης και 4ης γενιάς με τον φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς, η οποία είναι ισχυρή και διέπεται από νόμους προστασίας προσωπικών δεδομένων. Αυτό έχει ως αποτέλεσμα:

- τη μείωση της απόδοσης του όλου μηχανισμού, καθώς εισέρχεται μία ακόμη οντότητα εκτός του χρήστη, του φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς και του φορέα παροχής υπηρεσιών στο διαδίκτυο, με τις ανάλογες απαιτήσεις σε δικτυακό φορτίο,
- τις μη προσαρμοσμένες απαιτήσεις σε επεξεργαστική ισχύ στις προδιαγραφές του κινητού τερματικού εξοπλισμού του χρήστη, ο οποίος έχει περιορισμένες δυνατότητες επεξεργασίας και μνήμης και οι δυνατότητες του οποίου είναι αντιστρόφως ανάλογες των αποθεμάτων ενέργειας αυτού [87] και
- τη δημιουργία ερωτημάτων σε θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων του χρήστη, καθώς αυξάνονται τα ευαίσθητα μηνύματα που διακινούνται.

Συνοψίζουμε, λοιπόν, στην ανάγκη ύπαρξης ενός πρωτοκόλλου διαχείρισης ταυτότητας χρήστη για υπηρεσίες στο Διαδίκτυο πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς, το οποίο να απαντά στα παραπάνω ανοικτά προβλήματα.

1.2.1.1.3 Σύνοψη προβλημάτων διαχείρισης ταυτότητας χρήστη

Τα παραπάνω συνοψίζονται στις ακόλουθες ενότητες ανοικτών προβλημάτων στο χώρο της διαχείρισης ταυτότητας πάνω από δίκτυα 3ης και 4ης γενιάς και παρουσιάζονται στο Σχήμα 2.



Σχήμα 2: Σύνοψη προβλημάτων διαχείρισης ταυτότητας χρήστη

Το πρώτο πρόβλημα (A1.1 στο Σχήμα 2) αφορά στην απουσία ενός μοντέλου αποτίμησης επικινδυνότητας για βιομετρικά συστήματα, ώστε να είναι εφικτή η ασφαλής ενσωμάτωση αυτών σε ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς αλλά και σε οποιαδήποτε άλλη αρχιτεκτονική.

Το δεύτερο πρόβλημα (A1.1 στο Σχήμα 2), αφορά στο ότι η αλυσίδα ασφάλειας πρόσβασης χρήστη στο δίκτυο 3ης γενιάς, καταλήγει στην πιστοποίηση της ταυτότητας χρήστη στην τερματική συσκευή, η οποία υλοποιείται με την επισφαλή χρήση ενός PIN. Η εισαγωγή βιομετρικών για την υλοποίηση ισχυρής πιστοποίησης ταυτότητας δεν έχει μελετηθεί για ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς. Η μελέτη ασφάλειας και προστασίας των προσωπικών δεδομένων του χρήστη για την εισαγωγή βιομετρικών σε δίκτυα 3ης ή 4ης γενιάς είναι επιτακτική, όπως και η ύπαρξη ενός πρωτοκόλλου για ισχυρή πραγματική πιστοποίηση του χρήστη από άκρο σε άκρο.

Το τρίτο πρόβλημα (A2.1 στο Σχήμα 2), αφορά στο ότι η χρήση υπαρχόντων πρωτοκόλλων διαχείρισης ταυτότητας χρήστη για υπηρεσίες στο διαδίκτυο πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς επιβαρύνει την απόδοση

του συστήματος, δεν αξιοποιεί τις νέες αρχιτεκτονικές και δημιουργεί ερωτηματικά ασφάλειας. Δεν υπάρχει ενοποιημένο πρωτόκολλο διαχείρισης ταυτότητας για εφαρμογές διαδικτύου πάνω από δίκτυα 3ης και 4ης γενιάς.

1.2.1.2 Αρχιτεκτονική δικτυακής ασφάλειας κυρίως δικτύου φορέα παροχής υπηρεσιών ασύρματων ευρυζωνικών τηλεπικοινωνιών 3ης γενιάς

Οι ολοκληρωμένες αρχιτεκτονικές δικτυακής ασφάλειας είναι συνιστώσες τριών βασικών τεχνολογικών αντιμέτρων –της πρόληψης, της ανίχνευσης και της αντίδρασης. Το τρίπτυχο αυτό έχει γνωρίσει εξέλιξη τα τελευταία χρόνια, μέσα από την προσπάθεια ανάπτυξης της ευφυίας των τεχνολογιών, τη δημιουργία συστημάτων συσχετισμού των αποτελεσμάτων τους και την ανάπτυξη μοντέλων πρόβλεψης επιθέσεων μέσα από στατιστικές [26]. Παρόλα αυτά, οι αρχιτεκτονικές δικτυακής ασφάλειας παραμένουν ευάλωτες, επαληθεύοντας το αξίωμα του ανεπίτευκτου της απόλυτης ασφάλειας.

Προσπαθώντας να αιτιολογήσουμε τον παραπάνω χαρακτηρισμό, καταλήγουμε στο συμπέρασμα ότι το ανεπίτευκτο της απόλυτης ασφάλειας ταυτίζεται με το αστείρευτο της γνώσης, φέρνοντας στο προσκήνιο τον συνεχή αγώνα για την ανακάλυψη τρωτών σημείων και νέων τεχνικών εισβολής και αντιμέτρων μεταξύ της κοινότητας των εισβολέων και της κοινότητας της ασφάλειας πληροφοριακών συστημάτων.

Σύμφωνα με το ινστιτούτο SANS[16] ένα από τα σημαντικότερα σφάλματα στον τομέα της ασφάλειας είναι η αναζήτηση και μελέτη μεμονωμένων λύσεων ασφάλειας και όχι η σφαιρική αντιμετώπιση κάθε τεχνολογικού τομέα που αναδεικνύει το σύνολο του προβλήματος και οδηγεί σε ώριμες και αποτελεσματικές λύσεις. Αυτό είναι και το σημαντικότερο πρόβλημα ασφάλειας κατά την παροχή υπηρεσιών 3ης γενιάς, καθώς η βελτίωση της ασφάλειας από τα συστήματα 2ης γενιάς στα συστήματα 3ης γενιάς αφορά κυρίως στη ζεύξη ιερματικού εξοπλισμού χρήστη – σημείου πρόσβασης στο δίκτυο και όχι στο κυρίως δίκτυο (core network) ενός φορέα παροχής υπηρεσιών 3ης γενιάς.

[16] http://www.sans.org

Παρά τη δομημένη δημιουργία προτύπων, στην πράξη τα κυρίως δίκτυα παροχής κινητών υπηρεσιών 3ης γενιάς δεν αποτελούν δίκτυα τα οποία δημιουργήθηκαν εξ' αρχής, μέσα από σχεδίαση, ανάπτυξη και υλοποίηση που βασίζεται σε ανάλυση των σύγχρονων απαιτήσεων των παρεχόμενων υπηρεσιών. Αποτελούν μια μετεξέλιξη ή αλλιώς μια αναβάθμιση από δίκτυα προηγούμενων γενεών που παρείχαν υπηρεσίες φωνής και πολύ περιορισμένες υπηρεσίες δεδομένων, σε δίκτυα τα οποία παρέχουν ένα μεγάλο πλήθος ευρυζωνικών υπηρεσιών φωνής και δεδομένων. Πιο συγκεκριμένα, συντελέσθηκε μια μετεξέλιξη από τα κλειστά δίκτυα που βασίζονταν στο σύστημα σηματοδοσίας Signalling System 7 (SS7), το οποίο υπάρχει ακόμη στις υποδομές των φορέων παροχής υπηρεσιών 3ης γενιάς, στα ανοικτά δίκτυα IP παροχής υπηρεσιών πολυμέσων [54].

Το αποτέλεσμα αυτής της μετεξέλιξης, η οποία έγινε κάτω από τη χρονική πίεση για άμεση παροχή νέων υπηρεσιών, είναι ένα μείγμα παλαιών και νέων τεχνολογιών, εφαρμογών και συστημάτων, τα οποία δεν έχουν κοινές προδιαγραφές και δυνατότητες ασφάλειας. Αυτό, σε συνδυασμό με την έλλειψη των απαραίτητων αντιμέτρων πρόληψης, ανίχνευσης και αντίδρασης σε δικτυακές επιθέσεις, συνεπάγεται ανεπαρκή προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των βασικών κατηγοριών δεδομένων [72], που διαχειρίζονται τα κυρίως δίκτυα, συμπεριλαμβανομένων των δεδομένων χρηστών (user traffic), της σηματοδοσίας (signaling) και των δεδομένων ελέγχου (control data). Επιπλέον, η ανάγκη για εξειδικευμένη γνώση σε θέματα ασφάλειας για συστήματα 3ης γενιάς είναι ιδιαίτερα σημαντική για το προσωπικό των φορέων παροχής, καθώς η γνώση αυτή παρέχει τη δυνατότητα για την καλύτερη προστασία του συστήματος. Η έγκαιρη μάλιστα ανακάλυψη νέων τρωτών σημείων στο σύστημα μειώνει σημαντικά το κόστος ενός περιστατικού ασφάλειας [3].

Συνοψίζουμε στο παρακάτω πρόβλημα:

- Οι αρχιτεκτονικές δικτυακής ασφάλειας κυρίως δικτύου φορέα παροχής υπηρεσιών 3ης γενιάς είναι ανεπαρκείς, με κύριο χαρακτηριστικό μια επίπεδη αρχιτεκτονική ασφάλειας που βασίζεται σε ελλιπή αναχώματα ασφάλειας και απουσία συστημάτων ανίχνευσης και αναχαίτισης εισβολών. Οι ενδεχόμενες συνέπειες από την πραγματοποίηση κάποιας απειλής μέσα από την εκμετάλλευση κάποιας αδυναμίας του συστήματος καθιστούν επιτακτική τη δημιουργία μιας αποτελεσματικής αρχιτεκτονικής ασφάλειας για την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου. Πέρα από τη δημιουργία μιας πιο αποτελεσματικής αρχιτεκτονικής ασφάλειας για την αντιμετώπιση των υπαρχόντων ευπαθών σημείων, πολύ σημαντική είναι η ύπαρξη εξειδικευμένης γνώσης σε θέματα ασφάλειας στους φορείς παροχής 3ης γενιάς, ώστε να είναι σε θέση να αντιμετωπίζουν εξειδικευμένες επιθέσεις σε δίκτυα 3ης γενιάς.

1.2.1.3 Συσχετισμός προβλημάτων με το σχετικό νομικό πλαίσιο

Τα παραπάνω προβλήματα, γίνονται ιδιαίτερα σημαντικά, αν λάβουμε υπόψη μας και το σχετικό νομικό πλαίσιο, το οποίο αναλύεται στην παράγραφο 2.1.4: Νομικό πλαίσιο. Σύμφωνα με αυτό:

- Υπάρχει ανάγκη ισχυρής πιστοποίησης ταυτότητας χρήστη.
- Ο μηχανισμός ισχυρής πιστοποίησης πρέπει να διαφυλάσσει το απόρρητο της ταυτότητας.
- Τα προσωπικά δεδομένα του χρήστη συμπεριλαμβανομένης της ταυτότητας αυτού και των συναλλαγών του θα πρέπει να παραμένουν απόρρητα σε εφαρμογές στο Διαδίκτυο (και πάνω από δίκτυα 3ης και 4ηςγενιάς).
- Υπάρχει ανάγκη επαρκών μέτρων ασφάλειας στην παροχή υπηρεσιών μεταγωγής πακέτου ενός δικτύου 3ης και 4ηςγενιάς.

1.3 Περιεκτικη Περιγραφη Προτεινομενων Λυσεων

Η παρούσα διδακτορική διατριβή, προτείνει λύσεις για τα προβλήματα, που περιγράφηκαν παραπάνω. Η προτεινόμενη λύση για το πρόβλημα Α, χωρίζεται σε τρία μέρη, όσα και τα καταγεγραμμένα ανοικτά προβλήματα και τα αντιμετωπίζει ένα προς ένα:

- Προτείνει ένα μηχανισμό αποτίμησης επικινδυνότητας για βιομετρικά συστήματα, με στόχο την ασφαλή ενσωμάτωσή τους σε οποιαδήποτε αρχιτεκτονική ασφάλειας.
- Προτείνει ένα νέο πρωτόκολλο ενσωμάτωσης βιομετρικών σε μία αρχιτεκτονική 3G και 3G/WLAN (4ης γενιάς), με στόχο την ισχυρή πιστοποίηση χρήστη και επομένως τη βελτίωση της ασφάλειας των μηχανισμών πρόσβασης σε επίπεδο δικτύου.
- Προτείνει ένα νέο ασφαλές και πιο αποτελεσματικό από άποψη απόδοσης πρωτόκολλο διαχείρισης ταυτότητας χρηστών 3ης και 4ης γενιάς σε φορείς παροχής υπηρεσιών στο Διαδίκτυο.
- Προτείνει μια γενική αρχιτεκτονική πρόληψης, ανίχνευσης και αντίδρασης για την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου, η οποία βασίζεται σε μια λογική πολυ-επίπεδης ασφάλειας με διαχωρισμό κάθε τμήματος της υποδομής του φορέα παροχής υπηρεσιών 3ης γενιάς σε ζώνες. Στη συνέχεια, με στόχο την υλοποίηση μιας εξειδικευμένης, σε συστήματα 3ης γενιάς, πολιτικής συνεχούς μελέτης και βελτίωσης της ασφάλειας, προτείνεται η εφαρμογή Συστημάτων Παγίδευσης Εισβολέων (ΣΠΕ - Honeynets) στο κυρίως δίκτυο ενός φορέα παροχής ασύρματων υπηρεσιών 3ης γενιάς.

1.4 Δομη Διατριβης

Το κείμενο της διδακτορικής διατριβής αποτελείται από τα ακόλουθα κεφάλαια:

Το **κεφάλαιο 1**, αποτελεί την επιτελική σύνοψη της διδακτορικής διατριβής. Αρχικά περιγράφεται το ερευνητικό πεδίο της διατριβής και στη συνέχεια παρουσιάζονται οι ορισμοί κάποιων βασικών εννοιών με στόχο την ομαλή εισαγωγή του αναγνώστη σε περισσότερο λεπτομερή τεχνικά θέματα. Προσδιορίζεται η συμβολή της διατριβής σε κοινωνικό και επιστημονικό επίπεδο και ακολούθως αναφέρονται περιεκτικά τα ανοικτά

προβλήματα στα οποία η διατριβή επιδιώκει να δώσει λύσεις και παρέχεται μια συνοπτική περιγραφή των λύσεων αυτών.

Στο **κεφάλαιο 2**, παρουσιάζεται αναλυτικά η ερευνητική περιοχή της διατριβής. Παρουσιάζονται με ακρίβεια οι επιστημονικοί τομείς τους οποίους πραγματεύεται και ταυτόχρονα προσδιορίζονται με σαφήνεια τα ανοικτά προβλήματα ανά τομέα. Πιο συγκεκριμένα, παρουσιάζονται αρχιτεκτονικές τηλεπικοινωνιακών δικτύων 3ης και 4ης γενιάς και διακρίνονται δύο επιμέρους ερευνητικές περιοχές όπου και εντοπίζονται ανοικτά προβλήματα:

- Διαχείριση ταυτότητας χρήστη και
- Αρχιτεκτονική δικτυακής ασφάλειας κυρίως δικτύου του φορέα παροχής ασύρματων ευρυζωνικών τηλεπικοινωνιών 3ης γενιάς.

Στη συνέχεια, επικεντρώνοντας στις δύο διακεκριμένες ερευνητικές περιοχές, παρουσιάζονται συμπληρωματικοί ερευνητικοί τομείς που σχετίζονται με αυτές. Όσο αφορά στην ερευνητική περιοχή **διαχείρισης ταυτότητας χρήστη**, αφού έχει ήδη παρουσιαστεί ο μηχανισμός διαχείρισης ταυτότητας χρήστη στην υποδομή του φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς, ως τμήμα της αρχιτεκτονικής αυτού, παρουσιάζονται τα επικρατέστερα πρωτόκολλα διαχείρισης ταυτότητας χρήστη για υπηρεσίες στο Διαδίκτυο και ερευνάται η αποτελεσματικότητά τους σε συνδυασμό με το μέσο παροχής τηλεπικοινωνιακής σύνδεσης, δηλαδή την υποδομή 3ης και 4ης γενιάς. Εντοπίζονται ανοικτά προβλήματα τόσο σε θέματα ασφάλειας όσο και απόδοσης. Επίσης ερευνάται μια τεχνολογία η οποία υλοποιεί ισχυρή διαχείριση ταυτότητας, αυτή των βιομετρικών συστημάτων, με στόχο την αντιμετώπιση των ανοικτών προβλημάτων ασφάλειας που εντοπίστηκαν. Όσο αφορά στην ερευνητική περιοχή **αρχιτεκτονικής δικτυακής ασφάλειας κυρίως δικτύου του φορέα παροχής ασύρματων ευρυζωνικών τηλεπικοινωνιών 3ης γενιάς**, εντοπίζονται προβλήματα ασφάλειας και παρουσιάζονται τα συστήματα παγίδευσης εισβολέων και οι προοπτικές εφαρμογής τους στο κυρίως δίκτυο του φορέα παροχής ασύρματων ευρυζωνικών τηλεπικοινωνιών 3ης γενιάς, με στόχο την αντιμετώπιση των αναγνωρισμένων ανοικτών προβλημάτων.

Το κεφάλαιο αυτό ολοκληρώνεται με την παρουσίαση κάποιων βοηθητικών μεθοδολογιών και θεωριών, οι οποίες θα υποστηρίξουν την παρουσίαση και απόδειξη της

επιστημονικής αρτιότητας των προτεινόμενων λύσεων στη συνέχεια της διατριβής. Για το σκοπό αυτό, παρουσιάζεται η άλγεβρα μοντελοποίησης πρωτοκόλλων Communicating Sequential Processes (CSP), η θεωρία παιγνίων, η θεωρία αποστροφής ρίσκου και η μεθοδολογία ανάλυσης πολλαπλών κριτηρίων.

Το **κεφάλαιο 3** περιγράφει τις προτεινόμενες λύσεις για τα προβλήματα που εντοπίστηκαν στην ερευνητική περιοχή της διαχείρισης ταυτότητας χρήστη.

Το **κεφάλαιο 4** περιγράφει την προτεινόμενη λύση για τα προβλήματα που εντοπίστηκαν στην ερευνητική περιοχή της αρχιτεκτονικής δικτυακής ασφάλειας κυρίως δικτύου του φορέα παροχής ασύρματων ευρυζωνικών τηλεπικοινωνιών 3ης γενιάς.

Το **κεφάλαιο 5** παρουσιάζει μια σύνοψη των αποτελεσμάτων της διατριβής και παρέχει τα βασικά συμπεράσματα αυτής, καθώς και προτάσεις για μελλοντική έρευνα.

Το κείμενο της διατριβής, ολοκληρώνεται με τη **βιβλιογραφία**.

ΚΕΦΑΛΑΙΟ 2: ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΕΡΕΥΝΗΤΙΚΩΝ ΠΕΡΙΟΧΩΝ ΚΑΙ ΣΑΦΗΣ ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΡΟΒΛΗΜΑΤΩΝ

2.1 ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΑ ΔΙΚΤΥΑ 3ΗΣ ΚΑΙ 4ΗΣ ΓΕΝΙΑΣ

2.1.1 ΕΙΣΑΓΩΓΗ

Η τέταρτη γενιά δικτύων έχει ως κύριο στόχο την υλοποίηση ασύρματης ευρυζωνικής δικτύωσης μέσα από τη συνένωση ετερογενών ασύρματων τηλεπικοινωνιακών τεχνολογιών με σκοπό την επίτευξη της βέλτιστης σύνδεσης του τερματικού εξοπλισμού του χρήστη με το διαδίκτυο [38]. Ο τερματικός εξοπλισμός 4ης γενιάς, χαρακτηρίζεται από [39]:

- Πολλαπλές δικτυακές διεπαφές, συμπεριλαμβανομένων των διεπαφών για δίκτυα WLAN (802.11), δίκτυα δεδομένων κινητής τηλεφωνίας όπως το General Packet Radio Service (GPRS) και το UMTS.
- Δυνατότητα δυναμικής επιλογής του βέλτιστου ως προς την απόδοση και το κόστος δικτύου.
- Δυνατότητα διαφανούς στο χρήστη μεταγωγής από το ένα δίκτυο στο άλλο.

Οι κυριότερες πρωτοβουλίες για τη δημιουργία δικτύων 4ης γενιάς, αφορούν στο συνδυασμό των υπαρχόντων ετερογενών τηλεπικοινωνιακών δικτύων, χαρακτηριστική περίπτωση των οποίων αποτελεί ο συνδυασμός δικτύων 3ης γενιάς με τα ασύρματα τοπικά δίκτυα WLAN [42], τα οποία εξετάζονται στη συνέχεια.

2.1.2 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ 3ΗΣ ΓΕΝΙΑΣ

2.1.2.1 Περιγραφή αρχιτεκτονικής

Τα τηλεπικοινωνιακά δίκτυα 3ης γενιάς υπόσχονται εξελιγμένες ευρυζωνικές υπηρεσίες, υποστηρίζοντας ένα μεγάλο εύρος εφαρμογών πολυμέσων με αυξημένη απόδοση και ασφάλεια [54]. Τα κυριαρχα πρότυπα στο χώρο των δικτύων 3ης γενιάς είναι το Universal Mobile Telecommunications System (UMTS), με κύριο πεδίο εφαρμογής την Ευρώπη και το οποίο είναι και ο επικρατέστερος αντικαταστάτης των Global System Mobile (GSM) και το Code-Division Multiple Access 2000 (CDMA2000), με κύριο πεδίο εφαρμογής την Ασία και τη Βόρεια Αμερική. Τα πρότυπα αυτά περιγράφουν ασύρματα δίκτυα με κύρια

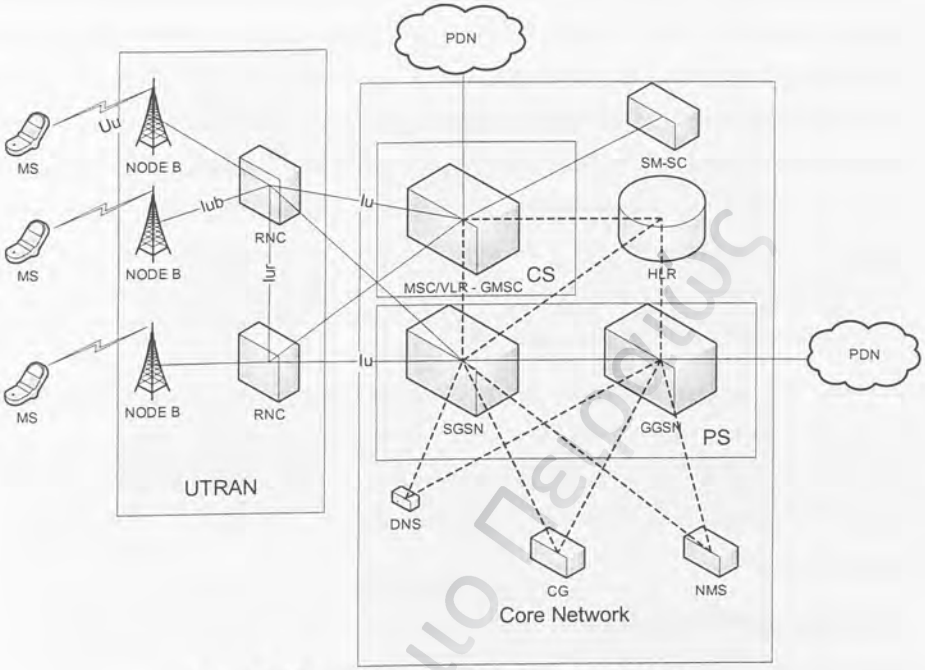
χαρακτηριστικά την κάλυψη μεγάλων γεωγραφικών περιοχών, με ρυθμούς μετάδοσης από 384 Kbs ως 2Mbs, ανάλογα με τις συνθήκες χρήσης (π.χ. ανοιχτός ή κλειστός χώρος).

Οι τελευταίες προδιαγραφές στο χώρο των δικτύων UMTS, προέρχονται από το 3rd Generation Partnership Project (3GPP)[11], το οποίο αποτελεί μία κοινή πρωτοβουλία οργανισμών τυποποίησης στο χώρο των τηλεπικοινωνιών από τις Ηνωμένες Πολιτείες, την Ευρώπη, την Ιαπωνία και τη Κορέα. Το αντίστοιχο παγκόσμιας κλίμακας 3GPP2[12] είναι υπεύθυνο για τις προδιαγραφές του CDMA2000.

Το UMTS αποτελεί τη μετεξέλιξη του GSM και του GPRS. Το Σχήμα 3 παρουσιάζει την αρχιτεκτονική ενός UMTS δικτύου σύμφωνα με τις προδιαγραφές του 3GPP, η οποία περιλαμβάνει βασικά δομικά συστατικά [71].

[11] http://www.3gpp.org

[12] http://www.3gpp2.org



Σχήμα 3: Η αρχιτεκτονική ενός δικτύου UMTS

Οι συνεχόμενες γραμμές του σχήματος αναπαριστούν τις τηλεπικοινωνιακές γραμμές δεδομένων και σηματοδοσίας, ενώ οι διακεκομμένες γραμμές αναπαριστούν αποκλειστικά τηλεπικοινωνιακές γραμμές σηματοδοσίας. Μία αρχιτεκτονική UMTS χωρίζεται σε δύο βασικά τμήματα:

- το επίγειο δίκτυο ραδιοζεύξεων (UMTS Terrestrial Radio Access Network - UTRAN), και
- το κυρίως δίκτυο (core network).

Το UTRAN αποτελείται από:

- τους κόμβους Β (Node B), οι οποίοι είναι υπεύθυνοι για τη μετάδοση και λήψη δεδομένων στην ασύρματη ζεύξη (διεπαφή Uu) με τον τερματικό εξοπλισμό χρήστη (Mobile Station - MS). Οι κόμβοι Β περιλαμβάνουν ένα σύνολο πομποδεκτών και καλύπτουν ένα αριθμό από κελιά (cells).
- τους ελεγκτές ραδιοζεύξεων (Radio Network Controllers - RNCs), οι οποίοι είναι ουσιαστικά μεταγωγείς δικτύων ασύγχρονης μετάδοσης (Asynchronous Transfer Mode - ATM) οι οποίοι πολυπλέκουν και αποπλέκουν δεδομένα και φωνή. Τα RNC συνδέονται μεταξύ τους μέσω της διεπαφής Iur, με στόχο την αυτονομία στον έλεγχο των ραδιοζεύξεων. Ένα RNC μπορεί να ελέγχει πολλαπλούς κόμβους Β, με τους οποίους συνδέεται μέσω της διεπαφής Iub.

Το κυρίως δίκτυο αποτελείται από δύο υποπεριοχές παροχής υπηρεσιών και κάποια κοινόχρηστα συστατικά, όπως η βάση δεδομένων Home Location Register (HLR), η οποία περιλαμβάνει πληροφορίες για τους συνδρομητές, τις υπηρεσίες που τους παρέχονται καθώς και παραμέτρους ασφάλειας. Άλλα κοινόχρηστα συστατικά μιας αρχιτεκτονικής UMTS συμπεριλαμβάνουν:

- Charging gateway -CG: Σύστημα τιμολόγησης
- Short Message Serving Center-SM-SC: Σύστημα υπηρεσιών μηνυμάτων

Οι υποπεριοχές περιλαμβάνουν:

- την υποπεριοχή παροχής υπηρεσιών μεταγωγής κυκλώματος (circuit switched service domain - CS),
- την υποπεριοχή παροχής υπηρεσιών μεταγωγής πακέτου (packet switched service domain - PS) και
- το υποσύστημα παροχής υπηρεσιών πολυμέσων Internet Protocol (IP) -IP multimedia subsystem: IMS.

Η υποπεριοχή παροχής υπηρεσιών μεταγωγής κυκλώματος CS αφορά σε υπηρεσίες φωνής (μετάδοση κίνησης και σηματοδοσίας) και χρησιμεύει στη σύνδεση του UTRAN με άλλα τηλεφωνικά δίκτυα, όπως το δημόσιο τηλεφωνικό δίκτυο μεταγωγής κυκλώματος (Public Switched Telephone Network). Βασικό συστατικό της αποτελεί ο μεταγωγός MSC

(Mobile Switching Center) / VLR (Visitor Location Register). Ο MSC/VLR ελέγχει τη μεταγωγή κυκλώματος για τη μετάδοση φωνής καθώς και ένα σύνολο λειτουργιών συμπεριλαμβανομένης της διαχείρισης της κινητικότητας των συνδρομητών (mobility management), της χρέωσης αυτών με χρήση των CDR (Call Detail Records) και κάποιων υπηρεσιών ασφάλειας. Τα RNC, μέσω της διεπαφής Iu, αποστέλλουν στο MSC δεδομένα φωνής πάνω από ένα δίκτυο ATM. Ένα ακόμη συστατικό είναι το Gateway MSC, το οποίο υλοποιεί μια πύλη πρόσβασης προς άλλα τηλεφωνικά δίκτυα.

Η υποπεριοχή παροχής υπηρεσιών μεταγωγής πακέτου PS αφορά στη μετάδοση ψηφιακών δεδομένων (μετάδοση κίνησης και σηματοδοσίας) και χρησιμεύει στη σύνδεση του UTRAN με άλλα δίκτυα δεδομένων (Packet Data Networks - PDNs), συμπεριλαμβανομένου του Διαδικτύου. Βασικά συστατικά του PS αποτελούν τα [45]:

- Serving GPRS Support Node (SGSN), το οποίο είναι υπεύθυνο για τη διαχείριση συνόδου και τη δρομολόγηση πακέτων προς τα κατάλληλα RNC. Το SGSN παρέχει τις ακόλουθες βασικές υπηρεσίες:
  - Πιστοποίηση ταυτότητας και δικαιωμάτων χρήστη
  - Έλεγχο υπηρεσιών
  - Συλλογή δεδομένων τιμολόγησης
  - Προώθηση μηνυμάτων
  - Δρομολόγηση μηνυμάτων
  - Μετάφραση και αντιστοίχηση διευθύνσεων
  - Ενθυλάκωση πακέτων (encapsulation)
  - Διέλευση πακέτων (tunneling)
  - Έλεγχο κινητικότητας (mobility)
- Gateway GPRS Support Node (GGSN), το οποίο αποτελεί πύλη για την επικοινωνία με εξωτερικά δίκτυα δεδομένων, αποτελώντας ουσιαστικά ένα περιφερειακό δρομολογητή. Ο GGSN παρέχει τις ακόλουθες βασικές υπηρεσίες:
  - Φιλτράρισμα – έλεγχο πακέτων
  - Έλεγχο υπηρεσιών

- Συλλογή δεδομένων τιμολόγησης (παραγωγή Call Detail Records - CDR)
- Προώθηση μηνυμάτων
- Δρομολόγηση μηνυμάτων
- Μετάφραση και αντιστοίχιση διευθύνσεων (για παράδειγμα από IP σε δείκτες GTP)
- Ενθυλάκωση πακέτων (encapsulation)
- Διέλευση πακέτων (tunneling)
- Έλεγχο κινητικότητας (mobility)

Τα RNC, μέσω της διεπαφής Iu, αποστέλλουν στο SGSN δεδομένα πάνω από ένα δίκτυο ATM (IP over ATM). Ειδικότερα, για υπηρεσίες δεδομένων, πριν ο χρήστης χρησιμοποιήσει κάποια από αυτές, θα πρέπει να αποκτήσει ένα συμφωνημένο με τον φορέα παροχής υπηρεσιών 3ης γενιάς σύνολο παραμέτρων, το οποίο ονομάζεται Packet Data Protocol context (PDP context). Το PDP context αποθηκεύεται από τον τερματικό εξοπλισμό, το SGSN και το GGSN και περιέχει πληροφορίες σύνδεσης, όπως παραμέτρους δρομολόγησης. Όταν ο χρήστης θελήσει να επικοινωνήσει με κάποιο PDN, χρησιμοποιείται ως αναγνωριστικό του δικτύου αυτού ένα όνομα σημείου πρόσβασης (Access Point Name - APN). Η πληροφορία για τα APN αποθηκεύεται στα HLR, GGSN και DNS, καθώς και στον τερματικό εξοπλισμό του χρήστη ως μια λίστα πιθανών σημείων πρόσβασης κατά την εγγραφή του χρήστη στο σύστημα. Για κάθε APN, ο εξυπηρετητής DNS φυλάσσει τη διεύθυνση IP του GGSN που εξυπηρετεί το συγκεκριμένο δίκτυο PDN το οποίο αντιστοιχεί στο APN. Όταν ο χρήστης θελήσει να συνδεθεί στο συγκεκριμένο PDN (για παράδειγμα το Διαδίκτυο), τότε το SGSN που εξυπηρετεί τον χρήστη, πραγματοποιεί μια αναζήτηση DNS για το APN, ως απάντηση της οποίας αποστέλλεται η διεύθυνση IP του κατάλληλου GGSN.

Για την παροχή υπηρεσιών δεδομένων εμπλέκονται και άλλες υπο-υπηρεσίες και πρωτόκολλα. Για παράδειγμα, για την ανάθεση μιας διεύθυνσης IP σε ένα τερματικό εξοπλισμό μπορεί να επιλεγεί από τον φορέα παροχής υπηρεσιών 3ης γενιάς η κατάσταση διαφανούς ή μη διαφανούς πρόσβασης. Στην πρώτη περίπτωση, ο φορέας παροχής υπηρεσιών 3ης γενιάς είναι εκείνος ο οποίος αναθέτει μια διεύθυνση IP από μια λίστα διαθέσιμων διευθύνσεων, ενώ στη δεύτερη περίπτωση, παρέχει απλά την υποδομή σύνδεσης και ο τερματικός εξοπλισμός αποκτά διεύθυνση IP από τον φορέα παροχής υπηρεσιών Διαδικτύου (Internet Service Provider - ISP). Άλλα πρωτόκολλα αφορούν σε συνδέσεις IP από άκρο σε άκρο (Peer to Peer) με χρήση του πρωτοκόλλου SIP (Session Initiation Protocol) ή για παράδειγμα στην κάλυψη των αναγκών διατήρησης μιας σύνδεσης (και διεύθυνσης IP) όταν ο χρήστης αλλάζει σημείο πρόσβασης στο δίκτυο, οπότε και χρησιμοποιείται το πρωτόκολλο Mobile IP.

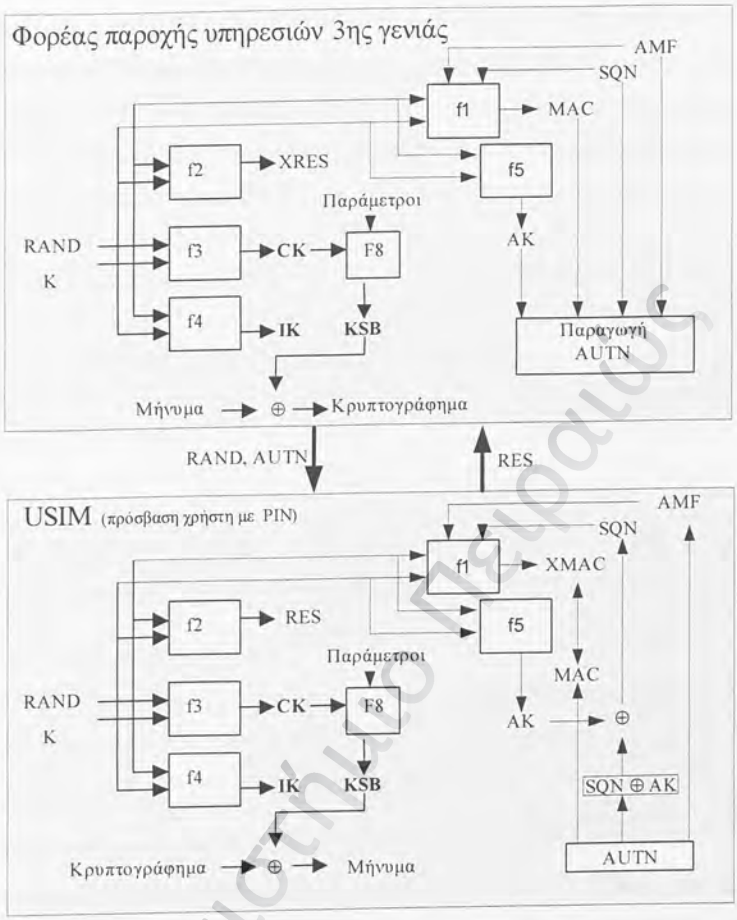
Το IMS παρέχει υπηρεσίες πολυμέσων IP πάνω από την υποπεριοχή PS.

2.1.2.2 Μηχανισμός ασφάλειας πρόσβασης χρήστη στην υποδομή 3ης γενιάς

Στην παρούσα παράγραφο εξετάζουμε το μηχανισμό σύνδεσης του τερματικού εξοπλισμού χρήστη στην υποδομή 3ης γενιάς. Τα περιστατικά ασφάλειας ήταν πολλαπλά στα δίκτυα 2ης γενιάς [55]. Τα δίκτυα 2ης γενιάς ήταν ευαίσθητα σε ενεργές και παθητικές επιθέσεις, όπως η χρήση μη εξουσιοδοτημένου εξοπλισμού για την αναπαράσταση νόμιμου κόμβου πρόσβασης στο δίκτυο, λόγω της μη πιστοποίησης του κόμβου πρόσβασης του φορέα παροχής υπηρεσιών 2ης γενιάς στον τερματικό εξοπλισμό χρήστη. Προβλήματα υπήρχαν και στο κρυπτογραφικό υπόβαθρο, επιτρέποντας την απόκτηση κρυπτογραφικών κλειδιών που αποστέλλονταν μη κρυπτογραφημένα στο ασύρματο μέσο καθώς και επιθέσεις ωμής δύναμης (brute force) στα κρυπτογραφημένα δεδομένα. Στα δίκτυα UTRAN η ασφάλεια έχει σχεδιαστεί ως αναπόσπαστο τμήμα της συνολικής αρχιτεκτονικής[68], αντιμετωπίζοντας τα σημαντικότερα προβλήματα ασφάλειας των δικτύων 2ης γενιάς.

Ο πυρήνας της ασφάλειας των UMTS δικτύων είναι ο μηχανισμός UMTS Authentication and Key Agreement (UMTS-AKA) [76], ο οποίος έχει ως στόχο την ικανοποίηση αναγκών διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας της πληροφορίας, συμπεριλαμβανομένης της εμπιστευτικότητας της ταυτότητας του χρήστη, των

χρησιμοποιούμενων από αυτόν υπηρεσιών και της γεωγραφικής του θέσης. Επίσης, πρωταρχικός στόχος είναι η ικανοποίηση των θεμελιωδών αναγκών αμφίδρομης αναγνώρισης, πιστοποίησης ταυτότητας χρήστη και δικτύου 3ης γενιάς, καθώς και της εξουσιοδότησης του χρήστη. Ο μηχανισμός UMTS-AKA, βασίζεται σε ένα προσυμφωνημένο κλειδί K μήκους 128-bit, μεταξύ της υποδομής 3ης γενιάς και της κάρτας UMTS Subscriber Identity Module (USIM) που βρίσκεται εγκατεστημένη στον εξοπλισμό του χρήστη. Η USIM είναι μια έξυπνη κάρτα με κρυπτογραφικές δυνατότητες, η οποία χαρακτηρίζεται από ένα μοναδικό αριθμό 15 ψηφίων, ο οποίος ονομάζεται International Mobile Subscriber Identity (IMSI). Η αμφίδρομη πιστοποίηση ταυτότητας επιτυγχάνεται με υλοποίηση ενός μηχανισμού ερωταπόκρισης (challenge and response) που βασίζεται σε ένα είδος συναρτήσεων σύνοψης βάσει κλειδιού (keyed-hashing), ενώ οι ανάγκες για εμπιστευτικότητα και ακεραιότητα των μηνυμάτων που ανταλλάσσονται ικανοποιούνται με συμμετρικούς κρυπτογραφικούς αλγόριθμους και κώδικες αυθεντικοποίησης μηνυμάτων (Message Authentication Codes - MAC) αντίστοιχα. Το Σχήμα 4 παρουσιάζει τα βασικά στοιχεία του μηχανισμού UMTS-AKA, τα οποία αναλύονται στη συνέχεια.



Σχήμα 4: Βασικά στοιχεία του μηχανισμού UMTS-AKA

Αρχικά, ο χρήστης εισάγει τον αριθμό PIN για την ενεργοποίηση της κάρτας USIM [77]. Η κάρτα USIM αναγνωρίζεται από την υποδομή 3ης γενιάς με αποστολή του IMSI. Στη συνέχεια παράγεται από την υποδομή 3ης γενιάς ένας τυχαίος αριθμός (RAND), μήκους 128-bit, και αποστέλλεται στη USIM μαζί με μία ακόμη τιμή (AUTN). Η τιμή AUTN παράγεται σύμφωνα με την παρακάτω εξίσωση (ο τελεστής | |, σημαίνει αλληλουχία):

$$AUTN = SQN \oplus AK \,||\, AMF \,||\, MAC$$

Η τιμή SQN είναι ένας σειριακός αριθμός, η τιμή AK είναι ένα κλειδί το οποίο παράγεται από το συνδυασμό των τιμών RAND και K μέσα από μία συνάρτηση (f5), η τιμή AMF εκφράζει ένα αναγνωριστικό πιστοποίησης και διαχείρισης κλειδιών και η τιμή MAC παράγεται από το συνδυασμό των K, RAND, SQN και AMF μέσα από μία συνάρτηση (f1). Η USIM, λαμβάνει τον τυχαίο αριθμό (RAND) και τον συνδυάζει με το προσυμφωνημένο κλειδί K, ώστε να αναλύσει την τιμή AUTN και να πιστοποιήσει την ταυτότητα της υποδομής 3ης γενιάς. Πιο συγκεκριμένα, με τη λήψη του AUTN, η USIM δέχεται τις τιμές $SQN \oplus AK$, AMF και MAC. Η USIM υπολογίζει την τιμή AK με συνδυασμό των τιμών RAND και K μέσα από τη συνάρτηση f5 και τη χρησιμοποιεί σύμφωνα με την παρακάτω εξίσωση για την ανάκτηση του SQN:

$$SQN = SQN \oplus AK \oplus AK$$

Στη συνέχεια, η USIM χρησιμοποιεί τις τιμές AMF, SQN, K και RAND για τον υπολογισμό της τιμής XMAC, μέσα από τη συνάρτηση f1. Στη συνέχεια συγκρίνονται οι τιμές XMAC και MAC για την πιστοποίηση του μηνύματος.

Στη συνέχεια, η USIM υπολογίζει μια τιμή (RES) με εφαρμογή του K και του RAND σε μια συνάρτηση (f2) και την αποστέλλει στην υποδομή 3ης γενιάς. Ο φορέας παροχής με τη σειρά του υπολογίζει ομοίως την τιμή (XRES) και τη συγκρίνει με τη RES, με στόχο την πιστοποίηση της ταυτότητας της USIM.

Για την υλοποίηση εμπιστευτικότητας και ακεραιότητας, παράγονται τα κλειδιά-βάσεις εμπιστευτικότητας (Cipher Key – CK) και ακεραιότητας (Integrity Key – IK) μήκους 128-bit, με εφαρμογή του K και ενός τυχαίου αριθμού RAND σε συγκεκριμένους αλγόριθμους (f3 και f4 αντίστοιχα). Η κρυπτογράφηση (X') της πληροφορίας (X), επιτυγχάνεται με την εφαρμογή του CK και μιας σειράς παραμέτρων σε μία συνάρτηση (f8), από όπου προκύπτει η τιμή Keystream Block (KSB). Ο συνδυασμός της τιμής αυτής με την πληροφορία μέσα από μια συνάρτηση της άλγεβρας Boole 'Αποκλειστικό ή' (Exclusive OR) πραγματοποιεί την κρυπτογράφηση σύμφωνα με την παρακάτω εξίσωση:

$$X' = KSB \oplus X$$

Το σύνολο των τιμών RAND, XRES, CK, IK και AUTN, αποτελούν τις βασικές προσωρινές παραμέτρους πιστοποίησης του χρήστη και συνιστούν το διάνυσμα πιστοποίησης (Authentication Vector – AV). Το διάνυσμα αυτό μεταλλάσσεται, με κάθε πλήρη διαδικασία πιστοποίησης του χρήστη, με βασική την αλλαγή της τιμής RAND, η οποία επηρεάζει όλες τις υπόλοιπες.

Για τη διαφύλαξη της εμπιστευτικότητας της ταυτότητας και γεωγραφικής θέσης του χρήστη, καθώς και των χρησιμοποιούμενων από αυτόν υπηρεσιών, ο μηχανισμός UMTS-AKA οφείλει να προφυλάσσει το αναγνωριστικό IMSI. Αυτό υλοποιείται προαιρετικά με την κρυπτογράφηση του IMSI κατά την πρώτη πλήρη διενέργεια του UMTS-AKA με ένα ομαδικό κλειδί. Στη συνέχεια, παράγονται προσωρινά, τυχαία αναγνωριστικά το οποίο ονομάζονται Temporary Mobile Subscriber Identities (TMSI), τα οποία αντιστοιχίζονται τοπικά στο IMSI, στην υποδομή 3ης γενιάς. Το TMSI, το οποία ανά περίπτωση μπορεί να συνοδεύεται και από ένα αναγνωριστικό περιοχής (Location Area Identity), αποστέλλεται κρυπτογραφημένο στη USIM. Η αναγνώριση μέσω του IMSI πραγματοποιείται μόνο όταν το δίκτυο εξυπηρέτησης (service network) δεν μπορεί να αναγνωρίσει τον χρήστη από το TMSI.

Συνοψίζοντας τα παραπάνω, η αλυσίδα ασφάλειας πρόσβασης χρήστη σε επίπεδο UTRAN καταλήγει στην πιστοποίηση της ταυτότητας χρήστη στην τερματική συσκευή, η οποία υλοποιείται με τη χρήση ενός PIN. Η περαιτέρω πιστοποίηση ταυτότητας χρήστη στο δίκτυο 3ης γενιάς πραγματοποιείται με χρήση προ-αποθηκευμένων αναγνωριστικών (IMSI) και συμμετρικών κλειδιών K, τα οποία ενεργοποιούνται αυτόματα με την εισαγωγή του PIN.

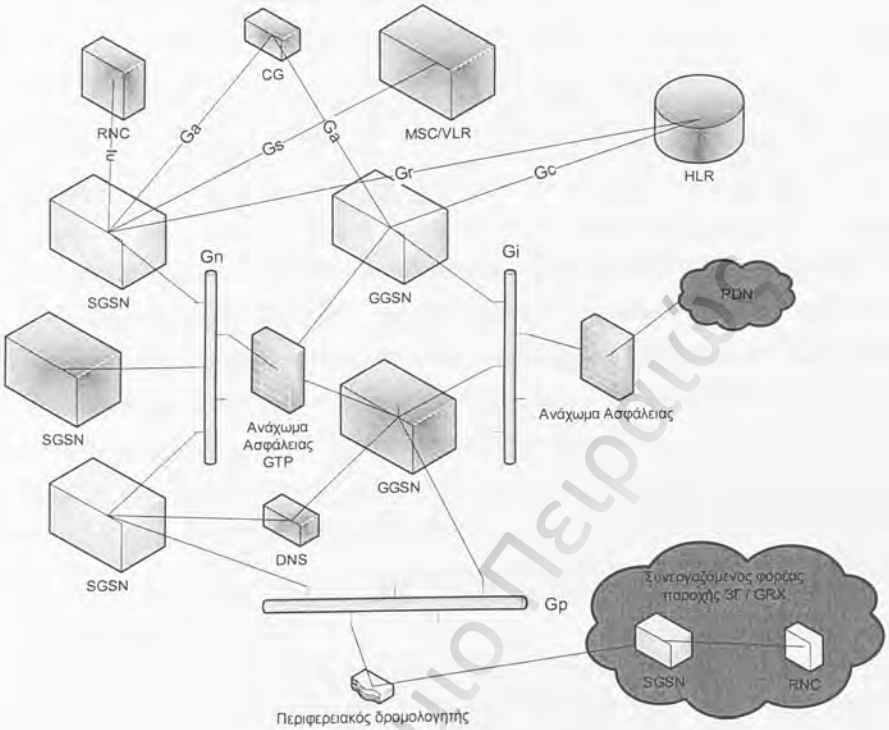
Τα συστήματα ενός (π.χ. χρήση PIN) και δύο (π.χ. χρήση PIN και έξυπνης κάρτας) κριτηρίων έχουν αδυναμίες που οφείλονται στο γεγονός ότι τόσο η γνώση όσο και η κατοχή τεκμηρίων δεν χαρακτηρίζουν μοναδικά το χρήστη [141]. Επιπροσθέτως, έχουν δημοσιευθεί ερευνητικές εργασίες με αντικείμενο την παραβίαση της ασφάλειας του PIN [70], τονίζοντας την ανάγκη για ισχυρότερους μηχανισμούς πιστοποίησης ταυτότητας χρήστη. Στο πλαίσιο παροχής αυξανόμενου πλήθους ευαίσθητων υπηρεσιών σε δίκτυα 3ης γενιάς [69], όπως οι υπηρεσίες ηλεκτρονικού εμπορίου, καθίσταται αναγκαίος ένας μηχανισμός ισχυρής πιστοποίησης ταυτότητας. Ειδικά μάλιστα στο χώρο των εφαρμογών πάνω από δίκτυα 3ης και 4ης γενιάς, η απαιτούμενη μελέτη είναι ιδιαίτερη σημαντική, λαμβάνοντας υπόψη την

ιδιαιτερότητα του μέσου μετάδοσης (ασύρματο) των προσωπικών δεδομένων των χρηστών, κάτι που αποτελεί διαπίστωση που εκφράζεται με ειδική μνεία στις σχετικές κυβερνητικές πολιτικές, τόσο των Ηνωμένων Πολιτειών της Αμερικής, όσο και της Ευρωπαϊκής Ένωσης [1,2].

2.1.2.3 Αρχιτεκτονική υπο-περιοχής μεταγωγής πακέτου κυρίως δικτύου

2.1.2.3.1 Περιγραφή

Πέρα από την ασφάλεια στο UTRAN, η οποία, παρ' όλες τις ατέλειες, σημείωσε βελτίωση στα δίκτυα 3ης γενιάς, είναι σημαντικό να εξετάσουμε όλα τα συστατικά τα οποία συμμετέχουν στην παροχή υπηρεσιών δεδομένων πάνω από μια αρχιτεκτονική 3ης γενιάς, δηλαδή την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου, η οποία είναι κοινή και για δίκτυα 4ης γενιάς, όπως θα δούμε σε επόμενη παράγραφο. Στο Σχήμα 5 παρουσιάζονται τα βασικά συστατικά της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου και η διασύνδεση αυτών με άλλα συστατικά του κυρίως δικτύου [71].



Σχήμα 5: Διασύνδεση συστατικών υπο-περιοχής μεταγωγής πακέτου με άλλα συστατικά του κυρίως δικτύου

Τα βασικά συστατικά της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου, όπως αναφέρθηκε και στην προηγούμενη παράγραφο, είναι τα SGSN και GGSN. Η μεταξύ τους επικοινωνία πραγματοποιείται μέσω της διεπαφής Gn. Το GGSN παρέχει διασύνδεση με εξωτερικά δίκτυα δεδομένων και το Διαδίκτυο, μέσω της διεπαφής Gi. Η διεπαφή Gp συνδέει τα SGSN και GGSN με άλλα δίκτυα συνεργαζόμενων φορέων μέσω περιμετρικού δρομολογητή, όπως με άλλους φορείς παροχής υπηρεσιών 3ης γενιάς στο πλαίσιο παροχής υπηρεσιών περιαγωγής (Roaming Partner / GPRS Roaming Exchange). Η διεπαφή Gp μπορεί να συνδυάζεται με τη διεπαφή Gn ή μπορεί να αποτελούν ξεχωριστές διεπαφές, ανάλογα με την υλοποίηση. Η διεπαφή Iu, συνδέει τα SGSN με τα RNC, η διεπαφή Ga, τα

SGSN και GGSN με την πύλη CG. Οι Gs και Gr, είναι οι διεπαφές του SGSN με τα MCS/VLR και HLR αντίστοιχα, ενώ η διεπαφή μεταξύ HLR και GGSN είναι η Gc.

Το βασικό πρωτόκολλο επικοινωνίας της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου είναι το GPRS Tunneling Protocol (GTP) [73]. Το GTP είναι ένα πρωτόκολλο το οποίο υλοποιεί τη δημιουργία μιας οδού διέλευσης (Tunneling) για τη μεταφορά πακέτων των χρηστών διαφόρων πρωτοκόλλων, των οποίων η ενθυλάκωση γίνεται μέσα σε πακέτα GTP, στο εσωτερικό μιας GPRS υποδομής και μεταξύ διαφορετικών GPRS υποδομών. Το GGSN πραγματοποιεί ενθυλάκωση πακέτων χρηστών που προέρχονται από εξωτερικά δίκτυα δεδομένων σε πακέτα GTP, τα οποία προωθούνται στο SGSN μέσω της διεπαφής Gn και από εκεί στο RNC, όπου και ακολουθείται η διαδικασία απο-ενθυλάκωσης για την παράδοση στους χρήστες ή σε άλλα δίκτυα μέσω της διεπαφής Gp, όπου τα παραλαμβάνουν και πάλι τα SGSN άλλων φορέων παροχής και στη συνέχεια το RNC. Προς την αντίθετη κατεύθυνση, το RNC ή το SGSN είναι το συστατικό που υλοποιεί την ενθυλάκωση και το GGSN την απο-ενθυλάκωση των πακέτων των χρηστών.

2.1.2.3.2 Προβλήματα ασφάλειας

Τα κυρίως δίκτυα (core networks) παροχής κινητών υπηρεσιών 3ης γενιάς δεν αποτελούν δίκτυα τα οποία δημιουργήθηκαν εξ' αρχής, μέσα από σχεδίαση, ανάπτυξη και υλοποίηση, που βασίζεται σε ανάλυση των σύγχρονων απαιτήσεων των παρεχόμενων υπηρεσιών. Αποτελούν μια μετεξέλιξη, ή αλλιώς μια αναβάθμιση από δίκτυα προηγούμενων γενεών που παρείχαν υπηρεσίες φωνής και πολύ περιορισμένες υπηρεσίες δεδομένων σε δίκτυα τα οποία παρέχουν ένα μεγάλο πλήθος ευρυζωνικών υπηρεσιών φωνής και δεδομένων. Πιο συγκεκριμένα, συντελέσθηκε μια μετεξέλιξη από κλειστά δίκτυα που βασίζονταν στο σύστημα σηματοδοσίας Signalling System 7 (SS7), το οποίο υπάρχει ακόμη στις υποδομές των φορέων παροχής υπηρεσιών 3ης γενιάς, σε ανοικτά δίκτυα IP παροχής υπηρεσιών πολυμέσων.

Το αποτέλεσμα αυτής της μετεξέλιξης, η οποία έγινε κάτω από τη χρονική πίεση για άμεση παροχή νέων υπηρεσιών, είναι ένα μείγμα παλαιών και νέων τεχνολογιών, εφαρμογών και συστημάτων, τα οποία δεν έχουν κοινές προδιαγραφές και δυνατότητες

ασφάλειας [81]. Αυτό συνεπάγεται ανεπαρκή προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των βασικών κατηγοριών δεδομένων, που διαχειρίζονται τα κυρίως δίκτυα, συμπεριλαμβανομένων των δεδομένων χρηστών (user traffic), της σηματοδοσίας (signaling) και των δεδομένων ελέγχου (control data). Ερευνητικές εργασίες αναφέρουν ευπαθή σημεία των σύγχρονων υποδομών υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου, όπως [56,57, 58, 59, 60]:

- επίπεδη αρχιτεκτονική ασφάλειας για όλα τα συστατικά του κυρίως δικτύου, ανεξαρτήτου των ιδιαιτεροτήτων και απαιτήσεων ασφάλειας κάθε συστατικού,
- κοινά συστήματα διαχείρισης και εποπτείας για όλη την υποδομή του κυρίως δικτύου, δημιουργώντας ένα ευάλωτο σημείο επίθεσης (single point of attack) και επιτρέποντας επιθέσεις από την μια υποπεριοχή (PS) στην άλλη (CS),
- διασυνδεδεμένα εταιρικά δίκτυα με το κυρίως δίκτυο, κάτω από κοινή υποδομή IP, με περιορισμένο ως ανύπαρκτο έλεγχο,
- μεγάλο αριθμό αρχείων καταγραφής (logs) από ετερογενή συστήματα, τα οποία δεν εξετάζονται αποτελεσματικά,
- αναποτελεσματικό ως ανύπαρκτο φιλτράρισμα δικτυακής κίνησης στις περιμέτρους και στο εσωτερικό του κυρίως δικτύου – αναποτελεσματικά αναχώματα ασφάλειας,
- απουσία συστημάτων εντοπισμού και αναχαίτισης εισβολών (intrusion detection and prevention systems),
- έλλειψη εξειδικευμένου προσωπικού –και γνώσης - σε θέματα ασφάλειας της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου.

Εξετάζοντας εναλλακτικές περιπτώσεις για την παραβίαση της ασφάλειας της υποδομής υπηρεσιών δεδομένων ενός φορέα παροχής υπηρεσιών 3ης γενιάς, διακρίνουμε τις πιθανές επιθέσεις σε εσωτερικές και εξωτερικές.

Οι εξωτερικές επιθέσεις μπορεί να πραγματοποιηθούν από εξωτερικά δίκτυα δεδομένων, μέσω της διεπαφής Gi, από άλλους φορείς παροχής υπηρεσιών 3ης γενιάς, μέσω της διεπαφής Gp και πιθανώς από τερματικές συσκευές χρηστών, μέσω του RNC. Το GGSN, ως πύλη διασύνδεσης με εξωτερικά δίκτυα, υλοποιεί ένα σύνολο αντιμέτρων ασφάλειας. Το

φιλτράρισμα των πακέτων αν και σύμφωνα με τις προδιαγραφές του 3GPP [73] υλοποιείται από το GGSN, πολλές φορές στην πράξη [45] αποτελεί ευθύνη ενός εξυπηρετητή αναχώματος ασφάλειας (firewall server), όπως παρουσιάζεται στο Σχήμα 5. Μικρότερη ως μηδενική σημασία δίνεται στη διεπαφή Gp και τη διασύνδεση με άλλους φορείς παροχής υπηρεσιών 3ης γενιάς, η ασφάλεια της οποίας περιορίζεται συνήθως στο φιλτράρισμα πακέτων στον περιφερειακό δρομολογητή, χωρίς αυτό να περιλαμβάνει ένα πλήρες σύνολο φιλτραρίσματος πληροφορίας IP ή περιορισμό πρόσβασης σε επίπεδο θυρών [57].

Οι επιθέσεις από το εσωτερικό αφορούν σε επιθέσεις από τα υπάρχοντα SGSN και GGSN, όσον αφορά την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου, την οποία και εξετάζουμε. Οι επιθέσεις αυτές μπορεί να υλοποιηθούν από τους χρήστες του συστήματος, ή να αποτελέσουν εφαλτήριο εισβολέων, οι οποίοι με επιθέσεις από το εξωτερικό έχουν καταφέρει να κατακτήσουν κάποιο GGSN ή SGSN. Στο Σχήμα 5, τονίζονται τα συστατικά, τα οποία είναι ιδιαίτερα ευάλωτα σε επιθέσεις από κάποιο GGSN ή SGSN, λόγω της άμεσης σύνδεσης που έχουν με αυτά και λόγω της έλλειψης αντιμέτρων προστασίας στη μεταξύ τους επικοινωνία. Αυτά μπορεί να περιλαμβάνουν τα HLR, MSC/VLR, CG, και RNC. Η κατάκτηση κάποιου GGSN ή SGSN είναι ιδιαίτερα σημαντική διότι εκτίθενται άμεσα (λόγω της μη διαχωρισμένης αρχιτεκτονικής) πολύ σημαντικά συστατικά με πολύ υψηλό κόστος λόγω των δεδομένων που διαχειρίζονται και τα οποία αφορούν και σε προσωπικά δεδομένα, συμπεριλαμβανομένων στοιχείων κλήσεων και τιμολόγησης, αλλά και λόγω των υψηλών απαιτήσεων σε διαθεσιμότητα με πολύ μικρά επιτρεπόμενα όρια μη λειτουργίας. Πέρα από την έκθεση άλλων συστατικών εκτίθενται και οι ίδιες οι λειτουργίες των GGSN ή SGSN, οι οποίες πέρα από την παροχή υπηρεσιών συνδεσιμότητας των χρηστών με εξωτερικά δίκτυα αφορούν και σε άλλες υπηρεσίες, όπως αυτές της συλλογής δεδομένων τιμολόγησης (παραγωγή Call Detail Records - CDR), σύμφωνα με τα όσα περιγράφονται στην προηγούμενη παράγραφο, οι οποίες στο σύνολό τους έχουν σημαντικό κόστος. Επιπλέον, κατάκτηση ή εσωτερική επίθεση από ένα SGSN ή GGSN εκθέτει την αντίστοιχη υποδομή άλλων φορέων παροχής υπηρεσιών 3ης γενιάς μέσω της διεπαφής Gp και θέτει υπόλογο τον φορέα από τον οποίο ξεκινά μια επίθεση. Οι Whitehouse και Murphy [57], έχουν προτείνει την υλοποίηση ενός αναχώματος ασφάλειας στη διεπαφή Gn με στόχο το φιλτράρισμα της πληροφορίας GTP και την αντιμετώπιση επιθέσεων κατά του πρωτοκόλλου. Τέτοια προϊόντα

είναι διαθέσιμα στην αγορά. Παρόλα αυτά η γνώση των φορέων παροχής υπηρεσιών 3ης γενιάς για επιθέσεις ενάντια στο GTP είναι περιορισμένη και η παραμετροποίηση του συγκεκριμένου αναχώματος περιορίζεται συνήθως στο τυπικό φιλτράρισμα που προτείνει ο κατασκευαστής.

Επιπλέον, στην ίδια εργασία [57] περιγράφονται εξειδικευμένα σενάρια επιθέσεων, όπως αυτό της υπερτιμολόγησης χρήστη (over-billing attack). Η επίθεση αυτή υλοποιείται με σύνδεση του επιτιθέμενου σε ένα GGSN και απόκτηση μιας διεύθυνσης IP μέσω του συστήματος δυναμικής απόδοσης διευθύνσεων (DHCP). Στη συνέχεια, ο επιτιθέμενος στέλνει μια αίτηση αποστολής δεδομένων σε ένα εξυπηρετητή στο Διαδίκτυο, ο οποίος ξεκινά την αποστολή δεδομένων προς τον επιτιθέμενο. Ο επιτιθέμενος στη συνέχεια αποσυνδέεται από το κυρίως δίκτυο, αποδεσμεύοντας την διεύθυνση IP. Η διεύθυνση IP είναι πολύ πιθανό στη συνέχεια να αποδοθεί σε κάποιον άλλο συνδρομητή και καθώς ο εξυπηρετητής στο Διαδίκτυο συνεχίζει να στέλνει δεδομένα στη συγκεκριμένη διεύθυνση IP. Αυτό έχει ως αποτέλεσμα την υπερ-τιμολόγηση του συνδρομητή. Η ίδια ερευνητική εργασία προτείνει την αποστολή σήματος από το GGSN προς τον εξυπηρετητή στο Διαδίκτυο για διακοπή της σύνδεσης (αποστολή μηνύματος ICMP destination unreachable), παρ' ολα αυτά, δεν είναι σίγουρο ότι ο εξυπηρετητής στο Διαδίκτυο θα σταματήσει την αποστολή δεδομένων (ίσως το μήνυμα κοπεί σε κάποιο ανάχωμα ασφάλειας ή αγνοηθεί λόγω της παραμετροποίησης του εξυπηρετητή). Οι εξειδικευμένες αυτές επιθέσεις αυτές φανερώνουν την ανάγκη ύπαρξης ενός συστήματος μελέτης επιθέσεων για την αποτελεσματική αντιμετώπισή τους.

2.1.2.4 Σύνοψη προβλήματος - μελέτη επίδρασης στη λειτουργία των φορέων παροχής υπηρεσιών 3ης και 4ης γενιάς

Από τα παραπάνω, συνοψίζουμε στο ότι η **οργάνωση της ασφάλειας της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου είναι επίπεδη και ανεπαρκής.** Τα ευπαθή σημεία που καταγράφηκαν στην προηγούμενη παράγραφο οδηγούν στις ακόλουθες απειλές:

- Κρίσιμα συστήματα όπως τα GGSN και SGSN εκτίθενται σε επιθέσεις

- Τα εκτεθειμένα GGSN και SGSN εκθέτουν με το φαινόμενο ντόμινο την ασφάλεια του κυρίως δικτύου. Τα GGSN και SGSN μπορεί να μετατραπούν σε εφαλτήρια επιθέσεων προς άλλα κρίσιμα συστήματα, όπως τα HLR, MSC/VLR, CG και συστήματα τιμολόγησης κλήσεων. Η απειλή αυτή φανερώνει τα ανεπαρκή μέτρα δικτυακής ασφάλειας στο εσωτερικό της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου.
- Το κυρίως δίκτυο του φορέα παροχής 3ης ή 4ης γενιάς αποτελεί λογική επέκταση του αντίστοιχου δικτύου συνεργαζόμενων φορέων παροχής 3ης ή 4ης γενιάς λόγω του ανεπαρκούς ελέγχου της διεπαφής Gp. Το γεγονός αυτό εκθέτει όλους του εμπλεκόμενους φορείς σε σημαντικές απειλές, τόσο διαρροής ευαίσθητων εταιρικών δεδομένων όσο και αδυναμίας απόδοσης ευθυνών σε περίπτωση ενός περιστατικού ασφάλειας.
- Η αναποτελεσματική υποδομή καταγραφής συμβάντων σε συνδυασμό με την απουσία συστημάτων εντοπισμού και αναχαίτισης εισβολών έχει επίδραση στην έγκαιρη αναγνώριση και αντιμετώπιση ενός συμβάντος ασφάλειας, καθώς και στη διαδικασία διερεύνησης αυτού από εναπομείναντα ίχνη.

Τα παραπάνω ανάγονται σε απειλές ενάντια στην εμπιστευτικότητα , την ακεραιότητα και τη διαθεσιμότητα ευαίσθητης πληροφορίας και συστημάτων, η πιθανή πραγματοποίηση των οποίων θα επιφέρει τις ακόλουθες επιδράσεις στον φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς:

- Άμεσες ή έμμεσες χρηματικές απώλειες: για παράδειγμα λόγω αδυναμίας παροχής υπηρεσιών κατά τη διάρκεια επιθέσεων άρνησης εξυπηρέτησης ή λόγω απώλειας της ακεραιότητας ή διαθεσιμότητας δεδομένων τιμολόγησης (billing data).
- Δυσφήμηση: για παράδειγμα λόγω διαρροής δεδομένων συνδρομητών, λόγω ανεπαρκούς παροχής υπηρεσιών κατά τη διάρκεια επιθέσεων άρνησης εξυπηρέτησης σε συστήματα όχι κατ' ανάγκη της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου, αλλά και περισσότερο κρίσιμων όπως το HLR, ή λόγω εξαπόλυσης επιθέσεων από παραβιασμένο GGSN ή SGSN στην υποδομή συνεργαζόμενου φορέα.

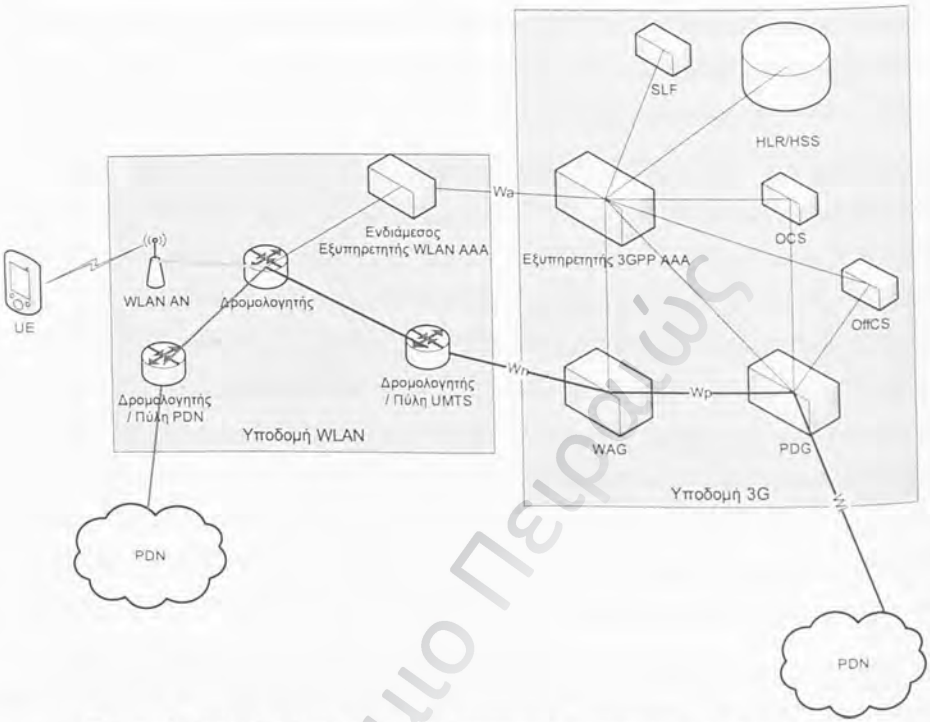
- Νομικές συνέπειες: για παράδειγμα, λόγω της απώλειας εμπιστευτικότητας προσωπικών δεδομένων συνδρομητών ή στοιχείων κλήσεων αυτών, ή λόγω αδυναμίας συμμόρφωσης με το νομικό πλαίσιο περί άρσης του απορρήτου, κυρίως λόγω έλλειψης της ακεραιότητας και της διαθεσιμότητας δεδομένων και συστημάτων.

Συνοψίζουμε στο ότι οι αρχιτεκτονικές δικτυακής ασφάλειας του κυρίως δικτύου ενός φορέα παροχής υπηρεσιών 3ης γενιάς είναι ανεπαρκείς, με κύριο χαρακτηριστικό μία επίπεδη αρχιτεκτονική ασφάλειας που βασίζεται σε ελλιπή αναχώματα ασφάλειας και απουσία συστημάτων ανίχνευσης και αναχαίτισης εισβολών. Οι ενδεχόμενες συνέπειες από την πραγματοποίηση κάποιας απειλής, μέσα από την εκμετάλλευση κάποιας αδυναμίας του συστήματος, καθιστούν επιτακτική τη δημιουργία μιας αποτελεσματικής αρχιτεκτονικής ασφάλειας για την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου. Πέρα από τη δημιουργία μιας πιο αποτελεσματικής αρχιτεκτονικής ασφάλειας για την αντιμετώπιση των υπαρχόντων ευπαθών σημείων, πολύ σημαντική είναι η ύπαρξη εξειδικευμένης γνώσης ασφάλειας στους φορείς παροχής υπηρεσιών 3ης γενιάς, ώστε να είναι σε θέση να αντιμετωπίζουν εξειδικευμένες επιθέσεις σε δίκτυα 3ης γενιάς.

2.1.3 Αρχιτεκτονική 4ης γενιάς – Συνδυασμένα δίκτυα 3ης γενιάς με ασύρματα τοπικά δίκτυα

2.1.3.1 Περιγραφή αρχιτεκτονικής

Στο χώρο των ασύρματων τοπικών δικτύων (Wireless Local Area Network –WLAN), τα κυριαρχα πρότυπα προέρχονται από το Institute of Electrical and Electronics Engineers (IEEE) και το European Telecommunications Standards Institute (ETSI) και είναι τα IEEE 802.11 και HiperLAN αντίστοιχα. Τα πρότυπα IEEE 802.11g [46] και HiperLAN, προδιαγράφουν ρυθμό μετάδοσης δεδομένων 54Mb/s και εμβέλεια από 30 ως 300 μέτρα. Η πιο διαδεδομένη σειρά προτύπων στην Ευρώπη και στη χώρα μας ειδικότερα είναι η IEEE 802.11. Το 2001, το 3GPP, αποφάσισε τη μελέτη του συνδυασμού 3G/WLAN και την ανάπτυξη προδιαγραφών αρχιτεκτονικής [74] και ασφάλειας [75]. Το Σχήμα 6 παρουσιάζει την αρχιτεκτονική ενός συνδυασμένου συστήματος 3G/WLAN.



Σχήμα 6: Αρχιτεκτονική ενός συνδυασμένου συστήματος 3G/WLAN

Σύμφωνα με τις προδιαγραφές του 3GPP υπάρχουν δύο διακριτά σενάρια λειτουργίας:

- Σενάριο Α: Άμεση πρόσβαση IP (WLAN Direct IP Access) μέσω ασύρματου τοπικού δικτύου, όπου η υποδομή 3ης γενιάς χρησιμεύει στην αναγνώριση, πιστοποίηση και εξουσιοδότηση του χρήστη, ο οποίος στη συνέχεια συνδέεται σε ένα δίκτυο δεδομένων (Packet Data Network - PDN) μέσω της υποδομής WLAN.
- Σενάριο Β: Πρόσβαση μέσω υποδομής 3ης γενιάς (WLAN 3GGP IP Access) όπου η αναγνώριση, πιστοποίηση και εξουσιοδότηση του χρήστη γίνεται και πάλι από την υποδομή 3ης γενιάς, αλλά η σύνδεση σε ένα PDN πραγματοποιείται μέσω της υποδομής 3ης γενιάς.

Πιο αναλυτικά, όταν ο εξοπλισμός χρήστη, ο οποίος είναι εφοδιασμένος με δύο τουλάχιστον διεπαφές, μία 3ης γενιάς και μία WLAN, είναι εκτός της εμβέλειας ενός WLAN, χρησιμοποιεί

τη διεπαφή 3ης γενιάς για πρόσβαση σε υπηρεσίες δεδομένων (όπως περιγράφηκε στην προηγούμενη παράγραφο). Όταν μπαίνει στο πεδίο εμβέλειας του WLAN, πραγματοποιείται μια διαδικασία αναγνώρισης, πιστοποίησης ταυτότητας και δικαιωμάτων του χρήστη, μετά από επικοινωνία με την υποδομή 3ης γενιάς και συγκεκριμένα με τον εξυπηρετητή 3GPP AAA (Authentication, Authorization, Accounting), ο οποίος χρησιμοποιεί τα στοιχεία του συνδρομητή (όπως πληροφορίες πιστοποίησης και προφίλ δικαιωμάτων χρήστη) που βρίσκονται στον εξυπηρετητή HLR/HSS (Home Location Register / Home Subscriber Server). Η διαδικασία αυτή μπορεί να περιλαμβάνει έναν αριθμό ενδιάμεσων εξυπηρετητών 3GPP AAA. Σε περίπτωση πολλαπλών HSS, το συστατικό Subscription Locator Function (SLF) χρησιμεύει στον εντοπισμό από τον εξυπηρετητή 3GPP AAA του κατάλληλου HSS, το οποίο φυλάσσει πληροφορίες για ένα συγκεκριμένο χρήστη.

Σύμφωνα με το σενάριο Α, μετά την πιστοποίηση της ταυτότητας του χρήστη βάσει παραμέτρων της αρχιτεκτονικής 3ης γενιάς, ο εξυπηρετητής AAA μεταφέρει την εντολή και τις κρυπτογραφικές παραμέτρους στον εξυπηρετητή πιστοποίησης του WLAN (Authentication Server – AS), ο οποίος αποτελεί τμήμα του δικτύου πρόσβασης WLAN, ώστε να επιτραπεί πρόσβαση του χρήστη σε υπηρεσίες δεδομένων με την κατάλληλη πολιτική πρόσβασης. Ο χρήστης χρησιμοποιεί πλέον τους υψηλότερους ρυθμούς μετάδοσης δεδομένων του WLAN για πρόσβαση στο Διαδίκτυο ή σε οποιοδήποτε άλλο PDN.

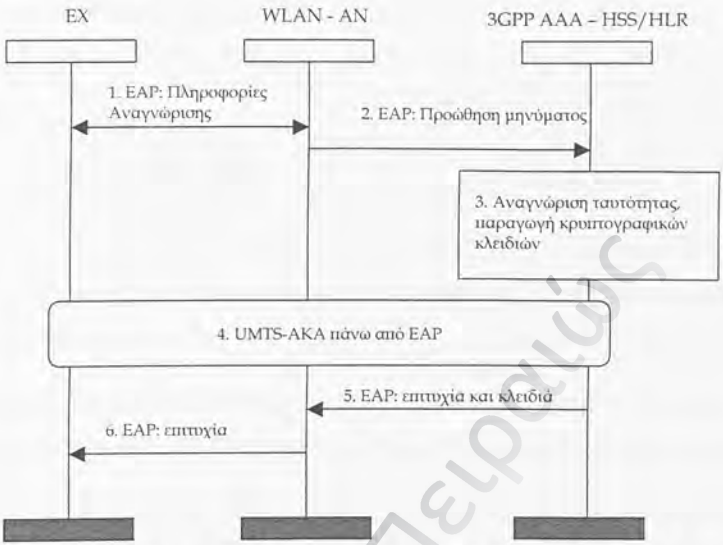
Σύμφωνα με το σενάριο Β, η σύνδεση με ένα εξωτερικό PDN πραγματοποιείται μέσω της πύλης δεδομένων (Packet Data Gateway - PDG) της υποδομής 3ης γενιάς, η οποία συνδέεται με το WLAN μέσω της πύλης WLAN Access Gateway. Πιο συγκεκριμένα, ο εξυπηρετητής 3GPP AAA, αποστέλλει τις κατάλληλες παραμέτρους δρομολόγησης, διευθυνσιοδότησης, πιστοποίησης και εξουσιοδότησης στο PDG (τις οποίες παραλαμβάνει από το HLR/HSS), ώστε να καταστεί δυνατή η ασφαλής από άκρο σε άκρο επικοινωνία με τον εξοπλισμό χρήστη μέσω μιας οδού διέλευσης (tunneling). Η πύλη πρόσβασης ασύρματου τοπικού δικτύου (WLAN Access Gateway – WAG) πραγματοποιεί εκτός των άλλων και φιλτράρισμα πακέτων τα οποία είναι μη κρυπτογραφημένα, εξασφαλίζοντας την ασφαλή προώθηση πακέτων από και προς το κατάλληλο PDG και WLAN AN αντίστοιχα.

Τα συστατικά χρέωσης OCS (Online Charging System) και OffCS (Offline Charging System) παρέχουν υπηρεσίες τιμολόγησης χρηστών.

2.1.3.2 Μηχανισμός ασφάλειας πρόσβασης χρήστη στην υποδομή 4ης γενιάς

Όσον αφορά στα WLAN, τα σημαντικότερα προβλήματα ασφάλειας εμφανίστηκαν με το πρωτόκολλο ασφάλειας Wireless Equivalent Privacy (WEP), το οποίο είχε σημαντικά ευπαθή σημεία στην παραγωγή των τυχαίων αριθμών και των κρυπτογραφικών κλειδιών καθώς επέτρεπε τη σύγκριση κρυπτογραφημένων μηνυμάτων για τμήμα του κλειδιού που ήταν γνωστό, το οποίο οδηγούσε τελικά στην αποκάλυψη της πληροφορίας [67]. Τα νέα πρωτόκολλα ασφάλειας WiFi Protected Access (WPA) και το υπό ανάπτυξη IEEE 802.11i αντιμετωπίζουν τα προβλήματα αυτά, χωρίς βέβαια όμως να στερούνται ευπαθών σημείων [65]. Ενδεικτικά αναφέρεται ότι το σύστημα προστασίας του προ-συμφωνημένου (μεταξύ τερματικού εξοπλισμού χρήστη και κόμβου πρόσβασης) μυστικού κλειδιού (pre shared key - PSK) του WPA το οποίο βασίζεται σε συνθηματικά (passwords) είναι ευαίσθητο σε επιθέσεις βάσει λεξικού (dictionary attacks), ενώ οι επιθέσεις άρνησης εξυπηρέτησης εξακολουθούν να αποτελούν πολύ σημαντική απειλή.

Ο μηχανισμός ασφάλειας πρόσβασης στο δίκτυο 3G/WLAN βασίζεται στο μηχανισμό UMTS-AKA [76]. Η αναγνώριση και πιστοποίηση ταυτότητας χρήστη πραγματοποιείται από την υποδομή 3ης γενιάς, ενώ η υποδομή WLAN έχει το ρόλο διαμεσολαβητή. Πιο συγκεκριμένα, η υποδομή WLAN προωθεί τα μηνύματα του UMTS-AKA μεταξύ της USIM και της υποδομής 3ης γενιάς πάνω από μια μέθοδο του πρωτοκόλλου Extensible Authentication Protocol (EAP), η οποία ονομάζεται EAP Authentication and Key Agreement (EAP-AKA) [79]. Ο μηχανισμός EAP-AKA, περιγράφεται συνοπτικά στη συνέχεια (Σχήμα 7).



Σχήμα 7: Ο μηχανισμός EAP-AKA

1. Αρχικά ο εξοπλισμός χρήστη συνδέεται με το WLAN. Ο εξυπηρετητής πιστοποίησης του WLAN ζητάει πληροφορίες αναγνώρισης από τον εξοπλισμό χρήστη χρησιμοποιώντας το πρωτόκολλο EAP πάνω από τα πρωτόκολλα του WLAN. Ο εξοπλισμός χρήστη αποστέλλει το IMSI κατά τη διάρκεια της πρώτης αλληλεπίδρασης ή σε διαφορετική περίπτωση με κάποιο προσωρινό ψευδώνυμο. Το IMSI ή το ψευδώνυμο είναι ενσωματωμένα σε ένα γενικότερο αναγνωριστικό το οποίο ονομάζεται Network Access Identifier (NAI) η μορφή του οποίου είναι συμβατή με το πρότυπο RFC 2486 [82].

2. Το μήνυμα προωθείται στον εξυπηρετητή 3GPP AAA, ο οποίος μετά από κάποιους εσωτερικούς ελέγχους αναγνωρίζει τον χρήστη και ελέγχει τα δικαιώματα πρόσβασης αυτού στο WLAN.

3. Στη συνέχεια παράγονται νέα κρυπτογραφικά κλειδιά βάσει των CK και IK. Περαιτέρω παράγονται κλειδιά ανάλογα με το εκάστοτε πρωτόκολλο ασφάλειας του WLAN, καθώς και νέες προσωρινές ταυτότητες, οι οποίες αποστέλλονται κρυπτογραφημένες στον εξοπλισμό του χρήστη σε επόμενα στάδια.

4. Στη συνέχεια πραγματοποιείται ο μηχανισμός UMTS-AKA πάνω από το πρωτόκολλο EAP και αποστέλλονται τα RAND και AUTN μέσω της υποδομής WLAN. Ομοίως παράγονται τα RES και XRES και τα αντίστοιχα μηνύματα του UMTS-AKA προωθούνται μέσω της υποδομής WLAN.

5. Αν όλα τα παραπάνω είναι επιτυχή, ο εξυπηρετητής 3GPP AAA στέλνει μήνυμα επιτυχίας στον WLAN-AN καθώς και όποια πρόσθετα κρυπτογραφικά κλειδιά παρήχθησαν για την προστασία της επικοινωνίας στο WLAN.

6. Ενημερώνεται ο εξοπλισμός χρήστη και μπορεί πλέον να διενεργηθεί ασφαλής επικοινωνία μέσω των μυστικών κλειδιών που μοιράζονται πλέον οι δύο οντότητες.

Κατά την εκτέλεση του μηχανισμού EAP-AKA, παράγονται επίσης τα προσωρινά κλειδιά k_encr και k_aut, μήκους 128-bit, με στόχο την προστασία των πακέτων του μηχανισμού.

Τα προβλήματα ασφάλειας μιας αρχιτεκτονικής 3ης γενιάς, λόγω χρήσης του μηχανισμού UMTS-AKA, κληρονομούνται και από τις αρχιτεκτονικές 3G/WLAN (4η γενιά αρχιτεκτονικών) [48]. Όπως και στο μηχανισμό UMTS-AKA, η αλυσίδα ασφάλειας πρόσβασης χρήστη σε επίπεδο δικτύου καταλήγει στην πιστοποίηση της ταυτότητας χρήστη στην τερματική συσκευή, η οποία υλοποιείται με τη χρήση ενός PIN.

2.1.4 Νομικο πλαισιο

Το Προεδρικό Διάταγμα (ΠΔ) 47[13], αφορά στις διαδικασίες και τις τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών, συμπεριλαμβανομένων των κινητών επικοινωνιών φωνής και δεδομένων. Το ΠΔ δημιουργεί έμμεσα την ανάγκη για αξιόπιστη διαχείριση ταυτότητας χρήστη κινητών τηλεπικοινωνιών 3ης γενιάς. Πιο συγκεκριμένα, η ισχυρή πιστοποίηση ταυτότητας γίνεται έμμεσα επιτακτική για την ορθή λειτουργία του κανονισμού, ώστε οι αρχές και τα αρμόδια όργανα να είναι σε θέση να γνωρίζουν με βεβαιότητα την ταυτότητα του συνδρομητή της κινητής συσκευής.

[13] Δημοσιευμένο στο Φύλλο της Εφημερίδος της Κυβέρνησης (ΦΕΚ) 64 της 10ης Μαρτίου 2005 (http://www.et.gr)

ώστε στη συνέχεια να μπορέσουν να αξιοποιήσουν με αποτέλεσμα τα στοιχεία που επιβάλλει το ΠΔ να αποδοθούν από τον φορέα παροχής υπηρεσιών κινητής τηλεφωνίας.

Επιπλέον, το ΦΕΚ 87 της 26ης Ιανουαρίου του 2005, ορίζει κανονισμό τόσο για διασφάλιση του απορρήτου κατά την παροχή κινητών τηλεπικοινωνιακών υπηρεσιών[14], όσο και κατά την παροχή τηλεπικοινωνιακών υπηρεσιών μέσω ασύρματων δικτύων[15] (συμπεριλαμβανομένων των ασύρματων τοπικών δικτύων). Πιο συγκεκριμένα, το ΦΕΚ 87 ορίζει τις υποχρεώσεις των φορέων παροχής τέτοιου είδους υπηρεσιών με στόχο την επίτευξη της ασφαλούς επικοινωνίας και την προστασία προσωπικών δεδομένων, τα οποία αναφέρονται στη συνέχεια:

- Καλών και καλούμενος αριθμός
- Καλών και καλούμενος συνδρομητής – χρήστης
- Χρόνος και διάρκεια επικοινωνίας
- Εντοπισμός καλούντος και καλούμενου χρήστη
- Στοιχεία χρέωσης επικοινωνίας
- Περιεχόμενα και δεδομένα επικοινωνίας
- Ταυτότητας συσκευής και σύνδεσης

Τα δεδομένα αυτά αφορούν άμεσα το μηχανισμό διαχείρισης ταυτότητας χρήστη και ορίζουν ξεκάθαρα τη σημασία διαφύλαξης του απορρήτου της ταυτότητας.

Το ΦΕΚ 88 επίσης, ορίζει κανονισμό για τη διασφάλιση του απορρήτου στις Διαδικτυακές επικοινωνίες. Τα δεδομένα αυτά αφορούν στα συστατικά της υποπεριοχής παροχής υπηρεσιών μεταγωγής πακέτου PS ενός δικτύου 3ης και 4ης γενιάς και μέσω του κανονισμού καθίστανται επιβεβλημένα μέτρα ασφάλειας υπό την ομπρέλα μίας πολιτικής ασφάλειας.

[14] Απόφαση 629α: κανονισμός για τη διασφάλιση του απορρήτου κατά την παροχή κινητών τηλεπικοινωνιακών υπηρεσιών

[15] Απόφαση 631α: κανονισμός για τη διασφάλιση του απορρήτου κατά την παροχή τηλεπικοινωνιακών υπηρεσιών μέσω ασύρματων δικτύων

Επιπλέον, η διαχείριση ταυτότητας χρήστη σε εφαρμογές στο Διαδίκτυο θα πρέπει να διαφυλάσσεται, όπως και οι συναλλαγές που τη συνοδεύουν.

Από τα παραπάνω συνοψίζουμε:

- Υπάρχει ανάγκη ισχυρής πιστοποίησης ταυτότητας χρήστη.
- Ο μηχανισμός ισχυρής πιστοποίησης πρέπει να διαφυλάσσει το απόρρητο της ταυτότητας.
- Τα προσωπικά δεδομένα του χρήστη συμπεριλαμβανομένης της ταυτότητας αυτού και των συναλλαγών του θα πρέπει να παραμένουν απόρρητα σε εφαρμογές στο Διαδίκτυο (και πάνω από δίκτυα 3ης και 4ης γενιάς).
- Υπάρχει ανάγκη επαρκών μέτρων ασφάλειας στην υποπεριοχή παροχής υπηρεσιών μεταγωγής πακέτου PS ενός δικτύου 3ης και 4ης γενιάς.

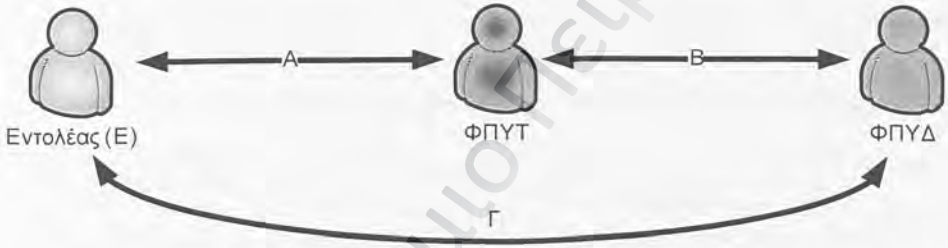
2.2 Πρωτοκολλα διαχειρισης ταυτοτητας για υπηρεσιες στο Διαδικτυο

2.2.1 Εισαγωγη

Η ανάγκη για τη διαχείριση ταυτότητας χρηστών σε υπηρεσίες που παρέχονται στο Διαδίκτυο, όπως για παράδειγμα υπηρεσίες ηλεκτρονικού εμπορίου, ηλεκτρονικής υγείας ή διακυβέρνησης, οδήγησε στη δημιουργία εξειδικευμένων πρωτοκόλλων, όπως το Microsoft .Net Passport, καθώς και οι συστάσεις-πρωτόκολλα του Liberty Alliance. Οι συστάσεις του Liberty Alliance, επεκτείνουν τη γλώσσα OASIS's Security Assertions Markup Language (SAML), η οποία βασίζεται στην Extensible Markup Language (XML) και αφορά στην ανταλλαγή πληροφοριών πιστοποίησης. Λιγότερο διαδεδομένα πρωτόκολλα και παρόμοια του Liberty Alliance που βασίζονται στην SAML είναι τα πρωτόκολλα του ερευνητικού έργου Shibboleth [100], για τη διαχείριση ταυτότητας μεταξύ πανεπιστημιακών ιδρυμάτων, καθώς και ένα σχετικά γενικό πρωτόκολλο με την ονομασία BBAE [101].

Οι κυριάρχες υπάρχουσες λύσεις (Microsoft .Net Passport και συστάσεις-πρωτόκολλα του Liberty Alliance) ορίζουν μία έμπιστη τρίτη οντότητα μεταξύ του χρήστη και του φορέα παροχής υπηρεσιών στο διαδίκτυο, η οποία λειτουργεί ως διαμεσολαβητής στην πιστοποίηση της ταυτότητας του χρήστη, ο οποίος ονομάζεται Φορέας Παροχής Υπηρεσιών Ταυτότητας – ΦΠΥΤ. Ταυτόχρονα, ο χρήστης αποφεύγει χρονοβόρες διαδικασίες πιστοποίησης ταυτότητας σε διαφορετικούς Φορείς Παροχής Υπηρεσιών στο Διαδίκτυο (ΦΠΥΔ), εκτελώντας τη διαδικασία μόνο μία φορά στον ΦΠΥΤ, ο οποίος στη συνέχεια αναλαμβάνει να αποστείλει τα κατάλληλα τεκμήρια πιστοποίησης ταυτότητας στον κατάλληλο ΦΠΥΔ.

Τα πρωτόκολλα του Liberty Alliance [90], καθώς και το Microsoft .Net Passport [95], βασίζονται σε μία κοινή αρχιτεκτονική, η οποία παρουσιάζεται στο Σχήμα 8.



Σχήμα 8: Λογική πρωτοκόλλων Liberty Alliance και Microsoft .Net Passport

Σύμφωνα με την αρχιτεκτονική αυτή, ορίζονται τρεις οντότητες: ο εντολέας (Ε), ο ΦΠΥΤ και ο ΦΠΥΔ.. Μεταξύ των οντοτήτων διακρίνονται οι παρακάτω σχέσεις:

Α. Ο Ε πιστοποιεί την ταυτότητά του στον ΦΠΥΤ, ώστε να καταστεί δυνατή η έκδοση πειστηρίων ταυτότητας από τον ΦΠΥΤ.

Β. Ο ΦΠΥΤ και ο ΦΠΥΔ έχουν κάποια συμφωνία αμοιβαίας εμπιστοσύνης καθώς και κάποια κοινή αντίληψη για τον Ε.

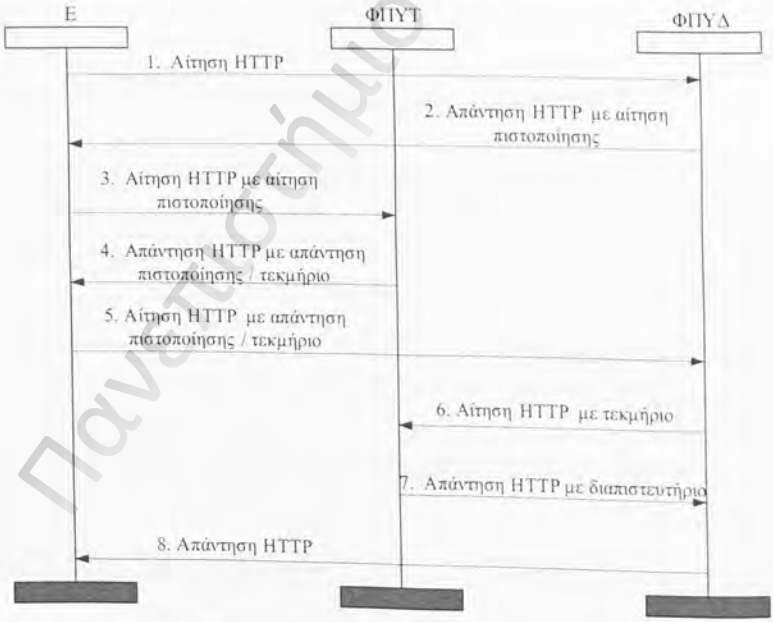
Γ. Ο ΦΠΥΔ παρέχει υπηρεσίες στον Ε. Για να του παράσχει τις υπηρεσίες αυτές, ο ΦΠΥΔ ζητά πειστήρια ταυτότητας που έχουν εκδοθεί από τον ΦΠΥΤ.

Έτσι αφού ο Ε πιστοποιεί μόνο μία φορά την ταυτότητά του στον ΦΠΥΤ, όταν θελήσει να έχει πρόσβαση στις υπηρεσίες του ΦΠΥΔ, ο ΦΠΥΔ ζητά τα πειστήρια. Ο Ε ζητά τα πειστήρια από τον ΦΠΥΤ, ο οποίος του τα παρέχει, αφού η ταυτότητά του είναι ήδη πιστοποιημένη. Ο Ε προωθεί τα πειστήρια στον ΦΠΥΔ, ο οποίος τα επεξεργάζεται και ανάλογα εξουσιοδοτεί τον Ε για χρήση των υπηρεσιών του.

Στις επόμενες παραγράφους, παρουσιάζονται περιληπτικά τα κυριαρχα πρωτόκολλα διαχείρισης ταυτότητας, αυτά του Liberty Alliance και το πρωτόκολλο Microsoft .Net Passport.

2.2.2 Συστασεις Liberty Alliance

Τα πρωτόκολλα του Liberty Alliance υλοποιούν διαχείριση ταυτότητας με μοναδική πιστοποίηση ταυτότητας χρήστη σε πολλαπλές εφαρμογές (single sign-on). Στο Σχήμα 9 παρουσιάζεται η επικοινωνία μεταξύ των τριών οντοτήτων (Ε, ΦΠΥΤ, ΦΠΥΔ) σε μια μορφή η οποία είναι κοινή για όλα τα πρωτόκολλα του Liberty Alliance [89,94].



Σχήμα 9: Λειτουργία των πρωτοκόλλων διαχείρισης ταυτότητας του Liberty Alliance

Τα πρωτόκολλα του Liberty Alliance λαμβάνουν ως δεδομένο ότι ο Ε έχει πιστοποιήσει ήδη την ταυτότητα του στον ΦΠΥΤ καθώς και την ύπαρξη μιας σχέσης εμπιστοσύνης μεταξύ των ΦΠΥΔ και ΦΠΥΤ.

Τα βήματα των πρωτοκόλλων του Liberty Alliance περιγράφονται στη συνέχεια:

1. Αρχικά ο Ε αποστέλλει μια αίτηση πρόσβασης στον ΦΠΥΔ.
2. Ο ΦΠΥΔ απαντά στην αίτηση, ζητώντας από τον Ε να πιστοποιήσει την ταυτότητά του.
3. Ο Ε δεν πιστοποιεί ξανά την ταυτότητά του (αυτό έχει ήδη γίνει στον ΦΠΥΤ). Ο Ε αποστέλλει μια αίτηση πιστοποίησης στον ΦΠΥΤ.
4. Ο ΦΠΥΤ επεξεργάζεται την αίτηση και αποστέλλει μία απάντηση πιστοποίησης η οποία περιέχει κάποιας μορφής τεκμήριο.
5. Το τεκμήριο προωθείται στον ΦΠΥΔ.
6. Το τεκμήριο αποστέλλεται από τον ΦΠΥΔ στον ΦΠΥΤ.
7. Ο ΦΠΥΤ επεξεργάζεται το τεκμήριο και αποστέλλει ανάλογα ένα διαπιστευτήριο για την ταυτότητα του Ε στον ΦΠΥΔ.
8. Ο ΦΠΥΔ στέλνει μια απάντηση στον Ε τερματίζοντας τη διαδικασία.

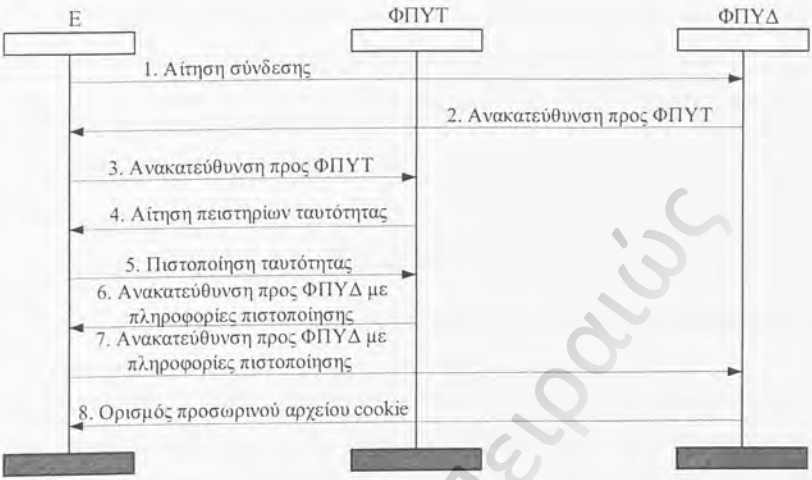
Τα παραπάνω μηνύματα αποτελούν τη βάση για τα πρωτόκολλα του Liberty Alliance, τα οποία τα υιοθετούν μερικώς η πλήρως. Παρακάτω αναφέρονται τα διάφορα είδη πρωτοκόλλων διαχείρισης ταυτότητας χρήστη [89]:

- Πρωτόκολλο Liberty με τεκμήριο (Liberty artifact profile for single sign-on): Το πρωτόκολλο αυτό χρησιμοποιεί όλα τα μηνύματα που αναφέρθηκαν παραπάνω υιοθετώντας τη λογική τεκμηρίου/ διαπιστευτηρίου.
- Πρωτόκολλο Liberty φυλλομετρητή με χρήση POST (Liberty browser POST profile for single sign-on): Το πρωτόκολλο αυτό επιτρέπει τη διακίνηση πληροφορίας πιστοποίησης ταυτότητας χρήστη, χωρίς τη χρήση τεκμηρίου που αποστέλλεται από τον ΦΠΥΔ στον ΦΠΥΤ. Τα μηνύματα 6 και 7 που περιγράφηκαν παραπάνω δεν χρησιμοποιούνται. Το διαπιστευτήριο αποστέλλεται στον Ε από τον ΦΠΥΤ στο μήνυμα 4 απ' ευθείας και προωθείται στον ΦΠΥΤ από τον Ε στο μήνυμα 5.

- Πρωτόκολλο Liberty με ενεργοποιημένο πελάτη κατά Liberty (Liberty-enabled client and proxy profile for single sign-on – χωρίς χρήση ενδιάμεσου εξυπηρετητή proxy). Το πρωτόκολλο αυτό, όμοια με το προηγούμενο, δεν χρησιμοποιεί τα μηνύματα 6 και 7. Επιπλέον, ο πελάτης (client) του Ε, έχει γνώση σχετικά με την ταυτότητα του ΦΠΥΤ που θα χρησιμοποιηθεί με κάθε ΦΠΥΔ (καθώς οι ΦΠΥΤ μπορεί να είναι πολλαπλοί), ή έχει τη δυνατότητα να αποκτήσει τη γνώση αυτή εκτός πρωτοκόλλου.
- Πρωτόκολλο Liberty με Liberty-ενεργοποιημένο πελάτη (Liberty-enabled client and proxy profile for single sign-on) με χρήση ενδιάμεσου εξυπηρετητή (proxy). Το πρωτόκολλο αυτό είναι όμοιο με το προηγούμενο με τη διαφορά ότι τις λειτουργίες του πρωτοκόλλου αναλαμβάνει να εκτελέσει αντί του πελάτη του Ε ένας ενδιάμεσος εξυπηρετητής proxy. Αυτό υλοποιείται για λόγους απόδοσης κυρίως σε περιβάλλοντα ασύρματης επικοινωνίας, με στόχο τη μείωση της πληροφορίας που διακινείται πάνω από το ασύρματο μέσο.

2.2.3 Microsoft .Net Passport

Το Microsoft .Net Passport [95] αποτελεί ένα σύνολο υπηρεσιών που υλοποιούν διαχείριση ταυτότητας με μοναδική πιστοποίηση ταυτότητας χρήστη σε πολλαπλές εφαρμογές (single sign-on), όπως και τα πρωτόκολλα του Liberty Alliance. Αυτό επιτυγχάνεται με τη δημιουργία ενός συνόλου διαπιστευτηρίων τα οποία μπορούν να πιστοποιήσουν την ταυτότητα του χρήστη σε οποιονδήποτε ΦΠΥΔ υποστηρίζει το Microsoft .Net Passport. Το Microsoft .Net Passport αρχικά απαιτεί την εγγραφή του χρήστη στο σύστημα. Στη συνέχεια η διαδικασία διαχείρισης ταυτότητας χρήστη γίνεται σύμφωνα με το Σχήμα 10.



Σχήμα 10: Το Microsoft .Net Passport

Τα μηνύματα του Microsoft .Net Passport είναι τα ακόλουθα:

1. Αρχικά ο Ε προσπαθεί να συνδεθεί σε μια περιοχή του ΦΠΥΔ, η οποία απαιτεί πιστοποίηση ταυτότητας
2. Ο ΦΠΥΔ αποστέλλει μήνυμα ανακατεύθυνσης του Ε στον ΦΠΥΤ.
3. Ο Ε ανακατευθύνεται στον ΦΠΥΤ.
4. Ο ΦΠΥΤ ζητά από τον Ε να πιστοποιήσει την ταυτότητά του, χρησιμοποιώντας ένα συνθηματικό.
5. Ο Ε πιστοποιεί την ταυτότητά του (αναγνωριστικό και συνθηματικό).
6. Ο ΦΠΥΤ αποστέλλει μήνυμα ανακατεύθυνσης του Ε στον ΦΠΥΤ στο οποίο επισυνάπτει πληροφορίες πιστοποίησης ταυτότητας του Ε, κρυπτογραφημένες με τον αλγόριθμο 3DES, του οποίου το συμμετρικό κλειδί έχουν ανταλλάξει προηγούμενα οι ΦΠΥΤ και ΦΠΥΔ.
7. Ο Ε ανακατευθύνεται στον ΦΠΥΔ, αποστέλλοντας τις κρυπτογραφημένες πληροφορίες πιστοποίησης ταυτότητας.

8. Ο ΦΠΥΔ ορίζει ένα προσωρινό αρχείο cookie στον φυλλομετρητή του Ε, το οποίο είναι και αυτό κρυπτογραφημένο.

Όταν ο χρήστης επιστρέψει μελλοντικά στον ΦΠΥΔ και το προσωρινό αρχείο cookie είναι ακόμη ενεργό η διαδικασία δεν χρειάζεται να επαναληφθεί, αλλά απλά αποστέλλεται στον ΦΠΥΔ το κρυπτογραφημένο προσωρινό αρχείο cookie.

Αντίστοιχα, ο ΦΠΥΤ θέτει ένα προσωρινό αρχείο cookie στον φυλλομετρητή του Ε, έτσι ώστε όταν ο Ε επισκεφθεί κάποιον άλλο ΦΠΥΔ, τα βήματα 4 και 5 να μην επαναληφθούν και να υλοποιηθεί μοναδική πιστοποίηση ταυτότητας χρήστη σε πολλαπλές εφαρμογές.

2.2.4 ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΑΝΟΙΚΤΑ ΠΡΟΒΛΗΜΑΤΑ

Εκτός από τις συστάσεις του Liberty Alliance, έχουν παρουσιαστεί πολλές μελέτες στο χώρο της ασφάλειας και της προστασίας προσωπικών δεδομένων κατά τη λειτουργία των πρωτοκόλλων. Ο Pfitzmann [103] τονίζει τη σημασία της προστασίας του ιδιωτικού απορρήτου κατά τη λειτουργία των πρωτοκόλλων που βασίζονται σε φυλλομετρητή, συμπεριλαμβανομένων των αντίστοιχων πρωτοκόλλων του Liberty Alliance και του Microsoft .Net Passport. Ο Damiani [84], παρουσιάζει τα αποτελέσματα του έργου RAPID (the Roadmap for Advanced Research in Privacy and Identity management). Στην εργασία αυτή τονίζεται η σημασία της ασφάλειας και της προστασίας των ιδιωτικών δεδομένων των χρηστών. Ως βασική απαίτηση ενός μηχανισμού διαχείρισης ταυτότητας χρήστη, πέρα από την ασφάλεια και την προστασία της ιδιωτικότητας, ορίζεται το μειωμένο φορτίο λειτουργίας του μηχανισμού σε κινητά περιβάλλοντα, κάτι το οποίο υπογραμμίζεται και από τον Buell [112]. Ο Damiani στην εργασία του παρουσιάζει επίσης τις δύο κυρίαρχες λύσεις - Microsoft .NET Passport και τις συστάσεις του Liberty Alliance - καθώς και λύσεις που βασίζονται σε Υποδομή Δημοσίου Κλειδιού επισημαίνοντας την πολυπλοκότητα και το υψηλό φορτίο των τελευταίων ως βασικά μειονεκτήματα που δεν τις καθιστούν ανταγωνιστικές των πρώτων, κυρίως σε κινητά περιβάλλοντα. Ο Mont [86] αναφέρει τις προδιαγραφές του W3C για τον ορισμό πολιτικών προστασίας της ιδιωτικότητας του χρήστη και προτείνει ένα μοντέλο επιβολής τέτοιων πολιτικών σε μηχανισμούς διαχείρισης ταυτότητας. Το μοντέλο χρησιμοποιεί έμπιστες τρίτες οντότητες για τη διαχείριση της

πρόσβασης σε ευαίσθητη πληροφορία. Η Siemens [87] περιγράφει τις ιδιαιτερότητες των κινητών εφαρμογών και τονίζει την ανάγκη ανάληψης του ρόλου του ΦΠΥΤ από τον φορέα παροχής υπηρεσιών 3ης γενιάς.

Οι συστάσεις του Liberty Alliance, αλλά και οι σχετικές μελέτες της ερευνητικής κοινότητας, ορίζουν ένα σύνολο βασικών απαιτήσεων για τα πρωτόκολλα διαχείρισης ταυτότητας οι οποίες συνοψίζονται στη συνέχεια:

- Διαφανές στο χρήστη.
- Να υποστηρίζει πολλαπλές ταυτότητες για κάθε χρήστη.
- Να είναι ελαφρύ.
- Να προστατεύει τα προσωπικά δεδομένα του χρήστη.
- Να είναι διαλειτουργικό.
- Να είναι ασφαλές.
- Να υλοποιεί επαρκώς ισχυρή πιστοποίηση ταυτότητας χρήστη.
- Να συνδέει ασφαλώς τις έννοιες της αναγνώρισης, της πιστοποίησης και της εξουσιοδότησης.

Παρόλα αυτά ο συνδυασμός όμως όλων των παραπάνω στην πράξη αποδεικνύεται δύσκολος, με κυρίαρχους τομείς προβλημάτων τον τομέα της ασφάλειας και τον τομέα της απόδοσης. Οι τομείς αυτοί είναι νευραλγικοί ιδιαίτερα σε ένα περιβάλλον 3ης και 4ης γενιάς, καθώς το ασύρματο μέσο επικοινωνίας απαιτεί αφενός αυξημένα επίπεδα ασφάλειας λόγω της εκπομπής του σήματος σε ένα κοινό μέσο και αφετέρου προσεκτική σχεδίαση όσο αφορά στην απόδοση, ώστε να μην επιβαρύνεται κυρίως η ευαίσθητη (σε λάθη) ζεύξη του τερματικού εξοπλισμού του χρήστη με την κεραία του φορέα παροχής υπηρεσιών τηλεπικοινωνίας [68].

Προβλήματα ασφάλειας έχουν αναφερθεί κατά καιρούς τόσο για τα πρωτόκολλα του Liberty Alliance όσο και για το Microsoft .NET passport. Ο Groß [99] παρουσιάζει ευπαθή σημεία για πρωτόκολλα που βασίζονται στο προφίλ SAML φυλλομετρητή / τεκμηρίου – όπως τα αντίστοιχα πρωτόκολλα του Liberty Alliance. Τα ευπαθή αυτά σημεία επιτρέπουν επιθέσεις επανεκπομπής, ενδιάμεσης οντότητας και πρωτοκόλλου HTTP. Για τα ευπαθή

σημεία προτείνονται πιθανές λύσεις, οι οποίες όμως δεν εξετάζονται για το πόσο επιβαρύνουν την απόδοση του πρωτοκόλλου, όπως για παράδειγμα η μονομερής πιστοποίηση ταυτότητας μιας οντότητας σε όλα τα στάδια του πρωτοκόλλου. Αντίστοιχες επιθέσεις, χωρίς μελέτη επιβάρυνσης της απόδοσης από τα προτεινόμενα αντίμετρα, περιγράφονται από τον Pfitzmann [98], για τα πρωτόκολλα Liberty με ενεργοποιημένο πελάτη κατά Liberty. Πιο συγκεκριμένα, η εργασία εκτός από την αναφορά κάποιων γενικών σημείων ασφάλειας για σχετικά πρωτόκολλα επικεντρώνεται σε επιθέσεις ενδιάμεσης οντότητας και προτείνει αντίμετρα.

Σημαντικά προβλήματα ασφάλειας έχουν επίσης δημοσιευθεί και για το Microsoft .Net Passport. Ο Kormann [96], περιγράφει προβλήματα που αφορούν στο γραφικό περιβάλλον διεπαφής του χρήστη, όπου η διαδικασία αποσύνδεσης του χρήστη, η οποία αφαιρεί τα προσωρινά αρχεία cookies, τα οποία εμπεριέχουν πληροφορίες πιστοποίησης ταυτότητας, δεν είναι ιδιαίτερα σαφής για το μέσο χρήστη και παρουσιάζει και κάποια προβλήματα ασυμβατότητας με φυλλομετρητές που δεν ανήκουν στη Microsoft. Άλλα προβλήματα, τα οποία αναφέρονται από τον Obliger [97], αφορούν στη διαχείριση κρυπτογραφικών κλειδιών που χρησιμεύουν για την κρυπτογράφηση των πληροφοριών πιστοποίησης ταυτότητας, καθώς και προβλήματα άρνησης εξυπηρέτησης στον εξυπηρετητή του ΦΠΥΤ. Ο Slemko [113] σε παλιότερη εργασία επισημαίνει αντίστοιχα προβλήματα και επιθέσεις.

Οι συνδρομητές υπηρεσιών 3ης και 4ης γενιάς, οι οποίοι θέλουν πραγματοποιήσουν αμοιβαία πιστοποίηση ταυτότητας με φορείς παροχής ηλεκτρονικών υπηρεσιών στο διαδίκτυο, μπορούν να χρησιμοποιήσουν τις υπάρχουσες λύσεις διαχείρισης ταυτότητας, με την εγγραφή τους σε μία έμπιστη τρίτη οντότητα παροχής υπηρεσιών ταυτότητας. Παρόλα αυτά, κατά την προσέγγιση αυτή δεν λαμβάνεται υπόψη η σχέση εμπιστοσύνης του συνδρομητή υπηρεσιών 3ης και 4ης γενιάς με τον φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς, η οποία είναι ήδη εδραιωμένη. Αυτό έχει ως αποτέλεσμα:

- τη μείωση της απόδοσης του όλου μηχανισμού, καθώς εισέρχεται μία ακόμη οντότητα εκτός του χρήστη, του φορέα παροχής υπηρεσιών 4ης γενιάς και του φορεα παροχής υπηρεσιών στο διαδίκτυο, με τις ανάλογες απαιτήσεις σε δικτυακό φορτίο,

- τις μη προσαρμοσμένες απαιτήσεις σε επεξεργαστική ισχύ στις προδιαγραφές του κινητού τερματικού εξοπλισμού του χρήστη, ο οποίος έχει περιορισμένες δυνατότητες επεξεργασίας και μνήμης και οι δυνατότητες του οποίου είναι αντιστρόφως ανάλογες των αποθεμάτων ενέργειας αυτού,
- τη δημιουργία ερωτημάτων σε θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων του χρήστη, καθώς οι υπάρχουσες λύσεις παρουσιάζουν προβλήματα τα οποία μπορεί να πολλαπλασιαστούν με την εφαρμογή τους στο ευαίσθητο περιβάλλον των δικτύων 3ης γενιάς και 4ης γενιάς.

Από τα παραπάνω συμπεραίνουμε ότι υπάρχει ανάγκη δημιουργίας ενός πρωτοκόλλου προσαρμοσμένου πλήρως στις ανάγκες ενός περιβάλλοντος 3ης γενιάς και 4ης γενιάς, το οποίο να ικανοποιεί τις απαιτήσεις διαχείρισης ταυτότητας που αναφέρθηκαν και κυρίως να συνδυάζει την ασφάλεια με την απόδοση.

2.3 Βιομετρικά Συστηματα

2.3.1 Βασικες αρχες λειτουργιας

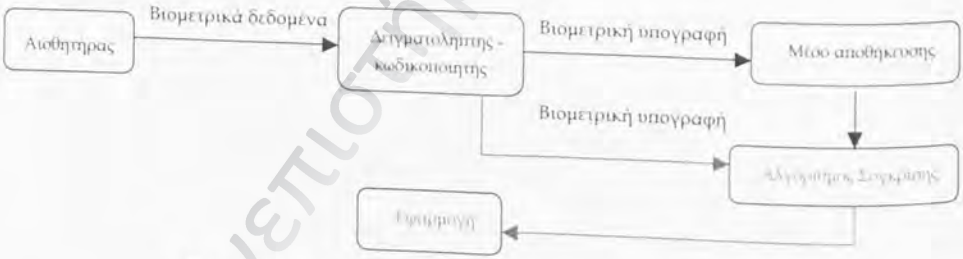
Τα συμβατικά συστήματα πιστοποίησης της ταυτότητας του χρήστη σε ηλεκτρονικές εφαρμογές είναι συνήθως ενός ή το πολύ δύο κριτηρίων. Τα κριτήρια αυτά είναι η απόδειξη μέσω γνώσης (π.χ. κωδικού) και η απόδειξη μέσω κατοχής ενός τεκμηρίου (όπως μαγνητικής ή έξυπνης κάρτας). Τα συστήματα δύο κριτηρίων έχουν αδυναμίες που οφείλονται στο γεγονός ότι τόσο η γνώση, όσο και η κατοχή τεκμηρίων δεν χαρακτηρίζουν μοναδικά το χρήστη. Την απάντηση στο παραπάνω πρόβλημα φιλοδοξούν να δώσουν τα βιομετρικά συστήματα, εισάγοντας το τρίτο κριτήριο στη διαδικασία, δηλαδή την απόδειξη μέσω ανθρώπινου χαρακτηριστικού.

Τα βιομετρικά συστήματα ορίζονται ως *συστήματα αναγνώρισης ή πιστοποίησης ταυτότητας ατόμου μέσω της αυτοματοποιημένης μέτρησης χαρακτηριστικών της φυσιολογίας ή της συμπεριφοράς του* [147]. Η φυσιολογία του ανθρώπου αφορά σε δακτυλικά αποτυπώματα, φωνή, χαρακτηριστικά προσώπου, ίριδας ή αμφιβληστροειδούς ματιού, σχήματος παλάμης, ενώ τα χαρακτηριστικά ανθρώπινης συμπεριφοράς, αφορούν στον τρόπο υπογραφής, ομιλίας,

κίνησης των χειλιών, πληκτρολόγησης, κίνησης του ποντικού του υπολογιστή. Τα βιομετρικά συστήματα είναι συστήματα στατιστικής μέτρησης των ανθρωπίνων χαρακτηριστικών, τα οποία βασίζονται στο γεγονός ότι είναι μοναδικά για κάθε άνθρωπο. Ανάλογα με τις ανάγκες της εκάστοτε εφαρμογής, τα βιομετρικά συστήματα χρησιμοποιούνται για:

- την **αναγνώριση** της ταυτότητας του χρήστη, όπου πραγματοποιείται σύγκριση του χαρακτηριστικού του χρήστη με ένα πλήθος προ-αποθηκευμένων χαρακτηριστικών διαφορετικών χρηστών, με στόχο την ταυτοποίηση ή μη με κάποιο από αυτά. Η αναγνώριση διακρίνεται σε:
  - **θετική**, όταν αντικείμενο είναι η αναζήτηση της ταυτότητας ενός χρήστη, και
  - **αρνητική**, όταν αντικείμενο είναι η διασφάλιση ότι ο χρήστης δεν ανήκει σε ένα σύνολο χρηστών (όπως για παράδειγμα σε ένα σύνολο τρομοκρατών).
- την **πιστοποίηση** της ταυτότητας του χρήστη όπου πραγματοποιείται σύγκριση ενός χαρακτηριστικού με ένα προ-αποθηκευμένο χαρακτηριστικό του χρήστη, με δήλωση της ταυτότητας του χρήστη και πιστοποίηση αυτής.

Τα παραπάνω γίνονται πιο συγκεκριμένα με την περιγραφή ενός τυπικού και απλοποιημένου μοντέλου βιομετρικού συστήματος, όπως αυτό που παρουσιάζεται στο Σχήμα 11.



Σχήμα 11: Τυπικό μοντέλο βιομετρικού συστήματος

Ο χρήστης αρχικά εγγράφεται στο σύστημα, μέσα από μια διαδικασία δειγματοληψίας των χαρακτηριστικών του. Ο αισθητήρας αποτυπώνει τα χαρακτηριστικά του χρήστη (μπορεί για παράδειγμα να είναι μία κάμερα ή ένας οπτικός ή επαγωγικός αισθητήρας δακτυλικών αποτυπωμάτων). Τα βιομετρικά δεδομένα σε αυτό το στάδιο, πριν δηλαδή

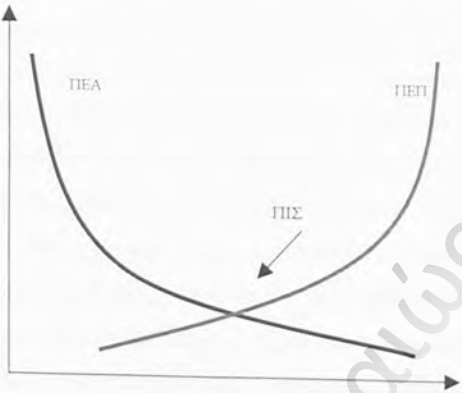
επεξεργαστούν από κάποιο συστατικό του συστήματος, ορίζονται ως *πρωτογενή βιομετρικά δεδομένα (raw biometric data)* [147].

Ο δειγματολήπτης-κωδικοποιητής εξάγει τα ζητούμενα (ανάλογα με τον αλγόριθμο) στοιχεία των χαρακτηριστικών και τα κωδικοποιεί με μία μονόδρομη συνάρτηση. Το αποτέλεσμα αυτής της συνάρτησης, ορίζεται ως *βιομετρική υπογραφή (biometric template)* [147]. Επισημαίνεται, ότι η βιομετρική υπογραφή διακρίνεται από τα πρωτογενή βιομετρικά δεδομένα και δεν αποτελεί το αυτό καθεαυτό χαρακτηριστικό του χρήστη. Δεν είναι για παράδειγμα μία εικόνα του δακτυλικού του αποτυπώματος ή του προσώπου του, αλλά μία κωδικοποιημένη μορφή της δειγματοληψίας αυτών, που υλοποιείται με μία συνάρτηση που δεν επιτρέπει την αναδημιουργία του χαρακτηριστικού από αυτή. Η βιομετρική υπογραφή, αποθηκεύεται σε κάποιο μέσο αποθήκευσης (για παράδειγμα σε μια βάση δεδομένων ή σε μια έξυπνη κάρτα).

Για να αναγνωριστεί ή να πιστοποιηθεί η ταυτότητα του χρήστη συλλέγονται τα χαρακτηριστικά του από έναν αισθητήρα, δημιουργείται η κωδικοποιημένη μορφή τους και συγκρίνεται με αυτή που έχει αποθηκευθεί. Ο αλγόριθμος σύγκρισης εξάγει το ποσοστιαίο αποτέλεσμα της σύγκρισης. Η απόφαση για το αν η πιστοποίηση ταυτότητας είναι επιτυχής ή όχι είναι ευθύνη του συστήματος ή της εφαρμογής (ανάλογα με την υλοποίηση). Για παράδειγμα ένα ποσοστό ομοιότητας 70% μπορεί να είναι αποδεκτό αποτέλεσμα για μία εφαρμογή που στοχεύει στη διευκόλυνση κάποιας διαδικασίας, αλλά μη αποδεκτό για μια εφαρμογή που υλοποιεί την ασφάλεια σε ένα σύστημα.

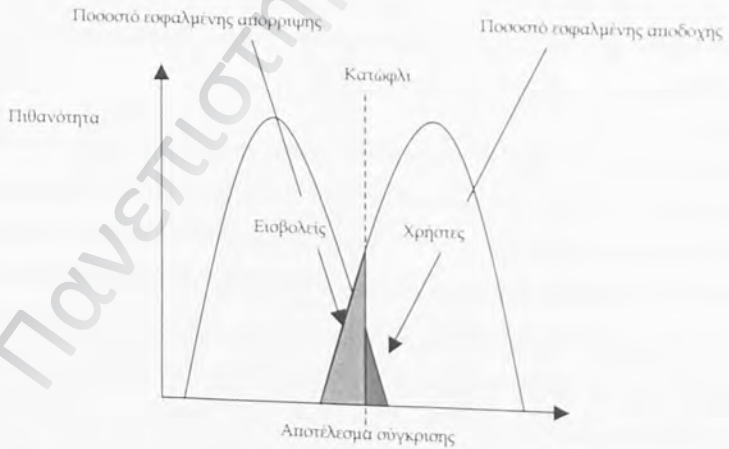
Τα βιομετρικά συστήματα παραμετροποιούνται ανάλογα με τις ειδικές απαιτήσεις της εκάστοτε εφαρμογής. Για το σκοπό αυτό μάλιστα αναπτύχθηκε από τον Ashbourn ειδική γλώσσα προδιαγραφής απαιτήσεων, η οποία ονομάστηκε BANTAM [137]. Δύο βασικές παράμετροι, είναι το Ποσοστό Εσφαλμένης Παραδοχής (False Acceptance Rate) και το Ποσοστό Εσφαλμένης Απόρριψης (False Rejection Rate), ενώ το σημείο τομής τους ονομάζεται Ποσοστό Ίσου Σφάλματος (ΠΙΣ - Equal Error Rate) [141]. Το Ποσοστό Εσφαλμένης Παραδοχής (ΠΕΠ) είναι η πιθανότητα λανθασμένης έγκρισης ενός μη εξουσιοδοτημένου χρήστη. Το Ποσοστό Εσφαλμένης Απόρριψης (ΠΕΑ) είναι η πιθανότητα

απόρριψης ενός εξουσιοδοτημένου χρήστη. Το Σχήμα 12 παρουσιάζει την κατανομή των παραμέτρων αυτών, δηλώνοντας τη μεταξύ τους σχέση.



Σχήμα 12: Καμπύλες Ποσοστών Εσφαλμένης Παραδοχής και Εσφαλμένης Απόρριψης [141]

Οι κατανομές είναι εκθετικές. Όσο αυξάνει το ΠΕΑ, τόσο μειώνεται το ΠΕΠ και αντίστροφα. Η επιλογή του σημείου λειτουργίας ή αλλιώς του κατωφλίου φαίνεται στο Σχήμα 13.



Σχήμα 13: Παραμετροποίηση βιομετρικού συστήματος [141]

Στο Σχήμα 13 παρουσιάζεται επίσης ότι για δεδομένο σύστημα, όσο μειώνεται το ΠΕΠ τόσο πιο αυστηρό γίνεται το σύστημα και τόσο αυξάνει το ΠΕΑ και το αντίστροφο. Μεγάλο ΠΕΠ για δεδομένο σύστημα σημαίνει υψηλότερο επίπεδο ασφάλειας, αλλά και περισσότερους δυσαρεστημένους χρήστες που πιθανώς απορρίπτονται λανθασμένα από το σύστημα [139].

2.3.2 Εφαρμογες

Τα βιομετρικά υλοποιούνται είτε ως μηχανισμοί ασφάλειας είτε ως μηχανισμοί διευκόλυνσης [131]. Στη δεύτερη περίπτωση τα πράγματα είναι σχετικά απλά – τα βιομετρικά αντικαθιστούν πλήρως κωδικούς και ο χρήστης δεν χρειάζεται να τους απομνημονεύει. Οι απαιτήσεις είναι μικρές και επιλέγεται το υψηλό ΠΕΠ χωρίς ιδιαίτερες ανησυχίες υλοποιώντας ένα φιλικό σύστημα.

Στο χώρο της ασφάλειας τα βιομετρικά συστήματα απευθύνονται σε εφαρμογές που απαιτούν υψηλά επίπεδα ασφάλειας, τα οποία είναι αποτελεσματικά και πειστικά για τους χρήστες που δεν εμπιστεύονται αυτοματοποιημένες διαδικασίες με το φόβο κάποιου περιστατικού ασφάλειας. Τέτοιες εφαρμογές είναι ενδεικτικά οι ακόλουθες:

- Εμπορικές Εφαρμογές, όπως ηλεκτρονικό εμπόριο, συναλλαγές με τράπεζες (από μηχανήματα ανάληψης μετρητών, από απομακρυσμένες εφαρμογές ηλεκτρονικής τράπεζας και πιστωτικές κάρτες), φυσική πρόσβαση σε ευαίσθητους χώρους και λογική πρόσβαση σε φορείς παροχής υπηρεσιών διαδικτύου.
- Εφαρμογές διακυβέρνησης, όπως πιστοποίηση ταυτότητας, πιστοποίηση άδειας οδήγησης, πρόσβαση σε ασφαλιστικά δεδομένα, εφαρμογές κοινωνικής πρόνοιας, αλληλεπίδραση με δημόσιους φορείς (έκδοση πιστοποιητικών, φορολογικές εφαρμογές), φυσική πρόσβαση σε ευαίσθητους χώρους, συνοριακός έλεγχος, πιστοποίηση διαβατηρίων, έλεγχος μεταναστών, αναγνώριση τρομοκρατών – εγκληματιών, ηλεκτρονική δημοκρατία – εκλογές και αναγνώριση χαμένων παιδιών
- Στρατιωτικές εφαρμογές

- Εφαρμογές υγείας, όπως πρόσβαση σε ιατρικά δεδομένα, άμεση αναγνώριση ασθενούς σε περίπτωση αναισθησίας από ατύχημα, πιστοποίηση ταυτότητας για την προμήθεια φαρμάκων και πιστοποίηση ταυτότητας για εφαρμογές τηλε-ιατρικής
- Προσωπικές εφαρμογές, όπως λογική πρόσβαση σε προσωπικούς υπολογιστές, λογική πρόσβαση σε κινητά τηλέφωνα, φυσική πρόσβαση σε ιδιωτικούς χώρους και αυτοκίνητα και φυσική πρόσβαση σε χρηματοκιβώτια.

Μια σωστά σχεδιασμένη και υλοποιημένη αρχιτεκτονική ασφάλειας που ενσωματώνει βιομετρικά συστήματα, αν αποτελέσει μέρος ενός επιχειρηματικού σχεδίου για τη σχεδίαση ή την αναδιοργάνωση μιας ηλεκτρονικής εφαρμογής, μπορεί να οδηγήσει σε επιτυχία για τους παρακάτω λόγους [142]:

- Επιτυγχάνεται η προσέλκυση περισσοτέρων χρηστών, προβάλλοντας το αυξημένο επίπεδο ασφάλειας και λειτουργικότητας του συστήματος.
- Μειώνεται το έμμεσο και το άμεσο κόστος από περιστατικά παραβίασης της ασφάλειας, είτε αυτό είναι χρηματικό, είτε έχει οποιαδήποτε άλλη μορφή, όπως νομικές συνέπειες και μείωση της αξιοπιστίας του ονόματος μίας επιχείρησης ή ενός οργανισμού.

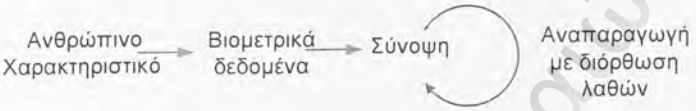
Για να επιτευχθούν τα παραπάνω, πρέπει να εξεταστεί η ασφάλεια των ίδιων των βιομετρικών συστημάτων κατά την ενσωμάτωσή τους ή τη συμπληρωματική λειτουργία τους σε μια αρχιτεκτονική ασφάλειας.

2.3.3 ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ ΒΙΟΜΕΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΥΧΑΙΟΤΗΤΑ

Ο μετασχηματισμός βιομετρικών δεδομένων σε άλλου είδους μη-αναστρέψιμα μυστικά και τυχαίους αριθμούς έχει μελετηθεί διεξοδικά από την ερευνητική κοινότητα, με στόχο το συνδυασμό των βιομετρικών με κρυπτογραφικές τεχνολογίες [195]. Το βασικό πρόβλημα προς αυτή την κατεύθυνση είναι ότι το αποτέλεσμα μιας βιομετρικής μέτρησης δεν είναι ποτέ το ίδιο, εξαιτίας μιας σειράς παραγόντων, όπως η αλληλεπίδραση του χρήστη με το σύστημα (για παράδειγμα η γωνία τοποθέτησης ενός δακτύλου στον αισθητήρα), η ελάχιστη αλλαγή των χαρακτηριστικών του ατόμου με την πάροδο του χρόνου και οι συνθήκες του περιβάλλοντος μέτρησης [128]. Κάτι τέτοιο εμποδίζει την αναπαραγωγή των ίδιων μυστικών,

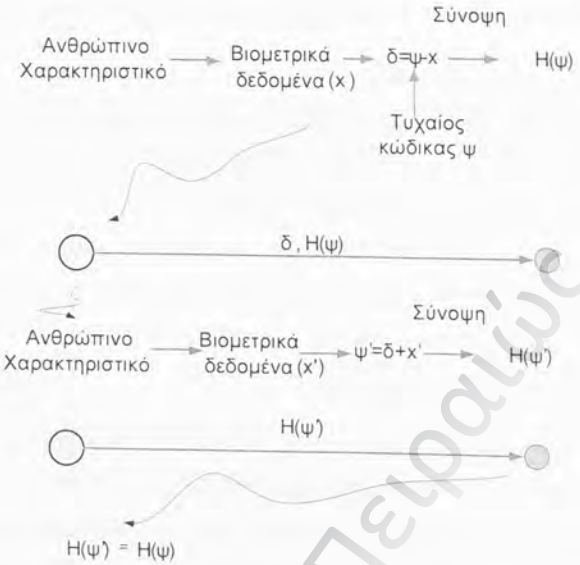
όπως για παράδειγμα τυχαίων αριθμών ή τιμών σύνοψης – hash values – με τις κοινές μεθόδους που απαιτούν ακρίβεια στην ομοιότητα της εισόδου που δέχονται [190,186].

Το πρόβλημα αυτό αντιμετωπίστηκε με διάφορες προσεγγίσεις που βασίζονταν κατά κύριο λόγω σε κώδικες διόρθωσης λαθών [194], όπως οι Hamming Distance, Set Difference και Edit Distance. Πιο συγκεκριμένα, ο Davida [178] πρότεινε τη δημιουργία τιμών σύνοψης από βιομετρικά δεδομένα, όπως φαίνεται στο Σχήμα 14.



Σχήμα 14: Δημιουργία σύνοψης βιομετρικών δεδομένων

Κώδικες διόρθωσης λαθών διορθώνουν τα λάθη κατά τη βιομετρική μέτρηση, ώστε στη συνέχεια να είναι εφικτή η αναπαραγωγή της ίδια τιμής σύνοψης με την αρχική. Ο Juels [179] πρότεινε μία "ασαφή δέσμευση" (fuzzy commitment) η οποία παρουσιάζεται στο Σχήμα 15.



Σχήμα 15: Ασαφής δέσμευση βιομετρικών [179]

Σύμφωνα με τον Juels υπολογίζεται η ακόλουθη διαφορά:

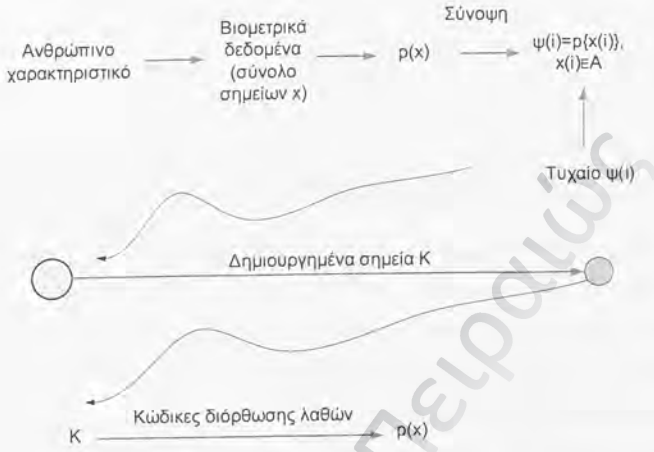
$$\delta=\psi-\chi$$

όπου ψ είναι μία τυχαία τιμή και χ είναι η βιομετρική υπογραφή. Στην συνέχεια, υπολογίζεται η σύνοψη (hash) του ψ, H(ψ) και αποθηκεύεται το δημόσιο ζεύγος (δ, H(ψ)). Αν χ′ είναι μια βιομετρική υπογραφή κοντά στη χ, τότε το σύστημα υπολογίζει την:

$$\psi'=\delta+\chi'$$

και στη συνέχεια τη σύνοψη H(ψ′). Τέλος, συγκρίνονται τα H(ψ) και H(ψ′)με τη βοήθεια κωδίκων διόρθωσης λαθών,.

Ο Juels [180], χρησιμοποίησε τον κώδικα διόρθωσης λαθών Set Difference με στόχο τη δημιουργία μιας "ασαφούς κρύπτης" (fuzzy vault), όπως φαίνεται στο Σχήμα 16.

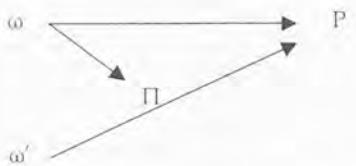


Σχήμα 16: Ασαφής κρύπτη βιομετρικών [180]

Τα βιομετρικά δεδομένα κωδικοποιούνται ως σημεία ενός πολυωνύμου p(x), του οποίου δημιουργείται η σύνοψη ψ(i), ενώ ταυτόχρονα προστίθενται και κάποια τυχαία σημεία στο ίδιο πολυώνυμο δημιουργώντας ένα νέο σύνολο σημείων K. Ο δέκτης του K χρησιμοποιεί κώδικες διόρθωσης λαθών για την ανάκτηση των αρχικών σημείων που αντιστοιχούν στα βιομετρικά δεδομένα και την αφαίρεση των τυχαίων σημείων. Παρόμοιες προσπάθειες έγιναν από τους Linnartz [181] και Verbitskiy [182], οι οποίοι υπέθεσαν μια πολυ-μεταβλητή κατανομή Gauss ως είσοδο στους μηχανισμούς τους, ενώ ο Csirmaz [183] πρότεινε μια διαφορετική προσέγγιση κβαντοποίησης στη διαδικασία διόρθωσης λαθών.

Οι παραπάνω μέθοδοι είχαν μειονεκτήματα που σχετίζονται με την γενικότητα κάποιων μαθηματικών ορισμών και δεν ήταν αποδεδειγμένα αποτελεσματικοί. Οι Frykholm [184] και Dodis [185] επέκτειναν τις ιδέες αυτές και όρισαν έννοιες με μεγαλύτερη ακρίβεια. Πιο συγκεκριμένα, ο Dodis δημιούργησε ένα μηχανισμό ασφαλούς παραγωγής τυχαίων αριθμών από μεταβλητή είσοδο με τη βοήθεια κωδίκων διόρθωσης λαθών, οι οποίοι μπορεί να

χρησιμοποιηθούν για την παραγωγή κρυπτογραφικών κλειδιών. Ο μηχανισμός αυτός παρουσιάζεται στο Σχήμα 17.



Σχήμα 17: Μηχανισμός ασφαλούς παραγωγής τυχαίων αριθμών από μεταβλητή είσοδο με τη βοήθεια κωδίκων διόρθωσης λαθών [185]

Ο μηχανισμός αυτός ονομάζεται ασαφής εξαγωγή και επιτρέπει την παραγωγή ενός τυχαίου αριθμού P από μία βιομετρική μέτρηση ω και την αναπαραγωγή του P, από μία μέτρηση ω', η οποία είναι κοντά στην ω. Η αναπαραγωγή υλοποιείται με τη χρήση ενός πολυώνυμου Π, το οποίο περιέχει πληροφορία διόρθωσης λαθών για το συγκεκριμένο ω και το οποίο παράγεται κατά την αρχική παραγωγή του P. Σύμφωνα με το μηχανισμό αυτό το P παραμένει τυχαίο, ακόμα και μετά τη δημοσίευση του Π. Στην εργασία [185] αποδεικνύεται θεωρητικά η αποτελεσματικότητα της μεθόδου.

Παρόμοιες τεχνικές έχουν αναπτυχθεί και με άλλους κώδικες διόρθωσης λαθών. Ο Hao [189] περιγράφει μία διαδικασία παραγωγής κρυπτογραφικών κλειδιών από βιομετρικά δεδομένα, η οποία βασίζεται σε διόρθωση λαθών δύο επιπέδων, χρησιμοποιώντας αρχικά το κώδικα Hadamard και στη συνέχεια τον Reed-Solomon. Η λογική είναι και πάλι ίδια, καθώς για τη διόρθωση λαθών χρησιμοποιούνται βοηθητικά δεδομένα, τα οποία είναι δημόσια και δεν προσβάλλουν την ασφάλεια του συστήματος. Η αποτελεσματικότητα της μεθόδου αποδεικνύεται με πειραματικές μετρήσεις που αποδεικνύουν ότι δεν αυξάνονται τα σφάλματα κατά τη βιομετρική μέτρηση [186, 188]

Ο συνδυασμός βιομετρικών συστημάτων και κρυπτογραφίας έχει επίσης προταθεί για συγκεκριμένες τεχνολογίες, όπως η αναγνώριση φωνής [191] και η αναγνώριση προσώπου [192]. Άλλες προσεγγίσεις, αφορούν τον έμμεσο μετασχηματισμό βιομετρικών δεδομένων. Ο Ellison [187], πρότεινε ένα μηχανισμό κρυπτογράφησης ενός τυχαίου μυστικού μέσα από την απάντηση ενός αριθμού ν ερωτήσεων από το χρήστη. Ο Monrose [188] πρότεινε μια

παρόμοια μέθοδο με χρήση της βιομετρικής μεθόδου δυναμικής πληκτρολόγησης, η οποία παρήγαγε ένα 15-διάστατο βιομετρικό χαρακτηριστικό, το οποίο κωδικοποιείται με την υποστήριξη κωδίκων διόρθωσης λαθών.

Σημειώνεται ότι οι μέθοδοι που αναφέρονται στην ενότητα αυτή αποδεικνύουν την αποτελεσματικότητά τους ως προς τη μη αύξηση των σφαλμάτων κατά τη βιομετρική μέτρηση, άλλοτε θεωρητικά και άλλοτε πρακτικά. Παρόλα αυτά, μέχρι στιγμής δεν υπάρχει σύστημα το οποίο να έχει περάσει από επίσημες διαδικασίες αξιολόγησης σύμφωνα με τα διεθνή πρότυπα και τις βέλτιστες πρακτικές αποτίμησης της απόδοσης των βιομετρικών.

2.3.4 ΑΣΦΑΛΕΙΑ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ο οργανισμός τυποποίησης American National Standards Institute, έχει δημιουργήσει το πρότυπο ANSI X9.84 "Biometric Information Management and Security", δίνοντας γενικές οδηγίες για τη διαχείριση των βιομετρικών δεδομένων (συλλογή, διαχείριση, χρήση και ασφάλεια) [145].

Ο οργανισμός τυποποίησης International Organization for Standardization (ISO) έχει τις ακόλουθες υπό-επιτροπές (subcommittees - SC), υπό την επιτροπή Joint Technical Committee 1 (JTC1):

- SC37: Δημιουργία προτύπων στο χώρο των βιομετρικών συστημάτων, αναπτύσσοντας συστάσεις που δεν περιλαμβάνουν άμεσα θέματα ασφάλειας.
- SC27: Δημιουργία προτύπων στο χώρο της ασφάλειας πληροφοριακών συστημάτων, αναπτύσσοντας γενικές συστάσεις ασφάλειας.

Η υποεπιτροπή SC37 αποτελείται από ειδικές ομάδες που αναπτύσσουν συστάσεις για τις ακόλουθες περιοχές:

- το λεξικό όρων των βιομετρικών συστημάτων (ειδική ομάδα 1 – special group 1: SG1),
- τις διεπαφές των βιομετρικών συστημάτων (ειδική ομάδα 2 – special group 2: SG2),

- τη δομή των μηνυμάτων δεδομένων που περιλαμβάνουν βιομετρικά συστήματα (ειδική ομάδα 3 – special group 3: SG3).Η ειδική ομάδα SG3 μελετά και το παλαιότερο πρότυπο Common Biometric Exchange File Format (CBEFF),
- τα προφίλ των βιομετρικών εφαρμογών (ειδική ομάδα 4 – special group 4: SG4),
- τον έλεγχο και τις δοκιμές των βιομετρικών συστημάτων (ειδική ομάδα 5 – special group 5: SG5),
- θέματα σχετικά με άλλους τομείς, όπως ο κοινωνικός τομέας (ειδική ομάδα 6 – special group 6: SG6).

Η υποεπιτροπή SC27 αναπτύσσει πρότυπα ασφάλειας ευρείας εφαρμογής, με κυριαρχο το πρότυπο ISO/IEC 17799:2005 "IT – Code of practice for information security management [17]. Το ISO/IEC 17799 είναι το πιο διαδεδομένο πρότυπο ασφάλειας πληροφοριακών συστημάτων, το οποίο αφορά και στο γενικότερα πλαίσιο ενός βιομετρικού συστήματος. Αποτελεί την ISO/IEC (International Organization for Standardization)/(International Electrotechnical Commission) έκδοση του BS7799: Part 1 προτύπου της BSI (British Standards Institution). Διακρίνει την ασφάλεια στους ακόλουθους τομείς:

- Πολιτική Ασφάλειας
- Οργάνωση Ασφάλειας
- Διαχείριση Πόρων
- Ασφάλεια Προσωπικού
- Φυσική και Περιβαλλοντολογική Ασφάλεια
- Διαχείριση Τηλεπικοινωνιών και Λειτουργιών
- Έλεγχος Πρόσβασης
- Προμήθεια, Ανάπτυξη και Συντήρηση Συστημάτων
- Διαχείριση Περιστατικών Ασφάλειας
- Διαχείριση Συνέχειας Δραστηριοτήτων
- Συμμόρφωση.

Η JTC1 προετοιμάζει μία νέα σειρά προτύπων ασφάλειας με κωδικό 2700Χ. Το πρώτο πρότυπο της σειράς είναι το ISO 27001: Information Security Management Systems –

Requirements, το οποίο προδιαγράφει τις απαιτήσεις για τη δημιουργία ενός συστήματος διαχείρισης ασφάλειας. Το πρότυπο αποτελεί απόγονο του αντίστοιχου BS7799 - Part 2, ενώ σύντομα το ISO/IEC 17799:2005 θα αντικατασταθεί από το ISO/IEC 27002. Η διαφορά μεταξύ των προτύπων ISO/IEC 27001 και ISO/IEC 17799:2005, είναι ότι το πρώτο δημιουργεί το πλαίσιο για τη δημιουργία ενός οργανωτικού συστήματος διαχείρισης της ασφάλειας ενώ το δεύτερο παρέχει τα γενικά μέτρα ασφάλειας για την υλοποίησή του.

Όσο αφορά στην πιστοποίηση της ασφάλειας συστημάτων, έχει αναπτυχθεί το ISO/IEC 15408 "Evaluation Criteria for IT security – Common Criteria (CC)" [30]. Το πρότυπο, χωρίζεται σε τρία τμήματα:

- Τμήμα 1: Εισαγωγή και Γενικό Μοντέλο: Το πρώτο τμήμα του προτύπου είναι μια εισαγωγή στην ασφάλεια των πληροφοριακών συστημάτων. Στο τμήμα αυτό, περιγράφεται το μοντέλο που χρησιμοποιεί το πρότυπο για την περιγραφή της ασφάλειας και ορίζονται διαδικασίες για την περιγραφή του συστήματος και της ασφάλειάς του. Οι διαδικασίες αυτές χρησιμοποιούν ως άξονα ένα σύνολο βασικών εννοιών του προτύπου, οι οποίες ορίζονται στο τμήμα αυτό του προτύπου, όπως επίσης ορίζονται και οι μεταξύ τους σχέσεις.
- Τμήμα 2: Λειτουργικές Απαιτήσεις Ασφάλειας: Στο δεύτερο τμήμα του προτύπου, παρουσιάζονται αναλυτικά οι κλάσεις με τα μέτρα (security requirements) για την αντιμετώπιση των απειλών και την επίτευξη των στόχων ασφάλειας (security objectives). Οι κλάσεις αυτές χρησιμεύουν στην περιγραφή της συμπεριφοράς του συστήματος σε θέματα ασφάλειας.
- Τμήμα 3: Απαιτήσεις Εγγύησης Ασφάλειας: Στο τελευταίο τμήμα του προτύπου παρουσιάζονται οι κλάσεις με τις απαιτήσεις ασφάλειας (security requirements) για την επίτευξη του ζητούμενου επιπέδου διαβεβαίωσης της ασφάλειας (EAL), υπό την έννοια των σωστών διαδικασιών μελέτης και υλοποίησης της ασφάλειας, της ύπαρξης πολιτικών και ανάλογων εγγράφων και του ελέγχου της λειτουργικότητας των μέτρων ασφάλειας. Γίνεται ορισμός των επιπέδων αυτών καθώς και των κριτηρίων για την αξιολόγηση των αναφορών. Τα επίπεδα ασφάλειας που ορίζει το πρότυπο είναι τα ακόλουθα:

- EAL1: Λειτουργικά δοκιμασμένο.
- EAL2: Δομικά δοκιμασμένο.
- EAL3: Μεθοδολογικά δοκιμασμένο και ελεγμένο.
- EAL4: Μεθοδολογικά σχεδιασμένο, δοκιμασμένο και ελεγμένο.
- EAL5: Ημιεπίσημα σχεδιασμένο και ελεγμένο.
- EAL6: Ημιεπίσημα επαληθευμένα σχεδιασμένο και ελεγμένο.
- EAL7: Επίσημα επαληθευμένα σχεδιασμένο και ελεγμένο.

Συμπληρωματικά των παραπάνω τμημάτων, έχει αναπτυχθεί η μεθοδολογία αξιολόγησης Common Evaluation Methodology (CEM). Ειδικά για τα βιομετρικά συστήματα έχει αναπτυχθεί ένα συμπλήρωμα της CEM, η Biometric Evaluation Methodology (BEM), η οποία όμως δεν είναι επίσημη και δεν έχει εγκριθεί από τον ISO ή το διοικητικό συμβούλιο των CC [149]. Η BEM αφορά κυρίως στην αξιολόγηση της απόδοσης των βιομετρικών. Περιλαμβάνει όμως και ένα πίνακα απειλών. Επιπλέον, έχουν αναπτυχθεί δύο προφίλ αξιολόγησης (protection profiles -PP):

- U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (2003) [151].
- UK: Biometric Device (Draft) [152]

Τόσο η BEM όσο και τα προφίλ αξιολόγησης:

- δεν αναφέρουν συγκεκριμένα αντίμετρα αντιμετώπισης απειλών,
- οι περιγραφές είναι πολύ γενικές και δεν περιγράφουν συγκεκριμένα τις απειλές,
- δεν συνδυάζονται με τις σύγχρονες εξελίξεις, όπως αυτές αποτυπώνονται σε πληθώρα από ερευνητικές εργασίες.

Μια εξελιγμένη έκδοση της BEM, είναι υπό ανάπτυξη από την SC37 με τίτλο: ISO/IEC 19792: IT security techniques - A framework for security evaluation and testing of biometric technology [150].

Ο οργανισμός τυποποίησης "US: INCITS – International Committee on Information Technology Standards", μέσω της ομάδας M1: Biometrics, μελετά γενικά θέματα για

βιομετρικά συστήματα, ενώ ο οργανισμός "EU: CEN – ISSS Information Society Standardization System", δημιούργησε μια ομάδα μελέτης βιομετρικών, χωρίς μέχρι στιγμής να έχουν εκδοθεί συστάσεις.

Πρότυπα που αφορούν σε βιομετρικά συστήματα έχουν συσταθεί και από τον διεθνή οργανισμό τυποποίησης για θέματα αερομεταφορών International Civil Aviation Organization (ICAO) και αφορούν στις προδιαγραφές χρήσης τους στο συγκεκριμένο τομέα.

Οι βέλτιστες πρακτικές πειραματικής αξιολόγησης της απόδοσης των βιομετρικών συστημάτων ορίζουν με ακρίβεια όλες τις σχετικές παραμέτρους για τη διεξαγωγή των μετρήσεων. Οι προδιαγραφές αυτές αφορούν στην απόδοση των συστημάτων που επηρεάζει έμμεσα και την ασφάλεια [146].

2.3.5 ΑΝΟΙΚΤΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Οι παραπάνω τομείς φανερώνουν σταθερά βήματα προόδου στο χώρο της ασφάλειας των βιομετρικών συστημάτων. Παρόλα αυτά, παρουσιάζεται μια βασική έλλειψη η οποία αφορά στο βασικότερο προπαρασκευαστικό βήμα για τη δημιουργία μιας αρχιτεκτονικής ασφάλειας που περιλαμβάνει βιομετρικά συστήματα. Το βήμα αυτό αφορά στην ασφάλεια των ίδιων των βιομετρικών συστημάτων και συγκεκριμένα στην **αποτίμηση επικινδυνότητας**, έννοια η οποία σύμφωνα με τα διεθνή πρότυπα ασφάλειας είναι συνυφασμένη με όλες της μεθοδολογίες δημιουργίας αρχιτεκτονικών ασφάλειας. Με τον όρο **αποτίμηση επικινδυνότητας** ορίζουμε την πιθανότητα μια συγκεκριμένη απειλή να πραγματοποιηθεί μέσα από την εκμετάλλευση μιας συγκεκριμένης αδυναμίας του συστήματος. Με τον όρο **απειλή** ορίζουμε ένα γεγονός με αρνητικές συνέπειες στο σύστημα, ενώ με τον όρο **αδυναμία** ορίζουμε μία ατέλεια ασφάλειας του συστήματος. Η αποτίμηση επικινδυνότητας είναι μία διαδικασία η οποία υποδεικνύει τις απειλές, τις αδυναμίες και την επικινδυνότητα του συστήματος, καθώς και μέτρα ασφάλειας για την αντιμετώπισή τους.

Τα σύγχρονα συστήματα αποτίμησης επικινδυνότητας, βασίζονται σε δύο δομικά συστατικά:

1. μια μεθοδολογία, και

2. μια βάση δεδομένων, η οποία περιλαμβάνει πιθανές απειλές, αδυναμίες, προτεινόμενα μέτρα ασφάλειας και παράγοντες επικινδυνότητας ανά αδυναμία (δηλαδή την επικινδυνότητα που εισάγει μια συγκεκριμένη αδυναμία στο σύστημα).

Στην περίπτωση των βιομετρικών συστημάτων, το πρώτο δομικό χαρακτηριστικό μπορεί να καλυφθεί από οποιαδήποτε αναγνωρισμένη μεθοδολογία αποτίμησης επικινδυνότητας, καθώς δεν περιέχει εξειδικευμένες απαιτήσεις. Όσον αφορά στο δεύτερο δομικό συστατικό παρατηρείται ένα κενό το οποίο δεν έχει καλυφθεί ως σήμερα.

Τα παραπάνω υποδεικνύουν την ανάγκη ύπαρξης ενός μεθοδικού συστήματος αποτίμησης επικινδυνότητας βιομετρικών συστημάτων, με στόχο τη δημιουργία ασφαλών μηχανισμών και αρχιτεκτονικών ασφάλειας που ενσωματώνουν βιομετρικά συστήματα.

2.4 ΣΥΣΤΗΜΑΤΑ ΠΑΓΙΔΕΥΣΗΣ ΕΙΣΒΟΛΕΩΝ (HONEYNETS)

2.4.1 ΟΡΙΣΜΟΣ ΚΑΙ ΕΙΣΑΓΩΓΙΚΑ ΣΤΟΙΧΕΙΑ

Τα **συστήματα παγίδευσης εισβολέων (ΣΠΕ - Honeynets)** ορίζονται ως εξελιγμένα συστήματα δικτυακής ασφάλειας, τα οποία συνδυάζουν προληπτικά, ανιχνευτικά και αντιδραστικά αντίμετρα με στόχο την εξαπάτηση και την παγίδευση εισβολέων, των οποίων η χρησιμότητα έγκειται στην παραβίαση αυτών, με σκοπό τη μελέτη τακτικών εισβολής [171]. Η πρώτη γενιά των ΣΠΕ έκανε την εμφάνισή της στις αρχές της δεκαετίας του '90 και αποτελούνταν από κοινά συστήματα που δέχονταν επιθέσεις χωρίς να υποστηρίζουν κάποια πραγματική εταιρική λειτουργία, με τους υπεύθυνους διαχείρισής τους, να παρακολουθούν τα αρχεία καταγραφής, προσπαθώντας να εντοπίσουν κινήσεις εισβολέων [174]. Τα εξελιγμένα συστήματα 2ης γενιάς εμφανίζονται στις αρχές του 2002, ως αποτελέσματα των προσπαθειών της μη κερδοσκοπικής ερευνητικής ομάδας Honeynet Alliance. Τα εξελιγμένα αυτά συστήματα έχουν κυρίως ερευνητικό χαρακτήρα είναι πολύ πιο ασφαλή και αποτελεσματικά [170].

Ένα ΣΠΕ μπορεί να αποτελείται από ένα μόνο υπολογιστή, ο οποίος εξομοιώνει διάφορα λειτουργικά συστήματα και υπηρεσίες, ή από ένα σύνολο πραγματικών συστημάτων που δε

διαφέρει σε τίποτα από ένα σύστημα που υποστηρίζει την παραγωγική διαδικασία του οργανισμού. Στην πρώτη περίπτωση, το ΣΠΕ ονομάζεται *Σύστημα Παγίδευσης* -ΣΠ- (*Honeypot*) και έχει κυρίως προληπτικό και ανιχνευτικό χαρακτήρα. Στη δεύτερη περίπτωση το ΣΠΕ ονομάζεται *Δίκτυο Παγίδευσης* -ΔΠ- (*Honeynet*), το οποίο αν και έχει κυρίως ερευνητικό χαρακτήρα, είναι πιο πλήρες και πιο ασφαλές.

Ένα ΔΠ έχει τις εξής χρήσεις:

- **Προληπτικού αντιμέτρου:** Λειτουργεί ως δόλωμα ή στοιχείο αντιπερισπασμού, ώστε το ενδιαφέρον του εισβολέα να περιοριστεί αρχικά σε αυτό το πιο ευπαθές σύστημα και να κρατηθεί μακριά από το πραγματικό πληροφοριακό σύστημα του οργανισμού.
- **Ανιχνευτικού αντιμέτρου:** Λειτουργεί ως ανιχνευτής εισβολών και προετοιμάζει ανώδυνα για μια πιθανή επίθεση στο πραγματικό σύστημα του οργανισμού.
- **Αντιδραστικού αντιμέτρου:** Παραμετροποιεί αυτόματα ή δίνει πληροφορίες για την απαραίτητη παραμετροποίηση της λοιπής αρχιτεκτονικής ασφάλειας, ώστε να προστατευθεί αποτελεσματικά το πραγματικό σύστημα. Αυτό επιτυγχάνεται με τη συλλογή πληροφοριών από τις επιθέσεις που δέχεται το ΔΠ, τις οποίες στη συνέχεια αναλύουν οι υπεύθυνοι ασφάλειας του πληροφοριακού συστήματος με σκοπό την αναβάθμιση της γνώσης τους και την παραμετροποίηση αποτελεσματικότερων αντιμέτρων.

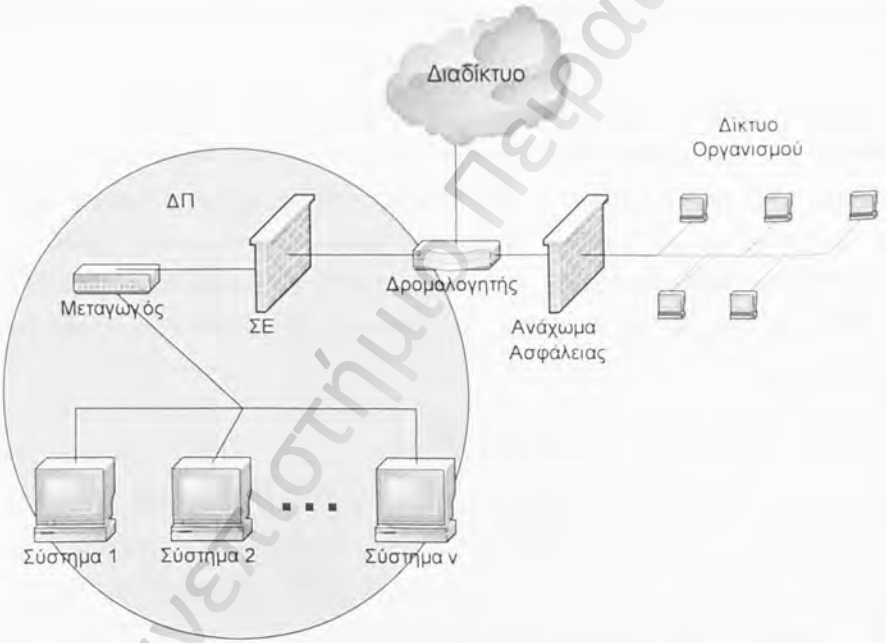
2.4.2 ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ

Για να πετύχουν τα ΔΠ το στόχο τους πρέπει να αποτελούνται από ευπαθή συστήματα. Αυτό το χαρακτηριστικό εισάγει το σημαντικό ρίσκο της εισβολής σε αυτά και της χρήσης τους για την υλοποίηση επιθέσεων σε τρίτους. Επιπλέον οι μηχανισμοί καταγραφής πληροφορίας πρέπει να είναι διαφανείς και πλήρεις. Για τους παραπάνω λόγους τα ΔΠ πρέπει να δημιουργούνται βάσει των παρακάτω θεμελιωδών αρχών:

- αποτελεσματικός έλεγχος ΔΠ και
- αποτελεσματική και πλήρης καταγραφή δεδομένων.

Η υλοποίηση ενός ΔΠ, γίνεται συνήθως με λογισμικό ανοικτού κώδικα. Σύμφωνα με το Honeynet Project [170] η υλοποίηση των θεμελιωδών αρχών πραγματοποιείται σε ένα Σημείο Ελέγχου (ΣΕ - honeywall) το οποίο συνδυάζει προληπτικά, ανιχνευτικά και αντιδραστικά αντίμετρα σε λειτουργικό Linux ή BSD.

Το ΣΕ λειτουργεί στο επίπεδο 2 του μοντέλου αναφοράς Open Systems Interconnection (OSI) και υλοποιεί γεφύρωση (bridging), έτσι ώστε να μην αποδίδονται διευθύνσεις IP στις δικτυακές διεπαφές του και να είναι ουσιαστικά αόρατο (τουλάχιστον σε επίπεδο διευθύνσεων IP) στον εισβολέα. Το Σχήμα 18, παρουσιάζει την αρχιτεκτονική ενός ΔΠ, η οποία ονομάζεται 2ης γενιάς, σύμφωνα με το Honeynet Project.



Σχήμα 18: Αρχιτεκτονική ΔΠ 2ης Γενιάς [170]

Στην αρχιτεκτονική αυτή διακρίνουμε τον πλήρη διαχωρισμό σε φυσικό επίπεδο του δικτύου του οργανισμού και του ΔΠ. Το ΣΕ ελέγχει όλη τη δικτυακή κίνηση από και προς τα ευπαθή συστήματα του ΔΠ, τα οποία είναι τυπικά παραμετροποιημένα λειτουργικά

συστήματα διαφόρων ειδών (Linux, Solaris, BSD, Windows κλπ) και τα οποία λειτουργούν ως δολώματα. Η αρχιτεκτονική του εταιρικού δικτύου παραμένει αναλλοίωτη, με το ανάχωμα ασφάλειας (firewall) να φιλτράρει την κίνηση από και προς σε αυτό και τον δρομολογητή να παραμετροποιείται ως αντίμετρο πρώτης γραμμής. Ο τρόπος υλοποίησης των θεμελιωδών αρχών μιας αρχιτεκτονικής ΔΠ 2ης γενιάς παρουσιάζεται αναλυτικά παρακάτω.

2.4.2.1 Υλοποίηση ελέγχου ΔΠ

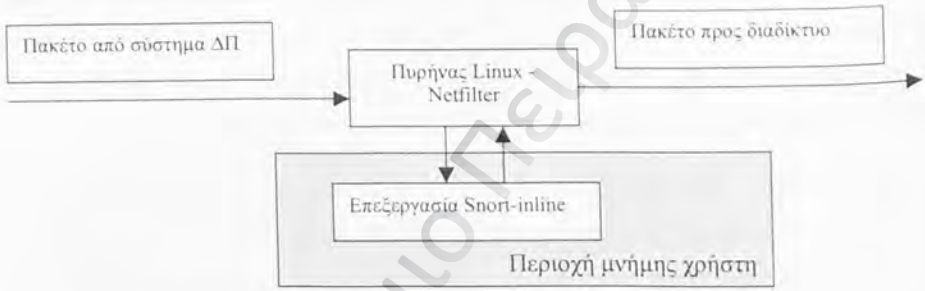
Ο βασικός στόχος της θεμελιώδους αρχής αποτελεσματικού έλεγχου είναι ο περιορισμός του εισβολέα στο ΔΠ και η αποφυγή χρήσης του ως εφαλτηρίου επιθέσεων σε άλλους στόχους. Για το σκοπό αυτό παρατάσσονται τεχνολογίες πρόληψης, ανίχνευσης και αντίδρασης (αναχαίτισης επιθέσεων) με αντίστροφο τρόπο, από ότι σε ένα κοινό σύστημα. Παραμετροποιούμε, δηλαδή, το ΔΠ με σκοπό να αναχαιτίσουμε επιθέσεις από το ΔΠ προς το Διαδίκτυο και όχι με σκοπό την προστασία του ΔΠ από εξωτερικές επιθέσεις.

Η παραμετροποίηση στο τμήμα αυτό του ΣΕ είναι πολύ σημαντική, διότι καθορίζουμε το πεδίο δράσης του εισβολέα και τους βαθμούς ελευθερίας του. Άλλωστε η γνώση που αποκομίζουμε από το ΔΠ είναι ανάλογη της ελευθερίας που παρέχουμε στον εισβολέα και αντιστρόφως ανάλογη του ρίσκου που λαμβάνουμε.

Πιο συγκεκριμένα, ο έλεγχος του ΔΠ μπορεί να υλοποιηθεί με ένα ανάχωμα ασφάλειας ανοικτού κώδικα όπως το Netfilter[16], το οποίο είναι ενσωματωμένο στον πυρήνα του Linux και έχει δυνατότητα λειτουργίας σε επίπεδο 2 του μοντέλου αναφοράς OSI. Με κατάλληλη παραμετροποίηση του Netfilter περιορίζουμε τον αριθμό των εξερχόμενων συνδέσεων, έτσι ώστε να περιορίσουμε την επιθετική συμπεριφορά του εισβολέα (πχ να αποτρέψουμε επιθέσεις άρνησης παροχής υπηρεσιών σε τρίτους στόχους).

[16] http://www.netfilter.org

Παράλληλα, χρησιμοποιούμε και ένα σύστημα ανίχνευσης και αναχαίτισης εισβολών. Αυτό μπορεί να υλοποιηθεί με μια ειδική έκδοση του συστήματος ανίχνευσης εισβολών ανοικτού κώδικα Snort[17], το οποίο ονομάζεται Snort_inline. Το Snort_inline, συνεργάζεται με το Netfilter, μέσω της ενεργοποίησης μιας υπομονάδας (module) του πυρήνα του Linux, η οποία ονομάζεται ip_queue. Με το ip_queue, το Netfilter τοποθετεί τα πακέτα στην περιοχή μνήμης χρήστη (user space), όπου τα επεξεργάζεται το Snort_inline, το οποίο στη συνέχεια τα επιστρέφει στο Netfilter προς δρομολόγηση. Ένα πακέτο, δηλαδή, προερχόμενο από κάποιο σύστημα του ΔΠ περνάει από τους κανόνες φιλτραρίσματος του Netfilter, προωθείται στο Snort_inline προς επεξεργασία και επιστρέφει στο Netfilter, από το οποίο δρομολογείται στον προορισμό του. Ο παραπάνω μηχανισμός παρουσιάζεται στο Σχήμα 19.



Σχήμα 19: Μηχανισμός ελέγχου εξερχόμενης δικτυακής κίνησης

Η επεξεργασία που κάνει το Snort_inline βασίζεται στην κλασική χρήση υπογραφών γνωστών επιθέσεων του Snort, με τη διαφορά ότι παρέχει περισσότερες δυνατότητες πέρα από την παραγωγή προειδοποιήσεων (alerts), όπως αυτές της απόρριψης ενός πακέτου και της αλλοίωσης του περιεχομένου του. Έτσι, ένα πακέτο που περιέχει επικίνδυνο περιεχόμενο που ταυτίζεται με κάποια υπογραφή επίθεσης μπορεί να απορριφθεί, ή να δρομολογηθεί κανονικά με αλλοιωμένο όμως περιεχόμενο, όντας πια ακίνδυνο.

[17] http://www.snort.org.

2.4.2.2 Υλοποίηση καταγραφής δεδομένων

Ο βασικός στόχος της θεμελιώδους αρχής καταγραφής δεδομένων είναι να καταγράψουμε την κάθε κίνηση του εισβολέα στο σύστημα. Αυτό υλοποιείται με κλασικές μεθόδους, όπως η χρήση συστήματος καταγραφής δικτυακής κίνησης (πχ με το λογισμικό ethereal[18]) και η χρήση αρχείων καταγραφής σε κάθε σύστημα του ΔΠ. Παρόλ' αυτά, η βασική καταγραφή πρέπει να γίνεται στο ΣΕ, διότι πιθανή εισβολή σε κάποιο σύστημα του ΔΠ θέτει αυτόματα σε κίνδυνο όλα τα αρχεία καταγραφής σε αυτό.

Στο ΣΕ, η καταγραφή γίνεται με γνωστές μεθόδους, όπως τα αρχεία καταγραφής του Netfilter, η χρήση του Snort, του Tcpdump και γενικότερα οποιουδήποτε συμβατικού εργαλείου καταγραφής δικτυακής κίνησης στο κομβικό αυτό σημείο του ΔΠ. Η καταγραφή είναι αόρατη στον εισβολέα, ο οποίος βλέπει μόνο την διεύθυνση IP του συστήματος στόχου απευθείας, καθώς το ΣΕ καταγράφει δικτυακή κίνηση λειτουργώντας ως γέφυρα (bridge). Πέρα από αυτό, αν είναι επιθυμητή η καταγραφή των εντολών που πληκτρολογεί ο εισβολέας σε ένα σύστημα συνίσταται η χρήση αισθητήρων πληκτρολογήσεων (keystroke sniffers) σε κάθε σύστημα του ΔΠ.

Το Honeynet Alliance έχει αναπτύξει ένα εξελιγμένο αισθητήρα πληκτρολογήσεων, τον οποίο ονομάζει Sebek 2 και ο οποίος εγκαθιστά μια υπομονάδα (module) στον πυρήνα κάθε συστήματος του ΔΠ και στη συνέχεια αποκρύπτει την υπομονάδα αυτή, επεμβαίνοντας στους δείκτες αναγνώρισης της [172]. Η υπομονάδα αυτή ουσιαστικά αποτυπώνει την πληκτρολόγηση των εντολών του εισβολέα, καθώς εκείνος τις εισάγει στο σύστημα και προωθεί την πληροφορία αυτή στο ΣΕ. Αυτό υλοποιείται επεμβαίνοντας στη διαδικασία εισαγωγής των πληκτρολογήσεων του εισβολέα (System Call Table) και δημιουργώντας ένα αντίγραφο των πληκτρολογήσεων, πριν αυτές επεξεργαστούν από τον πυρήνα του λειτουργικού. Έτσι λύνεται και το πρόβλημα με τις κρυπτογραφημένες πληκτρολογήσεις σε σενάρια χρήσης ασφαλών εφαρμογών απομακρυσμένης σύνδεσης, όπως το ssh, καθώς στην περιοχή του πυρήνα οι πληκτρολογήσεις είναι αποκρυπτογραφημένες, πριν επεξεργαστούν

[18] http://www.ethereal.com

από τον πυρήνα. Η απόκρυψη της υπομονάδας του Sebek 2, υλοποιείται με την εισαγωγή μιας νέας υπομονάδας, η οποία αναλαμβάνει να αλλοιώσει τη λίστα των εγκατεστημένων υπομονάδων του συστήματος. Η πληροφορία των πληκτρολογήσεων αποστέλλεται από κάθε σύστημα σε ένα κεντρικό εξυπηρετητή. Το Sebek 2 δεν χρησιμοποιεί τις δυνατότητες TCP/IP του μηχανήματος, αλλά δημιουργεί εξειδικευμένα πακέτα τα οποία αποστέλλει απευθείας στον οδηγό της κάρτας δικτύου, παρακάμπτοντας τις διαδρομές του raw socket code και packet filtering code, οι οποίες χρησιμοποιούνται από υπομονάδες που συνεργάζονται με εφαρμογές για τη συλλογή και ανάλυση πακέτων, κάνοντας αόρατη τη δικτυακή αυτή κίνηση από κάθε σύστημα. Επίσης κάθε σύστημα παραμετροποιείται έτσι ώστε να απορρίπτει σιωπηλά πακέτα Sebek 2 τα οποία προέρχονται από άλλα συστήματα, μεταβάλλοντας τη διεπαφή raw socket κάθε συστήματος.

2.4.3 Πλεονεκτηματα και μειονεκτηματα

Τα ΣΠΕ, υπό την προϋπόθεση της πολύ προσεκτικής σχεδίασης και παραμετροποίησης τους, υλοποιούν μια καινούρια και πολλά υποσχόμενη τάση στο χώρο της δικτυακής ασφάλειας. Μια σωστά υλοποιημένη αρχιτεκτονική ΔΠ 2ης γενιάς θεωρητικά, αλλά και πρακτικά αποδεδειγμένα [175], έχει τα παρακάτω πλεονεκτήματα σε σχέση με μια κοινή αρχιτεκτονική ασφάλειας:

- Αυξημένα επίπεδα ασφάλειας από εσωτερικούς κατειλημμένους κόμβους του συστήματος. Ένα ΔΠ 2ης γενιάς παρέχει αυξημένες δυνατότητες αναχαίτισης επιθέσεων από εσωτερικούς κόμβους προς εσωτερικούς κόμβους άλλων ζωνών ασφάλειας, με χρήση των τεχνολογιών που περιγράφηκαν παραπάνω.
- Αυξημένα επίπεδα ασφάλειας από εξωτερικούς κόμβους, υλοποιώντας πλήρως τις εξελιγμένες υπηρεσίες πρόληψης, ανίχνευσης και αντίδρασης που περιγράφηκαν παραπάνω.
- Αυξημένα επίπεδα ασφάλειας σε εξωτερικούς κόμβους. Ένα ΔΠ 2ης γενιάς παρέχει αυξημένες δυνατότητες αναχαίτισης επιθέσεων από εσωτερικούς κόμβους προς εξωτερικούς στόχους, με χρήση των τεχνολογιών που περιγράφηκαν παραπάνω.

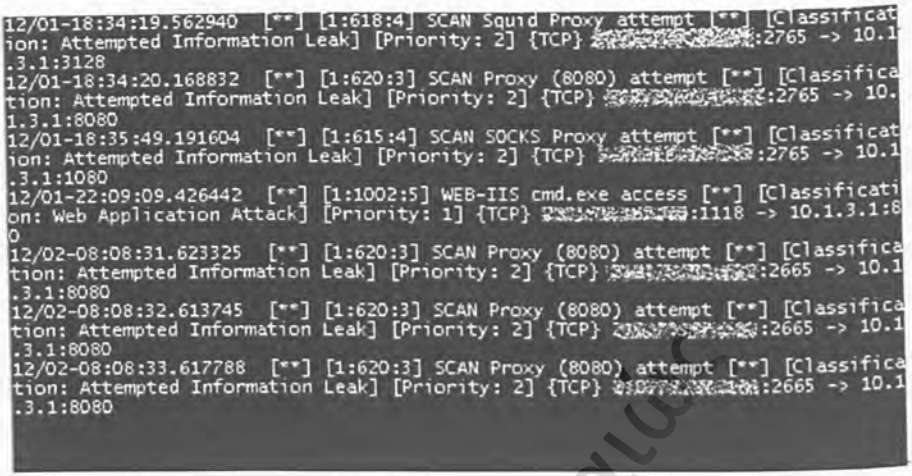
- Γνώση ασφάλειας, μέσα από τη μελέτη τακτικών και τεχνολογιών των εισβολέων, κάτι το οποίο αποτελεί και την πεμπτουσία των ΣΠΕ.

Σε σχέση με μια κοινή αρχιτεκτονική ασφάλειας, τα ΣΠΕ έχουν ως βασικό μειονέκτημα το πρόσθετο κόστος, διότι αποτελούν συμπληρωματικά μέτρα ασφάλειας και όχι κύρια. Παρόλα αυτά, το κόστος είναι αρκετά περιορισμένο. Το πάγιο κόστος λόγω της δυνατότητας χρήσης λογισμικού ανοικτού κώδικα για την υλοποίηση των ΣΠΕ είναι ιδιαίτερα μειωμένο. Ο βασικός συντελεστής κόστους αφορά στο λειτουργικό κόστος, δηλαδή στο κόστος παρακολούθησης των ΣΠΕ από ειδικούς σε θέματα ασφάλειας, το οποίο με τη σειρά του περιορίζεται σημαντικά αν ο οργανισμός διαθέτει ήδη ομάδα ασφάλειας.

2.4.4 Πειραματικη δοκιμη

Η παράγραφος αυτή παρουσιάζει μερικά χαρακτηριστικά αποτελέσματα από το πειραματικό ΔΠ 2ης γενιάς, το οποίο δημιουργήθηκε στο πλαίσιο της διδακτορικής διατριβής βάσει των θεμελιωδών αρχών που περιγράφηκαν προηγουμένως, στο πλαίσιο δοκιμών των δυνατοτήτων των ΣΠΕ. Το ΔΠ, εκτός από το ΣΕ, περιλαμβάνει συστήματα Linux, BSD και Windows και τέθηκε επίσημα σε λειτουργία με ανακοίνωση στο Honeynet Project. Ενδεικτικά αποτελέσματα επιθέσεων στο σύστημα του ΔΠ με όνομα meltemi και εσωτερική IP: 10.1.3.1, παρουσιάζονται παρακάτω – με τις διευθύνσεις IP των επιτιθέμενων να μην εμφανίζονται για ευνόητους λόγους.

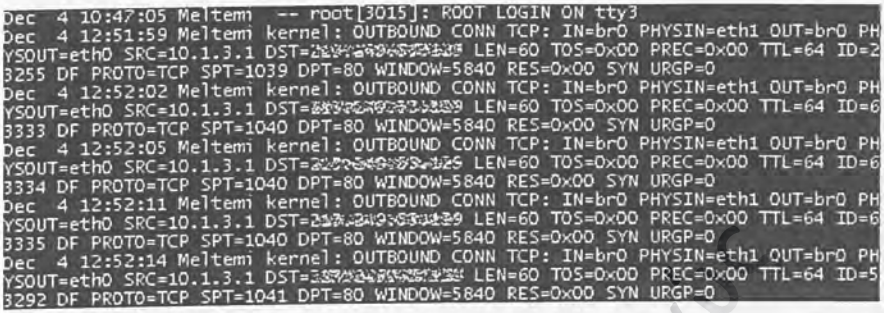
Καταγράψαμε πλήθος σαρώσεων θυρών, το οποίο συνήθως αποτελεί το πρώτο βήμα πριν την υλοποίηση μιας επίθεσης. Η πληθώρα αυτή φανερώνει τη μεγάλη συχνότητα επιθετικής δραστηριότητας στο Διαδίκτυο. Οι σαρώσεις θυρών έγιναν άμεσα αντιληπτές από το σύστημα ανίχνευσης εισβολών του ΣΕ, όπως χαρακτηριστικά φαίνεται στο Σχήμα 20 (σάρωση SCAN Proxy, SCAN SOCKS στο σύστημα του ΔΠ με διεύθυνση IP:10.1.3.1).



Σχήμα 20: Τμήμα αρχείου καταγραφής snort – σάρωση και επίθεση

Η σάρωση θυρών, έχει ως κύριο στόχο την ανεύρεση ανοικτών θυρών που θα φανερώσουν τις δικτυακές υπηρεσίες που έχει ενεργοποιημένες το δίκτυο-θύμα.

Παρατηρώντας την προσπάθεια εισβολής, αποφασίσαμε να δώσουμε αδύναμα συνθηματικά (weak passwords) στην υπηρεσία ασφαλούς απομακρυσμένης πρόσβασης (secure shell) που είχαμε ενεργοποιήσει. Τότε, είχαμε και το πρώτο περιστατικό εισβολής στο σύστημα. Η πρώτη κίνηση του εισβολέα μετά την απόκτηση πρόσβασης ήταν να σαρώσει τις θύρες των υπολοίπων διευθύνσεων του δικτύου μας προς ανίχνευση ευπαθειών. Αυτό έγινε άμεσα αντιληπτό από το ανάχωμα ασφάλειας (firewall) του ΔΠ, το οποίο εντόπισε εξερχόμενη κίνηση από το ΔΠ, όπως φαίνεται στο Σχήμα 21 (OUTBOUND CONN από σύστημα του ΔΠ με διεύθυνση IP:10.1.3.1),

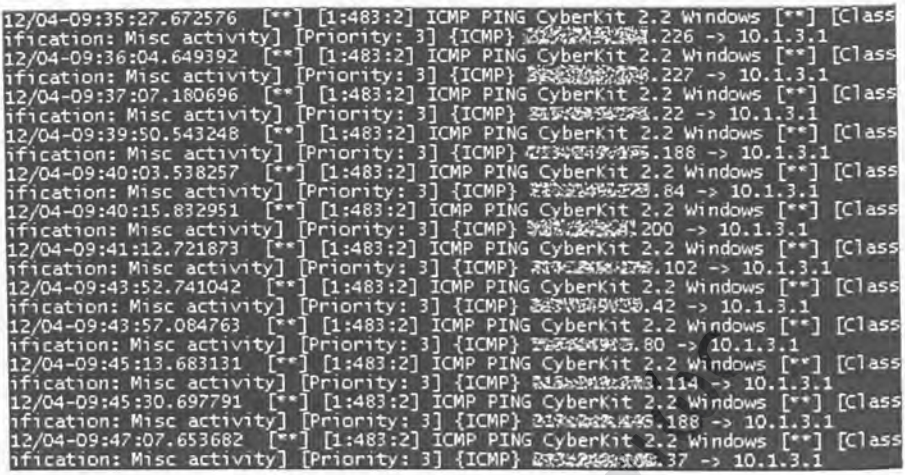


Σχήμα 21: Τμήμα αρχείου καταγραφής netfilter – εξερχόμενη κίνηση

αλλά και από το σύστημα αναχαίτισης εισβολών (snort_inline), όπως φαίνεται στο Σχήμα 22 (ICMP PING NMAP, από το σύστημα του ΔΠ με διεύθυνση IP:10.1.3.1).

Σχήμα 22: Τμήμα αρχείου καταγραφής snort_inline – σάρωση θυρών από ΣΠΕ

Σε μία άλλη περίπτωση, παρατηρήσαμε πολύ αυξημένη κίνηση πακέτων ICMP, υποθέτοντας ότι το δίκτυό μας δεχόταν κατανεμημένη επίθεση άρνησης εξυπηρέτησης. Αυτό έγινε αμέσως φανερό από το πλήθος των ασταμάτητων πακέτων ICMP που δεχόμασταν και που φαινόταν να έχουν διαφορετική κάθε φορά προέλευση, όπως παρουσιάζεται στο Σχήμα 23 (ICMP PING CyberKit 2.2).



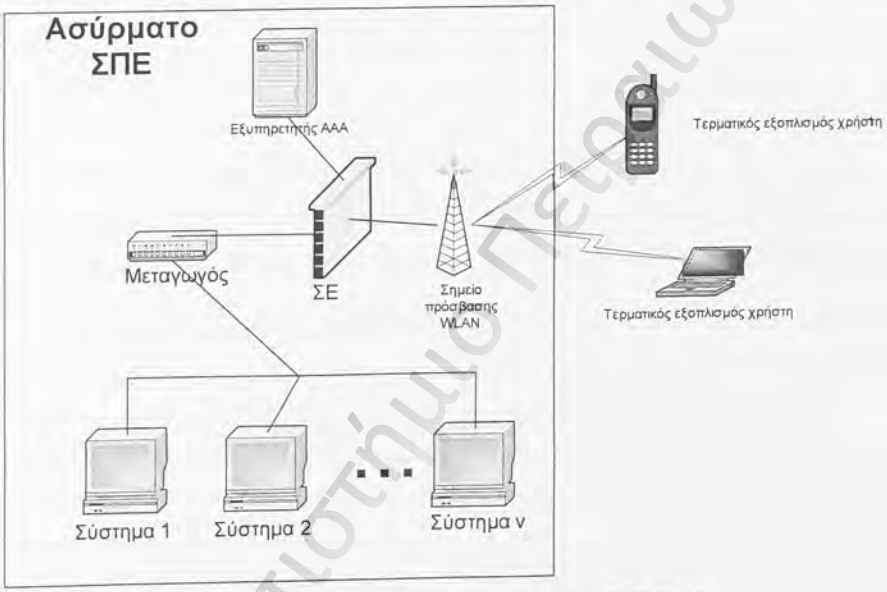
Σχήμα 23: Τμήμα αρχείου καταγραφής snort

Μετά από μελέτη σχετικών περιστατικών ασφάλειας, αναγνωρίσαμε το συγκεκριμένο σύμπτωμα ως αποτέλεσμα της μόλυνσης των υποτιθέμενων εισβολέων με τον ιό Nachia ή Welchia. Ο συγκεκριμένος ιός αυξάνει κατά πολύ την εξερχόμενη πληροφορία ICMP και προσπαθεί να εκμεταλλευτεί τα ευπαθή σημεία DCOM RPC και WebDav μηχανημάτων με λειτουργικό σύστημα Windows. Το περιεχόμενο και το μέγεθος μάλιστα των πακέτων ICMP και των πακέτων TCP στη θύρα 135 που αποστέλλει ένα μολυσμένο με τον ιό Welchia σύστημα, είναι πολύ συγκεκριμένο και ενεργοποιεί την ICMP PING Cyberkit προειδοποίηση του Snort. Οι παρατηρήσεις αυτές θα οδηγούσαν ένα οργανισμό που υλοποιεί ΔΠ, στο σωστό αντίμετρο, δηλαδή τον περιορισμό με συγκεκριμένες παραμέτρους (μεγέθους και περιεχομένου) της κίνησης ICMP αλλά και της κίνησης προς τη θύρα 135 του πραγματικού δικτύου του οργανισμού.

Σε διάστημα ενός μήνα, το ΔΠ δέχθηκε ποικίλες επιθέσεις, είτε από ιούς, είτε από επίδοξους εισβολείς που χρησιμοποιούν αυτοματοποιημένα εργαλεία επιθέσεων, είτε από περισσότερο μυημένους στο χώρο, οι κινήσεις των οποίων ήταν λιγότερο θορυβώδεις.

2.4.5 ΣΠΕ ΣΕ ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

ΣΠΕ και πιο συγκεκριμένα ΔΠ 2ης γενιάς έχουν μελετηθεί για δίκτυα WLAN, εξελίσσοντας και προσαρμόζοντας τα κοινά ενσύρματα ΔΠ σε ένα περιβάλλον WLAN. Πιο συγκεκριμένα, ο Oudot [176] περιγράφει με πιο τρόπο τα κοινά ΔΠ μπορεί να παραμετροποιηθούν διατηρώντας όλες τις βασικές αρχές λειτουργίας τους και τη δομή τους, ώστε να ανταποκρίνονται στις εξειδικευμένες επιθέσεις σε ένα περιβάλλον WLAN. Μία τέτοια αρχιτεκτονική, περιγράφεται στο Σχήμα 24, εξελίσσοντάς την σε 3G/WLAN:



Σχήμα 24: Απλοποιημένη αρχιτεκτονική του ΣΠΕ [176]

Στην αρχιτεκτονική αυτή διακρίνουμε τον εξοπλισμό του χρήστη (πχ κινητό τηλέφωνο ή φορητός υπολογιστής), ο οποίος επικοινωνεί με το σημείο πρόσβασης του τοπικού ασύρματου δικτύου το οποίο υλοποιεί και πύλη 3G/WLAN. Το ΣΕ ελέγχει όλη τη δικτυακή κίνηση από και προς τα ευπαθή συστήματα του ΣΠΕ, τα οποία είναι τυπικά παραμετροποιημένα λειτουργικά συστήματα διαφόρων ειδών (Linux, Solaris, BSD, Windows κλπ) και τα οποία λειτουργούν ως δολώματα. Ένας εξομοιωτής εξυπηρετητή AAA έχει το ρόλο του εξυπηρετητή πιστοποίησης ταυτότητας χρήστη.

2.5 Παρουσιαση βοηθητικων μεθοδολογιων και θεωριων

2.5.1 Η αλγεβρα μοντελοποιησης πρωτοκολλων CSP

2.5.1.1 Εισαγωγή και βασική σημειογραφία

Η CSP (Communicating Sequential Processes) είναι μία άλγεβρα μοντελοποίησης πρωτοκόλλων, η οποία χρησιμεύει όχι μόνο στην τυπική και μεθοδική περιγραφή ενός πρωτοκόλλου [155], αλλά επεκτείνεται και στην επαλήθευση της ασφάλειας αυτών [156]. Όσον αφορά στη μοντελοποίηση, η CSP χρησιμοποιεί διαδικασίες (processes) και γεγονότα (events) τα οποία σχετίζονται με τις διαδικασίες και τα οποία ουσιαστικά αποτελούν στιγμιότυπα μιας επικοινωνίας, τα οποία συνήθως εμπλέκουν ένα κανάλι επικοινωνίας και κάποια δεδομένα [154]. Η δομή των γεγονότων αυτών είναι της μορφής $\kappa.\delta$, όπου κ είναι το όνομα του καναλιού και δ η τιμή η οποία μεταδίδεται στο κανάλι. Τα γεγονότα μπορεί να είναι ατομικά, όσο αφορά στη δομή τους, ή να αποτελούνται από επιμέρους συστατικά.

Μια διαδικασία ουσιαστικά εκφράζει μια μορφή αλληλεπίδρασης. Η έκφραση $a\text{->}\Pi$, περιγράφει μία διαδικασία που αρχικά μπορεί να λειτουργήσει ως a και στη συνέχεια συμπεριφέρεται ως Π. Η διαδικασία τέλος (stop) είναι η απλούστερη διαδικασία που μπορεί να περιγραφεί, η οποία δεν έχει εναλλαγή γεγονότων και απλώς δηλώνει το τέλος της αλληλεπίδρασης. Μία διαδικασία μπορεί επίσης να συνδέεται με κανάλια επικοινωνίας, από τα οποία να δέχεται εισόδους και να παρέχει εξόδους. Η έκφραση $\kappa!v\text{->}\Pi$, περιγράφει μια διαδικασία, η οποία θα παρέχει στην έξοδο στην τιμή v, στο κανάλι κ και η οποία στη συνέχεια θα συμπεριφέρεται ως Π. Αντίστοιχα, η έκφραση $\kappa?\chi\text{->}\ \Pi(\chi)$, σημαίνει ότι η διαδικασία Π, δέχεται ως είσοδο την τιμή χ από τον κανάλι κ και στη συνέχεια η συμπεριφορά της δηλώνεται ως $\Pi(\chi)$, επηρεασμένη δηλαδή από την είσοδο που δέχθηκε. Μια οικογένεια διαδικασιών εκφράζεται ως $\{P_i \mid i \in I\}$ και η επιλογή από την οικογένεια αυτή ως $\underset{i \in I}{\square} P_i$.

Ο τελεστής $\underset{A}{\|}$ χρησιμοποιείται για να δηλώσει την παραλληλία δύο διαδικασιών και να τις συγχρονίσει με ένα κοινό σύνολο γεγονότων A, με την έννοια ότι μπορεί να συντελείται

ανταλλαγή τιμών πάνω από ένα κανάλι μεταξύ της εισόδου της μιας διαδικασίας και της εξόδου της άλλης και αντίστροφα. Έτσι δύο διαδικασίες Π και Γ συντελούνταν παράλληλα και συγχρονισμένα με ένα κοινό σύνολο γεγονότων A, τότε η έκφραση θα ήταν $\Pi \underset{A}{||} \Gamma$. Ο τελεστής δεν περιορίζει τις διαδικασίες να συνδέονται σε γεγονότα εκτός του A. Η έκφραση $\Pi \underset{A}{||} STOP$ δηλώνει ότι η διαδικασία δεν επιτρέπεται να εκτελέσει γεγονότα στο σύνολο A.

Ο τελεστής ||| χρησιμοποιείται για να δηλώσει ότι δύο διαδικασίες εκτελούνται παράλληλα χωρίς να αλληλεπιδρούν μεταξύ τους. Έτσι, αν οι δύο παράλληλες και μη αλληλεπιδρόμενες διαδικασίες είναι η Π και η Γ, αυτό εκφράζεται ως Π ||| Γ. Η έκφραση $|||_{i \in I} Pi$, εκφράζει την ανεξάρτητη εκτέλεση των διαδικασιών της οικογένειας $\{Pi \mid i \in I\}$. Οι εκφράσεις if, then, else, let, χρησιμοποιούνται για τη δημιουργία συνθηκών στα γεγονότα, όπως και στις γλώσσες προγραμματισμού.

Οι διαδικασίες μπορεί να ορίζονται και από περιοδικές αναφορές, οι οποίες ορίζουν μια συμπεριφορά η οποία προκύπτει από ένα σύνολο υπο-διαδικασιών, όπως στο παράδειγμα που ακολουθεί και αναφέρεται σε σχετική εργασία.

```
2COPY = in?x -> HOLDS (x)

HOLDS (x) = in?y -> out!x -> HOLDS (y)

  out!x -> 2COPY
```

Σε ορισμούς περιοδικών (recursive) αναφορών, κάθε μη-ορισμένη διαδικασία, πρέπει να αναφέρεται μοναδικά στο αριστερό τμήμα των σχέσεων. Στο παράδειγμα, ορίζεται από μια οικογένεια σχέσεων μια περιοχή προσωρινής μνήμης 2COPY, δύο θέσεων, η οποία δέχεται ως είσοδο την τιμή x από τον κανάλι in και στη συνέχεια η συμπεριφορά της δηλώνεται ως HOLDS(x). Η HOLDS(x), ορίζεται ως μια διαδικασία, η οποία δέχεται ως είσοδο την τιμή y από τον κανάλι in, στη συνέχεια παρέχει έξοδο την τιμή x, στο κανάλι out και η οποία στη συνέχεια θα συμπεριφέρεται ως HOLDS(y). Το τέλος της διαδικασίας ορίζεται με την έξοδο στο κανάλι out της τιμής x και την τελική συμπεριφορά της ως 2COPY.

2.5.1.2 Σημασιολογία ίχνους

Η σημασιολογία ίχνους (trace semantics) της CSP, επιτρέπει την αποτύπωση ως ίχνους μιας ακολουθίας γεγονότων και στη συνέχεια τη χρήση του ίχνους για τη μοντελοποίηση της συμπεριφοράς της.

Έστω το ίχνος $\tau\rho$, το οποίο αποτελεί την ακολουθία κάποιων γεγονότων. Το $\tau\rho$ είναι το ίχνος μιας διαδικασίας Π, αν κάποια εκτέλεση της Π αποτελείται ακριβώς από την ακολουθία των γεγονότων του ίχνους. Αυτό συμβολίζεται ως $\tau\rho \in traces(\Pi)$, όπου το $traces(\Pi)$ συμβολίζει το σύνολο όλων των πιθανών ιχνών της Π. Ένα παράδειγμα ίχνους θα μπορούσε να είναι το $<a,b>$, όπου το γεγονός β, ακολουθεί το γεγονός a. Για παράδειγμα, το ίχνος του παραδείγματος της προηγούμενης παραγράφου μπορεί να είναι το $\tau\rho = <in.7, out.7, in.5, in.8, out.5>$. Το $<>$, συμβολίζει το κενό ίχνος, ενώ η έκφραση a in $\tau\rho1$, συμβολίζει ότι το a, βρίσκεται σε κάποιο σημείο του ίχνους $\tau\rho1$.

Η συνένωση σε αλληλουχία δύο ιχνών $\tau\rho1$ και $\tau\rho2$ συμβολίζεται ως $\tau\rho1^\tau\rho2$. Η συνένωση αυτή θέτει σε αλληλουχία και τα γεγονότα των $\tau\rho1$ και $\tau\rho2$ (τα οποία ακολουθούν τα γεγονότα του $\tau\rho2$). Η έκφραση $<a>^\tau\rho'$, εκφράζει την ακολουθία του γεγονότος a, από το υπόλοιπο του ίχνους $\tau\rho$, όπου $\tau\rho' < \tau\rho$.

Το μήκος ενός ίχνους $\tau\rho$ συμβολίζεται ως $\#\tau\rho$ και εκφράζει τον αριθμό των γεγονότων από τα οποία αποτελείται. Για παράδειγμα το $\#<a,\beta,\gamma>=3$. Το σύνολο των γεγονότων ενός ίχνους $\tau\rho$, συμβολίζεται ως $\sigma(\tau\rho)$.

Η έκφραση $\tau\rho \lceil A$, συμβολίζει τη μέγιστη υπο-ακολουθία του $\tau\rho$, όλα τα γεγονότα της οποίας ανήκουν στο σύνολο A.

Η σημασιολογία ίχνους, μπορεί να χρησιμοποιηθεί για τον ορισμό χαρακτηριστικών ασφάλειας πρωτοκόλλων, με τη μορφή προδιαγραφών ίχνους. Αυτό υλοποιείται με τον ορισμό απαιτήσεων ασφάλειας και το έλεγχο των προδιαγραφών των ιχνών μιας διαδικασίας για το αν ικανοποιούν τις απαιτήσεις αυτές. Για παράδειγμα, για τη διαδικασία Π ορίζουμε τις απαιτήσεις ασφάλειας Σ και εκφράζουμε το παρακάτω:

$$\Pi \text{ sat } \Sigma \Leftrightarrow \forall\, \tau\rho \in traces(\Pi) \bullet \Sigma(\tau\rho).$$

Η έκφραση αυτή σημαίνει ότι η διαδικασία Π, ικανοποιεί (sat) τις απαιτήσεις Σ, αν και μόνο αν για κάθε ίχνος $\tau\rho$ το οποίο ανήκει στα ίχνη της Π, ισχύουν (•) οι απαιτήσεις ασφάλειας $\Sigma(\tau\rho)$.

Μια πιο σύνθετη και συχνά χρησιμοποιούμενη έκφραση για την επαλήθευση της ασφάλειας, είναι η ακόλουθη, όπου ορίζεται και το προβάδισμα (precedence) μιας ακολουθίας γεγονότων P από μια ακολουθία γεγονότων T:

$$\Pi \textbf{ sat } P \textbf{ precedes } T \Leftrightarrow \forall\, \tau\rho \in traces(\Pi) \bullet (\tau\rho \upharpoonright P \neq <> \Rightarrow \tau\rho \upharpoonright T \neq <>)$$

Σύμφωνα με την έκφραση αυτή, η διαδικασία Π ικανοποιεί (sat) το προβάδισμα (precedes) της ακολουθίας γεγονότων P από μια ακολουθία γεγονότων T, αν και μόνο αν για κάθε ίχνος $\tau\rho$ το οποίο ανήκει στα ίχνη της Π ισχύει (•) ότι η μέγιστη υπο-ακολουθία του $\tau\rho$, όλα τα γεγονότα της οποίας ανήκουν στο σύνολο P είναι διάφορη του κενού ίχνους και εν συνεχεία η μέγιστη υπο-ακολουθία του $\tau\rho$, όλα τα γεγονότα της οποίας ανήκουν στο σύνολο T είναι διάφορη του κενού ίχνους. Δηλαδή, μόνο αν εμφανιστεί γεγονός που ανήκει στην P εμφανίζεται γεγονός που ανήκει στην T.

Μια ακόμη συχνή έκφραση, είναι η ακόλουθη, η οποία αφορά στη σχέση εμπιστοσύνης δύο οντοτήτων και της κοινής κατοχής ενός κρυπτογραφικού κλειδιού:

SYSTEM **sat** running.B.A.k **precedes** doneA.B.k

Στην παραπάνω έκφραση, το σύστημα (SYSTEM) ικανοποιεί (sat), τη συνθήκη ότι το γεγονός running.A.B.k, που ορίζουμε ότι συμβολίζει τη λειτουργία ενός πρωτοκόλλου, όπου ο A, πιστοποιεί την ταυτότητα του B και συμφωνούν στο κλειδί k προηγείται της διαδικασίας χρήσης του k, μεταξύ των A και B.

2.5.1.3 Το μοντέλο δικτύου του Schneider

Ο Schneider πρότεινε τη μοντελοποίηση ενός πρωτοκόλλου ως ένα δίκτυο, όπου αλληλεπιδρά ένας αυθαίρετος αριθμός συμμετεχόντων οντοτήτων [159, 160]. Οι οντότητες αυτές μοντελοποιούνται ως διαδικασίες CSP οι οποίες εκτελούνται παράλληλα. Μοντελοποιείται επίσης μία ακόμη διαδικασία, η διαδικασία εισβολής, η οποία έχει

συγκεκριμένες δυνατότητες. Κατά την επαλήθευση της ασφάλειας ενός πρωτοκόλλου πρέπει να ληφθούν υπόψη όλες οι δυνατές επιθέσεις, πάντα σε συνάρτηση με το στόχο επαλήθευσης που έχει τεθεί. Επειδή η δοκιμή όλων των δυνατών επιθέσεων μπορεί να αποδειχθεί ιδιαίτερα πολύπλοκη υπόθεση, οι Dolev και Yao [158], για να καλύψουν την ανάγκη αυτή, όρισαν το Dolev-Yao μοντέλο, το οποίο περιγράφει ένα εχθρικό περιβάλλον από άποψη δυνατοτήτων του εισβολέα και όχι συγκεκριμένων επιθέσεων. Στο εχθρικό αυτό περιβάλλον, ο εισβολέας μπορεί να παρεμβληθεί στην επικοινωνία των διαφόρων οντοτήτων και να αλληλεπιδράσει με αυτές, μπλοκάροντας μηνύματα, επανεκπέμποντάς τα, αλλοιώνοντάς τα και πλαστοπροσωπώντας οντότητες, οι οποίες μπορεί να εμφανιστούν σε οποιοδήποτε κανάλι επικοινωνίας του δικτύου. Σύμφωνα με το μοντέλο του Schneider υπάρχει η δυνατότητα όλες οι οντότητες να επικοινωνούν μέσω της διαδικασίας εισβολής, ώστε η διαδικασία αυτή να αποκτήσει πλήρη έλεγχο του δικτύου.

Για την αναπαράσταση της εκπομπής και λήψης μηνυμάτων, ο Schneider χρησιμοποιεί δύο κανάλια επικοινωνίας, το send και receive αντίστοιχα. Τα κανάλια αυτά είναι δημόσια, μπορεί δηλαδή να χρησιμοποιηθούν για την αποστολή και λήψη μηνυμάτων από όλες τις διαδικασίες. Τα γεγονότα έχουν την ακόλουθη σύνταξη: `send.i.j.m`, όπου `m` είναι το μήνυμα, `i` είναι η πηγή και `j` ο προορισμός και `receive.i.j.m`, όπου `m` είναι το μήνυμα, `j` είναι η πηγή και `i` ο προορισμός.

Αν υποθέσουμε ότι O είναι το σύνολο των οντοτήτων του δικτύου και E είναι η διαδικασία – εισβολέας και για κάθε οντότητα $i \in O$ η διαδικασία CSP $USER_i$, συμβολίζει τη συμπεριφορά της οντότητας, τότε ορίζουμε το δίκτυο NET, ως:

$$NET = (|||_{i \in O} USER_i) \underset{\{send, receive\}}{||} E$$

όπου όλες οι οντότητες της O συγχρονίζονται με τον εισβολέα E για την αποστολή και λήψη μηνυμάτων μέσω των καναλιών `send` και `receive`.

Για τη μοντελοποίηση των δυνατοτήτων του εισβολέα κατά Dolev και Yao, ο Schneider, εισήγαγε τον τελεστή γέννησης $\vdash$, για να εκφράσει με ποιους ακριβώς τρόπους μπορούν να παραχθούν μηνύματα. Η σχέση $S \vdash m$ για παράδειγμα δηλώνει ότι το μήνυμα m μπορεί να

παραχθεί από το σύνολο μηνυμάτων S. Ο Schneider, όρισε τις τρεις ακόλουθες σχέσεις για τον τελεστή γέννησης:

- $m \in S$ τότε $S \vdash m$
- Αν $S \vdash m$ και $S \subseteq S'$ τότε $S' \vdash m$
- Αν $S \vdash mi$ για κάθε $mi \in S'$ και $S' \vdash m$ τότε $S \vdash m$.

Εν συνεχεία, ορίζεται ότι:

- $S \vdash m \wedge S \vdash k \Rightarrow S \vdash \{m\}k$
- $S \vdash \{m\}k \wedge S \vdash k \Leftrightarrow S \vdash m$
- $S \vdash m1 .m2 \Leftrightarrow S \vdash m1 \wedge S \vdash m2$
- $S \vdash m1 \wedge S \vdash m2 \Leftrightarrow S \vdash m1 .m2$.

Η χρήση του τελεστή μπορεί να επεκταθεί για τον ορισμό χαρακτηριστικών κρυπτογραφίας ή εξαγωγής μηνυμάτων. Επιπλέον μπορεί να συμβάλει στον πιο σαφή ορισμό κάποιων διαδικασιών. Για παράδειγμα, στην επόμενη έκφραση ορίζεται με μεγαλύτερη ακρίβεια η διαδικασία εισβολής:

$$Intruder(S) = send.i.j.m \rightarrow Intruder(S \cup \{m\})$$

$$\Omega$$

$$_{i,j \in U, S,m}\ receive.i.j.m \rightarrow Intruder(S)$$

Η παραπάνω έκφραση, ορίζει ότι η διαδικασία εισβολής παραμετροποιείται από ένα σύνολο μηνυμάτων S, τα οποία είναι στην κατοχή του εισβολέα (ο οποίος σύμφωνα με τα παραπάνω μπορεί να παρεμβάλλεται ως ενδιάμεση οντότητα μεταξύ δύο άκρων επικοινωνίας). Η διαδικασία ορίζεται σα να έχει δύο επιλογές:

- Η πρώτη σχέση αναπαριστά την εκπομπή μηνύματος m από την οντότητα i στην οντότητα j, μετά το πέρας της οποίας η διαδικασία εισβολής κατέχει το μήνυμα m.
- Στη δεύτερη σχέση, ο εισβολέας μπορεί να στείλει το μήνυμα m στην οντότητα i, προσποιούμενος την οντότητα j (επίθεση πλαστοπροσωπίας). Τελικά, η διαδικασία εισβολής παραμένει με την ίδια γνώση S.

Έτσι ο εισβολέας έχει τη δυνατότητα να συλλέξει γνώση για το δίκτυο ή να εξαπολύσει κάποια επίθεση πλαστοπροσωπίας. Η αρχική γνώση που συλλέγει ο εισβολέας συμβολίζεται με $\mathrm{In}K$ (Initial Knowledge).

2.5.1.4 Συναρτήσεις κατάταξης

Ας υποθέσουμε ότι U είναι ένα σύνολο ταυτοτήτων κάποιων οντοτήτων σε ένα δίκτυο, N είναι ένα σύνολο μοναδιαίων τιμών και K ένα σύνολο κρυπτογραφικών κλειδιών. Το σύνολο όλων των ατόμων ορίζεται ως A, όπου $A = U \cup N \cup K$. Ορίζουμε επίσης ως M, το σύνολο όλων των πιθανών μηνυμάτων τα οποία μπορεί να ανταλλαχθούν κατά τη λειτουργία του πρωτοκόλλου, έτσι ώστε $m \in A \Rightarrow m \in M$. Ο Schneider ορίζει ως συνάρτηση κατάταξης (rank function) ρ την αντιστοίχιση γεγονότων σε ακέραιους αριθμούς. Το σύνολο των μηνυμάτων χωρίζεται τότε σε δύο μέρη:

$$M_{\rho^-} = \{m \in M \mid \rho(m) < 0\} \qquad M_{\rho^+} = \{m \in M \mid \rho(m) > 0\}$$

Ο σκοπός αυτής της διάτμησης των μηνυμάτων είναι η διάκριση σε μηνύματα τα οποία μπορεί να αποκτήσει ο εισβολέας χωρίς επιπτώσεις ασφάλειας για το πρωτόκολλο και να οποία λαμβάνουν θετικό συντελεστή κατάταξης και σε μηνύματα τα οποία αν αποκτηθούν δημιουργείται διάρρηξη στην ασφάλεια του πρωτοκόλλου και τα οποία λαμβάνουν μη-θετικό συντελεστή κατάταξης. Από τα παραπάνω συμπεραίνουμε πως είναι επιθυμητό για μια διαδικασία να μην εκπέμψει ποτέ μήνυμα μη-θετικού συντελεστή κατάταξης και τα διατηρήσει θετική κατάταξη. Σύμφωνα με τη θεωρία η μη εκπομπή μηνύματος μη-θετικής κατάταξης συντελείται, εκτός αν προηγουμένως η διαδικασία έχει λάβει τέτοιο μήνυμα, ανεξαρτήτως αποστολέα. Αυτό για τη διαδικασία P εκφράζεται ως εξής:

$$P \textbf{ maintains } \rho \Rightarrow \forall\, tr \in traces(P) \bullet \rho(tr \Downarrow receive) > 0 \Rightarrow \rho(tr \Downarrow send) > 0$$

Ο Schneider παρουσίασε το θεώρημα συναρτήσεων κατάταξης (rank function theorem) το οποίο εξασφαλίζει ότι τα μηνύματα τα οποία αποκτά ο εισβολέας δεν παραβιάζουν την ασφάλεια του πρωτοκόλλου. Για να ισχύει ένα τέτοιο θεώρημα, καθώς τα κανάλια επικοινωνίας είναι δημόσια και πιθανώς υπό τον έλεγχο του εισβολέα, κάθε μήνυμα που διακινείται σε αυτά θα πρέπει να έχει θετικό συντελεστή κατάταξης. Αν ένα μήνυμα με μη-

θετικό συντελεστή περάσει μέσα από τα κανάλια επικοινωνίας, τότε η ασφάλεια του πρωτοκόλλου παρουσιάζει κενό που μπορεί να οδηγήσει στην παραβίασή της. Με τον παραπάνω συλλογισμό συντελείται και η επαλήθευση της ασφάλειας ενός πρωτοκόλλου. Το θεώρημα συναρτήσεων κατάταξης του Schneider, ορίζεται ως εξής:

Θεώρημα

Αν για τα σύνολα R και T, η συνάρτηση κατάταξης είναι η $\rho: M \to '$

τότε: NET sat R precedes T, δηλαδή το δίκτυο ικανοποιεί ότι η R προηγείται της T,

αν ικανοποιούνται οι παρακάτω συνθήκες:

- **Συνθήκη 1:** $\forall\ m \in IK \bullet \rho(m) > 0$

  Η συνθήκη αυτή υπαγορεύει ότι ο εισβολέας ξεκινά πάντα με μηνύματα θετικού συντελεστή κατάταξης.

- **Συνθήκη 2:** $\forall\ S \subseteq M,\ m \in M \bullet ((\forall m' \in S \bullet \rho(m') > 0) \wedge S \vdash m) \Rightarrow \rho(m) > 0$

  Η συνθήκη αυτή υπαγορεύει ότι ο εισβολέας μπορεί να παράγει μόνο μηνύματα θετικού συντελεστή κατάταξης, εκτός αν ήδη έχει υπό την κατοχή του μήνυμα μη θετικού συντελεστή κατάταξης.

- **Συνθήκη 3:** $\forall\ t \in T \bullet \rho(t) < 0$

  Η συνθήκη αυτή υπαγορεύει ότι κανένα γεγονός στο σύνολο T δεν έχει μήνυμα θετικού συντελεστή κατάταξης

- **Συνθήκη 4:** $\forall\ i \in U \bullet User_i \underset{R}{\|} Stop$ **maintains** ρ

Η συνθήκη αυτή υπαγορεύει ότι για κάθε χρήστη όταν σε αυτόν δεν επιτρέπονται γεγονότα από το σύνολο R, ισχύει ότι ο χρήστης αυτός διατηρεί θετικό ρ, δηλαδή όσο αποστέλλει μηνύματα θετικού συντελεστή κατάταξης, δέχεται τέτοια μηνύματα.

Το θεώρημα ορίζει ότι αν μια συνάρτηση κατάταξης ικανοποιεί τις τέσσερις παραπάνω σχέσεις, τότε κανένα μήνυμα μη-θετικού συντελεστή κατάταξης δεν μπορεί να διακινηθεί στο δίκτυο. Πιο συγκεκριμένα, ο εισβολέας δεν θα είναι σε θέση να παραβιάσει την ασφάλεια του πρωτοκόλλου, έχοντας τόσο την αρχική του γνώση InK, όσο και τη γνώση που αποκτά κατά

τη διάρκεια της λειτουργίας του πρωτοκόλλου, η οποία αντιστοιχεί στο σύνολο S. Επίσης, οι νόμιμες οντότητες του πρωτοκόλλου δε θα μπορούν να παράγουν μη νόμιμα μηνύματα, αν πρώτα δεν έχουν σταλεί τέτοιου είδους μηνύματα σε αυτές, δηλαδή κάθε νόμιμη διαδικασία διατηρεί το ρ της όσο περιορίζεται στο R.

Η επαλήθευση των συνθηκών του θεωρήματος πρέπει να γίνεται για κάθε συνάρτηση κατάταξης που ανήκει στο πρωτόκολλο. Η επαλήθευση διαφορετικών απαιτήσεων ασφάλειας μπορεί να απαιτεί τη δημιουργία περισσότερων της μίας συναρτήσεων κατάταξης για το ίδιο πρωτόκολλο, καθώς διαφορετικά γεγονότα του δικτύου μπορεί να ανταποκρίνονται σε διαφορετικές απαιτήσεις, δηλαδή τα σύνολα R και T να περιέχουν διαφορετικά γεγονότα για διαφορετικά σενάρια. Οι εργασίες του Schneider για τη μελέτη ασφάλειας πρωτοκόλλων έχουν βρει ευρεία εφαρμογή στην αξιολόγηση της ασφάλειας πρωτοκόλλων [157, 162, 163, 164, 165, 166, 167, 168].

2.5.2 Θεωρια Παιγνιων και Αποστροφη Ρισκου

Στην παράγραφο αυτή παρουσιάζονται βασικές γνώσεις της θεωρίας παιγνίων (game theory), η οποία στη συνέχεια χρησιμοποιείται για τους σκοπούς της διατριβής. Η θεωρία παιγνίων είναι ένα σύνολο εφαρμοσμένων μαθηματικών μοντέλων τα οποία χρησιμοποιούνται για τη μελέτη αλληλεπιδράσεων συνεργασίας ή ανταγωνισμού, ή αλλιώς για τη μελέτη της συμπεριφοράς των παικτών σε ένα παίγνιο και τις καλύτερες στρατηγικές αυτών [196]. Η θεωρία παιγνίων έχει εφαρμογή σε διάφορα επιστημονικά πεδία, όπως για παράδειγμα στα οικονομικά, στην πληροφορική [199, 200], στη βιολογία και στις πολιτικές επιστήμες.

Τα θεμέλια της θεωρίας παιγνίων, τέθηκαν με τη δημοσίευση της εργασίας "Researches into the Mathematical Principles of the Theory of Wealth" του Augustin Cournot. Η θεωρία παιγνίων εγκαθιδρύθηκε ως επιστημονικό πεδίο από τον John von Neumann το 1944 με τη δημοσίευση του βιβλίου *"The Theory of Games and Economic Behavior"*, την οποία έγραψε σε συνεργασία με τον Oskar Morgenstern. Το 1950 ο John Nash εισήγαγε την αρχή της ισορροπίας Nash (Nash equilibrium), αποδεικνύοντας ότι οι καλύτερες απαντήσεις όλων των παικτών ενός παιγνίου είναι σε συμφωνία μεταξύ τους [197].

Ένα παίγνιο στην κανονική του μορφή (*normal form game*) συνδυάζει ένα σύνολο πιθανών στρατηγικών για κάθε παίκτη και καταγράφει την απόδοση κάθε αποτελέσματος. Τα παίγνια κανονικής μορφής λέγονται και στατικά (static) παίγνια, διότι οι κινήσεις των παικτών είναι ταυτόχρονες. Αν N είναι ένα σύνολο παικτών, i κάθε παίκτης, Σ^i το σύνολο των στρατηγικών του παίκτη και το R^N σύνολο των αποδόσεων, τότε το παίγνιο ορίζεται ως:

$$\pi: \prod_{i \in N} \Sigma^i \to R^N$$

Οι πιο κοινές κατηγορίες παιγνίων είναι τα παίγνια μηδενικού αθροίσματος (zero sum), όπου το συνολικό κέρδος όλων των παικτών είναι μηδέν (δηλαδή οι παίκτες κερδίζουν εις βάρος των άλλων παικτών) και τα παίγνια μη μηδενικού αθροίσματος, όπου το σύνολο των κερδών μπορεί να είναι θετικό ή αρνητικό. Η μήτρα απόδοσης (payoff matrix) ενός παιγνίου αποτελεί ένα μέσο αναπαράστασης της απόδοσης της στρατηγικής των παικτών. Σε μία μήτρα απόδοσης παρουσιάζονται οι πιθανές στρατηγικές κάθε παίκτη και για κάθε συνδυασμό των παιγνίων αυτών καταγράφεται το κέρδος ή απώλειες του καθενός.

Από τη μήτρα απόδοσης, γίνονται επίσης φανερές οι ισορροπίες Nash. Οι ισορροπίες Nash υπολογίζονται ως εξής:

- αναζήτηση του μεγαλύτερου κέρδους σε ένα σύνολο κινήσεων ενός παίκτη
- λαμβάνοντας ως δεδομένη την κίνηση με το μεγαλύτερο κέρδος του παίκτη αυτού, αναζητούμε την κίνηση του άλλου παίκτη η οποία επιφέρει στον τελευταίο το μεγαλύτερο κέρδος.

Για πιο σύνθετα παίγνια είναι εφικτή η χρήση δενδροειδών διαγραμμάτων για την αναπαράσταση του συνδυασμού των πιθανών στρατηγικών των παικτών, οπότε και ορίζουμε το παίγνιο ως *αναλυτικής μορφής (extensive form game)*. Τα παίγνια αυτά ονομάζονται και δυναμικά (dynamic) παίγνια, διότι οι κινήσεις γίνονται σειριακά και η κίνηση του ενός παίκτη μπορεί να επηρεάσει την επιλογή του άλλου.

Τα παίγνια μπορούν επίσης να διακριθούν σε παίγνια συνεργασίας (cooperative) και σε παίγνια μη συνεργασίας (non-cooperative), όπου οι παίκτες μάχονται για τον ίδιο στόχο που θα τους αποφέρει κοινά κέρδη ή όχι αντίστοιχα.

Μία ακόμη έννοια που αφορά σε παίγνια και προέρχεται από οικονομικές επιστήμες είναι η έννοια της αποστροφής ρίσκου (risk aversion) [198]. Σύμφωνα με τη σχετική θεωρία, υπάρχουν τριών ειδών συμπεριφορές παίκτη:

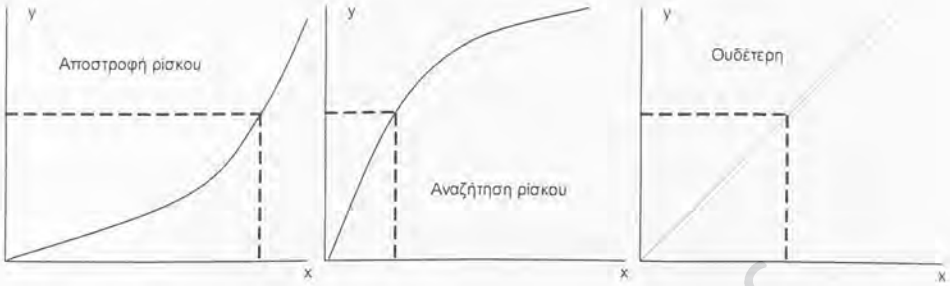
- η συμπεριφορά αποστροφής ρίσκου
- η συμπεριφορά αναζήτησης ρίσκου
- η ουδέτερη συμπεριφορά.

Η πρώτη συμπεριφορά αντιστοιχεί σε παίκτες οι οποίοι δεν παίρνουν ρίσκο και προτιμούν να επενδύσουν προς αυτή την κατεύθυνση, δηλαδή να μειώσουν το τελικό τους κέρδος έτσι ώστε να το κάνουν περισσότερο σίγουρο. Παράδειγμα τέτοιας συμπεριφοράς είναι η επιλογή ασφάλισης κάποιας περιουσίας, η οποία αφενός έχει κόστος, αφετέρου την προστατεύει.

Η δεύτερη συμπεριφορά αφορά αντιστοιχεί σε παίκτες που ρισκάρουν με στόχο το μέγιστο δυνατό κέρδος και επενδύουν στο ρίσκο αυτό με ποσά που οι πρώτοι παίκτες δε θα επένδυαν. Το αποτέλεσμα αυτής της συμπεριφοράς είναι πιο ασταθές και απρόβλεπτο από αυτό της προηγούμενης συμπεριφοράς.

Η ουδέτερη συμπεριφορά είναι μια ενδιάμεση συμπεριφορά μεταξύ των δύο παραπάνω, όπου το στοιχείο του ρίσκου είναι μειωμένο, όπως και οι επενδύσεις κατά του στοιχείου αυτού.

Αν ορίσουμε την συνάρτηση $y=f(x)$, η οποία εκφράζει το τελικό κέρδος, ως συνάρτηση της επένδυσης που κάνει ο παίκτης σε μία ασφάλιση περιουσίας, τότε σύμφωνα με τη θεωρία, η συνάρτηση είναι κυρτή αν ο παίκτης υιοθετεί συμπεριφορά αποστροφής ρίσκου, κοίλη αν υιοθετεί συμπεριφορά αναζήτησης ρίσκου και ευθεία αν υιοθετεί ουδέτερη συμπεριφορά. Τα παραπάνω παρουσιάζονται στο Σχήμα 25.



Σχήμα 25: Συμπεριφορές αποστροφής ρίσκου, αναζήτησης ρίσκου και ουδέτερη συμπεριφορά

Στα διαγράμματα, παρατηρούμε τις διακεκομμένες γραμμές, οι οποίες ορίζουν το ισοδύναμο βεβαιότητας (certainty equivalent). Το ισοδύναμο βεβαιότητας έχει το νόημα, ότι αν υπήρχε 50% πιθανότητα να συμβεί ένα αρνητικό περιστατικό με επιπτώσεις στην περιουσία του παίκτη, τότε ο πρώτος παίκτης θα επένδυε περισσότερα ώστε να είναι σίγουρος (πιθανώς κάποιο σε κάποιο είδος ασφάλισης), ο δεύτερος λιγότερα ρισκάροντας και ο τρίτος θα έκανε μία ενδιάμεση επένδυση. Τονίζεται ότι τα παραπάνω διαγράμματα σε περίπτωση εξέτασης εφαρμογών τυχερών παιγνίων, είναι αντεστραμμένα.

2.5.3 Μεθοδολογια Αναλυσης Πολλαπλων Κριτηριων

Η μεθοδολογία Ανάλυσης Πολλαπλών Κριτηρίων (Multi-Criteria Analysis - MCA), χρησιμοποιείται για την αξιολόγηση διαφορετικών οντοτήτων βάσει κριτηρίων και την κατηγοριοποίηση αυτών βάσει μιας ποσοτικής κλίμακας [14]. Η μεθοδολογία λαμβάνει υπόψη της ότι κάποια κριτήρια πιθανώς έχουν περισσότερη σημασία κατά τη διαδικασία της αξιολόγησης από κάποια άλλα, για το λόγο αυτό χρησιμοποιεί συντελεστές βαρύτητας των κριτηρίων.

Τα παρακάτω βήματα αποτελούν τη μεθοδολογία Ανάλυσης Πολλαπλών Κριτηρίων:

i. Επιλογή κριτηρίων: Επιλέγονται τα κατάλληλα κριτήρια, ανάλογα με το είδος των οντοτήτων που θέλουμε να συγκρίνουμε.
ii. Εισαγωγή βαθμών αξιολόγησης: Αξιολογούμε κάθε οντότητα ανά κριτήριο.

iii. Εισαγωγή συντελεστών βαρύτητας (ΣΒ): Εισάγουμε συντελεστές βαρύτητας, για να διακρίνουμε τα κριτήρια

Το Σχήμα 26 συνοψίζει τα τρία πρώτα βήματα της μεθοδολογίας για μια οντότητα Α.

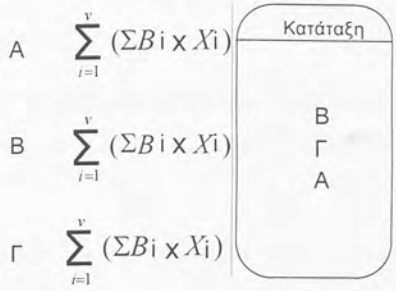
Βήμα 1	Βήμα 2	Βήμα 3
K1	Βαθμολόγηση Α στο Κ1	ΣΒ1*Βαθμός Α στο Κ1
K2	Βαθμολόγηση Α στο Κ2	ΣΒ2*Βαθμός Α στο Κ2
K3	Βαθμολόγηση Α στο Κ3	ΣΒ3*Βαθμός Α στο Κ3

Σχήμα 26: Τα τρία πρώτα βήματα της μεθοδολογίας Ανάλυσης Πολλαπλών Κριτηρίων: *κριτήρια, βαθμοί* και *συντελεστές βαρύτητας*

iv. Κατάταξη οντοτήτων: είναι μια απλή υπο-μέθοδος της μεθοδολογίας Ανάλυσης Πολλαπλών Κριτηρίων, η οποία χρησιμοποιεί τα γινόμενα των συντελεστών βαρύτητας με τους βαθμούς ανά κριτήριο και υπολογίζει το άθροισμα αυτών των γινομένων για κάθε οντότητα. Αν Χ είναι η εκάστοτε οντότητα, Χι είναι ο βαθμός της ανά κριτήριο (ι= 1,2,3,...ν) και ΣΒι είναι ο συντελεστής βαρύτητας κάθε κριτηρίου, τότε υπολογίζεται για κάθε οντότητα, το παρακάτω άθροισμα:

$$\sum_{i=1}^{v}(\Sigma B_i \times X_i)$$

Τα παραπάνω, παρουσιάζονται στο Σχήμα 27, για τρείς οντότητες Α, Β, Γ.



Σχήμα 27: Μοντέλο κατάταξης αδυναμιών ασφάλειας

Οι οντότητες κατατάσσονται ανάλογα με τη βαθμολογία τους. Για πιο σύνθετους υπολογισμούς η μεθοδολογία προτείνει την εισαγωγή ενός συντελεστή απόκλισης, ώστε να είναι δυνατός ο υπολογισμός της βεβαιότητας κάθε αποτελέσματος.

ΚΕΦΑΛΑΙΟ 3: ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ ΣΤΗΝ ΕΡΕΥΝΗΤΙΚΗ ΠΕΡΙΟΧΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΑΥΤΟΤΗΤΑΣ ΧΡΗΣΤΗ

3.1 ΕΙΣΑΓΩΓΗ

Η λύση που περιγράφεται στην παρούσα ενότητα, αντιμετωπίζει τα ανοικτά προβλήματα που περιγράφηκαν στην ενότητα 1.2.1.1.3: Σύνοψη προβλημάτων διαχείρισης ταυτότητας χρήστη.

Η προτεινόμενη λύση χωρίζεται σε τρία μέρη, όσα και τα παρουσιασθέντα ανοικτά προβλήματα αντιμετωπίζοντάς τα ένα προς ένα. Συνολικά, προτείνονται τα παρακάτω:

- Ένας μηχανισμός αποτίμησης επικινδυνότητας για βιομετρικά συστήματα, με στόχο την ασφαλή ενσωμάτωσή τους σε οποιαδήποτε αρχιτεκτονική ασφάλειας.
- Ένα νέο πρωτόκολλο ενσωμάτωσης βιομετρικών σε μία αρχιτεκτονική 3ης γενιάς και 3G/WLAN, με στόχο την ισχυρή πιστοποίηση χρήστη και επομένως τη βελτίωση της ασφάλειας των μηχανισμών πρόσβασης σε επίπεδο δικτύου.
- Ένα νέο ασφαλές και πιο αποτελεσματικό από άποψη απόδοσης πρωτόκολλο διαχείρισης ταυτότητας χρηστών 3ης και 4ης γενιάς, σε φορείς παροχής υπηρεσιών στο Διαδίκτυο.

3.2 ΣΥΣΤΗΜΑ ΑΠΟΤΙΜΗΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.2.1 ΓΕΝΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Η προτεινόμενη λύση αντιμετωπίζει το παρακάτω πρόβλημα, όπως αναλύθηκε προηγουμένως:

Δεν υπάρχει μοντέλο αποτίμησης επικινδυνότητας για βιομετρικά συστήματα, ώστε να είναι εφικτή η ασφαλής ενσωμάτωση αυτών σε ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς αλλά και σε οποιαδήποτε άλλη αρχιτεκτονική, με στόχο την υλοποίηση ισχυρής πιστοποίησης, βελτιστοποιώντας την ασφάλεια των υπαρχόντων μηχανισμών πρόσβασης σε επίπεδο δικτύου.

Για τη δημιουργία του συστήματος αποτίμησης επικινδυνότητας βιομετρικών συστημάτων, χρησιμοποιήθηκε αρχικά ένα γενικό μοντέλο αποτίμησης επικινδυνότητας πληροφοριακών συστημάτων. Το μοντέλο αυτό περιγράφεται στη σύγχρονη βιβλιογραφία και επιλέχθηκε ώστε να επιτευχθεί η μέγιστη δυνατή συμβατότητα του συστήματος με τις υπάρχουσες μεθοδολογίες και τα σύγχρονα εργαλεία αποτίμησης επικινδυνότητας [11,12,13]. Το μοντέλο περιλαμβάνει τα ακόλουθα βήματα:

1. Καταγραφή πόρων.
2. Προσδιορισμός απειλών (ορίζοντας ως απειλή, ένα γεγονός με αρνητικές συνέπειες στο πληροφοριακό σύστημα).
3. Προσδιορισμός αδυναμιών (ορίζοντας ως αδυναμία, μια ατέλεια ασφάλειας του πληροφοριακού συστήματος).
4. Υπολογισμός επικινδυνότητας (ορίζοντας ως επικινδυνότητα, την πιθανότητα μια συγκεκριμένη απειλή να πραγματοποιηθεί μέσα από την εκμετάλλευση μιας συγκεκριμένης αδυναμίας του πληροφοριακού συστήματος).
5. Προσδιορισμός μέτρων ασφάλειας με στόχο τη μείωση της επικινδυνότητας.

Για κάθε ένα από τα βήματα του παραπάνω μοντέλου αποτίμησης επικινδυνότητας, αναζητήθηκαν οι ελλείψεις οι οποίες καθιστούν μεθοδολογίες και εργαλεία μη ικανές να ανταποκριθούν στις απαιτήσεις πληροφοριακών συστημάτων που περιλαμβάνουν βιομετρικά συστήματα.

Τα δύο πρώτα βήματα καλύπτονται πλήρως από τις υπάρχουσες μεθοδολογίες αποτίμησης επικινδυνότητας, καθώς αφορούν σε γενικές απαιτήσεις και όχι συγκεκριμένα σε βιομετρικά συστήματα.

Το τρίτο βήμα δηλώνει την ανάγκη ύπαρξης ενός **καταλόγου αδυναμιών** που αφορούν σε βιομετρικά συστήματα. Ο κατάλογος αυτός δημιουργήθηκε με:

- αναλυτική μελέτη στης βιβλιογραφίας και των καταγεγραμμένων περιστατικών ασφαλείας,
- πειραματική μελέτη κάποιων αδυναμιών,

- αλληλεπίδραση με ειδικούς στο χώρο των βιομετρικών συστημάτων σε παγκόσμια κλίμακα.

Ο κατάλογος, έλαβε υπόψη του τη μεθοδολογία BEM των Common Criteria (CC) [149], καθώς και τα επίσημα προφίλ αξιολόγησης [151, 152], με αποτέλεσμα τη συμβατότητα του αποτελέσματος της μεθοδολογίας με αυτά.

Το τέταρτο βήμα μπορεί να υλοποιηθεί με ποικίλες μεθόδους. Μια δοκιμασμένη και αποτελεσματική πρακτική για την υλοποίηση του προσδιορισμού της επικινδυνότητας, είναι ο συνδυασμός πληροφοριών σχετικά με το σύστημα, με προ-επιλεγμένους παράγοντες επικινδυνότητας ανά αδυναμία συστήματος [9]. Το άθροισμα των παραγόντων επικινδυνότητας κάθε αναγνωρισμένης αδυναμίας οδηγεί στον προσδιορισμό της συνολικής επικινδυνότητας του συστήματος. Ο παράγοντας επικινδυνότητας κάποιας συγκεκριμένης αδυναμίας του συστήματος υπολογίζεται από την ευκολία εκμετάλλευσης της συγκεκριμένης αδυναμίας και την αποτελεσματικότητα της αδυναμίας αυτής στο να οδηγήσει στην πραγματοποίηση κάποιας απειλής.

Για κάθε αδυναμία που περιλαμβάνεται στον **κατάλογο αδυναμιών**, πρέπει να υπολογιστεί ένας παράγοντας επικινδυνότητας. Για το σκοπό αυτό, χρησιμοποιήθηκε η μεθοδολογία **Ανάλυσης Πολλαπλών Κριτηρίων (Multi-criteria Analysis – MCA)**.

Το τελευταίο βήμα, αφορά στον προσδιορισμό των μέτρων ασφάλειας και υλοποιήθηκε ως επέκταση της έρευνας των αδυναμιών με όμοια προσέγγιση.

Το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων, αποτελείται από μια βάση γνώσης που περιλαμβάνει τον **κατάλογο αδυναμιών**, τους **παράγοντες επικινδυνότητας** που σχετίζονται με κάθε αδυναμία του καταλόγου και τα **μέτρα ασφάλειας** που προτείνονται για τη μείωση της επικινδυνότητας του συστήματος.

3.2.2 Εφαρμογη Μεθοδολογιας Αναλυσης Πολλαπλων Κριτηριων

Οι οντότητες στην προκειμένη περίπτωση είναι οι αδυναμίες των βιομετρικών συστημάτων και η αξιολόγηση γίνεται ως προς την πιθανότητα εμφάνισής τους, με στόχο τον προσδιορισμό του παράγοντα επικινδυνότητας αυτών.

Τα παρακάτω βήματα εφαρμόστηκαν βάσει της μεθοδολογίας Ανάλυσης Πολλαπλών Κριτηρίων:

i. Επιλογή κριτηρίων: Μελέτη του προφίλ επιθέσεων σε πληροφοριακά συστήματα, οδήγησε στην επιλογή τριών κριτηρίων [174]. Τα κριτήρια εν συντομία δικαιολογούν μια απλή παρατήρηση, ότι δηλαδή η εκμετάλλευση κάποιας αδυναμίας είναι συχνότερη, όταν είναι εύκολα υλοποιήσιμη, αποτελεσματική και μη δαπανηρή σε συνάρτηση με το στόχο. Τα κριτήρια είναι τα ακόλουθα:
   - K_1: Δυσκολία εκμετάλλευσης της αδυναμίας, από άποψη απαιτούμενων εξειδικευμένων γνώσεων και πολυπλοκότητας.
   - K_2: Αποτελεσματικότητα επίθεσης.
   - K_3: Κόστος (για παράδειγμα του απαιτούμενου εξοπλισμού).

ii. Εισαγωγή βαθμών αξιολόγησης: Κάθε αδυναμία βαθμολογήθηκε μετά από σχετική μελέτη, για κάθε κριτήριο. Χρησιμοποιήθηκε ποσοτική κλίμακα από μηδέν ως δέκα. Συγκεκριμένα:
   - K_1: Ο υψηλότερος βαθμός (10) αντιστοιχεί στην χαμηλότερη δυσκολία υλοποίησης.
   - K_2: Ο υψηλότερος βαθμός (10) αντιστοιχεί στη μέγιστη αποτελεσματικότητα.
   - K_3: Ο υψηλότερος βαθμός (10) αντιστοιχεί στο μικρότερο κόστος.

iii. Εισαγωγή συντελεστών βαρύτητας (Σ): Μελέτη του προφίλ του σύγχρονου εισβολέα σε πληροφοριακά συστήματα, ανέδειξε ίσους συντελεστές και για τα τρία κριτήρια, χωρίς να διακρίνει κάποιο.

iv. Κατάταξη αδυναμιών: Χρησιμοποιήθηκε η υπο-μέθοδος της μεθοδολογίας Ανάλυσης Πολλαπλών Κριτηρίων (περιγράφηκε στη σχετική παράγραφο), η οποία παίρνει τα γινόμενα των συντελεστών βαρύτητας με τους βαθμούς ανά κριτήριο και υπολογίζει το άθροισμα αυτών για κάθε αδυναμία του συστήματος.

3.2.3 ΠΑΡΟΥΣΙΑΣΗ ΣΥΣΤΗΜΑΤΟΣ

3.2.3.1 Κατάλογος αδυναμιών και προτεινόμενων μέτρων ασφάλειας

Τα σύγχρονα βιομετρικά συστήματα, εμφανίστηκαν πριν από περίπου τρεις δεκαετίες. Η τεχνολογία των βιομετρικών συστημάτων έχει εξελιχθεί σε μεγάλο βαθμό, αλλά κάποια προβλήματα παραμένουν. Μερικά σημαντικά ζητήματα, αφορούν στην τεχνολογία των βιομετρικών αισθητήρων, στο αν χρησιμοποιείται κεντρική ή διανεμημένη αποθήκευση των βιομετρικών υπογραφών, στο αν ο αλγόριθμος σύγκρισης είναι ενσωματωμένος ή όχι στο υπόλοιπο σύστημα, στον τρόπο επικοινωνίας των διαφόρων συστατικών του βιομετρικού και στο πώς είναι υλοποιημένη η διαδικαστική ασφάλεια για τη χρήση του συστήματος [143]. Λάθος υλοποίηση σε κάποιο από τα παραπάνω, οδηγεί σε ευπάθειες που εκθέτουν το σύστημα σε σημαντικούς κινδύνους. Ο Πίνακας 1 αναφέρει τις κατηγορίες των αδυναμιών των βιομετρικών συστημάτων.

Πίνακας 1: Κατηγορίες αδυναμιών βιομετρικών συστημάτων

No.	Τίτλος
1.	Αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης.
2.	Κληρονομήσιμες αδυναμίες κεντρικοποιημένων αρχιτεκτονικών - πλαστές βιομετρικές υπογραφές.
3.	Αδυναμία ασφάλειας μετάδοσης - υποκλοπή σήματος και επανεκπομπή.
4.	Αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών.
5.	Αδυναμία προστασίας ακεραιότητας συστατικών του συστήματος.
6.	Διαδικαστικές αδυναμίες - διαχείριση βιομετρικών δεδομένων και υπογραφών.
7.	Αδυναμίες σε θόρυβο και λειτουργία εκτός των επιτρεπόμενων ορίων:
8.	Αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής.
9.	Αδυναμία αναγνώρισης εναπομένοντος χαρακτηριστικού.
10.	Αδυναμίες διάκρισης παρόμοιων βιομετρικών υπογραφών.
11.	Αδυναμίες σε επιθέσεις ωμής δύναμης.
12.	Αδυναμίες στο σύστημα διαχείρισης ταυτότητας.

Στη συνέχεια, παρουσιάζεται ένας αναλυτικός κατάλογος αδυναμιών που αφορούν σε βιομετρικά συστήματα:

3.2.3.1.1 Αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης

Περιγραφή: Ένα από τα σημαντικότερα προβλήματα στο χώρο είναι η δυνατότητα του συστήματος να ξεχωρίσει ένα πραγματικό χαρακτηριστικό από ένα αντίγραφο. Το πρόβλημα αυτό εμφανίζεται πολύ έντονο στη βιομετρική μέθοδο που έχει τη μεγαλύτερη ιστορία και το συντριπτικό μερίδιο στην αγορά, αυτό της αναγνώρισης δακτυλικών αποτυπωμάτων. Πρόσφατα πειράματα έδειξαν ότι σύγχρονα βιομετρικά είναι εύκολο να εξαπατηθούν από αντίγραφα δακτυλικών αποτυπωμάτων [114, 115, 148]. Τα τεχνητά δακτυλικά αποτυπώματα είναι σχετικά εύκολο να δημιουργηθούν από πυρίτιο ή ζελατίνη, με μία διαδικασία που διαρκεί από μερικές ώρες ως το πολύ μερικές μέρες. Ακόμα πιο εύκολη είναι η ανεύρεση και συλλογή των δακτυλικών αποτυπωμάτων ενός χρήστη (για παράδειγμα από γυάλινες επιφάνειες). Τα βιομετρικά συστήματα δείχνουν αδύναμα σε τέτοιου είδους επιθέσεις, κυρίως διότι τόσο η επιδερμίδα όσο και το πυρίτιο είναι νεκρά υλικά. Παρόμοια ευπαθή σημεία χαρακτηρίζουν και άλλες βιομετρικές τεχνικές. Εξελιγμένα συστήματα σύνθεσης ομιλίας, μπορούν να ξεγελάσουν τα βιομετρικά αναγνώρισης φωνής. Φωτογραφίες προσώπου και εικόνες ίριδας ξεγελούν συστήματα αναγνώρισης προσώπου και ίριδας αντίστοιχα.

Μέτρα ασφάλειας: Η επιστημονική κοινότητα έρευνας και ανάπτυξης βιομετρικών συστημάτων, είναι πλέον απασχολημένη με την ανάπτυξη ενός υποσυστήματος ανίχνευσης ζωτικότητας. Το υποσύστημα αυτό βασίζεται στη μέτρηση μερικών επιπλέον χαρακτηριστικών, όπως η σχετική διηλεκτρική σταθερά, η αγωγιμότητα, οι καρδιακοί παλμοί, η ελαστικότητα του δέρματος, ή η ροή του οξυγονωμένου αίματος. Η υλοποίηση του υποσυστήματος ανίχνευσης ζωτικότητας βρίσκεται ήδη σε τελικά στάδια από αρκετούς κατασκευαστές. Η ανίχνευση ζωτικότητας για τις βιομετρικές αναγνώρισης προσώπου και ίριδας, υλοποιείται αντίστοιχα με την ανάπτυξη βιομετρικών εξελιγμένης αναγνώρισης τρισδιάστατης κίνησης προσώπου και με εξελιγμένους ανιχνευτές της τυχαίας συστολής και διαστολής της κόρης του ματιού που δεν οφείλεται σε εξωτερικά ερεθίσματα [125, 126]. Η χρήση αλληλεπιδραστικών συστημάτων που ζητούν συγκεκριμένη συμπεριφορά από το χρήστη αποτελεί μια συμπληρωματική λύση για όλες τις μεθόδους, ενώ η δημιουργία συνδυασμένων βιομετρικών συστημάτων που μετρούν ταυτόχρονα δύο χαρακτηριστικά

(π.χ. πρόσωπο και κίνηση χειλιών κατά την ομιλία) είναι περισσότερο ανθεκτική σε αυτού του είδους τις επιθέσεις, διότι αυξάνει την απαιτούμενη πολυπλοκότητα για την εξαπάτηση του συστήματος [116].

3.2.3.1.2 Κληρονομήσιμες αδυναμίες κεντρικοποιημένων αρχιτεκτονικών - πλαστές βιομετρικές υπογραφές

Περιγραφή: Αν η βιομετρική υπογραφή είναι αποθηκευμένη σε κάποια κεντρική βάση δεδομένων, μια επίθεση στη βάση και ταυτόχρονη αντικατάσταση της βιομετρικής υπογραφής του χρήστη με αυτή του επιτιθέμενου δίνει πρόσβαση στον δεύτερο με το όνομα του πρώτου. Η αδυναμία αυτή αφορά κυρίως στα ευπαθή σημεία τα οποία κληρονομεί το σύστημα όταν επιλέγονται κεντρικοποιημένες αρχιτεκτονικές [127].

Μέτρα ασφάλειας: Οι βιομετρικές υπογραφές είναι ευαίσθητα προσωπικά δεδομένα τα οποία πρέπει να προστατεύονται με ισχυρά μέτρα ασφάλειας [153]. Όταν η απαίτηση για κεντρικοποιημένη αρχιτεκτονική είναι αναπόφευκτη, προτείνεται η υλοποίηση μιας πλήρους πολιτικής ασφάλειας, η οποία να συνδυάζει προτρεπτικά, ανιχνευτικά και αντιδραστικά αντίμετρα κατά των εισβολών και να επιβάλλει την κρυπτογραφημένη αποθήκευση των βιομετρικών υπογραφών, καθώς και μοντέλα διανεμημένης αποθήκευσης και διαχωρισμού ταυτότητας χρήστη και βιομετρικής υπογραφής. Όταν μια διανεμημένη αρχιτεκτονική αποτελεί την απαραίτητη επιλογή, είναι προτιμότερη η αποθήκευση της υπογραφής στη μη επανεγγράψιμη μνήμη μιας έξυπνης κάρτα υψηλών προδιαγραφών φυσικής και λογικής ασφάλειας [143].

3.2.3.1.3 Αδυναμία ασφάλειας μετάδοσης - υποκλοπή σήματος και επανεκπομπή

Περιγραφή: Η πληροφορία που μεταδίδεται μεταξύ των διαφόρων τμημάτων του βιομετρικού συστήματος, όπως παρουσιάζεται στο Σχήμα 11, μπορεί να υποκλαπεί και μελλοντικά να επαναληφθεί η εκπομπή της με στόχο την εξαπάτηση του συστήματος. Για παράδειγμα, αν η σύγκριση των βιομετρικών υπογραφών γίνεται σε ένα υποσύστημα εξωτερικό της συσκευής μέτρησης, μπορεί να υποκλαπεί η βιομετρική υπογραφή από το κανάλι επικοινωνίας κατά τη μεταφορά της και να επιχειρηθεί η εκπομπή της μελλοντικά για διείσδυση στο σύστημα [143].

Μέτρα ασφάλειας: Για την αντιμετώπιση επιθέσεων υποκλοπής και επανεκπομπής του σήματος απαιτείται η εισαγωγή τυχαίων τιμών ως τμημάτων του σήματος και η χρήση μηχανισμών διατήρησης της ακεραιότητας αυτών (υλοποίηση με συναρτήσεις σύνοψης), με στόχο την επίτευξη της μοναδικότητας κάθε εκπεμπόμενου σήματος. Επίσης, συνιστάται η πιστοποίηση ταυτότητας των διαφόρων συστατικών του συστήματος με μηχανισμούς ερωταπόκρισης μέσω συναρτήσεων σύνοψης. Τέλος, συνιστάται η ολοκλήρωση του συστήματος σε μια οντότητα περιορισμένης φυσικής πρόσβασης, όπου οι τηλεπικοινωνιακές ζεύξεις είναι προστατευμένες με φυσικά μέσα (για παράδειγμα σε μια έξυπνη κάρτα) [140].

3.2.3.1.4 Αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών

Περιγραφή: Η χρήση μιας βιομετρικής υπογραφής σε ένα σύστημα χαμηλών προδιαγραφών ασφάλειας μπορεί να την εκθέσει και να προκαλέσει την υποκλοπή της. Στη συνέχεια, η βιομετρική υπογραφή μπορεί να χρησιμοποιηθεί σε ένα σύστημα υψηλής ασφάλειας με στόχο τη διείσδυση σε αυτό με το λογαριασμό ενός νόμιμου χρήστη. Η αδυναμία αυτή θέτει το πρόβλημα της δυνατότητας ανάκλησης μιας βιομετρικής υπογραφής [143].

Μέτρα ασφάλειας: Η αδυναμία αυτή μπορεί να αντιμετωπιστεί με χρήση διακριτών αλγόριθμων δημιουργίας βιομετρικών υπογραφών, ώστε να επιτευχθεί η παραγωγή διαφορετικών βιομετρικών υπογραφών για κάθε χρήστη ανά εφαρμογή. Αν η εφαρμογή το απαιτεί, μπορεί να παραμετροποιηθούν βιομετρικοί αλγόριθμοι, ώστε να δημιουργούν βιομετρικές υπογραφές διαφορετικές από αυτές ενός κοινού προϊόντος της αγοράς που τους ενσωματώνει. Μια πιο σύνθετη λύση είναι η χρήση συναρτήσεων σύνοψης στο αποτέλεσμα του αλγόριθμου δημιουργίας υπογραφών, όπως περιγράφεται στην επόμενη παράγραφο.

3.2.3.1.5 Αδυναμία προστασίας ακεραιότητας συστατικών του συστήματος

Περιγραφή: Αν το βιομετρικό σύστημα δεν είναι σωστά θωρακισμένο μπορεί να προσβληθεί η ακεραιότητα κάποιου εκ των συστατικών του συστήματος και να αλλοιωθεί η συμπεριφορά του. Για παράδειγμα, ένας δούρειος ίππος μπορεί να εγκατασταθεί στο σύστημα κωδικοποίησης και να αλλοιώσει το αποτέλεσμα της μέτρησης παράγοντας

διαφορετικές βιομετρικές υπογραφές. Αντίστοιχα, μπορεί να επηρεαστεί ο αλγόριθμος σύγκρισης ώστε να επιτρέψει εισβολή στο σύστημα.

Μέτρα ασφάλειας: Για την αντιμετώπιση του προβλήματος, προτείνονται συστήματα ελέγχου της ακεραιότητας του λογισμικού κάθε συστατικού του συστήματος. Τα συστήματα αυτά βασίζονται σε συναρτήσεις σύνοψης, οι οποίες εφαρμόζονται στο σύνολο του εκτελέσιμου κώδικα και αποθηκεύουν το αποτέλεσμα για μελλοντική σύγκριση. Έτσι, η αλλοίωση του εκτελέσιμου κώδικα γίνεται αντιληπτή στην επόμενη σύγκριση με το αποθηκευμένο αποτέλεσμα σύνοψης. Τέλος, συνιστάται η ολοκλήρωση του συστήματος σε μια οντότητα περιορισμένης φυσικής πρόσβασης, όπου κάθε συστατικό του συστήματος είναι προστατευμένο με φυσικά μέσα (για παράδειγμα σε μια έξυπνη κάρτα).

3.2.3.1.6 Διαδικαστικές αδυναμίες - διαχείριση βιομετρικών δεδομένων και υπογραφών

Περιγραφή: Οι ανεπαρκείς πολιτικές και διαδικασίες διαχείρισης των βιομετρικών δεδομένων και υπογραφών αποτελούν σοβαρά ευπαθή σημεία. Για παράδειγμα, οι διαδικασίες εγγραφής του χρήστη στο σύστημα μπορεί να οδηγήσουν σε διαρροή βιομετρικών δεδομένων και υπογραφών, αν δεν είναι ορισμένο με ακρίβεια ότι ενδιάμεσα βιομετρικά δεδομένα και μετρήσεις δεν θα αποθηκεύονται, και ότι το τελικό αποτέλεσμα, δηλαδή η βιομετρική υπογραφή θα αποθηκεύεται μόνο σε ασφαλές μέσο. Όπως σε οποιοδήποτε σύστημα, οι διαχειριστές μπορεί να εκμεταλλευτούν τη δικαιοδοσία τους και να υποκλέψουν βιομετρικά δεδομένα ή να αλλάξουν την αντιστοιχία ονόματος χρήστη με βιομετρική υπογραφή ή ακόμα και την ίδια την παραμετροποίηση του συστήματος, ώστε να το κάνουν λιγότερο αυστηρό από όσο επιβάλλει η σημασία της εφαρμογής [121].

Μέτρα ασφάλειας: Απαιτούνται ολοκληρωμένες πολιτικές ασφάλειας και αναλυτικές διαδικασίες, οι οποίες να υλοποιούν διεθνή πρότυπα ασφάλειας πληροφοριακών συστημάτων και διαχείρισης βιομετρικών δεδομένων, ώστε να καλύπτονται όλοι οι απαιτούμενοι τομείς [145].

3.2.3.1.7 Αδυναμίες σε θόρυβο και λειτουργία εκτός των επιτρεπόμενων ορίων

Περιγραφή: Η παρούσα κατηγορία αδυναμιών αφορά σε μεταβλητές συνθήκες φωτισμού, οι οποίες επηρεάζουν τα συστήματα αναγνώρισης προσώπου, στον ηχητικό θόρυβο που επηρεάζει τα συστήματα αναγνώρισης φωνής και γενικότερα σε σήματα θορύβου που μπορεί να επηρεάσουν κάθε είδους βιομετρικό αισθητήρα. Επίσης, αφορά σε παροχή ηλεκτρικής ενέργειας στη βιομετρική συσκευή εκτός των ορίων λειτουργίας,, στη μεταβολή της θερμοκρασίας ή της υγρασίας της συσκευής σε μη επιτρεπτά όρια και στον ψεκασμό των αισθητήρων με χημικές ουσίες. Οι παραπάνω χαρακτηριστικές συνθήκες μπορεί να προκαλέσουν αποτυχία της βιομετρικής συσκευής [144].

Μέτρα ασφάλειας: Το περιβάλλον λειτουργίας της βιομετρικής συσκευής πρέπει να γίνει όσο το δυνατόν ελεγχόμενο κατά τη χρήση της. Αυτό υλοποιείται με ολοκληρωμένες πολιτικές ασφάλειας, ανάλογα με την εφαρμογή.

3.2.3.1.8 Αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής

Περιγραφή: Οι υλοποιήσεις ψηφιακής λογικής με μικροηλεκτρονικά κυκλώματα μπορεί να αποτελέσουν αντικείμενα επιθέσεων ανάλυσης των λειτουργιών τους. Οι επιθέσεις αυτές χωρίζονται σε δύο βασικές κατηγορίες, τις επιθέσεις ανάλυσης της κατανάλωσης ενέργειας και τις επιθέσεις χρονικής ανάλυσης των μικρο-ελεγκτών. Οι πιο γνωστές επιθέσεις ανάλυσης κατανάλωσης ενέργειας είναι η απλή ανάλυση ενέργειας (Simple Power Analysis) [15] και η διαφορική ανάλυση ενέργειας (Differential Power Analysis) [16], οι οποίες χρησιμοποιούνται για να παραβιάσουν κρυπτογραφικούς αλγόριθμους χρησιμοποιώντας στατιστικό λογισμικό, όπου το μυστικό κλειδί αποκαλύπτεται από τα μέγιστα ενός διαγράμματος ανάλυσης ενέργειας. Η λογική πίσω από τις επιθέσεις αυτές στηρίζεται στο γεγονός ότι ο μικρο-ελεγκτής ανάλογα με τις εντολές που εκτελεί και τα αποτελέσματα των εντολών αυτών, καταναλώνει διαφορετικά επίπεδα ενέργειας. Οι επιθέσεις χρονικής ανάλυσης, λειτουργούν αντίστοιχα, επεξεργάζοντας το χρόνο επεξεργασίας των δεδομένων και αποκαλύπτοντας τις εντολές που εκτελούνται. Στην περίπτωση των βιομετρικών είναι πιθανό να πραγματοποιηθούν επιθέσεις στα μικρο-ηλεκτρονικά κυκλώματα μιας βιομετρικής συσκευής, όπως για παράδειγμα σε ένα αλγόριθμο σύγκρισης και με

επαναλαμβανόμενες δοκιμές να αποκαλυφθούν δεδομένα, όπως για παράδειγμα μια βιομετρική υπογραφή.

Μέτρα ασφάλειας: Τα αντίμετρα για αδυναμίες τέτοιου είδους περιλαμβάνουν χρήση μικρο-ελεγκτών χαμηλής κατανάλωσης ενέργειας και γεννήτριες θορύβου, ώστε να δυσκολεύεται η ανίχνευση του επιπέδου ενέργειας που καταναλώνεται. Όσο αφορά στα αντίμετρα κατά των επιθέσεων χρονικής ανάλυσης, ως ισχυρότερο αναφέρεται η κατάλληλη σχεδίαση του κώδικα, ώστε να περιλαμβάνει χαρακτηριστικά χρονικής ουδετερότητας.

3.2.3.1.9 Αδυναμία αναγνώρισης εναπομένοντος χαρακτηριστικού

Περιγραφή: Η αδυναμία αυτή αφορά σε κάποιους οπτικούς αισθητήρες αναγνώρισης δακτυλικών αποτυπωμάτων [123]. Οι επιθέσεις αυτές, οι οποίες έχουν ονομαστεί επιθέσεις εναπομένουσας εικόνας, στηρίζονται στο γεγονός, ότι όταν ένας νόμιμος χρήστης χρησιμοποιεί το σύστημα, αφήνει πάνω στον οπτικό αισθητήρα το αποτύπωμά του. Στη συνέχεια, η τοποθέτηση μιας λεπτής σακούλας ζεστού νερού πάνω στον βιομετρικό αισθητήρα ενεργοποιεί το σύστημα το οποίο έδινε πρόσβαση στον μη εξουσιοδοτημένο χρήστη.

Μέτρα ασφάλειας: Η ανίχνευση ζωτικότητας, η αποτίμηση της χρησιμοποιούμενης τεχνολογίας (οπτικοί ή χωρητικοί αισθητήρες) και η χρήση μηχανισμών αλληλεπίδρασης με το χρήστη, καθώς και η απόρριψη της ακριβώς όμοιας μέτρησης μεταξύ δύο συνεχόμενων μετρήσεων, αποτελούν αποτελεσματικά αντίμετρα.

3.2.3.1.10 Αδυναμίες διάκρισης παρόμοιων βιομετρικών υπογραφών

Περιγραφή: Οι αδυναμίες αυτές αφορούν στην απόδοση του βιομετρικού συστήματος και συγκεκριμένα στη δυνατότητα του συστήματος να παράγει διαφορετικές βιομετρικές υπογραφές και να είναι ικανό να τις διακρίνει κατά τη διάρκεια της σύγκρισης.

Μέτρα ασφάλειας: Τα χρησιμοποιούμενα βιομετρικά συστήματα πρέπει να έχουν δοκιμαστεί από ανεξάρτητους φορείς και να είναι πιστοποιημένα για την ικανοποιητική τους απόδοση [119, 132].

3.2.3.1.11 Αδυναμίες σε επιθέσεις ωμής δύναμης

Περιγραφή: Οι επιθέσεις ωμής δύναμης, όπως και σε κάθε σύστημα πιστοποίησης ταυτότητας, πραγματοποιούνται με συνεχή προσπάθεια εισβολής στο σύστημα, μέσω αποστολής αυξανομένων δεδομένων σύγκρισης (για παράδειγμα συνδυασμών τμημάτων βιομετρικών δεδομένων), ωσότου επιτευχθεί πλήρης ομοιότητα. Στην περίπτωση των βιομετρικών αυτές οι επιθέσεις είναι πιο σύνθετες, καθώς πρέπει να συνδυαστούν με κάποια από τις προηγούμενες επιθέσεις, ώστε να μπορούν να εισαχθούν τα δεδομένα στο σύστημα [118]. Οι αδυναμίες αυτές είναι πιο έντονες σε συστήματα αναγνώρισης, όπου πραγματοποιείται σύγκριση μιας βιομετρικής υπογραφής με πολλές και όχι τόσο σε συστήματα πιστοποίησης, όπου η σύγκριση είναι μία προς μία.

Μέτρα ασφάλειας: Το πιο χαρακτηριστικό αντίμετρο είναι το κλείδωμα του λογαριασμού του χρήστη μετά από κάποιο αριθμό αποτυχημένων προσπαθειών.

3.2.3.1.12 Αδυναμίες στο σύστημα διαχείρισης ταυτότητας

Περιγραφή: Η χρήση βιομετρικών συστημάτων, επειδή συνδέει ισχυρά την ταυτότητα του χρήστη με τον ίδιο μπορεί να προκαλέσει παραβίαση της μυστικότητας των προσωπικών του δεδομένων, όπως αποκάλυψη της ταυτότητάς του ή παρακολούθηση της θέσης του και των συναλλαγών του με το σύστημα.

Μέτρα ασφάλειας: Το σύστημα πρέπει να περιλαμβάνει αντίμετρα προστασίας της πραγματικής ταυτότητας του χρήστη, όπως χρήση προσωρινών ταυτοτήτων αυστηρή χρήση βιομετρικών υπογραφών με δυνατότητα ανάκλησης (όπως περιγράφηκε στην παράγραφο 3.2.3.1.4)και όχι στην χρήση ακατέργαστων βιομετρικών δεδομένων.

3.2.3.2 Περιεκτική μορφή συστήματος

Σύμφωνα με τη μεθοδολογία Ανάλυσης Πολλαπλών Κριτηρίων, κάθε αδυναμία βαθμολογήθηκε για ένα από τα τρία κριτήρια. Η βαθμολόγηση έγινε βάσει της φύσης του κριτηρίου, μετά από σχετική μελέτη της αδυναμίας και ήταν συγκριτική, σε σχέση με τις υπόλοιπες αδυναμίες – η συγκριτική κατανομή είναι άλλωστε και ο στόχος μας. Στη συνέχεια

εισήχθηκαν οι συντελεστές βαρύτητας και τέλος έγινε άθροιση των τελικών βαθμών και για τα τρία κριτήρια. Για την πλήρη κατανόηση των υπολογισμών, παρουσιάζουμε το παράδειγμα της *αδυναμίας μυστικότητας λειτουργιών μικροηλεκτρονικής*. Η εκμετάλλευση των αδυναμιών αυτών είναι δύσκολη, απαιτώντας ειδικές γνώσεις, πολύ αποτελεσματική, αλλά και δαπανηρή, καθώς απαιτείται εξειδικευμένος εξοπλισμός. Έτσι, οι βαθμοί που δόθηκαν, είναι οι ακόλουθοι:

- Βαθμός K_1 = 1, ελάχιστος βαθμός, καθώς είναι οι τεχνικά δυσκολότερες προς εκμετάλλευση αδυναμίες.
- Βαθμός K_2 = 8, υψηλός βαθμός, λόγω αυξημένης αποτελεσματικότητας
- Βαθμός K_3 = 1, ελάχιστος βαθμός, καθώς απαιτεί το υψηλότερο κόστος σε εξοπλισμό.

Το τελικό άθροισμα για τη συγκεκριμένη αδυναμία είναι 10. Τα αποτελέσματα, μετασχηματίσθηκαν σε ποσοστιαίες μονάδες του αθροίσματος των αποτελεσμάτων όλων των αδυναμιών, με στόχο την έκφραση ενός μέγιστου επιπέδου επικινδυνότητας 100% στην περίπτωση που ένα βιομετρικό σύστημα περιλαμβάνει όλες τις κατηγορίες αδυναμιών. Οι παράγοντες επικινδυνότητας υπολογίσθηκαν ξεχωριστά για τις ακόλουθες βιομετρικές μεθόδους:

- Πιστοποίηση δακτυλικού αποτυπώματος
- Πιστοποίηση ίριδας
- Πιστοποίηση προσώπου
- Πιστοποίηση φωνής

Οι παραπάνω είναι και οι πιο διαδεδομένες βιομετρικές μέθοδοι [118], με την πιο ευρεία εξάπλωση σε πληροφοριακά συστήματα. Για τις περιπτώσεις όπου μία αδυναμία είναι ανεξάρτητη της βιομετρικής μεθόδου, υπολογίσθηκε ένας κοινός παράγοντας επικινδυνότητας.

Ο Πίνακας 2 παρουσιάζει μία συγκεντρωτική μορφή του συστήματος αποτίμησης επικινδυνότητας βιομετρικών συστημάτων, συμπεριλαμβανόμενων των αδυναμιών, των παραγόντων επικινδυνότητας και των αντίστοιχων μέτρων ασφάλειας.

Πίνακας 2: Συγκεντρωτική μορφή του συστήματος αποτίμησης επικινδυνότητας βιομετρικών συστημάτων

Αδυναμία	Παράγοντας Επικινδυνότητας (%)				Αριθμός Μέτρου Ασφάλειας
	Δ	Ι	Π	Φ	
1. Αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης.	10	8	11	13	i, ii, iii
2. Κληρονομήσιμες αδυναμίες κεντρικοποιημένων αρχιτεκτονικών - πλαστές βιομετρικές υπογραφές.	14				iv, v
3. Αδυναμία ασφάλειας μετάδοσης - υποκλοπή σήματος και επανεκπομπή.	10				vi, xiii, xiv, xv
4. Αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών.	5				vii
5. Αδυναμία προστασίας ακεραιότητας συστατικών του συστήματος.	10				vi, xv
6. Διαδικαστικές αδυναμίες - διαχείριση βιομετρικών δεδομένων και υπογραφών.	17				iv
7. Αδυναμίες σε θόρυβο και λειτουργία εκτός των επιτρεπόμενων ορίων.	3	3	3	5	iv
8. Αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής.	3				viii
9. Αδυναμία αναγνώρισης εναπομένοντος χαρακτηριστικού.	6	0	0	0	i, iii, ix, xvi
10. Αδυναμίες διάκρισης παρόμοιων βιομετρικών υπογραφών.	2	2	6	6	ix, x
11. Αδυναμίες σε επιθέσεις ωμής δύναμης.	3				xi
12. Αδυναμίες στο σύστημα διαχείρισης ταυτότητας.	14				xii

Μέτρα Ασφάλειας	
i.	Ανίχνευση ζωτικότητας.
ii.	Αρχιτεκτονική πολλαπλών βιομετρικών μοντέλων.
iii.	Πιστοποίηση με αλληλεπίδραση – ερωταπόκριση.
iv.	Ολοκληρωμένη πολιτική ασφάλειας.
v.	Αποθήκευση βιομετρικής υπογραφής σε ασφαλές μέσο.
vi.	Ολοκλήρωση συστήματος σε οντότητα περιορισμένης φυσικής πρόσβασης.
vii.	Εξειδικευμένοι αλγόριθμοι βιομετρικής κωδικοποίησης - συναρτήσεις σύνοψης (hash functions).
viii.	Γεννήτριες θορύβου, μικρο-ελεγκτές χαμηλής κατανάλωσης ενέργειας, σχεδιασμός λογισμικού με χαρακτηριστικά χρονικής ουδετερότητας.
ix.	Αποτίμηση τεχνολογίας.
x.	Δοκιμή και πιστοποίηση συστήματος από ανεξάρτητο φορέα.
xi.	Περιορισμός προσπαθειών πρόσβασης με κλείδωμα λογαριασμού.
xii.	Προστασία απορρήτου ταυτότητας με προσωρινές ταυτότητες και βιομετρικές υπογραφές με δυνατότητα ανάκλησης.
xiii.	Πιστοποίηση ταυτότητας συστατικών του συστήματος.
xiv.	Εισαγωγή τυχαίων τιμών ως τμημάτων του σήματος
xv.	Χρήση μηχανισμών διατήρησης ακεραιότητας.
xvi.	Απόρριψη εν συνεχεία όμοιων σημάτων.

3.2.3.3 Λειτουργίες και σημασία του συστήματος

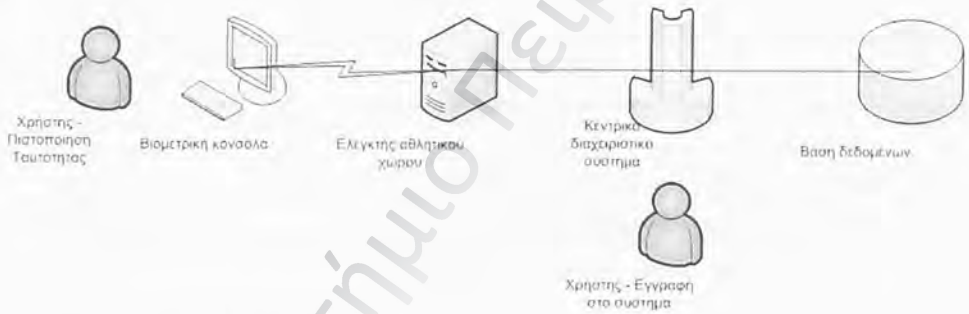
Το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων έχει τις παρακάτω πρακτικές λειτουργίες:

- Πλήρη προσδιορισμό των αδυναμιών ενός βιομετρικού συστήματος, μετά από μελέτη του καταλόγου αδυναμιών και αντιπαράθεση τους με τις προδιαγραφές του συστήματος.
- Υπολογισμό του επιπέδου επικινδυνότητας του συστήματος με άθροιση των παραγόντων επικινδυνότητας κάθε αναγνωρισμένης αδυναμίας.
- Επιλογή των κατάλληλων μέτρων ασφάλειας για μείωση του επιπέδου επικινδυνότητας.

- Επαλήθευση της μείωσης του επιπέδου επικινδυνότητας με επανάληψη της διαδικασίας και υπολογισμό της εναπομένουσας επικινδυνότητας.
- Δημιουργία συστήματος συμβατού με τη μεθοδολογία BEM των Common Criteria (CC), καθώς και με τα επίσημα προφίλ αξιολόγησης, με αποτέλεσμα τη δυνατότητα πιστοποίησης αυτού με το ISO/IEC 15408.

3.2.4 Πειραματικη εφαρμογη συστηματος

Το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων δοκιμάσθηκε πειραματικά σε ένα πραγματικό σύστημα με ονομασία "Ευφυές σύστημα ελέγχου πρόσβασης φιλάθλων και διαπιστευμένων ατόμων σε αθλητικές διοργανώσεις", το οποίο βασιζόταν σε βιομετρικά συστήματα. Το σύστημα έχει την αρχιτεκτονική που παρουσιάζεται στο Σχήμα 28.



Σχήμα 28: Βιομετρικό σύστημα πειραματικής δοκιμής

Ο χρήστης αρχικά εγγράφεται στο κεντρικό διαχειριστικό σύστημα, όπου παράγεται η βιομετρική του υπογραφή, η οποία αποθηκεύεται σε μία έξυπνη κάρτα. Για να εισέλθει σε ένα αθλητικό χώρο, ο χρήστης εισάγει την βιομετρική κάρτα στη βιομετρική κονσόλα και χρησιμοποιεί το δακτυλικό του αποτύπωμα για την πιστοποίηση της ταυτότητάς του. Αν η πιστοποίηση είναι επιτυχής, τα δικαιώματά του ελέγχονται από τον ελεγκτή του αθλητικού χώρου, ο οποίος έχει ενημερωθεί νωρίτερα από το κεντρικό διαχειριστικό σύστημα και τη βάση δεδομένων αυτού.

Η βιομετρική κονσόλα χρησιμοποιεί ένα εμπορικό προϊόν (Bioscrypt) το οποίο δημιουργεί βιομετρικές υπογραφές και τις αποθηκεύει κρυπτογραφημένες σε μία έξυπνη κάρτα. Ο βιομετρικός αλγόριθμος και αισθητήρας δεν έχουν δυνατότητα ανίχνευσης ζωτικότητας. Ο αισθητήρας παρόλα αυτά είναι επαγωγικός με επιφάνεια που δεν αφήνει ίχνη, καθιστώντας μη δυνατές τις επιθέσεις εναπομείναντος χαρακτηριστικού. Ο αλγόριθμος είναι ελεγμένος για την απόδοσή του. Ο αναγνώστης της έξυπνης κάρτας είναι ενσωματωμένος στο τμήμα του προϊόντος που εκτελεί τις βιομετρικές μετρήσεις και το σύνολο των βιομετρικών λειτουργιών. Οι έξυπνες κάρτες δεν έχουν υλοποιημένα αντίμετρα κατά επιθέσεων μικροηλεκτρονικής. Η λειτουργία του συστήματος δεν διέπεται από πολιτική ασφάλειας. Παρόλα αυτά, κάποια μέτρα ασφάλειας είναι υλοποιημένα, όπως φυσικά και λογικά προστατευμένες συνδέσεις. Η φυσική προστασία αφορά σε μη εκτεθειμένα καλώδια σύνδεσης και παρουσία φύλακα στους χώρους λειτουργίας του συστήματος (ελεγχόμενο περιβάλλον), ενώ τα λογικά αντίμετρα αφορούν στη χρήση κρυπτογραφίας και στην εισαγωγή τυχαίων τιμών στα μεταδιδόμενα σήματα, με τη διατήρηση της ακεραιότητας και εμπιστευτικότητας των μηνυμάτων, αλλά και της μοναδικότητας αυτών, με στόχο την αντιμετώπιση επιθέσεων επανεκπομπής.

Εφαρμόζοντας το σύστημα αποτίμησης επικινδυνότητας βιομετρικών δεδομένων, αναλύσαμε το σύστημα ως προς τις υπάρχουσες αδυναμίες. Αναζητήσαμε τις αδυναμίες εκείνες οι οποίες αφορούν στο σύστημα και καταλήξαμε στα ακόλουθα:

- Αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης: Καθώς δεν υπήρχαν αντίμετρα ανίχνευσης ζωτικότητας, χωρίς κάποιο άλλο υλοποιημένο αντίμετρο.
- Αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών: Καθώς ο βιομετρικός αλγόριθμος ήταν εμπορικός (Bioscrypt), χωρίς κάποιο άλλο υλοποιημένο αντίμετρο.
- Διαδικαστικές αδυναμίες - διαχείριση βιομετρικών δεδομένων και υπογραφών: Καθώς δεν υπήρχε πολιτική ασφάλειας στο σύστημα.
- Αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής: Καθώς οι έξυπνες κάρτες δεν είχαν τα κατάλληλα υλοποιημένα αντίμετρα.

Ενώ οι παρακάτω αδυναμίες δεν αφορούσαν στο σύστημα:

- Κληρονομήσιμες αδυναμίες κεντρικοποιημένων αρχιτεκτονικών - πλαστές βιομετρικές υπογραφές: καθώς η βιομετρική υπογραφή αποθηκεύεται σε έξυπνη κάρτα.
- Αδυναμία ασφάλειας μετάδοσης - υποκλοπή σήματος και επανεκπομπή: Καθώς η βιομετρική κονσόλα και οι συνδέσεις ήταν φυσικά και λογικά προστατευμένες.
- Αδυναμία προστασίας ακεραιότητας συστατικών του συστήματος: Καθώς ήταν υλοποιημένα τα κατάλληλα αντίμετρα.
- Αδυναμία αναγνώρισης εναπομένοντος χαρακτηριστικού: Καθώς ο συγκεκριμένος βιομετρικός αισθητήρας δεν είχε το σχετικό ευπαθές σημείο.
- Αδυναμίες σε θόρυβο και λειτουργία εκτός των επιτρεπόμενων ορίων: καθώς το περιβάλλον είναι ελεγχόμενο.
- Αδυναμίες διάκρισης παρόμοιων βιομετρικών υπογραφών: Καθώς ο βιομετρικός αλγόριθμος είχε περάσει δοκιμές από διεθνή διαγωνισμό απόδοσης.
- Αδυναμίες σε επιθέσεις ωμής δύναμης: Καθώς το περιβάλλον είναι ελεγχόμενο και δεν υπάρχει τρόπος εισαγωγής των δεδομένων στο σύστημα.
- Αδυναμίες στο σύστημα διαχείρισης ταυτότητας: Καθώς ο μηχανισμός χρησιμοποιούσε προσωρινές ταυτότητες.

Στη συνέχεια, αθροίσαμε τα επίπεδα επικινδυνότητας των αδυναμιών του συστήματος (όπως τα ορίζει ο Πίνακας 2). Ο Πίνακας 3 παρουσιάζει τον υπολογισμό της επικινδυνότητας του συστήματος.

Πίνακας 3: Υπολογισμός επικινδυνότητας

Αδυναμία συστήματος	Παράγοντας Επικινδυνότητας (%)
Αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης	10
Αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών	5
Διαδικαστικές αδυναμίες - διαχείριση βιομετρικών δεδομένων και υπογραφών	17
Αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής	3
Σύνολο	35

Υπολογίζεται με τον τρόπο αυτό, επικινδυνότητα 35%. Για τη μείωση του επιπέδου επικινδυνότητας, προχωρήσαμε στην επιλογή των κατάλληλων αντιμέτρων, όπως τα ορίζει ο Πίνακας 2. Άμεσα αποφασίσθηκε η ανάπτυξη λεπτομερούς πολιτικής ασφάλειας, η οποία μετά την υλοποίησή της μείωσε την επικινδυνότητα στο 18%. Τα αντίμετρα για περαιτέρω μείωση της επικινδυνότητας θεωρήθηκαν ασύμφορα για τη συγκεκριμένη πιλοτική εφαρμογή και η εναπομένουσα επικινδυνότητα έγινε αποδεκτή, εξετάζοντας μελλοντική της μείωση σε μη πιλοτικό σενάριο λειτουργίας. Πιο συγκεκριμένα, σε επίπεδο πιλοτικού συστήματος, δεν υπήρχε, λόγω κόστους, η δυνατότητα προμήθειας αλγορίθμου με χαρακτηριστικά ανίχνευσης ζωτικότητας και η επέμβαση σε αυτόν για τη δημιουργία μοναδικών βιομετρικών υπογραφών για τον ίδιο χρήστη, καθώς και η προμήθεια πιο ασφαλών έξυπνων καρτών για τον ίδιο λόγο. Παρόλα αυτά, η σχεδίαση του τελικού συστήματος μετά τη λειτουργία του πιλοτικού περιλαμβάνει τα παραπάνω αντίμετρα προς μείωση του επιπέδου επικινδυνότητας.

3.2.5 ΣΥΜΠΕΡΑΣΜΑΤΑ - ΑΣΦΑΛΗ ΣΥΣΤΗΜΑΤΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΑΥΤΟΤΗΤΑΣ ΤΡΙΩΝ ΠΑΡΑΓΟΝΤΩΝ

Η δημιουργία ενός μηχανισμού ή μιας αρχιτεκτονικής ασφάλειας που περιλαμβάνει βιομετρικά συστήματα πρέπει να σχεδιάζεται και να υλοποιείται προσεκτικά, ώστε το συνολικό αποτέλεσμα να είναι ασφαλές. Από τη μελέτη ασφάλειας των βιομετρικών συστημάτων που διενεργήθηκε στο πλαίσιο δημιουργίας του συστήματος αποτίμησης επικινδυνότητας και από τη μελέτη των αποτελεσμάτων που συγκεντρώνει ο Πίνακας 2, κυρίως όσον αφορά στις αδυναμίες με τους μέγιστους παράγοντες επικινδυνότητας, καταλήγουμε στα ακόλουθα συμπεράσματα:

- Το σύστημα πρέπει να υποστηρίζεται από μια ολοκληρωμένη πολιτική ασφάλειας, η οποία πρέπει να διέπει τη λειτουργία του διαδικαστικά και τεχνικά.
- Τα βιομετρικά δεδομένα είναι προτιμότερο να αποθηκεύονται σε έξυπνες κάρτες, οι οποίες έχουν υλοποιημένα τα κατάλληλα μέτρα ασφάλειας ασφαλούς αποθήκευσης δεδομένων και λειτουργίας.

- Το σύστημα διαχείρισης ταυτότητας του χρήστη πρέπει να περιλαμβάνει αντίμετρα όπως η χρήση προσωρινών ταυτοτήτων, για τη διασφάλιση του απορρήτου της ταυτότητας, της θέσης και των εφαρμογών του χρήστη.
- Το βιομετρικό σύστημα πρέπει να υλοποιεί μηχανισμούς ανίχνευσης ζωτικότητας.
- Η επικοινωνία πρέπει να προστατεύεται από τα κατάλληλα αντίμετρα μυστικότητας και ακεραιότητας της πληροφορίας. Οι βιομετρικές υπογραφές καλό είναι να μην μεταδίδονται πάνω από δίκτυα και η διαδικασία βιομετρικής πιστοποίησης να πραγματοποιείται τοπικά. Αν η εφαρμογή επιβάλλει απομακρυσμένη πιστοποίηση συνίσταται η ανεύρεση άλλων μοντέλων και μηχανισμών (όπως περιγράφεται στην παράγραφο 3.3) Η ιδανική μάλιστα σχεδίαση του συστήματος απαιτεί όλα τα υποσυστήματα του βιομετρικού να υλοποιούνται μέσα στην έξυπνη κάρτα.

3.3 ΠΡΩΤΟΚΟΛΛΟ ΕΝΣΩΜΑΤΩΣΗΣ ΒΙΟΜΕΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗ ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΤΑΥΤΟΤΗΤΑΣ ΧΡΗΣΤΗ ΥΠΗΡΕΣΙΩΝ 3ΗΣ ΚΑΙ 4ΗΣ ΓΕΝΙΑΣ

3.3.1 ΠΕΡΙΓΡΑΦΗ ΣΤΟΧΟΥ ΚΑΙ ΠΡΟΣΕΓΓΙΣΗΣ

Η παρούσα προτεινόμενη λύση αντιμετωπίζει το ακόλουθο πρόβλημα:

Η αλυσίδα ασφάλειας πρόσβασης χρήστη σε επίπεδο δικτύου καταλήγει στην πιστοποίηση της ταυτότητας χρήστη στην τερματική συσκευή, η οποία υλοποιείται με την επισφαλή χρήση ενός PIN. Η εισαγωγή βιομετρικών για την υλοποίηση ισχυρής πιστοποίησης ταυτότητας δεν έχει μελετηθεί για ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς. Η μελέτη ασφάλειας και προστασίας των προσωπικών δεδομένων του χρήστη για την εισαγωγή βιομετρικών σε δίκτυα 3ης ή 4ης γενιάς είναι επιτακτική, καθώς και η ύπαρξη ενός πρωτοκόλλου για ισχυρή πραγματική πιστοποίηση του χρήστη από άκρο σε άκρο, το οποίο να είναι συμβατό με τα αποτελέσματα της μελέτης.

Στόχος του κεφαλαίου αυτού είναι η μεθοδική αντιμετώπιση του παραπάνω προβλήματος με πλήρη υλοποίηση του πρότυπου κύκλου ζωής σχεδίασης συστημάτων και πρωτοκόλλων, ο οποίος αποτελείται από τον προσδιορισμό των απαιτήσεων, την εξαγωγή των

προδιαγραφών, τη σχεδίαση και τέλος την αξιολόγηση. Τα παραπάνω πραγματοποιήθηκαν ως εξής:

- Προσδιορισμός απαιτήσεων: Μελετήθηκαν οι απαιτήσεις ασφάλειας και προστασίας των προσωπικών δεδομένων του χρήστη στο συγκεκριμένο περιβάλλον των δικτύων 4ης γενιάς. Μελετήθηκαν επίσης απαιτήσεις ευχρηστίας, οικονομικότητας, εύκολης προσαρμογής και υλοποίησης. Για το στάδιο αυτό σημαντικό ρόλο έπαιξε η μελέτη της προτεινόμενης λύσης: *σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων*. Λήφθηκαν επίσης υπόψη οι απαιτήσεις προστασίας ταυτότητας, θέσης και παρεχόμενων στο χρήστη υπηρεσιών του 3GPP [72].
- Εξαγωγή προδιαγραφών: Ορίσθηκαν με αυστηρότητα οι προδιαγραφές του πρωτοκόλλου, βάσει των προσδιορισμένων απαιτήσεων
- Σχεδίαση: Σχεδιάστηκε το πρωτόκολλο βάσει των προδιαγραφών.
- Αξιολόγηση: Το πρωτόκολλο αξιολογήθηκε ως προς την ασφάλεια, την προστασία των προσωπικών δεδομένων του χρήστη, την απόδοση, την ευχρηστία και την πολυπλοκότητα υλοποίησης αυτού.

3.3.2 ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΠΡΟΔΙΑΓΡΑΦΕΣ

Τα βιομετρικά συστήματα αφενός αυξάνουν το επίπεδο ασφάλειας ενός πληροφοριακού συστήματος, καθώς υλοποιούν ισχυρή πιστοποίηση ταυτότητας χρήστη, προστατεύοντας εκτός των άλλων και προσωπικά δεδομένα [130]. Αφετέρου, αρχιτεκτονικές ασφάλειας που περιέχουν βιομετρικά συστήματα οι οποίες δεν είναι μεθοδικά σχεδιασμένες μπορεί να εισάγουν υψηλό επίπεδο επικινδυνότητας στο σύστημα, όπως αποδείχθηκε κατά την περιγραφή της προηγούμενης προτεινόμενης λύσης. Επιπλέον, τα προσωπικά δεδομένα του χρήστη και γενικότερα η προστασία του ιδιωτικού του απορρήτου μπορεί να παραβιαστούν, με αθέμιτη χρήση πληροφορίας που μπορεί να εξαχθεί από μία βιομετρική μέτρηση, όπως για παράδειγμα γενετική πληροφορία ή πληροφορία που συνδέεται με ιατρικά δεδομένα (η ίριδα για παράδειγμα περιέχει πληροφορία για την ανίχνευση διαφόρων ασθενειών) [118]. Βάσει των παραπάνω, τα βιομετρικά συστήματα μπορεί να χρησιμοποιηθούν με στόχο τη διάκριση πληθυσμών ανάλογα με τα χαρακτηριστικά τους. Περαιτέρω, το ιδιωτικό απόρρητο του χρήστη μπορεί να παραβιαστεί με αναγνώριση της ταυτότητας, της θέσης ή

των χρησιμοποιούμενων υπηρεσιών, λόγω της ισχυρής σχέσης του βιομετρικού δεδομένου με την ταυτότητα του χρήστη. Οι ανησυχίες στο χώρο της προστασίας του ιδιωτικού απορρήτου γίνονται εντονότερες αν αναλογιστούμε ότι τα περισσότερα ανθρώπινα χαρακτηριστικά δεν είναι δυνατό να διατηρηθούν μυστικά, λόγω της αλληλεπίδρασης του ανθρώπου με το περιβάλλον του, με πιο χαρακτηριστικό παράδειγμα το πρόσωπό του. Για το λόγο αυτό ο χρήστης πρέπει να ενημερώνεται για τη χρήση του συστήματος, προς αντιμετώπιση εφαρμογών πιστοποίησης χωρίς τη συγκατάθεση του χρήστη. Το βασικότερο μέτρο διαφύλαξης των προσωπικών δεδομένων και του ιδιωτικού απορρήτου του χρήστη είναι το σχετικό νομικό πλαίσιο, το οποίο υλοποιείται με τα κατάλληλα τεχνικά αντίμετρα [153].

Τα αποτελέσματα της αναλυτικής μελέτης για την εισαγωγή βιομετρικών στην αρχιτεκτονική 4ης γενιάς παρουσιάζονται στη συνέχεια.

3.3.2.1 Αποθήκευση βιομετρικών δεδομένων

Τα βιομετρικά δεδομένα θεωρούνται δεδομένα προσωπικού χαρακτήρα, λόγω της ισχυρής σχέσης τους με το άτομο στο οποίο ανήκουν. Σύμφωνα με ανάλυση της σχετικής νομοθεσίας [153], τα βιομετρικά δεδομένα πρέπει να αποθηκεύονται μόνο για ικανοποιητικά δικαιολογημένο σκοπό, αφότου ο χρήστης ενημερωθεί πλήρως και με σαφήνεια για αυτό, δημιουργώντας υψηλές απαιτήσεις για τους φορείς παροχής υπηρεσιών 4ης γενιάς, καθώς οι εφαρμογές δύσκολα δικαιολογούν την αποθήκευση βιομετρικών δεδομένων.

Τα πρωτογενή βιομετρικά δεδομένα είναι ιδιαίτερα ευαίσθητα, καθώς μπορεί να χρησιμοποιηθούν για εξαγωγή γενετικής ή ιατρικής πληροφορίας, αλλά και για τη δημιουργία βιομετρικών υπογραφών. Για το λόγο αυτό, προτείνεται τα πρωτογενή βιομετρικά δεδομένα, να μην αποθηκεύονται μόνιμα σε οποιοδήποτε μέσο αποθήκευσης, είτε στον φορέα παροχής υπηρεσιών 4ης γενιάς, είτε στη συσκευή του χρήστη, ενώ οι προσωρινές μνήμες να διαγράφονται με ασφάλεια.

Οι βιομετρικές υπογραφές πρέπει να αποθηκεύονται σε ασφαλή μέσα. Σύμφωνα με το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων που αναπτύξαμε, οι αρχιτεκτονικές κεντρικοποιημένης αποθήκευσης βιομετρικών υπογραφών εισάγουν σημαντική επικινδυνότητα στο σύστημα, αλλά και ερωτηματικά σχετικά με την ικανοποίηση

του σχετικού νομικού πλαισίου. Οι αρχιτεκτονικές αυτές είναι συνήθως αρκετά πολύπλοκες για να είναι και ασφαλείς, ενώ ο φορέας παροχής υπηρεσιών 4ης γενιάς πρέπει να υλοποιεί την αποθήκευση σε ζώνες, ώστε να μην συνδέονται άμεσα οι βιομετρικές υπογραφές με τις πραγματικές ταυτότητες των χρηστών. Η αποθήκευση βιομετρικών υπογραφών σε έξυπνες κάρτες – δηλαδή στη USIM στην προκειμένη περίπτωση - αποτελεί ασφαλέστερη προσέγγιση, η οποία όμως δεν στερείται αδυναμιών (αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής σύμφωνα με το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων).

Συνοψίζοντας τα παραπάνω η πιο ασφαλής προσέγγιση είναι η αποφυγή της αποθήκευσης βιομετρικών δεδομένων σε οποιοδήποτε μέσο, ούτε στην υποδομή του φορέα παροχής 4ης γενιάς ούτε στη USIM ή στην τερματική συσκευή του χρήστη.

3.3.2.2 Μετάδοση βιομετρικών δεδομένων

Διακρίνουμε δύο κατηγορίες τηλεπικοινωνιακών ζεύξεων κατά τη μετάδοση βιομετρικών δεδομένων. Τις τηλεπικοινωνιακές ζεύξεις της υποδομής 4ης γενιάς και τις τηλεπικοινωνιακές ζεύξεις στο εσωτερικό του τερματικού εξοπλισμού χρήστη, συμπεριλαμβανομένης της επικοινωνίας με τη USIM. Στην πρώτη κατηγορία, η ευαισθησία των βιομετρικών δεδομένων, όπως περιγράφηκε νωρίτερα, φανερώνει την ανάγκη για ισχυρούς μηχανισμούς ασφάλειας στην υποδομή 4ης γενιάς, ή προτιμότερα την ανάγκη για αποφυγή μετάδοσης βιομετρικής πληροφορίας (πρωτογενών βιομετρικών δεδομένων ή βιομετρικών υπογραφών). Στη δεύτερη κατηγορία, οι σχετικές σύμφωνα με τη μελέτη ασφάλειας της προηγούμενης παραγράφου αδυναμίες, όπως για παράδειγμα η αδυναμία ασφάλειας μετάδοσης (υποκλοπή σήματος και επανεκπομπή), πρέπει να αντιμετωπιστούν με τα κατάλληλα αντίμετρα. Σε κάθε περίπτωση πρέπει να διαφυλάσσονται η ακεραιότητα και η εμπιστευτικότητα της μεταδιδόμενης πληροφορίας.

3.3.2.3 Λειτουργίες συστήματος

Το βιομετρικό υποσύστημα του τερματικού εξοπλισμού 4ης γενιάς του χρήστη, αλλά και οι λειτουργίες της USIM, πρέπει να θωρακίζονται από τα σχετικά αντίμετρα σύμφωνα με το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων. Πιο συγκεκριμένα, το

βιομετρικό υποσύστημα πρέπει να υλοποιεί αντίμετρα για την αντιμετώπιση αδυναμιών, όπως η αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης, οι αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών, η αδυναμία αναγνώρισης εναπομένοντος χαρακτηριστικού, οι αδυναμίες σε θόρυβο, οι αδυναμίες διάκρισης παρόμοιων βιομετρικών υπογραφών οι αδυναμίες προστασίας ακεραιότητας συστατικών του συστήματος και οι αδυναμίες σε επιθέσεις ωμής δύναμης. Ειδικότερα η διαδικασία σύγκρισης της βιομετρικής υπογραφής (template matching) είναι ιδιαίτερα ευαίσθητη, τόσο ως αντικείμενο αλλοίωσης από πιθανή επίθεση, όσο και από παρακολούθηση του αποτελέσματος προς διευκόλυνση των επιθέσεων ωμής δύναμης. Τα σχετικά αντίμετρα περιγράφονται στο σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων, ενώ ο περιορισμός των παραπάνω λειτουργιών είναι επιθυμητός, όσο αυτό είναι εφικτό στο πλαίσιο εισαγωγής τους στην αρχιτεκτονική 4ης γενιάς.

3.3.2.4 Διαδικασίες εγγραφής και διαχείρισης

Σύμφωνα με το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων, οι διαδικαστικές αδυναμίες – η διαχείριση βιομετρικών δεδομένων και υπογραφών – εισάγουν το υψηλότερο ποσοστό επικινδυνότητας στο σύστημα. Σε ένα σενάριο κεντρικοποιημένης αποθήκευσης βιομετρικών δεδομένων, ο φορέας παροχής υπηρεσιών 4ης γενιάς πρέπει να υλοποιεί δαπανηρές διαδικασίες εγγραφής και διαχείρισης βιομετρικών δεδομένων. Η πιο οικονομική και ασφαλής λύση είναι ο εκμηδενισμός της ανάγκης για τις διαδικασίες εγγραφής και διαχείρισης βιομετρικών δεδομένων.

3.3.2.5 Σύνοψη προδιαγραφών πρωτοκόλλου

Η εισαγωγή βιομετρικών για την υλοποίηση ισχυρής πιστοποίησης ταυτότητας σε δίκτυα 3ης ή 4ης γενιάς, για να είναι οικονομική, λειτουργική και εύκολη στην υλοποίηση, πρέπει:

- να χρησιμοποιεί όσο είναι δυνατό τις υπάρχουσες υποδομές του τερματικού εξοπλισμού του χρήστη και της USIM,
- να είναι ελαφριά από άποψη τηλεπικοινωνιακού και υπολογιστικού φορτίου.

- δεν πρέπει να επιβαρύνει τον φορέα παροχής υπηρεσιών 4ης γενιάς, με την υποχρέωση δαπανηρών αλλαγών στην αρχιτεκτονική του,
- δεν πρέπει να επιβαρύνει τη διαδικασία προμήθειας συνδρομών από τους χρήστες,
- πρέπει να είναι απλή και απόλυτα διαφανής στο χρήστη, τον οποίο πρέπει να ενημερώνει για τη χρήση βιομετρικού συστήματος.

Σύμφωνα με τα όσα αναφέρθηκαν στις προηγούμενες παραγράφους και με στόχο το μέγιστο επίπεδο ασφάλειας και προστασίας των προσωπικών δεδομένων του χρήστη, συνοψίζουμε τις παρακάτω προδιαγραφές του πρωτοκόλλου:

- Η βιομετρική πιστοποίηση ταυτότητας πρέπει να πραγματοποιείται από άκρο σε άκρο.
- Τα βιομετρικά δεδομένα (πρωτογενή ή βιομετρικές υπογραφές) δεν πρέπει να αποθηκεύονται μόνιμα σε κανένα αποθηκευτικό μέσο.
- Τα βιομετρικά δεδομένα (πρωτογενή ή βιομετρικές υπογραφές) δεν πρέπει να μεταδίδονται πάνω από το δίκτυο 4ης γενιάς.
- Τα βιομετρικά δεδομένα, τα οποία μεταδίδονται στις τηλεπικοινωνιακές ζεύξεις στο εσωτερικό του τερματικού εξοπλισμού του χρήστη και μεταξύ αυτού και της USIM, πρέπει να προστατεύονται από επιθέσεις επανεκπομπής.
- Οποιαδήποτε μεταδιδόμενη πληροφορία πρέπει να προστατεύεται από άποψη εμπιστευτικότητας και ακεραιότητας.
- Ο τερματικός εξοπλισμός του χρήστη και η USIM πρέπει να υλοποιούν όλα τα αναγκαία αντίμετρα για την προστασία των λειτουργιών τους, δηλαδή ανίχνευση ζωτικότητας, γεννήτριες θορύβου, μικρο-ελεγκτές χαμηλής κατανάλωσης ενέργειας, σχεδιασμό λογισμικού με χαρακτηριστικά χρονικής ουδετερότητας, αμοιβαία πιστοποίηση ταυτότητας συστατικών του συστήματος, εισαγωγή τυχαίων τιμών στο σήμα και μηχανισμούς διαφύλαξης της ακεραιότητας αυτού. Πρέπει επίσης να εξασφαλιστεί η μοναδικότητα της τελικής μορφής κάθε βιομετρικού. Οι λειτουργίες που αφορούν το βιομετρικό τμήμα πρέπει να ελαχιστοποιηθούν και κυρίως εκείνη της σύγκρισης βιομετρικών υπογραφών ή άλλης μορφής βιομετρικών δεδομένων (matching).

- Η ανάγκη για εγγραφή στο σύστημα και διαχείριση βιομετρικών δεδομένων πρέπει να εκμηδενιστεί.

3.3.3 Περιγραφη πρωτοκολλου

Ονομάζουμε το πρωτόκολλο BIO4G (Biometrics in 4G). Το BIO4G υλοποιεί ισχυρή πραγματική πιστοποίηση του χρήστη σε δίκτυα 4ης γενιάς από άκρο σε άκρο και είναι συμβατό με τα αποτελέσματα της μελέτης. Εφαρμόζεται τόσο σε δίκτυα UMTS, όσο και σε UMTS/WLAN. Όσον αφορά στα δίκτυα CDMA2000 και CDMA2000/WLAN, το πρωτόκολλο μπορεί επίσης να εφαρμοστεί, καθώς το 3GPP2, υιοθέτησε με μικρές αλλαγές τον μηχανισμό UMTS-AKA για την ασφάλεια πρόσβασης στο δίκτυο [49].

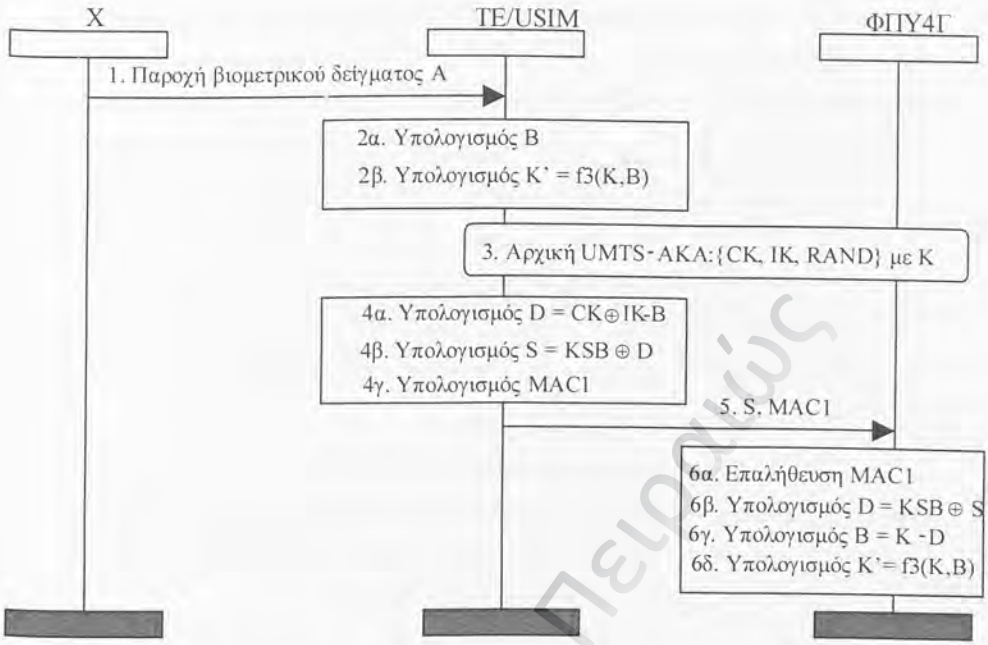
Ένα από τα βασικά συστατικά για την υλοποίηση του BIO4G, σύμφωνα με τις απαιτήσεις που ορίσθηκαν, είναι ο μετασχηματισμός των βιομετρικών δεδομένων σε μη αναστρέψιμα, τυχαία μυστικά, σύμφωνα με την περιγραφή της παραγράφου 2.3.3: Μετασχηματισμός βιομετρικών δεδομένων και τυχαιότητα.

Ορίζουμε τις ακόλουθες οντότητες:

- Χρήστης (X)
- Τερματικός εξοπλισμός και συνδεδεμένη κάρτα USIM (TE/USIM)
- Φορέας παροχής υπηρεσιών 4ης γενιάς (ΦΠΥ4Γ).

Το Σχήμα 29 παρουσιάζει το διάγραμμα ακολουθίας του BIO4G το οποίο είναι συμβατό με τη γλώσσα γραφικής αναπαράστασης Message Sequence Charts (MSC)[19], η οποία είναι τυποποιημένη από την International Telecommunication Union (ITU).

[19] http://www.sdl-forum.org/MSC/index.htm



Σχήμα 29: Το πρωτόκολλο BIO4G

Το πρωτόκολλο εκκινεί όταν ο χρήστης επιχειρεί πρόσβαση στον ΤΕ/USIM. Παρακάτω αναλύεται το διάγραμμα ακολουθίας του πρωτοκόλλου:

1. Ο Χ παρέχει ένα βιομετρικό δείγμα Α (μετά τη σχετική αίτηση για εισαγωγή δείγματος από τον ΤΕ) στο βιομετρικό αισθητήρα, ο οποίος είναι ενσωματωμένος στον ΤΕ και εκτελεί λειτουργίες ανίχνευσης ζωτικότητας, ανάλογα με τη βιομετρική μέθοδο που χρησιμοποιείται. Κατά την πρώτη βιομετρική μέτρηση, το βιομετρικό σύστημα εκτελεί έλεγχο ποιότητας του βιομετρικού δείγματος και πραγματοποιεί λήψη πολλαπλών δειγμάτων, ώστε να εξασφαλιστεί ότι η αρχική βιομετρική μέτρηση θα συλλέξει ένα αντιπροσωπευτικό δείγμα από το χρήστη. Επίσης ο αισθητήρας πρέπει να είναι σύγχρονος και να μη μπορεί να γίνει αντικείμενο επιθέσεων εναπομένοντος χαρακτηριστικού ή αδυναμίας διάκρισης παρόμοιων βιομετρικών. Αυτό εξασφαλίζεται κατά κύριο λόγο από τους αισθητήρες της αγοράς, αλλά πρέπει

πρώτα να υλοποιηθούν οι αναγκαίες δοκιμές, σύμφωνα με τις διεθνείς βέλτιστες πρακτικές [146].

2. Σε αυτό το βήμα:

   a) Ο ΤΕ δέχεται το βιομετρικό δείγμα Α και υπολογίζει ένα τυχαίο μη αναστρέψιμο 128-bit μυστικό αριθμό Β. Χρησιμοποιούνται κώδικες διόρθωσης λαθών με στόχο την εξασφάλιση του επανα-υπολογισμού του Β από ένα βιομετρικό δείγμα Α', το οποίο είναι αρκετά κοντά στο Α, σύμφωνα με την παράγραφο 2.3.3: Μετασχηματισμός βιομετρικών δεδομένων και τυχαιότητα. Πιο συγκεκριμένα, ορίζουμε f_{fe} τη συνάρτηση παραγωγής του Β από το Α. Η f_{fe} έχει τις εξής ιδιότητες:

      - Είναι ένα προς ένα και υλοποιεί διόρθωση λαθών για μέγιστο διάστημα απόκλισης d. Αυτό εκφράζεται ως εξής: αν T είναι το διάστημα απόκλισης μεταξύ δύο βιομετρικών δειγμάτων Α και Α', δηλαδή Α'=Α+Τ, τότε αν $T>d \Rightarrow f_{fe}(A) \neq f_{fe}(A')$, ενώ αν $T<d$, τότε $f_{fe}(A)=f_{fe}(A')$.
      - Είναι μονόδρομη, δηλαδή για δεδομένο το Β είναι πολύ δύσκολο υπολογιστικά να βρεθεί το Α.
      - Επίσης, πραγματοποιείται αμοιβαία πιστοποίηση ταυτότητας μεταξύ του βιομετρικού αισθητήρα και των υπολοίπων συστατικών του ΤΕ.

   b) Η τιμή Β προωθείται στη USIM. Πραγματοποιείται αμοιβαία πιστοποίηση ταυτότητας μεταξύ της USIM και του ΤΕ, με ένα μηχανισμό που βασίζεται σε ένα προσυμφωνημένο κρυπτογραφικό κλειδί, σύμφωνα με τις προδιαγραφές του 3GPP. Στη συνέχεια παράγεται ένα νέο μυστικό κλειδί Κ' από τη USIM, χρησιμοποιώντας την f3 συνάρτηση, η οποία δημιουργεί 128-bit κλειδιά με συνδυασμό δύο 128-bit τιμών – οι οποίες κατά τη φυσιολογική λειτουργία του UMTS-AKA είναι οι Κ και RAND. Η συνάρτηση που υλοποιεί τα παραπάνω είναι η ακόλουθη:

$$K' = f3(K, B)$$

3. Πραγματοποιείται ο μηχανισμός UMTS-AKA μεταξύ των USIM και ΠΥ4Γ, χρησιμοποιώντας το αρχικό κλειδί K. Σύμφωνα με τις συστάσεις του 3GPP, κατά τη φάση αυτή η USIM αναγνωρίζεται από το μόνιμο IMSI ή τις προσωρινές ταυτότητες TMSI, παράγεται ο τυχαίος αριθμός RAND από τον ΠΥ4Γ και αποστέλλεται στη USIM. Επίσης παράγονται τα κρυπτογραφικά κλειδιά CK και IK.

4. Σε αυτό το βήμα:

   a) Με στόχο την αποφυγή της άμεσης μετάδοσης του B, υπολογίζεται ένας νέος αριθμός D, σύμφωνα με την παρακάτω εξίσωση:

$$D = CK \oplus IK - B$$

   b) *O D* κρυπτογραφείται από τη USIM χρησιμοποιώντας τη συνάρτηση f8 του UMTS-AKA, σύμφωνα με την παρακάτω εξίσωση:

$$S = KSB \oplus D$$

   c) Υπολογίζεται ένας κώδικας αυθεντικοποίησης μηνυμάτων (MAC1) από τη USIM, για την προστασία της ακεραιότητας μηνύματος S, συμπεριλαμβάνοντας τον αριθμό RAND για προστασία από επιθέσεις επανεκπομπής.

5. Οι τιμές S και MAC1 αποστέλλονται στον ΠΥ4Γ.

6. Σε αυτό το βήμα:

   a) Επαληθεύεται ο MAC1.

   b) Υπολογίζεται ο D, σύμφωνα με την παρακάτω συνάρτηση:

$$D = KSB \oplus S$$

   c) Υπολογίζεται ο B, σύμφωνα με την παρακάτω συνάρτηση:

$$B = CK \oplus IK - D$$

d) Υπολογίζεται το κλειδί K' σύμφωνα με την παρακάτω συνάρτηση και αποθηκεύεται στη θέση του K, ενώ το B διαγράφεται οριστικά:

$$K' = f3(K, B)$$

Τα παραπάνω βήματα πραγματοποιούνται μόνο κατά την πρώτη σύνδεση του ΤΕ/USIM με τον ΠΥ4Γ. Μετά την ολοκλήρωσή των παραπάνω βημάτων, το K' είναι μοιρασμένο μεταξύ της USIM και του ΠΥ4Γ και αντικαθιστά το K, για την πραγματοποίηση του μηχανισμού UMTS-AKA στις επόμενες συνδέσεις, πιστοποιώντας την ταυτότητα του Χ από άκρο σε άκρο πραγματικά και ισχυρά, μόνο με πραγματοποίηση των βημάτων 1,2 και 3 του BIO4G. Υπογραμμίζεται ότι κατά το βήμα 2, το K' υπολογίζεται σε πραγματικό κάθε φορά χρόνο από το B (το οποίο δεν αποθηκεύεται ούτε στον ΤΕ/USIM ούτε στον ΠΥ4Γ).

Τα παραπάνω ισχύουν όταν ο χρήστης βρίσκεται τόσο σε σύνδεση UMTS, όσο και σεUMTS/WLAN. Σχετικά με την επικοινωνία στο εσωτερικό του ΠΥ4Γ, όταν ο χρήστης βρίσκεται σε σύνδεση UMTS/WLAN, το δίκτυο πρόσβασης WLAN, απλώς προωθεί τα μηνύματα του πρωτοκόλλου, όπως προωθεί και τα μηνύματα του UMTS-AKA με υλοποίηση του μηχανισμού EAP-AKA, όπως περιγράφεται στην παράγραφο 2.1.3: Αρχιτεκτονική 4ης γενιάς – Συνδυασμένα δίκτυα 3ης γενιάς με ασύρματα τοπικά δίκτυα.

3.3.4 ΑΞΙΟΛΟΓΗΣΗ ΠΡΩΤΟΚΟΛΛΟΥ

Στην ενότητα αυτή αξιολογούμε το πρωτόκολλο ως προς την ασφάλεια, της προστασία των προσωπικών δεδομένων του χρήστη, την απόδοση, την ευχρηστία και την πολυπλοκότητα υλοποίησης αυτού.

3.3.4.1 Ασφάλεια

Η αξιολόγηση της ασφάλειας του πρωτοκόλλου γίνεται σε τρία στάδια, λόγω της αυξημένης ευαισθησίας των δεδομένων που εμπεριέχονται στη λειτουργία αυτού:

- Εξέταση ασφάλειας συνολικής λειτουργίας του πρωτοκόλλου: Αρχικά, εξετάζεται αν τα κατάλληλα αντίμετρα είναι υλοποιημένα ώστε να αντιμετωπίζονται όλα τα είδη επιθέσεων. Για το σκοπό αυτό, χρησιμοποιείται η δομή βάσει της οποίας η IETF εκφράζει θέματα ασφάλειας για τα πρωτόκολλα που παράγει.
- Εξειδικευμένη εξέταση ασφάλειας βιομετρικού συστατικού: Στη συνέχεια, εξετάζεται η ασφάλεια όσον αφορά στη χρήση βιομετρικών συστημάτων, χρησιμοποιώντας το σύστημα αποτίμησης επικινδυνότητας βιομετρικών συστημάτων που αναπτύξαμε νωρίτερα.
- Εξειδικευμένη εξέταση και επαλήθευση ασφάλειας πιστοποίησης ταυτότητας χρήστη μέσω συναρτήσεων κατάταξης. Τέλος χρησιμοποιούμε συναρτήσεις κατάταξης CSP, για την εξέταση και επαλήθευση της ασφάλειας πιστοποίησης της ταυτότητας χρήστη, που είναι και ο βασικός στόχος του πρωτοκόλλου. Για την ανάλυσή μας επικεντρωνόμαστε στα μηνύματα που ανταλλάσσονται πάνω από το δίκτυο 4ης γενιάς, καθώς η διακίνηση μηνυμάτων στα εσωτερικά συστατικά του TE, της USIM και του βιομετρικού συστατικού αναλύεται στο προηγούμενο στάδιο (εξειδικευμένη εξέταση ασφάλειας βιομετρικού συστατικού).

3.3.4.1.1 Εξέταση ασφάλειας συνολικής λειτουργίας του πρωτοκόλλου

Το BIO4G αξιολογείται βάσει της προσέγγισης του Internet Engineering Task Force (IETF) για την αξιολόγηση της ασφάλειας των προτύπων Request For Comments (RFC) που εκδίδει. Η προσέγγιση αυτή αφορά στη μελέτη συγκεκριμένων περιοχών ασφάλειας. Οι περιοχές οι οποίες μελετώνται για το BIO4G είναι οι ακόλουθες:

- **Διαφύλαξη ταυτότητας χρήστη και προσωπικών δεδομένων:** Το BIO4G υλοποιεί εξελιγμένη προστασία ταυτότητας χρήστη και προσωπικών δεδομένων και αντιμετωπίζει επιθέσεις παθητικής και ενεργητικής παρακολούθησης πληροφορίας που μπορεί να αποκαλύψουν την ταυτότητα, τη θέση και τις υπηρεσίες που χρησιμοποιεί ο χρήστης, αλλά και οποιασδήποτε προσωπικής ή μη πληροφορίας που συνδέεται με την ταυτότητα αυτού. Πιο συγκεκριμένα, τα βιομετρικά δεδομένα μετασχηματίζονται σε μη αναστρέψιμα τυχαία μυστικά, τα οποία δεν περιέχουν κανένα στοιχείο ταυτότητας ή οποιοδήποτε άλλο προσωπικό στοιχείο του χρήστη. Τα μυστικά αυτά (B) χρησιμοποιούνται για την παραγωγή νέων μυστικών κλειδιών K', τα οποία υλοποιούν την ισχυρή από άκρο ως άκρο πιστοποίηση του χρήστη. Επιπλέον, το τυχαίο μυστικό B, το οποίο αποτελεί μη αναστρέψιμο μετασχηματισμό των βιομετρικών δεδομένων, μεταδίδεται μόνο μία φορά (την πρώτη φορά λειτουργίας του πρωτοκόλλου), έμμεσα ως D (διαφορά με ένα κώδικα) και κρυπτογραφημένο (S). Αυτό σημαίνει ότι ένας πιθανός εισβολέας πρέπει τη μια και μόνο φορά που μεταδίδεται το S να καταφέρει να το αποκτήσει, να το αποκρυπτογραφήσει (επιτιθέμενος στον κρυπτογραφικό αλγόριθμο του UMTS-AKA) για να αποκαλύψει το D και να υπολογίσει το B, αφού καταφέρει να αποκαλύψει την τιμή CK⊕ IK. Ακόμα και σε αυτό το υπερβολικό σενάριο, ο εισβολέας θα πρέπει να καταφέρει να αντιστρέψει τον μη-αντιστρέψιμο αριθμό B, ώστε να μπορέσει να φτάσει στα προσωπικά βιομετρικά δεδομένα του χρήστη.
- **Αμοιβαία πιστοποίηση ταυτότητας οντοτήτων:** Ο TE/USIM και ο ΠΥ4Γ πιστοποιούν αμοιβαία της ταυτότητές τους μέσω του μηχανισμού UMTS-AKA. Ο Χ πιστοποιεί την ταυτότητά του από άκρο σε άκρο στον ΠΥ4Γ μέσα από τη λειτουργία του BIO4G. Η USIM και ο ΤΕ πιστοποιούνται αμοιβαία μέσω ενός μηχανισμού προσυμφωνημένου κρυπτογραφικού κλειδιού, σύμφωνα με τις συστάσεις του 3GPP [78].
- **Εμπιστευτικότητα:** Η εμπιστευτικότητα της μεταδιδόμενης πληροφορίας εξασφαλίζεται με τη χρήση του κρυπτογραφικού κλειδιού CK και του αντίστοιχου αλγορίθμου f8, σύμφωνα με τις συστάσεις του 3GPP για το μηχανισμό UMTS-AKA.

- **Ακεραιότητα:** Η ακεραιότητα της μεταδιδόμενης πληροφορίας εξασφαλίζεται με τη χρήση του κρυπτογραφικού κλειδιού IK και του αντίστοιχου αλγορίθμου παραγωγής κωδίκων αυθεντικοποίησης μηνυμάτων (MAC) του μηχανισμού UMTS-AKA, σύμφωνα με τις συστάσεις του 3GPP.
- **Προστασία από επιθέσεις επανεκπομπής:** Το πρωτόκολλο έχει ενσωματωμένα αντίμετρα προστασίας από επιθέσεις επανεκπομπής (replay attacks). Τα αντίμετρα αυτά αφορούν κυρίως τα βήματα 1,2 και 3 του πρωτοκόλλου, καθώς όλα τα υπόλοιπα υλοποιούνται μόνο μία φορά. Το πρώτο αντίμετρο είναι η εναλλαγή των διανυσμάτων πιστοποίησης ταυτότητας (Authentication Vectors) του UMTS-AKA, η οποία προκαλεί και αλλαγή των αντιστοίχων παραμέτρων του BIO4G (CK και IK). Το δεύτερο αντίμετρο είναι η εναλλαγή του TMSI σύμφωνα με τον UMTS-AKA μηχανισμό. Τέλος, ένα τρίτο αντίμετρο είναι η χρήση του τυχαίου RAND στο βήμα 4c, το οποίο εξασφαλίζει τη μοναδικότητα του σχετικού μηνύματος, το οποίο ούτως ή άλλως μεταδίδεται μόνο μία φορά.
- **Προστασία από επιθέσεις ενδιάμεσης οντότητας:** Οι επιθέσεις αυτού του τύπου αντιμετωπίζονται με την υλοποίηση της εμπιστευτικότητας, ακεραιότητας και προστασίας από επιθέσεις επανεκπομπής, όπως περιγράφηκαν παραπάνω.
- **Προστασία από επιθέσεις ωμής δύναμης και λεξικού:** Το BIO4G δεν είναι πρωτόκολλο που βασίζεται σε συνθηματικά. Οι επιθέσεις ωμής δύναμης σε βιομετρικά συστήματα, είναι εξειδικευμένες και υλοποιούνται συνήθως με παρακολούθηση του αλγορίθμου σύγκρισης των βιομετρικών υπογραφών και ανάλογα με τα αποτελέσματα αυτού, αποστέλλονται ολοένα και πιο πιθανές τιμές κοντά στην πραγματική. Λειτουργία σύγκρισης στο BIO4G δεν υλοποιείται, ενώ η αποστολή τυχαίων αριθμών για την εύρεση ενός μυστικού 128-bit, όπως το B, είναι ιδιαίτερα δύσκολη εώς απίθανη.
- **Παραγωγή κρυπτογραφικών κλειδιών:** Τα κρυπτογραφικά κλειδιά (CK και IK) παράγονται από το μηχανισμό UMTS-AKA κληρονομώντας το επίπεδο ασφάλειας των αντίστοιχων συστάσεων του 3GPP.
- **Παραγωγή τυχαίων αριθμών:** Η τυχαιότητα του παραγόμενου μυστικού B εξασφαλίζεται από τη βιβλιογραφία [185].

3.3.4.1.2 Εξειδικευμένη εξέταση ασφάλειας βιομετρικού συστατικού

Η αποτίμηση επικινδυνότητας πραγματοποιείται βάσει του συστήματος αποτίμησης επικινδυνότητας βιομετρικών συστημάτων που αναπτύξαμε νωρίτερα. Το BIO4G, δεν είναι ευάλωτο στις παρακάτω αδυναμίες:

- Αδυναμία αναγνώρισης ομοιωμάτων και τεχνικών μίμησης: Καθώς έχουν προβλεφθεί αντίμετρα ανίχνευσης ζωτικότητας.
- Κληρονομήσιμες αδυναμίες κεντρικοποιημένων αρχιτεκτονικών - πλαστές βιομετρικές υπογραφές: καθώς δεν ακολουθείται κεντρικοποιημένη αρχιτεκτονική και τα βιομετρικά δεδομένα δεν αποθηκεύονται πουθενά μόνιμα.
- Αδυναμία ασφάλειας μετάδοσης - υποκλοπή σήματος και επανεκπομπή: Καθώς έχουν προβλεφθεί τα κατάλληλα αντίμετρα, όπως περιγράφηκε στην προηγούμενη παράγραφο.
- Αδυναμίες επαναχρησιμοποίησης βιομετρικών υπογραφών: Καθώς δεν χρησιμοποιούνται βιομετρικές υπογραφές και η μοναδικότητα των παραγόμενων μυστικών είναι εγγυημένη και ανά εφαρμογή, λόγω του συνδυασμού του τυχαίου Β με το μοναδικό κλειδί Κ.
- Αδυναμία προστασίας ακεραιότητας συστατικών του συστήματος: Καθώς είναι υλοποιημένα τα κατάλληλα αντίμετρα.
- Διαδικαστικές αδυναμίες - διαχείριση βιομετρικών δεδομένων και υπογραφών: Καθώς απουσίαζαν οι σχετικές διαδικασίες και η σχετική ανάγκη για την ύπαρξη αυτών.
- Αδυναμίες σε θόρυβο και λειτουργία εκτός των επιτρεπόμενων ορίων: καθώς αυτού του είδους οι επιθέσεις δεν μπορούν να οδηγήσουν το πρωτόκολλο στο ζητούμενο, το οποίο είναι η δημιουργία του τυχαίου αριθμού Β.
- Αδυναμία αναγνώρισης εναπομένοντος χαρακτηριστικού: Καθώς υπάρχει η σχετική πρόβλεψη στο BIO4G.
- Αδυναμίες διάκρισης παρόμοιων βιομετρικών υπογραφών: Καθώς υπάρχει η σχετική πρόβλεψη στο BIO4G.

- Αδυναμίες σε επιθέσεις ωμής δύναμης: Όπως αναλύθηκε στην προηγούμενη παράγραφο.
- Αδυναμίες στο σύστημα διαχείρισης ταυτότητας: Όπως αναλύθηκε στην προηγούμενη παράγραφο.

Η μόνη αδυναμία που πιθανώς αφορά στο πρωτόκολλο είναι η ακόλουθη:

- Αδυναμίες μυστικότητας λειτουργιών μικροηλεκτρονικής: Καθώς δεν υπάρχει εγγύηση ότι οι USIM υλοποιούν τα κατάλληλα αντίμετρα.

Σύμφωνα με τα παραπάνω, προκύπτει ένα ελάχιστο ποσοστό επικινδυνότητας 3%, το οποίο αντιστοιχεί στο μοναδικό παράγοντα επικινδυνότητας της αδυναμίας μυστικότητας λειτουργιών μικροηλεκτρονικής, όπως τον ορίζει ο Πίνακας 2.

3.3.4.1.3 Εξειδικευμένη εξέταση και επαλήθευση ασφάλειας πιστοποίησης ταυτότητας χρήστη μέσω συναρτήσεων κατάταξης

Για την ανάλυσή μας επικεντρωθήκαμε στα μηνύματα που ανταλλάσσονται πάνω από το δίκτυο 4ης γενιάς, καθώς η διακίνηση μηνυμάτων στα εσωτερικά συστατικά του ΤΕ, της USIM και του βιομετρικού συστατικού αναλύθηκε στο προηγούμενο στάδιο. Για το σκοπό αυτό, δημιουργούμε το μοντέλο CSP του πρωτοκόλλου και στη συνέχεια το αναλύουμε. Η ασφάλεια του βιομετρικού συστήματος θεωρείται ισχυρή, όπως και η εσωτερική επικοινωνία των ΤΕ και USIM. Στόχος μας είναι η εξέταση και επαλήθευση της ασφάλειας πιστοποίησης ταυτότητας χρήστη.

3.3.4.1.3.1 Μοντέλο CSP

Χρησιμοποιούμε την άλγεβρα CSP για να μοντελοποιήσουμε το πρωτόκολλο, ώστε να είναι εφικτή στη συνέχεια η εξέταση και η επαλήθευση της ασφάλειας του.

Χρησιμοποιούμε τα ακόλουθα κανάλια επικοινωνίας:

- Κανάλι `biosample`: το κανάλι για την απόκτηση του βιομετρικού δείγματος από τον βιομετρικό αισθητήρα.

- Κανάλια `submit` και `accept`: Τα κανάλια επικοινωνίας μεταξύ της USIM και του ΤΕ (ο οποίος στη μοντελοποίηση αναφέρεται ως UE- User Equipment).
- Κανάλια `send` και `receive`. Τα κανάλια επικοινωνίας του δικτύου 4ης γενιάς, δηλαδή τα κανάλια μεταξύ του ΤΕ/USIM και ΠΥ4Γ (ο οποίος στη μοντελοποίηση αναφέρεται ως MO – Mobile Operator).

Οι εκφράσεις της άλγεβρας CSP, όπου και ορίζεται μία διαδικασία για τον ΤΕ (UE), τη USIM και τον ΠΥ4Γ (MO), παρουσιάζονται παρακάτω.

`UE(a) = biosample?a →` // Ορισμός UE να δέχεται ως είσοδο α από κανάλι biosample

`Running.UE.USIM.a →` // Συνεργασία UE και USIM για το α

`submit.UE.USIM!`f_{1e}`(a) → Stop` // Παραγωγή της τιμής Β από USIM και αποστολή στον UE

`USIM(ksb,ck,ik,k) = accept.USIM.UE?b →` // Λήψη τιμής Β από UE

`Running.USIM.mo.b.k' →` // Συνεργασία (UMTS-AKA) MO και USIM για τα β, κ'

`send.USIM!mo!(ksb⊕ d,|ksb⊕ d|`$_{ik}$`) → Stop` // Αποστολή τιμών BIO4G μεταξύ USIM και MO

`MO(ksb,ck,ik,k)`

`= receive.MO?usim?(ksb⊕ d,|ksb⊕ d|`$_{ik}$`) →` // Λήψη τιμών από MO

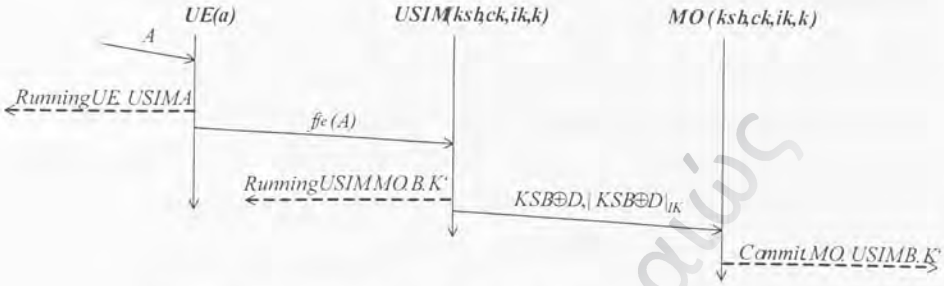
`Commit.MO.usim.b.k' → Stop` // Μοναδική λειτουργία του UMTS-AKA με χρήση του K'

Το μοντέλο δικτύου CSP παρουσιάζεται παρακάτω:

`NET = ((UE(a)`$_{\{submit\}||\{accept\}}$`USIM(ksb,ck,ik,k)) ||| MO(ksb,ck,ik,k)) || Medium`

όπου η έκφραση (`UE(a)`$_{\{submit\}||\{accept\}}$`USIM(ksb,ck,ik,k)`) αφορά στην συνδυασμένη οντότητα ΤΕ/USIM η οποία λειτουργεί παράλληλα με την οντότητα που αντιστοιχεί στο ΠΥ4Γ, ή σύμφωνα με το μοντέλο στον `MO(ksb,ck,ik,k)`. Στο μοντέλο δικτύου αναφέρεται

και μια διαδικασία, η Medium, η οποία εκφράζει την επικοινωνία μεταξύ των δύο οντοτήτων ΤΕ/USIM και ΠΥ4Γ, δηλαδή το δίκτυο 4ης γενιάς. Το Σχήμα 30, παρουσιάζει τη λειτουργία του πρωτοκόλλου σύμφωνα με την ορολογία της CSP.



Σχήμα 30: Λειτουργία BIO4G με την ορολογία της CSP

Στο Σχήμα 30, με τα πλάγια βέλη, απεικονίζουμε τα μηνύματα που ανταλλάσσει το πρωτόκολλο και με τα διακεκομμένα βέλη τα σχετικά γεγονότα. Πιο συγκεκριμένα απεικονίζουμε:

- Με πλάγιο βέλος την αποστολή του βιομετρικού δείγματος A προς τον ΤΕ και με διακεκομμένο το γεγονός Running.UE.USIM.A, το οποίο εκφράζει τη συνεργασία των ΤΕ και USIM, όσον αφορά στην τιμή A.
- Με πλάγιο βέλος την αποστολή του B= f_{1e}(A) από τον ΤΕ στη USIM και με διακεκομμένο το γεγονός Running.USIM.MO.B.K', το οποίο εκφράζει τη συνεργασία των USIM και MO, όσον αφορά στην τιμή K' που παράγεται από το B και η οποία είναι ουσιαστικά το νέο συμφωνημένο κλειδί για την εκτέλεση του UMTS-AKA.
- Με πλάγιο βέλος την αποστολή των S και MAC1, από τη USIM στον ΠΥ4Γ και με διακεκομμένο το γεγονός Commit.MO.USIM.B.K', για να εκφράσουμε τον τελικό στόχο του πρωτοκόλλου, δηλαδή τη μοναδική λειτουργία του UMTS-AKA με χρήση του K', μέσω του B, που συντελεί τελικά την πιστοποίηση ταυτότητας του χρήστη.

Μετά τη μοντελοποίηση, ορίζουμε ως απαίτηση ασφάλειας την ουσία του πρωτοκόλλου, δηλαδή την πιστοποίηση ταυτότητας χρήστη από τον ΠΥ4Γ. Αυτό απεικονίζεται από τις παρακάτω δύο προτάσεις προς απόδειξη:

Πρόταση 1:

$$\begin{aligned}&\text{BIO4G\_Auth\_Key}(tr) = tr' \,\hat{}\, \langle \text{Commit.MO.USIM.B.K'} \rangle \\ &\quad \leq tr \Rightarrow \langle \text{Running.USIM.MO.B.K'} \rangle \\ &\text{in } tr' \,\hat{}\, \#(tr \restriction \text{Running.USIM.MO.B.K'}) \\ &\quad \geq \#(tr \restriction \text{Commit.MO.USIM.B.K'}).\end{aligned}$$

Το πρώτο μέρος του ορισμού του BIO4G_Auth_Key(tr) ορίζει το προβάδισμα του γεγονότος Running.USIM.MO.B.K' από το γεγονός Commit.MO.USIM.B.K', που αντιστοιχεί στην ανταλλαγή του K', πριν τη λειτουργία του UMTS-AKA με χρήση του K'.

Το δεύτερο μέρος (συμφωνία κλειδιού), ορίζει τη δέσμευση ότι για κάθε Commit.MO.USIM.B.K', υπάρχει ένα μοναδικό Running.USIM.MO.B.K', το οποίο προηγείται του Commit.MO.USIM.B.K'.

Το δίκτυο NET, ικανοποιεί την απαίτηση ασφάλειας, αν όλα τα ίχνη του ικανοποιούν αυτό που παραπάνω ορίσθηκε ως απαίτηση ασφάλειας BIO4G_Auth_Key(tr). Αυτό εκφράζεται ως εξής:

$$\text{NET sat BIO4G\_Auth\_Key} \Leftrightarrow \forall tr \in \text{traces(NET)} \bullet \text{BIO4G\_Auth\_Key}(tr)$$

Πρόταση 2:

$$\begin{aligned}&\text{BIO4G\_User\_Auth}(tr) = tr' \,\hat{}\, \langle \text{Commit.MO.USIM.B.K'} \rangle \\ &\quad \leq tr \Rightarrow \langle \text{Running.UE.USIM.A} \rangle \\ &\text{in } tr' \,\hat{}\, \#(tr \restriction \text{Running.UE.USIM.A})\end{aligned}$$

$$\geq \#(tr \upharpoonright Commit.MO.USIM.B.K')$$

Η πρόταση αυτή εκφράζει την πιστοποίηση της ταυτότητας του χρήστη μέσω του πρωτοκόλλου. Το πρώτο μέρος της παραπάνω σχέσης ορίζει το προβάδισμα του γεγονότος Running.UE.USIM.A από το γεγονός Commit.MO.USIM.B.K'. Το δεύτερο μέρος ορίζει ότι όποτε ο ΠΥ4Γ επαληθεύει ένα σωστό βιομετρικό δείγμα A (μέσω του σωστού K', το οποίο παράχθηκε από το σωστό B, το οποίο παράχθηκε από το σωστό A) μέσω της λειτουργίας του πρωτοκόλλου ο νόμιμος χρήστης θα πρέπει να έχει λάβει μέρος στη βιομετρική μέτρηση. Το δίκτυο NET, ικανοποιεί την απαίτηση ασφάλειας, αν όλα τα ίχνη του ικανοποιούν αυτό που παραπάνω ορίσθηκε ως απαίτηση ασφάλειας BIO4G_User_Auth(tr), δηλαδή:

$$NET \text{ sat } BIO4G\_User\_Auth \Leftrightarrow$$

$$\forall tr \in traces(NET) \bullet BIO4G\_User\_Auth(tr)$$

3.3.4.1.3.2 Στρατηγική απόδειξης

Εξετάζουμε την ασφάλεια του πρωτοκόλλου, σύμφωνα με τις απαιτήσεις ασφάλειας που θέσαμε κατά τη μοντελοποίησή του κατά CSP. Για το σκοπό αυτό εισάγουμε μια οντότητα εισβολέα, την οποία απεικονίζουμε και στο δίκτυο ως εξής:

$$NET=((UE(A)_{\{submit\}} \mid\mid_{\{accept\}} USIM(KSB,CK,IK,K)) \mid\mid\mid MO(KSB,CK,IK,K)) \mid\mid Intruder$$

Αντικαθιστούμε δηλαδή τη διαδικασία Medium, η οποία εξέφραζε το μέσο επικοινωνίας των οντοτήτων, με μια διαδικασία εισβολέα, η οποία πλέον παρεμβάλλεται της επικοινωνίας και η οποία έχει συγκεκριμένες δυνατότητες κατά Dolev και Yao.

Στόχος μας είναι να επαληθεύσουμε την ουσία του πρωτοκόλλου, την πιστοποίηση δηλαδή από τον ΠΥ4Γ του βιομετρικού δείγματος A, μέσω του ορθού B άρα και K'. Πιο συγκεκριμένα, στόχος μας είναι να επαληθεύσουμε την ισχύ της Πρότασης 2, δηλαδή ότι κάθε φορά που ο ΠΥ4Γ πιστοποιεί (έμμεσα) ένα βιομετρικό δείγμα A, το οποίο εκφράζεται ως Commit.MO.USIM.B.K', το βιομετρικό αυτό δείγμα, έχει αποσταλεί στη USIM από τον ΤΕ, το οποίο εκφράζεται ως Running.UE.USIM.A.

Επίσης, θέλουμε να επαληθεύσουμε την Πρόταση 1 και πιο συγκεκριμένα, το προβάδισμα του Running.USIM.MO.B.K' από το Commit.MO.USIM.B.K'. Για το σκοπό αυτό, περιορίζουμε το δίκτυο, έτσι ώστε να μην έχει τη δυνατότητα να εκτελέσει το γεγονός Running.USIM.MO.B.K' και ελέγχουμε αν είναι δυνατή ή όχι η εμφάνιση του γεγονότος Commit.MO.USIM.B.K'. Τα παραπάνω εκφράζονται ως εξής:

$$\forall tr \in traces(\mathbf{NET} \underset{Running.USIM.MO.B.K'}{\|} Stop)$$

$$\bullet \mathbf{NET} \underset{Running.USIM.MO.B.K'}{\|} Stop$$

$$\mathbf{sat} tr \lceil Commit.MO.USIM.B.K' = <>$$

δηλαδή ελέγχουμε αν το δίκτυο επιτρέπει τη συμφωνία ΠΥ4Γ και USIM στο νέο κλειδί K', αν η ανταλλαγή των σχετικών παραμέτρων από το πρωτόκολλο δεν έχει υλοποιηθεί. Περιορίζουμε έτσι το δίκτυο στο γεγονός Running.USIM.MO.B.K', δηλαδή με την εμφάνιση του γεγονότος αυτού όλες οι διαδικασίες τερματίζεται και δεν επιτρέπεται άλλο γεγονός να εμφανιστεί στη συνέχεια. Έτσι ελέγχουμε, αν δημιουργώντας μια πρόκληση Running.USIM.MO.B.K', ο εισβολέας μπορεί να χρησιμοποιήσει μηνύματα για να φτάσει στη συμφωνία Commit.MO.USIM.B.K'.

3.3.4.1.3.3 Δημιουργία συνάρτησης κατάταξης

Βάσει της στρατηγικής απόδειξης της ασφάλειας, δημιουργούμε μια συνάρτηση κατάταξης και αξιολογούμε διαφορετικές συνθήκες σύμφωνα με το θεώρημα του Schneider, για την επαλήθευση της ασφάλειας του πρωτοκόλλου. Για το σκοπό αυτό, υποθέτουμε ότι οι ταυτότητες των ΤΕ, USIM και ΠΥ4Γ (ή UE, USIM και MO αντίστοιχα σύμφωνα με τη μοντελοποίηση), έχουν πλαστογραφηθεί από τον εισβολέα. Στη συνέχεια, αναθέτουμε θετικούς και μη συντελεστές κατάταξης, ανάλογα με το αν τα συστατικά του πρωτοκόλλου μπορεί ή όχι να αποκαλυφθούν αντίστοιχα, χωρίς να προσβληθεί η ασφάλεια.

Στον X θέτουμε μη-θετικό συντελεστή κατάταξης, καθώς στην ανάλυσή μας ο εισβολέας δεν μπορεί να πλαστοπροσωπήσει τον χρήστη (επιθέσεις σε βιομετρικά αναλύθηκαν προηγουμένως). Μη-θετικό συντελεστή κατάταξης έχουν και οι παράμετροι KSB, CK, IK και

K, που στη μοντελοποίηση αναφέρονται με μικρούς χαρακτήρες και οι οποίες υποθέτουμε ότι κατέχονται τέλεια από τη USIM και τον ΠΥ4Γ. Το κλειδί K' και το βιομετρικό δείγμα A, έχουν και αυτά μη-θετικό συντελεστή κατάταξης. Τα μηνύματα $KSB \oplus D$ και $|KSB \oplus D|_{IK}$, έχουν επίσης μη-θετικό συντελεστή κατάταξης, καθώς δεν πρέπει να εμφανίζονται στο περιορισμένο $NET \underset{Running.USIM.MO.B.K'}{\|} Stop$.

Επιπλέον ορίζουμε τα σύνολα του θεωρήματος του Schneider R και T, σύμφωνα με τη στρατηγική της προηγούμενης παραγράφου, ως εξής:

R = { Running.USIM.MO.B.K'} T = {Commit.MO.USIM.B.K'}

καθώς κατά Schneider τα R και T, ορίζονται έτσι ώστε το R να είναι το γεγονός που θέλουμε να αποδείξουμε ότι προηγείται του T.

Θετικό συντελεστή κατάταξης έχει το γεγονός Running.USIM.MO.B.K', καθώς μπορεί να εμφανιστεί, αλλά αν εμφανιστεί το δίκτυο NET σταματά, σύμφωνα με τον περιορισμό $NET \underset{Running.USIM.MO.B.K'}{\|} Stop$. Μη-θετικό συντελεστή κατάταξης έχει το Commit.MO.USIM.B.K', το οποίο δεν επιθυμούμε να εμφανιστεί, όσο δεν εμφανίζεται το Running.USIM.MO.B.K'. Στη συνέχεια, παρουσιάζεται η συνάρτηση κατάταξης, αντικατοπτρίζοντας όλα όσα περιγράφηκαν παραπάνω:

- ρ(A) = 0
- ρ(KSB⊕ D) = 0
- ρ(|KSB⊕ D|IK) = 0
- ρ(u) = 0 αν u = X, αλλιώς ρ(u) = 1, συμπεριλαμβανομένου του u = UE ν u = USIM ν u = MO
- ρ(K) = 0 αν k = K ν k = K' ν k = CK ν k = IK και ρ(K) = 1 σε άλλη περίπτωση
- ρ(ffe(m)) = 0 αν ρ(m) = 1, αλλιώς ρ(ffe(m)) = 1
- ρ(m1.m2) = min{ρ(m1).ρ(m2)}
- ρ(ksb) = 0 αν ksb = KSB, αλλιώς ρ(ksb) = 1
- ρ(f3(k,m)) = 1 αν ρ(k) = 1 ^ ρ(m) = 1, αλλιώς ρ(f3(k,m)) = 0
- ρ(|m|k) = 1 αν ρ(m) = 1 ^ ρ(k) = 1, αλλιώς ρ(|m|k) = 0

- $\rho(m1 \oplus m2) = 1$ αν $\rho(m1) = \rho(m2)$, αλλιώς $\rho(m1 \oplus m2) = 0$
- $\rho(Running.USIM.MO.B.K') = 1$
- $\rho(Commit.MO.USIM.B.K') = 0$

Προς επεξήγηση των παραπάνω, ορίζουμε τα ακόλουθα:

- Η συνένωση δύο μηνυμάτων m1 και m2 είναι θετικού συντελεστή, αν και τα δύο μηνύματα είναι θετικού συντελεστή.
- Το "αποκλειστικό ή" δύο μηνυμάτων είναι θετικού συντελεστή αν και τα δύο είναι του ίδιου συντελεστή. Αυτό μεταφράζεται στο ότι αν είναι και τα δύο θετικού συντελεστή, τότε είναι γνωστά στον εισβολέα ούτως ή άλλως, ενώ αν είναι μη-θετικού συντελεστή, τότε το "αποκλειστικό ή" αυτών μπορεί να σταλεί πάνω από δημόσιο κανάλι χωρίς τον εισβολέα να μπορεί να αποκαλύψει κάποιο από αυτά.
- Η έξοδος της συνάρτησης f_K είναι θετικού συντελεστή, μόνο αν η είσοδος είναι θετικού συντελεστή.
- Το μήνυμα MAC1, το οποίο σύμφωνα με την μοντελοποίηση έχει την τιμή $|m|_k$. Η τιμή αυτή είναι θετικού συντελεστή, μόνο αν το μήνυμα m και το κλειδί k είναι θετικού συντελεστή.
- Η συνάρτηση f3 του UMTS-AKA, η οποία έχει έξοδο $f_3(k,m)$, είναι θετικού συντελεστή μόνο αν και οι δύο παράμετροι k και m, είναι θετικού συντελεστή.

3.3.4.1.3.4 Επαλήθευση ασφάλειας

Αρχικά, επεκτείνουμε τις σχέσεις του τελεστή '$\vdash$', έτσι ώστε να περιλαμβάνει όχι μόνο τις δυνατότητες του εισβολέα κατά Dolev-Yao, αλλά και όλα όσα περιγράφηκαν στην προηγούμενη παράγραφο. Με τον τρόπο αυτό, εξειδικεύουμε την επαλήθευση ασφάλειας στο συγκεκριμένο πρωτόκολλο. Εκτός από τις σχέσεις της παραγράφου 2.5.1.3: Το μοντέλο δικτύου του Schneider, προσθέτουμε τις ακόλουθες:

- $\{m1, m2\} \vdash m1 \oplus m2$ // Από τα m1, m2, μπορεί να παραχθεί το XOR αυτών
- $\{m1 \oplus m2, m2\} \vdash m1$ // Από τα $m1 \oplus m2$ και m2, μπορεί να παραχθεί το m1
- $\{m1 \oplus m2, m1\} \vdash m2$ // Από τα $m1 \oplus m2$ και m1, μπορεί να παραχθεί το m2
- $\{m\} \vdash ffe(m)$ // Από το m μπορεί να παραχθεί το ffe(m)

- $\{m,k\} \vdash |m|k$ // Από τα m και k μπορεί να παραχθεί το m|k
- $\{m,k\} \vdash f3(k,m)$ // Από τα m και k μπορεί να παραχθεί το f3(k,m)

Στη συνέχεια, ελέγχουμε αν η συνάρτηση κατάταξης που ορίσαμε στην προηγούμενη παράγραφο, ικανοποιεί τις συνθήκες του θεωρήματος του Schneider.

- **Συνθήκη 1:** $\forall\ m \in InK \bullet \rho(m) > 0$

  Το σύνολο InK, απεικονίζει τη γνώση του εισβολέα στην αρχή του πρωτοκόλλου (Initial Knowledge). Συμπεριλαμβάνουμε στους εισβολείς και άλλους χρήστες που λαμβάνουν τις ίδιες υπηρεσίες από τον ΠΥ4Γ, γι' αυτό ορίζουμε υπό την κατοχή τους τις παραμέτρους *KSB'*, *CK'* and IK_I'. Επιπλέον, ο εισβολέας θα έχει υπό την κατοχή του και εκείνος ένα κλειδί που μοιράζεται με τον ΠΥ4Γ, το K_I. Το σύνολο λοιπόν InK, περιλαμβάνει όλη αυτή τη γνώση, δηλαδή $InK = \{UE, USIM, MO, KSB', CK', IK_I', K_I\}$. Καθώς στο σύνολο InK, δεν υπάρχει συστατικό με μη-θετικό συντελεστή κατάταξης, η συνθήκη αυτή ικανοποιείται.

- **Συνθήκη 2:** $\forall\ S \subseteq M,\ m \in M \bullet ((\forall m' \in S \bullet \rho(m') > 0) \wedge S \vdash m) \Rightarrow \rho(m) > 0$

  Η συνθήκη αυτή ελέγχει αν ένα μήνυμα μη-θετικού συντελεστή κατάταξης μπορεί να παραχθεί με χρήση του τελεστή '$\vdash$' σε ένα σύνολο μηνυμάτων θετικού συντελεστή κατάταξης. Κανένα από τα μηνύματα θετικού συντελεστή κατάταξης της συνάρτησης κατάταξης που ορίσαμε δεν επιτρέπει στον εισβολέα να παράγει μηνύματα μη-θετικού συντελεστή. Επιπλέον, ο X και το βιομετρικό δείγμα A, είναι εκτός εμβέλειας του εισβολέα. Έχουμε υποθέσει ότι οι παράμετροι *KSB*, *CK*, *IK*, *K* και *K'*, είναι ασφαλώς μοιρασμένοι μεταξύ του TE/USIM και ΠΥ4Γ, μέσα από την ασφαλή λειτουργία του UMTS-AKA. Ο εισβολέας δεν είναι σε θέση να παράγει μηνύματα μη-θετικού συντελεστή, όπως τα $KSB \oplus D$ or $|KSB \oplus D|_{IK}$, άρα η συνθήκη ικανοποιείται.

- **Συνθήκη 3:** $\forall\ t \in T \bullet \rho(t) < 0$

  Η συνθήκη αυτή υπαγορεύει, τα γεγονότα του T να μην είναι θετικού συντελεστή κατάταξης. Το μόνο γεγονός που ανήκει στο T, είναι το μη θετικού συντελεστή γεγονός-μήνυμα $Commit.MO.USIM.B.K'$, άρα η συνθήκη αυτή ικανοποιείται.

- **Συνθήκη 4:** $\forall\ i \in U \bullet User_i \underset{R}{\|} Stop$ **maintains** ρ

Για την ικανοποίηση της συνθήκης αυτής, όλες οι διαδικασίες του δικτύου πρέπει να διατηρήσουν (maintain) την κατάταξή τους ρ, ενώ είναι περιορισμένες από το να χρησιμοποιήσουν γεγονότα του συνόλου R, όπου R = {Running.USIM.MO.B.K'}. Για το σκοπό αυτό, εξετάζουμε τις διαδικασίες *UE(A)*, *USIM(KSB,CK,IK,K)* και *MO(KSB,CK,IK,K))*, περιορισμένες από το να χρησιμοποιήσουν το γεγονός Running.USIM.MO.B.K'. Η μόνη διαδικασία η οποία μπορεί να εκτελέσει το Running.A.B.NB. είναι η *UE(A)*, ενώ οι υπόλοιπες παραμένουν ανεπηρέαστες. Η διαδικασία ορίζεται ως εξής:

UE(A) = biosample?A →

Running.UE.USIM.A

submit.UE.USIM!f_{1e}(A) → Stop

Η διαδικασία *UE(A)* δεν περιορίζει τη μετάδοση της μη-θετικού συντελεστή τιμής $f_{1e}(A)$, στο κανάλι submit. Το κανάλι submit δεν είναι όμως δημόσιο κανάλι και αφορά στην επικοινωνία μεταξύ TE και USIM, άρα ο εισβολέας δεν έχει πρόσβαση στο κανάλι αυτό (τα μόνα δημόσια κανάλια είναι αυτά του δικτύου 4ης γενιάς, η μετάδοση πληροφορίας πάνω από το οποίο είναι η μόνη η οποία εξετάζεται σύμφωνα με την εισαγωγή του 3.3.4.1.3: Εξειδικευμένη εξέταση και επαλήθευση ασφάλειας πιστοποίησης ταυτότητας χρήστη μέσω συναρτήσεων κατάταξης). Άρα η διαδικασία *UE(A)*, διατηρεί το ρ.

Η διαδικασία USIM(KSB,CK,IK,K) μετά τον περιορισμό στη μη χρήση του Running.USIM.MO.B.K' ορίζεται ως ακολούθως:

USIM(KSB,CK,IK,K) $\underset{Running.USIM.MO.B.K'}{\|}$ Stop = accept.USIM.UE?B →

if b = B ^ k = K'

then Stop

else Running.USIM.MO.b.k' →

send.USIM!MO!(ksb⊕ d_1|ksb⊕ $d|_{1k}$) → Stop

Τα παραπάνω, έχουν την εξής σημασία: αν η διαδικασία $USIM(KSB,CK,IK,K) \underset{Running.USIM.MO.B.K'}{\|} Stop$ δεχθεί την τιμή B, η οποία οδηγεί στον υπολογισμό του K', τότε είναι προγραμματισμένη να σταματήσει. Για τιμή όμως $b \neq B$, η διαδικασία συνεχίζει να συμπεριφέρεται κανονικά, με τις κατάλληλες τιμές. Επιπλέον, λόγω του περιορισμού της διαδικασίας δεν της επιτρέπεται η εκπομπή των μη-θετικού συντελεστή $KSB\oplus D$ ή $|KSB\oplus D|_{IK}$, άρα η διαδικασία επιτυγχάνει να διατηρήσει το ρ.

Η διαδικασία MO(KSB,CK,IK,K), παραμένει ανεπηρέαστη του περιορισμού:

$$MO(KSB,CK,IK,K) = receive.MO?USIM?(KSB\oplus D, |KSB\oplus D|_{IK}) \rightarrow$$

$$Commit.MO.USIM.B.K' \rightarrow Stop$$

Δηλαδή, αν η διαδικασία αυτή δεν δεχθεί το μήνυμα $KSB\oplus D, |KSB\oplus D|_{IK}$, τότε δεν εκτελεί το Commit.MO.USIM.B.K'. Ο μόνος τρόπος για να εκτελέσει το μήνυμα, είναι να δεχθεί το παραπάνω συνενωμένο μήνυμα, το οποίο απαγορεύεται από την υπόθεση της συγκεκριμένης συνθήκης. Τελικά η διαδικασία επιτυγχάνει να διατηρήσει το ρ.

Συμπεραίνουμε ότι και οι τέσσερις συνθήκες του θεωρήματος του Schneider, ικανοποιούνται από τη συνάρτηση κατάταξης που ορίσαμε. Αυτό διαβεβαιώνει ότι:

$$\forall tr \in traces\ (NET \underset{Running.USIM.MO.B.K'}{\|} Stop) \bullet NET \underset{Running.USIM.MO.B.K'}{\|} Stop\ \mathbf{sat}$$

$$tr\lceil Commit.MO.USIM.B.K' = <>$$

Αποδείξαμε δηλαδή το πρώτο σκέλος της Πρότασης 1.

Στη συνέχεια αποδεικνύουμε το πρώτο σκέλος της Πρότασης 2, ότι δηλαδή:

$$\forall tr \in traces\ (NET \underset{Running.UE.USIM.A}{\|} Stop) \bullet NET \underset{Running.UE.USIM.A}{\|} Stop\ \mathbf{sat}$$

$$tr\lceil Commit.MO.USIM.B.K' = <>$$

Το δίκτυο ορίζεται ως:

$$NET = ((UE(A)_{\{submit\}} || _{\{accept\}}USIM(KSB,CK,IK,K)) \;|||\; MO(KSB,CK,IK,K)) \;||\; Intruder$$

Επικεντρωνόμαστε στο συστατικό $((UE(A)_{\{submit\}} || _{\{accept\}}USIM(KSB,CK,IK,K))$, το οποίο αναπαριστά την παράλληλη λειτουργία των ΤΕ και USIM. Κάθε φορά που η USIM δέχεται την τιμή Β, η τιμή αυτή έχει αποσταλεί από τον ΤΕ ($B = f_{fe}(A)$), λόγω της εσωτερικής επικοινωνίας των δύο συστατικών, η οποία αναπαρίσταται ως προδιαγραφή ίχνους ως εξής:

$$tr' \hat{} \langle Running.USIM.MO.B.K' \rangle < tr \Rightarrow \langle Running.UE.USIM.A \rangle \text{ in } tr'$$

Συνεπώς, ισχύει ότι:

$$\forall tr \in traces((UE(A)_{\{submit\}} || _{\{accept\}}USIM(KSB,CK,IK,K)) \bullet tr' \hat{} \langle Running.USIM.MO.B.K' \rangle < tr \Rightarrow \langle Running.UE.USIM.A \rangle \text{ in } tr'$$

Καθώς το υπόλοιπο δίκτυο δεν μπορεί να παρεμβληθεί στα παραπάνω, το σύνολο του δικτύου ικανοποιεί τα παρακάτω:

$$\forall\, tr \in traces(NET) \bullet tr' \hat{} \langle Running.USIM.MO.B.K' \rangle < tr \Rightarrow \langle Running.UE.USIM.A \rangle \text{ in } tr'$$

Έχουμε ήδη αποδείξει από την Πρόταση 1, ότι:

$$\forall\, tr \in traces(NET) \bullet tr' \hat{} \langle Commit.MO.USIM.B.K' \rangle < tr \Rightarrow \langle Running.USIM.MO.B.K' \rangle \text{ in } tr'$$

άρα:

$$\forall\, tr \in traces(NET) \bullet tr' \hat{} \langle Commit.MO.USIM.B.K' \rangle < tr \Rightarrow \langle Running.UE.USIM.A \rangle \text{ in } tr'$$

το οποίο μεταφράζεται στο ότι κάθε φορά που ο ΠΥ4Γ επαληθεύει έμμεσα την τιμή Β, το βιομετρικό δείγμα Α, έχει γίνει δεκτό από τον ΤΕ. Αποδείξαμε δηλαδή την ισχύ του πρώτου σκέλους της Πρότασης 2.

Οι Προτάσεις 1 και 2, πέρα των όσων επαληθεύθηκαν στην προηγούμενη παράγραφο, απαιτούν την απόδειξη κάποιων σχέσεων μοναδικότητας. Πιο συγκεκριμένα, απαιτείται στο

δεύτερο σκέλος της Πρότασης 1, η ύπαρξη μοναδικού Running.USIM.MO.B.K', για κάθε *Commit.MO.USIM.B.K'*, ή αλλιώς:

$$\#(tr \lceil Running.USIM.MO.B.K') > \#(tr \lceil Commit.MO.USIM.B.K')$$

ενώ στο δεύτερο σκέλος της Πρότασης 2, η ύπαρξη μοναδικού *Running.UE.USIM.A*, για κάθε Commit.MO.USIM.B.K', ή αλλιώς:

$$\#(tr \lceil Running.UE.USIM.A) > \#(tr \lceil Commit.MO.USIM.B.K')$$

Σύμφωνα με την εργασία του Schneider, το θεώρημα το οποίο βασίζεται σε συναρτήσεις κατάταξης, δεν παρέχει τη δυνατότητα επαλήθευσης μιας σχέσεως μοναδικότητας. Κάτι τέτοιο όμως δε θα ήταν ούτως ή άλλως αναγκαίο για το συγκεκριμένο πρωτόκολλο, καθώς η απόδειξη των δεύτερων σκελών των δύο Προτάσεων (1 και 2) είναι απλή μέσα από την ίδια τη ροή του πρωτοκόλλου, η οποία δεν επιτρέπει την επανάληψη της συμφωνίας σε ένα κοινό κλειδί K'. Τα βήματα του πρωτοκόλλου 4, 5 και 6, τα οποία και εκφράζουν τη διαδικασία ανταλλαγής του K', πραγματοποιούνται μοναδικά και μόνο όταν ο χρήστης συνδεθεί για πρώτη φορά στον ΠΥ4Γ.

3.3.4.2 Απόδοση, ευχρηστία και πολυπλοκότητα υλοποίησης

Το BIO4G χρησιμοποιεί τις υπάρχουσες υποδομές του τερματικού εξοπλισμού του χρήστη και της USIM και δεν επιβαρύνει τον φορέα παροχής υπηρεσιών 4ης γενιάς με την υποχρέωση δαπανηρών αλλαγών στην αρχιτεκτονική του.

Οι συναρτήσεις που υλοποιεί προϋπάρχουν στο σύνολο του μικροκώδικα της USIM και αφορούν σε απλές διαφορές ή πράξεις <<αποκλειστικού ή>> (exclusive or) της άλγεβρας Boole. Το μόνο επιπλέον τμήμα λογισμικού το οποίο απαιτείται, αφορά στην παραγωγή του τυχαίου αριθμού B, από ένα βιομετρικό δείγμα καθώς και στις λοιπές βιομετρικές λειτουργίες. Όσο αφορά στον αριθμό των μεταδιδόμενων μηνυμάτων, ανέρχεται στο μόλις ένα μήνυμα, επιπλέον των μηνυμάτων του κλασσικού μηχανισμού UMTS-AKA, το οποίο μάλιστα μεταδίδεται μία μόνο φορά. Κατά τη φυσιολογική λειτουργία (εκτός της πρώτης ζεύξης ΠΥ4Γ και ΤΕ/USIM) του πρωτοκόλλου, δεν υπάρχει αύξηση του αριθμού των μυνημάτων του UMTS-AKA, κάτι το οποίο κάνει το πρωτόκολλο ιδιαίτερα ελαφρύ.

Το BIO4G, εξαλείφει την ανάγκη δαπανηρών, χρονοβόρων και νομικά επικίνδυνων διαδικασιών εγγραφής στο σύστημα καθώς και διαχείρισης βιομετρικών δεδομένων και δεν επιβαρύνει τη διαδικασία προμήθειας συνδρομών από τους χρήστες. Η λειτουργία του πρωτοκόλλου ενημερώνει για τη χρήση βιομετρικού συστήματος, κατά την αίτηση στο χρήστη για παροχή βιομετρικού δείγματος και στη συνέχεια είναι απόλυτα διαφανής και απλή.

3.3.5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Λόγω της αυξημένης ευαισθησίας των βιομετρικών δεδομένων και των υποχρεώσεων που προκύπτουν από το αντίστοιχο νομικό πλαίσιο [153], η εισαγωγή τους στη διαδικασία πιστοποίησης ταυτότητας χρήστη είναι ιδιαίτερα απαιτητική. Για τη σχεδίαση του BIO4G ακολουθήθηκε μια μεθοδική διαδικασία προσδιορισμού απαιτήσεων και εξαγωγής προδιαγραφών, όσο αφορά σε θέματα ασφάλειας, προστασίας προσωπικών δεδομένων, ευχρηστίας, οικονομικότητας και πολυπλοκότητας. Το αποτέλεσμα ικανοποιεί τις ορισθείσες προδιαγραφές, υλοποιώντας από άκρο σε άκρο ισχυρή και πραγματική πιστοποίηση ταυτότητας χρήστη στον φορέα παροχής υπηρεσιών 4ης γενιάς με ένα μηχανισμό ο οποίος δεν απαιτεί μόνιμη αποθήκευση ή μετάδοση βιομετρικών δεδομένων, καθώς και διαδικασίες διαχείρισης αυτών και είναι ασφαλής, οικονομικός, εύχρηστος, απλός και συμβατός με τις προδιαγραφές πιστοποίησης ασφάλειας των Common Criteria. Το πρωτόκολλο BIO4G, βελτιώνει το μηχανισμό UMTS-AKA, ο οποίος στηρίζεται πλέον σε παράγοντες ισχυρής πιστοποίησης χρήστη και όχι σε ένα απλό PIN.

3.4 ΕΝΣΩΜΑΤΩΜΕΝΟ ΠΡΩΤΟΚΟΛΛΟ ΔΙΑΧΕΙΡΙΣΗΣ ΤΑΥΤΟΤΗΤΑΣ ΓΙΑ ΕΦΑΡΜΟΓΕΣ ΔΙΑΔΙΚΤΥΟΥ ΠΑΝΩ ΑΠΟ ΑΣΥΡΜΑΤΑ ΕΥΡΥΖΩΝΙΚΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΑ ΔΙΚΤΥΑ 3ΗΣ ΚΑΙ 4ΗΣ ΓΕΝΙΑΣ

3.4.1 ΠΕΡΙΓΡΑΦΗ ΣΤΟΧΟΥ ΚΑΙ ΠΡΟΣΕΓΓΙΣΗΣ

Η παρούσα προτεινόμενη λύση, αντιμετωπίζει το ακόλουθο πρόβλημα:

Η χρήση υπαρχόντων πρωτοκόλλων διαχείρισης ταυτότητας χρήστη για υπηρεσίες στο Διαδίκτυο πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς επιβαρύνει την απόδοση του συστήματος, δεν αξιοποιεί τις νέες αρχιτεκτονικές και δημιουργεί ερωτηματικά ασφάλειας. Δεν υπάρχει ενοποιημένο πρωτόκολλο διαχείρισης ταυτότητας για εφαρμογές Διαδικτύου πάνω από δίκτυα 3ης και 4ης γενιάς..

Στόχος είναι η δημιουργία ενός πρωτοκόλλου διαχείρισης ταυτότητας χρήστη για εφαρμογές διαδικτύου πάνω από δίκτυα 4ης γενιάς, σύμφωνα με τις απαιτήσεις των διεθνών προτύπων του χώρου, το οποίο να έχει βελτιωμένη απόδοση σε σχέση με τις υπάρχουσες λύσεις. Πιο συγκεκριμένα, το πρωτόκολλο πρέπει να είναι:

- Διαφανές στο χρήστη.
- Να υποστηρίζει πολλαπλές ταυτότητες για κάθε χρήστη.
- Να είναι ελαφρύ.
- Να προστατεύει τα προσωπικά δεδομένα του χρήστη.
- Να είναι διαλειτουργικό.
- Να είναι ασφαλές.
- Να υλοποιεί επαρκώς ισχυρή πιστοποίηση ταυτότητας χρήστη.
- Να συνδέει ασφαλώς τις έννοιες της αναγνώρισης, πιστοποίησης και εξουσιοδότησης.

Για την υλοποίηση των παραπάνω στο συγκεκριμένο περιβάλλον 4ης γενιάς, συνενώσαμε τους ρόλους του φορέα παροχής υπηρεσιών 4ης γενιάς και της έμπιστης τρίτης οντότητας παροχής υπηρεσιών ταυτότητας και συνδυάσαμε τις προδιαγραφές διαχείρισης ταυτότητας, με τα πρότυπα τηλεπικοινωνιακών συστημάτων 3ης γενιάς και 4ης γενιάς και πιο συγκεκριμένα, τις προδιαγραφές του Liberty Alliance, τη γλώσσα SAML και τις πιο πρόσφατες συστάσεις του 3GPP για την αρχιτεκτονική και την ασφάλεια των συστημάτων.

3.4.2 Περιγραφη πρωτοκολλου

Ονομάζουμε το πρωτόκολλο IDM4G (Identity Management in 4G). Το IDM4G, υλοποιεί αμοιβαία πιστοποίηση ταυτότητας μεταξύ χρήστη και φορέα παροχής υπηρεσιών στο Διαδίκτυο. Εφαρμόζεται τόσο σε δίκτυα UMTS, όσο και σε δίκτυα UMTS/WLAN. Όσον

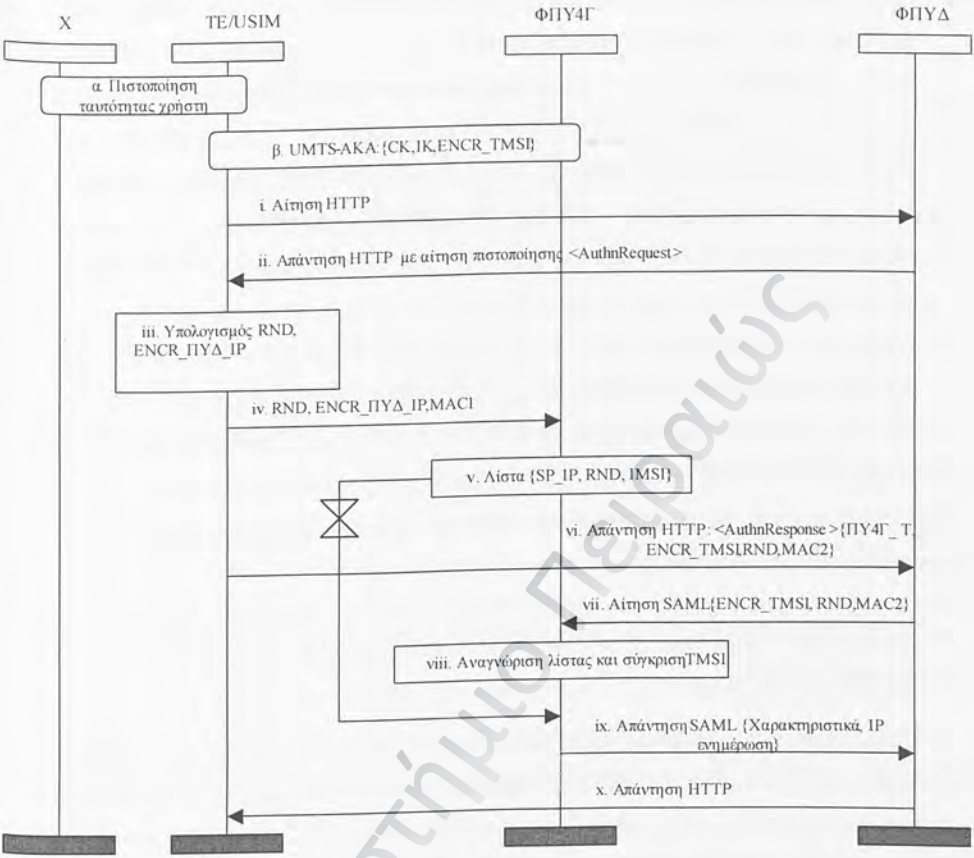
αφορά στα δίκτυα CDMA2000 και CDMA2000/WLAN, το πρωτόκολλο μπορεί επίσης να εφαρμοστεί, καθώς το 3GPP2, υιοθέτησε τον μηχανισμό UMTS-AKA για την ασφάλεια πρόσβασης στο δίκτυο.

Ορίζουμε τις ακόλουθες οντότητες:

- Χρήστης (Χ)
- Τερματικός εξοπλισμός και συνδεδεμένη κάρτα USIM (ΤΕ/USIM)
- Φορέας παροχής υπηρεσιών 4ης γενιάς (ΠΥ4Γ)
- Φορέας παροχής υπηρεσιών στο διαδίκτυο (ΦΠΥΔ).

Σύμφωνα με τις συστάσεις του Liberty Alliance, ο εντολέας είναι ο Χ, ο φορέας παροχής υπηρεσιών ταυτότητας είναι ο ΠΥ4G και ο φορέας παροχής υπηρεσιών είναι ο ΦΠΥΔ. Το Σχήμα 31 παρουσιάζει το διάγραμμα ακολουθίας του IDM4G, το οποίο είναι συμβατό με τη γλώσσα γραφικής αναπαράστασης Message Sequence Charts (MSC)[20].

[20] http://www.sdl-forum.org/MSC/index.htm



Σχήμα 31: Διάγραμμα ακολουθίας του πρωτοκόλλου IDM4G

Το πρωτόκολλο υποθέτει τα ακόλουθα σε αντιστοιχία με τα σχετικά πρωτόκολλα διαχείρισης ταυτότητας:

- Υπάρχει καθορισμένη επιχειρηματική και τεχνική συμφωνία εμπιστοσύνης μεταξύ του ΠΥ4Γ και του ΦΠΥΔ. Ο ΦΠΥΔ μπορεί να είναι σε συμφωνία με διαφορετικό ΠΥ4Γ, εξασφαλίζοντας την μη περιοριστική φύση του πρωτοκόλλου. Στην περίπτωση αυτή, τα απαραίτητα στοιχεία πιστοποίησης (μέσα από τα μηνύματα του πρωτοκόλλου) ανταλλάσσονται μεταξύ των δύο ΠΥ4Γ, όπως και στην περίπτωση απλής πιστοποίησης χρήστη σε σενάριο περιαγωγής. Σημειώνεται ότι αντίστοιχη συμφωνία εμπιστοσύνης υπάρχει μεταξύ του Χ και του ΠΥ4Γ, λόγω της συνδρομής του πρώτου στον δεύτερο.
- Υπάρχει προσυμφωνημένο μοντέλο αμοιβαίας κατανόησης ταυτοτήτων μεταξύ του ΠΥ4Γ και του ΦΠΥΔ.. Το μοντέλο αυτό βασίζεται σε ένα σύνολο χαρακτηριστικών για κάθε Χ, τα οποία αντιστοιχούν σε δικαιώματα πρόσβασης στις υπηρεσίες του ΦΠΥΔ και όχι σε πραγματικές ταυτότητες χρηστών.

Οι ακόλουθες δύο φάσεις προηγούνται του IDM4G καθώς πραγματοποιούνται όποτε ο Χ προσπαθεί να συνδεθεί στον ΠΥ4Γ:

α. Ο χρήστης πιστοποιείται τοπικά στον TE/USIM με τη χρήση ενός PIN, σύμφωνα με τις προδιαγραφές του 3GPP.

β. Πραγματοποιείται ο μηχανισμός UMTS-AKA μεταξύ του USIM και του ΠΥ4Γ. Κατά τη φάση αυτή, παράγονται τα κλειδιά CK (για διατήρηση μυστικότητας) και IK (για διατήρηση ακεραιότητας), σύμφωνα με τις προδιαγραφές του 3GPP, καθώς και η προσωρινή ταυτότητα TMSI η οποία κρυπτογραφείται στην τιμή ENCR_TMSI και αποστέλλεται στη USIM.

Η εκκίνηση του πρωτοκόλλου πραγματοποιείται όταν ο Χ δοκιμάζει να συνδεθεί με μία περιοχή του ΦΠΥΔ που απαιτεί πιστοποίηση ταυτότητας και εξουσιοδότηση. Παρακάτω αναλύεται το διάγραμμα ακολουθίας του πρωτοκόλλου:

i. Κατά την προσπάθεια σύνδεσης του Χ σε περιοχή του ΦΠΥΔ που απαιτεί πιστοποίηση ταυτότητας και εξουσιοδότηση αποστέλλεται μια αίτηση HTTP Request.
ii. Ο ΦΠΥΔ απαντάει με μία αίτηση πιστοποίησης ταυτότητας Authentication Request.

iii. Ο TE/USIM, υπολογίζει ένα τυχαίο αριθμό RND και κρυπτογραφεί τη διεύθυνση IP του ΦΠΥΔ με χρήση του κρυπτογραφικού αλγόριθμου f8 και του κλειδιού CK, που παράχθηκε στο βήμα β.

iv. Η τιμή RND και η κρυπτογραφημένη διεύθυνση IP του ΦΠΥΔ (ENCR_ΦΠΥΔ_IP), αποστέλλονται στον ΠΥ4Γ. Υπολογίζεται ένας κώδικας αυθεντικοποίησης μηνυμάτων MAC1 για το παραπάνω μήνυμα (με χρήση του IK) και επισυνάπτεται σε αυτό για διασφάλιση της ακεραιότητάς του. Η μοναδικότητα του τυχαίου αριθμού RND εξασφαλίζει και τη μοναδικότητα του μηνύματος προς αντιμετώπιση επιθέσεων επανεκπομπής.

v. Ο ΠΥ4Γ επαληθεύει τον MAC1, αποκρυπτογραφεί το ENCR_ΦΠΥΔ_IP προς αναγνώριση του ΦΠΥΔ και στη συνέχεια συνδυάζει την ταυτότητα IMSI του Χ (η οποία έχει αναγνωριστεί και πιστοποιηθεί στο βήμα β) με τη διεύθυνση IP του ΦΠΥΔ (ΦΠΥΔ_IP) και το RND. Ο συνδυασμός των τριών αυτών τιμών σε μία κοινή λίστα ορίζει ότι ο ΠΥ4Γ θα πρέπει να περιμένει μία αίτηση με ετικέτα RND από τον συγκεκριμένο ΦΠΥΔ για τον Χ με το συγκεκριμένο IMSI. Η λίστα αυτή θα πρέπει να αποθηκευθεί μαζί με το τρέχον διάνυσμα πιστοποίησης ταυτότητας (Authentication Vector - AV) του Χ, προς αποφυγή προβλημάτων συγχρονισμού, αν εν τω μεταξύ αλλάζει το AV. Η λίστα θα πρέπει να είναι ενεργή για περιορισμένο χρονικό διάστημα, το οποίο θα πρέπει να είναι προσυμφωνημένο μεταξύ του ΦΠΥΔ και του ΠΥ4Γ.

vi. Ο TE/USIM αποστέλλει μια απάντηση πιστοποίησης ταυτότητας στον ΦΠΥΔ, η οποία περιέχει την ταυτότητα του ΠΥ4Γ (ΠΥ4Γ_Τ), την κρυπτογραφημένη προσωρινή ταυτότητα ENCR_TMSI, η οποία αποκτήθηκε στο βήμα β, την τιμή RND και ένα κώδικα αυθεντικοποίησης μηνυμάτων MAC2 υπολογισμένο στο συνολικό μήνυμα προς διαφύλαξη της ακεραιότητας αυτού.

vii. Ο ΦΠΥΔ, αναγνωρίζει τον ΠΥ4Γ και του αποστέλλει μία αίτηση SAML Request [91] για τα χαρακτηριστικά του χρήστη, η οποία περιλαμβάνει τα ENCR_TMSI, RND και MAC2.

viii. Ο ΠΥ4Γ, αναγνωρίζει τον ΦΠΥΔ και συνδυάζει το ΦΠΥΔ_IP με το RND για να ανακαλύψει την αντίστοιχη λίστα. Η εύρεση της λίστας, σηματοδοτεί και την ταυτότητα IMSI του Χ, τα κλειδιά του οποίου (CK και IK) χρησιμοποιούνται για την αποκρυπτογράφηση του ENCR_TMSI και την επαλήθευση του MAC2 αντίστοιχα.

ix. Αν η σύγκριση του αποθηκευμένου και του απεσταλμένου TMSI είναι θετική, ο ΠΥ4Γ, στέλνει μια απάντηση SAML response [91] στον ΦΠΥΔ. Η απάντηση περιέχει τα χαρακτηριστικά πρόσβασης του χρήστη που αντιστοιχούν στα δικαιώματα αυτού, χωρίς να αποκαλύψει την ταυτότητά του. Επίσης αποστέλλεται και μια ενημέρωση της διεύθυνσης IP του ΤΕ/USIM, ώστε να είναι σε θέση ο ΦΠΥΔ να επικοινωνήσει ορθά στην περίπτωση που η διεύθυνση IP του ΤΕ/USIM έχει αλλάξει κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου (η αλλαγή προβλέπεται για διάφορους λόγους από τη λειτουργία του δικτύου 3ης και 4ης γενιάς από το 3GPP).

x. Ο ΦΠΥΔ αποστέλλει μια απάντηση στον ΤΕ/USIM, που του επιτρέπει την πρόσβαση στις υπηρεσίες του.

Σύμφωνα με την ορολογία του Liberty Alliance [92], το μοντέλο είναι έμμεσο / έμμεσο, καθώς ο Χ και ο ΦΠΥΔ δεν έχουν άμεσες επιχειρηματικές και τεχνικές συμφωνίες αλλά έμμεσες μέσω του ΠΥ4Γ.

3.4.3 ΑΞΙΟΛΟΓΗΣΗ ΠΡΩΤΟΚΟΛΛΟΥ

Κατά τη σχεδίαση του πρωτοκόλλου μελετήθηκε αναλυτικά το ιδιαίτερο τεχνικό περιβάλλον των δικτύων 4ης γενιάς, καθώς και οι περιορισμοί των κινητών τερματικών συσκευών. Το πρωτόκολλο μετά τη σχεδίασή του αξιολογήθηκε ως προς την ασφάλεια, την απόδοση και την πολυπλοκότητα.

3.4.3.1 Ασφάλεια

Η ασφάλεια του πρωτοκόλλου μελετήθηκε προσεκτικά, λαμβάνοντας υπόψη τη σύγχρονη βιβλιογραφία και κυρίως τις προδιαγραφές και απαιτήσεις ασφάλειας των 4ης γενιάς δικτύων. Λήφθηκε επίσης υπόψη η προσέγγιση του Internet Engineering Task Force (IETF)

για την παρουσίαση της ασφάλειας των προτύπων που εκδίδει. Διακρίνουμε τις ακόλουθες περιοχές:

- **Διαφύλαξη ταυτότητας χρήστη και προσωπικών δεδομένων:** Το IDM4G υλοποιεί εξελιγμένη προστασία ταυτότητας χρήστη και προσωπικών δεδομένων και αντιμετωπίζει επιθέσεις παθητικής και ενεργητικής παρακολούθησης πληροφορίας που μπορεί να αποκαλύψουν την ταυτότητα, τη θέση και τις υπηρεσίες που χρησιμοποιεί ο χρήστης, αλλά και οποιασδήποτε προσωπικής ή μη πληροφορίας που συνδέεται με την ταυτότητα αυτού. Πιο συγκεκριμένα, το IMSI και οποιαδήποτε μόνιμη ταυτότητα χρήστη δεν εκπέμπεται. Ο χρήστης αναγνωρίζεται από τον ΠΥ4Γ μέσω προσωρινών τυχαίων αναγνωριστικών (TMSI), η συσχέτιση των οποίων με τη μόνιμη ταυτότητα του χρήστη (IMSI) γίνεται μόνο τοπικά στην υποδομή του ΠΥ4Γ. Ο ΦΠΥΔ λαμβάνει πληροφορία σχετικά με τον χρήστη, μόνο με τη μορφή χαρακτηριστικών που συνδέονται αυστηρά με δικαιώματα χρήσης που εμπεριέχουν στοιχεία ταυτότητας και άλλα προσωπικά δεδομένα.
- **Αμοιβαία πιστοποίηση ταυτότητας οντοτήτων:** Αμοιβαία πιστοποίηση υλοποιείται μεταξύ όλων των οντοτήτων του IDM4G. Ο TE/USIM και ο ΠΥ4Γ πιστοποιούν αμοιβαία τις ταυτότητές τους μέσω του μηχανισμού UMTS-AKA. Η αμοιβαία πιστοποίηση ταυτότητας μεταξύ του ΠΥ4Γ και του ΦΠΥΔ εξασφαλίζεται από τις υποθέσεις του πρωτοκόλλου. Η αμοιβαία πιστοποίηση ταυτότητας μεταξύ του TE/USIM και του ΦΠΥΔ εξασφαλίζεται έμμεσα με παρεμβολή του ΠΥ4Γ. Η πιστοποίηση ταυτότητας του χρήστη στον TE/USIM, γίνεται με χρήση ενός PIN σύμφωνα με τις συστάσεις του 3GPP. Ισχυρή πιστοποίηση μπορεί να υλοποιηθεί με χρήση βιομετρικών τεχνολογιών (BIO4G). Τέλος, η USIM και ο TE, πιστοποιούνται αμοιβαία μέσω ενός μηχανισμού προσυμφωνημένου κρυπτογραφικού κλειδιού, σύμφωνα με τις συστάσεις του 3GPP.
- **Εμπιστευτικότητα:** Η εμπιστευτικότητα της μεταδιδόμενης πληροφορίας εξασφαλίζεται με τη χρήση του κρυπτογραφικού κλειδιού CK και του αντίστοιχου αλγορίθμου f8, σύμφωνα με τις συστάσεις του 3GPP για το μηχανισμό UMTS-AKA.

- **Ακεραιότητα:** Η ακεραιότητα της μεταδιδόμενης πληροφορίας, εξασφαλίζεται με τη χρήση του κρυπτογραφικού κλειδιού IK και του αντίστοιχου αλγορίθμου παραγωγής κωδίκων αυθεντικοποίησης μηνυμάτων (MAC) του μηχανισμού UMTS-AKA, σύμφωνα με τις συστάσεις του 3GPP.
- **Προστασία από επιθέσεις επανεκπομπής:** Το πρωτόκολλο έχει ενσωματωμένα αντίμετρα προστασίας από επιθέσεις επανεκπομπής (replay attacks). Το πρώτο αντίμετρο είναι η εναλλαγή των διανυσμάτων πιστοποίησης ταυτότητας (Authentication Vectors) του UMTS-AKA, η οποία προκαλεί και αλλαγή των αντιστοίχων παραμέτρων του IDM4G (CK και IK). Το δεύτερο αντίμετρο είναι η εναλλαγή του TMSI σύμφωνα με τον μηχανισμό UMTS-AKA. Το τρίτο αντίμετρο είναι η χρήση και εναλλαγή ενός τυχαίου αριθμού RND, η αποστολή του οποίου προστατεύεται από τον αντίστοιχο κώδικα αυθεντικοποίησης μηνύματος. Ο τυχαίος αυτός αριθμός όχι μόνο ορίζει τη μοναδικότητα κάθε μηνύματος, αλλά και κάθε λίστας που δημιουργείται στον ΠΥ4Γ και η οποία έχει περιορισμένη διάρκεια ζωής, υλοποιώντας το τέταρτο και τελευταίο αντίμετρο.
- **Προστασία από επιθέσεις ενδιάμεσης οντότητας:** Το IDM4G, δεν είναι ευπαθές σε τέτοιου είδους επιθέσεις, σε αντίθεση με άλλα ομοειδή πρωτόκολλα. Οι επιθέσεις αυτού του τύπου αντιμετωπίζονται με την υλοποίηση της εμπιστευτικότητας, της ακεραιότητας και της προστασίας από επιθέσεις επανεκπομπής, όπως περιγράφηκαν παραπάνω. Ένα επιπλέον αντίμετρο είναι η διαχωρισμένη απευθείας επικοινωνία μεταξύ του ΠΥ4Γ και του ΦΠΥΔ, που καθιστά αδύνατη την παρεμβολή όλων των λειτουργιών του πρωτοκόλλου από μία οντότητα σε ένα σημείο, σε αντίθεση με ομοειδή πρωτόκολλα που περνούν όλη την επικοινωνία από τον κόμβο του τερματικού εξοπλισμού του χρήστη.
- **Προστασία από επιθέσεις ωμής δύναμης και λεξικού:** Το IDM4G δεν είναι πρωτόκολλο που βασίζεται σε συνθηματικά, άρα δεν το αφορούν τέτοιου είδους επιθέσεις. Το μόνο αδύναμο σημείο αφορά στη χρήση PIN, η οποία μπορεί να αντικατασταθεί με χρήση βιομετρικών (BIO4G).

- **Παραγωγή κρυπτογραφικών κλειδιών:** Τα κρυπτογραφικά κλειδιά (CK και IK) παράγονται από το μηχανισμό UMTS-AKA κληρονομώντας το επίπεδο ασφάλειας των αντίστοιχων συστάσεων του 3GPP.
- **Παραγωγή τυχαίων αριθμών:** Ο τυχαίος αριθμός RND, πρέπει να βασίζεται στις συστάσεις του αντίστοιχου προτύπου του IETF [177].

3.4.3.2 Επίδοση

Η αξιολόγηση της επίδοσης του IDM4G διακρίνεται σε δύο στάδια, το θεωρητικό και το πρακτικό, τα οποία αναλύονται στη συνέχεια.

3.4.3.2.1 Θεωρητική αξιολόγηση

Μια σημαντική παράμετρος μιας εφαρμογής 4ης γενιάς, είναι οι περιορισμένες υπολογιστικές ικανότητες των τερματικών συσκευών των χρηστών, σε σχέση με τους επιτραπέζιους υπολογιστές. Μία ακόμη σημαντική παράμετρος είναι η ιδιαίτερη φύση της ασύρματης τηλεπικοινωνιακής ζεύξης με την τερματική συσκευή του χρήστη, η οποία χαρακτηρίζεται από σχετικά μειωμένη αξιοπιστία λόγω της αυξημένης ευαισθησίας της σε θέματα θορύβου, εξασθένησης σήματος και παρεμβολής [68]. Για το λόγο αυτό εξετάστηκαν δύο ειδών φορτία, το υπολογιστικό και το τηλεπικοινωνιακό, όσο αφορά κυρίως στη ζεύξη με την τερματική συσκευή του χρήστη, η μείωση των μηνυμάτων πάνω από την οποία αποτελεί ανάγκη που έχει εκφραστεί και από τις προδιαγραφές υλοποίησης του Liberty Alliance [93].

Το IDM4G παράγει πολύ περιορισμένο υπολογιστικό φορτίο, καθώς χρησιμοποιεί κατά βάση προ-υπολογισμένες τιμές του μηχανισμού UMTS-AKA. Πιο συγκεκριμένα, οι επιπρόσθετοι υπολογισμοί που απαιτούνται από το πρωτόκολλο, περιορίζονται:

- στην παραγωγή ενός τυχαίου αριθμού στο βήμα iii,
- στην κρυπτογράφηση της διεύθυνσης IP του ΦΠΥΔ στο βήμα iii και
- στον υπολογισμό δύο κωδίκων αυθεντικοποίησης μηνυμάτων (MAC), στα βήματα iv και vi.

Τα παραπάνω, υποστηρίζονται από τις κάρτες USIM της αγοράς που είναι συμβατές με τις προδιαγραφές του 3GPP, οι οποίες συμπεριλαμβάνουν και γεννήτριες τυχαίων αριθμών (π.χ. Renesas[21], Axalto[22], Hitachi[23] or Philips Semiconductors[24]).

Σχετικά με το τηλεπικοινωνιακό φορτίο, το IDM4G, συγκρίνεται με τα πρωτόκολλα του Liberty Alliance και το Microsoft .Net Passport. Για το σκοπό αυτό υπολογίστηκαν για κάθε πρωτόκολλο τα μηνύματα που ανταλλάσσονται στη ζεύξη με τον τερματικό εξοπλισμό του χρήστη, καθώς και ο συνολικός αριθμός των μηνυμάτων κάθε πρωτοκόλλου. Οι ίδιες συνθήκες λήφθηκαν υπόψη για κάθε πρωτόκολλο, συμπεριλαμβανομένης της υπόθεσης ότι ο φορέας παροχής υπηρεσιών στο διαδίκτυο και ο φορέας παροχής υπηρεσιών ταυτότητας είναι ήδη αμοιβαία πιστοποιημένοι, μη λαμβάνοντας υπόψη τα σχετικά μηνύματα. Πρέπει να τονιστεί ότι οι συστάσεις του Liberty Alliance υποθέτουν ότι ο χρήστης έχει ήδη πιστοποιήσει την ταυτότητά του στον φορέα παροχής υπηρεσιών ταυτότητας, σε αντίθεση με το Microsoft .Net Passport, το οποίο συμπεριλαμβάνει τα μηνύματα αυτά. Το IDM4G, λόγω της ενσωμάτωσής του στην αρχιτεκτονική 4ης γενιάς δεν χρειάζεται τα μηνύματα αυτά.

Για να ομαλοποιηθούν τα αποτελέσματα και να είναι συγκρίσιμα, λήφθηκαν υπόψη δύο σενάρια:

- Το σενάριο Α, κατά το οποίο ο ΠΥ4Γ είναι και ο φορέας παροχής υπηρεσιών ταυτότητας. Στο σενάριο αυτό δεχόμαστε ότι ο χρήστης έχει ήδη αναγνωριστεί από τον ΠΥ4Γ και για τα πρωτόκολλα Liberty Alliance.
- Το σενάριο Β, κατά το οποίο ο ΠΥ4Γ και ο φορέας παροχής υπηρεσιών ταυτότητας είναι διαφορετικές οντότητες. Στο σενάριο αυτό πρέπει να προστεθούν τουλάχιστον δύο μηνύματα (αίτηση και απάντηση πιστοποίησης ταυτότητας χρήστη στον φορέα παροχής υπηρεσιών ταυτότητας).

[21] http://www.renesas.com

[22] http://www.axalto.com

[23] http://www.hitachi.com

[24] http://www.semiconductors.philips.com

Ο Πίνακας 4 παρουσιάζει τα αποτελέσματα της αποτίμησης τηλεπικοινωνιακού φορτίου.

Πίνακας 4: Αποτελέσματα της αποτίμησης τηλεπικοινωνιακού φορτίου

Πρωτόκολλο	Αρ. Μηνυμάτων στη ζεύξη με τον τερματικό εξοπλισμό χρήστη Σενάρια Α/Β	Συνολικός αριθμός μηνυμάτων Σενάρια Α/Β
Πρωτόκολλο Liberty με τεκμήριο (Liberty artifact profile for single sign-on)	6 / 8	8 / 10
Πρωτόκολλο Liberty φυλλομετρητή με χρήση POST (Liberty browser POST profile for single sign-on)	6 / 8	6 / 8
Πρωτόκολλο Liberty με ενεργοποιημένο πελάτη κατά Liberty (Liberty-enabled client and proxy profile for single sign-on – χωρίς χρήση ενδιάμεσου εξυπηρετητή proxy)	6 / 8	6 / 8
Πρωτόκολλο Liberty με ενεργοποιημένο πελάτη κατά Liberty (Liberty-enabled client and proxy profile for single sign-on – με χρήση ενδιάμεσου εξυπηρετητή proxy)	4 / 6	10 / 12
Microsoft .Net Passport	8	8
IDM4G	5	7

Αναλύοντας τα αποτελέσματα του παραπάνω πίνακα είναι φανερό το πλεονέκτημα από τη συνένωση των ρόλων του ΠΥ4Γ και του φορέα παροχής υπηρεσιών ταυτότητας. Το πρωτόκολλο "Liberty με Liberty-ενεργοποιημένο πελάτη (Liberty-enabled client and proxy profile for single sign-on – με χρήση ενδιάμεσου εξυπηρετητή proxy)" έχει τον μικρότερο αριθμό μηνυμάτων στη ζεύξη με τον τερματικό εξοπλισμό χρήστη, αλλά και τον μεγαλύτερο συνολικό αριθμό μηνυμάτων. Αν και αυτό παρέχει ένα πλεονέκτημα απόδοσης, το πρωτόκολλο απαιτεί την ύπαρξη μιας ακόμη οντότητας (ενδιάμεσος εξυπηρετητής proxy), η οποία διαχειρίζεται τις λειτουργίες του πρωτοκόλλου, αντί του τερματικού εξοπλισμού του χρήστη, αρχιτεκτονική που έχει τα παρακάτω μειονεκτήματα σε σχέση με τα υπόλοιπα πρωτόκολλα:

- Αυξημένο κόστος και πολυπλοκότητα.

- Αβεβαιότητα στην αλυσίδα εμπιστοσύνης των οντοτήτων και ασυμβατότητα με τη φιλοσοφία της ασφάλειας του 3GPP που ορίζει με αυστηρότητα ως μόνη απομακρυσμένη έμπιστη οντότητα τη USIM.
- Αύξηση επιφάνειας πιθανών επιθέσεων, καθώς οι αρχιτεκτονικές αυτές είναι ευάλωτες σε επιθέσεις ενδιάμεσου χρήστη, απαιτώντας αμοιβαία πιστοποίηση ταυτότητας USIM και ενδιάμεσου εξυπηρετητή proxy, αυξάνοντας τελικά το αριθμό των μηνυμάτων.

Πέρα από αυτό, όπως αναφέρθηκε, τόσο η παραπάνω έκδοση, όσο και η απλή έκδοση του πρωτοκόλλου "Liberty με Liberty-ενεργοποιημένο πελάτη (Liberty-enabled client and proxy profile for single sign-on – χωρίς χρήση ενδιάμεσου εξυπηρετητή proxy)", παρουσιάζει κενά ασφάλειας [98]. Επιπλέον τα αντίμετρα που προτείνονται από τη βιβλιογραφία [98] για την κάλυψη των κενών ασφάλειας, δεν συνοδεύονται από μελέτη απόδοσης, ώστε να αναδειχθεί το νέο τηλεπικοινωνιακό φορτίο που εισάγουν.

Το IDM4G, συγκρινόμενο με τα αντίστοιχου επιπέδου ασφάλειας πρωτόκολλα, έχει το χαμηλότερο αριθμό μηνυμάτων που ανταλλάσσονται στη ζεύξη με τον τερματικό εξοπλισμό χρήστη και ένα από τους μικρότερους αριθμούς συνολικών μηνυμάτων. Ο συνδυασμός αυτός υψηλού επιπέδου ασφάλειας και αυξημένης απόδοσης είναι αποτέλεσμα τις ενσωμάτωσης του IDM4G στην αρχιτεκτονική 4ης γενιάς, που συνεπάγεται χρήση υπαρχόντων παραμέτρων, μηχανισμών και σχέσεων εμπιστοσύνης μεταξύ των εμπλεκομένων οντοτήτων.

3.4.3.2.2 Πειραματική αξιολόγηση

Το πρωτόκολλο υλοποιήθηκε και δοκιμάστηκε πειραματικά με χρήση του δικτυακού προσομοιωτή Network Simulator (ns-2)[25]. Βασικός στόχος είναι η αξιολόγηση της επίδοσης του IDM4G από άποψη τηλεπικοινωνιακού φορτίου στο τμήμα της ζεύξης με το τερματικό εξοπλισμό χρήστη που είναι και το πιο σημαντικό και μάλιστα στην πιο δυσμενή περίπτωση, κατά την οποία όλα τα πρωτόκολλα λειτουργούν στο σενάριο Α.

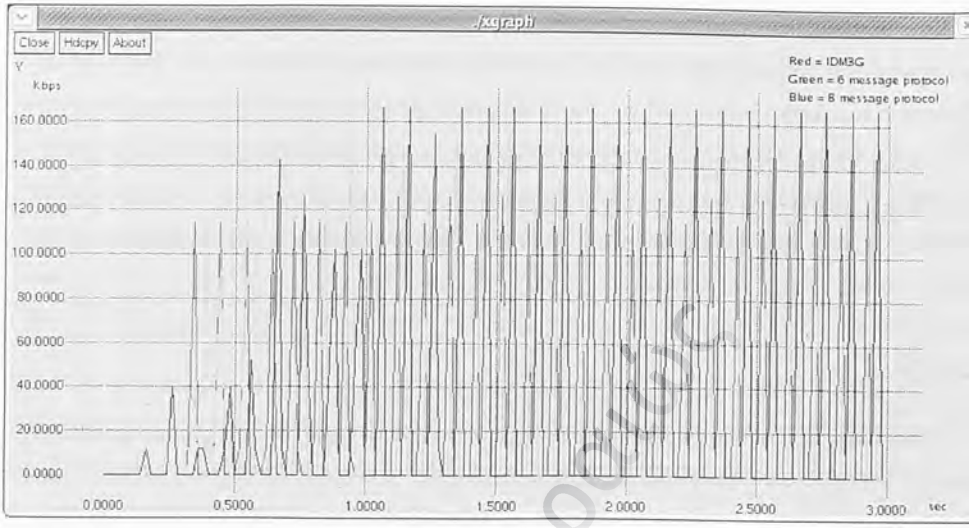
[25] http://www.isi.edu/nsnam/ns/

Στο πείραμα που πραγματοποιήθηκε, δημιουργήθηκαν τρεις κόμβοι, ένας για κάθε οντότητα (ΤΕ/USIM, ΠΥ4Γ, ΦΠΥΔ). Ο ρυθμός μετάδοσης δεδομένων στη ζεύξη με τον τερματικό εξοπλισμό χρήστη τέθηκε στα 384Kbps, το οποίο παρέχεται σε ένα περιβάλλον 3ης γενιάς. Οι ΦΠΥΔ και ΠΥ4Γ, συνδέθηκαν με μια γραμμή ρυθμού μετάδοσης δεδομένων 512Kbps. Τα μηνύματα που ανταλλάσσονται μεταξύ των διαφόρων οντοτήτων, είναι σύννομα με τον περιορισμό μέγιστου μεγέθους 256bytes του Universal Resource Locator (URL), όπως αυτός προδιαγράφεται από τα πρωτόκολλα του Liberty Alliance που χρησιμοποιούν την αλληλουχία ανεύρεσης (search string) του URL, ως μέσο μετάδοσης των μηνυμάτων τους.

Το πείραμα μέτρησε τη συνολική χρήση της ζεύξης με το τερματικό εξοπλισμό χρήστη, με τηλεπικοινωνιακή κίνηση που δημιουργήθηκε από ένα σύνολο πηγών i (τερματικοί εξοπλισμοί χρηστών). Αν ζ_1 είναι η κίνηση (σε Kbps) στη ζεύξη μεταξύ ΤΕ/USIM και ΠΥ4Γ και ζ_2 μεταξύ ΤΕ/USIM και ΦΠΥΔ, τότε η συνολική χρήση της ζεύξης R, με το τερματικό εξοπλισμό χρήστη, δίνεται από την παρακάτω εξίσωση:

$$R = \Sigma\zeta_1(i) + \Sigma\zeta_2(i)$$

Το Σχήμα 32, παρουσιάζει το αποτέλεσμα του πειράματος προσομοίωσης:



Σχήμα 32: Το αποτέλεσμα του πειράματος εξομοίωσης IDM4G

Το IDM4G παράγει το μικρότερο δικτυακό φορτίο σε σχέση με τα πρωτόκολλα που ανταλλάσσουν 6 μηνύματα και 8 μηνύματα, όπως αναφέρει ο Πίνακας 4. Ο Πίνακας 5 παρουσιάζει τις διακυμάνσεις του δικτυακού φορτίου για κάθε πρωτόκολλο.

Πίνακας 5: Διακυμάνσεις δικτυακού φορτίου

Χρονική στιγμή (sec)	IDM4G (Kbps)	Πρωτόκολλο 6 μηνυμάτων(Kbps)	Πρωτόκολλο 8 μηνυμάτων(Kbps)
2.7200000000000002	126.40000000000001	0.0	0.0
2.7400000000000002	0.0	154.40000000000001	0.0
2.7600000000000002	0.0	0.0	166.40000000000001
2.8200000000000021	114.40000000000001	0.0	0.0
2.8400000000000021	0.0	126.40000000000001	0.0
2.8600000000000021	0.0	0.0	166.40000000000001
2.9200000000000021	126.40000000000001	0.0	0.0
2.9400000000000022	0.0	154.40000000000001	0.0
2.9600000000000022	0.0	0.0	166.40000000000001

Παρατηρούμε ότι οι διακυμάνσεις έχουν μια περιοδικότητα που κυμαίνεται στις τριάδες τιμών (126.4 – 154.4 – 166.4) και (114.4 – 126.4 – 166.4) για το IDM4G, τα πρωτόκολλα που

ανταλλάσσουν 6 μηνύματα και τα πρωτόκολλα που ανταλλάσσουν 8 μηνύματα αντίστοιχα. Για την πρώτη τριάδα, στατιστικά, το IDM4G, έχει μειωμένο φορτίο κατά 18.1% σε σχέση με τα πρωτόκολλα που αναφέρει ο Πίνακας 4, τα οποία ανταλλάσσουν 6 μηνύματα και 24.3% σε σχέση με τα πρωτόκολλα τα οποία ανταλλάσσουν 8 μηνύματα. Για τη δεύτερη τριάδα, το IDM4G, έχει μειωμένο φορτίο κατά 9.49% σε σχέση με τα πρωτόκολλα 6 μηνυμάτων και 31.25% σε σχέση με τα πρωτόκολλα 8 μηνυμάτων. Οι τιμές αυτές, καθώς και οι μέσοι όροι αυτών, παρουσιάζονται στον πίνακα 6.

Πίνακας 6: Στατιστικά στοιχεία

Ποσοστό μειωμένου φορτίου IDM4G	Πρωτόκολλο 6 μηνυμάτων	Πρωτόκολλο 8 μηνυμάτων
Για την πρώτη τριάδα	18.1%	24.3%
Για τη δεύτερη τριάδα	9.49%	31.25%
Μέσος όρος για όλες τις περιπτώσεις	13.79%	27.77%

Το IDM4G, έχει κατά μέσο όρο μειωμένο φορτίο κατά 13.79% σε σχέση με τα πρωτόκολλα 6 μηνυμάτων και 27.77% σε σχέση με τα πρωτόκολλα 8 μηνυμάτων.

3.4.3.3 Πολυπλοκότητα υλοποίησης

Το IDM4G είναι ένα απλό πρωτόκολλο που βασίζεται σε διεθνή πρότυπα, εξασφαλίζοντας την εύκολη υλοποίησή του καθώς και τη συμβατότητα αυτού με τις τεχνικές προδιαγραφές τόσο του τερματικού εξοπλισμού του χρήστη, όσο και της υποδομής του ΠΥ4Γ. Πιο αναλυτικά, όσον αφορά στην πολυπλοκότητα υλοποίησης του IDM4G:

- ΤΕ/USIM: Ο τερματικός εξοπλισμός χρήστη, πρέπει να είναι συμβατός με τις προδιαγραφές του Liberty Alliance, συμπεριλαμβανομένης της υποστήριξης HTTP και Wireless Markup Language (WML). Οι δυνατότητες της USIM είναι επαρκείς για να καλύψουν τις απαιτήσεις του πρωτοκόλλου. Το IDM4G για να υλοποιηθεί απαιτεί απλά τη χρήση των υπαρχόντων αλγορίθμων της USIM και των τηλεπικοινωνιακών πρωτοκόλλων του εξοπλισμού χρήστη.

- ΠΥ4Γ: Οι ΠΥ3Γ και ΠΥ4Γ, έχουν ήδη σχέσεις εμπιστοσύνης με τους συνδρομητές τους και διαφυλάσσουν τα προσωπικά τους δεδομένα κάτω από ισχυρές αρχιτεκτονικές ασφάλειας που διέπονται από το αντίστοιχο νομικό πλαίσιο. Ο ΠΥ4Γ είναι λοιπόν ιδανική οντότητα για να λειτουργήσει ως φορέας παροχής υπηρεσιών ταυτότητας. Η μόνη αλλαγή που πρέπει να γίνει αφορά μία απλή επέκταση της βάσης δεδομένων των χρηστών, ώστε να αποθηκεύονται τα συμφωνημένα με τους ΦΠΥΔ χαρακτηριστικά χρήστη, καθώς και να δημιουργηθεί ένα απλό σύστημα διατήρησης λιστών με χρήση των υπαρχόντων υποδομών.
- ΦΠΥΔ: Ο ΦΠΥΔ, πρέπει να υλοποιήσει ασφαλή σύνδεση με τον ΠΥ4Γ και ένα απλό μηχανισμό αντιστοίχησης χαρακτηριστικών χρηστών με δικαιώματα χρήσης αυτών.

Το IDM4G, απαιτεί ελάχιστο κόστος υλοποίησης και μικρή αύξηση της πολυπλοκότητας για όλες τις εμπλεκόμενες οντότητες.

3.4.4 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το IDM4G υλοποιεί διαχείριση ταυτότητας με έμφαση στην ασφάλεια, την προστασία των προσωπικών δεδομένων του χρήστη και τη απόδοση. Το πρωτόκολλο υλοποιεί όλα εκείνα τα αντίμετρα που εξασφαλίζουν την ασφαλή λειτουργία του και δεν παρουσιάζει τα κενά ασφάλειας που αναφέρονται από τη βιβλιογραφία τόσο για τα πρωτόκολλα του Liberty Alliance, όσο και για το Microsoft .NET passport. Σε σχέση μάλιστα με τα τελευταία, τα οποία είναι και τα βασικά εναλλακτικά πρωτόκολλα του IDM4G, το προτεινόμενο πρωτόκολλο παρουσιάζει αποδεδειγμένα αυξημένη απόδοση.

Η έννοια της ταυτότητας αντιμετωπίζεται ως ένα σύνολο μη προσωπικής φύσης χαρακτηριστικών που μεταφράζονται σε δικαιώματα πρόσβασης, συνδέοντας με απλό τρόπο της έννοιες της αναγνώρισης, πιστοποίησης και εξουσιοδότησης του χρήστη. Η έμπιστη τρίτη οντότητα που παρέχει υπηρεσίες ταυτότητας, είναι ο φορέας παροχής υπηρεσιών 4ης γενιάς, μία οντότητα που διατηρεί εκ των προτέρων σχέσεις εμπιστοσύνης με τους συνδρομητές της και διαφυλάσσει τα προσωπικά τους δεδομένα κάτω από ισχυρές αρχιτεκτονικές ασφάλειας που διέπονται από το αντίστοιχο νομικό πλαίσιο.

Το IDM4G είναι διαφανές στο χρήστη, υποστηρίζει πολλαπλές ταυτότητες χρήστη με συνδυασμό διαφορετικών χαρακτηριστικών και είναι ελαφρύ από θέμα απόδοσης, τόσο όσο αφορά στο υπολογιστικό, όσο και στο δικτυακό φορτίο. Η διαλειτουργικότητα μπορεί να υλοποιηθεί με συμφωνίες μεταξύ των διαφόρων ΠΥ4Γ, όπως και στην περίπτωση της περιαγωγής.

3.4.5 ΣΥΝΔΥΑΣΜΟΣ ΤΩΝ ΔΥΟ ΠΡΩΤΟΚΟΛΛΩΝ

Οι προτεινόμενες λύσεις – πρωτόκολλα που περιγράφηκαν παραπάνω, μπορούν να συνδυαστούν σε ένα πρωτόκολλο, το οποίο χωρίζεται σε μία αρχική διαπραγμάτευση (αρχική λειτουργία BIO4G) και σε ένα βασικό τμήμα (κανονική λειτουργία BIO4G και IDM4G). Έτσι επιτυγχάνεται όχι μονο ισχυρή πιστοποίηση ταυτότητας χρήστη στον φορέα παροχής υπηρεσιών 3ης γενιάς και 4ης γενιάς αλλά και ασφαλής και λειτουργική πιστοποίηση ταυτότητας χρήστη στο ΦΠΥΔ.

ΚΕΦΑΛΑΙΟ 4: ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ ΣΤΗΝ ΕΡΕΥΝΗΤΙΚΗ ΠΕΡΙΟΧΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΔΙΚΤΥΑΚΗΣ ΑΣΦΑΛΕΙΑΣ ΚΥΡΙΩΣ ΔΙΚΤΥΟΥ ΦΟΡΕΑ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΑΣΥΡΜΑΤΩΝ ΕΥΡΥΖΩΝΙΚΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ 3ΗΣ ΓΕΝΙΑΣ

4.1 Εισαγωγη

Η παρούσα προτεινόμενη λύση αντιμετωπίζει το ακόλουθο πρόβλημα:

Οι αρχιτεκτονικές δικτυακής ασφάλειας του κυρίως δικτύου φορέα παροχής υπηρεσιών 3ης γενιάς, είναι ανεπαρκείς, με κύριο χαρακτηριστικό μια επίπεδη αρχιτεκτονική ασφάλειας που βασίζεται σε ελλιπή αναχώματα ασφάλειας και απουσία συστημάτων ανίχνευσης και αναχαίτισης εισβολών. Οι ενδεχόμενες συνέπειες από την πραγματοποίηση κάποιας απειλής, μέσα από την εκμετάλλευση κάποιας αδυναμίας του συστήματος, καθιστούν επιτακτική τη δημιουργία μιας αποτελεσματικής αρχιτεκτονικής ασφάλειας για την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου. Πέρα από τη δημιουργία μιας πιο αποτελεσματικής αρχιτεκτονικής ασφάλειας για την αντιμετώπιση των υπαρχόντων ευπαθών σημείων, πολύ σημαντική είναι η ύπαρξη εξειδικευμένης γνώσης ασφάλειας στους φορείς παροχής 3ης γενιάς, ώστε να είναι σε θέση να αντιμετωπίζουν εξειδικευμένες σε δίκτυα 3ης γενιάς επιθέσεις.

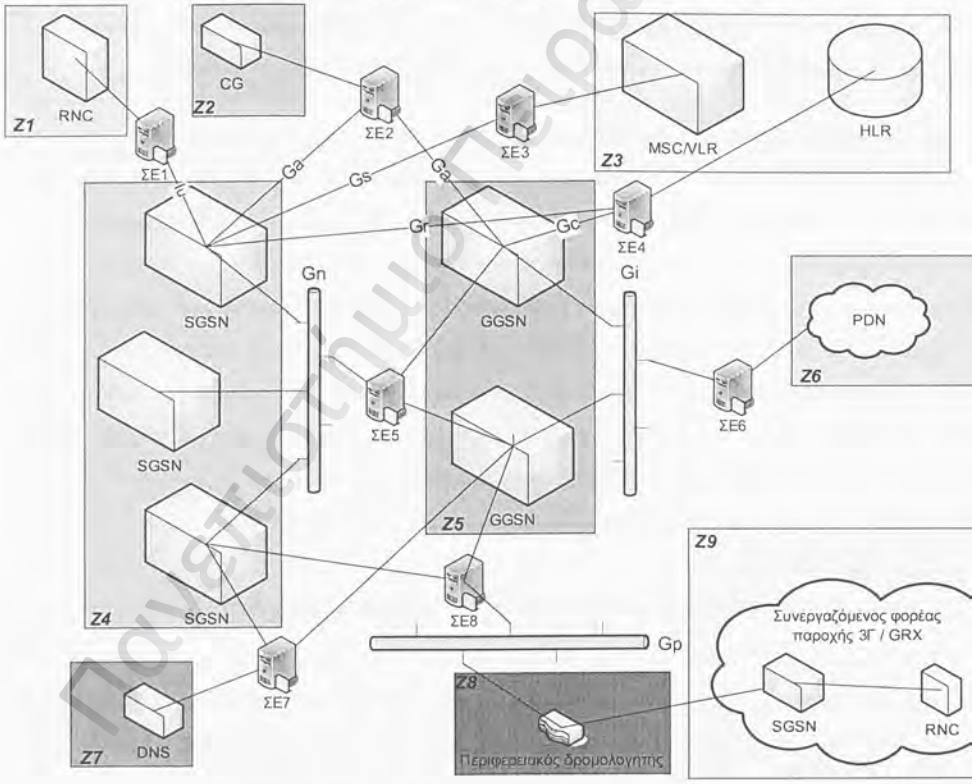
Για την αντιμετώπιση του προβλήματος, προτείνεται αρχικά μια γενική αρχιτεκτονική πρόληψης, ανίχνευσης και αντίδρασης, η οποία βασίζεται σε μια λογική πολυ-επίπεδης ασφάλειας με διαχωρισμό κάθε τμήματος της υποδομής του φορέα παροχής υπηρεσιών 3ης γενιάς σε ζώνες. Στη συνέχεια, με στόχο την υλοποίηση μιας εξειδικευμένης, σε συστήματα 3ης γενιάς πολιτικής συνεχούς μελέτης και βελτίωσης της ασφάλειας προτείνεται η εφαρμογή Συστημάτων Παγίδευσης Εισβολέων (ΣΠΕ - Honeynets) στο κυρίως δίκτυο ενός φορέα παροχής υπηρεσιών ασύρματων 3ης γενιάς. Για το σκοπό αυτό, εκπονήθηκε μια μελέτη για την χρησιμότητα και τη βιωσιμότητα ενός τέτοιου συστήματος, με εφαρμογή της Θεωρίας Παιγνίων, ώστε να αναδειχτούν τα πλεονεκτήματα μιας τέτοιας λύσης. Σημειώνεται ότι δεν έχει μελετηθεί ως σήμερα η εφαρμογή ΣΠΕ στα κυρίως δίκτυα 3ης γενιάς.

4.2 Γενικη παρουσιαση αρχιτεκτονικης ασφαλειας

Η προτεινόμενη αρχιτεκτονική αφορά κατά κύριο λόγο στην υποπεριοχή μεταγωγής πακέτου κυρίως δικτύου μιας 3ης γενιάς υποδομής. Όχι μόνο οι διεπαφές Gi, Gn και Gp δεν είναι επαρκώς προστατευόμενες, αλλά και η οργάνωση της ασφάλειας της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου είναι επίπεδη και ανεπαρκής, με αποτέλεσμα

κατάκτηση κάποιου SGSN ή GGSN, να μεταφράζεται σε έκθεση πολύ σημαντικών συστατικών της υπόλοιπης υποδομής του φορέα παροχής υπηρεσιών 3ης γενιάς, όπως τα HLR, MSC και CG.

Με στόχο την αντιμετώπιση των ανοικτών αυτών θεμάτων ασφάλειας, προτείνεται μια αρχιτεκτονική ζωνών ασφάλειας, η οποία υιοθετεί μια κοινή πρακτική στο χώρο της ασφάλειας δικτύων, αυτή του διαχωρισμού σε ζώνες έτσι ώστε η πραγματοποίηση μιας απειλής σε ένα συστατικό της υποδομής 3ης γενιάς, να μην αποκτήσει χαρακτήρα ντόμινο, εκθέτοντας την υποδομή στο σύνολό της. Η λογική του διαχωρισμού σε ζώνες μπορεί να υλοποιηθεί από μονάδες πρόληψης, ανίχνευσης και αντίδρασης ΣΕ τεχνολογίας ΔΠ 2ης γενιάς, ή από εμπορικά προϊόντα. Η αρχιτεκτονική παρουσιάζεται στο Σχήμα 33.



Σχήμα 33: Αρχιτεκτονική ζωνών ασφάλειας

Το Σχήμα 33 αφορά σε μια πρότυπη αρχιτεκτονική, η οποία παρουσιάζει τις διεπαφές των συστατικών της συγκεκριμένης υπο-περιοχής με άλλα συστατικά της υποδομής 3ης γενιάς. Οι ζώνες διαχωρίζονται από μονάδες ΣΕ, οι οποίες απομονώνουν τα συστατικά κάθε ζώνης και ελέγχουν την κίνηση από και προς αυτά. Ο αριθμός των ΣΕ ανά περίπτωση (για παράδειγμα ΣΕ1), εξαρτάται από το φορτίο της κάθε ζώνης. Οι ζώνες είναι οι ακόλουθες:

- Z1: Η ζώνη αυτή απομονώνει τα RNC, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ1.
- Z2: Η ζώνη αυτή απομονώνει την πύλη τιμολόγησης CG, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ2.
- Z3 Η ζώνη αυτή απομονώνει τα MSC/VLR και HLR, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ3 και ΣΕ4.
- Z4 Η ζώνη αυτή απομονώνει τα SGSN, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ1, ΣΕ2 και ΣΕ3, όσο αφορά σε συστατικά εκτός υπο-περιοχής μεταγωγής πακέτου. Η κίνηση μέσα από τη διεπαφή τους με τα GGSN ελέγχεται μέσω των μονάδων ΣΕ5. Η διεπαφή τους με το DNS ελέγχεται από τις μονάδες ΣΕ7, ενώ η διεπαφή Gp, με τις μονάδες ΣΕ8.
- Z5 Η ζώνη αυτή απομονώνει τα GGSN, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ2, ΣΕ4, ΣΕ5, και ΣΕ7, η κίνηση προς εξωτερικά PDNs, μέσω της διεπαφής Gi, από τις μονάδες ΣΕ6 και η κίνηση προς τη διεπαφή Gp, μέσω των μονάδων ΣΕ8.
- Z6 Η ζώνη αυτή απομονώνει τα εξωτερικά PDN, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ6.
- Z7 Η ζώνη αυτή απομονώνει τα DNS, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ7.
- Z8 Η ζώνη αυτή απομονώνει τον περιφερειακό δρομολογητή της διεπαφής Gp, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ8.
- Z9 Η ζώνη αυτή απομονώνει τα δίκτυα των συνεργαζόμενων φορέων παροχής υπηρεσιών 3ης γενιάς, η κίνηση από και προς τα οποία ελέγχεται από τις μονάδες ΣΕ8 σε συνεργασία με τον σχετικό περιφερειακό δρομολογητή.

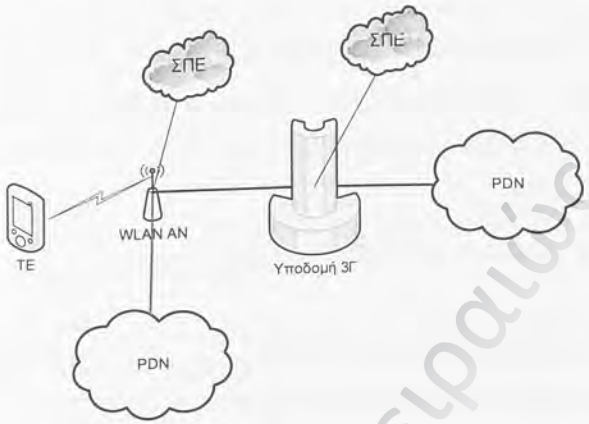
Η αρχιτεκτονική περιγράφει την υλοποίηση του ελέγχου της κίνησης στις διάφορες ζώνες που ορίστηκαν, έτσι ώστε να είναι δυνατή η εφαρμογή συγκεκριμένης πολιτικής ασφάλειας, ανάλογα με το είδος της κίνησης μεταξύ των ζωνών σε κάθε περίπτωση. Επίσης, σε περιπτώσεις που δεν είναι απαραίτητη η επικοινωνία μεταξύ κάποιων συστατικών της υποδομής προτείνεται η υλοποίηση εικονικών τοπικών δικτύων (VLANs), έτσι ώστε να διαχωριστούν εξολοκλήρου οι αντίστοιχες περιοχές.

Η παραπάνω πολυ-επίπεδη αρχιτεκτονική ζωνών ασφάλειας, μπορεί να υλοποιηθεί και με απλά αναχώματα ασφάλειας. Παρόλα αυτά η χρήση ΣΕ υλοποιεί ένα συνδυασμένο ανάχωμα ασφάλειας και σύστημα ανίχνευσης εισβολών, το οποίο είναι αόρατο σε επίπεδο IP (σύμφωνα με την παράγραφο 2.4: Συστήματα παγίδευσης εισβολέων (Honeynets)), ενώ ταυτόχρονα δίνει τη δυνατότητα υλοποίησης και ΣΠΕ.

Επιπλέον, οι πληροφορίες από τα ΣΕ μπορεί να προωθούνται σε ένα κεντρικό εργαστήριο ανάλυσης, όπου και να διασταυρώνονται, τόσο με πληροφορίες από ΔΠ του WLAN τμήματος μιας 3G/WLAN αρχιτεκτονικής (2.4.5: ΣΠΕ σε ασύρματα τοπικά δίκτυα), όσο και πιθανώς με αρχεία καταγραφής των συστημάτων της υποδομής. Τα παραπάνω παρουσιάζονται στο Σχήμα 34.

Σχήμα 34: Κεντρική συλλογή αρχείων καταγραφής

Με τον τρόπο αυτό καλύπτεται όλη η υποδομή 4ης γενιάς από συνεργαζόμενα ΣΠΕ, όπως φαίνεται στο Σχήμα 35.



Σχήμα 35: Συνεργαζόμενα ΣΠΕ που καλύπτουν όλο το τμήμα 3G/WLAN

Το εργαστήριο αυτό μπορεί να αποτελεί τόσο μια επέκταση των υπαρχόντων υποδομών ανάλυσης και διασταύρωσης αρχείων καταγραφής μιας υπάρχουσας υποδομής δικτυακής ασφάλειας, ή να αποτελεί ένα ξεχωριστό τμήμα.

Με την παραπάνω αρχιτεκτονική ασφάλειας επιτυγχάνουμε τα ακόλουθα:

- Η υποδομή ασφάλειας της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου δεν είναι πλέον επίπεδη, αλλά χωρίζεται σε ζώνες, αντιμετωπίζοντας τόσο εξωτερικά, όσο και εσωτερικά περιστατικά ασφάλειας και αντιμετωπίζοντας φαινόμενα ντόμινο σε περίπτωση έκθεσης κάποιου συστατικού.
- Η υποδομή του φορέα παροχής υπηρεσιών 3ης γενιάς, παύει να αποτελεί επέκταση της υποδομής ενός συνεργαζόμενου φορέα παροχής υπηρεσιών 3ης γενιάς, καθώς διαχωρίζεται με την εφαρμογή του ΣΕ8.

Στη συνέχεια, επικεντρωνόμαστε στη δημιουργία ενός ΣΠΕ στην υπο-περιοχή μεταγωγής πακέτου κυρίως δικτύου μιας υποδομής 3ης γενιάς.

4.3 ΥΛΟΠΟΙΗΣΗ ΣΠΕ ΣΤΟ ΚΥΡΙΩΣ ΔΙΚΤΥΟ ΦΟΡΕΑ ΠΑΡΟΧΗΣ 3ΗΣ ΓΕΝΙΑΣ

Στη παρούσα ενότητα, παρουσιάζονται τα ακόλουθα:

- Ανάλυση πλεονεκτημάτων λύσης μέσω θεωρίας παιγνίων και αποστροφής ρίσκου.
- Παρουσίαση εξειδικευμένης αρχιτεκτονικής ΣΠΕ.
- Παρουσίαση πειραμάτων.

Η προτεινόμενη αρχιτεκτονική ΣΠΕ ονομάζεται 3GHNET και έχει τις ακόλουθες λειτουργίες:

- Προληπτικού αντιμέτρου: λειτουργεί ως δόλωμα για επίδοξους εισβολείς, των οποίων η προσοχή αποσπάται από τα πραγματικά συστήματα του ΠΥ3Γ.
- Ανιχνευτικού αντιμέτρου: ανιχνεύει εισβολές πριν υλοποιηθούν στα πραγματικά συστήματα του ΠΥ3Γ και προειδοποιεί τους μηχανικούς ασφάλειας του ΠΥ3Γ.
- Αντιδραστικού αντιμέτρου: χρησιμεύει για την καταγραφή και ανάλυση μεθόδων εισβολής, παρέχοντας γνώση στους μηχανικούς ασφάλειας του ΠΥ3Γ και επιτρέποντας την έγκαιρη προσαρμογή και παραμετροποίηση της λοιπής αρχιτεκτονικής ασφάλειας του ΠΥ3Γ, ώστε να θωρακίσει τα πραγματικά συστήματα πιο αποτελεσματικά.

4.3.1 ΑΝΑΛΥΣΗ ΠΛΕΟΝΕΚΤΗΜΑΤΩΝ ΛΥΣΗΣ ΜΕΣΩ ΘΕΩΡΙΑΣ ΠΑΙΓΝΙΩΝ ΚΑΙ ΑΠΟΣΤΡΟΦΗΣ ΡΙΣΚΟΥ

Εφαρμόζουμε τη θεωρία παιγνίων με στόχο την ανάλυση της βιωσιμότητας της προτεινόμενης λύσης. Πιο αναλυτικά, στοχεύουμε να αποδείξουμε ότι ένας ΠΥ3Γ επωφελείται της υλοποίησης ενός ΣΠΕ στην υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου του, περισσότερο από ένα ΠΥ3Γ, ο οποίος παραμένει σε παραδοσιακές λύσεις ασφάλειας. Η θεωρία παιγνίων αποτελεί εργαλείο σαφέστερου ορισμού του σκεπτικού γύρω από την υλοποίηση ενός ΣΠΕ, το οποίο ταυτόχρονα αναδεικνύει πιο δομημένα και αυστηρά τα πλεονεκτήματα αυτού.

Αρχικά ορίζουμε τους παίκτες του παιγνίου, οι οποίοι είναι και οι οντότητες που θέλουμε να συγκρίνουμε, δηλαδή ο ΠΥ3Γ1, ο οποίος έχει υλοποιήσει ένα ΣΠΕ στην υποδομή του και ο ΠΥ3Γ2, ο οποίος παραμένει σε παραδοσιακές λύσεις ασφάλειας. Στη συνέχεια ορίζουμε το παίγνιο, το οποίο και ονομάζουμε 3GHNET-G και με το οποίο θα μελετήσουμε διαφορετικές καταστάσεις ασφάλειας και τον τρόπο αντίδρασης των υποδομών των δύο παικτών. Το 3GHNET-G είναι παίγνιο μη-συνεργασίας (non-cooperative), καθώς οι δύο ΠΥ3Γ, δεν έχουν κοινούς στόχους και αποδόσεις ασφάλειας αλλά λειτουργούν ως αυτόνομες οντότητες. Το 3GHNET-G είναι επίσης στατικό (static), γιατί οι κινήσεις στο παίγνιο μπορούν να γίνουν ταυτόχρονα και μη-μηδενικού αθροίσματος (non-zero sum), καθώς το κέρδος του ενός παίκτη δε συνδέεται με τις απώλειες του άλλου.

Το 3GHNET-G ορίζεται ως μια δομή ενός συνόλου N={1, 2}παικτών ΠΥ3Γ, ενός συνόλου στρατηγικών Σ και ενός συνόλου αποδόσεων P:

$$\pi: \prod_{i \in N} \Sigma^i \rightarrow R^N$$

όπου Σ^i είναι ο χώρος των στρατηγικών κάθε παίκτη i και R^N, είναι οι αποδόσεις των στρατηγικών στο τέλος του παιγνίου. Καθώς θέλουμε να μελετήσουμε καταστάσεις ασφάλειας, κάθε παίκτης μπορεί να έχει δυο πιθανές καταστάσεις – συμπεριφορές, οι οποίες αντιστοιχούν σε κινήσεις παικτών:

- Σ1: Συμπεριφορά κατειλημμένου κόμβου από εισβολέα - Επίθεση
- Σ2: Κανονική συμπεριφορά κόμβου – Κανονική Λειτουργία

Άρα ορίζουμε Σ^i=(Σ1, Σ2). Επιπλέον, ορίζουμε η απόδοση κάθε στρατηγικής, να δέχεται τιμές από ένα πεπερασμένο σύνολο P={P_1, P_2,…, P_m}, όπου $P \rightarrow R^N$. Επίσης, ορίζουμε κάθε απόδοση P_i, όπου i={1,2,…,m}, ως το άθροισμα κερδών (και απωλειών) G (Πίνακας 7), ανά περίπτωση.

Πίνακας 7: Περιγραφή και τιμές κερδών

No. G	Περιγραφή	Τιμή
G_1	Ασφάλεια από εσωτερικούς κατειλημμένους κόμβους.	10
G_2	Ασφάλεια από εξωτερικούς κατειλημμένους κόμβους.	10
G_3	Ασφάλεια σε εξωτερικούς κόμβους.	10
G_4	Γνώση ασφάλειας	10
G_5	Κόστος	-5

Ο πίνακας 7 αντιστοιχεί στα χαρακτηριστικά μιας υποδομής ασφάλειας, συμπεριλαμβανομένων των χαρακτηριστικών ενός ΣΠΕ. Πιο συγκεκριμένα, μία υποδομή ασφάλειας, ανάλογα με τη φύση της μπορεί να παρέχει ασφάλεια από εσωτερικά εχθρικά συστατικά (G_1), να παρέχει ασφάλεια από συστατικά εξωτερικά του δικτύου που προστατεύει (G_2), να παρέχει ασφάλεια προς τα εξωτερικά δίκτυα (G_3), να μελετά τις κινήσεις των εισβολέων παράγοντας γνώση ασφάλειας (G_4) και να έχει και κάποιο επιπλέον κόστος (G_5) πέρα από τις παραδοσιακές λύσεις που χρησιμοποιούν οι ΠΥ3Γ για την υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου τους.

Ορίζουμε λοιπόν τη συνολική απόδοση $Pi=a_1G_1 + a_2G_2 + a_3G_3 + a_4G_4 + a_5G_5$, όπου ο συντελεστής $a_n=\{0,1\}$ ($n=\{1,2,3,4,5\}$), είναι 1 αν ο παίκτης δέχεται το συγκεκριμένο κέρδος ή 0 στην αντίθετη περίπτωση. Η μήτρα απόδοσης του παιγνίου 3GHNET-G, παρουσιάζεται στη συνέχεια.

Πίνακας 8: Η μήτρα απόδοσης του παιγνίου 3GHNET-G

		ΠΥ4Γ2	
		Επίθεση	Κανονική Λειτουργία
ΠΥ4Γ1	Επίθεση	**35,10**	**25,10**
	Κανονική Λειτουργία	15,10	-5,0

Αναλύοντας τη μήτρα απόδοσης όταν και οι δύο ΠΥ3Γ έχουν κατειλημμένους από εισβολή κόμβους, μελετάμε την κατάσταση Επίθεση-Επίθεση. Στην κατάσταση αυτή, ο ΠΥ3Γ1 δέχεται όλα τα κέρδη του πίνακα, καθώς το ΣΠΕ υλοποιεί όλες τα κέρδη ασφάλειας, αλλά έχει και κάποιο επιπλέον κόστος (G_5).Ο ΠΥ3Γ2, ο οποίος υλοποιεί μια παραδοσιακή

αρχιτεκτονική ασφάλειας, δέχεται το κέρδος G_2, καθώς προστατεύεται από τον κόμβο του ΠΥ3Γ1, ο οποίος υλοποιεί το ΣΠΕ, άρα και ασφάλεια προς τους εξωτερικούς κόμβους, φανερώνοντας έτσι το μεταδιδόμενο κέρδος δικτύου (net benefit), που παρέχει ένα ΣΠΕ, ακόμη και σε οντότητες που δεν το υλοποιούν.

Στην κατάσταση Επίθεση-Κανονική Λειτουργίας, ο ΠΥ3Γ1 δεν δέχεται το κέρδος G_2, καθώς ο ΠΥ3Γ2 δεν επιτίθεται, αλλά δέχεται όλα τα υπόλοιπα κέρδη, όπως και στην προηγούμενη κατάσταση. Ο ΠΥ3Γ2, δέχεται το κέρδος G_2, όπως και προηγουμένως.

Στην κατάσταση Κανονική Λειτουργία – Επίθεση, ο ΠΥ3Γ1, δέχεται τα κερδη G_2, G_4 και G_5, ενώ ο ΠΥ3Γ2, δέχεται το κέρδος G_3, καθώς ο ΠΥ3Γ1 προστατεύεται από το ΣΠΕ.

Στην κατάσταση Κανονική Λειτουργία – Κανονική Λειτουργία, δεν υπάρχει θετικό κέρδος για του παίκτες, παρά μόνο το αρνητικό G_5, για τον ΠΥ3Γ1, ο οποίος επωμίζεται το κόστος του ΣΠΕ.

Μελετώντας της μήτρα απόδοσης, παρατηρούμε δύο ισορροπίες Nash. Οι ισορροπίες, υπολογίζονται σημειώνοντας (με πυκνούς χαρακτήρες στη μήτρα απόδοσης) την πιο κερδοφόρα κατάσταση, για κάθε παίκτη, κρατώντας σταθερή την κατάσταση του άλλου παίκτη. Οι ισορροπίες παρατηρούνται για τις καταστάσεις Επίθεση – Επίθεση και Επίθεση-Κανονική Λειτουργία.

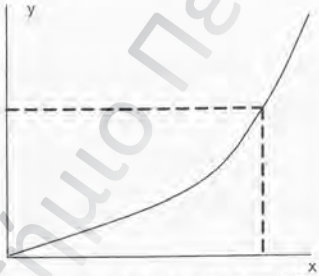
Τα συμπεράσματα του παιγνίου είναι τα ακόλουθα:

- Το υψηλότερο κέρδος λαμβάνεται από τον ΠΥ3Γ1, ο οποίος υλοποιεί το ΣΠΕ, σε όλες τις καταστάσεις που περιλαμβάνουν επίθεση τουλάχιστον ενός ΠΥ4Γ.
- Το ΣΠΕ, δημιουργεί αλυσιδωτό κέρδος για όλους τους παίκτες.
- Σύμφωνα με τις ισορροπίες Nash η υλοποίηση του ΣΠΕ είναι περισσότερο κερδοφόρα στις καταστάσεις Επίθεση – Επίθεση και Επίθεση-Κανονική Λειτουργία.

Η μόνη περίπτωση που ο ΠΥ3Γ έχει απώλειες είναι η περίπτωση όπου δεν παρουσιάζεται κανένα περιστατικό ασφάλειας. Παρόλα αυτά, είναι αποδεδειγμένο από διεθνείς στατιστικές, ότι οι πιθανότητες για την κατάσταση αυτή είναι εξαιρετικά μικρές, κάτι το οποίο θα πρέπει να εξετασθεί σε συνδυασμό με το χαμηλό κόστος μιας λύσης ανοικτού

κώδικα, όπως είναι ένα ΣΠΕ. Για να θέσουμε το σκεπτικό μας υπό θεωρητική βάση και να το περιγράψουμε με μεγαλύτερη σαφήνεια, χρησιμοποιούμε την έννοια της αποστροφής ρίσκου. Όπως περιγράφηκε στην παράγραφο αυτή, η συμπεριφορά αποστροφής ρίσκου, αφορά σε οντότητες οι οποίες προτιμούν να έχουν χαμηλότερο αλλά πιο σίγουρο τελικό κέρδος. Αυτή η συμπεριφορά, χαρακτηρίζει και τους ΠΥ3Γ, οι οποίοι υλοποιούν αντίμετρα ασφάλειας, έτσι ώστε να εξασφαλίσουν τις υποδομές τους, ενώ δεν ακολουθούν ουδέτερη συμπεριφορά ή συμπεριφορά αναζήτησης ρίσκου, έχοντας πάντα ως βασική παράμετρο το κόστος υλοποίησης των αντιμέτρων.

Ορίζουμε την συνάρτηση y=f(x), η οποία εκφράζει το κέρδος σε ασφάλεια y, ως συνάρτηση της επένδυσης που ο ΠΥ3Γ κάνει σε αντίμετρα. Σύμφωνα με τη θεωρία, η συνάρτηση είναι κυρτή όπως παρουσιάζεται στο ακόλουθο σχήμα με το ισοδύναμο βεβαιότητας να εκφράζει τη συμπεριφορά αποστροφής ρίσκου.



Σχήμα 36: Κέρδος σε ασφάλεια y, ως συνάρτηση της επένδυσης που ο ΠΥ3Γ κάνει σε αντίμετρα

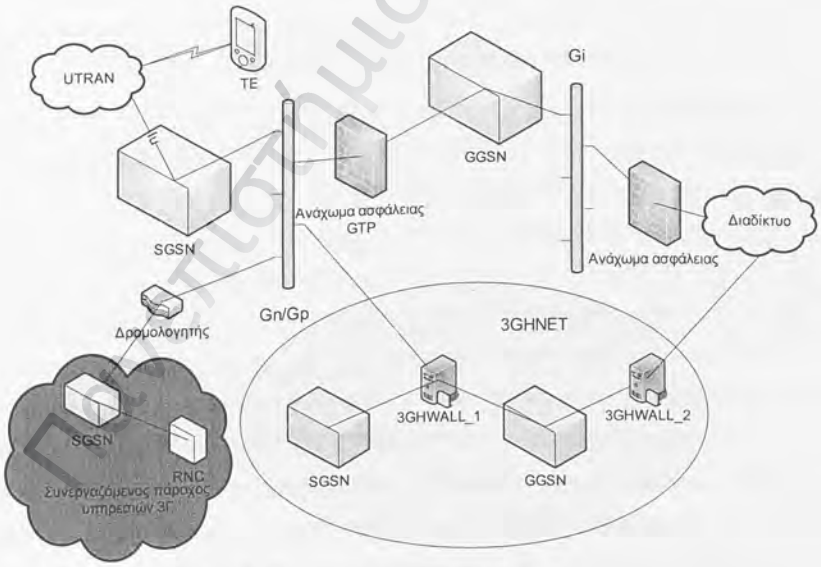
Στην περίπτωση όμως της χρήσης ΣΠΕ από τον ΠΥ3Γ, το κόστος του ανοικτού κώδικα ΣΠΕ είναι πολύ μικρότερο από το κόστος ενός περιστατικού ασφάλειας σε ευαίσθητα (χρονικά και μη) συστήματα παραγωγής, όπως αυτά της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου ενός ΠΥ3Γ. Συνεπώς ισχύει ότι και το κέρδος ασφάλειας είναι πολύ μεγαλύτερο του κόστους υλοποίησης του ΣΠΕ, δηλαδή ότι y>>x. Σχετικές εργασίες μάλιστα αποδεικνύουν, ότι η έγκαιρη ανακάλυψη νέων τρωτών σημείων στο σύστημα, μειώνει σημαντικά το κόστος από ένα περιστατικό ασφάλειας [3], ενώ η δημιουργία ειδικών ομάδων οι οποίες εργάζονται προς αυτή την κατεύθυνση, αποτελεί πλέον συνήθη πρακτική [6].

Συμπεραίνουμε λοιπόν ότι σε κάθε περίπτωση, ύπαρξης ή μη περιστατικών ασφάλειας η υλοποίηση ΣΠΕ αποτελεί συμφέρουσα λύση που στην πρώτη μάλιστα περίπτωση επιφέρει σημαντικά αποτελέσματα για τον ΠΥ3Γ.

4.3.2 Σχεδιαση και υλοποιηση αρχιτεκτονικης ΣΠΕ εξειδικευμενη σε δικτυα 3ης γενιας (3GHNET)

Το σύστημα επικεντρώνεται στις πλέον ευαίσθητες διεπαφές Gn/Gp, οι οποίες είναι και οι λιγότερο προστατευόμενες από τις κοινές αρχιτεκτονικές ασφάλειας των φορέων παροχής υπηρεσιών 3ης γενιάς. Η διεπαφή Gn δεν προστατεύεται επαρκώς, ενώ η διεπαφή Gp, η οποία πολλές φορές συνδυάζεται με την Gn, λόγω ελλιπών μέτρων ασφάλειας, υλοποιεί επέκταση της υποδομής του φορέα παροχής υπηρεσιών 3ης γενιάς στην υποδομή ενός συνεργαζόμενου φορέα παροχής υπηρεσιών 3ης γενιάς, εκθέτοντας και τους δύο φορείς σε υψηλή επικινδυνότητα.

Στο Σχήμα 37, παρουσιάζεται η αρχιτεκτονική του προτεινόμενου ΣΠΕ.



Σχήμα 37: Αρχιτεκτονική 3GHNET

Το 3GHNET αποτελείται από συστήματα-στόχους τα οποία εξομοιώνουν τις λειτουργίες ενός SGSN και ενός GGSN, καθώς και από δύο ΣΕ, τα οποία υλοποιούν έλεγχο και καταγραφή δικτυακής κίνησης, χρησιμοποιώντας ως βάση τεχνολογίες ΔΠ 2ης γενίας, όπως περιγράφηκαν στην παράγραφο 2.4: Συστήματα παγίδευσης εισβολέων (Honeynets). Τα ΣΕ, εξειδικεύτηκαν έτσι ώστε να ανταποκρίνονται στις απαιτήσεις της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου μιας υποδομής 3ης γενιάς, αλλά και στην ιδιομορφία μιας υλοποίησης σε παραγωγικό περιβάλλον, όπως αυτό ενός ΠΥ3Γ. Πιο συγκεκριμένα, ειδική μέριμνα δόθηκε στην ισχυρή προστασία του ΠΥ3Γ από κατεκτημένα SGSN και GGSN του 3GHNET, στον έλεγχο, την καταγραφή και ανάλυση πακέτων GTP και την προστασία εξωτερικών PDN, συμπεριλαμβανομένου του Διαδικτύου. Τα ΣΕ παρουσιάζονται στη συνέχεια:

- Το ΣΕ 3GHWALL_1, είναι μια πύλη επιπέδου 2 του OSI σε λειτουργικό σύστημα Linux, στην οποία δεν αποδίδεται διεύθυνση IP. Ελέγχει και καταγράφει δικτυακή κίνηση μεταξύ των εξομοιωτών SGSN και GGSN του 3GHNET εσωτερικά. Επίσης, ελέγχει και καταγράφει δικτυακή κίνηση, μεταξύ των εξομοιωτών SGSN και GGSN και των πραγματικών SGSN και GGSN του ΠΥ3Γ και των αντίστοιχων συστατικών του συνεργαζόμενου ΠΥ3Γ. Το 3GHWALL_1, χρησιμοποιεί ως ανάχωμα ασφάλειας το Netfilter, παραμετροποιημένο με ένα σύνολο κανόνων εξειδικευμένων σε πακέτα GTP, ελέγχοντας την κίνηση από και προς τις θύρες 2152 και 3386, που χρησιμοποιούν τα SGSN και GGSN για την ανταλλαγή GTP πληροφορίας. Το λογισμικό ανοιχτού κώδικα Snort, χρησιμοποιείται για την ανίχνευση εισβολών, ενώ το λογισμικό ανοιχτού κώδικα Ethereal χρησιμοποιείται για την ανάλυση πακέτων GTP. Όλη η κίνηση από το 3GHNET προς τα πραγματικά SGSN και GGSN του ΠΥ3Γ και των αντίστοιχων συστατικών του συνεργαζόμενου ΠΥ3Γ απαγορεύεται, λόγω της κρισιμότητας των συστατικών αυτών. Αν και δεν προτείνεται, σε περίπτωση που αποφασιστεί ελεγχόμενη κίνηση προς τα παραπάνω παραγωγικά συστατικά, με στόχο την αναλυτική μελέτη εισβολών από και προς SGSN και GGSN (η οποία στο 3GHNET πραγματοποιείται ήδη με εξομοιωτές), απαραίτητη είναι η χρήση του συστήματος αναχαίτισης εισβολών Netfilter/Snort_in_line, για το οποίο πρέπει να εγκατασταθεί προ-επεξεργαστής (preprocessor) του Snort για την ανάλυση GTP κίνησης.

- Το ΣΕ 3GHWALL_2, είναι μια πύλη επιπέδου 2 του OSI σε λειτουργικό σύστημα Linux, στην οποία δεν αποδίδεται διεύθυνση IP. Ελέγχει και καταγράφει δικτυακή κίνηση μεταξύ των εξομοιωτών SGSN και GGSN του 3GHNET και του Διαδικτύου. Το 3GHWALL_2, χρησιμοποιεί ως ανάχωμα ασφάλειας το Netfilter, το λογισμικό ανοιχτού κώδικα Snort, για την ανίχνευση εισβολών, ενώ η χρήση του συστήματος Netfilter/Snort_in_line επιτρέπει την αναχαίτιση επιθέσεων από το 3GHWALL_2 προς το Διαδίκτυο.

Τα SGSN και GGSN του 3GHNET, υλοποιήθηκαν με χρήση του εξομοιωτή ανοικτού κώδικα OpenGGSN σε λειτουργικά συστήματα Linux. Το OpenGGSN χρησιμοποιείται κυρίως από ΠΥ3Γ για πειραματικούς σκοπούς, στο πλαίσιο δοκιμής των πραγματικών συστημάτων τους GGSN και SGSN. Με το OpenGGSN υλοποιείται τόσο εξομοίωση SGSN, όσο και GGSN, με τις βασικές λειτουργίες αυτών, όπως GTP ενθυλάκωση και απ-ενθυλάκωση και δυναμική απόδοση διευθύνσεων IP από το GGSN.Εναλλακτικά του εξομοιωτή ανοικτού κώδικα OpenGGSN, μπορούν να χρησιμοποιηθούν εμπορικά προϊόντα, ή πραγματικά SGSN και GGSN (τα οποία ασφαλώς δε συμμετέχουν στην παραγωγική λειτουργία του ΠΥ3Γ).

4.3.3 Πειραματικη λειτουργια 3GHNET

Η αρχιτεκτονική που περιγράφηκε στην προηγούμενη ενότητα υλοποιήθηκε σε εργαστηριακό περιβάλλον. Κατά την πειραματική λειτουργία του 3GHNET, ελέγχθηκε η ικανότητα του συστήματος για την πρόληψη, ανίχνευση και αναχαίτιση εξειδικευμένων επιθέσεων στην υπο-περιοχή μεταγωγής πακέτου του κυρίως δικτύου. Πιο συγκεκριμένα, πραγματοποιήθηκαν επιθέσεις προς το 3GHNET από εξωτερικά δίκτυα μέσω της διεπαφής Gi καθώς και εξομοιούμενα GGSN και SGSN μέσω της διεπαφής Gn/Gp. Τα σενάρια επιθέσεων διακρίνονται στις παρακάτω ομάδες:

- Ομάδα Α: Επιθέσεις ενάντια στο πρωτόκολλο GTP
- Ομάδα Β: Επιθέσεις άρνησης εξυπηρέτησης
- Ομάδα Γ: Δοκιμές σύνδεσης σε GGSN και SGSN για λόγους διαχείρισης
- Ομάδα Δ: Επιθέσεις που βασίζονται σε μη επιτρεπόμενες δικτυακές διευθύνσεις

- Ομάδα Ε: Κοινές επιθέσεις σε πληροφοριακά συστήματα

Οι επιθέσεις της Ομάδας Α βασίζονται στην αποστολή μηνυμάτων GTP, με αλλοιωμένες τιμές πεδίων επικεφαλίδας, καθώς και μη επιτρεπόμενου περιεχομένου, όπως GTP πακέτα που ενθυλακώνουν πακέτα GTP, πακέτα GTP που ενθυλακώνουν μη-IP πακέτα, περιεχόμενο με διεύθυνση αποστολέα διαφορετική της διεύθυνσης που αποδόθηκε στον αποστολέα κατά τη διαπραγμάτευση του πρωτοκόλλου Packet Data Protocol (PDP context). Το 3GHNET, ανίχνευσε τις επιθέσεις αυτές, κατέγραψε τα ίχνη τους και μπλοκάρισε κάθε προσπάθεια επικοινωνίας προς την κατεύθυνση που αντιστοιχεί σε πραγματικά SGSN και GGSN.

Οι επιθέσεις της Ομάδας Β αφορούν σε επιθέσεις άρνησης εξυπηρέτησης που δε βασίζονται στο πρωτόκολλο GTP (τέτοιες επιθέσεις μελετήθηκαν στην Ομάδα Α). Οι επιθέσεις της Ομάδας Β, πραγματοποιήθηκαν με προσπάθεια έναρξης μεγάλου αριθμού διαπραγματεύσεων PDP context. Το 3GHNET ανίχνευσε και κατέγραψε τις επιθέσεις αυτές, επιδεικνύοντας τη δυνατότητα προειδοποίησης των μηχανικών ασφάλειας ενός ΠΥ3Γ, για την απαγόρευση πακέτων, μέσω παραμετροποίησης των περιμετρικών αναχωμάτων ασφάλειας, από συγκεκριμένες διευθύνσεις ως αντίμετρο σε επιθέσεις άρνησης εξυπηρέτησης, από συγκεκριμένη πηγή.

Οι επιθέσεις της Ομάδας Γ αφορούν σε προσπάθειες σύνδεσης σε SGSN και GGSN για λόγους διαχείρισης. Οι επιθέσεις αυτές εύκολα εντοπίζονται από το 3GHNET, παρακολουθώντας προσπάθειες σύνδεσης σε συγκεκριμένες θύρες διαχείρισης, τόσο μέσω του 3GHWALL_1, όσο και του 3GHWALL_2.

Οι επιθέσεις της Ομάδας Δ αφορούν σε επιθέσεις που βασίζονται σε μη επιτρεπόμενες δικτυακές διευθύνσεις. Οι επιθέσεις αυτές υλοποιήθηκαν με αποστολή πακέτων χρηστών με χρήση διευθύνσεων που ανήκουν στο πεδίο διευθύνσεων των SGSN και GGSN και γενικά με χρήση διευθύνσεων που δεν ανήκουν στο επιτρεπόμενο πεδίο διευθύνσεων της μορφής του αποστολέα. Τα 3GHWALL_1 και 3GHWALL_2 ανίχνευσαν και κατέγραψαν τις επιθέσεις αυτού του τύπου.

Οι επιθέσεις της Ομάδας Ε αφορούν σε κοινές ενεργητικές και παθητικές δικτυακές επιθέσεις εναντίων πληροφοριακών συστημάτων, όπως για παράδειγμα σάρωση θυρών και

αναζήτηση ίχνους λειτουργικού συστήματος για εκμετάλλευση αδυναμιών. Τα 3GHWALL_1 και 3GHWALL_2, ανταποκρίθηκαν στις επιθέσεις αυτές όπως ένα κοινό ΣΕ.

Το 3GHNET, παραμετροποιήθηκε επίσης για την ανίχνευση και καταγραφή πιο σύνθετων επιθέσεων, όπως η επίθεση υπερ-τιμολόγησης χρήστη, η οποία περιγράφηκε στην παράγραφο 2.1.2.3.2: Προβλήματα ασφάλειας. Για την αντιμετώπιση των επιθέσεων αυτών, ως αντίμετρο υλοποιήθηκε η παρακολούθηση της δυναμικής απόδοσης διευθύνσεων IP από το GGSN του 3GHNET, ώστε να γίνει αντιληπτή η αποστολή δεδομένων σε διεύθυνση που έχει αποδεσμευθεί και να ειδοποιηθούν οι μηχανικοί ασφάλειας του ΠΥ3Γ, σε περίπτωση εξαπόλυσης της επίθεσης.

4.4 ΣΧΟΛΙΑ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι ενδεχόμενες συνέπειες από την πραγματοποίηση κάποιας απειλής, μέσα από την εκμετάλλευση κάποιας αδυναμίας του κυρίως δικτύου ενός φορέα παροχής υπηρεσιών 3ης γενιάς, είναι σημαντικές καθιστώντας την αναβάθμιση της ασφάλειας επιτακτική, τουλάχιστον στο επίπεδο που αναβαθμίσθηκε η ασφάλεια στο UTRAN μέσα από τις προδιαγραφές του 3GPP. Για την αντιμετώπιση του προβλήματος, αρχικά προτείνεται μια γενική αρχιτεκτονική πρόληψης, ανίχνευσης και αντίδρασης, η οποία βασίζεται σε μια λογική πολυ-επίπεδης ασφάλειας με διαχωρισμό κάθε τμήματος της υποδομής του φορέα παροχής υπηρεσιών 3ης γενιάς σε ζώνες. Έτσι αντιμετωπίζονται οι αδυναμίες, όπως η επίπεδη αρχιτεκτονική ασφάλειας για όλα τα συστατικά κυρίως δικτύου, ανεξάρτητα των ιδιαιτεροτήτων και απαιτήσεων ασφάλειας κάθε συστατικού, το αναποτελεσματικό ως ανύπαρκτο φιλτράρισμα δικτυακή κίνησης στις περιμέτρους και στο εσωτερικό του κυρίως δικτύου και η απουσία συστημάτων εντοπισμού και αναχαίτισης εισβολών (intrusion detection and prevention systems).

Πέρα από τη δημιουργία μιας πιο αποτελεσματικής αρχιτεκτονικής ασφάλειας για την αντιμετώπιση των υπαρχόντων ευπαθών σημείων, πολύ σημαντική είναι η ύπαρξη εξειδικευμένης γνώσης ασφάλειας στους φορείς παροχής 3ης γενιάς, ώστε να είναι σε θέση να αντιμετωπίζουν εξειδικευμένες σε δίκτυα 3ης γενιάς επιθέσεις. Για το λόγο αυτό, προτείνεται

η εφαρμογή ενός συστήματος παγίδευσης εισβολέων (3GHNET) στο κυρίως δίκτύο ενός φορέα παροχής υπηρεσιών 3ης γενιάς, η χρησιμότητα και βιωσιμότητα του οποίου αποδεικνύεται, με εφαρμογή της Θεωρίας Παιγνίων. Το 3GHNET υλοποιήθηκε και δοκιμάστηκε στην πράξη, υλοποιώντας προληπτικό, ανιχνευτικό και αντιδραστικό αντίμετρο, το οποίο είναι σε θέση να ανιχνεύσει και να καταγράψει εξειδικευμένες επιθέσεις εναντίων της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου.

Το 3GHNET, λειτουργεί και ως ένα εργαστήριο μελέτης επιθέσεων ασφάλειας, το οποίο παρέχει σημαντική γνώση στους μηχανικούς ασφάλειας ενός ΠΥ3Γ και τους προειδοποιεί και εκπαιδεύει για την αναβάθμιση και κατάλληλη παραμετροποίηση των συστατικών ασφάλειας του κυρίως δικτύου.

ΚΕΦΑΛΑΙΟ 5: ΣΥΝΟΨΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ – ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα σύγχρονα ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς, ανοίγουν το δρόμο για αναβαθμισμένες αδιάλειπτες υπηρεσίες δεδομένων από κινητές τερματικές συσκευές συνδυάζοντας μεγάλη γεωγραφική κάλυψη και υψηλούς ρυθμούς μετάδοσης. Στο πλαίσιο παροχής όλο και μεγαλύτερου αριθμού ηλεκτρονικών υπηρεσιών πάνω από δίκτυα 3ης και 4ης γενιάς, η ασφάλεια καθίσταται επιτακτική ανάγκη για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της μεταδιδόμενης πληροφορίας, συμπεριλαμβανομένων των προσωπικών δεδομένων των χρηστών.

Η παρούσα διδακτορική διατριβή εντόπισε ανοικτά θέματα ασφάλειας στον τομέα των ασύρματων ευρυζωνικών δικτύων 3ης και 4ης γενιάς και πρότεινε λύσεις αντιμετώπισης αυτών, στοχεύοντας σε μία συνολικά ισχυρή αρχιτεκτονική ασφάλειας. Πιο συγκεκριμένα, η διατριβή μελέτησε τους μηχανισμούς διαχείρισης ταυτότητας χρήστη τόσο όσο αφορά στην πρόσβαση στον φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς όσο και στην πρόσβαση στους φορείς παροχής ηλεκτρονικών υπηρεσιών στο Διαδίκτυο, πάνω από τα δίκτυα αυτά.

Αρχικά εξετάσθηκε η αλυσίδα ασφάλειας πρόσβασης χρήστη στο δίκτυο 3ης γενιάς. Στο πλαίσιο παροχής ευαίσθητων υπηρεσιών πάνω από δίκτυα 3ης και 4ης γενιάς, όπως υπηρεσίες τραπεζικών συναλλαγών και ηλεκτρονικού εμπορίου, προτάθηκε βελτίωση του επιπέδου ασφάλειας, μέσω της υλοποίησης μηχανισμού ισχυρής πιστοποίησης χρήστη με χρήση βιομετρικών συστημάτων. Λόγω της αυξημένης ευαισθησίας των βιομετρικών δεδομένων και των υποχρεώσεων που προκύπτουν από το αντίστοιχο νομικό πλαίσιο, η εισαγωγή βιομετρικών στη διαδικασία πιστοποίησης ταυτότητας χρήστη είναι ιδιαίτερα απαιτητική. Για το λόγο αυτό αναπτύχθηκε ένα μοντέλο αποτίμησης επικινδυνότητας εξειδικευμένο σε βιομετρικά συστήματα, ώστε να είναι εφικτή η ασφαλής ενσωμάτωση αυτών σε ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς αλλά και σε οποιαδήποτε άλλη αρχιτεκτονική, βελτιστοποιώντας την ασφάλεια των υπαρχόντων μηχανισμών πρόσβασης σε επίπεδο δικτύου.

Το μοντέλο αποτίμησης επικινδυνότητας βιομετρικών συστημάτων παρέχει τη δυνατότητα για πλήρη προσδιορισμό των αδυναμιών ενός βιομετρικού συστήματος, για τον υπολογισμό του επιπέδου επικινδυνότητας του συστήματος με άθροιση των παραγόντων

επικινδυνότητας κάθε αναγνωρισμένης αδυναμίας, για την επιλογή των κατάλληλων μέτρων ασφάλειας για μείωση του επιπέδου επικινδυνότητας, για την επαλήθευση της μείωσης του επιπέδου επικινδυνότητας και για τον υπολογισμό της εναπομένουσας επικινδυνότητας. Το μοντέλο αποτίμησης επικινδυνότητας βιομετρικών συστημάτων επιτρέπει τη δημιουργία συστήματος συμβατού με τη μεθοδολογία BEM των Common Criteria (CC), καθώς και με τα επίσημα προφίλ αξιολόγησης, με αποτέλεσμα τη δυνατότητα πιστοποίησης αυτού με το ISO/IEC 15408.

Στη συνέχεια, το μοντέλο αυτό χρησιμοποιήθηκε ως βάση για τη μελέτη εισαγωγής βιομετρικών σε ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς. Η μελέτη εξήγαγε προδιαγραφές οι οποίες χρησιμοποιήθηκαν για την πρόταση ενός νέου πρωτοκόλλου (BIO4G) ενσωμάτωσης βιομετρικών σε μία αρχιτεκτονική 3ης και 4ης γενιάς, με στόχο την ισχυρή πιστοποίηση χρήστη και επομένως τη βελτίωση της ασφάλειας των μηχανισμών πρόσβασης σε επίπεδο δικτύου. Για τη σχεδίαση του BIO4G, ακολουθήθηκε μια μεθοδική διαδικασία προσδιορισμού απαιτήσεων και εξαγωγής προδιαγραφών, με έμφαση σε θέματα ασφάλειας, προστασίας προσωπικών δεδομένων, ευχρηστίας, οικονομικότητας και πολυπλοκότητας. Το αποτέλεσμα ικανοποιεί τις οριοθείσες προδιαγραφές, υλοποιώντας από άκρο σε άκρο ισχυρή πιστοποίηση ταυτότητας χρήστη στον φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς, με ένα μηχανισμό ο οποίος δεν απαιτεί μόνιμη αποθήκευση ή μετάδοση βιομετρικών δεδομένων, καθώς και διαδικασίες διαχείρισης αυτών και είναι ασφαλής, οικονομικός, εύχρηστος, απλός και συμβατός με τις προδιαγραφές των Common Criteria. Το πρωτόκολλο BIO4G, βελτιώνει το μηχανισμό πιστοποίησης ταυτότητας χρήστη (UMTS-AKA), ο οποίος στηρίζεται πλέον σε παράγοντες ισχυρής πιστοποίησης χρήστη.

Το επόμενο πρόβλημα, αφορά στη χρήση των υπαρχόντων πρωτοκόλλων διαχείρισης ταυτότητας χρήστη για υπηρεσίες στο Διαδίκτυο πάνω από ασύρματα ευρυζωνικά τηλεπικοινωνιακά δίκτυα 3ης και 4ης γενιάς, η οποία επιβαρύνει την απόδοση του συστήματος, δεν αξιοποιεί τις νέες αρχιτεκτονικές και δημιουργεί ανοικτά θέματα ασφάλειας.

Προς αντιμετώπιση του προβλήματος αυτού, η διατριβή, προτείνει ένα νέο ασφαλές και πιο αποτελεσματικό από άποψη απόδοσης πρωτόκολλο διαχείρισης ταυτότητας χρηστών 3ης

γενιάς και 4ης γενιάς, σε φορείς παροχής υπηρεσιών στο διαδίκτυο (IDM4G). Το IDM4G υλοποιεί διαχείριση ταυτότητας με έμφαση στην ασφάλεια, την προστασία των προσωπικών δεδομένων του χρήστη και τη απόδοση. Το πρωτόκολλο υλοποιεί όλα εκείνα τα αντίμετρα που εξασφαλίζουν την ασφαλή λειτουργία του και δεν παρουσιάζει τα κενά του Liberty Alliance και του Microsoft .NET passport.

Σε σχέση μάλιστα με τα τελευταία, τα οποία είναι και τα βασικά εναλλακτικά πρωτόκολλα του IDM4G, το προτεινόμενο πρωτόκολλο παρουσιάζει αποδεδειγμένα αυξημένη απόδοση. Η έννοια της ταυτότητας αντιμετωπίζεται ως ένα σύνολο χαρακτηριστικών που μεταφράζονται σε δικαιώματα πρόσβασης, συνδέοντας με απλό τρόπο τις έννοιες της αναγνώρισης, της πιστοποίησης και της εξουσιοδότησης. Η έμπιστη τρίτη οντότητα που παρέχει υπηρεσίες ταυτότητας, είναι ο φορέας παροχής υπηρεσιών 3ης/4ης γενιάς. Το IDM4G είναι διαφανές στο χρήστη, υποστηρίζει πολλαπλές ταυτότητες χρήστη με συνδυασμό διαφορετικών χαρακτηριστικών και είναι ελαφρύ, τόσο όσο αφορά στο υπολογιστικό, όσο και στο δικτυακό φορτίο.

Τα δύο πρωτόκολλα, BIO4G και IDM4G, μπορεί να συνδυαστούν σε ένα πρωτόκολλο, το οποίο χωρίζεται σε μία αρχική διαπραγμάτευση (αρχική λειτουργία BIO4G) και σε ένα βασικό τμήμα (κανονική λειτουργία BIO4G και IDM4G). Έτσι επιτυγχάνεται και ισχυρή πιστοποίηση ταυτότητας χρήστη στον φορέα παροχής υπηρεσιών 3ης και 4ης γενιάς, καθώς και ασφαλής και λειτουργική πιστοποίηση ταυτότητας χρήστη στους φορείς παροχής ηλεκτρονικών υπηρεσιών στο Διαδίκτυο.

Στη συνέχεια, η διδακτορική διατριβή, μελέτησε θέματα δικτυακής ασφάλειας και εντόπισε ανεπάρκεια στις αρχιτεκτονικές δικτυακής ασφάλειας του κυρίως δικτύου φορέα παροχής υπηρεσιών 3ης γενιάς, με κύριο χαρακτηριστικό μια επίπεδη αρχιτεκτονική ασφάλειας που βασίζεται σε ελλιπή αναχώματα ασφάλειας και σε απουσία συστημάτων ανίχνευσης και αναχαίτισης εισβολών. Οι ενδεχόμενες συνέπειες από την πραγματοποίηση κάποιας απειλής, μέσα από την εκμετάλλευση κάποιας αδυναμίας του κυρίως δικτύου ενός φορέα παροχής υπηρεσιών 3ης γενιάς, είναι σημαντικές καθιστώντας την αναβάθμιση της ασφάλειας επιτακτική.

Για την αντιμετώπιση του προβλήματος, αρχικά προτείνεται μια γενική αρχιτεκτονική πρόληψης, ανίχνευσης και αντίδρασης, η οποία βασίζεται σε μια λογική πολυ-επίπεδης ασφάλειας με διαχωρισμό κάθε τμήματος της υποδομής του φορέα παροχής υπηρεσιών 3ης γενιάς σε ζώνες. Έτσι αντιμετωπίζονται αδυναμίες όπως η επίπεδη αρχιτεκτονική ασφάλειας, το αναποτελεσματικό ως ανύπαρκτο φιλτράρισμα δικτυακής κίνησης στις περιμέτρους και στο εσωτερικό του κυρίως δικτύου και η απουσία συστημάτων εντοπισμού και αναχαίτισης εισβολών.

Πέρα από τη δημιουργία μιας πιο αποτελεσματικής αρχιτεκτονικής ασφάλειας για την αντιμετώπιση των υπαρχόντων ευπαθών σημείων, πολύ σημαντική είναι η ύπαρξη εξειδικευμένης γνώσης ασφάλειας στους φορείς παροχής δικτύων 3ης γενιάς, ώστε να είναι σε θέση να αντιμετωπίζουν εξειδικευμένες επιθέσεις. Για το λόγο αυτό, προτείνεται η εφαρμογή ενός συστήματος παγίδευσης εισβολέων (3GHNET) στο κυρίως δίκτυο ενός φορέα παροχής υπηρεσιών 3ης γενιάς, η χρησιμότητα και βιωσιμότητα του οποίου αποδεικνύεται, με εφαρμογή της Θεωρίας Παιγνίων.

Το 3GHNET υλοποιήθηκε και δοκιμάστηκε στην πράξη, υλοποιώντας προληπτικό, ανιχνευτικό και αντιδραστικό αντίμετρο, το οποίο είναι σε θέση να ανιχνεύσει και να καταγράψει εξειδικευμένες επιθέσεις εναντίων της υπο-περιοχής μεταγωγής πακέτου του κυρίως δικτύου. Το 3GHNET, λειτουργεί και ως ένα εργαστήριο μελέτης επιθέσεων ασφάλειας, το οποίο παρέχει σημαντική γνώση στους μηχανικούς ασφάλειας ενός ΠΥ3Γ και τους προειδοποιεί και εκπαιδεύει για την αναβάθμιση και κατάλληλη παραμετροποίηση των συστατικών ασφάλειας του κυρίως δικτύου.

Οι προτεινόμενες κατευθύνσεις για μελλοντική έρευνα και ανάπτυξη, αφορούν στην ενσωμάτωση του συστήματος αποτίμησης επικινδυνότητας βιομετρικών συστημάτων σε βάσεις δεδομένων υπαρχόντων μεθοδολογιών και προϊόντων λογισμικού. Επίσης προτείνεται συνεχής έρευνα για την αναγνώριση νέων επιθέσεων και μέτρων ασφάλειας για τα βιομετρικά συστήματα. Περαιτέρω προτάσεις για μελλοντική έρευνα και ανάπτυξη, αφορούν στην υλοποίηση του πρωτοκόλλου BIO4G και την αξιολόγηση σε πραγματικές συνθήκες της επίδοσης του αλγορίθμου διόρθωσης λαθών για βιομετρικά που προτείνει η βιβλιογραφία. Επίσης, προτείνεται η συνεργασία με το Liberty Alliance project για τη

δημιουργία συγκεκριμένου προφίλ Liberty το οποίο να περιγράφει το IDM4G. Τέλος, προτείνεται η εγκατάσταση του 3GHNET σε φορέα παροχής υπηρεσιών 3ης γενιάς με στόχο την περαιτέρω μελέτη επιθέσεων προς το κυρίως δίκτυο και την έρευνα για τη δημιουργία νέων τεχνικών αντιμετώπισης των επιθέσεων αυτών.

Βιβλιογραφικες Αναφορες

ΓΕΝΙΚΑ – ΑΣΦΑΛΕΙΑ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ

1. Eupopean Commision, Information Society Technologies, ISTAG: Scenarios for ambient intelligence in 2010. http://www.cordis.lu/ist/istag-reports.htm
2. Eeurope Action Plan 2005. http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm
3. Arora, A., Telang, R.: Economics of software vulnerability disclosure. IEEE Security & Privacy, vol. 3, no.1, 2005.
4. Power, E., Trope, R. L.: Averting security missteps in outsourcing. IEEE Security & Privacy, vol. 3, no.2, 2005.
5. Levy, E.: Worm propagation and generic attacks. IEEE Security & Privacy, vol. 3, no.2, 2005. IEEE Security & Privacy, vol. 3, no.4, 2005.
6. Ray, H. T., Vemuri, R., Kantubhukta, H.R.: Toward an automated attack model for red teams. IEEE Security & Privacy, vol.3, no.4 (2005)
7. Rezgui, A., Bouguettaya, A., Eltoweissy, M.Y.: Privacy on the Web: Facts, Challenges, and Solutions. IEEE Security & Privacy, vol. 1, no. 6, 2003.
8. Tudor, J., K.: Information Security Architecture. Auerbach, 2001.
9. Peltier, T.R.: Information Security Risk Analysis. CRC press LLC USA, 2001.
10. King, M., Dalton, C., Osmanoglu, T.: Security Architecture. RSA press USA, 2001.
11. Operationally Critical Threat, Asset, and Vulnerability Evaluation method (OCTAVE). http://www.cert.org/octave, 2003.
12. CCTA Risk Analysis and Management Method (CRAMM). http://www.cramm.com, 2003.
13. Consultative, Objective and Bi-functional Risk Analysis (COBRA). http://www.security-risk-analysis.com/introcob.htm
14. Multi-Criteria Analysis manual. http://www.odpm.gov.uk, 2003.
15. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. Lecture Notes in Computer Science, Vol. 2162. Springer-Verlag, 2001.
16. Kocher, P., Jaffe, J., Jun, B.: Introduction to Differential Power Analysis and Related Attacks. http://www.cryptography.com/technology/dpa/DPATechnicalInfo.PDF, 1998.
17. ISO/IEC 17799 IT – Code of practice for information security management, 2005.
18. Information Systems Audit and Control Association: COBIT: Control Objectives for Information and related Technology, 2004.
19. Schneier, B.: Secrets and Lies : Digital Security in a Networked World. John Wiley & Sons, 2000.

20.Cooper, M., Northcutt, S., Fearnow, M., Frederick, K.: Intrusion Signatures and Analysis. Que, 2001.
21.Nazario, J.: Defense and Detection Strategies against Internet Worms. Artech House, 2003.
22.Zwicky, e., Cooper, S., Chapman, D.:Building Internet Firewalls. O'Reilly & Associates (2000)
23.Rhee, MY.: Internet Security. John Wiley & Sons, 2003
24.McNAB, C.: Network Security Assessment. Oreilly, 2004.
25.Kaufman, C.: Network Security: Private Communication in a Public World, Prentice Hall PTR, 2002.
26.Ousley, M.R.: Network Security: The Complete Reference. McGraw-Hill Osborne Media, 2003.
27.Barmann, S.; Writing Information Security Policies. Que, 2001.
28.Lockhart, A.: Network Security Hacks. O'Reilly & Associates, 2004.
29.Ramachandran, J.: Designing Security Architecture Solutions. John Wiley & Sons, 2002.
30.ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security, 2001.
31. Myers, B.A., Beigl, M.: Handheld computing. IEEE Computer, vol. 36, no. 9, 2003.
32.Ashoc, R.L., Dharma, P. A.: Next generation wearable networks. IEEE Computer, vol. 36, no. 11, 2003.
33.US President's Information Technology Advisory Committee. Cyber Security: A crisis of prioritization, 2005.
34.Kshetri, N.: The simple economics of Cybercrimes. IEEE Security and Privacy, vol. 4, no. 1 (2006) pp 33-39
35.Gutmann, P., Naccache, D., Palmer, C.C.: Security Usability. IEEE Security & Privacy, vol.3, no.4 (2005)
36.European Union Eurobarometer, http://www.europa.eu.int/comm/public_opinion/ (2005)

ΔΙΚΤΥΑ 3ΗΣ ΚΑΙ 4ΗΣ ΓΕΝΙΑΣ/ ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

37.Ahmavaara, K., Haverinen, H., Pichna, R.: Interworking architecture between 3GPP and WLAN systems. IEEE Communications Magazine, vol. 41, no. 11, 2003.
38.Jamalipour, A., Valaee, S.: Towards seamless inteworking of wireless LAN and cellular networks. IEEE Wireless Networking, vol. 12, no. 3, 2005.
39.Gazis, V., Alonistioti, N., Merakos, L.: Toward a generic always best connected capability in integrated WLAN/UMTS cellular mobile networks (and beyond). IEEE Wireless Networking, vol. 12, no. 3, 2005.

40.Cavalcanti, D., Agrawal, D., Cordeiro, C., Xie, B., Kumar, A.: Issues in integrating cellular networks, WLANs, and MANETs: A futuristic heterogeneous wireless network. IEEE Wireless Networking, vol. 12, no. 3, 2005.

41.Marquez, F.G., Rodriguez, T.R.V., Miguel, T, Galindo, L.,A.: Interworking of IP multimedia core networks between 3GPP and WLAN. IEEE Wireless Networking, vol. 12, no. 3, 2005.

42.Bennaschi, M., Cacace, F., Iannello, G., Za, S., Pescape, A.: Seamless internetworking of WLANs and cellular networks: Architecture and performance issues in a mobile Ipv6 scenario. IEEE Wireless Networking, vol. 12, no. 3, 2005.

43.Beckman, C., Smith, G.: Shared networks: making wireless communication affordable. IEEE Wireless Networking, vol. 12, no. 2, 2005.

44.Chen, J-C., Jianh, M-C, Liu, Y-W.: Wireless LAN security and IEEE 802.11i. IEEE Wireless Networking, vol. 12, no. 1, 2005.

45.Chen, Y-K, Lin, Y-B.: IP connectivity for Gateway GPRS Support Node. IEEE Wireless Networking, vol. 12, no. 1, 2005.

46.Vassis., D., Kormentzas, G., Rouskas, A., Maglogiannis, I.: The IEEE 802.11g standard for high data rate WLANs. IEEE Network, vol. 19, no. 3, 2005.

47.Hui, S., Y., Yeung, K., H.: Challenges in the migration to 4G mobile systems. IEEE Communications Magazine, vol. 41, no. 12, pp. 54 – 59, 2003.

48.Køien, G., Haslestad, T.: Security aspects of 3G-WLAN interworking. IEEE Communications Magazine, vol. 41, no. 11, 2003.

49.Buddhikot, M. M., Chandranmenon, G., Han, D., Lee, Y-W., Miller, S., Salgarelli, L.: Design and implementation of a WLAN/CDMA2000 interworking architecture. IEEE Communications Magazine, vol. 41, no. 11, 2003.

50.Mahonen, P., Riihjarvi, J., Petrova, M., Shelby, Z.: Hop-by-hop toward future mobile broadband IP. IEEE Communications Magazine, vol. 42, no. 3, 2004.

51.Kim, Y-K., Yi, B.K.: 3G wireless and CDMA2000 1X evolution in Korea. IEEE Communications Magazine, vol. 43, no. 4, 2005.

52.Fantacci, R., Chiti, F., Marabissi, D., Mennuti, G., Morosi, S., Tarchi, D.: Perspectives for present and future CDMA-based communications systems. IEEE Communications Magazine, vol. 43, no. 2, 2005

53.Arbaugh, W.A.: Wireless security is different. IEEE Computer, vol. 36, no. 8, 2003.

54.Wisely, D., Eardley, P., Burness, L.: IP for 3G—Networking Technologies for Mobile Communications. John Wiley & Sons, 2002.

55.Neimi, V., Nyberg, K.: UMTS Security. John Wiley & Sons, 2003.

56.Whitehouse, O.: GPRS Wireless Security: Not ready for prime time, @stake press, 2002.

57.Whitehouse, O., Murphy, G.:Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks. @stake press, 2004.

58.Kotapati, K., Liu, P.., Sun, Y., LaPorta, T.F.: A Taxonomy of Cyber Attacks on 3G Networks. IEEE International Conference on Intelligence and Security, 2005.

59.Donald, W., Scott, L.: Wireless Security Threat Taxonomy, IEEE Workshop on Information Assurance, 2003.

60.El-Fishway, N., Nofal, M., Tadros, A.: An Improvement on Secure Communication in PCS. Performance, Computing, and Communications Conference, Conference Proceedings of the 2003 IEEE International, 2003.

61.Schafer, G.: Security in Fixed and Wireless Networks. John Wiley & Sons, 2004.

62.Held, G.: Securing Wireless LANs. John Wiley & Sons, 2002.

63.Peikari, C., Fogie, S.: Maximum Wireless Security. SAMS, 2002.

64.Nichols, R., Lekkas, P.: Wireless Security: Models, Threats, and Solutions. McGraw-Hill Professional, 2001.

65.Ednay, J., Arbaugh, W.: Real 802.11 Security: Wi-Fi Protected Access and 802.11iAddison-Wesley Pub Co, 2003.

66.Shi, N.: Wireless Communications and Mobile Commerce. Idea Group Publishing, 2003.

67.O'Farrell, N., Ouellet, E.: Hack Proofing Your Wireless Network. Syngress, 2003.

68.Mitchell, C., J.: Security for Mobility. IEE Telecommunication Series 51, 2004.

69.Huber, J.F.: Towards the mobile internet. IEEE Computer, October, 2002.

70.Benoit, O., Dabbous, N., Gauteron, L., Girard, P., Handschuh, H., Naccache, D., Socile, S., Whelan, C.:Mobile Terminal Security. Cryptology ePrint Archive: Report 2004/158, 2004.

71.3rd Generation Partnership Project: TS 23.002 - Network architecture, 2005.

72.3rd Generation Partnership Project: TS 21.133 – 3G Security; Security threats and requirements, 2005.

73.3rd Generation Partnership Project: TS 29.060 – GPRS Tunneling Protocol (GTP) across the Gn and Gp interface, 2005.

74.3rd Generation Partnership Project: TS 23.234 - 3GPP system to Wireless Local Area Network (WLAN) interworking; System description, 2005.

75.3rd Generation Partnership Project: TS 33.234 - 3G Security; Wireless Local Area Network (WLAN) interworking security , 2005.

76.3rd Generation Partnership Project: TS 33.102 - 3G Security; Security architecture, 2005.

77.3rd Generation Partnership Project: TS 31.101 - UICC terminal interface; physical and logical characteristics, 2005.

78.3rd Generation Partnership Project: TS 22.022 - Personalisation of Mobile Equipment (ME); Mobile functionality specification, 2005.

79.Arkko, J., Haverinen, H.: EAP AKA Authentication. IETF Draft, 2003.

80.Urien, P., Farrugia, A.J., Groot, M., Pujolle, G., Abellan, J.: EAP-Support in smartcard. IETF Draft, 2003.

81.Garq, V.K.: Wireless Network Evolution: 2G to 3G, Prentice Hall PTR, 2002.

82.Aboba, B., Beadles, M.: The Network Access Identifier. IETF RFC 2486, 1999.

ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΑΣ

83.Bonatii, P., Samarati, P.: A unified framework for regulating service access and information release on the web. Computer Security Journal, Vol10, No 3, 2003.

84.Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Managing Multiple and Dependable Identities. IEEE Internet Computing, Vol.7, No. 6, 2003.

85.Bernard, R.: Managing Identity Management, *Security Technology and Design*, **6/2005**, SecurityInfoWatch. 2005.

86.Mont, M., Pearson, S., Bramhall, P.: Towards Accountable Management of Identity and Privacy. Proceedings of 14th international workshop on database and expert systems applications, 2003.

87.Siemens: Identity management for micropayments in a mobile environment. Paycircle, 2003.

88.OASIS: Glossary for the OASIS Security Assertion Markup Language (SAML), 2003.

89.Liberty Alliance: Liberty ID-FF Protocols and Schema Specification, 2003.

90.Liberty Alliance: Liberty ID-FF Architecture Overview, 2003.

91.OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML), 2003.

92.Liberty Alliance: Liberty Trust Models Guidelines, 2003.

93.Liberty Alliance: Liberty ID-FF Implementation Guidelines, 2004.

94.Liberty Alliance: Liberty ID-FF Bindings and Profiles Specification, 2003.

95.Microsoft Corp.:Microsoft .NET passport review guide. http://www.passport.net, 2004.

96.Kormann, D., Rubin, A.: Risks of the Passport Single Signon Protocol. Computer Networks, Elsevier Science Press, Vol. 33, 2000.

97.Oppliger, R.: Microsoft .NET passport: a security analysis. IEEE Computer, vol. 36, no.7, 2003.

98.Pfitzmann, B., Waidner, M.: Analysis of Liberty Single-Signon with Enabled Clients. IEEE Internet Computing 7(6), Nov/Dec, 2003.

99.Gross, T.: Security Analysis of the SAML Single Sign-on Browser/Artifact Profile. 19th Annual Computer Security Applications Conference, 2003.

100.Cantor, S., Erdos, M.: Shibboleth-architecture draft v05, May 2002.

101.Pfitzmann, B., Waidner, M.: BBAE – a general protocol for browser-based attribute exchange. Research report RZ 3455 (# 93800), IBM Research Division, Zurich, June 2002.

102.Claub, S., Kohntopp, M.: Identity Management and Its Support of Multilateral Security. *Computer Networks*, vol. 37, 2001.

103.Pfitzmann, B.:Privacy in Enterprise Identity Federation: Policies for Liberty Single Signon, *Proc. Workshop on Privacy Enhancing Technologies*, Springer Verlag, 2003.

104. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil Pairing. Crypto 2001, 2001.

105., Casassa, M., Brown, R.: PASTELS project: Trust Management, Monitoring and Policy-driven Authorization Framework for E-Services in an Internet based B2B environment. HPL-2001-28, 2001.

106.Chen, L., Harrison, K., Moss, A., Soldera, D., Smart, N.P.: Certification of Public Keys within an Identity Based System, LNCS 2433, ed. G. Goos, J. Hartmanis and J. van Leeuwen, Proceedings of Information Security, pp. 332-333, 2002.

107.Cocks, C.: An Identity Based Encryption Scheme based on Quadratic Residues. Communications-Electronics Security Group (CESG), UK, 2001.

108.Karjoth, g., Hunter, M.: A Privacy Policy Model for Enterprises, IBM Research, Zurich - 15th IEEE Computer Foundations Workshop, June 2002.

109.TCPA, Trusted Computing Platform Alliance Main Specification v1.1, www.trustedcomputing.org, 2001.

110.W3C, The Platform for Privacy Preferences 1.0 specification (P3P 1.0). http://www.w3.org/tr/p3p - W3C Recommendation, 2002.

111.Chen, L., Harrison, K., Soldera, D., Smart, N.P.: Application of Multiple Trust Authorities in Pairing based Cryptosystems, Infrasec 2002, Proceedings, pp. 260-275, Bristol, UK, 2002.

112.Buell, D.A., Sandhu, R.: Identity management. IEEE Internet Computing, Vol.7, No. 6, 2003.

113.Slemko, M.: Microsoft passport to trouble, 2001.

ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ

114.Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial fingers on fingerprint systems. Proceedings of SPIE, Vol. 4677. Yokohama, 2002.

115.Van der Putte, T., Keuning, J.: Biometrical fingerprint recognition – don't get your fingers burned. IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications. Kluwer Academic Publishers, 2000.

116.Bolle, R.M., Connell, J.H., Ratha, N.K.: Biometric perils and patches. Pattern Recognition, Vol. 35, no. 12, 2002.

117.Smith, R.: The biometric Dilemma. Secure Computing, 2002.

118.Prabhakar, S., Pankanti, S., Jain, A.,K.: Biometric Recognition Security and Privacy Concerns. IEEE Security & Privacy, vol. 1, no. 2, 2003.

119.Maltoni, D. et al.: Handbook of Fingerprint Recognition. Springer, 2003.

120.Jain, A., K., Bolle, R., Pankanti, S.: Biometrics: Personal Identification in a Networked Society Kluwer Academic Publishers, 1999.

121.Soutar, C.: Biometric template protection and usage. Biometrics consortium conference, Crystal City, VA, 2002.

122. Ratha, N.,K., Connell, J., H., Bolle, R.,M.: Enhancing security and privacy in biometrics-based authentication systems. IBM systems journal, vol. 40, 2001.

123.Tekey Reseach Group: How to trick a bright field optical fingerprint capture sensor. Tekey Research Group Report, 2001.

124.Thalheim, L., Krissler, J., Ziegler, P.,M.: Biometric Access Protection Devices and their Programs Put to the Test. http://www.heise.de/ct/english/02/11/114/ Lisa, Jan, Peter-Michael, 2002.

125.Valencia, V.: Biometric Liveness Testing. CTST New Orleans, 2002.

126.Derakhshani, R., Shuckers, S.: Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern recognition conference, 2003.

127.Hill, C., J.: Risk of masquerade arising from the storage of biometrics. Australian National University Thesis, 2001.

128.Woodward, J., D.: Biometrics. McGraw-Hill Osborne Media, 2002.

129.Chirillo, J., Blaul, S.: Implementing Biometric Security. Wiley, 2003.

130.Nanavati, S., et al: Biometrics: Identity Verification in a Networked World. Wiley, 2002.

131.Bolle, R.: Guide to Biometrics. Springer Professional Computing, 2004.

132.Wayman, J., et al: Biometric Systems: Technology, Design and Performance Evaluation. Springer-Verlag, 2004.

133.Woodward, J., D., et al: Biometrics: A Look at Facial Recognition. RAND Corporation, 2003.

134.Kung, S.,Y., et al: Biometric Authentication : A Machine Learning Approach. Prentice Hall PTR, 2004.

135.Reid, P.: Biometrics for Network Security Prentice Hall PTR, 2003.

136.Lockie, M., Reidy, R.: The Biometric Industry Report - Forecasts and Analysis to 2006. Elsevier Science Ltd, 2002.

137.Ashbourn, J.: BANTAM User Guide: Biometric and Token Technology Application Modeling Language. Springer-Verlag, 2002.
138.Biometrics Market Trends. Faulkner Information Services, 2003.
139.Zhang, D., Jain, A., K.: Biometric Authentication: First International Conference, ICBA 2004, Hong Kong, China, July 15-17, 2004, Proceedings (Lecture Notes in Computer Science), 2004.
140.IST – 2002 –001766 Biometrics and Security (BIOSEC): Deliverable D3.3 – Security recommendations: biometric systems integration, basic research on security, network protocols and PKI. Biosec consortium, 2004.
141.IST-1999-20078 Business environment of biometrics involved in e-commerce – BEE: Deliverable D3.1 Desk Research Report. http://expertnet.net.gr/bee, 2002.
142.IST-1999-20078 Business environment of biometrics involved in e-commerce – BEE: Deliverable D6.2 Marketing and Business development strategies. http://expertnet.net.gr/bee, 2002.
143.IST-1999-20078 Business environment of biometrics involved in e-commerce – BEE: Deliverable D7.1 Conclusions and Recommendations. http://expertnet.net.gr/bee, 2002.
144.IST – 2001 – 38236 BioVision: User and Application Security Issues for Biometric Systems, 2003.
145.ANSI X9.84: Biometric Information Management and Security, 2001.
146.Wayman, J.L., Mansfield, A.J.: Best practices of testing and reporting performance of biometric devices. United Kingdom Biometric Working Group, http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf , 2002.
147.ISO/IEC JTC1, SC37/SG1: Biometric Vocabulary Corpus, 2004.
148.Matsumoto, T.: Gummy finger and paper iris – an update. Proceeding of workshop on information security research, Japan, 2004.
149.Common Criteria Biometric Evaluation Methodology Working Group: Biometric Evaluation Methodology, 2002.
150.ISO/IEC 19792: IT security techniques – A framework for security evaluation and testing of biometric technology, 2004.
151. US CC-Protection Profile: US Government biometric verification mode protection – profile for medium robusness environment, 2003.
152.UK CC-Protection Profile: UK Biometric Device – Draft, 2002.
153.Article 29 – EC data protection working party: Working document on biometrics, 2003.

Άλγεβρα CSP

154.Hoare, C. A. R.: Communicating Sequential Processes. Prentice-Hall International, 2004

155.Brookes, S. D., Hoare, C. A. R., and Roscoe, A. W. 'A Theory of Communicating Sequential Processes,' *Journal ACM* 31 (7), 1984.

156.Schneider, S.: Security Properties and CSP. IEEE Symposium Research in Security and Privacy, 1996.

157.Shaikh, S., Bush, V. and Schneider, S.: Kerberos – Specifying authenticity properties using signal events. In Proceedings of the Indonesia Cryptology and Information Security Conference, pages 87-93, March 2005.

158.Dolev, D, Yao, A.C: On the security of public key protocols. IEEE Trans. on Information Theory, 29(2), pp.198-208, March, 1983.

159.Schneider, S.: Verifying Authentication Protocols in CSP. IEEE Transactions on Software Engineering, 24(9), 1998.

160.Schneider, S.: Verifying authentication protocol implementations. In Proceedings of the Second Workshop on Automated Verification of Critical Systems, pages 239-253. University of Birmingham, 2002

161.Roscoe, A.W.: The Theory and Practice of Concurrency. Prentice-Hall International, 1997

162.Schneider, S.: Concurrent and Real-time Systems: the CSP Approach. Addison-Wesley London, 1999

163.Ryan, P., Schneider, S., Goldsmith, M., Lowe, G. and Roscoe, B.: Modelling and Analysis of Security Protocols. Addison-Wesley, 2001

164.Bryans, J., Schneider, S: CSP_ PVS_ and a recursive authentication protocol. In DIMACS Workshop on Design and Formal Verification of Crypto Protocols, 1997.

165.Dutertre, B., Schneider, S.: Embedding csp in pvs_ an application to authentication protocols. In tpHOL, 1997.

166.Evans, N., Schneider, S., A.: A practical introduction to using CSP and PVS to prove authentication properties of security protocols Technical report, Royal Holloway_ University of London, 2001

167.Heather, J., A.: Oh Is it really you? Using rank functions to verify authentication protocols. PhD thesis Royal Holloway, 2000.

168.Heather, J., A., Schneider, S., A.: Towards automatic verification of authentication protocols on unbounded networks. IEEE Computer Security Foundations Workshop, 2000.

ΣΥΣΤΗΜΑΤΑ ΠΑΓΙΔΕΥΣΗΣ ΕΙΣΒΟΛΕΩΝ

169.The Honeynet Project: Know Your Enemy: Honeynets in Universities, 2004.

170.The Honeynet Project: Know Your Enemy: GenII Honeynets, 2003.
171.The Honeynet Project: Know Your Enemy: Honeynets, 2003.
172.The Honeynet Project: Know Your Enemy: Sebek, 2003.
173.The Honeynet Project: Know Your Enemy: Passive Fingerprinting, 2002.
174.Spitzner, L.:Honeypots - Tracking Hackers. Addison-Wesley Pub Co, 2002.
175.Spitzner, L.: The Honeynet project: trapping the hackers. IEEE Security & Privacy, vol. 1, no.2, 2003.
176.Oudot, L.: Wireless honeypot trickery. Security Focus, infocus 1761, 2004.

ΤΥΧΑΙΟΤΗΤΑ, ΚΩΔΙΚΕΣ ΔΙΟΡΘΩΣΗΣ ΛΑΘΩΝ ΚΑΙ ΣΥΝΔΥΑΣΜΟΣ ΒΙΟΜΕΤΡΙΚΩΝ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

177.Eastlake, D., Crocker, S., Schiller, J.: Randomness Recommendations for Security. IETF RFC, 1994.
178.Davida, G. I., Frankel, Y., Matt, B.:On enabling secure applications through off-line biometric. In Symposium on Security and Privacy, 1998.
179.Juels, A., Wattenberg, M.: A Fuzzy Commitment Scheme. In Proc. ACM Conf. Computer and Communications Security, 1999.
180.Juels, A., Sudan, M.: A fuzzy vault scheme. In Conference on Computer and Communications Security, 2002.
181.Linnartz, J.-P.,. Tuyls, P.:New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In AVBPA, 2003.
182.Verbitskiy, E., Tuyls, P., Denteneer, D., Linnartz, J.-P.: Reliable Biometric Authentication with Privacy Protection. In Proc. 24th Benelux Symposium on Information theory, 2003.
183.Csirmaz, L., Katona, G.O.H.: Geometrical Cryptography. In Proc. International Workshop on Coding and Cryptography, 2003.
184.Frykholm, N., Juels, A.: Error-Tolerant Password Recovery. In Proc. ACM Conf. Computer and Communications Security, 2001.
185.Dodis, Y., Reyzin, L., Smith, A.: Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data. Advances in Cryptology – Eurocrypt 2004, Lecture Notes in Computer Science 3027, Springer-Verlag, 2004.
186.Shaltiel, R.: Recent developments in Explicit Constructions of Extractors. Bulletin of the EATCS, 77, 2002.

187.Ellison, C., Hall, C., Milbert, R., Schneier,B.: Protecting Keys with Personal Entropy. Future Generation Computer Systems, 16, 2000.

188.Monrose, ,F., Reiter, M. K., Wetsel, S.:. Password hardening based on keystroke dynamics. In Conference on Computer and Communications Security, 1999.

189.Hao, F., Anderson, R., Daugman, J.: Combining cryptography with biometrics effectively. University of Cambridge Technical report, No 640, 2005.

190.Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, Vol. 92, No. 6, 2004.

191.Monrose, F., Reiter, M.K., Li, Q., Wetzel, S.: Cryptographic key generation from voice. Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

192.Goh, A. Ngo, DCL.: Computation of cryptographic keys from face biometrics. International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1-13, 2003.

193.Boyen, X.: Reusable cryptographic fuzzy extractors. CCS ACM Press, 2004.

194.MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-correcting Codes, North Holland, 1991.

195.Soutar, S., Roberge, D., Stoianov, A., Gilroy, R., Kumar, B.V.K.: Biometric Encryption. ICSA Guide to Cryptography, McGrow-Hill, 1999.

Θεωρια Παιγνιων και Αποστροφη Ρισκου

196.Osborne, M.J., Rubinstein, A.: A course in game theory, MIT press, 1997.

197.Nash, J.: Equilibrium points in n-person games. Proceedings of the National Academy of the USA 36, 1950.

198.Rabin, M.: Risk Aversion and Expected-Utility Theory: A Calibration Theorem, Econometrica 68(5), 1281-1292, September, 2000.

199.Xiao, Y., Shan, X., Ren, Y.: Game theory models for IEEE802.11 DCF in Wireless Ad Hoc Networks. IEEE Communications Magazine, vol. 43, no. 3, 2005.

200.Michiardi, P., Molva, R.: Game theoretic analysis of cooperation enforcement in mobile ad hoc networks. Institute EuriCom, Research report no. RR-03-092, 2003.

Δικτυακοι τοποι με περιεχομενο ασφαλειας πληροφοριακων συστηματων

201.Internet Storm Center, http://isc.incidents.org

202.Australian Computer Emergency Response Team, http://www.auscert.org.au

203.CERT coordination center, http://www.cert.org

204.Computer incident advisory and capability (CIAC), http://www.ciac.org/ciac

205.US department of defense CERT, http://www.cert.mil

206.Forum of incident response and security teams (FIRST), http://www.first.org

207.The German Research Network Computer Emergency Response Team (DFN-CERT), http://www.cert.dfn.de/eng/dfncert

208.NASA incident response center, http://www-nasirc.nasa.gov/incidents.html

209.List of European CERTs, http://www.ti.terena.nl/teams

210.SANS institute, http://www.sans.org

211.Security Focus, http://www.securityfocus.com