Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων
Καθηγητής: Α.Α. Οικονομίδης

University of Macedonia
Master Information Systems
Networking Technologies
Professor: A.A. Economides

ΑΣΦΑΛΕΙΑ ΣΤΑ ΔΙΚΤΥΑ GSM

ΔΡΑΓΑΝΗΣ ΒΑΣΙΛΗΣ
Α.Μ.: 07/23
ΙΑΝΟΥΑΡΙΟΣ 2008

1.1 Ασφάλεια (1/3)

- Το θέμα της ασφάλειας της πληροφορίας διαδραματίζει πρωτεύοντα ρόλο σε όλα τα δίκτυα, ανεξάρτητα από τις εφαρμογές που υποστηρίζουν.
- Δίκτυα όπως το GSM, το GPRS, το UMTS, το Internet κτλ. που έχουν ανοικτή αρχιτεκτονική και είναι ευρέως διαδεδομένα αντιμετωπίζουν πολλές απειλές και για το λόγο αυτό πρέπει να προστατεύονται αποτελεσματικά.

1.1 Ασφάλεια (2/3)

- Στις μέρες μας μάλιστα η ανάπτυξη των παραπάνω (και όχι μόνο) δικτύων είναι τόσο αλματώδης, κάτι που συνεπάγεται περισσότερη κίνηση πληροφορίας, οδηγεί στην απαίτηση για ασφάλεια σε όλο και μεγαλύτερο αριθμό περιπτώσεων.
- Οι επίδοξοι υποκλοπείς δεδομένων είναι πια τόσο ενημερωμένοι και ικανοί που η αντιμετώπισή τους είναι συχνά αδύνατη.

1.1 Ασφάλεια (3/3)

- Ταυτόχρονα με αυτούς εκσυγχρονίζονται και εξαπλώνονται και ειδικές εφαρμογές που καθιστούν την υποκλοπή πιο εύκολη και την αποστολή του πιθανού κώδικα ασφαλείας πιο δύσκολη.
- Γίνεται επομένως αντιληπτό ότι το ζήτημα της ασφάλειας μέσα σε ένα δίκτυο, αν και αποτελεί βασική παράμετρο αυτού, συνιστά ένα πρόβλημα δυσεπίλυτο, εξαιτίας της ίδιας της εξέλιξης της τεχνολογίας και της αύξησης των κινδύνων που μπορούν να διακυβεύσουν το δίκτυο αυτό.

2.1 Γενικά χαρακτηριστικά του GSM (1/3)

- Το GSM σχεδιάστηκε κυρίως για τη μετάδοση ομιλίας και λιγότερο για τη μετάδοση δεδομένων (fax, e-mail, αρχεία) και αναμενόταν να παρέχει καλύτερη ποιότητα ήχου, πανευρωπαϊκή περιαγωγή (roaming), εφαρμογές με χαμηλότερο κόστος, δυνατότητα για αυξημένη φασματική απόδοση, υψηλή ευελιξία και ανοικτή αρχιτεκτονική που θα επιτρέπει την εισαγωγή νέων υπηρεσιών στο άμεσο μέλλον.

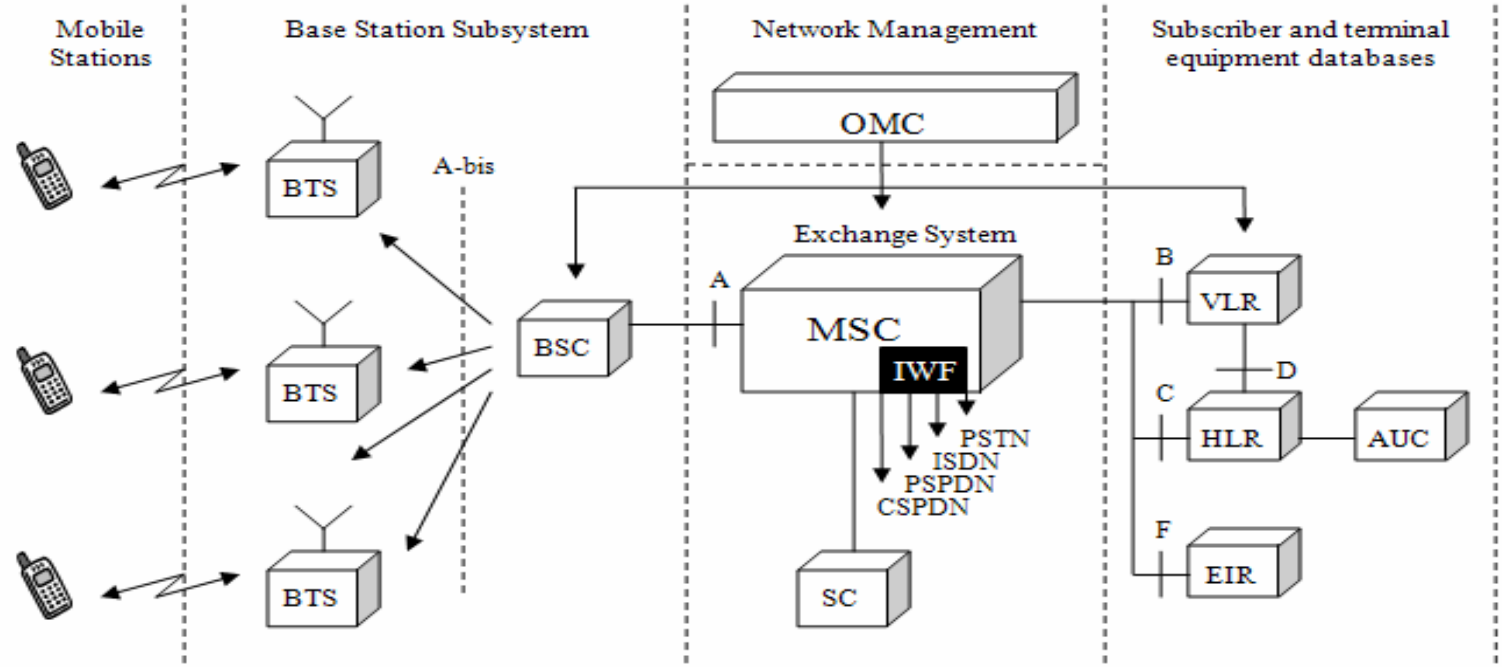
2.1 Γενικά χαρακτηριστικά του GSM (2/3)

- Το GSM χρησιμοποιεί Πολλαπλή Πρόσβαση με Διαίρεση Χρόνου (TDMA) και Διαίρεση Συχνότητας (FDMA). Έτσι, μπορούν να λαμβάνουν χώρα την ίδια χρονική στιγμή και στην ίδια συχνότητα πολλές συνδιαλλαγές χρησιμοποιώντας διαφορετικές χρονικές σχισμές (timeslots).
- Οι συχνότητες εκπομπής και λήψης είναι διαφορετικές με αποτέλεσμα οι μεταδόσεις από κινητό προς σταθμό βάσης και από σταθμό βάσης προς κινητό είναι ταυτόχρονες.

2.1 Γενικά χαρακτηριστικά του GSM (3/3)

- Σχετικά με τη μετάδοση, ο σταθμός βάσης κατευθύνει το κινητό να χρησιμοποιήσει την ελάχιστη ισχύ που είναι απαραίτητη για μια αξιόπιστη μετάδοση.
- Τόσο ο κινητός όσο και ο σταθμός βάσης χρησιμοποιούν Ασυνεχή Μετάδοση, προκειμένου το κινητό να διαφυλάξει τη μπαταρία του και ο σταθμός βάσης να μειώσει τη διακαναλική παρεμβολή.

2.2 Αρχιτεκτονική του GSM (1/15)



Δομή του συστήματος GSM

2.2 Αρχιτεκτονική του GSM (2/15)

- Από λειτουργικής πλευράς το πλήρες δίκτυο χωρίζεται σε δύο τμήματα:
  - το τμήμα μεταγωγής (Switching System - SS), το οποίο περιλαμβάνει το κέντρο MSC, τις βάσεις δεδομένων VLR, HLR, το κέντρο πιστοποίησης AUC, το κέντρο τεκμηρίωσης κινητών σταθμών EIR και τα κέντρα εποπτείας και συντήρησης OMC.
  - και το ραδιοηλεκτρικό τμήμα (Radio System - RS), το οποίο περιλαμβάνει τους σταθμούς βάσης BSS και τους κινητούς σταθμούς MS. [2]

2.2 Αρχιτεκτονική του GSM (3/15)

Λειτουργίες του MSC (1/3)

- Χειρίζεται τις κλήσεις που εκδηλώνονται ή καταλήγουν στην περιοχή που αυτό καλύπτει και για το λόγο αυτό είναι συνδεδεμένο με έναν αριθμό σταθμών βάσης με τους οποίους διατηρεί συνεχή επαφή.
- Συνδέεται με το δίκτυο PSTN/ISDN/PSPDN για να επιτυγχάνει σωστή δρομολόγηση όλων των κλήσεων.

2.2 Αρχιτεκτονική του GSM (4/15)

Λειτουργίες του MSC (2/3)

- Διαχειρίζεται τα διαθέσιμα ραδιοηλεκτρικά μέσα κατά τη διάρκεια των κλήσεων, καθορίζοντας τον τύπο ραδιοκαναλιού που χρησιμοποιείται σε κάθε φάση της κλήσης.
- Συμμετέχει στην εγγραφή της θέσης του συνδρομητή, διασφαλίζοντας τη μεταφορά των στοιχείων των κινητών σταθμών προς τη βάση επισκέψεως VLR και εκτελεί τις λειτουργίες χρέωσης.
- Υποστηρίζει τη διαδικασία μεταπομπής κυψέλης.

2.2 Αρχιτεκτονική του GSM (5/15)
Λειτουργίες του MSC (3/3)

- Μεταφέρει τις παραμέτρους πιστοποίησης μεταξύ του σταθμού βάσης και της βάσης επισκέψεως.
- Αναγνωρίζει την περιοδική και αυτόματη διακοπή λειτουργίας του κινητού σταθμού προς εξοικονόμηση ισχύος (λειτουργία “ασυνεχούς λήψης”).
- Ερευνά την οικεία βάση δεδομένων HLR του καλούμενου ώστε να εξακριβώσει τον αριθμό περιαγωγής του.
- Μεριμνά για την ασφάλεια της ταυτότητας του συνδρομητή καθώς και για την ασφάλεια των πληροφοριών που μεταδίδει. [2]

2.2 Αρχιτεκτονική του GSM (6/15)

- Η διασφάλιση του απορρήτου της συνδρομητικής ταυτότητας (IMSI) βασίζεται στη χρησιμοποίηση από τον κινητό σταθμό ενός παροδικού αριθμού (TMSI) που τον ορίζει η βάση δεδομένων επισκέψεως.
- Το κέντρο γνωρίζει την ταυτότητα αυτή και την χρησιμοποιεί σε όλες τις επαφές του με τον κινητό σταθμό για κάποιο χρονικό διάστημα.

2.2 Αρχιτεκτονική του GSM (7/15)

- Η βάση δεδομένων **VLR** χρησιμοποιείται για την εγγραφή της θέσης των ενεργοποιημένων κινητών σταθμών, για κάποιο χρονικό διάστημα, και αυτών που μόλις εισήλθαν στην περιοχή της.
- Οι πληροφορίες που αποθηκεύει η VLR αντλούνται ή από την οικεία βάση δεδομένων ή από τη βάση επισκέψεως στην οποία βρισκόταν προηγουμένως ο συνδρομητής.

2.2 Αρχιτεκτονική του GSM (8/15)

- Τα στοιχεία που απαραιτήτως διατηρεί η βάση για κάθε κινητό σταθμό είναι:
  - η ταυτότητα του συνδρομητή (IMSI)
  - ο αριθμός ISDN του κινητού (MSISDN)
  - ο αριθμός περιαγωγής του (MSRN), ο οποίος κατανέμεται στο κινητό κάθε φορά που εγγράφεται σε μια καινούρια περιοχή MSC, με σκοπό τη δρομολόγηση των εισερχόμενων προς αυτό κλήσεων
  - η παροδική ταυτότητα του κινητού (TMSI), με τη χρησιμοποίηση της οποίας αποφεύγεται η συχνή εκπομπή της IMSI
  - η περιοχή εντοπισμού του κινητού σταθμού (Location Area - LA)
  - η ταυτότητα του τρέχοντος MSC με το οποίο συνεργάζεται το VLR
  - οι πίνακες αντιστοίχησης IMSI – TMSI για κάθε χρήστη καθώς και τα στοιχεία πιστοποίησης που είναι οι τριάδες τυχαίου αριθμού, ενυπόγραφης απάντησης και κλείδας κρυπτογράφησης (RAND, SRES, K_C). Τις τριάδες αυτές το VLR τις αντλεί από το HLR και κάθε φορά που απαιτείται μεταβιβάζει το κλειδί K_C στο BSS για την κρυπτογράφηση / αποκρυπτογράφηση των δεδομένων. [1] [2]

2.2 Αρχιτεκτονική του GSM (9/15)

- Η οικεία βάση **HLR** αποτελεί τη βάση αναφοράς για κάθε συνδρομητή.
- Περιέχει όλα τα παραπάνω δεδομένα με τη μόνη διαφορά ότι κάποια από αυτά δεν αλλάζουν καθώς το κινητό τερματικό κινείται από μια περιοχή σε άλλη (π.χ. IMSI, MSISDN).

2.2 Αρχιτεκτονική του GSM (10/15)

- Το κέντρο πιστοποίησης **AUC** έχει ως βασική λειτουργία να παρέχει στο HLR τις τριάδες (triplets) προκειμένου να γίνει πιστοποίηση των συνδρομητών και κρατάει τα μυστικά κλειδιά K_i.
- Το κλειδί K_i και η IMSI ορίζονται με την εγγραφή ενός χρήστη και είναι τα δύο στοιχεία που αναγνωρίζουν κατά μοναδικό τρόπο το χρήστη αυτό.

2.2 Αρχιτεκτονική του GSM (11/15)

- Το κέντρο τεκμηρίωσης **EIR** εποπτεύει τους κινητούς σταθμούς και μπλοκάρει όσους δεν έχουν το δικαίωμα να εξυπηρετούνται.
- Στη βάση δεδομένων του κέντρου αυτού είναι εγγεγραμμένες όλες οι ταυτότητες των κινητών συσκευών (IMEI). [2]

2.2 Αρχιτεκτονική του GSM (12/15)

- Το κέντρο εποπτείας και συντήρησης **OMC** επικοινωνεί με διάφορα τμήματα του δικτύου και ουσιαστικά ελέγχει το όλο σύστημα.
- Λειτουργεί παράλληλα με το κέντρο διαχείρισης **NMC** το οποίο επίσης εκτελεί λειτουργίες διαχείρισης .
- Παρακολουθεί τους κόμβους ώστε αυτοί να μην είναι υπερφορτωμένοι ή εκτός λειτουργίας.
- Μερικές φορές διεκπεραιώνει και αρμοδιότητες του OMC.
  - Η διαφορά τους έγκειται στο ότι το OMC είναι ένα τοπικό εποπτικό κέντρο ενώ το NMC είναι το καθολικό κέντρο διαχείρισης του δικτύου.

2.2 Αρχιτεκτονική του GSM (13/15)

- Ο σταθμός βάσης **BSS** είναι η φυσική διάταξη που χρησιμοποιείται για να δώσει ραδιοηλεκτρική κάλυψη σε κάποια περιορισμένη γεωγραφική ζώνη η οποία περιλαμβάνει μία ή περισσότερες κυψέλες.
  - Αποτελείται από μια μονάδα κεντρικού ελέγχου, **BSC**, και μία ή περισσότερες ομάδες πομποδεκτών **BTS.**
  - Κάθε ομάδα πομποδεκτών εξυπηρετεί μία κυψέλη, ενώ ένα BSC συνδέεται με έναν αριθμό ομάδων BTS και συνήθως ελέγχει μια περιοχή εντοπισμού (LA).
  - Κάθε BTS περιλαμβάνει εξοπλισμό μετάδοσης, τις απαραίτητες διατάξεις εκπομπής και λήψης, τους ζεύκτες και τις κεραίες. [1] [2]

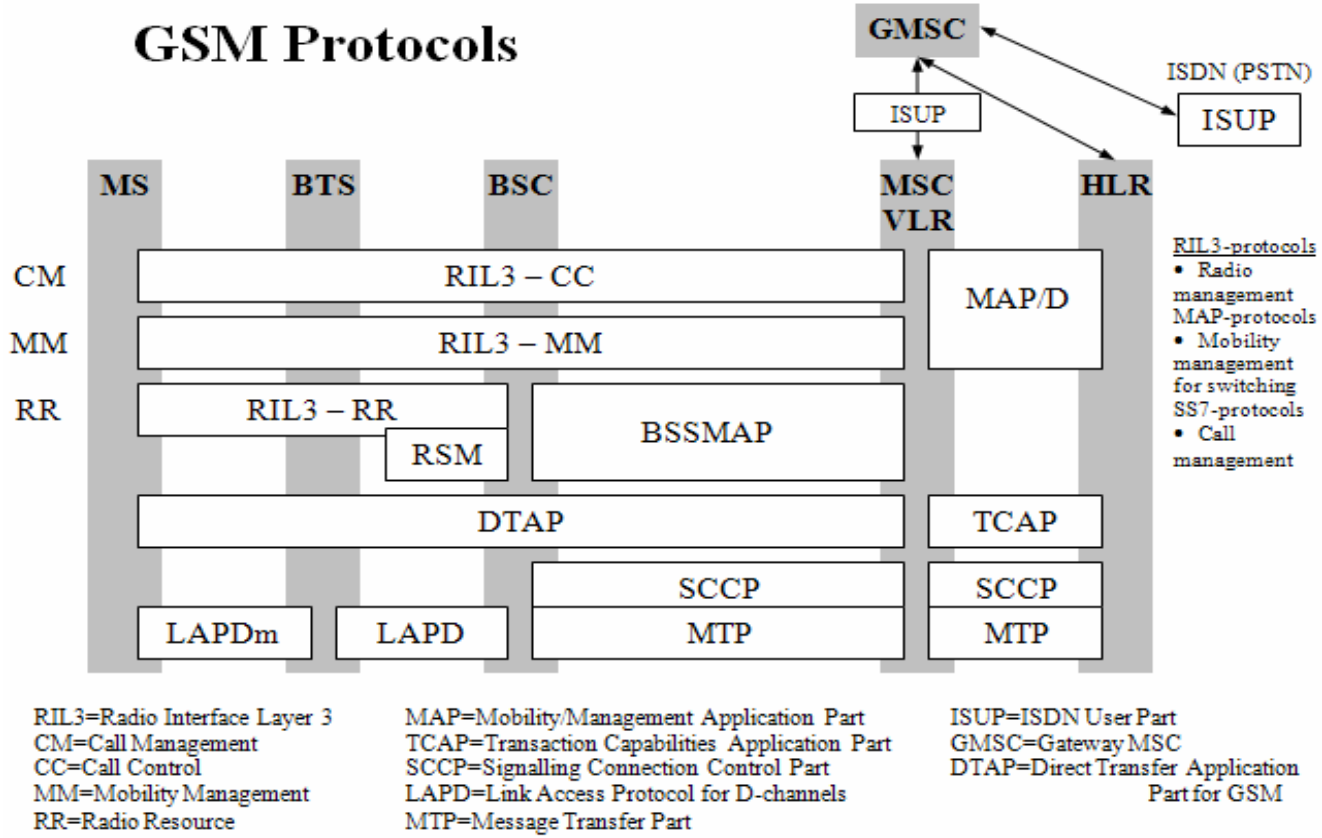
2.2 Αρχιτεκτονική του GSM (14/15)

- Ο κινητός σταθμός **MS** αποτελείται από τον εξοπλισμό (mobile equipment - ME) και την κάρτα SIM.
- Στον εξοπλισμό υπάρχει το κατάλληλο hardware ώστε να γίνεται αρχικά ψηφιοποίηση και κωδικοποίηση φωνής και τελικά μετά την κρυπτογράφηση και τη διαμόρφωση, εκπομπή του σήματος από την κεραία του κινητού.

2.2 Αρχιτεκτονική του GSM (15/15)

- Η κάρτα SIM περιλαμβάνει μικροεπεξεργαστή, μνήμη ενώ έχει και υπολογιστικές δυνατότητες.
- Σ’ αυτήν αποθηκεύονται:
  - οι ταυτότητες του κινητού IMSI και TMSI
  - ο αριθμός MSISDN
  - το κλειδί K_i
  - ο αλγόριθμος παραγωγής του κλειδιού κρυπτογράφησης K_c
  - το ίδιο το κλειδί
  - ο αλγόριθμος παραγωγής της ενυπόγραφης απάντησης SRES
  - η ταυτότητα της περιοχής εντοπισμού του σταθμού (LAI)
  - καθώς και ο κωδικός πρόσβασης του χρήστη στην κάρτα (PIN)

2.3 Τα πρωτόκολλα του GSM (1/2)



Τα πρωτόκολλα σηματοδοσίας του GSM

2.3 Τα πρωτόκολλα του GSM (2/2)

- Από όλες τις παραπάνω συνδέσεις μόνο η ραδιοζεύξη μεταξύ του κινητού σταθμού και του BTS κρυπτογραφείται, ενώ σε όλες τις υπόλοιπες τα μηνύματα μεταδίδονται χωρίς καμία προστασία. [9]

2.4 Οι μηχανισμοί ασφαλείας στο GSM

- Το σύστημα ασφαλείας του GSM έχει σκοπό να παρέχει:
  - **Ανωνυμία** στο συνδρομητή, μέσω της χρησιμοποίησης της ταυτότητας TMSI.
  - **Πιστοποίηση** της ταυτότητας του χρήστη στο δίκτυο , με τη χρήση τριπλετών.
  - **Κρυπτογράφηση** των δεδομένων στη ραδιοζεύξη.
  - **Προστασία των ευαίσθητων πληροφοριών** του χρήστη στην κάρτα **SIM.**

2.4.1 Προστασία της ταυτότητας του συνδρομητή

- Με τη χρησιμοποίηση της προσωρινής ταυτότητας TMSI αποφεύγεται η συχνή εκπομπή της IMSI στη ραδιοζεύξη.
- Έτσι παρέχεται στο χρήστη ανωνυμία και δεν είναι δυνατή η αναγνώρισή του από κάποιον που “ακούει” το δίαυλο. [3]

2.4.2 Πιστοποίηση της ταυτότητας του συνδρομητή

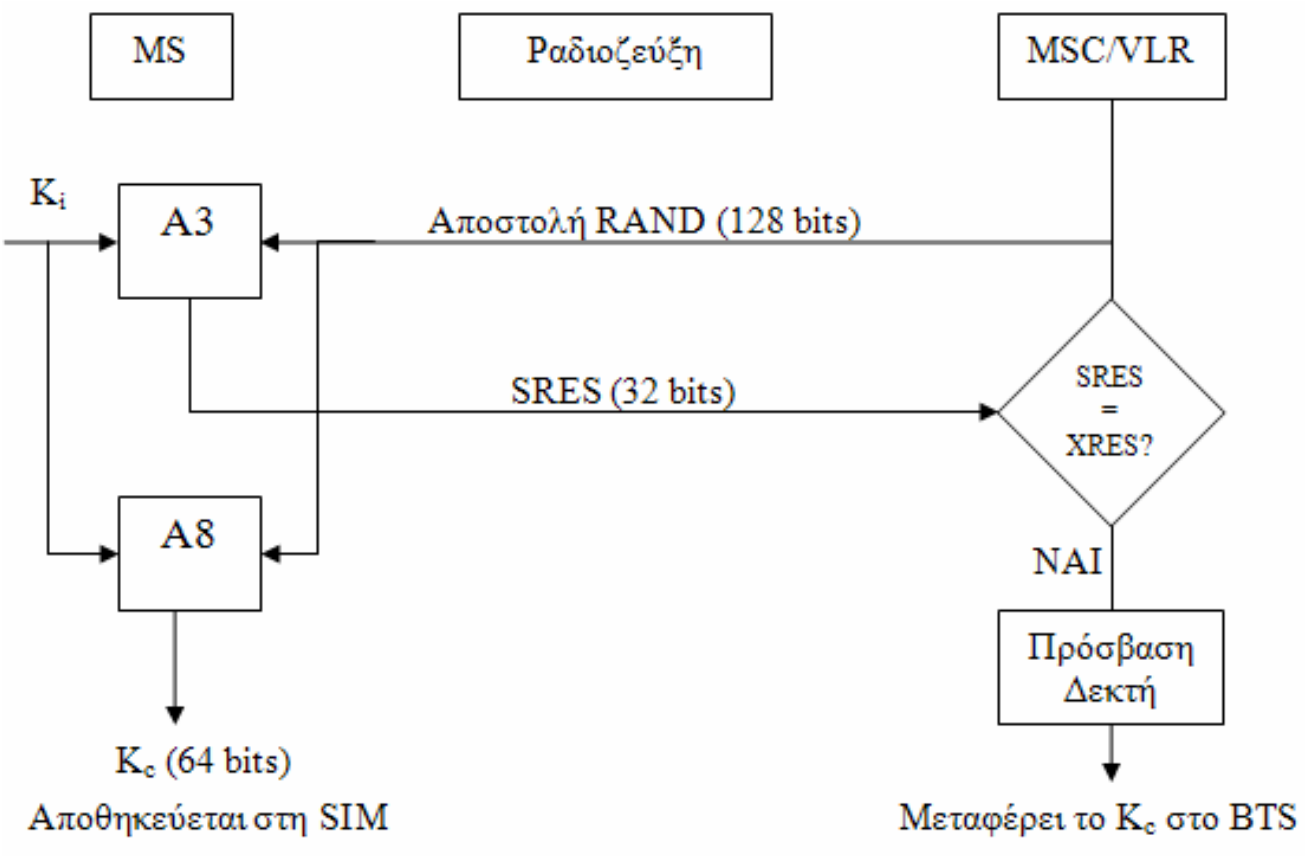
- Γίνεται προκειμένου να εξακριβωθεί ότι η ταυτότητα που εστάλη από το MS είναι αληθινή.
- Πιστοποίηση πραγματοποιείται σε κάθε εγγραφή, ενημέρωση θέσης και πρόσβαση του κινητού στο δίκτυο για εισερχόμενη ή εξερχόμενη κλήση.
- Η διαδικασία εκτελείται αφού πρώτα γίνει γνωστή η ταυτότητα του συνδρομητή και πριν κρυπτογραφηθεί το κανάλι.

Διαδικασία πιστοποίησης (1/2)

- Βασίζεται στην αποστολή από το MSC/VLR ενός τυχαίου αριθμού **RAND** το οποίο είναι 128 bits.
- Το MS μόλις λάβει τον αριθμό αυτό υπολογίζει με τον **αλγόριθμο A3**, χρησιμοποιώντας ως είσοδο στον αλγόριθμο αυτό και το μυστικό κλειδί $\mathbf{K_i}$ που είναι επίσης 128 bits και είναι αποθηκευμένο στην κάρτα SIM, την ενυπόγραφη απάντηση **SRES**, που έχει μήκος 32 bits, και την αποστέλλει στο VLR.

Διαδικασία πιστοποίησης (2/2)

- Έπειτα, με τον **αλγόριθμο Α8**, και με εισόδους πάλι τα RAND και K_i, εξάγει το κλειδί κρυπτογράφησης $\mathbf{K_c}$, που έχει μήκος μόλις 64 bits, το οποίο και αποθηκεύει για να χρησιμοποιήσει ύστερα κατά την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων.
- Με τη σειρά του το VLR μόλις αποκτήσει τη SRES, τη συγκρίνει με την XRES που έχει αποθηκευμένη στη βάση δεδομένων του και αν αυτές ταυτίζονται, ο κινητός σταθμός θεωρείται πιστοποιημένος. [3] [4]



Η διαδικασία πιστοποίησης στο GSM

Θετικά στοιχεία της πιστοποίησης του GSM

- Είναι σχεδόν αδύνατο για έναν τρίτο να μαντέψει το σωστό SRES.
- Ο κινητός σταθμός έχει μια μόνο ευκαιρία να επιστρέψει το SRES που αντιστοιχεί σε ένα συγκεκριμένο RAND, ενώ η παράμετρος SRES είναι 32 bits .
- Ένας τρίτος δεν μπορεί να εξάγει το κλειδί K_i ακόμα κι αν αποκτήσει ένα ζεύγος RAND – SRES κρυφακούοντας τη ραδιοζεύξη, αλλά ούτε και το K_c.
- Οι παράμετροι SRES και K_c, παρόλο που προκύπτουν από τις ίδιες εισόδους RAND και K_i είναι εντελώς ασυσχέτιστες μεταξύ τους.
- Τόσο το K_i όσο και οι αλγόριθμοι A3, A8 δε μεταφέρονται μέσα στο δίκτυο, αλλά είναι αποθηκευμένοι μόνο στην κάρτα SIM και στο AUC.

2.4.3 Κρυπτογράφηση των δεδομένων του συνδρομητή

- Με την κρυπτογράφηση επιτυγχάνεται προστασία των ευαίσθητων δεδομένων του χρήστη στη ραδιοζεύξη.
- Πραγματοποιείται μεταξύ του κινητού εξοπλισμού ΜΕ και του σταθμού βάσης BTS.
- Μετά την πιστοποίηση, το BTS ενημερώνει τον κινητό σταθμό σχετικά με το ποιους αλγορίθμους κρυπτογράφησης υποστηρίζει και δίνει εντολή για έναρξη της διαδικασίας (cipher command).
- Ο αλγόριθμος που χρησιμοποιείται είναι ο **A5** (με αρκετές εκδόσεις) και είναι ο μοναδικός που δε βρίσκεται στην SIM αλλά στη συσκευή του χρήστη σε μορφή hardware. [4]

2.4.4 Έλεγχος IMEI

- Ο έλεγχος της ταυτότητας του κινητού τερματικού (IMEI) γίνεται κάθε φορά που ο χρήστης προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο προκειμένου να διεκπεραιώσει κάποια λειτουργία (κλήση, αποστολή δεδομένων κ.τ.λ.).
- Ο έλεγχος αυτός αποσκοπεί στο να βεβαιωθεί το σύστημα ότι κανένα κλεμμένο ή μη εξουσιοδοτημένο κινητό δε χρησιμοποιείται.
- Πραγματοποιείται με τη συνεργασία του κέντρου τεκμηρίωσης EIR, το οποίο μετά τον έλεγχο αποφαίνεται αν μια κλήση πρέπει να συνεχιστεί ή να διακοπεί.
- Η ανταλλαγή μηνυμάτων μεταξύ του κινητού σταθμού και του MSC/VLR γίνεται σε κρυπτογραφημένη μορφή. [1]

2.5 Τα αδύνατα σημεία της ασφάλειας του GSM

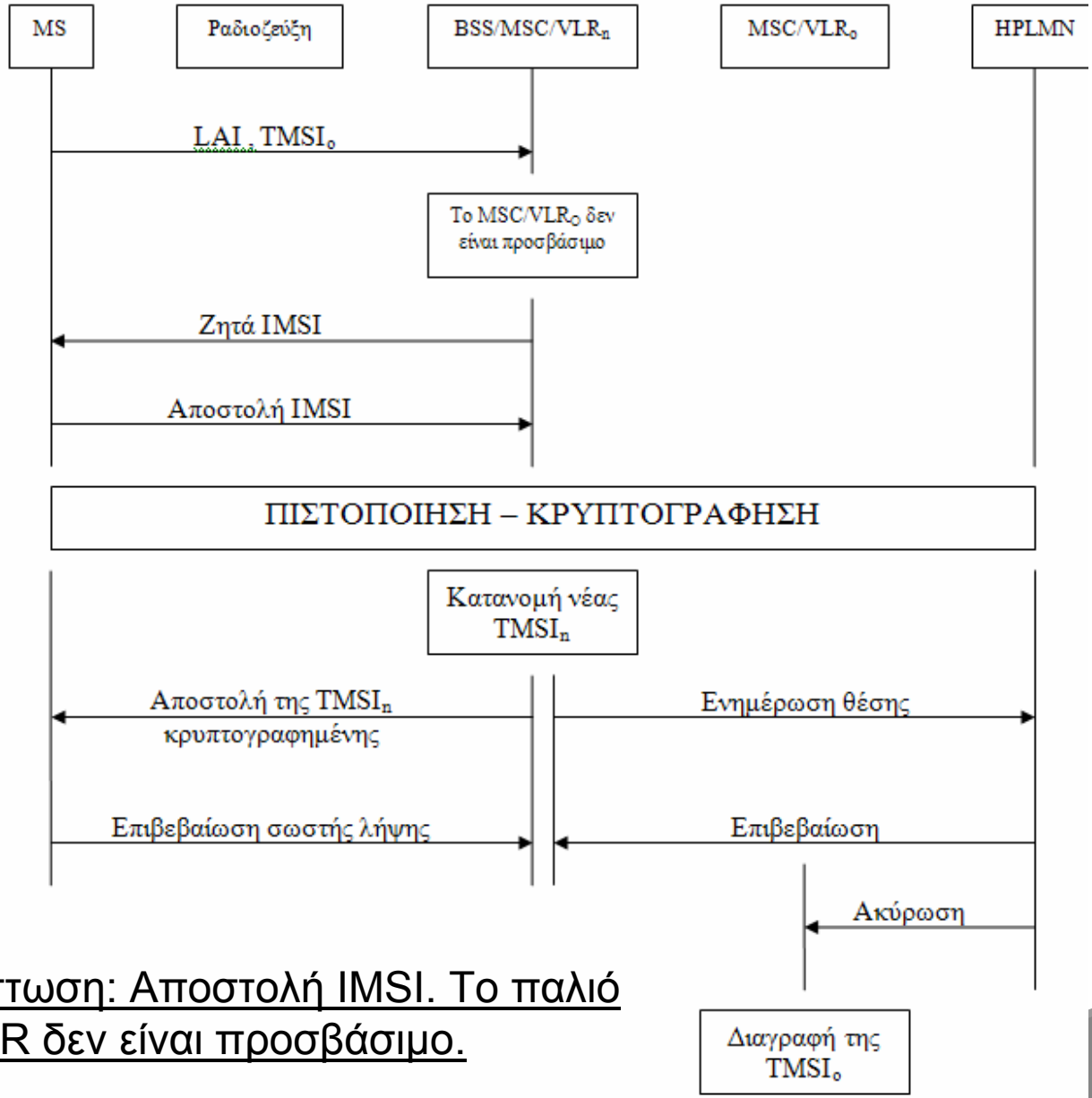
- Στην ενότητα αυτή περιγράφονται τα τρωτά σημεία που συναντώνται στο μοντέλο ασφαλείας του GSM.
- Γίνεται αναφορά σε διάφορες παθητικές ή ενεργές επιθέσεις που πραγματοποιούνται εκμεταλλευόμενες τις αδυναμίες αυτές, ενώ σε ορισμένες περιπτώσεις προτείνονται λύσεις για την αντιμετώπισή τους.

2.5.1 Αποστολή της IMSI αντί της TMSI στη ραδιοζεύξη

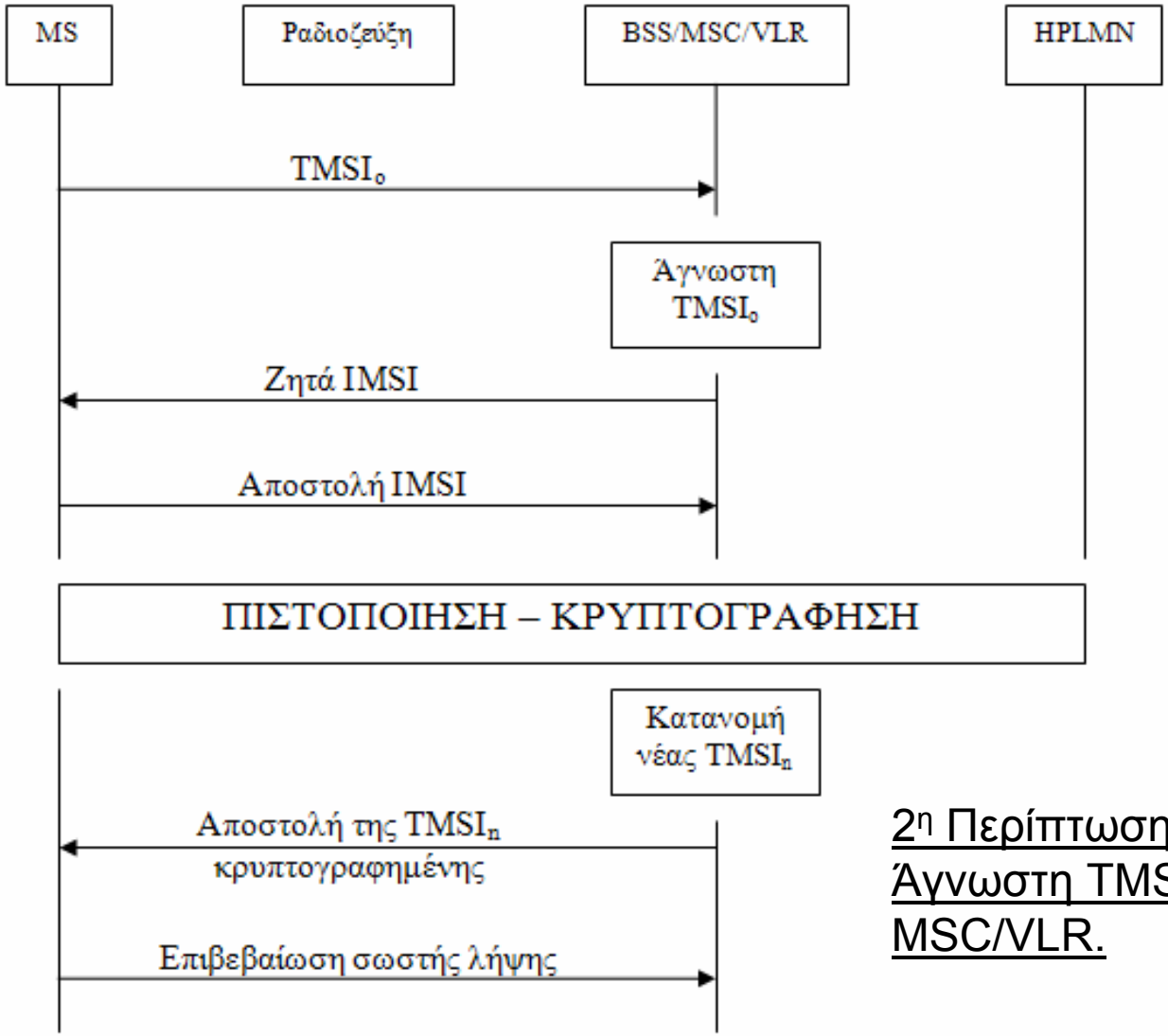
- Υπάρχουν μερικές περιπτώσεις – εξαιρέσεις κατά τις οποίες αποστέλλεται η μόνιμη ταυτότητα του συνδρομητή IMSI, και μάλιστα σε όχι κρυπτογραφημένη μορφή, πάνω από το air interface.
- Κάποιος που παρακολουθεί τη ραδιοζεύξη, έχοντας τον κατάλληλο εξοπλισμό, μπορεί να υποκλέψει την προσωπική ταυτότητα ενός χρήστη.

Οι τρεις περιπτώσεις που διακυβεύεται η μόνιμη ταυτότητα IMSI

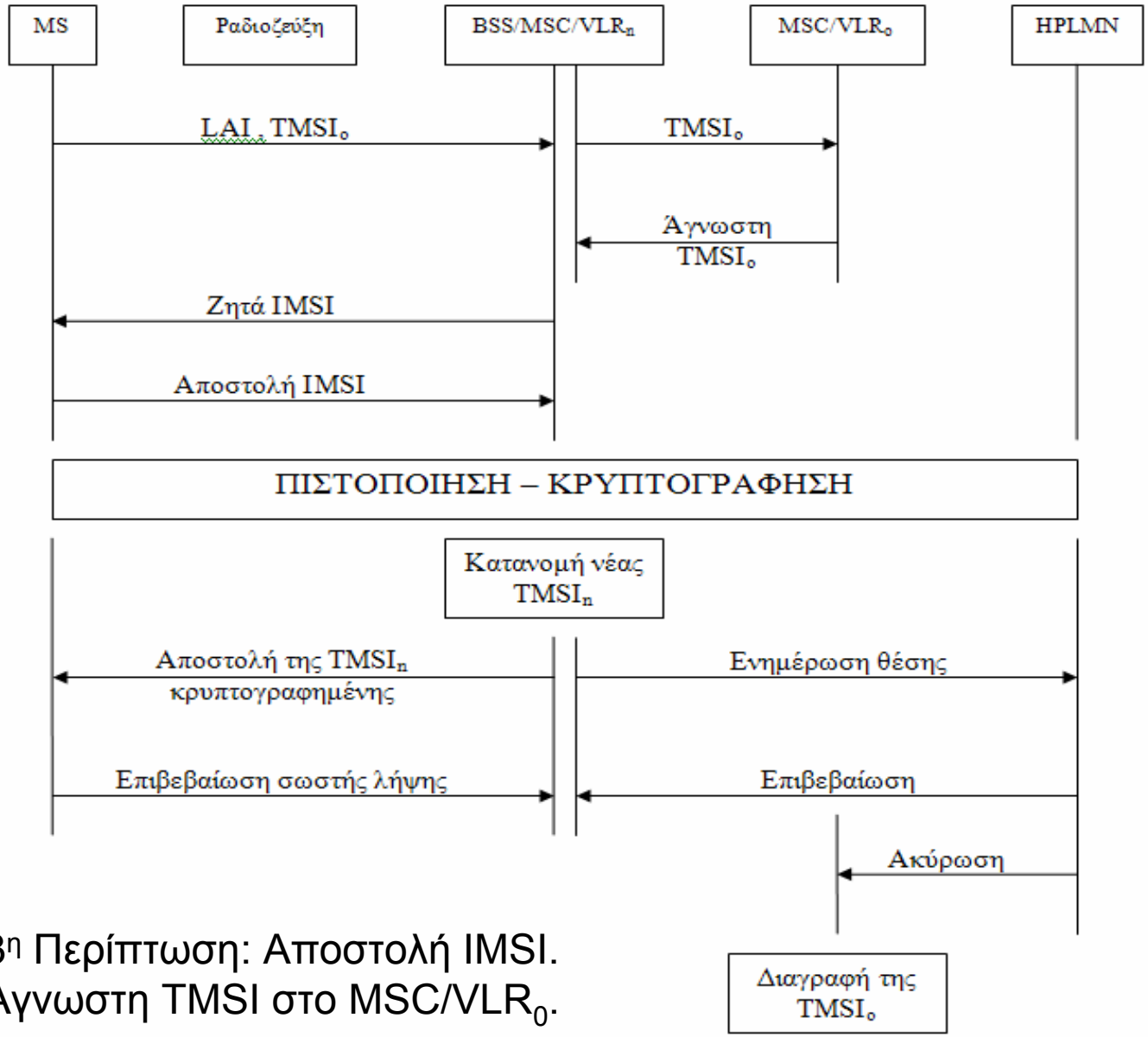
- Στην πρώτη περίπτωση το νέο MSC/VLR_n που εξυπηρετεί το χρήστη δεν μπορεί για κάποιο λόγο να αποκτήσει πρόσβαση στο παλιό MSC/VLR_o προκειμένου να παραλάβει την IMSI του κινητού.
- Στη δεύτερη περίπτωση η TMSI είναι άγνωστη στο τρέχον MSC/VLR πιθανόν λόγω κατάρρευσης της βάσης δεδομένων (database failure) για κάποιο χρονικό διάστημα.
- Στην τρίτη περίπτωση η TMSI είναι άγνωστη στο MSC/VLR_o.



1η Περίπτωση: Αποστολή IMSI. Το παλιό MSC/VLR δεν είναι προσβάσιμο.



2η Περίπτωση: Αποστολή IMSI. Άγνωστη TMSI στο τρέχον MSC/VLR.



3η Περίπτωση: Αποστολή IMSI. Άγνωστη TMSI στο MSC/VLR$_0$.

Τρόποι αποφυγής αποστολής της IMSI στη ραδιοζεύξη.

- Να τερματίζεται αυτόματα η επικοινωνία με το MS χωρίς καμία περαιτέρω προσπάθεια από πλευράς του δικτύου για εξακρίβωση της ταυτότητας του χρήστη.
- Να κατανέμονται στο κινητό τερματικό δύο ταυτότητες TMSI και σε περίπτωση που δεν αναγνωρίζεται η μία να αποστέλλεται η δεύτερη, ενώ αν δεν αναγνωρίζεται καμία να διακόπτεται αμέσως η επικοινωνία. [11]

Επιθέσεις στο σύστημα ασφαλείας του GSM (1/2)

- **Επιθέσεις κρυφακούσματος (eavesdropping):** Ο εισβολέας παρακολουθεί τη ραδιοζεύξη παραμένοντας αδρανής. Πρόκειται για παθητική επίθεση.

- **Επιθέσεις προσωποποίησης του δικτύου στο χρήστη:** Σε αυτήν την περίπτωση ο επιτιθέμενος στο σύστημα (attacker) παριστάνει στο συνδρομητή το γνήσιο δίκτυο, χρησιμοποιώντας ένα ψεύτικο σταθμό βάσης (false BTS). Πρόκειται για ενεργή επίθεση.

Επιθέσεις στο σύστημα ασφαλείας του GSM (2/2)

- **Επιθέσεις τύπου man-in-the-middle:** Ο εισβολέας χρησιμοποιεί ένα ψεύτικο BTS για να υποδυθεί το δίκτυο στο χρήστη σε συνδυασμό με ένα τροποποιημένο MS για να προσποιηθεί το νόμιμο χρήστη στο δίκτυο. Ο attacker έχει τη δυνατότητα να μετατρέψει, να αλλοιώσει, να διαγράψει ή και να πλαστογραφήσει τα δεδομένα που ανταλλάσσονται μεταξύ του πραγματικού BTS και του κινητού σταθμού. Πρόκειται για ενεργή επίθεση.[8]

2.5.2 Επισφαλείς οι αλγόριθμοι πιστοποίησης και κρυπτογράφησης (1/4)

- **<u>Ο αλγόριθμος COMP128</u>**
  - Ο αλγόριθμος πιστοποίησης **COMP128** δυστυχώς κατάφερε να σπάσει, οδηγώντας έτσι στην εύκολη **απόκτηση του μυστικού κλειδιού K_i**.[5]
  - Η επίθεση που χρησιμοποιήθηκε ονομάζεται επίθεση επιλεγμένου κειμένου (chosen plaintext attack) και μπορεί να πραγματοποιηθεί είτε με φυσική κατοχή της κάρτας SIM για μικρή χρονική περίοδο είτε από το air interface χάρη στη χρήση πλαστού BTS. [5]

2.5.2 Επισφαλείς οι αλγόριθμοι πιστοποίησης και κρυπτογράφησης (2/4)

- **Ο GSM – MILENAGE αλγόριθμος πιστοποίησης**
  - Ο νέος αυτός αλγόριθμος πιστοποίησης είναι πολύ πιο δυνατός σε σχέση με τον COMP128 και έχει αποδειχθεί ότι είναι λιγότερο ευάλωτος.
  - Η πολυπλοκότητά του είναι αυξημένη, ωστόσο αν απαιτείται υψηλή ασφάλεια στο δίκτυο, η χρησιμοποίησή του θεωρείται η πλέον ενδεδειγμένη.

2.5.2 Επισφαλείς οι αλγόριθμοι πιστοποίησης και κρυπτογράφησης (3/4)

- **<u>Ο αλγόριθμος A5</u>**
  - Ο αλγόριθμος A5 σχεδιάστηκε ειδικά για το GSM.
  - Αρχικά είχε θεωρηθεί αρκετά δύσκολο να καταφέρει κάποιος να τον σπάσει.
  - Σήμερα είναι γνωστές πάρα πολλές τεχνικές, οι οποίες επιτρέπουν την απόκτηση του κλειδιού συνόδου K_C ακόμα και σε πραγματικό χρόνο (real time). [6]

2.5.2 Επισφαλείς οι αλγόριθμοι πιστοποίησης και κρυπτογράφησης (4/4)

- **Ο GSM A5/3 αλγόριθμος κρυπτογράφησης**
  - Είναι πολύ πιο δυνατός σε σχέση με τους μέχρι τώρα χρησιμοποιούμενους.
  - Οι διαδικασίες που εφαρμόζει είναι αρκετά πολύπλοκες.
  - Προσφέρει ασφάλεια κατά την μεταφορά των δεδομένων πάνω από την επικίνδυνη ραδιοηλεκτρική οδό.
  - Έχει αρχίσει σιγά – σιγά να ενσωματώνεται στα κινητά τερματικά, προκειμένου να τα προστατέψει από τις ποικίλες επιθέσεις.

2.5.3 Δεν πιστοποιείται το δίκτυο στο χρήστη αλλά μόνο ο χρήστης στο δίκτυο

- Το GSM παρέχει μονομερή πιστοποίηση.
- Το γεγονός αυτό επιτρέπει τη διεξαγωγή επιθέσεων στο σύστημα, όπου ένας εισβολέας προσποιείται το σταθμό βάσης BTS σε ένα ή περισσότερα κινητά τερματικά. [3]

2.5.4 Δεν παρέχεται προστασία της ακεραιότητας των δεδομένων (1/2)

- Πολλά ευαίσθητα δεδομένα σηματοδοσίας (signaling data), όπως στοιχεία χρέωσης, πληροφορίες σχετικές με τη θέση του κινητού, η ταυτότητα του χρήστη καθώς και πληροφορίες που αναφέρονται στη διαχείριση ασφάλειας διακυβεύονται διότι οι πληροφορίες αυτές μεταφέρονται μη κρυπτογραφημένες και χωρίς να πιστοποιούνται.
- Κατά τη διάρκεια της συνομιλίας του κινητού σταθμού με το σταθερό δίκτυο ή με κάποιο άλλο κινητό, ο εισβολέας μπορεί να τροποποιεί το περιεχόμενο κάποιων δεδομένων του χρήστη (user data).[7]

2.5.4 Δεν παρέχεται προστασία της ακεραιότητας των δεδομένων (2/2)

Προτεινόμενες Λύσεις

- Θα ήταν καλό κάποια δεδομένα σηματοδοσίας (οι κρυπτογραφικές δυνατότητες του κινητού, η εντολή για έναρξη κρυπτογράφησης, η αποστολή της ταυτότητας του χρήστη) να κρυπτογραφούνται ή αν κάτι τέτοιο είναι δύσκολο , τουλάχιστον να πιστοποιούνται.
- Πιστοποίηση του χρήστη πρέπει να εφαρμόζεται όχι μόνο στην αρχή μιας διαδικασίας αλλά και κατά τη διάρκεια και στο τέλος, ώστε να είναι αδύνατο για έναν εισβολέα να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στις υπηρεσίες του δικτύου. [13]

2.5.5 Όχι τόσο ασφαλής η κάρτα SIM (1/2)

- Οι κάρτες SIM είναι επιρρεπείς στις επιθέσεις πλευρικών καναλιών (side channel attacks), οι οποίες εκμεταλλευόμενες επιπλέον και τις αδυναμίες του COPM128, μπορούν πολύ αποτελεσματικά να αποκαλύψουν το μυστικό κλειδί K_i.
- Είναι ευάλωτες και σε επιθέσεις που στηρίζονται στην εισαγωγή οπτικών σφαλμάτων που θέτουν άμεσα σε κίνδυνο ευαίσθητες πληροφορίες αποθηκευμένες στην κάρτα, όπως η ταυτότητα IMSI και το κλειδί K_i.

2.5.5 Όχι τόσο ασφαλής η κάρτα SIM (2/2)
Λύσεις στο πρόβλημα

- Πολλά τσιπάκια σήμερα έχουν αρχίσει να κατασκευάζονται με ένα υλικό που καταστρέφει το τσιπ αν αυτό μετακινηθεί.
- Στα νέα κυκλώματα εισάγονται πολλά κενά κυκλωματικά στοιχεία, που δεν εκτελούν καμία συγκεκριμένη λειτουργία, με σκοπό να εξαπατήσουν τους επίδοξους εισβολείς.

2.5.6 Οι ζεύξεις μετά το BTS δεν κρυπτογραφούνται (1/3)

- Το γεγονός ότι η σύνδεση BTS – BSC σε πολλές περιπτώσεις είναι μικροκυματική αποτελεί ένα επισφαλές σημείο στην ασφάλεια του GSM.
- Η ζεύξη μπορεί να κρυφακουσθεί από τη στιγμή που τα δεδομένα σ' αυτήν δεν κρυπτογραφούνται όπως στη ραδιοζεύξη.
- Και οι συνδέσεις BSC – MSC, που είναι άλλοτε μικροκυματικές και άλλοτε σταθερές, δεν κρυπτογραφούνται και όλες οι πληροφορίες σχετικά με τα κλειδιά κρυπτογράφησης και τα δεδομένα πιστοποίησης μεταφέρονται σε 'καθαρή' μορφή τόσο μέσα στο ίδιο το δίκτυο όσο και μεταξύ των δικτύων.

2.5.6 Οι ζεύξεις μετά το BTS δεν κρυπτογραφούνται (2/3)
Χρήση του πρωτοκόλλου ασφαλείας MAPSec

- Το πρωτόκολλο MAPSec έχει ως σκοπό να παρέχει προστασία σε επίπεδο εφαρμογής κατά τη μεταφορά των μηνυμάτων μέσα στο δίκτυο SS7 του GSM ή μεταξύ δύο διαφορετικών SS7 δικτύων.
- Αποτελεί ένα προσθετικό μέτρο ασφαλείας στο GSM και δεν επηρεάζει την υπάρχουσα δομή του συστήματος. [14]

2.5.6 Οι ζεύξεις μετά το BTS δεν κρυπτογραφούνται (3/3)
Χρήση του πρωτοκόλλου ασφαλείας MAPSec

- Οι υπηρεσίες που προσφέρονται από το MAPSec είναι:
  - Έλεγχος πρόσβασης χρηστών σε δεδομένα.
  - Πιστοποίηση ακεραιότητας δεδομένων.
  - Πιστοποίηση ταυτότητας χρηστών.
  - Αποφυγή επανεκπομπής πακέτων.
  - Απόκρυψη δεδομένων.

2.5.7 Δεν προστατεύονται επαρκώς οι οντότητες του δικτύου σηματοδοσίας (1/4)

- Η πρόσβαση στα κέντρα του δικτύου και στις βάσεις δεδομένων ελέγχεται χάρη στη χρησιμοποίηση username και password.
- Η πρόσβαση αυτή δεν είναι αρκετά αυστηρή, με αποτέλεσμα πολλοί εισβολείς να είναι σε θέση να μαντεύουν και να σπάνε τους κωδικούς ασφαλείας.
- Ο έλεγχος στα σημεία εισόδου δεν εφαρμόζεται για όλα τα μηνύματα και συνεπώς τα περισσότερα από αυτά λαμβάνονται χωρίς πρώτα να ‘φιλτράρονται’.

2.5.7 Δεν προστατεύονται επαρκώς οι οντότητες του δικτύου σηματοδοσίας (2/4)

Προτεινόμενες Λύσεις

- Δεν πρέπει να επιτρέπεται η χρησιμοποίηση ενός password από πολλούς διαφορετικούς χρήστες.
- Για όλους τους κωδικούς πρόσβασης στα κέντρα και στις βάσεις δεδομένων, πρέπει να υφίσταται σε κάθε δίκτυο ένα ξεχωριστό κέντρο διαχείρισης, που θα διαφυλάσσει τα passwords σε κρυπτογραφημένη μορφή.
- Η πρόσβαση σε αυτό το κέντρο να είναι αυστηρά περιορισμένη.
- Τα passwords πρέπει να επιλέγονται κατά τέτοιο τρόπο ώστε να έχουν την απαιτούμενη πολυπλοκότητα που δε θα επιτρέπει σε έναν τρίτο να τα μαντέψει εύκολα.

2.5.7 Δεν προστατεύονται επαρκώς οι οντότητες του δικτύου σηματοδοσίας (3/4)

Προτεινόμενες Λύσεις

- Κάθε οντότητα δεν πρέπει να πραγματοποιεί συνόδους διαμέσου θυρών οι οποίες δεν είναι εξουσιοδοτημένες να δεχθούν εισερχόμενα μηνύματα, ενώ αν μία σύνοδος για κάποιο λόγο διακόπτεται, η συγκεκριμένη θύρα πρέπει αμέσως να απορρίπτεται.
- Σε περίπτωση που κατά την πιστοποίηση ένα πεδίο εισάγεται εσφαλμένα, κανένα μήνυμα βοήθειας, όπως π.χ. ποιο πεδίο δεν έχει εισαχθεί σωστά, δεν πρέπει να εμφανίζεται και μόνο στο τέλος να παρουσιάζεται η πληροφορία ότι το login είναι άκυρο.
- Μετά από ένα συγκεκριμένο αριθμό αποτυχημένων προσπαθειών για πρόσβαση σε μία οντότητα, πρέπει να ενημερώνεται σχετικά το κέντρο διαχείρισης.

2.5.7 Δεν προστατεύονται επαρκώς οι οντότητες του δικτύου σηματοδοσίας (4/4)

Προτεινόμενες Λύσεις

- Πριν την έναρξη μιας συνόδου, πρέπει να παρέχεται στο χρήστη του κέντρου ή της βάσης δεδομένων ένα προειδοποιητικό μήνυμα σχετικά με τις συνέπειες μη εξουσιοδοτημένης πρόσβασης.
- Κατά την έναρξη της συνόδου, πρέπει να εμφανίζεται η ημερομηνία και η ώρα της τελευταίας επιτυχημένης πρόσβασης καθώς και ο αριθμός των αποτυχημένων προσπαθειών που έλαβαν χώρα από την τελευταία επιτυχή πρόσβαση.
- Αν για ένα χρονικό διάστημα δεν ανταλλάσσονται μηνύματα, πρέπει η σύνοδος να απελευθερώνεται και ο χρήστης μιας οντότητας να επαναπιστοποιείται. [12]

2.5.8 Άλλα αδύνατα σημεία του GSM (1/3)

- Είναι δυνατόν ένας τρίτος, που αποκτά μη εξουσιοδοτημένη πρόσβαση σε κάποιον κινητό σταθμό που είναι κλεμμένος ή φραγμένος, να τροποποιήσει κατάλληλα τον αριθμό IMEI ώστε να μπορεί από κει και πέρα να χρησιμοποιήσει νόμιμα τη συσκευή και να πραγματοποιεί νόμιμη πρόσβαση στους πόρους του δικτύου.
- Συνεπώς, οι αριθμοί IMEI, που αναγνωρίζουν κατά μοναδικό τρόπο μία συσκευή, πρέπει να καθορίζονται έτσι, ώστε να καθίσταται δύσκολη η μετατροπή αυτών σε περίπτωση γνωστοποίησής τους. [10]

2.5.8 Άλλα αδύνατα σημεία του GSM (2/3)

- Κατά το σχεδιασμό του GSM δεν είχε ληφθεί υπόψη η διενέργεια ‘νόμιμης παρεμβολής’ (Lawful Interception – LI).
- Σε κάθε δίκτυο, πρέπει να παρέχεται η δυνατότητα στους πράκτορες επιβολής του νόμου να παρεμβάλλονται και να παρακολουθούν κλήσεις ή άλλες υπηρεσίες, που σχετίζονται με τους χρήστες, σύμφωνα πάντα με τους διεθνείς νόμους.
- Η διαδικασία αυτή αποσκοπεί μόνο στη νόμιμη παρακολούθηση των ζεύξεων, αλλά στο GSM δεν έχει εισαχθεί.

2.5.8 Άλλα αδύνατα σημεία του GSM (3/3)

- Στο χρήστη δεν είναι εμφανή τα χαρακτηριστικά ασφαλείας που εφαρμόζονται (lack of visibility).
- Ο συνδρομητής δεν έχει καμία ένδειξη ότι είναι πιστοποιημένος ούτε και ότι πράγματι χρησιμοποιείται κρυπτογράφηση.
- Κάθε χρήστης πρέπει να βλέπει τα στοιχεία ασφαλείας που του προσφέρονται και να μπορεί κάθε φορά να επιλέξει ο ίδιος αυτά που επιθυμεί να εφαρμοστούν.
- Αν πρόκειται ένας συνδρομητής να μεταδώσει ευαίσθητα δεδομένα, πρέπει να μπορεί να ενεργοποιήσει τη δυνατότητα χρησιμοποίησης του MAPSec, για την προστασία των μηνυμάτων στο δίκτυο σηματοδοσίας, μαρκάροντας την αντίστοιχη επιλογή. [8]

3.1 Συμπεράσματα

- Διαπιστώνεται ότι το μοντέλο ασφαλείας του GSM εφαρμόζεται κατά κύριο λόγο στη ραδιοζεύξη.
- Το δίκτυο σηματοδοσίας, που περιλαμβάνει ως επί το πλείστον ενσύρματες και ενίοτε μικροκυματικές ζεύξεις, παραμένει σχεδόν απροστάτευτο.
- Παρόλα αυτά, παρουσιάζει πολλές και σοβαρές αδυναμίες που μπορούν να θέσουν σε κίνδυνο ευαίσθητα δεδομένα των χρηστών. Το γεγονός αυτό έχει ληφθεί υπόψη στα δίκτυα τρίτης γενιάς (UMTS), όπου αρκετές από τις υπάρχουσες αδυναμίες του GSM εξαλείφονται, καθώς το επίπεδο ασφαλείας αυξάνεται, οδηγώντας έτσι σε πιο ασφαλείς μεταδόσεις.

4.1 Βιβλιογραφία (1/3)

- **[1]**Asha Mehrotra, «*GSM System Engineering*», Artech House, 1997.
- **[2]**Δημοσθένης Σούλης, «*Το Πανευρωπαϊκό Σύστημα Κινητής Τηλεφωνίας G.S.M. και η Εφαρμογή του στην Ελλάδα*», Αθήνα – Μάρτιος 1992.
- **[3]**Paulo S. Pagliusi, «*A Contemporary Foreword on GSM Security*», Springer – Verlag, London UK, 2002 , http://www.portal.acm.org .
- **[4]**Pacharawit Topak – Ngarm, Panupat Poocharoen, «*GSM Security Vulnerability*», http://oregonstate.edu.
- **[5]**ISAAC Research Group, Ian Goldberg, Marc Briceno, «*GSM Cloning*», Publication, April, 1998, http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

4.1 Βιβλιογραφία (2/3)

- **[6]**Alex Biryukov, Adi Shamir, David Wagner, «*Real Time Cryptanalysis of A5/1 on a PC*», New York, April 2000 , http://cryptome.org/a51-bsw.htm.
- **[7]**Elad Barkan, Eli Biham, Nathan Keller, «*Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*», International Association for Cryptologic Research, 2003 , http://www.springerlink.com .
- **[8]**Bart Preneel, «*Mobile Network Security*», Katholieke Universiteit Leuven, June 2003, http://www.esat.kuleuven.ac.be .
- **[9]**Antti Siitonen, «*GSM & GPRS*», Lectures, November 2003, http://www.tml.hut.fi .

4.1 Βιβλιογραφία (3/3)

- **[10]**Geir Stian Bjåen, Erling Kaasin, «*Security in GPRS*», Master Thesis in Information and Communication Technology, Grimstad, May 2001, http://siving.hia.no/ikt01/ikt6400/ekaasin/Master%20Thesis%20Web.htm.
- **[11]**Christos Xenakis, Lazaros Merakos, «*Security in third Generation Mobile Networks*», Elsevier B.V., 2004.
- **[12]**3GPP TR *33.900*, 3rd Generation Partnership Project ; Technical Specification Group SA WG3 ; *A Guide to 3rd Generation Security*, January 2000.
- **[13]**3GPP TS *33.102*, 3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3G Security ; *Security Architecture*, December 2000, (Release 1999).
- **[14]**3GPP TS *33.200*, Network Domain Security; *MAP Application Layer Security*, December 2002, (Release 5).