



ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία
Μεταπτυχιακού Διπλώματος Ειδίκευσης

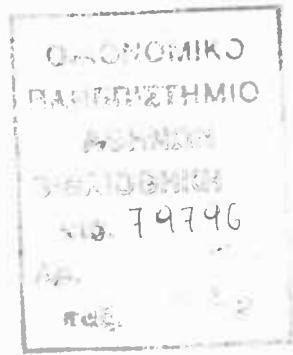
«Ασφάλεια και διαχείριση κλειδιών στο UMTS»

Βασίλειος Παναγιωτόπουλος

Επιβλέπων: Γεώργιος Ξυλωμένος

ΑΘΗΝΑ, ΙΟΥΝΙΟΣ 2006





Στην συζυγό μου Ανδρεάννα και
στα παιδιά μου Γιώργο και Μαρία.



ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΚΑΤΑΛΟΓΟΣ

0 000000570855



Ευχαριστίες

Οα ήθελα να εκφράσω τις ευχαριστίες μου στον Λέκτορα κ. Γεώργιο Ξυλωμένο, που ήταν υπεύθυνος για την επίβλεψη της εργασίας αυτής για την πολύτιμη βοήθειά του.

Οα ήθελα να ευχαριστήσω επίσης τον Καθηγητή κ. Γεώργιο Σταμούλη, Πρόεδρο του Μεταπτυχιακού προγράμματος της Επιστήμης των Υπολογιστών του Οικονομικού Πανεπιστημίου Αθηνών, για τις κατευθύνσεις και τις συμβουλές του.

Τέλος, θα ήθελα να ευχαριστήσω την συζυγό μου Ανδρεάννα για την ηθική συμπαραστασή της και την υπομονή της, χάρις στην οποία ολοκληρώνω τις σπουδές μου.



ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ	i
ΕΥΡΕΤΗΡΙΟ ΣΧΕΔΙΩΝ	iii
ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ	v
ΠΕΡΙΛΗΨΗ	vi
ΚΕΦΑΛΑΙΟ 1 Εισαγωγή	1
1.1 Γενικά	1
1.2 Δομή της εργασίας	3
ΚΕΦΑΛΑΙΟ 2 Γενικά θέματα ασφάλειας	5
2.1 Ασφάλεια –βασικές έννοιες	5
2.2 Στοιχεία κρυπτογραφίας	6
2.2.1 Συμμετρική κρυπτογραφία	7
2.2.2 Κρυπτογραφία Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογραφία)	8
2.2.3 Ψηφιακές υπογραφές (Digital Signatures)	10
2.2.4 Μιας χρήσης Υπογραφή (One-Time Signing):	11
2.2.5 Κώδικας Αυθεντικοποίησης Μηνυμάτων (MAC –Message Authentication Code)..	12
2.2.6 Μονόδρομες συναρτήσεις Σύνοψης (One Way Hash Function)	13
2.2.7 Αλυσίδα Σύνοψης (Hash chaining)	13
ΚΕΦΑΛΑΙΟ 3 Αρχιτεκτονική κινητών δικτύων	15
3.1 Αρχιτεκτονική GSM.....	15
3.2 Αρχιτεκτονική GPRS	18
3.3 Αρχιτεκτονική του UMTS	21
3.3.1 User Equipment (UE).....	22
3.3.2 UMTS Terrestrial Radio Access Network ή UTRAN	23
3.3.3 Το κυρίως δίκτυο (Core network (CN)).....	23
3.3.4 Πρωτόκολλα σηματοδοσίας και επιπέδου χρήστη στο UMTS	24
ΚΕΦΑΛΑΙΟ 4 Απαιτήσεις ασφαλείας του δικτύου	28
4.1 Χαρακτηριστικά ασφαλείας/Απαιτήσεις ασφαλείας/Σχεδίαση	28
4.1.1 Απειλές ασφαλείας.....	31
4.1.2 Απαιτήσεις ασφάλειας.....	36
4.1.2.3 Συγκέντρωση των απαιτήσεων ασφαλείας ενός δικτύου 3G	40
ΚΕΦΑΛΑΙΟ 5	42
5.1 Ασφάλεια στο UMTS	42
5.2 Ασφάλεια στο δίκτυο πρόσβασης	43
5.2.1 Αυθεντικοποίηση και συμφωνία κλειδιών (Authentication and key agreement (UMTS AKA))	44
5.2.2 Εμπιστευτικότητα δεδομένων	52
5.2.3 Εμπιστευτικότητα της ταυτότητας των χρηστών	54
5.2.4 Προστασία ακεραιότητας των μηνυμάτων σηματοδοσίας.....	56
ΚΕΦΑΛΑΙΟ 6	65
6.1 Προβλήματα ασφαλείας στο UMTS	65
6.1.1 Αδυναμίες.....	66
ΚΕΦΑΛΑΙΟ 7	71
7.1 Εναλλακτικές προτάσεις / Προτάσεις βελτίωσης του UMTS AKA	71
7.1.1 AP-AKA	71



Ασφάλεια και διαχείριση κλειδιών στο UMTS

7.1.2 UMTS X-AKA	74
7.1.3 Πρωτόκολλο Shu-Min Cheng et al.	77
7.1.4 Πρωτόκολλο Harn-Hsin	82
7.1.5 Πρόταση Yi-Bing Lin et al.....	85
7.2 Σύγκριση μεταξύ AKA (Authentication and Key Agreement Protocols) για το UMTS ..	86
ΚΕΦΑΛΑΙΟ 8 Ασφάλεια στο κυρίως δίκτυο (Network Domain Security NDS).	87
8.1 MAPsec (Ασφάλεια στο τμήμα μεταγωγής πακέτου CS).....	88
8.1.1 Μορφή των μηνυμάτων MAPsec.....	88
8.1.2 Αλγόριθμοι του MAPsec.....	90
8.1.3.Συσχετίσεις ασφαλείας (Security associations SAs).....	91
8.1.4 Προφύλ προστασίας.....	92
8.2 IPsec (Ασφάλεια στο τμήμα μεταγωγής πακέτων (PS))	92
8.2.1 Λειτουργία του IPsec	93
8.2.1.1. Η δομή του ESP	94
8.2.2 Τρόπος επικοινωνίας.....	96
8.2.3 Ασφάλεια στο IP κυρίως δίκτυο / Μηχανισμός Αυθεντικοποίησης (Network Domain Security Authentication Framework NDS/AF).....	98
8.3 Προβλήματα ασφαλείας στο κυρίως δίκτυο	100
ΚΕΦΑΛΑΙΟ 9 Ασφάλεια στο IMS (IP Multimedia CN Subsystem).....	102
9.1 Αρχιτεκτονική του IMS	102
9.2 Αρχιτεκτονική ασφαλείας του IMS	105
9.2.1 Μηχανισμοί ασφαλείας.....	108
9.3 Μη εξουσιοδοτημένη χρήση του IMS	121
9.4 Πρόταση Yi-Bing Lin et al.....	122
ΚΕΦΑΛΑΙΟ 10 Συμπεράσματα – Θέματα που χρειάζονται περαιτέρω μελέτη	124
ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ.....	129
ΒΙΒΛΙΟΓΡΑΦΙΑ	131



ΕΥΡΕΤΗΡΙΟ ΣΧΕΔΙΩΝ

Σχήμα 2.1 Συμμετρική κρυπτογραφία	8
Σχήμα 2.2 Ασύμμετρη κρυπτογραφία.....	9
Σχήμα 2.3 Ψηφιακή υπογραφή.....	10
Σχήμα 2.4 Κώδικας Αυθεντικοποίησης Μηνυμάτων.....	12
Σχήμα 2.5 Αλυσίδα σύνοψης (Hash chaining).....	14
Σχήμα 3.1 Αρχιτεκτονική GSM	16
Σχήμα 3.2 Αρχιτεκτονική GPRS	18
Σχήμα 3.3 Αρχιτεκτονική UMTS	22
Σχήμα 3.4: Αρχιτεκτονική πρωτοκόλλων σε επίπεδο ελέγχου για το τμήμα PS	24
Σχήμα 3.5: Αρχιτεκτονική πρωτοκόλλων σε επίπεδο χρήστη για το τμήμα PS	25
Σχήμα 5.1 Αρχιτεκτονική ασφάλειας στο UMTS	43
Σχήμα 5.2 Διάνυσμα αυθεντικοποίησης (AV)	46
Σχήμα 5.3 Πρωτόκολλο UMTS AKA.....	47
Σχήμα 5.4 Υπολογισμός του διανύσματος αυθεντικοποίησης (AV) από το AuC	47
Σχήμα 5.5 Μήνυμα απόρριψης από το UE προς το SN	48
Σχήμα 5.6 Αυθεντικοποίηση του δικτύου από τον κινητό σταθμό (MS)	49
Σχήμα 5.7 Διαδικασία επανασυγχρονισμού.....	51
Σχήμα 5.8 Κρυπτογράφηση δεδομένων	53
Σχήμα 5.9 Προστασία ακεραιότητας στο UMTS	59
Σχήμα 5.10 (Περιοδική τοπική αυθεντικοποίηση).....	60
Σχήμα 5.11 Εγκαθίδρυση ασφαλούς συνόδου στο UMTS	64
Σχήμα 7.1 Πρωτόκολλο AP-AKA	71
Σχήμα 7.2 AP-AKA όταν ο χρήστης είναι στα όρια του πατρικού δικτύου	73
Σχήμα 7.3 Πρωτόκολλο X-AKA.....	76
Σχήμα 7.4 Πρωτόκολλο Shu-Min Cheng et al	78
Σχήμα 7.5 Ακόλουθη διαδικασία αυθεντικοποίησης.....	80
Σχήμα 7.6 Πρωτόκολλο Harn-Hsin.....	83
Σχήμα 8.1 Δομή μηνυμάτων MAP.....	88
Σχήμα 8.2 AES cipher Block chaining (CBC).....	90
Σχήμα 8.3 Προστατευμένες διεπαφές του UMTS	93



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Σχήμα 8.4 Μηνύματα IPsec ESP	95
Σχήμα 8.5 Επικοινωνία στο NDS.....	98
Σχήμα 8.6 Αρχιτεκτονική του μηχανισμού Αυθεντικοποίησης.....	100
Σχήμα 9.1 Το IMS σε ένα UMTS δίκτυο	102
Σχήμα 9.2 Αρχιτεκτονική του IMS	104
Σχήμα 9.3 Δημιουργία συνόδου (INVITE).....	105
Σχήμα 9.4 Αρχιτεκτονική ασφαλείας IMS.....	107
Σχήμα 9.5 Αρχιτεκτονική ασφαλείας του IMS για το κυρίως δίκτυο όταν το P- CSCF ανήκει σε διαφορετικό δίκτυο.....	108
Σχήμα 9.6 Αρχιτεκτονική ασφαλείας του IMS για το κυρίως δίκτυο όταν το P- CSCF ανήκει στο πατρικό δίκτυο.....	108
Σχήμα 9.7 AKA για το IMS	109
Σχήμα 9.8 Αποτυχία αυθεντικοποίησης δικτύου στο IMS AKA.....	113
Σχήμα 9.9 Αποτυχία συγχρονισμού το IMS AKA.....	114
Σχήμα 9.10 Ανταλλαγή μηνυμάτων συμφωνίας ασφαλείας	118
Σχήμα 9.11 Παράδειγμα χρήσης των SAs	121
Σχήμα 9.12 Μη εξουσιοδοτημένη χρήση του IMS	122
Σχήμα 9.13 Αυθεντικοποίηση «one pass» για UMTS και IMS	123

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

Πίνακας 5.1 Οι ταυτότητες ενός κινητού σταθμού στο δίκτυο UMTS	54
Πίνακας 5.2 Αλγόριθμοι που χρησιμοποιούνται στο UMTS.....	59
Πίνακας 6.1 Σύγκριση δυνατοτήτων ασφαλείας GSM-UMTS.....	65
Πίνακας 7.1 Συντομεύσεις του πρωτοκόλλου Shu-Min Cheng et al	77
Πίνακας 7.2 Σύγκριση προτεινόμενων πρωτοκόλλων για AKA στο UMTS.....	86
Πίνακας 9.1 Χρήση προστατευμένων πορτών για τα προστατευμένα μηνύματα	119

ΠΕΡΙΛΗΨΗ

Το UMTS, έχει στόχο να συγκεράσει τα πλεονεκτήματα που προκύπτουν από τη διάδοση των κυψελοειδών δικτύων κινητών τηλεπικοινωνιών δεύτερης γενιάς, με τις υπηρεσίες του διαδικτύου όπως είναι το ηλεκτρονικό ταχυδρομείο, η πλοϊγηση σε ηλεκτρονικές σελίδες, η τηλεδιάσκεψη, το ηλεκτρονικό εμπόριο, οι υπηρεσίες πολυμέσων και όλες οι υπηρεσίες που προσφέρει η νέα τεχνολογία. Κινητό/ασύρματο διαδίκτυο διατίθεται με την εμφάνιση της τρίτης γενιάς κινητής τηλεφωνίας. Μαζί με την ποικιλία των νέων προοπτικών που προσφέρει, το κινητό Διαδίκτυο φέρνει επίσης νέες ανησυχίες σχετικά με τα ζητήματα ασφάλειας. Η ασύρματη πρόσβαση είναι εγγενώς λιγότερο ασφαλής και η κινητικότητα υπονοεί υψηλότερους κινδύνους ασφάλειας έναντι εκείνων που αντιμετωπίζονται στα σταθερά δίκτυα. Επίσης η εισαγωγή τεχνολογίας βασισμένης σε IP στον πυρήνα (κεντρικό δίκτυο) των 3G κινητών δικτύων φέρνει στο προσκήνιο πλήθος νέων ευπαθειών και πιθανών απειλών. Για να αντιδράσει ενάντια σε αυτά τα τρωτά σημεία, έχει αναπτυχθεί από τον οργανισμό προτυποποίησης του UMTS συγκεκριμένη αρχιτεκτονική ασφάλειας. Αυτή η αρχιτεκτονική στηρίζεται στις αρχές ασφάλειας του 2G, με βελτιώσεις σε ορισμένα σημεία προκειμένου να παρασχεθούν οι προηγμένες υπηρεσίες ασφάλειας. Κύριος στόχος είναι να εξασφαλιστεί ότι όλες οι πληροφορίες που σχετίζονται με έναν χρήστη, καθώς επίσης οι πόροι και οι υπηρεσίες που παρέχονται από το δίκτυο προστατεύονται επαρκώς από την κακή χρήση ή κατάχρηση. Οι κύριοι μηχανισμοί που χρησιμοποιεί αυτή η αρχιτεκτονική είναι: για το ασύρματο δίκτυο πρόσβασης α) η εμπιστευτικότητα των δεδομένων και της ταυτότητας του χρήστη, β)η ακεραιότητα των δεδομένων ελέγχου του δικτύου, και για το κυρίως δίκτυο α) η εμπιστευτικότητα και β) ακεραιότητα των δεδομένων ελέγχου του δικτύου.

Η εργασία αυτή περιγράφει τους μηχανισμούς που έχουν υιοθετηθεί από τον οργανισμό προτυποποίησης του UMTS προκειμένου να επιτευχθούν οι στόχοι ασφαλείας που έχουν τεθεί. Περιγράφει τους μηχανισμούς πρόσβασης του χρήστη στο δίκτυο και χρήσης του δικτύου, τόσο του ασύρματου όσο και του κεντρικού, για την μεταφορά της κίνησης των δεδομένων του. Περιγράφει επίσης, τους μηχανισμούς ασφαλείας που χρησιμοποιούνται από ένα πολύ σημαντικό τμήμα του κυρίως δικτύου το IMS (IP Mul-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

timedia Subsystem). Είναι όμως αυτοί οι μηχανισμοί αρκετοί; Καλύπτουν ικανοποιητικά τις τιθέμενες απαιτήσεις; Στην εργασία γίνεται μία προσπάθεια ανάλυσης των αδυναμιών των μηχανισμών, κυρίως αυτών που αφορούν στο πρωτόκολλο ασφάλειας του ασυρμάτου δικτύου πρόσβασης. Κατόπιν αναφέρονται κάποιες προτάσεις που υπάρχουν στην διεθνή βιβλιογραφία προκειμένου να καλυφθούν οι αδυναμίες και επιχειρεί μία σύγκριση μεταξύ τους.

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

1.1 Γενικά

Το παγκόσμιο κινητό σύστημα τηλεπικοινωνιών, (Universal Mobile Telecommunication system), (UMTS), είναι ένα από τα «τρίτης γενιάς» (3G) κυψελοειδή συστήματα επικοινωνιών που αναπτύσσονται μέσα το πλαίσιο που καθορίζεται από τη ITU γνωστό σαν IMT-2000.

Οι βασικές παράμετροι του συστήματος UMTS καθορίστηκαν από το Ευρωπαϊκό 1δρυμα προτύπων τηλεπικοινωνιών (ETSI) στις αρχές του 1998. Το ETSI είχε προτυποποιήσει προηγουμένως το εξαιρετικά επιτυχημένο σύστημα κινητής τηλεφωνίας δεύτερης γενιάς GSM (Global System for Mobile communications, 2G), το οποίο χρησιμοποιούν πάνω από 650 εκατομμύρια πελάτες παγκοσμίως και αντιστοιχεί περίπου στο 70% των ασυρμάτων επικοινωνιών της αγοράς. Ένα σημαντικό χαρακτηριστικό του UMTS, είναι η νέου τύπου ασύρματη πρόσβαση στο κυρίως δίκτυο (core network), το UMTS Terrestrial Radio Access (UTRA), βασισμένο στην τεχνολογία WCDMA.

Για να έχει παγκόσμια αποδοχή, η προτυποποίηση του UMTS μεταφέρθηκε το 1998 από το ETSI σε έναν φορέα που αποτελεί την συνεργασία πολλών οργανισμών προτύπων που ονομάστηκε 3GPP (3rd Generation Partnership Project). Μια διαφορετική ομάδα εργασίας από άλλους οργανισμούς προτύπων, γνωστή ως 3GPP2, αναπτύσσει ένα άλλο κυψελοειδές σύστημα τρίτης γενιάς βασισμένο σε διαφορετικό σύστημα ασύρματης πρόσβασης αποκαλούμενο CDMA2000 και ένα δίκτυο κορμού που εξελίσσεται βασιζόμενο στα βορειοαμερικανικά πρότυπα ANSI-41.

Το UMTS έχει στόχο να συγκεράσει τα πλεονεκτήματα που προκύπτουν από τη διάδοση των κυψελοειδών δικτύων κινητών τηλεπικοινωνιών δεύτερης γενιάς με τις υπηρεσίες του διαδικτύου, όπως είναι το ηλεκτρονικό ταχυδρομείο, η πλοήγηση σε ηλεκτρονικές σελίδες, η τηλεδιάσκεψη, το ηλεκτρονικό εμπόριο, οι υπηρεσίες πολυμέσων και όλες οι υπηρεσίες που προσφέρει η νέα τεχνολογία. Έτσι, προκύπτει ένα σύστημα κινητής τηλεπικοινωνίας τρίτης γενιάς, για την προτυποποίηση του οποίου συνεργάζονται πολλοί διεθνείς οργανισμοί προτυποποίησης, με κύριο άξονα τις απαιτήσεις και της ανάγκες της αγοράς.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Η μεγάλη επιτυχία που σημείωσε το δίκτυο GSM και η απήχηση που βρήκε, είχε ως βάση την ανάγκη για επικοινωνία (φωνής), από οπουδήποτε, οποτεδήποτε και με οποιονδήποτε. Παράλληλα, η μεγάλη διείσδυση του διαδικτύου στη ζωή του μέσου πιο λίτη των σύγχρονων αστικών κέντρων, έκανε επιτακτική την ανάγκη για πρόσβαση σε αυτό επί καθημερινής βάσης. Με αυτά τα δεδομένα, τα συστήματα επικοινωνιών τρίτης γενιάς έχουν ως στόχο, να προσφέρουν ένα ολοκληρωμένο περιβάλλον που θα συνδυάζει σε μία επικοινωνιακή πλατφόρμα ένα προσωπικό (τελικά) για κάθε χρήστη «εργαλείο» με απεριόριστες δυνατότητες επικοινωνίας οποιασδήποτε μορφής.

Κινητό/ασύρματο διαδίκτυο διατίθεται με την εμφάνιση της τρίτης γενιάς κινητής τηλεφωνίας. Μαζί με την ποικιλία των νέων προοπτικών που προσφέρει, το κινητό διαδίκτυο φέρνει επίσης νέες ανησυχίες σχετικά με τα ζητήματα ασφάλειας. Η ασύρματη πρόσβαση είναι εγγενώς λιγότερο ασφαλής, και η κινητικότητα υπονοεί υψηλότερους κινδύνους ασφάλειας έναντι εκείνων που αντιμετωπίζονται στα σταθερά δίκτυα. Το ασύρματο και ενσύρματο δίκτυο του 3G/UMTS συνιστούν μία υποδομή, η οποία υποστηρίζει υψηλότερες ταχύτητες πρόσβασης, αλλά και συνεχή πρόσβαση, η οποία όμως μπορεί να αυξήσει τον αριθμό και την ποιότητα των πιθανών επιθέσεων. Επιπλέον, αυξάνεται η δυνατότητα οι εισβολείς να είναι σε θέση να προωθήσουν τις κακόβουλες επιθέσεις, από κινητές συσκευές με ενισχυμένες ικανότητες επεξεργασίας, οι οποίες είναι δύσκολο να ανιχνευθούν. Επίσης η εισαγωγή τεχνολογίας βασισμένης σε IP στον πυρήνα (κεντρικό δίκτυο) των 3G κινητών δικτύων φέρνει στο προσκήνιο πλήθος νέων ευπαθειών και πιθανών απειλών. Προς το παρόν, οι εταιρείες κινητής τηλεφωνίας δεν επεκτείνουν τα ιδιωτικά δίκτυά τους, αλλά στηρίζονται μάλλον στην υπάρχουσα υποδομή διαδικτύου, για επικοινωνίες IP μέσα στο δίκτυό τους αλλά και με άλλα δίκτυα. Για να αντιδράσει ενάντια σε αυτά τα τρωτά σημεία, έχει αναπτυχθεί από τον οργανισμό προτυποποίησης του UMTS συγκεκριμένη αρχιτεκτονική ασφάλειας. Αυτή η αρχιτεκτονική στηρίζεται στις αρχές ασφάλειας του 2G με βελτιώσεις σε ορισμένα σημεία, προκειμένου να παρασχεθούν οι προηγμένες υπηρεσίες ασφάλειας.

Κύριος στόχος είναι να εξασφαλιστεί ότι όλες οι πληροφορίες που σχετίζονται με έναν χρήστη, καθώς επίσης οι πόροι και οι υπηρεσίες που παρέχονται από το δίκτυο, προστατεύονται επαρκώς από την κακή χρήση ή κατάχρηση.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Η εργασία αυτή περιγράφει τους μηχανισμούς που έχουν υιοθετηθεί από τον οργανισμό προτυποποίησης του UMTS προκειμένου να επιτευχθούν οι στόχοι ασφαλείας που έχουν τεθεί. Περιγράφει τους μηχανισμούς κατά την πρόσβαση του χρήστη στο δίκτυο και κατά την χρήση του δικτύου, τόσο του ασύρματου όσο και του κεντρικού, για την μεταφορά της κίνησης των δεδομένων του. Περιγράφει επίσης, τους μηχανισμούς ασφαλείας που χρησιμοποιούνται από ένα πολύ σημαντικό τμήμα του κυρίως δικτύου, το IMS (IP Multimedia Subsystem). Τα τμήματα αυτά είναι υπεύθυνο, ανάμεσα σε άλλα, για την παροχή εφαρμογών πολυμέσων στον τελικό χρήστη. Είναι όμως αυτοί οι μηχανισμοί αρκετοί; Καλύπτουν ικανοποιητικά τις τιθέμενες απαιτήσεις; Η εργασία περιγράφει επίσης τις αδυναμίες των μηχανισμών, κυρίως αυτών που αφορούν στο πρωτόκολλο ασφαλείας του ασυρμάτου δικτύου πρόσβασης, τις προτάσεις που υπάρχουν στην διεθνή βιβλιογραφία προκειμένου να καλυφθούν οι αδυναμίες και επιχειρεί μία σύγκριση μεταξύ τους. Η εργασία αυτή έχει την παρακάτω δομή.

1.2 Δομή της εργασίας.

Η δομή της εργασίας είναι:

- Κεφάλαιο 1:

Σε αυτό το κεφάλαιο αναφέρονται κάποια εισαγωγικά στοιχεία που αφορούν στην εξέλιξη των κυψελοειδών δικτύων, από τα αναλογικά δίκτυα πρώτη πρώτης γενιάς, στα ψηφιακά τρίτης γενιάς, (3G), καθώς και μία γενική επισκόπηση της εργασίας και των στόχων της.

- Κεφάλαιο 2:

Εδώ αναφέρονται γενικά κάποιες έννοιες και κρυπτογραφικοί μηχανισμοί που είναι απαραίτητοι για την κατανόηση των επομένων κεφαλαίων.

- Κεφάλαιο 3:

Αναλύεται η αρχιτεκτονική των δικτύων GSM, GPRS και UMTS καθώς και τα πρωτόκολλα σηματοδοσίας και επιπέδου χρήστη στο UMTS.

- Κεφάλαιο 4:

Αναλύονται και αποτιμώνται σε σπουδαιότητα, οι απειλές ασφαλείας για το 3G/UMTS δίκτυο από όπου και προκύπτουν οι απαιτήσεις ασφαλείας.

- Κεφάλαιο 5:



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Από αυτό το κεφάλαιο ξεκινά ουσιαστικά η ανάλυση και η αποτίμηση των μηχανισμών ασφαλείας. Γίνεται αρχικά αναφορά στους μηχανισμούς και στις περιοχές που καλύπτουν και προχωρά σε μία αναλυτική μελέτη των μηχανισμών του ασυρμάτου δικτύου πρόσβασης. Αναλύεται δηλαδή το UMTS AKA, και οι μηχανισμοί του.

- **Κεφάλαιο 6:**

Διερευνώνται οι αδυναμίες του UMTS AKA, όπως έχουν αναπτυχθεί στην διεθνή βιβλιογραφία.

- **Κεφάλαιο 7:**

Παρουσιάζονται άλλες προτάσεις και μηχανισμοί, από την διεθνή βιβλιογραφία, που έχουν σκοπό να βελτιώσουν την ασφάλεια και να καλύψουν τις αδυναμίες του UMTS AKA. Τέλος επιχειρείται μία σύγκριση αυτών των προτάσεων, με γνώμονα κατά πόσο και σε ποιο ποσοστό η κάθε μία καλύπτει τις αδυναμίες που αναγνωρίσθηκαν

- **Κεφάλαιο 8:**

Επιχειρείται μία ανάλυση των μηχανισμών ασφαλείας του κυρίως δικτύου. Οι μηχανισμοί ασφαλείας που έχουν αναπτυχθεί αφορούν μόνο τα δεδομένα ελέγχου, (σηματοδοσία) και όχι τα δεδομένα του χρήστη. Αναλύονται οι μηχανισμοί τόσο του τμήματος μεταγωγής κυκλώματος, δηλαδή το MAPsec, όσο και του τμήματος μεταγωγής πακέτων, IPsec. Επιχειρείται τέλος μία αποτίμηση της αποτελεσματικότητάς τους.

- **Κεφάλαιο 9:**

Αναλύεται η αρχιτεκτονική του IMS (IP Multimedia Subsystem) και οι μηχανισμοί ασφαλείας του, προκειμένου ο χρήστης να έχει ασφαλή πρόσβαση στις υπηρεσίες του. Ουσιαστικά αναλύεται ο μηχανισμός ασφαλείας πρόσβασης πρώτου άλματος μέσω του πρωτοκόλλου IMS AKA, καθώς η μεταφορά δεδομένων μέσα στο κυρίως δίκτυο καλύπτεται από τους μηχανισμούς που αναλύθηκαν στο κεφάλαιο 8. Αναλύεται επίσης μία εναλλακτική πρόταση που παρουσιάζει μικρότερο αριθμό ανταλλαγής μηνυμάτων.

- **Κεφάλαιο 10:**

Τέλος, αναφέρονται τα συμπεράσματα τη εργασίας, καθώς και μερικά προς περαιτέρω μελέτη θέματα που αφορούν την ασφάλεια του UMTS.

ΚΕΦΑΛΑΙΟ 2

Γενικά θέματα ασφάλειας

Σε αυτό το κεφάλαιο θα παρουσιάσουμε κάποιες βασικές γνώσεις σε θέματα ασφάλειας, αναγκαίες για την παρουσίαση της υπόλοιπης εργασίας. Η παράθεσή τους είναι σύντομη και εστιάζεται στις έννοιες που εμφανίζονται στα επόμενα κεφάλαια.

2.1 Ασφάλεια – βασικές έννοιες

Σε αυτή την ενότητα θα περιγράψουμε τις βασικότερες έννοιες επί των θεμάτων ασφαλείας. Δίνοντας τον γενικό ορισμό της ασφάλειας της Πληροφορίας (Information security) [41] θα λέγαμε πως είναι ο συνδυασμός της προστασίας της Διαθεσιμότητας , της εμπιστευτικότητας , της ακεραιότητας, και της αυθεντικότητας των πληροφοριών.

- *Διαθεσιμότητα (Information Availability)* είναι η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε Εξουσιοδοτημένους χρήστες.
- *Ακεραιότητα (Integrity)* είναι η αποφυγή Μη Εξουσιοδοτημένης τροποποίησης μιας Πληροφορίας.
- *Εμπιστευτικότητα(Confidentiality)* είναι η αποφυγή αποκάλυψης Πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους.
- *Αυθεντικότητα (Authenticity)* είναι η αποφυγή ατελειών και ανακριβειών κατά την διάρκεια των εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.

Επιπλέον των ανωτέρω θα δώσουμε κάποιες έννοιες που θα συναντήσουμε στην συνέχεια της παρουσίασης της εργασίας.

- *Αυθεντικοποίηση οντότητας (Entity Authentication)* είναι η διαδικασία επαλήθευσης του ισχυρισμού μιας οντότητας ότι κατέχει μια συγκεκριμένη ταυτότητα.
- *Εξουσιοδότηση (Authorization)* είναι η άδεια που παρέχεται από έναν ιδιοκτήτη πληροφοριών για ένα συγκεκριμένο σκοπό.
- *Αυθεντικοποίηση μηνύματος (message authentication)* είναι η επαλήθευση ότι ένα μήνυμα στάλθηκε από το συγκεκριμένο αποστολέα (πηγή) στον επιδιωκόμενο παραλήπτη χωρίς να μεταβληθεί, είναι γνωστή και ως αυθεντικοποίηση πηγής.

- Υπογραφή (*Signature*) είναι ένας τρόπος δέσμευσης μιας πληροφορίας με μία συγκεκριμένη οντότητα.
- Πιστοποίηση (*Certification*) είναι η επιβεβαίωση της πληροφορίας από μία Τρίτη έμπιστη οντότητα.
- Μη αποποίηση (*Non Repudiation*) είναι η αμοιβαία αυθεντικοποίηση της αποστολής και της παραλαβής δεδομένων από ένα υπολογιστικό συγκρότημα , με δυνατότητα παράλληλου ελέγχου της αυθεντικότητας του μηνύματος. Με την μη αποποίηση πετυχαίνουμε την εμπόδιση της άρνησης προηγούμενων δεσμεύσεων ή ενεργειών.
- Ανωνυμία(*anonymity*) είναι η μη δημοσίευση της ταυτότητας μιας οντότητας μου εμπλέκεται σε μία συναλλαγή.
- Ανάκληση (*revocation*) είναι η αναίρεση μιας πιστοποίησης ή μιας αυθεντικοποίησης.

Αφού δώσαμε τις σημαντικότερες έννοιες που διαπραγματεύεται η ασφάλεια ενός πληροφοριακού συστήματος θα προχωρήσουμε δίνοντας βασικές κρυπτογραφικές έννοιες.

2.2 Στοιχεία κρυπτογραφίας

Σε αυτή την ενότητα θα δώσουμε βασικές κρυπτογραφικές πληροφορίες που χρησιμοποιούνται στα επόμενα κεφάλαια. «Η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων» (Rivest 1990).

Μελετά μαθηματικούς τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή. Στοχεύει στο να πετύχει την Εμπιστευτικότητα , την Ακεραιότητα των δεδομένων, την Αυθεντικοποίηση και την Μη Αποποίηση. Πετυχαίνοντας αυτούς τους τέσσερις στόχους ασφαλείας, μπορεί να καλύψει και όλους τους άλλους. Οι κρυπτογραφικές τεχνικές που χρησιμοποιούνται και θα μας απασχολήσουν στην συνέχεια είναι η συμμετρική κρυπτογραφία, η ασύμμετρη κρυπτογραφία (Symmetric and asymmetric cryptography), οι συναρτήσεις σύνοψης (κατακερματισμού-Hash Functions), τεχνικές αυθεντικοποίησης, όπως ο κώδικας αυθεντικοποίησης μηνύματος (MAC- Message Authentication Code) και οι ψηφιακές υπογραφές.

2.2.1 Συμμετρική κρυπτογραφία

Ένα σχήμα συμμετρικής κρυπτογραφίας αποτελείται από πέντε οντότητες (σχήμα 2.1):

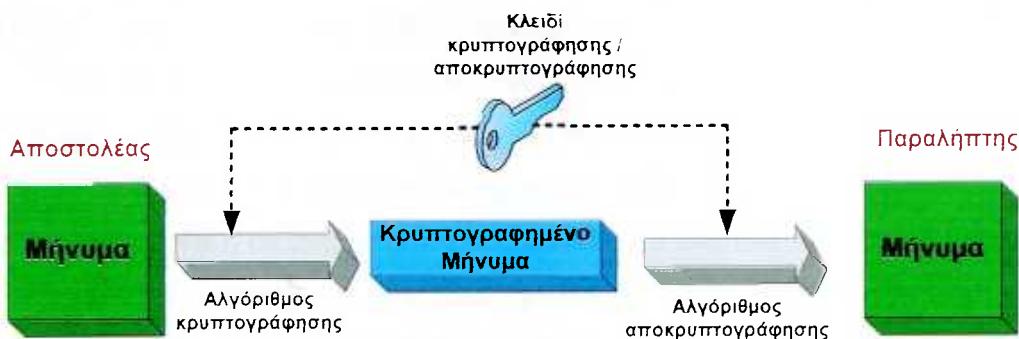
- Το αρχικό κείμενο (Plaintext). Είναι το αρχικό κείμενο ή τα αρχικά δεδομένα τα οποία αποτελούν την είσοδο στον αλγόριθμο κρυπτογράφησης.
- Ο αλγόριθμός κρυπτογράφησης (Encryption Algorithm). Ένας αλγόριθμος κρυπτογράφησης παίρνει ως είσοδο ένα αρχικό κείμενο (plaintext) και το μετασχηματίζει στο κρυπτογράφημα (ciphertext).
- Μυστικό κλειδί (secret Key). Αποτελεί την μυστική πληροφορία που εισάγεται μαζί με το αρχικό κείμενο στον αλγόριθμο κρυπτογράφησης. Είναι υπεύθυνο για τις ακριβείς αντικαταστάσεις και τους επιμέρους μετασχηματισμούς που πραγματοποιεί ο αλγόριθμος κρυπτογράφησης.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (Ciphertext) . Είναι το μετασχηματισμένο μήνυμα που εξάγεται από τον αλγόριθμο κρυπτογράφησης . Εξαρτάται τόσο από το μυστικό κλειδί , όσο και από το αρχικό μήνυμα.
- Ο αλγόριθμος αποκρυπτογράφησης (Decryption Algorithm) μετασχηματίζει το κρυπτογράφημα πίσω στο αρχικό κείμενο (plaintext) κάνοντας χρήση του ίδιου μυστικού κλειδιού .

Τα βήματα που ακολουθούνται είναι:

- Κάθε χρήστης διαθέτει ένα μυστικό κοινό κλειδί που χρησιμοποιείτε για την κρυπτογράφηση /αποκρυπτογράφηση.
- Εάν κάποιος χρήστης Α επιθυμεί να στείλει ένα εμπιστευτικό μήνυμα σε έναν χρήστη Β, τότε το κρυπτογραφεί με το κοινό μυστικό κλειδί και στέλνει το κρυπτογράφημα στον χρήστη Β.
- Ο Β μόλις λάβει το κρυπτογράφημα , μπορεί να το αποκρυπτογραφήσει κάνοντας χρήση το κοινό μυστικό τους κλειδί. Ένας τρίτος χρήστης που γνωρίζει το μυστικό κλειδί μπορεί να αποκρυπτογραφήσει το κρυπτογράφημα που ο Α έστειλε στον Β.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Για την ασφαλή χρήση της συμμετρικής κρυπτογραφίας απαιτείται η ύπαρξη ισχυρού αλγορίθμου κρυπτογράφησης (Encryption Algorithm) και ο αποστολέας και ο παραλήπτης να παραλάβουν με ασφαλή τρόπο το μυστικό κλειδί. Αυτή είναι και η αδυναμία της συμμετρικής κρυπτογραφίας δηλαδή η ασφαλή μεταφορά του μυστικού κλειδιού και για αυτό το λόγο πρέπει να αλλάζει τακτικά, ώστε ακόμα και αν κάποια στιγμή υποκλαπεί, ένα νέο να το αντικαταστήσει. Είναι σημαντικό να τονίσουμε πως στην συμμετρική κρυπτογραφία το μυστικό κλειδί είναι το ίδιο και για την διαδικασία κρυπτογράφησης και για την αντίστοιχη της αποκρυπτογράφησης. Οι ευρύτερα χρησιμοποιούμενοι αλγόριθμοι συμμετρικής κρυπτογραφίας είναι ο DES (Data Encryption standard), Triple DES και ο AES (Advanced Encryption Standard).



Σχήμα 2.1 Συμμετρική κρυπτογραφία

2.2.2 Κρυπτογραφία Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογραφία)

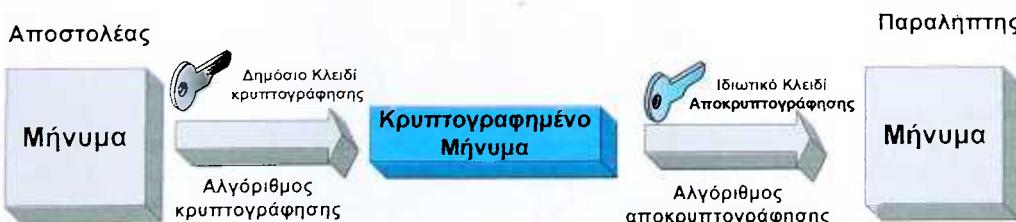
Η κρυπτογραφία δημόσιου κλειδιού είναι εξίσου σημαντική με την συμμετρική κρυπτογραφία. Χρησιμοποιείται κατά προτεραιότητα για αυθεντικοποίηση μηνυμάτων και διανομή μυστικών κλειδιών.

Η κρυπτογράφηση δημόσιου κλειδιού (Public Key encryption) προτάθηκε το 1976 από τους W.Diffie και M.Hellman. Οι αλγόριθμοι κρυπτογραφίας δημόσιου κλειδιού βασίζονται σε μαθηματικές πράξεις και όχι σε απλές πράξεις με bits. Η κρυπτογράφηση δημόσιου κλειδιού είναι ασύμμετρη (asymmetric) διότι χρησιμοποιεί δύο διαφορετικά κλειδιά σε αντίθεση με την συμμετρική που χρησιμοποιεί μόνο ένα. Η ασύμμετρη συγκριτικά με την συμμετρική δεν είναι πιο ισχυρή, καθώς η ισχύς ενός κρυπτογραφικού αλγορίθμου εξαρτάτε από το μήκος του κλειδιού (όσο πιο μεγάλο τόσο πιο ανθεκτικός).

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ένα σχήμα ασύμμετρης κρυπτογραφίας, (σχήμα 2.2), αποτελείται και αυτό από πέντε οντότητες. Αρχικό κείμενο, αλγόριθμο κρυπτογράφησης, ζεύγη κλειδιών, κρυπτογράφημα και αλγόριθμο αποκρυπτογράφησης. Η διαφορά με την συμμετρική είναι πως κάνουμε χρήση εδώ δύο ζευγών κλειδιών. Τα κλειδιά συσχετίζονται από μαθηματική άποψη έτσι ώστε ένα κλειδί του ζεύγους να εκτελεί μια λειτουργία στα δεδομένα που μόνο το άλλο κλειδί μπορεί να ανατρέψει. Το ένα ονομάζεται δημόσιο κλειδί και όπως υποδεικνύει το όνομα του είναι για δημόσια χρήση και το άλλο ονομάζεται ιδιωτικό και δεν αποκαλύπτεται σε κανέναν. Ένας γενικής χρήσης αλγόριθμος κρυπτογράφησης (αποκρυπτογράφησης) βασίζεται σε ένα δημόσιο κλειδί για την κρυπτογράφηση και σε ένα άλλο αλλά μοναδικά συσχετιζόμενο ιδιωτικό κλειδί για την αποκρυπτογράφηση. Τα βήματα που ακολουθούνται είναι:

- Κάθε χρήστης διαθέτει ένα ζεύγος μυστικών κλειδιών (Δημόσιο και Ιδιωτικό) που χρησιμοποιούνται για την κρυπτογράφηση /αποκρυπτογράφηση.
- Το δημόσιο κλειδί του κάθε χρήστη τοποθετείται σε μία βάση δεδομένων ενός έμπιστου φορέα ή σε ένα προσβάσιμο αρχείο. Το ιδιωτικό το κρατά ο χρήστης και διαφύλασσει την μυστικότητα του. Θα πρέπει για λόγους λειτουργικότητας το δημόσιο κλειδί ενός χρήστη να είναι εύκολα προσβάσιμο.
- Εάν κάποιος χρήστης Α επιθυμεί να στείλει ένα εμπιστευτικό μήνυμα σε έναν χρήστη Β, τότε το κρυπτογραφεί με το δημόσιο κλειδί του Β.
- Ο Β μόλις λάβει το κρυπτογράφημα, μπορεί να το αποκρυπτογραφήσει μόνο αυτός με το ιδιωτικό του κλειδί. Ένας τρίτος χρήστης που γνωρίζει το δημόσιο κλειδί του Β δεν μπορεί να αποκρυπτογραφήσει το κρυπτογράφημα που ο Α έστειλε στον Β.

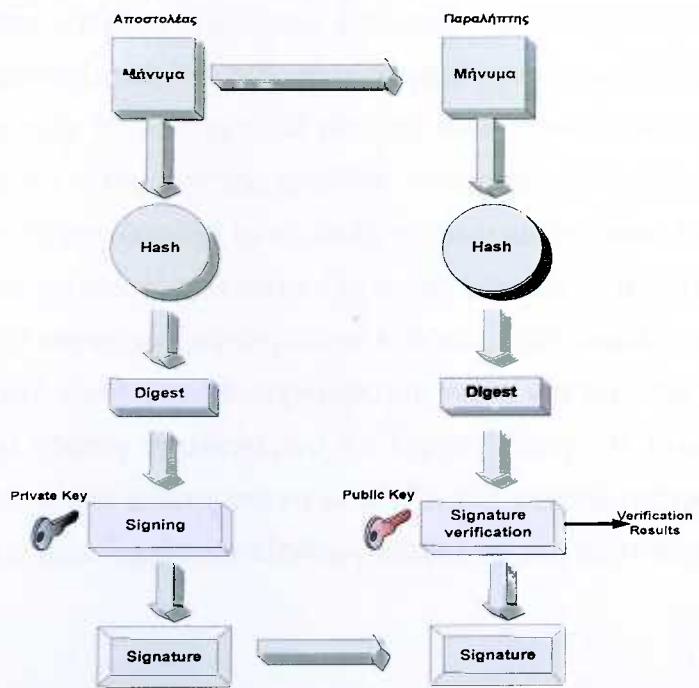


Είναι σημαντική προϋπόθεση όλοι οι χρήστες που παίρνουν μέρος σε ένα τέτοιο σχήμα, να έχουν πρόσβαση στα δημόσια κλειδιά των άλλων. Τα κρυπτοσυστήματα δημοσίου κλειδιού χρησιμοποιούνται για την κρυπτογράφηση/αποκρυπτογράφηση (Encryption/Decryption).

tion-Decryption), στις ψηφιακές υπογραφές (Digital Signature) και στις ανταλλαγές κλειδιών (Key Exchange).

2.2.3 Ψηφιακές υπογραφές (Digital Signatures)

Μπορούμε να χρησιμοποιήσουμε ένα ασύμμετρο κρυπτοσύστημα και με τον ακόλουθο τρόπο. Υποθέτουμε πως ένας χρήστης A επιθυμεί να αποστέλει ένα μήνυμα σε ένα χρήστη B. Μέσα στις απαιτήσεις επικοινωνίας δεν περιλαμβάνεται η εμπιστευτικότητα, αλλά η αυθεντικοποίηση του αποστολέα. Σε αυτή την περίπτωση ο χρήστης A κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί και το αποστέλλει στον χρήστη B. Ο χρήστης B γνωρίζοντας το δημόσιο κλειδί του A μπορεί να αποκρυπτογραφήσει τα δεδομένα και έχει εξασφαλίσει έτσι ότι το μήνυμα κρυπτογραφήθηκε από τον A (Αυθεντικοποίηση του A). Κανένας δεν γνωρίζει το ιδιωτικό κλειδί του A, συνεπώς μόνο αυτός μπορεί να δημιουργήσει κρυπτογραφήματα, που να αποκρυπτογραφούνται από το δημόσιο κλειδί του. Έτσι όλο το κρυπτογραφημένο κείμενο αποτελεί την ψηφιακή υπογραφή (Digital Signature) του χρήστη A (σχήμα 2.3).



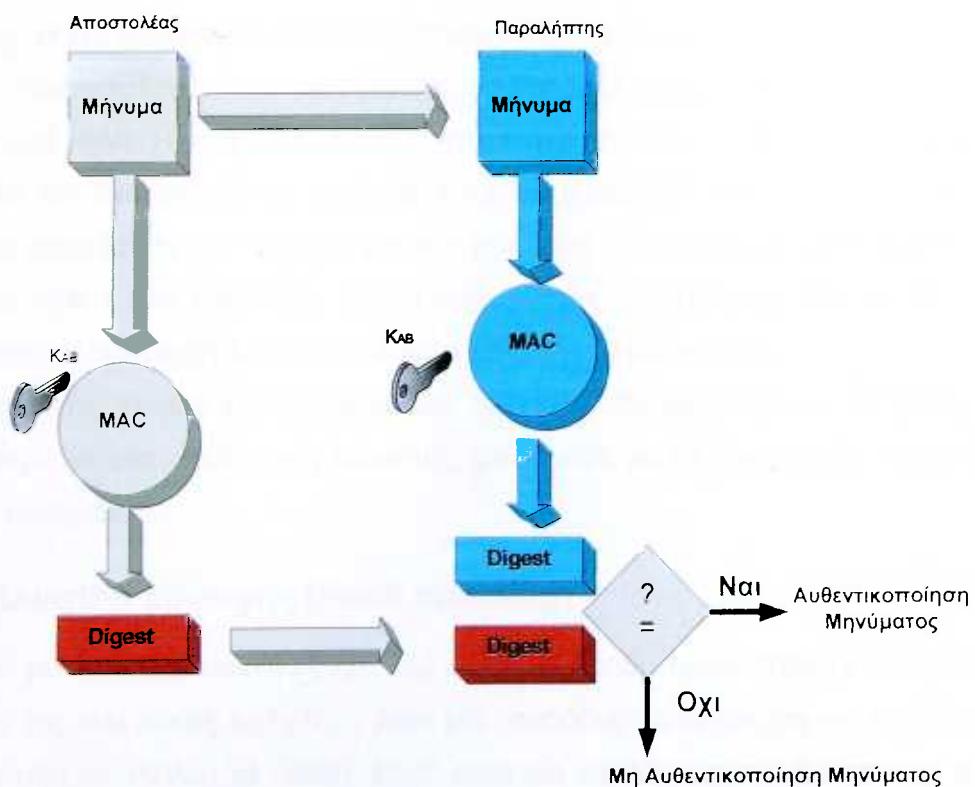
Σχήμα 2.3 Ψηφιακή υπογραφή.

2.2.4 Μιας χρήσης Υπογραφή (One-Time Signing):

Οι συμβατικοί ψηφιακοί μηχανισμοί υπογραφών όπως οι RSA και DSA είναι πολύ ακριβοί υπολογιστικά. Η Μιας χρήσης (one-time) υπογραφή είναι μία γρήγορη εναλλακτική λύση, με αντάλλαγμα την παροχή πιο αδύνατης ασφάλειας, που περιορίζει τη χρήση ενός ζευγαριού των one-time ιδιωτικών/δημόσιων κλειδιών σε ένα μόνο μήνυμα. Η γενική ιδέα ενός one-time σχεδίου υπογραφών είναι ότι το ιδιωτικό κλειδί χρησιμοποιείται ως εισαγωγή σε μια ακολουθία μονόδρομων συναρτήσεων που οδηγούν σε μια ακολουθία ενδιάμεσων αποτελεσμάτων και τελικά στο δημόσιο κλειδί. Η μονόδρομη σχέση της συνάρτησης υπονοεί ότι είναι απραγματοποίητο να υπολογιστεί το ιδιωτικό κλειδί, ή οποιοδήποτε ενδιάμεσο αποτέλεσμα του υπολογισμού, από το δημόσιο κλειδί. Μια υπογραφή για ένα δεδομένο μήνυμα αποτελείται από ένα υποσύνολο των ενδιάμεσων αποτελεσμάτων αυτού του υπολογισμού, όπου το μήνυμα που υπογράφεται καθορίζει ποιο ιδιαίτερο υποσύνολο αποκαλύπτεται ως αντίστοιχη υπογραφή. Για να ελέγξει μια one-time υπογραφή, ένας παραλήπτης, εφαρμόζει ένα υποσύνολο των μονόδρομων υπολογισμών στην one-time υπογραφή. Εάν το αποτέλεσμα αυτών των υπολογισμών είναι ίσο με το δημόσιο κλειδί, κατόπιν η one-time υπογραφή επιβεβαιώνεται. Ένα one-time σχέδιο υπογραφών επιτρέπει την υπογραφή μόνο ενός ενιαίου μηνύματος χρησιμοποιώντας ένα δεδομένο ζευγάρι των ιδιωτικών/δημόσιων κλειδιών. Ένα πλεονέκτημα ενός τέτοιου σχεδίου είναι ότι είναι γενικά αρκετά γρήγορο. Εντούτοις, είναι γνωστό ότι η παραχθείσα one-time υπογραφή είναι αρκετά μεγάλη. Εκτός αυτού, δεδομένου ότι ένα ζευγάρι των one-time (ιδιωτικό/δημόσιο) κλειδιών μπορεί να χρησιμοποιηθεί για να υπογράψει μόνο ένα ενιαίο μήνυμα, ο αποστολέας πρέπει για να εκδώσει ένα νέο πιστοποιητικό δημόσιου κλειδιού, κάθε φορά που αλλάζει αυτό το ζευγάρι των κλειδιών. Αυτή η πολύ συχνή ανάγκη για τα νέα δημόσια κλειδιά μπορεί να προκαλέσει υψηλό κόστος υπολογισμού και εύρους ζώνης. Η K-χρονική υπογραφή έκφρασης χρησιμοποιείται επίσης για να υποδείξει ένα σχέδιο υπογραφών του οποίου το ζευγάρι των ιδιωτικών/δημόσιων κλειδιών μπορεί να χρησιμοποιηθεί για K μηνύματα το πολύ-πολύ.

2.2.5 Κώδικας Αυθεντικοποίησης Μηνυμάτων (MAC –Message Authentication Code)

Μία τεχνική αυθεντικοποίησης μηνύματος είναι ο Κώδικας Αυθεντικοποίησης Μηνυμάτων (MAC –Message Authentication Code). Στην τεχνική αυτή απαιτείται η χρήση ενός μυστικού κλειδιού, ώστε να παραχθεί ένα μικρό τμήμα δεδομένων το οποίο προσαρτάται στο μήνυμα. Έστω ότι έχουμε δύο χρήστες A και B που γνωρίζουν ένα μυστικό κλειδί K_{AB} και θέλουν να επικοινωνήσουν. Όταν ο A θέλει να στείλει ένα μήνυμα στον B, τότε υπολογίζει το MAC σαν συνάρτηση του μηνύματος και του μυστικού κλειδιού. Το MAC επισυνάπτεται στο μήνυμα που αποστέλλεται στον B. Ο B εκτελεί τον ίδιο υπολογισμό και συγκρίνει τα MAC, εάν είναι ίδια τότε ο παραλήπτης επιβεβαιώνει την ακεραιότητα του μηνύματος, ότι δηλαδή δεν έχει αλλαχθεί κατά την μετάδοση του, επιβεβαιώνει ακόμα ότι το μήνυμα προέρχεται από τον συγκεκριμένο αποστολέα που μοιράζονται την γνώση του μυστικού κλειδιού. Πετυχαίνουμε δηλαδή τον έλεγχο ακεραιότητας και την αυθεντικοποίηση του μηνύματος (σχήμα 2.4).



Σχήμα 2.4 Κώδικας Αυθεντικοποίησης Μηνυμάτων

2.2.6 Μονόδρομες συναρτήσεις Σύνοψης (One Way Hash Function)

Μία τεχνική για να διασφαλίσουμε την ακεραιότητα ενός μηνύματος είναι και οι Μονόδρομες συναρτήσεις Σύνοψης(One Way Hash Function). Μία τέτοια συνάρτηση δέχεται ως είσοδο ένα μήνυμα M αυθαίρετου μήκους και παράγει ως έξοδο μία σύνοψη (Hash ή Digest) $H(M)$ σταθερού μήκους. Σε αντίθεση με το MAC, μία συνάρτηση σύνοψης δεν χρειάζεται την γνώση ενός μυστικού κλειδιού. Η συνάρτηση H πρέπει να επιλεγεί έτσι ώστε να είναι:

- Εύκολος ο υπολογισμός της $H(M)$
- Έχοντας δεδομένη την $y=H(M)$ να είναι υπολογιστικά απραγματοποίητο να βρεθεί το M .
- Να είναι υπολογιστικά απραγματοποίητο να βρεθεί M και M' , (δηλαδή δύο διαφορετικά μηνύματα), τέτοια ώστε $H(M)=H(M')$ (Αντίσταση στην σύγκρουση (collision resistant)).

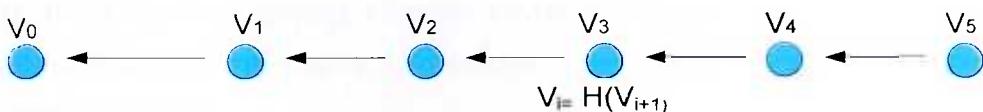
Έστω ότι έχουμε δύο χρήστες A και B που έχουν συμφωνήσει σε μία συνάρτηση σύνοψης H και θέλουν να επικοινωνήσουν. Όταν ο A θέλει να στείλει ύποτη ένα μήνυμα M στον B , τότε υπολογίζει την τιμή $H(M)$ και στην συνέχεια στέλνει μαζί με το μήνυμα M και την τιμή $H(M)$. Η τιμή $H(M)$ επισυνάπτεται στο μήνυμα που αποστέλλεται στον B . Ο B εκτελεί τον ίδιο υπολογισμό γνωρίζοντας το μήνυμα M' που παρέλαβε και την συνάρτηση συνόδου H και παράγει μία νέα τιμή $H(M')$. Στην συνέχεια συγκρίνει τις τιμές $H(M)$ και $H(M')$, εάν είναι ίδιες τότε ο παραλήπτης επιβεβαιώνει την ακεραιότητα του μηνύματος , ότι δηλαδή δεν έχει αλλαχθεί κατά την μετάδοση του.

Κάνοντας χρήση κρυπτογραφικών τεχνικών (Συμμετρικών – Ασύμμετρων) σε συνδυασμό με μία συνάρτηση σύνοψης, μπορούμε να πετύχουμε και την αυθεντικοποίηση μηνυμάτων.

2.2.7 Αλυσίδα Σύνοψης (Hash chaining)

Μία μονόδρομη αλυσίδα (V_0, \dots, V_n) είναι μία ομάδα τιμών τέτοιων ώστε, κάθε τιμή V_i (εκτός της τελευταίας τιμής V_n), είναι μία μονόδρομη συνάρτηση της επόμενης τιμής V_{i+1} . Δηλαδή $V_i = H(V_{i+1})$, με $0 \leq i \leq N$. Η H είναι μία μονόδρομη συνάρτηση και συνήθως επιλέγεται μία κρυπτογραφική συνάρτηση σύνοψης, γι' αυτό και η αλυσίδα λέγεται α-

λυσίδα σύνοψης. Για την δημιουργία της μονόδρομης αλυσίδας, η γεννήτρια επιλέγει μία τυχαία τιμή ως πυρήνα, (ρίζα), της αλυσίδας. Παράδειγμα την τιμή V_N και εξάγει από αυτή όλες τις προηγούμενες τιμές V_i εφαρμόζοντας επαναληπτικά την συνάρτηση σύνοψης όπως περιγράψαμε παραπάνω. Η τιμή V_0 που την ονομάζουμε τελική τιμή, συνήθως είναι δημόσια γνωστή, και συνδέεται με την ταυτότητα του χρήστη που επεξεργάζεται την τιμή του πυρήνα. Ένα παράδειγμα μίας σύνοψης αλυσίδας φαίνεται στο σχήμα 2.5.



Σχήμα 2.5 Αλυσίδα σύνοψης (Hash chaining)

Επαλήθευση των τιμών μίας σύνοψης αλυσίδας. Ας υποθέσουμε ότι αυτός που θέλει να επαληθεύσει τις τιμές της αλυσίδας, ξέρει μία τιμή της αλυσίδας και συνήθως αυτή είναι η τελευταία τιμή V_0 που είναι και δημόσια. Για να επαληθεύσει μία τιμή V_i της αλυσίδας, εκτελεί επαναληπτικά την μονόδρομη συνάρτηση H i φορές και συγκρίνει το αποτέλεσμα με την τιμή V_0 . Δηλαδή επαληθεύει ότι η τιμή $H_i(V_i)$ ισούται με V_0 . Αν η υπολογισθείσα τιμή και η γνωστή είναι ίδιες, τότε η τιμή V_i είναι αυθεντική. Αν μία άλλη τιμή V_k για $k < i$ είναι ήδη γνωστή, τότε είναι αρκετό να εκτελεστεί επαναληπτικά η μονόδρομη συνάρτηση i-k φορές και να συγκριθεί το αποτέλεσμα με αυτή την ενδιάμεση τιμή.

Καθώς υπολογίζονται οι τιμές της αλυσίδας, είτε αποθηκεύονται στη μνήμη, είτε υπολογίζονται κάθε φορά από την αρχή από τον πυρήνα.

Δεδομένης μιας έγκυρης τιμής V_i της αλυσίδας, είναι ακατόρθωτο να βρεθεί μία τιμή V_j όπου $j > i$ τέτοια ώστε $H^{j-i}(V_j) = V_i$.

ΚΕΦΑΛΑΙΟ 3

Αρχιτεκτονική κινητών δικτύων

Η πρώτη γενεά των δικτύων κινητής τηλεφωνίας (PLMN) χαρακτηρίζεται από την χρήση αναλογικού ασύρματου δικτύου πρόσβασης, ενώ η δεύτερη γενεά (GSM) χαρακτηρίζεται από την χρήση ψηφιακού. Οι πρώτες δύο γενεές δικτύων κινητής τηλεφωνίας σχεδιάζονται και βελτιστοποιούνται για μετάδοση φωνής. Έχουν το ίδιο χαρακτηριστικό, της αποκλειστικής χρήσης κάποιου καναλιού του ασύρματου δικτύου πρόσβασης, κατά τη διάρκεια της κλήσης. Το κεντρικό δίκτυο είναι μεταγωγής κυκλώματος (circuit switched, CS).

Στο General Packet Radio System (GPRS), που καλείται και 2.5G, η περιοχή μεταγωγής πακέτων (PS) προστίθεται στο κυρίως δίκτυο, για να υποστηρίξει υπηρεσίες/εφαρμογές που απαιτούν τέτοιου είδους κίνηση. Το δίκτυο GPRS μπορεί να παρέχει τους χρήστες ρυθμό μετάδοσης μέχρι 171,2 Kbps.

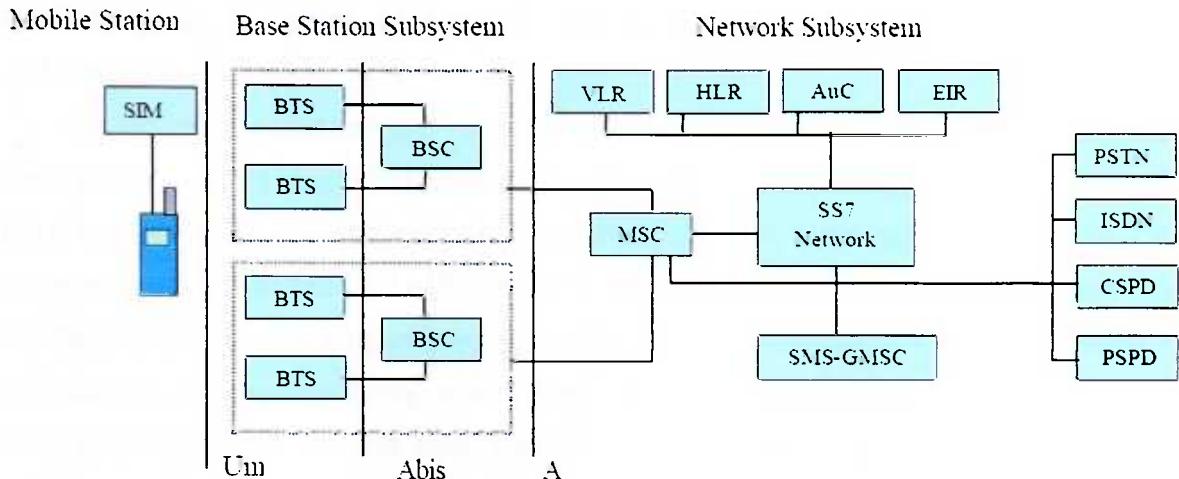
Στην τρίτη γενεά (3G), η αρχιτεκτονική του κεντρικού δικτύου παραμένει η ίδια με την 2.5G. Εντούτοις, οι αλληλεπιδράσεις μεταξύ των κόμβων του δικτύου είναι διαφορετικές. Παραδείγματος χάριν, η περιοχή μεταγωγής κυκλώματος μπορεί να έχει πολύ μικρό ρόλο και όλες οι υπηρεσίες φωνής να μεταβιβάζονται δια μέσου της περιοχής μεταγωγής πακέτων με τη χρήση της τεχνολογίας (VoIP). Η σημαντικότερη εξέλιξη στα 3G δίκτυα, είναι η τεχνολογία που χρησιμοποιείται στο ασύρματο δίκτυο πρόσβασης. Η κύρια τεχνολογία που χρησιμοποιείται είναι η CDMA. Αυτή η τεχνολογία κάνει δυνατούς ρυθμούς μετάδοσης μέχρι 2 Mbps.

Σε αυτό το κεφάλαιο θα κάνουμε μία σύντομη περιγραφή της αρχιτεκτονικής των παραπάνω αναφερομένων δικτύων.

3.1 Αρχιτεκτονική GSM

Ένα δίκτυο GSM [40] απαρτίζεται από αρκετές δικτυακές οντότητες, όπως φαίνεται και στο σχήμα 3.1, και χωρίζεται σε τρία μέρη: τον κινητό σταθμό, το υποσύστημα σταθμού βάσης και το υποσύστημα δικτύου.

Ασφάλεια και διαχείριση κλειδιών στο UMTS



Σχήμα 3.1 Αρχιτεκτονική GSM [23]

Ο Κινητός Σταθμός (Mobile Station – MS) είναι η τερματική συσκευή που έχει μαζί του ο χρήστης της κινητής τηλεφωνίας (κινητό τηλέφωνο, φορητός υπολογιστής συνδεδεμένος με το κινητό τηλέφωνο, κτλ.). Το κινητό τηλέφωνο περιέχει μια «έξυπνη» κάρτα, που ονομάζεται SIM (Subscriber Identity Card) και περιέχει πληροφορίες για το συνδρομητή της κινητής τηλεφωνίας. Έτσι, ο χρήστης μπορεί να αλλάξει συσκευή αλλά να εξακολουθεί να χρησιμοποιεί την ίδια SIM κάρτα, διατηρώντας τον ίδιο αριθμό και την ίδια συνδρομή. Η SIM κάρτα περιέχει το Διεθνές Αναγνωριστικό Συνδρομητή Κινητής Τηλεφωνίας (International Mobile Subscriber Identity – IMSI), που είναι μοναδικό για κάθε συνδρομητή και χρησιμοποιείται για να γνωστοποιήσει στο σύστημα την ταυτότητα του χρήστη, καθώς και για τις διαδικασίες αυθεντικοποίησης. Επιπλέον, κάθε τερματική συσκευή αναγνωρίζεται μοναδικά από το Διεθνές Αναγνωριστικό Ασύρματης Συσκευής (International Mobile Equipment Identity – IMEI).

Το Υποσύστημα Σταθμού Βάσης (Base Station Subsystem – BSS) απαρτίζεται από δύο οντότητες: τον Πομποδέκτη του Σταθμού Βάσης (Base Transceiver Station – BTS) και τον Ελεγκτή του Σταθμού Βάσης (Base Station Controller – BSC). Η λειτουργία του BTS είναι να λαμβάνει και να εκπέμπει ραδιοσήματα από και προς τους κινητούς σταθμούς, να επεξεργάζεται τα σήματα, να (απο)κωδικοποιεί τη φωνή και να προσαρμόζει τον ρυθμό μετάδοσης. Ένας BTS υλοποιεί μία κυψέλη του συστήματος GSM. Πολλοί BTSs ελέγχονται από έναν BSC. Ο BSC ευθύνεται για την διαχείριση των ασύρματων πόρων. Δηλαδή ασχολείται με την διανομή των καναλιών στους κινη-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

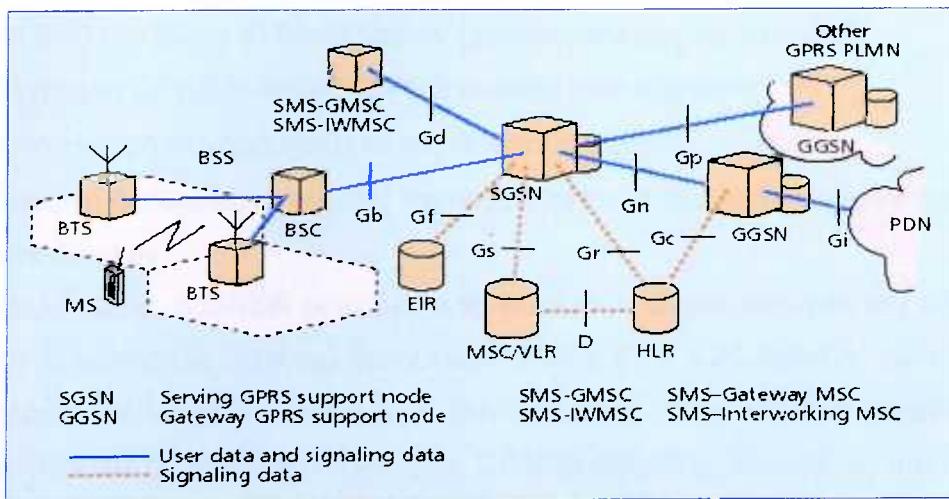
τούς σταθμούς, την άρση της διανομής, την αλλαγή συχνότητας και το χρονισμό των ραδιοσημάτων.

Η κεντρική μονάδα του υποσυστήματος του κεντρικού δικτύου (Network Subsystem – NSS) είναι το Κέντρο Μεταγωγής (Mobile Switching Center – MSC). Οι ροές που προέρχονται από τους κινητούς σταθμούς στις αντίστοιχες κυψέλες, δρομολογούνται μέσω του MSC. Ο MSC παρέχει όλη τη λειτουργικότητα που χρειάζεται για την διαχείριση ενός χρήστη κινητής τηλεφωνίας, όπως εγγραφή στην υπηρεσία κινητής τηλεφωνίας, αυθεντικοποίηση, τοπολογική ενημέρωση και δρομολόγηση κλήσης για τους χρήστες που βρίσκονται εκτός αρχικού δικτύου. Οι ροές από και προς ένα σταθερό δίκτυο τηλεφωνίας (π.χ. PSTN, ISDN, PDN) διαχειρίζονται από ένα αφιερωμένο γι' αυτή τη δουλειά Κέντρο Μεταγωγής (Gateway Mobile Switching Center – GMSC). Τα GSM δίκτυα είναι ιεραρχικά δομημένα. Αποτελούνται από τουλάχιστον μία διοικητική περιοχή που ανατίθεται σε έναν MSC. Κάθε διοικητική περιοχή αποτελείται από τουλάχιστον μία τοπολογική περιοχή (Location Area – LA). Η κάθε τοπολογική περιοχή απαρτίζεται από πολλά σύνολα κυψελών. Κάθε σύνολο κυψελών ανατίθεται σε έναν BSC. Ένα σύνολο από βάσεις δεδομένων είναι διαθέσιμες για τον έλεγχο κλήσεων και τη διαχείριση δικτύου: το HLR (Home Location Register), το VLR (Visitor Location Register), το AUC (Authentication Center) και το EIR (Equipment Identity Register. Για όλους τους χρήστες που είναι συνδρομητές σε έναν παροχέα κινητής τηλεφωνίας, τα μόνιμα δεδομένα (όπως το προφίλ του χρήστη) καθώς και κάποια προσωρινά δεδομένα (όπως η τρέχουσα θέση του χρήστη) αποθηκεύονται στο HLR. Στην περίπτωση που υπάρχει κλήση για έναν χρήστη, το HLR είναι πάντα η πρώτη βάση που ερωτάται για την τρέχουσα τοποθεσία του χρήστη. Το VLR είναι υπεύθυνο για ένα σύνολο περιοχών και αποθηκεύει δεδομένα για τους χρήστες που είναι την τρέχουσα στιγμή μέσα στην περιοχή της δικαιοδοσίας του. Αυτό σημαίνει ότι και μέρος από τα μόνιμα δεδομένα ενός χρήστη μεταφέρονται από το HLR στο υπεύθυνο VLR για γρηγορότερη προσπέλαση. Παρόλα αυτά, και το VLR μπορεί να αποθηκεύσει προσωρινά δεδομένα για δική του χρήστη. Τα άλλα δύο μητρώα, το AUC και το EIR χρησιμοποιούνται για θέματα ασφάλειας και αυθεντικοποίησης. Το AUC είναι μια προστατευμένη βάση δεδομένων που αποθηκεύει ένα αντίγραφο του μυστικού κλειδιού της SIM κάρτας κάθε συνδρομητή, το οποίο χρησιμοποιείται για αυθεντικοποίηση και κρυπτογράφηση πάνω

από το ασύρματο κανάλι. Το EIR είναι μια βάση που περιέχει μια λίστα με όλα τις έγκυρες συσκευές κινητής τηλεφωνίας του δικτύου. Κάθε κινητός σταθμός αποθηκεύεται στη βάση με το αντίστοιχο αναγνωριστικό του (IMEI). Ένας κινητός σταθμός μπορεί να θεωρηθεί άκυρος αν το κινητό έχει δηλωθεί ως κλεμμένο ή αν δεν είναι συμβατού τύπου.

3.2 Αρχιτεκτονική GPRS

Όπως έχει ήδη αναφερθεί, το GPRS, που αναπτύχθηκε από το ETSI [40], μπορεί να θεωρηθεί ως ένα επιπλέον επίπεδο πάνω από το υπάρχον δίκτυο GSM, με σκοπό να εξυπηρετήσει μετάδοση δεδομένων με τεχνικές μεταγωγής πακέτου. Η λογική υλοποίηση της τεχνολογίας GPRS από ένα GSM δίκτυο περιλαμβάνει μετατροπές στο λογισμικό και προσθέσεις στο υλικό των δομικών στοιχείων του GSM, αλλά και την εισαγωγή δύο νέων κόμβων στο δίκτυο. Οι δύο νέοι αυτοί κόμβοι είναι ο SGSN (Serving GPRS Support Node) και ο GGSN (Gateway GPRS Support Node). Μαζί με τους δύο αυτούς κόμβους χρησιμοποιήθηκαν νέες διεπαφές και νέα πρωτόκολλα επικοινωνίας μεταξύ των δομικών στοιχείων του GPRS δικτύου (σχήμα 3.2).



Σχήμα 3.2 Αρχιτεκτονική GPRS

Ο SGSN είναι υπεύθυνος για την παράδοση των πακέτων από και προς τους κινητούς σταθμούς που βρίσκονται μέσα στην περιοχή εξυπηρέτησής του. Βρίσκεται στο

Ασφάλεια και διαχείριση κλειδιών στο UMTS

ίδιο ιεραρχικό επίπεδο με τον MSC/VLR και ουσιαστικά κάνει ό,τι και ο MSC/VLR για το δίκτυο μεταγωγής κυκλώματος. Πιο συγκεκριμένα είναι υπεύθυνος για τις ακόλουθες λειτουργίες:

- Δρομολόγηση και μεταγωγή πακέτων από και προς τους κινητούς σταθμούς που βρίσκονται στην περιοχή εξυπηρέτησής του (packet routing and switching)
- Διαχείριση της συνόδου (session management)
- Διαχείριση της μεταφερσιμότητας των κινητών σταθμών (mobility management)
- Διαχείριση της λογικής ζεύξης (logical link management)
- Κρυπτογράφηση και αυθεντικοποίηση (ciphering and authentication)
- Εξαγωγή δεδομένων χρέωσης για κάθε κινητό σταθμό, που σχετίζονται με την χρήση των ασύρματων πόρων του δικτύου

Ο GGSN είναι ο κύριος υπεύθυνος για την διασύνδεση του GRPS δικτύου (PLMN) με τα εξωτερικά δίκτυα μεταφοράς πακέτων. Πιο συγκεκριμένα επιτελεί τις ακόλουθες λειτουργίες:

- Παροχή διεπαφής προς τα εξωτερικά δίκτυα δεδομένων. Σχετικά με την μεταγωγή πακέτων σε IP εξωτερικά δίκτυα, ο GGSN έχει λειτουργίες για παροχή ISP υπηρεσιών. Αποτέλεσμα των παραπάνω είναι, οι κόμβοι των εξωτερικών δικτύων με τα οποία επτικοινωνεί, να τον βλέπουν ως έναν δρομολογητή που κάνει μεταγωγή πακέτων για το δικό του χώρο IP διευθύνσεων (χρήστες κινητής τηλεφωνίας).
- Διαχείριση GPRS συνόδου (GPRS session management)
- Αντιστοίχηση συνδρομητών στους σωστούς SGSNs
- Εξαγωγή δεδομένων χρέωσης που σχετίζονται με την χρήση πόρων των εξωτερικών δικτύων

Με άλλα λόγια, ο GGSN μετατρέπει τα πακέτα που έρχονται από τον SGSN στο κατάλληλο πρωτόκολλο πακέτου δεδομένων (PDP), IP ή X.25 δηλαδή, και τα στέλνει στο εξωτερικό δίκτυο με το οποίο είναι συνδεδεμένος. Στην αντίθετη κατεύθυνση, ο GGSN μετατρέπει τις PDP διευθύνσεις σε GSM διευθύνσεις. Έπειτα, το πακέτο μεταφέρεται στον αντίστοιχο SGSN. Διαφαίνεται λοιπόν, ότι υπάρχει μια πολλά προς πολλά σχέση μεταξύ SGSN και GGSN. Ένα GPRS δίκτυο μπορεί να έχει πολλούς SGSNs, αλλά έχει έναν GGSN για κάθε εξωτερικό δίκτυο με το οποίο διασυνδέεται.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ένας SGSN μπορεί να δρομολογεί πακέτα σε πολλούς GGSNs για να φτάσουν σε διαφορετικά εξωτερικά δίκτυα.

Οι υπόλοιποι κόμβοι του GPRS δίκτυου έχουν παραμείνει από την αρχιτεκτονική του GSM δίκτυου, με κάποιες μικρές μετατροπές έτσι ώστε να υποστηρίζουν και την μετάδοση πακέτων. Έτσι ο BSS είναι υπεύθυνος για την εγκαθίδρυση, την εποπτεία και την αποσύνδεση των συνόδων μεταγωγής πακέτων. Επίσης, έχει όλες τις λειτουργίες που απαιτούνται για την εκχώρηση καναλιού επικοινωνίας, την ρύθμιση παραμέτρων της κυψέλης και την παροχή διεπαφής με τον SGSN (διεπαφή Gb).

Τέλος, προστέθηκε μια νέα οντότητα στον BSS, η Μονάδα Ελέγχου Πακέτων (Packet Control Unit – PCU) που θα υλοποιεί ουσιαστικά την Gb διεπαφή και θα ελέγχει και εποπτεύει τα κανάλια μετάδοσης πακέτων στο ασύρματο δίκτυο πρόσβασης.

Ο MSC/VLR πρέπει και αυτός να αναβαθμιστεί ώστε να υποστηρίζει την Gs διεπαφή με τον SGSN. Η διεπαφή αυτή περιλαμβάνει σηματοδοσία μεταξύ των MSC/VLR και του SGSN ώστε να υπάρχει συντονισμός στις λειτουργίες διαχείρισης της μεταφερσιμότητας των κινητών σταθμών, τόσο στην κατάσταση μεταγωγής κυκλώματος όσο και στην κατάσταση μεταγωγής πακέτου. Με τον τρόπο αυτό, ένας κινητός σταθμός που βρίσκεται σε κατάσταση μεταγωγής πακέτου, μπορεί να ειδοποιηθεί μέσα από ένα κανάλι μετάδοσης δεδομένων ότι έχει μία τηλεφωνική κλήση (μεταγωγή κυκλώματος), να αλλάξει την κατάστασή του σε μεταγωγή κυκλώματος, να δεχθεί την κλήση, και μετά το τέλος της κλήσης να αλλάξει κατάσταση και να συνεχίσει την μετάδοση δεδομένων. Βέβαια, για να γίνουν τα παραπάνω θα πρέπει ο κινητός σταθμός να είναι κλάσης B.

Ο HLR πρέπει και αυτός να αναβαθμιστεί ώστε να μπορούν να αποθηκεύονται σε αυτόν και νέου τύπου δεδομένα. Ο νέος HLR αποθηκεύει στη βάση δεδομένων του το προφίλ του χρήστη (π.χ. παράμετροι ποιότητας υπηρεσίας), την τρέχουσα SGSN διεύθυνση και την PDP διεύθυνση (ή και διευθύνσεις) για κάθε χρήστη που βρίσκεται στο δίκτυο (PLMN). Η διεπαφή Gr χρησιμοποιείται για ανταλλαγή πληροφοριών ανάμεσα στον SGSN και τον HLR (π.χ. ενημέρωση του HLR από τον SGSN για το που βρίσκεται ο κινητός σταθμός). Όταν ένας κινητός σταθμός εγγραφεί σε έναν νέο SGSN, τότε ο HLR θα στείλει στον SGSN το προφίλ του χρήστη. Η διεπαφή Gc χρησιμοποιείται συνήθως από τον GGSN για ενημερώσεις τη βάση του με τα τρέχοντα στοιχεία για έναν χρήστη.

Οι διεπαφές Gn και Gp ορίζονται μεταξύ δυο SGSNs για να ανταλλάσσουν προφίλ χρηστών όταν ένας κινητός σταθμός μετακινείται από έναν SGSN σε έναν άλλον. Μέσω της διεπαφής Gf ο SGSN μπορεί να μάθει πληροφορίες για το IMEI ενός κινητού σταθμού που προσπαθεί να εγγραφεί στο δίκτυο. Τέλος, η διεπαφή Gi διασυνδέει το δημόσιο δίκτυο ξηράς της κινητής τηλεφωνίας (PLMN) με εξωτερικά δημόσια ή ιδιωτικά δίκτυα μεταγωγής πακέτου (PDNs), όπως το Διαδίκτυο ή ιδιωτικά εσωτερικά δίκτυα. Υποστηρίζονται διεπαφές προς IP (IPv4 και IPv6) και X.25 δίκτυα.

3.3 Αρχιτεκτονική του UMTS

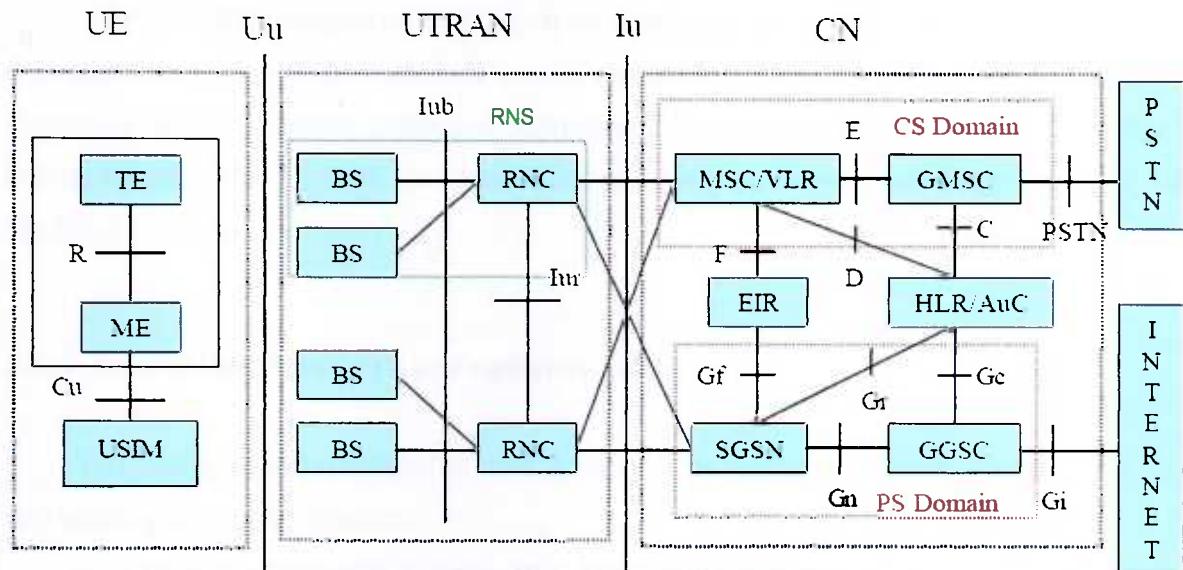
Το UMTS έχει τυποποιηθεί σε διάφορες εκδόσεις, που αρχίζουν από την έκδοση 1999 (R99), κατόπιν η έκδοση 4 (rel-4), σε συνέχεια η 5 (rel-5), ακολουθεί η 6 (rel-6), και την ώρα που γράφεται αυτή η εργασία προτυποποιείται η 7 (rel-7). Ο κύριος στόχος του είναι να παράσχει ένα ευρύ φάσμα εφαρμογών πολυμέσων πραγματικού χρόνου με διαφοροποιημένα επίπεδα ποιότητας υπηρεσιών στους κινητούς χρήστες. Η θεμελιώδης διαφορά μεταξύ GSM/GPRS και του UMTS R99 είναι ότι το τελευταίο υποστηρίζει τα υψηλότερους ρυθμούς πρόσβασης (μέχρι 2 Mbps) [8]. Αυτό επιτυγχάνεται μέσω μιας νέας ευρυζωνικής ασύρματης πρόσβασης στο κυρίως δίκτυο (WCDMA), που ονομάζεται UMTS επίγειο κινητό δίκτυο ραδιο πρόσβασης (UMTS Terrestrial Access Network (UTRAN)). Το σχήμα 3.3 απεικονίζει τη γενική δικτυακή αρχιτεκτονική του UMTS.

Ενώ το UMTS R99 είναι μια λογική εξέλιξη της αρχιτεκτονικής του συστήματος 2G, Τα UMTS rel-4 και rel-5 είναι επαναστατικά, εισάγοντας νέες έννοιες και προηγμένα χαρακτηριστικά γνωρίσματα [8]. Ένα σημαντικό σημείο διαφοροποίησης είναι η μετατόπιση προς μια δικτυακή αρχιτεκτονική στηριζόμενη στην μεταγωγή πακέτων (στο πρωτόκολλο IP) που τελικά θα αντικαταστήσει τη τεχνολογία μεταγωγής κυκλώματος. Μια άλλη διαφορά είναι η ενσωμάτωση μιας ανοικτής αρχιτεκτονικής παροχής υπηρεσιών, η οποία επιτρέπει σε τρίτα δίκτυα να παρέχουν πρόσβαση στις υπηρεσίες UMTS. Επομένως, η εξέλιξη της αρχιτεκτονικής του δικτύου UMTS δηλώνει όχι μόνο μια μετατόπιση προς μια κοινή πλατφόρμα, βασισμένη στο IP, η οποία εγγυάται την



Ασφάλεια και διαχείριση κλειδιών στο UMTS

αλληλεπίδραση με υπάρχοντα και προσεχή δίκτυα, αλλά και μια μετατόπιση προς ένα ανοικτό και με πολλούς τρόπους προσπελάσιμο δίκτυο.



Σχήμα 3.3 Αρχιτεκτονική UMTS [23]

Όπως φαίνεται και από το ανωτέρω σχήμα, τρία είναι τα κύρια μέρη που αποτελούν ένα δίκτυο τρίτης γενιάς, το UE, το UTRAN και το CN, με τις διεπαφές Uu και Iu να τα συνδέουν μεταξύ τους

3.3.1 User Equipment (UE)

Αποτελείται από δύο διαφορετικές υπομονάδες που συνδέονται μεταξύ τους με τη διεπαφή Cu :

- Ο κινητός σταθμός (MS) ή Mobile Equipment ή απλά ME, που είναι το τερματικό που χρησιμοποιείται για τη ραδιοεπικοινωνία διαμέσου της διεπαφής Uu.
- Το UMTS Subscriber Identity Module (USIM), είναι μια έξυπνη κάρτα που περιέχει την ταυτότητα του συνδρομητή, εκτελεί αλγορίθμους πιστοποίησης και παρέχει κλειδιά πιστοποίησης και κρυπτογράφησης όπως και κάποιες πληροφορίες συνδρομής που χρειάζονται για το τερματικό.
- Η διεπαφή Cu είναι η ηλεκτρική διεπαφή που διασυνδέει τη USIM με το ME. Η διεπαφή αυτή ακολουθεί μια συγκεκριμένη τυποποίηση για κάρτες.

3.3.2 UMTS Terrestrial Radio Access Network ή UTRAN

Το UTRAN αποτελείται από ένα ή περισσότερα υποδίκτυα RNS (Radio Network Sub-systems). Ένα RNS είναι ένα υποδίκτυο αποτελούμενο από ένα Radio Network Controller (RNC Ελεγκτή Σταθμών Βάσης) και ένα ή περισσότερα Node B (σταθμοί βάσης στο UMTS). Τα RNC συνδέονται μεταξύ τους και με τα Node B με διεπαφές Iur και Iub αντίστοιχα.

3.3.3 Το κυρίως δίκτυο (Core network (CN))

Το κυρίως δίκτυο αποτελείται από 2 τομείς. Τον τομέα μεταγωγής κυκλώματος και τον τομέα μεταγωγής πακέτου.

α. Ο τομέας μεταγωγής κυκλώματος αποτελείται από το Gateway Mobile Services Switching Centre (GMSC) server και από το MSC/VLR (Visitor Location Register).

β Ο τομέας μεταγωγής πακέτου αποτελείται από τα Serving GPRS Support Node (SGSN) και το GGSN (Gateway GPRS Support Node).

Το κυρίως δίκτυο επίσης περιλαμβάνει σαν κοινά στοιχεία και για τους 2 τομείς τα:

α Home location register (HLR) το οποίο περιέχει πληροφορίες για τους εγγραμμένους χρήστες του δικτύου. και εκτελεί αυθεντικοποίηση (Auc) των χρηστών.

β. Το Equipment Identity Register (EIR) το οποίο εχει αποθηκευμένες πληροφορίες για τις συσκευές των χρηστών

Από το UTRAN στο κυρίως δίκτυο το RNC θα αποφασίσει προς τα πού θα κατευθυνθεί η κίνηση των δεδομένων. Τα πακέτα θα αποσταλούν προς το SGSN και κατόπιν στο GGSN. Οι λειτουργίες του GGSN μοιάζουν με κοινή IP Gateway, το οποίο θα μεταφέρει την κίνηση σε ένα άλλο IP δίκτυο.

Από την άλλη μεριά αν υπάρχει ένα τηλεφώνημα από έναν χρήστη, το RNC θα μεταφέρει την κίνηση στο MSC. Αν ο χρήστης εχει πιο πριν αυθεντικοποιηθεί από το δίκτυο, το MSC θα μεταφέρει την κίνηση σε άλλο MSC αν το τηλεφώνημα απευθύνεται

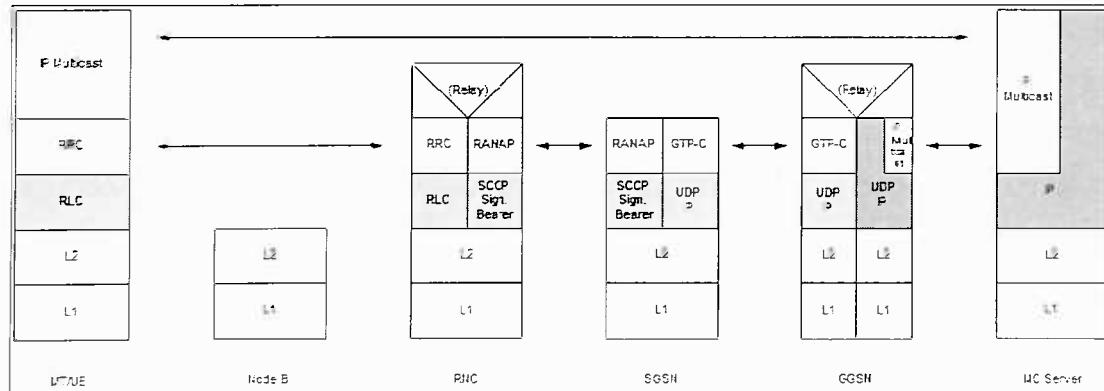
Ασφάλεια και διαχείριση κλειδιών στο UMTS

σε άλλο χρήστη, του δικτύου η προς το GMSC αν απευθύνεται σε έναν χρήστη ενός δημοσίου σταθερού τηλεφωνικού δικτύου.

3.3.4 Πρωτόκολλα σηματοδοσίας και επιπέδου χρήστη στο UMTS

Σε αυτή την παράγραφο θα παρουσιαστούν περιληπτικά τα πρωτόκολλα επιπέδου δικτύου (σηματοδοσίας, C-plane) και επιπέδου χρήστη (U-plane) που χρησιμοποιούνται για την δημιουργία συνδέσεων μεταξύ των κόμβων του δικτύου UMTS. Σε αυτό το σημείο πρέπει να πούμε ότι, για τη μετάδοση των πακέτων ελέγχου και δεδομένων (control και data plane αντίστοιχα) στο ενσύρματο (σταθερό) κομμάτι του δικτύου, χρησιμοποιούνται μία από τις ήδη ανεπτυγμένες τεχνολογίες ATM ή IP. Η παρουσίαση που θα γίνει σε αυτή την παράγραφο δε θα ασχοληθεί με τον τρόπο που μεταδίδονται τα πακέτα και θα εστιάσουμε στα επίπεδα δικτύου και πάνω.

Ακολουθούν δύο σχήματα (3.4 και 3.5), όπου παρουσιάζονται απλουστευμένες εκδόσεις της αρχιτεκτονικής πρωτοκόλλων που χρησιμοποιείται στο UMTS για τα επίπεδα ελέγχου και δεδομένων αντίστοιχα.

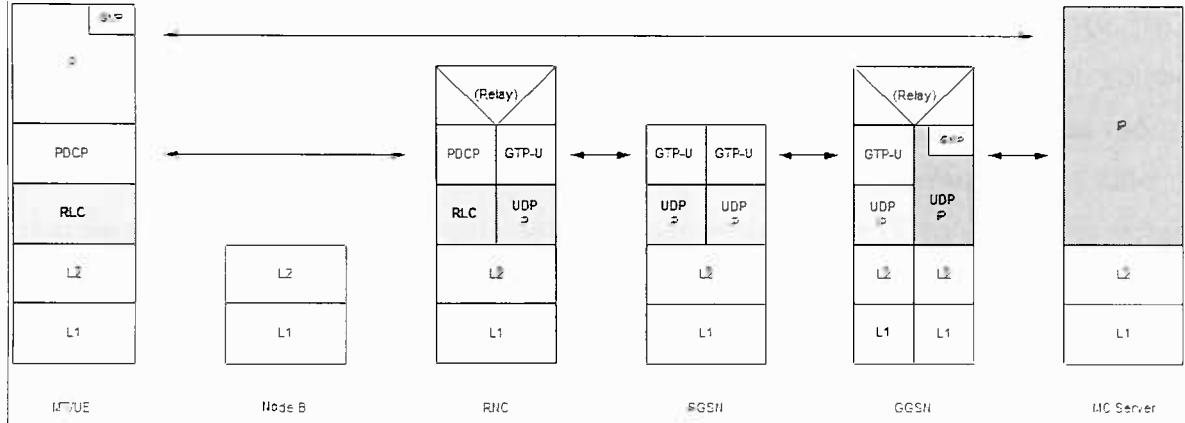


Σχήμα 3.4: Αρχιτεκτονική πρωτοκόλλων σε επίπεδο ελέγχου για το τμήμα PS [39]

Στο σχήμα που προηγείται όπως και στο σχήμα που ακολουθεί φαίνονται με βέλη οι συνδέσεις που εγκαθίστανται. Για τις υπηρεσίες που μας ενδιαφέρουν και που αφορούν μεταγωγή πακέτου, αυτό που έχει σημασία είναι να εγκατασταθούν οι συνδέσεις από άκρο σε άκρο, όπως φαίνονται με τα μεγάλα βέλη στο πάνω μέρος του κάθε σχήματος. Οι συνδέσεις αυτές στην πράξη αποτελούνται από επιμέρους συνδέσεις μεταξύ

Ασφάλεια και διαχείριση κλειδιών στο UMTS

των κόμβων του συστήματος, που σημειώνονται με μικρότερα βέλη. Τα πρωτόκολλα που χρησιμοποιούνται για το σκοπό αυτό θα παρουσιαστούν στη συνέχεια.



Σχήμα 3.5: Αρχιτεκτονική πρωτοκόλλων σε επίπεδο χρήστη για το τμήμα PS [39]

Για την παρουσίαση αυτή θα ακολουθηθεί σειρά από κάτω προς τα πάνω όσον αφορά τα επίπεδα του δικτύου και τα χρησιμοποιούμενα πρωτόκολλα. Οι ήταν ωστόσο παράληψη να μην αναφερθεί ότι κάθε φορά που ο κινητός σταθμός θέλει να ανταλλάξει μηνύματα σηματοδοσίας με το δίκτυο για μεταγωγή πακέτου, πρέπει να μεταβεί σε κατάσταση PMM-CONNECTED (από πλευράς Διαχείρισης Κινητικότητας – Mobility Management). Όταν η σύνδεση σηματοδοσίας με το δίκτυο διακοπεί ο κινητός σταθμός μεταβαίνει σε κατάσταση PMM-IDLE από όπου δύναται περιοδικά να εκτελεί τη διαδικασία της ενημέρωσης της περιοχής δρομολόγησης (routing area update).

Σε επίπεδο σηματοδοσίας λοιπόν, αλλά και στο επίπεδο χρήστη, χρησιμοποιείται το πρωτόκολλο RLC (Radio Link Control) τόσο από την πλευρά του κινητού τερματικού όσο και από την πλευρά του κόμβου RNC, το οποίο και υλοποιείται κατά κανόνα πάνω από το στρώμα ζεύξης, (που για το UMTS είναι το WCDMA), για να προσδώσει την απαιτούμενη λειτουργικότητα σε αυτό. Σε επίπεδο σηματοδοσίας το RLC χρησιμοποιείται από το πρωτόκολλο RRC ενώ σε επίπεδο χρήστη από το PDCP. Οι λειτουργίες που αναλαμβάνει κατά περίσταση και πάντα ανάλογα με τις «υποδείξεις» του αμέσως ανώτερου πρωτοκόλλου είναι αρκετές και οι σημαντικότερες από αυτές είναι η κατάτμηση και η επανένωση των πακέτων, η διόρθωση λαθών, η παράδοση κατά σειρά των πακέτων, ο εντοπισμός διπλών αντιτύπων, ο έλεγχος ροής, κ.α.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Για το επίπεδο σηματοδοσίας το πρωτόκολλο κλειδί για τη διαχείριση των πόρων, είναι το RRC (Radio Resource Control), για το UTRAN. Αυτό υλοποιείται μεταξύ των κινητών τερματικών και των RNC κόμβων και χρησιμοποιεί τις συνδέσεις και τα μηνύματα που του παρέχονται από το RLC. Για τη συνέχιση της σηματοδοσίας μεταξύ RNC και SGSN ή αλλιώς μεταξύ του UTRAN και του κεντρικού δικτύου κορμού (CN), χρησιμοποιείται το RANAP (Radio Access Network Application Protocol) με τέτοιο τρόπο ώστε η εξέλιξη των δύο τμημάτων του δικτύου να είναι ουσιαστικά ανεξάρτητη αλλά η επικοινωνία να παραμένει ικανοποιητική. Η συνεργασία του δε με το RRC είναι τέτοια που επιτρέπει ουσιαστικά τη σύνδεση του κινητού τερματικού με το CN. Προϋποθέτουμε ωστόσο ότι υπάρχει εγκατεστημένη η σύνδεση σηματοδοσίας στο παρακάτω επίπεδο, γεγονός για το οποίο φροντίζει το SCCP. Αν κάτι δε λειτουργεί καλά στο κάτω επίπεδο, το SCCP οφείλει να ενημερώσει το RANAP. Τέλος, για τις συνδέσεις σηματοδοσίας, η επικοινωνία των κόμβων SGSN με τους GGSN επιτυγχάνεται μέσω του πρωτοκόλλου GTP-C (GPRS Tunnelling Protocol for Control Plane). Αυτό επιτρέπει στον SGSN να συνδεθεί με τον GGSN και να προωθήσει τα πακέτα δεδομένων προς τους χρήστες. Επίσης, το πρωτόκολλο GTP-C χρησιμοποιείται και για την επικοινωνία μεταξύ δύο SGSNs προκειμένου να ανταλλάξουν πληροφορίες σχετικά με κάποιο χρήστη όταν αυτός αποφασίζει να αλλάξει περιοχή δρομολόγησης και να εισέλθει στη δικαιοδοσία κάποιου άλλου SGSN.

Από την άλλη, στο επίπεδο χρήστη, το πρωτόκολλο που χρησιμοποιεί το RLC είναι το PDCP (Packet Data Convergence Protocol) το οποίο είναι σχεδιασμένο να κάνει τα πρωτόκολλα του WCDMA κατάλληλα για μεταφορά των πιο κοινών τύπων πακέτων πρωτοκόλλων δεδομένων των χρηστών, όπως είναι το TCP/IP. Με τον τρόπο αυτό επιτυγχάνεται η σύνδεση των κινητών τερματικών με τους κόμβους RNC. Η κύρια λειτουργία του είναι να συμπιέζει τα περιεχόμενα των επικεφαλίδων των πακέτων, τα οποία ασυμπίεστα θα σπαταλούσαν πολύτιμους πόρους του δικτύου. Τέλος, για τη σύνδεση του κινητού (του κόμβου RNC στην πραγματικότητα) με το δίκτυο κορμού και τους κόμβους SGSN και GGSN, δεδομένου ότι μεγάλο μέρος της κίνησης πακέτων χρηστών μέσω του δικτύου έχει να κάνει με το IP πρωτόκολλο, χρησιμοποιείται το GTP-U (GPRS Tunnelling Protocol for data User Plane). Αυτό, παρέχει μεταφορά δε-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

δομένων χωρίς σύνδεση (connectionless) και συνεργάζεται πολύ καλά με το UDP πρωτόκολλο [39].

ΚΕΦΑΛΑΙΟ 4

Απαιτήσεις ασφαλείας του δικτύου

Τα ζητήματα ασφαλείας δεν αντιμετωπίστηκαν κατάλληλα στα πρώτης γενιάς (1G) αναλογικά συστήματα. Με χαμηλού κόστους εξοπλισμό, ένας εισβολέας θα μπορούσε να κρυφακούσει την κίνηση των χρηστών, ή ακόμα και να αλλάξει την ταυτότητα του τηλεφώνου προκειμένου να αποκτήσει πρόσβαση σε μια υπηρεσία.

Λαμβάνοντας υπόψη αυτό το υπόβαθρο, τα μέτρα ασφαλείας που θα έπρεπε να ληφθούν, έπαιξαν σημαντικό ρόλο στο σχεδιασμό της δεύτερης γενεάς (2G) ψηφιακά κυψελοειδή συστήματα. Το GSM σχεδιάστηκε από την αρχή με την ασφάλεια κατά νου και γι' αυτό έχει υιοθετήσει αρκετούς μηχανισμούς ώστε να παρέχει την πιστοποίηση των χρηστών και εμπιστευτικότητα στα δεδομένα τους. Παρόλα αυτά εκ των υστέρων αποδείχτηκε ότι τα μέτρα αυτά δεν ήταν αρκετά.

Η προστασία ασφαλείας στα 3G-δίκτυα απαιτεί την εκτίμηση διάφορων πτυχών και ζητημάτων, όπως η ασύρματη πρόσβαση, η κινητικότητα των τελικών χρηστών, οι ιδιαίτερες απειλές ασφαλείας, το είδος πληροφοριών που θα προστατευθούν, και η πολυπλοκότητα στη δικτυακή αρχιτεκτονική. Η χρήση του ασυρμάτου δικτύου πρόσβασης είναι από τη φύση της πιο ευάλωτη σε ωτακουστές. Η κινητικότητα χρηστών στο δίκτυο προκαλεί επίσης προβλήματα στην ασφάλεια. Οι διαφορετικοί τύποι στοιχείων, όπως τα στοιχεία χρηστών, δεδομένα χρέωσης και τιμολόγησης, πληροφορίες που αφορούν τους χρήστες και δεδομένα διαχείρισης του δικτύου, τα οποία μεταβιβάζονται μέσα στα κινητά δίκτυα απαιτούν διαφορετικούς τύπους και επίπεδα προστασίας. Επιπλέον, οι σύνθετες τοπολογίες δικτύων και η ετερογένεια διευρύνουν το πρόβλημα.

4.1 Χαρακτηριστικά ασφαλείας/Απαιτήσεις ασφαλείας/Σχεδίαση

Προκειμένου να επιτευχθούν οι στόχοι ασφαλείας απαιτείται προσεκτικός σχεδιασμός. Η διαδικασία σχεδιασμού ενός συστήματος ασφαλείας περιέχει τις ακόλουθες φάσεις [39]:

Ανάλυση απειλής. Η πρόθεση είναι εδώ να απαριθμηθούν όλες οι πιθανές απειλές ενάντια στο σύστημα. Σε αυτήν την φάση δεν υπάρχει ανάγκη να ανακαλυφθεί ποια είδη ενεργειών και συσκευών απαιτούνται για να υλοποιήσουν μια επίθεση ώστε να πραγματοποιηθεί η απειλή.

Ανάλυση κινδύνου. Σε αυτήν την φάση το βάρος κάθε απειλής υπολογίζεται πιστοπά ή τουλάχιστον, σε σχέση με άλλες απειλές. Αυτό απαιτεί την εκτίμηση της πιο λυπλοκότητας της απειλής και την πιθανή βλάβη που προκαλεί στο σύστημα.

Η σύλληψη των απαιτήσεων. Με βάση τις προηγούμενες φάσεις, αποφασίζουμε τώρα τι είδους προστασία απαιτείται για το σύστημα. Οι απαιτήσεις είναι ευκολότερο να καθοριστούν στο πλαίσιο ενός μοντέλου εμπιστοσύνης που πρέπει να καθοριστεί πρώτα.

Φάση σχεδιασμού. Σε αυτήν την φάση, οι πραγματικοί μηχανισμοί προστασίας σχεδιάζονται με σκοπό να καλυφθούν οι απαιτήσεις. Τα υπάρχοντα δομικά στοιχεία (π.χ., πρωτόκολλα ασφάλειας) προσδιορίζονται, ενδεχομένως δημιουργούνται νέοι μηχανισμοί και χτίζεται μια αρχιτεκτονική ασφάλειας. Εδώ οι περιορισμοί πρέπει να ληφθούν υπόψη και είναι πιθανό ότι όλες οι απαιτήσεις δεν μπορούν να καλυφθούν, υπονοώντας μια επιστροφή στις προηγούμενες φάσεις, ειδικά στην ανάλυση του κινδύνου.

Ανάλυση ασφάλειας. Είναι σημαντικό να πραγματοποιηθεί μια αξιολόγηση των αποτελεσμάτων της προηγούμενης φάσης χρησιμοποιώντας τα κατάλληλα εργαλεία ελέγχου.

Φάση αντίδρασης. Στη φάση αυτή σχεδιάζεται ο τρόπος διαχείρισης της λειτουργίας των συστημάτων έπειτα από ένα γεγονός παραβίασης της ασφάλειας. Βέβαια, δεν είναι δυνατόν να σχεδιαστεί εκ των προτέρων η αντίδραση σε όλες τις απροσδόκητες παραβιάσεις ασφάλειας. Στη φάση αντίδρασης είναι ζωτικής σημασίας το αρχικό σχέδιο ασφαλείας του συστήματος είναι αρκετά εύκαμπτο ώστε να επιτρέπει βελτιώσεις. Για την μείωση των δυσκολιών στη φάση αντίδρασης, κάποιο περιθώριο ανοχής ασφάλειας πρέπει να έχει συμπεριληφθεί στους μηχανισμούς που σχεδιάζονται. Αυτά τα περιθώρια τείνουν να είναι χρήσιμα σε περιπτώσεις όπου οι νέες μεθοδολογίες και τα εργαλεία επίθεσης αναπτύσσονται γρηγορότερα από το αναμενόμενο.



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ο στόχος είναι το δίκτυο 3G να έχει τα ακόλουθα γενικά χαρακτηριστικά γνωρίσματα ασφάλειας [2]:

α) Να εξασφαλίσει ότι οι πληροφορίες που παράγονται ή σχετίζονται με έναν χρήστη προστατεύονται επαρκώς από την κακή χρήση ή την κατάχρηση.

β) Να εξασφαλίσει ότι οι πόροι και οι υπηρεσίες που παρέχονται από τα εξυπηρετούντα δίκτυα αλλά και τα πατρικά, προστατεύονται επαρκώς από την κακή χρήση ή την κατάχρηση.

γ) Να εξασφαλίσει ότι τα χαρακτηριστικά γνωρίσματα ασφάλειας που τυποποιούνται είναι συμβατά και διαθέσιμα παγκοσμίως. Να υπάρχει δηλαδή τουλάχιστον ένα αλγόριθμος κρυπτογράφησης που μπορεί να εξαχθεί προς όλες τις άλλες χώρες χωρίς να υπόκειται σε περιοριστικούς κανονισμούς ασφαλείας, (σύμφωνα με τη συμφωνία Wassenaar))

δ) Να εξασφαλίσει ότι τα χαρακτηριστικά γνωρίσματα ασφάλειας είναι επαρκώς τυποποιημένα για να εξασφαλίσουν την παγκόσμια διαλειτουργικότητα και την περιαγωγή μεταξύ των διαφορετικών δικτύων εξυπηρέτησης.

ε) Να εξασφαλίσει ότι το επίπεδο προστασίας που διατίθεται στους χρήστες και τους παροχείς υπηρεσιών είναι καλύτερο από αυτό που παρέχεται στα σύγχρονα σταθερά και τα κινητά δίκτυα.

στ) Να εξασφαλίσει ότι η εφαρμογή των μηχανισμών ασφάλειας στα 3G δίκτυα θα είναι τέτοια, που να μπορεί να επεκταθεί και να ενισχυθεί όπως απαιτείται από τις νέες απειλές και τις υπηρεσίες.

Οι διαφορετικοί τύποι δεδομένων απαιτούν διαφορετικούς τύπους και επίπεδα προστασίας. Έτσι στο δίκτυο UMTS παρουσιάζονται οι παρακάτω τύποι δεδομένων [2, 9]:

- Τα δεδομένα χρηστών, περιλαμβάνουν το περιεχόμενο που εκπέμπεται από άκρη σε άκρη. Η ασφάλεια αυτών μέσα στο κινητό δίκτυο είναι ευθύνη του δικτύου.
- Τα στοιχεία χρέωσης και τιμολόγησης περιλαμβάνουν στοιχεία που σχετίζονται με χρεώσεις προς τους χρήστες για όσο χρησιμοποιούν πόρους και υπηρεσίες, του δικτύου.

- Τα στοιχεία πληροφοριών χρηστών περιλαμβάνουν στοιχεία θέσης του χρήστη, στοιχεία σχετικά με τις υπηρεσίες που χρησιμοποιεί και γενικά στοιχεία που καθορίζουν την ταυτότητα των χρηστών.

- Τα δεδομένα διαχείρισης του δικτύου περιλαμβάνουν τα στοιχεία που αφορούν στην πρόσβαση ενός κινητού χρήστη στο δίκτυο, στοιχεία σχετικά με τη διαχείριση ασφάλειας, όπως τα κλειδιά κρυπτογράφησης και η αυθεντικοποίηση μηνυμάτων, στοιχεία που αναφέρονται στη δρομολόγηση και τελικά στοιχεία που αφορούν στην δημιουργία, διατήρηση και τερματισμό κλήσεων.

4.1.1 Απειλές ασφαλείας

Χωρίζουμε τις απειλές ασφαλείας στις εξής κατηγορίες [2]:

1 Μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα:

α Υποκλοπή (Eavesdropping): Ένας κακόβουλος υποκλέπτει μηνύματα χωρίς να γίνει αντιληπτός.

β Μεταμφίεση (Masquerading): Ένας κακόβουλος εξαπατά έναν νόμιμο χρήστη ότι είναι το νόμιμο σύστημα, ώστε να δεχτεί εμπιστευτικές πληροφορίες από το χρήστη, ή ένας κακόβουλος χρήστης εξαπατά ένα νόμιμο σύστημα ότι είναι εξουσιοδοτημένος χρήστης, ώστε να έχει την παροχή υπηρεσιών του συστήματος ή εμπιστευτικές πληροφορίες.

γ Ανάλυση κυκλοφορίας (Traffic analysis): Ένας κακόβουλος παρατηρεί το χρόνο, το ρυθμό, την έκταση, την πηγή, και τον προορισμό των μηνυμάτων για να καθορίσει την θέση ενός χρήστη ή για να μάθει εάν πραγματοποιείται μια σημαντική επιχειρηματική συναλλαγή.

δ Ξεφύλλισμα (Browsing): Ένας κακόβουλος ψάχνει τα αποθηκεμένα στοιχεία για ευαίσθητες πληροφορίες.

ε Διαρροή (Leakage): Ένας κακόβουλος λαμβάνει ευαίσθητες πληροφορίες με την εκμετάλλευση των διαδικασιών πρόσβασης σε νόμιμα στοιχεία.

σ Συμπέρασμα (Inference): Ένας κακόβουλος παρατηρεί την αντίδραση του συστήματος με την αποστολή μιας ερώτησης ή ενός σήματος στο σύστημα. Για παράδειγμα, ένας κακόβουλος μπορεί ενεργά να εγκαθιδρύσει συνόδους επικοινωνιών και έπειτα να επιτύχει πρόσβαση σε πληροφορίες μέσω παρατήρησης του χρόνου, του

ρυθμού, του μήκους, των πηγών ή των προορισμών των σχετικών μηνυμάτων στο ασύρματο δίκτυο πρόσβασης.

2 Παραποίηση των ευαίσθητων στοιχείων (παραβίαση της ακεραιότητας)

α Παραποίηση των μηνυμάτων (Manipulation of messages): Τα μηνύματα μπορούν να τροποποιηθούν σκόπιμα, να παρεμβληθούν, να επαναληφθούν, ή να διαγραφούν από έναν κακόβουλο.

3 Διατάραξη ή κακή χρήση των υπηρεσιών του δικτύου (που οδηγούν στην άρνηση της υπηρεσίας ή της μείωση της διαθεσιμότητάς της)

α Επέμβαση (Intervention): Ένας κακόβουλος μπορεί να αποτρέψει έναν εξουσιοδοτημένο χρήστη από τη χρησιμοποίηση μιας υπηρεσίας με το μπλοκάρισμα της κυκλοφορίας του χρήστη, της σηματοδοσίας, ή των δεδομένων ελέγχου.

β Εξουθένωση των πόρων (Resource exhaustion): Ένας εισβολέας μπορεί να αποτρέψει έναν εξουσιοδοτημένο χρήστη από τη χρησιμοποίηση μιας υπηρεσίας με την υπερφόρτωση της υπηρεσίας.

γ Κακή χρήση των προνομίων (Misuse of privileges): Ένας χρήστης ή ένα δίκτυο μπορεί να εκμεταλλευτούν τα προνόμια τους για να έχουν πρόσβαση σε υπηρεσίες ή πληροφορίες.

4 Αποκήρυξη (Repudiation): Ένας χρήστης ή ένα δίκτυο αρνείται τις ενέργειες που έχουν πραγματοποιηθεί.

5 Μη εξουσιοδοτημένη πρόσβαση στις υπηρεσίες

Οι εισβολείς μπορούν να έχουν πρόσβαση στις υπηρεσίες με μεταμφίεση ως χρήστες ή οντότητες δικτύων.

Οι χρήστες ή οι οντότητες του δικτύου μπορούν να επιτύχουν αναρμόδια πρόσβαση στις υπηρεσίες με την κακή χρήση των δικαιωμάτων πρόσβασής τους.

4.1.1.1 Απειλές ασφαλείας που σχετίζονται με απειλές στο ασύρματο δίκτυο πρόσβασης.

Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα		
Κωδ.	Περιγραφή	Αξία των απειλών
T1a	Υποκλοπή της κίνησης δεδομένων του χρήστη	Μεγάλη
T1b	Υποκλοπή των δεδομένων σηματοδοσίας ή ελέγχου	Μέτρια
T1c	Μεταμφίεση σε συμμετέχοντα νόμιμο μέλος μιας επικοινωνίας	Μεγάλη
T1d	Παθητική ανάλυση της κίνησης των δεδομένων	Μεγάλη
T1e	Ενεργητική ανάλυση της κίνησης των δεδομένων	Μικρή
Απειλές ακεραιότητας		
T2a	Παραποίηση της κίνησης δεδομένων του χρήστη	Μικρή
T2b	Παραποίηση των δεδομένων σηματοδοσίας ή ελέγχου του δικτύου	Μικρή
Επιθέσεις άρνησης υπηρεσίας (DOS)		
T3a	Φυσική παρέμβαση (π.χ jamming)	Μικρή
T3b	Παρέμβαση στην λειτουργία του πρωτοκόλλου	Μικρή
T3c	Άρνηση υπηρεσίας μεταμφιεζόμενος σε ένα νόμιμα συμμετέχοντα μέλος μιας επικοινωνίας	Μικρή
Μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες		
T4a	Μεταμφίεση σε άλλο χρήστη	Μεγάλη

4.1.1.2 Απειλές που σχετίζονται με επιθέσεις σε άλλα τμήματα του συστήματος.

Κωδ.	Περιγραφή	Αξία των απειλών
Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα		
T5a	Υποκλοπή της κίνησης του χρήστη	Μικρή
T5b	Υποκλοπή των δεδομένων σηματοδοσίας ή ελέγχου	Μέτρια
T5c	Μεταμφίεση σε ένα παραλήπτη δεδομένων	Μικρή
T5d	Παθητική ανάλυση της κίνησης	Μικρή

Ασφάλεια και διαχείριση κλειδιών στο UMTS

T5e	Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα που βρίσκονται αποθηκευμένα σε οντότητες του συστήματος	Μικρή
T5f	Γνωστοποίηση της θέσης του χρήστη	Μικρή
Απειλές ακεραιότητας		
T6a	Παραποίηση της κίνησης δεδομένων του χρήστη	Μικρή
T6b	Παραποίηση των δεδομένων σηματοδοσίας ή ελέγχου του δικτύου	Μικρή
T6c	Παραποίηση μεταμφιεζόμενος σε συμμετέχοντα σε μία επικοινωνία.	Μικρή
T6d	Παραποίηση εφαρμογών και/η δεδομένων που έχουν προορισμό το τερματικό (τηλέφωνο) ή την USIM	Μικρή
T6e	Παραποίηση της συμπεριφοράς του τηλεφώνου, (τερματικού), μεταμφιεζόμενος σε πηγή των εφαρμογών και/η των δεδομένων	Μέτρια
T6f	Παραποίηση στα δεδομένα που βρίσκονται αποθηκευμένα σε οντότητες του συστήματος	Μικρή
Επιθέσεις άρνησης υπηρεσίας (DOS)		
T7a	Φυσική παρέμβαση	Μικρή
T7b	Παρέμβαση στην λειτουργία του πρωτοκόλλου	Μικρή
T7c	Άρνηση υπηρεσίας μεταμφιεζόμενος σε ένα νόμιμα συμμετέχοντα μέλος μιας επικοινωνίας	Μικρή
T7d	Κατάχρηση των επειγουσών υπηρεσιών	Μικρή
Αποποίηση		
T8a	Αποποίηση της χρέωσης	Μικρή
T8b	Αποποίηση του αποστολέα	Μικρή
T8c	Αποποίηση της διανομής της κίνησης χρήστη	Μικρή
Μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες		
T9a	Μεταμφίεση σε χρήστη	Μεγάλη
T9b	Μεταμφίεση σε δίκτυο χρήσης	Μέτρια
T9c	Μεταμφίεση σε πατρικό περιβάλλον	Μικρή

Ασφάλεια και διαχείριση κλειδιών στο UMTS

T9d	Κακή χρήση των προνομίων του χρήστη	Μεγάλη
T9e	Κακή χρήση των προνομίων του δικτύου εξυπηρέτησης	Μικρή

4.1.1.3 Απειλές που σχετίζονται με επιθέσεις στο τερματικό και την κάρτα (UICC/USIM)

Κωδ.	Περιγραφή	Αξία των απειλών
T10a	Χρήση κλεμμένου τερματικού και κάρτας (UICC)	Μεγάλη
T10b	Χρήση δανεικού τερματικού και κάρτας (UICC)	Μικρή
T10c	Χρήση κλεμμένου τερματικού	Μικρή
T10d	Παραποίηση της ταυτότητας του τερματικού	Μεγάλη
T10e	Ακεραιότητα δεδομένων αποθηκευμένων σε ένα τερματικό	Μέτρια
T10f	Ακεραιότητα δεδομένων αποθηκευμένων στην USIM	Μέτρια
T10g	Υποκλοπή στην διεπαφή του UUIC και του τερματικού	Μικρή
T10h	Μεταμφίεση σε παραλήπτη δεδομένων στην διεπαφή UICC και τερματικού	Μικρή
T10i	Παραποίηση των δεδομένων στην διεπαφή UICC και τερματικού	Μικρή
T10j	Εμπιστευτικότητα στα δε-	Μικρή

Ασφάλεια και διαχείριση κλειδιών στο UMTS

	δομένα ενός χρήστη στο τερματικό ή στην κάρτα (UICC/USIM)	
T10k	Εμπιστευτικότητα των δεδομένων αυθεντικοποίησης στα UICC,USIM	Μεγάλη

Μπορούμε λοιπόν να πούμε ότι οι σημαντικές απειλές μπορούν να κατηγοριοποιηθούν σε τρεις ομάδες [2]:

- **Μεταμφίεση** σε άλλους χρήστες προκειμένου να επιτύχουν μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες.
- **Υποκλοπή** η οποία μπορεί να οδηγήσει σε άρση της εμπιστευτικότητας της κίνησης δεδομένων του χρήστη, ή σε αποκάλυψη πληροφοριών σχετικά με την κλήση (πληροφορίες για τον αριθμό κλήσης, τη θέση κλπ).
- **Απάτη εγγεγραμμένων πελατών**, οι οποίοι χρησιμοποιούν τις υπηρεσίες χωρίς την διάθεση να πληρώσουν.

4.1.2 Απαιτήσεις ασφάλειας

Μετά την ανάλυση των απειλών και του κινδύνου που η κάθε μία εγκυμονεί προκύπτουν οι παρακάτω απαιτήσεις ασφαλείας:

4.1.2.1 Απαιτήσεις που προέρχονται από την ανάλυση απειλής

4.1.2.1.1 Απαιτήσεις στην ασφάλεια 3GPP των υπηρεσιών

4.1.2.1.1.1 Απαιτήσεις για ασφαλή πρόσβαση στις υπηρεσίες

R1a Μία έγκυρη USIM να απαιτείται για πρόσβαση σε οποιαδήποτε 3G υπηρεσία εκτός από τις κλήσεις έκτακτης ανάγκης όπου το δίκτυο θα μπορεί να αποφασίσει εάν οι κλήσεις έκτακτης ανάγκης πρέπει ή όχι να επιτραπούν χωρίς την ύπαρξη USIM. (T7d, T9a, d)

R1b Να είναι δυνατό να αποτραπούν οι εισβολείς από πρόσβαση στις 3G στις υπηρεσίες με μεταμφίεση ως εξουσιοδοτημένοι χρήστες. (T4a, T9a, c)

R1c Να είναι δυνατό για τους χρήστες να ελέγξουν ότι τα δίκτυα εξυπηρέτησης εξουσιοδοτούνται για να προσφέρουν τις 3G υπηρεσίες εξ ονόματος του πατρικού δικτύου του χρήστη στην έναρξη, και κατά τη διάρκεια, της παροχής υπηρεσιών. (T1c, e, T3c, T4a, T9b, c)

4.1.2.1.1.2 Απαιτήσεις για ασφαλή παροχή υπηρεσιών

R2a Να είναι δυνατό για τους φορείς παροχής υπηρεσιών να αυθεντικοποιήσουν τους χρήστες στην έναρξη και κατά τη διάρκεια της παροχής υπηρεσιών, για να αποτρέψουν τους εισβολείς από τη λήψη της αναρμόδιας πρόσβασης στις 3G υπηρεσίες με μεταμφίεση ή την κακή χρήση προτεραιότητας. (T4a, T8a, T9a, d)

R2b Να είναι δυνατό να ανιχνευθεί και να αποτραπεί η απάτη χρήσης των υπηρεσιών.

Οα πρέπει να υπάρχουν μηχανισμοί προειδοποίησης για να προειδοποιούν τους παρόχους υπηρεσιών για τα γεγονότα σχετικά με την ασφάλεια. Επίσης πρέπει να παράγονται ημερολόγια σχετικά με γεγονότα ασφάλειας. (T8a, b, c, T9d, e, T10a, b)

R2c Να είναι δυνατό να αποτραπεί η πρόσβαση ενός συγκεκριμένου USIM στις υπηρεσίες 3G. (T9a, δ, T10a)

R2d Να είναι δυνατό για το πατρικό δίκτυο να προκαλέσει μια άμεση λήξη όλων των υπηρεσιών που παρέχονται σε ορισμένους χρήστες, επίσης για εκείνες που προσφέρονται από το δίκτυο εξυπηρέτησης. (T9a, δ, T10a, b)

R2e Το δίκτυο εξυπηρέτησης να είναι σε θέση να αυθεντικοποιήσει την προέλευση των δεδομένων των χρηστών, σηματοδοσίας και ελέγχου όσον αφορά τα ασύρματα δίκτυα πρόσβασης. (T8a, b, c, T9c)

R2f Να είναι δυνατό να αποτραπούν οι εισβολείς που έχουν σκοπό τον περιορισμό της διαθεσιμότητας των υπηρεσιών. (T3b, c, T7e)

R2g Να υπάρξει μια ασφαλής υποδομή μεταξύ των δικτύων, σχεδιασμένη έτσι ώστε η ύπαρξη ανάγκης του πατρικού δικτύου (HN) να εμπιστεύεται το δίκτυο εξυπηρέτησης (SN) για την λειτουργία της ασφάλειας να ελαχιστοποιείται.

4.1.2.1.2 Απαιτήσεις στην ακεραιότητα του συστήματος.

R3a Να είναι δυνατό να προστατεύσει από μη εξουσιοδοτημένη τροποποίηση την κίνηση των δεδομένων των χρηστών. (T2a, T6a, c, T7b, c)

R3b Να είναι δυνατό να προστατεύσει από την μη εξουσιοδοτημένη τροποποίηση συγκεκριμένα δεδομένα σηματοδοσίας και ελέγχου, ιδιαίτερα στην ασύρματη πρόσβαση. (T2b, T3b, c, T6b, c, T7a, b, c)

R3c Να είναι δυνατό να προστατεύσει από την μη εξουσιοδοτημένη τροποποίηση των στοιχείων του χρήστη που είναι αποθηκεμένα στο τερματικό ή στο USIM. (T6d, e, T6c, T10f, i)

R3d Να είναι δυνατό να προστατεύσει από μη εξουσιοδοτημένη τροποποίηση τα σχετικά με τους χρήστες στοιχεία που είναι υποθηκευμένα ή επεξεργάζονται από έναν πάροχο. (T6c, f)

R3e Να είναι δυνατό να εξασφαλιστεί ότι η προέλευση και η ακεραιότητα των εφαρμογών ή/και των δεδομένων που «κατεβαίνουν» στο τερματικό ή/και το UICC μπορούν να ελεγχθούν. Μπορεί επίσης να είναι απαραίτητο να εξασφαλιστεί η εμπιστευτικότητα τους. (T6c, d, e, f, T10e, f, i)

R3f Να είναι δυνατό να εξασφαλιστεί η προέλευση, η ακεραιότητα και η φρεσκάδα των δεδομένων αυθεντικοποίησης, ιδιαίτερα του κλειδιού κρυπτογράφησης πάνω στο ασύρματο δίκτυο πρόσβασης. (T1a, b, T2b, T5c, T6c)

R3g Να είναι δυνατό να εξασφαλιστεί η υποδομή μεταξύ των παρόχων. (T5a, b, c, T6a, b, c, T7a, b, c, T9b, c)

4.1.2.1.3 Απαιτήσεις για την προστασία των στοιχείων σχετικών με τον χρήστη.

4.1.2.1.3.1 Ασφάλεια των εκπεμπομένων δεδομένων που αφορούν τους χρήστες

R4a Να είναι δυνατό να προστατευθεί η εμπιστευτικότητα ορισμένων δεδομένων σηματοδοσίας και ελέγχου, ιδιαίτερα πάνω στο ασύρματο δίκτυο πρόσβασης. (T1b, δ, T5b, γ, δ)

R4b Να είναι δυνατό να προστατευθεί η εμπιστευτικότητα της κυκλοφορίας των δεδομένων των χρηστών, ιδιαίτερα πάνω στο ασύρματο δίκτυο πρόσβασης. (T1a, T5a)

R4c Να είναι δυνατό να προστατευθεί η εμπιστευτικότητα των στοιχείων της ταυτότητας των χρηστών, ιδιαίτερα πάνω στο ασύρματο δίκτυο. (T1b, d, T3b, T5b, c, d, e)

R4d Να είναι δυνατό να προστατευθεί η εμπιστευτικότητα των στοιχείων της θέσης για τους χρήστες, ιδιαίτερα πάνω στο ασύρματο δίκτυο . (T1b, T3b, T5b, c, d, e)

R4e Να είναι δυνατό να προστατευθεί η ανεπιθύμητη κοινοποίηση των στοιχείων της θέσης ενός χρήστη που συμμετέχει στο μία υπηρεσία 3G, από τα άλλα μέρη που συμμετέχουν στην ίδια 3G υπηρεσία. (T5f)

R4f Να είναι δυνατό για το χρήστη να ελέγξει εάν η κυκλοφορία των δεδομένων του και σχετικές με οι την κλήση πληροφορίες προστατεύονται ως προς την εμπιστευτικότητα. Αυτό πρέπει να απαιτεί την ελάχιστη δραστηριότητα των χρηστών. (T1a, b)

4.1.2.1.3.2 Ασφάλεια των σχετικών με το χρήστη αποθηκευμένων στοιχείων

R5a Να είναι δυνατό να προστατευθεί η εμπιστευτικότητα των σχετικών με τον χρήστη στοιχείων που αποθηκεύονται ή υποβάλλονται σε επεξεργασία από τον πάροχο. (T5c, e)

R5b Να είναι δυνατό να προστατευθεί η εμπιστευτικότητα των στοιχείων του χρήστη που αποθηκεύονται από τον ίδιο το χρήστη στο τερματικό ή στο USIM. (T10h, j)

4.1.2.1.4 Απαιτήσεις στο τερματικό/USIM

4.1.2.1 4.1 Ασφάλεια του USIM

R6a Να είναι δυνατό να ελεγχθεί η πρόσβαση σε ένα USIM έτσι ώστε μπορεί να χρησιμοποιηθεί για πρόσβαση στις υπηρεσίες 3G μόνο από τον χρήστη/συνδρομητή στον οποίο ανήκει ή από χρήστες που εγκρίθηκαν ρητά από εκείνον. (T10a, c)

R6b Να είναι δυνατό να ελεγχθεί η πρόσβαση στα δεδομένα του USIM. Για παράδειγμα, μερικά στοιχεία μπορούν μόνο να είναι προσπελάσιμα μόνο από το πατρικό δίκτυο. (T10h, j, K)

R6c Να μην είναι δυνατό να προσπελαστούν τα στοιχεία σε ένα USIM που προορίζονται να χρησιμοποιηθεί μόνο μέσα στο USIM, π.χ. κλειδιά και αλγόριθμοι αυθεντικοποίησης. (T10h, K)

4.1.2.1.4.2 Ασφάλεια του τερματικού

R7a Να είναι δυνατό να αποτραπεί η κλοπή των τερματικών. (T10a, c, d)

R7b Να είναι δυνατό να γίνει φραγή σε ένα συγκεκριμένο τερματικό από την πρόσβαση σε 3G υπηρεσίες. (T10a, c, d)

R7c Να είναι δύσκολο να αλλαχτεί η ταυτότητα ενός τερματικού για να καταστρατηγήθούν τα μέτρα που λαμβάνονται για να αποτρέψουν έναν συγκεκριμένο τερματικό από την πρόσβαση στις υπηρεσίες 3G. (T10a, c, d)

4.1.2.2 Εξωτερικές απαιτήσεις

4.1.2.2.1 Απαιτήσεις ρυθμιστών

4.1.2.2.1.2 Νόμιμη παρεμβολή

R8a Να είναι δυνατό για τα όργανα επιβολής του νόμου να ελέγχουν ή να παρεμποδίζουν κάθε κλήση, ή προσπάθεια κλήσης, σύμφωνα με τις εθνικές νομοθεσίες. Επιπλέον να είναι δυνατό να παρεμβάλλονται σε μία κλήση σύμφωνα με τις εθνικές νομοθεσίες.

4.1.2.3 Συγκέντρωση των απαιτήσεων ασφαλείας ενός δικτύου 3G

Από τα παραπάνω διαφαίνεται ότι, αν και τα κινητά δίκτυα διαφέρουν στη φύση από τα σταθερά επίγεια δίκτυα, η ασφάλειάς τους πρέπει να ακολουθεί τις αρχές που καθορίζονται για την παραδοσιακή IP δικτύωση, όπως η εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση, διαθεσιμότητα, εξουσιοδότηση, απονομή ευθυνών και μη αποποίηση. Αυτά τα μέτρα προστατεύουν σε διάφορες πιθανές επιθέσεις όπως τη μεταμφίεση, μη εξουσιοδοτημένη χρήση των πτώρων, μη εξουσιοδοτημένη κοινοποίηση πληροφοριών, παραποίηση των πληροφοριών, αποκήρυξη ενεργειών και την άρνηση της υπηρεσίας.

Συγκεκριμένα, ένας κινητός χρήστης που συνδέεται με ένα 3G δίκτυο πρέπει να είστε σε θέση να ελέγξει ότι το δίκτυο που τον εξυπηρετεί εξουσιοδοτείται για να προσφέρει υπηρεσίες εξ ονόματος πατρικού δικτύου του χρήστη στην έναρξη, αλλά και κατά τη διάρκεια της παροχής υπηρεσιών. Όλη η ανταλλαγή στοιχείων, που γίνεται μεταξύ του κινητού χρήστη και δικτύου που τον εξυπηρετεί ή του παρόχου/πατρικού δικτύου (SP), πρέπει να είναι προστατευμένες από μη εξουσιοδοτημένη τροποποίηση. Επιπλέον, ο κινητός χρήστης πρέπει να είναι ικανός να διακρίνει εάν η κυκλοφορία των δεδομένων και οι πληροφορίες σχετικές με την κλήση είναι εμπιστευτικά προστατευμένες. Ο τελικός χρήστης πρέπει να βεβαιωθεί επίσης ότι καμία προσωπική πληροφορία, όπως η ταυτότητα χρηστών ή η θέση, δεν αποκαλύπτεται σε άλλα άτομα.



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Από την πλευρά του δικτύου εξυπηρέτησης, οποιοσδήποτε πιθανός εισβολέας πρέπει να αποτρέπεται από μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες μεταμφιεζόμενος σε εξουσιοδοτημένο χρήστη. Πρέπει να είναι δυνατό για το πατρικό δίκτυο, να διακόψει αμέσως όλες τις υπηρεσίες που παρέχονται σε έναν ορισμένο χρήστη ή ομάδα χρηστών, σε περίπτωση που παραβιάζουν τους κανόνες παροχής των υπηρεσιών. Το πατρικό δίκτυο πρέπει να είναι σε θέση να επικυρώσει την προέλευση των δεδομένων του χρήστη, σηματοδοσίας και ελέγχου, ειδικά πάνω από το τρωτό ασύρματο δίκτυο πρόσβασης. Επιπλέον, το δίκτυο πρέπει προστατεύει την εμπιστευτικότητα καθώς επίσης και την μη εξουσιοδοτημένη τροποποίηση των δεδομένων των χρηστών και των δεδομένων σηματοδότησης και ελέγχου.

Τέλος, ο πάροχος πρέπει να αυθεντικοποιήσει τους χρήστες στην έναρξη και κατά τη διάρκεια της παροχής υπηρεσιών, προκειμένου να αποτραπούν οι εισβολείς από τη λήψη μη εξουσιοδοτημένης πρόσβασης. Επιπλέον, ο πάροχος πρέπει να είναι σε θέση να ανιχνεύσει και να αποτρέψει την εξαπάτηση για την χρήση υπηρεσιών (π.χ. αναρμόδια πρόσβαση σε δεδομένα καθώς «κατεβαίνουν» σε έναν εξουσιοδοτημένο χρήστη).

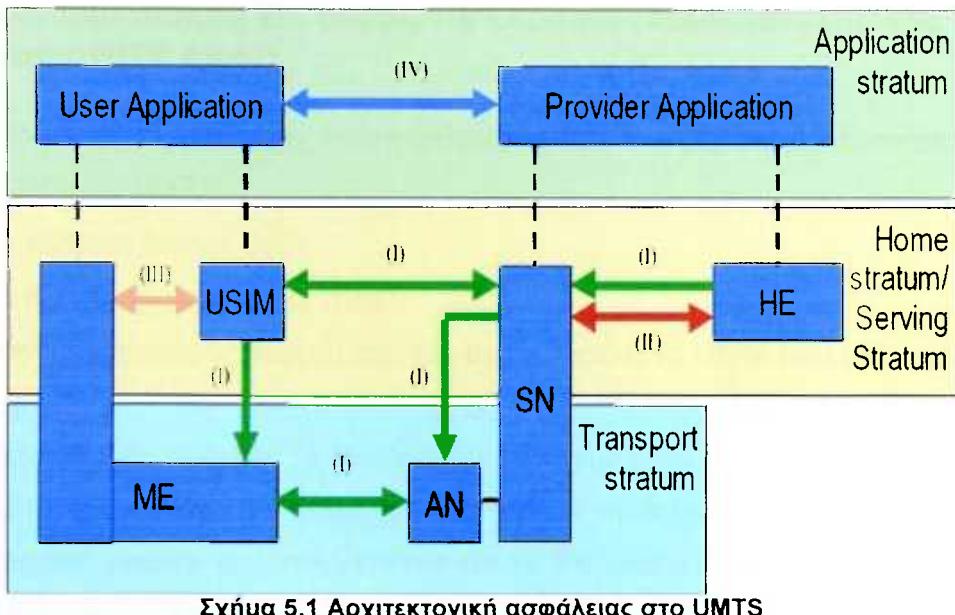
ΚΕΦΑΛΑΙΟ 5

5.1 Ασφάλεια στο UMTS

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο η ασφάλεια στα συστήματα 3G στηρίζεται στις αρχές ασφάλειας των 2G συστημάτων, με βελτιώσεις σε ορισμένα σημεία προκειμένου να παρασχεθεί η προηγμένη υπηρεσία ασφάλειας. Τα στοιχειώδη χαρακτηριστικά γνωρίσματα ασφάλειας που χρησιμοποιούνται στα δίκτυα 2G, όπως η αυθεντικοποίηση των συνδρομητών, η κρυπτογράφηση των δεδομένων πάνω από το ασύρματο δίκτυο πρόσβασης, η εμπιστευτικότητα της ταυτότητας των συνδρομητών, διατηρούνται και ενισχύονται όπου απαιτείται. Ο κεντρικός στόχος της ασφάλειας στα 3G δίκτυα είναι να εξασφαλιστεί ότι όλες οι πληροφορίες που παράγονται και σχετίζονται με έναν χρήστη, καθώς επίσης οι πόροι και υπηρεσίες που παρέχονται από το δίκτυο εξυπηρέτησης, προστατεύονται επαρκώς από την κακή χρήση ή την κατάχρηση. Το επίπεδο ασφαλείας να είναι καλύτερο από των σύγχρονων σταθερών και κινητών δικτύων. Τα χαρακτηριστικά γνωρίσματα ασφάλειας πα είναι επαρκώς τυποποιημένα για να εξασφαλίσει παγκόσμια διαθεσιμότητα, διαλειτουργικότητα, και περιαγωγή μεταξύ διαφορετικών δικτύων Επιπλέον, τα χαρακτηριστικά γνωρίσματα-ασφάλειας και μηχανισμοί να μπορούν να επεκταθούν και να ενισχυθούν όπως απαιτείται από νέες απειλές και υπηρεσίες. Η αρχιτεκτονική ασφαλείας του UMTS χωρίζεται σε πέντε κατηγορίες [3]:

- α) Ασφάλεια στο δίκτυο πρόσβασης
- β) Ασφάλεια στην περιοχή του δικτύου κορμού (κεντρικού δικτύου)
- γ) Ασφάλεια στην περιοχή των χρηστών
- δ) Ασφάλεια στην περιοχή της εφαρμογής
- ε) Διαφάνεια και διαμόρφωση του επιπέδου ασφάλειας

Το σχήμα 5.1 δίνει μια επισκόπηση της αρχιτεκτονική ασφάλειας, και των πέντε σημαντικών κατηγοριών ασφαλείας [3]:



Σχήμα 5.1 Αρχιτεκτονική ασφάλειας στο UMTS

5.2 Ασφάλεια στο δίκτυο πρόσβασης

Η ασφάλεια στο ασύρματο δίκτυο πρόσβασης είναι ένα βασικό συστατικό της αρχιτεκτονικής ασφάλειας του 3G. Παρακάτω θα εξετάσουμε το σύνολο των μηχανισμών ασφάλειας που παρέχουν στους χρήστες ασφαλή πρόσβαση στις υπηρεσίες του 3G δικτύου, καθώς επίσης και προστασία από τις επιθέσεις στο ασύρματο δίκτυο πρόσβασης. Οι μηχανισμοί αυτοί περιλαμβάνουν [3]:

- Αυθεντικοποίηση και συμφωνία κλειδιών.
- Εμπιστευτικότητα της ταυτότητας των χρηστών.
- Εμπιστευτικότητα δεδομένων.
- Προστασία ακεραιότητας των μηνυμάτων σηματοδοσίας.

Η ασφάλεια πρόσβασης στο δίκτυο πραγματοποιείται ανεξάρτητα σε κάθε περιοχή υπηρεσιών (δηλ. περιοχή μεταγωγής κυκλώματος (CS), ή περιοχή μεταγωγής πακέτου (PS)).

5.2.1 Αυθεντικοποίηση και συμφωνία κλειδιών (Authentication and key agreement (UMTS AKA))

Υπάρχουν τρεις οντότητες που περιλαμβάνονται στο μηχανισμό αυθεντικοποίησης στο σύστημα UMTS:

- Το πατρικό δίκτυο. (HE)
- Το δίκτυο εξυπηρέτησης (SN).
- Ο κινητός σταθμός (τερματικό), πιο συγκεκριμένα το USIM που είναι μία έξυπνη κάρτα.

Η βασική ιδέα είναι ότι το δίκτυο εξυπηρέτησης (SN) ελέγχει την ταυτότητα του συνδρομητή, (όπως και στο GSM), με μια τεχνική πρόκλησης-απάντησης (challenge and response), ενώ το τερματικό ελέγχει ότι το SN είναι εγκεκριμένο από το πατρικό δίκτυο (HE), με τον έλεγχο των αριθμών ακολουθίας. Αυτό το τελευταίο γίνεται μόνο στο UMTS ,(μη διαθέσιμο στο GSM), και μέσω αυτού το τερματικό μπορεί να ελέγξει αν συνδέεται με ένα νόμιμο δίκτυο.

Ο ακρογωνιαίος λίθος του μηχανισμού αυθεντικοποίησης, είναι ένα κύριο κλειδί ή κλειδί αυθεντικοποίησης του συνδρομητή K, το οποίο μοιράζεται μεταξύ του USIM του χρήστη και του κέντρου αυθεντικοποίησης του πατρικού δικτύου (AuC). Το κλειδί κρατιέται μόνιμα μυστικό και έχει μήκος 128 bits. Το κλειδί K δεν μεταφέρεται ποτέ έξω από αυτές τις δύο θέσεις (δηλ., ο χρήστης δεν έχει καμία γνώση του κύριου κλειδιού).

Εκτός από την αμοιβαία αυθεντικοποίηση, δημιουργούνται και τα κλειδιά για την κρυπτογράφηση και τον έλεγχο ακεραιότητας. Αυτά είναι προσωρινά κλειδιά, (με το ίδιο μήκος 128 bits) και προέρχονται από το μόνιμο κρυφό κλειδί K κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης.

Υπάρχουν λοιπόν τρεις στόχοι για το UMTS AKA: α) η αμοιβαία αυθεντικοποίηση μεταξύ του χρήστη και του δικτύου β) η καθιέρωση ενός κλειδιού κρυπτογράφησης και ενός κλειδιού ακεραιότητας κατά την διαδικασία της επιτυχούς αυθεντικοποίησης και γ) η διαβεβαίωση του χρήστη για την φρεσκάδα των κλειδιών κρυπτογράφησης, (εμπιστευτικότητας και ακεραιότητας). Μια επισκόπηση του UMTS AKA δίνεται στο σχέδιο 5.3.

Το UMTS AKA πρωτόκολλο αποτελείται από δύο φάσεις: α) η διανομή των δεδομένων αυθεντικοποίησης, (αποκαλούμενα διανύσματα αυθεντικοποίησης), από το πα-



τρικό δίκτυο στο δίκτυο εξυπηρέτησης και β) την αυθεντικοποίηση και διαδικασία συμφωνίας κλειδιών μεταξύ του χρήστη και του εξυπηρετούντος δικτύου. Όταν το πρωτόκολλο εκτελείται στο πατρικό δίκτυο ή όταν το δίκτυο εξυπηρέτησης έχει αχρησιμοποίητα διανύσματα αυθεντικοποίησης για το χρήστη, η πρώτη φάση δεν εκτελείται.

5.2.1.1 Διανομή των διανυσμάτων αυθεντικοποίησης

Το δίκτυο εξυπηρέτησης προκαλεί τη διαδικασία με την αποστολή κατάλληλου μηνύματος, (μήνυμα αιτήματος αυθεντικοποίησης δεδομένων), στο πατρικό δίκτυο, συμπεριλαμβάνοντας την ταυτότητα του κινητού σταθμού. Με την παραλαβή του μηνύματος, το πατρικό δίκτυο επιστρέφει μια απάντηση αυθεντικοποίησης δεδομένων, συμπεριλαμβάνοντας μια διαταγμένη σειρά διανυσμάτων αυθεντικοποίησης (Authentication Vectors, AV). Κάθε τέτοιο διάνυσμα αποτελείται από 5 στοιχεία, είναι δηλαδή μία πεντάδα, (quintet), ανάλογο της «τριπλέτας», του GSM. Συγκεκριμένα κάθε τέτοιο διάνυσμα περιλαμβάνει [3]: α) Έναν τυχαίο αριθμό (RAND), β) μία αναμενόμενη απάντηση (XRES), γ) ένα κλειδί κρυπτογράφησης(CK), δ) ένα κλειδί ελέγχου ακεραιότητας (IK) και ε) ένα αναγνωριστικό αυθεντικοποίησης (AUTN). Κάθε τέτοια πεντάδα(σχέδιο 5.2) παράγεται με την παρακάτω διαδικασία (σχέδιο 5.4):

1) Το κέντρο αυθεντικοποίησης του πατρικού δικτύου (HE/AuC), ξεκινά παράγοντας έναν ακολουθιακό αριθμό (SQN_{HN}), ο οποίος κάθε φορά αυξάνεται από τον προηγούμενο για τον συγκεκριμένο χρήστη. Δηλαδή το HE/AuC κρατά μία λίστα με αριθμούς που έχει δώσει σε κάθε χρήστη και κάθε φορά τον αυξάνει. Ο σκοπός του SQN_{HN} είναι να παρέξει στον χρήστη, (συγκεκριμένα στο USIM), την απόδειξη ότι το συγκεκριμένο διάνυσμα αυθεντικοποίησης είναι νέο (FRESH), έτσι ώστε να μπορεί να χρησιμοποιηθεί για μία και μόνη φορά. Παράλληλα με την επιλογή του SQN_{HN} ;ένας τυχαίος αριθμός RAND μήκους 128 bit παράγεται, από την μονόδρομη συνάρτηση f_0 (SQN_{HN})= RAND.

2) Το HE/AuC υπολογίζει τις ακόλουθες τιμές :

- 1) $XRES = f_k^2(RAND)$
- 2) $CK = f_k^3(RAND)$ (Κλειδί αυθεντικοποίησης-Cipher Key)
- 3) $IK = f_k^4(RAND)$ (Κλειδί ακεραιότητας-Integrity Key)
- 4) $AK = f_k^5(RAND)$ (Κλειδί Ανωνυμίας-Anonymity Key)
- 5) $MAC = f_k^1(SQN \parallel RAND \parallel AMF)$ όπου \parallel σημαίνει παράθεση.

3) Το HE/AuC κατόπιν δημιουργεί το

$AUTN = SQN \oplus AK \parallel AMF \parallel MAC$ και την πεντάδα (RAND,XRES,CK,IK,AUTN) και την αποστέλλει στο δίκτυο εξυπηρέτησης SN (σχέδιο 4.3).

Το κλειδί ανωνυμίας ΑΚ χρησιμοποιείται για να αποκρύψει τον ακολουθιακό αριθμό (SQN), καθώς αν αυτό δεν γίνει, μπορεί να αποκαλυφθεί η θέση του χρήστη. Σε κάθε διάνυσμα αυθεντικοποίησης, εμπεριέχεται ένα πεδίο αυθεντικοποίησης και διαχείρισης κλειδιών (AMF-Authentication and key Management Field), το οποίο χρησιμοποιείται για να καθορίσει τις δυνατότητες από μεριά του δικτύου στην διαδικασία αυθεντικοποίησης (π.χ. χρήση πολλαπλών αλγορίθμων αυθεντικοποίησης ή κλειδί με περιορισμένο χρόνο ζωής).

```

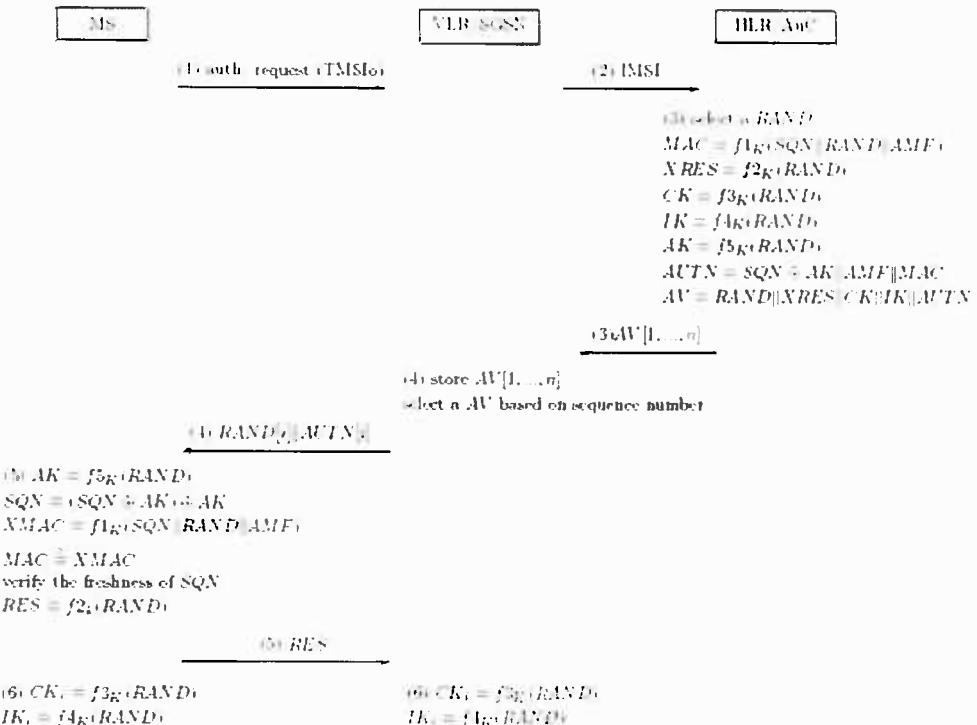
Authentication Vector = AV
{
    RAND   :      128-bit;    --- Pseudo-random number, challenge data;
    XRES   :      32-128 bit;  --- Expected Response, answer to challenge;
    CK     :      128-bit;    --- Cipher Key;
    IK     :      128-bit;    --- Integrity Key;
    AUTN   :      128-bit;    --- Authentication Token, challenge data;
}

Authentication Token = AUTN
{
    SQN    :      48-bit;    --- Sequence Number;
    AMF    :      16-bit;    --- Authentication Management Field;
    MAC-A  :      64-bit;    --- MAC value used for Authentication;
}

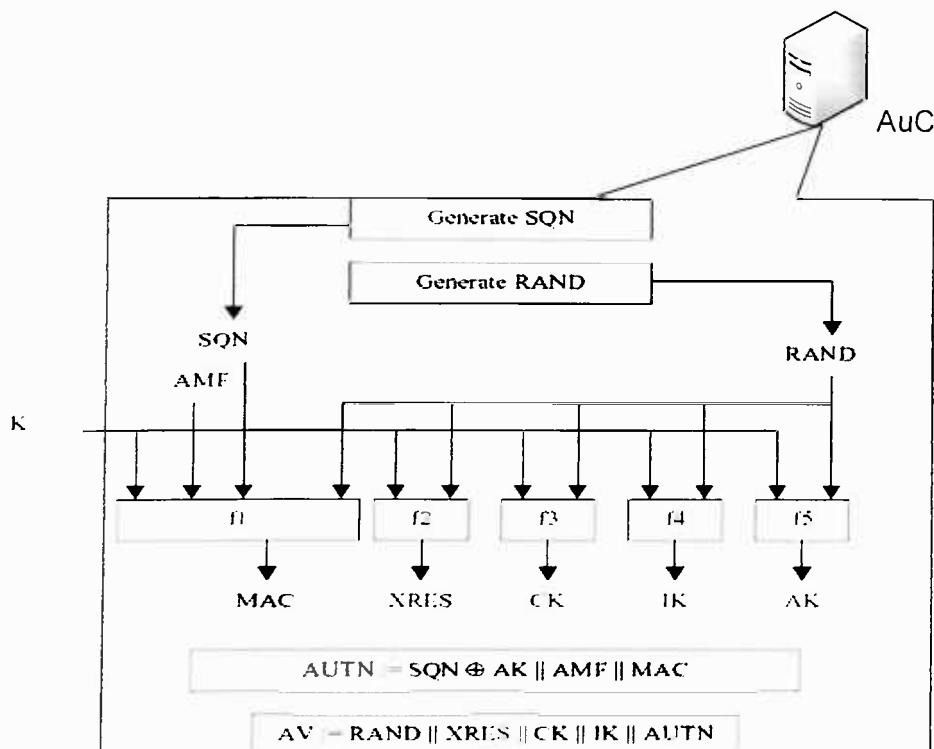
```

Σχήμα 5.2 Διάνυσμα αυθεντικοποίησης (AV) [15]

Ασφάλεια και διαχείριση κλειδιών στο UMTS



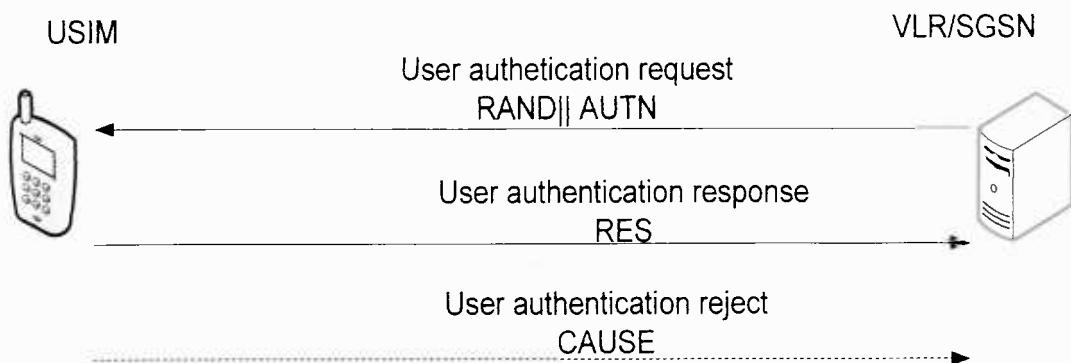
Σχήμα 5.3 Πρωτόκολλο UMTS AKA



Σχήμα 5.4 Υπολογισμός του διανύσματος αυθεντικοποίησης (AV) από το AuC

5.2.1.2 Αυθεντικοποίηση και συμφωνία κλειδιών

Το δίκτυο εξυπηρέτησης ζεκινά αυτήν την διαδικασία, με την επιλογή του επόμενου αχρησιμοποίητου διανύσματος αυθεντικοποίησης από τη διαταγμένη σειρά των διανυσμάτων επικύρωσης που του απεστάλησαν και βρίσκονται αποθηκευμένα στη βάση δεδομένων του. Κάθε διάνυσμα αυθεντικοποίησης χρησιμοποιείται για μία και μόνο αυθεντικοποίηση και συμφωνία κλειδιών μεταξύ του κινητού τερματικού/σταθμού και του δικτύου εξυπηρέτησης. Το δίκτυο εξυπηρέτησης SN στέλνει στο κινητό σταθμό (Mobile Station-MS ή ME) το RAND και το AUTN. Μετά την παραλαβή, αυτός υπολογίζει το κλειδί ανωνυμίας (AK), ($AK = f_k^5(RAND)$), από τον οποίο βρίσκει τον ακολουθιακό αριθμό SQN. (Όπως είναι γνωστό αν εκτελέσουμε 2 φορές την πράξη XOR, (\oplus), αυτή ακυρώνεται). Έτσι με το $SQN = (SQN \oplus AK) \oplus AK$ υπολογίζει το SQN. Κατόπιν υπολογίζει το $MAC = f_k^t(SQN \parallel RAND \parallel AMF)$, το οποίο το συγκρίνει με το MAC που περιέχεται στο AUTN. Εάν είναι διαφορετικά, στέλνει ένα μήνυμα απόρριψης στο δίκτυο εξυπηρέτησης με μια ένδειξη για την αιτία και εγκαταλείπει την διαδικασία (Σχήμα 5.5).



Σχήμα 5.5 Μήνυμα απόρριψης από το UE προς το SN

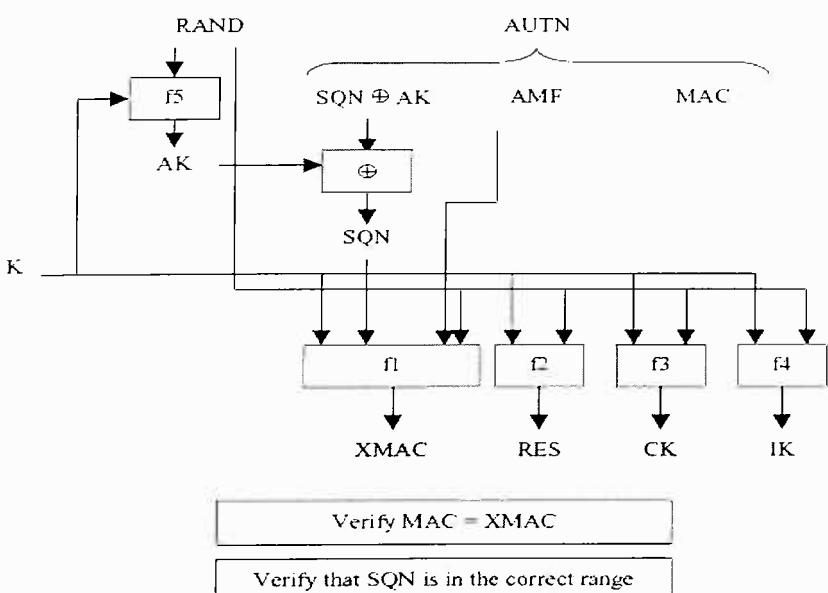
Κατόπιν ελέγχει εάν ο λαμβανόμενος αριθμός ακολουθίας είναι στη σωστή σειρά, δηλαδή εξετάζει εάν αν ο ακολουθιακός αριθμός $SQN_{MS} < SQN_{HN}$.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Αν θεωρήσει ότι ο ακολουθιακός αριθμός δεν είναι στη σωστή σειρά, στέλνει πίσω ένα μήνυμα αποτυχίας συγχρονισμού. Σε αυτήν την περίπτωση, το HN μπορεί να χρειαστεί να επανασυγχρονίσει τον μετρητή SQN_{HN} .

Αν θεωρήσει ότι το SQN_{HN} είναι στο σωστό εύρος, η αυθεντικοποίηση του δικτύου είναι επιτυχημένη. Σε αυτή την περίπτωση, το MS υπολογίζει το $RES = f_k^2(RAND)$ και το αποστέλλει πίσω στο δίκτυο εξυπηρέτησης (SN). Κατόπιν θέτει το $SQN_{MS} = SQN_{HN}$ αν $SQN_{MS} < SQN_{HN}$. Αν όμως $SQN_{MS} \geq SQN_{HN}$ ο κινητός σταθμός, (για την ακρίβεια το USIM), θα δημιουργήσει ένα μήνυμα αποτυχίας συγχρονισμού χρησιμοποιώντας τον μεγαλύτερο ως τώρα αριθμό ακολουθίας που έχει δεχτεί. Πρέπει να τονιστεί επίσης, ότι ο κινητός σταθμός δεν θα δεχτεί έναν αριθμό ακολουθίας, του οποίου η διαφορά από τον προηγούμενο αριθμό είναι μεγαλύτερη από μία τιμή Δ (δηλαδή πρέπει $SQN_{HN} - SQN_{MS} \leq \Delta$). Τέλος υπολογίζει τα $CK = f_k^3(RAND)$ και $IK = f_k^4(RAND)$ (Σχήμα 5.6).

Με την παραλαβή της απάντησης αυθεντικοποίησης του χρήστη, το SN συγκρίνει το RES με την αναμενόμενη απάντηση XRES του διανύσματος αυθεντικοποίησης που έχει επιλεγεί. Αν το $RES = XRES$ η αυθεντικοποίηση του χρήστη είναι επιτυχημένη και το SN παίρνει το κλειδί κρυπτογράφησης (CK), και το κλειδί ακεραιότητας (IK) από το επιλεγμένο διάνυσμα. Αν το $RES \neq XRES$, το SN στέλνει ένα μήνυμα αποτυχημένης αυθεντικοποίησης στο HN και εγκαταλείπει την διαδικασία.



Σχήμα 5.6 Αυθεντικοποίηση του δικτύου από τον κινητό σταθμό (MS)

Αν παρατηρήσουμε το πρωτόκολλο προσεκτικά θα δούμε ότι αποτελείται από 2 φάσεις αλλά από ένα γύρο μηνυμάτων συνολικά. Η επιλογή ενός σχήματος AKA ενός γύρου βεβαιώνει τη σημασία που έχει δοθεί στην απόδοση του AKA. Δεν μπορεί να δαπανηθεί περισσότερος χρόνος από τον χρήστη από αυτόν που είναι αυστηρά απαραίτητος κατά τη διάρκεια της σύνδεσης. Επιλέχτηκε επίσης ένας μηχανισμός που βασίζεται σε MAC. Λύσεις βασισμένες σε MACs έχουν καλή υπολογιστική απόδοση, γεγονός πολύ σημαντικό λαμβανομένου υπόψη ότι οι συναρτήσεις f^1 και f^2 εκτελούνται στο USIM. Κάποιος θα μπορούσε εναλλακτικά να έχει σχεδιάσει τον μηχανισμό με τη χρήση τεχνολογίας δημόσιου κλειδιού και ψηφιακών υπογραφών. Λαμβάνοντας υπόψη το γεγονός ότι οι αλγόριθμοι αυθεντικοποίησης πρέπει να εκτελεστούν σε πραγματικό χρόνο, η ομάδα εργασίας ασφάλειας (SA3) του φορέα προτυποποίησης του UMTS, δηλαδή το 3GPP, αποφάσισε να στηριχθεί στις συμβατικές μεθόδους βασισμένες στη MAC. Οι συναρτήσεις MAC ήταν ήδη σε λειτουργία στο σύστημα GSM/GPRS, και αυτό βεβαίως επηρέασε την απόφασή τους. Βέβαια έχουν προταθεί διάφορα σχήματα αυθεντικοποίησης που στηρίζονται σε κρυπτογραφία δημοσίου κλειδιού. Προγράμματα όπως τα ASPeCT [35] και USECA [36], καθώς επίσης και άλλες πρόσφατες εργασίες [21] περιμένουν μία τέτοια εξέλιξη. Το eNorge 2005 [37] εισαγάγει το PKI για τη Νορβηγία, ενώ τα πρότυπα MexE, WAP, και i-mode της NTT DoCoMo κινούνται προς μηχανισμούς δημοσίου κλειδιού. Επιτυχείς ασύρματες εφαρμογές PKI και λύσεις από επιχειρήσεις όπως οι “Sonera Smarttrust”, “Lucent Technologies” και “Entrust”, ενισχύουν τον ισχυρισμό ότι το PKI αποτελεί έναν πολλά υποσχόμενο μηχανισμό για τα μελλοντικά πρότυπα [21].

5.2.1.3 Επανασυγχρονισμός

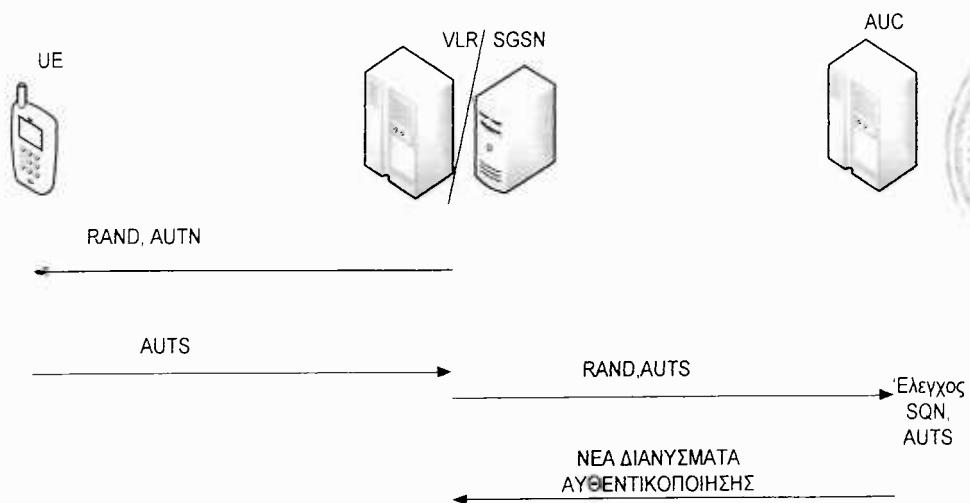
Ένα μήνυμα αποτυχίας συγχρονισμού που εκπέμπεται από το MS, συμπεριλαμβάνει το AUTS το οποίο είναι της μορφής $AUTS = Conc(SQN_{MS}) \parallel MAC-S$ όπου $Conc(SQN_{MS}) = SQN_{MS} \oplus f_k^{S'}(RAND)$ και $MAC-S = f_k^{1'}(SQN_{MS} \parallel RAND \parallel AMF)$.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Όπου SQN_{MS} , είναι η τιμή του αριθμού ακολουθίας που έχει ο κινητός σταθμός (MS). Με την παραλαβή του μηνύματος αποτυχίας συγχρονισμού, το SN στέλνει τα RAND και AUTS στο πατρικό δίκτυο μαζί με μία ένδειξη λάθους συγχρονισμού (σχέδιο 5.7).

Το πατρικό δίκτυο αφού λάβει την ένδειξη αποτυχίας συγχρονισμού εκτελεί τα παρακάτω:

1. Εξάγει το SQN_{MS} και επαληθεύει αν η τιμή του του SQN_{HN} πρέπει να αλλάξει δηλαδή αν $SQN_{HN} < SQN_{MS}$. Αν είναι απαραίτητο, το HN στέλνει μία άλλη σειρά διανυσμάτων αυθεντικοποίησης
2. Με βάση την τιμή SQN_{HN} , το AuC ελέγχει εάν το επόμενο διάνυσμα αυθεντικοποίησης θα ήταν αποδεκτό από το USIM.
 - i. εάν NAI, η διαδικασία συνεχίζεται από το βήμα 4
 - ii. εάν OXI, τότε:
3. Το AuC ελέγχει εάν η τιμή MAC-s στο AUTS είναι σωστή
 - i. εάν NAI, η αξία SQN_{HN} επαναρυθμίζεται σε SQN_{MS} και η διαδικασία συνεχίζεται από το βήμα το 4
 - ii. εάν OXI, τότε SQN_{HN} δεν επαναρυθμίζεται αλλά η διαδικασία συνεχίζεται από το βήμα 4.
4. Το AuC στέλνει καινούρια διανύσματα αυθεντικοπίησης στο VLR/SGSN.



Σχήμα 5.7 Διαδικασία επανασυγχρονισμού

5.2.2 Εμπιστευτικότητα δεδομένων

Μόλις ο χρήστης και το δίκτυο αυθεντικοποιήσουν ο ένας τον άλλον, μπορούν να αρχίσουν ασφαλή επικοινωνία. Όπως περιγράφηκε νωρίτερα, το κυρίως δίκτυο, (δίκτυο κορμού), και ο κινητός σταθμός, (τερματικό), μοιράζονται ένα κλειδί CK, μετά από μία επιτυχημένη αυθεντικοποίηση. Πριν μπορέσει να αρχίσει η κρυπτογράφηση, τα επικοινωνούντα μέρη πρέπει επίσης να συμφωνήσουν σχετικά με τον αλγόριθμο κρυπτογράφησης.

Η κρυπτογράφηση και η αποκρυπτογράφηση πραγματοποιούνται στο τερματικό και στο RNC, το οποίο σημαίνει ότι το κλειδί κρυπτογράφησης CK πρέπει να μεταφερθεί από το κεντρικό δίκτυο στο UTRAN. Αυτό γίνεται, μέσω ενός ειδικού μηνύματος του πρωτοκόλλου RANAP το οποίο ονομάζεται Security Mode Command (SMC). Όταν το RNC κατέχει πια το CK, μπορεί να αρχίσει η κρυπτογράφηση των δεδομένων και γι'αυτό στέλνει μια εντολή στο τερματικό.

Η κρυπτογράφηση στο UTRAN πραγματοποιείται είτε στο επίπεδο ελέγχου πρόσβασης, (Medium Access Control (MAC)), είτε στο επίπεδο ελέγχου συνδέσεων (Radio Link Control layer (RLC)).

Και στις δύο περιπτώσεις, υπάρχει ένας μετρητής που αλλάζει για κάθε μονάδα δεδομένων, (Protocol Data Unit (PDU)), του πρωτοκόλλου. Στο MAC αυτός είναι ο αριθμός σύνδεσης πλαισίου (Connection Frame Number (CFN)) και στο RLC είναι ένας συγκεκριμένος αριθμός ακολουθίας RLC (RLC-SN). Ένας ακόμη πιο μεγάλος μετρητής αποκαλούμενος Hyper Frame Number (HFN) έχει εισαχθεί. Αυτός αυξάνεται όποτε ο σύντομος μετρητής, CFN στην περίπτωση που η κρυπτογράφηση γίνεται στο επίπεδο MAC και RLC-SN στην περίπτωσης που το επίπεδο κρυπτογράφησης είναι το RLC, μηδενίζεται. Ο συνδυασμός του HFN και του σύντομου μετρητή, καλείται COUNT-C και χρησιμοποιείται ως συνεχώς μεταβαλλόμενη εισαγωγή στη γεννήτρια ροής κλειδιών μέσα στο μηχανισμό κρυπτογράφησης.

Ο μακρύτερος αριθμός HFN μηδενίζεται όποτε ένα νέο κλειδί παράγεται κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης του AKA.

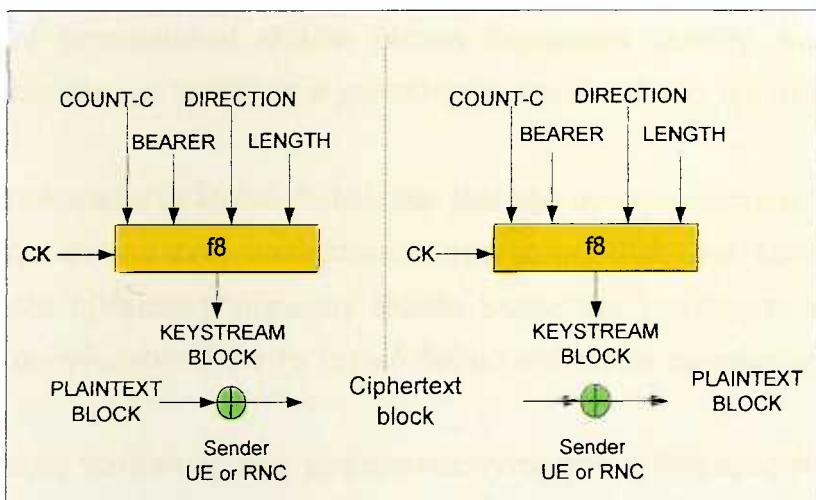
Η ταυτότητα του ασύρματου φορέα (**BEARER**) χρησιμοποιείται επίσης ως εισαγωγή στον αλγόριθμο κρυπτογράφησης καθώς οι μετρητές για δύο διαφορετικούς ασύρματους φορείς διατηρούνται ανεξάρτητα ο ένας από τον άλλον. Εάν λοιπόν δεν ή-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

ταν στην είσοδο του αλγορίθμου, θα μπορούσε να συμβεί η ίδια ομάδα παραμέτρων να αποτελέσει είσοδο στον αλγόριθμο, οπότε αυτό θα οδηγούσε στην ίδια έξοδο της γεννήτριας κλειδοροής.

Η παράμετρος κατεύθυνσης (**DIRECTION**) δείχνει εάν κρυπτογραφούμε ανιούσα (uplink) ή κατιούσα (downlink) κυκλοφορία δεδομένων. Η παράμετρος μήκους (**LENGTH**) δείχνει το μήκος των στοιχείων που κρυπτογραφούνται.

Ο πυρήνας του μηχανισμού κρυπτογράφησης είναι ένας αλγόριθμος, που αναφέρεται σαν συνάρτηση f8 (Σχήμα 5.8). Η προδιαγραφή του 3GPP για την συνάρτηση αυτή είναι βασισμένη στον κρυπταλγόριθμο τμήματος (block cipher) KASUMI (Σχήμα 5.11, Πίνακας 2)



Σχήμα 5.8 Κρυπτογράφηση δεδομένων

Όπως αναφέρθηκε ήδη, είναι δυνατό να μην γίνει αυθεντικοποίηση και συμφωνία κλειδιών στην αρχή της σύνδεσης. Σε αυτήν την περίπτωση, το προηγούμενο κλειδί κρυπτογράφησης CK χρησιμοποιείται για την κρυπτογράφηση. Το κλειδί αποθηκεύεται μέσα στο USIM. Η παράμετρος ΕΝΑΡΞΗΣ, (START), η οποία αποτελείται από το σημαντικότερο τμήμα, (most significant part), τής μέγιστης μέχρι τώρα χρησιμοποιούμενης τιμής του μετρητή HFN, αποθηκεύεται επίσης στο USIM. Για την επόμενη σύνδεση, η αποθηκευμένη τιμή αυξάνεται κατά 2 και χρησιμοποιείται ως τιμή έναρξης για το σημαντικότερο τμήμα του HFN. Υπάρχει επίσης μια σταθερή παράμετρος στη USIM, που λέγεται κατώφλι, (THRESHOLD), το οποίο μπορεί να χρησιμοποιηθεί για να περιορίσει τη μέγιστη διάρκεια ζωής των κλειδιών κρυπτογράφησης CK και ακεραιότητας

ΙΚ. Όποτε η τιμή START φθάνει στην τιμή κατωφλίου, απαιτείται από το UE η παραγωγή νέων κλειδιών, (δηλ., το UE ενημερώνει το δίκτυο ότι δεν έχει κανένα έγκυρο κλειδί).

5.2.3 Εμπιστευτικότητα της ταυτότητας των χρηστών

Οι ταυτότητες που καθορίζονται στο UMTS για κάποιον χρήστη είναι [22] :

- MSISDN (Mobile Subscriber Integrated Services Digital Network) που αντιπροσωπεύει τον τηλεφωνικό αριθμό των χρηστών.
- IMEI (International Mobile Equipment Identity) που αντιπροσωπεύει τον αύξοντα αριθμό της συσκευής και μπορεί να χρησιμοποιηθεί για την πρόληψη κλοπής.
- IMEISV (International Mobile Station Equipment Identity and Software Number) είναι παρόμοια με το IMEI και χαρακτηρίζει την ταυτότητα του υλικού και λογισμικού.
- IMSI (International Mobile Subscriber Identity) αντιπροσωπεύοντας τη μόνιμη ταυτότητα χρηστών που είναι αποθηκευμένη στην στην USIM, (δηλ. έξυπνη κάρτα).
- [P]-TMSI ([Packet]-Temporary Mobile Subscriber Identity) το όποιο είναι ένα προσωρινό αναγνωριστικό για το τοπικό δίκτυο στο οποίο εγγράφεται ένας χρήστης.

Οι διάφορες ταυτότητες που χρησιμοποιούνται από τι διάφορες οντότητες σε ένα UMTS δίκτυο φαίνεται στον παρακάτω πίνακα 5.1.

Ταυτότητα	Τύπος	HLR	VLR	SGSN	GGSN
MSISDN	T	M	M	M	M
IMEI	T	-	-	C	-
IMSI	P	M	M	M	M
[P]-TMSI	T	-	-	C	-

Υπόμνημα: M = mandatory C = conditional T = temporary P = permanent.

Πίνακας 5.1 Οι ταυτότητες ενός κινητού σταθμού στο δίκτυο UMTS

Η αρχιτεκτονική του UMTS για την εμπιστευτικότητα της ταυτότητας των χρηστών πρέπει να έχει τις παρακάτω ιδιότητες:

- **Εμπιστευτικότητα της ταυτότητας των χρηστών:** η ιδιότητα ώστε η μόνιμη ταυτότητα (IMSI) ενός χρήστη στον οποίο οι υπηρεσίες παρέχονται δεν μπορεί να υποκλαπεί από το δίκτυο ασύρματης πρόσβασης.
- **Εμπιστευτικότητα θέσης χρηστών:** η ιδιότητα ώστε η άφιξη ή η αναχώρηση ενός χρήστη από μία περιοχή (ένα δίκτυο) να μην γίνεται αντιληπτή.
- **Μη ανίχνευση (untraceability) των χρηστών:** η ιδιότητα ώστε ένας κακόβουλος να μην μπορεί να καταλάβει εάν διαφορετικές υπηρεσίες χρησιμοποιούνται από τον ίδιο χρήστη υποκλέπτοντας τα δεδομένα πάνω στο ασύρματο δίκτυο πρόσβασης.

Για την επίτευξη των παραπάνω ο προσδιορισμός του χρήστη στο UTRAN γίνεται σχεδόν σε όλες τις περιπτώσεις με τη βοήθεια των προσωρινών ταυτοτήτων: την TMSI για το δίκτυο μεταγωγής κυκλώματος και P-TMSI για το δίκτυο μεταγωγής πακέτων. Έτσι η εμπιστευτικότητα της ταυτότητας χρηστών είναι σχεδόν πάντα προστατευμένη από τους παθητικούς ωτακουστές. Η αρχική εγγραφή στο δίκτυο είναι βέβαια η εξαίρεση, καθώς εκεί μια προσωρινή ταυτότητα δεν μπορεί να χρησιμοποιηθεί δεδομένου ότι το δίκτυο δεν ξέρει ακόμα τη μόνιμη ταυτότητα του χρήστη. Μετά από αυτό είναι δυνατό να χρησιμοποιηθούν προσωρινές ταυτότητες.

Υποθέστε ότι ο χρήστης έχει ήδη αναγνωρισθεί από το δίκτυο που τον εξυπηρετεί από την μόνιμη ταυτότητά του (IMSI). Κατόπιν το δίκτυο, (VLR ή SGSN), διαθέτει στον χρήστη μια προσωρινή ταυτότητα (TMSI ή P-TMSI) και διατηρεί μια συσχέτιση μεταξύ της μόνιμης και προσωρινής ταυτότητας. Η τελευταία, έχει μόνο τοπική αξία και κάθε VLR ή SGSN φροντίζει να μην διαθέτει το ίδια προσωρινή ταυτότητα σε δύο διαφορετικούς χρήστες. Η διατιθέμενη προσωρινή ταυτότητα μεταφέρεται στους χρήστες μία και μόνη φορά μόλις γίνει δυνατή η κρυπτογράφηση των δεδομένων. Αυτή η ταυτότητα χρησιμοποιείται έπειτα για την αναγνώριση του χρήστη από το δίκτυο, μέχρι αυτό να του διαθέσει μία νέα προσωρινή ταυτότητα.

Όταν ο κινητός σταθμός με την αποστολή μηνύματος αποδοχής (ACK) καταστήσει σαφές προς το δίκτυο ότι έχει παραλάβει μια νέα προσωρινή ταυτότητα, η παλαιά προσωρινή ταυτότητα αφαιρείται από το VLR (ή SGSN). Εάν το ACK δεν παραληφθεί από το VLR/SGSN, αυτό κρατά την παλιά και την νέα προσωρινή ταυτότητα, χρησιμοποιώντας και τις δύο για την αναγνώριση του κινητού σταθμού από το δίκτυο. Για

Ασφάλεια και διαχείριση κλειδιών στο UMTS

την κίνηση των δεδομένων προς το τερματικό χρησιμοποιείται η μόνιμη ταυτότητα (IMSI), επειδή το δίκτυο δεν ξέρει ποια προσωρινή ταυτότητα έχει το τερματικό. Σε αυτήν την περίπτωση, το VLR/SGSN λέει στον κινητό σταθμό να σβήσει τα αποθηκευμένα TMSI/P-TMSI και του διανέμει μία άλλη προσωρινή ταυτότητα.

Δεδομένου ότι η προσωρινή ταυτότητα έχει μόνο τοπική έννοια, η ταυτότητα της περιοχής πρέπει να παρατίθεται προκειμένου να υπάρχει μια μοναδική ταυτότητα για το χρήστη. Αυτό επιλύεται παραθέτοντας την ταυτότητα της περιοχής Location Area Identity (LAI) στην ταυτότητα TMSI και την Routing Area Identity (RAI) στο P-TMSI.

Αλλά πώς το δίκτυο εξυπηρέτησης παίρνει το IMSI για πρώτη φορά; Όταν ο χρήστης μπει σε μια νέα περιοχή, η σχέση μεταξύ IMSI και (P-)TMSI ανακαλείται από την παλιά τοποθεσία. Συγχρόνως, αχρησιμοποίητα διανύσματα αυθεντικοίσης (AVs) μπορούν επίσης να μεταφερθούν από το παλαιό VLR/SGSN στο νέο VLR/SGSN (εάν υπάρχουν). Εάν κάτι τέτοιο δεν είναι δυνατό, το IMSI πρέπει να ξαναζητηθεί από τον κινητό σταθμό. Υπάρχουν ορισμένες θέσεις, όπως οι αερολιμένες, όπου πολλά IMSIs διαβιβάζονται πάνω από το ασύρματο δίκτυο πρόσβασης καθώς οι χρήστες θέτουν σε λειτουργία τις συσκευές τους. Αυτό σημαίνει ότι σε τέτοια μέρη είναι δυνατή η υποκλοπή των μονίμων ταυτοτήτων των χρηστών.

Αν και ο μηχανισμός εμπιστευτικότητας της ταυτότητας των χρηστών στο UMTS δεν δίνει 100% προστασία, ωστόσο προσφέρει ένα αρκετά καλό επίπεδο προστασίας. Σημειώστε ότι ένας κακόβουλος, μπορεί να προσποιηθεί ότι είναι ένα νέο δίκτυο εξυπηρέτησης και ο χρήστης είναι πιθανό να αποκαλύψει τη μόνιμη ταυτότητά του. Ο αμοιβαίος ο μηχανισμός αυθεντικοίσης δεν βοηθά εδώ, δεδομένου ότι ο χρήστης πρέπει να αναγνωρισθεί από το δίκτυο πριν μπορέσει να αυθεντικοποιηθεί.

5.2.4 Προστασία ακεραιότητας των μηνυμάτων σηματοδοσίας

Η υπηρεσία ασφάλειας ακεραιότητας πραγματοποιείται μέσω ενός μηχανισμού αυθεντικοίσης μηνυμάτων (MAC), η οποία παρέχει αυθεντικοίση των μηνυμάτων και προστασία ακεραιότητας ενάντια στις σκόπιμες τροποποιήσεις. Η προεπιλεγμένη συνάρτηση MILENAGE f4 (Πίνακας 5.2) παράγει ένα IK με 128 σημαντικά bits. Η

Ασφάλεια και διαχείριση κλειδιών στο UMTS

προστασία ακεραιότητας στο UMTS καλύπτει μέχρι εκεί που καλύπτει και η εμπιστευτικότητα (δηλ., η προστασία ακεραιότητας υιοθετείται μεταξύ τερματικού και RNC).

Ενώ η εμπιστευτικότητα στο UMTS καλύπτει τόσο τα δεδομένα του χρήστη όσο και σηματοδοσίας, η ακεραιότητα καλύπτει μόνο τα δεδομένα σηματοδοσίας.

Ο σκοπός της προστασίας ακεραιότητας είναι να αυθεντικοποιηθούν τα μεμονωμένα μηνύματα ελέγχου. Αυτό είναι σημαντικό, δεδομένου ότι οι χωριστές διαδικασίες αυθεντικοποίησης δίνουν διαβεβαίωση για τις ταυτότητες των επικοινωνούντων μερών μόνο κατά την διάρκεια της αυθεντικοποίησης. Αυτό αφήνει το περιθώριο σε έναν κακόβουλο, να ενεργήσει ως απλός αναμεταδότης και να παραδώσει όλα τα μηνύματα στη σωστή μορφή τους μέχρι τη διαδικασία της αυθεντικοποίησης, ενώ μετά μπορεί να τα μεταβάλλει. Αν όμως τα μηνύματα είναι προστατευμένα για ακεραιότητα, αυτή η μεταβολή δεν μπορεί να γίνει.

Η προστασία ακεραιότητας εφαρμόζεται στο επίπεδο RRC (δηλ., μεταξύ του τερματικού και RNC) και ο μηχανισμός προστασίας ακεραιότητας είναι βασισμένος στην έννοια του MAC, το οποίο είναι μια μονόδρομη συνάρτηση. Η συνάρτηση είναι η f9 από την οποία παράγεται το MAC-I μία τριανταδυάμπιτη τυχαία συμβολοσειρά, η οποία παρατίθεται σε κάθε μήνυμα.

Στην πλευρά του αποστολέα, το MAC-I υπολογίζεται και επισυνάπτεται σε κάθε μήνυμα, (ας το ονομάσουμε μήνυμα RRC), ενώ στην πλευρά του παραλήπτη, το MAC-I υπολογίζεται επίσης και το αποτέλεσμα του υπολογισμού ελέγχεται για να εξασφαλιστεί ότι είναι ίσο με αυτό που επισυνάπτεται στο μήνυμα. Οποιαδήποτε αλλαγή σε οποιαδήποτε από τις παραμέτρους εισόδου έχει επιπτώσεις στο MAC-I με έναν απρόβλεπτο τρόπο.

Η συνάρτηση f9 απεικονίζεται στο σχήμα 5.9. Οι είσοδοι της είναι το IK, το μήνυμα RRC, ένας μετρητής COUNT-I, ένα bit κατεύθυνσης (uplink/downlink) και μια τυχαία συμβολοσειρά (FRESH). Η παράμετρος COUNT-I μοιάζει με τον αντίστοιχο μετρητή για την κρυπτογράφηση. Το σημαντικότερο τμήμα του HFN που αποτελείται από 28 bits σε αυτήν την περίπτωση, όπου τα τέσσερα λιγότερο σημαντικά bits περιέχουν τον αριθμό ακολουθίας του μηνύματος RRC. Το COUNT-I, προστατεύει από την επανάληψη προηγούμενων μηνυμάτων ελέγχου εγγυώμενο ότι το σύνολο των τιμών των παραμέτρων εισαγωγής είναι διαφορετικό για κάθε αποτέλεσμα της συνάρτησης f9.



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ο αλγόριθμος για την προστασία ακεραιότητας είναι βασισμένος στον ίδιο πυρήνα με της κρυπτογράφησης. Ο κρυπταλγόριθμος ροής KASUMI χρησιμοποιείται σε έναν ειδικό τρόπο λειτουργίας για να δημιουργήσει μία συνάρτηση MAC.

Η παράμετρος FRESH επιλέγεται από το RNC και διαβιβάζεται στον κινητό σταθμό. Απαιτείται για να προστατευθεί το δίκτυο από μια κακόβουλα επιλεγμένη τιμή έναρξης για το COUNT-I. Πράγματι, καθώς το σημαντικότερο τμήμα του HFN αποθηκεύεται στο USIM, ένας κακόβουλος, θα μπορούσε να μεταμφιεστεί ως USIM και να στείλει μία ψεύτικη τιμή στο δίκτυο, αναγκάζοντας την αρχική τιμή του HFN, (START), να είναι πάρα πολύ μικρή. Εάν η διαδικασία αυθεντικοποίησης δεν απαιτηθεί να ξεκινήσει και χρησιμοποιηθεί το παλαιό κλειδί ακεραιότητας IK, δημιουργείται η πιθανότητα για τον κακόβουλο, αν η παράμετρος FRESH δεν υπήρχε, να επαναλάβει τα μηνύματα RRC από προηγούμενες συνδέσεις με τις τιμές MAC-I που έχει καταγράψει,. Επιλέγοντας την FRESH τυχαία, το RNC προστατεύεται από μια τέτοια επίθεση. Δηλαδή, ο συνεχώς αυξανόμενος ο μετρητής COUNT-I προστατεύει από τις επιθέσεις επανάληψης που είναι βασισμένες στην καταγραφή των παραμέτρων κατά τη διάρκεια της μιας σύνδεσης, επειδή η τιμή του FRESH παραμένει σταθερή κατά την διάρκεια μιας σύνδεσης ενώ αλλάζει στην επόμενη.

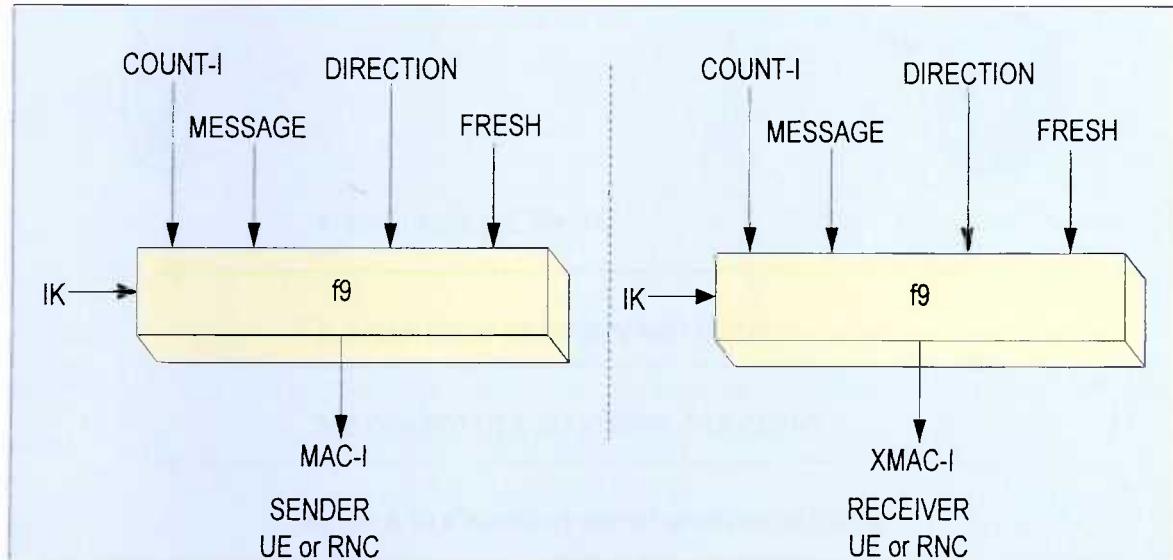
Υπάρχουν όμως μηνύματα ελέγχου RRC, των οποίων ακεραιότητα δεν μπορεί να προστατευθεί από τον μηχανισμό που μόλις περιγράψαμε. Παράδειγμα, τα μηνύματα που στέλνονται πριν το IK τεθεί σε ισχύ δεν μπορούν να προστατευθούν. Ένα χαρακτηριστικό παράδειγμα είναι το RRC μήνυμα αίτησης σύνδεσης (connection request) που στέλνεται από το UE.

ΑΛΓΟΡΙΘΜΟΣ	ΣΚΟΠΟΣ/ΧΡΗΣΗ	O: Operator specific S: Fully standardized	ΤΟΠΟΘΕΣΙΑ
f0	Random challenge generating function	O	AuC
f1	Network authentication function	O – (MILENAGE)	USIM and AuC
f1*	Resynchronization message authentication function	O – (MILENAGE)	—
f2	User challenge-response authentication function	O – (MILENAGE)	—

Ασφάλεια και διαχείριση κλειδιών στο UMTS

f3	Cipher key derivation function	O – (MILENAGE)	—
f4	Integrity key derivation function	O – (MILENAGE)	—
f5	Anonymity key derivation function for normal operation	O – (MILENAGE)	—
f5*	Anonymity key derivation function for resynchronization	O – (MILENAGE)	—
f6	MAP encryption algorithm	S	MAP nodes
f7	MAP integrity algorithm	S	—
f8	UMTS encryption algorithm	S – (KASUMI)	MS and RNC
f9	UMTS integrity algorithm	S – (KASUMI)	—

Πίνακας 5.2 Αλγόριθμοι που χρησιμοποιούνται στο UMTS



Σχήμα 5.9 Προστασία ακεραιότητας στο UMTS

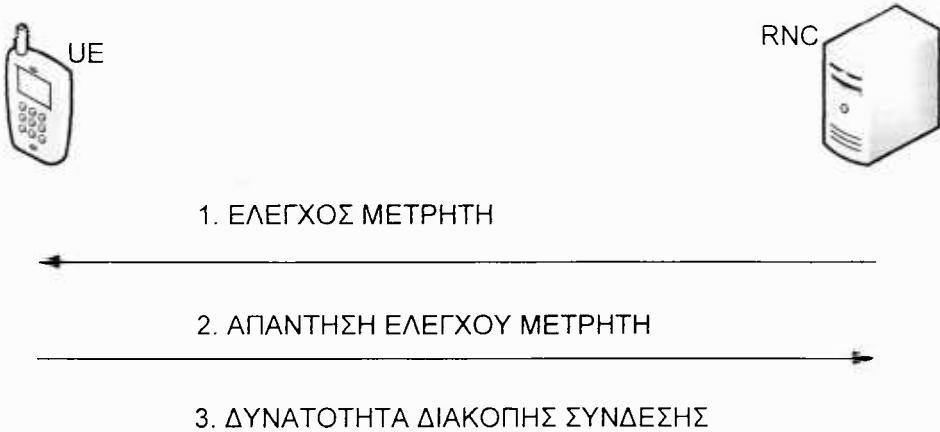
5.2.4.1 Περιοδική Αυθεντικοποίηση

Ο μηχανισμός προστασίας ακεραιότητας στο UTRAN δεν εφαρμόζεται στα δεδομένα του χρήστη, (U-plane), για λόγους απόδοσης. Εντούτοις, υπάρχει μία συγκεκριμένη (προστατευμένη από ακεραιότητα) διαδικασία στο επιπέδου ελέγχου, (C-plane), που χρησιμοποιείται για περιοδική τοπική αυθεντικοποίηση. Ως αποτέλεσμα αυτής της διαδικασίας, η ποσότητα των δεδομένων που στέλνεται κατά τη διάρκεια της σύνδεσης RRC ελέγχεται. Ως εκ τούτου, η αριθμητική τιμή των όγκου των δεδομένων των χρη-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

στών που έχουν μεταφερθεί είναι προστατευμένη από ακεραιότητα και συγχρόνως, η διαδικασία παρέχει τοπική αυθεντικοποίηση των οντοτήτων.

Η περιοδική τοπική αυθεντικοποίηση αρχίζει από το RNC και προκαλείται από το COUNT-C όταν φθάνει σε μία κρίσιμη τιμή, (π.χ. ένα συγκεκριμένο bit στο HFN αλλάξει). Τότε το RNC στέλνει ένα μήνυμα ελέγχου που περιέχει το σημαντικότερο τμήμα από το COUNT-C, που αντιστοιχεί σε κάποια ενεργή σύνδεση. Ο κινητός σταθμός UE συγκρίνει το με το δικό του σημαντικότερο τμήμα από το COUNT-C. Όλες οι διαφορές αναφέρονται με ένα μήνυμα ελέγχου μετρητή (counter check response). Εάν το μήνυμα απάντησης δεν περιέχει τιμές, η διαδικασία τελειώνει. Εάν υπάρχουν διαφορές, το RNC μπορεί να τερματίσει τη σύνδεση (στην περίπτωση που οι διαφορές δεν μπορούν να γίνουν αποδεκτές). Η διαδικασία απεικονίζεται στο σχήμα 5.10.



Σχήμα 5.10 (Περιοδική τοπική αυθεντικοποίηση)

Η περιοδική τοπική αυθεντικοποίηση δίνει προστασία ενάντια σε έναν κακόβουλο που προσπαθεί να τοποθετήσει εμβόλιμα ή να διαγράψει πακέτα δεδομένων κατά τη διάρκεια μιας σύνδεσης. Η προστασία είναι ιδιαίτερα σημαντική σε περίπτωση που η κρυπτογράφηση δεν είναι σε χρήση. Σημειώστε ότι σε αυτήν την περίπτωση και το UE και το RNC είναι ανάγκη να διατηρούν τιμές COUNT-C παρά το γεγονός δεν χρησιμοποιούνται για την κρυπτογράφηση.

Ο κακόβουλος θα μπορούσε ίσως να δοκιμάσει να εισάγει και να διαγράψει τον ίδιο αριθμό πακέτων προκειμένου να κρατηθούν οι τιμές COUNT-C συγχρονισμένες. Ο νόμιμος χρήστης δεν μπορεί να σταματήσει αυτόν τον τύπο επίθεσης.

5.2.4.2 Διαδικασία εγκαθίδρυσης ασφαλούς συνόδου επικοινωνίας

Ας δούμε τώρα τα πράγματα συνολικά για την εγκαθίδρυση μιας ασφαλούς συνόδου. Τα βήματα τα οποία γίνονται είναι τα παρακάτω (Σχήμα 5.11):

1. Ο κινητός σταθμός και ο σταθμός βάσεως εγκαθιδρύουν μία σύνδεση RRC (Radio Recourse Control Connection (RRC)). Κατά τη διάρκεια της εγκαθίδρυσης της σύνδεσης, ο κινητός σταθμός στέλνει τις δυνατότητες ασφαλείας του στο σταθμό βάσεως. Οι δυνατότητες ασφάλειας περιλαμβάνουν τους υποστηριζόμενους UMTS αλγόριθμους ακεραιότητας και κρυπτογράφησης και προαιρετικά GSM ικανότητες κρυπτογράφησης. Ο κινητός σταθμός στέλνει επίσης την παράμετρο ENAPΞΗΣ, (START), του οποίου η τιμή είναι η τιμή του σημαντικότερου τμήματος του μέγιστου χρησιμοποιούμενου μέχρι τώρα HFN, αυξανομένου κατά 2 σε κάθε καινούρια σύνδεση
2. Ο κινητός σταθμός στέλνει επίσης την τρέχουσα προσωρινή ταυτότητά του TMSI στο δίκτυο, δηλαδή στέλνει το αρχικό L3 μήνυμα (που περιλαμβάνει αίτημα ανανέωσης θέσης, αίτημα παροχής υπηρεσιών, αίτημα αναπροσαρμογής περιοχής δρομολόγησης, αίτημα σύνδεσης κ.λπ....), στο VLR/SGSN. Αυτό το μήνυμα περιέχει την ταυτότητα χρηστών και το KSI, (Key set identifier)). Το συμπεριλαμβανόμενο KSI (ομάδα κλειδιών αναγνώρισης (Key set identifier)) είναι αυτό που δόθηκε στον κινητό σταθμό από την περιοχή υπηρεσιών μεταγωγής κυκλώματος (CS) ή την περιοχή υπηρεσιών μεταγωγής πακέτου (PS) στην τελευταία αυθεντικοποίηση.
3. Εάν το δίκτυο δεν μπορεί να συσχετίσει το TMSI ζητά από τον κινητό σταθμό να στείλει τη μόνιμη ταυτότητά του και οι κινητός σταθμός απαντά στο αίτημα με το IMSI.
4. Το δίκτυο εξυπηρέτησης ζητά τα στοιχεία αυθεντικοποίησης από το πατρικό δίκτυο του κινητού σταθμού.
5. Το πατρικό δίκτυο απαντά με το διάνυσμα αυθεντικοποίησης (RAND, AUTN, XRES, IK, CK).
6. Το δίκτυο εξυπηρέτησης στέλνει τα RAND και AUTN στον κινητό σταθμό.
7. Ο κινητός σταθμός επαληθεύει το AUTN και υπολογίζει την απάντηση αυθεντικοποίησης. Εάν το AUTN δεν είναι σωστό ο κινητός σταθμός απορρίπτει το μήνυμα.

8. Ο κινητός σταθμός στέλνει την απάντηση επικύρωσής του RES στο δίκτυο εξυπηρέτησης.

9. Το δίκτυο ελέγχει εάν RES=XRES και αποφασίζει ποιοι αλγόριθμοι ασφάλειας επιτρέπεται να χρησιμοποιηθούν στο UTRAN.

10. Το δίκτυο εξυπηρέτησης στέλνει τους επιτρεπόμενους προς χρήση αλγορίθμους στο UTRAN δηλαδή, το VLR/SGSN αρχίζει την ακεραιότητα και την εμπιστευτικότητα με την αποστολή του τρόπου ασφάλειας (μήνυμα RANAP) στο SRNC. Αυτό το μήνυμα περιέχει έναν διαταγμένο κατάλογο των δυνατοτήτων ασφαλείας, UIAs (User equipment Integrity Capabilities), και UEAs (User equipment Encryption Capabilities) κατά σειρά την προτίμηση, το κλειδί ακαιρεότητας IK και κρυπτογράφησης CK. Εάν μια νέα αυθεντικοποίηση και παραγωγή κλειδιών έχουν εκτελεστεί (βλ. 4 έως 9 ανωτέρω), αυτό θα υποδειχθεί στο μήνυμα που στέλνεται στο SRNC. Η ένδειξη χρήσης των νέων κλειδιών θα προκαλέσει τον μηδενισμό της τιμής START. Διαφορετικά, παραμένει η τιμή START που είναι ήδη διαθέσιμη στο SRNC που θα χρησιμοποιηθεί (βήμα 1).

11. Το δίκτυο ασύρματης πρόσβασης αποφασίζει ποιους από τους επιτρεπόμενους αλγορίθμους να χρησιμοποιήσει. Με την επιλογή δηλαδή του προτιμώμενου αλγορίθμου από τον κατάλογο των αλγορίθμων που απεστάλησαν από τον κινητό σταθμό, το SRNC παράγει μια τυχαία τιμή FRESH και αρχίζει την προστασία ακεραιότητας των δεδομένων που αποστέλλονται στον κινητό σταθμό. Εάν οι απαιτήσεις που απεστάλησαν από το VLR/SGSN δεν μπορούν να ικανοποιηθούν, το SRNC στέλνει ένα μήνυμα απόρριψης (SECURITY MODE REJECT) στο VLR/SGSN.

12. Το ασύρματο δίκτυο πρόσβασης ενημερώνει τον κινητό σταθμό για την επιλογή του με ένα μήνυμα ασφαλούς τρόπου ασφάλειας (security mode command message). Το μήνυμα περιλαμβάνει επίσης τις δυνατότητες ασφάλειας που το δίκτυο παραλαμβάνει από τον κινητό σταθμό στο βήμα 1.

13. Ο κινητός σταθμός επικυρώνει την προστασία ακεραιότητας και ελέγχει την ακρίβεια των δυνατοτήτων ασφάλειας, (δηλαδή αυτές που είχε στείλει στο βήμα 1, με αυτές που παρέλαβε στο βήμα 12. Ο κινητός σταθμός υπολογίζει το MAC-I στο μήνυμα που λαμβάνει με τη χρησιμοποίηση του UIA, (User equipment Integrity Capabilities), που λαμβάνει, του αποθηκευμένου COUNT-I και της λαμβανόμενης

Ασφάλεια και διαχείριση κλειδιών στο UMTS

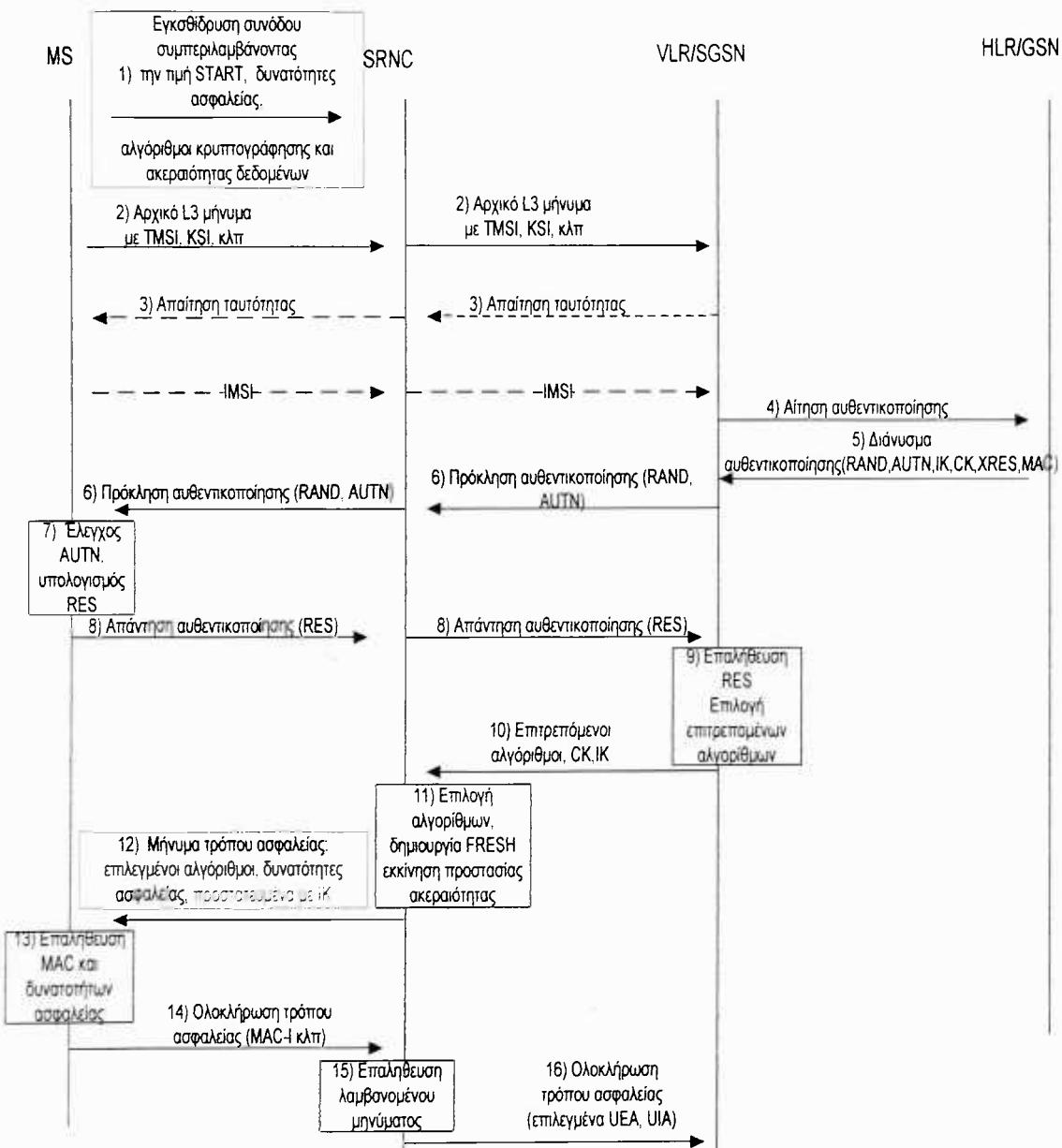
FRESH παραμέτρου. Ο κινητός σταθμός ελέγχει την ακεραιότητα του μηνύματος με τη σύγκριση του λαμβανόμενου MAC-I με το παραγόμενο MAC-I.

14. Αν όλοι οι έλεγχοι είναι επιτυχείς, ο κινητός σταθμός ακολουθεί τον τρόπο ασφάλειας που προδιαγράφει το μήνυμα RRC και παράγει το MAC-I για αυτό το μήνυμα. Εάν οποιοσδήποτε έλεγχος δεν είναι επιτυχής, η διαδικασία τελειώνει στον κινητό σταθμό.

15. Με τη λήψη του μηνύματος απάντησης, το SRNC υπολογίζει το MAC-I του μηνύματος. Το SRNC ελέγχει την ακεραιότητα στοιχείων του μηνύματος με τη σύγκριση του λαμβανόμενου MAC-I με το παραγόμενο MAC-I.

16. Η διαδικασία τελειώνει τη με τη μεταφορά του μηνύματος απάντησης RANAP που περιλαμβάνει τις παραμέτρους ασφαλείας, συμπεριλαμβανομένων των επιλεγμένων αλγορίθμων, από SRNC στο VLR/SGSN.

Ασφάλεια και διαχείριση κλειδιών στο UMTS



Σχήμα 5.11 Εγκαθίδρυση ασφαλούς συνόδου στο UMTS

ΚΕΦΑΛΑΙΟ 6

Όπως έχει γραφτεί πολλές φορές στα πλαίσια αυτής της εργασίας, η ασφάλεια στο UMTS αποτελεί μία σαφή βελτίωση της ασφάλειας του GSM/GPRS (Πίνακας 6.1). Η αρχιτεκτονική ασφαλείας του GSM/GPRS όμως, (κυρίως για λόγους προς τα πίσω συμβατότητας), δεν παύει να αποτελεί την βάση στην οποία στηρίχθηκε και αναπτύχθηκε η αρχιτεκτονική ασφαλείας του UMTS. Έτσι εξαιτίας αυτού του γεγονότος, η αρχιτεκτονική ασφαλείας του UMTS εμφανίζει ορισμένα τρωτά σημεία/αδυναμίες που ίσως θα μπορούσε να εκμεταλλευτεί κάποιος κακόβουλος. Αυτά θα προσπαθήσουμε να αναδείξουμε σε αυτό το κεφάλαιο.

	GSM	UMTS
Network authentication	no	Yes
User traffic confidentiality coverage	MS↔BS	MS↔RNC
Confidentiality in core network	No	Yes
Confidentiality in inter-network	No	Yes
Confidentiality key length	64-bit	128-bit
User traffic integrity protection	No	No
System signalling integrity protection	No	Yes
Integrity key length	N/A	128-bit
Bandwidth consumption between VLR and HLR	Yes	Yes
Memory overhead in VLR	Yes	Yes
Secure subscriber identity/location confidentiality	No	No
Authentication vectors transferable	Yes	Yes

Πίνακας 6.1 Σύγκριση δυνατοτήτων ασφαλείας GSM-UMTS

6.1 Προβλήματα ασφαλείας στο UMTS

Μέσω των αριθμών ακολουθίας, ο χρήστης εξασφαλίζεται ότι οι πληροφορίες αυθεντικοποίησης (δηλαδή RAND και AUTN) δεν μπορούν να επαναχρησιμοποιηθούν από έναν κακόβουλο ή από ένα δίκτυο εξυπηρέτησης. Το δίκτυο εξυπηρέτησης αυθεντικοποιεί το χρήστη με την επαλήθευση της απάντησης RES που λαμβάνει από αυτού.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ο χρήστης, εντούτοις, μπορεί μόνο να ελέγξει μέσω του αριθμού ακολουθίας, εάν ένα διάνυσμα αυθεντικοποίησης δόθηκε από το πατρικό δίκτυο στο δίκτυο εξυπηρέτησης κατόπιν αίτησης του τελευταίου.

6.1.1 Αδυναμίες

1 Η μεταφορά των διανυσμάτων αυθεντικοποίησης μέσα στο δίκτυο ή διαμέσου των δικτύων που παρεμβάλλονται μεταξύ του SGSN και του HS καταστρατηγεί έναν βασικό κανόνα ασφαλείας, σύμφωνα με τον οποίο η ανταλλαγή κλειδιών μέσα στο δίκτυο υποβαθμίζει την ασφάλεια του δικτύου [19].

2 Η υπηρεσία ακεραιότητας στο UMTS περιορίζεται μόνο στα σήματα σηματοδοσίας μεταξύ των κινητών σταθμών και του RNC, αλλά όχι στα δεδομένα του χρήστη. Ο λόγος είναι ότι αυτά τα σήματα σηματοδοσίας θεωρούνται ευαίσθητα και πρέπει να προστατευθούν από ακεραιότητα. Επίσης, το δίκτυο UMTS είναι σε θέση να καθοδηγήσει τους κινητούς σταθμούς να εγκαθιδρύσουν μία σύνοδο χωρίς κρυπτογράφηση για πολλούς λόγους. Έτσι ένας κακόβουλος μπορεί να υποδυθεί ένα δίκτυο για να καθιερώσει μία μη κρυπτογραφημένη σύνοδο με τον κινητό σταθμό. Κατόπιν να υποκλέψει τα δεδομένα και να κάνει εισαγωγή, αλλαγή, ακόμη και διαγραφή των δεδομένων του χρήστη καθώς αυτά δεν προστατεύονται από ακεραιότητα.

3 Η ταυτότητα και η θέση του κινητού χρήστη είναι πολύτιμες πληροφορίες που απαιτούν προστασία. Μια αδυναμία στην αρχιτεκτονική ασφάλειας του UMTS είναι η παρουσίαση της ταυτότητας του χρήστη προς το δίκτυο εξυπηρέτησης (MSC/VLR). Συγκεκριμένα, όποτε το VLR του δικτύου εξυπηρέτησης δεν μπορεί να συνδέσει το TMSI με το διεθνή κινητή ταυτότητα του συνδρομητή (IMSI) το VLR ζητάει από τον χρήστη να εκπέμψει το IMSI, το οποίο ο κινητός σταθμός εκπέμπει πάνω από το ασύρματο δίκτυο πρόσβασης. Επιπλέον, όταν ο χρήστης αλλάζει δίκτυα κατά την διάρκεια της κινησής του και το νέο VLR (SN/VLR_n) δεν μπορεί να έρθει σε επαφή με το προηγούμενο VLR (VLR_o), ή δεν μπορεί να ανακτήσει την ταυτότητα του χρήστη για οποιοδήποτε λόγο, το SN/VLR_n πρέπει επίσης να ζητήσει από το χρήστη να προσδιοριστεί με το IMSI, που εκπέμπεται πάνω στο ασύρματο δίκτυο πρόσβασης [3]. Αυτό μπορεί να οδηγήσει έναν κακόβουλο να προσποιηθεί ότι είναι ένα νέο SN στο οποίο ο

Ασφάλεια και διαχείριση κλειδιών στο UMTS

χρήστης πρέπει να αποκαλύψει η μόνιμη ταυτότητά του. Τα IMSI και TMSI διαβιβάζονται με την μορφή καθαρού κειμένου (clear-text), γεγονός που παραβιάζει την εμπιστευτικότητα της ταυτότητας και την μη ανίχνευση των χρηστών [8].

4 Το πατρικό δίκτυο (HLR/AuC) εμπιστεύεται το δίκτυο εξυπηρέτησης (VLR/SGSN), χωρίς να εξετάσει αν τα δεδομένα που το τελευταίο του αποστέλλει είναι έγκυρα ή όχι.

5 Το κλειδί ακεραιότητας εκπέμπεται προς τον κινητό σταθμό χωρίς κρυπτογράφηση και σε συνδυασμό με το ότι τα δεδομένα του χρήστη επιτρέπεται να κυκλοφορούν πάνω στο ασύρματο δίκτυο μη κρυπτοκαλυμμένα, η υποκλοπή του κλειδιού ακεραιότητας θα δημιουργήσει σοβαρά προβλήματα [25].

6 Επίσης το UMTS AKA είναι ευάλωτο σε επιθέσεις ψεύτικου σταθμού βάσης

α)Επίθεση αναδρομολόγησης [10]:

Υποθέστε ότι ένας κακόβουλος κατέχει μια συσκευή που μπορεί να εκτελεί τις λειτουργίες ενός σταθμού βάσεως. Μια τέτοια συσκευή καλείται ψεύτικος σταθμός βάσεως και είναι εμπορικά διαθέσιμος, π.χ. υποκλοπέας IMSI (IMSI Catcher). Επίσης υποθέστε ότι η συσκευή του κακόβουλου είναι σε θέση να μιμείται έναν κινητό σταθμό. Μέσω αυτής της συσκευής, ο κακόβουλος μπορεί να υποδυθεί έναν γνήσιο σταθμό βάσεως και να παρασύρει έναν νόμιμο κινητό σταθμό να επικοινωνήσει ασύρματα με τον ψεύτικο σταθμό βάσης. Ο κακόβουλος μπορεί επίσης να υποδυθεί έναν νόμιμο κινητό σταθμό και να εγκαθιδρύσει σύνδεση με έναν γνήσιο σταθμό βάσεως. Αυτή η εναλλαγή μεταξύ ενός ψεύτικου σταθμού βάσης και ενός ψεύτικου κινητού σταθμού επιτρέπει στον κακόβουλο να λειτουργήσει ως αναμεταδότης, (man in the middle), και να αναμεταδώσει τα μηνύματα μεταξύ ενός νόμιμου κινητού σταθμού και ενός γνήσιου σταθμού βάσης.

Τώρα, ας υποθέσουμε ότι ένας χρήστης βρίσκεται στην περιοχή του πατρικού του δικτύου και σκοπεύει να ξεκινήσει μια σύνοδο επικοινωνίας με το πατρικό δίκτυο. Αφού ο κακόβουλος υποκλέψει την προσπάθεια σύνδεσης του κινητού σταθμού, τον αναγκάζει να ξεκινήσει μία επικοινωνία με αυτόν αντί με το πατρικό δίκτυο. Μόλις ξεκινήσει να επικοινωνεί ο κινητός σταθμός με τον ψεύτικο σταθμό βάσεως, (είναι έξω από την δυνατότητα λήψης οποιουδήποτε σήματος που αποστέλλεται από οποιονδήποτε γνήσιο σταθμό βάσης του πατρικού δικτύου), μέσω του ψεύτικου κινητού σταθμού ο κα-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

κόβουλος στέλνει έπειτα ένα αίτημα σύνδεσης σε έναν ξένο δίκτυο εξ ονόματος του κινητού σταθμού του χρήστη. Έπειτα, ο κακόβουλος αναμεταδίδει πιστά τα μηνύματα μεταξύ του νόμιμου κινητού σταθμού και του ξένου δικτύου. Η αμοιβαία αυθεντικοποίηση του κινητού σταθμού και στο ξένου δικτύου θα είναι επιτυχής και η επικοινωνία θα προστατεύεται μέσω των καθιερωμένων κλειδιών. Με αυτό τον τρόπο ο κακόβουλος μπορεί να αναδρομολογήσει την κίνηση δεδομένων του χρήστη σε ένα άλλο δίκτυο. Αξίζει να σημειωθεί ότι η επίθεση αναδρομολόγησης έχει πρακτικές επιπτώσεις. Σύμφωνα με το [3], η κρυπτογράφηση των δεδομένων δεν είναι υποχρεωτική, ενώ η ακεραιότητα των μηνυμάτων του δικτύου είναι υποχρεωτική. Για να υποκλέψει την κυκλοφορία δεδομένων των χρηστών, ο κακόβουλος μπορεί να την αναδρομολογήσει σε ένα δίκτυο στο οποίο δεν υποστηρίζεται η κρυπτογράφηση των δεδομένων ή η κρυπτογράφηση είναι πολύ αδύνατη. Ωστόσο να υποστηριχτεί ότι ο κίνδυνος θα μπορούσε να μετριαστεί εάν όλα τα δίκτυα "εμπιστεύονται" το ένα το άλλο και χρησιμοποιούν όλα έναν συμφωνημένο ισχυρό αλγόριθμο κρυπτογράφησης. Η επίθεση αναδρομολόγησης θα μπορούσε να προκαλέσει το πρόβλημα επιπλέον χρέωσης στον χρήστη γιατί ενώ είναι στην εμβέλεια του πατρικού του δικτύου συνδέεται με ένα ξένο δίκτυο και χρεώνεται γι' αυτό.

β) Ενεργός επίθεση από αλλοιωμένα από κακόβουλους δίκτυα.

Στο UMTS AKA, τα διανύσματα αυθεντικοποίησης μεταφέρονται μεταξύ και διαμέσω δικτύων. Κάθε δίκτυο είναι κάτω από διαφορετική διαχείριση. Όταν ένα δίκτυο αλλοιώνεται, (εννοώντας ότι οι λειτουργίες του βρίσκονται υπό την επήρεια ενός ακόβουλου), ένας κακόβουλος θα μπορούσε να κάνει ένα αίτημα στοιχείων αυθεντικοποίησης χρησιμοποιώντας το αλλοιωμένο δίκτυο, για να λάβει τα διανύσματα αυθεντικοποίησης για οποιοδήποτε χρήστη, ανεξάρτητα της πραγματικής θέσης του χρήστη. Κατόπιν, ο κακόβουλος θα μπορούσε να χρησιμοποιήσει τα αποκτηθέντα διανύσματα αυθεντικοποίησης για να υποδυθεί άλλα δίκτυα (ψεύτικος σταθμός βάσης), ώστε να συνδεθούν σε αυτόν νόμιμοι χρήστες. Επιπλέον, με την πλημμύρα αιτημάτων αυθεντικοποίησης στο πατρικό δίκτυο, ο κακόβουλος θα μπορούσε να αναγκάσει τον μετρητή SQN_{HN} που διατηρεί το πατρικό δίκτυο για έναν συνδρομητή να πάρει υψηλή τιμή. Δεδομένου ότι η μέγιστη τιμή που μπορεί να πάρει είναι περιορισμένη, αυτό περιορίζει τη διάρκεια ζωής του κινητού σταθμού.



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Από τις αλλοιωμένες λειτουργίες ενός δίκτυου μπορεί να διακινδυνεύσει ολόκληρο το σύστημα, άρα είναι κρίσιμο τα μέτρα ασφάλειας να είναι σε ισχύ σε κάθε ενδιάμεσο δίκτυο. Αν και οι μηχανισμοί που παρέχουν ασφάλεια μεταξύ και μέσα στα δίκτυα αναπτύσσονται αυτήν την περίοδο, είναι απίθανο η ασφάλεια να εφαρμοστεί σε όλα τα δίκτυα συγχρόνως. Καταστάσεις όπου τα δίκτυα A και B έχουν κάνει συμφωνία ασφαλείας, αλλά το A και το Γ δεν έχουν, μπορεί να παραμείνει για πολύ ακόμη. Αυτό ενθαρρύνει ενεργητικές και παθητικές επιθέσεις στα μη προστατευμένα καλά δίκτυα.

7 Λειτουργική δυσκολία με τους αριθμούς ακολουθίας:

Στο UMTS AKA, απαιτείται το πατρικό δίκτυο να διατηρεί έναν μετρητή για κάθε συνδρομητή. Εάν προκληθεί κάποια καταστροφή στη βάση δεδομένων που αποθηκεύει τους μετρητές στο πατρικό δίκτυο, αυτό έχει επιπτώσεις σε όλους τους κινητούς σταθμούς που είναι εγγεγραμμένοι σε αυτό το δίκτυο. Σε μια τέτοια περίπτωση, το κόστος θα είναι τεράστιο για να επιτευχθεί επανασυγχρονισμός στους μετρητές που διατηρούνται για κάθε μεμονωμένο συνδρομητή. Επιπλέον, ακόμα κι αν δεν υπάρχει κανένα ελάπτωμα στη βάση δεδομένων, η κανονική λειτουργία του πρωτοκόλλου AKA θα μπορούσε να προκαλέσει αιτήματα επανασυγχρονισμού. Όπως αναλύθηκε πρωτύτερα, ένα αίτημα επανασυγχρονισμού ζητείται από τον κινητό σταθμό και όχι από το πατρικό δίκτυο. Όταν ένας αριθμός ακολουθίας θεωρείται ότι δεν είναι σωστή σειρά, ο κινητός σταθμός αποφασίζει ότι μία αποτυχία συγχρονισμού έχει εμφανιστεί στο πατρικό δίκτυο και αρχίζει συνεπώς ένα αίτημα επανασυγχρονισμού, καθώς το γεγονός ότι ένας αριθμός ακολουθίας δεν είναι στη σωστή σειρά, δεν σημαίνει απαραιτήτως μία αποτυχία στον μετρητή SQN_{Hn}. Μπορεί να προκληθεί από έναν κακόβουλο με την επανάληψη ενός ζευγαριού RAND και AUTN (που έχουν ήδη χρησιμοποιηθεί). Η χρήση των διανυσμάτων αυθεντικοποίησης εκτός σειράς στο δίκτυο εξυπηρέτησης θα μπορούσαν επίσης να προκαλέσουν την αποτυχία συγχρονισμού. Μια ομάδα διανυσμάτων αυθεντικοποίησης μπορεί να φθάσει στο δίκτυο εξυπηρέτησης εκτός σειράς, π.χ., η αρχική σειρά των διανυσμάτων αυθεντικοποίησης μπορεί να αλλάξει στο δρόμο από το πατρικό δίκτυο στο δίκτυο εξυπηρέτησης. Επιπλέον, η μετακίνηση των χρηστών μεταξύ διαφορετικών δικτύων (VLRs), τα οποία δεν ανταλλάσσουν πληροφορίες αυθεντικοποίησης θα μπορούσε να προκαλέσει αποτυχίες συγχρονισμού. Όταν ο χρήστης επιστρέφει σε ένα VLR που έχει

Ασφάλεια και διαχείριση κλειδιών στο UMTS

επισκεφθεί προηγουμένως, από ένα VLR που επισκέφθηκε τελευταία, οι διαδικασίες αυθεντικοποίηση και συμφωνίας κλειδιών (AKA) που βασίζονται σε διανύσματα αυθεντικοποίησης που δεν έχουν χρησιμοποιηθεί, μπορούν μέσα να προκαλέσουν τις αποτυχίες συγχρονισμού. Ο κινητός σταθμός, εντούτοις, δεν μπορεί να διακρίνει τον πραγματικό λόγο που ο αριθμός ακολουθίας δεν είναι στη σωστή σειρά. Ψεύτικοι επανασυγχρονισμοί δημιουργούν πρόσθετο σημαντικό κόστος στην σηματοδοσία μεταξύ του δικτύου εξυπηρέτησης και του πατρικού δικτύου.

Το πρωτόκολλο επίσης παρουσιάζει μία σειρά αδυναμιών απόδοσης:

8 Κατανάλωση εύρους ζώνης μεταξύ SN και HN: Όπως είδαμε στην ανάλυση του πρωτοκόλλου αυθεντικοποίησης, το SN πρέπει να γυρίσει πίσω στο HN για να υποβάλει ένα αίτημα για μια νέα σειρά διανυσμάτων αυθεντικοποίησης, όταν ο κινητός σταθμός παραμένοντας για αρκετό χρόνο σε ένα δίκτυο εξυπηρέτησης εξαντλεί τα προηγούμενα διανύσματα αυθεντικοποίησης, ή όταν συνδέεται για πρώτη φορά σε ένα δίκτυο. Έτσι υπάρχει κατανάλωση εύρους ζώνης εμφανίζεται μεταξύ SN και HN.

9 Καθυστέρηση αυθεντικοποίησης του κινητού σταθμού: Επίσης λόγω του ότι, το πατρικό δίκτυο ίσως απέχει πολύ από το δίκτυο εξυπηρέτησης, σε συνδυασμό με τα πιολλά μηνύματα που απαιτεί το πρωτόκολλο, ιδίως σε αποτυχία συγχρονισμού, μπορεί να προκαλέσει καθυστερήσεις, γεγονός που δεν είναι επιθυμητό, ιδιαίτερα στις εφαρμογές πραγματικού χρόνου ή όταν ο χρήστης δεν θέλει να διακόπτει μία ήδη παρεχόμενη υπηρεσία όταν αλλάζει δίκτυο.

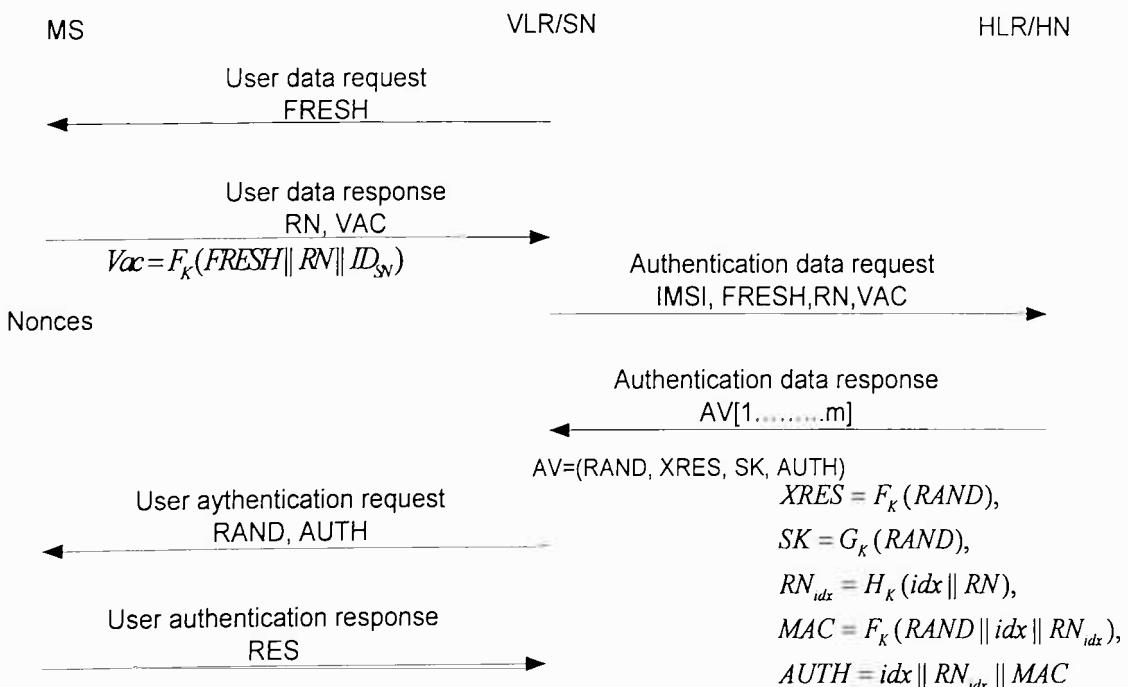
10 Χώρος αποθήκευσης στο SN: Μια σειρά η διανυσμάτων αυθεντικοποίησης για κάθε κινητό σταθμό πρέπει να αποθηκευτεί στο SN. Εάν υπάρχουν τα κινητοί σταθμοί στο δίκτυο εξυπηρέτησης, με τα διανύσματα ο καθένας πρέπει να αποθηκευτούν ταχινά διανύσματα αυθεντικοποίησης.

ΚΕΦΑΛΑΙΟ 7

7.1 Εναλλακτικές προτάσεις / Προτάσεις βελτίωσης του UMTS AKA

7.1.1 AP-AKA

Το AP- AKA [10] πρωτόκολλο διατηρεί το πλαίσιο του πρωτοκόλλου 3GPP AKA, αλλά αποβάλλει το συγχρονισμό, (αριθμούς ακολουθίας), μεταξύ κινητού σταθμού και του πατρικού δικτύου του. Στο AP- AKA, κάθε κινητός σταθμός και το πατρικό δίκτυο του μοιράζονται ένα κλειδί αυθεντικοποίησης K και τρεις κρυπτογραφικούς αλγόριθμους, F, G και H , όπου οι F και H είναι MAC (Message, Authentication Codes), ενώ ο G είναι μία συνάρτηση δημιουργίας κλειδιών. Το AP- AKA πρωτόκολλο καθορίζει μια ακολουθία έξι ροών. Κάθε ροή καθορίζει έναν τύπο μηνυμάτων, που παραλαμβάνεται από μια οντότητα. Ανάλογα με το περιβάλλον εκτέλεσης, οι οντότητες έχουν την ευελιξία να προσαρμόσουν, να επιλέξουν τις ροές που απαιτούνται. Από αυτή την άποψη καλούμε το AP- AKA προσαρμοστικό πρωτόκολλο (Adaptive Protocol (AP)). Ας δούμε το πρωτόκολλο λίγο πιο αναλυτικά (Σχήμα 7.1):



Σχήμα 7.1 Πρωτόκολλο AP-AKA

Ας υποθέσουμε ότι ένας κινητός σταθμός MS, κινείται σε ένα δίκτυο εξυπηρέτησης SN. Ανάλογα με το αν το δίκτυο έχει διανύσματα αυθεντικοποίησης ή όχι για τον κινητό σταθμό, το πρωτόκολλο λειτουργεί με δύο διαφορετικούς τρόπους.

1) Αν το SN δεν έχει διανύσματα αυθεντικοποίησης:

i. Το SN θα στείλει στον κινητό σταθμό έναν τυχαίο αριθμό FRESH ο οποίος περιέχεται σε ένα μήνυμα/αίτηση μαζί με την ταυτότητα του δικτύου.

ii. Λαμβάνοντας το μήνυμα/αίτηση ο κινητός σταθμός υπολογίζει το $Vac = F_K(FRESH \parallel RN \parallel ID_{SN})$ όπου το RN είναι ένας τυχαίος αριθμός και ID_{SN} είναι η ταυτότητα του δικτύου εξυπηρέτησης (ξένου δικτύου). Επίσης ο κινητός σταθμός υπολογίζει μία σειρά από αριθμούς μιας χρήσης (nonces) που θα τους χρησιμοποιήσει αργότερα για να κάνει μία γρήγορη αυθεντικοποίηση του πατρικού δικτύου. Υπολογίζει δηλαδή το $RN_r = H_K(r, RN)$, $r = 0, 1, \dots, m$ και τους αποθηκεύει.

iii. Ο κινητός σταθμός στέλνει στο δίκτυο εξυπηρέτησης τα RN και Vac .

iv. Το δίκτυο εξυπηρέτησης, SN, λαμβάνοντας το μήνυμα, στέλνει στο πατρικό δίκτυο ένα αίτημα αυθεντικοποίησης που περιέχει τα IMSI, FRESH, RN, VAC.

v. Με την παραλαβή του μηνύματος, το πατρικό δίκτυο, ανακτά το μυστικό κλειδί K του χρήστη και εξακριβώνει την ορθότητα του VAC. Αν ο έλεγχος είναι επιτυχημένος, δημιουργεί ένα σύνολο m διανυσμάτων AV[1,...,m] και τα στέλνει πίσω στο SN. Κάθε διάνυσμα αποτελείται από τα: (RAND, XRES, SK, AUTH), και χαρακτηρίζεται από έναν δείκτη idx, $1 \leq idx \leq m$. Ο δείκτης αυτός περιγράφει την θέση ενός διανύσματος αυθεντικοποίησης, σε αυτά που δημιούργησε το πατρικό δίκτυο για να αυθεντικοποιήσει τον κινητό σταθμό. Συγκεκριμένα: το πατρικό δίκτυο δεσμεύει έναν αριθμό $1 \leq idx \leq m$ και δημιουργεί έναν τυχαίο αριθμό RAND. Κατόπιν υπολογίζει το

$$XRES = F_K(RAND), SK = G_K(RAND), RN_{idx} = H_K(idx \parallel RN),$$

$$MAC = F_K(RAND \parallel idx \parallel RN_{idx}), AUTH = idx \parallel RN_{idx} \parallel MAC$$

vi. Το δίκτυο εξυπηρέτησης όταν λάβει τα διανύσματα, χρησιμοποιεί ένα από αυτά στέλνοντας το στον κινητό σταθμό και αποθηκεύει τα υπόλοιπα. Δηλαδή στέλνει τα RAND και AUTH στον κινητό σταθμό.

vii. Ο κινητός σταθμός εξακριβώνει την ορθότητα του MAC. Εξακριβώνει επίσης αν το RN_{idx} είναι ορθό υπολογίζοντας το: $RN_{idx} = H_K(idx \parallel RN)$, βλέποντας αν έ-



Ασφάλεια και διαχείριση κλειδιών στο UMTS

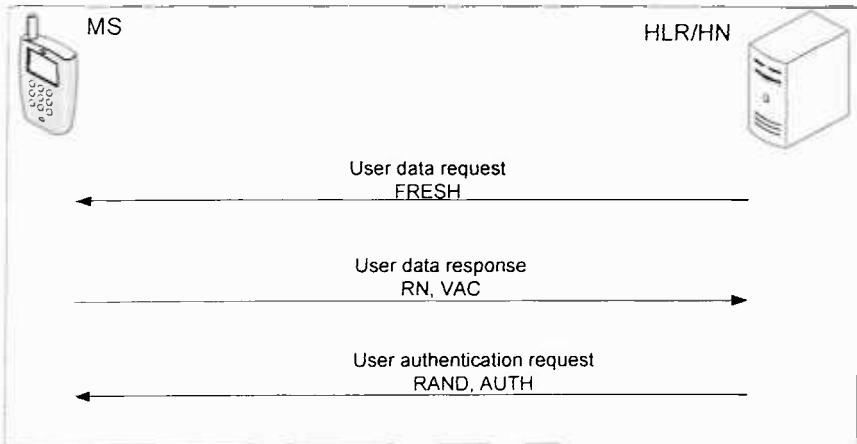
χει ξαναχρησιμοποιηθεί. Αν δεν έχει, υπολογίζει το $SK = G_k(RAND)$ και αν $idx > 0$, ανανεώνει την εσωτερική του κατάσταση και απαντά με το $RES = F_k(RAND)$. Αν $idx = 0$, ο κινητός σταθμός δεν στέλνει την απάντηση. Για την γρήγορη εξακρίβωση του RN_{idx} , ο κινητός σταθμός χρησιμοποιεί τα RN_r που έχει υπολογίσει στο βήμα 1 (ii). Κατόπιν διαγράφει το χρησιμοποιημένο RN_r από την λίστα.

2) Αν το SN έχει διανύσματα αυθεντικοποίησης για τον χρήστη: διαλέγει ένα που δεν έχει χρησιμοποιηθεί από τα αποθηκευμένα και ξεκινάει το πρωτόκολλο από το βήμα (vi).

Ας δούμε τώρα τι συμβαίνει όταν ο κινητός σταθμός βρίσκεται στα όρια του πατρικού δίκτυου.

1. Αν το HN (πατρικό δίκτυο) έχει διανύσματα αυθεντικοποίησης για τον χρήστη, τότε το πρωτόκολλο λειτουργεί κανονικά όπως περιγράψαμε παραπάνω δηλαδή διαλέγοντας ένα και στελνοντάς το στον κινητό σταθμό.

2. Αν το HN δεν έχει διανύσματα αυθεντικοποίησης για τον χρήστη, τότε το πρωτόκολλο λειτουργεί με 3 ροές όπως φαίνεται στο σχήμα 7.2.



Σχήμα 7.2 AP-AKA όταν ο χρήστης είναι στα όρια του πατρικού δίκτυου

Η διαφορά δηλαδή είναι στο ότι το HN, επιστρέφει μόνο RAND και AUTH και στους υπολογισμούς που κάνει βάζει $idx=0$.

Από τη λειτουργία του πρωτοκόλλου μπορούμε να δούμε ότι λειτουργεί προσαρμοζόμενο στο περιβάλλον, χρησιμοποιώντας έτσι περιστασιακά λιγότερο εύρος ζώνης για την ανταλλαγή μηνυμάτων. Είναι επίσης ανθεκτικό στις επιθέσεις αναδρομολόγησης και αλλοιωμένου δικτύου λόγω του ότι ανταλλάσσεται η ταυτότητα του δικτύου ε-

ξυπηρέτησης. Δεν υπάρχει ανάγκη συγχρονισμού αλλά υπάρχει αποστολή διανυσμάτων αυθεντικοποίησης από τα πατρικό δίκτυο στο δίκτυο εξυπηρέτησης όπως επίσης και ανάγκη αποθηκευσή τους.

7.1.2 UMTS X-AKA

Στο προτεινόμενο πρωτόκολλο X- AKA UMTS[13], ένας κινητός σταθμός μοιράζεται ένα μυστικό κλειδί K και ορισμένους κρυπτογραφικούς αλγόριθμους με το HN . Οι κοινοί κρυπτογραφικοί αλγόριθμοι μεταξύ των κινητών σταθμών και του HN περιλαμβάνουν (I) δύο συναρτήσεις κώδικα επικύρωσης μηνυμάτων (MAC), f^1 και f^2 και (II) τρείς συναρτήσεις δημιουργίας κλειδιών f^3 f^4 και f^x . Η συνάρτηση f^5 επίσης χρησιμοποιείται για την παραγωγή των προσωρινών κλειδιών. Εντούτοις, δεδομένου ότι η συνάρτηση f^5 παράγει μία σύνοψη 48 bits, το επίπεδο ασφάλειας της f^5 δεν είναι ικανοποιητικό να παραγάγει ένα ασφαλές κλειδί. Επομένως, χρησιμοποιείται μια άλλη βασική συνάρτηση παραγωγής κλειδιών f^x , η οποία μπορεί να παραγάγει μία 128 bits ή υψηλότερη σύνοψη, με αποτέλεσμα, να είναι σε θέση να φθάσει στο ικανοποιητικό επίπεδο ασφάλειας. Το πρωτόκολλο αποτελείται από 2 φάσεις:

1. Η πρώτη φάση:

i) Ο κινητός σταθμός δημιουργεί μία χρονοσφραγίδα t , υπολογίζει το $MAC_U = f_K^1(t)$, και τα αποστέλλει μαζί με το IMSI και μία αίτηση εγγραφής στο δίκτυο εξυπηρέτησης (SN).

ii) Το δίκτυο εξυπηρέτησης SN αναμεταδίδει τα στοιχεία στο HN (πατρικό δίκτυο).

iii) Το πατρικό δίκτυο HN ελέγχει καταρχάς την χρονοσφραγίδα t για να δεί αν βρίσκεται μέσα σε ένα επιτρεπτό παράθυρο και επαληθεύει το $MAC_U = f_K^1(t)$. Κατόπιν δημιουργεί έναν τυχαίο αριθμό RAND και υπολογίζει ένα προσωρινό κλειδί TK= $f_K^x(t)$ και το $MAC_H = f_K^1(RAND \parallel AMF)$.

iv) Αποστέλλει στο SN τα $AUTH = (MAC_H \parallel RAND \parallel AMF)$ και το TK.

v) To SN λαμβάνει και αποθηκεύει τα στοιχεία.

2. Η δεύτερη φάση:

vi) Εκτελώντας το πρωτόκολλο την ίστη φορά το δίκτυο εξυπηρέτησης SN δημιουργεί έναν τυχαίο αριθμό RAND και υπολογίζει το $MAC_S = f_{TK}^1(MAC_H \parallel RAND_S + j(RAND))$.

vii) Κατόπιν στέλνει το $AUTH_S = MAC_S \parallel RAND_S \parallel RAND \parallel AMF$ στον κινητό σταθμό.

viii) Μετά την παραλαβή του $AUTH_S$ ο κινητός σταθμός αυθεντικοποιεί τα HN και SN επαληθεύοντας την MAC_S κάνοντας τα παρακάτω βήματα:

α. Αν το j είναι μεγαλύτερο ή ίσο με αυτό που έχει ο κινητός σταθμός, θέτει το j ίσο με αυτό, διαφορετικά απορρίπτει την διαδικασία.

β. Υπολογίζει το $MAC_H^* = f_K^1(RAND \parallel AMF)$

γ. Βεβαιώνει την ισότητα: $MAC_S = f_{TK}^1(MAC_H \parallel RAND_S + j(RAND))$,

όπου j είναι η φορά που εκτελεί την διαδικασία. Αν αυτό ισχύει τότε τα HN και SN έχουν αυθεντικοποιηθεί σωστά. Κατόπιν υπολογίζει την τιμή $XSES = f_{TK}^2(RAND_S)$ και την αποστέλλει στο SN. Υπολογίζει επίσης τα κλειδιά κρυπτογράφησης $CK = f_{TK}^4(RAND_S)$ και ακεραιότητας $IK = f_{TK}^3(RAND_S)$.

ix. Το SN αυθεντικοποιεί τον κινητό σταθμό (MS). Λαμβάνοντας το XSES ελέγχει αν $XSES = RES = f_{TK}^1(RAND_S)$ και υπολογίζει με τη σειρά του τα CK και IK.

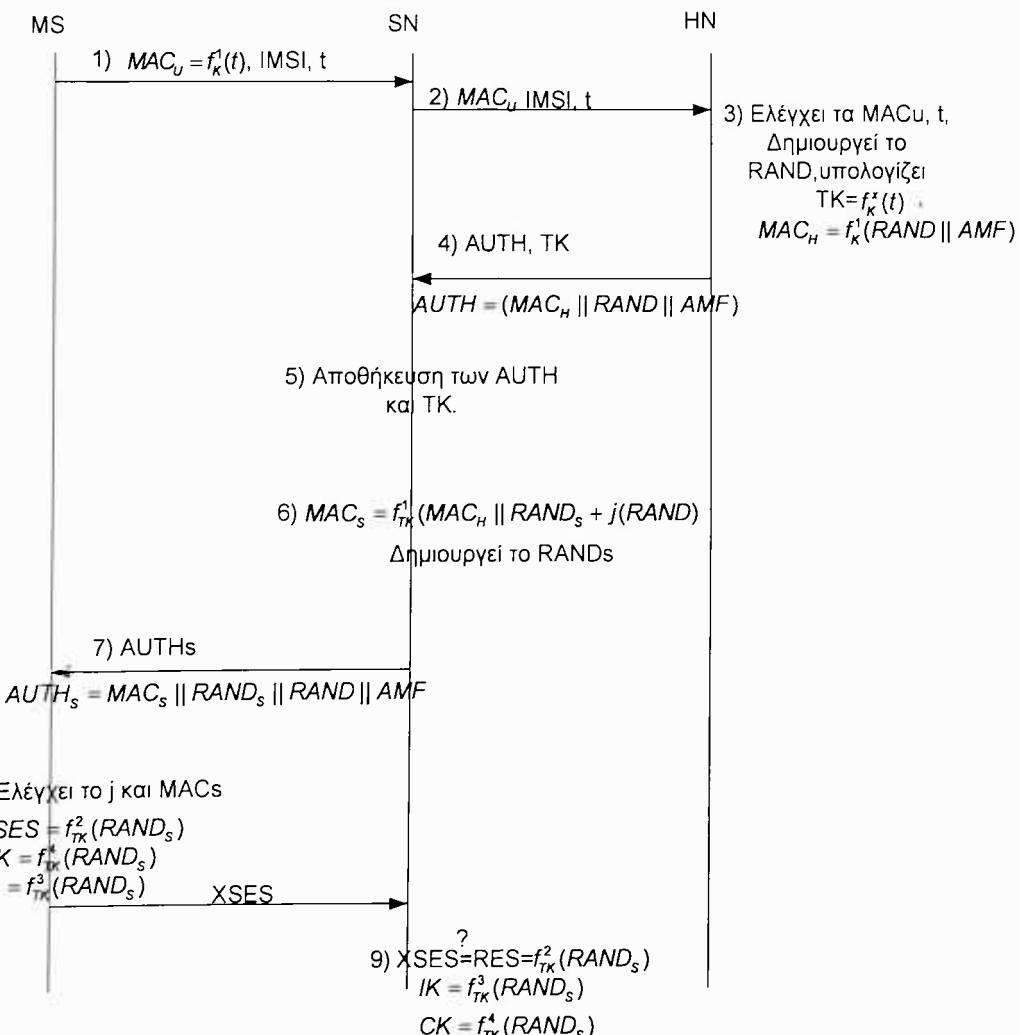
Τα παραπάνω φαίνονται στο Σχήμα 7.3.

Μπορούμε να δούμε ότι στο πρωτόκολλο UMTS AKA, το πατρικό δίκτυο HN δεν έχει κανέναν μηχανισμό για να αυθεντικοποιήσει τον κινητό σταθμό. Αντίθετα, στο πρωτόκολλο X- AKA UMTS έχει. Στο βήμα 3 του πρωτοκόλλου X- AKA UMTS, το HN επιβεβαιώνει την ταυτότητα των κινητών σταθμών με την επαλήθευση χρονοσφραγίδων,(timestamps), t και MAC. Σημειώστε ότι η επαλήθευση timestamp και MAC μπορεί να αντισταθεί σε επίθεση επανάληψης καθώς η χρονοσφραγίδα είναι μοναδική.

Το πρωτόκολλο δεν χρησιμοποιεί σειριακούς αριθμούς συγχρονισμού, (αποφεύγοντας έτσι το πρόβλημα που αναλύσαμε στο προηγούμενο κεφάλαιο), αλλά μηχανισμούς προσωρινού κλειδιού κι έτσι το SN μπορεί αμέσως να αυθεντικοποιήσει το MS μειώνοντας το πλήθος των μηνυμάτων που ανταλλάσσονται κυρίως σε περιπτώσεις

Ασφάλεια και διαχείριση κλειδιών στο UMTS

αποτυχίας συγχρονισμού κι έτσι την κατανάλωση του εύρους ζώνης. Στο πρωτόκολλο μεταφέρεται διάνυσμα αυθεντικοποίησης από το HN στο SN μόνο την πρώτη φορά καθώς μετά η αυθεντικοποίηση γίνεται από το SN με το προσωρινό κλειδί. Προσφέρει αμοιβαία αυθεντικοποίηση και ακεραιότητα μηνυμάτων σηματοδοσίας και εμπιστευτικότητα στην μετάδοση δεδομένων του χρήστη. Δεν προσφέρει μη αποποίηση (ουσιαστικά μόνο τα πρωτόκολλα που χρησιμοποιούν ψηφιακές υπογραφές το κάνουν), αλλά ούτε και ιδιωτικότητα της ταυτότητας του χρήστη καθώς το IMSI μεταφέρεται μη κρυπτοκαλλυμένο πάνω από το ασύρματο δίκτυο πρόσβασης, (πίνακας 7.2).



Σχήμα 7.3 Πρωτόκολλο X-AKA

7.1.3 Πρωτόκολλο Shu-Min Cheng et al.

Οι συγγραφείς [26] παρουσιάζουν ένα ασφαλές πρωτόκολλο αυθεντικοποίησης που ικανοποιεί τις απαιτήσεις ασφάλειας του 3GPP. Στο προτεινόμενο πρωτόκολλο, τα δίκτυα εξυπηρέτησης και τα πατρικά δίκτυα έχουν δημόσια/ιδιωτικά ζεύγη κλειδιών και χρησιμοποιούν ασύμμετρη κρυπτογραφία. Επιπρόσθετα, πρέπει να υπάρχει υποδομή δημόσιου κλειδιού έτσι ώστε τα δημόσια κλειδιά να μπορούν να διανεμηθούν σωστά και αποτελεσματικά. Αυτό επιτρέπει στα δίκτυα εξυπηρέτησης και τα πατρικά δίκτυα να αυθεντικοποιούν αμοιβαία ο ένας τον άλλον εύκολα. Ο χρόστης και το πατρικό δίκτυο μοιράζονται ένα μυστικό κλειδί. Στον παρακάτω πίνακα δίνονται επεξηγήσεις για τις συντομεύσεις που χρησιμοποιούνται στην περιγραφή του πρωτοκόλλου.

<i>IMUI</i>	International mobile user identity.
<i>TMUIs</i>	Temporary user identity generated by service provider (SP) ¹
<i>TMUIn</i>	Temporary user identity generated by network operator (NO) ²
<i>Knp, Kns</i>	Public/private key pair of network operator
<i>Ksp, Kiss</i>	Public/private key pair of service provider
<i>Kc</i>	Session key shared by the user and network operator
<i>Ku</i>	Secret key shared by the user and service provider
<i>N, Nk</i>	Nonce numbers
<i>CMn</i>	Candidate mechanisms
<i>T</i>	Subscribed Service Period

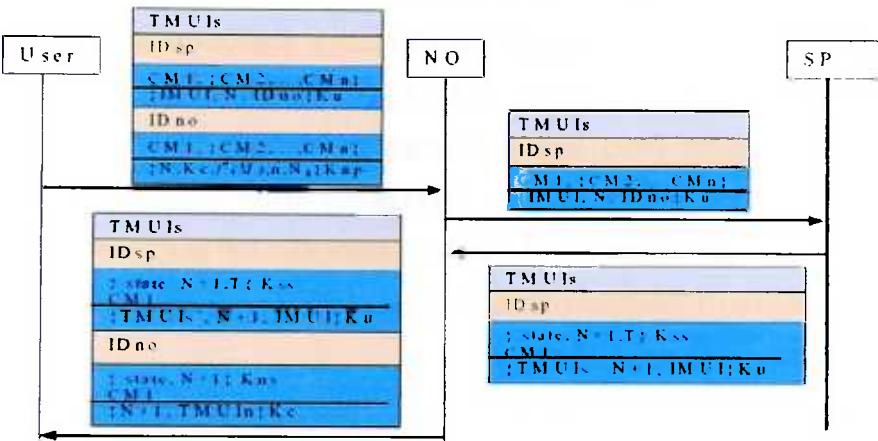
Πίνακας 7.1 Συντομεύσεις του πρωτοκόλλου Shu-Min Cheng et al [26]

Τα μηνύματα και η διαδικασία του πρωτοκόλλου φαίνονται στο Σχήμα 7.4 και αναλύεται παρακάτω.

¹ Εδώ με τον όρο service provider SP, εννοείται το πατρικό δίκτυο HN.

² Εδώ με τον όρο network operator NO, εννοείται το δίκτυο εξυπηρέτησης SN.

Ασφάλεια και διαχείριση κλειδιών στο UMTS



Σχήμα 7.4 Πρωτόκολλο Shu-Min Cheng et al [26]

1. Στο πρώτο βήμα ο κινητός σταθμός δημιουργεί το αίτημα, το οποίο περιέχει την προσωρινή ταυτότητα του χρήστη TMUI_s, την ταυτότητα του εξυπηρέτη αυθεντικοποίησης ID_{sp}, τους υποψήφιους μηχανισμούς αυθεντικοποίησης, {CM2.....CMn}, και το μήνυμα για την αυθεντικοποίηση του χρήστη. Ο μηχανισμός CM1 είναι ο προτεινόμενος από τον χρήστη. Ο χρήστης δημιουργεί μία προσωρινή τυχαία τιμή, (nonce), N και την τοποθετεί με το IMUI και την ταυτότητα του δικτύου εξυπηρέτησης, (ID_{no}), στο μήνυμα αυθεντικοποίησης SP. Το μήνυμα αυθεντικοποίησης κρυπτογραφείται με το κλειδί K_u δηλαδή {IMUI, N, IDno}K_u.

2. Ο χρήστης δημιουργεί το κλειδί συνόδου K_c. Κατόπιν στο μήνυμα αυθεντικοποίησης που θα αποσταλεί προς το δίκτυο εξυπηρέτησης NO, προσθέτει το {N, K_c, f'(M), n, N_kK_{np}}. Όπου f'(M), είναι μία μονόδρομη συνάρτηση σύνοψης, M είναι μία κρυφή πληροφορία που δημιουργείται από το χρήστη και το n αντιπροσωπεύει τον μεγαλύτερο αριθμό υπηρεσιών που ο χρήστης μπορεί να ζητήσει για να έχει πρόσβαση μετά την αυθεντικοποίηση. Το N_k χρησιμοποιείται για την δημιουργία ενός κλειδιού της συνόδου.

3. Ο χρήστης στέλνει τα παραπάνω στο δίκτυο εξυπηρέτησης (NO).
4. Αφού το NO λάβει το αίτημα προωθεί το μήνυμα αυθεντικοποίησης {IMUI, N, ID_{no}}K_u στο πατρικό δίκτυο (SP).
5. Με την παραλαβή του μηνύματος, αυτό αποφασίζει τον μηχανισμό που θα χρησιμοποιήσει για να αυθεντικοποίσει τον χρήστη. Αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το K_u, και από το TMUI_s βρίσκει την μόνιμη ταυτότητα του χρήστη

Ασφάλεια και διαχείριση κλειδιών στο UMTS

IMUI. Σαν αποτέλεσμα της διαδικασίας επαλήθευσης η κατάσταση για την αυθεντικοποίηση μπορεί να είναι αποδοχή, «accept», ή απόρριψη, «reject». Η κατάσταση αυτή κρυπτογραφείται μαζί με την τιμή (N+1) με το ιδιωτικό κλειδί του πατρικού δικτύου K_{SS} δηλαδή {state, N+1, T} K_{SS} . Κατόπιν το πατρικό δίκτυο, (SP), δημιουργεί μία νέα προσωρινή τιμή $TMUI_s$ για τον χρήστη και χρησιμοποιεί το K_{SS} για να το κρυπτογραφήσει μαζί με τα $TMUI_s$, (N+1) και IMUI δηλαδή { $TMUI_s$, (N+1), IMUI} K_{SS} .

6. Το πατρικό δίκτυο δημιουργεί ένα μήνυμα απάντησης το οποίο το αποστέλλει στο NO.

7. Όταν λάβει το μήνυμα αίτησης από το βήμα 4, το δίκτυο εξυπηρέτησης NO, αποκρυπτογραφεί το μήνυμα αυθεντικοποίησης που περιέχεται σε αυτό, χρησιμοποιώντας το προσωπικό του κλειδί K_{ns} για να εξάγει τα N, $f^N(M)$, n, N_k και K_c , τα οποία τα αποθηκεύει για τις μετέπειτα αυθεντικοποίήσεις και δημιουργία κλειδιών. Αν η κατάσταση αυθεντικοποίησης που του αποστέλλει το πατρικό δίκτυο δεν είναι «reject», και αν η τιμή (N+1) είναι ορθή το NO δημιουργεί ένα μήνυμα και το αποστέλλει στο χρήστη. Το μήνυμα αυθεντικοποίησης του NO κρυπτογραφείται χρησιμοποιώντας το κλειδί K_c και περιέχει τα N, $TMUI_N$ και την κατάσταση που είναι «accept». Επιπρόσθετα το δίκτυο κρατά το χρόνο για τον οποίο ισχύει η αυθεντικοποίηση.

8. Το NO αποστέλλει το μήνυμα που δημιούργησε μαζί με αυτό που παρέλαβε από το πατρικό δίκτυο στο χρήστη.

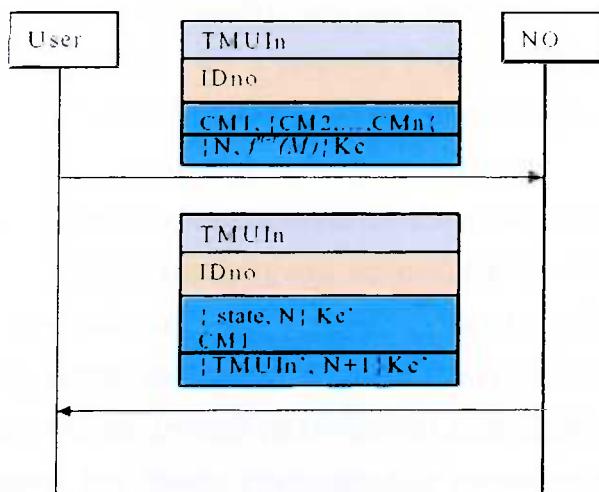
9. Αν οι καταστάσεις και των 2 μηνυμάτων που παρέλαβε ο χρήστης, (κινητός σταθμός), είναι «accept», τότε αυτός χρησιμοποιεί το K_u να αποκρυπτογραφήσει το { $TMUI_s$, N+1, IMUI} K_u που παράλαβε από το πατρικό δίκτυο και χρησιμοποιεί το K_c για να αποκρυπτογραφήσει το {N+1, $TMUI_n$ } K_c που παρέλαβε από το δίκτυο εξυπηρέτησης NO. Ο χρήστης τότε επαληθεύει την τιμή N+1. Αν είναι σωστή η αυθεντικοποίηση έχει επιτευχθεί, και ο χρήστης αποκτά 2 νέες προσωρινές ταυτότητες $TMUI_s$ και $TMUI_n$.

Στο πρωτόκολλο η αυθεντικοποίηση μεταξύ του χρήστη και του πατρικού δικτύου στηρίζεται στη χρήση ενός κοινού μυστικού κλειδιού K_u . Από το $TMUI_s$, το πατρικό δίκτυο μπορεί να βρει μυστικό βασικό K_u . Κατ' αυτό τον τρόπο, το πατρικό δίκτυο μπορεί να επικυρώσει το χρήστη, και ο χρήστης το πατρικό δίκτυο. Το μήνυμα αυθεντικοποίησης (authenticator) που στέλνεται στο δίκτυο εξυπηρέτησης, κρυπτογραφείται

Ασφάλεια και διαχείριση κλειδιών στο UMTS

χρησιμοποιώντας το δημόσιο κλειδί του δικτύου εξυπηρέτησης έτσι ώστε ο χρήστης μπορεί να αυθεντικοποιήσει το δίκτυο. Εντούτοις, το μήνυμα που στέλνεται από το χρήστη μπορεί να παραχθεί από άλλες κακόβουλες οντότητες, δηλαδή το δίκτυο εξυπηρέτησης δεν μπορεί να αυθεντικοποιήσει τον χρήστη βασιζόμενο μόνο στο αποτέλεσμα της αυθεντικοποίησης που θα του στείλει το πατρικό δίκτυο. Επομένως, το δίκτυο εξυπηρέτησης πρέπει να ελέγχει εάν η τιμή $(N + 1)$ είναι σωστή ή όχι. Έτσι το δίκτυο εξυπηρέτησης μπορεί να διακρίνει, ότι ο χρήστης είναι νόμιμος και ότι το αίτημα είναι νέο.

Μετά από την αρχική αυθεντικοποίηση, το δίκτυο εξυπηρέτησης (NO) κατέχει το μυστικό κλειδί K_c της συνόδου που μοιράζεται με το χρήστη και μπορεί στη συνέχεια να ολοκληρώσει με αυτό την αυθεντικοποίηση του χρήστη. Δηλαδή η επόμενη αυθεντικοποίηση συμβαίνει μεταξύ του χρήστη και του δικτύου εξυπηρέτησης χρησιμοποιώντας δύο ανταλλαγών μηνυμάτων όπως φαίνεται στο σχήμα 7.5.



Σχήμα 7.5 Ακόλουθη διαδικασία αυθεντικοποίησης

Όπως βλέπουμε η μετέπειτα της αρχικής διαδικασία αυθεντικοποίησης δηλαδή περιέχει μόνο δύο ανταλλαγές μηνυμάτων.

To nonce N που διαβιβάζεται μεταξύ του χρήστη και του δικτύου εξυπηρέτησης χρησιμοποιείται για να ανανεώσει του κλειδιού συνόδου. Κατ' αυτό τον τρόπο, το κλειδί κρυπτογράφησης που χρησιμοποιείται για κάθε σύνοδο είναι διαφορετικό. Εκτός από το πρώτο κλειδί συνόδου, η παραγωγή κλειδιών εκτελείται και από το δίκτυο εξυπηρέτησης.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Είναι σημαντικό να αναφερθεί ότι το πρωτόκολλο είναι ικανό να παρέχει από άκρο σε άκρο ασφάλεια επικοινωνίας καθώς οι χρήστες είναι δυνατόν να ανταλλάξουν ασφαλώς κλειδιά συνόδου όπως παρακάτω:

1. Υποθέστε ότι χρήστης 1 ξεκινά την κλήση. Κατόπιν, παράγει τυχαία ένα κλειδί κρυπτογράφησης K_e και στέλνει το $\{N, (K_e)K_{s1}, [(N)K_e]K_{p2}\}$ στον χρήστη 2, όπου τα N , K_{s1} , και K_{p2} είναι ο αριθμός nonce, το ιδιωτικό κλειδί του χρήστη 1 και το δημόσιο κλειδί του χρήστη 2, αντίστοιχα.

2. Ο χρήστης 2 αποκρυπτογραφεί αρχικά το μήνυμα και εξάγει το κλειδί κρυπτογράφησης K_e , με την αποκρυπτογράφηση του $((K_e)K_{s1})K_{p1}$ χρησιμοποιώντας το δημόσιο κλειδί του χρήστη 1. Αυτός έπειτα χρησιμοποιεί το K_e και το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το $[(N)K_e]K_{p2}$ και επιβεβαιώνει το αποτέλεσμα με το N .

3. Ο χρήστης 2 εκπέμπει το μήνυμα $(N + 1)K_e$ στον χρήστη 1. Όταν λάβει το μήνυμα ο χρήστης 1 το αποκρυπτογραφεί για να πάρει $N + 1$ και χρησιμοποιεί έπειτα το nonce N για να ελέγξει ότι οι πληροφορίες που του στάλθηκαν είναι σωστές. Εάν είναι σωστές, ο χρήστης 1 εξασφαλίζει ότι ο χρήστης 2 έχει παραλάβει σωστά το κλειδί κρυπτογράφησης K_e . Τώρα μπορεί να ξεκινήσει μία από άκρο σε άκρο ασφαλής επικοινωνία.

Το πρωτόκολλο παρέχει αμοιβαία αυθεντικοποίηση (δικτύου και χρήστη). Επειδή το μήνυμα που στέλνει ο κινητός σταθμός στο πατρικό δίκτυο κρυπτογραφείται χρησιμοποιώντας το κοινό μυστικό κλειδί K_u , κανένας εκτός από το πατρικό δίκτυο δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Επομένως, η αυθεντικοποίηση μεταξύ του χρήστη και του πατρικού δίκτυου μπορεί να επιτευχθεί χρησιμοποιώντας το K_u .

Το μήνυμα που στέλνεται στο δίκτυο εξυπηρέτησης κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί του δίκτυου, έτσι ο χρήστης βεβαιώνεται ότι μόνο το σωστό δίκτυο μπορεί να το αποκρυπτογραφήσει. Συγκρίνοντας τους δύο αριθμούς nonce που στέλνονται από το χρήστη και το πατρικό δίκτυο, το δίκτυο εξυπηρέτησης μπορεί να αυθεντικοποιήσει τον χρήστη.

Το πρωτόκολλο είναι ανθεκτικό σε επιθέσεις επανάληψης και αναδρομολόγησης καθώς χρησιμοποιούνται nonces και τα δεδομένα κρυπτογραφούνται από την αρχή.

Προσφέρει κρυπτογράφηση των δεδομένων και μάλιστα από άκρο σε άκρο. Δεν χρησιμοποιεί ακολουθιακούς αριθμούς συγχρονισμού αλλά nonces. Προσφέρει μη



αποτοποίηση μέσω την χρήση της μονόδρομης συνάρτησης f^{n-i} . Δεν επιβαρύνει με κίνηση το κανάλι καθώς δεν μεταφέρει διανύσματα αυθεντικοποίησης. Δεν απαιτεί χώρο αποθήκευσης για την αποθήκευση των διανυσμάτων αυθεντικοποίησης. Προσφέρει ανωνυμία στον χρήστη καθώς δημιουργεί μία προσωρινή ταυτότητα μετά την αυθεντικοποίησή του.

Από την άλλη μεριά, παρουσιάζει αρκετή πολυπλοκότητα, χρησιμοποιεί ασύμμετρη κρυπτογράφηση που απαιτεί συσκευή υψηλής υπολογιστικής ικανότητας, ενώ απαιτεί υποδομή δημοσίου κλειδιού για την λειτουργία του (πίνακας 7.2).

7.1.4 Πρωτόκολλο Harn-Hsin

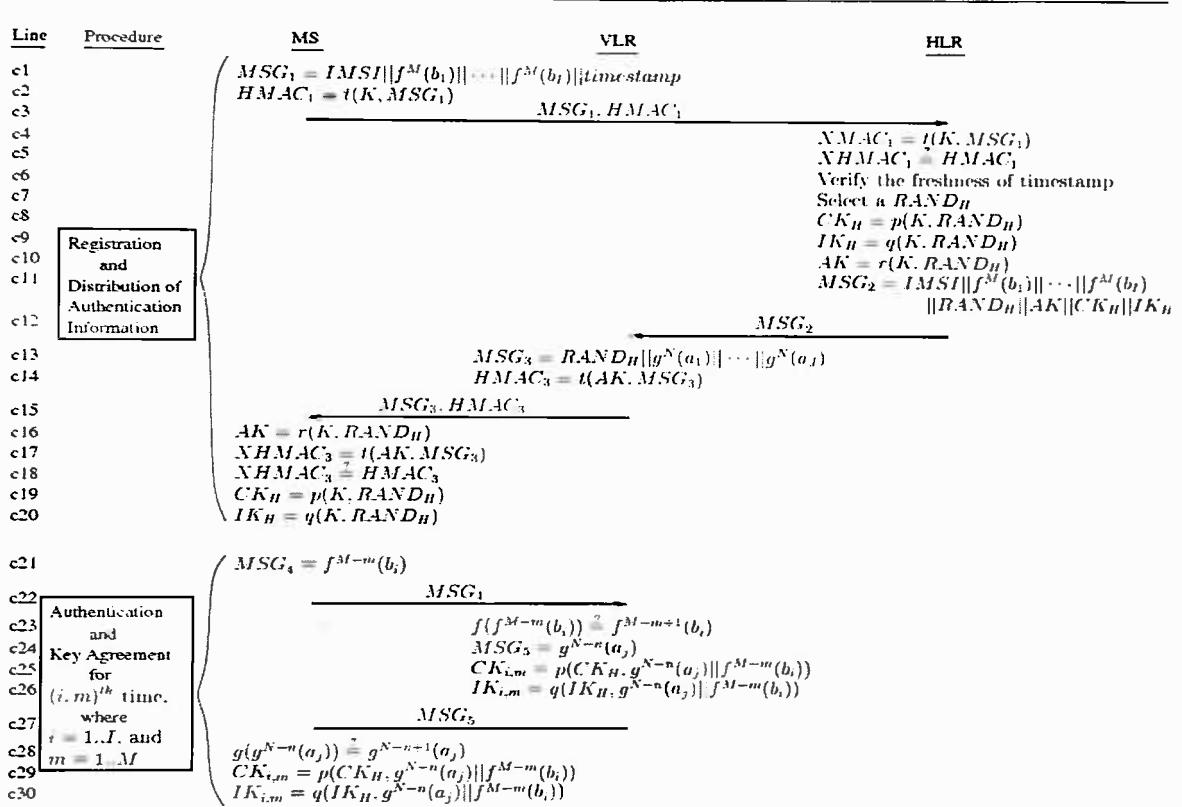
Οι Harn-Hsin [27] πρότειναν ένα σχέδιο AKA για το UMTS. Εισάγοντας hash-chaining, (αναλύεται στην παράγραφο 2.2.7) και τεχνικές HMAC, οι Harn-Hsin ισχυρίστηκαν ότι το προτεινόμενο πρωτόκολλο μπορεί να παρέχει ισχυρή περιοδική αμοιβαία αυθεντικοποίηση, ισχυρή συμφωνία κλειδιών, και υπηρεσία μη αποτοποίησης με έναν απλό και κομψό τρόπο. Το πρωτόκολλο χωρίζεται σε δύο φάσεις (σχήμα 7.6):

1) Φάση εγγραφής και διανομής πληροφοριών αυθεντικοποίησης. Ας υποθέσουμε ότι ένας κινητός σταθμός, (MS), βρίσκεται στην περιοχή ενός εξυπηρετούντος δικτύου. Ο MS πρέπει να στείλει στο HLR του ένα σύνολο στοιχείων δια μέσου του VLR. Συγκεκριμένα, τα MSG1 και HMAC1, (γραμμές c1 και c2), στέλνονται από τον κινητό σταθμό μέσω του VLR στο HLR.

Κατόπιν αφού το HLR ελέγξει την αυθεντικότητα του MSG1, δημιουργεί το MSG2 για να στείλει στο VLR. Για να ελέγξει ο κινητός σταθμός (MS) την αυθεντικότητα του VLR αργότερα στη φάση AKA, τα MSG3 και HMAC3 δημιουργούνται από το VLR.

2) Φάση αυθεντικοποίησης και συμφωνίας κλειδιών. Αυτή η διαδικασία χρησιμοποιείται από τον κινητό σταθμό και το VLR ώστε να αυθεντικοποιήσει αμοιβαία ο ένας τον άλλον (σχήμα 7.6).

Ασφάλεια και διαχείριση κλειδιών στο UMTS



Σχήμα 7.6 Πρωτόκολλο Harn-Hsin

Στο παραπάνω σχήμα χρησιμοποιούνται οι εξής έννοιες:

- $t(x,y)$: HMAC με κλειδί x και μήνυμα y ,
- $p(x,y)$: συνάρτηση δημιουργίας κλειδιών με κλειδί x και τυχαία δεδομένα y ,
- $r(x,y)$: συνάρτηση δημιουργίας κλειδιών ανωνυμίας με παραμέτρους το κλειδί x και τα τυχαία δεδομένα y ,
- AK : κλειδί ανωνυμίας,
- $RAND_H$: ένας τυχαίος αριθμός επιλεγμένος από το HLR,
- CK_H : το κλειδί κρυπτογράφησης που δημιουργείται από το HLR, χρησιμοποιώντας το $RAND_H$,
- IK_H : το κλειδί ακεραιότητας που δημιουργείται από το HLR και το MS χρησιμοποιώντας το $RAND_H$,
- $CK_{i,m}$: το κλειδί κρυπτογράφησης με ταυτότητα $id(i,m)$ που δημιουργείται από τα MS και VLR για χρήση ανάμεσά τους,

Ασφάλεια και διαχείριση κλειδιών στο UMTS

- $\text{IK}_{i,m}$: το κλειδί ακεραιότητας με ταυτότητα $\text{id}(i,m)$ που δημιουργείται από τα MS και VLR για χρήση ανάμεσά τους,
- $f^m(b_i)$: μία μονόδρομη συνάρτηση σύνοψης με τυχαίο πυρήνα b_i που αντιστοιχεί στη θέση i της αλυσίδας,
- M : το μήκος της αλυσίδας,
- I : ο μέγιστος αριθμός τυχαίων πυρήνων μιας αλυσίδας σύνοψης
- $g^n(a_j)$: μία μονόδρομη συνάρτηση σύνοψης με τυχαίο πυρήνα a_j που αντιστοιχεί στη θέση j της αλυσίδας,
- N : το μήκος της αλυσίδας g

Το πρωτόκολλο προσφέρει μη αποποίηση καθώς ο συνδυασμός της HMAC_1 στη γραμμή c2 και της τιμής $f^{M-m}(b_i)$ μπορεί να λειτουργήσει σαν απόδειξη μη αποποίησης από το VLR δηλαδή τη επισκέψεις στην $i^{\text{η}}$ αλυσίδα από τον κινητό σταθμό. Επίσης ο συνδυασμός HMAC_3 στην γραμμή c14 και η τιμή $g^{N-n}(a_j)$ μπορεί να λειτουργήσει σαν απόδειξη μη αποποίησης από τον κινητό σταθμό.

Προσφέρει επίσης αμοιβαία αυθεντικοποίηση, καθώς δημιουργούνται 2 αλυσίδες σύνοψης για τα MS και VLR. Αυτό αποτρέπει τους μη νόμιμους χρήστες να υπολογίσουν μία προηγούμενη τιμή της αλυσίδας χρησιμοποιώντας την δημόσια τιμή. Με αυτόν τον τρόπο αποφεύγεται η μεταφορά διανυσμάτων μεταξύ των VLRs.

Στο UMTS η περιοδική αυθεντικοποίηση γίνεται συγκρίνοντας έναν μετρητή αριθμών ακολουθίας μεταξύ των MS και VLR. Σε αυτό το πρωτόκολλο γίνεται με την χρήση των ιδιοτήτων των αλυσίδων σύνοψης όποτε απαιτείται. Δεν χρησιμοποιεί αριθμούς ακολουθίας, ενώ τα κλειδιά της συνόδου απαιτούν για την δημιουργία τους στοιχεία και των τριών οντοτήτων που εμπλέκονται στο πρωτόκολλο προσφέροντας μεγαλύτερη ασφάλεια.

Στα μειονεκτήματα του πρωτοκόλλου συγκαταλέγονται : α) το πρωτόκολλο θέτει σαν προαπαίτηση την αμοιβαία εμπιστοσύνη μεταξύ VLR και HLR. Επιπλέον θεωρεί ότι η επικοινωνία μεταξύ τους είναι ασφαλής, β) για να επαληθευτεί μία τιμή της αλυσίδας V_j , δεδομένης μίας τιμής V_i πρέπει να εκτελεστούν $j-i$ το πλήθος πράξεις. Επίσης απαιτείται αρκετό μεγάλο εύρος καναλιού προκειμένου να αποσταλούν αυτές οι τιμές, γ) επιτρέπει την μετάδοση της ταυτότητας του χρήστη πάνω από το ασύρματο κανάλι χωρίς προστασία (πίνακας 7.2).



7.1.5 Πρόταση Yi-Bing Lin et al.

Προκειμένου να λυθεί το πρόβλημα που αναφέρεται στο προηγούμενο κεφάλαιο και αφορά στο κόστος της μεταφοράς των διανυσμάτων αυθεντικοποίησης καθώς και της αποθηκευσής τους, οι Lin και Chen, [24], πρότειναν την υιοθέτηση ενός μηχανισμού ο οποίος υπολογίζει δυναμικά το πλήθος των διανυσμάτων αυθεντικοποίησης που χρειάζεται κάθε φορά να αποσταλούν από το HLR/AUC στο SGSN. Σκοπός είναι το ότι που αποτελεί το πλήθος των διανυσμάτων που στέλνονται από το HLR/AUC να είναι τέτοιο έτσι ώστε:

- 1 Να φτάνει για την αυθεντικοποίηση του χρήστη για όσο καιρό παραμείνει στην περιοχή που ελέγχει κάποιο SGSN, έτσι ώστε να περιορίζεται το κόστος μεταφοράς διανυσμάτων αυθεντικοποίησης από το πατρικό δίκτυο που αποτελεί ακριβή ενέργεια, καθώς αυτό μπορεί να βρίσκεται πολύ μακριά και
- 2 Να μην περισσεύουν διανύσματα όταν ο χρήστης αλλάζει SGSN που αποτελεί σπατάλη πόρων του δικτύου.

Για να επιτευχθεί αυτό οι συγγραφείς προτείνουν να συμπεριληφθεί ένας μηχανισμός στον κινητό σταθμό ή στο AUC ο οποίος θα επιλέγει αυτόμata το K βάση ενός μηνύματος που θα αποστέλλεται από τον κινητό σταθμό όταν αλλάζει SGSN αν ο μηχανισμός υλοποιείται σε αυτόν,(κινητό σταθμό), ή από το SGSN όταν ο μηχανισμός υλοποιείται στο AuC. Το K κατ' αρχήν τίθεται στο 5 όπως ορίζει το 3GPP TS 29.002 και κατόπιν υπολογίζεται λαμβάνοντας υπόψη την κινητικότητα του χρήστη στις κυψέλες και το πλήθος των προηγούμενων αιτήσεων αυθεντικοποίησης του χρήστη.

7.2 Σύγκριση μεταξύ AKA (Authentication and Key Agreement Protocols) για το UMTS

Στον παρακάτω πίνακα, γίνεται μία σύγκριση των πρωτοκόλλων της προηγούμενης παραγράφου. Ο πίνακας είναι αρκετά αναλυτικός και δεν χρειάζεται περαιτέρω ανάλυση, ενώ τα χαρακτηριστικά του κάθε πρωτοκόλλου που φαίνονται στον πίνακα, έχουν αναλυθεί στην προηγούμενη παράγραφο κατά την παρουσίαση των πρωτοκόλλων.

Σύγκριση μεταξύ AKA (Authentication and Key Agreement Protocols) για το UMTS					
	UMTS-AKA	Harn&Hsia	AP-AKA	UMTS X-AKA	Shu-Min Cheng et al
1	Ναι	Ναι	Ναι	Ναι	Ναι
2	Ναι	Ναι	Ναι	Ναι	Ναι
3	Ναι	Ναι	Ναι	Ναι	Ναι
4	Οχι	Οχι	Οχι	Ναι	Ναι
5	Οχι	Ναι	Οχι	Ναι	Ναι
6	Ναι	Οχι	Οχι	Οχι	Οχι
7	Ναι	Ναι	Ναι	Ναι	Οχι
8	Οχι	Οχι	Οχι	Οχι	Ναι
9	Οχι	Ναι	Ναι	Ναι	Ναι
10	Συμμετρική	Συμμετρική	Συμμετρική	Συμμετρική	Ασύμμετρη
1.	Αμοιβαία αυθεντικοποίηση				
2.	Εμπιστευτικότητα των δεδομένων του χρήστη				
3.	Ακεραιότητα μηνυμάτων σηματοδοσίας				
4.	Μείωση κατανάλωσης εύρους ζώνης μεταξύ Sn και HN				
5.	Μείωση χώρου αποθήκευσης στο SN				
6.	Ανάγκη συγχρονισμού μεταξύ MS και SN				
7.	Μεταφορά διανυσμάτων αυθεντικοποίησης μεταξύ MS και SN				
8.	Ιδιωτικότητα της ταυτότητας του χρήστη				
9.	Μη αποποιήση				
10.	Τύπος Κρυπτογράφησης				

Πίνακας 7.2 Σύγκριση προτεινόμενων πρωτοκόλλων για AKA στο UMTS

ΚΕΦΑΛΑΙΟ 8

Ασφάλεια στο κυρίως δίκτυο (Network Domain Security NDS).

Η ασφάλεια στην περιοχή του κυρίως δικτύου (Network domain security, NDS) στο UMTS, καλύπτει τις προδιαγραφές για ασφαλή επικοινωνία μεταξύ των στοιχείων του δικτύου. Ειδικότερα, ο κινητός σταθμός των χρηστών δεν επηρεάζεται καθόλου από την ασφάλεια στη περιοχή του κυρίως δικτύου. Τα δύο στοιχεία που επικοινωνούν μπορεί να είναι στο ίδιο δίκτυο, ή μπορεί να ανήκουν σε δύο διαφορετικά δίκτυα. Στην τελευταία περίπτωση, (δηλ., διαδικτυακή επικοινωνία), σαφώς απαιτούνται τυποποιημένες λύσεις γιατί ειδάλλως, κάθε ζευγάρι δικτύων θα πρέπει να συμφωνήσει χωριστά σχετικά με μια κοινή λύση. Επίσης με την τυποποίηση, το υλικό θα μπορεί να κατασκευάζεται από πολλούς διαφορετικούς προμηθευτές.

Μια αναγνωρισμένη αδυναμία ασφάλειας στα συστήματα 2G είναι η απουσία ασφάλειας στο κεντρικό δίκτυο. Αυτό στο παρελθόν δεν ήταν αντιληπτό σαν πρόβλημα, δεδομένου ότι τα 2G δίκτυα ανήκαν σε λίγους μεγάλους οργανισμούς που εμπιστευόντουσαν ο ένας τον άλλο. Αυτό δεν είναι ισχύει πλέον και έτσι τώρα υπάρχει μια ανάγκη για υιοθέτηση μηχανισμών ασφαλείας. Άλλος σημαντικός παράγοντας είναι, η εισαγωγή του IP ως επίπεδο δικτύου στο GPRS και αργότερα στο UMTS. Η εισαγωγή του IP επομένως δηλώνει, όχι μόνο μια μετατόπιση προς μετάδοση μεταγωγής πακέτου, η οποία είναι μια σημαντική αλλαγή, αλλά και μια μετατόπιση προς τα απολύτως ανοικτά και ευπρόσιτα πρωτόκολλα. Η επίπτωση από άποψη ασφάλειας είναι, ότι πρέπει να αντιμετωπιστεί ένα νέο σύνολο απειλών και κινδύνων.

Ένας σαφής στόχος λοιπόν για τα 3G συστήματα, είναι να είναι σε θέση να προστατεύσουν τα πρωτόκολλα σηματοδοσίας των κεντρικών δικτύων και αυτομάτως αυτό σημαίνει, ότι πρέπει να βρεθούν λύσεις ασφάλειας για πρωτόκολλα βασισμένα στα IP και SS7.

Το τμήμα του πρωτοκόλλου σηματοδοσίας SS7 που έχει να κάνει με τα κινητά δίκτυα καλείται Mobile Application Part (MAP). Προκειμένου να προστατευθεί όλη η επικοινωνία στο δίκτυο SS7 δεν είναι αρκετό να προστατευθεί μόνο το πρωτόκολλο MAP. Είναι όμως ουσιαστικό να προστατευθεί, καθώς τα κλειδιά της συνόδου που προστατεύουν τα δεδομένα κατά την μεταφορά τους στο ασύρματο δίκτυο πρόσβασης μετα

φέρονται μέσω του MAP [4]. Η προστασία γίνεται σε επίπεδο εφαρμογής εκτός αν το SS7 είναι πάνω από IP οπότε μπορεί να γίνει και σε επίπεδο δικτύου.

8.1 MAPsec (Ασφάλεια στο τμήμα μεταγωγής πακέτου CS)

Το σύνολο των μηχανισμών και βελτιώσεων που έχουν υιοθετηθεί για να προστατεύσουν το πρωτόκολλο MAP δημιουργούν την έννοια του Mapsec. Η βασική ιδέα πίσω από MAPsec μπορεί να περιγραφεί ως εξής. Ένα μήνυμα MAP καθαρού κειμένου κρυπτογραφείται και το αποτέλεσμα τοποθετείται μέσα σε ένα άλλο MAP. Συγχρόνως ένα κρυπτογραφημένο άθροισμα ελέγχου (checksum), (δηλ., MAC), που καλύπτει το αρχικό μήνυμα συμπεριλαμβάνεται στο νέο μήνυμα MAP.

Για να μπορούν να χρησιμοποιηθούν κρυπτογράφηση και MACs, απαιτούνται κλειδιά κρυπτογράφησης. Το MAPsec έχει δανειστεί την έννοια της συσχέτισης ασφάλειας, (Security Association, SA), από το IPsec. Η SA καθορίζει, ανάμεσα σε άλλα, τα κρυπτογραφικά κλειδιά, τους κρυπτογραφικούς αλγορίθμους, αλλά και άλλες σχετικές πληροφορίες. Οι συσχετίσεις ασφάλειας, (SAs), του MAPsec μοιάζουν με τις IPsec SAs, αλλά δεν είναι ίδιες.

8.1.1 Μορφή των μηνυμάτων MAPsec

Το MAPsec [4] έχει τρεις τύπους λειτουργίας, σε ανάλογα με τις υπηρεσίες ασφαλείας που προσφέρει:

- α. Καμία προστασία (Mode 0).
- β. Προστασία ακεραιότητας (Mode 1)
- γ. Κρυπτογράφηση και προστασία ακεραιότητας (Mode 2).

Τα μηνύματα MAP έχουν την παρακάτω δομή (σχήμα 8.1).

Security header	Protected payload
-----------------	-------------------

Σχήμα 8.1 Δομή μηνυμάτων MAP

Και στους 3 τύπους, η κεφαλίδα ασφαλείας (security header) εκπέμπεται σε καθαρό κείμενο, προκειμένου να επεξεργαστεί σωστά το μήνυμα η λαμβάνουσα πλευρά.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Το προστατευμένο αφέλιμο φορτίο, (Protected payload), περιέχει ουσιαστικά το αρχικό αφέλιμο φορτίο του μηνύματος MAP σε προστατευμένη μορφή. Στον τύπο 1, η MAC υπολογίζεται πάνω από την κεφαλίδα ασφάλειας και το αρχικό αφέλιμο φορτίο. Στον τύπο 2, η MAC υπολογίζεται πάνω από την κεφαλίδα ασφάλειας και το κρυπτογραφημένο αφέλιμο φορτίο. Το αποτέλεσμα του υπολογισμού επισυνάπτεται στο μήνυμα MAPsec.

Η κεφαλίδα ασφάλειας έχει την ακόλουθη μορφή (στον τύπο 0, μόνο τα δύο πρώτα στοιχεία χρησιμοποιούνται):

$$\text{Securityheader} = \text{SPI} \parallel \text{Original component ID} \parallel \text{TVP} \parallel \text{Ne-Id} \parallel \text{Prop}$$

Το SPI είναι ένας δείκτης παραμέτρων ασφάλειας που μαζί με την ταυτότητα του προορισμού, (PLMN), χαρακτηρίζει μοναδικά μία συσχέτιση ασφαλείας (MAPsec SA). Το Original component ID, αναφέρεται στον τύπο του αρχικού μηνύματος MAP, (απαιτείται να είναι σε καθαρό κείμενο για να γίνει επεξεργασία του MAP σωστά). Το TVP είναι μια μεταβλητή παράμετρος χρόνου που απαιτείται για να παρέχει προστασία ενάντια στις επιθέσεις επανάληψης. Το Ne-Id, προσδιορίζει το στοιχείο του αποστέλλοντας δικτύου και το Prop είναι ένας ιδιόκτητο, δηλαδή πεδίο που σχετίζεται με το συγκεκριμένο δίκτυο, προοριζόμενο για τοπική χρήση κατά τη δημιουργία του αρχικού διανύσματος IV. Το αρχικό διάνυσμα είναι $\text{IV}=\text{TVP} \parallel \text{NE-Id} \parallel \text{Prop} \parallel \text{PAD}$, όπου το PAD χρησιμοποιείται για να επεκτείνει το μήκος του IV στις 16 οκτάδες, που απαιτείται στους αλγορίθμους κρυπτογράφησης.

Το προστατευμένο αφέλιμο φορτίο σε ένα προστατευμένο μήνυμα MAP τύπου 2, έχει την παρακάτω μορφή: $f_6(\text{cleartext}) \parallel f_7(\text{Security Header} \parallel f_6(\text{Cleartext}))$, ενώ για MAP τύπου 1 έχει την μορφή: $\text{cleartext} \parallel f_7(\text{Security Header} \parallel \text{Cleartext})$.

Όπου f_6 είναι ο προηγμένος τυποποιημένος αλγόριθμος κρυπτογράφησης (AES) και f_7 είναι ο AES cipher Block chaining (CBC) σε MAC μορφή.

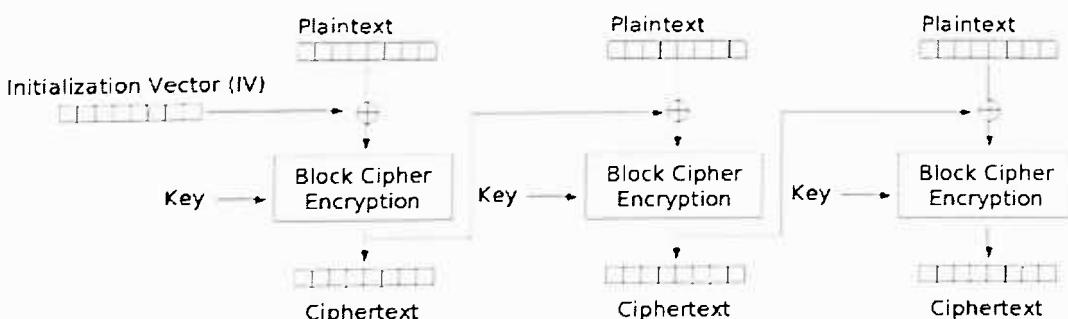
Το καθαρό κείμενο "cleartext", είναι το αρχικό αφέλιμο φορτίο των μηνυμάτων MAP σε καθαρό κείμενο. Η εμπιστευτικότητα επιτυγχάνεται κρυπτογραφώντας το καθαρό κεί-

μενο, “cleartext”, χρησιμοποιώντας τη συνάρτηση κρυπτογράφησης f6, με το κλειδί κρυπτογράφησης που καθορίζεται από την συσχέτιση ασφαλείας, (SA) και το διάνυσμα αρχικοποίησης. Η αυθεντικοποίηση του αποστολέα και η ακεραιότητα επιτυγχάνονται με την εφαρμογή της συνάρτησης αυθεντικοποίησης μηνυμάτων (MAC-M), συνάρτηση f7, με το κλειδί ακεραιότητας που καθορίζεται από την SA. Το μήκος MAC-M θα είναι 32 bits. Το μήκος του κρυπτοκειμένου είναι το ίδιο με το μήκος του καθαρού κειμένου.

8.1.2 Αλγόριθμοι του MAPsec

Το MAPsec επιτρέπει τη χρήση διάφορων αλγορίθμων κρυπτογράφησης, έτσι υπάρχει δυνατότητα αλλαγής αν διαπιστωθεί κάποια αδυναμία στον ήδη χρησιμοποιούμενο αλγόριθμο. Εντούτοις, μόνο ένας αλγόριθμος έχει καθορισθεί μέχρι και την έκδοση 6. Αυτός είναι ο MIA-1 (αλγόριθμος κρυπτογράφησης MAPsec) και είναι ισοδύναμος με τον AES σε counter mode με κλειδί κρυπτογράφησης μήκους 128 bits [4].

Για την προστασία ακεραιότητας, ένας αλγόριθμος έχει καθορισθεί μέχρι την έκδοση 6 και είναι ο MIA-1. Ο MIA-1 είναι AES cipher Block chaining (CBC) σε MAC λειτουργία με μήκος κλειδιού 128 bits. CBC-MAC, (Cipher Block Chaining-Message Authentication Code), (σχήμα 8.2), είναι μία μέθοδος ακεραιότητας μηνυμάτων που χρησιμοποιεί αλγορίθμους κρυπτογράφησης τμήματος (block ciphers) όπως DES και AES. Κάθε τμήμα καθαρού κειμένου (plaintext) κρυπτογραφείται και έπειτα λαμβάνει μέρος σε μία αποκλειστική διάζευξη, (XOR), με ένα δεύτερο κρυπτογραφημένο τμήμα. Το αποτέλεσμα λαμβάνει μέρος σε μία αποκλειστική διάζευξη, (XOR) με ένα τρίτο κρυπτογραφημένο τμήμα και συνεχίζεται.



Σχήμα 8.2 AES cipher Block chaining (CBC)

8.1.3. Συσχετίσεις ασφαλείας (Security associations SAs)

Όπως αναφέρθηκε, το MAPsec χρησιμοποιεί SAs οι οποίες δημιουργήθηκαν αρχικά για το IPsec. Εκτός από τα κλειδιά που απαιτούνται για τις κρυπτογραφικές διαδικασίες, μία SA περιέχει άλλες σχετικές πληροφορίες έτσι ώστε το κλειδιά να μπορεί να χρησιμοποιηθεί με το σωστό τρόπο.

Οι απαραίτητες MAPsec SAs μεταξύ των δικτύων συζητιούνται και συμφωνούνται μεταξύ των διαχειριστών των δικτύων. Η SA που συμφωνήθηκε ισχύει σε όλο το δίκτυο και σε κάθε στοιχείο του δικτύου που επικοινωνεί με το δίκτυο με το οποίο συμφωνήθηκε η SA. Ουσιαστικά δηλαδή οι SAs πρέπει να τοποθετηθούν στα διάφορα στοιχεία του δικτύου χειροκίνητα. Οι διαχειριστές των δικτύων πρέπει να συμφωνήσουν μεταξύ τους όσον αφορά τις SAs τα παρακάτω:

- πώς θα πραγματοποιηθεί η αρχική ανταλλαγή των MAPsec SAs
- πώς θα γίνεται η ανανέωση των MAPsec SAs
- πώς θα αποσύρονται οι MAPsec SAs (συμπεριλαμβανομένων των απαιτήσεων για το πόσο γρήγορα θα εκτελείται την απόσυρση)
- εάν η συμβατότητα με τον μη προστατευμένο τρόπο λειτουργίας πρόκειται να επιτραπεί
- σχετικά με τα μήκη των κλειδιών, τους αλγορίθμους, τους τρόπους λειτουργίας της προστασίας, χρόνοι λήξης των SAs, κ.λπ

Mία SA περιέχει:

- Την ταυτότητα του δικτύου προορισμού PLMN
- SPI
- Την ταυτότητα του δικτύου αποστολέα
- Κλειδί κρυπτογράφησης
- Αλγόριθμο κρυπτογράφησης
- Κλειδί ακεραιότητας
- Αλγόριθμο ακεραιότητας
- Ταυτότητα προφίλ προστασίας
- Ταυτότητα αναθεώρησης προφίλ προστασίας

- Μαλακό χρόνος λήξης
- Σκληρό χρόνο λήξης

Αφότου έχει επιτευχθεί ο μαλακός χρόνος λήξης, η SA δεν πρέπει χρησιμοποιείται για αποστολή εκτός αν είναι η μόνη έγκυρη SA διαθέσιμη. Με την επίτευξη του σκληρού χρόνου λήξης, η SA δεν μπορεί να χρησιμοποιηθεί καθόλου. Όλες οι SAs αποθηκεύονται σε μια βάση δεδομένων (Security association database, SAD) και όλα τα στοιχεία του δικτύου που χρησιμοποιούν MAPsec πρέπει να έχουν πρόσβαση σε αυτήν.

8.1.4 Προφίλ προστασίας

Στο MAPsec, για λόγους απόδοσης, προστατεύονται μόνο οι κρισιμότερες λειτουργίες (π.χ authentication data transfer και reset) του MAP. Επιπλέον, τα διαφορά στοιχεία που λαμβάνουν μέρος σε μία επικοινωνία MAP μπορούν να έχουν διαφορετικούς τύπους προστασίας. Αυτές οι ιδιότητες του MAPsec έχουν οδηγήσει στην δημιουργία μιας ιεραρχίας προστασίας καθώς και στην εισαγωγή κάποιων νέων εννοιών. Έτσι, έχουμε διαφορετικά επίπεδα προστασίας (Protection Levels), διαφορετικές ομάδες προστασίας (Protection Groups) κλπ, [4].

Επίσης έχουν οδηγήσει στην δημιουργία της έννοιας «προφίλ προστασίας» (protection profile). Κάθε «προφίλ προστασίας» καθορίζει την έκταση και τον τύπο προστασίας για κάθε προστατευόμενο μήνυμα MAP. Οι πολιτικές ασφάλειας που αφορούν στη διαχείριση κλειδιών του MAPsec καθορίζονται στις βάσεις δεδομένων ασφαλείας για τα στοιχεία του δικτύου (Network equipment security profile databases, (NEs SPD)). Οι καταχωρήσεις στις βάσεις δεδομένων καθορίζουν ποιες λειτουργίες του MAP προστατεύονται και ποιες MAP SAs θα χρησιμοποιηθούν για να προστατεύσουν τη σηματοδοσία MAP προς το δίκτυο με το οποίο επικοινωνεί το στοιχείο του δικτύου. Κάθε στοιχείο του δικτύου, (NE), πρέπει να έχει πρόσβαση σε μία SPD και μία SAD.

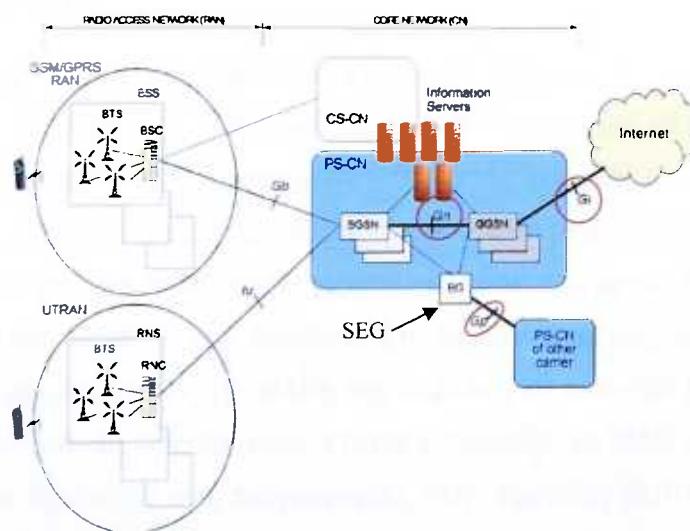
8.2 IPsec (Ασφάλεια στο τμήμα μεταγωγής πακέτων (PS))

Όπως έχει αναφερθεί και πρωτότερα, η ασφάλεια του UMTS στο κεντρικό δίκτυο (Network domain Security (NDS)), αφορά μόνο τη σηματοδοσία του δικτύου κα οχι τα δεδομένα του χρήστη. Η ασφάλεια του κυρίως δικτύου χωρίζεται σε επιμέρους περιο-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

χές ασφάλειας, οι οποίες συμπίπτουν με τα όρια των δικτύων που έχουν διαφορετικούς διαχειριστές.

Οι πύλες ασφάλειας, (Security gateways, SEGs), είναι οντότητες στα σύνορα των IP περιοχών ασφάλειας και χρησιμοποιούνται για την ασφάλεια των IP πρωτοκόλλων. Όλη η κίνηση από μία περιοχή ασφαλείας προς μία άλλη και κατ' επέκταση από ένα δίκτυο προς ένα άλλο περνά μέσα από τις SEGs. Η ασφάλεια δεν επεκτείνεται στην περιοχή των δεδομένων των χρηστών, (U-Plane), το οποίο σημαίνει ότι το πακέτο του χρήστη που κυκλοφορεί πάνω από την διασύνδεση Gi (προς άλλα εξωτερικά δίκτυα) δεν θα προστατευθεί από τις πύλες ασφαλείας SEGs. Αντίθετα, προστατεύονται τα δεδομένα πάνω από τις διασυνδέσεις Gp και Gn, σχήμα 8.3, για το πρωτόκολλο GTP-C. Μία περιοχή ασφαλείας μπορεί να έχει πολλές SEGs για διαφοροποίησης της κίνησης προς άλλα δίκτυα για λόγους κατανομής του φορτίου και αποφυγής της ύπαρξης μονού σημείου αποτυχίας.



Σχήμα 8.3 Προστατευμένες διεπαφές του UMTS

8.2.1 Λειτουργία του IPsec

Τα κύρια στοιχεία του IPsec είναι:

- Η κεφαλίδα αυθεντικοποίησης (Authentication Header (AH)).
- Το ασφαλές ωφέλιμο φορτίο (Encapsulation Security Payload (ESP)).
- Το πρωτόκολλο IKE (Internet key exchange protocol (IKE)).

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Όπως έχει ήδη αναφερθεί ο σκοπός του IPsec είναι να προστατευθούν τα πακέτα IP. Αυτό γίνεται με τη βοήθεια του ESP και/ή του AH. Το ESP παρέχει προστασία εμπιστευτικότητας και ακεραιότητας ενώ το AH μόνο ακεραιότητας. Στο UMTS χρησιμοποιείται μόνο το ESP.

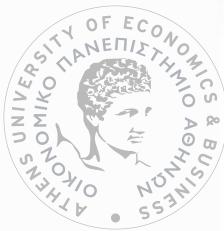
Και τα δύο, ESP και AH, έχουν για την λειτουργία τους ανάγκη από κλειδιά. Να λοιπόν γιατί οι SAs είναι ουσιώδεις για το IPsec. Εκτός από τα κλειδιά κρυπτογράφησης και αυθεντικοποίησης, μία SA περιέχει πληροφορίες για τον χρησιμοποιούμενο αλγόριθμο, τη διάρκεια ζωής των κλειδιών και την ίδια τη SA. Περιέχει επίσης έναν αριθμός ακολουθίας που προστατεύει από την επίθεση επανάληψης. Οι SAs πρέπει να δημιουργηθούν πριν από την χρήση των ESP ή AH. Μία SA απαιτείται για κάθε κατεύθυνση επικοινωνίας.

8.2.1.1. Η δομή του ESP

Υπάρχουν δύο είδη ESP: transport και tunnel. Οι λειτουργίες του transport είναι βασικά οι ακόλουθες. Σε ένα πακέτο IP, όλα εκτός από την κεφαλή IP κρυπτογραφούνται. Κατόπιν μια νέα κεφαλή ESP προστίθεται μεταξύ της κεφαλής IP και του κρυπτογραφημένου μέρους. Επίσης, η κρυπτογράφηση προσθέτει μερικά bits στο τέλος του πακέτου (padding). Τέλος, μία MAC υπολογίζεται πάνω σε όλα εκτός από την κεφαλίδα IP και επισυνάπτεται στο τέλος του πακέτου. Στο λαμβάνον μέρος, πρώτα ελέγχεται η ακεραιότητα. Αυτό γίνεται με την αφαίρεση της κεφαλής IP από την αρχή του πακέτου και της MAC από το τέλος του πακέτου, έπειτα υπολογίζει τη MAC, (χρησιμοποιείται ο αλγόριθμος που βρίσκεται στις πληροφορίες στην κεφαλή ESP), πάνω από το υπόλοιπο πακέτο και τέλος σύγκριση του αποτελέσματος με τη MAC του πακέτου. Εάν η έκβαση του ελέγχου ακεραιότητας είναι θετική, κατόπιν η κεφαλή ESP αφαιρείται και το υπόλοιπο αποκρυπτογραφείται (πάλι βασιζόμενοι στις πληροφορίες της κεφαλής ESP) (σχήμα 8.4).

Η μορφή tunnel διαφέρει από την transport με τον ακόλουθο τρόπο. Μια νέα κεφαλή IP προστίθεται στην αρχή του πακέτου. Κατόπιν οι ίδιες διαδικασίες όπως στη μορφή transport ισχύουν για το νέο πακέτο. Αυτό σημαίνει ότι προστατεύεται και η κεφαλίδα IP του αρχικού πακέτου (όπως διευκρινίζεται στο σχήμα 8.4).

Για την επικοινωνία των στοιχείων των δικτύων, (NEs), απαιτείται:

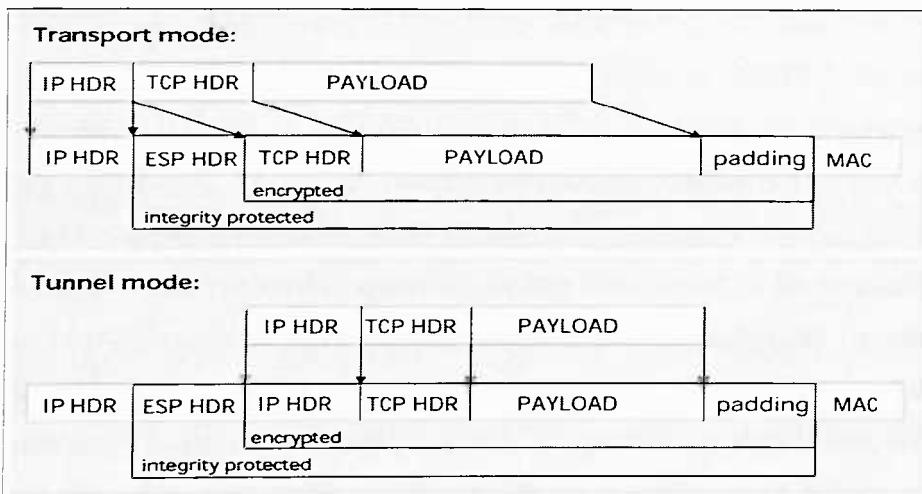


Ασφάλεια και διαχείριση κλειδιών στο UMTS

- να ξέρει τη διεύθυνση IP το ένα του άλλου
- να υποστηρίζουν και τα δύο IPsec.

Η χαρακτηριστική περίπτωση χρήσης του τύπου tunnel συσχετίζεται με την έννοια ενός εικονικού ιδιωτικού δικτύου (VPN). Το IPsec χρησιμοποιείται μεταξύ δύο ενδιαμέσων κόμβων (SEGs ή πύλες VPN), και παρέχεται προστασία από άκρο σε άκρο επειδή όλο το πακέτο είναι μέσα στο ωφέλιμο φορτίο του πακέτου που προστατεύεται μεταξύ των πυλών (gateways).

Η συνιστώμενη μέθοδος προστασίας της επικοινωνίας μεταξύ των SEGs για το UMTS όσον αφορά στα μηνύματα ελέγχου στο κεντρικό δίκτυο είναι να η χρηση ESP σε μορφή σήραγγας, (ESP tunnel mode). [6].



Σχήμα 8.4 Μηνύματα IPsec ESP

8.2.1.2 Συσχετίσεις ασφαλείας στο IPsec (IPsec SAs)

Όπως αναφέθηκε και στις προηγούμενες παραγράφους, για την ασφάλεια της επικοινωνίας στο κυρίως δίκτυο, (δίκτυο κορμού), στο UMTS, χρησιμοποιείται IPsec ESP τύπου σήραγγας, (tunnel) και απαιτούνται SAs. Μία SA, είναι η σχέση μεταξύ δύο SEGs που επιτρέπει την προστασία των δεδομένων που ανταλλάσσουν μεταξύ τους και που καθορίζει πώς αυτές, (οι SEGs), πρέπει να χρησιμοποιήσουν τις υπηρεσίες ασφάλειας για την επικοινωνία τους.

Οι SAs περιλαμβάνουν πληροφορίες για τους αλγορίθμους αυθεντικοποίησης ή/και κρυπτογράφησης, για τα κλειδιά κρυπτογράφησης και τα μήκη τους, καθώς επίσης και

Ασφάλεια και διαχείριση κλειδιών στο UMTS

τα διανύσματα έναρξης (IV) που μοιράζονται μεταξύ των οντοτήτων. Μία SA αφορά μία κατεύθυνση και άρα δύο SAs απαιτούνται για μια αμφίδρομη κυκλοφορία δεδομένων. Μία για την εισερχόμενη κυκλοφορία δεδομένων και μια για την εξερχόμενη κυκλοφορία. Τα πρωτόκολλα ασφάλειας χρησιμοποιούν τις συσχετίσεις ασφάλειας, (SAs), προκειμένου να παρέξουν τις υπηρεσίες ασφάλειας.

Στην αρχιτεκτονική ασφάλειας των περιοχών των κυρίως δικτύων στο UMTS η διαχείριση των SAs γίνεται μέσω του πρωτοκόλλου διαχείρισης συσχέτισης ασφαλείας και κλειδιού διαδικτύου, (Internet security association and key Management protocol) ISKMP, ενώ η διανομή των κλειδιών μεταξύ SEGs γίνεται μέσω του IKE (Internet key exchange).

Δηλαδή οι διαδικασίες για την αποκατάσταση και αποσύνδεση μιας SA ορίζονται από το πρωτόκολλο Διαχείρισης Συσχέτισης Ασφαλείας και Κλειδιού διαδικτύου, (Internet security association and key Management protocol, ISKMP). Κατόπιν γίνεται η ανταλλαγή των κλειδιών με ασφαλή τρόπο, με τη βοήθεια του πρωτοκόλλου IKE (Internet key exchange). Υπάρχουν διάφοροι τύποι IKE αλλά η βασική ιδέα είναι η ακόλουθη: τα επικοινωνούντα μέρη είναι ικανά να παραγάγουν κλειδιά και SAs, τα οποία χρησιμοποιούνται για να προστατεύσουν την επικοινωνία που ακολουθεί. Το IKE χρησιμοποιεί ασύμμετρη κρυπτογραφία όπου τα μυστικά κλειδιά για την ασφαλή επικοινωνία μπορούν να ανταλλαχθούν πάνω από ένα επισφαλές κανάλι. Εντούτοις, η αυθεντικοποίηση των μερών που τρέχουν IKE δεν μπορεί να γίνει χωρίς κάποια αρχικά κλειδιά. Αυτή η ανταλλαγή γίνεται είτε από πριν, ή εναλλακτικά, μέσω μιας υποδομής δημοσίου κλειδιού (PKI).

Οι IPsec SAs καθορίζονται μοναδικά από τις ακόλουθες παραμέτρους [6]:

- Ένας δείκτης παραμέτρου ασφάλειας (SPI).
- Μια διεύθυνση προορισμού IP.
- Ένα προσδιοριστικό πρωτοκόλλου ασφάλειας (που είναι πάντα το ESP πρωτόκολλο).

8.2.2 Τρόπος επικοινωνίας

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Για να εξασφαλιστεί την κυκλοφορία IP μεταξύ δύο NEs, εφαρμόζεται ένα σχήμα βήμα προς βήμα (hop by hop). Αυτό απαιτεί το NE που αποστέλλει δεδομένα να δημιουργήσει μια σήραγγα IPsec με το κατάλληλο SEG στην ίδια περιοχή ασφάλειας για να διαβιβάσει τα δεδομένα σε αυτό. Το SEG ολοκληρώνει αυτήν την σήραγγα και στέλνει τα δεδομένα μέσω μιας άλλης σήραγγας IPsec προς το λαμβάνον δίκτυο. Η δεύτερη σήραγγα ολοκληρώνεται από το SEG στην λαμβάνουσα περιοχή, η οποία χρησιμοποιεί στη συνέχεια IPsec για να περάσει τα στοιχεία στον τελικό προορισμό του (Σχέδιο 8.5).

Κάθε SEG έχει μία SAD και μία SPD. Η SPD είναι μία βάση δεδομένων πολιτικής ασφαλείας που αποφασίζει τι υπηρεσίες ασφαλείας προσφέρονται και σε ποια μορφή. Πριν την αποστολή δεδομένων προς άλλο δίκτυο, τα στοιχεία του δικτύου τη συμβουλεύονται, προκειμένου να καθοριστεί η ασφάλεια που θα πληρούν τα δεδομένα που αποστέλλονται. Άρα η SPD διαδραματίζει έναν κεντρικό ρόλο κατά την καθορισμό των πολιτικών ασφαλείας, τόσο εσωτερικά του δικτύου όσο και προς άλλα δίκτυα. Η πολιτική ασφαλείας προς άλλα δίκτυα υπόκειται στις συμφωνίες roaming. Η βάση δεδομένων συσχετίσεων ασφαλείας (SAD) περιέχει τις παραμέτρους που συνδέονται με τις ενεργές συσχετίσεις ασφαλείας.

Κάθε SA έχει μια εγγραφή στο SAD. Κατά την επεξεργασία των εξερχόμενων, δεδομένων μια εγγραφή στην SPD θα δείξει μια αντίστοιχη εγγραφή στην SAD. Εάν μια εγγραφή SPD δεν δείχνει σε μία SA που είναι κατάλληλη για τα δεδομένα, μία SA θα δημιουργηθεί αυτόματα.

Οι ακόλουθες διεπαφές καθορίζονται για την προστασία των IP πρωτοκόλλων:

- Διεπαφή Za (SEG-SEG):

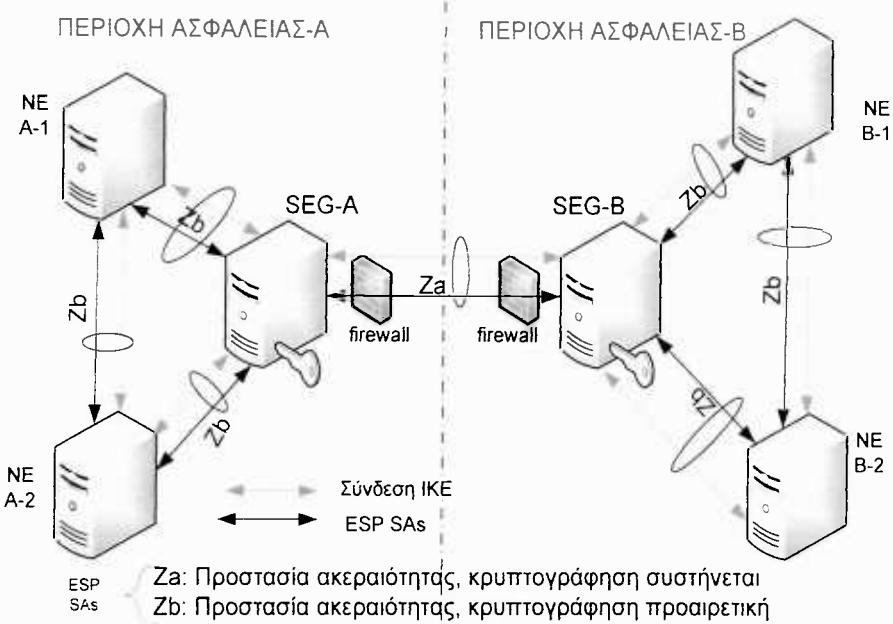
Η διεπαφή Za καλύπτει όλη την κυκλοφορία, (NDS/IP), μεταξύ των περιοχών ασφάλειας. Στην Διεπαφή Za, η προστασία αυθεντικοποίησης/ ακεραιότητας είναι υποχρεωτικές και η κρυπτογράφηση συστήνεται. Το ESP χρησιμοποιείται για την παροχή προστασίας αυθεντικοποίησης/ακεραιότητας και κρυπτογράφησης .Οι SEGs κάνουν χρήση του IKE για να διαπραγματευτούν, να καθιερώσουν και να διατηρήσουν μία σήραγγα ESP μεταξύ τους.

- Διεπαφή Zb (NE-SEG/ NE-SEG):

Η διεπαφή Zb καλύπτει την επικοινωνία μεταξύ SEGs και NEs αλλά και μεταξύ NEs μέσα στην ίδια περιοχή ασφάλειας. Η διεπαφή Zb είναι προαιρετική στην εφαρμο-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

γή της. Εάν εφαρμόζεται, θα εφαρμόσει ESP και IKE. Το ESP θα χρησιμοποιηθεί πάντα για την προστασία ακεραιότητας. Η χρήση της κρυπτογράφησης είναι προαιρετική. Οι SEGs μπορεί να έχουν και λειτουργίες firewall (σχήμα 8.5).



Σχήμα 8.5 Επικοινωνία στο NDS

8.2.3 Ασφάλεια στο IP κυρίως δίκτυο / Μηχανισμός Αυθεντικοποίησης (Network Domain Security Authentication Framework NDS/AF).

Ο φορέας προδιαγραφής του UMTS, δηλαδή το 3GPP, δημιούργησε μία προδιαγραφή για έναν γενικό μηχανισμό αυθεντικοποίησης (authentication framework) με σκοπό την υποστήριξη της ασφάλειας στο κυρίως δίκτυο. Η κρίσιμη έννοια εδώ είναι μία ειδικά προσαρμοσμένη υποδομή δημοσίου κλειδιού, PKI, που μπορεί να χρησιμοποιηθεί μεταξύ δικτύων (ή γενικότερα, μεταξύ των περιοχών ασφαλείας) έτσι ώστε, να μπορεί γίνει αυθεντικοποίηση.

8.2.3.1 Αρχιτεκτονική του Μηχανισμού Αυθεντικοποίησης (Network Domain Security Authentication Framework NDS/AF).

Παρακάτω θα παρουσιαστεί συνοπτικά και σε απλοποιημένη μορφή ο μηχανισμός αυτός [7].

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ο μηχανισμός περιλαμβάνει:

- SEG CA (Security Gateway Certificate Authority (Έμπιστη οντότητα πύλη ασφαλείας)): Διανέμει τα πιστοποιητικά των οντοτήτων στις SEGs μέσα σε μία ασφαλή περιοχή (ένα συγκεκριμένο δίκτυο).
- Interconnection CA: (Έμπιστη οντότητα Διασύνδεσης) Διανέμει τα πιστοποιητικά εξ ονόματος του διαχειριστή ενός δικτύου, (ασφαλούς περιοχής), στις SEG CAs άλλων περιοχών με τις οποίες τα SEGs του δικτύου έχουν διασύνδεση.

Κάθε περιοχή ασφάλειας έχει τουλάχιστον μία SEG CA και μία Interconnection CA. Η έμπιστη οντότητα πύλη ασφαλείας (SEG CA) της περιοχής διανέμει τα πιστοποιητικά στις πύλες (SEGs) της περιοχής οι οποίες διασυνδέονται με πύλες (SEGs) άλλων περιοχών (βλέπε σχήμα 8.6). Η έμπιστη οντότητα διασύνδεσης (Interconnection CA) μιας περιοχής, διανέμει τα πιστοποιητικά στα SEG CAs άλλων περιοχών με τις οποίες οι SEGs της συγκεκριμένης περιοχής στην οποία ανήκει η έμπιστη οντότητα διασύνδεσης (Interconnection CA) έχουν διασύνδεση.(Σχήμα 8.5). Γενικά, όλα τα πιστοποιητικά βασίζονται στην προδιαγραφή πιστοποιητικών Διαδικτύου X.509

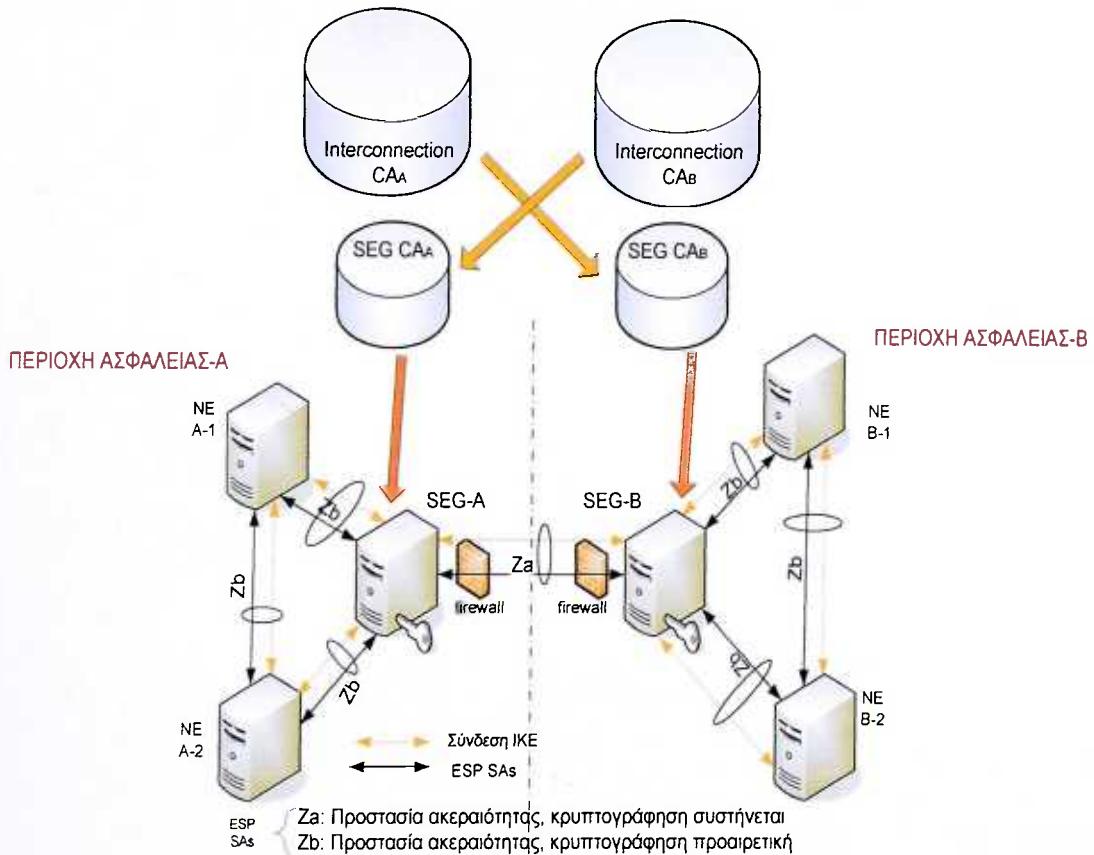
Η έμπιστη οντότητα πύλη ασφαλείας, (SEG CA), θα εκδώσει πιστοποιητικά για τις πύλες ασφαλείας, (SEGs), της συγκεκριμένης περιοχής που λαμβάνουν μέρος σε διεπαφή Za. Η αμοιβαία αυθεντικοποίηση ελέγχεται χρησιμοποιώντας τα πιστοποιητικά που οι SEG CAs εξέδωσαν για τις SEGs. Έτσι όταν η SEG της περιοχής ασφάλειας A εγκαθιστά μια ασφαλή σύνδεση με τη SEG της περιοχής B, θα είναι σε θέση να αυθεντικοποιήσει η μία την άλλη.

Όταν υπάρχει μια συμφωνία περιαγωγής μεταξύ των περιοχών, η έμπιστη οντότητα διασύνδεσης, (Interconnection CA), της μιας περιοχής πιστοποιεί τις SEG SA της άλλης περιοχής. Το πιστοποιητικό, το οποίο η έμπιστη οντότητα Διασύνδεσης, (Interconnection CA), της μιας περιοχής δημιουργεί για τις πύλες ασφαλείας, (SEG SA), της άλλης περιοχής πρέπει να εισαχθεί χειροκίνητα στη άλλη περιοχή.

Μετά από την αμοιβαία ανταλλαγή πιστοποιητικών μεταξύ των περιοχών, η SEG_A είναι σε θέση να επαληθεύσει το μονοπάτι: SEG_B → SEG CA_B → Interconnection CA_A. Δηλαδή οι οντότητες στην περιοχή A χρειάζεται να εμπιστεύονται μόνο την Το πιστοποιητικό της έμπιστης οντότητας Διασύνδεσης, Interconnection CA_A της ίδιας περιοχής. Ομοία για την περιοχή B.



Δηλαδή η Interconnection CA υπογράφει το δεύτερο πιστοποιητικό στο μονοπάτι. Παραδείγματος χάριν, στην περιοχή A, το πιστοποιητικό για τη SEG CA_B υπογράφεται από την Interconnection CA της περιοχής A όταν γίνεται η διαγώνια πιστοποίηση.



Σχήμα 8.6 Αρχιτεκτονική του μηχανισμού Αυθεντικοποίησης

8.3 Προβλήματα ασφαλείας στο κυρίως δίκτυο

Παρ' όλα αυτά δεν έχουν εξαλειφθεί τα προβλήματα ασφαλείας όσον αφορά στο κύριο δίκτυο.

α. Κατ' αρχάς τα δεδομένα του χρήστη δεν προστατεύονται και έτσι είναι εκτεθειμένα σε «πάσης φύσεως» επιθέσεις.

β. Αρχικά δεν είχε συμπεριληφθεί κάποιος μηχανισμός αυθεντικοποίησης για διαδικτυακή επικοινωνία με αποτέλεσμα κάποιες υλοποιήσεις δικτύων UMTS να ακολουθήσουν αυτή την προδιαγραφή, η οποία θέτει σε σοβαρούς κινδύνους την επικοινωνία μεταξύ δικτύων (ασφαλών περιοχών).

Ασφάλεια και διαχείριση κλειδιών στο UMTS

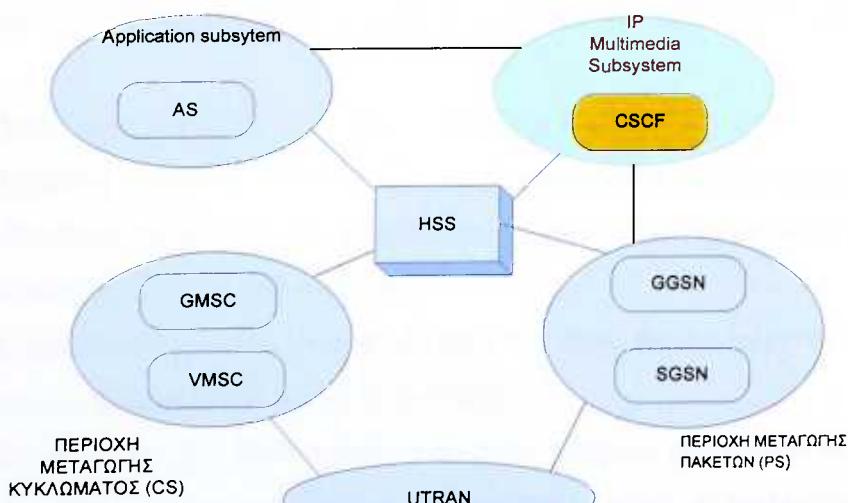
γ. Τόσο τα δεδομένα μέσα στο ίδιο κεντρικό δίκτυο (SGSN→GGSN), όσο και μεταξύ δικτύων γίνεται με IP πακέτα με αποτέλεσμα αυτά να υπόκεινται σε όλες τις γνωστές επιθέσεις.

ΚΕΦΑΛΑΙΟ 9

Ασφάλεια στο IMS (IP Multimedia CN Subsystem)

9.1 Αρχιτεκτονική του IMS

Η σχέση του IMS με τα τμήματα μεταγωγής κυκλώματος και πακέτου, CS και PS αντίστοιχα, του κυρίως δικτύου είναι αυτή που φαίνεται στο σχήμα 9.1. Το IMS είναι δηλαδή ένα υποσύστημα του κυρίως δικτύου (CN). Βρίσκεται ουσιαστικά πάνω από την PS περιοχή και έχει χαμηλή εξάρτηση από αυτή. Η πραγματική μεταφορά δεδομένων για τις υπηρεσίες που παρέχονται, γίνεται από τους υπάρχοντες μηχανισμούς IP του GPRS και του UMTS. Αυτό που κάνει το IMS, είναι να παρέχει διαχείριση συνόδου πολυμέσων χρησιμοποιώντας μηχανισμούς IP. Για να παρέχεται πλήρη λειτουργικότητα στις εφαρμογές, το IMS πρέπει να στηρίζεται στις υπηρεσίες που παρέχονται από έναν εξωτερικό εξυπηρέτη εφαρμογών (Application server (AS)). Το ίδιο το IMS παρέχει μόνο τις λειτουργίες δημιουργίας και ελέγχου συνόδου, λειτουργίες επεξεργασίας των μέσων καθώς και λειτουργίες διαλειτουργικότητας σηματοδοσίας [34]. Υποχρεώνει εντούτοις ότι όλα τα μέσα (media) πρέπει να μεταφέρονται με τη χρήση του *Real Time Protocol* (RTP) πανω από UDP/IP και επιπλέον. Πρέπει επίσης να τονισθεί ότι το IMS σχεδιάστηκε για χρήση αποκλειστικά με το IPv6.



Σχήμα 9.1 Το IMS σε ένα UMTS δίκτυο

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Η γενική αρχιτεκτονική του IMS περιγράφεται στο σχήμα 9.2. Οι σύνοδοι πολυμέσων οργανώνονται και ελέγχονται μέσω των διάφορων τύπων λειτουργιών ελέγχου συνόδων (Call Session Control Functions,(CSCF)):

Ο πληρεξούσιος λειτουργιών ελέγχου συνόδων, (Proxy CSCF (P- CSCF)), είναι το τοπικό σημείο επαφής του κινητού σταθμού UE με το δίκτυο που επισκέπτεται. Είναι ανάλογο με το SGSN στο UMTS. Εκτελεί τις λειτουργίες:

- Προωθεί την αίτηση καταχώρησης SIP που δέχεται από τον κινητό σταθμό, σε ένα I-CSCF.
- Προωθεί την αίτηση καταχώρησης SIP που δέχεται από τον κινητό σταθμό, σε έναν εξυπηρέτη SIP (δηλαδή στο S-CSCF).
- Προωθεί μηνύματα SIP στον κινητό σταθμό UE.
- Συμπιέζει- αποσυμπιέζει τα μηνύματα SIP.

Ο εξυπηρέτης λειτουργιών ελέγχου συνόδων, Serving CSCF (S-CSCF), ελέγχει τη σύνοδο στο πατρικό δίκτυο του χρήστη. Είναι ανάλογο με το GGSN στο UMTS. Ένα δίκτυο μπορεί να περιέχει πολλά S- CSCFs για την εξισορρόπηση της κίνησης.

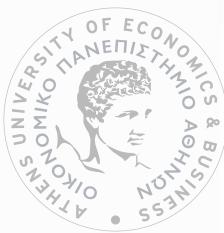
Εκτελεί τις λειτουργίες:

- Δέχεται αιτήσεις καταχώρησης και πληροφορεί τον πατρικό εξυπηρέτη εγγραφής/καταχώρησης (Home subscriber server, HSS).
- Εκτελεί έλεγχο της συνόδου.
- Αλληλεπιδρά με άλλες πλατφόρμες υπηρεσιών για παροχή διαφόρων υπηρεσιών.
- Διαβιβάζει μηνύματα SIP προς τα I-CSCF και P-CSCF

Ο Interrogating CSCF, (I-CSCF), βρίσκεται στο σημείο εισόδου ενός δικτύου, ώστε να κατευθυνθούν οι σύνοδοι στο κατάλληλο S-CSCF. Εκτελεί τις λειτουργίες:

- Ορίζει ένα S-CSCF σε έναν χρήστη.
- Οδηγεί μία αίτηση κλήσης που έλαβε από ένα άλλο δίκτυο προς το S-CSCF.
- Διαβιβάζει μηνύματα SIP προς το S-CSCF.

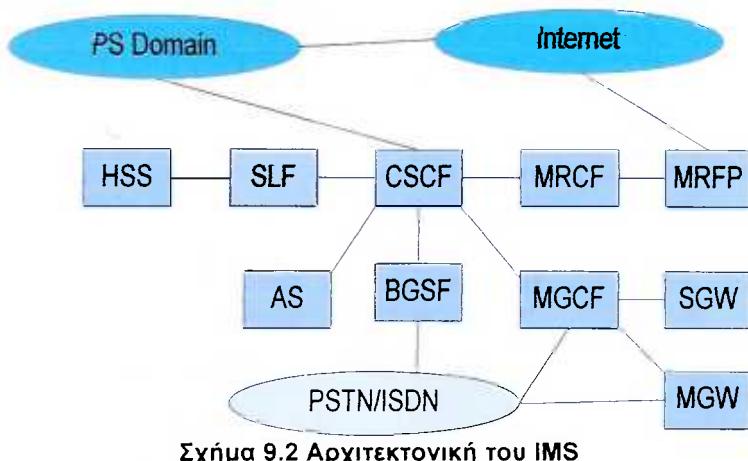
Τα P- CSCF και το S-CSCF στηρίζονται στον πατρικό εξυπηρέτη συνδρομητών, (HSS/HLR), για πληροφορίες σχετικές με τον χρήστη. Δίκτυα με πολλαπλά HSSs παρέχουν επίσης τη λειτουργία εύρεσης θέσης συνδρομητή Subscription Locator Function (SLF), εντοπίζοντας το HSS που διαχειρίζεται έναν δεδομένο χρήστη.



Ασφάλεια και διαχείριση κλειδιών στο UMTS

Ενώ το IMS δεν τυποποιεί καμία εφαρμογή, παρέχει τη λειτουργία επεξεργασίας πόρων των μέσων, Media Recourse Function Processor (MRFP). Αυτή είναι σε θέση να αναμίξει, να παραγάγει και να επεξεργαστεί ρεύματα μέσων, (media streams), υπό τον έλεγχο του Media Resource Function Controller (MRFC). Αυτές οι οντότητες μπορούν να χρησιμοποιηθούν από κοινού με έναν κατάλληλο εξυπηρέτη εφαρμογών (Application server, AS), για να υποστηρίξουν διάφορες εφαρμογές.

Το MRFP μπορεί επίσης να παρέχει τη διακωδικοποίηση, για να επιτρέψει στις εφαρμογές IMS να διαλειτουργήσουν με άλλες βασισμένες στο IP εφαρμογές που χρησιμοποιούν διαφορετικούς τύπους κωδικοποίησης.

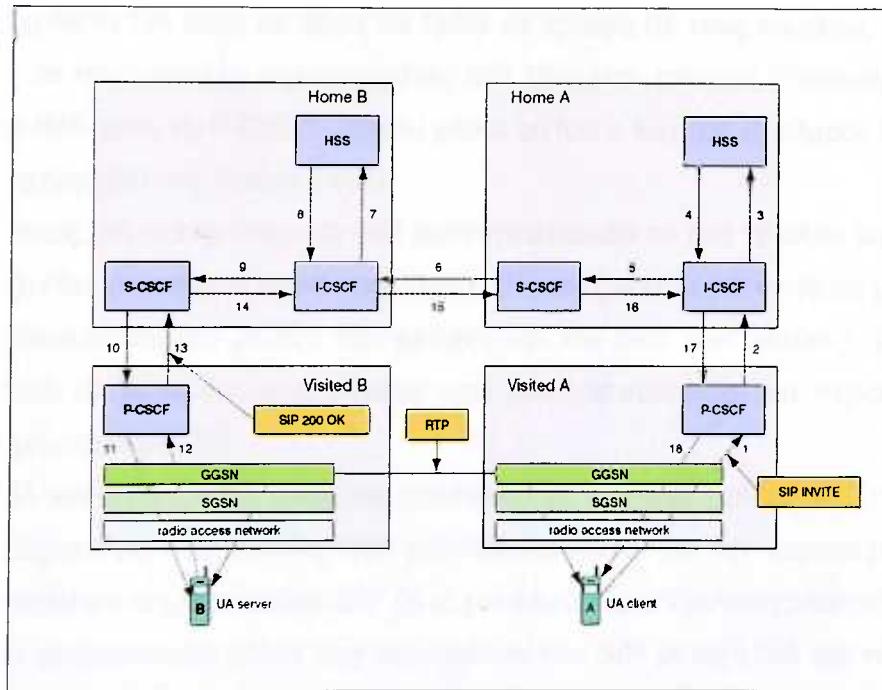


Το IMS παρέχει επίσης λειτουργίες πύλης, Media GateWay (MGW), για να επιτρέψει στις συνόδους IMS να διαλειτουργήσουν με περιοχές μεταγωγής κυκλώματος (CS). Το MGW διακωδικοποιεί απλά τις ροές δεδομένων σε κάποια μορφή που χρησιμοποιείται από κάποιο εξωτερικό δίκτυο. Αυτό ελέγχεται από την πύλη ελέγχου λειτουργίας πολυμέσων, Media Gateway Control Function (MGCF), που χειρίζεται και τη σηματοδοσία από ή προς ένα δίκτυο μεταγωγής κυκλώματος (CS). Για μερικούς τύπους CS δικτύων, το MGCF υποστηρίζεται από μία χωριστή πύλη σηματοδοσίας, Signaling GateWay (SGW). Τέλος, η πύλη ελέγχου λειτουργίας εξόδου, Breakout Gateway Control Function (BGC), καθορίζει που πρέπει να γίνει η αλλαγή, δηλ. σε ποιο σημείο μια εξερχόμενη σύνοδος πρέπει να βγει από το IMS και να εισαχθεί σε ένα CS δίκτυο.

Οι σύνοδοι δημιουργούνται με τη χρήση INVITE μηνυμάτων. Το σχήμα 9.3 περιγράφει ένα σενάριο όπου ένα μήνυμα INVITE στέλνεται από έναν τερματικό σταθμό σε

Ασφάλεια και διαχείριση κλειδιών στο UMTS

έναν άλλο, που και οι δύο ανήκουν σε κάποιο UMTS/IMS δίκτυο. Το μήνυμα INVITE από τον κινητό σταθμό (UE) A περνά αρχικά μέσω ενός P-PCSCF και έπειτα από ένα I-PCSCF. Το τελευταίο διαβιβάζει το μήνυμα στο πατρικό του δίκτυο (HSS), το οποίο κοιτάζει σε ποιο S-CSCF ο χρήστης είναι καταχωρημένος. Μία παρόμοια διαδικασία γίνεται στο δίκτυο B και το INVITE τελικά ολοκληρώνεται στον κινητό σταθμό (UE) B. Η συνομιλία μπορεί τώρα να αρχίσει, με τη χρησιμοποίηση του πρωτοκόλλου μεταφοράς σε πραγματικό χρόνο RTP.



Σχήμα 9.3 Δημιουργία συνόδου (INVITE)

9.2 Αρχιτεκτονική ασφαλείας του IMS

Όπως αναφέρθηκε, το IMS βρίσκεται ουσιαστικά πάνω από την περιοχή μεταγωγής πακέτου PS και έχει χαμηλή εξάρτηση από αυτή. Προκειμένου να χορηγηθεί σε ένα κινητό σταθμό η πρόσβαση σε υπηρεσίες πολυμέσων του δικτύου εξυπηρέτησης απαιτείται η ύπαρξη συσχέτισης ασφαλείας (SA) μεταξύ του κινητού σταθμού και του IMS το δικτύου εξυπηρέτησης. Τα κλειδιά και οι λειτουργίες αυθεντικοποίησης στο IMS από την πλευρά χρηστών αποθηκεύονται σε ένα ISIM (IM Subscriber Identity Module). Είναι δυνατό κλειδιά και λειτουργίες αυθεντικοποίησης για το IMS να είναι λογικά ανε-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

ξάρτητα από κλειδιά και λειτουργίες που χρησιμοποιούνται για την αυθεντικοποίηση στην περιοχή PS. Εντούτοις, αυτό δεν αποκλείει την χρήση κοινών κλειδιών.

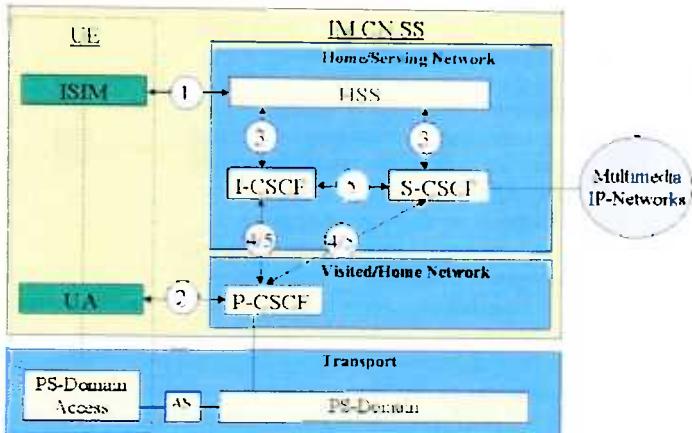
Όταν ένας πράκτορας χρήστη (User Agent, UA) θέλει να έχει πρόσβαση στο IMS, δημιουργεί αρχικά ένα πλαίσιο PDP (Packet Data Protocol) με την περιοχή PS. Σε αυτήν την διαδικασία, η ασφάλεια παρέχεται όπως έχουμε αναπτύξει έως τώρα. Αμοιβαία αυθεντικοποίηση μεταξύ του κινητού σταθμού UE και της περιοχής PS, προστασία ακεραιότητας και κρυπτογράφηση μεταξύ του UE και του RNC. Μέσω του GGSN ο πράκτορας χρήστη UA είναι σε θέση να έρθει σε επαφή με τους κόμβους IMS χρησιμοποιώντας το πρωτόκολλο σηματοδοσίας SIP (Session Internet Protocol). Η πρώτη επαφή με το IMS είναι το P-CSCF. Μέσω μέσω αυτού ο κινητός σταθμοός UA είναι σε θέση να καταχωρηθεί στο πατρικό IMS.

Συγχρόνως UA και το πατρικό IMS αυθεντικοποιούν το ένα το άλλο και γι'αυτό το λόγο μοιράζονται μία μόνιμη κοινή ταυτότητα. (Προσέξτε ότι εδώ υπάρχει μία δεύτερη αμοιβαία αυθεντικοποίηση μεταξύ του χρήστη και του IMS του δικτύου). Συμφωνούν επίσης σχετικά με τα προσωρινά κλειδιά που χρησιμοποιούνται για περαιτέρω προστασία των μηνυμάτων SIP.

Έπειτα, ο UA και το P-CSCF διαπραγματεύονται με ασφαλή τρόπο όλες τις παραμέτρους των μηχανισμών ασφάλειας που χρησιμοποιούνται για την περαιτέρω προστασία των μηνυμάτων σηματοδοσίας SIP (π.χ., οι αλγόριθμοι κρυπτογράφησης). Τέλος, η προστασία ακεραιότητας όλων των μηνυμάτων του SIP μεταξύ UA και του P-CSCF αρχίζει, βασισμένη στα προσωρινά κλειδιά που συμφωνήθηκαν κατά τη διάρκεια της φάσης αυθεντικοποίησης.

Τα μηνύματα SIP μεταξύ του IMS του δικτύου εξυπηρέτησης και του IMS του πατρικού δικτύου προστατεύονται από τους μηχανισμούς ασφάλειας περιοχής κυρίου δικτύου που αναλύσαμε στο προηγούμενο κεφάλαιο. Άρα λοιπόν η ασφάλεια στο IMS έγκειται στο πρώτο βήμα ,(hop), μεταξύ UA και P-CSCF καθώς μετά οι μηχανισμοί ασφαλείας είναι αυτοί του κυρίως δικτύου.

Η αρχιτεκτονική ασφάλειας του IMS παρουσιάζεται σε μία γενική μορφή στο σχήμα 9.4. [5].



Σχήμα 9.4 Αρχιτεκτονική ασφαλείας IMS

Υπάρχουν πέντε διαφορετικές συσχετίσεις ασφαλείας, προκειμένου να καλύψουν διαφορετικές ανάγκες ασφαλείας του IMS, που φαίνονται στο σχήμα 9.4.

Η 1 παρέχει αμοιβαία αυθεντικοποίηση. Το HSS εξουσιοδοτεί το S- CSCF για την αυθεντικοποίηση των συνδρομητών. Εντούτοις το HSS είναι αρμόδιο για την παραγωγή των κλειδιών. Το μόνιμο κλειδί το οποίο μοιράζονται το ISIM και το HSS συνδέεται με το IMPI (IP Multimedia Private Identity). Ο συνδρομητής θα έχει μια ιδιωτική ταυτότητα, (εσωτερικά του δικτύου), χρήστη την IMPI και τουλάχιστο μια εξωτερική δημόσια ταυτότητα χρήστη (IMPU, IP Multimedia Public Identity).

Η 2 παρέχει μια ασφαλή σύνδεση μεταξύ του UE και του P-CSCF. Παρέχεται αυθεντικοποίηση προέλευσης στοιχείων δηλ. επιβεβαίωση ότι η πηγή των λαμβανόμενων στοιχείων είναι αυτή που ισχυρίζεται.

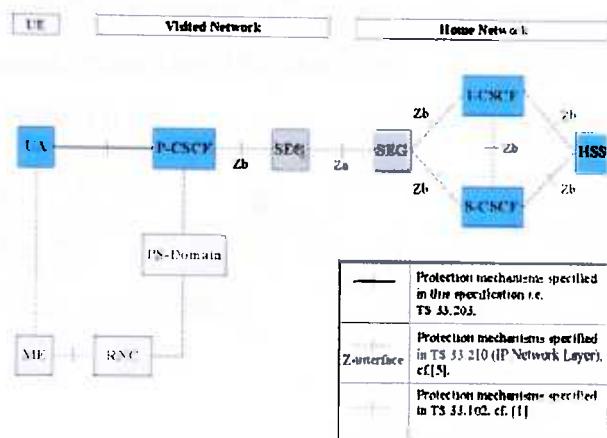
Η 3 παρέχει την ασφάλεια μέσα στην περιοχή δικτύου για την διεπαφή Cx.

Η 4 παρέχει ασφάλεια μεταξύ των διαφορετικών δικτύων για τους κόμβους που ανταλλάσουν μηνύματα SIP. Αυτή η συσχέτιση ασφάλειας ισχύει μόνο όταν τα P- CSCF και S- CSCF ή I- CSCF ανήκουν σε διαφορετικά δίκτυα.

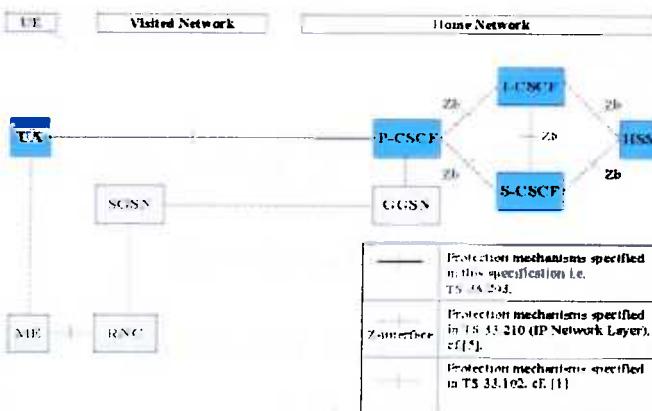
Η 5 παρέχει ασφάλεια εσωτερικά στο δίκτυο μεταξύ των κόμβων που ανταλλάσουν μηνύματα SIP. Σημειώστε ότι αυτή η συσχέτιση ασφάλειας ισχύει επίσης όταν το P- CSCF βρίσκεται στο πατρικό δίκτυο.

Η γενική εικόνα της αρχιτεκτονικής ασφαλείας του IMS σε σχέση με την ασφάλεια στο κυρίως δίκτυο είναι αυτή που φαίνεται στα σχήματα 9.5 και 9.6. Στο σχήμα 9.5 το P- CSCF ανήκει στο δίκτυο εξυπηρέτησης ενώ στο σχήμα 9.6 στο πατρικό δίκτυο.

Ασφάλεια και διαχείριση κλειδιών στο UMTS



Σχήμα 9.5 Αρχιτεκτονική ασφαλείας του IMS για το κυρίως δίκτυο όταν το P- CSCF ανήκει σε διαφορετικό δίκτυο



Σχήμα 9.6 Αρχιτεκτονική ασφαλείας του IMS για το κυρίως δίκτυο όταν το P- CSCF ανήκει στο πατρικό δίκτυο

9.2.1 Μηχανισμοί ασφαλείας

9.2.1.1 Αυθεντικοποίηση και συμφωνία κλειδιών

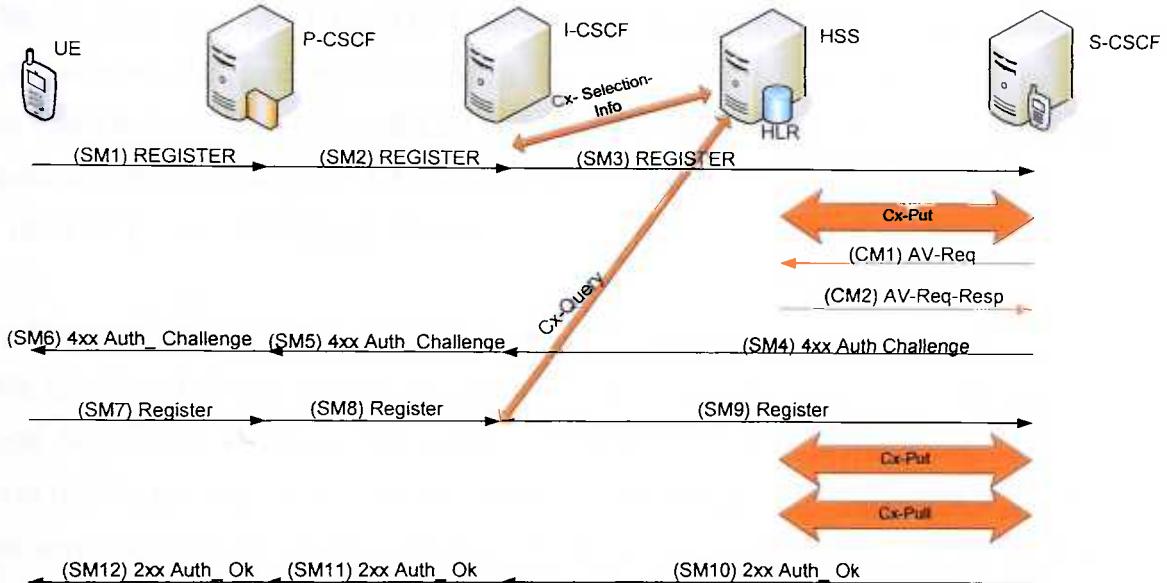
Το σχήμα για την αυθεντικοποίηση και τη συμφωνία κλειδιών στο IMS λέγεται IMS AKA. Το IMS AKA μοιάζει με το UMTS AKA.

Πριν να μπορέσει ένας χρήστης να έχει πρόσβαση στις IM υπηρεσίες πρέπει α) τουλάχιστον μία δημόσια ταυτότητα, (IMPU) του χρήστη να καταχωρηθεί στο μητρώο SIP και β) η μόνιμη ταυτότητα του χρήστη (IMPI) να αυθεντικοποιηθεί από το IMS σε επίπεδο εφαρμογής.

Προκειμένου να καταχωρηθεί το UE για να έχει πρόσβαση στις υπηρεσίες στέλνει ένα μήνυμα SIP REGISTER προς τον εξυπηρετητή μητρώου SIP (SIP REGISTER).

Ασφάλεια και διαχείριση κλειδιών στο UMTS

SERVER) δηλ. το S-CSCF, βλ. σχήμα 9.7, το οποίο θα εκτελέσει την αυθεντικοποίηση του χρήστη. Η ροή μηνυμάτων είναι ίδια ανεξάρτητα από εάν η IMPU του χρήστη έχει ήδη καταχωρεί στο μητρώο ή όχι.



Σχήμα 9.7 AKA για το IMS

Το SMn αντιπροσωπεύει το μήνυμα SIPn και το CMm το μήνυμα m του Cx της διαδικασίας επικύρωσης:

Ο χρήστης στέλνει το μήνυμα στο S-CSCF:

SM1:

REGISTER(IMPI, IMPU)

Τα P-CSCF και I-CSCF αντίστοιχα προωθούν τα μηνύματα SM2 και SM3 καταχώρησης SIP προς το S-CSCF.

Αφού το S-CSCF λάβει το SM3:

- Εάν το IMPU δεν είναι καταχωρημένο στο μητρώο του S-CSCF, αυτό πρέπει να εδοποιήσει το HSS ότι η εγγραφή του χρήστη στο μητρώο εκκρεμεί μέσω ενός δείκτη που ονομάζεται δείκτης εγγραφής. Ο δείκτης εγγραφής αποθηκεύεται στο HSS μαζί με το όνομα του S-CSCF και την ταυτότητα του χρήστη. Προκειμένου να ενημερωθεί ο δείκτης εγγραφής το S-CSCF στέλνει ένα μήνυμα Cx-Put στο HSS.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

β) Εάν το IMPU έχει ήδη καταχωρηθεί στο μητρώο, το S-CSCF θα αφήσει τον δείκτη εγγραφής στην θέση καταχωρημένο. Σε αυτή τη φάση το HSS έχει εκτελέσει έναν έλεγχο ότι το IMPI και το IMPU ανήκουν στον ίδιο χρήστη.

Με τη λήψη του SIP REGISTER το S-CSCF θα χρησιμοποιήσει ένα διάνυσμα (AV) αυθεντικοποίησης για την αυθεντικοποίηση του χρήστη. Εάν το S-CSCF δεν έχει κανένα έγκυρο διάνυσμα, AV, το S-CSCF θα στείλει ένα αίτημα CM1 για αποστολή διανυσμάτων αυθεντικοποίησης, AV, στο HSS μαζί με τον αριθμό m των AVs που θέλει, όπου το m είναι τουλάχιστον ένα. Δηλαδή:

CM₁:

Cx-AV-Req(IMPI, m)

Με την παραλαβή του αιτήματος από το S-CSCF, το HSS στέλνει μια διατεταγμένη σειρά διανυσμάτων αυθεντικοποίησης, n , στο S-CSCF με το μήνυμα CM₂. Τα διανύσματα αυθεντικοποίησης είναι διατεταγμένα. Κάθε διάνυσμα αυθεντικοποίησης αποτελείται από τα ακόλουθα συστατικά: έναν τυχαίο αριθμό RAND, μια αναμενόμενη απάντηση XRES, ένα κλειδί κρυπτογράφησης CK, ένα κλειδί ακεραιότητας IK και το AUTN, όπως δηλαδή και στο UMTS AKA

CM₂:

Cx-AV-REQ-RESp(IMPI, RAND1 || AUTN1 || XRES || CK1 || IK1, ..., RANDn || AUTNn || XRESn || CKn || IKn)

Όταν το S-CSCF πρέπει να στείλει μια πρόκληση αυθεντικοποίησης στο χρήστη, επιλέγει το επόμενο διάνυσμα αυθεντικοποίησης από τη διαταγμένη σειρά.

Το S-CSCF στέλνει ένα SIP 4xx Auth_Challenge, δηλ. μια πρόκληση αυθεντικοποίησης, προς τον κινητό σταθμό, UE, συμπεριλαμβάνοντας το RAND, το AUTN το κλειδί ακεραιότητας IK, το κλειδί κρυπτογράφησης CK στο SM4 και το αποστέλλει στο P-CSCF. Το S-CSCF αποθηκεύει επίσης το RAND που έστειλε για τη χρήση σε περίπτωση αποτυχίας συγχρονισμού.

Η επαλήθευση του σειριακού αριθμού SQN από το USIM και το ISIM θα αναγκάσει το UE να απορρίψει μια προσπάθεια από το S-CSCF να επαναχρησιμοποιηθεί ένα διάνυσμα αυθεντικοποίησης AV. Επομένως κανένα διάνυσμα αυθεντικοποίησης, AV, δεν θα σταλεί περισσότερο από μία φορά.

SM4: 4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Όταν το P-CSCF λάβει το SM5 θα αποθηκεύσει το κλειδιά, θα τα αφαιρέσει από το μήνυμα και θα διαβιβάσει το υπόλοιπο μήνυμα στο UE.

SM6: 4xxAuth_Challenge(IMPI, RAND, AUTN)

Μετά τη λήψη του SM6, ο κινητός σταθμός παίρνει το AUTN, το οποίο περιλαμβάνει τη MAC και το SQN. Υπολογίζει το XMAC, ελέγχει ότι XMAC=MAC και ότι το SQN είναι στη σωστή σειρά. Εάν και οι δύο αυτοί έλεγχοι είναι επιτυχείς ο κινητός σταθμός χρησιμοποιεί το RES και μερικές άλλες παραμέτρους για να υπολογίσει μια απάντηση επικύρωσης. Αυτή η απάντηση αποστέλλεται μέσω των P-CSCF και I-CSCF τελικά στο S-CSCF με το μήνυμα SM7. Πρέπει να σημειωθεί ότι το UE σε αυτή τη φάση επίσης υπολογίζει τα κλειδιά συνόδου CK και IK και έτσι το IK παρέχει προστασία ακεραιότητας.

SM7: REGISTER(IMPI, Authentication response)

Το P-CSCF διαβιβάζει την απάντηση αυθεντικοποίησης μέσω του μηνύματος SM8 στο I-CSCF, το οποίο ρωτά το HSS για να βρει τη διεύθυνση του S-CSCF. Με τη λήψη της διεύθυνσης από το HSS, διαβιβάζει την απάντηση αυθεντικοποίησης SM9 στο S-CSCF.

Μετά τη λήψη του SM9, το S-CSCF ανακτά το XRES για εκείνο τον χρήστη και το χρησιμοποιεί για έλεγχο της απάντησης που στέλνεται από το UE. Εάν ο έλεγχος είναι επιτυχής ο χρήστης έχει αυθεντικοποιηθεί και το IMPU έχει καταχωρηθεί στο S-CSCF. Εάν το IMPU καταχωρήθηκε σωστά, το S-CSCF θα στείλει ένα μήνυμα Cx-Put για να θέσει τον ενδείκτη εγγραφής του HSS στη θέση καταχωρήθηκε και αυτή η εγγραφή θα ισχύσει για κάποια χρονική περίοδο.

Εάν ο χρήστης έχει αυθεντικοποιηθεί επιτυχώς, το S-CSCF στέλνει ένα SM10 μήνυμα SIP 2xx Auth_OK στο I-CSCF δείχνοντας ότι η εγγραφή ήταν επιτυχής. Με τα μηνύματα SM11 και SM12 τα I-CSCF και P-CSCF προωθούν το SIP 2xx Auth_OK προς τον κινητό σταθμό UE.

Πρέπει να σημειωθεί ότι η επανεγγραφή του κινητού σταθμού, (UE), ανοίγει μια πιθανή πόρτα για επίθεση άρνησης υπηρεσιών. Δηλαδή, ένας κακόβουλος θα μπορούσε να προσπαθήσει να καταχωρήσει ένα ήδη καταχωρημένο IMPU και να αποκριθεί με μια ανακριβή απάντηση αυθεντικοποίησης προκειμένου να κάνει το πατρικό δίκτυο, HN, να διαγράψει το IMPU. Για αυτόν τον λόγο ένας συνδρομητής, όταν εγγρά-

φεται, δεν θα διαγραφεί εάν αποτύχει μια αυθεντικοποίηση. Τα μήκη των παραμέτρων IMS AKA είναι τα ίδια με του UMTS AKA.

9.2.1.1.1 Αποτυχίες Αυθεντικοποίησης

9.2.1.1.1.1 Αποτυχία αυθεντικοποίησης χρήστη

Σε αυτήν την περίπτωση η αυθεντικοποίηση του χρήστη πρέπει να αποτύχει στο S-CSCF εξαιτίας της ανακριβής απάντησης που αυτό λαμβάνει με το SM9.

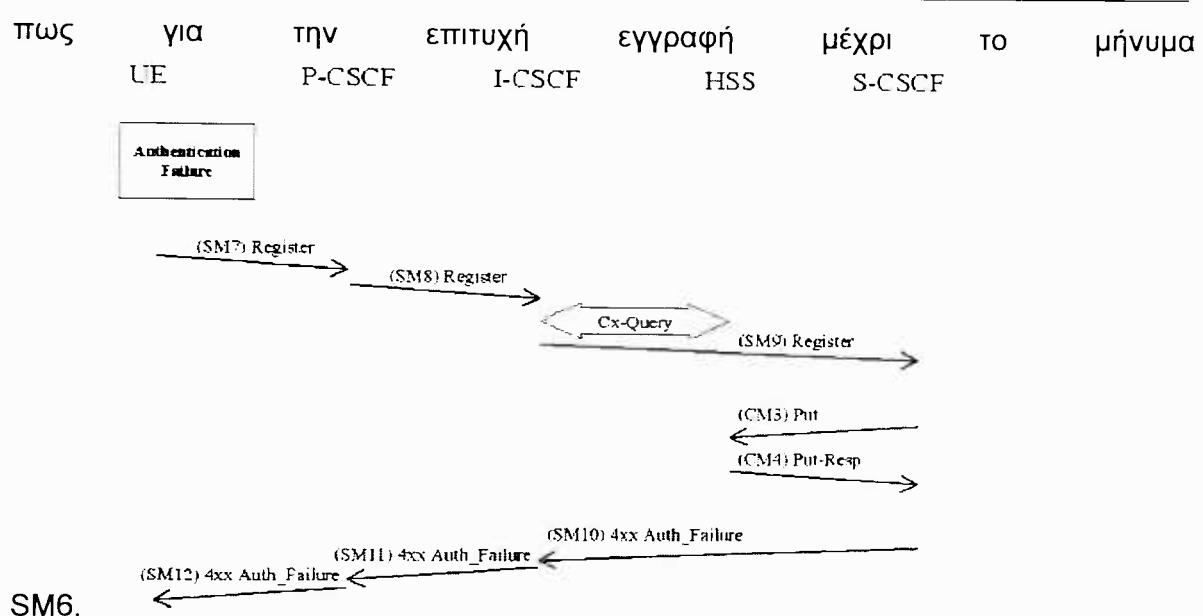
Ωστόσο, εάν η απάντηση είναι ανακριβής, τότε το ΙΚ που χρησιμοποιείται για να προστατεύσει το SM7 θα είναι κανονικά ανακριβές επίσης, το οποίο κανονικά θα αναγκάσει τον έλεγχο ακεραιότητας στο P-CSCF να αποτύχει προτού να μπορέσει η απάντηση να επαληθευτεί στο S-CSCF. Σε αυτήν την περίπτωση SM7 απορρίπτεται από το IPsec στο P-CSCF.

Εάν περάσει τον έλεγχο ακεραιότητας αλλά η απάντηση είναι ανακριβής, οι ροές μηνυμάτων είναι ίδιες μέχρι και το μήνυμα SM9 σαν μία επιτυχή αυθεντικοποίηση. Μόλις το S-CSCF ανιχνεύσει την αποτυχία αυθεντικοποίησης του χρήστη, πρέπει να προχωρήσει με τον ίδιο τρόπο όπως σαν να είχε λάβει το SM9 σε μια αποτυχία αυθεντικοποίησης δικτύου που αναφέρεται στην επόμενη παράγραφο (9.2.1.1.2).

9.2.1.1.2 Αποτυχία αυθεντικοποίησης δικτύου

Όταν ο έλεγχος της MAC στο UE αποτύχει, το δίκτυο δεν μπορεί να αυθεντικοποιηθεί και ως εκ τούτου η εγγραφή αποτυγχάνει. Η ροή των μηνυμάτων είναι ίδια ό-

Ασφάλεια και διαχείριση κλεδιών στο UMTS



Σχήμα 9.8 Αποτυχία αυθεντικοποίησης δικτύου στο IMS AKA

Το κινητός σταθμός, UE, θα στείλει ένα μήνυμα καταχώρησης (register) προς το πατρικό δίκτυο, HN, συμπεριλαμβανομένης μιας ένδειξης για την αιτία της αποτυχίας SM7. Το P-CSCF και το I-CSCF- διαβιβάζουν αυτό το μήνυμα στο S-CSCF (σχήμα 9.8).

SM7: REGISTER (Failure=Authentication Failure, IMPU)

Με τη λήψη του μηνύματος SM9, το οποίο περιέχει την αιτία της αποτυχίας αυθεντικοποίησης, το S-CSCF θέτει τον ενδείκτη εγγραφής στο HSS στη θέση μη καταχωρημένο αν το IMPU δεν είναι ήδη καταχωρημένο. Για να γίνει αυτό το S-CSCF στέλνει ένα μήνυμα Cx-Put στο HSS με το CM3. Αν το IMPU είναι ήδη καταχωρημένο δεν θα αλλάξει τον ενδείκτη.

CM3: Cx-AV-Put (IMPU, Clear S-CSCF name)

Το πατρικό δίκτυο, HSS, απαντά στο μήνυμα CM3 με ένα Cx-Put-Resp που συμπεριλαμβάνεται στο μήνυμα CM4.

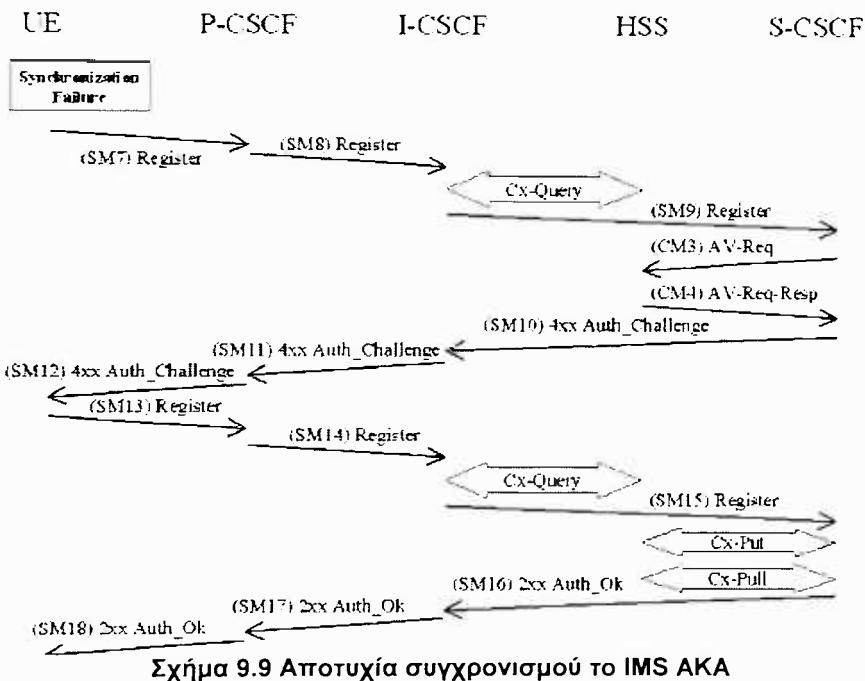
Στο SM10 το S-CSCF στέλνει ένα μήνυμα αποτυχίας αυθεντικοποίησης.

SM10: SIP/2.0 4xx Auth_Failure.

9.2.1.1.3 Αποτυχία συγχρονισμού

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Μετά από τον επανασυγχρονισμό, η αυθεντικοποίηση είναι πιθανό να μπορεί να ολοκληρωθεί επιτυχώς, αλλά μπορεί επίσης να συμβεί στις επόμενες προσπάθειες να υπάρξουν άλλοι λόγοι αποτυχίας (δηλ. αποτυχία αυθεντικοποίησης χρηστών, αποτυχία αυθεντικοποίησης δικτύων κλπ). Ας δούμε την περίπτωση που η επόμενη προσπάθεια είναι επιτυχής.



Η ροή των μηνυμάτων δεν αλλάζει μέχρι το SM6. Όταν το UE λαμβάνει το SM6 ανιχνεύει ότι το SQN είναι εκτός εύρους και στέλνει μια αποτυχία συγχρονισμού πίσω στο S-CSCF με το SM7 (σχήμα 9.9).

SM7:

REGISTER(Failure = Synchronization Failure, AUTS, IMPI)

Με τη λήψη της αποτυχίας συγχρονισμού και του AUTS το S-CSCF στέλνει ένα AV-Req στο HSS με το CM3 συμπεριλαμβανομένου του RAND που αποθηκεύτηκε στο S-CSCF και των απαραίτητο αριθμό AVs, m.

CM3:

Cx-AV-Req(IMPI, RAND, AUTS, m)

Το HSS ελέγχει το AUTS. Μετά από ενδεχομένως την ενημέρωση του SQN, το HSS στέλνει νέα AVs στο S-CSCF στο CM4.

CM4:

Cx-AV-Req-Resp

(IMPI, n ,RAND1||AUTN1||XRES1||CK1||I K_1 ,...,RAND n ||AUTN n ||XRES n ||CK n ||I K_n)

Όταν το S-CSCF λαμβάνει τη νέα ομάδα διανυσμάτων επικύρωσης από το HSS διαγράφει τα παλαιά για εκείνο τον χρήστη

Τα υπόλοιπα μηνύματα δηλ. SM10-SM18 συμπεριλαμβανομένων των μηνυμάτων του Cx είναι ακριβώς τα ίδια με τα SM4-SM12 και τα αντίστοιχα μηνύματα του Cx της κανονικής διαδικασίας αυθεντικοποίησης § 9.2.1.1.

9.2.1.2 Μηχανισμοί εμπιστευτικότητας/κρυπτογράφησης.

Εάν η τοπική πολιτική ασφαλείας στο P-CSCF απαιτεί τη χρήση κρυπτογράφησης μεταξύ UE και P-CSCF, το IPsec ESP σε μορφή μεταφοράς (transport mode) θα παράσχει την προστασία εμπιστευτικότητας στα μηνύματα σηματοδοσίας ανάμεσα στο UE και το P-CSCF (πχ από SEG σε SEG). Προστατεύοντας όλα τα μηνύματα σηματοδοσίας στο επίπεδο IP.

Σαν αποτέλεσμα μιας διαδικασίας αυθεντικοποίησης, σαν αυτή που περιγράφαμε παραπάνω δύο ζευγάρια SAs μεταξύ του UE και του P-CSCF θα δημιουργηθούν. Ένα ζευγάρι SA είναι για την κυκλοφορία μεταξύ μιας πόρτας πελάτη στο UE και μιας πόρτας εξυπηρετητή στο P-CSCF και το άλλο ζευγάρι SA, είναι για την κυκλοφορία μεταξύ μιας πόρτας πελάτη στο στο P-CSCF και μιας πόρτας εξυπηρετητή στο UE.

Η κλειδί κρυπτογράφησης CK_{ESP} είναι ίδιο για τα δύο ζευγάρια των SAs. Το κλειδί κρυπτογράφησης CK_{ESP} δημιουργείται από το κλειδί CK_{IM} που παράγεται ως αποτέλεσμα της διαδικασίας AKA, χρησιμοποιώντας μία κατάλληλη συνάρτηση επέκτασης κλειδιών. Η επέκταση του κλειδιού κρυπτογράφησης από την πλευρά χρηστών γίνεται στο UE. Η επέκταση από την πλευρά του δικτύου γίνεται στο P-CSCF.

9.2.1.3 Μηχανισμοί εξασφάλισης ακεραιότητας

Το IPsec ESP σε μορφή μεταφοράς (transport mode) θα παράσχει την προστασία ακεραιότητας στα μηνύματα σηματοδοσίας SIP μεταξύ του UE και του P-CSCF, προστατεύοντας όλα τα μηνύματα σηματοδοσίας SIP στο επίπεδο IP.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Σαν αποτέλεσμα μιας διαδικασίας αυθεντικοποίησης, σαν αυτή που περιγράφαμε παραπάνω δύο ζευγάρια SAs μεταξύ του UE και του P- CSCF θα δημιουργηθούν. Ένα ζευγάρι SA είναι για την κυκλοφορία μεταξύ μιας πόρτας πελάτη στο UE και μιας πόρτας εξυπηρετητή στο P- CSCF και το άλλο ζευγάρι SA είναι για την κυκλοφορία μεταξύ μιας πόρτας πελάτη στο P- CSCF και μιας πόρτας εξυπηρετητή στο UE.

Η κλειδί ακεραιότητας IK_{Esp} είναι ίδιο για τα δύο ζευγάρια των SAs. Το κλειδί ακεραιότητας IK_{ESP} δημιουργείται από το κλειδί CK_M που παράγεται ως αποτέλεσμα της διαδικασίας AKA, χρησιμοποιώντας μία κατάλληλη συνάρτηση επέκτασης κλειδιών. Η επέκταση του κλειδιού κρυπτογράφησης από την πλευρά χρηστών γίνεται στο UE. Η επέκταση από την πλευρά του δικτύου γίνεται στο P- CSCF.

9.2.1.4 Μηχανισμοί απόκρυψης

Ο μηχανισμός απόκρυψης είναι προαιρετικός στην εφαρμογή του. Όλοι οι κόμβοι I-CSCF στο πατρικό δίκτυο (HN), μοιράζονται το ίδιο κλειδί κρυπτογράφησης και απόκρυπτογράφησης Kv. Εάν ο μηχανισμός χρησιμοποιείται και η πολιτική δηλώνει ότι η τοπολογία θα παραμείνει κρυμμένη, το I-CSCF θα κρυπτογραφήσει τα στοιχεία κρύβοντας πληροφορίες όταν διαβιβάζει τα μηνύματα SIP έξω από την περιοχή του δικτύου που θέλει ν παραμείνει κρυμμένη. Οι κρυμμένες πληροφορίες είναι καταχωρήσεις στις κεφαλίδες των μηνυμάτων SIP, οι οποίες περιέχουν τις διευθύνσεις των πληρεξούσιων (proxy) SIP του κρυμμένου δικτύου.

Ο σκοπός της κρυπτογράφησης στην απόκρυψη δικτύων είναι, να προστατευθούν οι ταυτότητες των πληρεξουσίων SIP και η τοπολογία του δικτύου. Ο αλγόριθμος AES στην μορφή CBC, (Cipher Block Chaining, §8.2.1), με εκατον εικοσι οκτώ bits τμήμα και εκατον εικοσι οκτώ bits κλειδί χρησιμοποιείται ως αλγόριθμος κρυπτογράφησης για το κρύψιμο της τοπολογίας των δικτύων. Στην μορφή CBC με ένα δεδομένο κλειδί, εάν ένα σταθερό (διάνυσμα αρχικοποίησης), IV, χρησιμοποιείται για να κρυπτογραφήσει δύο ίδια κείμενα, τότε τα κρυπτογραφημένα τμήματα των κρυπτογραφημένων κειμένων θα είναι επίσης ίσα. Αυτό είναι ανεπιθύμητο για το κρύψιμο δικτύων. Έτσι, ένα τυχαίο IV χρησιμοποιείται για κάθε κρυπτογράφηση. Το ίδιο IV απαιτείται για την αποκρυπτογράφηση των πληροφοριών. Έτσι το IV θα συμπεριληφθεί στην ίδια κεφαλίδα SIP που περιλαμβάνει τις κρυπτογραφημένες πληροφορίες.



9.2.1.5 Διαδικασία δημιουργίας συσχέτισης ασφαλείας

Η διαδικασία δημιουργίας συσχέτισης ασφαλείας (SA), είναι απαραίτητη προκειμένου να αποφασιστούν ποιοι παράμετροι ασφαλείας που θα ισχύσουν κατά την έναρξη των υπηρεσιών ασφαλείας. Όπως είπαμε, στο IMS η αυθεντικοποίηση των χρηστών εκτελείται κατά τη διάρκεια της εγγραφής/καταχώρησης στο μητρώο.

Μετά την αυθεντικοποίηση, τα μηνύματα της συνόδου θα έχουν προστασία ακεραιότητας βασισμένη στα κλειδιά που παράγονται κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης.

Για την προστασία της σηματοδοσίας του IMS μεταξύ του κινητού σταθμού UE και του P- CSCF, είναι απαραίτητο να συμφωνηθούν τα κοινά κλειδιά που παρέχονται από το IMS AKA, και ένα σύνολο άλλων παραμέτρων συγκεκριμένων για τη μέθοδο προστασίας. Οι παράμετροι μίας SA είναι:

- Ο Αλγόριθμος κρυπτογράφησης
- Ο Αλγόριθμος ακεραιότητας
- To SPI (Security Parameter index)
- Η διάρκειά της
- Ο τύπος της (είναι πάντα μεταφοράς (transport))
- Το μήκος του κλειδιού ακεραιότητας $I_{KE_{SP}}$ που είναι 128 bits για τον αλγόριθμο HMAC-MD5-96 και 160 bits για τον αλγόριθμο HMAC-SHA-1-96

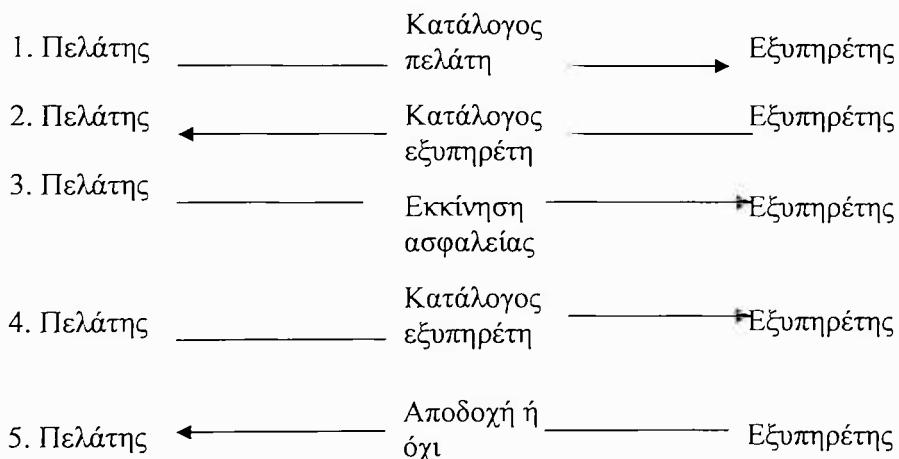
Η τριάδα SPI, IP αποστολέα, IP παραλήπτη χαρακτηρίζει μοναδικά μία SA. Η βασική ιδέα για την δημιουργία μίας SA είναι, πρώτα, να γίνει ανταλλαγή ενός καταλόγου δυνατοτήτων ασφαλείας (security capability lists) μεταξύ του πελάτη και του εξυπηρετητή κατά τρόπο μη προστατευμένο και κατόπιν ελέγχεται η εγκυρότητα της επιλογής όταν η προστασία τεθεί εντός. Η διαδικασία είναι παρόμοια με αυτήν πού περιγράφτηκε στην παράγραφο 5.2.4.2 (Διαδικασία εγκαθίδρυσης ασφαλούς συνόδου επικοινωνίας).

Η ροή μηνυμάτων απεικονίζεται στο σχήμα 9.10.

- Στο πρώτο βήμα, ο πελάτης στέλνει τον κατάλογο εκείνων των μηχανισμών ασφαλείας που υποστηρίζει στον εξυπηρέτη.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

- Στο δεύτερο βήμα, ο εξυπηρέτης στέλνει τους μηχανισμούς ασφάλειάς που ίδιος υποστηρίζει και άλλες παραμέτρους.
- Στο βήμα 3, ο πελάτης μπορεί να ανακαλύψει τον μηχανισμό με την υψηλότερη προτίμηση των 2 μερών. Ξεκινά η εκτέλεση ασφάλειας με αυτόν τον μηχανισμό.
- Στο βήμα 4, ο πελάτης επιστρέφει τον κατάλογο μηχανισμών και παραμέτρων ότι έλαβε προηγουμένως στο βήμα 2.
- Στο τελικό βήμα, ο εξυπηρέτης ελέγχει ότι ο κατάλογος που παραλαμβάνεται από τον πελάτη στο βήμα 4 είναι, πράγματι, ίδιος με τον κατάλογο ο εξυπηρέτης έστειλε στο βήμα 2. Ο πελάτης στη ροή μηνυμάτων είναι το UAC (User Agent Client), ενώ ο εξυπηρέτης το UAS (user agent server).



Σχήμα 9.10 Ανταλλαγή μηνυμάτων συμφωνίας ασφαλείας

Όλες οι SAs αποθηκεύονται στη SAD (SA Database). Εκτός από τη SAD, απαιτείται μία SPD (Security policy Database), η οποία χρησιμοποιείται για να αποφασίσει τι είδους προστασία απαιτείται για κάθε εξερχόμενο ή εισερχόμενο πακέτο. Λόγω της SPD, οι SAs είναι συνδεδεμένες με διάφορους μηχανισμούς επιλογής (selectors):

- διευθύνσεις IP αποστολέα και προορισμού
- πρωτόκολλα μεταφοράς που μπορούν να χρησιμοποιηθούν με τη SA (για το IMS, τα UDP και TCP)
- πόρτες αποστολέα και προορισμού.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Οι πόρτες χρησιμοποιούνται για να διαφοροποιήσουν τα προστατευμένα μηνύματα από τα μη προστατευμένα μηνύματα και τις νέες SAs από τις παλαιές στις περιπτώσεις που οι SAs ανανεώνονται. Βασικά, η χρήση των πορτών μπορεί να επιτρέψει τις περιπτώσεις, όπου η ίδια διεύθυνση IP μοιράζεται μεταξύ διάφορων χρηστών και η διαφοροποίησης μεταξύ τους μπορεί να γίνει με τους αριθμούς των πορτών.

Το P-CSCF επιλέγει δύο αριθμούς πορτών ως προστατευμένες, (protected), πόρτες (port_pc και port_ps), οι οποίες επικοινωνούν ασφαλώς με τον κινητό σταθμό UE και είναι διαφορετικές από την τυποποιημένη πόρτα με αριθμό 5060 του SIP. Μόνο τα προστατευμένα μηνύματα μπορούν να παραληφθούν από τις προστατευμένες πόρτες στο P-CSCF. Το IPsec που φροντίζει γι' αυτό.

Το UE από την άλλη μεριά επιλέγει δύο τοπικές προστατευμένες πόρτες όπου μόνο προστατευμένα μηνύματα μπορούν να παραληφθούν και να αποσταλούν (port_uc και port_us) από το UE.

Οι προστατευμένους πόρτες πελατών port_uc και port_pc αλλάζουν κάθε φορά που μια νέα SA δημιουργείται, αλλά οι προστατευμένες πόρτες port_us και port_ps των εξυπηρετητών παραμένουν αμετάβλητες.

Η χρήση των αριθμών πορτών για τα προστατευμένα μηνύματα συνοψίζεται στον πίνακα 9.1.

Τα μη προστατευμένα μηνύματα μπορούν να σταλούν και να παραληφθούν σε οποιοδήποτε πόρτα εκτός από τις προστατευμένες

Ενώ το επίπεδο IPsec, ελέγχει ότι όλα τα μηνύματα που παραλαμβάνονται από τις προστατευμένες πόρτες είναι προστατευμένα, δεν μπορεί να εγγυηθεί ότι μερικά μηνύματα που πρέπει να είναι προστατευμένα, εστάλησαν σε μη προστατευμένες πόρτες. Αυτός ο έλεγχος πρέπει να γίνει στο επίπεδο SIP. Τα μόνα μη προστατευμένα μηνύματα που μπορεί να λάβει το P-CSCF είναι οι αιτήσεις καταχώρησης, ενώ ο κινητός σταθμός UE, μπορεί να παραλάβει χωρίς προστασία μόνο απαντήσεις σε αυτές τις μη προστατευμένες αιτήσεις καταχώρησης και μερικά άλλα μηνύματα λάθους.

UE port ↔ P-CSCF port	SIP requests (UDP and TCP) SIP responses (UDP)	SIP responses (TCP)
plink	port_uc → port_ps	port_us → port_pc
Downlink	port_us ← port_pc	port_uc ← port_ps

Πίνακας 9.1 Χρήση προστατευμένων πορτών για τα προστατευμένα μηνύματα

9.2.1.6 Διαχείριση των συσχετίσεων ασφαλείας (SAs στο επίπεδο SIP)

Τα συσχετίσεις ασφαλείας SAs όπως έχουμε αναφέρει, είναι ουσιαστικά για το IPsec. Η σύνδεση μεταξύ των χρησιμοποιούμενων SAs και ταυτότητων SIP, γίνεται στο επίπεδο SIP.

Στο P-CSCF, το επίπεδο SIP διατηρεί μια βάση δεδομένων όπου κάθε SA προσδιορίζεται από τη διεύθυνση IP του κινητού σταθμού UE και τους αριθμούς των προστατευμένων πορτών των UE και P-CSCF. Επιπλέον, ταυτότητες SIP, IMPI και IMPU καταγράφονται για κάθε SA. Καταγράφεται επίσης η διάρκεια ζωής του SA στη βάση δεδομένων.

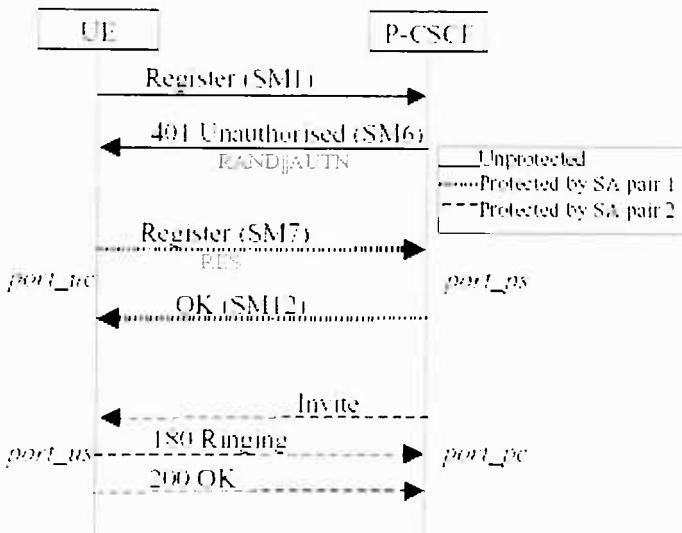
Για κάθε εισερχόμενο μήνυμα στο P-CSCF, το επίπεδο SIP (μετά από ελέγχο ότι το μήνυμα δεν είναι αίτηση καταχώρησης στον κατάλογο δηλ., REGISTER) ελέγχει ότι η SA που χρησιμοποιείται από το IPsec ταιριάζει με τις ταυτότητες SIP μέσα στο μήνυμα.

Στο UE, η βάση δεδομένων είναι απλούστερη: για κάθε SA, οι αριθμοί των προστατευμένων αριθμών πορτών αποθηκεύονται μαζί με τη διάρκεια ζωής της SA και κάθε εισερχόμενο μήνυμα ελέγχεται σε σχέση με τα στοιχεία της βάσης δεδομένων.

Όταν το UE αρχίζει μία καταχώρηση στο μητρώο, (reregistration), το αίτημα μπορεί να προστατευθεί με μια υπάρχουσα SA. Στην περίπτωση που εκτελείται ένα πρωτόκολλο AKA, δύο νέα ζευγάρια SAs δημιουργούνται. Για κάποιο χρόνο κατά τη διάρκεια της εγγραφής, οι δύο παλαιές SAs και οι δύο νέες SAs πρέπει να αποθηκευτούν. Αυτό οφείλεται στο γεγονός ότι, το P-CSCF δεν γνωρίζει αν το τελευταίο μήνυμα έχει παραληφθεί από το UE μέχρι ένα νέο μήνυμα που προστατεύεται από μία νέα SA παραλαμβάνεται από το UE. Οι SAs διαγράφονται φυσικά όταν λήγει ο χρόνος ζωής τους. Στο P-CSCF, μπορεί να συμβεί το γεγονός οκινητός σταθμός UE να αρχίσει μια νέα διαδικασία καταχώρησης (reregistration) ενώ η προηγούμενη διαδικασία reregistration βρίσκεται ακόμα σε εξέλιξη. Αυτό μπορεί να συμβεί, παραδείγματος χάριν, εάν η τελική επικύρωση επιτυχούς καταχώρησης δεν φθάνει ποτέ στο UE. Σε αυτήν την περίπτωση, το P-CSCF μπορεί να έχει 6 ζευγάρια SA ταυτόχρονα (για το ίδιο UE). Εντούτοις,

αυτή η εξαιρετική περίπτωση διαρκεί για πολύ περιορισμένο χρόνο έως ότου δύο από τα έξι ζευγάρια SA διαγραφούν.

Ένα παράδειγμα για το πώς χρησιμοποιούνται δύο ζευγάρια SAs για ανταλλαγή μηνυμάτων INVITE πάνω από το TCP που προστατεύονται από τις αντίστοιχες IPsec SAs φαίνεται στο σχήμα 9.12.



Σχήμα 9.11 Παράδειγμα χρήσης των SAs

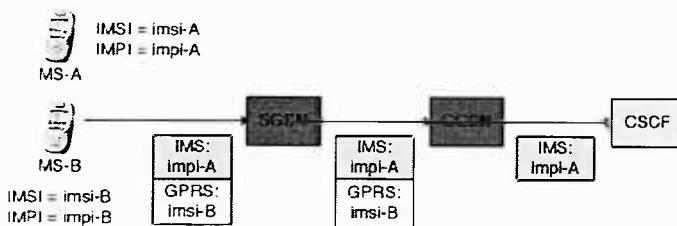
9.3 Μη εξουσιοδοτημένη χρήση του IMS

Όπως αναφέρθηκε, προκειμένου ο χρήστης να έχει πρόσβαση στο δίκτυο UMTS,

πρέπει να αυθεντικοποιηθεί και αυτό γίνεται μέσω του UMTS-AKA. Επίσης, για να μπορέσει ο χρήστης να χρησιμοποιήσει τις υπηρεσίες του IMS, πρέπει να αυθεντικοποιηθεί μέσω του IMS AKA. Ουσιαστικά τα 2 πρωτόκολλα AKA είναι τα ίδια. Άρα ο χρήστης πρέπει να τρέξει το AKA 2 φορές για να έχει πρόσβαση στο IMS.

Αυτό είναι απαραίτητο καθώς με πρόσβαση στο IMS χωρίς αυθεντικοποίηση, ένας χρήστης θα μπορούσε να υποδυθεί κάποιον άλλο ο οποίος έχει πρόσβαση σε αυτό. Ας θεωρήσουμε το παράδειγμα στο σχήμα 9.12, όπου υπάρχουν δύο κινητοί σταθμοί. Ο κινητός σταθμός MS-A, έχει IMSI με τιμή imsi-A και IMPI με τιμή impi-A. Αντίστοιχα ο κινητός σταθμός MS-B, έχει IMSI με τιμή imsi-B και IMPI με τιμή impi-B. Υποθέτουμε ότι ο MS-B είναι ένας νόμιμος χρήστης του UMTS και έχει περάσει με επιτυχία τον έ-

λεγχό αυθεντικοποίησης, με χρήση του imsi-B. Αν η αυθεντικοποίηση για πρόσβαση στο IMS δεν ήταν απαραίτητη, ο χρήστης MS-B θα μπορούσε να κάνει επιτυχημένη εγγραφή στο μητρώο του IMS, άρα να χρησιμοποιήσει τις υπηρεσίες του, στέλνοντας στο S-CSCF ένα μήνυμα αίτησης εγγραφής το οποίο περιέχει την τιμή impi-A του MS-A σαν παράμετρο. Το S-CSCF θα θεωρήσει αυτή την αίτηση νόμιμη και θα επιτρέψει την είσοδο του MS-B στις υπηρεσίες IMS.



Σχήμα 9.12 Μη εξουσιοδοτημένη χρήση του IMS

9.4 Πρόταση Yi-Bing Lin et al

Προκειμένου να αποφευχθεί η διπλή αυθεντικοποίηση του χρήστη για πρόσβαση στο IMS, προτάθηκε ένα πρωτόκολλο, με το οποίο επιτυγχάνεται σχεδόν ταυτόχρονη αυθεντικοποίηση, («one pass»), για το UMTS και IMS. Με αυτόν τον τρόπο μειώνεται κατά 50% περίπου το πλήθος των ανταλλασσόμενων μηνυμάτων, αλλά και των διανυσμάτων αυθεντικοποίησης που αποθηκεύονται, με αποτέλεσμα την ταχύτερη πρόσβαση στις υπηρεσίες και την καλύτερη εκμετάλλευση των πόρων του δικτύου.

Το πρωτόκολλο έχει ως εξής (σχήμα 9.14).

Αρχικά γίνεται η αυθεντικοποίηση του κινητού σταθμού, (χρήστη), στο δίκτυο UMTS με την διαδικασία που περιγράφηκε αναλυτικά στο κεφάλαιο 5. Κατόπιν:

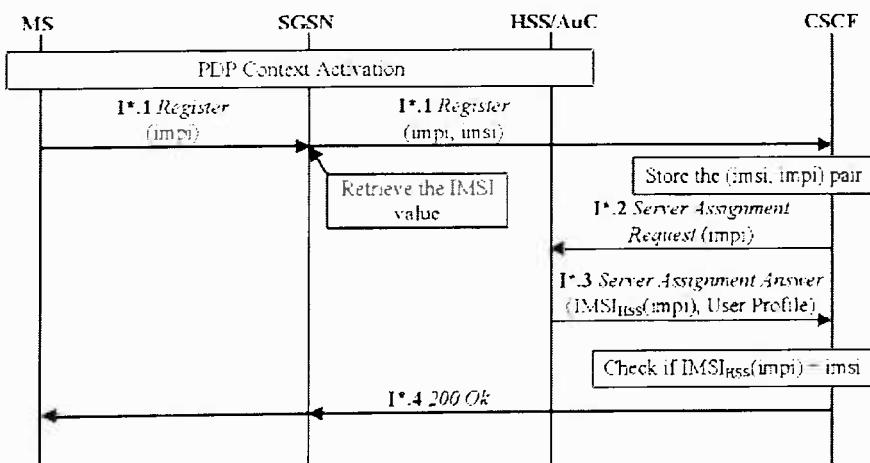
1. Ο κινητός σταθμός, στέλνει ένα μήνυμα SIP εγγραφής στο SGSN με παράμετρο την ταυτότητα IMPI. Παρατηρείστε ότι, λόγω του ότι ο τερματικός σταθμός έχει ήδη αυθεντικοποιηθεί για πρόσβαση στο UMTS, το SGSN μπορεί να αναγνωρίσει την ταυτότητα IMSI του κινητού σταθμού που αυτός εκπέμπει. Το SGSN, προσθέτει το IMSI του κινητού σταθμού στο μήνυμα καταχώρησης/εγγραφής και το προωθεί στο CSCF.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

2. Το CSCF αποθηκεύει τα (IMPI, IMSI) και στέλνει ένα μήνυμα Cx στο HSS/AuC με παράμετρο το IMPI, προκειμένου να ενημερώσει τον ενδείκτη εγγραφής.

3. Το HSS/AuC χρησιμοποιεί το IMPI για να βρεί το IMSI του κινητού σταθμού/χρήστη καθώς και αν έχει δικαίωμα πρόσβασης στις υπηρεσίες του IMS. Ας ονομάσουμε IMSI_{HSS} το IMSI που ανασύρθηκε από τα αρχεία του HSS. Το HSS αποθηκεύει το όνομα του CSCF και στέλνει μία απάντηση Cx σε αυτό, με παραμέτρο το IMSI_{HSS} .

4. Το CSCF ελέγχει αν τα IMSI και IMSI_{HSS} είναι τα ίδια. Αν είναι, το CSCF στέλνει ένα μήνυμα SIP 200 Ok στο SGSN αυτό με τη σειρά του στο MS και η αυθεντικοποίηση θεωρείται επιτυχής. Αν τα IMSI και IMSI_{HSS} δεν είναι τα ίδια, τότε η αυθεντικοποίηση δεν πραγματοποιείται.



Σχήμα 9.13 Αυθεντικοποίηση «one pass» για UMTS και IMS

ΚΕΦΑΛΑΙΟ 10

Συμπεράσματα – Θέματα που χρειάζονται περαιτέρω μελέτη

Η ασφάλεια, είναι ένα από τα σημαντικότερα ζητήματα που ένα κυψελοειδές δίκτυο πρέπει να υποστηρίξει, με σκοπό να παράσχει την κατάλληλη μυστικότητα στους συνδρομητές. Ακριβέστερα, πρέπει να είναι σε θέση προστατεύσει τους χρήστες από απάτη τιμολόγησης και γενικά από όλα τα είδη απάτης, ενώ τα δεδομένα και οι πληροφορίες που αφορούν στους χρήστες πρέπει να κρυπτογραφούνται κατά τέτοιο τρόπο, ώστε θα είναι διαθέσιμα μόνο στους σωστούς αποδέκτες, αποτρέποντας οποιονδήποτε πιθανό ωτακουστή.

Οι θεμελιώδεις μηχανισμοί που απαιτούνται για να παρέχονται όλες οι ανωτέρω υπηρεσίες είναι, η εμπιστευτικότητα της ταυτότητας του χρήστη, η αυθεντικοποίηση της ταυτότητας του χρήστη και η κρυπτογράφηση των μηνυμάτων σηματοδοσίας.

Ο στόχος της εμπιστευτικότητα της ταυτότητας του χρήστη είναι, να παρασχεθεί η μυστικότητα στο χρήστη ώστε να αποτραπεί ο προσδιορισμός του προσώπου που συναλλάσσεται με το δίκτυο.

Επιπρόσθετα, η αυθεντικοποίηση χρησιμοποιείται προκειμένου να προσδιοριστεί ο χρήστης που χρησιμοποιεί το σύστημα για σκοπούς τιμολόγησης, να επιτραπεί η πρόσβαση μόνο στους εξουσιοδοτημένους χρήστες και να αποτραπούν οι εισβολείς να αναλάβουν τη σύνδεση.

Επιπλέον, η προστασία των σημάτων σηματοδοσίας εφαρμόζεται με σκοπό να προστατευθούν τα ευαίσθητα στοιχεία του που αφορούν στο χρήστη και μεταδίδονται πάνω από το ασύρματο δίκτυο πρόσβασης.

Τα αναλογικά κυψελοειδή συστήματα πρώτης γενεάς σχεδιάστηκαν με τα ελάχιστα χαρακτηριστικά γνωρίσματα ασφάλειας και η ανεπάρκεια τους σε αυτόν τον τομέα έγινε γρήγορα αισθητή.

Συνεπώς, ένας από τους στόχους κατά την ανάπτυξη των συστημάτων δεύτερης γενεάς (GSM) ήταν η παροχή ικανοποιητικής ασφάλειας. Μηχανισμοί όπως η εμπιστευτικότητα της ταυτότητας του χρήστη, η αυθεντικοποίηση των χρηστών και η κρυπτογράφηση των σημάτων σηματοδοσίας εισήχθησαν, οι οποίες εφαρμόστηκαν με την χρήση ισχυρών αλγορίθμων. Εντούτοις, το κύριο μειονέκτημα της παρεχόμενης ασφά-

Ασφάλεια και διαχείριση κλειδιών στο UMTS

λειας ήταν το γεγονός ότι όλες οι σημαντικοί παράμετροι ασφάλειας (δηλ. κλειδιά, αλγόριθμοι), διαβιβάζονταν πάνω από το ασύρματο δίκτυο πρόσβασης χωρίς προστασία. Επιπλέον, ένας κακόβουλος με τον κατάλληλο εξοπλισμό θα μπορούσαν να μεταμφιεσθεί ως πιθανό δίκτυο ή ως χρήστης και να πάρει σημαντικές πληροφορίες. Η χρήση ασυρμάτων μέσων μετάδοσης δημιουργεί διάφορες πιθανές απειλές που μπορούν να αξιοποιηθούν από έναν κακόβουλο για να κρυφακούσει τις μεταδόσεις. Είναι προφανές ότι, το πιο αδύνατο από πλευράς ασφαλείας μέρος του συστήματος είναι το ασύρματο τμήμα, καθώς αυτό μπορεί να υποκλαπεί εύκολα. Συνεπώς, η ασφάλεια δεν ήταν αποδοτική δεδομένου ότι υπήρχε δυνατότητα διασπασής της με διάφορους τρόπους.

Είναι σημαντικό επίσης να αναφερθεί ότι, ο κύριος στόχος της ασφάλειας του συστήματος GSM ήταν να καταστήσει το σύστημα τόσο ασφαλές όσο το δημόσιο τηλεφωνικό δίκτυο μεταγωγής κυκλώματος. Επομένως σε αυτήν την πτυχή το GSM όχι μόνο πέτυχε αλλά παρέχει ανώτερη ποιότητα ομιλίας και ποικίλες νέες ευκολίες και υπηρεσίες. Οι μηχανισμοί ασφάλειας που διευκρινίζονται στα πρότυπα GSM το καθιστούν το ασφαλέστερο διαθέσιμο κυψελοειδές σύστημα τηλεπικοινωνιών. Για όλους αυτούς τους λόγους το GSM θεωρείται ως το επιτυχέστερο κινητό δίκτυο στις ημέρες μας.

Το GPRS είναι αναμφισβήτητα ένα πολύ σημαντικό βήμα προς την εξέλιξη για τα κινητά δίκτυα τρίτης γενεάς. Είναι βασισμένο σε κυκλοφορία μεταγωγής πακέτων και έτσι μπορεί να παρέχει υπηρεσίες διαδικτύου. Λίγο πολύ, το GPRS χρησιμοποιεί παρόμοιες τεχνολογίες ασφάλειας με το δίκτυο GSM. Όμως, τα ασφαλή πακέτα δεδομένων δεν φθάνουν μόνο ως το BTS, αλλά προχωρούν ως το BSC, συν το γεγονός ότι ένας νέος αλγόριθμος A5 κρυπτογραφεί την κίνηση δεδομένων. Το GPRS αναμφισβήτητα είναι ασφαλέστερο δίκτυο από το GSM. Οι απειλές στο δίκτυο GPRS είναι πολύ διαφορετικές από το σύστημα μεταγωγής κυκλώματος GSM. Το σύστημα GPRS είναι πολύ περισσότερο εκτεθιμένο στους εισβολείς, λόγω του ότι βασίζεται στο IP.

Τα τρίτης γενιάς κυψελοειδή συστήματα είναι βασισμένα στην επιτυχία των δικύων GSM/GPRS και εισάγουν νέα και ενισχυμένα χαρακτηριστικά γνωρίσματα ασφάλειας, προκειμένου να βελτιωθεί η ασφάλεια και να προστατευθούν οι νέες υπηρεσίες, που δεν μπορούν να καλυφθούν από τα κινητά συστήματα δεύτερης γενεάς. Τα δεδομένα που διαβιβάζει ο χρήστης πάνω από το ασύρματο δίκτυο πρόσβασης προστατεύονται από εμπιστευτικότητα (κρυπτογραφούνται).

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Η σημαντικότερη βελτίωση ασφάλειας είναι ότι, όχι μόνο ο συνδρομητής πρέπει να αυθεντικοποιείται από το δίκτυο εξυπηρέτησης SN, μέσω ενός πρωτοκόλλου πρόκλησης απάντησης αλλά και το δίκτυο εξυπηρέτησης SN πρέπει να αυθεντικοποιηθεί από τον κινητό σταθμό του χρήστη, μέσω ενός μηχανισμού αριθμών ακολουθίας (sequence number). Το σημαντικότερο νέο συστατικό από άποψη ασφαλείας όμως, είναι η προσθήκη του μυστικού κλειδιού K που μοιράζεται ο κινητός σταθμός (η κάρτας USIM του χρήστη) και το πατρικό δίκτυο, χωρίς να μεταφέρεται ποτέ έξω από αυτές τις δύο θέσεις. Επιπλέον, άλλοι σημαντικοί παράμετροι ασφάλειας μεταφέρονται κρυπτοκαλυμμένες πάνω από το ασύρματο δίκτυο πρόσβασης και επομένως δεν μπορούν να υποκλαπούν.

Ο μηχανισμός αυθεντικοποίησης εκτελείται παράγοντας ένα διάνυσμα αυθεντικοποίησης, σαν αποτέλεσμα μονόδρομων συναρτήσεων. Αυτό σημαίνει ότι εάν το διάνυσμα αυθεντικοποίησης είναι γνωστό, δεν είναι δυνατό να εξαχθούν οι παράμετροι εισόδου. Ο μηχανισμός επίσης παρέχει ανταλλαγή των κλειδιών κρυπτογράφησης CK και ακεραιότητας IK μήκους 128 bits έτσι ώστε να είναι δύσκολο να σπάσει.

Επιπλέον, το IPSEC βελτιώνει την ασφάλεια στο επίπεδο ελέγχου (U-plane) για το IP τμήμα του κυρίως δικτύου, με την χρήση του ESP IPSEC σε tunnel mode. Αντίστοιχα το MAPSEC προστατεύει τη σηματοδοσία για το τμήμα του κυρίως δίκτυου που βασίζεται στην μεταγωγή κυκλώματος. Έτσι λοιπόν όλοι αυτοί οι μηχανισμοί κάνουν την ασφάλεια του UMTS να δείχνει αρκετά βελτιωμένη, έναντι των 2G συστημάτων. Εδώ πρέπει να σημειωθεί ότι η ασφάλεια στο κυρίως δίκτυο έχει να κάνει μόνο τα δεδομένα του, (control plane), και όχι του χρήστη (user plane).

Για την αμοιβαία αυθεντικοποίηση των περιοχών ασφαλείας, που συνήθως ταυτίζονται με τα όρια διαφορετικών δικτύων, που πρέπει να διασχίσουν τα δεδομένα ελέγχου από το πατρικό δίκτυο έως το δίκτυο εξυπηρέτησης, δημιουργήθηκε ένας γενικός μηχανισμός ανταλλαγής πιστοποιητικών μεταξύ τους.

Επίσης για τη μεταφορά πολυμέσων, που είναι ένα από τους κύριους λόγους για τους οποίους αναπτύχθηκαν τα 3G συστήματα, υπάρχει το IP Multimedia subsystem (IMS). Τοποθετημένο πάνω από το IP τμήμα του κυρίως δικτύου χρησιμοποιεί τους ίδιους μηχανισμούς ασφαλείας με αυτό κατά την μεταφορά των δεδομένων σηματοδοσίας του δικτύου. Κατά το πρώτο βήμα όμως της επικοινωνίας του χρήστη το IMS, δηλαδή με το P-CSCF, έχει υιοθετηθεί ο ίδιος μηχανισμός αυθεντικοποίησης με το UMTS

Ασφάλεια και διαχείριση κλειδιών στο UMTS

AKA. Απαιτείται δηλαδή η χρήση του πρωτοκόλλου 2 φορές, την μία σαν UMTS AKA για την πρόσβαση του κινητού σταθμού στο δίκτυο UMTS και την δεύτερη σαν IMS AKA για την πρόσβαση στις υπηρεσίες του IMS.

Παρ’ολούς τους μηχανισμούς ασφαλείας, υπάρχουν ακόμη σημαντικά προβλήματα στην ασφάλεια των συστημάτων UMTS που τα καθιστά τρωτά σε διαφόρων τύπων επιθέσεις. Τα προβλήματα αναφέρονται στο κεφάλαιο 7.

Δηλαδή: α) Το πατρικό δίκτυο (HLR/Auc) εμπιστεύεται το δίκτυο εξυπηρέτησης (VLR/SGSN) χωρίς να εξετάσει αν τα δεδομένα που του αποστέλλει είναι έγκυρα ή όχι. β) Τα διανύσματα αυθεντικοποίησης μεταφέρονται από το πατρικό δίκτυο στο δίκτυο εξυπηρέτησης μέσω πολλών ενδιάμεσων δικτύων που αυτό αποτελεί μία εν δυνάμει αδυναμία, γ) Το κλειδί ακεραιότητας εκπέμπεται χωρίς κρυπτοκάλυψη. δ) Τα δεδομένα του χρήστη δεν κρυπτοκαλύπτονται, καθώς μέσα στο κύριο δίκτυο δεν υπάρχει τέτοια πρόβλεψη, ενώ στο δίκτυο ασύρματης πρόσβασης, η κρυπτοκάλυψη των δεδομένων του χρήστη δεν είναι υποχρεωτική. ε) Τα δεδομένα του χρήστη δεν καλύπτονται από μηχανισμούς προστασίας ακεραιότητας. στ) Η χρήση και διαχείριση αριθμών ακολουθίας κατά την διαδικασία AKA παρουσιάζει μερικές αδυναμίες που θα μπορούσαν να δημιουργήσουν σημαντικά προβλήματα. ζ) Επίσης το UMTS AKA είναι ευάλωτο σε μία σειρά επιθέσεων ψεύτικων σταθμών βάσης. Αυτή η ευπάθεια επιτρέπει σε έναν κακόβουλο να ανακατευθύνει την κυκλοφορία των χρηστών από ένα δίκτυο σε άλλο και να επαναχρησιμοποιήσει αλλοιωμένα διανυσμάτα επικύρωσης από ένα δίκτυο σε όλα τα άλλα δίκτυα. η) Η ταυτότητα και η θέση του κινητού χρήστη εκπέμπονται χωρίς κανένα μηχανισμό ασφαλείας πάνω από το ασύρματο δίκτυο, ενώ είναι πολύτιμες πληροφορίες που απαιτούν προστασία.

Επίσης οι μηχανισμοί ασφαλείας του UMTS μια σειρά από προβλήματα απόδοσης:

α)Κατανάλωση εύρους ζώνης μεταξύ SN και HN, β) Καθυστέρηση αυθεντικοποίησης του κινητού σταθμού λόγω απόστασης, γ)κατανάλωση αποθηκευτικού χώρου για τα διανύσματα αυθεντικοποίησης, δ) εκτέλεση για δεύτερη φορά του UMTS AKA στην περίπτωση σύνδεσης του κινητού σταθμού με το IMS.

Για την αντιμετώπιση κάποιων από αυτά τα προβλήματα έχουν προταθεί τόσο νέα πρωτόκολλα AKA όσο και μηχανισμοί που βελτιώνουν τα προβλήματα απόδοσης.

Ασφάλεια και διαχείριση κλειδιών στο UMTS

Χρειάζεται λοιπόν να γίνει δουλειά ακόμη προ αυτή την κατεύθυνση, για την υιοθέτηση ενός πρωτοκόλλου AKA που να αντιμετωπίζει τα παραπάνω προβλήματα, λαμβάνοντας υπόψη τις χαμηλές υπολογιστικές δυνατότητες των κινητών σταθμών αλλά και το ότι τροφοδοτούνται από συσσωρευτές, (μπαταρίες) φροντίζοντας οι μηχανισμοί του να μην είναι ενεργοβόροι. Επιπλέον ίσως ένα νέο πρωτόκολλο AKA για το IMS πρέπει να υιοθετηθεί, που θα εκμεταλλεύεται αποδοτικότερα το UMTS AKA, και δεν θα απαιτεί την ανταλλαγή τόσο μεγάλου πλήθους μηνυμάτων.

Τέλος, ο σκοπός για τα συστήματα 3^{ης} γενιάς είναι να προσφέρουν τις υπηρεσίες τους στους χρήστες που εισέρχονται στο δίκτυό τους με οποιοδήποτε τρόπο πρόσβασης. Σε αυτά τα πλαίσια, βρίσκεται σε εξέλιξη ο συνδυασμός των ασύρματων και κινητών δίκτυων. Η πρόσβαση δηλαδή στο κεντρικό δίκτυο UMTS από κάποιο ασύρματο δίκτυο Wi Fi. Τα δίκτυα Wi Fi προσφέρουν μεγαλύτερους ρυθμούς μετάδοσης και άρα εκμεταλλεύονται με τον καλύτερο τρόπο τις υπηρεσίες που παρέχονται από το δίκτυο. Αυτή η διαλειτουργικότητα είναι σημαντική και έχει αρχίσει να συγκεντρώσει το ενδιαφέρον πολλών ερευνητών. Ένα νέο πρωτόκολλο AKA απαιτείται γι' αυτή την διαλειτουργικότητα που να συνδυάζει τις 2 τεχνολογίες και να ενσωματώνει τέτοιους μηχανισμούς ώστε αυτή η διαλειτουργικότητα να είναι ασφαλής για τον νόμιμο χρήστη του δικτύου, αντλώντας εμπειρία από την ως τώρα προσπάθεια για το UMTS. Ο συνδυασμός αυτός έχει ακόμη πολλά τεχνικά προβλήματα να λύσει από πλευράς ασφάλειας και χρειάζεται ακόμη πολλή δουλειά. Αξίζει όμως ιδιαίτερης προσπάθειας και προσοχής καθώς αποτελεί πολύ σημαντικό βήμα προκειμένου να επιτευχθεί ένα ενοποιημένο περιβάλλον υπηρεσιών προς τον τελικό χρήστη.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
BG	Border Gateway
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
CSCF	Call State Control Function
DES	Data Encryption Standard
Dol	Domain of Interpretation
ESP	Encapsulating Security Payload
FALLBACK	Fallback to unprotected mode indicator
GTP	GPRS Tunnelling Protocols
HE	Home Environment
HLR	Home Location Register
HSS	Home Subscriber Server
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange
IM	IP Multimedia
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	IP security - a collection of protocols and algorithms for IP security incl. key mgmt.
ISAKMP	Internet Security Association Key Management Protocol
IV	Initialisation Vector
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	Message Authentication Code

Ασφάλεια και διαχείριση κλειδιών στο UMTS

MAC-M	MAC used for MAP
MAP	Mobile Application Part
MAP-NE	MAP Network Element
MAPsec	MAP security – the MAP security protocol suite
ME	Mobile Equipment
MEA	MAP Encryption Algorithm identifier
MEK	MAP Encryption Key
MIA	MAP Integrity Algorithm identifier
MIK	MAP Integrity Key
MS	Mobile Station
MSC	Mobile Services Switching Centre
NAT	Network Address Translator
NDS	Network Domain Security
NDS/IP	NDS for IP based protocols
NE	Network Entity
PPI	Protection Profile Indicator
PPRI	Protection Profile Revision Identifier
PROP	Proprietary field
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SA	Security Association
SAD	Security Association Database (sometimes also referred to as SADB)
SADB	Security Association DataBase (also referred to as SAD)
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SIP	Session Initiation Protocol
SN	Serving Network
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
SQN	Sequence number
SQNHE	Individual sequence number for each user maintained in the HLR/AuC
SQNMS	The highest sequence number the USIM has accepted
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
TrGW	Transition Gateway
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
XRES	Expected Response

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1]. 3GPP TS 23.101 V6.0.0 (2004-12) Technical Specification Universal Mobile Telecommunications System (UMTS); General UMTS Architectue (Release 6).
- [2]. 3GPP TS 21.133 V6.0.0 (2004-12) Technical Specification Universal Mobile Telecommunications System (UMTS); Security threats and requirements (Release 6).
- [3]. 3GPP TS 33.102 V6.5.0 (2005-12) Technical Specification Universal Mobile Telecommunications System (UMTS) 3GSecurity; Security architecture (Release 6).
- [4]. 3GPP TS 33.200 V6.1.0 (2005-03) Technical Specification Universal Mobile Telecommunications System (UMTS); 3GSecurity; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security (Release 6).
- [5]. 3GPP TS 33.203 V6.9.0 (2005-12) Digital Mobile Telecommunications System (Phase 2+); Technical Specification Universal Mobile Telecommunications System (UMTS); 3GSecurity; Access Security for IP-based services (Release 6).
- [6]. 3GPP TS 33.210 V6.5.0 (2004-06) Technical Specification Digital Mobile Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3GSecurity; Network Domain Security (NDS); IP network layer security (Release 6).
- [7]. 3GPP TS 33.310 V6.2.0 (2004-09) Technical Specification Universal Mobile Telecommunications System (UMTS); Network Domain Security; Authentication framework (NDS/AF); (Release 6).
- [8]. Christos Xenakis, Lazaros Merakos "Security in third Generation Mobile Networks", Computer Communications 27 (2004) 638-650.



Ασφάλεια και διαχείριση κλειδιών στο UMTS

-
- [9]. Christos Xenakis, Lazaros Merakos "Security Standardization and Services in UMTS"
- [10]. Muxiang Zhang, Yuguang Fang "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", IEEE transactions on wireless communications, Vol. 4, No. 2, March 2005.
- [11]. Zhipeng Liu "Security in 3G Wireless Networks."
- [12]. Ulrike Meyer, Susanne Wetzel "A Man-in-the-Middle Attack on UMTS" Wise 04, October 1 2004, Philadelphia, Pennsylvania, USA.
- [13]. Chung-Ming Huang, Jian-Wei Li "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption" Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA 05).
- [14]. Geir M. Køien "Privacy Enhanced Cellular Access Security", Wise'05, September 2, 2005, Cologne, Germany.
- [15]. Geir M. Køien, Telenor R&D and Agder University College "An Introduction to Access Security in UMTS". IEEE Wireless Communications, February 2004.
- [16]. K Boman, G. Horn, P. Howard, V. Niemi, "UMTS security" Electronics & Communication Engineering Journal, October 2002.
- [17]. David Amizade, "GPRS/UMTS Security Threats- New Vistas for Old Attacks" 3rd International Workshop in wireless security technologies, Proceedings 4-5 April 2005, London UK.



- [18]. Konstantinos S. Saninas (+), George C. Polyzos "Evaluating and Comparing Privacy and Anonymity of Mobile Network Authentication Schemes" 3rd International Workshop in wireless security technologies, Proceedings 4-5 April 2005, London UK.
- [19]. Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos Venieris "Introduction of the Assymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration" Mobile Networks and Applications 8, 145-150, 2003.
- [20]. Christos Xenakis, Lazaros Merakos "Alternative Schemes for Dynamic Secure VPN Deployments in UMTS" Wireless Personal Communications (2006) 36: 163-194.
- [21]. Georgios Kambourakis, Angelos Rouskas, Stefanos Gritzalis "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems", EURASIP Journal on wireless Communications and Networking 2004:1, 184-197
- [22]. Michel Borreau, Jean-Marc Robert "Perfect Identity Concealment in UMTS over Radio Access Links" IEEE 2005.
- [23]. Ioannis Doukas "Security Technologies for Mobile Radio Systems" Report as a part of the MSc Degree in CCDSP at the University of Strathclyde.
- [24]. Yi-Bing Lin, Yuan-Kai Chen "Reducing Authentication Signalling Traffic in Third-Generation Mobile Network" IEEE Transactions on Wireless Communications, Vol. 2, No 3, May 2003.
- [25]. Yan Zhang, Masayaki Fusise "Security Management in the Next Generation Wireless Networks" International Journal of Network Security, Vol. 3, No. 1, PP. 1-7, July 2006.



-
- [26]. Shu-Min Cheng, Shiuhyung Shieh, Wen-Her Yang "Designing Authentication Protocols for Third Generation Mobile Communication Systems" Journal of Information science and Engineering 21, 361-378 (2005).
- [27]. Lein Harn, Wen-Jung Hsin "On the Security of Wireless Network Access with Enhancements" Wise'03, September 19, 2003, San Diego, California, USA.
- [28]. Stefen Putz, Roland Schmitz, Tobias Martin "Security Mechanisms in UMTS" DuD Datenschutz und Datensicherheit 25 (2001)
- [29]. Wie Liang, Weyne Wang "A Lightweight Authentication Protocol with Local Security Association Control in Mobile Networks" Department of Electrical Engineering and Computer Engineering North Carolina State University.
- [30]. Muhammad Sher, Thomas Magedanz " Secure Service Provisioning Framework (SSFP) for IP Multimedia Systems and Next Generation Mobile Networks" 3rd International Workshop in wireless security technologies, Proceedings 4-5 April 2005, London UK.
- [31]. Muhammad Sher, Thomas Magedanz, Walter T. Penzhorn "Inter- Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)" Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06).
- [32]. Yi-Bing Lin, Meng-Ta Hsu, Lin-Yi Wu "One-Pass GPRS and IMS Authentication Procedure for UMTS" IEEE Journal on Selected Areas in Communications, Vol 23. No 6, June 2005.
- [33]. Vassilios Koukolidis, Mehul Shah "The IP Multimedia Domain in Wireless Networks: Concepts, Architecture, Protocols and Applications" Proceedings of the IEEE 6th International Symposium on Multimedia Software Engineering (IMSE'04).

-
- [34]. George Xylomenos, Vasilis Vogkas "Wireless Multimedia in 3G networks" Mobile Multimedia Laboratory Department of Informatics Athens University of Economics and Business Patision 76, Athens 104 34, Greece.
- [35]. ASPeCT Project, Securing the future of mobile communications, 1999, <http://www.esat.kuleuven.ac.be/cosic/aspect>.
- [36]. USECA Project, "UMTS security architecture: Intermediate report on a PKI architecture for UMTS," Public Report, July 1999.
- [37]. eNorge 2005, Naerings – og handelsdepartementet, 2002.
- [38]. Σπύρος Παπαγεωργίου "Ασφάλεια στη Ασύρματη Πολυεκπομπή" Διπλωματική εργασία, Μεταπτυχιακό Δίπλωμα Ειδίκευσης στη "Επιστήμη των Υπολογιστών", Οικονομικό Πανεπιστήμιο Αθηνών Τμήμα Πληροφορικής, 2005.
- [39]. Ιγγλέσης Ευάγγελος "Μετάδοση Δεδομένων σε Κινητά Δίκτυα Επικοινωνιών 3ης Γενιάς", Διπλωματική Εργασία, Μεταπτυχιακό Δίπλωμα Ειδίκευσης (ΜΔΕ)"Επιστήμη και Τεχνολογία των Υπολογιστών ", Τμήμα Μηχανικών Η/Υ και Πληροφορικής Πολυτεχνικής Σχολής Πατρών 2005.
- [40]. Σούρσος Σέργιος "Προσαρμογή και χρέωση των Διαφοροποιημένων Υπηρεσιών του Διαδικτύου στο GPRS περιβάλλον", Διπλωματική εργασία, Μεταπτυχιακό Δίπλωμα Ειδίκευσης στα "Πληροφοριακά Συστήματα", Οικονομικό Πανεπιστήμιο Αθηνών Τμήμα Πληροφορικής, 2001.
- [41]. Min-Shiang Hwang "A Study of Security in Global Mobility Networks" Master Thesis, Graduate Institute of Networking and Communication Engineering Chao Yang University of Technology.
- [42]. K. Nyberg, V. Niemi. "UMTS Security". Wiley, 2003.

[43]. Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siama k Naghian, Valtteri Niemi, "UMTS Networks Architecture, Mobility and Services", Second Edition, Wiley 2005.

[44]. Σ.Κ.Κάτσικας, Σ. Γκρίτζαλης, και Δ. Γκρίτζαλης, "Ασφάλεια Πληροφοριακών Συστημάτων", Εκδόσεις Νέων Τεχνολογιών,2004.

[45]. A.Menezes, P van Oorschot, and S.Vastone, "Handbook of Applied Cryptography", CRC Press,1996

