ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Ιωάννης Κ. Μαυρίδης

Επίκουρος Καθηγητής
Τμήμα Εφαρμοσμένης Πληροφορικής
Πανεπιστήμιο Μακεδονίας
mavridis@uom.gr

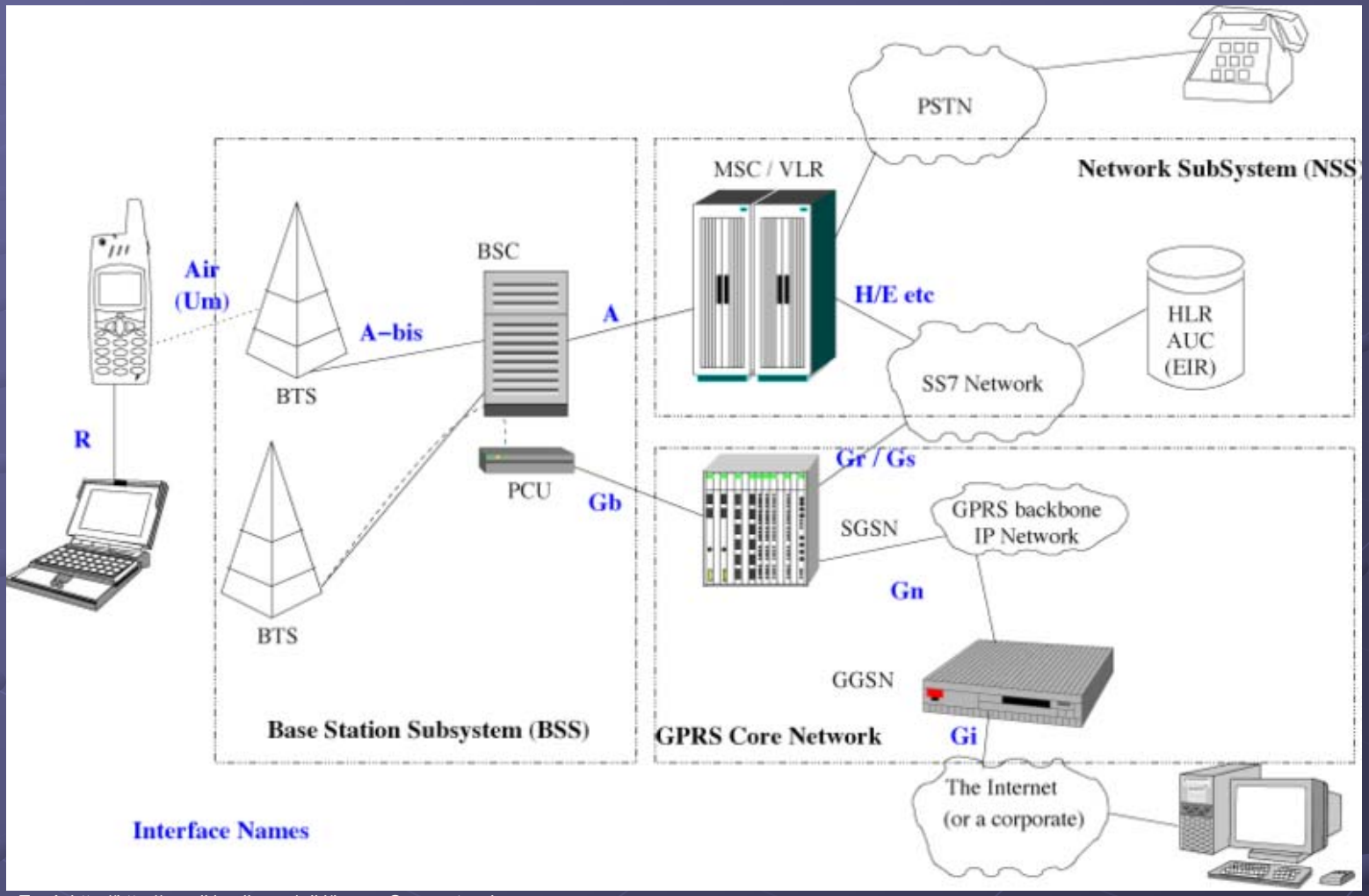
Ασφάλεια Δημοσίων Δικτύων Κινητών Επικοινωνιών (PLMN)

- Εμπιστευτικότητα (confidentiality) δεδομένων
- Αυθεντικοποίηση (authentication) οντοτήτων
- Ακεραιότητα (integrity) δεδομένων
- Έλεγχος πρόσβασης (access control)
- Διαθεσιμότητα (availability)

Κινητή Τηλεφωνία 1ης Γενιάς (1G)

- Ιδιαίτερα ανασφαλείς αναλογικές συσκευές
- Κλωνοποίηση (cloning):
  - αποστολή της ταυτότητας μέσω της ασύρματης σύνδεσης χωρίς κρυπτογράφηση
  - εύκολη υποκλοπή της ταυτότητας
  - ρύθμιση της συσκευής του εισβολέα
  - χρέωση όλων των κλήσεων στο λογαριασμό του θύματος
- Κρυφάκουσμα (eavesdropping)
  - με απλό συντονισμό ενός απλού ραδιοδέκτη

Κινητή Τηλεφωνία 2ης Γενιάς (2G)



Πηγή: http://http://en.wikipedia.org/wiki/Image:Gsm_network.png

- Δομή GSM

Απαιτήσεις ασφάλειας GSM

- Εμπιστευτικότητα (confidentiality)
  - προστασία δεδομένων στην ασύρματη σύνδεση
- Ανωνυμία (anonymity)
  - προστασία από καταγραφές της θέσης χρήστη ή της ταυτότητας των κλήσεων από και προς το χρήστη
- Αυθεντικοποίηση (authentication)
  - επιβεβαίωση της ταυτότητας συνδρομητή από το δίκτυο
- Έλεγχος πρόσβασης (access control)
  - στη βάση των ταυτοτήτων
    - συνδρομητή (IMSI)
    - συσκευής (IMEI)

Υπηρεσίες ασφάλειας GSM

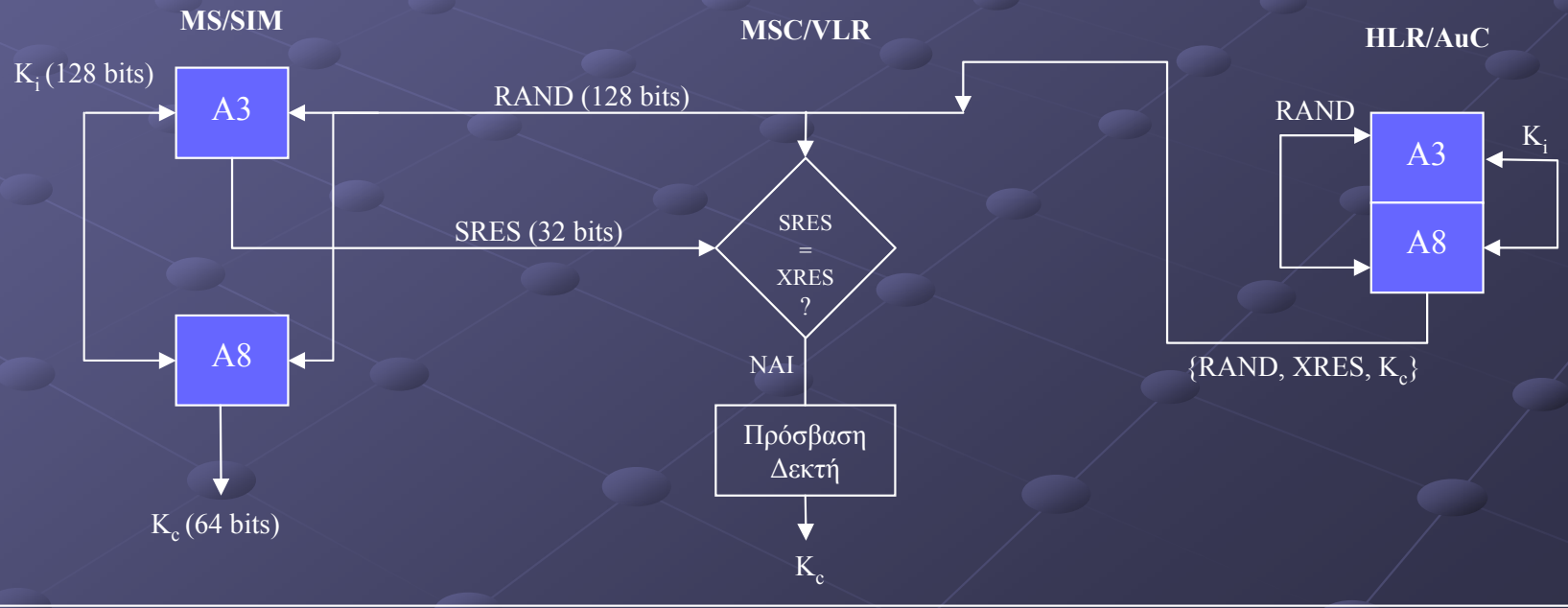
- Εμπιστευτικότητα ταυτότητας χρήστη
- Αυθεντικοποίηση και συμφωνία κλειδιών
- Κρυπτογράφηση διακινούμενων δεδομένων
- Κάρτα SIM ως βασικό τμήμα ασφάλειας
- Έλεγχος ταυτότητας συσκευής

Εμπιστευτικότητα ταυτότητας χρήστη

- Προστασία από αποκάλυψη της ταυτότητας του συνδρομητή σε τρίτα μέρη
  - Χρήση προσωρινών (TMSI) αντί της μόνιμης ταυτότητας του συνδρομητή (IMSI)
  - Αντιστοιχία TMSI και IMSI
  - Δημιουργία νέου TMSI μετά από αλλαγή θέσης
- Αποστολή του IMSI μόνον όταν:
  - ο συνδρομητής συνδέεται για πρώτη φορά στο δίκτυο
  - υπάρχουν προβλήματα επικοινωνίας ή λειτουργίας του δικτύου

Αυθεντικοποίηση και συμφωνία κλειδιών

- Μυστικό κλειδί συνδρομητή: K_i
- Αυθεντικοποίηση: A3 (SRES = XRES)
  - challenge (RAND) – response (SRES)
- Παραγωγή κλειδιού K_c : A8



Κρυπτογράφηση δεδομένων

- Εμπιστευτικότητα διακινούμενων δεδομένων στην ασύρματη σύνδεση (MS - BTS)

Κάρτα SIM ως βασικό τμήμα ασφάλειας

- Ασφαλής αποθήκευση του K_i
- Υπολογίζει τα SRES και K_c
- Έλεγχος πρόσβασης μέσω PIN και PUK

Έλεγχος ταυτότητας της συσκευής

- IMEI (International Mobile Equipment Identity)
- Έλεγχος για κάθε αίτημα πρόσβασης στο δίκτυο

Ευπάθειες GSM

- Αυθεντικοποίηση της ταυτότητας χρήστη
- Αλγόριθμοι αυθεντικοποίησης (COMP128) και κρυπτογράφησης (A5)
- Το δίκτυο δεν αυθεντικοποιείται στο χρήστη
- Περιορισμένη ασφάλεια της κάρτας SIM
- Περιορισμός της κρυπτογράφησης στην ασύρματη σύνδεση
- Επανειλημμένη χρήση τριπλετών ασφαλείας

Ευπάθειες κατά την αυθεντικοποίηση χρήστη

- Αποστολή IMSI χωρίς κρυπτογράφηση
- Κρυφάκουσμα του IMSI, σε περίπτωση αποστολής του λόγω:
  - ανανέωσης θέσης σε νέο VLR και
    - το παλιό VLR δεν είναι προσβάσιμο
    - το παλιό VLR έχει υποστεί απώλεια δεδομένων
  - απώλειας δεδομένων σε VLR (TMSI άγνωστο)
- Επιπτώσεις
  - Προσποίηση νόμιμου χρήστη (masquerading)
  - Εντοπισμός της θέσης χρήστη στο δίκτυο

Ευπάθειες COMP128

- COMP128 (A3/8)
  - Επιδιώχθηκε να μείνει μυστικός
    - security by obscurity
  - Ευάλωτος σε επιθέσεις
    - επιλεγμένου κειμένου (chosen challenge attack - Briceno,Goldberg,Wagner 1998)
    - πλευρικών καναλιών (side channel/partition attacks - IBM 2002)
  - Επίπτωση: κλωνοποίηση της SIM

Ευπάθειες A5

- Ευάλωτος σε επιθέσεις εξαντλητικής αναζήτησης
- Κρυπταναλυτικές επιθέσεις (Biryukov, Shamir, Wagner - 2000)
- Επίπτωση: εύρεση κλειδοροής

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

Πηγή: Alex Biryukov, Adi Shamir, David Wagner, "Real Time Cryptanalysis of A5/1on PC", http://cryptome.org/a5.ps

Το δίκτυο δεν αυθεντικοποιείται

- Επίπτωση: επίθεση Ενδιάμεσου (Man-in-the-middle attack) με ψεύτικο σταθμό βάσης που
  - προωθεί RAND και SRES
  - επιβάλλει ασθενή (A5/2) ή καθόλου κρυπτογράφηση
  - αν χρειαστεί, υπολογίζει το κλειδί K_c
  - καταγράφει το σύνολο της συνομιλίας

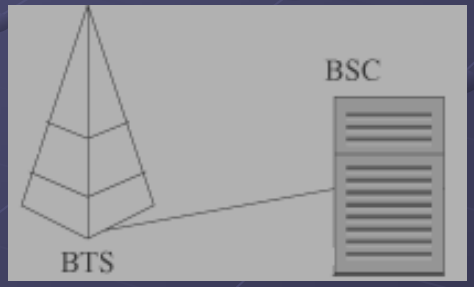
Ασφάλεια της κάρτας SIM

- Επιθέσεις
  - σε COMP128 (A3/8)
  - εισαγωγής οπτικών σφαλμάτων

  για εξαγωγή IMSI ή K_i
- Επιπτώσεις κλωνοποίησης της SIM:
  - Υποκλοπή συνομιλιών
  - Πραγματοποίηση κλήσεων με χρέωση του νόμιμου συνδρομητή

Η σύνδεση BTS - BSC δεν κρυπτογραφείται

- Επίπτωση: μεταφέρονται χωρίς προστασία (plaintext) τα:
  - δεδομένα της κλήσης
  - τα στοιχεία RAND και SRES
  - το κλειδί συνόδου K_c



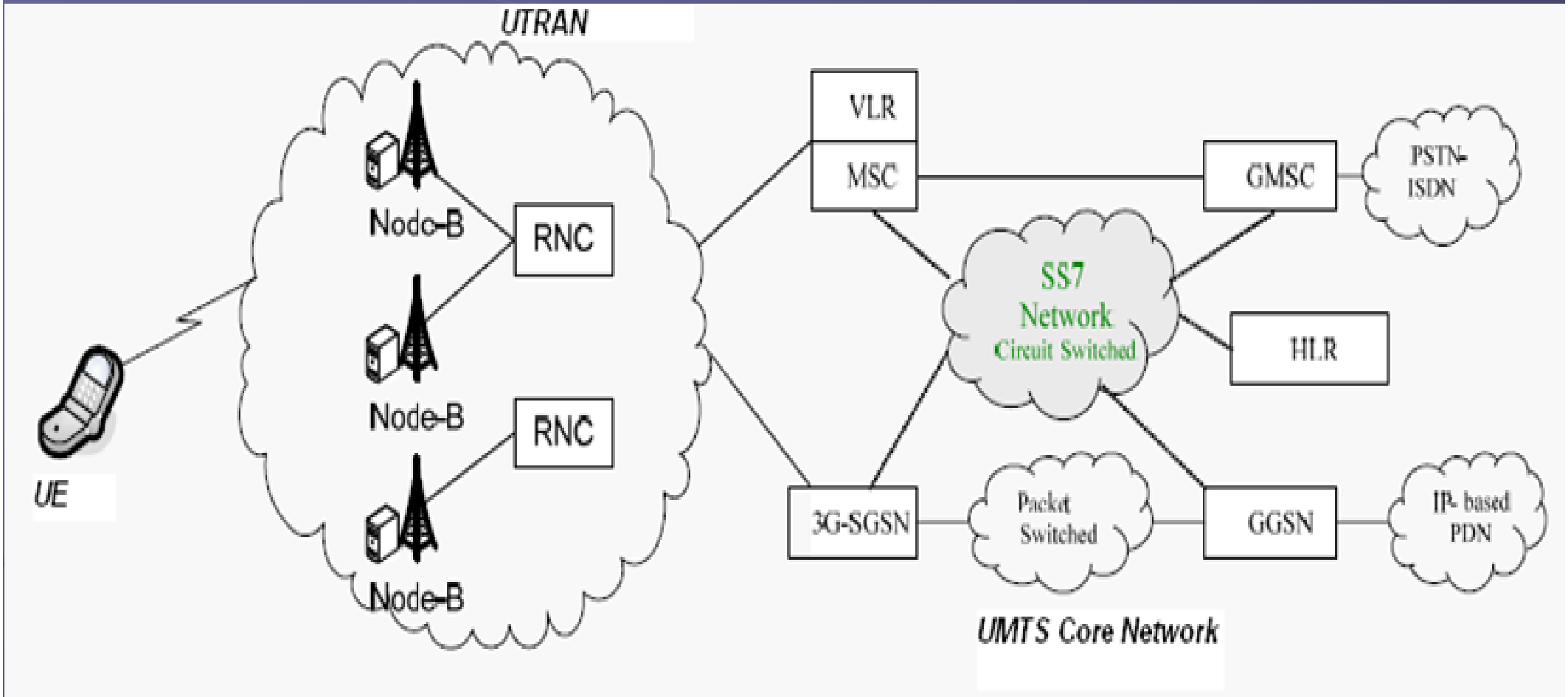
Επανειλημμένη χρήση τριπλετών ασφαλείας

- Δεν απαγορεύεται η επαναχρησιμοποίηση τριπλετών ασφαλείας {RAND, SRES, K_c}, όταν
  - υπάρχει πρόβλημα επικοινωνίας (VLR - HLR)
  - είναι διαθέσιμες μόνο χρησιμοποιημένες (HLR)
- Επίπτωση: υποκλοπή τριπλετών ασφάλειας και παρακολούθηση των συνομιλιών

Προβλήματα - Ελλείψεις

- Επιθέσεις Άρνησης Υπηρεσίας (DoS attacks)
- Έλλειψη μηχανισμών ασφάλειας για SMS
- Έλλειψη ενημέρωσης χρήστη για παρεχόμενους μηχανισμούς ασφάλειας (lack of visibility)
- Έλλειψη μηχανισμών ακεραιότητας δεδομένων (data integrity)
- Εκ των υστέρων μέριμνα για σύστημα νόμιμων συνακροάσεων (Lawful Interception)

Κινητή Τηλεφωνία 3ης Γενιάς (3G)



- Δομή UMTS (Release 99)

Υπηρεσίες Ασφάλειας UMTS

- Ασφάλεια δικτύου πρόσβασης
- Ασφάλεια πεδίου δικτύου
- Ασφάλεια πεδίου χρήστη
- Ασφάλεια πεδίου εφαρμογών
- Διαφάνεια και διαμόρφωση ασφάλειας

Ασφάλεια δικτύου πρόσβασης

- **Εμπιστευτικότητα ταυτότητας χρήστη** User Identification Confidentiality (UIC)
- **Αυθεντικοποίηση και συμφωνία κλειδιού** Authentication and Key Agreement (AKA)
- **Εμπιστευτικότητα δεδομένων** Data Confidentiality (DC)
- **Ακεραιότητα δεδομένων** Data Integrity (DI)

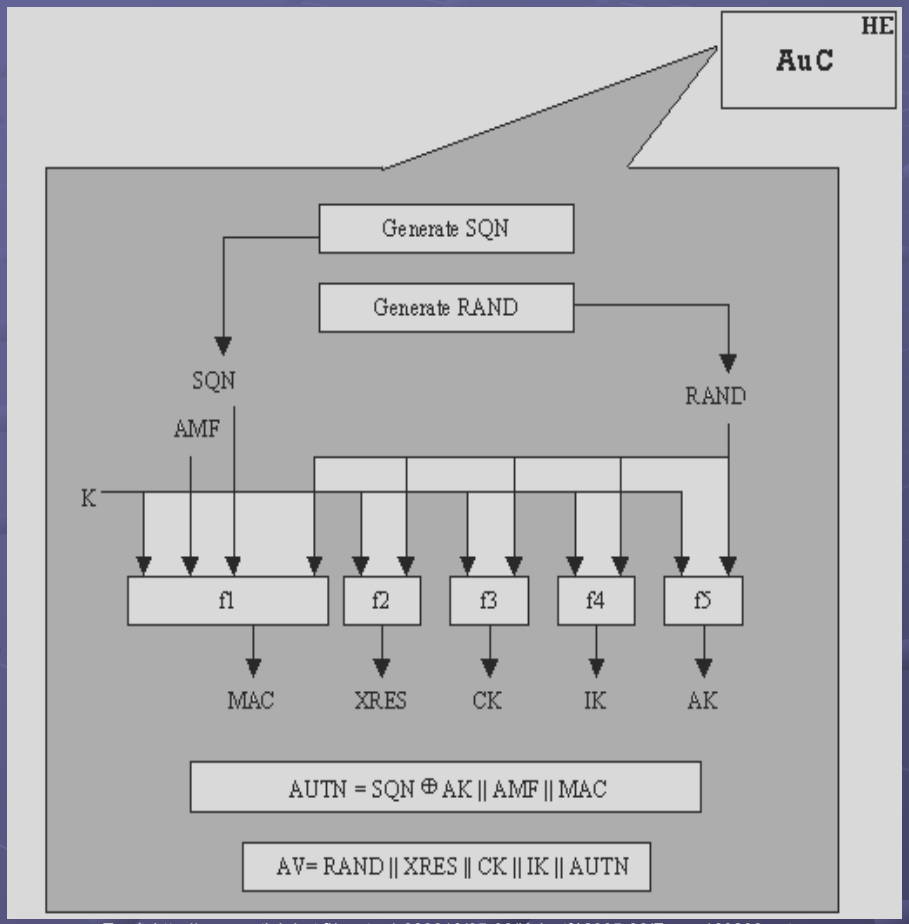
Ασφάλεια δικτύου πρόσβασης

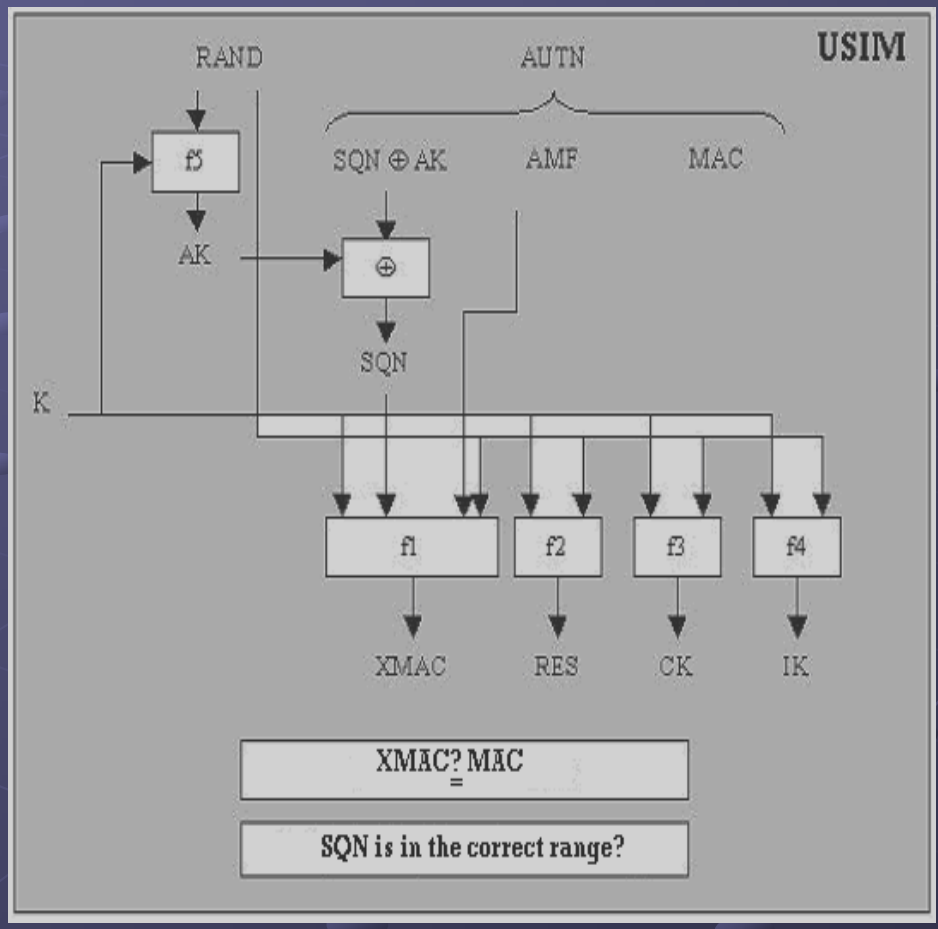
- Εμπιστευτικότητα ταυτότητας χρήστη
  - Χρήση προσωρινών ταυτοτήτων TMSI (CS) ή P-TMSI (PS)
  - Το IMSI αποστέλλεται
    - κατά την πρώτη σύνδεση
    - αν δεν είναι εφικτή η επικοινωνία παλιού-νέου VLR
  - Απόδοση TMSI μετά την έναρξη εφαρμογής κρυπτογράφησης

Ασφάλεια δικτύου πρόσβασης

- Αυθεντικοποίηση και Συμφωνία Κλειδιών
  - Αυθεντικοποίηση
    - δικτύου, f1: XMAC = MAC
    - κάρτας, f2: RES = XRES
  - Παραγωγή κλειδιών
    - κρυπτογράφησης, f3: CK
    - ακεραιότητας, f4: IK
    - ανωνυμίας, f5: AK

Ασφάλεια δικτύου πρόσβασης



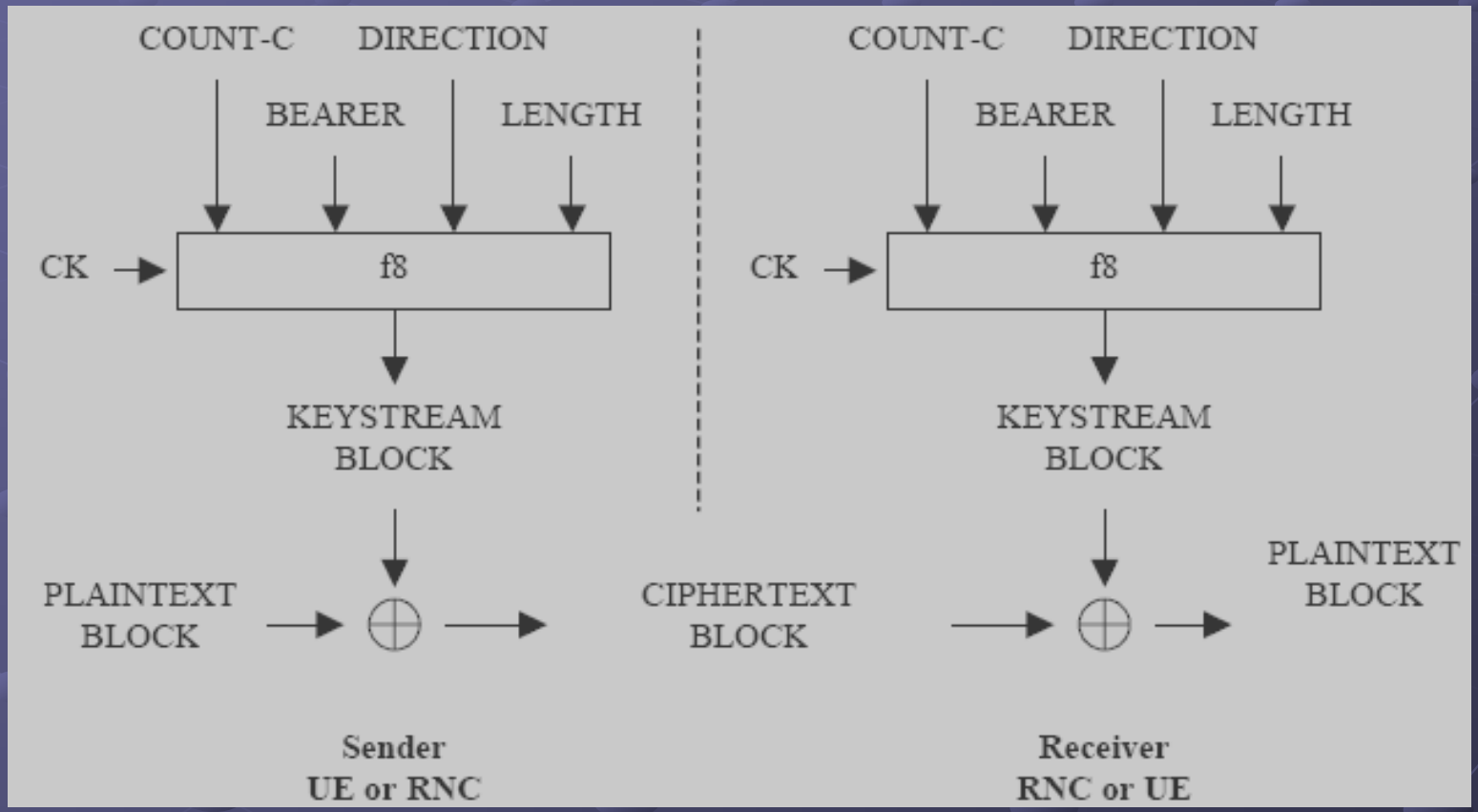


Πηγή: http://www.netlab.hut.fi/opetus/s383310/05-06/Kalvot%2005-06/Feng_160206.ppt

- Authentication and Key Agreement (AKA)

Ασφάλεια δικτύου πρόσβασης

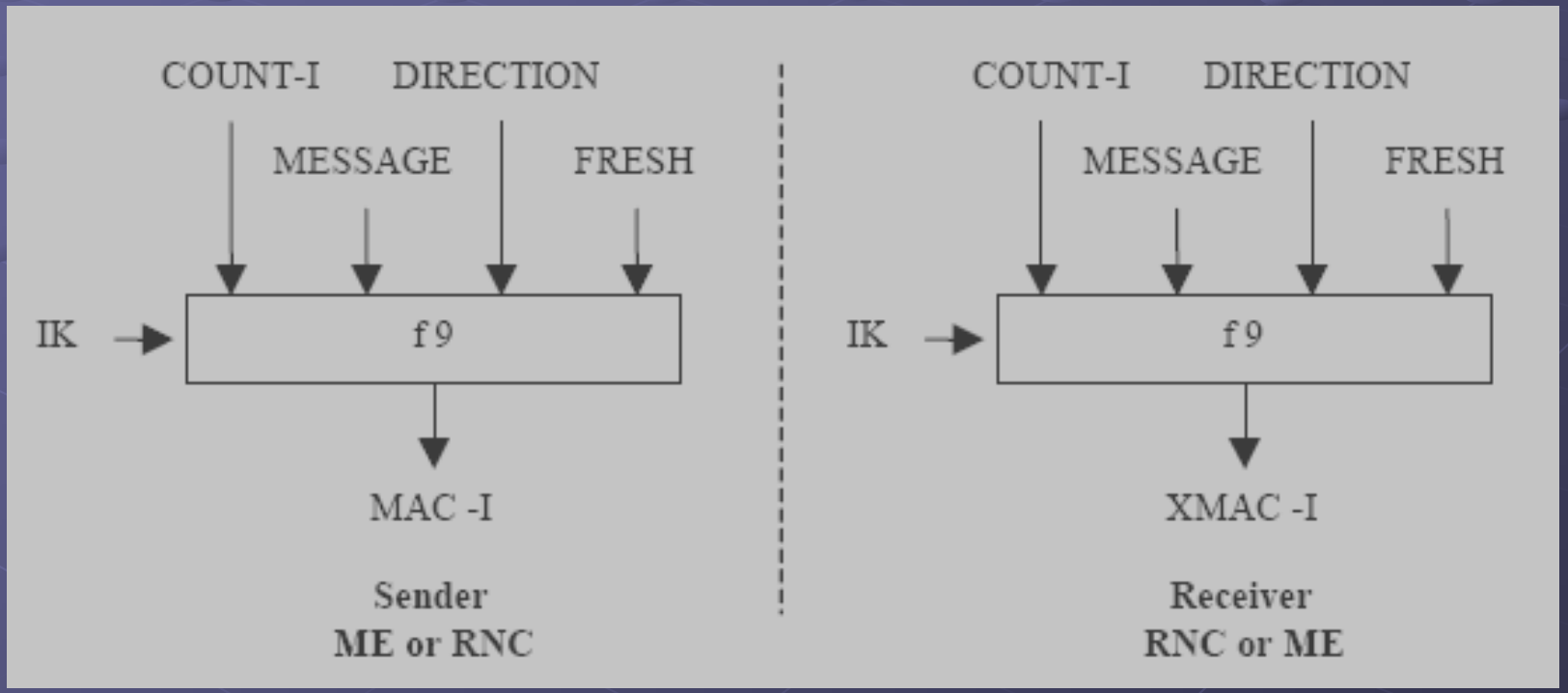
- Εμπιστευτικότητα δεδομένων χρήστη



Πηγή: 3GPP TS 35.201 (5.0.0)

Ασφάλεια δικτύου πρόσβασης

- Ακεραιότητα δεδομένων σηματοδοσίας



Πηγή: 3GPP TS 35.201 (5.0.0)

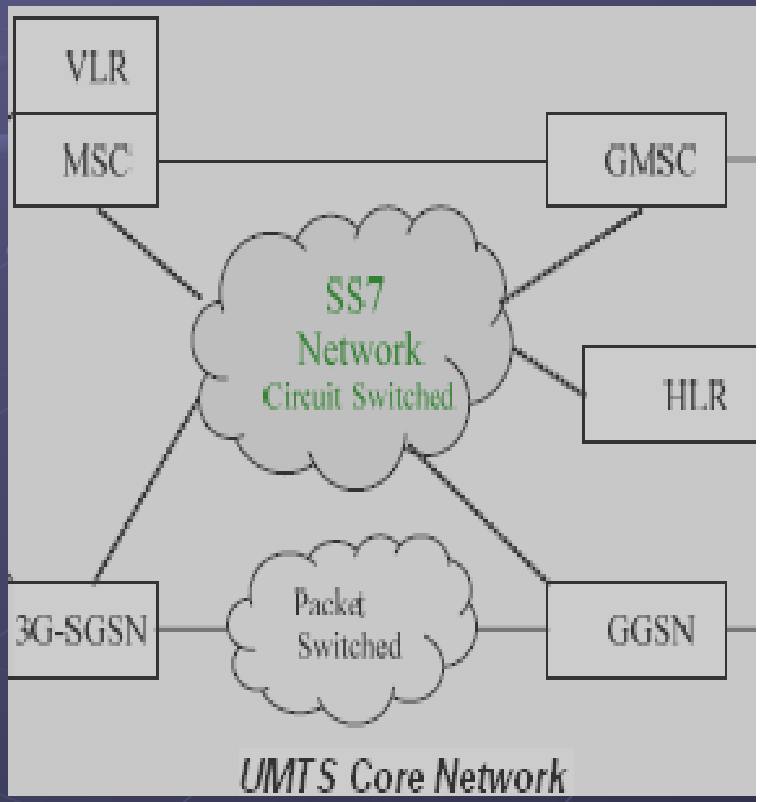
Ασφάλεια πεδίου δικτύου

- Circuit-Switched (CS) domain:

  MAP ⟶ MAPsec

- Packet-Switched (PS) domain:

  IP ⟶ IPsec



Ασφάλεια πεδίου δικτύου

- MAPsec
  - Παρέχει:
    - ακεραιότητα
    - αυθεντικοποίηση προέλευσης
    - προστασία επανάληψης
    - εμπιστευτικότητα
  - Καταστάσεις προστασίας:
    - Protection mode 0. Χωρίς προστασία
    - Protection mode 1. Ακεραιότητα
    - Protection mode 2. Εμπιστευτικότητα, ακεραιότητα

Ασφάλεια πεδίου δικτύου

- IPsec
  - Παρέχει
    - εμπιστευτικότητα (3DES)
    - ακεραιότητα (SHA-1)
    - μη απάρνηση
    - αυθεντικοποίηση προέλευσης
  - Πρωτόκολλο ESP σε tunnel mode
  - Ανταλλαγή κλειδιών με Internet Key Exchange (IKE)

Ασφάλεια πεδίου χρήστη

- Αυθεντικοποίηση χρήστη προς USIM
  - χρήση PIN
- Σύνδεση USIM με συσκευή
  - SIM-lock

Ασφάλεια πεδίου εφαρμογών

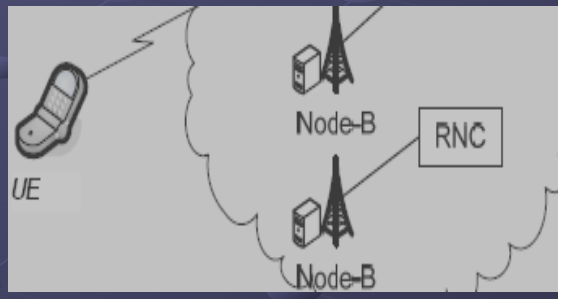
- αυθεντικοποίηση εφαρμογών
- αυθεντικοποίηση προέλευσης δεδομένων
- ακεραιότητα δεδομένων
- ανίχνευση επανάληψης δεδομένων
- ακεραιότητα αλληλουχίας δεδομένων
- απόδειξη παραλαβής
- εμπιστευτικότητα δεδομένων

Διαφάνεια και διαμόρφωση ασφάλειας

- Κατάλληλες ενδείξεις για:
  - εφαρμογή κρυπτογράφησης,
  - επίπεδο ασφάλειας του δικτύου (3G → 2G)
- Διαμόρφωση χαρακτηριστικών ασφάλειας:
  - ενεργοποίησης ή μη user – USIM αυθεντικοποίησης
  - αποδοχής ή μη εισερχόμενων κλήσεων χωρίς κρυπτογράφηση
  - δημιουργία κλήσεων με ή χωρίς κρυπτογράφηση
  - αποδοχή / απόρριψη αλγορίθμων κρυπτογράφησης

Διατήρηση και βελτίωση GSM υπηρεσιών ασφάλειας στο UMTS

- Αυθεντικοποίηση χρήστη στο δίκτυο
  - βελτίωση των μηχανισμών αυθεντικοποίησης
- Κρυπτογράφηση δεδομένων κίνησης και σηματοδοσίας στην ασύρματη σύνδεση
  - νέοι και δημοσιοποιημένοι αλγόριθμοι
  - επέκταση εφαρμογής μέχρι το RNC
  - μεγαλύτερο κλειδί (GSM: 64-bit, UMTS: 128-bit)



- Εμπιστευτικότητα ταυτότητας χρήστη στην ασύρματη σύνδεση
  - παρόμοια με το GSM
- Σύστημα Νόμιμων Συνακροάσεων (Lawful Interception)
  - καθορισμένο από τον αρχικό σχεδιασμό

Νέες υπηρεσίες ασφάλειας στο UMTS

- Αμοιβαία αυθεντικοποίηση οντοτήτων
  - αυθεντικοποίηση του δικτύου στο χρήστη
- Ακεραιότητα δεδομένων σηματοδοσίας
  - Προστασία της ακεραιότητας δεδομένων σηματοδοσίας μεταξύ κινητού και RNC
- Προστασία από επιθέσεις
  - Ψεύτικου σταθμού βάσης (false base station attacks)
  - Επανάληψης (replay attacks)
  - Ενδιάμεσου (man-in-the-middle attacks)

Συμπεράσματα

- Από τη 2η στην 3η γενιά
  - βελτίωση υπηρεσιών ασφάλειας 2ης γενιάς
  - νέες υπηρεσίες ασφάλειας
- 4η γενιά: All-IP, end-to-end security
- Ανάγκη για συνδυασμένη προσπάθεια ανάπτυξης κατάλληλου νομικού πλαισίου προστασίας του απορρήτου των επικοινωνιών