ΑΣΦΑΛΕΙΑ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ ΚΑΙ ΥΠΟΔΟΜΩΝ

ΠΑΥΛΟΣ Λ. ΠΑΝΤΕΛΙΔΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων καθηγητής: Μαυρίδης Ιωάννης

Εξεταστές: Μανιτσάρης Αθανάσιος

Τμήμα Εφαρμοσμένης Πληροφορικής

Πανεπιστήμιο Μακεδονίας
Θεσσαλονίκη

Ιούνιος 2008

ΠΕΡΙΛΗΨΗ

Στην εργασία αυτή εξετάζεται το ζήτημα της ασφάλειας στα κινητά συστήματα τηλεπικοινωνιών 2ης και 3ης γενιάς. Ειδικότερα εξετάζονται τα συστήματα GSM και UMTS/3G, που αποτελούν και τους κυριότερους εκπροσώπους των κυψελωτών δικτύων στις μέρες μας.

Στα δύο πρώτα κεφάλαια της εργασίας περιγράφονται οι στόχοι του κάθε συστήματος, η αρχιτεκτονική και οι οντότητες που αποτελούν τον βασικό κορμό του καθενός. Στη συνέχεια, αναλύονται οι μηχανισμοί ασφαλείας που έχουν θεσμοθετηθεί και εφαρμόζονται, καθώς επίσης οι σκοποί που εκπληρώνουν και τα μέρη του δικτύου τα οποία προστατεύουν. Εξετάζονται ακόμη τα κενά που υπάρχουν σε κάθε μηχανισμό, οι ευπάθειες που παρουσιάζουν και οι πιθανές επιθέσεις που είναι δυνατόν να πραγματοποιηθούν και να διακυβεύσουν το απόρρητο των τηλεπικοινωνιακών δεδομένων.

Επιπρόσθετα, γίνεται μια εξαγωγή των βασικότερων συμπερασμάτων και υπογραμμίζονται οι τρόποι που μπορούν να επιλύσουν τα κυριότερα προβλήματα των μηχανισμών ασφαλείας στα δύο συστήματα. Προτείνονται, τέλος, πρακτικές και συστάσεις για την ασφαλή χρήση των κινητών τηλεφώνων από τους συνδρομητές, έτσι ώστε να προλαμβάνονται οι κίνδυνοι που απορρέουν σε κάθε περίπτωση.

ABSTRACT

The scope of this thesis is the study and the analysis of the security issues in the 2nd and the 3rd generation mobile communication systems. In particular, the systems that are examined are the GSM system and the UMTS/3G system, which constitute the major representatives of the cellular networks nowadays.

At the first two chapters of this study, the scopes of each system are described, as well as the architecture and the components that comprise their main backbone. Afterwards, there is an analysis on the security mechanisms that have been adapted and applied, their achieving goals and the special parts of the networks which they protect. Also, the security weakenings and vulnerabilities are introduced, besides the possible attacks which are likely to be accomplished and compromise the confidentiality of the telecommunications data.

Moreover, the most important conclusions are made and the ways to solve the most crucial problems of the security mechanisms in each system are emphasized. Finally, in order to prevent the dangers that derive from each case, several practices and recommendations are proposed to guarantee the secure use of the mobile devices by the networks' subscribers.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ.....

.. **..8**

ΚΕΦΑΛΑΙΟ 1: ΘΕΩΡΗΤΙΚΟ

ΥΠΟΒΑΘΡΟ.....9

1.1 Το Σύστημα GSM.…….....9

1.1.1 Εισαγωγή...…….....9

1.1.2 Στόχοι του GSM…….....….....10

1.1.3 Αρχιτεκτονική του GSM……....10

1.2 Το Σύστημα UMTS……...…13

1.2.1 Εισαγωγή.....…….....13

1.2.2 Τεχνικά χαρακτηριστικά του συστήματος 3GPP…….....16

1.2.3 Η αρχιτεκτονική του UMTS…….…….....…..17

ΚΕΦΑΛΑΙΟ 2: ΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ GSM…….....……22

2.1 Στόχοι των μηχανισμών ασφάλειας……..22

2.2 Ανάλυση των μηχανισμών ασφάλειας.....23

2.2.1 Εμπιστευτικότητα της ταυτότητας του συνδρομητή.....……..23

2.2.2 Αυθεντικοποίηση της ταυτότητας του συνδρομητή.....25

2.2.3 Κρυπτογράφηση των δεδομένων του συνδρομητή.....30

2.2.4 Μηχανισμοί ασφάλειας της κάρτας SIM……..33

2.3 Αξιολόγηση των μηχανισμών ασφάλειας.....34

2.3.1 Ευπάθειες στο μηχανισμό αυθεντικοποίησης της ταυτότητας συνδρομητή.....34

2.3.2 Ευπάθειες στους αλγόριθμους αυθεντικοποίησης (COMP128) και κρυπτογράφησης (A5).....39

2.3.2.1 Ευπάθειες του αλγόριθμου COMP128…….39

2.3.2.2 Ευπάθειες του αλγόριθμου A5.....43

2.3.3 Μη πιστοποίηση του δικτύου στο χρήστη.....45

2.3.4 Ασφάλεια της κάρτας SIM……..47

2.3.5 Μη κρυπτογράφηση της ζεύξης BTS-BSC……48
2.3.6 Επανειλημμένη χρήση ενός σετ τριπλετών ασφαλείας……49
2.3.7 Λοιπές αδυναμίες και ευπάθειες ……..50
2.4 Συμπεράσματα.....53

ΚΕΦΑΛΑΙΟ 3: ΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ UMTS……..55

3.1 Στόχοι των μηχανισμών ασφάλειας.....55
3.2 Παρουσίαση και ανάλυση των μηχανισμών ασφάλειας.....59
3.2.1 Ασφάλεια δικτύου πρόσβασης.....59
3.2.1.1 Πιστοποίηση ταυτότητας χρηστών.....59
3.2.1.2 Δημιουργία των διανυσμάτων αυθεντικοποίησης και επεξεργασία των παραμέτρων στη USIM.....62
3.2.1.3 Εμπιστευτικότητα της ταυτότητας του χρήστη.....66
3.2.1.4 Εμπιστευτικότητα των δεδομένων του χρήστη.....68
3.2.1.5 Ακεραιότητα δεδομένων σηματοδοσίας.....69
3.2.1.6 Ανακεφαλαίωση των Μηχανισμών Ασφάλειας στο Δίκτυο Πρόσβασης.....71
3.2.2 Ασφάλεια στην περιοχή δικτύου.....73
3.2.2.1 MAPSEC…….....75
3.2.2.2 IPSEC……...…78
3.2.2.3 Σύστημα νόμιμων συνακροάσεων.....80
3.2.3 Ασφάλεια της περιοχής του χρήστη.....83
3.2.3.1. Αυθεντικοποίηση Χρήστη στη USIM.....83
3.2.3.2 Σύνδεση USIM – Συσκευής.....84
3.2.4 Ασφάλεια της περιοχής εφαρμογών.....84
3.2.5 Διαφάνεια και διαμόρφωση της ασφάλειας.....85
3.3 Αξιολόγηση των μηχανισμών ασφάλειας.....86
3.3.1 Αξιολόγηση του μηχανισμού εμπιστευτικότητας της ταυτότητας χρήστη.....86
3.3.2 Αξιολόγηση του μηχανισμού εμπιστευτικότητας δεδομενων χρήστη.....87

3.3.3 Αξιολόγηση του μηχανισμού ακεραιότητας των δεδομένων σηματοδοσίας.....89
3.3.4 Γενική αξιολόγηση στους μηχανισμούς ασφάλειας στο Δίκτυο Πρόσβασης.....90
3.4 Συμπεράσματα.....92

ΚΕΦΑΛΑΙΟ 4: ΤΕΧΝΙΚΕΣ ΕΠΙΘΕΣΕΩΝ.....94

4.1 Είδη επιθέσεων.....94
4.1.1 Επιθέσεις άρνησης υπηρεσίας.....94
4.1.2 Επιθέσεις υποκλοπής της ταυτότητας του χρήστη.....96
4.1.3 Επιθέσεις προσωποποίησης του δικτύου.....96
4.1.4 Επιθέσεις προσωποποίησης του χρήστη.....98
4.1.5 Επιθέσεις κρυφακούσματος των δεδομένων του χρήστη.....100

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ – ΑΝΑΦΟΡΕΣ.....101

5.1 Σύνοψη εργασίας και κυριότερα συμπεράσματα.....101
5.2 Θέματα μελλοντικής εργασίας.....103
5.3 Αναφορές.....104

ΕΙΣΑΓΩΓΗ

Η μεγάλη διάδοση των ασύρματων τηλεπικοινωνιών επέφερε τεράστιες αλλαγές στον τρόπο ζωής και τις δραστηριότητες των ανθρώπων. Στις μέρες μας η ευκολία πρόσβασης στο ασύρματο τηλεφωνικό δίκτυο και η πληθώρα των δυνατοτήτων που προσφέρουν τα σύγχρονα κινητά τηλέφωνα, έχουν κάνει ιδιαιτέρως ελκυστικές τις υπηρεσίες που προσφέρουν τα ασύρματα δίκτυα στο μέσο χρήστη. Ωστόσο, δεδομένου ότι οι τεχνολογίες αυτές χρησιμοποιούν ως μέσο μετάδοσης τον αέρα και όχι τα καλώδια, όπως το απλό τηλεφωνικό δίκτυο, καθιστούν την ασφάλεια των διακινούμενων πληροφοριών ως μείζον ζήτημα, καθώς κάποιος μπορεί να υποκλέψει δεδομένα που μεταδίδονται και που δεν προορίζονται για αυτόν. Έτσι, θεωρείται αδήριτη η ανάγκη για την διασφάλιση της εμπιστευτικότητας των δεδομένων των χρηστών και η επισήμανση των κινδύνων που μπορούν να την διακυβεύσουν.

Η παρούσα εργασία χωρίζεται σε πέντε μέρη. Στο πρώτο μέρος παρουσιάζεται η αρχιτεκτονική των συστημάτων δεύτερης (2G) και τρίτης γενιάς (3G) και τα δομικά συστατικά του καθενός. Στο δεύτερο μέρος και τρίτο μέρος εξετάζονται οι μηχανισμοί ασφάλειας στα δίκτυα $2^{ης}$ και $3^{ης}$ γενιάς αντίστοιχα, καθώς και τα ζητήματα ασφάλειας που προκύπτουν από τα ευάλωτα σημεία των μηχανισμών αυτών. Προτείνονται επίσης μέτρα που θα μπορούσαν να παρθούν ώστε να αντιμετωπιστούν τα προβλήματα αυτά. Στο τέταρτο μέρος, γίνεται μια επισκόπηση στις τεχνικές των επιθέσεων που είναι δυνατόν να πραγματοποιηθούν στα συστήματα κινητών τηλεπικοινωνιών και εξετάζεται αν και κατά πόσον αυτές είναι αντιμετωπίσιμες από τους υφιστάμενους μηχανισμούς ασφάλειας. Τέλος, στο πέμπτο μέρος καταγράφονται τα κυριότερα συμπεράσματα για τις δυνατότητες των μηχανισμών ασφάλειας και για το επίπεδο της ασφάλειας που αυτοί τελικά προσφέρουν στο χρήστη.

ΚΕΦΑΛΑΙΟ 1

ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

1.1 Το Σύστημα GSM

1.1.1 Εισαγωγή

Το σύστημα GSM (Group Special Mobile ή Global System for Mobile communications) αποτελεί την έκβαση της κοινής προσπάθειας πολλών οργανισμών για την υιοθέτηση ενός κοινού προτύπου για κυψελωτά συστήματα κινητών επικοινωνιών. Η ιδέα της κυψελωτής κάλυψης εισήχθη από τα Bell Labs στις Ηνωμένες Πολιτείες στα μέσα της δεκαετίας του ’70, με την πρόταση και λειτουργία του προτύπου AMPS (Advanced Mobile Phone Service). Στην Ευρώπη τη δεκαετία του ’80 εξαπλώθηκαν αντίστοιχα αναλογικά συστήματα, με παραδείγματα το NMT (Nordic Mobile Telephony) και το TACS (Total Access Communications System). Βασικός στόχος όλων των συστημάτων πρώτης γενιάς ήταν η παροχή υπηρεσιών φωνητικής τηλεφωνίας σε όσο το δυνατόν μεγαλύτερη κάλυψη. Όλα τα συστήματα μετέδιδαν τη φωνή αναλογικά, χρησιμοποιώντας πολλαπλή προσπέλαση με διαίρεση συχνότητας (Frequency Division Multiple Access – FDMA).

Τα συστήματα αυτά υπόκειντο σε ποικίλους περιορισμούς:

- η ποιότητα της παρεχόμενης υπηρεσίας εμφάνιζε μεγάλες διακυμάνσεις,
- η ασφάλεια των συνδιαλέξεων ήταν περιορισμένη,
- η χωρητικότητά τους περιορίζονταν σε μερικούς εκατοντάδες χιλιάδες συνδρομητές, πολύ μικρότερη της ζήτησης και των επιχειρηματικών σχεδίων των πάροχων,
- τα συστήματα ήταν ασύμβατα, με αποτέλεσμα να περιορίζεται η δυνατότητα περιαγωγής των χρηστών.

Οι παραπάνω περιορισμοί οδήγησαν το 1982 στη δημιουργία μιας ομάδας εργασίας στο CEPT (Conference on European Posts and Telegraphs), με στόχο την προτυποποίηση ενός κοινού προτύπου για τις ψηφιακές επικοινωνίες κινητών στην

Ευρώπη. Το πρώτο βήμα είχε γίνει μερικά χρόνια νωρίτερα, όταν είχε αποφασιστεί η δέσμευση ενός συγκεκριμένου εύρους ζώνης συχνοτήτων, γύρω από την περιοχή των 900MHz, για κινητές επικοινωνίες στην Ευρώπη. Το 1990, μετά από παράκληση της Μ. Βρετανίας, καθορίστηκε μία παραλλαγή του συστήματος GSM-900, γνωστού και ως DCS-1800 (Digital Cellular System 1800) ή GSM-1800, προσθέτοντας μία ακόμη ζώνη συχνοτήτων στην περιοχή των 1800MHz.

1.1.2 Στόχοι του GSM

Οι βασικοί στόχοι του GSM συνίστανται:

- στην παροχή δυνατότητας περιαγωγής (roaming) οπουδήποτε στην Ευρώπη,
- στην εγγύηση ποιότητας υπηρεσίας τουλάχιστον εφάμιλλη αυτής των συστημάτων πρώτης γενιάς,
- στη μέγιστη επαναχρησιμοποίηση του φάσματος, με δυνατότητες κλιμάκωσης του συστήματος,
- στην κρυπτογράφηση της μεταδιδόμενης πληροφορίας του χρήστη,
- στην ευελιξία κλιμάκωσης των ρυθμών μετάδοσης, άρα και των παρεχόμενων υπηρεσιών,
- στη δυνατότητα εφαρμογής ευέλικτων συστημάτων χρέωσης.

Σήμερα, το GSM είναι ένα συνεχώς εξελισσόμενο πρότυπο μέσα στο Ευρωπαικό Ινστιτούτο Τυποποίησης Τηλεπικοινωνιών (ETSI – European Telecommunications Standards Institute), επιδεικνύοντας μια διαρκή πορεία εξέλιξης προς υπηρεσίες πολυμέσων 3ης γενιάς. Από τον Ιούνιο του 2000, οι εργασίες εξέλιξης της τεχνολογίας στη ραδιοζεύξη έχουν μεταφερθεί στο 3GPP (3rd Generation Partnership Project).

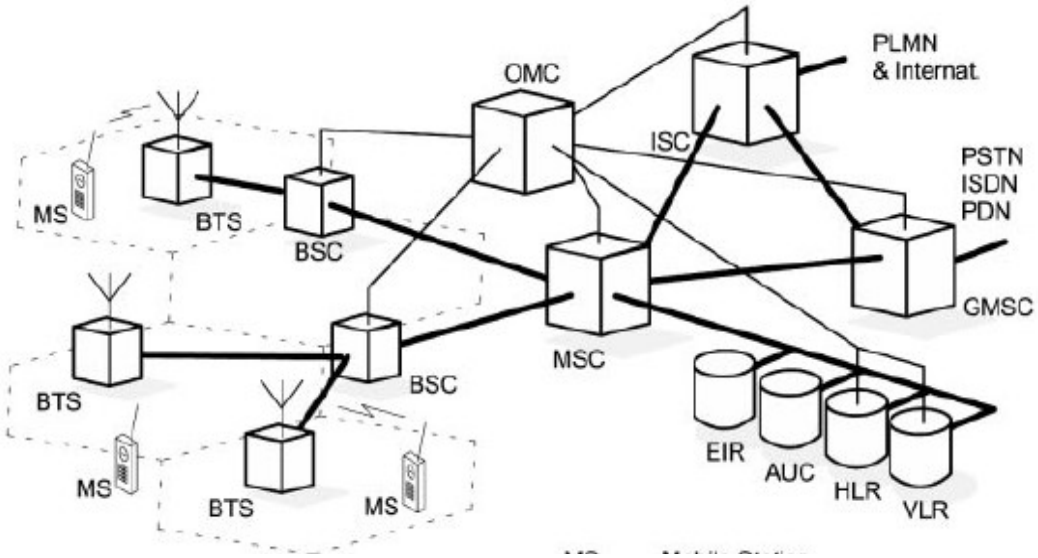
1.1.3 Αρχιτεκτονική του GSM

Το σύστημα GSM αποτελείται από τέσσερα υποσυστήματα:

- τον κινητό σταθμό (Mobile Station – MS),

- το υποσύστημα διαχείρισης και λειτουργίας (OSS – Operation and Support Subsystem),
- το υποσύστημα σταθμού βάσης (BSS – Base Station Subsystem),
- το υποσύστημα μεταγωγής δικτύου (NSS – Network Switching Subsystem)

Στο σχήμα 1 απεικονίζεται η βασική αρχιτεκτονική ενός GSM δικτύου.



BTS: Σταθμός βάσης
BSC: Ελεγκτής σταθμού βάσης
MSC: Κέντρο Μεταγωγής Κινητών Τηλεπικοινωνιών
GMSC: Διαβιβαστικό Κέντρο Μεταγωγής Τηλεπικοινωνιών
ISC: Διεθνές Κέντρο Μεταγωγής
MS: Κινητός σταθμός
HLR: Καταχωρητής Θέσης Οικείων
VLR: Καταχωρητής Θέσης Επισκεπτών
EIR: Καταχωρητής Ταυτότητας Εξοπλισμού
AUC: Κέντρο Αυθεντικοποίησης
OMC: Κέντρο Λειτουργιών και Συντήρησης
PLMN: Δημόσιο επίγειο δίκτυο Κινητών Επικοινωνιών
PSTN: Σταθερό Δίκτυο Επικοινωνιών

Σχήμα 1. Η αρχιτεκτονική του δικτύου GSM [1]

Ο Κινητός σταθμός αποτελείται από:

- τον κινητή συσκευή (Mobile Equipment – ME), που αναλαμβάνει τις λειτουργίες της ραδιοζεύξης,

- την κάρτα SIM (Subscriber Identity Module), μία έξυπνη κάρτα στην οποία καταχωρείται, μεταξύ άλλων, ο προσωπικός αριθμός αναγνώρισης του συνδρομητή (International Mobile Subscriber Identity - IMSI).

Το υποσύστημα σταθμού βάσης (BSS) αποτελείται από:

- τον πομποδέκτη σταθμού βάσης (Base Transceiver Station – BTS), ο οποίος περιλαμβάνει το μηχανολογικό εξοπλισμό και την κεραία για εκπομπή και λήψη του σήματος,
- τον ελεγκτή σταθμού βάσης (Base Station Controller– BSC), υπεύθυνο για την εκχώρηση και απελευθέρωση καναλιών και για λειτουργίες μεταπομπής (handover).

Το υποσύστημα δικτύου μεταγωγής (NSS) αποτελείται από:

- το κέντρο μεταγωγής κινητών υπηρεσιών (Mobile services Switching Centre – MSC), επιφορτισμένο με τις διαδικασίες εγκαθίδρυσης και μεταγωγής κλήσης,
- τον καταχωρητή οικείας θέσης (Home Location Register – HLR), μία βάση δεδομένων η οποία περιλαμβάνει το προφίλ του χρήστη και κάποιες πληροφορίες για την τρέχουσα θέση,
- τον καταχωρητή θέσης επισκέπτη (Visitor Location Register – VLR), μία βάση δεδομένων η οποία αποθηκεύει προσωρινά διάφορα δεδομένα του συνδρομητή ο οποίος βρίσκεται έξω από την περιοχή της HLR καθώς και την ακριβή του θέση σε επίπεδο BTS,
- το κέντρο αυθεντικοποίησης (Authentication Centre – AuC), ο ρόλος του οποίου έγκειται στη διαχείριση δεδομένων για την αυθεντικοποίηση της ταυτότητας του χρήστη,
- το διαβιβαστικό κέντρο μεταγωγής κινητής τηλεφωνίας (Gateway Mobile Switching Centre – GMSC), το οποίο αναλαμβάνει τη δρομολόγηση εισερχομένων κλήσεων προς το κατάλληλο MSC.

Τέλος, το υποσύστημα διαχείρισης (OSS) δεν είναι πλήρως τυποποιημένο, επιτρέποντας στους κατασκευαστές και τους πάροχους να υιοθετήσουν διάφορες

στρατηγικές διαχείρισης, υλοποιώντας το κατάλληλο Τηλεπικοινωνιακό Δίκτυο Διαχείρισης (Telecommunications Management Network – TMN). Η διαχείριση της συνδρομής γίνεται από την HLR και το AuC, η δε διαχείριση του κινητού τερματικού πραγματοποιείται από τον καταχωρητή ταυτότητας συσκευής (Equipment Identity Register - EIR), μία βάση δεδομένων υπεύθυνη για την αποθήκευση δεδομένων που αφορούν την κινητή συσκευή.

1.2 Το Σύστημα UMTS

1.2.1 Εισαγωγή

Οι συνεχώς αυξανόμενες απαιτήσεις των χρηστών για προηγμένες υπηρεσίες και μεγαλύτερες ταχύτητες πρόσβασης οδήγησαν τους σημαντικότερους διεθνής τηλεπικοινωνιακούς οργανισμούς τυποποίησης ITU (International Telecommunications Union) και ETSI (European Telecommunications Standards Institute)**,** στις αρχές της δεκαετίας του 1990, στην έναρξη του σχεδιασμού των δικτύων τρίτης γενιάς (3rd Generation, 3G). Η ITU αναφέρεται στα δίκτυα αυτά με την ονομασία IMT-2000 (International Mobile Telecommunications 2000), ενώ η ETSI με την ονομασία Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών (Universal Mobile Telecommunications System, UMTS). Βασικός στόχος των δικτύων αυτών είναι να προσφέρουν στο χρήστη ταχύτητες μέχρι 2Mbps ώστε να του δώσουν τη δυνατότητα να χρησιμοποιήσει εφαρμογές που μέχρι τώρα, λόγω κυρίως της περιορισμένης ταχύτητας, ήταν αδύνατο να προσφερθούν (π.χ., γρήγορη πρόσβαση στο διαδίκτυο, τηλεδιάσκεψη, κ.α.).

Η τεράστια ανάπτυξη του Internet, και ειδικότερα του πρωτοκόλλου IP έχει οδηγήσει τους βασικούς οργανισμούς προτυποποίησης τηλεπικοινωνιών (ITU και ETSI), να υιοθετήσουν τη χρήση του ως βασικού μέσου για τη διακίνηση δεδομένων στα κινητά δίκτυα τρίτης γενιάς. Η τάση αυτή αναφέρεται συχνά και σαν IP-based ή All-IP λύση. Με τη χρήση της τεχνολογίας IP στην τηλεφωνία μπορεί κανείς να συνδεθεί γρήγορα σε δίκτυα IP, οποιαδήποτε στιγμή το θελήσει. Το IP θεωρείται ότι μπορεί να υποστηρίξει όλους τους τύπους δεδομένων, αλλά και πολλές εφαρμογές πραγματικού χρόνου, συμπεριλαμβανομένης και της φωνής. Η εφαρμογή φωνής

πάνω από IP (Voice over IP—VoIP) έχει ποικίλα πλεονεκτήματα σε σχέση με την παραδοσιακή τηλεφωνία. Για τους διαχειριστές δικτύου σημαίνει μικρότερο κόστος στον εξοπλισμό και στη διαχείριση του δικτύου. Επίσης, το VoIP, σε συνδυασμό με τεχνικές για την καταστολή των διαστημάτων σιωπής, μπορεί να οδηγήσει σε ένα μεγάλο κέρδος στο εύρος ζώνης, σε σχέση με αυτό που καταλαμβάνεται για μία συνδιάλεξη με τις υπάρχουσες συνδέσεις PCM στα 64 Kbps. Αυτό μπορεί να οδηγήσει με τη σειρά του σε χαμηλότερο κόστος τηλεπικοινωνιών για τους τελικούς χρήστες. Τέλος, η χρήση συνόδων IP από άκρο-σε-άκρο, με το μεγάλο διαθέσιμο εύρος ζώνης που παρέχεται από το UMTS, ανοίγει το δρόμο στους κινούμενους τελικούς χρήστες για ένα εντελώς καινούργιο σύνολο από υπηρεσίες πολυμέσων, όπως η τηλεδιάσκεψη, τα συστήματα ατομικής καθοδήγησης, και τα δικτυακά παιχνίδια. Έτσι οι κινητές τηλεπικοινωνίες έχουν εμπλουτιστεί με ενοποιημένες υπηρεσίες πολυμέσων, οι οποίες συνδυάζουν όλα ή κάποια από τα παρακάτω πολυμέσα:

- Ήχο: ομιλία, μουσική, κλπ.
- Γραφικά: στατικά ή κινούμενα (animation).
- Εικόνες: φωτογραφίες ή video.
- Κείμενο
- Δεδομένα: αρχεία ηλεκτρονικών υπολογιστών

Αυτές οι υπηρεσίες πιστεύεται ότι θα αποτελέσουν κίνητρα για τη χρήση του συστήματος UMTS. Η χρήση της ίδιας τεχνολογίας (δηλ. των υπηρεσιών IP) σε δίκτυα σταθερών και σε κινητών τηλεπικοινωνιών, διευκολύνει τη συνεργασία καθώς και τη διαδικασία ενοποίησης αυτών των τύπων δικτύου· παράλληλα, η διαδικασία ανάπτυξης και δημιουργίας καινούργιων υπηρεσιών παρέχεται με έναν συνεπή και αμετάβλητο τρόπο, ανεξάρτητο από τον τύπο του χρησιμοποιούμενου δικτύου.

Τα συστήματα 3G αναπτύσσονται και προτυποποιούνται από δύο μη κερδοσκοπικούς οργανισμούς, γνωστούς ως 3rd Generation Partnership Project (3GPP) και 3GPP2. Ο πρώτος δημιουργήθηκε το 1998 και ασχολείται με την εξέλιξη των συστημάτων GSM και την ανάπτυξη προτύπων για το UMTS, ενώ ο δεύτερος

καθορίζει τα πρότυπα για μια άλλη τεχνολογία δικτύων 3G, γνωστής ως CDMA-2000. Στην ομάδα 3GPP συμμετέχουν μερικοί από τους μεγαλύτερους οργανισμούς προτυποποίησης, όπως το ETSI της Ευρώπης, το ARIB (Association of Radio Industries and Businesses) της Ιαπωνίας, το CCSA (China Communications Standards Association) της Κίνας, το ATIS (Alliance for Telecommunications Industry Solutions) της Β. Αμερικής και το TTA (Telecommunications Technology Association) της Ν. Κορέας. [2]

Η ομάδα 3GPP έχει αναπτύξει από το 1998 διάφορες εκδόσεις για τον τρόπο λειτουργίας των δικτύων 3ης γενιάς. Κάθε έκδοση περιγράφεται αναλυτικά μέσα από έγγραφα που περιγράφουν όχι μόνο το κομμάτι της ραδιο-επαφής (Air-Interface) και του δικτύου κορμού (Core Network), αλλά και πληροφορίες για την κοστολόγηση των υπηρεσιών και την κωδικοποίηση της φωνής, καθώς και για την κρυπτογράφηση των διακινούμενων δεδομένων. Οι εκδόσεις αυτές είναι οι εξής [3] [4]:

- **Release 99 (R99)**. Η έκδοση αυτή περιλαμβάνει όλα τα βασικά χαρακτηριστικά του πρώτων δικτύων 3ης γενιάς και δημοσιεύτηκε το πρώτο τρίμηνο του 2000.
- **Release 4 (R4)**. Η έκδοση αυτή δημοσιεύτηκε το 2001 και περιλαμβάνει πολλά επιπρόσθετα χαρακτηριστικά για τα δίκτυα 3G, και προβλέπει τον τρόπο λειτουργίας του δικτύου κορμού βασισμένου εξ' ολοκλήρου στο πρωτόκολλο IP (all-IP). Επιπλέον, αναπτύσσονται νέα περιβάλλοντα εκτέλεσης, όπως το Mobile Execution Environment (MExE), για την εκτέλεση συγκεκριμένων εφαρμογών του παρόχου στις κινητές συσκευές (π.χ. εφαρμογές Java), καθώς και νέες τεχνολογίες, όπως η ανταλλαγή πολυμεσικών μηνυμάτων (Multimedia Messaging).
- **Release 5 (R5)**. Το 2002 δημοσιεύεται η έκδοση R5 που καθορίζει τη λειτουργία του Υποσυστήματος Πολυμέσων IP (IP Multimedia Subsystem, IMS) για τη διακίνηση πολυμεσικών στοιχείων και εφαρμογών μεταξύ των χρηστών, μέσω του πρωτοκόλλου IP. Επίσης, προτυποποιείται η τεχνολογία HSDPA (High-Speed Downlink Packet Access), γνωστή και ως 3.5G, που αποτελεί ουσιαστικά εξέλιξη του συστήματος UMTS, αφού υπόσχεται ταχύτερη μεταφορά δεδομένων μέχρι και 14,4 Mbit/s.

- **Release 6 (R6)**. Στην έκδοση αυτή, που δημοσιεύεται στα τέλη του 2004, περιγράφονται οι τρόποι αλληλεπίδρασης των 3G δικτύων με ασύρματα τοπικά δίκτυα (Wireless LAN), προτείνονται βελτιώσεις στο υποσύστημα IMS και καθορίζονται οι προδιαγραφές της τεχνολογίας HSUPA (High-Speed Uplink Packet Access), που αποσκοπεί στη βελτίωση της ταχύτητας «ανεβάσματος» (uplink) δεδομένων μέχρι και 5,8 Mbit/s.
- **Release 7 (R7)**. Η έκδοση αυτή είναι σε εξέλιξη και αναμένεται να δημοσιευτεί μέσα στο 2008. Στόχος της είναι η βελτίωση της ποιότητας παροχής υπηρεσιών (Quality of Service) στους χρήστες με την αύξηση της αποδοτικότητας του φάσματος συχνοτήτων που χρησιμοποιείται από τα δίκτυα 3ης γενιάς. Επίσης, προβλέπονται νέα χαρακτηριστικά για τις υπηρεσίες VoIP, ενώ βασικό στοιχείο είναι και η εφαρμογή του πρωτοκόλλου HSPA+ (Evolved HSPA), που αναμένεται να αυξήσει τους ρυθμούς μετάδοσης δεδομένων των χρηστών από και προς το δίκτυο (downlink και uplink) σε 42 Mbit/s και 22 Mbit/s αντίστοιχα.
- **Release 8 (R8)**. Σε εξέλιξη βρίσκονται ακόμη ερευνητικές προσπάθειες για την πλήρη ενοποίηση όλων των ασύρματων και ενσύρματων συστημάτων διαφορετικών τεχνολογιών σε ένα κοινό περιβάλλον, με στόχο την περαιτέρω βελτιστοποίηση του επιπέδου παροχής υπηρεσιών στο χρήστη. Η συγκεκριμένη έκδοση, που αναμένεται να δημοσιευτεί μέσα στο 2009, προβλέπει την αναμόρφωση του συστήματος UMTS και τη μετατροπή του σε ένα δίκτυο 4ης γενιάς (4G), που θα είναι πλήρως βασισμένο στο πρωτόκολλο IP.

1.2.2 Τεχνικά χαρακτηριστικά του συστήματος 3GPP

Η λειτουργία των δικτύων 3G βασίζεται στο πρωτόκολλο μετάδοσης W-CDMA (Wideband-Code Division Multiple Access), που αναπτύχθηκε από την κοινοπραξία 3GPP. Το W-CDMA χρησιμοποιεί τη μέθοδο CDMA, δηλαδή προβλέπει τη χρήση του ίδιου φυσικού καναλιού από πολλούς χρήστες, αλλά σε μεγαλύτερο εύρος ζώνης που φτάνει τα 5 MHz. Έτσι, σε σχέση με το πρωτόκολλο TDMA (Time Division Multiple Access) που χρησιμοποιείται στα συστήματα 2ης γενιάς, το W-CDMA μπορεί να πετύχει μεγαλύτερους ρυθμούς μετάδοσης δεδομένων και να εξυπηρετήσει περισσότερους χρήστες. Με βάση το πρωτόκολλο αυτό, καθορίζονται

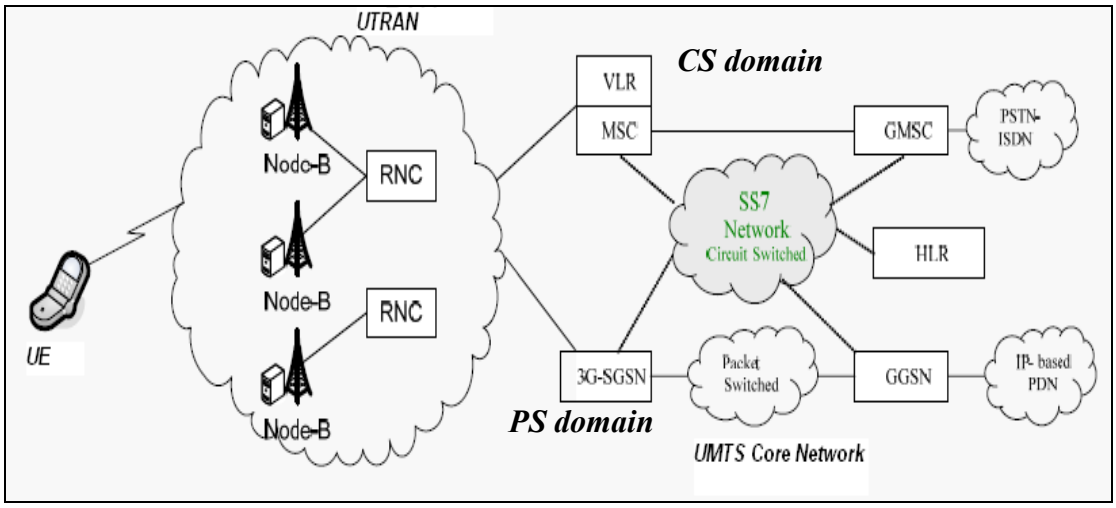
δύο τρόποι ασύρματης πρόσβασης: η Αμφίδρομη Διαίρεση Συχνότητας (Frequency Division Duplex, FDD) και η Αμφίδρομη Διαίρεση Χρόνου (Time Division Duplex, TDD). Η Αμφίδρομη Διαίρεση Συχνότητας (FDD) χρησιμοποιεί ζεύγος συχνοτήτων και είναι κατάλληλη για κάλυψη ευρέων περιοχών υποστηρίζοντας υψηλή κινητικότητα με ρυθμούς μετάδοσης μέχρι 384 kbps. Η Αμφίδρομη Διαίρεση Χρόνου (TDD) χρησιμοποιεί την ίδια ραδιο-ζεύξη για εκπομπή και λήψη και υποστηρίζει ρυθμούς μετάδοσης μέχρι 2 Mbps για χαμηλή κινητικότητα (πεζοί).

Οι συχνότητες που αποδόθηκαν στα συστήματα τρίτης γενιάς για την Ευρώπη είναι 2*60 MHz (1920 – 1980 MHz άνω ζεύξη και 2110 – 2170 MHz κάτω ζεύξη) για FDD συστήματα, 25MHz (1900 – 1920 MHz και 2020 – 2025MHz) για TDD συστήματα με υποχρέωση έκδοσης άδειας, και 10MHz (2010 – 2020 MHz) για TDD συστήματα χωρίς αδειοδότηση.

1.2.3 Η αρχιτεκτονική του UMTS

Σήμερα η κυρίαρχη προτεινόμενη αρχιτεκτονική για το UMTS είναι αυτή που προτείνεται από τη 3GPP για IP-based δίκτυα κινητών επικοινωνιών. Το γενικό σχήμα της αρχιτεκτονικής κατά 3GPP φαίνεται στο σχήμα 2. Οι βασικές λειτουργικές οντότητες είναι δανεισμένες από το GPRS, ενώ υπάρχουν και οι απαραίτητες πύλες (gateways) προς άλλα δίκτυα, όπως το κλασσικό δίκτυο Internet, το τηλεφωνικό δίκτυο (PSTN-- Public Switched Telephone Network) και τα δίκτυα $2^{ης}$ γενιάς.

Η αρχιτεκτονική αυτή αποτελείται από το **Επίγειο Ασύρματο Δίκτυο Πρόσβασης** του UMTS (UMTS Terrestrial Radio Access Network, UTRAN) και από το **Δίκτυο Κορμού** (Core Network, CN). Στην πλευρά του χρήστη βρίσκεται το τερματικό του, το οποίο καλείται **Εξοπλισμός Χρήστη** (User Equipment, UE).



Σχήμα 2. Η κατά 3GPP αρχιτεκτονική του UMTS (Release 99) [5]

Το UE τμήμα αποτελείται από δύο δομικά στοιχεία. Την **Κινητή Συσκευή** (Mobile Equipment, ME) και την **κάρτα USIM** (UMTS Subscriber Identity Module). Το ME, είναι στην ουσία το κινητό τηλέφωνο τρίτης γενιάς που έχει ο χρήστης, και το USIM η κάρτα που του παρέχει η εταιρεία με τη σύνδεση (αντίστοιχη της κάρτας SIM).

Το UTRAN τμήμα αποτελείται από δύο δομικά στοιχεία. Το ένα είναι ο κόμβος B (Node B), πρακτικά ο σταθμός βάσης τρίτης γενιάς, και το δεύτερο είναι ο **Ελεγκτής Ασύρματου Δικτύου** (Radio Network Controller, RNC), που αφενός ελέγχει την κίνηση στο αέρα, αφετέρου ανταλλάσσει δεδομένα με και σηματοδοσίες με το CN. Σε αναλογία με το GSM, Node B είναι ο σταθμός βάσης ενώ το RNC είναι το BSC.

Το CN τμήμα για την έκδοση R99 αποτελείται από δύο υποσυστήματα. Το **Υποσύστημα Μεταγωγής Κυκλωμάτων** (Circuit Switched, CS domain) και το **Υποσύστημα Μεταγωγής Πακέτων** (Packet Switched, PS domain). Το πρώτο από αυτά αποτελεί εξέλιξη του δικτύου κορμού του GSM. Τα τμήματά του είναι:

- Το **Κέντρο Μεταγωγής Κινητών Υπηρεσιών** (Mobile Services Switching Centre, MSC) και ο **Καταχωρητής Θέσης Επισκέπτη** (Visitor Location Register, VLR), δηλαδή ο βασικός μεταγωγέας του δικτύου και η βάση δεδομένων που αποθηκεύει τα προσωρινά στοιχεία του συνδρομητή π.χ. τρέχουσα θέση του.

- Το **Διαβιβαστικό Κέντρο Μεταγωγής Κινητών Υπηρεσιών** (Gateway MSC, GMSC) δηλαδή ο μεταγωγέας που συνδέει το UMTS δίκτυο με άλλα δίκτυα CS.

Εδώ πρέπει να σημειωθεί ότι από την έκδοση R5 του UMTS και μετά το υποσύστημα CS έχει καταργηθεί.

Από την άλλη πλευρά, το υποσύστημα PS αποτελείται από:

- Τον **Εξυπηρετών Κόμβο Υποστήριξης GPRS** (Serving GPRS Support Node, SGSN), που παίζει το ρόλο του MSC στο GSM και διαχειρίζεται τη μεταφορά των πακέτων.
- Τον **Διαβιβαστικό Κόμβο Υποστήριξης GPRS** (Gateway GPRS Support Node, GGSN), που παρέχει πύλη εξόδου προς άλλες IP υπηρεσίες.

Γενικά, ένα Δίκτυο Κορμού μπορεί να λειτουργεί ως **οικείο δίκτυο** (Home Network, HN) για έναν συνδρομητή, με την έννοια ότι έχει κάνει σε αυτό την εγγραφή του ή ως **δίκτυο εξυπηρέτησης** (Serving Network, SN). Το τελευταίο έχει συνάψει συμφωνία περιαγωγής (roaming agreement) με το οικείο δίκτυο του συνδρομητή με σκοπό να τον εξυπηρετεί όταν αυτός κινείται στην περιοχή που καλύπτει, με την προϋπόθεση ότι στην ίδια περιοχή δεν παρέχει επαρκή ή καθόλου κάλυψη το οικείο δίκτυο του συνδρομητή.

Τέλος, υπάρχουν και οι γνωστές από το GSM οντότητες, που είναι:

- Ο **Καταχωρητής Οικείας Θέσης** (Home Location Register, HLR, UMTS R5) ή **Εξυπηρετητής Οικείου Συνδρομητή** (Home Subscriber Server, HSS, UMTS R6), όπου αποθηκεύονται στατικές πληροφορίες για όλους τους συνδρομητές που χρησιμοποιούν τις υπηρεσίες του συγκεκριμένου παρόχου (π.χ. έχουν συνάψει με αυτόν συμβόλαιο και είναι για αυτούς οικείο δίκτυο). Εκτός των πληροφοριών αυτών όμως, δημιουργεί και άλλες, οι οποίες χρησιμοποιούνται για υπηρεσίες όπως στην αυθεντικοποίηση χρηστών και κατ' επέκταση κατά τον έλεγχο πρόσβασης στο δίκτυο.
- Στα 3GPP δίκτυα, το AuC του δικτύου GSM έχει ολοκληρωθεί με το αντίστοιχο HLR/HSS της 3G αρχιτεκτονικής.

Σε γενικές γραμμές, οι απαιτήσεις από το βασισμένο στην τεχνολογία IP δίκτυο κορμού του UMTS συνοψίζονται στα εξής:

- Υποστήριξη περιαγωγής και μεταπομπής σε δίκτυα δεύτερης γενιάς (π.χ. GSM, GPRS).
- Υποστήριξη τερματικών τρίτης γενιάς που χρησιμοποιούν μεταγωγή κυκλώματος, σε ένα δίκτυο κορμού UMTS εξολοκλήρου βασισμένο σε IP.
- Υποστήριξη καινούργιων (π.χ. IP και πολυμέσα) αλλά και υπαρχόντων υπηρεσιών, όπως η ομιλία, τα μηνύματα SMS και κάποιες συμπληρωματικές υπηρεσίες ευφυών δικτύων. Η υποστήριξη των υπηρεσιών δεύτερης γενιάς αποτελεί σοβαρή απαίτηση, αφού οι συνδρομητές που έχουν συνηθίσει να χρησιμοποιούν τις υπηρεσίες του GSM, ίσως να μην είναι διατεθειμένοι να τις εγκαταλείψουν όταν θα κάνουν χρήση του καινούργιου συστήματος UMTS ή όταν θα περιαχθούν σε ένα τέτοιο σύστημα.

  Από τη δεύτερη απαίτηση συνεπάγεται ότι θα συνυπάρχουν τρεις τύποι κινητών τερματικών τρίτης γενιάς: αυτά που θα υποστηρίζουν τη μεταγωγή κυκλώματος, αυτά που θα υποστηρίζουν τη μεταγωγή πακέτου, και αυτά που θα υποστηρίζουν και τα δύο είδη μεταγωγής. Στη ραδιοδιεπαφή θα πρέπει να υποστηρίζεται τόσο η μεταγωγή κυκλώματος όσο και η μεταγωγή πακέτου. Η μεταγωγή κυκλώματος θα πρέπει να χρησιμοποιείται για τα παραδοσιακά τερματικά μεταγωγής κυκλώματος, κάνοντας βέλτιστη χρήση των ραδιοπόρων για τις υπηρεσίες φωνής. Η μεταγωγή πακέτου θα πρέπει να είναι περισσότερο ευέλικτη ώστε να επιτρέπει την παροχή διαφόρων ειδών υπηρεσιών και θα πρέπει να διευκολύνει τη δημιουργία εφαρμογών πολυμέσων, θα είναι όμως λιγότερο αποδοτική ως προς την κατανάλωση φάσματος, εξαιτίας της κεφαλίδας IP που θα περιέχει κάθε πακέτο.

Ένα βασικό πλεονέκτημα του UMTS είναι οι τέσσερις κλάσεις που έχουν οριστεί για την ποιότητα των παρεχομένων υπηρεσιών.

- *Conversational*:
  για εφαρμογές πραγματικού χρόνου (π.χ. ομιλία ή τηλεδιάσκεψη).

- *Streaming*:
  για ελεγχόμενη μεταβλητότητα στην καθυστέρηση (π.χ. εφαρμογές Video, RealAudio).
- *Interactive*:
  για μικρό ποσοστό απωλειών με ύπαρξη μεγίστου επιτρεπόμενου χρόνου διεκπεραίωσης (π.χ. ανάγνωση ιστοσελίδων).
- *Background*:
  για μικρό ποσοστό απωλειών, χωρίς ύπαρξη εγγύησης για το συνολικό χρόνο διεκπεραίωσης (π.χ. ανάκτηση ηλεκτρονικού ταχυδρομείου). [6]

Εντούτοις, μεγάλη τεχνολογική πρόκληση για το UMTS, είναι το αν θα μπορέσει τελικά να παράσχει επαρκή ποιότητα υπηρεσιών (QoS-- Quality of Service), ιδιαίτερα όσον αφορά το ασύρματο δίκτυο πρόσβασης, στις υπηρεσίες πραγματικού χρόνου που πρεσβεύει προκειμένου να ελέγχονται οι καθυστερήσεις εξαιτίας της μεταπομπής, να πραγματοποιείται η διαχείριση των λιγοστών ραδιοπόρων, και να ελέγχεται η εισαγωγή των χρηστών.

ΚΕΦΑΛΑΙΟ 2

ΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ GSM

2.1 Στόχοι των μηχανισμών ασφάλειας

Η χρήση των τηλεπικοινωνιών για μετάδοση δεδομένων καθιστά τα εκάστοτε Δημόσια Επίγεια Δίκτυα Κινητών Επικοινωνιών (PLMN, Public Land Mobile Networks) ευπαθή στις ακόλουθες καταστάσεις [7]:

- χρήση των πόρων τους από μη εξουσιοδοτημένους χρήστες που με τη βοήθεια στρεβλών κινητών συσκευών προσπαθούν να προσωποποιηθούν νόμιμους συνδρομητές
- παράνομη καταγραφή των πληροφοριών που ανταλλάσσονται στο ραδιοκανάλι.

Για το λόγο αυτό, οι όποιοι μηχανισμοί ασφάλειας θα έπρεπε να εξασφαλίζουν :

- ότι το ραδιοκανάλι θα ήταν τόσο ασφαλές όσο τουλάχιστον και το σταθερό τηλεφωνικό δίκτυο, δηλαδή θα παρείχε ανωνυμία και εμπιστευτικότητα σε ευαίσθητα δεδομένα και προστασία απέναντι σε παράνομες υποκλοπές.
- τη χρήση μηχανισμού αυθεντικοποίησης της ταυτότητας του συνδρομητή, που να εξασφαλίζει προστασία του δικτύου από λανθασμένες χρεώσεις στα τιμολόγια
- ότι ένα δίκτυο κινητής δε θα μπορούσε να υποβαθμίσει το επίπεδο ασφάλειας ενός άλλου, είτε σκόπιμα είτε ακούσια.

Επίσης, οι μηχανισμοί ασφάλειας υπόκεινται σε συγκεκριμένους περιορισμούς που εξασφαλίζουν την απρόσκοπτη επικοινωνία των νόμιμων συνδρομητών. Ειδικότερα, οι διαδικασίες ασφάλειας δεν πρέπει :

- να επιβαρύνουν με πρόσθετη καθυστέρηση την εγκατάσταση μιας τηλεφωνικής κλήσης
- να αυξάνουν το εύρος ζώνης του καναλιού που διατίθεται για την επικοινωνία

- να προσθέτουν επιπλέον πολυπλοκότητα στο υπόλοιπο σύστημα
- να επιβαρύνουν με επιπλέον κόστος τους συνδρομητές.

Οι αρχές του συστήματος ασφαλείας του GSM είναι οι εξής [8] :

- **Εμπιστευτικότητα της ταυτότητας του συνδρομητή**, ώστε να είναι δύσκολη η ταυτοποίησή του από τρίτους,
- **Αυθεντικοποίηση της ταυτότητας του συνδρομητή** στο δίκτυο, με σκοπό τη σωστή τιμολόγησή του,
- **Κρυπτογράφηση** των δεδομένων του χρήστη και των δεδομένων ελέγχου,
- **Χρήση της κάρτας SIM** ως μηχανισμό ασφάλειας.

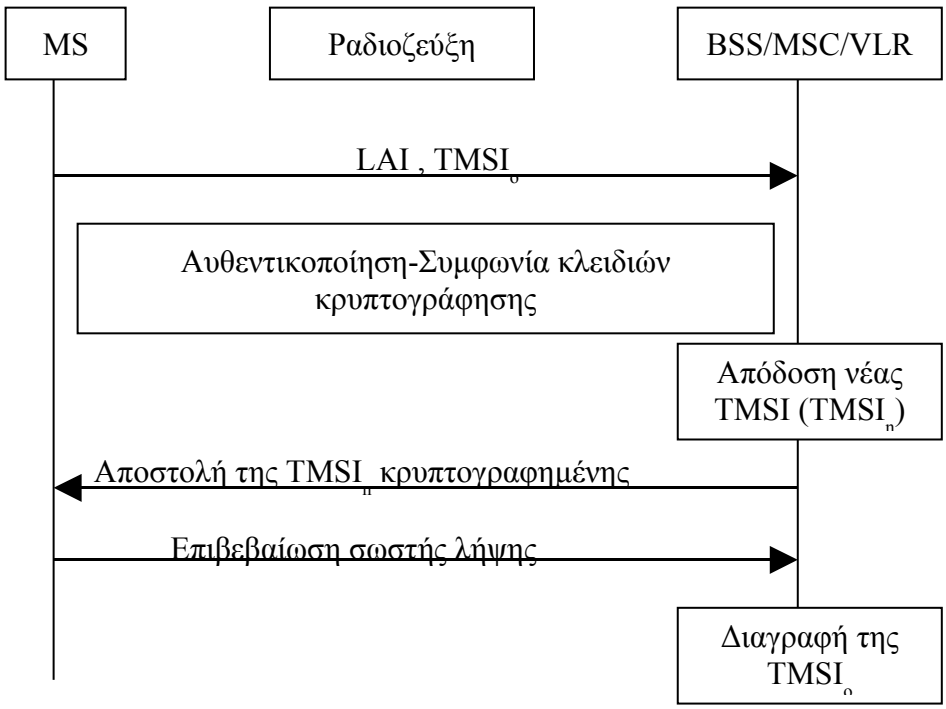
2.2 Ανάλυση των μηχανισμών ασφάλειας

Στις ενότητες που ακολουθούν παρουσιάζονται οι μηχανισμοί ασφάλειας του συστήματος GSM. Η λειτουργία των μηχανισμών αυτών περιγράφεται αναλυτικά στο [16].

2.2.1 Εμπιστευτικότητα της ταυτότητας του συνδρομητή

Ο συγκεκριμένος μηχανισμός έχει σκοπό να αποτρέψει τη διάθεση ή την αποκάλυψη της ταυτότητας IMSI σε μη εξουσιοδοτημένα άτομα ή οντότητες. Προκειμένου να επιτυγχάνεται το απαιτούμενο επίπεδο προστασίας, η χρήση και μετάδοση της ταυτότητας IMSI πρέπει να αποφεύγεται σε όλα τα επίπεδα σηματοδοσίας. Επισημαίνεται ότι η γνωστοποίηση της IMSI σε τρίτους είναι δυνατόν να διευκολύνει την ανίχνευση της γεωγραφικής του θέσης, αλλά και των πόρων του δικτύου που χρησιμοποιεί. Για το σκοπό αυτό χρησιμοποιείται μια προσωρινή ταυτότητα, που καλείται Temporary Mobile Subscriber Identity (TMSI). Η ταυτότητα TMSI έχει ισχύ μόνο σε μια ορισμένη γεωγραφική περιοχή και πρέπει να συνοδεύεται από την ταυτότητα Location Area Identification (LAI), για την αποφυγή οποιασδήποτε ασάφειας.

Όταν ο κινητός σταθμός (MS) προσπαθήσει για πρώτη φορά να αποκτήσει πρόσβαση σε ένα PLMN, χρησιμοποιεί την IMSI για να δηλώσει την ταυτότητά του. Ακολουθεί η αυθεντικοποίηση του MS από το PLMN, και ο διαμοιρασμός του κλειδιού κρυπτογράφησης (Kc). Αφού το PLMN ενεργοποιήσει την κρυπτογράφηση, το VLR «γεννά» και αποδίδει στον κινητό σταθμό μια προσωρινή ταυτότητα TMSI, ενώ παράλληλα καταγράφει και αποθηκεύει τη σχέση μεταξύ των ταυτοτήτων IMSI και TMSI του MS. Η TMSI αποστέλλεται στο MS κρυπτογραφημένη με το κλειδί Kc, έτσι ώστε την επόμενη φορά που το MS ζητήσει πρόσβαση στο PLMN να χρησιμοποιήσει την TMSI αντί της IMSI. Τότε, το VLR του PLMN θα αναζητήσει τη μόνιμη ταυτότητα του MS μέσα από τον πίνακα αντιστοίχησης TMSI-IMSI. Αφού πιστοποιηθεί επιτυχώς, το VLR αναθέτει στο MS μια άλλη ταυτότητα TMSI. Στην περίπτωση που το MS μεταβεί σε κελί που υπόκειται σε άλλο VLR, ή ακόμη και στην περίπτωση επιτυχημένης επαναπιστοποίησης στο ίδιο VLR, αποστέλλεται πάντα μια νέα TMSI στον κινητό σταθμό. Τότε, ο κινητός σταθμός αποθηκεύει στη SIM τη νέα TMSI και διαγράφει τη συσχέτιση με προηγούμενες TMSI. Το ίδιο συμβαίνει και στην πλευρά του VLR, το οποίο απομακρύνει την συσχέτιση της συγκεκριμένης IMSI με την παλιά TMSI.



Σχήμα 3 : Προστασία της IMSI μέσω της χρησιμοποίησης της TMSI [7]

Ωστόσο, θα πρέπει να επισημανθεί ότι στην περίπτωση που ο κινητός σταθμός πιστοποιείται για πρώτη φορά σε ένα PLMN, θα πρέπει να αποστείλει – μετά τη διαδικασία της αυθεντικοποίησης - την ταυτότητα IMSI για να αποκτήσει εν συνεχεία μια προσωρινή ταυτότητα. Επίσης, το ίδιο συμβαίνει και σε περίπτωση ανανέωσης θέσης, όταν το παλιό VLR είτε δεν είναι προσβάσιμο από το νέο VLR, είτε έχει υποστεί βλάβη στο λογισμικό και απώλειες δεδομένων. Στις περιπτώσεις αυτές, το νέο VLR δε γνωρίζει τη συσχέτιση μεταξύ της παλιάς TMSI και της IMSI, οπότε απαιτεί από το MS να του αποστείλει τη μόνιμη ταυτότητά του. Οι εξαιρετικές αυτές περιπτώσεις ελλοχεύουν κινδύνους αποκάλυψης της μόνιμης ταυτότητας IMSI σε κάποιους που είναι δυνατόν να «ακούν» το δίαυλο επικοινωνίας.

2.2.2 Αυθεντικοποίηση της ταυτότητας του συνδρομητή

Σκοπός του συγκεκριμένου μηχανισμού είναι να διασφαλίσει ότι ο μόνιμος προσωπικός αριθμός αναγνώρισης του συνδρομητή (IMSI) ή ο αριθμός της προσωρινής του ταυτότητας (TMSI), που μεταφέρονται από την κινητή συσκευή του συνδρομητή στο PLMN κατά τη διαδικασία αναγνώρισής του στη ραδιοζεύξη είναι αληθινή. Η ύπαρξη αυτού του μηχανισμού αποσκοπεί τόσο στην προστασία του δικτύου από μη εξουσιοδοτημένη χρήση του, όσο και στην προστασία των νόμιμων συνδρομητών του PLMN από εισβολείς που ενδέχεται να προσπαθήσουν να τους προσωποποιηθούν.

Η έναρξη της διαδικασίας μπορεί να ενεργοποιηθεί από το δίκτυο, όποτε κριθεί αναγκαίο. Συνήθως λαμβάνει χώρα στις ακόλουθες περιπτώσεις :

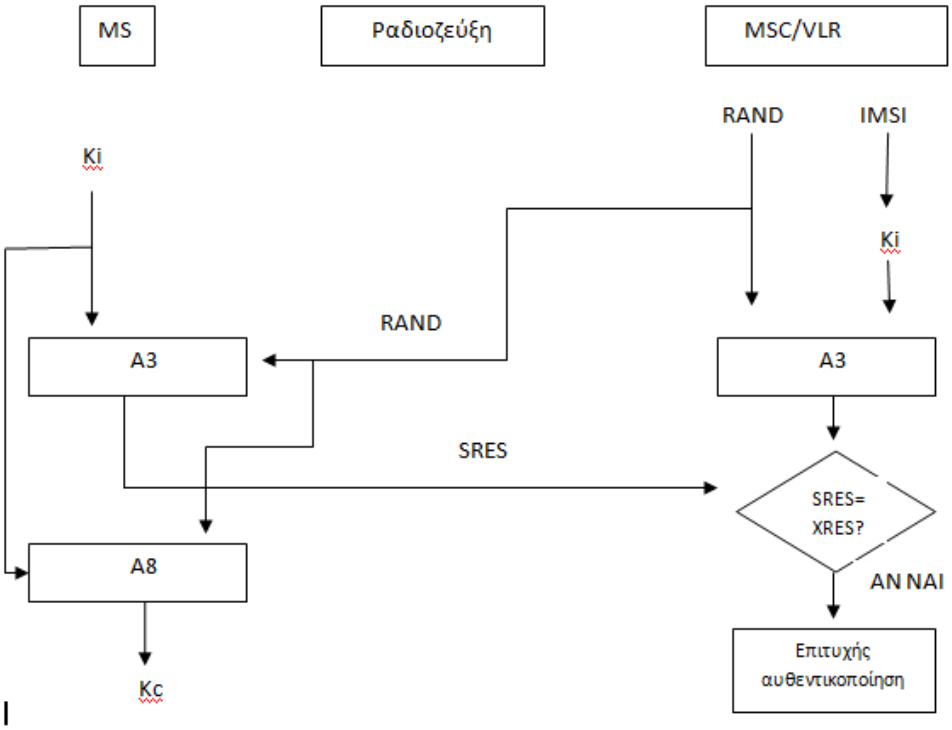
- Όταν γίνεται μια αλλαγή στα δεδομένα που σχετίζονται με το συνδρομητή και που υπάρχουν στο VLR ή στο HLR (π.χ. ενημέρωση θέσης με αλλαγή του VLR, εγγραφή ή διαγραφή σε/από μια νέα υπηρεσία κτλ)
- Όταν ζητείται πρόσβαση σε μια υπηρεσία (π.χ. κλήση από/προς το συνδρομητή)
- Κατά την πρώτη αίτηση πρόσβασης στο δίκτυο.

Η ασφάλεια της διαδικασίας βασίζεται στο μυστικό κλειδί K_i , μήκους 128 bits, το οποίο είναι αποθηκευμένο στην κάρτα SIM. Κάθε SIM, άρα και ο συνδρομητής που

τη διαθέτει, έχει, από τη στιγμή που θα δημιουργηθεί, ένα μοναδικό μυστικό κλειδί K_i. Το ίδιο κλειδί είναι αποθηκευμένο στο δίκτυο στη μονάδα AuC, όπως και όλα τα μυστικά κλειδιά των συνδρομητών[1].

Όταν ο MS τεθεί σε λειτουργία ψάχνει να βρει ένα δίκτυο για να συνδεθεί, «ακούγοντας» σε ένα σύνολο συχνοτήτων. Μόλις βρει ένα ασύρματο δίκτυο ζητά πρόσβαση σε αυτό στέλνοντας ένα μήνυμα στο BTS, αποστέλλοντας παράλληλα την προσωρινή του ταυτότητα (TMSI). Το BTS επικοινωνεί με το MSC, το οποίο είναι υπεύθυνο για την παροχή ή μη της πρόσβασης του αιτούμενου MS στο PLMN. Το MSC ζητά από το HLR να του αποστείλει πέντε σετ τριπλετών ασφαλείας. Μια τριπλέτα περιλαμβάνει τρεις αριθμούς: το RAND (τυχαίος αριθμός 128 bits), το SRES (ένας αριθμός 32-bit που υπολογίζεται από το RAND και το μυστικό κλειδί με τον αλγόριθμο A3) και το κλειδί κρυπτογράφησης K_c που υπολογίζεται με τη βοήθεια του K_i. Οι τριπλέτες υπολογίζονται μέσα στο AuC, του οικείου PLMN (HPLMN) και αποστέλλονται στο HLR, όταν ζητηθούν. Το HLR προμηθεύει αυτές τις τριπλέτες στο MSC. Ακολούθως, το MSC επιλέγει μια τριπλέτα και τη στέλνει στο MS. Στη SIM του MS, εκτελείται ο αλγόριθμος A3, που δέχεται στην είσοδο το RAND και το K_i και υπολογίζεται η "απάντηση" SRES, η οποία και αποστέλλεται πίσω στο MSC. Σε περίπτωση που τα XRES και SRES συμφωνούν, το MSC θεωρεί ότι η SIM περιέχει ένα νόμιμο μυστικό κλειδί και η διαδικασία ολοκληρώνεται με το MS να αποκτά πρόσβαση στο δίκτυο. Διαφορετικά, το MSC δεν επιτρέπει την πρόσβαση στο MS. Επίσης, κατά τη διάρκεια της διαδικασίας αυτής υπολογίζεται στη SIM, με τον αλγόριθμο A8 και με τα ίδια στοιχεία για είσοδο (RAND, K_i), το κλειδί K_c, που θα χρησιμοποιηθεί αργότερα για την κρυπτογράφηση/ αποκρυπτογράφηση των μηνυμάτων.

[1] Ένα PLMN μπορεί να περιλαμβάνει ένα ή περισσότερα AuC. Το AuC μπορεί να βρίσκεται μέσα στο HLR.



Σχήμα 4: Η διαδικασία αυθεντικοποίησης ταυτότητας στο GSM.

Σε ότι αφορά τη διαδικασία αυθεντικοποίησης επισημαίνονται τα παρακάτω:

- Σε κάθε πρόσβαση του κινητού στο δίκτυο πρέπει να αποστέλλεται διαφορετικό RAND κάθε φορά, έτσι ώστε ακόμα και η απόκτησή του από κάποιον τρίτο κατά τη διάρκεια μιας σύνδεσης να καταστεί άχρηστη την επόμενη. Η χρησιμοποίηση κάθε φορά και άλλου RAND οδηγεί και στον υπολογισμό διαφορετικών σε κάθε περίπτωση SRES και K_c .
- Η διαδικασία δημιουργίας τριπλετών λαμβάνει χώρα στο AuC του οικείου δικτύου HPLMN. Έτσι, όταν ο χρήστης περιάγεται μέσα στα όρια άλλου δικτύου (Visited PLMN, VPLMN), ζητείται από το HPLMN του χρήστη να αποσταλούν οι τριπλέτες για την αυθεντικοποίηση. Έτσι, το VPLMN δε χρειάζεται να γνωρίζει το κλειδί K_i του συνδρομητή, ούτε τους αλγόριθμους αυθεντικοποίησης που μπορεί να είναι διαφορετικοί μεταξύ δυο PLMN.
- Αν και για την αυθεντικοποίηση είναι αρκετό μόνο ένα σετ τριπλετών το HLR ζητά από το AuC του PLMN πέντε τέτοια σετ. Αυτό συμβαίνει έτσι ώστε να μη

χρειάζεται το HLR να ρωτά το AuC κάθε φορά που το ΜΕ ζητά πρόσβαση στο δίκτυο από κάποιον άλλο πάροχο, στα όρια του οποίου μπορεί να βρίσκεται. Έτσι, κερδίζεται χρόνος και βελτιώνεται η απόδοση του συστήματος.

- Οι αλγόριθμοι A3 και A8 μπορεί να υλοποιούνται διαφορετικά από πάροχο σε πάροχο. Στην πραγματικότητα, τα ονόματα "A3", "A8" δεν είναι συγκεκριμένοι αλγόριθμοι αλλά χρησιμοποιούνται για να υποδείξουν το είδος των αλγορίθμων για την εξαγωγή του SRES και του κλειδιού K_c. Πάντως, στις περισσότερες των περιπτώσεων η λειτουργικότητα των A3 και A8 εμπεριέχεται σε έναν κοινό αλγόριθμο, τον COMP128. Οι περισσότεροι πάροχοι χρησιμοποιούν τον συγκεκριμένο αλγόριθμο, ο οποίος σχεδιάστηκε μυστικά και δεν είχε δοθεί επίσημα στη δημοσιότητα αρχικά. Νεότερες εκδόσεις του, που υιοθετήθηκαν σταδιακά από τους περισσότερους παρόχους, επειδή παρείχαν μεγαλύτερη ασφάλεια, είναι ο COMP128-2 και ο COMP128-3, ο κώδικας των οποίων παραμένει επίσης μυστικός.

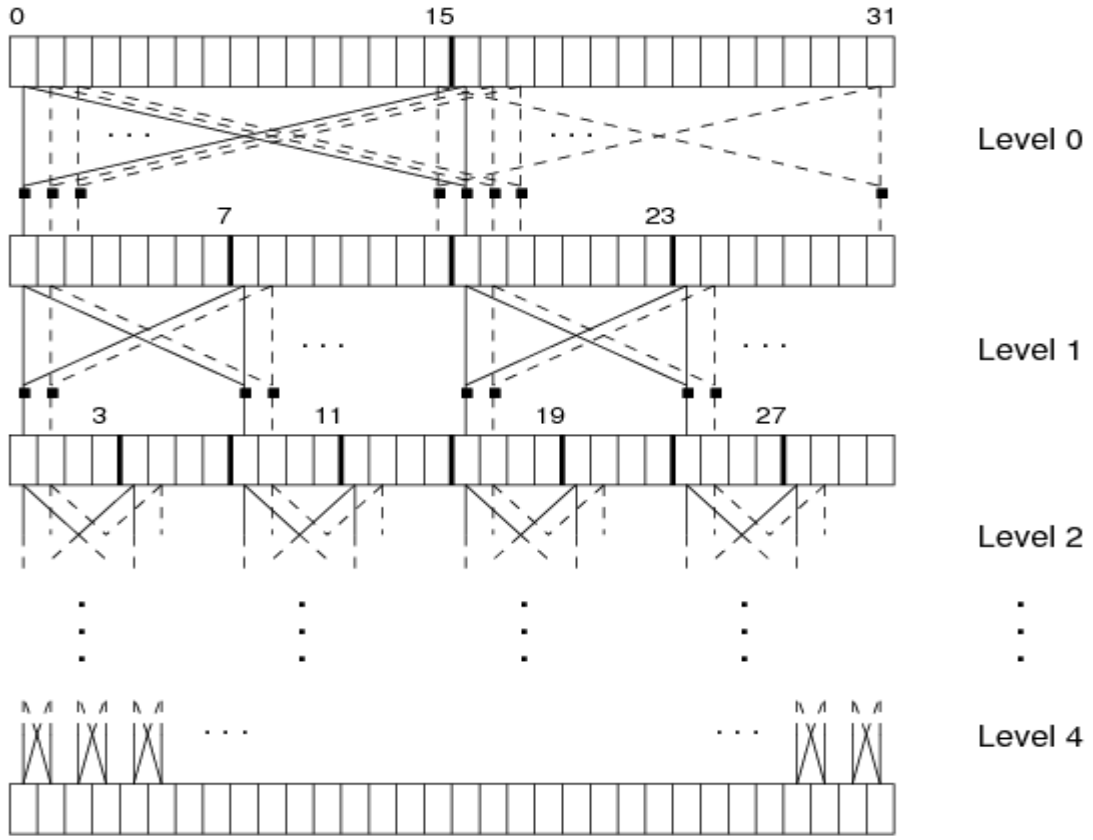
Ο αλγόριθμος COMP128

Ο αλγόριθμος COMP128 είναι μια συνάρτηση κατακερματισμού με κλειδί [9]. Λαμβάνει ως είσοδο το μήκους 16 bytes κλειδί Ki και την τιμή RAND (16 bytes) και παράγει ως έξοδο 96 bits, από τα οποία 32 bits για την απάντηση SRES και 54+10=64 bits για το κλειδί κρυπτογράφησης Kc. Ο αλγόριθμος αποθηκεύει αρχικά τις τιμές εισόδου σε ένα διάνυσμα X[] των 32 bytes. Το Ki αποθηκεύεται στα πρώτα 16 bytes (X[0…15]) και το RAND στα υπόλοιπα (X[16…31]). Ακολούθως, εφαρμόζονται οκτώ επαναληπτικοί βρόχοι στο διάνυσμα X[]. Κάθε επανάληψη αρχίζει με συμπίεση των bytes που μοιάζει με δομή «πεταλούδας». Η συμπίεση διεξάγεται σε πέντε επίπεδα αναζητήσεων στους πίνακες T0[512], T1[256], T2[128], T3[64] και T4[32] αντίστοιχα. Σε όλες τις επαναλήψεις εκτός από την τελευταία, τη συμπίεση ακολουθεί μια διαδικασία αντιμετάθεσης. Κάθε Ti περιέχει τιμές των (8-i) bits. Έτσι, η συμπίεση έχει ως αποτέλεσμα 32 τιμές των 4 bits, που στη συνέχεια συγκροτούν 16 bytes πριν γίνει η αντιμετάθεση. Αυτά τα 16 bytes αποθηκεύονται στο X[16…31] και το Ki φορτώνεται στο X[0…15] πριν ξεκινήσει η επόμενη επανάληψη. Τα 128 bits που προκύπτουν μετά τις 8 επαναλήψεις συμπιέζονται

περαιτέρω σε 12 bytes, που αποτελούν και την έξοδο του αλγόριθμου. Ο ψευδοκώδικας συμπίεσης του COMP128 είναι ο παρακάτω:

```
for j = 0 to 4 do {
  for k = 0 to 2^j – 1 do {
    for l = 0 to 2^(4 – j) – 1 do  {
      m = l + k*2^(5 – j) ;
      n = m + 2^(4 – j) ;
      y = (X[m] + 2*X[n]) mod 2^(9 – j) ;
      z = (2*X[m] + X[n]) mod 2^(9 – j) ;
      X[m] = T[j][y] ;
      X[n] = T[j][z] ;
     }
   }
 }
```

Σε κάθε επίπεδο, η συμπίεση εφαρμόζεται σε ζεύγη τομέων του X[] ίσων διαστάσεων. Στο επίπεδο 0 (j=0) το X[] χωρίζεται σε 2 τομείς : X[0…15] και X[16…31]. Η τιμή του καθενός από τα «δεξιά» στοιχεία, X[i+16], (i=0…15), συνδυάζεται με αυτή από τα αντίστοιχα «αριστερά», X[i], για να υπολογιστεί η τιμή y=(X[i] + 2*X[i+16]) mod 512. Παρομοίως, η τιμή καθενός από τα «αριστερά» στοιχεία X[i] συνδυάζεται με την τιμή του αντίστοιχου δεξιού στοιχείου για να υπολογιστεί η τιμή z=(2*X[i] + X[i+16]) mod 512. Τα X[i] και X[i+16] αντικαθίστανται στη συνέχεια από τις τιμές T0[y] και T0[z], πριν ξεκινήσει το επόμενο επίπεδο. Αυτή η σταυρωτή αντικατάσταση, η οποία απεικονίζεται στο σχήμα 6, αναφέρεται και ως “δομή πεταλούδας”. Σε κάθε νέο επίπεδο, ένας τομέας διαιρείται σε ένα ζεύγος από τομείς στο οποίο εφαρμόζεται η ίδια διαδικασία. Σημειώνεται ότι το μέγεθος του πίνακα μειώνεται σταδιακά σε κάθε νέο επίπεδο. Επομένως, στο επίπεδο 1 υπολογίζεται το y=(X[i] + 2*X[i+8]) mod 256, και το z=(2*X[i] + X[i+8]) mod 256, για i=0..7, 16..23. Στο επίπεδο 2, υπολογίζεται το y=(X[i] + 2*X[i+4]) mod 128 και το z=(2*X[i] + X[i+4]) mod 128, για i=0..3, 8..11, 16..19, 24..27 και ούτω καθεξής.



Σχήμα 5. Δομή «πεταλούδας» στη διαδικασία συμπίεσης στον COMP128 [9]

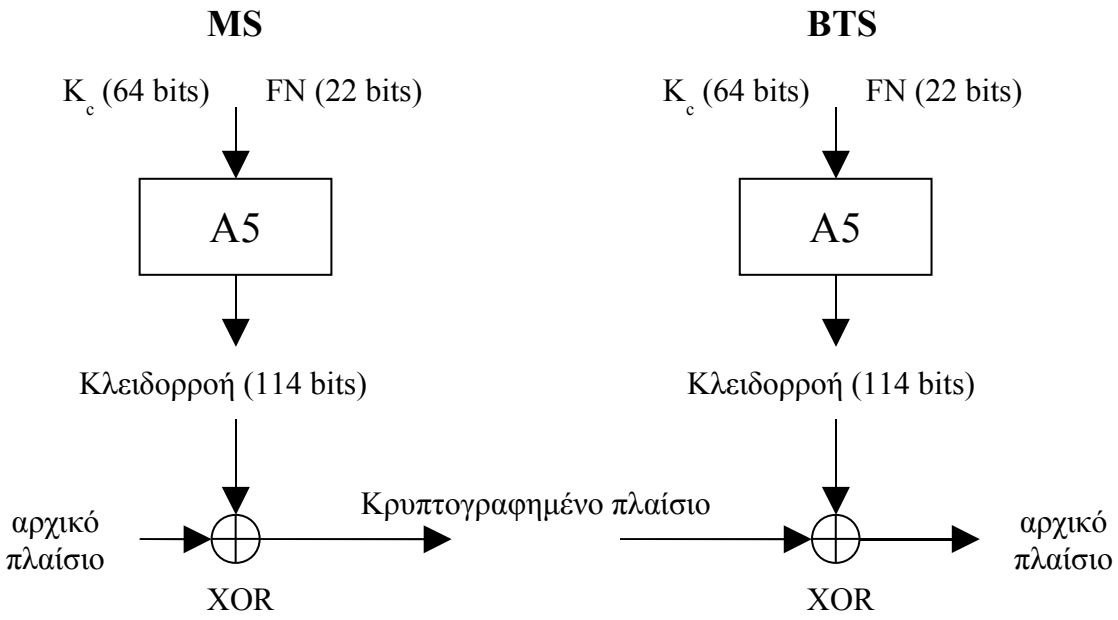
2.2.3 Κρυπτογράφηση των δεδομένων του συνδρομητή

Η κρυπτογράφηση των δεδομένων του συνδρομητή αφορά τις πληροφορίες που μεταδίδονται σε ένα ράδιο-κανάλι στη διεπαφή MS-BTS. Η κρυπτογράφηση δεν πραγματοποιείται στα πλαίσια ενός από άκρη σε άκρη (end-to-end) μηχανισμού ασφάλειας. Βασίζεται στη χρήση του κλειδιού Kc, το οποίο δημιουργείται κατά τη διαδικασία της αυθεντικοποίησης του συνδρομητή, και χρησιμοποιείται για να προσφέρει εμπιστευτικότητα δεδομένων του χρήστη και σηματοδοσίας (π.χ. TMSI) στην ασύρματη διεπαφή MS-BTS και προστασία από «ωτακουστές» του ραδιο-καναλιού.

Όπως αναφέρθηκε στην παράγραφο 2.2.2, αφού το MSC αποστείλει στον κινητό σταθμό το RAND, υλοποιείται μέσα στην κάρτα SIM του MS, ο αλγόριθμος A3 για την παραγωγή του SRES, αλλά και ο αλγόριθμος A8. Ο τελευταίος παίρνει ως

είσοδο το RAND και το Ki, και παράγει το κλειδί κρυπτογράφησης Kc, με μήκος 54 bits, στα οποία προστίθενται δέκα μηδενικά για να πάρει το τελικό του μήκος (64 bits). Το κλειδί αυτό, που βρίσκεται στην τριπλέτα που χρησιμοποιείται από το δίκτυο για τη διαδικασία της αυθεντικοποίησης (είναι δηλαδή στην κατοχή του BTS)[2], θα χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που μεταδίδει και δέχεται ο χρήστης. Μετά την αυθεντικοποίηση, το BTS ενημερώνει τον κινητό σταθμό σχετικά με το ποιους αλγορίθμους κρυπτογράφησης υποστηρίζει και δίνει εντολή για έναρξη της διαδικασίας (cipher mode command). Ο αλγόριθμος για την κρυπτογράφηση των δεδομένων είναι ο A5, ο οποίος σε αντίθεση με τους A3/8, είναι υλοποιημένος στην κινητή συσκευή και όχι στη SIM. Δέχεται στην είσοδο το κλειδί Kc (64 bits) και τον αριθμό πλαισίου που πρόκειται να κρυπτογραφηθεί (Frame Number, FN -22 bits) ή να αποκρυπτογραφηθεί. Ο αριθμός πλαισίου χρησιμοποιείται για λόγους συγχρονισμού μεταξύ του MS και του BTS. Ο αλγόριθμος παράγει μια κλειδική ακολουθία 228 bits, που είναι μοναδική για κάθε πλαίσιο δεδομένων, αφού το FN αλλάζει κατά τη διάρκεια της κλήσης. Τα πρώτα 114 bits χρησιμοποιούνται για την κρυπτογράφηση των μεταδιδόμενων δεδομένων και αποτελούν το BLOCK1. Τα υπόλοιπα 114 bits χρησιμοποιούνται για την αποκρυπτογράφηση (BLOCK2) των δεδομένων που λαμβάνονται από το MS. Τα δεδομένα που πρόκειται να μεταδοθούν προστίθενται (XOR) με την κλειδική ακολουθία που παράγεται και δημιουργούν την κρυπτογραφημένη ακολουθία δεδομένων. Η διαδικασία της αποκρυπτογράφησης γίνεται με τον ίδιο ακριβώς τρόπο και έτσι ο δέκτης λαμβάνει τελικά το καθαρό κείμενο. Ο συγχρονισμός μεταξύ των δύο μερών επιτυγχάνεται ως εξής: τη στιγμή που το BTS αποστείλει τη cipher command στον κινητό σταθμό ξεκινά την αποκρυπτογράφηση. Η κρυπτογράφηση και αποκρυπτογράφηση ξεκινά στην πλευρά του MS, όταν αυτό λάβει σωστά την εντολή κρυπτογράφησης (cipher mode complete). Όταν το δίκτυο λάβει το πρώτο κρυπτογραφημένο μήνυμα από το MS και το αποκρυπτογραφήσει σωστά, ξεκινά και η κρυπτογράφηση από πλευράς δικτύου.

[2] Το Kc μεταφέρεται από το HPLMN (AuC→HLR) στο VPLMN (VLR→BS).



Σχήμα 6: Κρυπτογράφηση/αποκρυπτογράφηση πλαισίου

Πρέπει να σημειωθεί ότι το ίδιο κλειδί Kc χρησιμοποιείται για όσο διάστημα το δίκτυο δεν πιστοποιεί τον κινητό σταθμό. Στην περίπτωση που γίνει αυθεντικοποίηση δημιουργείται ένα νέο κλειδί Kc. Ωστόσο, η διαδικασία αυθεντικοποίησης δεν είναι υποχρεωτικό να γίνεται σε κάθε νέα κλήση, οπότε το ίδιο κλειδί Kc μπορεί να χρησιμοποιείται για μέρες. Σε περίπτωση μεταπομπής (handover) κατά τη διάρκεια μιας κλήσης, το K_c και όλα τα στοιχεία ασφαλείας, μεταφέρονται στο καινούριο BTS που εξυπηρετεί τον κινητό σταθμό. Το κλειδί K_c παραμένει αναλλοίωτο παρά τη μεταπομπή.

Ο αλγόριθμος A5 διαφέρει από τους αλγόριθμους A3/8 και σε ένα ακόμα σημείο. Ενώ οι δυο τελευταίοι μπορεί να διαφοροποιούνται από πάροχο σε πάροχο, ο αλγόριθμος A5 είναι συγκεκριμένος και χρησιμοποιείται από όλα τα δίκτυα. Ωστόσο, υπάρχουν αρκετές εκδόσεις του αλγόριθμου αυτού, που εφαρμόζουν και προσφέρουν διαφορετικά επίπεδα ασφάλειας:

- Ο A5/0 δεν εφαρμόζει κρυπτογράφηση.
- Ο A5/1 είναι ο γνήσιος αλγόριθμος A5 που χρησιμοποιείται στην Ευρώπη.
- Ο A5/2 είναι μια, σκόπιμα, πιο «αδύναμη» έκδοση του A5 που δημιουργήθηκε για εξαγωγή εκτός Ευρώπης και χρησιμοποιείται στις ΗΠΑ.

- Ο A5/3 είναι ένας ισχυρότερος αλγόριθμος, που υλοποιήθηκε από την 3GPP για χρήση στα δίκτυα 3ης γενιάς, αλλά χρησιμοποιείται και στο GSM.

2.2.4 Μηχανισμοί ασφάλειας της κάρτας SIM

Πρόκειται για μια «έξυπνη» κάρτα (smart card), η οποία διαθέτει μικροεπεξεργαστή και είναι κατασκευασμένη από πλαστικό υλικό, όπως ακριβώς και οι πιστωτικές κάρτες (σχήμα 7). Μέσα στη SIM είναι αποθηκευμένο το μυστικό κλειδί Ki, το οποίο χρησιμοποιείται, όπως έχει περιγραφεί, στη διαδικασία αυθεντικοποίησης για την παραγωγή της ακολουθίας SRES, αλλά και για του κλειδιού Kc για τις διαδικασίες κρυπτογράφησης, με την εκτέλεση των αλγορίθμων A3 και A8, δηλαδή του COMP128 ή των μεταγενέστερων εκδόσεών του. Το κλειδί Ki είναι γνωστό, εκτός από τη SIM, και στη μονάδα AuC του δικτύου. Η "απάντηση" SRES αποστέλλεται εν συνεχεία στο MSC/VLR του HPLMN, για να επιβεβαιωθεί το γεγονός ότι η συγκεκριμένη κάρτα SIM είναι νόμιμη και δικαιούται πρόσβασης στο δίκτυο. Αν συμβεί αυτό, τότε το MSC/VLR ενημερώνει το VPLMN (serving PLMN) για το κλειδί Kc, ενώ η SIM μεταβιβάζει το ίδιο κλειδί που παρήγαγε από τον A8 στην κινητή συσκευή, για να χρησιμοποιηθεί για την εκτέλεση του A5 και τις διαδικασίες κρυπτογράφησης/αποκρυπτογράφησης.

Σχήμα 7. Η κάρτα SIM

Η κάρτα SIM προστατεύεται από μη εξουσιοδοτημένη χρήση με έναν αριθμό PIN, τον οποίο εισάγει ο χρήστης από το πληκτρολόγιο της συσκευής μετά το άνοιγμά της. Αν ο χρήστης αποτύχει για τρεις συνεχείς φορές να δώσει το σωστό αριθμό PIN, η κάρτα κλειδώνει. Τότε ζητείται να πληκτρολογηθεί ένας δεύτερος αριθμός ασφάλειας, ο PUK (PIN UnlocK). Αν και ο αριθμός αυτός δεν εισαχθεί σωστά για 10 συνεχείς φορές, η κάρτα SIM αρνείται οριστικά την πρόσβαση στο χρήστη σε διαδικασίες αυθεντικοποίησης και πρόσβασης στο δίκτυο, και καθίσταται άχρηστη.

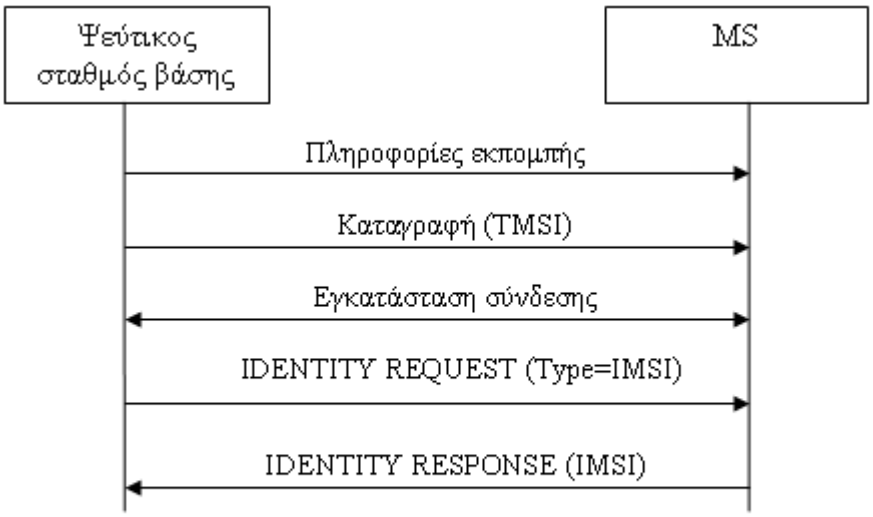
2.3 Αξιολόγηση των μηχανισμών ασφάλειας του GSM

Στην ενότητα αυτή περιγράφονται αναλυτικά τα τρωτά σημεία που συναντώνται στο μοντέλο ασφαλείας του GSM. Γίνεται αναφορά σε διάφορες παθητικές ή ενεργές επιθέσεις που πραγματοποιούνται εκμεταλλευόμενες τις αδυναμίες αυτές, ενώ σε ορισμένες περιπτώσεις προτείνονται λύσεις για την αντιμετώπισή τους.

2.3.1 Ευπάθειες στο μηχανισμό αυθεντικοποίησης της ταυτότητας συνδρομητή

Όπως αναφέρθηκε στην παράγραφο 2.2.1, προκειμένου να προστατευθεί η εμπιστευτικότητα της ταυτότητας του συνδρομητή, η οποία αντιπροσωπεύεται από τον αριθμό IMSI, εφαρμόζεται ο μηχανισμός των προσωρινών ταυτοτήτων. Για να αναγνωριστεί η ταυτότητα ενός νόμιμου συνδρομητή από το δίκτυο, αποστέλλεται από το χρήστη η προσωρινή ταυτότητα TMSI, που έχει ισχύ μόνο τοπικά, δηλαδή σε μια δεδομένη περιοχή, και η οποία συνοδεύεται και από τον αριθμό LAI, που προσδιορίζει αυτήν την περιοχή. Μια νέα TMSI αποδίδεται στο χρήστη σε περίπτωση ανανέωσης της θέσης του (location update). Το δίκτυο κατέχει σε ένα VLR, και διαχειρίζεται, βάσεις δεδομένων όπου αντιστοιχίζεται η TMSI με την IMSI του κάθε συνδρομητή, σε μια δεδομένη χρονική στιγμή. Ωστόσο, μπορούν να υπάρξουν περιπτώσεις, στις οποίες, ο χρήστης, προκειμένου να αναγνωριστεί ή να πιστοποιηθεί αργότερα, καλείται από το δίκτυο, μέσω ενός σήματος "IDENTITY REQUEST", να στείλει την μόνιμη ταυτότητά του IMSI, αντί της προσωρινής. Προφανώς, εφόσον δεν έχει αναγνωριστεί ακόμα ο χρήστης δεν είναι δυνατόν να εφαρμοστεί κρυπτογράφηση, και έτσι η IMSI στέλνεται σε μορφή καθαρού κειμένου. Το γεγονός αυτό μπορεί να επιτρέψει σε έναν επιτιθέμενο, που «ακούει» τη ραδιοζεύξη, να υποκλέψει την IMSI και να μάθει ότι ο συγκεκριμένος χρήστης βρίσκεται στην περιοχή, ή ακόμη να χρησιμοποιήσει την IMSI για να προσωποποιηθεί έναν νόμιμο χρήστη. Αν ληφθεί υπ' όψη και το γεγονός ότι το δίκτυο δεν πιστοποιείται στο χρήστη, ο επιτιθέμενος μπορεί υλοποιώντας ένα ψεύτικο σταθμό βάσης να αντιστοιχίσει την TMSI με την IMSI ενός συνδρομητή,

αφού του στείλει ένα μήνυμα IDENTITY REQUEST, όπως φαίνεται στο σχήμα 8 [13].



Σχήμα 8. Υποκλοπή IMSI από ψεύτικο σταθμό βάσης.

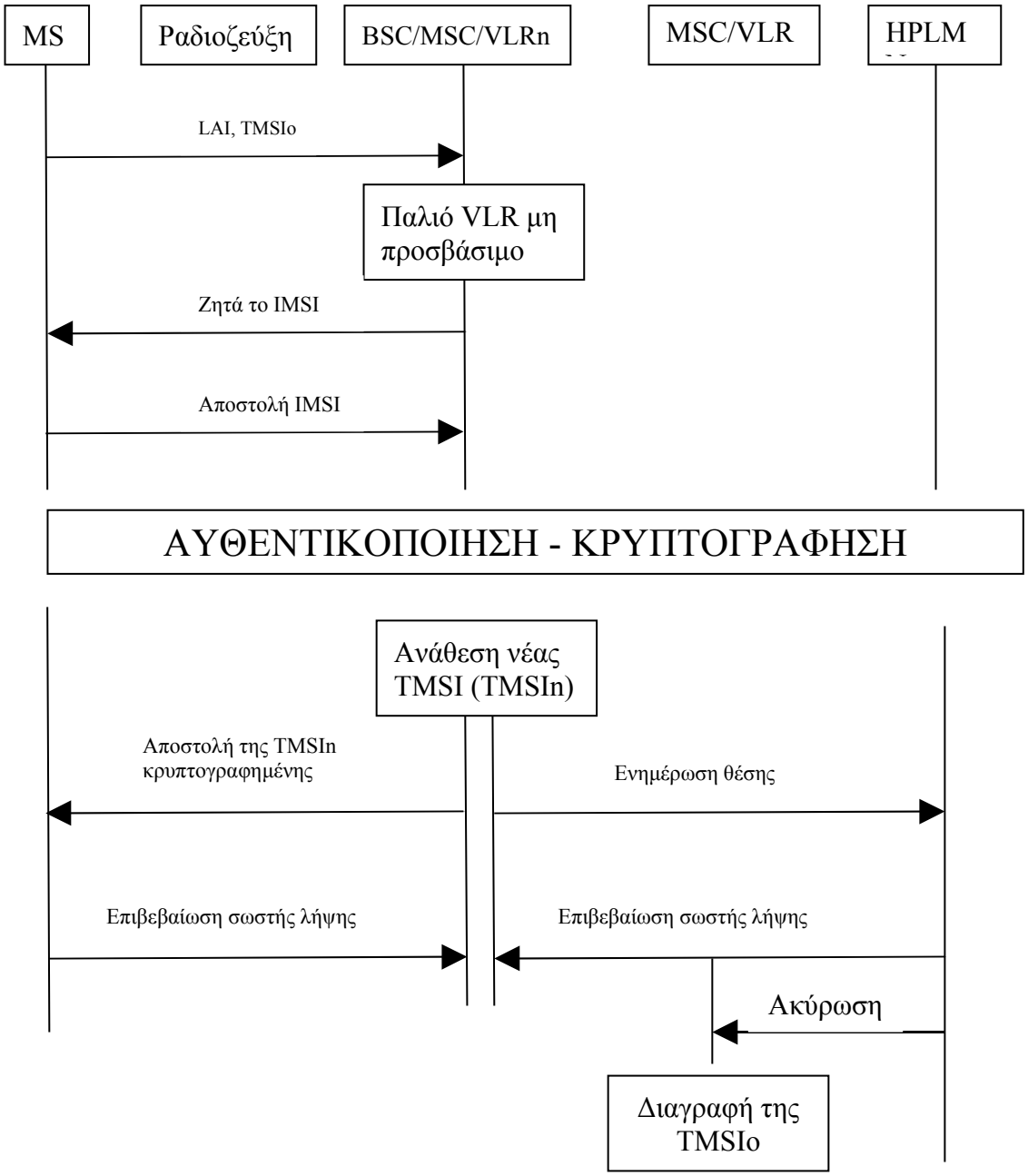
Οι περιπτώσεις στις οποίες ζητείται από το δίκτυο η αποστολή από το MS της μόνιμης ταυτότητας IMSI αντί της προσωρινής είναι:

1)Σε περίπτωση ανανέωσης θέσης σε ένα νέο VLR και το παλιό VLR δεν είναι προσβάσιμο. Γενικά, όταν συμβεί ανανέωση θέσης (location update) σε μια περιοχή που υπάγεται σε διαφορετικό VLR, το νέο VLR (VLRn), στέλνει το TMSI του χρήστη (TMSIo) στο προηγούμενο – "παλιό" – VLR (VLRo), και αυτό στέλνει πίσω το IMSI του συγκεκριμένου χρήστη μαζί με τις πληροφορίες ασφάλειας για τις διαδικασίες αυθεντικοποίησης και κρυπτογράφησης. Αν όμως το VLRo δεν είναι προσβάσιμο από το VLRn, τότε το VLRn ζητά από το χρήστη να του στείλει το IMSI «καθαρό» (σχήμα 9).

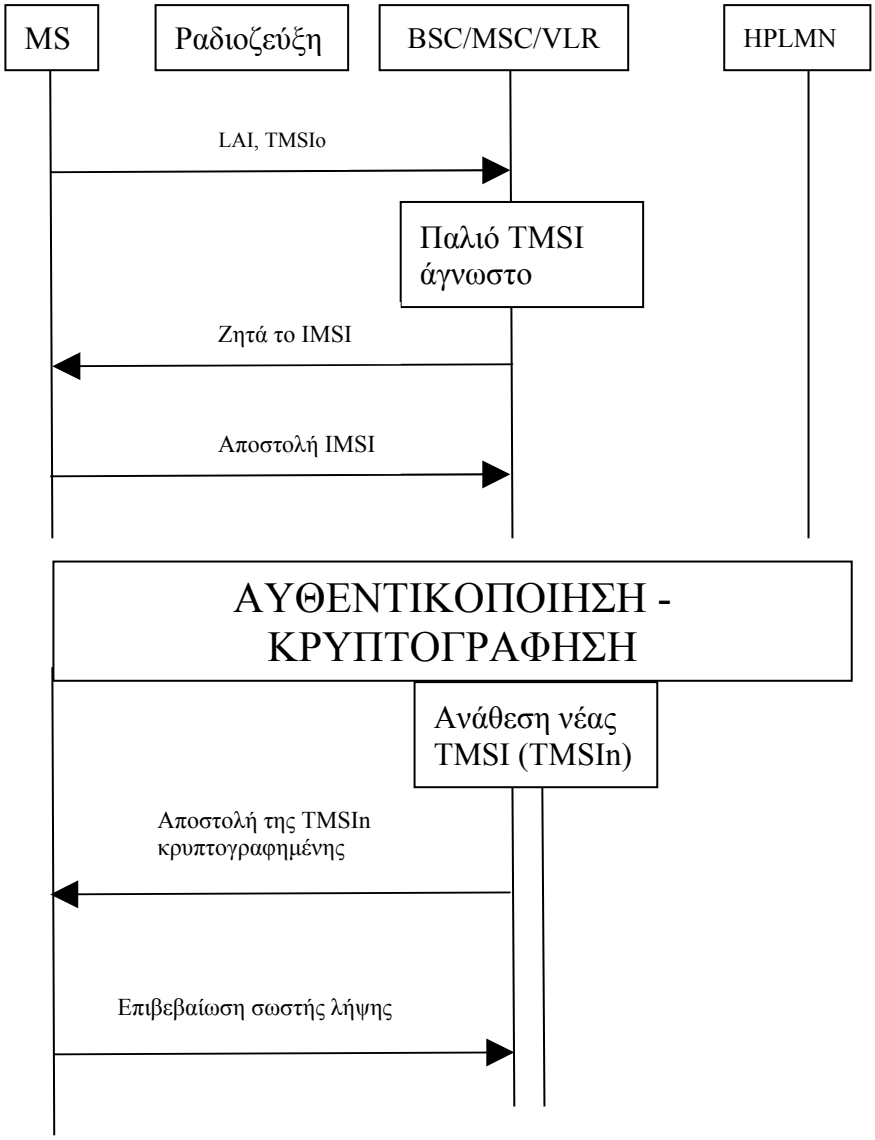
2)Σε περίπτωση που συμβεί μια απώλεια δεδομένων σε ένα VLR με αποτέλεσμα το MS να χρησιμοποιεί μια TMSI, που θα απορρίπτεται ως άγνωστη από αυτό το VLR. Τότε το συγκεκριμένο VLR θα στείλει το μήνυμα "IDENTITY REQUEST" στο MS και αυτό θα αποστείλει το καθαρό IMSI του, προκειμένου να αναγνωριστεί και να του ανατεθεί στη συνέχεια μια νέα TMSI σε κρυπτογραφημένο μήνυμα, αφού σταλούν και οι τριπλέτες ασφάλειας από το HPLMN στο VLR που εξυπηρετεί το MS (σχήμα 10).

3) Σε περίπτωση ανανέωσης της θέσης του MS σε νέο VLR (VLRn), ενώ το παλιό VLR (VLRo) έχει υποστεί απώλεια δεδομένων και δεν αναγνωρίζει το TMSIo. Και

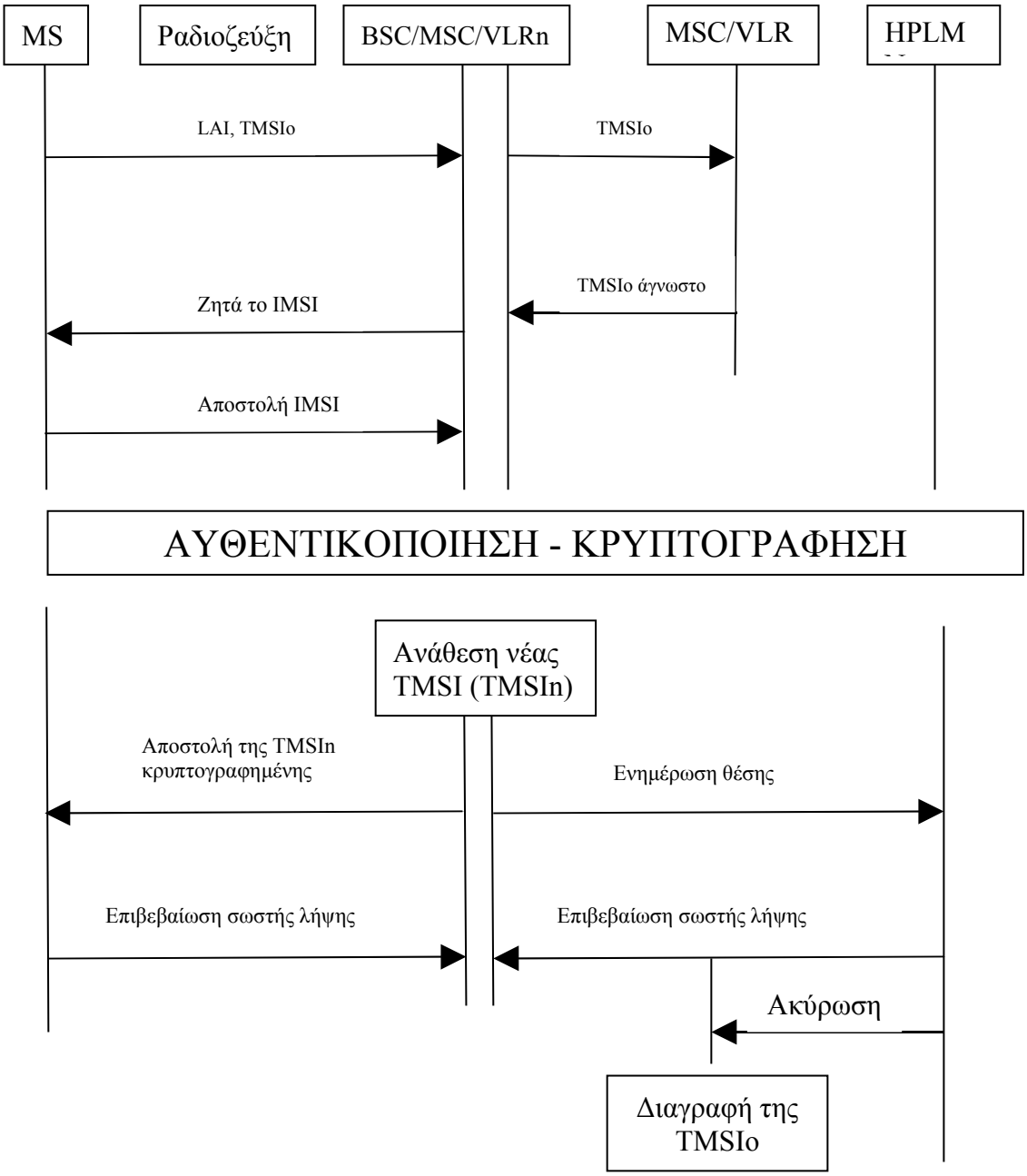
σε αυτήν την περίπτωση το VLRn ζητά από το MS να σταλεί το IMSI, για να του αποδοθεί μια νέα προσωρινή ταυτότητα (TMSIn) (σχήμα 11).



Σχήμα 9. Αποστολή IMSI όταν το παλιό MSC/VLR δεν είναι προσβάσιμο.



Σχήμα 10. Αποστολή IMSI λόγω άγνωστης TMSI στο τρέχον VLR



Σχήμα 11. Αποστολή IMSI. Άγνωστη TMSI στο VLR_o.

Αναφορικά με την διακύβευση της IMSI, αυτή μπορεί να πραγματοποιηθεί είτε με επιθέσεις κρυφακούσματος είτε με επιθέσεις προσωποίησης του δικτύου είτε με επιθέσεις ενδιάμεσου, όπως θα περιγραφεί στο σχετικό κεφάλαιο._

2.3.2 Ευπάθειες στους αλγόριθμους αυθεντικοποίησης (COMP128) και κρυπτογράφησης (A5)

Οι αλγόριθμοι που χρησιμοποιούνται στα δίκτυα GSM για την αυθεντικοποίηση του συνδρομητή (COMP128) αλλά και για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων και των σημάτων (A5) έχει αποδειχτεί ότι παρουσιάζουν ευάλωτα σημεία και μπορούν να αποτελέσουν στόχο επιθέσεων. Για το λόγο αυτό, έχουν υιοθετηθεί νεότερες και πιο ασφαλείς εκδόσεις, κυρίως όσον αφορά τον αλγόριθμο αυθεντικοποίησης. Οι ευπάθειες και τα είδη των επιθέσεων αυτών αναλύονται παρακάτω.

2.3.2.1 Ευπάθειες του αλγόριθμου COMP128

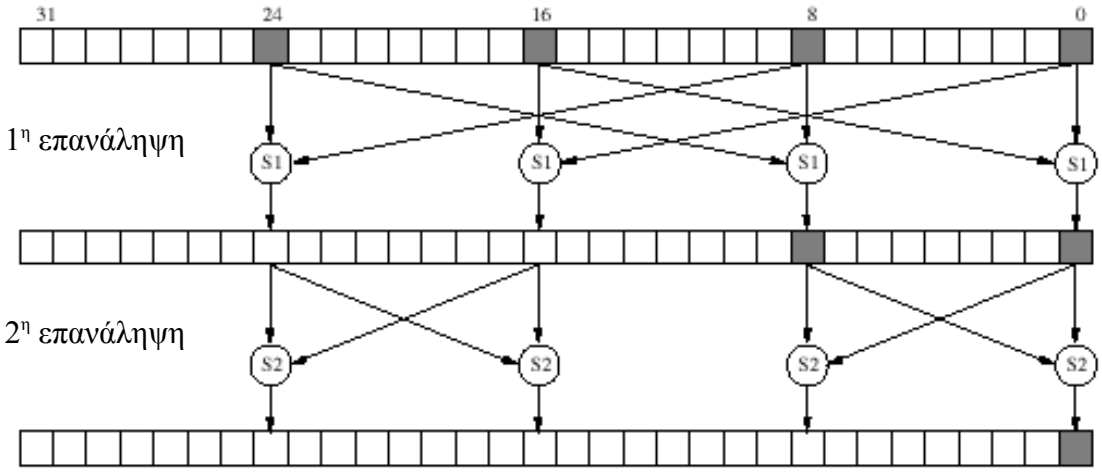
Ο αλγόριθμος COMP128 αν και ήταν – και παραμένει να είναι, τυπικά – μυστικός έχει "σπάσει" μετά την αποκάλυψη κάποιων απόρρητων εγγράφων και πληροφοριών καθώς και με τεχνικές αντίστροφης μηχανικής.

Τον Απρίλιο του 1998 οι Briceno, Goldberg και Wagner δημοσίευσαν μια επίθεση στον αλγόριθμο COMP128 με την οποία ήταν δυνατό να εξαχθεί το μυστικό κλειδί Ki. Έτσι, κατέστη δυνατή η κλωνοποίηση μιας κάρτας SIM και η χρησιμοποίηση της για να κάνει κάποιος κλήσεις χωρίς να χρεώνεται ο ίδιος ή να παρακολουθεί παράνομα τις κλήσεις του νόμιμου ιδιοκτήτη της SIM. Στη δημοσίευση αυτή εξηγείται ο τρόπος με τον οποίο γίνεται η επίθεση με φυσική πρόσβαση στην ίδια την κάρτα. Πρόκειται για μια επίθεση επιλεγμένου κειμένου (chosen-challenge attack ή chosen plaintext attack). Βασίζεται στην επιλογή ενός αριθμού από ειδικά επιλεγμένα RAND που στέλνονται το καθένα στην κάρτα SIM, η οποία υπολογίζει για το καθένα από αυτά το αντίστοιχο SRES. Αναλύοντας τα SRES, μπορεί να αποκαλυφθεί το μυστικό κλειδί. Η επίθεση απαιτεί, εκτός από την φυσική κατοχή της ίδιας της κάρτας, έναν αναγνώστη "έξυπνων" καρτών (smartcard reader) και έναν υπολογιστή. Πραγματοποιήθηκε χρησιμοποιώντας 150.000 RAND που στάλθηκαν στη SIM, μέσω του αναγνώστη, ο οποίος εκτελούσε 6,25 ερωτήματα το δευτερόλεπτο. Στη συνέχεια, έγινε ανάλυση των απαντήσεων και λίγοι επιπλέον

υπολογισμοί για να γίνει γνωστό το κλειδί Ki. Έτσι, η όλη επίθεση διήρκεσε περίπου 8 ώρες.

Η επίθεση όμως μπορεί να πραγματοποιηθεί και δια του αέρος, χωρίς φυσική πρόσβαση στην κάρτα. Για να συμβεί αυτό, ο επιτιθέμενος θα πρέπει να υλοποιήσει ένα ψεύτικο BTS, το σήμα του οποίου θα πρέπει να είναι ισχυρότερο από τα πλησιέστερα γνήσια BTS, έτσι ώστε να μπορέσει να εγκατασταθεί μια ραδιο-σύνδεση με τον κινητό σταθμό – στόχο. Στη συνέχεια, ο επιτιθέμενος επιλέγει RAND που, μέσω μηνυμάτων AUTHENTICATION REQUEST, στέλνονται στο MS, το οποίο υπολογίζει και αποστέλλει τα αντίστοιχα SRES. Η διαδικασία αυτή επαναλαμβάνεται πολλές φορές και συλλέγονται οι απαντήσεις μέχρι να συγκεντρωθούν πληροφορίες αρκετές για να γίνει γνωστό το Ki. Επειδή η επίθεση αυτή μπορεί να διαρκέσει μέχρι και 9 ώρες και λόγω του ότι η μπαταρία του MS προφανώς θα εξαντληθεί, η επίθεση μπορεί να πραγματοποιηθεί τμηματικά, σε διαφορετικές χρονικές περιόδους και πάλι μέχρι να μαζευτούν οι πληροφορίες που χρειάζονται.

Οι επιθέσεις αυτές εκμεταλλεύονται ένα αδύνατο σημείο του αλγόριθμου. Αυτό προέρχεται από το γεγονός ότι κατά τη $2^{η}$ επανάληψη εκτέλεσης του αλγόριθμου οι τιμές των bytes εξόδου στις θέσεις i, i+8, i+16, i+24 εξαρτώνται μόνο από τα αντίστοιχα bytes εισόδου. Αυτό το τρωτό σημείο ονομάστηκε "στενός σωλήνας" (Narrow Pipe) και απεικονίζεται στο σχήμα 12.



Σχήμα 12. "Narrow Pipe" στην εκτέλεση του COMP128. [14]

Οι επιθέσεις που εκμεταλλεύονται το συγκεκριμένο τρωτό σημείο ονομάζονται επιθέσεις σύγκρουσης (collision attacks). Λόγω του παράδοξου των γενεθλίων μπορεί να περιμένει κανείς μια σύγκρουση μετά από $2^{14,326}$ διαφορετικά RANDs, άρα μπορεί να «αποκομίσει» 2 bytes του κλειδιού μετά από 20.358 αποστολές RAND. Αφού το κλειδί έχει μήκος 16 bytes, η αποκάλυψη ολόκληρου του κλειδιού θα γίνει μετά από $8*2^{14,326}$=164.300 προσπάθειες. Παρόμοια, αλλά πιο πολύπλοκη επίθεση έχει γίνει από τον D. Kaljevic, μέσω μιας εφαρμογής (Sim Scan) που καταφέρει να πετύχει πιο γρήγορα αποτελέσματα. Συγκεκριμένα, έχει καταφέρει να εξάγει ολόκληρο το Ki σε χρόνο που αντιστοιχεί σε 18.000 RANDs μόνο, δηλαδή σε περίπου μία ώρα.

Επιπρόσθετα, πιο επικίνδυνες δείχνουν να είναι οι επιθέσεις "πλευρικού καναλιού" (side channel attacks) και ειδικότερα ένα συγκεκριμένο είδος αυτών των επιθέσεων, οι επιθέσεις "διαχωρισμού" (partition attacks) [9]. Οι επιθέσεις πλευρικού καναλιού είναι έμμεσες κρυπταναλυτικές επιθέσεις που μπορούν να προσδιορίσουν τη σχέση και την εξάρτηση μεταξύ των πληροφοριών εισόδου και εξόδου που διαρρέουν από τα πλευρικά κανάλια κατά τη διάρκεια υπολογισμών, όπως π.χ. οι χρόνοι εκτέλεσης των διαδικασιών, η κατανάλωση ρεύματος, οι εκπομπές ηλεκτρομαγνητικών κυμάτων κτλ. Σε έναν αλγόριθμο, προκειμένου αυτός να θεωρείται ανθεκτικός απέναντι σε τέτοιες επιθέσεις, θα πρέπει τα bits που παράγονται κατά τους ενδιάμεσους κύκλους επεξεργασίας και οι τιμές τους να είναι στατιστικά ανεξάρτητα από τα δεδομένα εισόδου, εξόδου και άλλες ευαίσθητες πληροφορίες, όπως π.χ. κλειδιά. Η τήρηση αυτής της βασικής αρχής είναι και ο μόνος τρόπος αποφυγής και εξουδετέρωσης αυτού του είδους των επιθέσεων. Αν ο αλγόριθμος έχει ανεπαρκή υλοποίηση, π.χ. για λόγους περιορισμού του κόστους του, μπορεί να παρουσιάζει κάποιες στατιστικές εξαρτήσεις που να τον καθιστούν επιρρεπή σε μερικές από αυτές τις επιθέσεις. Οι επιθέσεις "διαχωρισμού" συνιστούν μια κατηγορία αυτών των επιθέσεων, που ήρθαν στο φως από ερευνητές της IBM το Μάιο του 2002. Ουσιαστικά, πρόκειται για μια μέθοδο που προσπαθεί να εξάγει τις ευαίσθητες πληροφορίες από τη στατιστική εξάρτηση που παρατηρείται στα σήματα των πλευρικών καναλιών. Μπορούν να χρησιμοποιηθούν αποτελεσματικά για επίθεση σε υλοποιήσεις που εμπλέκουν αναζήτηση σε μεγάλους πίνακες ή και σε άλλους

αλγόριθμους, στους οποίους δεν έχουν εφαρμοστεί κατάλληλα αντίμετρα απέναντι σε μεθόδους διαφορικής ανάλυσης των πλευρικών καναλιών. Ο αλγόριθμος COMP128 που υλοποιείται στις κάρτες SIM των δικτύων GSM, και ο οποίος εφαρμόζει αναζήτηση σε μεγάλους πίνακες έχει αποδειχτεί ότι μπορεί να "σπάσει" με μια επίθεση διαχωρισμού, που περιλαμβάνει λιγότερες από 1000 εκτελέσεις του αλγόριθμου με τυχαίες εισόδους (random inputs), ή 255 επιλεγμένες εισόδους (chosen inputs), ή μόνο 8 προσαρμοστικά επιλεγμένες εισόδους (adaptively chosen inputs). Έτσι, το κλειδί Ki μπορεί να εξαχθεί μέσα σε 1 λεπτό. Γίνεται κατανοητό, ότι με αυτήν την επίθεση μπορεί κάποιος να κλωνοποιήσει μια SIM στην οποία χρειάζεται να έχει φυσική πρόσβαση λίγα μόνο δευτερόλεπτα. [15]

Από την ανάλυση που προηγήθηκε, οδηγείται κανείς στο συμπέρασμα ότι ο αλγόριθμος COMP128 παρουσιάζεται αρκετά πλέον ευάλωτος σε επιθέσεις που στόχο έχουν να αποκαλύψουν το μυστικό κλειδί Ki. Από εκεί και πέρα, είναι δυνατόν να κλωνοποιηθεί μια κάρτα SIM και να χρησιμοποιηθεί για επιθέσεις «κρυφακούσματος» κλήσεων, μηνυμάτων SMS και φωνητικού ταχυδρομείου, για την πραγματοποίηση κλήσεων με χρέωση του νόμιμου ιδιοκτήτη κτλ. Το σπάσιμο του αλγόριθμου ήρθε σαν φυσικό αποτέλεσμα της τακτικής που εφαρμόστηκε για την παροχή ασφάλειας στις τηλεπικοινωνίες μέσα από την απόκρυψη και τη μη δημοσιοποίηση στην επιστημονική κοινότητα του κώδικα του COMP128. Η επιτροπή GSM, μετά τη γνωστοποίηση των πρώτων επιτυχημένων επιθέσεων απάντησε ότι ο COMP128 αποτελεί απλώς ένα παράδειγμα αλγόριθμου αυθεντικοποίησης και ότι οι πάροχοι θα πρέπει να αρχίσουν να εφαρμόζουν νέους ασφαλέστερους αλγόριθμους. Επίσης, προχώρησε και στην έκδοση δύο νέων αλγορίθμων, τους COMP128-2 και COMP128-3, χωρίς και αυτούς να τους δημοσιοποιήσει. Σήμερα, έχει σχεδιαστεί και μια τέταρτη έκδοση, η COMP128-4, που βασίζεται σε ένα γνωστό δημοσιευμένο αλγόριθμο, τον AES, και χρησιμοποιείται στα δίκτυα 3G. Εξάλλου, για την αντιμετώπιση των επιθέσεων πλευρικού καναλιού, έχει προταθεί από την ερευνητική ομάδα της IBM, κατά την εκτέλεση του αλγόριθμου αυθεντικοποίησης, αντί να γίνεται αναζήτηση σε συγκεκριμένες θέσεις μεγάλων πινάκων, γεγονός που αποτελεί τον κύριο λόγο διαρροής πληροφοριών από πλευρικά κανάλια, να χρησιμοποιούνται μικρότεροι

επικουρικοί πίνακες και οι αναζητήσεις να γίνονται σε τυχαίες θέσεις αυτών των πινάκων. Με αυτόν τον τρόπο οι διαρρέουσες πληροφορίες πλευρικού καναλιού ουσιαστικά υποβαθμίζονται και καθίστανται άχρηστες για τον επιτιθέμενο. Επειδή αυτή η τεχνική χρησιμοποιεί λίγη RAM για κάθε επικουρικό πίνακα, μπορεί να εφαρμοστεί εύκολα σε συσκευές με περιορισμένη μνήμη, όπως τα κινητά τηλέφωνα, για προστασία από τις επιθέσεις πλευρικού καναλιού. Επίσης, και οι ίδιοι οι χρήστες θα πρέπει να μην αφήνουν τις κινητές συσκευές τους σε τρίτα άτομα ή αφύλακτες.

2.3.2.2 Ευπάθειες του αλγόριθμου A5

Ο αλγόριθμος A5 σχεδιάστηκε για την κρυπτογράφηση και αποκρυπτογράφηση μιας συνομιλίας για το σύστημα GSM. Ο αλγόριθμος αυτός έχει σπάσει και σήμερα υπάρχουν πολλές τεχνικές που μπορούν να εξάγουν το κλειδί Kc ακόμα και σε πραγματικό χρόνο. Οι τεχνικές αυτές εκμεταλλεύονται το γεγονός ότι τα 10 τελευταία bits του 64-bit κλειδιού Kc θέτονται "0" από τον αλγόριθμο. Αυτό πρακτικά σημαίνει ότι μπορεί κάποιος αποκτώντας το κλειδί να αποκρυπτογραφήσει και «κρυφακούσει» το περιεχόμενο μιας συνομιλίας. Αν, δηλαδή, κάποιος γνωρίζει το κλειδί Kc μπορεί να βρει την "ακολουθία κλειδιού" (key stream) που χρησιμοποιείται για την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων, αφού αυτή η ακολουθία παράγεται από το κλειδί συνόδου Kc και τον αριθμό του πλαισίου που κρυπτογραφείται. Πρακτικά, το Kc δεν αλλάζει κατά τη διάρκεια μιας κλήσης και μάλιστα μπορεί να χρησιμοποιείται το ίδιο για μέρες, ενώ οι αριθμοί πλαισίων αυξάνονται κατ' απόλυτη τιμή.

Η πιο απλή επίθεση κατά του A5 είναι μια εξαντλητική αναζήτηση (brute force attack) για την εξεύρεση του κλειδιού Kc. Η επίθεση μπορεί να πραγματοποιηθεί με έναν Pentium III στα 600 MHz. Σε αυτήν την περίπτωση, αφού τα 10 λιγότερο σημαντικά bits είναι μηδέν, μια εξαντλητική αναζήτηση στα 2^{54} πιθανά κλειδιά θα απαιτούσε 250 ώρες, με έναν επεξεργαστή. Η επίθεση όμως μπορεί να βελτιστοποιηθεί, αν σταματούσαμε να ελέγχουμε τις ακολουθίες στις οποίες βρεθεί το πρώτο λανθασμένο bit. Αυτό θα βελτίωνε το χρόνο εύρεσης κατά 1/3. Αν μάλιστα χρησιμοποιηθούν παράλληλοι επεξεργαστές, ο χρόνος μειώνεται δραστικά. Αν και

το «κρυφάκουσμα» μιας κλήσης σε πραγματικό χρόνο φαίνεται αρχικά αδύνατη, διότι απαιτείται κάποιος χρόνος για να γίνει κρυπτανάλυση του Kc, ο αντίπαλος μπορεί να καταγράψει τα δεδομένα που κρυφακούει και να τα αποκρυπτογραφήσει αργότερα, αφού εκτελέσει μια εξαντλητική αναζήτηση για να βρει το μυστικό κλειδί.

Ωστόσο, αρκετές μελέτες έδειξαν ότι υπάρχουν και άλλες μέθοδοι για το σπάσιμο του A5 σε μικρότερο χρόνο, πράγμα που μπορεί να κάνει το κρυφάκουσμα μιας κλήσης σε πραγματικό χρόνο πιο πιθανό. Η πιο γνωστή από αυτές (Divide-and-Conquer attack) του J. Golic, μπορεί να μειώσει την πολυπλοκότητα αναζήτησης στο $2^{40,16}$ χρησιμοποιώντας ένα γνωστό κείμενο (known plaintext) και προσπαθώντας να βρει την αρχική κατάσταση των τριών καταχωρητών ολίσθησης από μια γνωστή κλειδική ακολουθία. Επιπλέον, οι Alex Biryukov, Adi Shamir και David Wagner έχουν δημοσιεύσει δυο νέες κρυπταναλυτικές επιθέσεις στον A5/1 (την έκδοση του A5 για την Ευρώπη), στις οποίες εξάγεται το κλειδί Kc σε πραγματικό χρόνο με ένα απλό PC, από μια μικρή ποσότητα δεδομένων εξόδου [11]. Η πρώτη από αυτές τις επιθέσεις, που αναφέρεται ως "biased birthday attack", απαιτεί δύο λεπτά δεδομένων και ένα μόνο δευτερόλεπτο επεξεργασίας, ενώ η δεύτερη, γνωστή ως "Random Subgraph attack", απαιτεί δύο δευτερόλεπτα δεδομένων και αρκετά λεπτά για επεξεργασία. Υπάρχουν πολλές πιθανές εναλλακτικές σε αυτές τις επιθέσεις, που χειρίζονται διαφορετικές παραμέτρους. Τρεις από αυτές φαίνονται στο παρακάτω σχήμα.

Τύπος επίθεσης	**Βήματα προ-επεξεργασίας**	**Διαθέσιμα δεδομένα**	**Δίσκοι χωρητικότητας 73 GB**	**Χρόνος επίθεσης**
Biased Birthday Attack (1)	2^{42}	2 λεπτά	4	1 δ/λεπτο
Biased Birthday Attack (2)	2^{48}	2 λεπτά	2	1 δ/λεπτο
Random Subgraph Attack	2^{48}	2 δ/λεπτα	4	Μερικά λεπτά

Σχήμα 13. Επιθέσεις στον A5 [11]

Τόσο ο A5/1 όσο και ο A5/2, που είναι η ασθενέστερη και πιο ευάλωτη έκδοση του A5, θεωρούνται πλέον επισφαλείς, αφού είναι δυνατόν να σπάσουν μέσα σε λίγο

χρόνο. Μια πιο πρόσφατη έκδοση του αλγόριθμου, γνωστή ως A5/3, σχεδιάστηκε από την ομάδα Security Algorithms Group of Experts (SAGE) του Ευρωπαϊκού Ινστιτούτου Τηλεπικοινωνιακών Προτύπων (European Telecommunications Standards Institute, ETSI). Ο A5/3 βασίζεται στον αλγόριθμο KASUMI και χρησιμοποιείται στα δίκτυα 3ης γενιάς ως ο κύριος αλγόριθμος για την εμπιστευτικότητα και ακεραιότητα των δεδομένων κλήσης.

2.3.3 Μη πιστοποίηση του δικτύου στο χρήστη

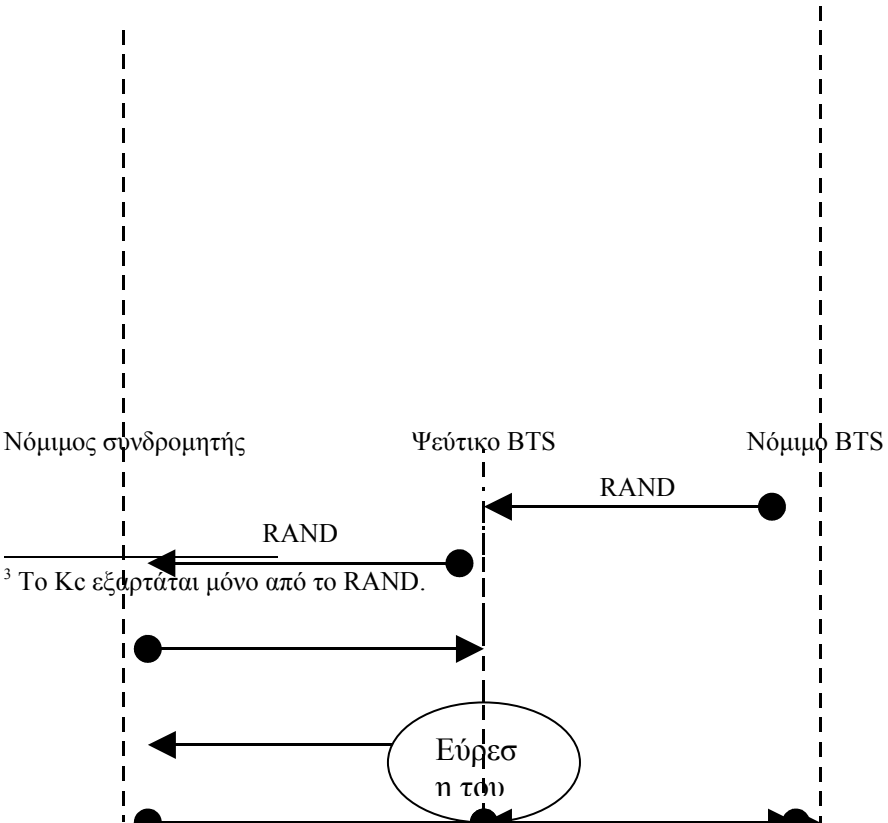
Το γεγονός ότι το δίκτυο δεν πιστοποιείται στο χρήστη είναι ίσως η σημαντικότερη ελαττωματικότητα του μηχανισμού αυθεντικοποίησης του δικτύου GSM. Ο μηχανισμός αυτός, όπως περιγράφτηκε, δεν απαιτεί από το δίκτυο να αποδείξει την αυθεντικότητά του στο συνδρομητή. Η μόνη απαίτηση είναι η αυθεντικοποίηση του συνδρομητή στο δίκτυο. Αυτό σημαίνει ότι μπορεί κάποιος δημιουργώντας έναν ψεύτικο σταθμό βάσης (false BTS) να παρεμβληθεί μεταξύ του συνδρομητή και του νόμιμου δικτύου, υλοποιώντας μια επίθεση γνωστή ως "man-in-the-middle attack". [10]. Αφού ο μηχανισμός αυθεντικοποίησης ενεργοποιείται κατά την κρίση του δικτύου, ένα ψεύτικος σταθμός βάσης μπορεί να στείλει το RAND στο χρήστη και να αγνοήσει την απάντηση. Μπορεί επίσης να μην ενεργοποιήσει το μηχανισμό για την κωδικοποίηση των δεδομένων. Ένας επιτιθέμενος θα πρέπει επίσης να θέσει τις παραμέτρους του σταθμού βάσης του τέτοιους ώστε να ενθαρρύνει τα θύματά του να συνδέονται με αυτόν για να επικοινωνήσουν με το δίκτυο και να πραγματοποιούν κλήσεις. Έτσι, οι κλήσεις ενός νόμιμου συνδρομητή ή ακόμα και τα σύντομα μηνύματα (SMS) θα υποκλέπτονται μέσω αυτής της επίθεσης. Μια τέτοια απειλή θεωρούνταν απίθανη την εποχή που σχεδιάζονταν τα μέτρα ασφάλειας για το δίκτυο GSM, διότι ο εξοπλισμός που απαιτείται για την πραγματοποίηση μιας τέτοιας επίθεσης ήταν τότε πολύ ακριβός και δυσεύρετος. Ωστόσο, σήμερα με τη γιγάντωση των δικτύων κινητής τηλεφωνίας – και φυσικά του GSM – η πρόσβαση σε τέτοιου είδους εξοπλισμού είναι πλέον σχετικά εύκολη και το κόστος χαμηλό, άρα και οι συγκεκριμένες επιθέσεις πολύ πιο πιθανές.

Μια παραλλαγή της επίθεσης "man-in-the-middle" που υλοποιείται με επίθεση στον A5/2 είναι η εξής:

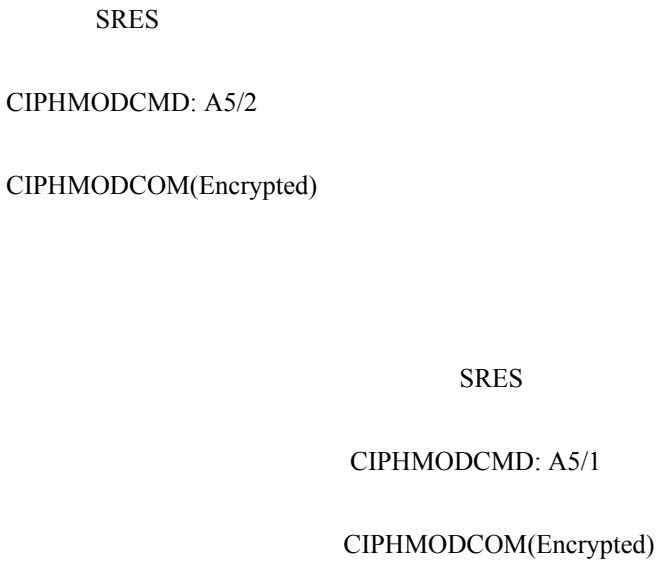
1. Όταν εκκινείται ο μηχανισμός αυθεντικοποίησης από το δίκτυο, το δίκτυο στέλνει στο επιτιθέμενο το RAND το οποίο αυτός προωθεί στο νόμιμο συνδρομητή.
2. Η νόμιμη SIM υπολογίζει το SRES και το στέλνει στο επιτιθέμενο, δηλαδή στο ψεύτικο BTS.
3. Ο επιτιθέμενος που δε γνωρίζει ακόμα το Kc, ζητά από το νόμιμο MS να αρχίσει κρυπτογράφηση χρησιμοποιώντας τον αλγόριθμο A5/2.
4. Το νόμιμο MS αρχίζει να κρυπτογραφεί χρησιμοποιώντας τον A5/2. Έτσι επιτρέπει στον επιτιθέμενο να πραγματοποιήσει την επίθεση που περιγράφηκε στην προηγούμενη παράγραφο για να εξάγει το μυστικό κλειδί Kc.
5. Ο επιτιθέμενος απαντάει στο νόμιμο BTS στέλνοντας του την απάντηση SRES που του είχε στείλει το νόμιμο MS.
6. Η επικοινωνία μεταξύ του χρήστη και του δικτύου μπορεί τώρα να ξεκινήσει, με τον επιτιθέμενο να "ακούει" στη ραδιοζεύξη.

Σημειώνεται ότι η επίθεση μπορεί να λειτουργήσει άσχετα με το ποιον αλγόριθμο κρυπτογράφησης χρησιμοποιεί το νόμιμο δίκτυο, αφού το Kc δεν εξαρτάται από αυτόν[3]. Η επίθεση απεικονίζεται σχηματικά στο σχήμα 14.

Σημειώνεται τέλος ότι η συγκεκριμένη ευπάθεια του GSM έχει διορθωθεί στο UMTS, όπου εκτός από το συνδρομητή και το δίκτυο πιστοποιεί την αυθεντικότητά του.



[3] Το Kc εξαρτάται μόνο από το RAND.



Σχήμα 14. Man-in-the-middle attack

2.3.4 Ασφάλεια της κάρτας SIM

Στην παράγραφο 2.3.2.1 έγινε αναφορά στις ευπάθειες του αλγόριθμου COMP128 και επισημάνθηκε ότι το "σπάσιμο" αυτού του αλγόριθμου καθιστά την κάρτα SIM του συνδρομητή ευάλωτη σε κλωνοποιήσεις. Τον ίδιο κίνδυνο διατρέχουν οι SIM και από τις επιθέσεις πλευρικού καναλιού, μέσω τον οποίων μπορεί να εξαχθεί το κλειδί αυθεντικοποίησης Ki. Η κλωνοποίηση μιας SIM συνεπάγεται όχι μόνο την υποκλοπή μιας συνομιλίας αλλά και την πραγματοποίηση κλήσεων με χρέωση του νόμιμου συνδρομητή. Η κλωνοποίηση μπορεί να γίνει με τη βοήθεια ενός αναγνώστη "έξυπνων" καρτών, στον οποίο τοποθετείται η κάρτα. Με τη χρήση λογισμικού, ο αλγόριθμος COMP128-1 "σπάζει", εξάγεται το IMSI και το κλειδί Ki., και στη συνέχεια, δημιουργείται το λογισμικό για την κάρτα-κλώνο, η οποία και προγραμματίζεται με κατάλληλη συσκευή. Σημειώνεται ότι ο εξοπλισμός και τα λογισμικά που απαιτούνται σε αυτήν την περίπτωση είναι εύκολα προσβάσιμα στο διαδίκτυο. [15]

Ωστόσο, ένας άλλος κίνδυνος προέρχεται από επιθέσεις που βασίζονται στην "εισαγωγή οπτικών σφαλμάτων" [17]. Σχετικές έρευνες έχουν δείξει ότι η λειτουργία του μικροεπεξεργαστή της SIM μπορεί να διακοπεί, εκθέτοντάς την στο φως μιας ηλεκτρονικής κάμερας. Στη συνέχεια, με τη χρήση ενός μικροσκοπίου κατέστη δυνατή η εξαγωγή μυστικών πληροφοριών, όπως η ταυτότητα IMSI και το κλειδί Ki. Σύμφωνα με την έρευνα, ο φωτισμός ενός τρανζίστορ το κάνει να συμπεριφέρεται σαν αγωγός και να εισάγει ένα προσωρινό σφάλμα. Μάλιστα, τέτοιες επιθέσεις είναι σχετικά εύκολες και δεν απαιτούν ακριβό εξοπλισμό. Στο πρώτο στάδιο, το κύκλωμα της κάρτας εκτίθεται στο φως, αφού πρώτα αφαιρεθεί η προστατευτική επικάλυψη του μικροεπεξεργαστή που υπάρχει σε κάθε έξυπνη κάρτα. Το φως επικεντρώθηκε προσεκτικά σε συγκεκριμένα τρανζίστορ του τσιπ, διοχετεύοντας το μέσα από ένα μικροσκόπιο. Αλλάζοντας σειριακά τις τιμές των τρανζίστορ που χρησιμοποιούνται για την αποθήκευση των δεδομένων, οι ερευνητές κατόρθωσαν με μεθόδους αντίστροφης μηχανικής (reverse engineering) να εξάγουν τον πίνακα διευθύνσεων της μνήμης, και στη συνέχεια, τα ευαίσθητα δεδομένα της κάρτας. Σύμφωνα με τους ερευνητές και εφευρέτες αυτής της επίθεσης, αναπτύχθηκε μια τεχνολογία για την αποτροπή αυτών των επιθέσεων.

2.3.5 Μη κρυπτογράφηση της ζεύξης BTS - BSC

Σύμφωνα με τον αρχιτεκτονικό σχεδιασμό του GSM, η μετάδοση δεδομένων κρυπτογραφείται μόνο μεταξύ του κινητού του συνδρομητή και του σταθμού βάσης. Από εκεί και πέρα, η επικοινωνία μεταξύ του BTS και του BSC, η οποία συνήθως είναι μια μικροκυματική ζεύξη, δεν κρυπτογραφείται και τα δεδομένα του χρήστη και σηματοδοσίας μεταδίδονται όπως είναι (plain text). Αυτό σημαίνει ότι η συγκεκριμένη ζεύξη δεν παρέχει ασφάλεια και μπορεί κάποιος, αν έχει πρόσβαση στο δίκτυο, να ακούει σε κάθε τι που μεταδίδεται, δηλαδή των δεδομένων της κλήσης, τα στοιχεία RAND και SRES, καθώς και το κλειδί συνόδου Kc. Αξίζει να σημειωθεί ότι η ζεύξη μεταξύ MSC/VLR - BSC – BTS στην οποία μεταφέρεται το κλειδί συνόδου Kc για να φτάσει στο σταθμό βάσης και να ξεκινήσει η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης μεταξύ αυτού και του MS, δεν προστατεύεται με κάποιο μηχανισμό κρυπτογράφησης, δηλαδή το Kc μεταφέρεται

σαν "καθαρό" κείμενο μέχρι το σταθμό βάσης. Το ίδιο συμβαίνει και για τις ζεύξεις από το BSC στο MSC, που μπορεί να είναι είτε μικροκυματικές είτε σταθερές, και οι οποίες δεν χρησιμοποιούν μηχανισμούς κρυπτογράφησης κατά τη μετάδοση δεδομένων και σημάτων. Το γεγονός αυτό συνιστά ένα σαφές μειονέκτημα στο σύστημα ασφάλειας του GSM. Στα κυψελωτά δίκτυα 3ης γενιάς η κρυπτογράφηση επεκτείνεται μέχρι το RNC (Radio Network Controller), που είναι το αντίστοιχο του BSC στο GSM, και επομένως η συγκεκριμένη μικροκυματική ζεύξη προστατεύεται.

2.3.6 Επανειλημμένη χρήση ενός σετ τριπλετών ασφαλείας

Όπως έχει αναφερθεί, οι τριπλέτες ασφαλείας που χρησιμοποιούνται στο σύστημα GSM για την αυθεντικοποίηση ενός νόμιμου συνδρομητή εμπεριέχουν τις τιμές RAND, SRES και το κλειδί συνόδου Kc, τα οποία είναι αποθηκευμένα στο VLR στο οποίο περιάγεται ο χρήστης καθώς και στο HLR του οικείου PLMN του χρήστη. Όταν ένα VLR έχει χρησιμοποιήσει ένα σετ τριπλετών για να πιστοποιήσει ένα χρήστη θα πρέπει να το διαγράψει ή να το σημειώσει ως χρησιμοποιημένο, έτσι ώστε στην επόμενη αυθεντικοποίηση να κάνει χρήση ενός νέου αχρησιμοποίητου σετ τριπλετών [7]. Ωστόσο, στην τεκμηρίωση των μηχανισμών ασφάλειας του GSM, δεν απαγορεύεται ρητά η επαναχρησιμοποίηση τριπλετών. Για την ακρίβεια, αν το VLR δεν μπορέσει να βρει ένα νέο σετ, τότε νομιμοποιείται να χρησιμοποιήσει ξανά ένα παλιό σετ τριπλετών. Αυτό θα συμβεί στις περιπτώσεις που :

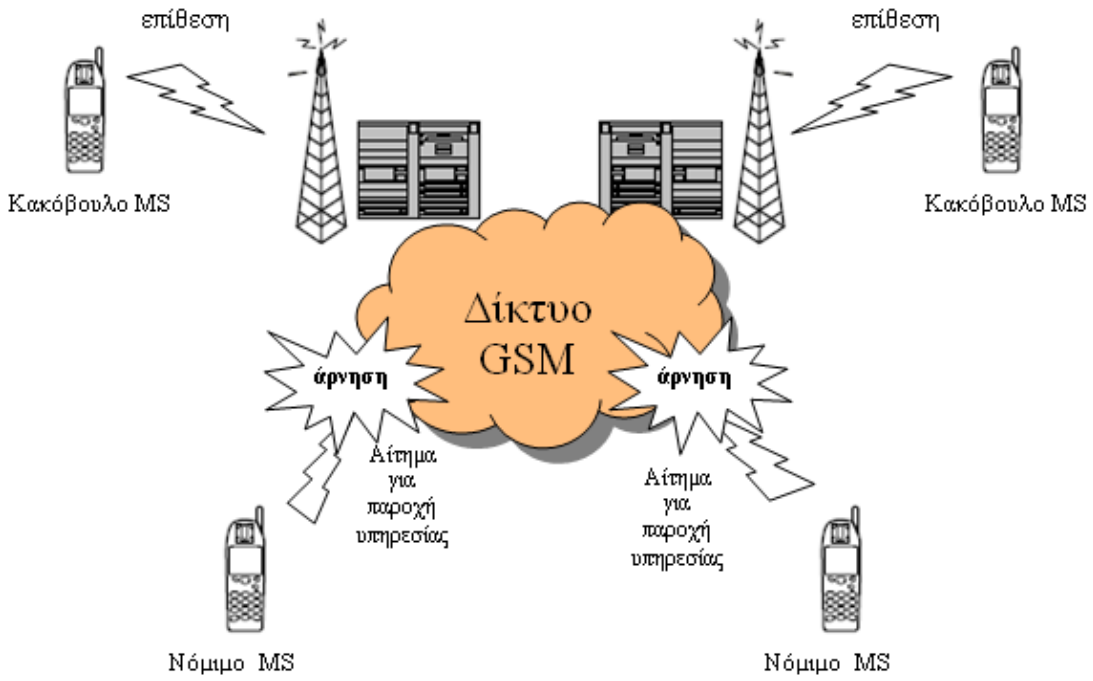
- το VLR δεν καταφέρει να συνδεθεί με το HLR,
- το HLR επιστρέψει μια θετική βεβαίωση λήψης (acknowledgement) που δεν περιέχει σετ τριπλετών,
- το HLR επιστρέψει ένα μήνυμα σφάλματος που να σχετίζεται είτε με αποτυχία του συστήματος είτε με λανθασμένη διατύπωση του αιτήματος που παρέλαβε.

Αν, βέβαια, το HLR κάνει γνωστό στο VLR ότι ο συνδρομητής είναι άγνωστος ή έχει αποκλειστεί, το VLR δεν πρέπει να προχωρήσει σε επαναχρησημοποίηση παλαιών σετ. Το πόσες φορές μπορεί να γίνει χρήση ενός σετ τριπλετών καθορίζεται από τον λειτουργό του δικτύου, έτσι ώστε να περιοριστεί η χρήση τους. Επίσης, και το HLR όταν δεν έχει νέα σετ τριπλετών μπορεί να αποστείλει στο VLR

ένα χρησιμοποιημένο σετ, όπου και πάλι καθορίζεται ο μέγιστος αριθμός των περιστάσεων που το HLR μπορεί να επαναποστείλει αυτό το σετ. Σε κάθε περίπτωση πάντως, το γεγονός αυτό εγκυμονεί κινδύνους, καθώς αν κάποιος, ο οποίος χρησιμοποιεί ένα ψεύτικο σταθμό βάσης, καταφέρει να υποκλέψει ένα σετ τριπλετών, με δεδομένο ότι στην τριπλέτα υπάρχει και το μυστικό κλειδί Kc, μπορεί να το χρησιμοποιήσει για να καταλάβει τη ραδιοζεύξη και να αποκρυπτογραφεί τα δεδομένα επικοινωνίας του νόμιμου συνδρομητή. Για το λόγο αυτό, η επαναχρησιμοποίηση τριπλετών θα πρέπει να αποφεύγεται και η αυθεντικοποίηση να γίνεται με νέα τριπλέτα, ενώ αν αυτό δεν είναι δυνατόν να καθίσταται αδύνατη η σύνδεση στο δίκτυο και η πραγματοποίηση κλήσεων.

2.3.7 Λοιπές αδυναμίες και ευπάθειες

Άλλη μια απειλή για το GSM προέρχεται από το γεγονός ότι πριν από την αυθεντικοποίηση ενός συνδρομητή προηγείται μια προκαταρκτική συνομιλία μεταξύ MS – BTS – BSC, για τη δέσμευση καναλιών επικοινωνίας. Ωστόσο, το δίκτυο δε μπορεί να γνωρίζει αν το MS που ζητά κανάλι είναι νόμιμος συνδρομητής ή όχι. Πιο συγκεκριμένα, ένα MS μεταβιβάζει ένα αίτημα “CHANNEL REQUEST” στο BTS και αυτό ενημερώνει το BSC, το οποίο πληροφορεί το BTS για τον τύπο και τον αριθμό του καναλιού που πρέπει να δεσμευτεί για το σκοπό αυτό. Κατόπιν, το BTS ενημερώνει το MS για το κανάλι που δεσμεύτηκε. Το αίτημα αυτό κατατίθεται πριν ξεκινήσει η διαδικασία αυθεντικοποίησης. Είναι δυνατόν ένα MS να περιέχει ειδικό λογισμικό που να πραγματοποιεί συνεχώς αιτήματα για δέσμευση καναλιών σηματοδοσίας, και, αφού το πλήθος των καναλιών είναι περιορισμένο, να προκληθεί συμφόρηση στο δίκτυο. Οι επιθέσεις αυτές είναι ευρέως γνωστές ως επιθέσεις “Denial-of-Service” (DoS) και έχουν ως αποτέλεσμα να μην ικανοποιούνται αιτήματα που προέρχονται από νόμιμους συνδρομητές. Αν και τέτοιες επιθέσεις καταγράφονται με τη χρήση σαρωτών, μετρητών και άλλων ειδοποιήσεων ασφαλείας, η δυσκολία έγκειται στον εντοπισμό της ακριβούς θέσης του κακόβουλου MS και την εξουδετέρωση των αντίστοιχων αιτημάτων. Η επίθεση απεικονίζεται στο σχήμα 15.



Σχήμα 15. Επίθεση "Denial-of-Service" σε ένα δίκτυο GSM. [18]

Η υπηρεσία σύντομων μηνυμάτων (Short Message Service, SMS) υλοποιείται σε όλα τα δίκτυα GSM και επιτρέπει στους συνδρομητές να στέλνουν και να δέχονται γραπτά μηνύματα. Ωστόσο, το δίκτυο GSM δεν προσφέρει κάποιο μηχανισμό ασφάλειας για την υπηρεσία αυτή. Στην πραγματικότητα, όλα τα μηνύματα μέσω SMS στέλνονται σε 'καθαρή' μορφή κειμένου χωρίς κρυπτογράφηση. Επιπλέον, η διεύθυνση του αποστολέα ενός SMS μπορεί εύκολα να πλαστογραφηθεί. Αυτή η αδυναμία μπορεί να επιτρέψει σε κάποιον να στέλνει μηνύματα με κακόβουλο περιεχόμενο προσποιούμενος μια ιδιότητα, π.χ. να ζητά από τον παραλήπτη, εκ μέρους μιας τράπεζας, να αποστείλει ευαίσθητες προσωπικές πληροφορίες ή να δεχτεί ένα συνημμένο αρχείο. Για τους λόγους αυτούς, οι χρήστες κινητών τηλεφώνων θα πρέπει να είναι πολύ προσεκτικοί σε μηνύματα με αμφιλεγόμενη ή ασυνήθιστη διεύθυνση αποστολέα. [19] [20]

Επιπρόσθετα, ο συνδρομητής ενός δικτύου GSM δεν έχει γνώση των μηχανισμών της ασφάλειας που του παρέχονται μια δεδομένη χρονική στιγμή (lack of visibility) [21]. Για παράδειγμα, δεν έχει καμία ένδειξη για το αν εφαρμόζεται κάποιος μηχανισμός κρυπτογράφησης κατά τη διάρκεια των κλήσεών του. Επίσης, το οικείο

δίκτυο ενός χρήστη δεν έχει γνώση για την ορθή εφαρμογή του μηχανισμού αυθεντικοποίησης κατά την περιαγωγή του συνδρομητή σε άλλα δίκτυα κινητής. Το γεγονός αυτό έχει ληφθεί υπόψη στο UMTS και έχει εν μέρει διορθωθεί.

Τέλος, κατά το σχεδιασμό της αρχιτεκτονικής του GSM δεν λήφθηκε υπόψη η περίπτωση της 'νόμιμης υποκλοπής' (Lawful Interception, LI) και δεν αναπτύχθηκε κάποιο πλαίσιο μηχανισμών που θα την επέτρεπαν. Ως νόμιμη υποκλοπή καλείται η παρακολούθηση κλήσεων και άλλων τηλεπικοινωνιακών δεδομένων χρηστών εκ μέρους της Υπηρεσίας Επιβολής του Νόμου (Law Enforcement Agency, LAE) κάθε κράτους. Αντίθετα, στο UMTS υπάρχει πρόβλεψη για περιπτώσεις νόμιμων υποκλοπών, οπότε είναι δυνατή η πιο έγκαιρη καταγραφή καταστάσεων που διακυβεύουν την σωστή και ασφαλή λειτουργία του δικτύου.

2.4 Συμπεράσματα

Το GSM σχεδιάστηκε πρωταρχικά για να είναι τόσο ασφαλές όσο τουλάχιστον τα σταθερά τηλεφωνικά δίκτυα, με τα οποία θα συνδεόταν. Η υιοθέτηση και χρησιμοποίηση προχωρημένων – σε σχέση με τα δίκτυα 1ης γενιάς – τεχνικών κρυπτογράφησης ήταν ένα από τα σημαντικότερα πλεονεκτήματα των κυψελωτών δικτύων 2ης γενιάς. Ωστόσο, με την πάροδο των χρόνων και την αλματώδη ανάπτυξη του GSM (και των άλλων δικτύων 2ης γενιάς) έγιναν φανερές οι ευπάθειες των μηχανισμών ασφαλείας και τα προβλήματα που θα προέκυπταν από πιθανές επιθέσεις που θα τις εκμεταλλεύονταν. Έτσι, για παράδειγμα, οι επιθέσεις με ψεύτικο σταθμό βάσης αποδείχθηκε ότι είναι ικανές να υποβαθμίσουν την ασφαλή διενέργεια κλήσεων μεταξύ νόμιμων συνδρομητών. Μάλιστα, μερικά από τα προβλήματα στους μηχανισμούς ασφαλείας σκόπιμα δεν λύθηκαν, καθώς εκτιμήθηκε ότι το κόστος για την αντιμετώπιση και επίλυσή τους θα ήταν πολλαπλάσιο από το κόστος των παραγόμενων κινδύνων. Είναι, πάντως δεδομένο ότι τα περισσότερα προβλήματα των μηχανισμών ασφαλείας προέρχονται από το γεγονός ότι η υλοποίηση των περισσότερων σημείων της αρχιτεκτονικής του GSM βασίστηκαν στην μυστικότητα (security through obscurity) και στη μη δημοσίευσή τους στην επιστημονική κοινότητα, με αποτέλεσμα να μην κριθούν έγκαιρα από

αυτήν και να αποκαλυφθούν κάποια στιγμή. Σε γενικές γραμμές, η ασφάλεια που παρέχεται από το σύστημα GSM κρίνεται ικανοποιητική τόσο για τον συνδρομητή όσο και για το δίκτυο, με την προϋπόθεση της απαρέγκλιτης τήρησης των κανόνων και μηχανισμών και της απαγόρευσης της υποβάθμισης τους (π.χ. υποβάθμιση της κρυπτογράφησης με τη χρήση πιο αδύναμων μηχανισμών όπως ο A5/2). Θα πρέπει ωστόσο να επανεξεταστούν και να κριθούν με τα νέα δεδομένα της εποχής, προκειμένου να αποφευχθούν όσο το δυνατό περισσότερο οι τηλεπικοινωνιακές απάτες.

1 ΚΕΦΑΛΑΙΟ 3

ΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ UMTS

3.1 Στόχοι των μηχανισμών ασφάλειας

Οι αντικειμενικοί στόχοι και οι αρχές που διέπουν τους μηχανισμούς ασφάλειας στο UMTS συγκεκριμενοποιούνται στο [22]. Βασική γραμμή των στόχων αυτών είναι να διασφαλίσουν ότι τα δεδομένα και οι πληροφορίες που προέρχονται από ή σχετίζονται με το χρήστη, καθώς και οι υπηρεσίες που παρέχονται στο χρήστη από το δίκτυο είναι προστατευμένα από κακόβουλη χρήση τρίτων. Επίσης, κύριος στόχος αυτών των μηχανισμών ασφάλειας είναι η παροχή ασφάλειας στις συναλλαγές μεταξύ των στοιχείων που αποτελούν το δίκτυο σε επίπεδο υψηλότερο από το επίπεδο ασφάλειας που καθορίστηκε από τα προηγούμενα δίκτυα κινητών υπηρεσιών (GSM). Τέλος, οι μηχανισμοί ασφάλειας θα πρέπει να είναι προτυποποιημένοι, έτσι ώστε να είναι συμβατοί και να εφαρμόζονται μεταξύ διαφορετικών δικτύων υπηρεσιών παγκοσμίως. Με βάση τους στόχους αυτούς, οι μηχανισμοί ασφάλειας που υιοθετήθηκαν για τα δίκτυα τρίτης γενιάς βασίζονται στους αντίστοιχους μηχανισμούς που βρίσκουν εφαρμογή στα δίκτυα προηγούμενων γενεών (2G/GSM), αλλά επεκτάθηκαν και δημιουργήθηκαν νέοι με σκοπό να καλύψουν τις αδυναμίες και τα κενά ασφάλειας που παρουσιάστηκαν σε αυτά. Τα σημαντικότερα μειονεκτήματα σε ότι αφορά την ασφάλεια στο GSM και σε άλλα δίκτυα δεύτερης γενιάς είναι:

- Η αδυναμία να παρεμποδιστούν σκόπιμες επιθέσεις εναντίον του δικτύου από τρίτο πρόσωπο που, διαθέτοντας τα κατάλληλα μέσα, μπορεί να προσποιηθεί είτε ότι φέρει την ιδιότητα ενός νόμιμου χρήστη είτε ότι αποτελεί στοιχείο του δικτύου. Οι επιθέσεις αυτές είναι γνωστές ως επιθέσεις ψεύτικου σταθμού βάσης (false base station attacks).

- Η μη χρήση κρυπτογράφησης κατά την αποστολή ευαίσθητων δεδομένων ελέγχου (π.χ. κλειδιών), που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων της ραδιοζεύξης, όταν αυτή γίνεται μεταξύ διαφορετικών δικτύων.
- Η μη δημοσιοποίηση των αλγόριθμων κρυπτογράφησης που χρησιμοποιούνται στα δίκτυα αυτά, γεγονός που τους καθιστά μη διαθέσιμους για περαιτέρω έρευνα και ανάλυση των χαρακτηριστικών και των αδυναμιών τους από τη διεθνή επιστημονική κοινότητα.
- Η ανυπαρξία μηχανισμών που να εξασφαλίζουν την ακεραιότητα των δεδομένων που ανταλλάσσονται (data integrity), δηλαδή την αποτροπή της παραποίησής τους από μη εξουσιοδοτημένους χρήστες.

Θα πρέπει να επισημανθεί ότι οι μηχανισμοί ασφάλειας που εφαρμόστηκαν στα GSM συστήματα κάλυπταν σε μεγάλο βαθμό τις απαιτήσεις για ασφάλεια των δημιουργών τους αλλά και των χρηστών κατά τα πρώτα στάδια υιοθέτησης αυτής της τεχνολογίας. Για το λόγο αυτό χρησιμοποιήθηκαν ως βάση για την ανάπτυξη των αντίστοιχων μηχανισμών στα δίκτυα τρίτης γενιάς. Ωστόσο, η ραγδαία εξέλιξη της τεχνολογίας με την πάροδο των χρόνων είχε συμβολή και στην χρησιμοποίηση πιο εξελιγμένων τεχνικών και εξοπλισμού για την προσβολή των συστημάτων κινητής τηλεφωνίας και την διεξαγωγή πιο αποτελεσματικών επιθέσεων εναντίον τους. Έτσι, κρίθηκε αναγκαία η βελτίωση της ασφάλειας στα νέα δίκτυα τρίτης γενιάς που δημιουργήθηκαν. Τα χαρακτηριστικά των μηχανισμών ασφάλειας στα συστήματα 3G που συνθέτουν την αρχιτεκτονική του UMTS ομαδοποιούνται σε πέντε κύριες κατηγορίες [22] :

1. **Ασφάλεια του δικτύου πρόσβασης (Network access security)**: τα χαρακτηριστικά που εξασφαλίζουν στους χρήστες ασφαλή πρόσβαση στις υπηρεσίες του δικτύου και προστασία από επιθέσεις στα μέσα (ραδιο-συνδέσεις) του δικτύου.
2. **Ασφάλεια της περιοχής δικτύου (Network domain security)**: τα χαρακτηριστικά που καθιστούν ασφαλή την ανταλλαγή πληροφοριών μεταξύ των κόμβων του κυρίως δικτύου.

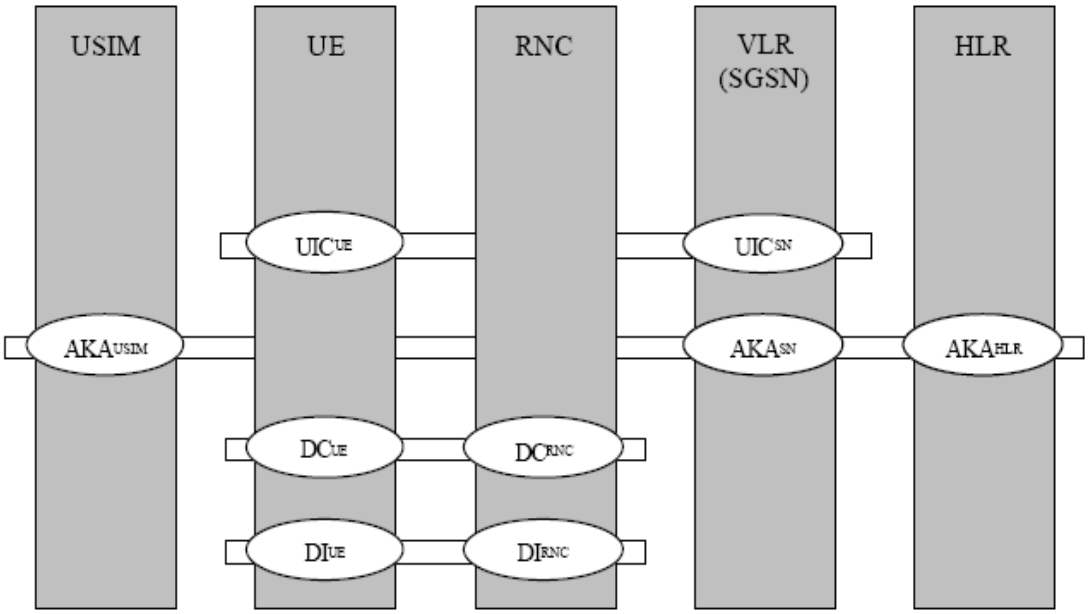
3. **Ασφάλεια της περιοχής χρήστη (User domain security):** τα χαρακτηριστικά που διασφαλίζουν την πρόσβαση στις κινητές συσκευές από το χρήστη.
4. **Ασφάλεια της περιοχής εφαρμογών (Application domain security):** τα χαρακτηριστικά που εξασφαλίζουν την ασφαλή ανταλλαγή δεδομένων μεταξύ χρήστη και παρόχου σε επίπεδο εφαρμογών.
5. **Διαφάνεια και διαμόρφωση της ασφάλειας (Visibility and configurability of the security):** τα χαρακτηριστικά που δίνουν τη δυνατότητα στο χρήστη να γνωρίζει αν ένας μηχανισμός ασφάλειας είναι σε λειτουργία και αν συγκεκριμένες υπηρεσίες εξαρτώνται από αυτόν.

Οι παραπάνω «ομάδες» μηχανισμών ικανοποιούν κάποιες απαιτήσεις που είχαν τεθεί εξ αρχής και που ίσχυαν και σε προγενέστερα δίκτυα. Οι απαιτήσεις αυτές σχετίζονται με την εξασφάλιση κάποιων εγγυήσεων, όπως η αυθεντικοποίση του χρήστη στο σύστημα, η εμπιστευτικότητα ή ιδιωτικότητα των ευαίσθητων δεδομένων, η διαθεσιμότητα και η αξιοπιστία του δικτύου, η ακεραιότητα των δεδομένων του χρήστη αλλά και των δεδομένων σηματοδοσίας, καθώς και η κρυπτογράφησή τους. Συγκεκριμένα:

- Η **αυθεντικοποίηση** (authentication) του χρήστη είναι η ιδιότητα που έχει το δίκτυο να πιστοποιεί την ταυτότητα κάθε συνδρομητή. Στο UMTS, εισάγεται ένας επιπλέον μηχανισμός, αυτός της αυθεντικοποίησης του ίδιου του δικτύου στον χρήστη, κάτι που δεν υπήρχε στους μηχανισμούς ασφάλειας στο GSM, όπου ο συνδρομητής δεν είχε τη δυνατότητα να εξακριβώσει τη νομιμότητα του δικτύου στο οποίο συνδέεται.
- Η **εμπιστευτικότητα** (confidentiality) των δεδομένων είναι η ιδιότητα που εξασφαλίζει ότι τα δεδομένα ενός νόμιμου συνδρομητή δεν έχουν γίνει διαθέσιμα σε μη εξουσιοδοτημένα άτομα.
- Η **ακεραιότητα** (integrity) των δεδομένων είναι η ιδιότητα που εξασφαλίζει ότι τα δεδομένα ενός νόμιμου συνδρομητή δεν έχουν παραποιηθεί από μη εξουσιοδοτημένα άτομα.

Στο Σχήμα 16 απεικονίζονται οι τέσσερις κυριότεροι μηχανισμοί ασφάλειας που διέπουν τη λειτουργία του δικτύου UMTS, καθώς και ποια τμήματα του δικτύου εμπλέκονται σε κάθε έναν μηχανισμό. Οι μηχανισμοί αυτοί είναι :

1. **Εμπιστευτικότητα ταυτότητας χρήστη** (User Identification Confidentiality). Υλοποιείται μεταξύ UE και VLR (ή SGSN), με τη χρήση προσωρινών ταυτοτήτων.
2. **Αυθεντικοποίηση και συμφωνία κλειδιού**(Authentication and Key Agreement). Υλοποιείται μεταξύ USIM, VLR/SGSN και HLR. Είναι ο μηχανισμός αμοιβαίας αυθεντικοποίησης μεταξύ του χρήστη – μέσω της USIM – και του δικτύου που τον εξυπηρετεί (Serving Netowork, SN). Κατά τη διαδικασία αυτή παράγονται τα κλειδιά που θα παρέχουν εμπιστευτικότητα και ακεραιότητα στα δεδομένα που θα ανταλλάξουν αργότερα ο χρήστης και το δίκτυο πρόσβασης (access network).
3. **Εμπιστευτικότητα δεδομένων** (Data Confidentiality). Υλοποιείται μεταξύ UE και RNC, δηλαδή μεταξύ του χρήστη και του δικτύου πρόσβασης. Ο μηχανισμός αυτός αφορά τόσο τα δεδομένα του χρήστη (user data) όσο και τα δεδομένα σηματοδοσίας (signalling data). Το κρυπτογραφικό κλειδί που χρησιμοποιείται παράγεται κατά την διαδικασία της αυθεντικοποίησης.



AKA: Authentication and Key Agreement

UIC: User Identification Confidentiality
DC: Data Confidentiality
DI: Data Integrity

Σχήμα 16. Οι κυριότεροι μηχανισμοί ασφάλειας στο UMTS [23]

4. **Ακεραιότητα δεδομένων** (Data Integrity). Υλοποιείται μεταξύ UE και RNC. Ο μηχανισμός αυτός αφορά μόνο στα δεδομένα σηματοδοσίας και όχι στα δεδομένα του χρήστη. Το κλειδί που χρησιμοποιείται εδώ, παράγεται επίσης κατά τη διαδικασία της αυθεντικοποίησης.

3.2 Παρουσίαση και ανάλυση των μηχανισμών ασφαλείας

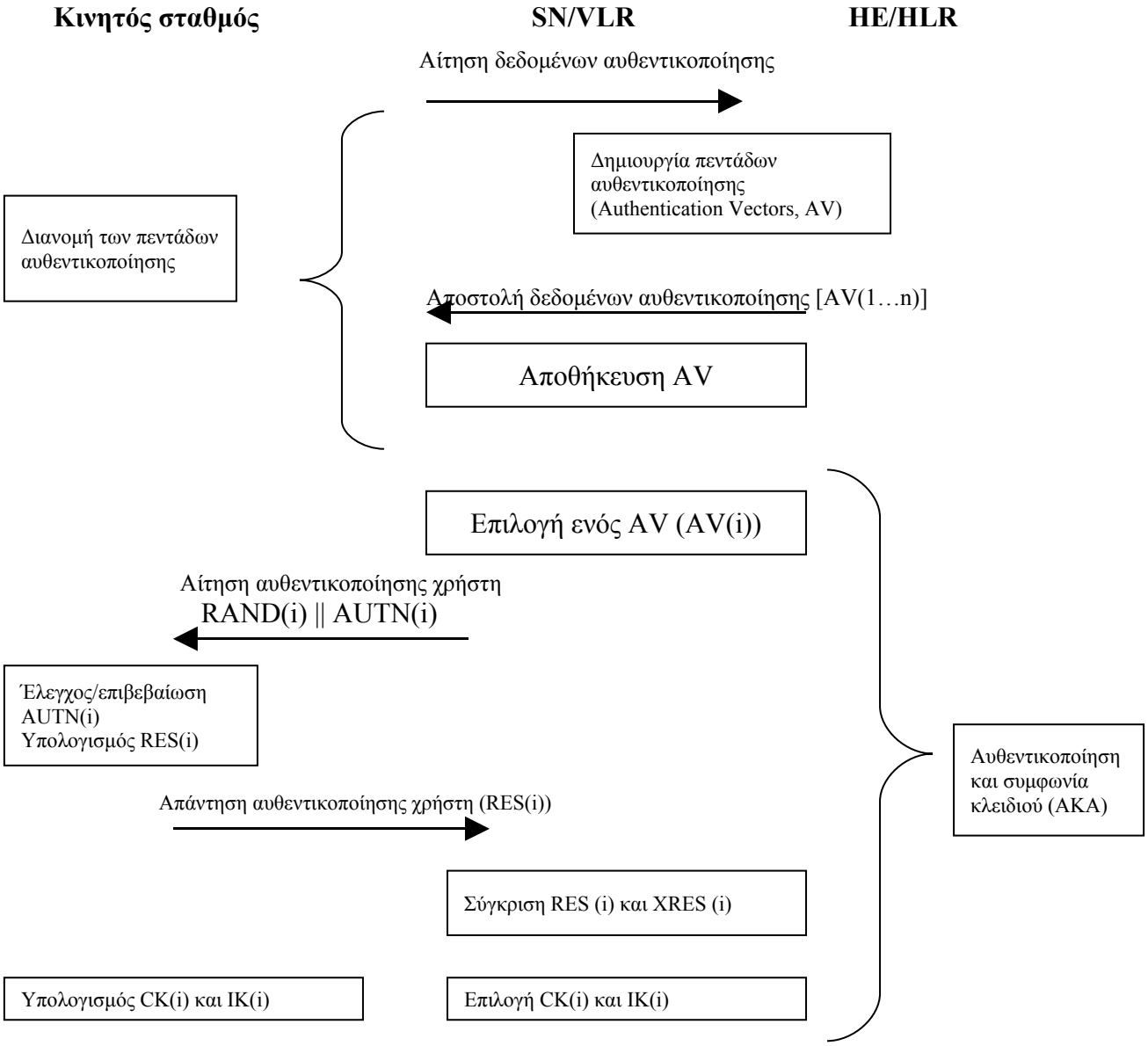
Οι μηχανισμοί ασφάλειας στο σύστημα UMTS ομαδοποιούνται στις πέντε κύριες κατηγορίες που αναφέρθηκαν στην προηγούμενη παράγραφο. Οι κυριότεροι από αυτούς αφορούν στην ασφάλεια του δικτύου πρόσβασης, δηλαδή στην ασφάλεια των ραδιο-ζεύξεων που εξυπηρετούν τον συνδρομητή.

3.2.1 Ασφάλεια δικτύου πρόσβασης (Network Access Security)

3.2.1.1 Πιστοποίηση ταυτότητας χρηστών

Ο μηχανισμός αυθεντικοποίησης των χρηστών στο UMTS είναι γνωστός και ως **Αυθεντικοποίηση και Συμφωνία Κλειδιού** (Authentication and Key Agreement, AKA). Στόχος της διαδικασίας είναι η αυθεντικοποίηση τόσο του χρήστη στο δίκτυο, όσο και του δικτύου στο χρήστη, σε αντίθεση με την αντίστοιχη διαδικασία στα δίκτυα GSM, όπου ο χρήστης δεν πιστοποιεί τη νομιμότητα του δικτύου. Στη διαδικασία αυτή, η οποία βασίζεται στο συμμετρικό κλειδί Ki μήκους 128 bits, που είναι αποθηκευμένο στην κάρτα USIM του χρήστη και στο HLR του οικείου δικτύου του (HN), συμμετέχουν το τερματικό του χρήστη (κάρτα USIM), το VLR/SGSN του HN ή του δικτύου εξυπηρέτησης (Serving Network, SN) στην περιοχή του οποίου

περιάγεται ο χρήστης και τον εξυπηρετεί, καθώς και του HLR/AuC του HN. Η διαδικασία περιγράφεται στο σχήμα 18.



Σχήμα 18. Διαδικασία αυθεντικοποίησης και συμφωνίας κλειδιού (AKA) [22]

Η διαδικασία αυθεντικοποίησης ξεκινά όταν η ταυτότητα του χρήστη αναγνωριστεί από το δίκτυο εξυπηρέτησης, που μπορεί να είναι και το οικείο δίκτυο. Αυτό μπορεί να συμβεί κατά την πρώτη εγγραφή του χρήστη στο δίκτυο, μετά από μια αίτηση για παροχή μιας υπηρεσίας, για επανεγκατάσταση της σύνδεσης, για ενημέρωση της τοποθεσίας του χρήστη κτλ. Σε αυτές τις περιπτώσεις ο χρήστης στέλνει στο δίκτυο

είτε τη μόνιμη ταυτότητά του (IMSI), είτε την προσωρινή (TMSI/P-TMSI). Η ταυτότητα στέλνεται από το υποδίκτυο UTRAN στο δίκτυο κορμού και συγκεκριμένα είτε στο VLR (CS domain) είτε στο SGSN (PS domain) του SN. Ακολούθως, το στοιχείο που παραλαμβάνει την αίτηση σύνδεσης του χρήστη στο δίκτυο, αποστέλλει στο HLR/AuC του HN του συνδρομητή μια αίτηση για δεδομένα αυθεντικοποίησης (authentication data request), και το τελευταίο ανταποκρίνεται δημιουργώντας - με βάση το κλειδί Ki - και αποστέλλοντας **ν** διανύσματα αυθεντικοποίησης[4] (Authentication Vector, AV). Ένα διάνυσμα αυθεντικοποίησης, που είναι το αντίστοιχο της τριπλέτας στο GSM, αποτελείται από πέντε συνολικά τιμές: ένα τυχαίο αριθμό RAND, μια τιμή αναμενόμενης απάντησης XRES, ένα κλειδί κρυπτογράφησης CK, ένα κλειδί ακεραιότητας IK και μια σκυτάλη αυθεντικοποίησης (authentication token, AUTN). Κάθε διάνυσμα αυθεντικοποίησης χρησιμοποιείται μόνο για μια διαδικασία AKA μεταξύ USIM και VLR/SGSN.

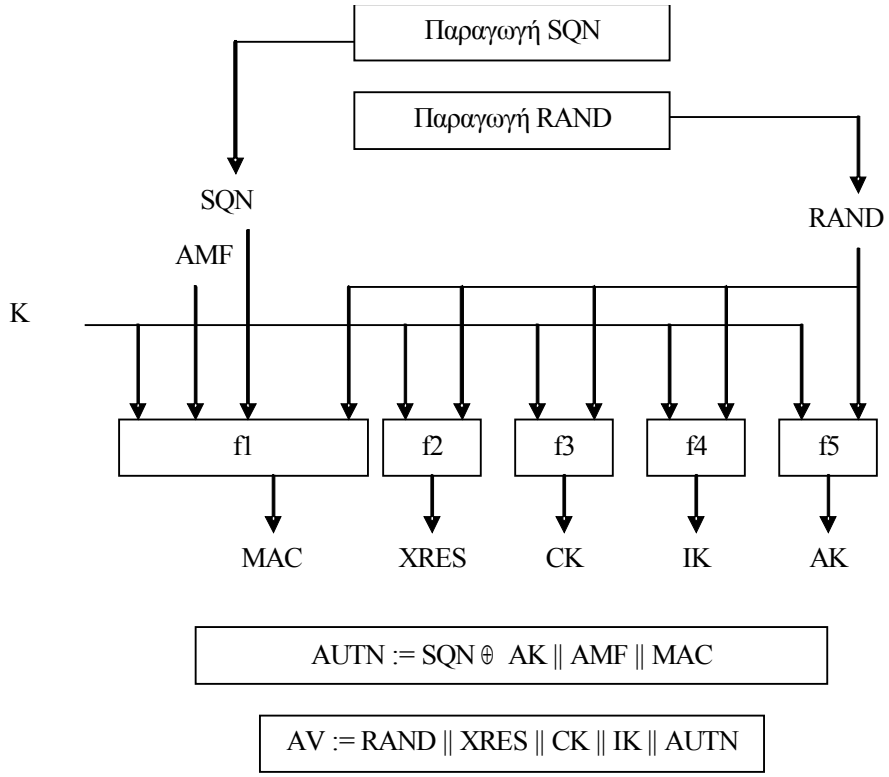
Στη συνέχεια της διαδικασίας, το VLR/SGSN στέλνει στο συνδρομητή μια αίτηση για αυθεντικοποίηση (user authentication request), στην οποία περιέχονται οι τιμές RAND και AUTN από το πρώτο από τα διανύσματα που παρέλαβε. Από την πλευρά της η USIM, με τη χρήση του κλειδιού Ki και τις παραμέτρους που παρέλαβε, όπως περιγράφεται αργότερα, θα προβεί σε υπολογισμούς αντίστοιχους με αυτούς που έγιναν για την παραγωγή του διανύσματος αυθεντικοποίησης, προκειμένου να επιβεβαιώσει ότι η παράμετρος AUTN δημιουργήθηκε από το HLR/AuC του οικείου δικτύου και επιπλέον ότι δεν έχει σταλεί προηγουμένως. Επίσης, παράγει τα κλειδιά CK και IK, καθώς και την τιμή RES την οποία στέλνει στο VLR/SGSN, για να συγκριθεί από το στοιχείο του δικτύου με την XRES. Αν XRES=RES, τότε η διαδικασία της αυθεντικοποίησης ολοκληρώνεται με επιτυχία. Το τελευταίο βήμα είναι η μεταφορά των κλειδιών κρυπτογράφησης και ακεραιότητας CK και IK, που δημιουργούνται ως παράγωγα της διαδικασίας αυθεντικοποίησης, από το VLR/SGSN στο υποδίκτυο UTRAN, και συγκεκριμένα στο RNC.

[4] Αποστέλλει περισσότερα από ένα διανύσματα αυθεντικοποίησης, προκειμένου να ελαχιστοποιηθεί η ανταλλαγή μηνυμάτων μεταξύ οικείου δικτύου και δικτύου εξυπηρέτησης.

3.2.1.2 Δημιουργία των διανυσμάτων αυθεντικοποίησης και επεξεργασία των παραμέτρων στη USIM

Όπως αναφέρθηκε στην προηγούμενη ενότητα, η παραγωγή των διανυσμάτων αυθεντικοποίησης λαμβάνει χώρα στο HLR/AuC του οικείου δικτύου του συνδρομητή. Το στοιχείο αυτό ξεκινά τη διαδικασία παράγοντας ένα σειριακό αριθμό SQN και μια τιμή RAND μήκους 128 bits με τη βοήθεια μιας γεννήτριας ψευδοτυχαίων αριθμών που μπορεί να παράγει απρόβλεπτες τιμές. Σε ότι αφορά το SQN, αυτό μπορεί να παράγεται με διαφορετικούς τρόπους για κάθε πάροχο υπηρεσιών. Στη γενικότερη περίπτωση, το SQN είναι ένας μετρητής που αυξάνεται σειριακά για κάθε χρήστη, δηλαδή κάθε χρήστης έχει το δικό του αριθμό SQN. Ωστόσο, είναι δυνατόν ο αριθμός αυτός να αυξάνεται με βάση μια καθολική αρίθμηση, όπως π.χ. ένα ρολόι (universal timer) ή να εφαρμόζεται ένας συνδυασμός των δύο τεχνικών και να αποτελείται από δύο μέρη: το πρώτο να αφορά έναν μεμονωμένο χρήστη και το δεύτερο έναν καθολικό μετρητή. Επίσης, δεδομένου ότι τα διανύσματα χρησιμοποιούνται και στο CS αλλά και στο PS υποσύστημα, είναι δυνατόν να χρησιμοποιούνται οι άρτιοι αριθμοί για το πρώτο και οι περιττοί για το δεύτερο. Από την πλευρά του χρήστη, η USIM ελέγχει την τιμή του SQN για να διαπιστώσει αν το διάνυσμα είναι «φρέσκο», δηλαδή δεν έχει χρησιμοποιηθεί ξανά στο παρελθόν.

Στη συνέχεια, το HLR/AuC κάνει χρήση πέντε μονόδρομων συναρτήσεων – f1 έως f5 – προκειμένου να παράγει τις πέντε τιμές που αποτελούν το διάνυσμα αυθεντικοποίησης. Η όλη διαδικασία περιγράφεται σχηματικά στο Σχήμα 19.

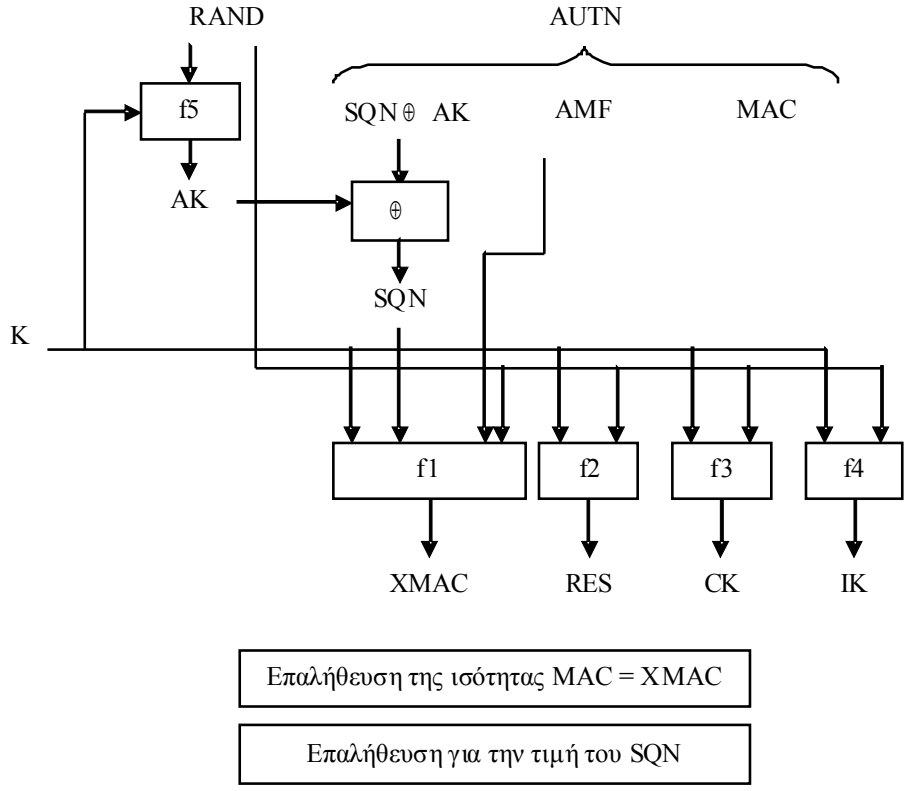


Σχήμα 19. Δημιουργία των τιμών των διανυσμάτων αυθεντικοποίησης στο HLR/AuC

Η συνάρτηση f1 δέχεται σαν εισόδους το κλειδί Ki, την τιμή RAND, τον αριθμό SQN και την παράμετρο AMF (Authentication Management Field), που αποτελεί διαχειριστικό πεδίο. Στην έξοδο παράγεται η τιμή MAC (Message Authentication Code) μήκους 64 bits. Η συνάρτηση f2 δέχεται στην είσοδο τις τιμές RAND και Ki και παράγει στην έξοδο την τιμή XRES (expected response) με μήκος από 32 έως 128 bits. Οι δυο αυτές συναρτήσεις είναι συναρτήσεις αυθεντικοποίησης μηνύματος. Οι συναρτήσεις κρυπτογράφησης f3, f4 και f5 δέχονται όλες στην είσοδο τις τιμές RAND και Ki και παράγουν αντίστοιχα τα κλειδιά κρυπτογράφησης CK, IK με μήκος 128 bits το καθένα, καθώς και το κλειδί AK (Anonymity Key) με μήκος 64 bits. Το κλειδί AK χρησιμοποιείται για να αποκρύψει τον σειριακό αριθμό SQN, καθώς ο τελευταίος, σε περίπτωση διακύβευσής του από μια παθητική επίθεση, είναι δυνατόν να αποκαλύψει την ταυτότητα και την τοποθεσία που βρίσκεται ο χρήστης. Τέλος, παράγεται και η παράμετρος AUTN = SQN ⊕ AK || AMF || MAC. Έτσι, το διάνυσμα αυθεντικοποίησης περιλαμβάνει τις παραμέτρους {RAND, XRES, CK, IK,

AUTN}. Πρέπει, τέλος να επισημανθεί ότι η επιλογή των αλγόριθμων για τις συναρτήσεις f1 έως f5 είναι στην ευχέρεια του εκάστοτε παρόχου.

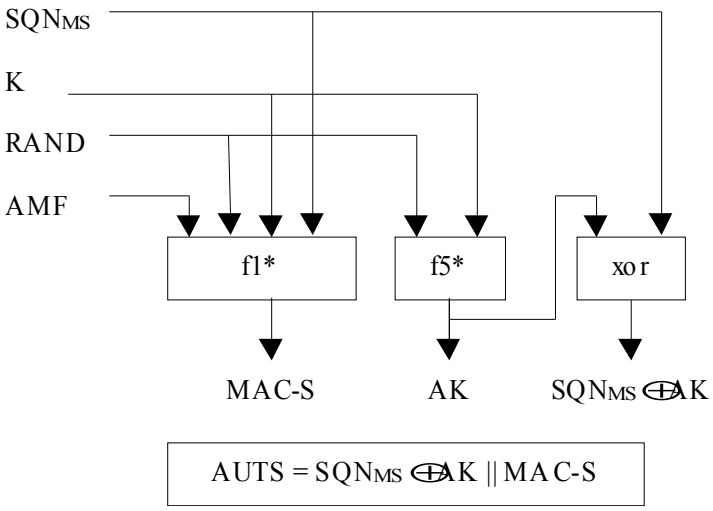
Από την πλευρά της USIM, όπως αναφέρθηκε, θα γίνουν ανάλογοι υπολογισμοί, προκειμένου ο χρήστης να αυθεντικοποιήσει το δίκτυο. Η διαδικασία φαίνεται στο Σχήμα 20.



Σχήμα 20. Η αυθεντικοποίηση του χρήστη στην USIM.

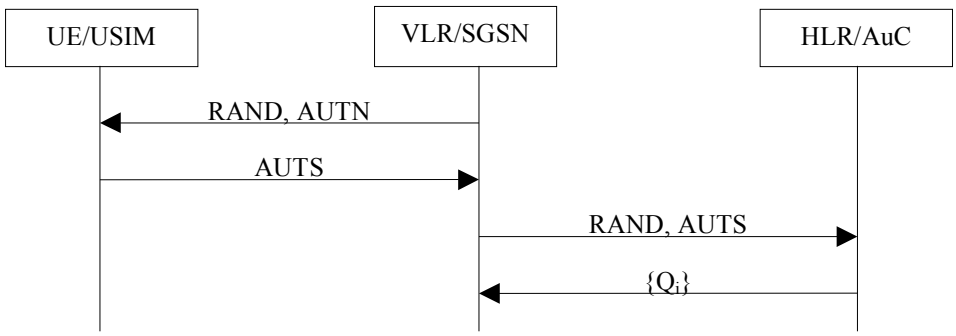
Ο χρήστης δέχεται στην USIM του τις τιμές RAND και AUTN από το VLR/SGSN. Οι συναρτήσεις που θα εκτελέσει η USIM για τους υπολογισμούς είναι οι ίδιες – f1 έως f5 – με τις ίδιες εισόδους, όπως και στο HLR/AuC, με διαφορετική όμως σειρά. Πρώτα εκτελείται η συνάρτηση f5 για να εξαχθεί το κλειδί $AK= f5_K (RAND)$ και κατόπιν ο αριθμός SQN = (SQN ⊕ AK) ⊕ AK. Στο σημείο αυτό η USIM θα επιβεβαιώσει την εγκυρότητα του SQN, με δεδομένο ότι διατηρεί στη μνήμη της τον τελευταίο αριθμό SQN (SQN_{MS}). Έτσι, αν SQNreceived > $SQN_{MS,}$ θα θεωρήσει το SQN που έλαβε ως έγκυρο. Αν όμως το SQNreceived <= $SQN_{MS,}$ η αυθεντικοποίηση αποτυγχάνει και αποστέλλει στο VLR/SGSN ένα μήνυμα αποτυχίας συγχρονισμού

(synchronization failure). Το συγκεκριμένο μήνυμα περιλαμβάνει την παράμετρο AUTS = Conc(SQN_{MS}) || MAC-S, όπου η Conc(SQN_{MS}) = $SQN_{MS} \oplus f5^*_K(RAND)$ χρησιμοποιείται για να αποκρύψει το SQN_{MS} , δηλαδή τον τελευταίο αποθηκευμένο αριθμό SQN στη μνήμη της USIM, και MAC-S = $f1^*_K(SQN_{MS} || RAND || AMF)$. Οι f1* και f5* είναι συναρτήσεις που φέρουν την ιδιότητα ότι καμία χρήσιμη πληροφορία δε μπορεί να εξαχθεί από τις τιμές της για τις τιμές των συναρτήσεων f1,…,f5. Η δημιουργία του AUTS απεικονίζεται στο Σχήμα 21.



Σχήμα 21. Δημιουργία της παραμέτρου AUTS.

Το VLR/SGSN αναλαμβάνει να προωθήσει το μήνυμα με τον αριθμό AUTS και την τιμή RAND στο HLR/AuC, το οποίο δημιουργεί καινούρια διανύσματα για να αυθεντικοποιηθεί ο χρήστης (re-synchronisation procedure).



Σχήμα 22. Η διαδικασία επανασυγχρονισμού

Αν δεν υπάρχει πρόβλημα συγχρονισμού με την τιμή του SQN, η διαδικασία συνεχίζεται με τον υπολογισμό του XMAC (expected MAC): XMAC = $f1_K$ (SQN || RAND || AMF) και τη σύγκρισή του με την τιμή MAC που έλαβε με την παράμετρο AUTN. Αν XMAC≠MAC, ο χρήστης αποστέλλει ένα μήνυμα απόρριψης αυθεντικοποίησης (user authentication reject) στο VLR/SGSN με μια ένδειξη της αιτίας και εγκαταλείπει τη διαδικασία. Στην περίπτωση αυτή, το VLR/SGSN θα πρέπει να στείλει μια αναφορά σφάλματος αυθεντικοποίησης στο HLR, ενώ έχει τη δυνατότητα να επανεκκινήσει τη διαδικασία αυθεντικοποίησης του χρήστη. Ακολούθως, υπολογίζει τα RES = $f2_K$ (RAND), CK = $f3_K$ (RAND) και IK = $f4_K$ (RAND). Η τιμή RES θα αποσταλεί πίσω στο VLR/SGSN, ενώ τα κλειδιά CK και IK θα αποθηκευτούν στη USIM, μέχρι την επόμενη επιτυχημένη αυθεντικοποίηση του χρήστη.[22]

3.2.1.3 Εμπιστευτικότητα της ταυτότητας του χρήστη

Η εμπιστευτικότητα της μόνιμης ταυτότητας του χρήστη (IMSI) προστατεύεται με τη χρήστη προσωρινών ταυτοτήτων (TMSI στο CS domain ή P-TMSI στο PS domain). Έτσι, η ταυτότητα του χρήστη προστατεύεται από «παθητικές» επιθέσεις. Ακόμη, η χρήση TMSI προσφέρει εμπιστευτικότητα σε ότι αφορά την παρουσία ή απουσία του χρήστη σε μια περιοχή, καθώς επίσης αποτρέπει κάποιον τρίτο (ωτακουστή) από το να διαπιστώσει αν διάφορες υπηρεσίες προσφέρονται στον ίδιο χρήστη. Από τη στιγμή που ο χρήστης θα αποκτήσει μια προσωρινή ταυτότητα, το δίκτυο θα τον ταυτοποιεί μέσω αυτής και όχι της IMSI.

Η διαδικασία ξεκινά αφού ενεργοποιηθούν οι μηχανισμοί κρυπτογράφησης, δηλαδή μετά από μια επιτυχή αμοιβαία αυθεντικοποίηση χρήστη και δικτύου και αφού παραχθεί το σχετικό κλειδί CK. Τότε το SN (VLR ή SGSN) αναθέτει μια προσωρινή ταυτότητα (TMSI ή P-TMSI) στο χρήστη, την οποία του διαβιβάζει κρυπτογραφημένη, ενώ παράλληλα δημιουργεί και διατηρεί μέχρι την επόμενη αυθεντικοποίηση μια συσχέτιση ανάμεσα στη μόνιμη και την προσωρινή ταυτότητά του ($IMSI_i$, $TMSI_i$). Ο χρήστης παραλαμβάνει τη νέα TMSI και διαγράφει οποιασδήποτε συσχέτιση με την παλιά, στέλνοντας συγχρόνως μια βεβαίωση λήψης

(acknowledgement) στο SN. Ακολούθως, το VLR/SGSN διαγράφει την προηγούμενη συσχέτιση ($IMSI_i$, $TMSI_{old}$) και αποθηκεύει την νέα. Στην περίπτωση που το VLR/SGSN δε λάβει μήνυμα επιβεβαίωσης λήψης από το χρήστη, είναι υποχρεωμένο να διατηρήσει και τις δυο συσχετίσεις – την παλιά και την καινούρια – και να κάνει αποδεκτές είτε τη μία είτε την άλλη όταν ο χρήστης επικοινωνεί με το δίκτυο. Στην περίπτωση όμως που το δίκτυο στείλει μήνυμα σηματοδοσίας στο χρήστη, τον ενημερώνει να διαγράψει κάθε προσωρινή ταυτότητα που διαθέτει και ξεκινά τη διαδικασία απόδοσης νέας προσωρινής ταυτότητας. Για να αποφευχθεί η όποια πιθανότητα να καταγραφούν από τρίτο οι κινήσεις του χρήστη, θα πρέπει να μη χρησιμοποιείται η ίδια προσωρινή ταυτότητα για μεγάλο χρονικό διάστημα, προκειμένου να αναγνωρίζεται ο χρήστης.

Όπως είχε αναφερθεί στη σχετική ενότητα, πριν από τη διαδικασία AKA, ο χρήστης θα πρέπει να δηλώσει την ταυτότητά του στο σύστημα. Ωστόσο, η διαδικασία ανάθεσης και αποστολής της TMSI από το VLR/SGSN στο χρήστη θα πρέπει να γίνει μετά την ενεργοποίηση της κρυπτογράφησης, δηλαδή μετά την παραγωγή του κρυπτογραφικού κλειδιού CK στη USIM και στο δίκτυο, ώστε να προστατευθεί η TMSI από τρίτες παρεμβάσεις. Όμως, η παραγωγή του κλειδιού CK στις αντίστοιχες οντότητες προϋποθέτει την αναγνώριση και αυθεντικοποίηση του χρήστη στο δίκτυο. Το πρόβλημα λύνεται αν ληφθεί υπ' όψη ότι η TMSI ισχύει μόνο στην περιοχή που βρίσκεται ο χρήστης και είναι καταγραμμένη στο τοπικό VLR, όπως και η συσχέτισή της με το IMSI του χρήστη. Αν ο χρήστης αλλάξει περιοχή (κελί), το νέο VLR (VLR_1), λόγω του ότι δεν αναγνωρίζει το TMSI του χρήστη, ζητά από το VLR της προηγούμενης περιοχής (VLR_0) να του δώσει το IMSI με το οποίο συσχετίζεται ο «άγνωστος», ως τώρα, χρήστης. Αν το VLR_0 δεν μπορέσει να ανακτήσει αυτήν την πληροφορία, μόνο τότε θα ζητηθεί από το χρήστη να αποστείλει το IMSI του, χωρίς κρυπτογράφηση, στο VLR_1. Διαφορετικά, όπως είναι και το πιο σύνηθες, ο χρήστης αναγνωρίζεται και ακολουθεί η διαδικασία AKA, η παραγωγή κλειδιών CK και η ανάθεση νέας προσωρινής ταυτότητας, που χρησιμοποιείται εφ' εξής.

Ωστόσο, στις περιπτώσεις κατά τις οποίες γίνεται για πρώτη φορά η ταυτοποίηση και η καταγραφή του χρήστη στο δίκτυο, δεν είναι δυνατόν να χρησιμοποιηθεί ο μηχανισμός της προσωρινής ταυτότητας, διότι το δίκτυο δεν γνωρίζει ακόμα τη μόνιμη ταυτότητα του χρήστη. Στην περίπτωση αυτή, ο χρήστης θα πρέπει να αποστείλει το IMSI στο SN, χωρίς κρυπτογράφηση, για να του ανατεθεί στη συνέχεια μια TMSI. Επίσης, το IMSI χρησιμοποιείται ως μέσο αναγνώρισης του συνδρομητή και στις περιπτώσεις, που το VLR/SGSN έχει υποστεί μια βλάβη στη βάση δεδομένων του.

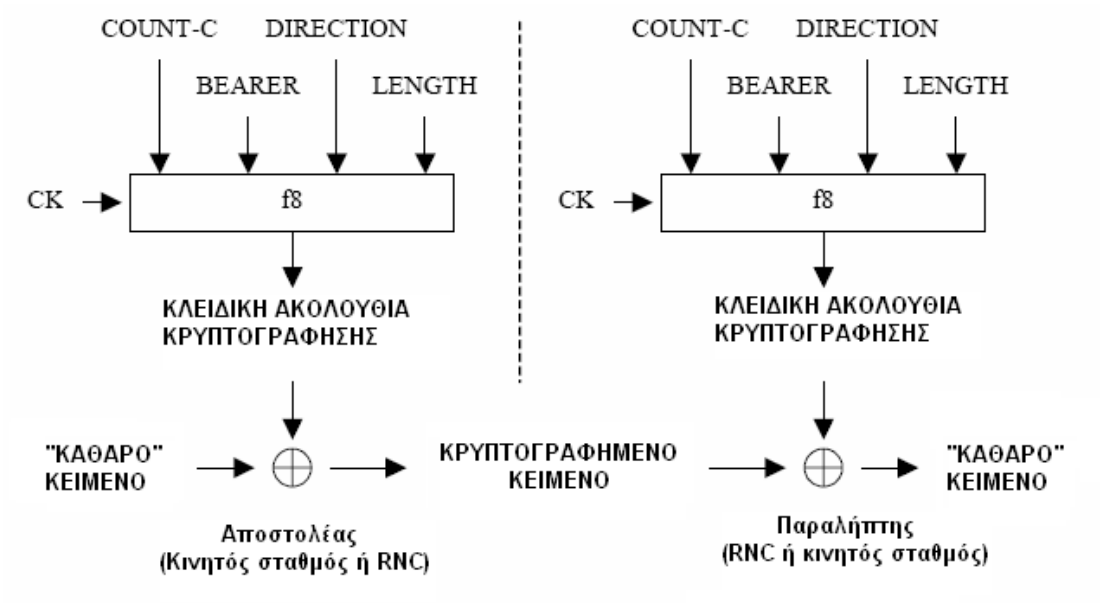
3.2.1.4 Εμπιστευτικότητα των δεδομένων του χρήστη

Τα δεδομένα που επιθυμεί να μεταδώσει ο χρήστης μέσω των ραδιο-καναλιών του δικτύου, όπως επίσης και τα ραδιο-σήματα που εκπέμπονται μεταξύ αυτού και του δικτύου θεωρούνται ευαίσθητα δεδομένα και πρέπει να προστατεύονται από μη εξουσιοδοτημένες οντότητες που θα προσπαθήσουν να τα υποκλέψουν. Είδαμε προηγουμένως ότι η εμπιστευτικότητα της ταυτότητας του προστατεύεται με το μηχανισμό της ασφαλούς μεταφοράς της προσωρινής του ταυτότητας TMSI. Η εμπιστευτικότητα των διακινούμενων πληροφοριών του χρήστη (φωνή, ψηφιακά δεδομένα κτλ) αλλά και των δεδομένων σηματοδοσίας προστατεύεται με έναν αλγόριθμο κρυπτογράφησης. Ο αλγόριθμος που χρησιμοποιείται συνήθως είναι ο αλγόριθμος KASUMI. Η κρυπτογράφηση λαμβάνει χώρα στον κινητό σταθμό, από την πλευρά του χρήστη και στο RNC, από την πλευρά του δικτύου. [24]

Η λειτουργία του συγκεκριμένου αλγόριθμου βασίζεται στο κρυπτογραφικό κλειδί CK, το οποίο παράγεται, όπως αναφέρθηκε κατά τη διαδικασία της αυθεντικοποίησης του χρήστη, τόσο στο SN (VLR/SGSN), όσο και στη USIM[5] (σχήμα 23). Το κλειδί CK μεταφέρεται από το SN στο RNC, με ένα ειδικό μήνυμα που καλείται “security mode command”. Στο κείμενο που θα κρυπτογραφηθεί προστίθεται (XOR) μια κλειδική ακολουθία κρυπτογράφησης (keystream block) που παράγεται σαν αποτέλεσμα της εκτέλεσης της συνάρτησης f8, που υλοποιεί τον αλγόριθμο KASUMI, πάνω σε μια ομάδα παραμέτρων. Οι παράμετροι αυτοί είναι:

[5] Αν δεν έχει γίνει αυθεντικοποίηση πριν από την έναρξη της σύνδεσης και τη μετάδοση δεδομένων χρησιμοποιείται το προηγούμενο CK που είναι αποθηκευμένο στη USIM.

το κρυπτογραφικό κλειδί CK (128 bits), το LENGTH (το μέγεθος του keystream block-16 bits), το DIRECTION (downlink ή uplink-1 bit), το BEARER (ταυτότητα του ραδιο-καναλιού που μεταφέρει τα δεδομένα-5 bits) και η παράμετρος COUNT-C (μετρητής-32 bits) που αυξάνεται κάθε φορά που μεταφέρεται ένα νέο πακέτο δεδομένων. Με τον τρόπο αυτό παράγεται ένα κρυπτογραφημένο κείμενο, το οποίο αποκρυπτογραφείται από τον παραλήπτη απλά προσθέτοντας το ίδιο keystream block.



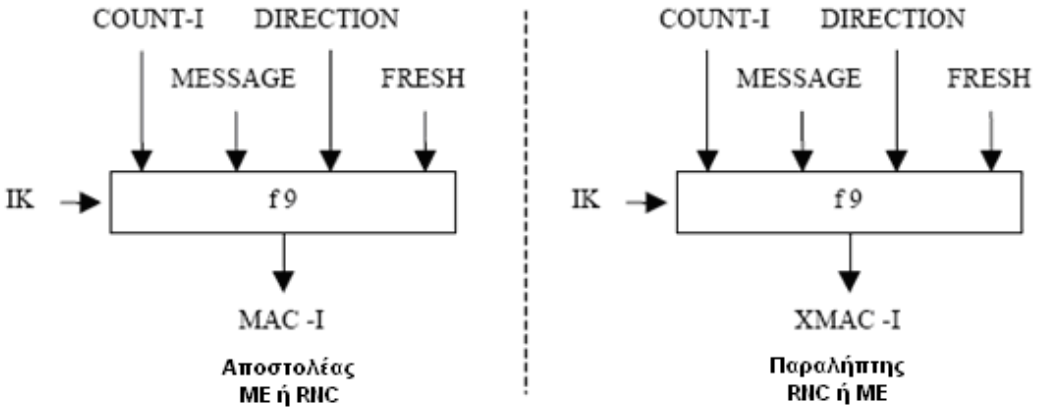
Σχήμα 23. Μηχανισμός εμπιστευτικότητας user/signalling data [24]

3.2.1.5 Ακεραιότητα δεδομένων σηματοδοσίας

Σκοπός του μηχανισμού ακεραιότητας δεδομένων (data integrity) είναι να προστατέψει τα δεδομένα σηματοδοσίας, που ανταλλάσσονται μεταξύ του κινητού σταθμού και του δικτύου πρόσβασης (RNC), από μεταβολή τους από τρίτα πρόσωπα που ενδεχομένως να προσπαθήσουν να υποκλέψουν την ραδιοζεύξη. Η υλοποίηση του πραγματοποιείται στο RRC Layer μεταξύ του κινητού σταθμού και του RNC, και γίνεται με το κλειδί IK που παράγεται κατά τη διαδικασία της αυθεντικοποίησης (AKA), όπως και το κλειδί CK, και μεταφέρεται με “security mode command” στο RNC.

Ο μηχανισμός της ακεραιότητας δεδομένων βασίζεται στην εκτέλεση της συνάρτησης “message authentication code”, γνωστής ως f9, που παράγεται επίσης από τον αλγόριθμο KASUMI [24] (σχήμα 24). Ως είσοδοι της συνάρτησης αυτής ορίζονται οι παράμετροι IK (128 bits), DIRECTION (1 bit), FRESH(32 bits) και COUNT-I (32 bits), όπως επίσης και το RRC μήνυμα που πρόκειται να μεταδοθεί. Η παράμετρος FRESH είναι ένας τυχαίος αριθμός, ενώ η COUNT-I μοιάζει με τον αντίστοιχο μετρητή της κρυπτογράφησης δεδομένων, καθώς η τιμή του αυξάνεται για κάθε μήνυμα που μετέχει στη διαδικασία και αρχικοποιείται στην αρχή της σύνδεσης. Στην έξοδο, παράγεται μια παράμετρος MAC-I (32 bits), που προσαρτάται στο αρχικό RRC μήνυμα και αποστέλλεται στον παραλήπτη, μαζί με την παράμετρο FRESH. Ο παραλήπτης υπολογίζει με την ίδια συνάρτηση το αναμενόμενο MAC-I (XMAC-I) και επαληθεύει την ακεραιότητα δεδομένων, συγκρίνοντας αυτήν την τιμή με την MAC-I.

Ο μηχανισμός της ακεραιότητας δεδομένων, που απεικονίζεται στο σχήμα 24, εφαρμόζεται για κάθε μήνυμα που περιέχει δεδομένα σηματοδοσίας ή ελέγχου (signaling/control data) εκτός από εκείνα που στέλνονται πριν δημιουργηθεί το κλειδί IK, όπως για παράδειγμα το μήνυμα “RRC connection request” από το χρήστη στο δίκτυο, πριν από την AKA. Επίσης, θα πρέπει να τονιστεί ότι ο μηχανισμός αυτός δεν εφαρμόζεται για να προστατέψει τα δεδομένα του χρήστη (user data) από τροποποιήσεις, λόγω επιβάρυνσης της απόδοσης που θα προκληθεί. Ωστόσο, υπάρχει ένας παρεμφερής μηχανισμός ελέγχου και ακεραιότητας της ποσότητας των δεδομένων που διακινούνται. Συγκεκριμένα, η διαδικασία αυτή επιτρέπει στο RNC να κάνει χρήση μετρητών για να παρακολουθεί τα sequence numbers για κάθε πακέτο στο οποίο εφαρμόζονται οι μηχανισμοί εμπιστευτικότητας και ακεραιότητας από κάθε ραδιο-κανάλι. Το RNC ενημερώνει την κινητή συσκευή στέλνοντας ένα σχετικό μήνυμα με τις τιμές των μετρητών, που αντικατοπτρίζουν την ποσότητα των δεδομένων που διακινήθηκαν σε κάθε ενεργό ραδιο-κανάλι. Η κινητή συσκευή συγκρίνει αυτές τις τιμές με τις αντίστοιχες που έχει αποθηκευμένες, και αν υπάρχει διαφορά στέλνει ένα κατάλληλο μήνυμα.



Σχήμα 24. Μηχανισμός ακεραιότητας δεδομένων [24]

3.2.1.6 Ανακεφαλαίωση των Μηχανισμών Ασφάλειας στο Δίκτυο Πρόσβασης

Μέχρι τώρα, περιγράφηκαν οι επιμέρους μηχανισμοί που ισχύουν στο δίκτυο πρόσβασης του UMTS σε ότι αφορά την αυθεντικοποίηση του χρήστη και του δικτύου, την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων του χρήστη και των δεδομένων σηματοδοσίας και ελέγχου. Στη συνέχεια θα γίνει αναφορά στο πως αυτοί οι μηχανισμοί συνεργάζονται και εμπλέκονται στη γενικότερη αρχιτεκτονική ασφάλειας του UMTS, η οποία απεικονίζεται στο σχήμα 25.

Η όλη διαδικασία θα μπορούσε να διαιρεθεί στα παρακάτω βήματα [25]:

1. Ο κινητός σταθμός (ME) στέλνει στο σταθμό βάσης μια αίτηση για εγκατάσταση RRC σύνδεσης (RRC connection request), οπότε μια τέτοια σύνδεση εγκαθίσταται ανάμεσα στο ME και το RNC. Κατά τη διάρκεια αυτής της σύνδεσης ο κινητός σταθμός αποστέλλει στο RNC μια δήλωση της κλάσης της συσκευής (classmark) υποδεικνύοντας σε αυτό τις δυνατότητες ασφαλείας του, δηλαδή τους αλγόριθμους κρυπτογράφησης και ακεραιότητας που υποστηρίζει. Το RNC αποθηκεύει αυτές τις πληροφορίες.

2. Στη συνέχεια, ο κινητός σταθμός αποστέλλει με ένα άλλο μήνυμα στο δίκτυο εξυπηρέτησης (SN), την ταυτότητα του συνδρομητή, δηλαδή την προσωρινή του ταυτότητα TMSI. Αν αυτή δεν αναγνωριστεί από το SN, ζητείται και αποστέλλεται η μόνιμη ταυτότητα IMSI. Επίσης στέλνει το KSI set, δηλαδή τα κλειδιά

κρυπτογράφησης και ακεραιότητας (CK, IK) που χρησιμοποιήθηκαν κατά την τελευταία σύνδεση.

3. Το VLR/SGSN - που αντιπροσωπεύει το SN – αναγνωρίζει την ταυτότητα του ΜΕ, και αποφασίζει αν θα εκκινήσει την διαδικασία AKA για την αμοιβαία αυθεντικοποίηση[6]. Αν γίνει αυτό, τότε παράγεται μια νέα ομάδα κλειδιών που θα χρησιμοποιηθούν μεταξύ χρήστη και δικτύου και λαμβάνουν χώρα όλα όσα περιγράφηκαν στην αντίστοιχη ενότητα της AKA. (Ο κινητός σταθμός υπολογίζει την παράμετρο RES και την αποστέλλει και το SN επιβεβαιώνει ότι RES=XRES). Έτσι, και τα δύο μέρη είναι σίγουρα ότι γίνεται χρήση των ίδιων κλειδιών.

4. Ακολούθως, το SN αποφασίζει ποιους αλγόριθμους για την κρυπτογράφηση και την ακεραιότητα επιθυμεί να χρησιμοποιήσει στο εξής και πληροφορεί με την εντολή security mode command το RNC, στο οποίο αποστέλλει επίσης και τα κλειδιά κρυπτογράφησης (CK) και ακεραιότητας (IK).

5. Το RNC, γνωρίζοντας τις δυνατότητες ασφάλειας του ΜΕ, λαμβάνει την τελική απόφαση για τους αλγόριθμους που θα χρησιμοποιηθούν. Το επόμενο βήμα είναι να στείλει στον κινητό σταθμό με ένα μήνυμα προστατευμένης ακεραιότητας (integrity protected) τόσο τους αλγόριθμους που θα χρησιμοποιηθούν όσο και τις δυνατότητες ασφάλειας του κινητού σταθμού, όπως αυτός τους είχε στείλει αρχικά (βήμα 1). Από εδώ και πέρα όλα τα μηνύματα είναι προστατευμένα, διότι είναι κρυπτογραφημένα με τα κλειδιά που συμφωνήθηκαν[7].

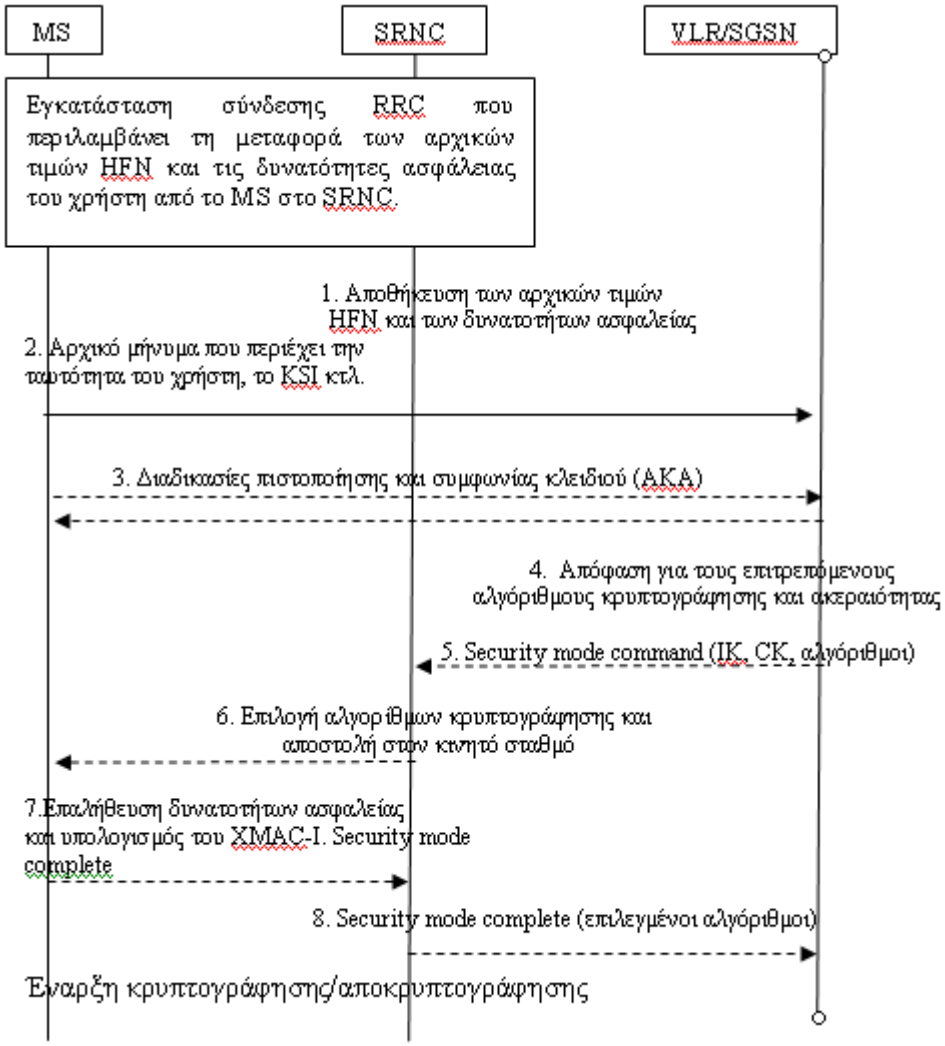
6. Ο κινητός σταθμός ελέγχει αν το μήνυμα είναι προστατευμένης ακεραιότητας υπολογίζοντας το XMAC-I και συγκρίνοντάς το με την τιμή MAC-I που έλαβε. Επίσης, κάνει έλεγχο για το αν οι δυνατότητες ασφάλειας που του επεστράφησαν είναι οι ίδιες με αυτές που είχε στείλει στην αρχή (βήμα 1). Αν διαπιστώσει την εγκυρότητα, στέλνει στο RNC ένα μήνυμα sequrity mode complete.

7. Τέλος, το RNC πληροφορεί το SN (VLR/SGSN) για τους αλγόριθμους που συμφωνήθηκαν τελικά. Έτσι, χρήστης και δίκτυο έχουν αυθεντικοποιηθεί αμοιβαία, και έχουν όλα τα απαραίτητες προϋποθέσεις (κλειδιά, αλγόριθμους) για να αποστέλλουν μηνύματα προστατευμένα σε ότι αφορά την εμπιστευτικότητα και την ακεραιότητα.

---

[6] Ο πάροχος υπηρεσιών είναι αυτός που αποφασίζει πότε (και πόσο συχνά) θα ξεκινήσει μια διαδικασία αυθεντικοποίησης.

[7] Όλα τα προηγούμενα μηνύματα δεν ήταν προστατευμένα γιατί δεν είχαν ακόμα συμφωνηθεί τα κοινά κλειδιά.



Σχήμα 25. Μηχανισμός ασφάλειας στο δίκτυο πρόσβασης του UMTS [26]

3.2.2 Ασφάλεια στην Περιοχή Δικτύου (network domain security)

Η ασφάλεια στην περιοχή δικτύου αναφέρεται στους μηχανισμούς ασφάλειας που παρέχονται μεταξύ δύο συστατικών του ίδιου ή διαφορετικών δικτύων [27]. Στην περίπτωση που τα αυτά τα στοιχεία αυτά βρίσκονται σε διαφορετικά δίκτυα, οι μηχανισμοί πρέπει, προφανώς, να είναι προτυποποιημένοι έτσι ώστε να καλύπτονται οι απαιτήσεις ασφάλειας και η επικοινωνία μεταξύ τους να μην είναι ευάλωτη σε επιθέσεις. Στα δίκτυα προηγούμενων γενιών, η ασφάλεια ήταν βασισμένη στο πρωτόκολλο SS7. Το κυρίως δίκτυο θεωρούνταν μια ασφαλής περιοχή, καθώς πρόσβαση στο συγκεκριμένο πρωτόκολλο είχαν μόνον λίγες μεγάλες εταιρείες

παροχής υπηρεσιών κινητής τηλεφωνίας και ήταν σχεδόν αδύνατον κάποιος τρίτος να διεισδύσει και να υποκλέψει μηνύματα. Έτσι, το πρωτόκολλο αυτό δεν προέβλεπε την κρυπτογραφημένη μετάδοση σημάτων και δεδομένων μεταξύ των μερών του κυρίως δικτύου. Ακόμα και στην έκδοση 99 του UMTS (UMTS Release 99), δεν είχαν γίνει σημαντικές βελτιώσεις στον τομές αυτόν, και έτσι η ασφάλεια ήταν σχεδόν η ίδια με αυτή που παρείχε το GSM.

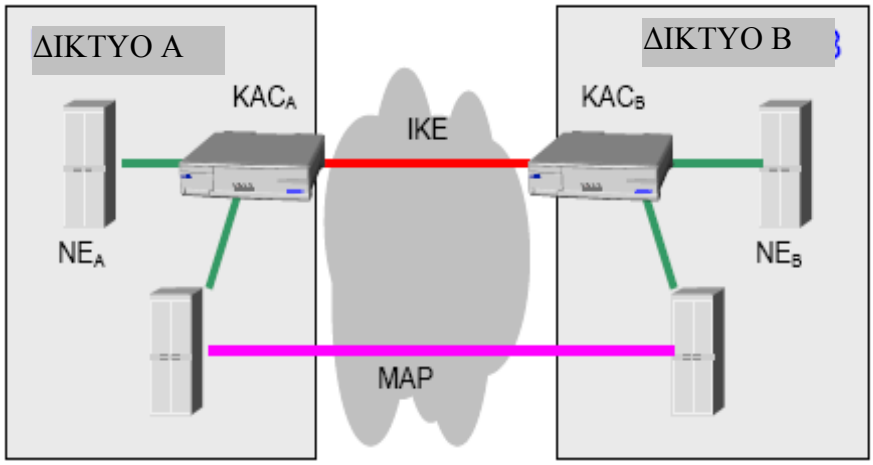
Με την πάροδο των χρόνων, και καθώς ο αριθμός των εταιρειών που παρείχαν αντίστοιχες υπηρεσίες σταδιακά αυξανόταν, η κατάσταση αρχίζει να αλλάζει. Οι διαφορετικοί πάροχοι θα πρέπει να εξασφαλίζουν την απρόσκοπτη και ασφαλή κινητότητα του χρήστη από το ένα δίκτυο στο άλλο. Εξάλλου, σε αυτό συντείνει και η εμφάνιση μιας τάσης για αντικατάσταση των SS7 δικτύων από δίκτυα βασισμένα στο πρωτόκολλο IP, που μπορεί να φέρει πολλά πλεονεκτήματα, ωστόσο σημαίνει ότι οι κίνδυνοι που υπάρχουν στο διαδίκτυο είναι δυνατόν να μεταφερθούν και στις τηλεπικοινωνίες.

Για αυτούς τους λόγους, η έλλειψη κρυπτογράφησης στα μηνύματα μεταξύ των μερών των ίδιων ή διαφορετικών δικτύων θα ήταν ένα μεγάλο ρίσκο. Έτσι, αποφασίστηκε στην έκδοση 4 του UMTS να συμπεριληφθούν μηχανισμοί που προστατεύουν το πρωτόκολλο MAP (Mobile Application Part), το οποίο καθορίζει τους κανόνες μετάδοσης σημάτων και άλλων δεδομένων (π.χ. authentication data) μεταξύ στοιχείων του δικτύου (ή των δικτύων). Το πρωτόκολλο αυτό «κληρονομήθηκε» από το δίκτυο GSM και χρησιμοποιήθηκε στο UMTS, για να ελέγξει την επικοινωνία, αρχικά, μεταξύ των στοιχείων του δικτύου που αποτελούν το CS domain (MSC, GMSC) και του home network (HLR, EIR, AuC) και αργότερα, μετά την εμφάνιση των GPRS δικτύων, επεκτάθηκε για να ελέγξει και τις διεπαφές μεταξύ του PS domain (SGSN, GGSN) και του home network. Οι μηχανισμοί που προστατεύουν το πρωτόκολλο MAP αποτελούν το MAPSEC, σκοπός του οποίου είναι να παρέχει ασφάλεια με χρήση κρυπτογράφησης για τα μηνύματα MAP.

Επίσης, σε ότι αφορά την ασφάλεια των δικτύων 3G που η λειτουργία τους βασίζεται στο πρωτόκολλο IP (IP-based networks), έχει υιοθετηθεί από την έκδοση 5 του UMTS το πρωτόκολλο IPSEC, που έχει δημιουργηθεί από την IETF για τα δίκτυα αυτά. Το 3GPP ρυθμίζει απλώς τον τρόπο με τον οποίο το IPSEC θα προστατέψει τις τηλεπικοινωνίες που είναι βασισμένες στο IP. Έτσι, υπάρχουν δύο δυνατές επιλογές για την ασφάλεια του MAP: το MAPSEC κα το IPSEC. Η λειτουργία των μηχανισμών αυτών περιγράφεται παρακάτω.

3.2.2.1 MAPSEC

Στο πρωτόκολλο ασφάλειας MAPSEC εισάγεται μια νέα οντότητα, η οποία φέρει την ονομασία «Κέντρο Διαχείρισης Κλειδιού» (Key Administration Centre, KAC). Κάθε δίκτυο που θέλει να χρησιμοποιήσει το MAPSEC πρέπει να έχει ένα τέτοιο κέντρο. Σκοπός του KAC ενός δικτύου είναι να δημιουργήσει συσχετισμούς ασφάλειας (Security Association, SA) με το αντίστοιχο KAC ενός άλλου δικτύου, με το οποίο θέλει να ανταλλάξει μηνύματα MAP (Σχήμα 26). Η δημιουργία των SAs, που βασίζεται στο πρωτόκολλο IKE (Internet Key Exchange), έχει σαν στόχο κάθε SA να περιλαμβάνει όλους τους μηχανισμούς ασφάλειας, όπως π.χ. αλγόριθμους κρυπτογράφησης, κλειδιά, χρονικά όρια χρήσης των κλειδιών κτλ., που θα χρησιμοποιήσουν τα δίκτυα για να καταστήσουν ασφαλή τα μηνύματα MAP που θα ανταλλάξουν. Το KAC διανέμει αυτά τα SAs στα υπόλοιπα μέρη του κυρίως δικτύου (NE), τα οποία τα χρησιμοποιούν για να προστατέψουν τα MAP μηνύματα που θα στείλουν.

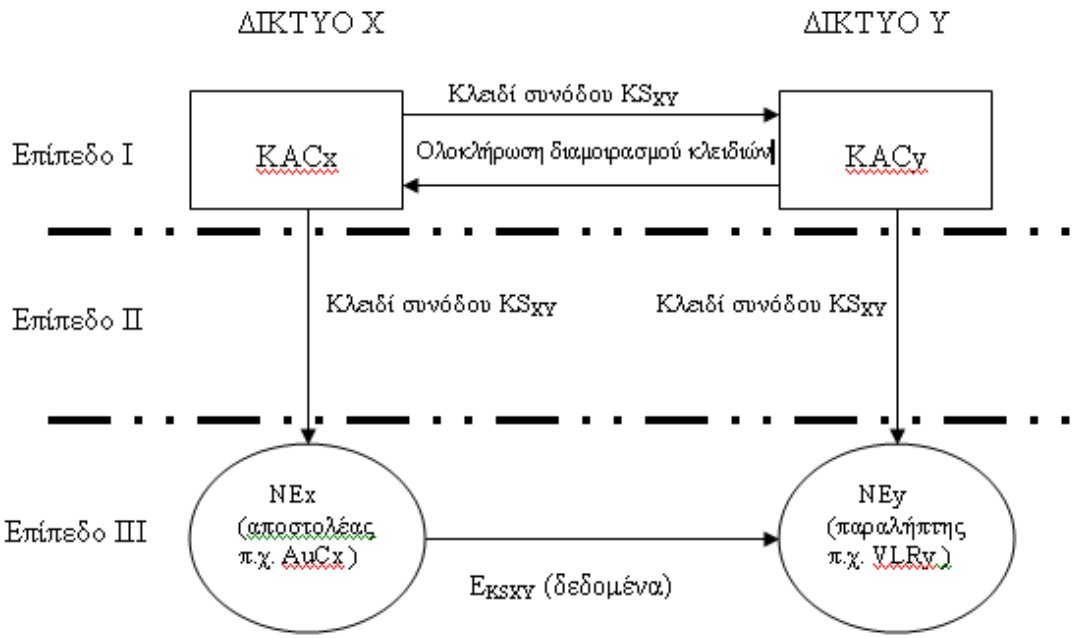


Σχήμα 26. MAPSEC [27]

Αναλυτικά, η διαδικασία έχει ως εξής:

1. Η μονάδα που θέλει να στείλει δεδομένα ενεργοποιεί το μηχανισμό διαλέγοντας ένα κλειδί που θα το χρησιμοποιήσει για να στείλει αυτά τα δεδομένα στην άλλη πλευρά. Στο σχήμα 27 (Layer I), το KACx του δικτύου X δημιουργεί ένα κλειδί συνόδου (session key, KSxy) για την επικοινωνία του με το KACy του δικτύου Y. Η μεταφορά του κλειδιού προστατεύεται με ασύμμετρη κρυπτογράφηση. Έτσι, τα δύο KACs συμφωνούν για τα κλειδιά που θα χρησιμοποιήσουν[8].
2. Το KACx ενημερώνει τα στοιχεία του δικτύου του, που θέλουν να στείλουν δεδομένα στην άλλη πλευρά, για το session key που θα χρησιμοποιηθεί. Το KACx μεταδίδει το KSxy σε ένα συστατικό του δικτύου π.χ. στο AuCx. Η μεταφορά του κλειδιού πρέπει να γίνει με ασφαλή τρόπο, κι αυτό επιτυγχάνεται με τεχνικές παρόμοιες με αυτές του προηγούμενου βήματος (Layer II)
3. Το κομμάτι του δικτύου που θέλει να μεταδώσει χρησιμοποιεί το session key για να προστατέψει τα δεδομένα που θα στείλει με τη βοήθεια ενός συμμετρικού αλγόριθμου κρυπτογράφησης. Π.χ. το AuCx κρυπτογραφεί το μήνυμα με το κλειδί συνόδου που έλαβε από το KACx, και το αποστέλλει κάνοντας χρήση του MAC πρωτοκόλλου (Layer III).

[8] Σημειώνεται ότι για την επικοινωνία KACy→ KACx, θα χρησιμοποιηθεί άλλο κλειδί που θα επιλέξει το KACy.



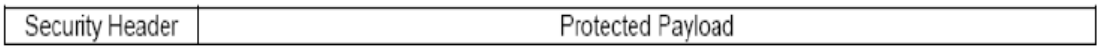
Σχήμα 27. Μηχανισμός για τη διανομή και χρήση κλειδιών για την αποστολή δεδομένων μεταξύ διαφορετικών δικτύων [22]

Δομή των προστατευμένων MAP μηνυμάτων

Τα μηνύματα MAP, όταν αποστέλλονται, μπορούν να έχουν τρεις μορφές (modes):

- Μορφή 0: Δεν παρέχεται προστασία.
- Μορφή 1: Παρέχεται προστασία ακεραιότητας και αυθεντικοποίησης.
- Μορφή 2: Παρέχεται εμπιστευτικότητα, ακεραιότητα και αυθεντικοποίηση.

Η δομή των MAP μηνυμάτων είναι η εξής:



Σχήμα 28. Δομή MAP μηνυμάτων

Μορφή 1:

Επικεφαλίδα ασφαλείας (Security Header):

SPI || Original Component Id || TVP || NE-id || Prop

Η επικεφαλίδα ασφαλείας περιέχει πληροφορίες για την επεξεργασία του μηνύματος από την πλευρά του λήπτη. Το SPI (Security Parameters Index) είναι μια τιμή που καθορίζει το MAPSEC. Το Original Component Id καθορίζει το είδος του συστατικού που μεταφέρεται, το TVP είναι μια «χρονική σφραγίδα» που χρησιμοποιείται για την προστασία επανάληψης, ενώ το Prop είναι μια τιμή που αντιστοιχεί σε κάθε μήνυμα στην ίδια TVP περίοδο και στο ίδιο NE.

Protected Payload:

Cleartext || f7 (Security Header || Cleartext)

Είναι το άθροισμα του καθαρού κειμένου και του αποτελέσματος μιας συνάρτησης f7 στο καθαρό μήνυμα και στην επικεφαλίδα ασφαλείας. Η f7 εφαρμόζεται για να προσφέρει προστασία της ακεραιότητας των δεδομένων και αυθεντικοποίηση προέλευσης.

Μορφή 2:

Η επικεφαλίδα ασφαλείας είναι η ίδια με αυτή της μορφής 1.

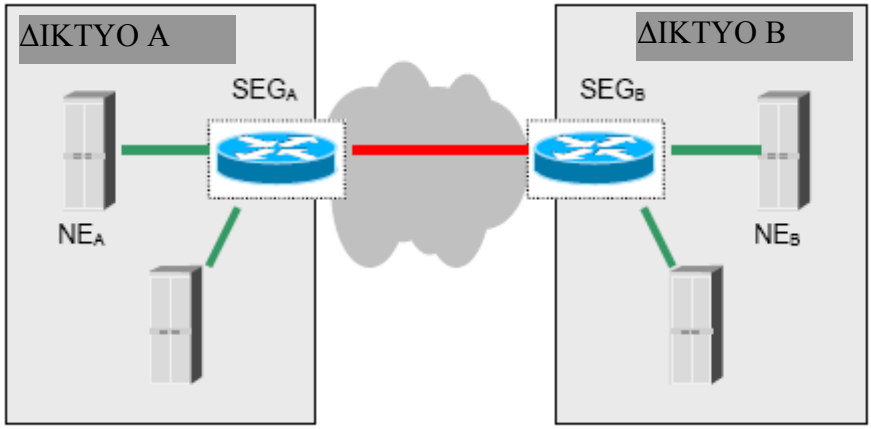
Protected Payload:

f6(Cleartext) || f7 (Security Header || f6(Cleartext))

Σε αυτήν τη μορφή εξασφαλίζεται η εμπιστευτικότητα με την εφαρμογή της συνάρτησης f7 στο καθαρό κείμενο.

3.2.2.2 IPSEC

Το πρωτόκολλο IPSEC είναι το βασικό εργαλείο για την προστασία της μετάδοσης δεδομένων στην περιοχή του δικτύου. Παρέχει εμπιστευτικότητα και ακεραιότητα στην επικοινωνία μεταξύ του ίδιου ή δυο διαφορετικών δικτύων στο IP layer. Επίσης, οι μηχανισμοί ασφάλειας του IPSEC δίνουν τη δυνατότητα στα στοιχεία που συμμετέχουν στην επικοινωνία να πιστοποιήσουν την αυθεντικότητά τους το ένα στο άλλο. [25]



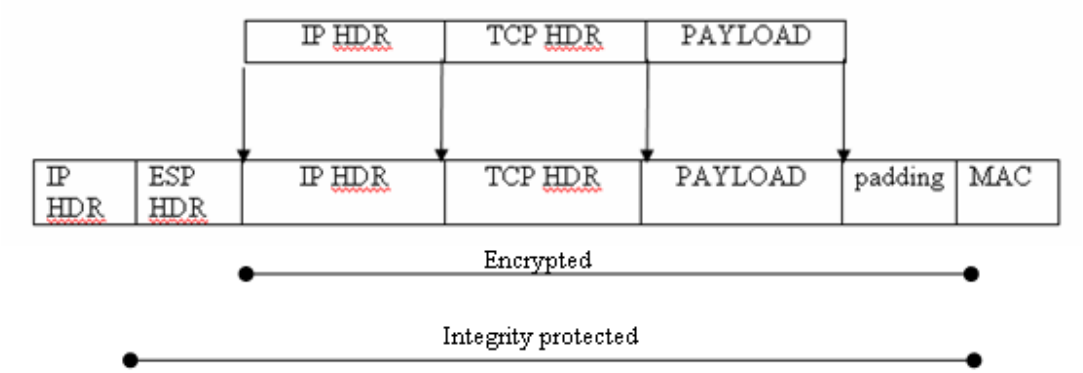
Σχήμα 29. Ασφάλεια περιοχής δικτύου για μηνύματα IP-based [27]

Για την παροχή ασφάλειας στα μηνύματα ελέγχου που αποτελούνται από πακέτα (IP-based), το πρωτόκολλο IPSEC υλοποιείται μεταξύ δύο κόμβων, έναν για κάθε δίκτυο, που λέγονται Security Gateways (SEG). Η λειτουργία των SEG είναι παρόμοια με αυτή των KACs, με τη διαφορά ότι οι SEG δεν διανέμουν τα SAs στα στοιχεία του δικτύου, αλλά διατηρούν μια βάση δεδομένων με τα SAs (SAD), καθώς και μια βάση δεδομένων με πληροφορίες για το πώς και σε ποιες περιπτώσεις πρέπει να χρησιμοποιηθούν (SPD). Έτσι, η επικοινωνία των δυο δικτύων γίνεται σ' αυτή την περίπτωση μέσω των SEG. Στο σχήμα 29, όταν κάποιο στοιχείο του δικτύου Α θέλει να στείλει ένα μήνυμα, το στέλνει στο SEG_A του δικτύου και το τελευταίο είναι υπεύθυνο να συμφωνήσει με το SEG_B για τα SAs που θα χρησιμοποιηθούν και, με βάση αυτά, να κρυπτογραφήσει τα μηνύματα που πρέπει να σταλούν.

Στο IPSEC, υπάρχουν πολλοί κανόνες και εξειδικεύσεις για τη χρήση τους. Για τη χρήση του πρωτοκόλλου αυτού στα κυρίως δίκτυα των UMTS δικτύων, χρησιμοποιούνται μόνο οι παρακάτω επιλογές:

- Προστασία των πακέτων με ESP σε tunnel mode.
- Ο αλγόριθμος κρυπτογράφησης είναι ο 3DES.
- Ο αλγόριθμος για την προστασία ακεραιότητας δεδομένων είναι ο SHA-1.
- Για την ανταλλαγή κλειδιών γίνεται χρήση του IKE.

Το ESP παρέχει εμπιστευτικότητα και προστασία ακεραιότητας στα μηνύματα ελέγχου. Η χρήση του σε tunnel mode σημαίνει ότι εισάγεται ένα νέο IP header στην αρχή του πακέτου. Όλο το μήνυμα κρυπτογραφείται. Επίσης, ένα ESP header προστίθεται μεταξύ του νέου IP header και του κρυπτογραφημένου μέρους και περιέχει πληροφορίες για το SA που χρησιμοποιείται. Στο τέλος του μηνύματος προστίθενται κάποια επιπλέον bits (padding), ενώ μια συνάρτηση MAC, που εξασφαλίζει την ακεραιότητα, εφαρμόζεται σε όλο το μήνυμα και το αποτέλεσμα της προστίθεται στο τέλος. Ο λήπτης αφού ελέγξει την ακεραιότητα, απομακρύνει τα πεδία IP HDR και MAC, υπολογίζει τη συνάρτηση MAC στο υπόλοιπο κομμάτι και το αποτέλεσμα συγκρίνεται με το MAC στο πακέτο. Αν το αποτέλεσμα του ελέγχου είναι θετικό αφαιρείται το ESP HDR και το υπόλοιπο αποκρυπτογραφείται.



Σχήμα 30. Δομή μηνυμάτων πρωτοκόλλου IPSEC. [25]

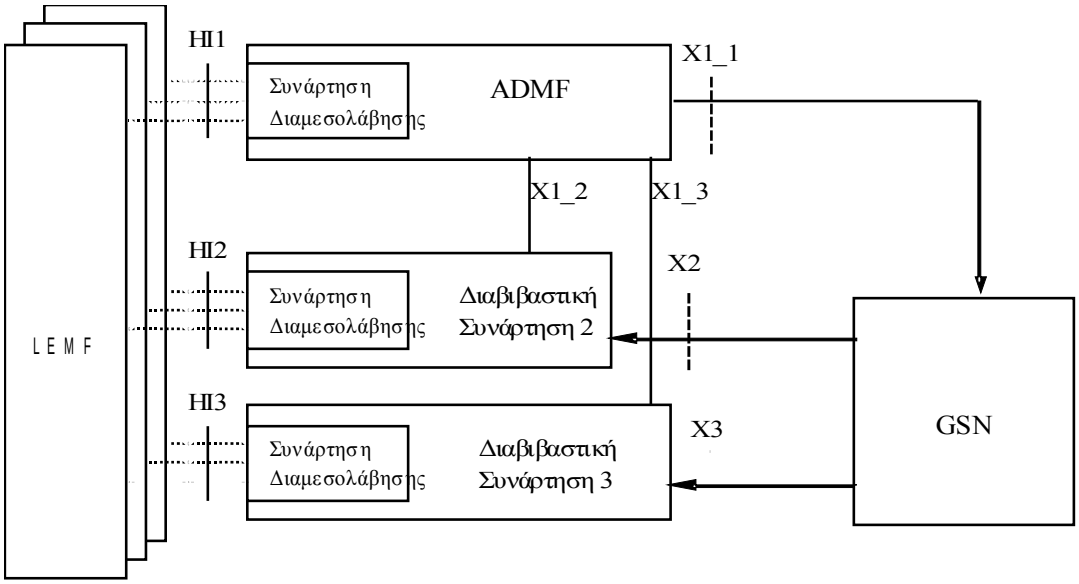
3.2.2.3 Σύστημα Νόμιμων Συνακροάσεων (Lawful Interception, LI)

Οι νομοθεσίες ορισμένων χωρών ή οργανισμών (π.χ. η Ευρωπαϊκή Ένωση) προβλέπουν την ανάγκη υποκλοπής δεδομένων ορισμένων συνδιαλέξεων που πραγματοποιούνται σε ένα δίκτυο κινητών τηλεπικοινωνιών. Η υποκλοπή ή συνακρόαση (interception) θα πρέπει να είναι σύμφωνη με την ισχύουσα νομοθεσία του γεωγραφικού τόπου, όπου λαμβάνει χώρα, έτσι ώστε να θεωρείται νόμιμη (lawful interception).

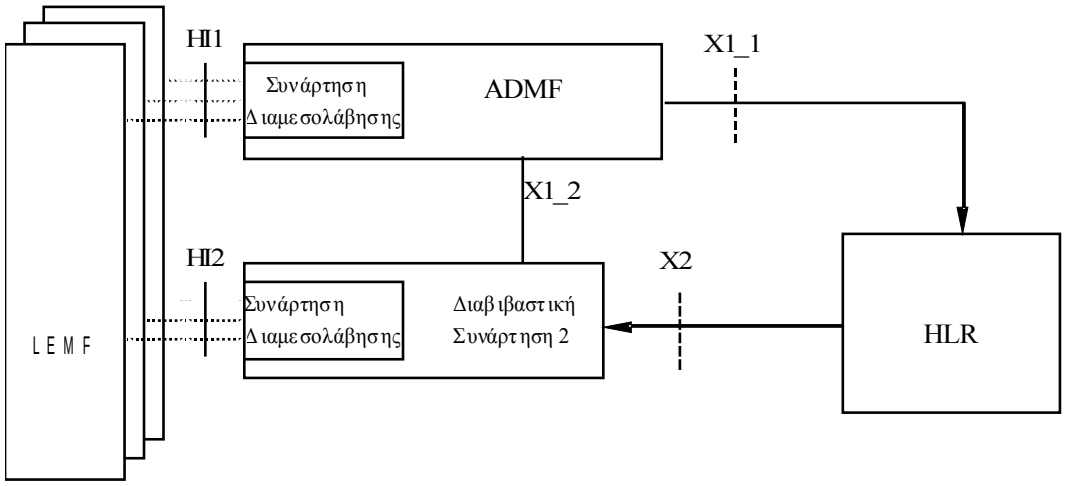
Η δυνατότητα νόμιμων συνακροάσεων δεν είχε προβλεφθεί κατά τη σχεδίαση του συστήματος GSM, αλλά προστέθηκε αργότερα σαν πρόσθετο χαρακτηριστικό με τη μορφή υλικολογισμικού (add-on). Αντίθετα, στο UMTS το υποσύστημα που θα υλοποιούσε τη συγκεκριμένη δυνατότητα σχεδιάστηκε από την αρχή.

Στην περίπτωση του UMTS, τα δεδομένα συνακρόασης (interception data) μπορεί να είναι δύο ειδών: δεδομένα που σχετίζονται με το περιεχόμενο μιας συνομιλίας του χρήστη-στόχου (Content of Communication, CC) και δεδομένα σηματοδοσίας που έχουν σχέση με τον χρήστη που παρακολουθείται (Intercept Related Information, IRI). Στην πρώτη κατηγορία ανήκουν και τα δεδομένα που μεταφέρονται μέσω γραπτών μηνυμάτων (SMS). Στη δεύτερη κατηγορία, τα δεδομένα που συνακροώνται μπορεί να φανερώνουν τη θέση που ο στόχος κινείται. Ο στόχος παρακολούθησης προσδιορίζεται συνήθως με βάση το IMSI ή άλλη ταυτότητα (π.χ το IMEI). [5]

Τα σχήματα που ακολουθούν περιγράφουν τη γενική αρχιτεκτονική του υποσυστήματος νόμιμων συνακροάσεων όταν το πρόκειται για δίκτυα μεταγωγής πακέτου (PS) (σχήμα 31) και όταν το στοιχείο δικτύου που εμπλέκεται είναι το HLR (σχήμα 32).



Σχήμα 31. Γενική LI αρχιτεκτονική για το PS domain.[28]



Σχήμα 32. Γενική LI αρχιτεκτονική για το HLR. [28]

Οι συναρτήσεις διαμεσολάβησης (mediation functions) μετατρέπουν τις πληροφορίες που μετβιβάζονται από τις διεπαφές HI1, HI2 και HI3 στη μορφή που περιγράφεται από τις εκάστοτε προδοαγραφές που ορίζονται από τις υπεύθυνες αρχές της κάθε χώρας. Οι διεπαφές HI1, HI2 και HI3 υφίστανται μεταξύ των συναρτήσεων αυτών και των υπηρεσιών επιβολής του νόμου (Law Enforcement Agencies, LEAs). Οι πληροφορίες για τα LEAs μπορεί να συγκεντρώνονται σε κάποιο κέντρο παρακολούθησης για την επιβολή του νόμου (Law Enforcement

Monitoring Facility, LEMF). Όταν κάποια LEA επιθυμεί να ξεκινήσει μια διαδικασία LI στέλνει, μέσω της διεπαφής HI1, ένα αίτημα στο κέντρο διαχείρισης νόμιμων συνακροάσεων (Administration Function, ADMF). Το τελευταίο συνδέεται τόσο με τα LEAs όσο και με το δίκτυο, μέσω της διεπαφής X1_1, και είναι υπεύθυνο για το διαχωρισμό των δραστηριοτήτων LI που μπορεί να πραγματοποιούν διαφορετικά LEAs την ίδια στιγμή. Σημειώνεται ότι κάθε δίκτυο παρόχου υπηρεσιών διαθέτει μόνο ένα τέτοιο κέντρο. Το ADMF με τη σειρά του, ενημερώνει τα στοιχεία του δικτύου που εμπλέκονται (π.χ. GSN) στέλνοντάς τους την ταυτότητα του χρήστη που παρακολουθείται και ενεργοποιεί τις διαβιβαστικές συναρτήσεις DF2 και DF3 (Delivery Functions). Οι συναρτήσεις αυτές είναι υπεύθυνες για τη μεταβίβαση των δεδομένων IRI μέσω της διεπαφής HI2 και των δεδομένων CC μέσω της διεπαφής HI3 στο LEMF, αντίστοιχα, ενώ η επικονωνία μεταξύ αυτών και του ADMF γίνεται μέσω των διεπαφών X1_2 και X1_3 (σχήμα 34). Στην περίπτωση του HLR, μπορεί να αποσταλούν μόνο IRI δεδομένα, όπως φαίνεται και στο σχήμα 35. Τα στοιχεία του δικτύου κορμού που μπορεί να συμμετέχουν στο σύστημα LI μπορεί να είναι τα παρακάτω: 3G MSC, 3G GMSC, SGSN, GGSN, HLR, καθένα από τα οποία έχει τη δική του ξεχωριστή διεπαφή X1_1 με το ADMF.

3.2.3 Ασφάλεια της Περιοχής του Χρηστη (User Domain Security)

3.2.3.1. Αυθεντικοποίηση Χρήστη στη USIM

Αυτός ο μηχανισμός παρέχει προστασία της κάρτας USIM ενός νόμιμου συνδρομητή από μη εξουσιοδοτημένους χρήστες. Πρόσβαση στην USIM, η οποία περιέχει τα προσωπικά δεδομένα του χρήστη, πρέπει να έχει μόνο ο νόμιμος κάτοχός της. Για το σκοπό αυτό, χρήστης και USIM μοιράζονται έναν μυστικό κωδικό (PIN), που αποθηκεύεται ασφαλώς στην κάρτα και που πρέπει να πληκτρολογήσει ο χρήστης κάθε φορά που ζητά πρόσβαση στην κάρτα μέσω του κινητού. Ο συγκεκριμένος μηχανισμός είναι ο ίδιος με αυτόν που υπάρχει και στο GSM.

3.2.3.2 Σύνδεση USIM - Συσκευής

Ο συγκεκριμένος μηχανισμός εξασφαλίζει ότι η πρόσβαση σε μια συσκευή αποτρέπεται στην περίπτωση που ζητηθεί από μη εξουσιοδοτημένη USIM. Για το σκοπό αυτό, USIM και συσκευή έχουν αποθηκευμένο έναν μυστικό κωδικό. Αν μια USIM δεν δώσει το σωστό κωδικό, θα απαγορευτεί η πρόσβαση της στη συσκευή. Ο μηχανισμός, που είναι ίδιος με τον αντίστοιχο στο GSM, είναι γνωστός και ως "SIM-lock".

3.2.4 Ασφάλεια της Περιοχής Εφαρμογών (Application Domain Security)

Η ασφάλεια στην περιοχή εφαρμογών αναφέρεται στην προστασία των μηνυμάτων που μεταφέρονται στις εφαρμογές της USIM από το δίκτυο. Το "USIM Application Toolkit" είναι μια υπηρεσία της κάρτας USIM που δίνει στους παρόχους τη δυνατότητα να δημιουργούν εφαρμογές που μπορούν να εγκατασταθούν στη USIM. Τα μηνύματα που προορίζονται για τις εφαρμογές της USIM πρέπει να μεταφέρονται με ασφάλεια, το επίπεδο της οποίας καθορίζει κάθε φορά ο πάροχος. Θα πρέπει, πάντως να εξασφαλίζονται κάποιες απαιτήσεις, οι οποίες είναι:

- Η αυθεντικοποίηση της οντότητας των εφαρμογών: δύο εφαρμογές που «συνομιλούν» θα πρέπει να μπορούν να επιβεβαιώνουν η μια την ταυτότητα της άλλης.
- Η αυθεντικοποίηση της προέλευσης των δεδομένων: η εφαρμογή που δέχεται δεδομένα θα πρέπει να μπορεί να πιστοποιήσει την προέλευσή τους.
- Η ακεραιότητα των δεδομένων των εφαρμογών: η εφαρμογή που δέχεται δεδομένα θα πρέπει να μπορεί να διαπιστώσει ότι τα δεδομένα που έλαβε δεν αλλοιώθηκαν ή τροποποιήθηκαν.
- Ανίχνευση επανάληψης των δεδομένων: μια εφαρμογή θα πρέπει να μπορεί να διαπιστώσει αν τα δεδομένα που δέχεται επαναλαμβάνονται.

- Ακεραιότητα της αλληλουχίας των δεδομένων: μια εφαρμογή θα πρέπει να μπορεί να διαπιστώσει ότι τα δεδομένα που δέχεται έρχονται με τη σωστή ακολουθία.
- Απόδειξη παραλαβής: η εφαρμογή που έχει στείλει δεδομένα θα πρέπει να μπορεί να αποδείξει ότι τα δεδομένα αυτά παρελήφθησαν από την εφαρμογή στην οποία τα έστειλε.
- Εμπιστευτικότητα των δεδομένων: τα δεδομένα των εφαρμογών δε θα πρέπει να αποκαλύπτονται από μη εξουσιοδοτημένες οντότητες.

3.2.5 Διαφάνεια και Διαμόρφωση της Ασφάλειας (Visibility and Configurability of the Security)

Αν και γενικά τα χαρακτηριστικά γνωρίσματα ασφάλειας πρέπει να μην είναι ορατά στο χρήστη, για ορισμένα γεγονότα και σύμφωνα με το ενδιαφέρον του χρήστη, πρέπει να παρασχεθεί μεγαλύτερη διαφάνεια στη λειτουργία των χαρακτηριστικών γνωρισμάτων ασφάλειας. Στο πλαίσιο αυτό, υπάρχει ένας ενδείκτης κρυπτογράφησης, που πληροφορεί το χρήστη για το αν προστατεύεται η εμπιστευτικότητα των δεδομένων στη ραδιοζεύξη, π.χ. στην περίπτωση κλήσεων χωρίς κρυπτογράφηση. Επίσης, υπάρχει ένας ενδείκτης για το επίπεδο της ασφάλειας του δικτύου που εξυπηρετεί μια χρονική στιγμή τον χρήστη, π.χ. τον πληροφορεί όταν μετακινείται σε ένα δίκτυο με χαμηλότερη ασφάλεια (3G→2G).

Επιπρόσθετα, δίνεται η δυνατότητα στο χρήστη να διαμορφώσει ο ίδιος κάποια χαρακτηριστικά των μηχανισμών ασφάλειας. Τα χαρακτηριστικά αυτά είναι:

- Ενεργοποίηση / απενεργοποίηση user – USIM αυθεντικοποίησης
- Αποδοχή / απόρριψη εισερχόμενων μη κρυπτογραφημένων κλήσεων.
- Εγκατάσταση ή μη εγκατάσταση μη κρυπτογραφημένων κλήσεων.
- Αποδοχή / απόρριψη χρήσης συγκεκριμένων αλγόριθμων κρυπτογράφησης.

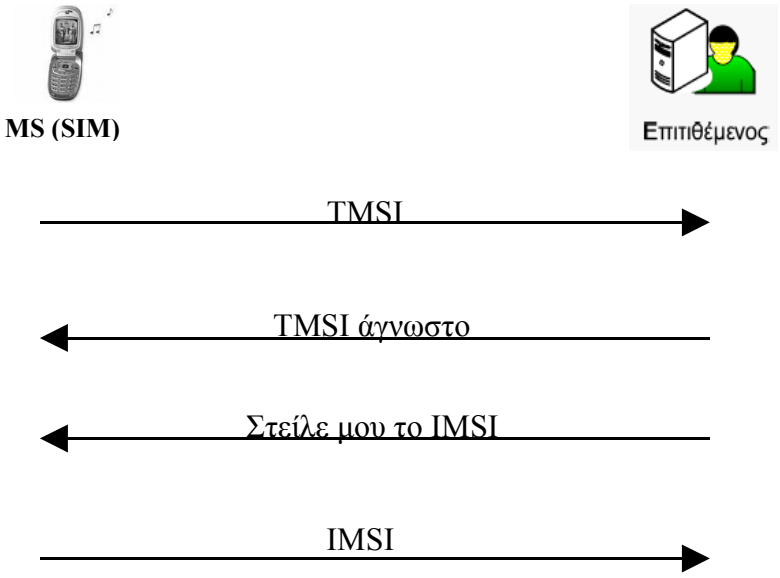
3.3 Αξιολόγηση των Μηχανισμών Ασφάλειας

3.3.1 Αξιολόγηση του Μηχανισμού Εμπιστευτικότητας της Ταυτότητας Χρήστη

Στην παράγραφο 3.2.1.3 έγινε αναφορά στην προστασία της μόνιμης ταυτότητας του συνδρομητή με τη χρήση του μηχανισμού των προσωρινών ταυτοτήτων (TMSI), την οποία ο χρήστης αποστέλλει στο δίκτυο, προκειμένου να αυθεντικοποιηθεί. Ωστόσο, υπάρχουν περιπτώσεις, στις οποίες χρειάζεται να γίνει αποστολή του IMSI από το χρήστη, και μάλιστα σε μορφή καθαρού κειμένου (cleartext), για να δηλώσει την ταυτότητά του. Οι περιπτώσεις αυτές είναι:
α) Όταν ο χρήστης εγγράφεται για πρώτη φορά στο δίκτυο ή μετά από μεγάλο διάστημα κατά το οποίο διατηρούσε κλειστή τη συσκευή του.
β) Όταν το δίκτυο εξυπηρέτησης (SN) δεν μπορεί να τον αναγνωρίσει μέσω της προσωρινής του ταυτότητας, π.χ σε περιπτώσεις μεταβίβασης κλήσης σε νέα κυψέλη, που εξυπηρετείται από διαφορετικό VLR/SGSN, το οποίο είτε δε μπορεί να αναγνωρίσει τη διεύθυνση του προηγούμενου VLR/SGSN που του μεταβιβάζει τη συσχέτιση {IMSI, TMSI} για τον συγκεκριμένο χρήστη είτε δεν είναι δυνατή η επικοινωνία μαζί του.
γ) Όταν έχει συμβεί κάποιο σφάλμα ή βλάβη στη βάση δεδομένων ενός VLR/SGSN.

Στις παραπάνω περιπτώσεις, η μετάδοση του IMSI του χρήστη προς το δίκτυο σε μη κρυπτογραφημένη μορφή εγκυμονεί κινδύνους για την εμπιστευτικότητα της ταυτότητάς του και της θέσης στην οποία αυτός κινείται. Ένας επιτιθέμενος, πραγματοποιώντας μια παθητική επίθεση (passive attack) τύπου man-in-the-middle, μπορεί να παρεμβληθεί μεταξύ χρήστη και δικτύου και να κρυφακούσει το εκπεμπόμενο IMSI, το οποίο μπορεί στη συνέχεια να χρησιμοποιήσει για να πλαστογραφήσει στην ταυτότητά του και να πραγματοποιήσει επιθέσεις «άρνησης υπηρεσίας» (DoS attacks) προκαλώντας αναστάτωση στο δίκτυο. Επίσης, στην περίπτωση των ενεργών επιθέσεων (active attacks), ένας επιτιθέμενος είναι δυνατόν να προσποιηθεί ένα ψεύτικο σταθμό βάσης (false base station - RNC attack), με το

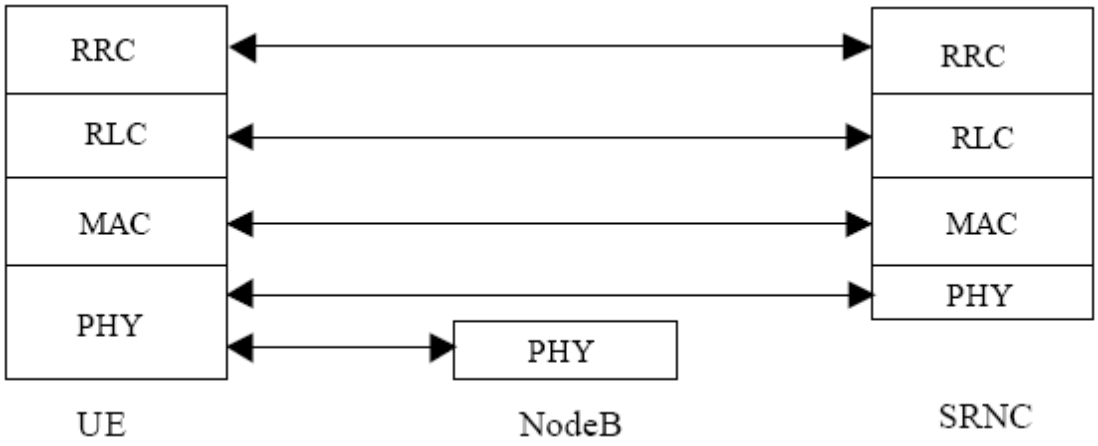
οποίο να παγιδεύσει το χρήστη και να του ζητήσει να του αποστείλει τη μόνιμη ταυτότητά του για να τον αναγνωρίσει, όπως περιγράφεται στο σχήμα 33.



Σχήμα 33. Ενεργή επίθεση για την απόκτηση του IMSI [5]

3.3.2 Αξιολόγηση του Μηχανισμού Εμπιστευτικότητας Δεδομενων Χρήστη

Ο συγκεκριμένος μηχανισμός κρυπτογράφησης στο UMTS εφαρμόζεται σε όλα τα μεταφερόμενα δεδομένα του συνδρομητή και στα δεδομένα σηματοδοσίας και λαμβάνει χώρα στο επίπεδο MAC ή στο επίπεδο RLC (Σχήμα 34). Η προστασία της εμπιστευτικότητας των δεδομένων που εξασφαλίζει ο μηχανισμός αυτός κρίνεται αποτελεσματικότερος από τον αντίστοιχο που εφαρμόζεται στα δίκτυα GSM. Στα δίκτυα GSM η κρυπτογράφηση γινόταν μεταξύ της κινητής συσκευής και του σταθμού βάσης του (BTS), με αποτέλεσμα η διαδρομή από το σταθμό βάσης μέχρι το BSC (το αντίστοιχο RNC του UMTS) να είναι μη ασφαλής για την εμπιστευτικότητα των δεδομένων. Αντίθετα, η διαδικασία της κρυπτογράφησης στο UMTS υλοποιείται από τη συσκευή του χρήστη μέχρι το RNC, καλύπτοντας έτσι το σχετικό κενό στην ασφάλεια.



Σχήμα 34. Τα πρωτόκολλα μεταξύ κινητού εξοπλισμού (UE) και RNC [25]

Όπως περιγράφηκε, το κλειδί κρυπτογράφησης CK μεταφέρεται από το VLR/SGSN του δικτύου που εξυπηρετεί το χρήστη (SN) στο RNC αμέσως μετά την διαδικασία αυθεντικοποίησης του χρήστη και την απόφαση από το VLR/SGSN για τους επιτρεπόμενους αλγόριθμους κρυπτογράφησης και ακεραιότητας, με την εντολή security mode command. Παράλληλα, με την ίδια εντολή μεταβιβάζεται και το κλειδί για την ακεραιότητα (IK). Η εντολή αυτή δεν προστατεύεται με κρυπτογράφηση, καθώς αυτή ξεκινάει αργότερα, όπως φαίνεται στο Σχήμα 28. Επομένως, τα κλειδιά μεταφέρονται «καθαρά» από το VLR/SGSN στο RNC, γεγονός που συνιστά κίνδυνο για πιθανή υποκλοπή και χρησιμοποίησή τους από επιτιθέμενους.

Άλλο ένα σημείο αναφοράς είναι το γεγονός ότι για την κρυπτογράφηση καθενός από τα πακέτα που συνθέτουν τα μεταδιδόμενα δεδομένα χρησιμοποιείται κάθε φορά άλλη «μάσκα» κρυπτογράφησης. Αυτό εξασφαλίζεται από την παρουσία στη συνάρτηση f8 της παραμέτρου COUNT-C, που εμπεριέχει τον μετρητή HFN, ο οποίος αυξάνεται μετά από κάθε πακέτο. Το γεγονός αυτό με τη σειρά του εξασφαλίζει ότι δε θα χρησιμοποιηθεί η ίδια «μάσκα» για την κρυπτογράφηση δυο διαφορετικών πακέτων δεδομένων. Σε αντίθετη περίπτωση το XOR άθροισμα δύο πακέτων P1, P2 θα ήταν ίσο με το άθροισμα των αντίστοιχων κρυπτογραφημένων κειμένων τους, λόγω του ότι το άθροισμα δύο ίδιων keystream blocks είναι μηδέν. Για κάποιον ο οποίος υποκλέπτει τα κρυπτογραφημένα blocks στη ραδιοζεύξη, θα

ήταν εύκολο να αποκαλύψει τα δύο πακέτα P1 και P2, γνωρίζοντας το άθροισμά τους.

Η χρήση της κρυπτογράφησης στο UMTS αν και προτείνεται δεν είναι απαραίτητη, πράγμα που σημαίνει ότι μπορεί να γίνει επικοινωνία μεταξύ χρήστη και δικτύου χωρίς τη χρήση κρυπτογραφικών μηχανισμών. Αυτό συμβαίνει στην περίπτωση που το δίκτυο διαπιστώσει ότι δεν υπάρχουν κοινοί αλγόριθμοι κρυπτογράφησης ανάμεσα σε αυτούς που υποστηρίζει το δίκτυο και σε αυτούς που διαθέτει η συσκευή του χρήστη, για τους οποίους έχει ενημερώσει το δίκτυο δηλώνοντας σε αυτό το classmark της συσκευής. Σε αυτήν την περίπτωση είναι προφανές ότι ένας μη εξουσιοδοτημένος χρήστης μπορεί να παρεμβληθεί και να υποκλέψει τα μηνύματα που ανταλλάσσονται χωρίς κρυπτογράφηση.

3.3.3 Αξιολόγηση του Μηχανισμού Ακεραιότητας Δεδομένων Σηματοδοσίας

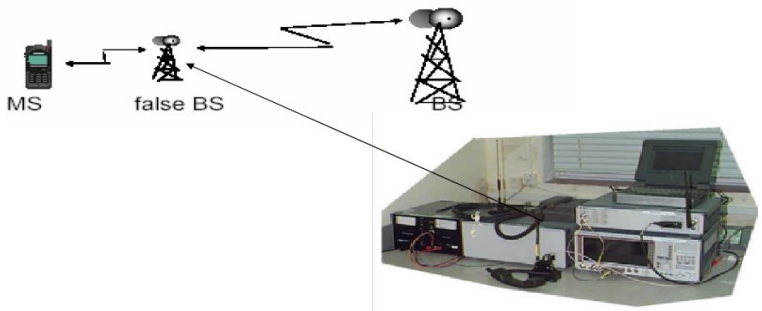
Ο συγκεκριμένος μηχανισμός αποτελεί μια καινοτομία για τα δίκτυα UMTS, καθώς, όπως έχει αναφερθεί δεν υφίστατο αντίστοιχος μηχανισμός στα δίκτυα GSM. Τα σημεία που θα πρέπει να επισημανθούν είναι τα παρακάτω:

- Η προστασία της ακεραιότητας είναι εγγυημένη μόνο για τη σηματοδοσία μεταξύ κινητού σταθμού και RNC. Στα δεδομένα των χρηστών δεν εφαρμόζεται ο μηχανισμός της ακεραιότητας για λόγους απόδοσης και γι' αυτό το λόγο παραμένουν ευαίσθητα σε παραποιήσεις. Ωστόσο, υπάρχει μια συγκεκριμένη διαδικασία που καλείται περιοδική αυθεντικοποίηση (periodic authentication), μέσω της οποίας ελέγχεται η ποσότητα των δεδομένων που στάλθηκαν κατά τη διάρκεια μιας κλήσης. Έτσι, τα δεδομένα των χρηστών προστατεύονται περιοδικά σε ότι αφορά το μέγεθός τους, γεγονός που εμποδίζει επιτιθέμενους να εισάγουν ή να διαγράψουν πακέτα δεδομένων που αποστέλλονται είτε προς τον κινητό σταθμό είτε προς το δίκτυο. Βεβαίως, μπορεί κάποιος επιτιθέμενος να μην γίνει αντιληπτός αν προσπαθήσει να εισάγει ή να διαγράψει τον ίδιο ακριβώς αριθμό πακέτων. [5]

- Οι παράμετροι COUNT-I και FRESH αποτρέπουν την περίπτωση να αναμεταδοθεί το ίδιο MAC-I από το δίκτυο ή από το χρήστη, προστατεύοντας έτσι από «επιθέσεις επανάληψης» (replay attacks). [23]
- Όπως αναφέρθηκε στην προηγούμενη παράγραφο, τα κλειδιά ακεραιότητας μεταβιβάζονται χωρίς κρυπτογράφηση από το VLR/SGSN, όπου και δημιουργούνται, στο RNC που θα εξυπηρετήσει το συνδρομητή.
- Τέλος, θα πρέπει να επισημανθεί ότι αν ένας χρήστης διατηρεί συνδέσεις και στην CS και στην PS περιοχή του κυρίως δικτύου (CN), αυτό σημαίνει ότι έχει αυθεντικοποιηθεί ανεξάρτητα και στις δύο περιοχές. Άρα, διατηρεί διαφορετικά IK κλειδιά για κάθε περιοχή. [23]

3.3.4 Γενική Αξιολόγηση στους Μηχανισμούς Ασφάλειας στο Δικτυο Προόσβασης

Προκειμένου κάποιος μη εξουσιοδοτημένος χρήστης να πραγματοποιήσει ένα είδος «επίθεσης» εναντίον ενός νόμιμου συνδρομητή του δικτύου UMTS, θα πρέπει να προσποιηθεί ότι είναι ένας νόμιμος σταθμός βάσης του δικτύου. Η επίθεση αυτή είναι γνωστή ως “man-in-the-middle attack” και μια μορφή της απεικονίζεται στο σχήμα 35.



Σχήμα 35. ‘Man-in-the-middle active attack’ με τη χρήση ψεύτικου BS [9]

Στην περίπτωση αυτή ο «επιτιθέμενος» προσπαθεί να υποκλέψει τα μηνύματα που ανταλλάσουν ο χρήστης και το δίκτυο και να τα ιδιοποιηθεί. Ωστόσο, η αρχιτεκτονική ασφάλειας του UMTS προσφέρει ικανοποιητική προστασία από τέτοιου είδους επιθέσεις με το συνδυασμό των μηχανισμών αυθεντικοποίησης και ακεραιότητας. Συγκεκριμένα, η παράμετρος AUTN που παράγεται κατά την

εκτέλεση της διαδικασίας AKA, περιέχει έναν αύξοντα αριθμό SQN, καθώς και μια παράμετρο MAC. Όταν η κινητή μονάδα λάβει το AUTN, ελέγχει το MAC και διαπιστώνει αν, για την παραγωγή του, χρησιμοποιήθηκε το ίδιο μυστικό κλειδί K που έχει αποθηκευμένο. Στην περίπτωση αυτή, αυτό σημαίνει ότι προήλθε από το δικό της οικείο δίκτυο (δηλ. το AuC του δικού της δικτύου). Στη συνέχεια, ελέγχει αν το SQN που έλαβε ανήκει στο αναμενόμενο πεδίο τιμών. Αν ναι, τότε σημαίνει ότι το AUTN παράχθηκε πρόσφατα από το οικείο δίκτυο. Αν αυτό δεν συμβαίνει σημαίνει ότι είναι επανάληψη ενός παλιού SQN, που πιθανώς να έχει υποκλαπεί ή ότι πρόκειται για σφάλμα συγχρονισμού μεταξύ των δύο πλευρών.

Βέβαια, η αυθεντικοποίηση της εγκυρότητας των παραμέτρων AUTN και MAC δεν προστατεύει απόλυτα τον χρήστη από τον κίνδυνο να μην προήλθαν απ' ευθείας από το νόμιμο δίκτυο αλλά να αποτελούν αναμετάδοση ενός μη εξουσιοδοτημένου σταθμού βάσης. Όμως, ο μηχανισμός που εγγυάται την ακεραιότητα των δεδομένων (σηματοδοσίας) αποτρέπει τον επιτιθέμενο να έχει κάποιο όφελος από αυτήν την επίθεση. Στο βήμα 5 της διαδικασίας που περιγράφεται στην παράγραφο 3.2.1.6, το RNC στέλνει ένα μήνυμα στο χρήστη το οποίο:

- είναι προστατευμένης ακεραιότητας διότι παράχθηκε μέσω του αλγόριθμου f9 και του ίδιου κλειδιού IK, που υπάρχει και στην κινητή μονάδα,
- περιέχει όλους τους μηχανισμούς ασφάλειας που είχε πληροφορήσει η κινητή μονάδα ότι διαθέτει, μέσω του μηνύματος που απέστειλε αρχικά στο σταθμό βάσης για την εγκατάσταση RRC σύνδεσης.

Έτσι, η κινητή μονάδα ελέγχοντας την ακεραιότητα αυτού του μηνύματος σιγουρεύεται ότι αυτό προήλθε από ένα δίκτυο που έχει στην κατοχή του το ίδιο κλειδί ακεραιότητας IK. Επίσης, ελέγχει αν οι μηχανισμοί ασφάλειας (αλγόριθμοι) είναι οι ίδιοι με αυτούς που είχε στείλει στην αρχή της διαδικασίας στο RNC. Έτσι, ο επιτιθέμενος δεν μπορεί να ξεγελάσει τις δύο πλευρές να χρησιμοποιήσουν καθόλου ή αδύναμη κρυπτογράφηση, ούτως ώστε να υποκλέψει εύκολα τα μηνύματα που ακολουθούν. Αν αυτές οι δυνατότητες κρυπτογράφησης της συσκευής δεν εσωκλείονταν στο μήνυμα του RNC, θα μπορούσε, αφού είχε υποκλέψει το μήνυμα αίτησης για RRC σύνδεση (RRC connection request) – που δεν είναι

προστατευμένης ακεραιότητας – να ζητήσει από το δίκτυο, ως νόμιμος χρήστης, να μην χρησιμοποιηθεί κρυπτογράφηση, αποκρύβοντας έτσι τις πραγματικές δυνατότητες τις συσκευής, και μετά να ενημερώσει τον νόμιμο χρήστη για τη μη χρήση κρυπτογράφησης. Σημειώνεται, ότι αν και δεν υπάρχουν μέθοδοι που να αποτρέπουν τέτοιες επιθέσεις, εν τούτοις, όπως ειπώθηκε, δεν αποκομίζεται κάποιο ουσιαστικό όφελος για τον επιτιθέμενο.

Τέλος, μια αδυναμία του μηχανισμού αυθεντικοποίησης προέρχεται από το γεγονός ότι επιτιθέμενοι που εφαρμόζουν παθητικές ή ενεργητικές μεθόδους, μπορούν να υποκλέψουν διανύσματα αυθεντικοποίησης είτε από τα SGSN, HLR είτε από το δίαυλο επικοινωνίας μεταξύ αυτών. Συγκεκριμένα, όταν ένας χρήστης περιάγεται μεταξύ διαφορετικών δικτύων, το HN θα πρέπει να αποστείλει στο SN διανύσματα αυθεντικοποίησης έτσι ώστε το τελευταίο να μπορέσει να αυθεντικοποιήσει το συνδρομητή. Στις περιπτώσεις αυτές τα διανύσματα μεταφέρονται μεταξύ διαφορετικών παρόχων, που μπορεί να εφαρμόζουν διαφορετικές πολιτικές ασφαλείας, και έτσι είναι πιθανότερο να υποκλαπούν ή να καταστραφούν. [5]

3.4 Συμπεράσματα

Ανακεφαλαιώνοντας, το UMTS κληρονομεί τα περισσότερα βασικά χαρακτηριστικά ασφάλειας των δικτύων GSM, υιοθετώντας όμως και κάποιες νέες πρακτικές, όπως η αμοιβαία αυθεντικοποίηση μεταξύ χρηστών και δικτύου και η προστασία της ακεραιότητας των δεδομένων σηματοδοσίας. Γενικά, το UMTS προσφέρει μεγαλύτερη ασφάλεια στους συνδρομητές σε σχέση με τα δίκτυα δεύτερης γενιάς (GSM/GPRS), κλείνοντας τα πιο σημαντικά κενά ασφάλειας, χωρίς όμως να αποτρέπονται ολοκληρωτικά οι επιθέσεις μέσω ψεύτικων σταθμών βάσης. Επίσης, οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται στο UMTS είναι πλέον γνωστοί, και όχι μυστικοί, πράγμα που επιτρέπει τον εντοπισμό των αδυναμιών τους και την πρόληψη των κινδύνων από το «σπάσιμό» τους. Τέλος, η ασφάλεια που παρέχεται εντός του κυρίως δικτύου, με μηχανισμούς που βασίζονται στα πρωτόκολλα MAPSEC και IPSEC, χαρακτηρίζεται γενικά επαρκής, ωστόσο νέα χαρακτηριστικά ασφάλειας θα πρέπει να καθιερωθούν καθώς οι δυνατότητες και οι

υπηρεσίες των κινητών τηλεφώνων 3ης γενιάς επεκτείνονται ολοένα και περισσότερο.

ΚΕΦΑΛΑΙΟ 4

ΤΕΧΝΙΚΕΣ ΕΠΙΘΕΣΕΩΝ

4.1 Είδη επιθέσεων

Οι μηχανισμοί ασφαλείας που καθορίζονται για τα δίκτυα τηλεπικοινωνιών 2ης γενιάς έχουν σκοπό να προστατεύσουν το δίκτυο και το χρήστη από επιθέσεις που μπορούν να διακυβεύσουν τα ευαίσθητα προσωπικά δεδομένα του χρήστη αλλά και τα δεδομένα σηματοδοσίας, καθώς και την αξιοπιστία των ραδιο-ζεύξεων. Οι επιθέσεις αυτές πιστεύεται ότι σήμερα ή στο εγγύς μέλλον είναι πιο πιθανές λόγω του ότι οι πιθανοί εισβολείς έχουν πλέον στη διάθεσή τους περισσότερα μέσα, ικανότητες και εξοπλισμό για να τις υλοποιήσουν. Οι επιθέσεις αυτές θα ήταν δυνατόν να διακριθούν στις εξής κατηγορίες [29] [30]:

1. Επιθέσεις άρνησης υπηρεσίας
2. Επιθέσεις υποκλοπής της ταυτότητας του χρήστη
3. Επιθέσεις προσωποποίησης του δικτύου
4. Επιθέσεις προσωποποίησης του χρήστη
5. Επιθέσεις κρυφακούσματος των δεδομένων του χρήστη

4.1.1 Επιθέσεις άρνησης υπηρεσίας

Οι επιθέσεις αυτές έχουν σαν αποτέλεσμα την άρνηση παροχής υπηρεσιών ενός δικτύου σε ένα νόμιμο χρήστη. Μπορούμε να διακρίνουμε τις παρακάτω παραλλαγές:

1. Πλαστογράφηση μηνύματος αποσύνδεσης από το δίκτυο

Στην επίθεση αυτή ο επιτιθέμενος πλαστογραφεί ένα μήνυμα αποσύνδεσης από το δίκτυο (IMSI-detach) και το αποστέλλει στο νόμιμο δίκτυο του συνδρομητή. Έτσι,

το νόμιμο δίκτυο διαγράφει το χρήστη από τη λίστα των συνδεδεμένων χρηστών του VLR και δίνει οδηγία στο HLR να κάνει το ίδιο, με αποτέλεσμα ο χρήστης να μην έχει πλέον πρόσβαση στις υπηρεσίες του δικτύου του.

2. Πλαστογράφηση αίτησης ανανέωσης θέσης

Ο επιτιθέμενος πλαστογραφεί και στέλνει στο δίκτυο μια αίτηση ανανέωσης θέσης σε μια διαφορετική περιοχή από αυτήν που περιάγεται ο νόμιμος χρήστης. Το δίκτυο καταχωρεί τον χρήστη σε αυτήν την νέα περιοχή, και, συνεπώς, ο χρήστης δε μπορεί πλέον να έχει πρόσβαση στις παρεχόμενες υπηρεσίες του δικτύου του.

3. Παγίδευση σε ψεύτικο σταθμό βάσης (BTS)

Στην επίθεση αυτή ο συνδρομητής συνδέεται με έναν ψεύτικο σταθμό βάσης (false BS, σχήμα 36), που έχει δημιουργήσει ο επιτιθέμενος, με αποτέλεσμα να μη λαμβάνει πλέον τα ραδιο-σήματα του νόμιμου δικτύου στο οποίο είναι καταχωρημένος. Η επίθεση αυτή διαρκεί για όσο χρονικό διάστημα ο επιτιθέμενος είναι ενεργός. Σε μια άλλη παραλλαγή αυτής της επίθεσης, ο επιτιθέμενος μπορεί, υλοποιώντας ένα τροποποιημένο σταθμό βάσης σε συνδυασμό με ένα τροποποιημένο κινητό σταθμό, να δρα σαν ενδιάμεσος μεταξύ του χρήστη και του νόμιμου δικτύου και να αναμεταδίδει τα μηνύματα που ανταλλάσσουν, αλλά και να μεταβάλλει ή να αγνοεί το περιεχόμενο συγκεκριμένων αιτήσεων για παροχή υπηρεσιών στο χρήστη.

Σχήμα 36. Ψεύτικος σταθμός βάσης (BTS)

Σημειώνεται ότι ο μηχανισμός προστασίας της ακεραιότητας των μηνυμάτων σηματοδοσίας που προβλέπεται στον αρχιτεκτονικό σχεδιασμό της ασφάλειας στα δίκτυα τρίτης γενιάς αποτρέπει τις δυο πρώτες παραλλαγές των επιθέσεων άρνησης υπηρεσίας. Το δίκτυο εξυπηρέτησης είναι σε θέση να επιβεβαιώσει την εγκυρότητα τόσο ενός μηνύματος αποσύνδεσης όσο και μιας αίτησης για ανανέωση της θέσης του συνδρομητή. Δεν είναι δυνατόν, όμως, να αποτραπεί εντελώς το ενδεχόμενο ένας χρήστης να παγιδευτεί και να συνδεθεί σε ένα ψεύτικο σταθμό βάσης. Ωστόσο, η προστασία της ακεραιότητας σε κρίσιμα δεδομένα σηματοδοσίας μπορεί να εμποδίσει τέτοιου είδους επιθέσεις.

4.1.2 Επιθέσεις υποκλοπής της ταυτότητας του χρήστη

Οι επιθέσεις που μπορούν να πλήξουν την εμπιστευτικότητα της ταυτότητας του συνδρομητή διακρίνονται σε παθητικές και ενεργητικές. Μια παθητική επίθεση πραγματοποιείται με τη βοήθεια ενός τροποποιημένου κινητού σταθμού και αποσκοπεί στην υποκλοπή (κρυφάκουσμα) της ταυτότητας του συνδρομητή όταν το δίκτυο απαιτεί σε κάποιες περιπτώσεις από το συνδρομητή του να στείλει την ταυτότητά του σε μορφή καθαρού κειμένου. Αντίθετα, μια ενεργή επίθεση απαιτεί έναν τροποποιημένο (ψεύτικο) σταθμό βάσης για την υλοποίησή της και βασίζεται στο γεγονός ότι όταν ο συνδρομητής δεν είναι δυνατόν να αναγνωριστεί μέσω της προσωρινής του ταυτότητας ή όταν παρουσιαστεί μια βλάβη στη βάση δεδομένων του VLR, καλείται από το δίκτυο να αποστείλει τη μόνιμη ταυτότητά του (IMSI). Ένας ψεύτικος σταθμός βάσης που έχει παγιδεύσει έναν συνδρομητή του ζητά να αποστείλει τη μόνιμη ταυτότητά του για να τον αναγνωρίσει, στέλνοντας του ένα αίτημα ταυτότητας χρήστη (user identity request).

4.1.3 Επιθέσεις προσωποποίησης του δικτύου

Σκοπός αυτών των επιθέσεων το κρυφάκουσμα δεδομένων που ανήκουν ή προορίζονται για έναν νόμιμο χρήστη του δικτύου από έναν επιτιθέμενο, ο οποίος μιμείται τη λειτουργία ενός νόμιμου δικτύου και παραπλανεί έναν χρήστη

αποστέλλοντας σε αυτόν μηνύματα και πληροφορίες που πιστεύει ότι προέρχονται από το νόμιμο δίκτυο. Σε αυτές τις επιθέσεις διακρίνουμε τρεις διαφορετικές παραλλαγές.

1. **Προσωποποίηση του δικτύου με την υποβάθμιση της κρυπτογράφησης μεταξύ χρήστη και επιτιθέμενου.**

Ο επιτιθέμενος με τη συνδρομή ενός ψεύτικου σταθμού βάσης μπορεί να παγιδεύσει το συνδρομητή. Όταν ο χρήστης στείλει ένα μήνυμα με το οποίο αιτείται μια υπηρεσία, ο επιτιθέμενος δεν ενεργοποιεί το μηχανισμό κρυπτογράφησης και καλεί τον χρήστη να κάνει το ίδιο, πλαστογραφώντας μια εντολή τρόπου κρυπτογράφησης (cipher mode command), την οποία του αποστέλλει. Ο επιτιθέμενος διατηρεί ενεργή την κλήση για όσο χρονικό διάστημα χρειάζεται ή όσο η επίθεση δεν έχει ανιχνευθεί.

2. Προσωποποίηση του δικτύου με την υποβάθμιση της κρυπτογράφησης μεταξύ χρήστη και νόμιμου δικτύου.

Ο επιτιθέμενος χρησιμοποιεί έναν τροποποιημένο κινητό σταθμό ενσωματωμένο με έναν ψεύτικο σταθμό βάσης και παγιδεύει το χρήστη. Όταν ο χρήστης πραγματοποιεί μια κλήση ο επιτιθέμενος τροποποιεί το μήνυμα του χρήστη προς το νόμιμο δίκτυο που εμπεριέχει τις δυνατότητες κρυπτογράφησης του κινητού του σταθμού κατά τέτοιον τρόπο ώστε να φαίνεται ότι υπάρχει φυσική ασυμβατότητα μεταξύ των μηχανισμών που διαθέτει ο κινητός σταθμός του χρήστη και αυτών που υποστηρίζει το δίκτυο εξυπηρέτησης. Σε περίπτωση που το δίκτυο αποφασίσει να εγκαταστήσει μια σύνδεση χωρίς τη χρήση κρυπτογράφησης, ο επιτιθέμενος κόβει τη σύνδεση του χρήστη με το δίκτυο και προσωποποιείται το δίκτυο εξυπηρέτησης στον χρήστη.

3. Προσωποποίηση του δικτύου με εξαναγκασμένη χρήση ενός υποκλαπέντος κλειδιού κρυπτογράφησης.

Και σε αυτήν την περίπτωση, ο επιτιθέμενος παγιδεύει τον χρήστη σε έναν ψεύτικο σταθμό βάσης και, όταν ενεργοποιείται μια κλήση επιβάλει στο συνδρομητή τη χρησιμοποίηση ενός κλειδιού κρυπτογράφησης, το οποίο έχει στην κατοχή του. Για την πραγματοποίηση αυτής της επίθεσης ο επιτιθέμενος θα πρέπει να έχει υποκλέψει ένα διάνυσμα αυθεντικοποίησης (authentication vector), στο οποίο ενυπάρχει το κλειδί κρυπτογράφησης.

Σε ότι αφορά τα δίκτυα 3ης γενιάς, οι δυο πρώτες παραλλαγές αυτού του είδους επιθέσεων δεν είναι δυνατόν να πραγματοποιηθούν, εξαιτίας του γεγονότος ότι τόσο ο κινητός σταθμός του συνδρομητή όσο και το δίκτυο εξυπηρέτησης μπορούν να διαπιστώσουν αν η κρυπτογράφηση έχει υποβαθμιστεί από κάποιον επιτιθέμενο, διότι η εντολή τρόπου κρυπτογράφησης που στέλνει το δίκτυο στο χρήστη καθώς και το μήνυμα αναφοράς των μηχανισμών κρυπτογράφησης του κινητού σταθμού που στέλνει ο χρήστης στο δίκτυο προστατεύονται με μηχανισμούς αυθεντικοποίησης και αποτροπής επανάληψης. Στην τρίτη περίπτωση, η παρουσία ενός σειριακού αριθμού επιτρέπει στην USIM του χρήστη να διαπιστώσει αν ένα κλειδί κρυπτογράφησης είναι παλιό και έχει ήδη χρησιμοποιηθεί. Ωστόσο, αν ένας επιτιθέμενος καταφέρει να υποκλέψει διανύσματα αυθεντικοποίησης πριν αυτά χρησιμοποιηθούν από το δίκτυο εξυπηρέτησης, τότε το δίκτυο καθίσταται ευάλωτο σε αυτές τις επιθέσεις.

4.1.4 Επιθέσεις προσωποποίησης του χρήστη

4.1.4.1 Προσωποποίηση του χρήστη με τη χρήση υποκλαπέντων πληροφοριών

Εφόσον ο επιτιθέμενος μπορέσει να υποκλέψει είτε ένα διάνυσμα αυθεντικοποίησης είτε μια απάντηση αυθεντικοποίησης (authentication response, SRES) είναι σε θέση να τη χρησιμοποιήσει για να υποδυθεί το νόμιμο χρήστη. Αυτή η επίθεση

εκμεταλλεύεται το γεγονός ότι ένα διάνυσμα αυθεντικοποίησης μπορεί να χρησιμοποιηθεί πολλές φορές. Στα δίκτυα 3ης γενιάς, όπως έχει προαναφερθεί, η ύπαρξη μιας παραμέτρου συγχρονισμού (sequence number) αποτρέπει τη χρησιμοποίηση παλιών διανυσμάτων.

4.1.4.2 Κατάληψη εξερχόμενων κλήσεων σε δίκτυα χωρίς κρυπτογράφηση

Ο επιτιθέμενος εξαναγκάζει το χρήστη-στόχο να ενεργοποιήσει τη διαδικασία εκκίνησης μιας κλήσης. Αυτό μπορεί να συμβεί, για παράδειγμα, στέλνοντας στο χρήστη μια παραπλανητική ένδειξη εισερχόμενης κλήσης. Ο επιτιθέμενος παραποιεί τα δεδομένα σηματοδοσίας ώστε το δίκτυο εξυπηρέτησης να θεωρεί ότι ο χρήστης θέλει να πραγματοποιήσει μια εξερχόμενη κλήση. Αφού ο γνήσιος σταθμός βάσης πιστοποιήσει επιτυχώς το χρήστη, ο επιτιθέμενος καταλαμβάνει τη ραδιο-ζεύξη για να πραγματοποιήσει δικές του κλήσεις, χρεώνοντας το νόμιμο συνδρομητή. Η επίθεση αυτή προϋποθέτει ότι το δίκτυο δεν χρησιμοποιεί κρυπτογράφηση.

4.1.4.3 Κατάληψη εισερχόμενων κλήσεων σε δίκτυα χωρίς κρυπτογράφηση

Όπως και πριν, υποθέτουμε ότι ο επιτιθέμενος έχει τη δυνατότητα να παρεμβληθεί μεταξύ του χρήστη και του γνήσιου σταθμού βάσης που τον εξυπηρετεί. Επίσης υποθέτουμε ότι ο χρήστης-στόχος περιάγεται σε περιοχή διαφορετική από αυτήν του οικείου δικτύου του. Ένας χρήστης που σχετίζεται με τον επιτιθέμενο πραγματοποιεί μια κλήση στο χρήστη-στόχο. Αφού γίνει η αυθεντικοποίηση επιτυχώς και εγκατασταθεί η σύνδεση, ο επιτιθέμενος καταλαμβάνει τη ραδιο-ζεύξη και απαντάει στην κλήση του χρήστη-συνδέσμου, με αποτέλεσμα ο χρήστης-στόχος να χρεωθεί για την περιαγωγή.

Στα δίκτυα 3ης γενιάς, αν και δεν προβλέπεται μηχανισμός προστασίας της ακεραιότητας των δεδομένων του χρήστη[9] για λόγους απόδοσης, ωστόσο, υπάρχει μια συγκεκριμένη διαδικασία που καλείται περιοδική αυθεντικοποίηση (periodic authentication), σύμφωνα με την οποία το ποσό των δεδομένων που στάλθηκαν κατά

[9] Ο μηχανισμός ακεραιότητας προστατεύει μόνο τα δεδομένα σηματοδοσίας μεταξύ κινητού σταθμού και RNC.

τη διάρκεια μιας σύνδεσης ελέγχεται. Αυτό έχει σαν αποτέλεσμα τα δεδομένα των χρηστών να προστατεύονται περιοδικά όσο αφορά το μέγεθός τους, παράλληλα με τη διαδικασία επανάληψης της αυθεντικοποίησης. Η διαδικασία αυτή αποτρέπει εν μέρει την κατάληψη μη κρυπτογραφημένων συνδέσεων μετά την αρχική εγκατάσταση της σύνδεσης.

4.1.5 Επιθέσεις κρυφακούσματος των δεδομένων του χρήστη

Στις επιθέσεις αυτές ο επιτιθέμενος λειτουργεί και πάλι ως ενδιάμεσος με τη βοήθεια ενός τροποποιημένου κινητού σταθμού/σταθμού βάσης και επιχειρεί να υποβαθμίσει το επίπεδο προστασίας με κρυπτογράφηση αναγκάζοντας το χρήστη και το δίκτυο να χρησιμοποιήσουν πιο ευάλωτους αλγόριθμους κρυπτογράφησης (A5/2). Ο επιτιθέμενος παγιδεύει τον κινητό σταθμό, ενώ διατηρεί τη σύνδεσή του με το νόμιμο δίκτυο μέσω της δικής του συνδρομής. Με τον τρόπο αυτό μπορεί να κρυφακούει τη ραδιο-ζεύξη και να υποκλέπτει τα δεδομένα του χρήστη.

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Σύνοψη εργασίας και κυριότερα συμπεράσματα

Στην παρούσα εργασία παρουσιάστηκαν τα δύο σημαντικότερα συστήματα των κυψελωτών δικτύων τηλεπικοινωνιών $2^{ης}$ και $3^{ης}$ γενιάς. Συγκεκριμένα, παρουσιάστηκαν οι αρχιτεκτονικές των δύο συστημάτων, GSM και UMTS, οι οντότητες που περιλαμβάνουν και η επικοινωνία που συνδέει αυτές τις οντότητες. Επίσης, αναλύθηκαν οι μηχανισμοί ασφάλειας που διέπουν τα δύο συστήματα, οι σκοποί που προτίθενται να εκπληρώσουν και για τους οποίους υλοποιήθηκαν, τα ιδιαίτερα χαρακτηριστικά του κάθε μηχανισμού και ο τρόπος λειτουργίας και εφαρμογής τους. Στη συνέχεια, έγινε εκτενής αναφορά και αξιολόγηση στα μειονεκτήματα και τις ευπάθειες αυτών των μηχανισμών, τα ευαίσθητα σημεία που παρουσιάζουν και τα προβλήματα που προκύπτουν από αυτές τις ευπάθειες και που μπορούν να θέσουν σε κίνδυνο την ασφάλεια των τηλεπικοινωνιών, το απόρρητο των συνομιλιών και των άλλων πληροφοριών που σχετίζονται με τηλεπικοινωνιακές υπηρεσίες και να επηρεάσουν τη χρέωση των νόμιμων συνδρομητών.

Στο σύστημα GSM αναπτύχθηκαν νέοι και ασφαλέστεροι μηχανισμοί για την ασφάλεια των ευαίσθητων δεδομένων που διακινούνται μέσω των κινητών συσκευών σε σχέση με τα πρώτα δίκτυα κινητής που εμφανίστηκαν. Οι μηχανισμοί αυτοί εξασφαλίζουν ένα αρκετά υψηλό βαθμό ασφάλειας για τους συνδρομητές, χωρίς βέβαια να εκλείψουν τελείως ορισμένα κενά και ευπάθειες. Πολλά από τα κενά αυτά καλύφθηκαν και πολλοί κίνδυνοι εξαλείφθηκαν με τους μηχανισμούς που υιοθετήθηκαν στα δίκτυα $3^{ης}$ γενιάς. Στο UMTS, λόγω κυρίως του γεγονότος ότι οι αλγόριθμοι για την αυθεντικοποίηση και την κρυπτογράφηση των δεδομένων δεν είναι πλέον μυστικοί, αλλά ‘ανοιχτοί’, το επίπεδο ασφάλειας έχει αναβαθμιστεί σημαντικά. Ωστόσο, και εδώ παρατηρούνται κάποιες ευπάθειες.

Σαν γενικό συμπέρασμα, θα πρέπει να τονιστεί ότι όπως και σε πολλούς άλλους τομείς, έτσι και στον τομέα των κινητών τηλεπικοινωνιών, αποδεικνύεται ότι κανένα σύστημα δεν είναι απολύτως ασφαλές. Όμως, η ασφάλεια που παρέχεται στο μέσο χρήστη κρίνεται, γενικά, απολύτως ικανοποιητική αφού, σε αυτό το επίπεδο των συνδρομητών είναι μάλλον απίθανο να δαπανήσει κανείς ένα αρκετά σημαντικό χρηματικό πόσο για να προμηθευτεί τον εξοπλισμό που απαιτείται, για να υποκλέψει τα δεδομένα που μεταδίδει και λαμβάνει ένας μέσος χρήστης. Άλλωστε, οι διαδικασίες της υποκλοπής και της αποκρυπτογράφησης δεδομένων, με τη βοήθεια ψεύτικων σταθμών βάσης, είναι εξαιρετικά πολύπλοκες και απαιτούν πολύ χρόνο και κόπο. Όταν οι χρήστες είναι μεγάλες εταιρείες, οπότε έχουμε να κάνουμε με μεγαλύτερα οικονομικά και άλλα συμφέροντα, η πιθανότητα κάποιος να προσπαθήσει να υποκλέψει σχετίζεται άμεσα με το αν τα οικονομικά οφέλη που θα αποκομίσει θα είναι μεγαλύτερα από το – καθόλου αμελητέο – κόστος της επίθεσης. Έτσι, και λόγω του σκληρού ανταγωνισμού μεταξύ των διαφόρων επιχειρήσεων στην εποχή μας, κάθε μια από αυτές θα πρέπει να λάβει μέτρα για την πρόληψη οικονομικών απατών.

Από την πλευρά του, ο μέσος χρήστης, προκειμένου να είναι – και να νιώθει – ασφαλής, θα πρέπει να είναι ιδιαίτερα προσεκτικός με τη χρήση της συσκευής του και της κάρτας SIM/USIM που χρησιμοποιεί. Για παράδειγμα, δε θα πρέπει να αφήνει ποτέ τη συσκευή του απροστάτευτη σε χώρους όπου έχουν πρόσβαση και άλλα άτομα. Θα πρέπει επίσης να ελέγχει τις χρεώσεις του και να ενημερώνει τον πάροχο κινητής τηλεφωνίας όταν διαπιστώσει κάτι ύποπτο ή περίεργο είτε σε αυτές, είτε σε σχέση με την ποιότητα των υπηρεσιών που του προσφέρονται. Σε γενικές γραμμές, η υιοθέτηση των παρακάτω απλών και «καλών» συνηθειών εξασφαλίζει κατά ένα μεγάλο ποσοστό την ασφαλή επικοινωνία και χρήση των υπηρεσιών του δικτύου:

- Να μην απενεργοποιούμε το PIN και να το χρησιμοποιούμε και στο «κλείδωμα» πληκτρολογίου.
- Το PIN να μην είναι «εύκολο» και να το αλλάζουμε συχνά.
- Να μην αφήνουμε τη συσκευή μας χωρίς επίβλεψη και «ξεκλείδωτη».

- Να ενεργοποιούμε το «κλείδωμα» της συσκευής με την κάρτα SIM ή/και τον κωδικό (password) συσκευής.
- Να μην αποθηκεύουμε κωδικούς (passwords) στις επιμέρους ρυθμίσεις των εφαρμογών της συσκευής.
- Να αποφεύγουμε την αποθήκευση «ευαίσθητων» δεδομένων στη συσκευή για μεγάλο χρονικό διάστημα.
- Να ελέγχουμε τις λίστες εισερχόμενων και εξερχόμενων κλήσεων/διασυνδέσεων και μηνυμάτων στη συσκευή αλλά κυρίως στο λογαριασμό. [31]

5.2 Θέματα μελλοντικής εργασίας

Ορισμένα από τα θέματα και ερωτήματα που προκύπτουν από την ανάλυση και αξιολόγηση των μηχανισμών ασφαλείας που προηγήθηκε και που θα μπορούσαν να εξεταστούν περαιτέρω είναι:

- Η εξασφάλιση αμοιβαίας εμπιστοσύνης μεταξύ διαφορετικών παρόχων κινητής τηλεφωνίας, κυρίως όταν τίθεται το ζήτημα της περιαγωγής.
- Κατά πόσο τα πρωτόκολλα MAPSEC και IPSEC είναι η ενδεδειγμένη και κατάλληλη λύση για ασφαλή επικοινωνία μεταξύ δικτύων.
- Κατά πόσο μπορούν δυο κινητές συσκευές να επικοινωνήσουν με ασφάλεια, χωρίς να χρειάζεται να βασίζονται τόσο πολύ στα δίκτυα που τους εξυπηρετούν και πώς μπορούν, σε αυτήν την περίπτωση, να πιστοποιούνται μεταξύ τους και να μοιράζονται μυστικά κλειδιά.
- Με ποιους τρόπους μπορούν να επιλυθούν τα προβλήματα ασφάλειας που διαπιστώνονται στα δίκτυα 3ης γενιάς.
- Ποια θα είναι τα χαρακτηριστικά των μηχανισμών ασφαλείας για τα κινητά δίκτυα 4ης γενιάς.

5.3 ΑΝΑΦΟΡΕΣ

[1] Eberspacher, J., Vogel, H.-J. & Bettstetter, C. (2001). *GSM Switching, Services and Protocols*, Chichester, John Wiley & Sons Ltd., σ. 29 – 45, 95 – 122.

[2] Τσουμελέας, Η. (2004). *Ασφάλεια Τηλεπικοινωνιών*. Διπλωματική εργασία, Εθνικό Μετσόβιο Πολυτεχνείο.

[3] http://www.3gpp.org/specs/releases-contents.htm

[4] http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

[5] Καμπουράκη, Γ., Γκρίτζαλη, Σ., Κάτσικα, Σ. (2006). *Ασφάλεια Ασύρματων και Κινητών Δικτύων Επικοινωνιών*. Αθήνα. Εκδόσεις Παπασωτηρίου, σελ. 419 – 485

[6] http://portal.gunet.gr/index.pl?id=3192&isa=Item&op=download

[7] GSM 02.09, Digital Cellular Telecommunications (Phase 2+); Security Aspects (version 6.1.0 Release 1997)

[8] Pagliusi, P.S., *"A Contemporary Foreword on GSM Security"*, London UK, 2002, http://www.portal.acm.org

[9] Rao, J.R., Rohatgi, P., Scherzer, H. & Tinguely, S. (2002). Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards. In: *The 2002 IEEE Symposium on Security and Privacy*, Oakland, CA, USA.

[10] Stausholm M., Dahl M. (2006) *"Insecurity of GSM Communication"*. Ανάκτηση από : http://www.daimi.au.dk/~ivan/GsmSecurity.pdf

[11] Biryukov, A., Shamir, A., Wagner, D. (2000). Real Time Cryptanalysis of A5/1 on a PC.

[12] Σταθάκη, Α. (2004). *Το Ζήτημα της Ασφάλειας στα Δίκτυα GSM και GPRS.* Διπλωματική εργασία, Εθνικό Μετσόβιο Πολυτεχνείο.

[13] Quirke, J. (2004). *Security in the GSM system.* AusMobile, Australia. Ανάκτηση από World Wide Web: http://www.ausmobile.com

[14] Brumley, B. (2004). *A3/A8 & COMP128.* Special Course on Cryptology. Helsinki University of Technology.

[15] Brookson, C. (2002). *Can you clone a GSM Smart Card (SIM)?*. Ανάκτηση από World Wide Web : http://www.brookson.com/gsm/clone.pdf

[16] GSM 03.20, Digital Cellular Telecommunications (Phase 2+); Security Related Network Functions (version 4.4.1)

[17] Skorobogatov, S.P. & Anderson, R. J. (2002). Optical Fault Induction Attacks. In: *2002 IEEE Symposium on security and privacy,* Oakland, USA.

[18] Bocan, V., Cretu, V. (2004). "Security and Denial of Service Threats in GSM Networks*", PERIODICA POLITECHNICA - Transactions on Automatic Control and Computer Science*, 49(63), 3-6.

[19] Huynh, T. & Nguyen, H. (2003). *Overview of GSM and GSM Security.* Department of Electrical Engineering and Computer Science. Oregon State University. Ανάκτηση από: http://www.gsm-security.net/gsm-security-papers.shtml

[20] Yousef, P. (2004). *GSM-Security: a Survey and Evaluation of the Current Situation.* Thesis, Linköping Institute of Technology.

[21] Walker, M., (2000). On The Security of 3GPP Networks. In: *Eurocrypt 2000.* London, UK. Ανάκτηση από World Wide Web: http://www.isrc.rhul.ac.uk/useca/OtherPublications/pks2000.pps

[22] 3GPP TS 33.102, *3G Security; Security Architecture* (version 6.5.0, Dec. 2005)

[23] Langnes, R., Aamodt, T.E., Friiso, T., Koien, G., Eilertsen, O. (2001) *Security in UMTS – Integrity*. Telenor R&D, February 2001.

[24] 3GPP TS 35.201, Specification of the 3GPP Confidentiality and Integrity Algorithms; *f8 and f9 Specification*, June 2002, (Release 5)

[25] Kaaranen, H., Ahtiainen, A., Laitinen, L., Naghian, S., Niemi, V. (2001) *UMTS Networks – Architecture, Mobility And Services*. New York. Wiley & Sons.

[26] Meyer, U. & Wetzel, S. (2004). A Man-In-The-Middle Attack on UMTS. In: *WiSe '04*, Philadelphia, Pennsylvania, USA.

[27] Boman, K., Horn, G., Howard, P., Niemi, V. (2002) "UMTS Security", *IEEE Electronics & Communication Engineering Journa, October 2002.*

[28] 3GPP TS 33.107, *3rd Generation Partnership Project; Lawful Interception architecture and functions* (**version 7.3.0, Release 7**) March 2006.

[29] 3GPP TS 21.133, *3rd Generation Partnership Project; 3G Security; Security threats and requirements* (version 4.1.0, Release 4) January 2002.

[30] 3G TR 33.900, *3rd Generation Partnership Project; A Guide to 3rd Generation Security.* (version 1.2.0) January 2000.

[31] Κορίνθιος, Γ. *Μέθοδοι Αυτοπροστασίας Συνδρομητών Κινητής Τηλεφωνίας*. Ανάκτηση από World Wide Web: http://www.adae.gr