ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ

« ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΩΝ ΣΕ ΣΥΣΚΕΥΕΣ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ»

ΦΟΙΤΗΤΡΙΑ : ΓΡΙΒΑ ΚΩΝΣΤΑΝΤΙΝΑ

ΑΡΙΘΜΟΣ ΜΗΤΡΩΟ : 1175

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : Δρ. Τσακανίκας Βασίλειος Επίκουρος Καθηγητής Τμήματος ΤΕΣΥΔ ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΟΣ

ΝΑΥΠΑΚΤΟΣ, ΙΟΥΛΙΟΣ 2014

ΠΕΡΙΛΗΨΗ

Στην πτυχιακή αυτή εργασία αναλύονται η ιστορία της κινητής τηλεφωνίας, από την πρώτη γενιά έως και την τέταρτη γενιά κινητών δικτύων. Καθώς, τα χαρακτηριστικά και την ανάγκη των χρηστών για να αποκτήσουν τις νέες συσκευές κινητών που κυκλοφορούν μέσα από παραδείγματα. Στην συνέχεια, θα αναφερθούν αναλυτικά στα κυριότερα δίκτυα κινητής τηλεφωνίας GSM, GPRS και UMTS. Στα γενικά χαρακτηριστικά τους, στην αρχιτεκτονική – δομή των δικτύων και στα πρωτόκολλα που υλοποιούν. Τέλος, θα γίνει μια αναλυτική περιγραφή των επιθέσεων και των απειλών στα συστήματα Android, Symbian και στα κινητά τηλέφωνα smartphone και τα tablet που καθημερινά απειλούνται από νέους ιούς.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Ιστορική αναδρομή κινητής τηλεφωνίας, 1^{η} γενιά, 2^{η} γενιά, 2.5^{η} γενιά, 3^{η} γενιά, 3.5γενιά, 4^{η} γενιά κινητής τηλεφωνίας, αρχιτεκτονική και πρωτόκολλα των GSM, GPRS, UMTS, LTE, επιθέσεις σε δίκτυα και λογισμικά,

ABSTRACT

In this thesis work analyzes the history of the mobile phone, from the first generation through fourth generation mobile networks. As the characteristics and the user need to acquire new mobile devices that circulate through examples. Then, you mentioned in detail in the main mobile networks GSM, GPRS and UMTS. In general characteristics, architecture - structure of networks and protocols implement. Finally, there will be a detailed description of the attacks and threats to systems Android, Symbian and mobile phones smartphone and tablet that daily threatened by new viruses.

KEYWORDS

1G, 2G, 3G, 4G, GSM, GPRS, UMTS, LTE, attacks mobile networks: Eavesdropping, Impersonation of a user, Impersonation of the network, Man in the middle, Compromising authentication vectors in the network, attacks Symbian, Android, Smartphone, Tablet

ΕΥΧΑΡΙΣΤΙΕΣ

Κλείνοντας την σύντομη περίληψη θα ήθελα να ευχαριστήσω τους γονείς μου Ευάγγελο και Παναγιώτα που με στήριξαν, καθώς και τα αδέλφια μου Μαρία και Γιώργο που ανέχτηκαν τις ατέλειωτες ώρες απουσίας μου. Ιδιαίτερα θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κύριο Τσακανίκα Βασίλειο, επιβλέποντα καθηγητή της πτυχιακής, για την άριστη συνεργασία μας και την πολύτιμη βοήθεια του. Φυσικά δεν θα παραλείψω να ευχαριστήσω όλους τους καθηγητές του τμήματος Τηλεπικοινωνιακών Συστημάτων και Δικτύων ΤΕΙ Δυτικής Ελλάδας που επιβράβευσαν την προσπάθεια μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΟ ΕΙΚΩΝΩΝ

ΑΚΡΟΝΥΜΙΑ

ATM: Asynchronous Transfer Mode
AuC: Authentication Center
BSS: Base Station Subsystem
BTS: Base Transceiver Station
BSC: Base Station Controler
CN: Core Network
CDMA: Code Division Multiple Access
D-AMPS: Digital Advanced Mobile Phone Service
ETSI: European Telecommunications Standards Institute
E-GSM: Extended- Global System for Mobile
EDGE: Enhanced Data Rates for Global Evolution
GPRS: General Packet Radio Services
GGSN: Gateway GPRS Support Node
GSM: Global System for Mobile
GMSC: Gateway Mobile Services Switching Center
HSCSD: High-Speed Circuit- Switched Data
HSPA: High Speed Packet Access
HLR: Home Location Register
HSDPA: High Speed Downlink Packet Access
HSUPA: High Speed Uplink Packet Access
HS-DSCH: High-Speed Downlink Shared Channel
Iu-CS: Iu-Circuit Switched
Iu-PS: Iu-Packet Switched
LTE: Long Term Evolution
MMS: Multimedia Messaging Service
MSC: Mobile Services Switching Center
MS: Mobile Station

NNS: Network Switching Subsystem
NMT: Nordic Mobile Telephone
PDC: Personal Digital Cellular
PDA: Personal Digital Assistant
RNC: Radio Network Controllers
RA: Routing Areas
SGSN: Serving GPRS Support Node
TACS: Total Access Communication System
UMTS: Universal Mobile Telecommunication System
UE: User Equipment
VLR: Visitor Location Register

ΚΕΦΑΛΑΙΟ 1^{ο}

"ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΔΙΚΤΥΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ"

Το κεφάλαιο αυτό κάνει μία εισαγωγική αναφορά στα δίκτυα κινητής τηλεφωνίας έως και την τέταρτη γενιά. Αρχικά, γίνεται μία ιστορική αναδρομή και παρουσιάζονται τα βασικά χαρακτηριστικά των συστημάτων κινητής τηλεφωνίας. Έπειτα, γίνεται ιστορική αναδρομή στα χαρακτηριστικά των κινητών, παραδείγματα συσκευών κινητής τηλεφωνίας και την ανάγκη των χρηστών για να τα αποκτήσουν.

1. Ιστορία της Κινητής Τηλεφωνίας

Από το 1940 και μετά παρατηρούμε την ανάπτυξη και την εξέλιξη της κινητής τηλεφωνίας. Η περιπέτεια της κινητής τηλεφωνίας ξεκίνησε αμέσως μετά τον Β΄ Παγκόσμιο Πόλεμο, με τις πρώτες προσπάθειες των Σουηδών, Φινλανδών και Αμερικανών. Όμως ως ληξιαρχική πράξη γέννησής της θεωρείται η 3η Απριλίου 1973.

Το πρώτο αυτοματοποιημένο δίκτυο κινητής τηλεφωνίας λειτούργησε στις αρχές της δεκαετίας του '80 στη Σκανδιναβία. Μέχρι τα τέλη της δεκαετίας του '80 τα κινητά τηλέφωνα ήταν ογκώδη για να μεταφέρονται στην τσέπη κι έτσι ήταν εγκατεστημένα κυρίως σε αυτοκίνητα. Το πρώτο κινητό που έλαβε άδεια έγκρισης ήταν το μοντέλο της MotorolaDynaTAC8000X είχε ύψος 25 εκατοστά και βάρος 900 γραμμάρια. Υπήρξε η ναυαρχίδα των λεγόμενων κινητών πρώτης γενιάς (1G).

Στην αρχή της δεκαετίας του '90 άρχισε η απογείωση των κινητών τηλεφώνων, με την ψηφιοποίηση δικτύων (GSM) και συσκευών. Τα κινητά έγιναν μικρότερα (100-200 γραμμάρια), χωρούσαν στην παλάμη και έμπαιναν έστω και με δυσκολία στην

τσέπη του χρήστη τους. Περάσαμε έτσι στα κινητά της δεύτερης γενιάς (2G) που παρείχαν και άλλες ευκολίες, όπως την αποστολή σύντομων γραπτών μηνυμάτων (SMS) και τη λήψη φωτογραφιών.
Στις αρχές του 21ου αιώνα ήρθαν τα κινητά τρίτης γενιάς (3G) η τεχνολογία UMTS έρχεται με απεριόριστες δυνατότητες των πολυμέσων και μεταφοράς δεδομένων. Το 2010 η τέταρτη γενιά (4G) η τεχνολογία LTE κάνει την εμφάνισή της στις ΗΠΑ, Ασία και Ιαπωνία. Τα κινητά αποκτούν μεγάλες ταχύτητες στην πρόσβαση διαδικτύου και όχι μόνο. Σήμερα, η διείσδυση του κινητού τηλεφώνου στον πλανήτη ξεπερνά το 30%, με αλματώδη άνοδο στις φτωχές χώρες του πλανήτη και κυρίως στην Αφρική. Στην Ελλάδα, μάλιστα, η κινητή τηλεφωνία έκανε την εμφάνισή της το 1992.

1.1 Η 1η Γενιά Κινητών Δικτύων

Η πρώτη γενιά συστημάτων κυψελωτής κινητής τηλεφωνίας εμφανίστηκε τη δεκαετία του 1980. Παρόλα αυτά, η συγκεκριμένη γενιά δεν αποτέλεσε το ξεκίνημα των κινητών τηλεπικοινωνιών. Αντίθετα από πιο πριν είχαν εμφανιστεί αρκετά συστήματα κινητών τηλεπικοινωνιών τα οποία όμως δεν είχαν τα χαρακτηριστικά των κινητών δικτύων με τον τρόπο που τα εννοούμε σήμερα. Το βασικότερο από αυτά είναι η κυψελωτή δομή του δικτύου. Τα πρώιμα αυτά δίκτυα είχαν περιορισμένες δυνατότητες σε σχέση με τα κυψελωτά. Ένα άλλο σημαντικό μειονέκτημα ήταν η υποτυπώδης και προβληματική υποστήριξη της κινητικότητας των χρηστών.

Στα κυψελωτά κινητά δίκτυα, που στο εξής θα αναφέρονται απλώς σαν κινητά δίκτυα, η περιοχή κάλυψης διαιρείται σε μικρά κελιά. Με αυτόν τον τρόπο οι ίδιες συχνότητες μπορούν να χρησιμοποιούνται πολλές φορές στο ίδιο δίκτυο χωρίς να δημιουργούνται έντονα φαινόμενα παρεμβολής. Επομένως, οι δυνατότητες του δικτύου αυξάνονται σημαντικά. Η πρώτη γενιά χρησιμοποιούσε τεχνικές αναλογικής μετάδοσης για την κίνηση η οποία ήταν αποκλειστικά η φωνή. Δεν υπήρξε κάποιο πρότυπο που να επικράτησε, αντίθετα υπήρξαν αρκετά πετυχημένα πρότυπα όπως το Nordic Mobile Telephone (NMT), το Total Access Communication System (TACS) και το Advanced Mobile Phone Service (AMPS). Τα δύο πρώτα είχαν μία σχετική επιτυχία στις ευρωπαϊκές χώρες, ενώ το τρίτο ήταν πιο διαδεδομένο στις Η.Π.Α.

Αξίζει να σημειωθεί εδώ ότι παρόλο που σήμερα η εξέλιξη στις τηλεπικοινωνίες έχει εστιαστεί στα κινητά δίκτυα τρίτης γενιάς, υπάρχουν πολλά δίκτυα πρώτης γενιάς που εξακολουθούν να βρίσκονται σε λειτουργία. Βέβαια, στις χώρες όπου υπάρχει προχωρημένη υποδομή στις τηλεπικοινωνίες τα συστήματα αυτά έχουν εγκαταλειφθεί καθώς θεωρείται ότι σπαταλούν πολύτιμο φάσμα συχνοτήτων το οποίο τα σύγχρονα ψηφιακά κινητά δίκτυα επικοινωνιών εκμεταλλεύονται πιο αποδοτικά.

1.2 Η 2η Γενιά Κινητών Δικτύων

Η δεύτερη γενιά κινητών δικτύων επικοινωνιών χρησιμοποιεί ψηφιακή μετάδοση της κίνησης. Αυτή είναι και η κύρια διαφοροποίηση μεταξύ των κινητών συστημάτων

πρώτης και δεύτερης γενιάς: ο διαχωρισμός αναλογικού – ψηφιακού. Τα δίκτυα δεύτερης γενιάς έχουν πολύ ευρύτερες δυνατότητες από αυτά της πρώτης. Ένα κανάλι συχνοτήτων διαιρείται και μπορεί να χρησιμοποιηθεί από διαφορετικούς χρήστες (είτε με διαίρεση χρόνου, είτε με διαίρεση κώδικα). Επιπλέον χρησιμοποιούνται ιεραρχικές δομές κελιών. Πιο συγκεκριμένα η περιοχή κάλυψης διαιρείται σε macrocells (κελιά μεγάλης έκτασης), microcells (κελιά μικρής έκτασης) και picocells (κελιά περιορισμένης έκτασης κυρίως σε μεγάλα αστικά κέντρα), με αποτέλεσμα την περαιτέρω αύξηση των δυνατοτήτων των δικτύων.

Υπάρχουν τέσσερα κύρια πρότυπα για τα κινητά δίκτυα δεύτερης γενιάς: το Global System for Mobile (GSM) communications, το Digital AMPS (D-AMPS), το Code Division Multiple Access (CDMA) IS-95 καθώς και το Personal Digital Cellular (PDC). **Το GSM** είναι μακράν το πιο επιτυχημένο και διαδεδομένο σύστημα δεύτερης γενιάς. Ξεκίνησε ως ένα ευρωπαϊκό σύστημα αλλά τελικά υιοθετήθηκε παγκοσμίως. Η μόνη ήπειρος στην οποία η διάδοση του υστερεί είναι η Αμερικανική. Το βασικό σύστημα GSM χρησιμοποιεί τη ζώνη συχνοτήτων των 900 MHz. Όμως υπάρχουν και αρκετά παράγωγα τα οποία χρησιμοποιούν τις ζώνες των 1800 ή 1900 MHz. Ο βασικότερος λόγος ήταν η έλλειψη χωρητικότητας χρηστών στη ζώνη των 900 MHz. Η ζώνες των 1800 ή 1900 MHz μπορούν να εξυπηρετήσουν πολύ μεγαλύτερο αριθμό χρηστών, κυρίως σε πυκνοκατοικημένες περιοχές. Η περιοχή κάλυψης όμως μειώνεται σε σχέση με τα συστήματα που λειτουργούν στη ζώνη των 900 MHz. Αξίζει στο σημείο αυτό να αναφερθεί και το πρότυπο GSM-400 που αναπτύχθηκε από το ίδρυμα European Telecommunications Standards Institute (ETSI) και το οποίο χρησιμοποιήθηκε συμπληρωματικά των δικτύων GSM με υψηλότερες συχνότητες. Παρόλο που το σύστημα αυτό ήταν αρκετά αποδοτικό σε αραιοκατοικημένες και παράκτιες περιοχές, το πρότυπο GSM-400 δε χρησιμοποιείται πλέον [1].

Το D-AMPS (επίσης γνωστό ως US-TDMA, IS-136, ή απλά TDMA) χρησιμοποιείται για την Αμερική, το Ισραήλ, και σε ορισμένες χώρες της Ασίας. Είναι συμβατό με το AMPS. Το AMPS, είναι ένα αναλογικό σύστημα. Το D-AMPS, ορίζεται στο πρότυπο IS-54, εξακολουθεί να χρησιμοποιεί ένα αναλογικό κανάλι ελέγχου, αλλά το κανάλι της φωνή είναι ψηφιακό. Εισήχθη για πρώτη φορά το 1990. Το επόμενο βήμα στην εξέλιξη των κινητών επικοινωνιών ήταν ένα πλήρως ψηφιακό σύστημα το 1994.

Το CDMA (Code Division Multiple Access), και εδώ εννοούμε το πρότυπο IS-95 που αναπτύχθηκε από την Qualcomm, χρησιμοποιεί μια διαφορετική προσέγγιση στη μετάδοση μέσω του αέρα. Αντί για τη διαίρεση συχνοτήτων σε χρονοθυρίδες TDMA, το CDMA χρησιμοποιεί διαφορετικούς κωδικούς σε ξεχωριστές μεταδόσεις στην ίδια συχνότητα. Το IS-95 είναι το μόνο 2G CDMA πρότυπο μέχρι σήμερα που λειτουργεί εμπορικά. Χρησιμοποιείται στις Ηνωμένες Πολιτείες, τη Νότια Κορέα, Χονγκ Κονγκ, Ιαπωνία, Σιγκαπούρη, και σε πολλές άλλες χώρες της Ανατολικής Ασίας. Τα δίκτυα που χρησιμοποιούν αυτό το πρότυπο είναι επίσης γνωστά με την επωνυμία cdmaOne.

Το PDC είναι το Ιαπωνικό 2G πρότυπο. Αρχικά, ήταν γνωστό ως Japanese Digital Cellular (JDC), αλλά το όνομα άλλαξε σε Personal Digital Cellular (PDC) για να κάνει το σύστημα πιο ελκυστικό εκτός Ιαπωνίας. Ωστόσο, αυτή η μετονομασία δεν

έφερε τα επιθυμητά αποτελέσματα, με αποτελέσματα αυτό το πρότυπο χρησιμοποιηθεί εμπορικά μόνο στην Ιαπωνία. Οι προδιαγραφές που είναι γνωστές ως RCR STD-27, και το σύστημα λειτουργεί σε δύο ζώνες συχνοτήτων: 800 MHz και 1500 MHz. Μπορεί να χρησιμοποιήσει αναλογική και ψηφιακή μετάδοση. Το φυσικό επίπεδο είναι παρόμοιο με D-AMPS, αλλά η στοίβα πρωτοκόλλου μοιάζει στο GSM.

1.3 Η 2,5η Γενιά Κινητών Δικτύων

Με τον όρο «γενιά 2,5» αναφερόμαστε στο ευρύτερο σύνολο των αναβαθμίσεων που έγιναν πάνω στα κινητά δίκτυα δεύτερης γενιάς. Πολλές από αυτές τις αναβαθμίσεις παρέχουν σχεδόν τις ίδιες δυνατότητες με αυτές των κινητών δικτύων τρίτης γενιάς. Η διαχωριστική γραμμή μεταξύ των κινητών δικτύων δεύτερης γενιάς και αυτών της γενιάς 2,5 είναι λεπτή. Η γενιά 2,5 χαρακτηρίζεται από ορισμένες τεχνολογίες οι οποίες είναι : η High-Speed Circuit- Switched Data (HSCSD), η General Packet Radio Services (GPRS) και η Enhanced Data Rates for Global Evolution (EDGE).

Το μεγαλύτερο πρόβλημα που παρουσίασαν οι αρχικές μορφές του GSM ήταν οι χαμηλοί ρυθμοί μετάδοσης στον αέρα που περιορίζονταν στα 9,6 Kbps. Αργότερα, τέθηκαν οι προδιαγραφές για τα 14,4 Kbps παρόλο που δε χρησιμοποιήθηκαν ευρέως. Η λύση που προτάθηκε ήταν η τεχνολογία HSCSD. Μέσω αυτής της τεχνολογίας ένας χρήστης μπορεί να χρησιμοποιεί, αντί μίας, περισσότερες χρονοσχισμές (timeslots) για μία σύνδεση μεταφοράς δεδομένων. Συνεπώς, ο ρυθμός μετάδοσης για αυτόν το χρήστη είναι το γινόμενο των χρονοσχισμών επί το ρυθμό μετάδοσης για μία χρονοσχισμή. Η υλοποίηση της συγκεκριμένης τεχνολογίας είναι σχετικά απλή και φθηνή. Πρόσθετο λογισμικό χρειάζεται να υλοποιηθεί στα κέντρα καθώς και καινούριες φορητές συσκευές που θα υποστηρίζουν την τεχνολογία HSCSD. Το βασικότερο μειονέκτημα ήταν η χρήση μεταγωγής κυκλώματος. Που είχε ως αποτέλεσμα τη σπατάλη πόρων του δικτύου αφού οι χρονοσχισμές δεσμεύονταν ακόμα και όταν η χωρητικότητά τους δεν χρησιμοποιούνταν.

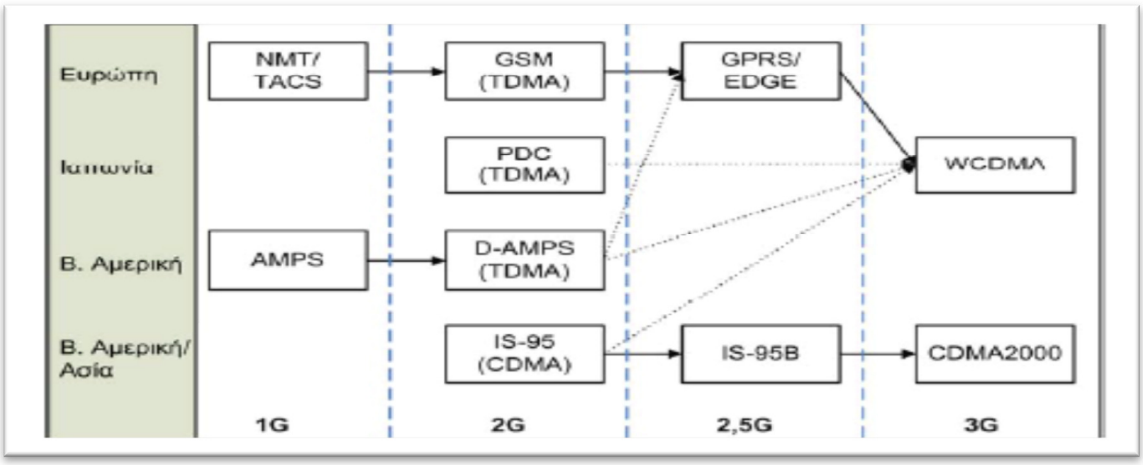
Η επόμενη λύση που προτάθηκε ήταν η τεχνολογία GPRS. Με αυτήν την τεχνολογία μπορούν να επιτευχθούν ρυθμοί μετάδοσης των 115 Kbps ή και ακόμα μεγαλύτεροι αν αγνοηθεί η διόρθωση σφαλμάτων. Αυτό που έχει μεγάλη σημασία είναι ότι η τεχνολογία GPRS χρησιμοποιεί τεχνολογία μεταγωγής πακέτου. Αναλυτικότερα, δεσμεύει τους πόρους του δικτύου μόνο όταν υπάρχει ανάγκη για αποστολή ή λήψη δεδομένων. Η υλοποίηση του GPRS είναι αρκετά πιο ακριβή σε σχέση με αυτή του HSCSD. Επιπρόσθετα, το HSCSD συμπεριφέρεται με μεγαλύτερη συνέπεια σε εφαρμογές πραγματικού χρόνου. Παρόλα αυτά, η τεχνολογία GPRS προσφέρει πολύ μεγαλύτερες δυνατότητες για την αποστολή δεδομένων μέσω των κινητών δικτύων. Είναι σίγουρο πλέον πως η αύξηση της κίνησης δεδομένων στα κινητά δίκτυα, καθιστά την τεχνολογία GPRS αναπόσπαστο στοιχείο ενός συστήματος κινητής τηλεφωνίας.

Τέλος, η τρίτη και τελευταία βελτίωση του GSM προκειμένου να εξελιχθεί σε ένα δίκτυο γενιάς 2,5 είναι η EDGE. Η βασική ιδέα πίσω από το EDGE είναι μία τεχνική διαμόρφωσης που ονομάζεται Eight-Phase Shift Keying (8PSK). Αυτή η τεχνική επηρεάζει μόνο το λογισμικό των σταθμών βάσης και προσφέρει έως και τριπλάσιο ρυθμό μετάδοσης από το βασικό ρυθμό μετάδοσης του GSM. Επιπλέον, μπορεί να

συνυπάρξει με την τεχνική διαμόρφωσης Gaussian Minimum Shift Keying (GMSK) η οποία χρησιμοποιείται στη βασική μορφή του GSM.
Αν το EDGE χρησιμοποιείται με το GPRS, τότε ο συνδυασμός είναι γνωστός ως ενισχυμένο GPRS (EGPRS). Το μέγιστο ποσοστό των δεδομένων που μπορεί να φτάσει κάποιος χρησιμοποιώντας το EGPRS είναι 384 Kbps χρησιμοποιώντας οκτώ χρονοθυρίδες (μαζί με κώδικες σφαλμάτων). Σημειώστε ότι οι ρυθμοί των 384 Kbps επιτυγχάνονται μόνο με τη χρήση όλων των πόρων του ραδιοφωνικού φάσματος και ακόμη και τότε μόνο όταν το κινητό βρίσκεται κοντά στο σταθμό βάσης. Το ECSD είναι ο συνδυασμός των EDGE και HSCSD και παρέχει επίσης τριπλάσιες ταχύτητες από το πρότυπο HSCSD. Ο συνδυασμός των τριών αυτών μεθόδων παρέχει ένα ισχυρό σύστημα, και είναι ένα πρόωιμο στάδιο για τα δίκτυα 3G.

1.4 Η 3η Γενιά Κινητών Δικτύων

Η γρήγορη εξέλιξη των κινητών τηλεπικοινωνιών ήταν ένα από τα αναμφισβήτητα γεγονότα της δεκαετίας του 1990. Το πρώτο εμπορικό δίκτυο GSM λειτούργησε στη Φινλανδία το 1991. Την ίδια χρονιά, το ίδρυμα ETSI ξεκινούσε την προτυποποίηση της επόμενης γενιάς δικτύων κινητών τηλεπικοινωνιών. Το σύστημα που προέκυψε από αυτή την προτυποποίηση ονομάστηκε Universal Mobile Telecommunications System (UMTS). Η ανάπτυξη των κινητών δικτύων τρίτης γενιάς δεν έγινε μόνο στο ETSI. Υπήρξαν πολλοί οργανισμοί και ερευνητικά ιδρύματα, σε παγκόσμιο επίπεδο, που είχαν τον ίδιο σκοπό. Στην Εικόνα 1 δείχνει σχηματικά την εξέλιξη των προτύπων για τα κυψελωτά κινητά δίκτυα μέχρι την τρίτη γενιά [2][3].



Εικόνα 1: Η εξέλιξη των προτύπων για τα κυψελωτά κινητά δίκτυα έως το 3G

Ο βασικός στόχος της ανάπτυξης των κινητών δικτύων τρίτης γενιάς είναι η παροχή των κινητών υπηρεσιών «οπουδήποτε» και «κάθε στιγμή». Αυτό σημαίνει ότι ένας χρήστης δικτύων κινητής τηλεφωνίας τρίτης γενιάς μπορεί να μετακινείται οπουδήποτε και να εξυπηρετείται ακόμα και σε περιοχές όπου δεν υπάρχει κάλυψη από συστήματα τρίτης γενιάς αλλά υπάρχουν άλλου είδους ασύρματα δίκτυα. Για την

ακρίβεια, ο χρήστης θα μπορεί να εξυπηρετείται από οικιακά ασύρματα συστήματα, από άλλα κυψελωτά κινητά δίκτυα καθώς και από δορυφορικά δίκτυα.

Επιπλέον, οι παρεχόμενες υπηρεσίες επεκτείνονται σε υπηρεσίες διαδικτύου και σε υπηρεσίες πολυμέσων με υψηλούς ρυθμούς μετάδοσης (προβλέπονται ρυθμοί που ξεκινούν από τα 144 Kbps και φτάνουν ακόμα και σε ρυθμούς της τάξης των Mbps). Με τον όρο υπηρεσίες πολυμέσων αναφερόμαστε σε υπηρεσίες κατά τις οποίες υπάρχει συνδυασμός εικόνας, ήχου και κειμένου σε ένα διαρκώς μεταβαλλόμενο ψηφιακό περιβάλλον. Τέλος, θα πρέπει να αναφερθούν τα επικρατέστερα, προς το παρόν, συστήματα τρίτης γενιάς τα οποία είναι: το UMTS (Ευρώπη), το CDMA2000και το NTT Docomo (Ιαπωνία).

Η 3G τεχνολογία αποτελεί βελτίωση των 2G συστημάτων. Χρησιμοποιεί μεταγωγή πακέτων αντί για μεταγωγή κυκλώματος. Χρησιμοποιώντας μεταγωγή πακέτων το σύστημα γίνεται πιο αποτελεσματικό, κατά συνέπεια, την καλύτερη κατανομή του capacity. Όταν επίσης χρησιμοποιούμε πακέτα μεταγωγής επιτρέπει στους χρήστες να είναι πάντα online.

1.5 Η 3,5η Γενιά Κινητών Δικτύων

Με τον όρο «γενιά 3,5» (3.5G ή 3G+) αναφερόμαστε στη νέα γενιά κινητών δικτύων τα οποία εκτός από την τεχνολογία WCDMA έχουν ενσωματώσει την τεχνολογία High Speed Packet Access (HSPA). Η ορολογία HSPA αναφέρεται σε μία γενικότερη έννοια που υιοθετήθηκε από το UMTS Forum προκειμένου να τονίσει τις αναβαθμίσεις του UMTS Radio Interface στις εκδόσεις 5 και 6 του 3GPP στάνταρ και να προσδιορίσει τα δίκτυα επικοινωνιών επόμενης γενιάς.

Η HSPA αποτελεί μία νέα τεχνολογία η οποία σχεδιάστηκε προκειμένου να αυξήσει τη χωρητικότητα πρώτα του κατερχόμενου και σε δεύτερη φάση του ανερχόμενου ασύρματου συνδέσμου για τα κινητά δίκτυα τρίτης γενιάς. Το γεγονός αυτό θεωρήθηκε απαραίτητο καθώς, στην πράξη, οι μέγιστοι ρυθμοί μετάδοσης για τα κινητά δίκτυα τρίτης γενιάς αποδείχθηκαν χαμηλοί για πολυμεσικές εφαρμογές. Ιδιαίτερα στην περίπτωση που θα υπήρχαν πολλοί χρήστες πολυμεσικών εφαρμογών στο ίδιο κελί, αυτό θα σήμαινε ραγδαία πτώση της απόδοσης του δικτύου στο συγκεκριμένο κελί.

Το HSPA αναφέρεται σε βελτιώσεις που πραγματοποιήθηκαν τόσο στον κατερχόμενο ασύρματο σύνδεσμο, μέσω του High Speed Downlink Packet Access (HSDPA) όσο και στον ανερχόμενο, μέσω του High Speed Uplink Packet Access (HSUPA). Αξίζει να αναφερθεί ότι τόσο το HSDPA όσο και το HSUPA μπορούν να υλοποιηθούν στο ίδιο εύρος ζώνης με το UMTS (των 5 MHz), γεγονός που επιτρέπει την παράλληλη λειτουργία τόσο του HSPA όσο και του κλασσικού UMTS. Το HSDPA, προτάθηκε στην έκδοση 5 του 3GPP στάνταρ (ανακοινώθηκε το 2003 και υλοποιήθηκε το 2005) και υποστηρίζει ρυθμούς μετάδοσης έως και 14,4 Mbps ανά χρήστη. Αναφορικά με τον ανερχόμενο ασύρματο σύνδεσμο, το HSUPA εισήχθη στην έκδοση 6 του 3GPP στάνταρ δίνοντας τη δυνατότητα υποστήριξης μέχρι και 5,8 Mbps μέσω ενός αφιερωμένου uplink καναλιού.

Η βασική ιδέα του HSPA είναι η προσθήκη ενός νέου τύπου ευρυζωνικού καναλιού το οποίο θα είναι βελτιστοποιημένο για πολύ υψηλούς ρυθμούς μετάδοσης. Πρόκειται για το κανάλι High-Speed Downlink Shared Channel (HS-DSCH) το οποίο χρησιμοποιείται για τη βελτίωση της ρυθμαπόδοσης (throughput) μόνο του κατερχόμενου συνδέσμου. Στο κανάλι αυτό έχουν ενσωματωθεί διάφορες τεχνικές που αποσκοπούν στη βελτιστοποίηση των δυνατοτήτων του όσον αφορά το ρυθμό μετάδοσης.

Ανάμεσα στα σημαντικότερα πλεονεκτήματα της HSPA τεχνολογίας συγκαταλέγονται οι αυξημένες ταχύτητες για τους τελικούς χρήστες, η αυξημένη διαδραστικότητα των υπηρεσιών καθώς και η παροχή υψηλής χωρητικότητας του δικτύου προς όφελος κυρίως των πάροχων. Η μείωση των καθυστερήσεων μετάδοσης παράλληλα με τις αυξημένες πλέον ταχύτητες μετάδοσης στο ασύρματο μέσο μεταφράζονται στην δυνατότητα παροχής μίας μεγάλης γκάμας πολυμεσικών εφαρμογών. Κατά συνέπεια, οι κινητοί χρήστες έχουν πλέον την ικανότητα να απολαμβάνουν υπηρεσίες που μέχρι τώρα παρέχονταν μόνο σε χρήστες με ενσύρματη ευρυζωνική σύνδεση. Τέτοιες υπηρεσίες είναι η πολύ γρήγορη, ευρυζωνική σύνδεση στο διαδίκτυο, VoIP, multi-player παιχνίδια, Mobile TV, ενισχυμένη μετάδοση video/MP3 streaming, video telephony και video conferencing για κινητούς χρήστες.

Τέλος, αξίζει να σημειωθεί ότι ήδη μελετώνται περαιτέρω δυνατότητες αναβάθμισης της ίδιας της HSPA τεχνολογίας από το 3GPP, κατά κύριο λόγο προς τον τομέα της βελτιστοποίησης του ασύρματου μέσου μετάδοσης.

1.6 *Η 4η Γενιά Κινητών Δικτύων*

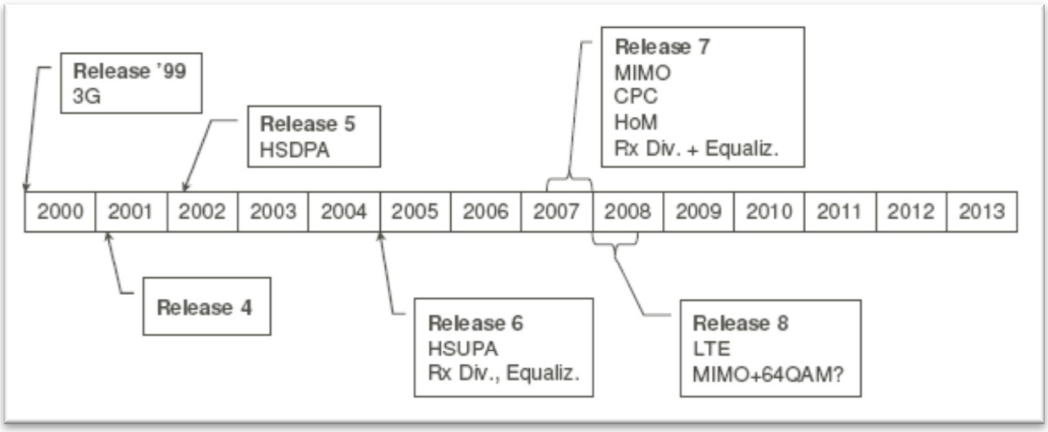
Τα κινητά τηλέφωνα 4ης γενιάς είναι το μέλλον της κινητής τηλεφωνίας. Τα χαρακτηριστικά της 4ης γενιάς κινητών τηλεφώνων είναι η IP λύση που δίνεται όπου φωνή, δεδομένα και πολυμέσα θα παρέχονται οποτεδήποτε και οπουδήποτε. Η τέταρτη γενιά έχει αρχίσει ήδη να εμφανίζεται σιγά-σιγά (ήδη κάνει τα πρώτα της βήματα στις Η.Π.Α, τις σκανδιναβικές χώρες, την Νοτιοανατολική Ασία και Ιαπωνία).Οι χρήστες κινητών τηλεφώνων θα έχουν πιο γρήγορη πρόσβαση στο Διαδίκτυο, γεγονός που αναμένεται να δώσει μια νέα δυναμική στην αγορά των κινητών τηλεφωνίας τόσο σε υπηρεσίες (μετεωρολογικές προβλέψεις, GPS) όσο και σε περιεχόμενο (ειδήσεις, ραδιόφωνο, παιχνίδια). Τα κινητά τηλέφωνα αυτής της γενιάς μπορούμε να πούμε ότι μοιάζουν περισσότερο με μικρούς υπολογιστές με απεριόριστες δυνατότητες. Οι επεξεργαστές τους φτάνουν σε συχνότητα το 1GHz, οι οθόνες τους είναι 3 και 4 ιντσών και διαθέτουν υψηλή ποιότητα και ευκρίνεια, οι κάμερες ξεπερνούν τα 5 Megapixels, η σύνδεση στο διαδίκτυο γίνεται με κάθε δυνατό τρόπο, υπάρχει σύγκλιση μεταξύ ασύρματης και ενσύρματης τεχνολογίας, η πρόσβαση στις ιστοσελίδες κοινωνικής διαδικτύωσης (Facebook και Twitter) έχει τα χαρακτηριστικά της αμεσότητας και της ταχύτητας. Τέλος, μπορεί να παρέχει ασύρματη ευρυζωνική πρόσβαση, Multimedia Messaging Service (MMS), videochat, mobile TV, υψηλής πιστότητας τηλεοπτικό περιεχόμενο (HDTV) και ψηφιακή μετάδοση video (DVB) και υψηλή ασφάλεια.

Παρά το γεγονός ότι οι τεχνολογίες HSPA και HSPA+, που οριοθετούν την «γενιά 3,5», αναμένονται να προσφέρουν τη δυνατότητα παροχής πληθώρας ευρυζωνικών υπηρεσιών, το 3GPP ήδη μελετά και επεξεργάζεται νέες τεχνολογίες που θα επικρατήσουν την αμέσως επόμενη δεκαετία στην αγορά των κινητών επικοινωνιών. Το νέο αυτό project αποκαλείται 3GPP Long Term Evolution (LTE) και στοχεύει στην επίτευξη ακόμη υψηλότερων ρυθμών μετάδοσης σε συνδυασμό με την αξιοποίηση μεγαλύτερου εύρος ζώνης. Κύρια προοπτική του LTE αποτελεί η διασφάλιση της ανταγωνιστικότητας και η επικράτηση του προτύπου στο χρονικό ορίζοντα της επόμενης δεκαετίας.

Το LTE εστιάζει αποκλειστικά στη βελτιστοποίηση υποστήριξης και μετάδοσης packet-switched εφαρμογών, όπως είναι οι πολυμεσικές εφαρμογές. Επίσης, θέτει πολύ υψηλούς και φιλόδοξους στόχους προκείμενου να ξεπεράσει τα όρια των 14.4 Mbps και 5.8 Mbps που επιτυγχάνονται στο HSDPA και HSUPA αντίστοιχα. Το πρότυπο υποστηρίζει κλιμακωτή χρήση φάσματος εύρους ζώνης της τάξης των 5, 10, 15 και 20 MHz. Επίσης, μπορεί να γίνει και χρήση εύρους ζώνης μικρότερου των 5 MHz (1.5 MHz και 2.5 MHz) για επιπλέον ευελιξία. Επιπλέον, στοχεύει στην επίτευξη μέγιστων ρυθμών μετάδοσης της τάξης των 100 Mbps στον κατερχόμενο σύνδεσμο και 50 Mbps στον ανερχόμενο σύνδεσμο για εύρος ζώνης ίσο με 20 MHz.

Στο σημείο αυτό πρέπει να αναφερθεί ότι το «αντίπαλο» πρότυπο που ανταγωνίζεται το LTE είναι το Mobile WiMAX. Το LTE ήδη γνωρίζει έντονη ερευνητική δραστηριότητα έχει λειτουργήσει στην αγορά , ξεκινώντας από το 2010.

Συγκεντρωτικά, η χρονολογική εξέλιξη των 3GPP κυψελωτών προτύπων, ξεκινώντας από τα κινητά δίκτυα 3G έως και τα αντίστοιχα δίκτυα επόμενης γενιάς LTE, απεικονίζεται στην Εικόνα 2. Το πρότυπο 3G/UMTS υιοθετήθηκε αρχικά στην 3GPP Release ’99 έκδοση, στην Release 5 πραγματοποιήθηκε η εισαγωγή του HSDPA, στην Release 6 η εισαγωγή του HSUPA, ενώ μέσω της ενδιάμεσης Release 7 φθάνουμε στο LTE που περιγράφεται και αναλύεται στην Release 8 του 3GPP.



Εικόνα 2: Χρονολογική Εξέλιξη κινητών δικτύων επόμενης γενιάς από το 3G έως το LTE

“ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ (ΣΥΣΚΕΥΕΣ)”

2. ΣΥΣΚΕΥΕΣ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ 1G

2.1 Χαρακτηριστικά κινητών 1G

Τα χαρακτηριστικά των κινητών της πρώτης γενιάς ήταν περιορισμένα καθώς ήταν τα πρώτα κινητά τηλέφωνα που κυκλοφόρησαν στην αγορά και πρόσφεραν «απλές» υπηρεσίες φωνής. Μέχρι τα τέλη της δεκαετίας του '80 τα κινητά τηλέφωνα ήταν ογκώδη ζύγιζαν περίπου ένα κιλό για να μεταφέρονται στην τσέπη κι έτσι ήταν εγκατεστημένα κυρίως σε αυτοκίνητα, είχαν χαμηλές ταχύτητες, χαμηλή ποιότητα και μετάδοση φωνής με αναλογικό τρόπο, αλλά και πολλά προβλήματα σύνδεσης. Στην αρχή της δεκαετίας του '90 άρχισε η απογείωση των κινητών τηλεφώνων. Έτσι τα κινητά έγιναν μικρότερα (100-200 γραμμάρια), χωρούσαν στην παλάμη και έμπαιναν έστω και με δυσκολία στην τσέπη του χρήστη τους. Το βασικό σύστημα ήταν GSM με ζώνη συχνοτήτων 900MHz, το έτος κυκλοφορίας των παρακάτω κινητών συσκευών ήταν το 1940 και 1999 χρησιμοποιούσαν κάρτα mini-SIM και μπορούσαμε να ρυθμίσουμε την ώρα, και είχαν υπέρυθρες για να μπορούσαν να μεταφέρουν ήχους, εικόνες, αλλά και παιχνίδια.

2.2 Παραδείγματα κινητών 1G

Τα κινητά τηλέφωνα που ανήκουν σε αυτή την κατηγορία είναι τα εξής το Motorola Dyna TAC που είναι το πρώτο κινητό που εμφανίστηκε στην αγορά το 1940, και το Nokia που εμφανίστηκε στην αγορά 1999. Οι παρακάτω φωτογραφίες απεικονίζουν τα κινητά αυτά.

Motorola DynaTAC

Nokia

2.3 Ανάγκη χρηστών για 1G

Η κύρια τεχνολογική εξέλιξη που έφερε η 1η γενιά κινητής τηλεφωνίας, ήταν η δυνατότητα που παρείχε στο χρήστη να επικοινωνεί μέσω του κινητού τηλεφώνου χωρίς να διακόπτεται η σύνδεση όταν μεταφέρεται από περιοχή σε περιοχή. Το πρώτο αυτοματοποιημένο κυψελωτό δίκτυο (cellular network) τέθηκε σε εφαρμογή στην Ιαπωνία το 1979 και έως το 1984 έγινε το πρώτο εθνικό δίκτυο 1ης γενιάς κινητής τηλεφωνίας. Ακολούθησαν οι Σκανδιναβικές Χώρες με το δικό τους δίκτυο 1ης

γενιάς (1G) το NMT (Nordic Mobile Telephone) το οποίο τέθηκε σε εφαρμογή το 1981, ενώ και άλλες χώρες ξεκίνησαν να θέτουν σε λειτουργία τα πρώτα δίκτυα κινητής τηλεφωνίας. Ωστόσο, κάθε χώρα δημιουργούσε τα δικά της πρότυπα και συστήματα επικοινωνίας και για να υπάρξει ολοκληρωμένη επικοινωνία ήταν απαραίτητη η ενοποίηση των διεθνών αγορών προκειμένου η χρήση των κινητών τηλεφώνων να μην περιορίζεται σε συγκεκριμένες γεωγραφικές περιοχές.

3. ΣΥΣΚΕΥΕΣ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ 2G

3.1 Χαρακτηριστικά κινητών 2G

Στα χαρακτηριστικά των κινητών της δεύτερης γενιάς βελτιώθηκαν ελάχιστα σε σχέση με τα κινητά την πρώτης γενιάς. Ποιο συγκεκριμένα, παρείχαν και άλλες ευκολίες όπως την αποστολή σύντομων γραπτών μηνυμάτων (SMS) και την λήψη φωτογραφιών (MMS). Είχαν περιορισμένα χρώματα όπως: Predictive text input, Smart messaging(Over the Air SMS), Calculator, Organizer, Voice dialing, και Voice answering, επίσης παιχνίδια που εκείνη την εποχή ήταν επίκαιρα γιατί η νεολαία έφερε στην μόδα μερικά από αυτά είναι τα παρακάτω: Arimona, Contrary, North territory, Yukon Struggle, Memory, Snake, Logic. Το βασικό σύστημα ήταν GSM με ζώνη συχνοτήτων είναι 900-1800-1900MHz, οι συσκευές κινητών ήταν τεχνολογίας 1998 και 2002, χρησιμοποιούσαν κάρτα mini-SIM, είναι κινητά απλά με κουμπιά και μπορούσαμε να ρυθμίσουμε την ώρα. Όμως η τεχνολογία εξελίσσεται και έτσι στα κινητά τηλέφωνα τοποθετούνται επιπλέων δεδομένα όπως: GRPS: class 4(3+1 slots), 24-36 kbps και Bluetooth: v1.0b. Το ποιο σημαντικό που αφορά τον χρήστη είναι ο δείκτης SAR που μας δείχνει την μέτρηση της ακτινοβολίας μιας συσκευής. Παραδείγματος χάριν στο κινητό Sony Ericsson T68i ο δείκτης SAR για Αμερική(US) είναι: 0,54 W/kg (head) και SAR για την Ευρώπη(EU) είναι: 0,38 W/kg (head).

3.2 Παραδείγματα κινητών 2G

Σε αυτή την κατηγορία ανήκουν τα κινητά τηλέφωνα όπου περιγράψαμε και χαρακτηρίσαμε αναλυτικά παραπάνω. Τα κινητά αυτά είναι το Nokia 5110 που είναι της χρονιάς 1998 και το Sony Ericsson T68i που είναι της χρονιάς 2002. Οι παρακάτω φωτογραφίες απεικονίζουν τα κινητά αυτά.

Nokia 5110

Sony Ericsson T68i

3.3 Ανάγκη χρηστών για 2G

Το 1990 η 2η γενιά κινητής είναι γεγονός. Έτσι στη Φινλανδία, το 1991 τίθεται σε λειτουργία το πρώτο δίκτυο GSM και η αναλογική μετάδοση σήματος δίνει τη θέση της στην ψηφιακή. Το GSM (Global System for Mobile communications) καθορίζει ενιαία πρότυπα επικοινωνίας στην κινητή τηλεφωνία, αντιμετωπίζοντας έτσι το φαινόμενο κατακερματισμού των προτύπων και αγορών, ανοίγοντας το δρόμο τόσο για τη δυνατότητα διεθνών κλήσεων όσο και για τη μεγαλύτερη εξάπλωση των συσκευών. Η ψηφιακή του λειτουργία επιτρέπει την εξυπηρέτηση μεγαλύτερου αριθμού συνδρομητών, τη συμβατότητα με άλλα συστήματα, την επεκτασιμότητα και τη καλύτερη ποιότητα υπηρεσιών. Μαζί της η δεύτερη γενιά έφερε και ένα νέο τρόπο επικοινωνίας, τα γραπτά μηνύματα SMS (Short Message Service), τα MMS (Multimedia Messaging Service) και κυρίως τα παιχνίδια που έγιναν αποδεκτά από όλους τους χρήστες αλλά και το πρώτο διαφημιστικό γραπτό μήνυμα που ενημέρωνε το χρήστη για τα καθημερινά γεγονότα.

4. ΣΥΣΚΕΥΕΣ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ 3G

4.1 Χαρακτηριστικά κινητών 3G

Τα χαρακτηριστικά των κινητών τηλεφώνων της τρίτης γενιάς έχουν αναβαθμιστεί σε σχέση με τις δύο προηγούμενες γενιές. Ποιο συγκεκριμένα, στις αρχές του 21ου αιώνα τα κινητά έχουν απεριόριστες αναβαθμισμένες δυνατότητες των πολυμέσων. Τα νέα αυτά κινητά όπως όλοι γνωρίζουμε είναι τα λεγόμενα Smartptones. Τα πρώτα ήταν συσκευές οι όποιες συνδύαζαν τις λειτουργιές ενός PDA και ενός κινητού τηλέφωνου ή ενός κινητού με κάμερα Ένα από τα κύρια οφέλη του UMTS είναι η ταχύτητά του. Τα τρέχοντα ποσοστά μεταφοράς δεδομένων για τις ευρυζωνικές πληροφορίες είναι 2 Mbits το δευτερόλεπτο. Αυτή η ταχύτητα καθιστά πιθανό το είδος του streaming video που μπορεί να υποστηρίξει το download ταινιών και την τηλεοπτική σύσκεψη (video conferencing). Το βασικό σύστημα ήταν υπηρεσίας GSM με ζώνη συχνοτήτων 850-900-1800-1900 MHz,τα Data protocols είναι EDGE, GPRS και HSDPA , τα κινητά αυτά χρησιμοποιούν mini-SIM και micro-SIM, έτος κυκλοφορίας είναι 2012 και 2011, ο χειρισμός οθόνης είναι αφής (Touch Screen), η

κάμερα είναι 3,15Mpixels (αλλά υπάρχουν και 2/5/6/8/13/20.7/41MP) και η οθόνη είναι 3,2΄΄ και 3,14΄΄ (αλλά υπάρχουν και 2,4΄΄/IPS LCD 4,0΄΄/Super LCD 4,3΄΄/ IPS LCD 5.0΄΄). Διαθέτουν εσωτερική μνήμη 2,9GB και 160MB(αλλά και 1,78/2/4/26,28/35GB). Επίσης το UMTS υποστηρίζει ασύρματο δίκτυο Wi-Fi για να έχουμε οποιαδήποτε στιγμή internet, videoκλήσεις, download μουσικής live-TV, Bluetooth, SMS, MMS, e-Mail, Video ακόμα και GPS. Το λειτουργικό σύστημα των κινητών αυτών είναι Android σε διάφορες εκδόσεις όπως Android 2.3/4.1/4.2/4.3/4.4, Apple iOS, Asha Touch 1.1, Windows Phone 8, BlackBerry OS 7.1/7.10. Η ισχύς επεξεργαστή είναι 800MHz, 600MHz. Τέλος ο δείκτης SAR όπου μας δείχνει την μέτρηση της ακτινοβολίας μιας συσκευής είναι 1,62W/kg και σε 0,96 W/kg.

4.2 Παραδείγματα κινητών 3G

Τα συστήματα τρίτης γενιάς σχεδιάζονται για να έχουν λειτουργίες νέας τεχνολογίας όπως το φωνητικό ταχυδρομείο, τη σελιδοποίηση, τη πρόσβαση Διαδικτύου, το βίντεο και το SMS. Τέτοια παραδείγματα κινητών τηλεφώνων είναι το Samsung Galaxy Mini S 5570 που είναι της χρονιάς 2011 και το Sony Xperia Tipo της χρονιάς 2012.

Samsung Galaxy Mini S 5570 *Sony Xperia Tipo*

4.3 Ανάγκη χρηστών για 3G

Τα τελευταία χρόνια έχουν παρατηρηθεί ραγδαίες εξελίξεις στις τεχνολογίες κινητής και ασύρματης επικοινωνίας με κορυφαία αυτή της έναρξης λειτουργίας των δικτύων

τρίτης γενιάς (3G). Η νέα τεχνολογία UMTS (Universal Mobile Telecommunication System) έρχεται να συμπληρώσει, να βελτιώσει και να επεκτείνει τις δυνατότητες επικοινωνίας των συνδρομητών κινητής τηλεφωνίας. Ήδη οι υπηρεσίες φωνής και δεδομένων που προσφέρονται από τα δίκτυα GSM/GPRS (2G/2.5G) επεκτείνονται με νέες υπηρεσίες και εφαρμογές όπως: εφαρμογές πολυμέσων, πλοήγηση σε ιστοσελίδες και μεταφορά δεδομένων.

Καθώς, οι άνθρωποι άρχισαν να χρησιμοποιούν το κινητό τους τηλέφωνο όλο και περισσότερο στην καθημερινότητα τους η ανάγκη για νέες προηγμένες υπηρεσίες και πρόσβαση στο διαδίκτυο φάνταζε επιτακτική. Αυτές οι αλλαγές έχουν επιφέρει μεγαλύτερη κίνηση δεδομένων για τις εταιρίες κινητής τηλεφωνίας, και ικανοποιούν τις απαιτήσεις για πληροφόρηση ή διασκέδαση πολλών χρηστών του Διαδικτύου. Παρόλα αυτά η συνεχώς αυξανόμενη ζήτηση νέων υπηρεσιών καθώς και των χαρακτηριστικών που εκτιμούν οι χρήστες είναι η αξία που τους προσφέρει, η ευκολία χρήσης και το κόστος χρήσης καθιστά αναγκαία τη μετάβαση σε ένα πιο εξελιγμένο δίκτυο ικανό να προσφέρει μια πλειάδα νέων υπηρεσιών.

Η εμφάνιση της τεχνολογίας 3G παρουσιάζει μεγάλο ερευνητικό ενδιαφέρον για τις εφαρμογές που μπορούν να εκμεταλλευτούν τα προηγμένα χαρακτηριστικά της, όπως η επικοινωνία με εικόνα και ήχο ταυτόχρονα, η αποστολή μηνυμάτων πολυμέσων, υπηρεσίες πλοήγησης/εντοπισμού θέσης(GPS), η αποστολή και λήψη αρχείων δεδομένων, μουσικών κομματιών, και το ηλεκτρονικό εμπόριο είναι μερικά παραδείγματα.

5. ΣΥΣΚΕΥΕΣ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ 4G

5.1 Χαρακτηριστικά κινητών 4G

Τα χαρακτηριστικά των κινητών τέταρτης γενιάς είναι πλέον διαδομένα και τα καλύτερα από τις τρείς προηγούμενες γενιές. Ποιο συγκεκριμένα, το LTE ήδη γνωρίζει έντονη ερευνητική δραστηριότητα αφού ξεκίνησε από το 2010 να λειτουργεί στην αγορά. Οι χρήστες αποδέχτηκαν τις συσκευές αυτές άμεσα και γρήγορα έγιναν αναγνωρίσιμες. Τα κυριότερα χαρακτηριστικά που υπάρχουν στις συσκευές τις τέταρτης γενιάς είναι το βασικό σύστημα υπηρεσίας GSM με ζώνη συχνοτήτων 850-900-1800-1900 MHz, τα Data protocols είναι EDGE, GPRS,HSDPA και LTE, στην πλειοψηφία τους χρησιμοποιούν κάρτες nano-SIM και micro-SIM κάποια από αυτά mini-SIM. Επιπλέον έχουν την δυνατότητα πρόσβασης στο internet και μάλιστα πολύ γρήγορη ώστε να απολαμβάνουν υπηρεσίες που μέχρι τώρα παρέχονταν μόνο από σταθερούς υπολογιστές, laptop και tablet, ακόμη διαθέτουν ασφάλεια στο χρήστη γιατί περιέχουν adivirus. Λειτουργούν και ως φωτογραφική μηχανή έχουν κάμερα 13 Mpixels και οθόνη αφής 4,99΄΄ και 5,5΄΄ ίντες. Η εσωτερική μνήμη είναι 32,0GB και 16GB, υψηλής ταχύτητας πρόσβαση σε δεδομένα μέσω Wi-Fi και ευζωνικού διαδικτύου κινητής τηλεφωνίας (mobile broadband), ο επεξεργαστής είναι 4πύρηνος οι συσκευές διαθέτουν GPS, ραδιόφωνο, Bluetooth, SMS, MMS, e-Mail, Video και παιχνίδια. Μερικά από τα πιο κοινά λειτουργικά συστήματα κινητών που χρησιμοποιούνται από τα σύγχρονα Smartphones είναι το iOS της Apple, το Android

της Google, το Windows Mobile της Microsoft, το Symbian της Nokia, το BlackBerryOS. Τέτοια λειτουργικά συστήματα μπορούν να εγκατασταθούν σε πολλά διαφορετικά μοντέλα κινητών τηλεφώνων, και συνήθως κάθε συσκευή μπορεί να κάνει πολλές αναβαθμίσεις όσον αφορά το λειτουργικό της σύστημα κατά τη διάρκεια ζωής του. Τέλος για τον δείκτη SAR βλέπουμε ότι οι τιμές πέφτουν και αυτό είναι κάτι που μας αφορά όλους για την υγείας μας, έτσι ο δείκτης είναι 0,28W/kg.

5.2 Παραδείγματα κινητών 4G

Σε αυτή την κατηγορία ανήκουν τα κινητά τηλέφωνα όπου περιγράψαμε και χαρακτηρίσαμε αναλυτικά παραπάνω. Έτσι μιλάμε για το Samsung Galaxy S4 I9505(32GB) της χρονιάς 2013 και το ZTE Grand S II (16GB) της χρονιάς 2014. Οι παρακάτω φωτογραφίες απεικονίζουν τα κινητά αυτά.

Samsung Galaxy S4 I9505 (32GB)

ZTE Grand S II (16GB)

5.3 Ανάγκη χρηστών για 4G

Τα κινητά τηλέφωνα 4ης γενιάς είναι το μέλλον της κινητής τηλεφωνίας. Είχε αρχίσει ήδη να εμφανίζεται σιγά-σιγά και να κάνει τα πρώτα της βήματα στις Η.Π.Α, τις σκανδιναβικές χώρες, την Νοτιοανατολική Ασία και Ιαπωνία. Οι χρήστες αυτών των κινητών τηλεφώνων απολαμβάνουν γρήγορη πρόσβαση στο Διαδίκτυο, γεγονός που έχει δώσει μια νέα δύναμη στην αγορά των κινητών τηλεφώνων τόσο σε υπηρεσίες όπως είναι οι μετεωρολογικές προβλέψεις, το GPS όσο και σε περιεχόμενο ειδήσεων, ραδιοφώνου και παιχνίδια. Τα κινητά τηλέφωνα αυτής της γενιάς μπορούμε να πούμε ότι μοιάζουν περισσότερο με μικρούς υπολογιστές με απεριόριστες δυνατότητες. Οι επεξεργαστές τους φτάνουν σε συχνότητα το 1GHz, οι οθόνες τους είναι 3 και 4 ιντσών και διαθέτουν υψηλή ποιότητα και ευκρίνεια, οι κάμερες ξεπερνούν τα 5 Megapixels, η σύνδεση στο διαδίκτυο γίνεται με κάθε δυνατό τρόπο, υπάρχει η σύγκλιση μεταξύ ασύρματης και ενσύρματης τεχνολογίας, η πρόσβαση στις ιστοσελίδες κοινωνικής διαδικτύωσης όπως το **Facebook, Twitter, Viber, και**

Skype, έχουν τα χαρακτηριστικά της αμεσότητας και της ταχύτητας. Επίσης, μπορεί να παρέχει ασύρματη ευρυζωνική πρόσβαση, Multimedia Messaging Service, videochat, mobile TV, υψηλής πιστότητας τηλεοπτικό περιεχόμενο (HDTV) και ψηφιακή μετάδοση video (DVB) και υψηλή ασφάλεια.

Η τεχνολογία LTE επιτρέπει τη βελτίωση της ποιότητας των υπηρεσιών διαδικτύου και μεταφοράς δεδομένων, και την αύξηση των ρυθμών μετάδοσης δεδομένων στους κινητούς χρήστες.

ΚΕΦΑΛΑΙΟ 2^{Ο}

"ΠΟΙΑ ΕΙΝΑΙ ΤΑ ΚΥΡΙΟΤΕΡΑ ΔΙΚΤΥΑ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ"

Στο κεφάλαιο αυτό γίνεται αρχικά μια εισαγωγική αναφορά στα κυριότερα δίκτυα κινητής τηλεφωνίας, συγκεκριμένα στο GSM, GPRS και UMTS. Στην συνέχεια, θα αναφερθούμε στην αρχιτεκτονική την δομή που υλοποιούν. Και τέλος, στα πρωτόκολλα ασφάλειας που υλοποιούν.

1.*GSM*

Το μειονέκτημα της ύπαρξης μεγάλου αριθμού αναλογικών συστημάτων στην Ευρώπη μαζί με την ανάγκη εξυπηρέτησης του διαρκώς αυξανόμενου αριθμού χρηστών και την καθιέρωση συμβατότητας των δικτύων κινητής επικοινωνίας με το σταθερό δίκτυο που ολοένα ψηφιακοποιείται, οδήγησαν τη CEPT στη σύσταση της ομάδας "Group Special Mobile" με σκοπό τη σύνταξη προδιαγραφών για ένα νέο σύστημα. Το έργο της ομάδας αυτής κατέληξε στο σύστημα GSM (Global System for Mobile communications).

Το νέο σύστημα 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. Κρίθηκε, έτσι, απαραίτητο να ενσωματωθούν στο σύστημα και όλοι εκείνοι οι αναγκαίοι μηχανισμοί ασφαλείας προκειμένου αυτό να προστατευτεί σε ενδεχόμενες ανεπιθύμητες επιθέσεις. Το πρότυπο GSM δεν ήταν μόνο ένα Ευρωπαϊκό πρότυπο, αφού υιοθετήθηκε από πολλές χώρες των άλλων Ηπείρων, εκμεταλλεύοντας διάφορες ζώνες συχνοτήτων.

1.1 Ζώνες Συχνοτήτων GSM

1.1.1 GSM 900:

Τα πρώτα δίκτυα GSM ήταν το 1990 που άρχισαν να λειτουργούν στη ζώνη συχνοτήτων των 900MHz. Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) παραχώρησε ένα ζεύγος συχνοτήτων, από τα 890 έως τα 915 MHz και από τα 935 έως τα 960 MHz. Η πρώτη περιοχή χρησιμοποιείται για την επικοινωνία του κινητού με τον σταθμό βάσης (Uplink), ενώ η δεύτερη για την επικοινωνία του σταθμού βάσης με το κινητό

(Downlink).Οι περιοχές (ζώνες) των 25 MHz υποδιαιρούνται η καθεμία σε 124+(1 ελεύθερο) κανάλια συχνότητας και κάθε κανάλι έχει εύρος ζώνης 200 KHz. Όλο αυτό το σύστημα ονομάστηκε GSM 900 ή Standard GSM.

1.1.2 GSM 1800:

Στη συνέχεια, το 1991, αναπτύχθηκε το DCS 1800 σύστημα, όπου διατηρείται η δομή ενός GSM 900 δικτύου αλλά χρησιμοποιούνται διαφορετικά ζεύγη συχνοτήτων, από τα 1710 έως τα 1785 MHz για Uplink και από τα 1805 έως τα 1880 MHz για Downlink. Οι περιοχές των 75 MHz υποδιαιρούνται η καθεμία σε 374+(1 ελεύθερο) κανάλια και κάθε κανάλι έχει εύρος ζώνης 200 KHz. Αυτή η αλλαγή στην ζώνη συχνοτήτων έγινε διότι οι ζώνες του GSM 900 στην Ευρώπη ήταν πιασμένες από άλλους παροχής κινητής τηλεφωνίας. Όπως και στην χώρα μας σήμερα όλες οι εταιρίες κινητής τηλεφωνίας χρησιμοποιούν και τα δύο συστήματα(GSM 900/GSM 1800) στα δίκτυα τους αυξάνοντας αισθητά τη χωρητικότητά στα δίκτυα τους. Στα τέλη δεκαετίας του 1990 το GSM World Association αποφάσισε να μετονομάσει το DCS 1800 σε GSM 1800 για να φανεί η δυναμικότητα και η παγκοσμιότητα του GSM.

1.1.3 GSM 1900:

Στο GSM 1900 χρησιμοποιείται σε αρκετές χώρες της Αμερικής, διατηρείται και πάλι η δομή ενός GSM 900 δικτύου, αλλά χρησιμοποιούνται και εδώ διαφορετικά ζεύγη συχνοτήτων: Από τα 1850 έως τα 1910 MHz για Uplink και από τα 1930 έως τα 1990 MHz για Downlink. Οι περιοχές των 60 MHz υποδιαιρούνται η καθεμία σε 299+(1 ελεύθερο) κανάλια συχνότητας και κάθε κανάλι έχει εύρος ζώνης 200 KHz. Στα τέλη δεκαετίας του 1990 το GSM World Association αποφάσισε να μετονομάσει το PCS 1900 που λεγότανε παλιότερα σε GSM 1900 για να φανεί η δυναμικότητα και η παγκοσμιότητα του GSM.

1.1.4 E-GSM Extended-GSM 900 - Εκτεταμένη ζώνη GSM:

Το E-GSM καθορίστηκε από την Ευρωπαϊκή Επιτροπή Ράδιο Επικοινωνιών στα τέλη της δεκαετίας του 1990 για να «αντικαταστήσει» το κλασικό GSM 900 διατηρώντας βέβαια την δομή του αυξάνοντας όμως τις περιοχές συχνοτήτων από 880 έως 915 MHz για Uplink και 925 έως 960 MHz για Downlink. Έτσι επέτρεψε στα δίκτυα κινητής τηλεφωνίας να αυξήσουν τη χωρητικότητά τους και να καλύψουν τις ανάγκες από την αυξημένη κίνηση των πελατών τους.

1.1.5 Κυψελοειδής Δομή Δικτύου:

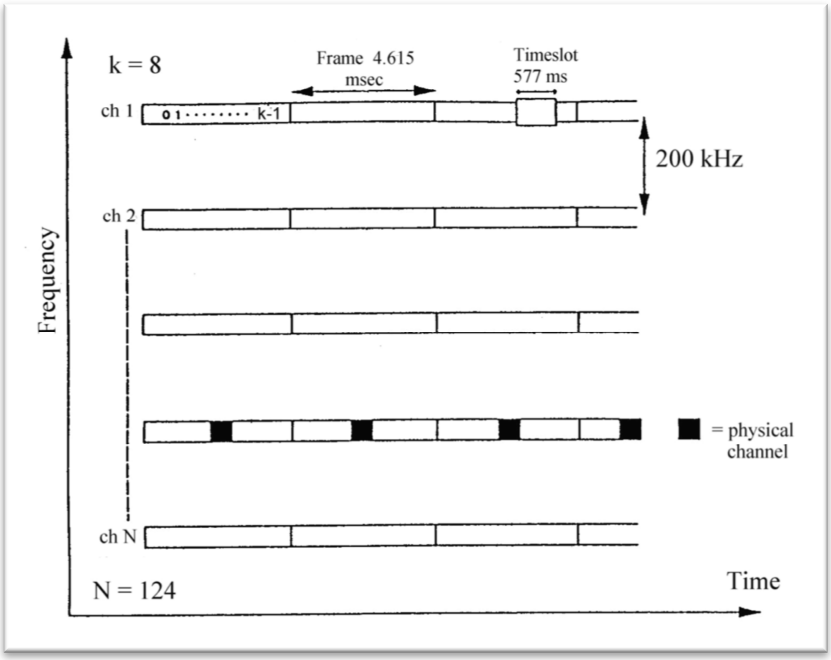
Η εμβέλεια ενός δικτύου GSM σε μία γεωγραφική περιοχή για να γίνει, πρέπει η περιοχή αυτή να διαμελίζεται σε μικρότερες περιοχές που λέγονται κυψέλες, οι οποίες εφάπτονται μεταξύ τους έτσι ώστε κάθε κυψέλη να έχει και ένα σταθμό βάσης (Base Station), συνθέτοντας έτσι μια δομή κυψελών. Η δομή αυτή επαναλαμβάνεται όσες φορές χρειάζεται για την απαιτούμενη κάλυψη μιας περιοχής κάνοντας επαναχρησιμοποίηση συχνοτήτων. Με την μέθοδο αυτή αυξάνεται η χωρητικότητα του δικτύου αλλά πρέπει η ισχύς κάθε κυψέλης να είναι όση χρειάζεται ώστε να μην ξεπερνάει τα όρια της και να υπερχειλίζει άλλες κυψέλες της ίδιας δομής ενώ για να μην δημιουργείται ενδοκαναλική

παρεμβολή σε γειτονικές κυψέλες η επαναχρησιμοποίηση συχνοτήτων πρέπει να σχεδιάζεται έτσι ώστε να απέχουν επαρκή απόσταση οι κυψέλες μιας δομής που έχουν την ίδια συχνότητα με τις κυψέλες μιας άλλης δομής .Η ενδοκαναλική παρεμβολή μειώνεται όσο αυξάνει ο αριθμός των κυψελών της δομής. Η ακτίνα κάθε κυψέλης σε αραιοκατοικημένες περιοχές είναι έως και 35 Km ενώ σε πυκνοκατοικημένες περιοχές δεν ξεπερνά τα 300 μέτρα.

Σε περιοχές με πολύ μεγάλη ζήτηση χωρητικότητας δικτύου όπως σε αστικά κέντρα, οι σταθμοί βάσης υπερφορτώνονται και έτσι υπάρχει ανάγκη για μεγαλύτερη χωρητικότητα του δικτύου. Έτσι για να επιτευχθεί αυτός ο σκοπός γίνεται διάσπαση των υπαρχόντων κυψελών σε μικρότερες, ενώ γ' αυτές χρησιμοποιούνται κεραίες μικρότερης ισχύος (macro bs-micro- bs - pico bs) όπως σε κτίρια, στο μετρό, Δημόσιους Οργανισμούς, οδικές αρτηρίες και τα λοιπά.

1.2 Γενικά χαρακτηριστικά του GSM

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), όπως φαίνεται στο Εικόνα 3. Ένα πλαίσιο (frame) έχει διάρκεια 4.615ms και αποτελείται από οκτώ τέτοιες χρονοσχισμές (577ms διάρκεια η καθεμία). Οι συχνότητες εκπομπής και λήψης είναι διαφορετικές με αποτέλεσμα οι μεταδόσεις της άνω ζεύξης (κινητό προς σταθμό βάσης) και της κάτω ζεύξης (σταθμό βάσης προς κινητό) να είναι ταυτόχρονες.



Εικόνα 3 : Σύστημα TDMA / FDMA

Το εύρος ζώνης του GSM είναι 25 MHz και παρέχει 125 φέρουσες, που καθεμία έχει εύρος ζώνης 200 kHz. Βέβαια λόγω φαινομένων παρεμβολής από άλλα συστήματα, η πρώτη φέρουσα συνήθως δε χρησιμοποιείται οπότε ο αριθμός των καναλιών

μειώνεται σε 124. Με δεδομένο ότι αντιστοιχούν 8 χρήστες ανά κανάλι, μπορούν να υπάρξουν περίπου 1000 πραγματικά κανάλια για ομιλία ή δεδομένα. Η χωρητικότητα αυτή μπορεί να διπλασιαστεί αν πέσει στο μισό ο ρυθμός κωδικοποίησης φωνής. Η περιοχή συχνοτήτων για την άνω ζεύξη είναι 890 MHz έως 915 MHz (με τις φέρουσες να βρίσκονται σε συχνότητες 890.2 , 890.4), ενώ για την κάτω ζεύξη είναι 935 MHz έως 960 MHz (με φέρουσες αντίστοιχα τις συχνότητες 935.2, 935.4). Δηλαδή το εύρος διαχωρισμού εκπομπής και λήψης είναι 45 MHz [4].

Η διαμόρφωση, τώρα, που χρησιμοποιεί το GSM είναι η GMSK . Ο τύπος αυτός διαμόρφωσης θεωρείται ανθεκτικός σε παρεμβολές "συγγενούς καναλιού", ενώ παράλληλα εξασφαλίζει ότι το μέγιστο ποσοστό της ακτινοβολούμενης ισχύος συγκεντρώνεται πλησίον της κεντρικής συχνότητας χωρίς να διασπείρεται σε μεγάλο εύρος. Ο ρυθμός εκπομπής είναι 270.833 Kbps (ισομοιράζεται ανάμεσα στους 8 χρήστες, οπότε αντιστοιχεί στον καθένα ρυθμός 33.85 Kbps), ενώ για τη διόρθωση σφαλμάτων χρησιμοποιείται συνελικτική κωδικοποίηση με ρυθμό κωδικοποίησης 13 Kbps ή 6.5 Kbps.

Ένα σημαντικό πρόβλημα που εμφανίζεται στο GSM είναι η διασυμβολική παρεμβολή, η οποία αντιμετωπίζεται με έναν ισοσταθμιστή Viterbi. Η παρεμβολή λόγω πολλαπλών δρόμων αντιμετωπίζεται με διαφορική λήψη, η οποία, ανάλογα με το περιβάλλον μπορεί να περιορίσει σε μεγάλο βαθμό τις διαλείψεις. Σε μερικά περιβάλλοντα, όπως παράδειγμα στις πόλεις, τα 200 KHz του εύρους ζώνης δεν αρκούν πλέον για την επίλυση του θέματος των πολλαπλών διαδρομών, οπότε και τα αργά κινούμενα τερματικά αντιμετωπίζουν μεγάλης διάρκειας ριπές σφαλμάτων. Η κατάσταση αυτή μπορεί να βελτιωθεί σημαντικά μεταπηδώντας συχνότητα από σχισμή σε σχισμή (frequency hopping) [5].

Τέλος, αναφορικά 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 (Discontinuous Transmission), προκειμένου το μεν κινητό να διαφυλάξει τη μπαταρία του, ο δε σταθμός βάσης να μειώσει τη διακαναλική παρεμβολή.

1.3 Αρχιτεκτονική- Δομή του GSM

ΑΡΧΙΤΕΚΤΟΝΙΚΗ GSM
Ένα GSM δίκτυο χωρίζεται σε 3 βασικά μέρη:

1.3.1 <u>Τον Κινητό Σταθμό (Mobile Station):</u> Έχει οπωσδήποτε πομπό-δέκτη, κεραία, οθόνη και την κάρτα SIM. Η μέγιστη επιτρεπόμενη ισχύς εκπομπής στην Ευρώπη μιας κινητής μονάδας είναι στα 2 Watt ενώ σε Αυστραλία και Αμερική είναι 1,6W, οι τιμές αυτές καθορίστηκαν από την Διεθνή Επιτροπή για την προστασία από τη μη ιονίζουσα ακτινοβολία.

1.3.2 <u>Το Βασικό Υποσύστημα Σταθμού (Base Station Subsystem):</u> Το BSS διαχειρίζεται τις κλήσεις σε μια γεωγραφική περιοχή όπου καλύπτεται από ένα σύνολο κεραιών διαφόρων μεγεθών σε σειρά σαν αυτούς που βλέπουμε σε λόφους,

ταράτσες πολυκατοικιών-εταιριών-σχολείων-οργανισμών και τα λοιπά. και κάθε τέτοια κεραία εξυπηρετεί και από μια κυψέλη. Το BSS χωρίζεται στο βασικό σταθμό πομπό-δέκτη Base Transceiver Station (BTS) και στο βασικό σταθμό ελέγχου Base Station Controller (BSC).

• ***Το Βασικό Υποσύστημα Σταθμού (BTS:*** **Base Transceiver Station** ***)*** φροντίζει την επικοινωνία μεταξύ του δικτύου GSM και του κινητού σταθμού. Ένα BTS μπορεί να ελέγχει μια ή περισσότερες κεραίες. Η ισχύς των κεραιών σε ένα BTS μπορεί είναι 40 W έως 500W. Για παράδειγμα, όταν ένας χρήστης Α θέλει να πραγματοποιήσει μια κλήση σε έναν άλλο συνδρομητή Β, ο σταθμός βάσης μεταβιβάζει το σήμα με το αίτημά του Α για αναζήτηση και εντοπισμό του άλλου συνδρομητή Β στο τηλεπικοινωνιακό κέντρο της εταιρείας του Α. Το κέντρο της εταιρείας εντοπίζει την κυψέλη στην οποία βρίσκεται ο Β και στέλνει το σήμα στον πλησιέστερο σταθμό βάσης. Από εκεί, πάλι με τη χρήση των διαθέσιμων συχνοτήτων, στέλνεται το σήμα στο κινητό του Β κι έτσι μπορεί να επικοινωνήσει μαζί του ο Α. Το πεδίο μιας GSM κεραίας ενός σταθμού βάσης ή κινητής μονάδας, είναι παλμικό με κανάλια διάρκειας 4,616 ή 9,232 msec το καθένα, που είναι χωρισμένα σε 8 ή 16 διαστήματα-χρονοθυρίδες, διάρκειας 0.577 msec η καθεμία (8Χ0,577 ή 16Χ0,577). Κάθε χρήστης χρησιμοποιεί για μια τηλεφωνική κλήση από μια χρονοθυρίδα άρα ένα κανάλι μπορεί να χρησιμοποιηθεί μέχρι και από 8 ή 16 συνδρομητές. Οι 8 ή 16 χρονοθυρίδες που χωρίζονται σε ένα κανάλι αποκαλούνται πλαίσιο TDMA ενώ κάθε χρονοθυρίδα αντιστοιχεί σε 156 bits.

• **Το BSC (Base Station Controler-Βασικός Σταθμός Ελέγχου)** ελέγχει τα σήματα παίρνοντας τα από ένα ή περισσότερα BTS ενώ εκχωρεί και απελευθερώνει κανάλια. Τα σήματα που λαμβάνει τα κατευθύνει στο MSC- Mobile Switching Centre και όταν χρειάζεται μετατρέπει τα 16kbps φωνής που είναι στην κινητή τηλεφωνία σε 64kbps που χρησιμοποιείται στην σταθερή τηλεφωνία.

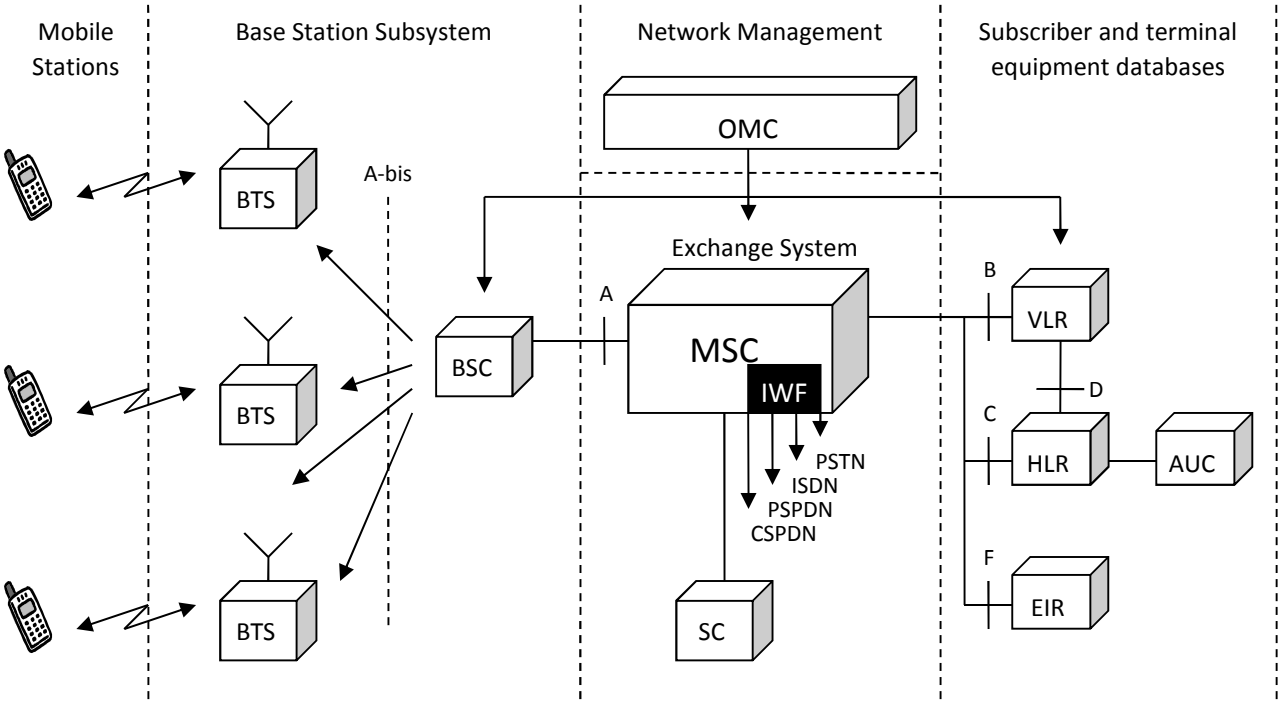
1.3.3 <u>Το Υποσύστημα Δικτύου μεταγωγής (NNS- Network Switching Subsystem) που αποτελείται από:</u>

Το Κέντρο Διανομής (Mobile Switching Center), είναι υπεύθυνο για την διασύνδεση, τον έλεγχο και την δρομολόγηση εισερχόμενων/εξερχόμενων κλήσεων μεταξύ του δικτύου κινητής τηλεφωνίας και ενός άλλου δικτύου ή άλλων. Όταν ένα MSC συνδέεται με ένα δίκτυο σταθερής τηλεφωνίας θα πρέπει να δέχεται 64kbps φωνής, όταν όμως ο MSC συνδέεται με ένα δίκτυο κινητής τηλεφωνίας τότε θα πρέπει να γνωρίζει που βρίσκεται εκείνη τη δεδομένη χρονική στιγμή ο χρήστης, αυτό επιτυγχάνεται με την βοήθεια καταχωρητών VLR (Visitor Locator Register), Home Locator Register (HLR). Ο πάτριος καταχωρητής θέσης αναζήτησης ή τοπικά κέντρα εγγραφής-HLR έχει μια Βάση Δεδομένων που κρατά στοιχεία προφίλ ενός συνδρομητή και πληροφορίες για την τρέχουσα θέση του, κάθε τέτοιο κέντρο η εμβέλεια του είναι σε τοπικό επίπεδο. Όταν ο συνδρομητής βγει από τα όρια της τοπικής περιοχής που καλύπτει το HLR δηλαδή είναι πολύ μακριά από το σπίτι του τότε αναλαμβάνει τον χρήστη ο καταχωρητής θέσης αναζήτησης ή εικονικό κέντρο εγγραφής - VLR ο οποίος έχει μια βάση δεδομένων, που συγκρατεί προσωρινά δεδομένα καθώς και την τρέχουσα θέση του, αναλαμβάνοντας τις κλήσεις του καλύτερα κατά τις ώρες αιχμής στο κέντρο της πόλης. Το κέντρο πιστοποίησης

(Authentication Centre – AuC) ο ρόλος του οποίου έγκειται στη διαχείριση δεδομένων για την πιστοποίηση της ταυτότητας του χρήστη.

Δομή GSM

Η δομή του συστήματος GSM φαίνεται στην Εικόνα 4. Από λειτουργικής πλευράς το πλήρες δίκτυο χωρίζεται σε δύο τμήματα: το τμήμα μεταγωγής (Switching System-SS) και το ραδιοηλεκτρικό τμήμα (Radio System - RS). Το πρώτο 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, ενώ το δεύτερο τους σταθμούς βάσης BSS και τους κινητούς σταθμούς MS [6].



Εικόνα 4 : Αρχιτεκτονική του GSM

Το κέντρο **MSC** καλείται να διεκπεραιώσει επιπλέον λειτουργίες σε σχέση μ' ένα αντίστοιχο κέντρο σταθερής τηλεφωνίας. Έτσι, η αντιμετώπιση της κλήσης γίνεται με τέτοιο τρόπο ώστε να λαμβάνεται υπόψη ότι ο συνδρομητής είναι κινούμενος και όχι ακίνητος σε γνωστό σημείο. Γ' αυτό ανιχνεύεται για τον ακριβή εντοπισμό της θέσης του. Βασική αποστολή του κέντρου είναι να χειρίζεται τις κλήσεις που εκδηλώνονται ή καταλήγουν στην περιοχή που αυτό καλύπτει . Για το λόγο αυτό είναι συνδεδεμένο με έναν αριθμό σταθμών βάσης με τους οποίους διατηρεί συνεχή επαφή, ενώ από την άλλη πλευρά συνδέεται με το δίκτυο PSTN/ISDN/PSPDN. Έτσι επιτυγχάνει σωστή δρομολόγηση όλων των κλήσεων. Παράλληλα το MSC διαχειρίζεται τα διαθέσιμα ραδιοηλεκτρικά μέσα κατά τη διάρκεια των κλήσεων, καθορίζοντας τον τύπο ραδιοκαναλιού που χρησιμοποιείται σε κάθε φάση της κλήσης (αν θα είναι δηλαδή κανάλι κίνησης ή ελέγχου), 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, μεταφέρει τις παραμέτρους πιστοποίησης μεταξύ του σταθμού βάσης και της βάσης επισκέψεως, παρέχει στους σταθμούς βάσης τους οποίους ελέγχει τον απαραίτητο συγχρονισμό, αναγνωρίζει την περιοδική και αυτόματη διακοπή λειτουργίας του κινητού σταθμού προς εξοικονόμηση ισχύος (λειτουργία "ασυνεχούς λήψης" "discontinuous reception'') και έχει την ευθύνη των διατάξεων καταστολής ήχους (echo canceler). Τέλος, ερευνά την οικεία βάση δεδομένων HLR του καλούμενου ώστε να εξακριβώσει τον αριθμό περιαγωγής του και μεριμνά για την ασφάλεια της ταυτότητας του συνδρομητή καθώς και για την ασφάλεια των πληροφοριών που μεταδίδει [6]. 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.

Η βάση δεδομένων **VLR** έχει ως αποστολή την τοπική και παροδική ενταμίευση όλων των μεταβλητών που είναι απαραίτητες για τον χειρισμό των κλήσεων που εξέρχονται ή εισέρχονται στην περιοχή που ελέγχει. Χρησιμεύει δηλαδή 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. 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), οι συμπληρωματικές υπηρεσίες που ενδεχομένως έχει ενεργοποιήσει ένας συνδρομητής, 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. Τέλος κατά τη διαγραφή του κινητού σταθμού από ένα VLR ενημερώνεται αντίστοιχα και το HLR. [4],[6]

Η οικεία βάση **HLR** 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 (παράδειγμα IMSI, MSISDN). Αποτελεί δηλαδή τη βάση αναφοράς για κάθε συνδρομητή. Περιλαμβάνει ακόμα και πληροφορίες σχετικά με τη διακοπή παροχής κάποιας υπηρεσίας προς ένα συνδρομητή ώστε να καθοδηγείται η βάση επισκέψεως αν μια υπηρεσία προς ή από αυτόν επιτρέπεται ή όχι.

Το κέντρο πιστοποίησης **AUC** έχει ως βασική λειτουργία να παρέχει στο HLR τις τριάδες (triplets) προκειμένου να γίνει πιστοποίηση των συνδρομητών. Στο AUC φυλάσσονται 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.

Το κέντρο τεκμηρίωσης **EIR** εποπτεύει τους κινητούς σταθμούς και μπλοκάρει όσους δεν έχουν το δικαίωμα να εξυπηρετούνται . Τα περιεχόμενα του κέντρου αυτού (λευκές, γκρι και μαύρες λίστες) μπορούν να μεταβάλλονται μέσω εντολών από το OMC. Οι κινητοί σταθμοί που βρίσκονται στις λευκές λίστες είναι αποδεκτοί από το σύστημα και ελεύθεροι να επικοινωνήσουν. Οι ευρισκόμενοι σε γκρι λίστα παρακολουθούνται και σε μαύρη είναι φραγμένοι (παράδειγμα κλεμμένες συσκευές). Στη βάση δεδομένων του κέντρου αυτού είναι εγγεγραμένες όλες οι ταυτότητες των κινητών συσκευών (IMEI) [6]. Όποτε το MSC/VLR ζητά από τον κινητό σταθμό να εξακριβώσει το IMEI του, τον συγκρίνει με τον αριθμό που λαμβάνει από το EIR.

Το κέντρο εποπτείας και συντήρησης **O&M** επικοινωνεί με διάφορα τμήματα του δικτύου και ουσιαστικά ελέγχει το όλο σύστημα . Λειτουργεί παράλληλα με το κέντρο διαχείρισης **NMC** το οποίο επίσης εκτελεί λειτουργίες διαχείρησης , παρακολουθεί τους κόμβους ώστε αυτοί να μην είναι υπερφορτωμένοι ή εκτός λειτουργίας και ενίοτε διεκπεραιώνει 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.

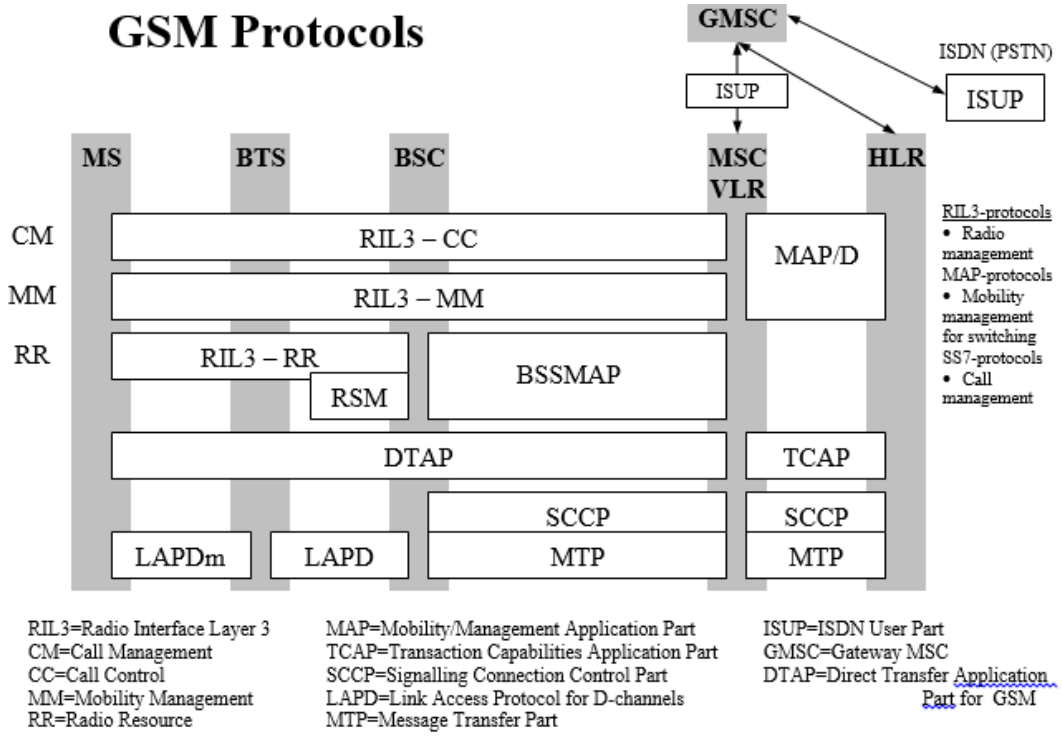
Ο σταθμός βάσης, τώρα, **BSS** είναι η φυσική διάταξη που χρησιμοποιείται για να δώσει ραδιοηλεκτρική κάλυψη σε κάποια περιορισμένη γεωγραφική ζώνη η οποία περιλαμβάνει μία ή περισσότερες κυψέλες . Αποτελείται από μια μονάδα κεντρικού ελέγχου, **BSC**, και μία ή περισσότερες ομάδες πομποδεκτών **BTS**. Κάθε ομάδα πομποδεκτών εξυπηρετεί μία κυψέλη, ενώ ένα BSC συνδέεται με έναν αριθμό ομάδων BTS και συνήθως ελέγχει μια περιοχή εντοπισμού (LA). Κάθε BTS επομένως περιλαμβάνει εξοπλισμό μετάδοσης, τις απαραίτητες δηλαδή διατάξεις εκπομπής και λήψης, τους ζεύκτες και τις κεραίες. Παράλληλα διαθέτει τα κυκλώματα ώστε τα σήματα να μεταδίδονται κωδικοποιημένα, κρυπτογραφημένα, πολυπλεγμένα και διαμορφωμένα (τα αντίθετα κατά τη λήψη), ενώ είναι υπεύθυνο και για την μεταπήδηση συχνότητας από σχισμή σε σχισμή (frequency hopping), την πραγματοποίηση μετρήσεων της στάθμης ισχύος στα ραδιοκανάλια, το συγχρονισμό ως προς το χρόνο και τη συχνότητα των σημάτων και τον καθορισμό της χρονικής προπορείας (timing advance) με την οποία πρέπει να μεταδώσει ένας κινητός σταθμός ώστε τα δεδομένα του να φτάσουν στο σωστό χρόνο το παράθυρο λήψης που του αντιστοιχεί στο BTS. Από την άλλη, το BSC εκτελεί λειτουργίες διαχείρησης. Καθορίζει και απελευθερώνει τις συχνότητες και τις χρονοσχισμές για τα τερματικά της περιοχής του, ελέγχει τη μεταπομπή, κάνει ανακατανομή συχνοτήτων στα BTS της δικαιοδοσίας του προκειμένου να εξυπηρετηθούν τοπικά υψηλές απαιτήσεις στις ώρες αιχμής ή σε ειδικές περιπτώσεις και είναι υπεύθυνο για τη διαχείρηση ισχύος των BTS. Παράλληλα συνδέεται με το μεταγωγικό κέντρο για τη δρομολόγηση της κίνησης προς το υπόλοιπο δίκτυο [4],[6].

Τέλος, 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 που οδηγεί σε ρυθμό 13 Kbps. Κατόπιν με την προσθήκη δυαδικών ψηφίων διόρθωσης λάθους

και τη συνελικτική κωδικοποίηση κάθε "φέτα λόγου" φτάνει να εκπέμπεται με ρυθμό 22.8 Kbps. Σε κάθε χρονοθυρίδα προστίθεται επίσης μια "εκπαιδευτική" σειρά που χρησιμοποιείται από τον εξισωτή (equalizer) του δέκτη για τη σωστή αναπαραγωγή του σήματος. Τελικά, μετά και από την διαγώνια διεμπλοκή ψηφίων (interleaving), την κρυπτογράφηση και τη διαμόρφωση , το σήμα εκπέμπεται από την κεραία του κινητού με ρυθμό 33.85 Kbps (ή 270.833Kbps/TS). Τα αντίστροφα βήματα λαμβάνουν χώρα στην περίπτωση εισερχόμενων σημάτων. Ο κινητός σταθμός πραγματοποιεί περιοδικά ενημέρωση θέσης ενώ παρακολουθεί και την ισχύ των κυψελών που το περιβάλλουν για ενδεχόμενη περίπτωση μεταπομπής[4]. 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) .

1.4 Τα πρωτόκολλα του GSM

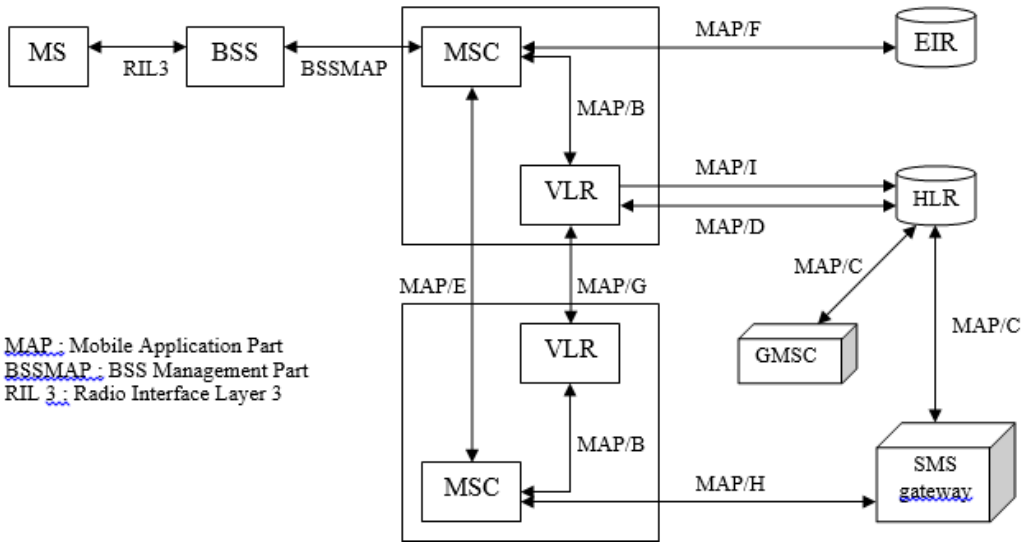
Χρησιμοποιείται το σύστημα σηματοδοσίας #7 (SS7) για την επικοινωνία των επιμέρους τμημάτων του δικτύου [7]. Στην Εικόνα 5 φαίνεται η αρχιτεκτονική των πρωτοκόλλων σηματοδοσίας του GSM. Μεταξύ του κινητού τερματικού και του σταθμού βάσης εφαρμόζεται το πρωτόκολλο LAPDm, με σκοπό να προσφέρει ασφαλή μεταφορά δεδομένων. Η διεπαφή ανάμεσά τους είναι ασύρματη. Το LAPD είναι το πρωτόκολλο επικοινωνίας μεταξύ του BTS και του BSC και παρέχει υπηρεσία μεταφοράς πληροφορίας χωρίς ή με επαλήθευση. Η διεπαφή ανάμεσά τους είναι το A–bis interface. Τα πρωτόκολλα MTP προσφέρουν μια αξιόπιστη υπηρεσία χωρίς σύνδεση για τη δρομολόγηση των μηνυμάτων μέσω του δικτύου SS7, ενώ το



Εικόνα 5 : Τα πρωτόκολλα σηματοδοσίας του GSM

SCCP, που ανήκει στο στρώμα δικτύου σηματοδοσίας, εμπλουτίζει την υπηρεσία χωρίς σύνδεση που παρέχει το MTP, ώστε τούτο να ανταποκρίνεται στις απαιτήσεις των τμημάτων χρηστών που ζητούν βελτιωμένη υπηρεσία χωρίς σύνδεση ή με σύνδεση για τη μεταφορά της πληροφορίας σηματοδοσίας μεταξύ των κόμβων [5]. Το στρώμα διαχείρησης ασυρμάτων πόρων (RIL3-RR) είναι υπεύθυνο για την εγκατάσταση, λειτουργία και απελευθέρωση των συνδέσεων μεταξύ του MS και του BSC, ενώ το BSSMAP, που λειτουργεί ως γέφυρα μεταξύ του στρώματος RR του BSC και του MSC, μεταφέρει μηνύματα διαχείρισης ανάμεσα στα δύο αυτά κέντρα σχετικά με τον έλεγχο διαπομπής, την αντιστοίχηση διαύλου και την μεταγωγή κατά την εγκατάσταση της κλήσης. Το RSM παρέχει υπηρεσίες RR μεταξύ BTS και BSC και το DTAP αναλαμβάνει την άμεση μεταφορά μηνυμάτων μεταξύ MSC και κινητού τερματικού διαφανώς μέσω του BSC. Τα μηνύματα αυτά σχετίζονται με τον έλεγχο μιας κλήσης και με τη διαχείριση κινητικότητας. Το TCAP αντίστοιχα περιέχει πρωτόκολλα και υπηρεσίες για την πραγματοποίηση απομακρυσμένων λειτουργιών , ενώ με τη χρήση του είναι δυνατό να αφαιρεθούν τα κοινά πρωτόκολλα από κάθε εφαρμογή και να προστεθεί αντί αυτών μια κοινή πλατφόρμα [4]. Το πρωτόκολλο διαχείρισης κίνησης μεταξύ MS και δικτύου (RIL3-MM) είναι υπεύθυνο για την πραγματοποίηση ενημέρωσης θέσης, αναγνώρισης και πιστοποίησης του κινητού, κατανομής TMSI στον κινητό σταθμό και γενικά για την ανταλλαγή μηνυμάτων σχετικών με τη διαχείριση της κινητικότητας. Στο ανώτερο στρώμα του μοντέλου, το πρωτόκολλο διαχείρισης κλήσεων (RIL3-CC) αναλαμβάνει την εγκατάσταση, διατήρηση και τερματισμό των κλήσεων ανάμεσα στον κινητό σταθμό και το δίκτυο. Η σηματοδοσία μεταξύ MSC και εξωτερικών δικτύων , που αφορά στις

κλήσεις, χρησιμοποιεί τα πρωτόκολλα ISUP (ISDN User Part) και TUP (Telephone User Part).



Εικόνα 6 : Οι συνδέσεις MAP του δικτύου GSM

Τέλος, το πρωτόκολλο MAP παρέχει τις απαραίτητες διαδικασίες προκειμένου να καταστεί δυνατή η ανταλλαγή πληροφοριών μεταξύ οντοτήτων του σταθερού μέρους του δικτύου GSM. Χρησιμοποιεί το SS7 για τη μεταφορά των πληροφοριών και το TCAP ως διεπαφή. Στην Εικόνα 6 φαίνονται οι συνδέσεις MAP των στοιχείων του δικτύου . Είναι πολύ σημαντικό να αναφέρουμε ότι 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. Οι συνδέσεις από το BTS και μετά είναι συνήθως ή από σημείο σε σημείο μικροκυματικές ζεύξεις ή οπτικών ινών ή σταθερές (fixed) ζεύξεις.

2. *GPRS*

Το General Packet Radio Service (GPRS) είναι μια κινητή υπηρεσία δεδομένων διαθέσιμη στους χρήστες των κινητών τηλεφώνων GSM και IS-136. Παρέχει ταχύτητα μεταφοράς δεδομένων από 56 μέχρι 114 Kbps. Η μεταφορά δεδομένων GPRS χρεώνεται τυπικά ανά kilobyte των μεταφερόμενων δεδομένων, ενώ η μετάδοση δεδομένων μέσω του παραδοσιακού συνεχής κατανομή πόρων (circuit switching0 τιμολογείται ανά λεπτό του χρόνου σύνδεσης, ανεξάρτητα από το εάν ο χρήστης έχει μεταφέρει πραγματικά τα δεδομένα ή αν βρισκόταν σε κατάσταση αναμονής.

Το GSM προσφέρει παγκόσμια διαθεσιμότητα και σχεδόν απεριόριστη κινητικότητα τερματικού κυρίως για τις υπηρεσίες φωνής. Ωστόσο, εξαιτίας της περιορισμένης ποιότητας υπηρεσιών που παρέχει όσον αφορά στη μετάδοση δεδομένων, κρίθηκε απαραίτητη η εισαγωγή ενός νέου συστήματος που θα υποστηρίζει μεταφορά δεδομένων. Οι τωρινές υπηρεσίες δεδομένων του GSM, των 9.6 Kbps, επιφέρουν μια

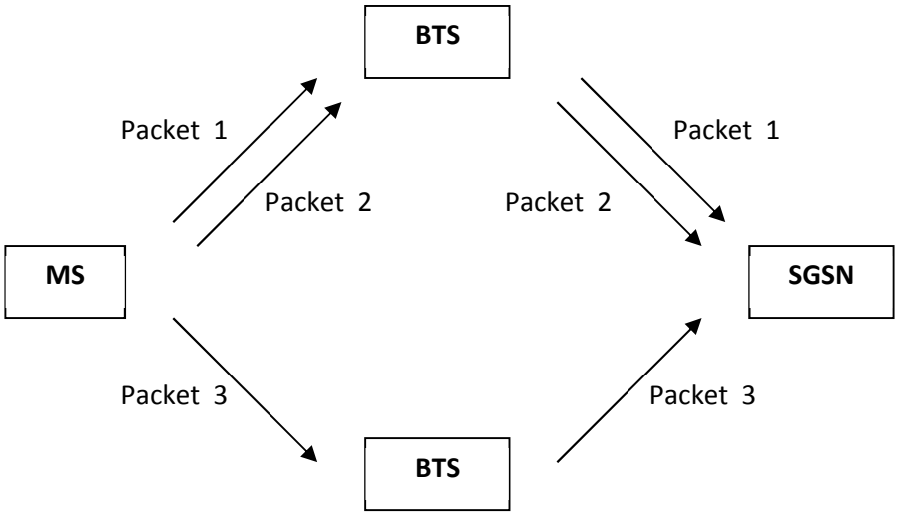
ιδιαίτερα υψηλή πολυπλοκότητα στην ασύρματη διεπαφή και στις διαδικασίες σηματοδοσίας του δικτύου . Με την ανάπτυξη, όμως, του GPRS, η μετάδοση των δεδομένων γίνεται πλέον πολύ πιο εύκολα εξασφαλίζοντας παράλληλα υψηλή ποιότητα και αξιοπιστία.

Το σύστημα *γενικής ασύρματης υπηρεσίας μεταγωγής πακέτου (General Packet Radio Service , GPRS)* παρέχει αποτελεσματική χρησιμοποίηση των ασυρμάτων πόρων για υπηρεσίες μεταγωγής πακέτου που χαρακτηρίζονται από ασυνεχή ρυθμό μετάδοσης bit, ενώ οι ρυθμοί μετάδοσης που δύναται να προσεγγίσει το GPRS, θεωρητικά μπορούν να φτάσουν μέχρι 160 Kbps περίπου. Επομένως, δεδομένου ότι ένα τέτοιο σύστημα έχει τόσο αυξημένες δυνατότητες και σαφώς βελτιωμένα χαρακτηριστικά, είναι αναγκαία η προστασία του με ένα εξίσου δυναμικό μοντέλο ασφαλείας .

2.1 Γενικά χαρακτηριστικά και αρχιτεκτονική του GPRS

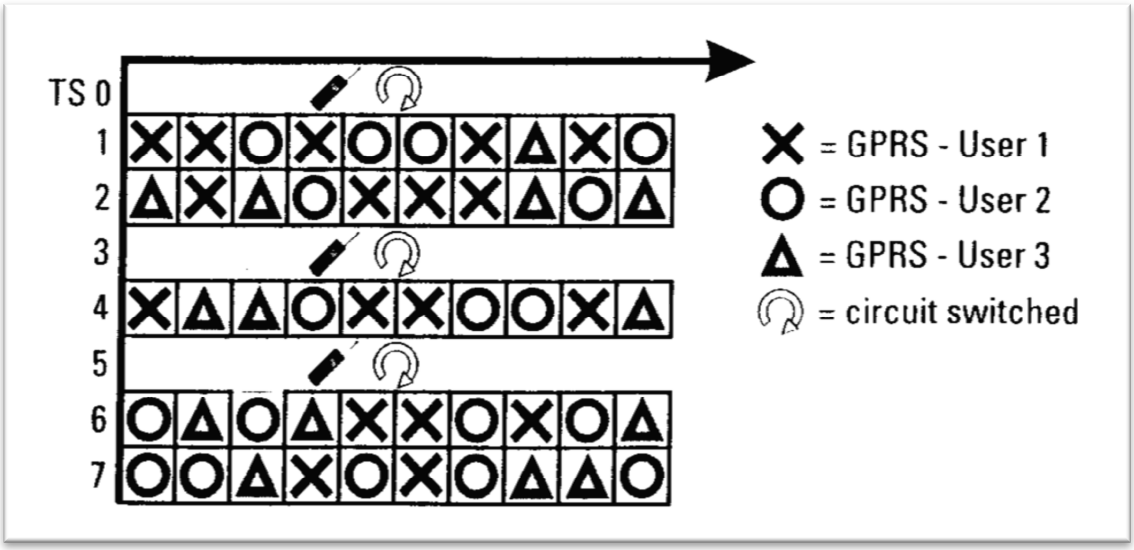
Η βασική ιδέα στο GPRS είναι η χρησιμοποίηση των χρονοσχισμών της ασύρματης διεπαφής του GSM που δεν χρησιμοποιούνται για φωνή , για τη μεταφορά ασύγχρονων δεδομένων με μεταγωγή πακέτου. Για να επιτύχει αυτό το σκοπό, το GPRS χρησιμοποιεί την ίδια ασύρματη πρόσβαση, που χρησιμοποιεί το GSM για την τηλεφωνία, με αναβαθμίσεις στο υλικό και στο λογισμικό του BSS και εισάγει νέο δίκτυο κορμού με στοιχεία δικτύου ειδικά για μετάδοση πακέτων. Βέβαια όπως είπαμε, το GPRS προβλέπει ρυθμούς μετάδοσης μέχρι 160 Kbps, το εύρος ζώνης, προφανώς, πρέπει να χρησιμοποιείται από κοινού με τις υπηρεσίες φωνής. Στην πραγματικότητα, η τηλεφωνία και οι υπηρεσίες μεταγωγής κυκλώματος συμπληρώνονται με την υπηρεσία GPRS , αλλά η τηλεφωνία έχει προτεραιότητα. Τούτο σημαίνει ότι, αν οι ραδιοδίαυλοι είναι κατειλημμένοι από την τηλεφωνία, εμποδίζεται η πρόσβαση των χρηστών GPRS, εκτός αν κρατούνται κάποιοι ασύρματοι πόροι (ραδιοδίαυλοι ή χρονοσχισμές) σε κάθε κυψέλη για τους χρήστες GPRS. Συνεπώς, μπορεί να υπάρχει αποκλεισμός στην κίνηση GPRS ή καθυστέρηση στην κίνηση που μεταφέρεται μέσω ζεύξεων GPRS. [5]

Το GPRS παρέχει τη δυνατότητα στο χρήστη να είναι συνδεδεμένος με το Internet και να κατεβάζει αρχεία , να διαβάζει e-mail ή απλά να ανοίγει σελίδες του παγκόσμιου ιστού. Το πρωτοποριακό στοιχείο του συστήματος αυτού μεταγωγής πακέτων αφορά στην κατανομή των πόρων (resource allocation). Συγκεκριμένα, το GPRS επιτρέπει την ταυτόχρονη χρήση μιας χρονοσχισμής από πολλούς χρήστες. Ισοδύναμα, σε έναν χρήστη μπορούν να κατανεμηθούν πολλές χρονοσχισμές από το δίκτυο, προκειμένου να μεταδώσει, και γ’ αυτό το λόγο άλλωστε αυξάνεται ο ρυθμός μετάδοσης που επιτυγχάνει το GPRS. Όπως φαίνεται και στην Εικόνα 7, τα πλαίσια δεδομένων αποστέλλονται σε ‘παράλληλες’ χρονοσχισμές στο ίδιο BTS ή σε δύο διαφορετικά BTS αν ο κινητός σταθμός μεταπέμπεται από το ένα BTS στο άλλο (ο ρόλος του SGSN εξηγείται παρακάτω) [8].



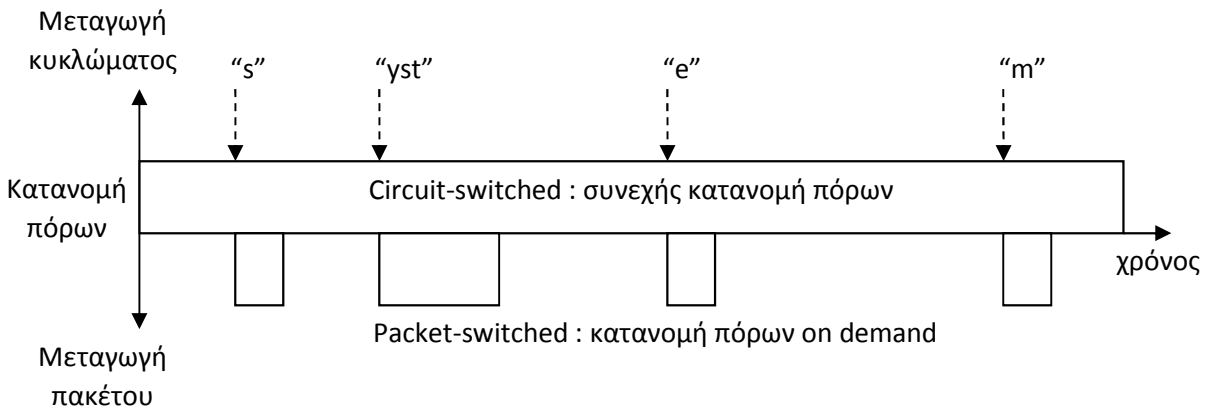
Εικόνα 7 : Σε κάθε MS κατανέμονται περισσότερες από μία χρονοσχισμές για μετάδοση

Ενώ, λοιπόν, στις υπηρεσίες μεταγωγής κυκλώματος κατανέμεται σε έναν χρήστη μία χρονοσχισμή για μετάδοση, στο GPRS οι συνδρομητές μοιράζονται τους πόρους σε κάθε timeslot, όπως είναι εμφανές στην Εικόνα 8.



Εικόνα 8 : Μοίρασμα των πόρων μεταξύ GSM και GPRS

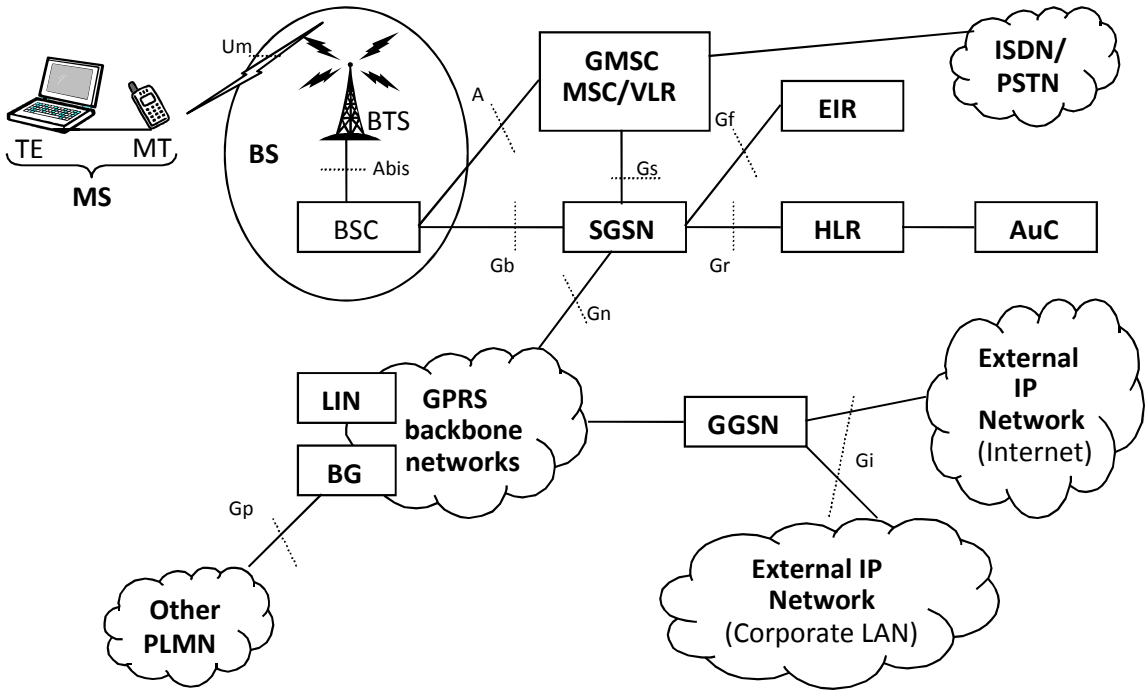
Πολύ σημαντικό χαρακτηριστικό του GPRS αποτελεί το γεγονός ότι οι πόροι διατίθενται στα κινητά τερματικά μόνο όταν πραγματικά χρειάζονται (resource on demand) [8]. Ένα παράδειγμα παρουσιάζεται στην Εικόνα 9, όπου κατά τη διάρκεια μιας συνόδου μεταφέρεται η ακολουθία ‘‘system’’. Το GSM, ως δίκτυο μεταγωγής κυκλώματος , καταλαμβάνει τον απαιτούμενο πόρο για όλη τη διάρκεια της μετάδοσης, ενώ το GPRS, ως δίκτυο μεταγωγής πακέτου, ζητά έναν πόρο μόνο κάθε φορά που πρόκειται να μεταδοθεί ένας χαρακτήρας και μετά το πέρας της μετάδοσης, ο πόρος αυτός απελευθερώνεται . Πολλές φορές μάλιστα συμβαίνει, κατά την απασχόληση ενός πόρου να μεταδίδονται πολλοί χαρακτήρες διαδοχικά, όπως γίνεται στο εν λόγω παράδειγμα με τους χαρακτήρες ‘‘yst’’.



Εικόνα 9 : *Κατανομή πόρων κατά τη μεταγωγή κυκλώματος και πακέτου.*

2.2 Αρχιτεκτονική του GPRS

Η αρχιτεκτονική του GPRS απεικονίζεται στην Εικόνα 10 όπου φαίνονται τα νέα στοιχεία που εισάγονται στο δίκτυο, οι διεπαφές μεταξύ τους καθώς και οι διεπαφές με εξωτερικά δίκτυα. Το GPRS χρησιμοποιεί πολλά από τα στοιχεία του GSM και τα νέα στοιχεία που προστίθενται θα μπορούσαμε να πούμε ότι συμπληρώνουν το σύστημα GSM [9].



Εικόνα 10 : Αρχιτεκτονική του GPRS

Δύο νέα και ιδιαιτέρως σημαντικά στοιχεία του GPRS είναι τα κέντρα SGSN και GGSN. Ο εξυπηρετών κόμβος υποστήριξης GPRS (**SGSN**) είναι υπεύθυνος για τη μεταφορά των πακέτων δεδομένων από και προς τα κινητά τερματικά της περιοχής

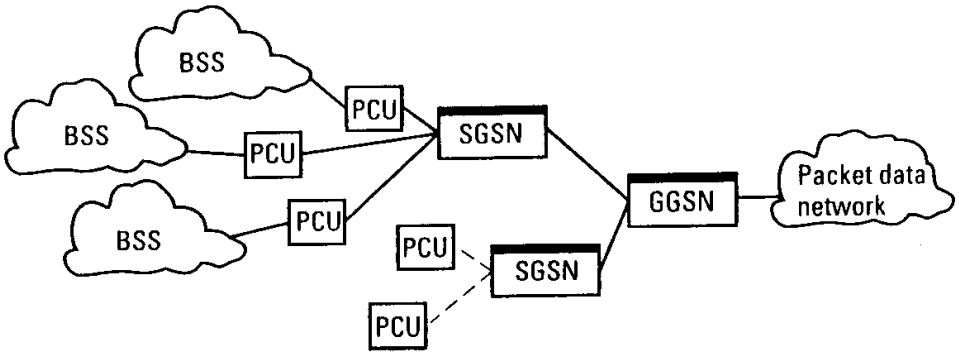
που εξυπηρετεί, δηλαδή ουσιαστικά λειτουργεί ως ένας δρομολογητής. Εκτός όμως από τη δρομολόγηση και μεταφορά πακέτων, το SGSN πραγματοποιεί και διαχείριση κίνησης, διαχείριση συνόδων, πιστοποίηση, κρυπτογράφηση/αποκρυπτογράφηση, συμπίεση/αποσυμπίεση, ενώ επιπλέον αλληλεπιδρά , όποτε απαιτείται , με το HLR, το MSC/VLR και το EIR. Ακόμα συλλέγει τις χρεώσεις σύμφωνα με τη χρήση των πόρων του εσωτερικού δικτύου και ενημερώνει την πύλη χρέωσης (CG – charging gateway), ελέγχει τη μεταπομπή και φυσικά υποστηρίζει την περιαγωγή των κινητών σταθμών. Στο SGSN αποθηκεύονται πολλές σημαντικές πληροφορίες που αφορούν τους συνδρομητές, όπως η μόνιμη ταυτότητα του χρήστη (IMSI), η προσωρινή P-TMSI (αντίστοιχη της TMSI στο GSM), οι αριθμοί IMEI και MSISDN, η περιοχή δρομολόγησης του κινητού (RA – routing area) (Η RA αποτελείται από μια ομάδα κυψελών και περιέχεται σε μια περιοχή εντοπισμού LA. Δηλαδή ένα ή περισσότερα RA (max 256) σχηματίζουν μια LA. Όλα τα BTS σε μια LA που δεν υποστηρίζουν GPRS αποτελούν τη λεγόμενη null RA), η ταυτότητα της κυψέλης στην οποία βρίσκεται το κινητό, οι τριπλέτες πιστοποίησης, οι αλγόριθμοι πιστοποίησης και κρυπτογράφησης, η classmark του κινητού, η ταυτότητα TLLI, με την οποία αναγνωρίζεται η λογική σύνδεση μεταξύ MS και SGSN και σχετίζεται πάντα με ένα RAI (RA Identity) κ.τ.λ. Τέλος, περιλαμβάνει και στοιχεία που αφορούν την ύπαρξη και λειτουργία ενδεχόμενης συνόδου του MS με κάποιο εξωτερικό δίκτυο. Για κάθε τέτοια σύνοδο δημιουργείται ένα πλαίσιο λειτουργίας PDP (PDP context) που περιέχει τον τύπο πρωτοκόλλου που υποστηρίζεται (παράδειγμα IP v4), την ζητούμενη ποιότητα υπηρεσίας QoS, τη διεύθυνση IP του MS και του GGSN που εξυπηρετεί το MS όντας το σημείο πρόσβασης (access point) στο εξωτερικό δίκτυο. Αυτό το πλαίσιο αποθηκεύεται στο SGSN, καθώς και στο MS και στο GGSN. [10]

Ο διαβιβαστικός κόμβος υποστήριξης GPRS (**GGSN**) είναι ένας δρομολογητής συνδεδεμένος σε εξωτερικό δίκτυο δεδομένων PDN (παράδειγμα το Internet) και είναι υπεύθυνος για τη δρομολόγηση των πακέτων προς το κατάλληλο SGSN. Επιπρόσθετα χειρίζεται τη δημιουργία και διατήρηση των PDP contexts, όπως προαναφέρθηκε, και συλλέγει τις χρεώσεις σύμφωνα με τη χρήση των πόρων του εξωτερικού δικτύου. Πολλές από τις πληροφορίες σχετικά με τους χρήστες που συναντώνται στο SGSN περιέχονται και στο GGSN. Η δρομολόγηση μεταξύ των SGSN και GGSN πραγματοποιείται με το πρωτόκολλο σήραγγας GPRS (GTP), το οποίο επιτρέπει σε πακέτα διαφόρων πρωτοκόλλων να μεταφέρονται με μέθοδο σήραγγας μέσω του δικτύου κορμού του GPRS προς τα εξωτερικά δίκτυα πακέτων.

Οι κινητοί σταθμοί MS στο GPRS μπορεί να είναι τάξης A,B ή C. Σε έναν τάξης A κινητό σταθμό οι διαδικασίες μεταγωγής κυκλώματος και πακέτου μπορούν να είναι σε εξέλιξη την ίδια στιγμή, δηλαδή ταυτόχρονα με ένα τηλεφώνημα να εκτελείται παράδειγμα το κατέβασμα (download) ενός αρχείου. Ο τάξης B κινητός σταθμός έχει πρόσβαση και στις CS και στις PS υπηρεσίες αλλά δεν μπορεί να χρησιμοποιήσει και τις δύο την ίδια στιγμή. Έτσι, όταν πραγματοποιεί μετάδοση πακέτων και ταυτόχρονα δέχεται μήνυμα για CS κίνηση, μπορεί να αναστείλει τη λειτουργία της μεταφοράς των δεδομένων για όσο χρονικό διάστημα διαρκεί η CS σύνδεση και αμέσως μετά να ενεργοποιήσει πάλι την PS λειτουργία. Ο τάξης C κινητός σταθμός έχει πρόσβαση σε μία υπηρεσία . Συνεπώς ένα MS που υποστηρίζει

μόνο GPRS και όχι CS κίνηση (παράδειγμα laptop) θα λειτουργεί πάντα σε τάξη C. [9]

Τέλος ένα νέο δομικό στοιχείο στο GPRS αποτελεί η μονάδα ελέγχου πακέτων **PCU** [8]. Πρόκειται ουσιαστικά για επέκταση του BSS και έχει αναλάβει εξ' ολοκλήρου την ευθύνη της κατανομής των πόρων στη ραδιοζεύξη για το GPRS. Δηλαδή ενώ το BSC διαχειρίζεται κατά κύριο λόγο την κατανομή των πόρων στο GSM, το PCU αναλαμβάνει το σκοπό αυτό για το GPRS . Η ενσωμάτωση του PCU στο BSS φαίνεται στην Εικόνα 11.

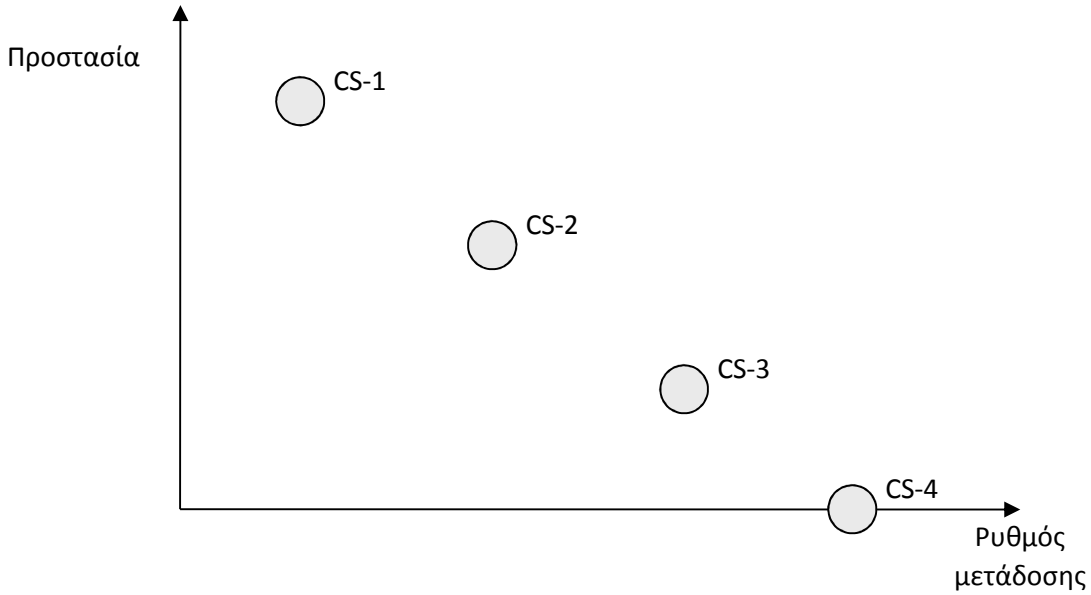


<u>Εικόνα 11</u> : Η μονάδα PCU στο GPRS

Οι βάσεις δεδομένων του GPRS που είναι κοινές με αυτές του GSM (HLR, EIR κτλ) παραμένουν αναλλοίωτες, με τη μόνη διαφορά ότι στις ήδη αποθηκεμένες πληροφορίες που περιλαμβάνουν, προστίθενται και αυτές που σχετίζονται με τους χρήστες GPRS και τις υπηρεσίες που αυτοί έχουν ενεργοποιήσει.

Το GPRS προβλέπει 4 διαφορετικές στάθμες κωδικοποίησης διαύλου, από CS-1 έως CS-4, από τις οποίες η CS-1 υποστηρίζει τον κατώτατο ρυθμό μετάδοσης bit χρήστη, ενώ η CS-4 τον ανώτατο [5]. Οι CS-3 και CS-4 μπορούν να χρησιμοποιηθούν μόνο σε περίπτωση που ο λόγος σήματος προς θόρυβο είναι υψηλός και τούτο συμβαίνει όταν το κινητό τερματικό GPRS βρίσκεται κοντά στο σταθμό βάσης. Αυτό σημαίνει ότι ο χρήστης μπορεί να έχει πρόσβαση με πλήρη ρυθμό στις χρονοσχισμές GPRS, σε περιορισμένη περιοχή κάλυψης. Από την άλλη, το σχήμα κωδικοποίησης CS-1 εξασφαλίζει μέγιστη προστασία στη μετάδοση και μπορεί να χρησιμοποιηθεί αποδοτικά ακόμα και σε μια 'φτωχή' ραδιοζεύξη. Πάντως ο σταθμός βάσης πρέπει να είναι σε θέση να αντιδρά γρήγορα σε περίπτωση για παράδειγμα της αύξησης του ρυθμού εσφαλμένων μπλοκ (BER – block error rate) και να μετάγει σε μία χαμηλότερη στάθμη κωδικοποίησης, όπως αντίστοιχα σε περίπτωση που ο BER είναι χαμηλός να μη χρησιμοποιεί τα αργά σχήματα CS-1 ή CS-2 αλλά κάποιο ταχύτερο.

Η αντιστοιχία μεταξύ ρυθμού μετάδοσης και διόρθωσης σφαλμάτων για κάθε ένα σχήμα φαίνεται ενδεικτικά στην Εικόνα 12, όπου είναι εμφανές ότι το CS-1 διορθώνει σχεδόν όλα τα λάθη παρέχοντας μέγιστη ασφάλεια στα μπλοκ και υψηλή αξιοπιστία στη μετάδοση, σε αντίθεση με το CS-4 που, αν και υποστηρίζει το μέγιστο ρυθμό μετάδοσης, δεν προσφέρει καμία προστασία.



Εικόνα 12 : Οι 4 στάθμες κωδικοποίησης που χρησιμοποιεί το GPRS

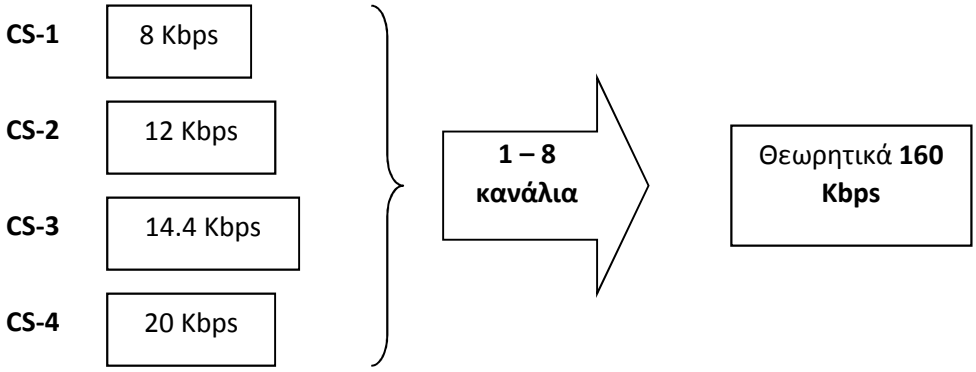
Οι πιο σημαντικές παράμετροι για τα σχήματα CS-1 έως CS-4 δίνονται στον Πίνακα που ακολουθεί[8].

	Μέγιστος αριθμός bits δεδομένων	**Πλεονάζοντα bits για διόρθωση σφαλμάτων**	**Αριθμός bits που δεν μεταδίδονται (punctured)**	**Ρυθμός κώδικα**	**Μέγιστος καθαρός ρυθμός μετάδοσης**
CS-1	160	40	0	1/2	**8 Kbps**
CS-2	240	16	132	2/3	**12 Kbps**
CS-3	288	16	220	3/4	**14.4 Kbps**
CS-4	400	16	0	1	**20 Kbps**

Σημείωση : Ο χρόνος μετάδοσης του κάθε μπλοκ είναι 20ms, συνεπώς ο μέγιστος καθαρός ρυθμός μετάδοσης προκύπτει από το μέγιστο αριθμό bits δεδομένων δια 20. Επίσης στα τρία πρώτα σχήματα , το μπλοκ που σχηματίζεται μετά και την προσθήκη της επικεφαλίδας και των πλεοναζόντων bits ελέγχου, περνά από έναν συνελικτικό κώδικα με ρυθμό ½ οπότε δημιουργείται το τελικό μπλοκ για μετάδοση. Το τελικό αυτό μπλοκ πρέπει σε κάθε σχήμα να αποτελείται από 456 bits. Στο CS-1 οδηγούνται στον κώδικα 228 bits, ο οποίος παράγει στην έξοδο τα διπλάσια, δηλαδή 456, κι έτσι κανένα bit δεν αποκόπτεται από τη μετάδοση . Στα σχήματα CS-2, CS-3 οδηγούνται στον κώδικα 294 και 338 bits και προκύπτουν 588 και 676 bits αντίστοιχα, οπότε δεν μεταδίδονται 132 και 220 bits (τα bits αυτά ονομάζονται punctured). Η διαδικασία αυτή αποκοπής κάποιων bits δε γίνεται τυχαία αλλά με συγκεκριμένο τρόπο και τελικά πομπός και δέκτης γνωρίζουν ακριβώς ποιες θέσεις bits δεν έχουν μεταδοθεί. Επομένως, ο ρυθμός κώδικα για τα δύο αυτά σχήματα προκύπτει από τον αριθμό των bits που οδηγούνται στον κώδικα δια του αριθμού bits που μεταδίδονται εν τέλει,

δηλαδή για το CS-2 είναι 294/456 ≈ 2/3 και για το CS-3 338/456 ≈ 3/4. Στη στάθμη CS-4, το μπλοκ που σχηματίζεται είναι 456 bits, οπότε δεν οδηγείται καν στο συνελικτικό κώδικα (ρυθμός κώδικα =1). Έπειτα, από την κωδικοποίηση εκτελείται η διαγώνια διεμπλοκή ψηφίων, η κρυπτογράφηση και η διαμόρφωση, όπου και στο GPRS χρησιμοποιείται το σχήμα GMSK, προτού το σήμα μεταδοθεί στη ραδιοζεύξη. Τα αντίθετα, φυσικά συμβαίνουν κατά τη λήψη.

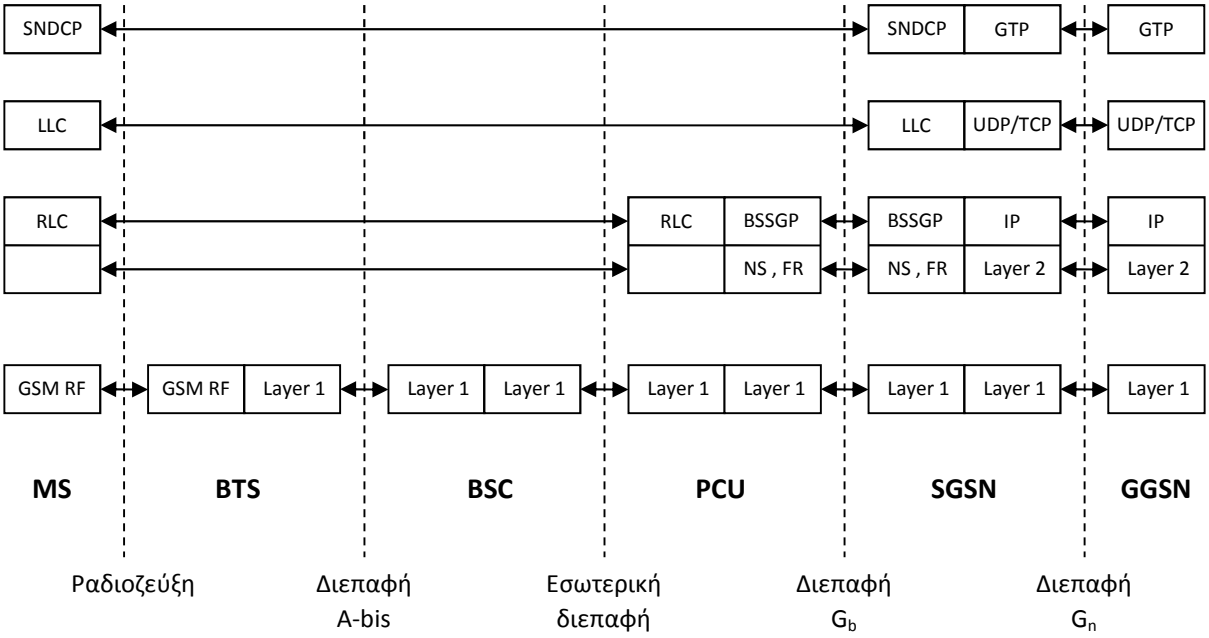
Παρατηρούμε στην Εικόνα 13 γιατί το GPRS μπορεί να φτάσει θεωρητικά σε ρυθμό μετάδοσης μέχρι και 160 Kbps. Ωστόσο, πρακτικά, οι ρυθμοί που προσεγγίζονται κυμαίνονται από 10 έως 40 Kbps. [7]



Εικόνα 13 : Θεωρητικοί και πρακτικοί ρυθμοί μετάδοσης στο GPRS

2.3 Τα πρωτόκολλα του GPRS

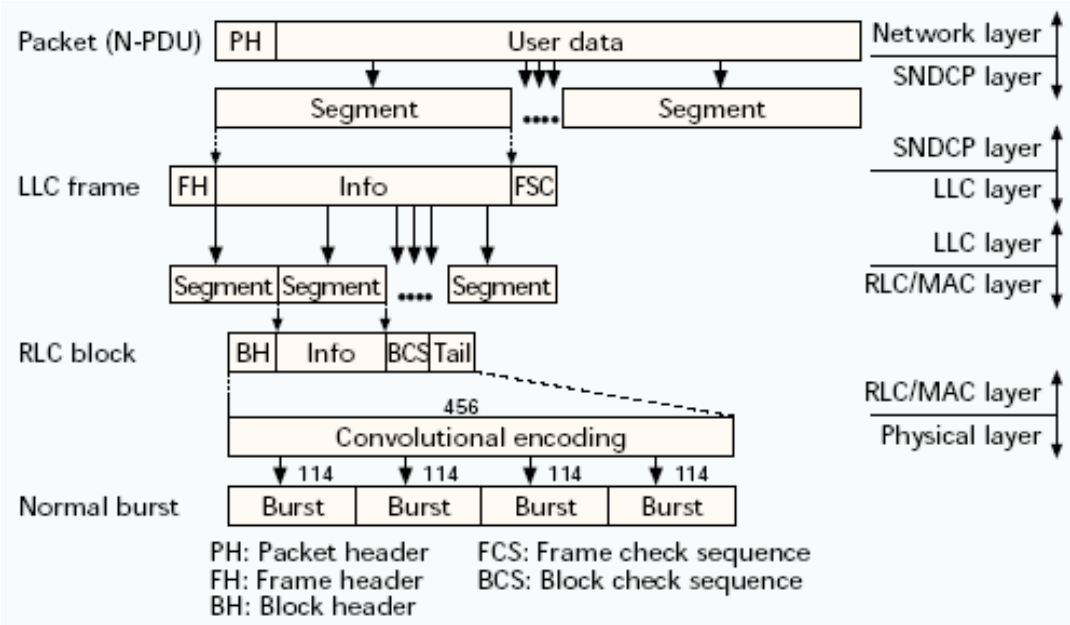
Η στοίβα πρωτοκόλλων που χρησιμοποιεί το GPRS παρουσιάζεται στην Εικόνα 14 που ακολουθεί.



<u>Εικόνα 14</u> : Τα πρωτόκολλα του GPRS

Η διαχείριση κίνησης (GMM) και συνόδου (SM) ανήκουν στο πρώτο στρώμα (SNDCP). Το στρώμα αυτό παρέχει άμεση επικοινωνία του κινητού χρήστη GPRS με τον κόμβο εξυπηρέτησης SGSN και μια πολύ σημαντική λειτουργία που επιτελεί είναι η συμπίεση. Άλλωστε, στο GPRS, ο συνδρομητής πληρώνει για κάθε byte που μεταδίδει και λαμβάνει και δεδομένου ότι σε ένα τέτοιο δίκτυο μεταγωγής πακέτων, όπως το GPRS, κάθε πακέτο μεταφέρει τη δικιά του επικεφαλίδα με όλα τα απαραίτητα στοιχεία δρομολόγησης, είναι αναγκαίο να εφαρμοστεί συμπίεση. Δύο μέθοδοι συμπίεσης χρησιμοποιούνται στο GPRS: α) η RFC 1144, αποκλειστικά για TCP/IP επικεφαλίδες, με την οποία 40 bytes συνολικής TCP/IP επικεφαλίδας συμπιέζονται σε 2 με 3 bytes, και η V.42 bis για τη συμπίεση επικεφαλίδων κάθε είδους .

Το αμέσως επόμενο επίπεδο LLC παρέχει κρυπτογράφηση, έλεγχο ροής και έλεγχο σειράς και προαιρετικά ανίχνευση και διόρθωση σφαλμάτων μετάδοσης, ενώ η προσαρμογή των πακέτων LLC (LLC PDU) στο φυσικό στρώμα πραγματοποιείται από το στρώμα RLC/MAC. Πέραν τούτου, το στρώμα αυτό ελέγχει την πρόσβαση στους πόρους του δικτύου, κατανέμει τους πόρους μεταξύ των διαφόρων κινητών σταθμών και φυσικά έχει την ευθύνη για την απελευθέρωσή τους. Ακριβώς επειδή αναλαμβάνει τη διαχείριση των πόρων του δικτύου, το επίπεδο RLC/MAC επεκτείνεται ανάμεσα στο MS και το PCU. Ο έλεγχος ροής και η μετάδοση – με τη μέθοδο σήραγγας – από το PCU μέχρι το SGSN γίνεται με το πρωτόκολλο BSSGP. Η διασύνδεση μεταξύ των στοιχείων του δικτύου πρόσβασης και του δικτύου κορμού (διεπαφή G_b) εξασφαλίζεται με το πρωτόκολλο FR (Frame Relay). Στην Εικόνα 15 φαίνεται η μετατροπή των πακέτων που μεταδίδονται από το MS μέχρι το SGSN, η οποία λαμβάνει χώρα από το αρχικό στρώμα SNDCP μέχρι την τελική μετάδοσή τους στη ραδιοζεύξη [11].



Εικόνα 15 : Μετατροπή των πακέτων μέχρι τη μετάδοσή τους στο φυσικό στρώμα

Όπως βλέπουμε στη στοίβα πρωτοκόλλων, η διασύνδεση των στοιχείων του δικτύου κορμού (διεπαφή G_n) γίνεται με το πρωτόκολλο IP. Πρόκειται για μη αξιόπιστη υπηρεσία δικτύωσης χωρίς σύνδεση με κύρια ευθύνη τη δρομολόγηση των πακέτων μεταξύ των κόμβων SGSN και GGSN. Το TCP και το UDP αποτελούν το επίπεδο μεταφοράς, είναι δηλαδή υπεύθυνα για τη μεταφορά και τη σωστή απόδοση των πακέτων από τον έναν κόμβο στον άλλο (SGSN προς GGSN ή αντίστροφα). Το TCP παρέχει αξιόπιστη υπηρεσία μεταφοράς μέσω σύνδεσης, ενώ το UDP μη αξιόπιστη μεταφορά χωρίς σύνδεση [12]. Και τα δύο αυτά πρωτόκολλα μεταφοράς χρησιμοποιούν τις υπηρεσίες του IP για τον κατακερματισμό των μηνυμάτων σε πακέτα και τη δρομολόγηση των πακέτων αυτών . Στην περίπτωση του UDP, πακέτα μπορεί να χαθούν ή να φτάσουν σε πολλαπλά αντίγραφα ή με λάθος σειρά, ενώ αυτά δε συμβαίνουν στο TCP γιατί εφαρμόζει έλεγχο ροής , αλγορίθμους για αποφυγή συμφόρησης, μηχανισμούς αναμετάδοσης σε περιπτώσεις μεγάλης καθυστέρησης, διόρθωση σφαλμάτων , παράδοση των πακέτων στη σωστή σειρά κ.τ.λ. Τέλος, το GTP παρέχει έναν μηχανισμό σήραγγας για την μετάδοση των πακέτων στο δίκτυο κορμού. Για κάθε πλαίσιο λειτουργίας PDP (PDP context) που έχει ενεργοποιημένο ένας κινητός σταθμός και επικοινωνεί με κάποιο εξωτερικό δίκτυο, ένα μοναδικό GTP τούνελ εγκαθίσταται προκειμένου να μεταφέρει τα δεδομένα. Άλλωστε το γεγονός ότι το GPRS συνδέεται με δίκτυα όπως το Internet οφείλεται στο ότι τόσο το δίκτυο κορμού του GPRS όσο και το Internet βασίζονται στο κοινό πρωτόκολλο IP.

3. ***UMTS***

Αν θέλαμε να περιγράψουμε συνοπτικά το σύστημα που αναπτύσσει και εξελίσσει το 3GPP, τότε θα λέγαμε ότι είναι «μία διεπαφή CDMA στον αέρα μέσω της οποίας ανταλλάσσονται πακέτα, σε συνδυασμό με ένα εξελιγμένο κεντρικό δίκτυο GSM/GPRS». Από την άλλη πλευρά, η οικογένεια προτύπων IMT-2000 περιλαμβάνει πολλές άλλες τεχνολογίες. Όμως, η τεχνολογία που συνδυάζει το WCDMA με το GSM και η οποία αναπτύσσεται από το 3GPP, είναι η πιο δημοφιλής.

Ο λόγος για αυτή την επικράτηση είναι προφανής: μεταξύ των τεχνολογιών δεύτερης γενιάς, η τεχνολογία GSM ήταν η πιο διαδεδομένη. Συνεπώς, οι εταιρίες επέλεξαν την οικονομικότερη μεταξύ των προτάσεων του IMT-2000, δηλαδή αυτήν την πρόταση η οποία διατηρούσε την αξία και τη λειτουργικότητα των προηγούμενων επενδύσεών τους. Ο συνδυασμός του WCDMA με τις εξελίξεις του GSM όσον αφορά το δίκτυο κορμού, ονομάζεται Universal Mobile Telecommunications System (UMTS). Πρόκειται για το σύστημα τρίτης γενιάς που έχει επικρατήσει στην Ευρώπη και σταδιακά επεκτείνεται στη Βόρεια Αμερική με αποτέλεσμα η τρίτη γενιά κυψελωτών κινητών συστημάτων να τείνει να ταυτιστεί με αυτό το σύστημα. Επίσης θα παρουσιαστούν τα χαρακτηριστικά, η δομή, η λειτουργία και η αρχιτεκτονική του συστήματος UMTS.

3.1 Γενικά Χαρακτηριστικά του UMTS

Όπως έχει ήδη αναφερθεί, η μετάβαση ενός δικτύου GSM σε ένα δίκτυο UMTS είναι ιδιαίτερα ομαλή. Αυτή η εξέλιξη είναι ακόμα απλούστερη αν στο δίκτυο GSM έχει ενσωματωθεί και η τεχνολογία GPRS. Τα συστήματα GSM σταδιακά ενσωμάτωσαν πολλά χαρακτηριστικά τα οποία είναι συμβατά με τις απαιτήσεις του UMTS. Η Εικόνα 16 παρουσιάζει τα βασικά χαρακτηριστικά του UMTS και εξετάζει το κατά πόσο υπάρχει συμβατότητα με τις λειτουργίες του GSM

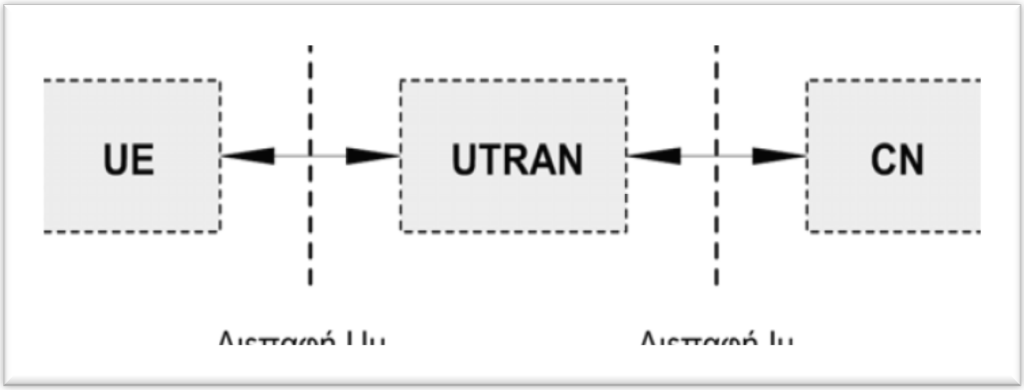
ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ UMTS	**ΣΥΜΒΑΤΟΤΗΤΑ ΤΟΥ GSM**
Μικρές και άνετες φορητές συσκευές	Ναι
Οπουδήποτε και κάθε στιγμή (συμβατά με οικιακά ασύρματα δίκτυα)	Ναι (picocells, GSM office)
Οπουδήποτε (συμβατά με δορυφορικά δίκτυα)	Ναι
Διεισδυτικότητα σε κτίρια, υπόγεια κ.α	Ναι
Ομιλία υψηλής ποιότητας	Ναι
Παγκόσμια περιαγωγή	Ναι
Υπηρεσίες νοήμονος δικτύου	Ναι
Υπηρεσίες Δεδομένων	Ναι (GPRS)
Υποστήριξη υψηλής πυκνότητας χρηστών	Ναι (ιεραρχίες κελιών)
Πολυμέσα, ψυχαγωγία	Ναι (HSCSD)
Εναλλαγή μεταξύ φορέων πραγματικού χρόνου και όχι	Όχι

Υπηρεσίες ρυθμών μετάδοσης άνω των 200 Kbps	Όχι

Εικόνα 16: Τα χαρακτηριστικά του UMTS και η συμβατότητα του GSM

Το δίκτυο GSM με όλες τις προσθήκες και τις βελτιώσεις προσεγγίζει ένα δίκτυο UMTS. Τα μόνα χαρακτηριστικά του UMTS τα οποία δεν καλύπτονται από ένα δίκτυο GSM οφείλονται στην πιο ευέλικτη διεπαφή CDMA που χρησιμοποιεί στον αέρα, η οποία μπορεί να υποστηρίξει ταυτόχρονα διαφορετικούς τύπους φορέα. Επίσης, το UMTS μπορεί να υποστηρίξει μεγαλύτερους ρυθμούς μετάδοσης που όμως δεν απέχουν πολύ από τους ρυθμούς μετάδοσης που υποστηρίζουν τα δίκτυα GSM της γενιάς 2,5.

3.2 Η Αρχιτεκτονική του UMTS



Εικόνα 17: Η αρχιτεκτονική του UMTS σε υψηλό επίπεδο

3.2.1 User Equipment

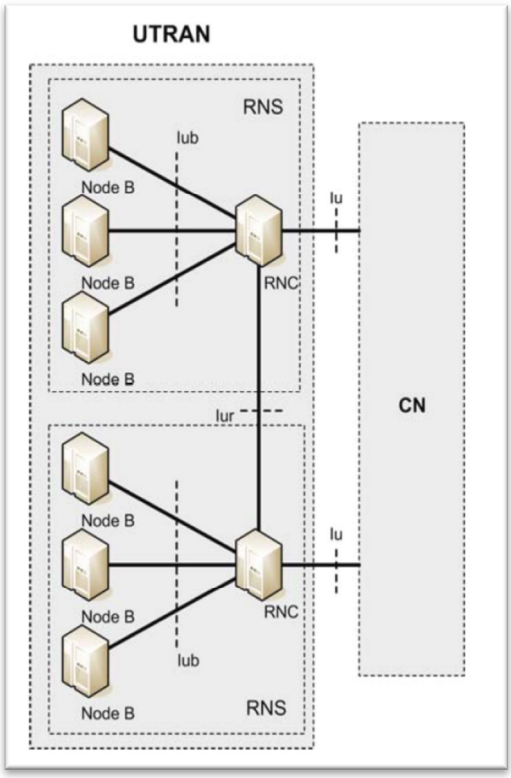
Ο όρος User Equipment (UE) θα λέγαμε ότι ταυτίζεται με την έννοια της φορητής συσκευής. Για παράδειγμα, UE μπορεί να αποτελέσει ένα κινητό τηλέφωνο, μία συσκευή Personal Digital Assistant (PDA) ή ένας φορητός υπολογιστής. Το UE είναι συνδεδεμένο μέσω της διεπαφής Uu, που είναι βασισμένη στην τεχνολογία WCDMA, με το UTRAN. Ένα UE μπορεί να συνδεθεί ταυτόχρονα με περισσότερα του ενός κελιά [13],[14]. Το UE αποτελείται από δύο τμήματα:

• Τον Mobile Equipment: αποτελείται από το ίδιο το hardware της φορητής συσκευής. Όμως, η συσκευή από μόνη της δε μπορεί να παρέχει καμία υπηρεσία.

• Την κάρτα USIM: πρόκειται για μία κάρτα η οποία περιέχει όλες τις απαραίτητες πληροφορίες προκειμένου να είναι δυνατή η πρόσβαση στο δίκτυο UMTS και η ταυτοποίηση από αυτό. Η κάρτα USIM είναι μία κάρτα αντίστοιχη της κάρτας SIM των δικτύων GSM. Όμως, ενώ η χωρητικότητα μίας κάρτας SIM είναι 8 ή 32 Kbytes, η χωρητικότητα της κάρτας USIM είναι τέτοια ώστε να μπορεί να αποθηκεύει προσωπικά δεδομένα της τάξης των Mbytes.

3.2.2 UTRAN

Το UMTS Terrestrial Radio Access Network είναι ένα νέο δίκτυο ασύρματης πρόσβασης το οποίο είναι ειδικά σχεδιασμένο για το σύστημα UMTS. Διαχωρίζεται από το UE μέσω της διεπαφής Uu και από το Core Network (CN) μέσω της διεπαφής Iu. Η βασικότερη λειτουργία του UTRAN είναι η εποπτεία και η διαχείριση των ασύρματων πόρων του δικτύου. Η λειτουργία αυτή συμπεριλαμβάνει την ευθύνη για τον έλεγχο της ισχύος καθώς και την υποστήριξη και διαχείριση των handovers. Η Εικόνα 18 απεικονίζει την δομή του UTRAN.



Εικόνα 18: Η δομή του UTRAN

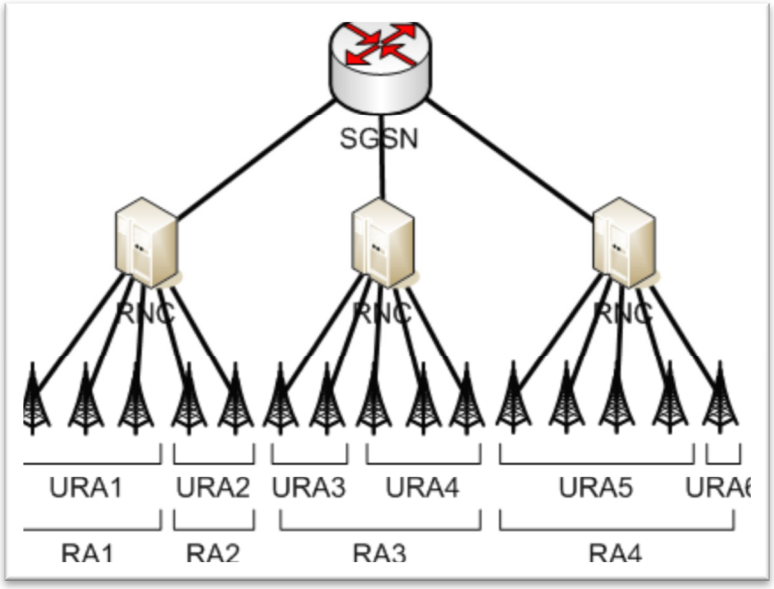
Όπως φαίνεται από την Εικόνα 18, το δίκτυο UTRAN αποτελείται από τους Radio Network Controllers (RNCs) και τους Node Bs. Οι Node Bs είναι υπεύθυνοι για τον έλεγχο ενός ή περισσοτέρων κελιών. Μία ομάδα από Node Bs συνδέεται, μέσω των διεπαφών Iub, με έναν κόμβο RNC. Ο Node B λειτουργεί στο επίπεδο φυσικού μέσου και δικτύου (μοντέλο OSI) και μεταφέρει δεδομένα προς τον RNC στον οποίο είναι συνδεδεμένος. Επιπλέον, κάνει μετρήσεις πάνω στην ποιότητα και την ισχύ των ασύρματων συνδέσμων προς τα UEs και δίνει αναφορές στον RNC.

Κάθε κόμβος RNC ελέγχει έναν ή περισσότερους Node Bs. Ένας κόμβος RNC μαζί με τους συνδεδεμένους σε αυτόν Node Bs αποτελούν ένα Radio Network Subsystem (RNS). Ο RNC λαμβάνει τις πληροφορίες που συλλέγουν οι Node Bs του δικού του RNS και προσαρμόζει τις παραμέτρους του ασύρματου υποσυστήματος. Μία τέτοια παράμετρος μπορεί να είναι η ισχύς του ασύρματου σήματος στο UE ή στον Node B.

Επίσης, ο RNC είναι υπεύθυνος για την ανάθεση του κώδικα WCDMA που θα χρησιμοποιήσουν ο Node B και το UE στη μεταξύ τους επικοινωνία, έτσι ώστε να μην υπάρξουν παρεμβολές από άλλους ασύρματους συνδέσμους. Τέλος, μία άλλη λειτουργία των κόμβων RNC είναι ο έλεγχος των handovers που λαμβάνουν χώρα μεταξύ διαφορετικών RNSs. Προκειμένου να υλοποιηθεί η συγκεκριμένη διαδικασία οι RNCs είναι συνδεδεμένοι μεταξύ τους μέσω της διεπαφής Iur (Εικόνα 18). Πρόκειται για μία διεπαφή η οποία είναι υλοποιημένη με δίκτυο Asynchronous Transfer Mode (ATM).

Όπως φαίνεται στην Εικόνα 20, ένας κόμβος RNC συνδέεται με το CN μέσω της διεπαφής Iu. Η συγκεκριμένη διεπαφή έχει δύο συνιστώσες: τη συνιστώσα Iu-Circuit Switched (Iu-CS) που χρησιμοποιείται για υπηρεσίες μεταγωγής κυκλώματος (φωνή) και τη συνιστώσα Iu-Packet Switched (Iu-PS) που χρησιμοποιείται για υπηρεσίες μεταγωγής πακέτων (υπηρεσίες δεδομένων).

Στο UTRAN τα κελιά ομαδοποιούνται σε ομάδες κελιών οι οποίες ονομάζονται Routing Areas (RAs). Επίσης, τα κελιά σε μια RA ομαδοποιούνται περαιτέρω σε UTRAN Registration Areas (URAs) όπως παρουσιάζεται στην Εικόνα 19.



Εικόνα 19: RAs και URAs

3.2.3 CN

Το CN είναι το δίκτυο κορμού του συστήματος UMTS. Είναι συνδεδεμένο με άλλα δίκτυα όπως τηλεφωνικά δίκτυα Public Telephone Switched Network (PSTN), δίκτυα δεδομένων Public Data Networks (PDNs) όπως το Internet καθώς και με άλλα κινητά δίκτυα. Το CN είναι υπεύθυνο για τη δρομολόγηση, την ταυτοποίηση, τον εντοπισμό των χρηστών καθώς και για άλλες πολλές βασικές λειτουργίες. Το CN διαιρείται σε δύο πεδία: το πεδίο μεταγωγής κυκλώματος (CS) και το πεδίο μεταγωγής πακέτων (PS).

Όσον αφορά το πεδίο CS, αυτό περιλαμβάνει τους εξής κόμβους:

• **Mobile Services Switching Center (MSC):** Ο κόμβος MSC αποτελεί έναν κόμβο μεταγωγής ο οποίος δρομολογεί τα δεδομένα των υπηρεσιών μεταγωγής κυκλώματος εντός του δικτύου UMTS. Κάθε κόμβος MSC διαχειρίζεται πολλά RNCs τα οποία συνδέονται σε αυτόν μέσω της διεπαφής Iu-CS. Επίσης, είναι συνδεδεμένος με τις βάσεις δεδομένων του δικτύου όπως τη βάση δεδομένων Home Location Register (HLR) και τη Visitor Location Register (VLR). Τέλος, μία άλλη πολύ χρήσιμη λειτουργία του κόμβου MSC είναι η διαχείριση της κινητικότητας των χρηστών για τις υπηρεσίες μεταγωγής κυκλώματος.

• **Gateway Mobile Services Switching Center (GMSC):** Ο κόμβος GMSC είναι συνδεδεμένος με τους κόμβους MSC. Η λειτουργία του είναι να διασυνδέει το δίκτυο UMTS με άλλα δίκτυα μεταγωγής κυκλώματος όπως PSTN και ISDN.

• **Visitor Location Register (VLR):** Ο κόμβος VLR είναι μία βάση δεδομένων. Συνήθως κάθε VLR αντιστοιχεί σε έναν MSC. Η βάση VLR αποθηκεύει προσωρινή πληροφορία σχετικά με την ταυτοποίηση και την ασφάλεια καθώς και άλλες χρήσιμες πληροφορίες που σχετίζονται με όλους τους χρήστες που διαχειρίζεται κάθε δεδομένη στιγμή ο αντίστοιχος MSC. Η βάση VLR λαμβάνει την αρχική πληροφορία από τη βάση HLR και αναλαμβάνει να την ενημερώσει για τυχόν μεταβολές στα δεδομένα της. Όλες οι συναλλαγές μεταξύ VLR και HLR γίνονται μέσω ενός MSC.

Όσον αφορά το πεδίο PS, αυτό αποτελείται από τους παρακάτω κόμβους. Αξίζει να επισημανθεί η αντιστοιχία που υπάρχει με τους κόμβους του πεδίου CS.

• **Serving GPRS Support Node (SGSN):** Ο SGSN αποτελεί τον αντίστοιχο κόμβο του MSC στο πεδίο CS. Αυτό σημαίνει ότι αναλαμβάνει τη δρομολόγηση δεδομένων των υπηρεσιών μεταγωγής πακέτων εντός του δικτύου UMTS. Επιπλέον, διαχειρίζεται τους κόμβους RNCs οι οποίοι είναι συνδεδεμένοι σε αυτόν μέσω της διεπαφής Iu-PS. Επίσης, αλληλεπιδρά με βάσεις δεδομένων, όπως η βάση HLR. Τέλος, ο κόμβος SGSN είναι υπεύθυνος για τη διαχείριση της κινητικότητας των χρηστών για τις υπηρεσίες μεταγωγής πακέτων.

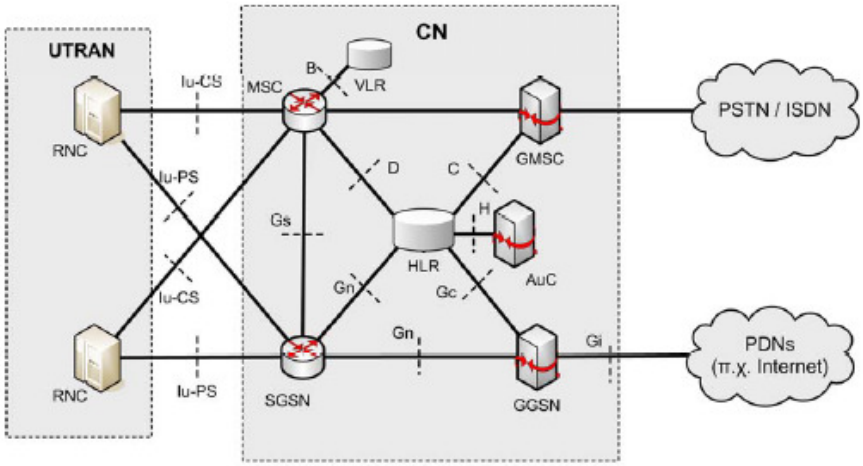
• **Gateway GPRS Support Node (GGSN):** Πρόκειται για έναν κόμβο αντίστοιχο του GMSC του πεδίου CS. Διασυνδέει τους κόμβους SGSNs με εξωτερικά δίκτυα μεταγωγής πακέτων όπως το X.25 και το Internet.

Τέλος, υπάρχουν ορισμένοι κόμβοι του CN οι οποίοι είναι κοινοί, δηλαδή τους χρησιμοποιούν και τα δύο πεδία. Παρακάτω, αναφέρονται οι δύο σημαντικότεροι από αυτούς:

• **Home Location Register (HLR):** Πρόκειται για μία βάση δεδομένων η οποία αποθηκεύει δεδομένα των χρηστών τα οποία μένουν σχετικά σταθερά στο χρόνο. Αυτά τα δεδομένα είναι αναγνωριστικά, πληροφορίες για τις υπηρεσίες του δικτύου στις οποίες συμμετέχει ο συνδρομητής κ.α.

• **Authentication Center (AuC):** Αποτελεί έναν κόμβο που είναι συσχετισμένος με έναν HLR. Ο κόμβος αυτός αποθηκεύει πληροφορίες ταυτοποίησης και κρυπτογράφησης για τους συνδρομητές. Οι πληροφορίες αυτές φορτώνονται στον κόμβο κατά την έναρξη της συνδρομής από το χρήστη.

Η Εικόνα 20 δείχνει τη δομή του CN. Εκτός από τους κόμβους που προαναφέρθηκαν, στην εικόνα αυτή σημειώνονται οι διεπαφές μεταξύ των κόμβων του CN [14].



Εικόνα 20: Η δομή του CN

3.3 Βασικές Διεπαφές και Αρχιτεκτονική Πρωτοκόλλων

Στην παράγραφο αυτή θα παρουσιαστούν οι βασικότερες διεπαφές του δικτύου UMTS. Επίσης, για κάθε διεπαφή θα παρουσιαστούν τα πρωτόκολλα επικοινωνίας και σηματοδοσίας που χρησιμοποιούνται για την επικοινωνία των κόμβων που αλληλεπιδρούν. Η ανάλυση που θα ακολουθήσει θα εστιαστεί στο πεδίο.

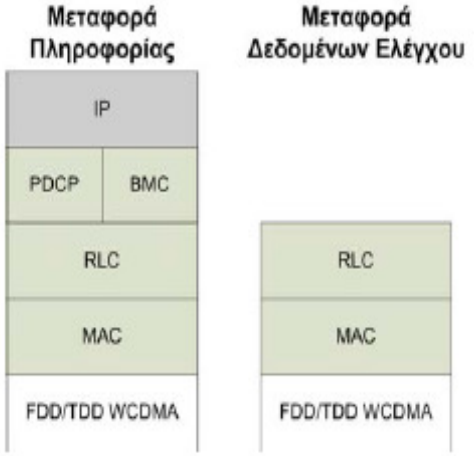
3.3.1 Η Διεπαφή Uu

Η ασύρματη διεπαφή είναι πάντοτε η πιο κρίσιμη διεπαφή κατά το σχεδιασμό των πρωτοκόλλων ενός κινητού δικτύου. Για το UMTS, η διεπαφή Uu μεταξύ του Node B και του UE, έχει υλοποιηθεί με την αρχιτεκτονική που απεικονίζει η Εικόνα 21. Όπως φαίνεται, έχουν προσδιοριστεί τα επίπεδα πρωτοκόλλων που αντιστοιχούν στο επίπεδο φυσικού μέσου, το επίπεδο ζεύξης δεδομένων καθώς και το επίπεδο δικτύου.

Το επίπεδο φυσικού μέσου (1ο επίπεδο στο μοντέλο διασυνδέσεων OSI) είναι υπεύθυνο για τη μετάδοση των δεδομένων μέσω της ασύρματης διεπαφής. Για το επίπεδο αυτό οι προδιαγραφές του UMTS καθορίζουν τη χρήση των τεχνολογιών FDD και TDD του WCDMA.

Όσον αφορά το επίπεδο ζεύξης δεδομένων (2ο επίπεδο), αυτό περιέχει τέσσερα υπό-επίπεδα. Τα δύο πρώτα υπό-επίπεδα χρησιμοποιούνται για τη μεταφορά δεδομένων ελέγχου αλλά και πληροφορίας. Το πρώτο υπό-επίπεδο χρησιμοποιεί το πρωτόκολλο Medium Access Control (MAC) [15]. Το πρωτόκολλο MAC βρίσκεται αμέσως μετά το φυσικό επίπεδο. Χρησιμοποιεί λογικά κανάλια και τα αντιστοιχίζει σε κανάλια μεταφοράς για την επικοινωνία του φυσικού επιπέδου με τα υψηλότερα επίπεδα.

Επίσης, το πρωτόκολλο αυτό διαχειρίζεται τις προτεραιότητες μεταξύ των UEs, όπως επίσης και τις προτεραιότητες μεταξύ των ροών δεδομένων που αφορούν ένα συγκεκριμένο UE. Άλλες λειτουργίες που εκτελεί το πρωτόκολλο MAC είναι ο έλεγχος των κινήσεων, η κρυπτογράφηση, η πολυπλεξία κ.α. Το δεύτερο πρωτόκολλο που συναντάμε στο επίπεδο ζεύξης δεδομένων της διεπαφής Uu είναι το Radio Link Control (RLC). Το πρωτόκολλο αυτό είναι υπεύθυνο για την εγκατάσταση και παρακολούθηση της μεταφοράς δεδομένων καθώς και για τις ρυθμίσεις QoS.



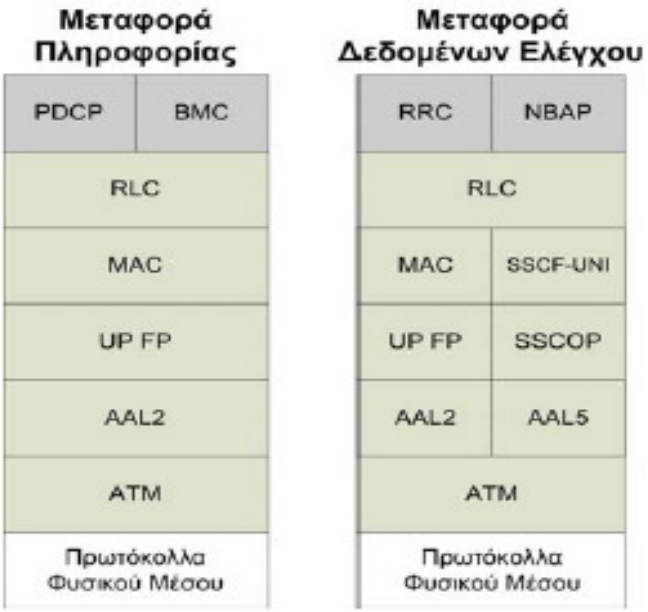
Εικόνα 21: Τα πρωτόκολλα της διεπαφής Uu

Τα επόμενα δύο πρωτόκολλα χρησιμοποιούνται μόνο για τη μεταφορά πληροφορίας και όχι για τη μεταφορά δεδομένων ελέγχου. Τα πρωτόκολλα αυτά είναι το Packet Data Convergence Protocol (PDCP) και το Broadcast Control (BMC). Το πρώτο είναι υπεύθυνο για τη μετατροπή των δεδομένων που παρέχουν τα πραγματικά πρωτόκολλα δεδομένων των πιο πάνω επιπέδων, σε ασύρματα πρωτόκολλα. Το PDCP προς το παρόν υποστηρίζει τα πρωτόκολλα IPv4 και IPv6 και μπορεί εύκολα να επεκταθεί προκειμένου να υποστηρίξει περισσότερα. Το πρωτόκολλο BMC είναι υπεύθυνο για τις υπηρεσίες broadcast και multicast μετάδοσης.

3.3.2 Η Διεπαφή Iub

Η διεπαφή Iub είναι αυτή που διασυνδέει τους κόμβους RNC με τους Node Bs. Η Εικόνα 22 δείχνει την ιεραρχία των πρωτοκόλλων που χρησιμοποιούνται για την υλοποίηση της συγκεκριμένης διεπαφής. Πρόκειται για μία διεπαφή η οποία είναι ενσύρματη και, κατά συνέπεια, το επίπεδο φυσικού μέσου μπορεί να υλοποιηθεί από πρωτόκολλα όπως το ETSI STM-1, STM-4, SONET STS-3c, ITU STS-1 κ.α. Πάνω από το επίπεδο αυτό, στο επίπεδο ζεύξης δεδομένων χρησιμοποιείται το πρωτόκολλο ATM. Πρόκειται για ένα πρωτόκολλο το οποίο χρησιμοποιείται σε όλες τις ενσύρματες διεπαφές του δικτύου UMTS. Αυτό γιατί μπορεί να χειρίζεται όλους τους τύπους κινήσεων. Για την ακρίβεια, το ATM μπορεί να χρησιμοποιηθεί για σύγχρονες αλλά και για ασύγχρονες κινήσεις όπως επίσης και για κινήσεις μεταγωγής πακέτων αλλά και κυκλώματος.

Όπως δείχνει η Εικόνα 22, πάνω από το επίπεδο του ATM χρησιμοποιούνται τα πρωτόκολλα ATM Adaptation Layer (AAL) 2 και 5. Το AAL2 χρησιμοποιείται για τη μεταφορά δεδομένων ελέγχου όπως επίσης και για τη μεταφορά πληροφορίας. Το AAL5 χρησιμοποιείται μόνο για τη μεταφορά δεδομένων ελέγχου. Τα πρωτόκολλα αυτά αναλαμβάνουν την επεξεργασία των δεδομένων από τα υψηλότερα επίπεδα προκειμένου να μπορούν να μεταδοθούν από το επίπεδο ATM.



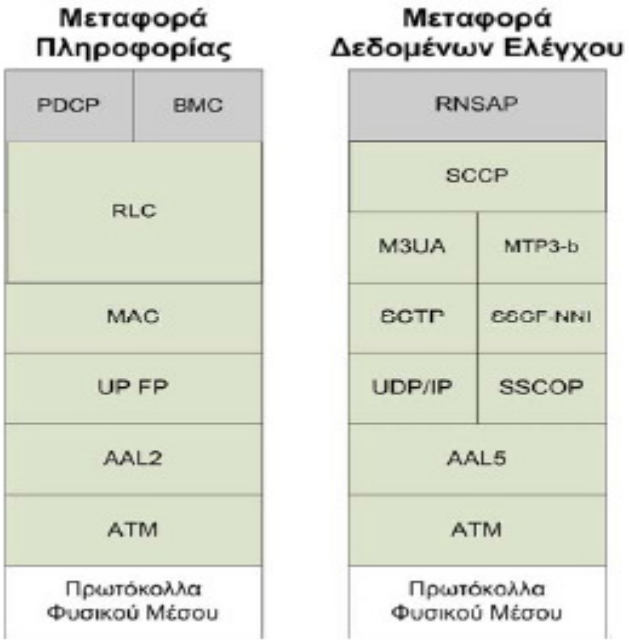
Εικόνα 22: Τα πρωτόκολλα της διεπαφής Iub

Στο αμέσως υψηλότερο υπό-επίπεδο συναντούμε δύο άλλα πρωτόκολλα. Πρόκειται για το User Plane Framing Protocol (UP FP) και Service Specific Connection-Oriented Protocol (SSCOP). Το πρώτο πρωτόκολλο βρίσκεται πάνω από το AAL2 και χρησιμοποιείται για τη μεταφορά δεδομένων ελέγχου αλλά και πληροφορίας. Αντίθετα, το πρωτόκολλο SSCOP τοποθετείται πάνω από το AAL5. Πρόκειται για ένα πρωτόκολλο που παρέχει αξιόπιστη μεταφορά δεδομένων παράλληλα με συντήρηση της σύνδεσης και έλεγχο ροής. Η χρήση του στη διεπαφή Iub σχετίζεται με τη μεταφορά δεδομένων ελέγχου. Όπως φαίνεται από την Εικόνα 22, στα ανώτερα υπό-επίπεδα του επιπέδου ζεύξης δεδομένων συναντούμε το πρωτόκολλο Service Specific Coordination Function for Support of Signaling at the User-Network Interface (SSCF-UNI) καθώς και τα ήδη γνωστά πρωτόκολλα MAC, RLC, RRC, και PDCP. Τέλος, το πρωτόκολλο Node B Application Part (NBAP) χρησιμοποιείται προκειμένου να δίνεται η δυνατότητα στον RNC να διαχειρίζεται κάθε Node B που έχει συνδεθεί σε αυτόν.

3.3.3 Η Διεπαφή Iur

Η διεπαφή Iur διασυνδέει δύο RNCs. Πρόκειται για μία διεπαφή η οποία εισήχθη στα συστήματα UMTS, ενώ στα συστήματα GSM δεν υπήρχε άμεση σύνδεση μεταξύ των

αντίστοιχων κόμβων. Χρησιμοποιείται για τη μεταφορά δεδομένων ελέγχου αλλά και πληροφορίας. Ειδικότερα, όσον αφορά τα δεδομένα ελέγχου, αυτά σχετίζονται με τη διαχείριση των ασύρματων πόρων καθώς και με τις διαδικασίες του handover και του SRNS relocation.



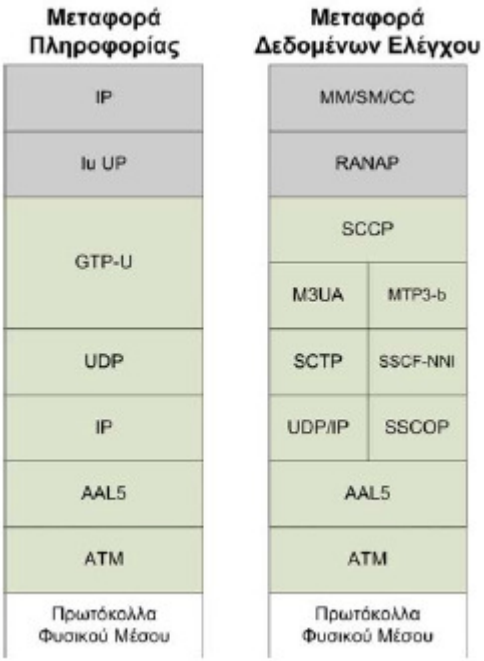
Εικόνα 23: Τα πρωτόκολλα της διεπαφής Iur

Όπως φαίνεται από την Εικόνα 23, η ιεραρχία των πρωτοκόλλων για τη μεταφορά πληροφορίας δε διαφέρει από τη διεπαφή Iub. Όσον αφορά τα δεδομένα ελέγχου έχουμε τη χρήση αρκετών νέων πρωτοκόλλων σε σχέση με τις προηγούμενες διεπαφές. Καταρχήν, η Εικόνα 23 δείχνει ότι χρησιμοποιείται ο συνδυασμός Internet Protocol (IP)/User Datagram Protocol (UDP) ακριβώς πάνω από το επίπεδο του AAL5. Πρόκειται για την υλοποίηση του «IP over ATM» κατά την οποία η πληροφορία του IP καταμερίζεται με τέτοιο τρόπο ώστε να μπορεί να μεταδοθεί πάνω από το ATM. Επιπλέον, τα υπόλοιπα τέσσερα νέα πρωτόκολλα ελέγχου και σηματοδοσίας είναι: το Message Transfer Part Level 3 (MTP3-b) για τον έλεγχο της δρομολόγησης των μηνυμάτων, το MTP3 User Adaptation Layer (M3UA), το Signaling Connection Control Part (SCCP) και το Radio Network Sublayer Application Part (RNSAP). Ειδικότερα για το RNSAP, πρόκειται για ένα πρωτόκολλο το οποίο παρέχει όλες τις λειτουργίες για τη διαχείριση των ασύρματων πόρων, για τις μετρήσεις πάνω σε αυτούς και για την υποστήριξη των διαδικασιών του handover και SRNS relocation.

3.3.4 Η Διεπαφή Iu-PS

Η παρούσα παράγραφος παρουσιάζει την ιεραρχία των πρωτοκόλλων όσον αφορά τη διεπαφή Iu-PS. Η διεπαφή Iu-PS είναι, για το πεδίο PS, ο σύνδεσμος όχι μόνο των RNCs με τους κόμβους SGSN αλλά και μεταξύ των δύο δομικών στοιχείων του

UMTS, του UTRAN και του CN. Το βασικότερο πρωτόκολλο μεταφοράς δεδομένων ελέγχου που χρησιμοποιείται πάνω από αυτή τη διεπαφή είναι το Radio Access Network Application Part (RANAP) το οποίο απεικονίζεται μεταξύ των άλλων στην παρακάτω Εικόνα 24.



Εικόνα 24: Τα πρωτόκολλα της διεπαφής Iu-PS

Το RANAP είναι το πρωτόκολλο που εξασφαλίζει τη σηματοδοσία μεταξύ του UTRAN και του CN. Το πρωτόκολλο αυτό παρέχει υπηρεσίες που σχετίζονται με τη διαδικασία SRNS relocation, τη διαχείριση ροής και συμφόρησης της διεπαφής Iu-PS, τον εντοπισμό της θέσης κάθε UE καθώς και τη διαχείριση σφαλμάτων γενικότερα. Προκειμένου να μπορεί να εκτελεί τις πιο πάνω λειτουργίες διαχείρισης, το πρωτόκολλο RANAP διαθέτει και τις αντίστοιχες δυνατότητες για εποπτεία και αναφορά της κατάστασης του συστήματος. Τέλος, θα πρέπει να αναφερθούν οι λειτουργίες κρυπτογράφησης που παρέχει το συγκεκριμένο πρωτόκολλο. Μέσω της διεπαφής Iu-PS ανταλλάσσονται οι πληροφορίες κρυπτογράφησης μεταξύ UTRAN και CN προκειμένου τα δεδομένα που ανταλλάσσονται να είναι προστατευμένα από τυχόν απόπειρα υποκλοπής.

3.4 Τα Κανάλια του UTRAN

Στο UTRAN υπάρχουν τρεις διαφορετικοί τύποι καναλιών: τα λογικά κανάλια, τα κανάλια μεταφοράς και τα φυσικά κανάλια. Στις επόμενες παραγράφους περιγράφεται κάθε τύπος καναλιού και δίνονται ορισμένα παραδείγματα κατά περίπτωση.

3.4.1 Λογικά Κανάλια

Οι υπηρεσίες μεταφοράς δεδομένων του πρωτοκόλλου MAC παρέχονται μέσω των λογικών καναλιών. Τα λογικά κανάλια είναι αυτά που προσδιορίζουν τον τύπο της πληροφορίας που μεταδίδεται. Χρησιμοποιούνται στη διεπαφή μεταξύ των επιπέδων RLC και MAC. Τα κανάλια αυτά μπορούν να διαχωριστούν σε δύο κατηγορίες: τα κανάλια ελέγχου και τα κανάλια κίνησης. Στη συνέχεια, ένα κανάλι ελέγχου μπορεί να είναι είτε κοινό είτε αφιερωμένο. Κοινά λέγονται τα κανάλια point-to-multipoint, ενώ αφιερωμένα λέγονται τα κανάλια point-to-point, δηλαδή αυτά που χρησιμοποιούνται μόνο από ένα χρήστη [14]. Η Εικόνα 25 παρουσιάζει τα λογικά κανάλια καθώς και τη λειτουργία τους.

Λογικό Κανάλι Ελέγχου	Λειτουργία
Broadcast Control Channel (BCCH)	Κατερχόμενο κανάλι για broadcasting πληροφοριών ελέγχου
Paging Control Channel (PCCH)	Κατερχόμενο κανάλι μεταφορά πληροφορίας paging
Dedicated Control Channel (DCCH)	Κανάλι διπλής κατεύθυνσης για μεταφορά πληροφοριών αφιερωμένου ελέγχου
Common Control Channel (CCCH)	Κανάλι διπλής κατεύθυνσης για μεταφορά πληροφοριών ελέγχου μεταξύ του δικτύου και των UEs
Dedicated Traffic Channel (DTCH)	Αφιερωμένο κανάλι για τη μεταφορά πληροφοριών για ένα UE
Common Traffic Channel (CTCH)	Κατερχόμενο κανάλι point-to-multipoint για μεταφορά πληροφοριών για όλους ή μία ομάδα UEs

Εικόνα 25: Τα λογικά κανάλια του UTRAN

3.4.2 Κανάλια Μεταφοράς

Τα κανάλια μεταφοράς είναι αυτά που προσδιορίζουν τον τρόπο με τον οποίο θα μεταφερθούν τα δεδομένα από το επίπεδο φυσικού μέσου. Ουσιαστικά, τα κανάλια αυτά χρησιμοποιούνται στη διεπαφή που βρίσκεται μεταξύ του MAC πρωτοκόλλου και του αμέσως κατώτερου επιπέδου [13],[14].

	Αφιερωμένα Κανάλια	Κοινά Κανάλια		
	DCH	HS-DSCH	FACH	RACH
Ανερχόμενος / Κατερχόμενος Σύνδεσμος	Και οι δύο	Κατερχόμενος	Κατερχόμενος	Ανερχόμενος
Χρήση Κώδικα	Σύμφωνα με το μέγιστο ρυθμό μετάδοσης	Κοινός κώδικας μεταξύ των χρηστών	Σταθεροί κώδικες για κάθε κελί	Σταθεροί κώδικες για κάθε κελί
Γρήγορος Έλεγχος Ισχύος	Ναι	Όχι	Όχι	Όχι
Soft handover	Ναι	Όχι	Όχι	Όχι
Ενδεικνυόμενη Χρήση	Μεγάλα ποσά δεδομένων	Μεγάλα ποσά δεδομένων	Μικρά ποσά δεδομένων	Μικρά ποσά δεδομένων
Κατάλληλο για Καταιγιστικότητα	Όχι	Ναι	Ναι	Ναι
Τεχνολογία Διαθέσιμη στα Πρώιμα Συστήματα	Ναι	Όχι	Ναι	Ναι

Εικόνα 26: Οι ιδιότητες των καναλιών μεταφοράς

Υπάρχουν τρεις κατηγορίες καναλιών μεταφοράς: τα κοινά κανάλια (common channels), τα αφιερωμένα (dedicated) και τα διαμοιραζόμενα (shared). Τα κοινά κανάλια είναι κανάλια μονής κατεύθυνσης τα οποία χρησιμοποιούνται από όλους τους χρήστες σε ένα κελί. Τα σημαντικότερα από τα κανάλια αυτά είναι το Forward Access Channel (FACH) για τον κατερχόμενο σύνδεσμο και το Random Access Channel (RACH) για τον ανερχόμενο. Στην κατηγορία των διαμοιραζόμενων καναλιών ανήκει το Downlink Shared Channel (DSCH) καθώς και το High-Speed DSCH (HS-DSCH). Τα συγκεκριμένα κανάλια είναι πάντα συσχετισμένα με ένα αφιερωμένο κανάλι. Ειδικότερα, το HS-DSCH αποτελεί ένα κανάλι που υλοποιεί την τεχνολογία High-Speed Downlink Packet Access (HSPDA). Είναι ένα βελτιστοποιημένο κανάλι για ταχύτατη μετάδοση δεδομένων το οποίο ενσωματώνει έναν ευέλικτο μηχανισμό προσαρμογής του ρυθμού μετάδοσης. Από την άλλη πλευρά, στην κατηγορία του αφιερωμένου καναλιού ανήκει το Dedicated Channel (DCH) το οποίο είναι διπλής κατεύθυνσης και δεσμεύεται για ένα μόνο χρήστη. Αυτό σημαίνει ότι αν ένα DCH δεσμευθεί είτε ως ανερχόμενος είτε ως κατερχόμενος σύνδεσμος, τότε πρέπει να δεσμευθεί και για την αντίθετη κατεύθυνση. Στην αντίθετη κατεύθυνση όμως, ο ρυθμός μετάδοσης μπορεί να διαφέρει [16],[17].

Η Εικόνα 26 απεικονίζει τις βασικές ιδιότητες των σημαντικότερων καναλιών μεταφοράς. Όπως φαίνεται στον πίνακα, η διαδικασία του soft handover υποστηρίζεται μόνο από το κανάλι DCH. Αντίθετα, τα υπόλοιπα κανάλια υποστηρίζουν άλλων ειδών handovers. Επιπλέον, μόνο το HS-DSCH υποστηρίζει υψηλούς ρυθμούς δεδομένων. Επιπλέον, όλα τα κανάλια μεταφορά εκτός του DCH δεν υποστηρίζουν γρήγορο έλεγχο ισχύος (Fast Power Control). Αυτό είναι λογικό

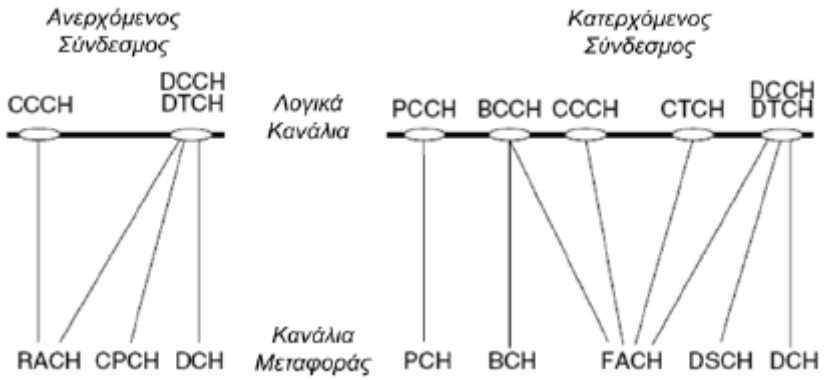
αφού είναι κοινά μεταξύ των χρηστών που βρίσκονται στο ίδιο κελί, με αποτέλεσμα ο έλεγχος ισχύος να μην είναι εύκολα εφικτός.

Κοινά Κανάλια	Λειτουργία
Broadcast Channel (BCH)	Κατερχόμενο κανάλι για broadcasting πληροφοριών
Paging Channel (PCH)	Κατερχόμενο κανάλι μεταφορά πληροφορίας paging
Random Access Channel (RACH)	Ανερχόμενο κανάλι για αρχική πρόσβαση στο δίκτυο
Common Packet Channel (CPCH)	Ανερχόμενο κανάλι για μετάδοση καταιγιστικής πληροφορίας
Forward Access Channel (FACH)	Κατερχόμενο κανάλι για μεταφορά μικρών ποσοτήτων πληροφορίας
Downlink Shared Channel (DSCH)	Κατερχόμενο κανάλι για μεταφορά αφιερωμένων δεδομένων ελέγχου και κίνησης
High-Speed Downlink Shared Channel (HS-DSCH	Κατερχόμενο κανάλι βελτιστοποιημένο για υψηλούς ρυθμούς μετάδοσης
Uplink Shared Channel (USCH)	Ανερχόμενο κανάλι για μεταφορά αφιερωμένων δεδομένων ελέγχου και κίνησης
Αφιερωμένο Κανάλι	**Λειτουργία**
Dedicated Channel (DCH)	Κανάλι διπλής κατεύθυνσης αφιερωμένο σε ένα UE

Εικόνα 27: Τα κανάλια μεταφοράς του UTRAN

Η Εικόνα 27 παρουσιάζει συνοπτικά όλα τα κανάλια μεταφοράς που χρησιμοποιούνται στο UTRAN καθώς και τη λειτουργία τους.

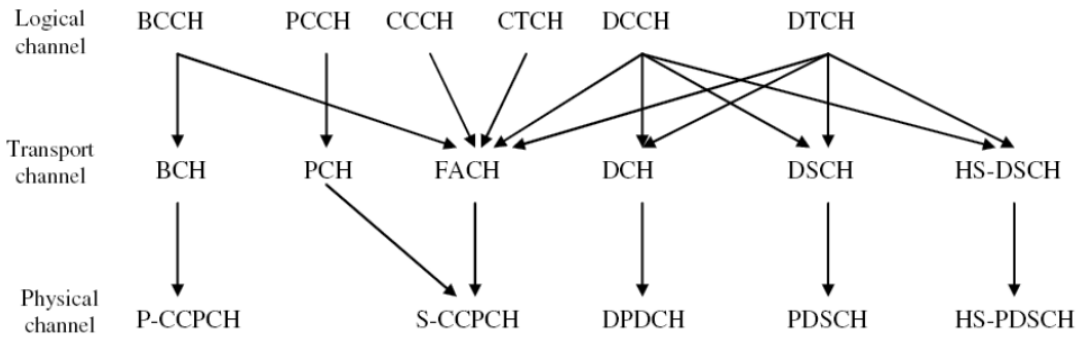
Όπως έχει ήδη αναφερθεί στην παράγραφο διεπαφή Uu, ο ρόλος του πρωτοκόλλου MAC είναι να αντιστοιχίζει τα λογικά κανάλια σε κανάλια μεταφοράς. Οι συγκεκριμένες αντιστοιχίες που υπάρχουν μεταξύ των λογικών και των καναλιών μεταφοράς, όσον αφορά τους κατερχόμενους και τους ανερχόμενους συνδέσμους, απεικονίζονται στην Εικόνα 28 [13].



Εικόνα 28: Η αντιστοιχία λογικών καναλιών σε κανάλια μεταφοράς

3.4.3 Φυσικά Κανάλια

Τα φυσικά κανάλια είναι αυτά που προσδιορίζουν τα ακριβή χαρακτηριστικά του φυσικού μέσου. Αυτό γιατί αποτελούν τα κανάλια τα οποία χρησιμοποιούνται στο επίπεδο φυσικού μέσου της ασύρματης διεπαφής. Το φάσμα συχνοτήτων που διατίθεται σε αυτά τα κανάλια μπορεί να χρησιμοποιηθεί με δύο τρόπους. Στη λειτουργία FDD, οι ανερχόμενοι και οι κατερχόμενοι σύνδεσμοι έχουν το δικό τους κανάλι συχνοτήτων. Αντίθετα, στη λειτουργία TDD υπάρχει μόνο ένα κανάλι συχνοτήτων το οποίο χωρίζεται σε χρονοσχισμές. Στη συνέχεια οι χρονοσχισμές μοιράζονται στον ανερχόμενο και τον κατερχόμενο σύνδεσμο. Με βάση τον τρόπο διαχείρισης του φάσματος συχνοτήτων τα φυσικά κανάλια διαχωρίζονται σε FDD και TDD φυσικά κανάλια. Κάθε κατηγορία διαιρείται περαιτέρω σε άλλες δύο κατηγορίες ανάλογα με το αν το συγκεκριμένο φυσικό κανάλι χρησιμοποιείται στον ανερχόμενο ή στον κατερχόμενο σύνδεσμο [13]. Στην Εικόνα 29 παρουσιάζεται η αντιστοιχία όλων των καναλιών του UMTS που χρησιμοποιούνται στην downlink κατεύθυνση.



Εικόνα 29: Αντιστοίχιση καναλιών για την downlink κατεύθυνση

4. ΠΙΝΑΚΑΣ ΣΥΓΚΡΙΣΕΙΣ GSM-GPRS-UMTS

	GSM	***GPRS***	***UMTS***
ΓΕΝΙΑ ΚΙΝΗΤΩΝ ΔΙΚΤΥΩΝ	2G	2,5G	3G
ΕΜΠΟΡΙΚΗ ΧΡΗΣΗ	1991	1999	2002
ΕΥΡΟΣ ΖΩΝΗΣ	14,4Kbps	384Kbps	2Mbps
ΥΠΗΡΕΣΙΕΣ	SMS, MMS	SMS, MMS	SMS, MMS, video, e-mail, internet
ΠΡΩΤΟΚΟΛΛΑ	MAP, LAPD, MTP,	IP(v4, v6), Frame	MAC, RLC,

	SCCP	Relay, BSSGP	RNSAP, RANAP

ΚΕΦΑΛΑΙΟ 3ο

Σε αυτό το κεφάλαιο θα δώσουμε μια περιγραφή των επιθέσεων και των απειλών που εκμεταλλεύονται μια αδυναμία των συστημάτων. Οι επιθέσεις αυτές αφορούν τα δίκτυα GSM, GPRS και UMTS.

1. ΟΙ ΕΠΙΘΕΣΕΙΣ ΤΩΝ ΔΙΚΤΥΩΝ

1.1 Να κρυφακούσει (Eavesdropping): Ο εισβολέας είναι σε θέση να ακούσει τη σηματοδότηση που συνδέεται άλλους χρήστες ή τις συνδέσεις των δεδομένων τους.

1.2 Πλαστή προσωποποίηση ενός χρήστη (Impersonation of a user): Επιτρέπει στον εισβολέα να αλληλεπιδράσει με το δίκτυο ως ο πραγματικός χρήστης.

1.3 Πλαστή προσωποποίηση του δικτύου (Impersonation of the network): Επιτρέπει στον εισβολέα για να αλληλεπιδράσει με το χρήστη σαν να λαμβάνει τα σήματα από ένα γνήσιο δίκτυο.

1.4 Man-in-the-middle attack: Μια δυνατότητα του εισβολέα να τεθεί μεταξύ δύο επικοινωνούντων συμβαλλόμενων μερών, ενός χρήστη και του δικτύου, επιτρέποντας του διάφορες ενέργειες συμπεριλαμβανομένου να κρυφακούσει, να τροποποιήσει, να διαγραφεί, να ξανά παραγγείλει, επανάληψη και διάδοση υποκριτικών στοιχείων σηματοδότησης και χρηστών (spoof signaling).

1.5 Compromising authentication vectors in the network: Ο εισβολέας παίρνει τον έλεγχο ενός συμβιβασμένου πίνακα αυθεντικοποίησης (authentication vector) με το συμβιβασμό των κόμβων ή των συνδέσεων δικτύων.

2. Επίθεση I: DDos σε Τηλεφωνικά Κέντρα (Attack I: DDos attack to Call Centers).

Ο σκοπός της επίθεσης εδώ δεν είναι να εξαντληθούν οι ραδιοφωνικές πηγές αλλά να σταματήσουν τα κέντρα κλήσεων. Στο ίδιο πνεύμα κινούνται οι επιθέσεις DDos του διαδικτύου στους εξυπηρετητές δικτύων. Τέτοιες επιθέσεις δεν ήταν εφικτές στο παρελθόν με τα παραδοσιακά τηλέφωνα, διότι θα έπρεπε να γίνει κλήση δια χειρός στα τηλεφωνικά κέντρα, με κίνδυνο ο επιτιθέμενος να εντοπιστεί ή να διωχθεί ποινικά. Στην περίπτωση των «zombies» των Smartphone οι ιδιοκτήτες τους είναι θύματα παρά επιτιθέμενοι.

Παρόμοιες επιθέσεις DDos ξεκινούν ενάντια στο PSTN και στους κινητούς διακόπτες που είναι σχεδιασμένοι για προσπάθειες περιορισμένης ώρα κλήσεων αιχμής (BHCA). Αυτοί οι διακόπτες καταρρέουν όταν η αξία αυτών των κλήσεων αιχμής είναι εκτός του προγραμματισμένου φάσματος.

3. Επίθεση ΙΙ: Spamming (Attack II: Spamming).

Οι επιτιθέμενοι χειρίζονται τα «zombies» των Smartphone για να στέλνουν μηνύματα ανεπιθύμητης αλληλογραφίας μέσω SMS. Στην περίπτωση που το μοντέλο είναι επίπεδο, ένα διακινδυνευμένο ζητούμενο Smartphone στέλνει τέτοιου είδους αλληλογραφίας δωρεάν και ως εκ' τούτου ο ιδιοκτήτης του δεν παρατηρεί την «κακή» συμπεριφορά του. Το δωρεάν spamming δίνει κίνητρα να διακινδυνεύουν τα Smartphone.

4. Επίθεση ΙΙΙ: Κλοπή Ταυτότητας και Απάτη (Attack III: Identity Theft and Spoofing).

Οι τηλεφωνικοί αριθμοί στις κάρτες SIM είναι δύσκολο να υποστούν απάτη, διότι είναι η βάση αυθεντικότητας στα δίκτυα τηλεπικοινωνιών. Στο παρελθόν οι ερευνητές επιχείρησαν και κατάφεραν να ξεγελάσουν τις κάρτες SIM, αλλά η διαδικασία αυτή θέλει φυσική πρόσβαση σε κάρτες SIM και απαιτεί 150.000 ερωτήματα-απορίες για την κλεμμένη κάρτα, το οποίο διαρκεί μέχρι 8ώρες. Αυτό *δεν ισχύει* για τα Smartphone.

Η κλοπή ταυτότητας με τα Smartphone είναι μηδαμινή όταν το τηλέφωνο διακινδυνεύει ο επιτιθέμενος κατέχει ελεύθερα την ταυτότητα του ιδιοκτήτη για δραστηριότητες στο όνομα της. Με την απόκτηση ταυτότητας, ο επιτιθέμενος πετυχαίνει προσωπικότητα.

5. Επίθεση IV: Απομακρυσμένη Υποκλοπή Τηλεφωνημάτων (Attack IV: Remote Wiretapping).

Το zombie των Smartphone παθητικά καταγράφει συνομιλίες του ιδιοκτήτη του με άλλους και τις αναφέρει σε κατάσκοπους. Αυτές οι επιθέσεις είναι λίγο δύσκολο να εντοπιστούν γιατί η καταγραφή και η αναφορά είναι δυο ασύγχρονα βήματα και είναι δύσκολο για τον ιδιοκτήτη να παρατηρήσει την δραστηριότητα κατασκοπείας.

6. Παθητικού Κι Ενεργού Τύπου Επιθέσεις.

Η απουσία ελέγχων πρόσβασης στο (ράδιο)μέσο δίνει τη δυνατότητα στους επιτιθέμενους να παρακολουθούν (eavesdrop / snoop) οποιοδήποτε ασύρματο δίκτυο *παθητικά* (passively). Σκοπός τους για παράδειγμα μπορεί να είναι η καταγραφή των εκπεμπόμενων δεδομένων με στόχο την εκ των υστέρων αποκωδικοποίηση τους προκειμένου να αποκτήσουν πρόσβαση στις πληροφορίες που ανταλλάχθηκαν μεταξύ των νόμιμων χρηστών και του δικτύου. Χαρακτηριστικό είναι
το γεγονός πως ο επιτιθέμενος σε αυτή την περίπτωση δεν χρειάζεται τίποτα περισσότερο από μια απλή συσκευή πρόσβασης στο δίκτυο για παράδειγμα, μια ασύρματη κάρτα δικτύου, που μπορεί να προμηθευτεί από οποιοδήποτε κατάστημα εμπορίας υπολογιστών, δαπανώντας λίγες δεκάδες ευρώ. Εξάλλου μην ξεχνάμε πως όλες οι ασύρματες συσκευές έχουν τη δυνατότητα να εκπέμψουν και να λάβουν

δεδομένα στο ράδιο-μέσο. Με μικρές δε τροποποιήσεις στο υλικό ή στο λογισμικό τους ορισμένες από αυτές είναι ικανές να λαμβάνουν οτιδήποτε εκπέμπεται μέσα στην εμβέλεια τους.

Επιπλέον, τέτοιου είδους συν-ακροάσεις είναι πολύ δύσκολο αν όχι αδύνατο να ανιχνευτούν ή να εμποδιστούν για οποιοδήποτε ασύρματο δίκτυο. Παραδείγματος χάριν, ακόμα και στην περίπτωση των ασύρματων δικτύων που ακολουθούν το πρότυπο IEEE 802.11 ο επιτιθέμενος με τη βοήθεια κατάλληλης κεραίας και πιθανώς ενισχυτών μπορεί να βρίσκεται αρκετά μακρύτερα (ακόμα και 20 χιλιόμετρα) από το στόχο του π.χ. ένα σημείο ασύρματης πρόσβασης.

Πρέπει να σημειωθεί πως τα σημεία ασύρματης πρόσβασης σε ένα δίκτυο WLAN λειτουργούν όπως ακριβώς οι επαναλήπτες (repeater) και οι κατανεμητές καλωδίων (hub). Αυτό έχει ως αποτέλεσμα όλες οι συσκευές που είναι συνδεδεμένες στο δίκτυο να μπορούν υπό προϋποθέσεις (για παράδειγμα όταν ο προσαρμογέας δικτύου τους τεθεί σε promiscuous λειτουργία) να ακούσουν την κίνηση δεδομένων από τις υπόλοιπες συσκευές.

Σημειώνεται ότι συνήθως η παρακολούθηση του δικτύου δεν αποσκοπεί, τουλάχιστον αρχικά, στην υποκλοπή των δεδομένων που μεταδίδονται, αλλά στη συλλογή διάφορων πληροφοριών, οι οποίες θα επιτρέψουν στον επιτιθέμενο αργότερα ύστερα από σχετική ανάλυση (traffic analysis) να εξαπολύσει την πραγματική (ενεργή, active) επίθεση εναντίον των αδύνατων σημείων που πιθανώς ανακάλυψε. Μερικές από τις πληροφορίας που είναι χρήσιμες σε κάθε επιτιθέμενο ενώ είναι παθητικός ωτακουστής μπορεί να είναι το ποιος χρησιμοποιεί το δίκτυο, η τοπολογία του δικτύου, οι δυνατότητες και τα χαρακτηριστικά των συσκευών, IP και Medium Access Control (MAC) διευθύνσεις, η εμβέλειά του, κλπ. Πολλά επίσης πρωτόκολλα δικτύου είναι πιθανό να μεταδίδουν υπό ορισμένες συνθήκες ή και συνεχώς, απροστάτευτα σε μορφή αρχικού κειμένου (cleartext) ευαίσθητα δεδομένα των χρηστών, όπως είναι το όνομα πρόσβασης (login name) και το συνθηματικό τους (password).

Ακόμα και στην περίπτωση που όλα τα δεδομένα μεταδίδονται μεταξύ των σταθμών του δικτύου κρυπτογραφημένα υπάρχει η δυνατότητα καταγραφής τους με σκοπό για παράδειγμα την εξαντλητική αναζήτηση του κλειδιού κρυπτογράφησης. Ακόμα χειρότερα, πολλοί αλγόριθμοι κρυπτογράφησης παρουσιάζουν εν γένει αδυναμίες.

Εκτός από την παθητική παρακολούθηση των δεδομένων του ασύρματου δικτύου, πολλές φορές οι επιτιθέμενοι εφαρμόζουν τακτικές ενεργού ωτακουστή (active eavesdropping). Παραδείγματος χάριν, ο εισβολέας εκμεταλλεύεται το πρωτόκολλο Address Resolution Protocol (ARP), το οποίο χρησιμοποιείται από τους σταθμούς του δικτύου για να ανακαλύψουν την MAC διεύθυνση άλλων σταθμών, γνωρίζοντας την IP διεύθυνσή τους. Πιο συγκεκριμένα, ο επιτιθέμενος απαντάει στις ARP αιτήσεις διάφορων σταθμών στέλνοντας τη δική του MAC, με αποτέλεσμα τελικώς να λαμβάνει πληροφορίες, οι οποίες απευθύνονταν στους σταθμούς «θύματα». Η επίθεση αυτή αναφέρεται συχνά ως ARP poisoning. Ο επιτιθέμενος μπορεί επίσης να επαναπροωθεί τα μηνύματα που λαμβάνει στα θύματα του δρώντας ως ενδιάμεσος (man-in-the-middle, MITM).

Οι περισσότερες ενεργού τύπου μέθοδοι επιθέσεων στα ασύρματα δίκτυα προσομοιάζουν με αυτές που αντιμετωπίζονται στα ενσύρματα δίκτυα. Αυτές περιλαμβάνουν μεταξύ άλλων: πρόσβαση στο δίκτυο χωρίς εξουσιοδότηση (unauthorized access), πλαστογράφηση των δεδομένων, της σηματοδοσίας ή ακόμα και υπόδηση ή προσποίηση) της ταυτότητας (πλαστοπροσωπία) άλλων κόμβων του δικτύου (spoofing / masquerading / impersonating), επιθέσεις άρνησης πρόσβασης στο δίκτυο ή παροχής υπηρεσιών (Denial of Service, DoS), επιθέσεις πλημμύρας

(flooding), εισαγωγή κακόβουλου κώδικα (malware), κλπ. Είναι επίσης γεγονός πως με την εξέλιξη των ασύρματων δικτύων συνεχώς παρουσιάζονται και νέες παραλλαγές επιθέσεων. Μια από αυτές είναι η λεγόμενη *drive-by-spamming,* Σύμφωνα με αυτή, ο επιτιθέμενος που είναι εγκατεστημένος σε κινούμενο όχημα στέλνει εκατοντάδες χιλιάδες ενοχλητικά μηνύματα spam σε δίκτυα στα οποία έχει καταφέρει να αποκτήσει πρόσβαση.

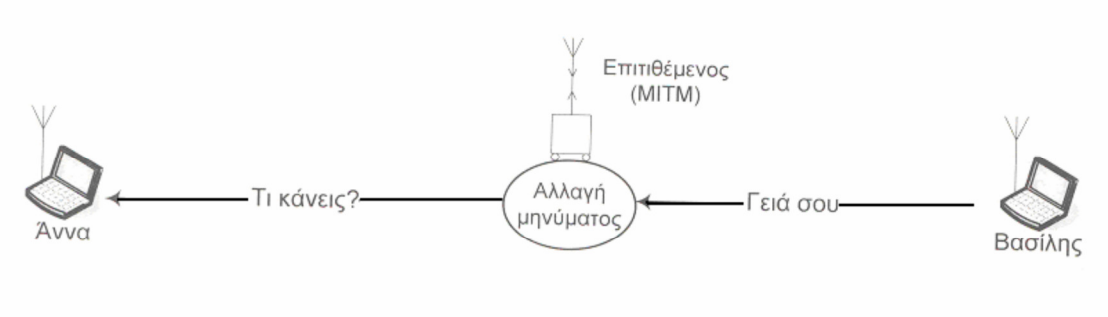
Μια κοινή επίθεση τύπου spoofing / masquerading / impersonating λαμβάνει χώρα όταν ο επιτιθέμενος είναι σε θέση να χρησιμοποιήσει ένα πλαστό στοιχείο δικτύου που εισάγεται κατάλληλα από αυτόν και ταυτόχρονα να το παρουσιάζει στους υπολοίπους σταθμούς ως απολύτως νόμιμο. Παραδείγματος χάριν, στο σύστημα Global System for Mobile Communication (GSM) όπου μόνο ο συνδρομητής αυθεντικοποιείται στο δίκτυο και όχι το αντίθετο (one-way authentication), ο επιτιθέμενος θα μπορούσε έχοντας στη διάθεση του κατάλληλο εξοπλισμό να παριστάνει την κεραία και το σταθμό βάσης που συνδέονται οι συνδρομητές.

7. Επιθέσεις Ενδιάμεσου Και Επιθέσεις Μεταβολής Πληροφοριών Ή Λαθροχειρίας.

Οι επιθέσεις τύπου Man-in-the-Middle (MITM) μπορούν να εκδηλωθούν με διαφόρους τρόπους σε ένα ασύρματο δίκτυο, έχοντας κύριο στόχο να υπονομεύσουν την ακεραιότητα ή και την εμπιστευτικότητα της συνόδου (session). Παραδείγματος χάριν, ο επιτιθέμενος μπορεί να υποδύεται ένα σταθμό βάσης σε ένα δίκτυο κινητών επικοινωνιών ή ένα σημείο πρόσβασης (AP) σε ένα τοπικό ασύρματο δίκτυο. Με αυτό τον τρόπο ενεργεί ως ενδιάμεσος μεταξύ του χρήστη και του νόμιμου δικτύου, υποκλέπτοντας και πιθανώς μεταβάλλοντας τις πληροφορίες που ανταλλάσσονται μεταξύ των δύο άκρων και κατόπιν προωθώντας τις κατάλληλα στο νόμιμο αποδέκτη τους, όπως παρουσιάζεται στην Εικόνα 30.

Υπάρχουν τουλάχιστον δύο τρόποι για την μεταβολή ενός μηνύματος. Ο πρώτος θεωρεί την επιτόπου (on-the-fly) αλλαγή του, ενώ ο δεύτερος εφαρμόζει τακτικές καταγραφής του μηνύματος, αλλαγής του και τέλος επαναπροώθησής του σε ύστερο χρόνο (store and forward). Η πρώτη μέθοδος αν και θεωρητικά εφαρμόσιμη είναι στην πράξη πολύ δύσκολο να υλοποιηθεί.

Η μεταβολή των πληροφοριών (data spoofing / modification / tampering) μπορεί να περιλαμβάνει εισαγωγή (injection) παραπλανητικού ή κακόβουλο περιεχομένου και εντολών, αλλά και την τροποποίηση των δεδομένων σηματοδοσίας (control messages) του δικτύου έτσι ώστε να προκαλείται κατάσταση DoS. Για παράδειγμα, ο επιτιθέμενος μπορεί εισάγοντας κατάλληλες εντολές να επιτύχει τη βίαιη αποσύνδεση (disassociation) των χρηστών από το δίκτυο. Επίσης, ο εισβολέας είναι πιθανό να πλημμυρίσει (flood) το δίκτυο με μηνύματα σύνδεσης (connect messages) στα ασύρματα σημεία πρόσβασης, αποκλείοντας με αυτό τον τρόπο τους εξουσιοδοτημένους χρήστες να συνδεθούν. Ο αποτελεσματικότερος τρόπος άμυνας για επιθέσεις αυτού του τύπου είναι η προστασία της ακεραιότητας (integrity) των δεδομένων που μεταδίδονται.



Εικόνα 30: Το αλλοιωμένο μήνυμα εμφανίζεται να έχει σταλεί από το Βασίλη

Στην πράξη μια επίθεση MITM σε ασύρματο περιβάλλον ακολουθεί τα επόμενα βήματα:

1. Ο επιτιθέμενος κρυφακούει για μηνύματα που προέρχονται από τη συσκευή του χρήστη και κατευθύνονται στη κεραία του δικτύου (για παράδειγμα σε κάποιο σημείο πρόσβασης).
2. Μόλις αντιληφθεί κάποιο μήνυμα το αποθηκεύει.
3. Αλλοιώνει το άθροισμα ελέγχου (checksum) του πλαισίου δεδομένων του μηνύματος, το οποίο χρησιμοποιείται από τον δέκτη προκειμένου να αντιληφθεί σφάλματα στα δεδομένα. Αυτό θα αναγκάσει το σημείο πρόσβασης να αγνοήσει το μήνυμα ως λανθασμένο (αλλοιωμένο). Η αλλοίωση μπορεί να γίνει εκπέμποντας μια ξαφνική ριπή θορύβου.
4. Παραλλάσσει ένα μήνυμα επιβεβαίωσης (Acknowledgement, ACK.) λήψης τοποθετώντας τη διεύθυνση του AP και ακολούθως το αποστέλλει στον σταθμό του χρήστη. Έτσι ο τελευταίος πιστεύει ότι το μήνυμα που έστειλε παρελήφθη κανονικά από το AP.
5. Επανασυνθέτει το αρχικό μήνυμα - υπολογίζοντας το άθροισμα ελέγχου – και το προωθεί στο AP. Το τελευταίο πιστεύει πως το μήνυμα προέρχεται από το σταθμό του χρήστη.
6. Αναμένει για μήνυμα επιβεβαίωσης από το AP προς το σταθμό του χρήστη και μόλις το αντιληφθεί εκπέμπει ριπή θορύβου έτσι ώστε το μήνυμα να αγνοηθεί από το δέκτη. Με αυτόν τον τρόπο ο δέκτης δεν θα λάβει δύο επιβεβαιώσεις για το ίδιο μήνυμα.

Οι πληροφορίες που μπορεί να μεταδίδονται στο πλαστό σημείο πρόσβασης είναι δυνατό να περιλαμβάνουν αιτήσεις αυθεντικοποίησης, μυστικά κλειδιά και τα λοιπά: αλλά και απλή κίνηση δεδομένων που καταγράφεται από τον επιτιθέμενο με σκοπό την αποκάλυψη π.χ. του WEP (Wired Equivalency Privacy) κλειδιού. Οι επιθέσεις αυτού του τύπου σχετίζονται με το επίπεδο συνδέσμου μεταφοράς δεδομένων (data link layer) του OSI μοντέλου. Επιπλέον, ο επιτιθέμενος μπορεί να διαθέτει ένα φορητό υπολογιστή με δύο προσαρμογείς δικτύου (Network Interfaces, NICs) έτσι ώστε ο ένας να χρησιμοποιείται μεταξύ του πλαστού AP και του υπολογιστή του, ενώ ο άλλος είναι επιφορτισμένος με το να προωθεί τα μηνύματα που λαμβάνονται από τον πρώτο στο νόμιμο AP (μεταβάλλοντας κατάλληλα τη MAC διεύθυνση πηγής). Εννοείται ότι η ίδια διαδικασία επαναλαμβάνεται και προς την αντίθετη κατεύθυνση. Σημειώστε επίσης ότι σε αυτή την περίπτωση ο επιτιθέμενος δεν χρειάζεται να γνωρίζει κανένα μυστικό κλειδί, γιατί οι διευθύνσεις MAC που χρειάζεται να μεταβάλλει δεν είναι κρυπτογραφημένες.

8. Επιθέσεις Παρεμβολών Ή Παρακώλυσης Επικοινωνιών.

Παρακώλυση ή παρεμπόδιση των επικοινωνιών μέσω παρεμβολών (jamming) έχουμε στην περίπτωση που το σήμα του πομπού, του δέκτη ή του σημείου ασύρματης πρόσβασης (π.χ. κεραία) σε μια ασύρματη ζεύξη παρεμποδίζεται ή αλλοιώνεται εξαιτίας κάποιων παρεμβολών ή θορύβων (noise) που προκαλούνται ηθελημένα ή αθέλητα. Το αποτέλεσμα της επίθεσης jamming είναι να καταστεί το κανάλι επικοινωνίας ακατάλληλο. Γι' αυτό το λόγο θεωρείται κατά βάση επίθεση που εντάσσεται στη γενική κατηγορία DoS καν εκδηλώνεται συνήθως στο φυσικό επίπεδο (PHY layer) του OSI μοντέλου. Το εύρος (range) της περιοχής παρεμβολών εξαρτάται άμεσα από την ισχύ του πομπού που έχει στη διάθεση του ο επιτιθέμενος. Όπως είναι φανερό οι επιθέσεις αυτού του τύπου είναι ιδιαίτερα προσιτές στα ασύρματα δίκτυα σε αντίθεση με το σύνηθες περιβάλλον ενός ενσύρματου δικτύου. Προκειμένου ο επιτιθέμενος να εξαπολύσει μια επίθεση παρεμβολής και παρακώλυσης επικοινωνιών σε ένα ασύρματο δίκτυο θα πρέπει πρώτα να αναλύσει το φάσμα συχνοτήτων που αυτό χρησιμοποιεί και κατόπιν να εκπέμψει με τη βοήθεια κάποιας σχετικής συσκευής ένα ισχυρό σήμα που συγκρούεται, παρεμποδίζει ή παρεμβαίνει (interfere) στις συχνότητες που το δίκτυο θύμα χρησιμοποιεί.

Η εισαγωγή θορύβου είναι ακόμα μια αποτελεσματική τεχνική. Ο εισαγόμενος στο δίκτυο θόρυβος πρέπει να είναι χαμηλής εντάσεως (amplitude) έτσι ώστε να προκαλέσει το φαινόμενο θανάτου από επανειλημμένη προσπάθεια (Death by Retry, DBR). Αυτό συμβαίνει όταν ο δέκτης ζητάει συνεχώς την επανάληψη αποστολής των μηνυμάτων, που σκοπίμως δεν εκπέμπονται όπως πρέπει, με αποτέλεσμα να εμπλακεί σε κατάσταση ατέρμονα βρόγχου. Από την άλλη πλευρά, ένας απλός τρόπος για την παρακώλυση των επικοινωνιών είναι η συνεχής πλημμύρα με άχρηστα δεδομένα των σημείων πρόσβασης έτσι ώστε αυτά να υπερφορτωθούν και να μην είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες. Παραδείγματος χάριν, μια επίθεση στο επίπεδο δικτύου (network layer) αυτή τη φορά, μπορεί να εκδηλωθεί πλημμυρίζοντας το δίκτυο με πλήθος αιτήσεων ping (ping flood atlack), αμέσως μόλις ο επιτιθέμενος αποκτήσει πρόσβαση σε ένα AP.

Επίσης, μια κοινή τεχνική για την εκδήλωση επίθεσης παρεμπόδισης επικοινωνιών που εκδηλώνεται όμως στο επίπεδο σύνδεσης δεδομένων (data link layer) του OSI μοντέλου είναι αυτή που εκμεταλλεύεται την ύπαρξη κεραιών πολλαπλής λήψης (diversity antennas) σε ένα AP (βλ. Εικόνα 31). Ας υποθέσουμε ότι ένα AP διαθέτει δύο κεραίες. Η πρώτη (1) καλύπτει την περιοχή αριστερά, ενώ η δεύτερη (2) την περιοχή δεξιά του AP. Ως αποτέλεσμα, οι χρήστες Α και Β ευρισκόμενοι αριστερά και δεξιά του AP θα συνδεθούν στις κεραίες 1 και 2 αντίστοιχα. Ακολούθως, ο Β αλλάζει τη MAC διεύθυνση του σε αυτή του Α και μέσω ενός ενισχυτή ενισχύει το σήμα του έτσι ώστε να είναι τουλάχιστον ίσο ή καλύτερα δυνατότερο οπό αυτό του Α. Τότε ο Α αποκλείεται από την επικοινωνία με το AP και για όσο διάστημα ο Β εξακολουθεί να εκπέμπει στη συγκεκριμένη MAC.

<u>Εικόνα 31</u>: Επίθεση τύπου DoS στο επίπεδο σύνδεσης δεδομένων

Επιπλέον, οι περισσότεροι χρήστες δεν έχουν τρόπο να αντιληφθούν ότι μια επίθεση παρακώλυσης είναι σε εξέλιξη. Γι' αυτούς η συγκεκριμένη επίθεση εμφανίζεται σαν απουσία δικτύου και υπηρεσιών, όπως στην περίπτωση των κινητών τηλεφώνων όταν δεν υπάρχει δίκτυο. Οι διαχειριστές του ασύρματου δικτύου είναι τις περισσότερες φορές πολύ δύσκολο να ανακαλύψουν την πηγή των παρεμβολών γιατί κάτι τέτοιο απαιτεί φυσική επιτήρηση του χώρου. Τέλος, η απόκτηση μιας συσκευής παρεμβολών από το Διαδίκτυο για παράδειγμα δεν απαιτεί ιδιαίτερο κόστος.

ΚΕΦΑΛΑΙΟ 4ο

1.ΕΠΙΘΕΣΕΙΣ ΣΕ ΛΟΓΙΣΜΙΚΑ

Σε αυτό το κεφάλαιο θα δώσουμε μια περιγραφή των επιθέσεων και των απειλών που εκμεταλλεύονται μια αδυναμία των λογισμικών. Οι επιθέσεις αυτές αφορούν τα συστήματα Android, Symbian, και συσκευές των κινητών που απειλούνται από διάφορους ιούς καθημερινά.

1.1 Τοπίο κινητή απειλή.

Στο τοπίο κινητή απειλή, οι δημιουργοί του κακόβουλου λογισμικού συνεχίζουν να επικεντρώνονται στην πλατφόρμα Android. Αυτό δεν πρέπει να έρχεται ως έκπληξη λαμβάνοντας υπόψη ότι το Android κατέχει το **79.3%** του συνολικού μεριδίου της αγοράς[18] στα κινητά τηλέφωνα και συσκευές ταμπλετών. Από τις **259** νέες οικογένειες απειλών και των νέων παραλλαγών από υπάρχουσες οικογένειες που ανακάλυψε το Q3 2013, οι **252** ήταν *Android* απειλές, ενώ οι άλλες **7** ήταν *Symbian* (εικόνα 32). Το κακόβουλο λογισμικό δεν έχει ακόμη καταγραφεί το 2013 στις άλλες πλατφόρμες (Blackberry, iOS, Windows Phone).

Η πλειοψηφία των απειλών αυτών εμπίπτουν από το «malicious program» ή κατηγορία Malware με trojans που αποτελούν το μεγαλύτερο ποσοστό των δειγμάτων (εικόνα 33). Οι υπόλοιποι θεωρούνται ως «potentially unwanted applications» ή pua, όπου το πρόγραμμα μπορεί να θεωρηθεί ανεπιθύμητη ή ενοχλητική εάν χρησιμοποιηθεί με ύποπτο τρόπο ή μπορεί ακούσια να εισάγει προστασία της ιδιωτικής ζωής ή κινδύνους για την ασφάλεια.

Με βάση τα στατιστικά στοιχεία που καταγράφονται από τα εσωτερικά συστήματα και δεδομένα τηλεμετρίας, μια άλλη τάση που έχουμε δει είναι η αυξανόμενη ανάπτυξη των απειλών υποκινούνται από το κέρδος (εικόνα 34), που συνήθως κάνει νομισματική κέρδος από την αποστολή SMS υψηλής χρέωσης από μολυσμένες συσκευές, χωρίς τη συγκατάθεση των χρηστών. Αυτή η αύξηση θα μπορούσε να αποδοθεί στην ανάπτυξη SMS που στέλνουν οι οικογένειες trojan όπως FakeInst, OpFake, PremiumSms και SmsSend, στα οποία οι προγραμματιστές δίνουν έξω νέες παραλλαγές κάθε τρίμηνο.

1.2 Developments this quarter = Εξελίξεις αυτό το τρίμηνο.

- **identifying pincer's creator = τον εντοπισμό του τανάλια δημιουργός**

Στις αρχές Απριλίου του τρέχοντος έτους, έχουμε αναφερθεί σχετικά με Pincer [19], ένα Android malware που συνδέεται με μια command-and-control ή C&C server (εικόνα 35) και serves ένα στοιχείο ενός συστήματος που χρησιμοποιείται για να νικήσει δύο παράγοντα ελέγχου ταυτότητας για διαδικτυακές τραπεζικές συναλλαγές. Τον Αύγουστο, ο ερευνητής ασφάλειας Brian Krebs φέρεται να εντόπισε συγγραφέας τού trojan προγραμματιστής σε μια ρωσική εφαρμογή, ο οποίος είχε προφανώς δημιουργήσει 'τανάλια' για αγνώστων στοιχείων πελάτη[20].

- **creating malware gets easier = τη δημιουργία malware γίνεται πιο εύκολο**

Το 1ο τρίμηνο του 2013, έχουμε αναφερθεί στην εργαλειοθήκη Perkele που χρησιμοποιούνται για την δημιουργία Android trojans για την παρακολούθηση και προώθηση μηνυμάτων SMS που περιέχει mTANs [21,22]. Τον Ιούλιο, υπήρξαν αναφορές για ένα νέο σύνολο εργαλείων (γνωστός και ως συνδετικά) που απλοποιεί τη διαδικασία της εισαγωγής κακόβουλο κώδικα σε νόμιμες εφαρμογές Android. Το συνδετικό υλικό, που ονομάζεται «Androrat APK binder» χρησιμοποιείται για την εισαγωγή ενός εργαλείου απομακρυσμένης πρόσβασης (RAT) γνωστή ως AndroRAT, σε ένα «φορέα» εγαρμογών, trojanizing[23].

Μόλις η εφαρμογή του φορέα είναι εγκατεστημένη σε μια συσκευή, το AndroRAT επιτρέπει στον επιτιθέμενο να ελέγχει από απόσταση και μεταξύ άλλων να παρακολουθεί και να πραγματοποιεί κλήσεις και μηνύματα, να ενεργοποιεί την κάμερα και το μικρόφωνο, και πρόσβαση σε αποθηκευμένα αρχεία.

- **"Masterkey" vulnerability = Ευπάθεια 'Masterkey'**

Τον Ιούλιο, οι ερευνητές ασφαλείας, δημοσίως ανακοίνωσαν την ανακάλυψη της κρυπτογραφικής υπογραφής για την παροχή Android εφαρμογών, αν αξιοποιηθούν θα επιτρέψουν σε έναν εισβολέα να τροποποιήσει ένα νόμιμο κώδικα εφαρμογών χωρίς να επηρεάζει την κρυπτογραφική υπογραφή[24] κρατώντας ουσιαστικά η παραποίηση από being εντοπισμός κατά τη διάρκεια της επαλήθευσης. Λίγο μετά την ανακοίνωση, οι ερευνητές ήταν σε θέση να βρούν δείγματα τροποποιημένων εφαρμογών που διανέμονται[25,26]. Λίγες μέρες αργότερα Κινέζοι ερευνητές ασφαλείας ανακοίνωσαν την ανακάλυψη ενός παρόμοιο θέμα ευπάθειας, αν και σε αυτή την περίπτωση το θέμα περιστράφηκε γύρω από το χειρισμό της διαδικασίας επαλήθευσης αναντιστοιχία μεταξύ υπογεγραμμένες και μη ακέραιους αριθμούς.

Η Google κοινοποίησε το θέμα «Masterkey» στις αρχές του έτους, και κατά τη στιγμή της ανακοίνωσης είχε καθορίσει το θέμα στο Android ανοικτού κώδικα[27]. Patches για την επακόλουθη ευπάθεια «συνδεδεμένος ακέραιος επαλήθευση» κυκλοφόρησαν επίσης λίγο μετά την ανακοίνωση. Οι χρήστες ωστόσο θα πρέπει να περιμένουν για μια ενημερωμένη έκδοση υλικό λογισμικού από τους κατασκευαστή της συσκευής για να λάβετε το patched κωδικό. Εν τω μεταξύ, βασικά προληπτικά μέτρα ασφαλείας είναι γενικά επαρκής για να αποφύγει την αντιμετωπίζουν.

1.3 Android and Symbian news.

Android:

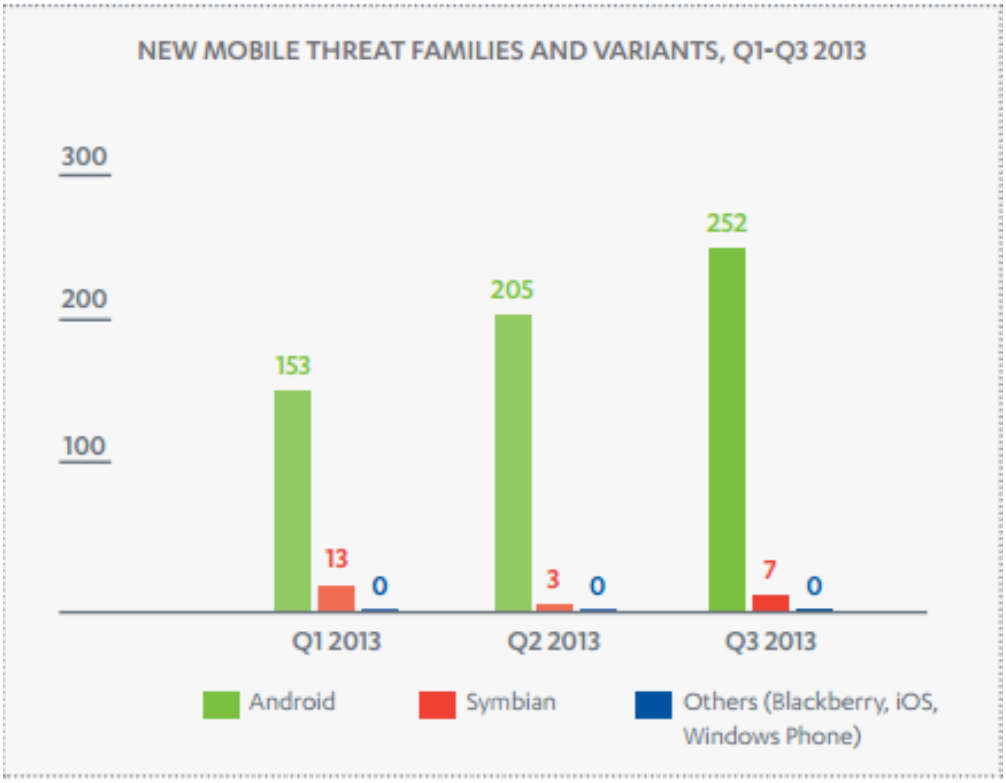
Όταν η Google παρουσίασε τα μέτρα ασφαλείας στο Google Play κατάστημα app βοήθησε να διατηρήσει κακόβουλές εφαρμογές από το κατάστημα, αλλά αυτό δεν είχε εξαλειφθεί εντελώς από τους κινδύνους. Για παράδειγμα, τα μέτρα είναι αναποτελεσματικά στον αποκλεισμό κακόβουλων διαφημίσεων σε εφαρμογές, όπως στην περίπτωση της Fakedefender, οι επιτιθέμενοι μπορούν απλώς να παρακάμψουν την ενσωματωμένη ασφάλεια του καταστήματος χρησιμοποιώντας διαφημιστικές ενότητες ως φορέας επίθεσης για να παρασύρουν τους χρήστες, σε εξωτερικούς χώρους όπου μπορούν να μολυνθούν.

Εκτός αυτού, ορισμένες απειλές είναι πέρα από το πεδίο της εφαρμογής των μέτρων ασφαλείας της Google Play όπως στην περίπτωση με το Masterkey. Επειδή μια τρύπα ασφαλείας στο λειτουργικό σύστημα Android, κακόβουλα προγράμματα θα μπορούσαν να εξακολουθούν να γλιστρήσουν στο κατάστημα ενώ κρύβονται μέσα σε νόμιμες εφαρμογές

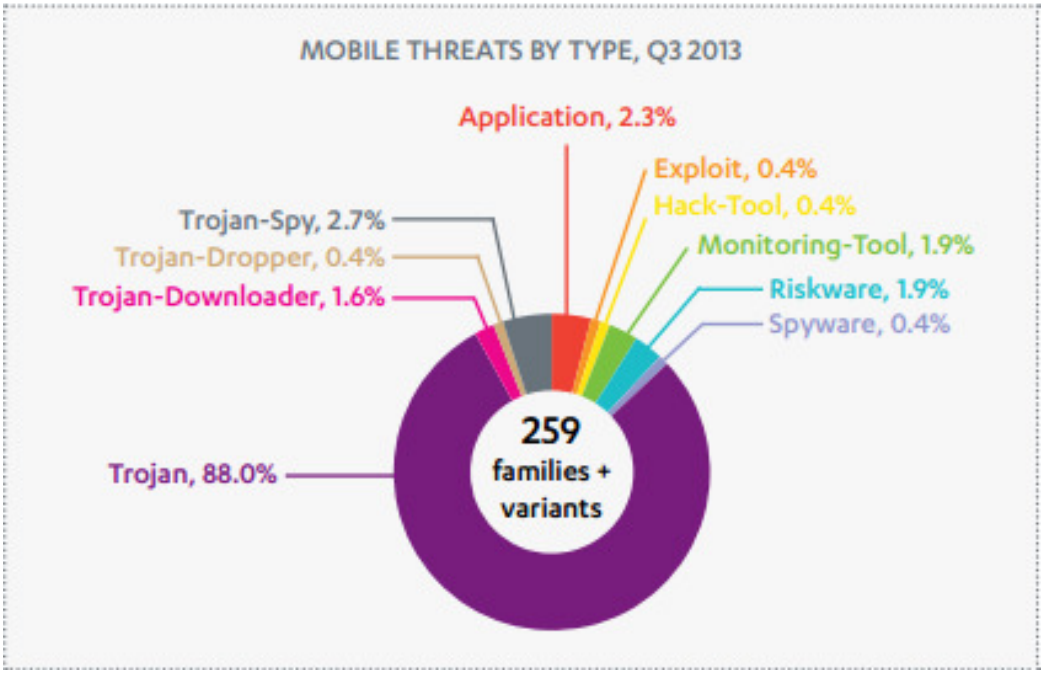
Symbian:

Ενώ το Android έχει ραγδαία αύξηση, το Symbian έχει την αντίθετη μοίρα. Το οικοσύστημά οδηγείται προς τα κάτω και την αυξανόμενη πίεση αφού ανακοίνωσε πρόσφατα η Nokia συσκευές και υπηρεσίες από τη Microsoft είναι χωρίς αμφιβολία επιτάχυνση της διαδικασίας. Στις 4 Οκτωβρίου 2013, η Nokia Developer News ανακοίνωσε ότι οι κατασκευαστές δεν θα είναι πλέον σε θέση να δημοσιεύσουν τα νέα περιεχόμενα ή ενημερώσεις από το κατάστημα της Nokia, που ξεκινούν την 1η Ιανουαρίου 2014 [28].

Το Symbian υπογεγραμμένο πρόγραμμα θα έρθει στο τέλος της ίδιας ημερομηνίας. Ως δεδομένο ότι όλα τα Symbian $3^{ης}$ έκδοσης και νεότερες εκδόσεις απαιτούν την υπογραφή εφαρμογών που κανείς δεν μπορεί να δημοσιεύσει νέες εκδόσεις των αρχείων εγκατάστασης μετά τον Ιανουαρίου 2014. Από αυτή τη στιγμή, δεν υπάρχει ρητή δημόσια δήλωση που σχετικά πρόκειται να συμβεί για να εκφράσει την υπογραφή ή από κάποιες τρίτες υπηρεσίες. Αν δεν είναι διαθέσιμες, πραγματικά σημαίνει το τέλος του Symbian.

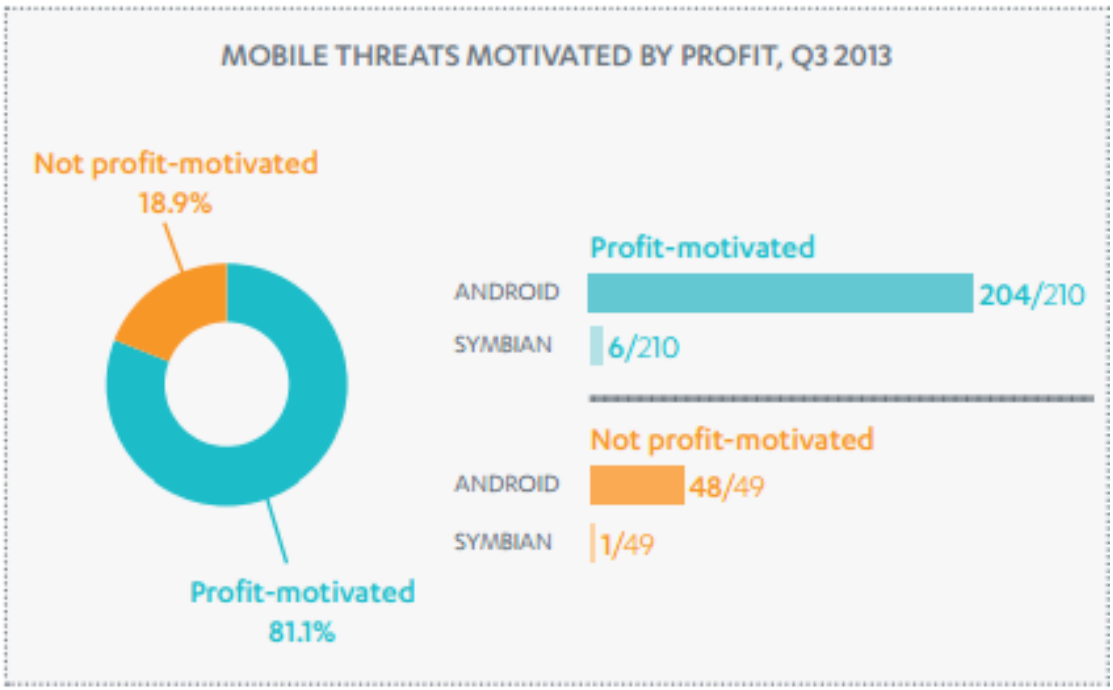


Εικόνα 32: Νέες οικογένειες και νέες παραλλαγές των υφιστάμενων οικογενειών που ανακάλυψε σε διαφορετικές πλατφόρμες από Q1-Q3 2013.

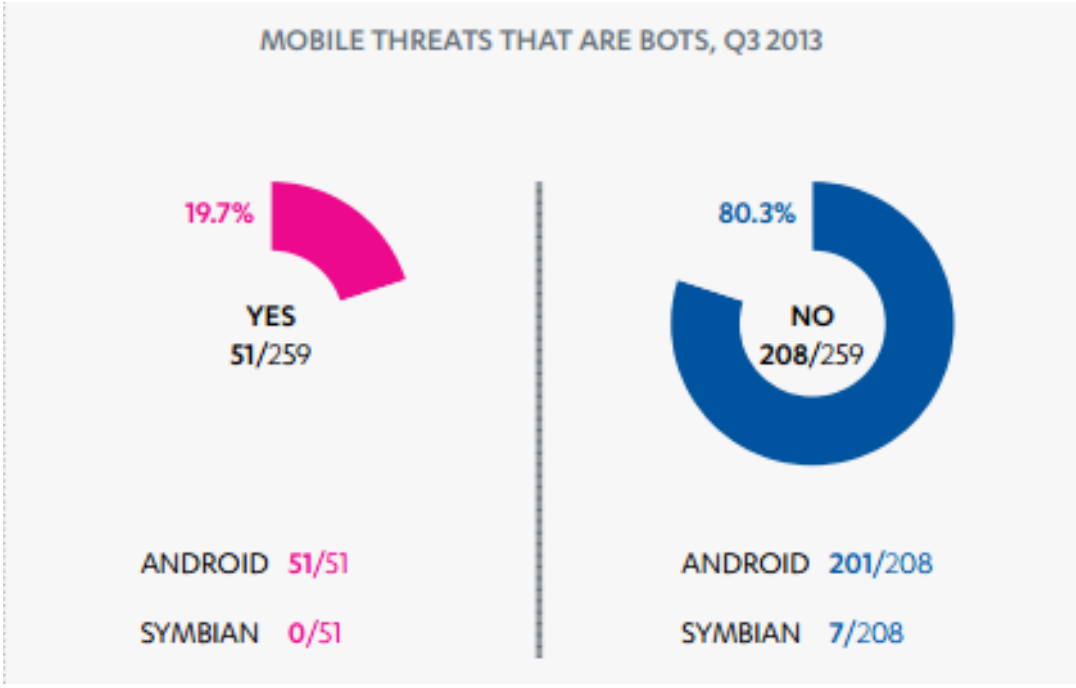


Εικόνα 33: Νέο κινητό απειλές οικογένειες και παραλλαγές που ανακάλυψε το Q3 2013, αναλύονται σε τύπους

Σημείωση: Νέων οικογενειών adware ή παραλλαγές ανακαλύφθηκαν το 3ο τρίμηνο του 2013. Νέων οικογενειών ή παραλλαγές του PUA (π.χ., Spyware, Riskware) καταγράφηκαν κατά το διάστημα αυτό.



Εικόνα 34 : Σύγκριση μεταξύ νέες απειλές που ανακάλυψε το Q3 2013 που υποκινούνται από το κέρδος σε σχέση με μη-κερδοσκοπικές κίνητρα αυτά.



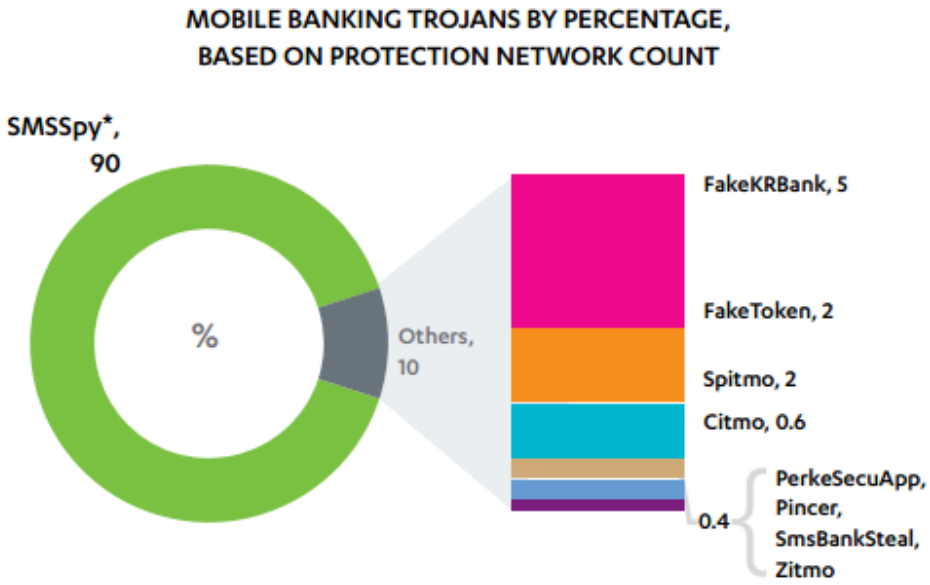
Εικόνα 35: Σύγκριση μεταξύ νέες απειλές που ανακάλυψε το Q3 2013 που συνδέεται με server C&C έναντι εκείνων που δεν είχαν.

2. Οι κυριότερες απειλές

Η κατάσταση των κινητών με κακόβουλο λογισμικό γίνεται όλο και πιο ενδιαφέρουσα ως προς τα κινητά τηλέφωνα και tablet γίνεται η προτιμώμενη συσκευή κατανάλωσης των μέσων ενημέρωσης για τους περισσότερους χρήστες. Η τρέχουσα τάση για κακόβουλο λογισμικό έχει να ακολουθήσει και να στοχεύσει το πιο ευρέως χρησιμοποιούμενο λειτουργικό σύστημα ή πλατφόρμα

Ένας κρίσιμος παράγοντας που οδηγεί στην ανάπτυξη των κινητών με κακόβουλο λογισμικό έχει αυξανόμενη χρήση των κινητών συσκευών ως έλεγχο ασφάλειας και συνήθως ως μια μορφή δύο παραγόντων ελέγχου ταυτότητας, για τις πιστοποιήσεις χρήσεις online. Η πιο κοινή εκδήλωση είναι το mtan (mobile transaction authentication number) που χρησιμοποιείται κατά τη διάρκεια της online τραπεζικές συναλλαγές από ορισμένες τράπεζες ως ένα επιπλέον επίπεδο ασφάλειας. Συγγραφείς του malware είναι σε θέση να παρακάμψουν αυτό το επιπλέον επίπεδο προστασίας, δημιουργώντας ένα κινητό πρόγραμμα ή εφαρμογή που διακόπτει τα SMS που χρησιμοποιούνται για την επικύρωση αυτών των συναλλαγών, κατά συνέπεια η γέννηση του mobile banking trojans.

Οι πιο κοινές από αυτές εξακολουθούν να είναι μόνο ένα συστατικό ενός πιο πολύπλοκου συστήματος, καθώς πρέπει να λειτουργούν παράλληλα με διαφορετικές τράπεζες κακόβουλου λογισμικού που κάνει την πραγματική νομισματική κλοπή. Είναι ενδιαφέρον, αν και η mobile banking trojans εξακολουθεί να αποτελεί ένα μικρό κομμάτι της συνολικής αρίθμησης της συλλογής δειγμάτων του malware βλέπουμε μια αυξανόμενη τάση του αριθμού των banking trojans.



Γενικότερα, μια άλλη τάση για να τονίσει την τριμηνιαία εξέλιξη της Android malware από την άποψη της πολυπλοκότητα και του περιβάλλοντος. Ένα παράδειγμα είναι η εξέλιξη από μια απλή αποστολή SMS app που έχει αναπτύξει το δικό της 'οικοσύστημα' εξελίσσεται σε ένα SDK που υποστηρίζει έναν ασφαλέστερο αριθμό εγγραφής, κάπως σαν τον διαφημιστικές ενότητες που σχετίζονται με διαφημιστικά δίκτυα. Ένα SDK, μπορεί να ενσωματωθεί εύκολα σε μια εφαρμογή. Η αλλαγή σημαίνει ότι δύο πράγματα μπορούν να συμβούν, μπορεί να χρησιμοποιηθεί αποκλειστικά για τις «παραδοσιακές» εγγραφή ρουτίνα ασφάλιστρο-SMS, ή το SDK άθελά διαφοροποιείται νόμιμα προγραμματιστές απληροφόρητα του αντίκτυπου της

συμπεριφοράς του. Ακολουθώντας τα βήματα των προηγουμένως αναφερθεί malware Badnews αυτό το τρίμηνο αυτό παρατηρήθηκε σε sxJolly.a. Αν και δεν είναι νέα, obad.a έδειξε επίσης περισσότερη ανάπτυξη αυτό το τρίμηνο σε σχέση με το οικοσύστημα.

Συμπεριφορά κλασικού Trojan-clicker παρατηρείται συχνότερα σε PC malware, επανεμφανίστηκε σε uten.a, αν και τις ίδιες αρχές είχαν ήδη δει στο Adrd.A[29] το 2011. Ερευνώντας περαιτέρω σε ειδικά malware, η δημοσιοποίηση «Masterkey» αυτό το τέταρτο έδειξε τις μεγαλύτερες δυνατότητες για χρήση σε πραγματικό malware, και αρκετά ακολουθήθηκε γρήγορα από την ανακάλυψη των in-the-wild malware εκμεταλλεύεται αυτό το κενό. Στο μέτωπο της Symbian, η μόνη νέα απειλή ήταν Kleaq.a, αν και ακόμα και τότε δεν είναι ασυνήθιστο για Symbian malware. Και τέλος, όσον αφορά την κατασκοπεία-malware, η πιο αξιοσημείωτη ανάπτυξη ήταν tramp.a της Google Cloud Messaging (GCM).

2.1 Τα κυριότερα σημεία απειλών

Καταμέτρηση γνωστών μοναδικών δειγμάτων (Count of Known Unique Samples) : ο αριθμός των μοναδικών δειγμάτων για μια συγκεκριμένη παραλλαγή της οικογένειας βρίσκονται σε συλλογές αρχείων μας. Ο αριθμός αυτός χρησιμοποιείται για να παρέχει μια ουσιαστική ιδέα του πόσο μεγάλο μπορεί να είναι ένα δεδομένο κακόβουλο λογισμικό (malware).

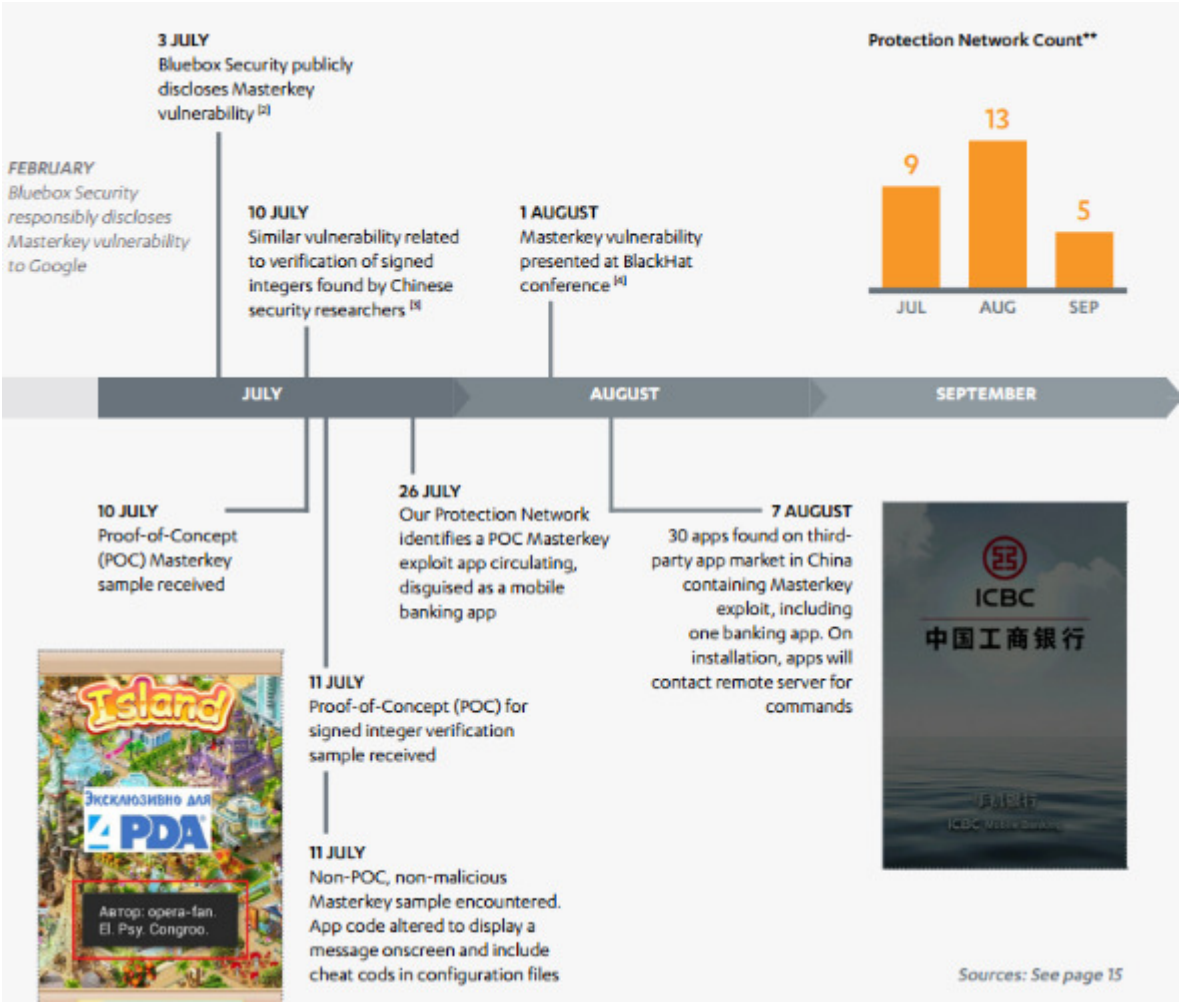
Καταμέτρηση του δικτύου προστασίας (Protection Network Count): ο αριθμός των φορών που μια εγκατάσταση πελάτη της F-Secure που αναφέρθηκε κλείδωμα μιας προσπάθειας εγκατάστασης κακόβουλου προγράμματος στην προστατευόμενη συσκευή του cloud-based συστήματος τηλεμετρίας, κατά τη διάρκεια του Q3 2013.

2.1.1 Exploit: Android/MasterKey.A

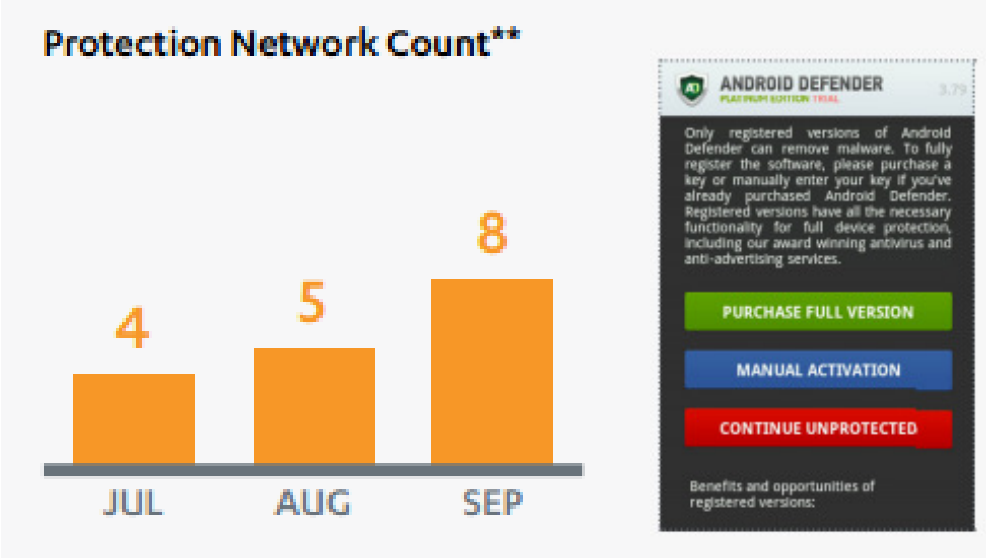
Καταμέτρηση των γνωστών μοναδικών δειγμάτων : 101

Διανομή : Καταλαμβάνετε σε τρίτες αγορές app στοχευμένη σε Κινέζους χρήστες

Περίληψη : Αυτό το κακόβουλο λογισμικό εκμεταλλεύεται την Masterkey σε Android, το οποίο επιτρέπει στους επιτιθέμενους να κάνετε αλλαγές σε μια εφαρμογή του κώδικα χωρίς να επηρεάζεται η κρυπτογραφική υπογραφή που χρησιμοποιείται για να ελέγξει τη νομιμότητα ενός app.



2.1.2 Trojan: Android/Fakedefender.A

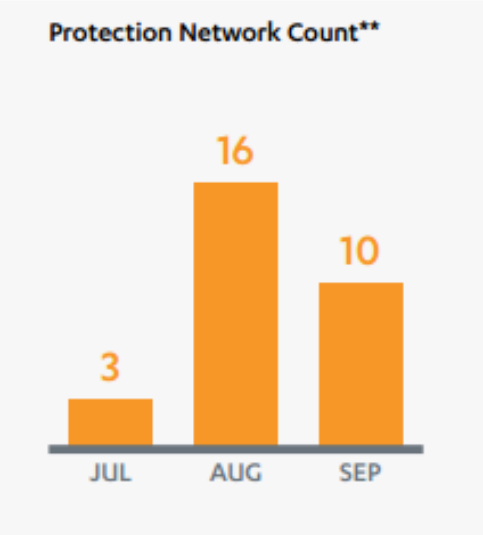


Καταμέτρηση των γνωστών μοναδικών δειγμάτων : 34

Διανομή : Διαφημίζετε σε διαφημίσεις τρίτων που εμφανίζεται σε κινητές συσκευές

Περίληψη: Παρόμοια με anti-spyware προγράμματα βρίσκονται σε υπολογιστές, FakeDefender είναι ένα πρόγραμμα anti-spyware για την κινητή συσκευή. Το πρόγραμμα δεν παρέχει την σάρωση ή την απομάκρυνση λειτουργιών του κακόβουλου λογισμικού όπως ισχυρίστηκε

2.1.3 Trojan: Android/Obad.A

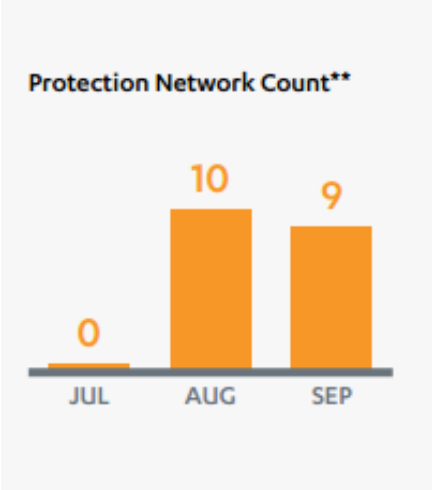


Καταμέτρηση των γνωστών μοναδικών δειγμάτων : 14

Διανομή: Παρατηρήθηκαν παραλλαγές που διαφημίζεται σε μια κακόβουλη ιστοσελίδα κατά την περιήγηση σε μια συσκευή Android, και είναι πιθανό να φθάσει στη συσκευή του πελάτη μέσω μιας mobile drive by download.

Περίληψη: Μόλις εγκατασταθεί στη συσκευή Obad, αποκτούν δικαιώματα διαχειριστή και χρησιμοποιεί μια εκμετάλλευση να σπάσει μέσω του Android λειτουργικού συστήματος ασφαλείας στρώμα. Το Obad συλλέγει και στέλνει τα ακόλουθα στοιχεία σχετικά με τη συσκευή με έναν απομακρυσμένο C&C server: η διεύθυνση έλεγχου πρόσβασης (MAC) και IMEI, το όνομα του χειριστή, την ώρα και πρόσβαση στη βάση. Ο C&C server είναι επίσης σε θέση να εκδίδουν εντολές για την εγκατεστημένη εφαρμογή, καθώς και να στείλετε SMS, να κάνει τη συσκευή ενεργεί ως ένα πληρεξούσιο, την διεύθυνση URL στο browser του κινητού, τη λήψη και εγκατάσταση πρόσθετων στοιχείων, να πάρει τη λίστα επαφών, καθώς και περισσότερες λεπτομέρειες σχετικά με μια εγκαταστημένη εφαρμογή και να στείλει ένα αρχείο μέσω Bluetooth.

2.1.4 Trojan: Android/Sxjolly.A

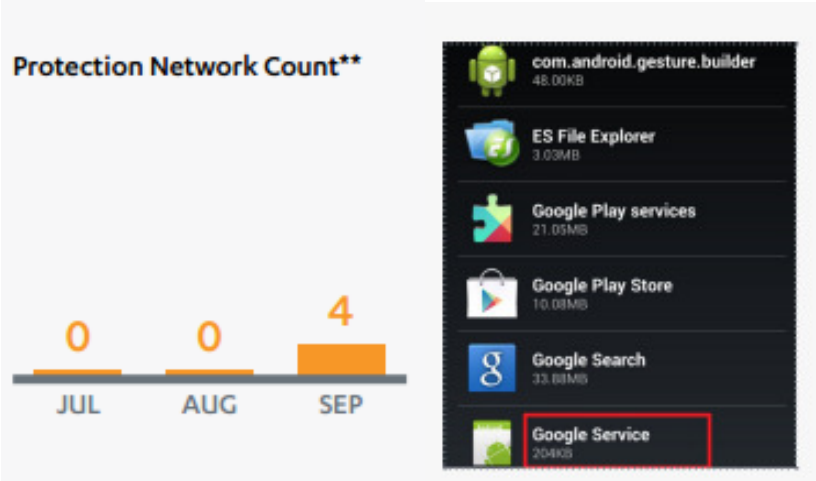


Καταμέτρηση των γνωστών μοναδικών δειγμάτων :19

Διανομή: Καταλαμβάνετε σε τρίτες αγορές app στοχευμένη σε Ρωσικούς χρήστες.

Περίληψη: Μια Bot ικανή να λαμβάνει εντολές για την αποστολή SMS ή εγγραφή της συσκευή σε μια ασφαλέστερη υπηρεσία SMS, και την αλλαγή ή ενημέρωση του C&C server.

2.1.5 Trojan: Android/Tramp.A



Καταμέτρηση των γνωστών μοναδικών δειγμάτων: 31

Διανομή: Άγνωστο

Περίληψη: Σε γενικές γραμμές αυτό το κακόβουλο λογισμικό παρακολουθεί τα SMS του χρήστη και κλέβει τα ακόλουθα στοιχεία από το τηλέφωνο του χρήστη: τους αριθμούς τηλεφώνου μεταφορέα και SMS. Μια ενδιαφέρουσα πτυχή αυτού του κακόβουλου λογισμικού είναι ότι μπορεί να δεχθεί τις ακόλουθες εντολές μέσω Google Cloud Messaging (GCM):

- send message (αποστολή μηνύματος)
- block call (block κλήση)

- get current location (πάρει την τρέχουσα θεσή)
- observe (παρατηρούν)
- contact (επικοινωνία)

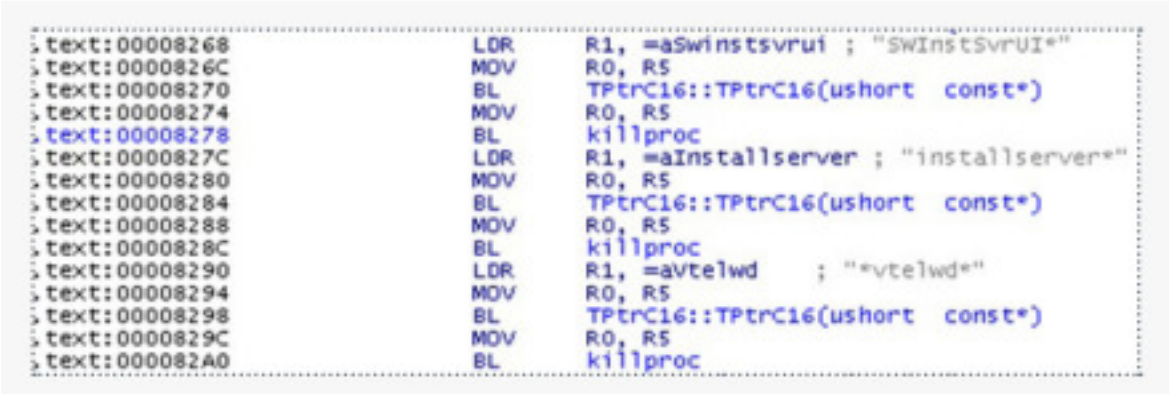
2.1.6 Trojan: Android/uten.A

Καταμέτρηση των γνωστών μοναδικών δειγμάτων: 192

Διανομή: Αυτό το κακόβουλο λογισμικό είναι ένα Trojan app βασίζεται σε ένα παιχνίδι που είναι διαθέσιμο από την Google Play και πιστεύεται ότι θα εξαπλωθεί σε διάφορες αγορές app τρίτων.

Περίληψη: Αυτό το κακόβουλο λογισμικό μεταμφιέζεται ως 'Umeng' SDK βιβλιοθήκη, μια κινητή πλατφόρμα αναλυτική χρησιμοποιείται από προγραμματιστές. Η αρχική αίτηση που ήταν trojanized δημιουργήσε αυτό που φαίνεται να είναι μια νόμιμη εφαρμογή τυχαίων παιχνιδιών που διατίθεται στην επίσημη Google Play Market.

2.1.7 Trojan: Symbos/Kleaq.A

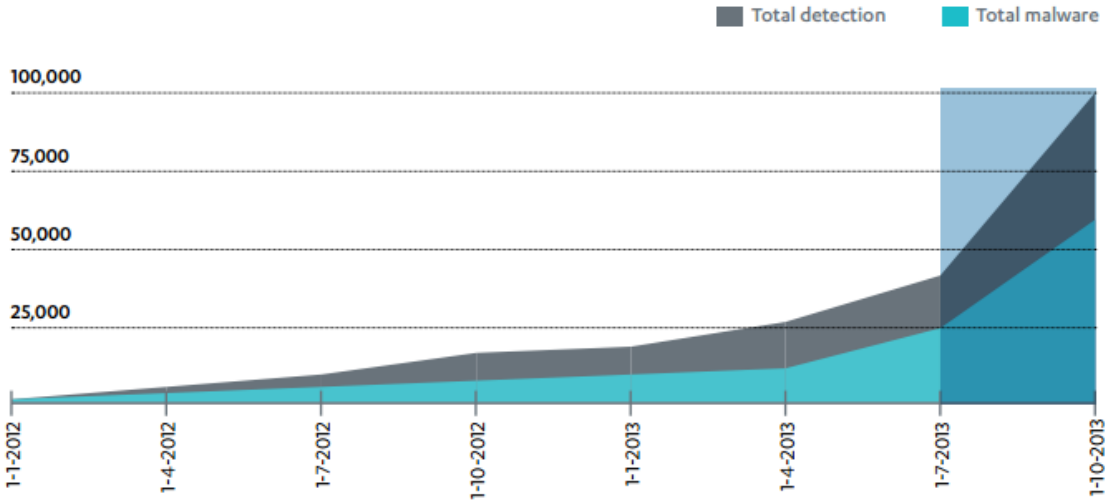


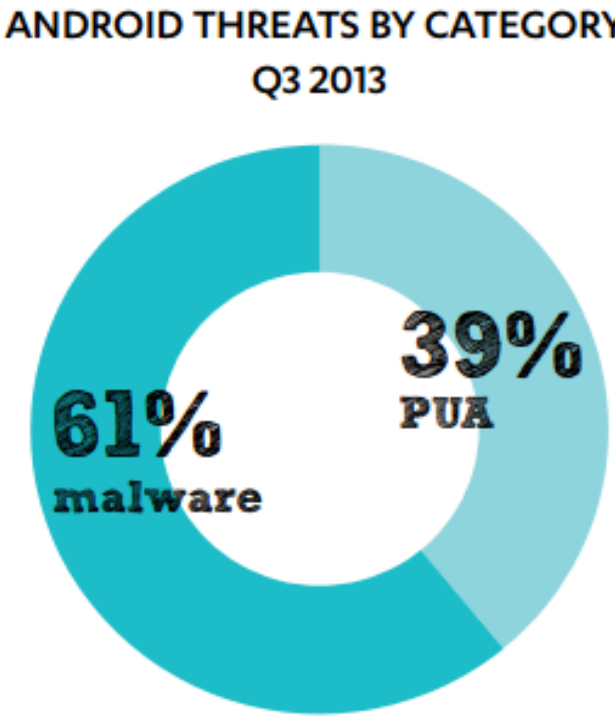
Διανομή: Άγνωστο

Περίληψη: Το πακέτο εγκατάστασης αυτού του κακόβουλου λογισμικού περιέχει δύο εκτελέσιμα αρχεία, ένα το οποίο είναι υπεύθυνο για τη λήψη και την εγκατάσταση, ενώ το άλλο εκτελέσιμο 'σκοτώνει' κάθε απόπειρα κατάργησης της εγκατάστασης των σχετικών διαδικασιών. Τυπικά, ο κατάλογος περιλαμβάνει κάποια antivirus και ενδείξεις κατάστασης σύνδεσης με το δικτύο.

2.2 Android Malware Statistics

Total Malware Count Against Total Detection Count For Android Threats 2012-2013





TOP-15 ANDROID MALWARE RECEIVED AND IDENTIFIED IN Q3 2013

DETECTION	COUNT
Trojan:Android/FakeInst	90,252
Trojan:Android/GinMaster	15,853
Trojan:Android/OpFake	11,319
Suspicious:Android/Malware	7,245
Trojan:Android/SmsSend	7,062
Trojan:Android/Vdloader	4,111
Trojan:Android/Boxer	2,590
Trojan-Downloader:Android/Boqx	2,210
Trojan:Android/SmsSpy	2,099
Suspicious:Android/GinMaster	1,857
Trojan:Android/Downloader	1,734
Trojan:Android/Mseg	1,709
Trojan:Android/Vidro	789
Trojan:Android/Temai	657
Trojan:Android/FakeNotify	558

3. Η κατηγοριοποίηση των απειλών για τα κινητά

Τα ασφαλής εργαλεία για τις απειλές των κινητών χωρίζονται σε δύο κατηγορίες ανάλογα με τις δυνατότητες τους για την καταστροφή της συσκευής (Malware) και των δεδομένων του χρήστη (pua). Η παρακάτω λίστα παρέχει μια σύντομη περίληψη των κριτηρίων ταξινομούν κινητό απειλές:

3.1 Malware:

Το λογισμικό χαρακτηρίζεται ως κακόβουλο όταν βάσει των προθέσεων του προγραμματιστή διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα *«ξενιστή»* και σε αυτό που *δεν χρειάζεται «ξενιστή»* και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα. Με άλλα λόγια, είναι το σύνολο των κακόβουλων προγραμμάτων που μπορεί να κολλήσει μια κινητή συσκευή και όχι μόνο. Παράδειγμα malware είναι τα εξής κερκόπορτα (backdoor), Trojan, (που μας εκθέτει), και worm (που πολλαπλασιάζεται μέσω δικτύου)

3.1.1 Κερκόπορτα (Backdoor):

Ένα κακόβουλο λογισμικό που μπορεί να έχουμε κολλήσει στον υπολογιστή μας το οποίο κάνει κάτι πολύ συγκεκριμένο: τρέχει συνέχεια χωρίς να το καταλαβαίνουμε και κρατάει ανοιχτή μία "πόρτα" ώστε ο δημιουργός του να μπορεί να μπει στον υπολογιστή μας. Το backdoor έχει σαν στόχο να αφήνει πάντα ανοιχτή μια πόρτα

στον υπολογιστή μας, ώστε ο δημιουργός του να μπορεί να έχει πρόσβαση στα αρχεία μας και σε διάφορα άλλα, να υποκλέπτει δεδομένα, κλπ.

3.1.2 Trojan:

Είναι ένα κακόβουλο πρόγραμμα που μπορεί να κολλήσουμε από το internet. Πρόκειται για ένα πρόγραμμα το οποίο ανοίγει και κρατάει ανοιχτή μία "πίσω πόρτα" ώστε να μπορεί ο δημιουργός του να εισέρχεται έτσι στον υπολογιστή μας και να κλέψουν σημαντικά αρχεία ή να αποκτήσουν τον έλεγχο του συστήματος. Τις περισσότερες φορές το συγκεκριμένο λογισμικό δεν έχει στόχο τη μόλυνση του υπολογιστή, δηλαδή δεν αναπαράγεται, και για αυτό τα προγράμματα αυτά δεν χαρακτηρίζονται και επίσημα ως ιοί. Το trojan συνήθως δεν γίνεται αντιληπτό παρά μόνο αν εγκαταστήσουμε ένα antivirus το οποίο θα το εντοπίσει, θα το σβήσει και δεν θα μας αφήσει να κολλήσουμε άλλο τέτοιο ξανά. Η πλήρης ονομασία του είναι trojan horse και αλλιώς ονομάζεται backdoor.

3.1.3 Σκουλήκι (worm):

Είναι κακόβουλο λογισμικό το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Η ικανότητά του να πολλαπλασιάζεται αυτόματα στο σύστημα στο οποίο βρίσκεται του δίνει τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Τέλος, ένα άλλο αρνητικό χαρακτηριστικό είναι ότι επιβαρύνουν το δίκτυο, φορτώνοντάς το με άχρηστη δραστηριότητα.

3.2 PUA:

Είναι μια ευρεία κατηγορία του λογισμικού, του οποίου ο σκοπός δεν είναι τόσο κατηγορηματικά κακόβουλο και με άλλους τύπους malware, όπως ιούς ή δούρειους ίππους. Ωστόσο μπορεί να εγκαταστήσει επιπλέον ανεπιθύμητο λογισμικό, όπως να αλλάζει τη συμπεριφορά της ψηφιακής συσκευής, να εκτελέσει τις δραστηριότητες που δεν έχουν εγκριθεί ή αναμένεται από τον χρήστη. Οι κατηγορίες περιλαμβάνουν: adware, spyware, trackware,

3.2.1 Spyware:

Κακόβουλα προγράμματα τα οποία επιτελούν ένα συγκεκριμένο έργο. Κολλάνε στον υπολογιστή μας και "αθόρυβα", χωρίς να το καταλάβουμε, μας από-κλέπτουν πληροφορίες και τις στέλνουν σε κάποιον συγκεκριμένο προορισμό. Για παράδειγμα αν κάνουμε είσοδο στο ebanking (ηλεκτρονική τράπεζα) και έχουμε κολλήσει ένα spyware υπάρχει περίπτωση να υποκλέψει το username και το

password μας και να τα στείλει στον δημιουργό του. Έτσι αυτός θα έχει τα στοιχεία μας και θα μπορεί να εισέλθει κανονικά στο ebanking και να μας πάρει τα λεφτά.

3.2.2 Trackware:

Trackware μπορεί να θεωρηθεί ως spyware. Το πρόγραμμα αυτό παρακολουθεί κρυφά τη συμπεριφορά των χρηστών ή συγκεντρώνει εμπιστευτικές πληροφορίες, στη συνέχεια διαβιβάζει τις πληροφορίες σε τρίτους. Οι πληροφορίες που συγκεντρώνονται μπορεί μερικές φορές να περιλαμβάνει προσωπικά αναγνωρίσιμα στοιχεία, λαμβανομένων υπόψη και ονόματα σύνδεσης, κωδικούς πρόσβασης ή άλλα ευαίσθητα δεδομένα.

3.2.3 Adware:

Είναι ένα λογισμικό που μπορεί να κολλήσει ο υπολογιστής μας και είναι υπεύθυνο να προβάλλει ανεπιθύμητες για εμάς διαφημίσεις ανά τακτά χρονικά διαστήματα. Το adware στην ουσία δεν κάνει κακό στον υπολογιστή μας αλλά μας πετάει ενοχλητικές διαφημίσεις κάθε τόσο και λιγάκι με στόχο να επωφεληθεί οικονομικά από τις διαφημίσεις αυτές ο δημιουργός του εις βάρος μας.

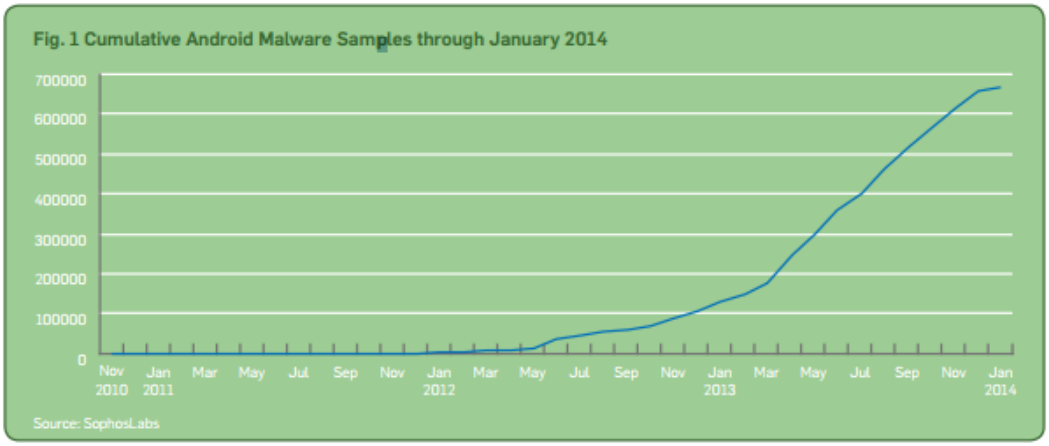
4. 10 χρόνια κακόβουλου λογισμικού για τις κινητές συσκευές

Έχουν περάσει 10 χρόνια από το πρώτο mobile malware κατά το 2004, αλλά μόνο μέσα στα τελευταία χρόνια έχει γίνει πραγματική απειλή για τους τελικούς χρήστες. Πράγματι, η ταχεία ανάπτυξη των smartphone και tablet της χρήσης κατά τη διάρκεια των δύο τελευταίων ετών οδήγησε στην αναπόφευκτη αύξηση των συσκευών από κυβερνοχώρου. Η εκθετική ανάπτυξη των συσκευών Android και η έντονη σε μεγάλο βαθμό ανεξέλεγκτη Android εφαρμογές παράγει μία απότομη αύξηση κακόβουλου λογισμικού με στόχο την πλατφόρμα. Μέχρι σήμερα SophosLabs έχει δει πάνω από 650.000 ατομικά κομμάτια του κακόβουλου λογισμικού για το Android και ένα μικρό μέρος του αριθμού των τεμαχίων των malware εκεί έξω για το παραδοσιακό

PC, αλλά η αυξανόμενη απειλή. Κακόβουλο λογισμικό Android έχει αυξηθεί γρήγορα σε σύντομο χρονικό διάστημα, και φαίνεται ότι θα κρατήσει διευρύνεται συνεχώς με τη χρήση των συσκευών κινητής τηλεφωνίας.

4.1 Μεγάλη αύξηση των Smartphones και Tablet

Με συνδρομές κινητής τηλεφωνίας παγκοσμίως συνολικού ύψους περίπου 7 δισ. ευρώ μέχρι το τέλος του 2013, είναι σαφές ότι τα κινητά αντικαθιστούν γρήγορα το προσωπικού υπολογιστή στο σπίτι και στο εργασιακό χώρο. Τώρα βασίζονται σε smartphones και tablets γιατι τα πάντα στη ζωή μας σχετίζονται με το Internet, από περιήγηση στο διαδίκτυο σε συναλλαγές ηλεκτρονικού εμπορίου και στις ηλεκτρονικές τράπεζες.



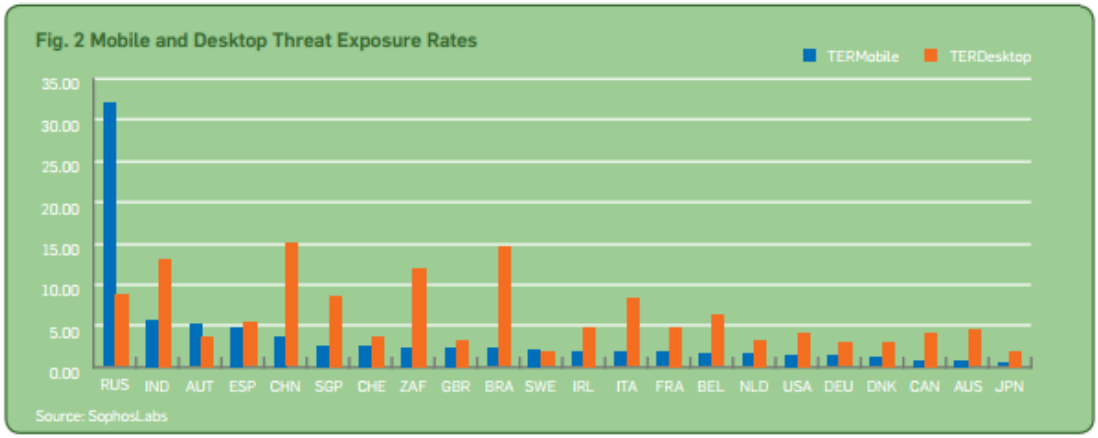
Η γραφική παράσταση στην εικόνα 2 δείχνει mobile και desktop απειλές έκθεσης (TER), μετράει το ποσοστό των υπολογιστών και των φορητών συσκευών που γνώρισε μια επίθεση κακόβουλου λογισμικού, είτε επιτυχημένες ή αποτυχημένες, σε διάρκεια περιόδου τριών μηνών. Η γραφική παράσταση δείχνει μόνο malware απόπειρες για συσκευές που προστατεύονται από Sophos, αλλά είναι αποκαλυπτικό ότι ενώ η πλειοψηφία των malware εξακολουθεί να βρίσκεται στην επιφάνεια εργασίας, σε ορισμένες χώρες, τα mobile malware εξελίσσονται σε μεγάλο φαινόμενο.

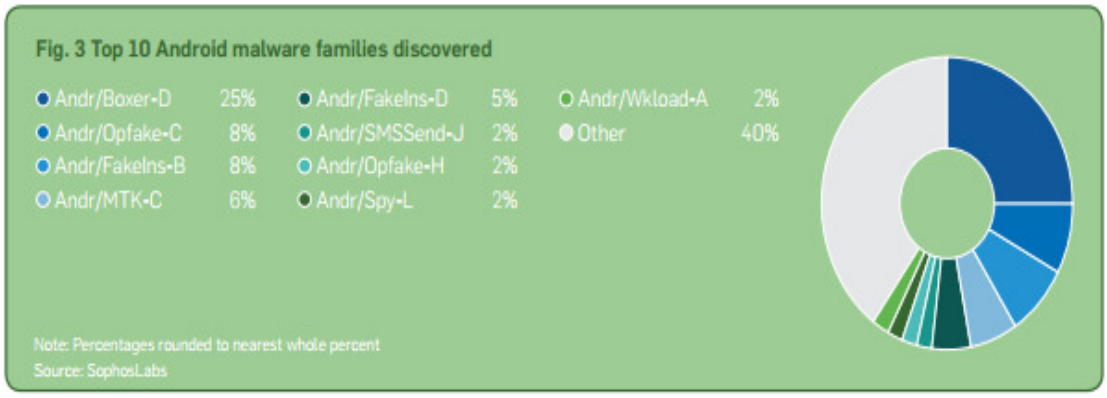
4.2 Android vs. iOS

Οι συγγραφείς των κινητών κακόβουλου λογισμικού γνωρίζουν τον καλύτερο τρόπος για να "μολύνουν" πολλές συσκευές όπως είναι δυνατόν να επιτεθούν κεντρικές εφαρμογές αγορών. Επομένως, σήμερα ο πιθανότερος τρόπος ότι το malware θα βρει τον τρόπο πάνω σε μια κινητή συσκευή είναι μέσα από τη λήψη ενός κακόβουλου app που δεν έχει ελεγχθεί επαρκώς.

Αναπόφευκτα, η πλατφόρμα Android της Google έχει γίνει ένα πολύ μεγαλύτερο στόχο για τους συγγραφείς κινητών malware από την Apple iOS σε αντίθεση με την Apple δεν εκτελεί πολιτική όσον αφορά τις εφαρμογές. Είναι επίσης σημαντικό ότι το Android έχει ένα μεγάλο ποσοστό της αγοράς

κινητής τηλεφωνίας έως 79% το 2013, σύμφωνα με την στρατηγική Analytics.1





4.3 Google και Android

Όπως η Apple, η Google παρέχει μια κεντρική αγορά για κινητές εφαρμογές, που ονομάζεται Google Play. Ωστόσο, αντισταθμίζεται από την ικανότητα του Android να εγκαταστήσουν εφαρμογές από τρίτες πηγές. Μερικές είναι πολύ γνωστές και αξιόπιστες όπως το Amazon. Άλλοι δεν είναι, και προέρχονται από κακόβουλο λογισμικό hotspots στη Ρωσία και στη Κίνα. Οι προγραμματιστές αναδομούν και ανακατασκευάζουν δημοφιλείς εφαρμογές όπως το Angry Birds, και δημοσιεύει κακόβουλες εκδόσεις και τα διαθέτουν δωρεάν.

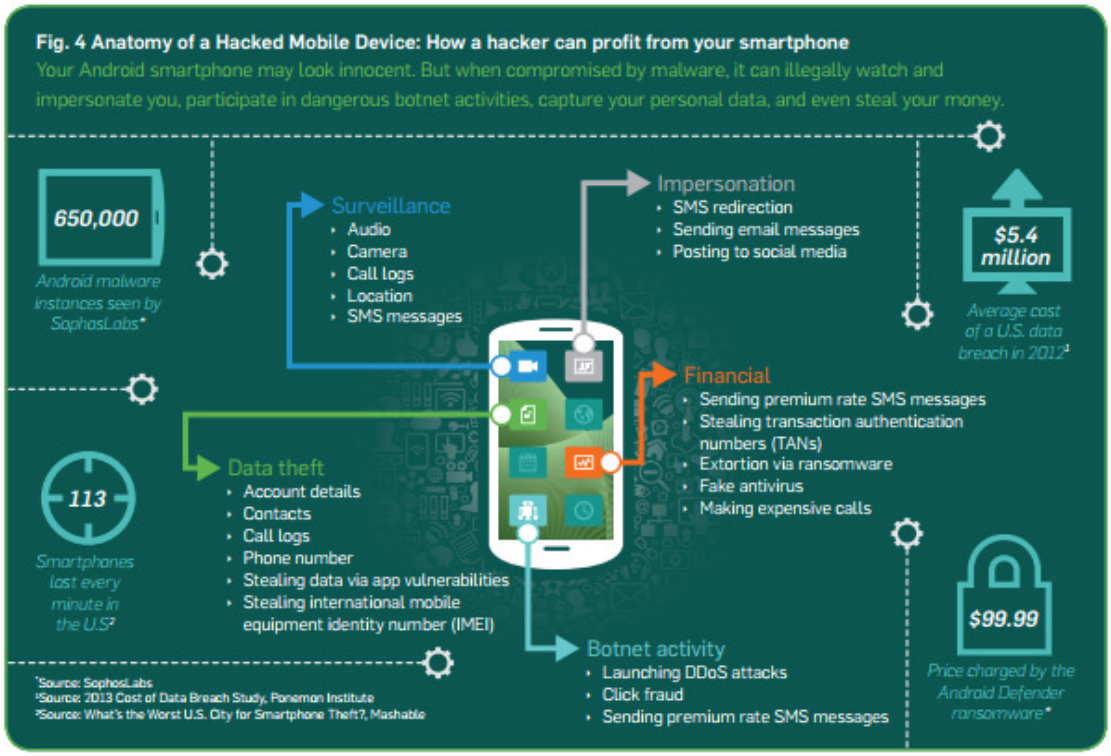
5. Τύποι επίθεσης: πώς ένας χάκερ κερδίζει

Στην εικόνα 4 δείχνει τους διαφορετικούς τρόπους που μπορούν να επωφεληθούν οι hacker από μια κινητή συσκευή που είναι σε κίνδυνο. Ορισμένες από αυτές, όπως ransomware, fake AV, botnet activity και data theft(κλοπή δεδομένων), έχουν μεταναστεύσει από το παραδοσιακό PC.

Παρόλα αυτά λόγω της φύσης των κινητών συσκευών, είναι επίσης ανοικτή σε νέους τύπους επίθεση. Για παράδειγμα, οι εγκληματίες του κυβερνοχώρου είδαν την αξία νωρίς από τη χρήση κακόβουλων εφαρμογών για κινητά που

στέλνουν μηνύματα με αριθμούς κινητών τηλεφώνων με μη εξουσιοδοτημένες χρεώσεις. Και για αυτούς που έχουν πολύ φορητότητα προφανώς είναι ευάλωτο να έχουν απώλεια δεδομένων που έχει ως αποτέλεσμα η συσκευή δεν κρυπτογραφείται ή δεν ασφαλίζεται κατάλληλα.

Σήμερα, η εξέλιξη της κινητή τραπεζική θέτει ένα δυνητικά ακόμη μεγαλύτερο κίνδυνο για τους χρήστες. Επειδή οι ισχυρές φορητές συσκευές σήμερα καθιστούν εύκολη για τους χρήστες να διεξάγουν χρηματοοικονομικές συναλλαγές σε κίνηση, αυτοί είναι ήδη ενεργά στο στόχαστρο από το malware με σκοπό να κλέψουν τα στοιχεία και τα χρήματα. Ως εκ τούτου, προστατεύοντας το smartphone σας από κακόβουλο λογισμικό και keyloggers πρέπει να είναι μια βασική αρχή της ασφαλή κινητή τραπεζική.



5.1 Ανδροειδές Malware – μετάλλαξη και όλο και πιο έξυπνος

Τον Αύγουστο του 2010, δεδομένου ότι εντοπίσαμε τα πρώτα android κακόβουλα λογισμικά έχουν καταγράφει πάνω από 300 οικογένειες κακόβουλου λογισμικού και πάνω από 650.000 μεμονωμένα κομμάτια του android malware. Το οικοσύστημα android malware ακολουθεί πολλές απόψεις από τα μονοπάτια για πρώτη φορά που ιδρύθηκε πριν από χρόνια από το κακόβουλο λογισμικό Windows.

Πρόσφατα, είδαμε μεγάλη καινοτομία πώς το android malware προσπαθεί να αποφύγει την αντιμετώπιση των μεθόδων ανίχνευσης. Ginmaster είναι ένα τέτοιο παράδειγμα. Ανακαλύφθηκε για πρώτη φορά στην Κίνα τον Αύγουστο του 2011, αυτό το πρόγραμμα Trojan αυτών εγχέεται από πολλές νόμιμες εφαρμογές που διανέμονται επίσης μέσω αγορές από τρίτους.

Το 2012, Ginmaster άρχισε να παραποιεί ονόματα τάξη, κρυπτογράφηση URLs και οδηγίες C&C, και την κίνηση προς τις τεχνικές πολύμορφισμού που έχουν γίνει κοινός τόπος σε Windows malware. Το 2013, οι προγραμματιστές του Ginmaster εφαρμόζεται πολύ πιο περίπλοκη και λεπτή συσκότιση και κρυπτογράφηση, καθιστώντας αυτό το κακόβουλο λογισμικό πιο δύσκολο να ανιχνεύσει ή να αναστρέψει τη λειτουργία του. Εν τω μεταξύ, κάθε τρίμηνο από τις αρχές του 2012, έχουμε δει μια σταθερή αύξηση ανιχνεύσεις των Ginmaster, που φθάνει σχεδόν 7500 δείγματα από τα τέλη του Ιανουαρίου 2014.

5.2 Νέα Android botnets

Στα τέλη του 2013, μεγάλη κλίμακα botnet αναφέρεται για τον έλεγχο συσκευών Android και το ίδιο τρόπο botnets ελέγχονται στα PC. το Botnet αυτό, ανιχνεύει ως ΑΝΔΡ/GGSmart-A, μέχρι στιγμής φαίνεται περιορισμένη στην Κίνα. Χρησιμοποιεί κεντρικής διοίκησης και ελέγχου να αναθέσει όλες τις κινητές συσκευές που έχουν μολυνθεί από τα ίδια για παράδειγμα, για να στείλετε SMS πριμοδότησης που θα χρεωθεί στον κάτοχο της συσκευής. Σε αντίθεση με την τυπική Android επίθεση μπορεί να αλλάξει και ελέγχει τους premium αριθμούς περιεχόμενο και ακόμη και θυγατρικά καθεστώτα SMS σε ένα ολόκληρο μεγάλο δίκτυο.

5.3 Ransomware έρχεται στο Android

Ransomware έχει μια μακρά ιστορία οι πρώτες εκδόσεις εντοπίστηκαν πριν από 25 χρόνια. Για όσους δεν είναι εξοικειωμένοι με αυτό, το ransomware κάνει τα αρχεία ή τις συσκευές απρόσιτες, και στη συνέχεια απαιτεί μια πληρωμή να απελευθερωθούν. Τον Ιούνιο του 2013, ο ερευνητής Sophos Rowland Yu ανακάλυψε ένα επίθεση ransomware ενάντια σε συσκευές Android. Αυτό το ψεύτικο antivirus/ransomware app ονομάζεται Android Defender, και απαιτεί μια πληρωμή $99.99 για να επαναφέρετε την πρόσβαση στη συσκευή σας Android.

Κατά την εκκίνηση, Android Defender χρησιμοποιεί μια ποικίλα κοινωνικής μηχανικής στρατηγικής και μια ασυνήθιστη επαγγελματική εμφάνιση και αίσθηση να ζητήσει επανειλημμένα δικαιώματα διαχειριστή συσκευής. Αν δοθούν προνόμια, μπορεί να περιορίσει την πρόσβαση σε όλες τις άλλες εφαρμογές, καθιστώντας αδύνατο να κάνει τις κλήσεις, να αλλάξει τις ρυθμίσεις, να καταστρέψει εργασίες, να απεγκαταστήσει εφαρμογές, ή ακόμη και να εκτελέσετε μια επαναφορά εργοστασιακών ρυθμίσεων. Παρουσιάζει ένα προειδοποιητικό μήνυμα σχετικά με την μόλυνση που είναι ορατά στην οθόνη, ανεξάρτητα από το τι κάνει ένας χρήστης. Ακόμη μπορεί να απενεργοποιήσει τα κουμπιά πίσω και κεντρικό μενού και να ξεκινήσει την επανεκκίνηση για να αντισταθεί αφαίρεση. Για το μόνο πράγμα που δεν κάνει είναι να κρυπτογραφεί το περιεχόμενο ή τα προσωπικά στοιχεία.

5.4 Κλοπή τραπεζικό λογαριασμό, που παραδίδονται μέσω smartphone

Το Σεπτέμβριο του 2013, εντοπίσαμε μια νέα μορφή τραπεζικού malware που συνδυάζει παραδοσιακές επιθέσεις browser εναντίον των Windows, σχεδιασμένο με κοινωνική μηχανική έτσι ώστε να παραβιάσει συσκευές Android και να ολοκληρώσει την κλοπή μέσω smartphone. Τα εργαστήρια του Sophos εντόπισαν κακόβουλο λογισμικό Andr/Spy-ABN και παρά το γεγονός ότι αντιμετωπίζουμε σχετικά χαμηλά επίπεδα αυτό έχει ήδη στοχεύσει γαλλικά, ολλανδικά και ινδικά χρηματοπιστωτικά ιδρύματα.

Όπως και ο προκάτοχός του Zeus, Andr/Spy-ABN αρχίζει από την πλευρά των Windows, εγχέοντας κώδικα σε Internet Explorer να υποκλέψει πληροφορίες χρήστη πριν αυτό έχει κρυπτογραφηθεί και προωθηθεί στα χρηματοπιστωτικά ιδρύματα. Επίσης, αιχμαλωτίζει προσωπικά πιστοποιητικά προγράμματος περιήγησης και cookies. Μόλις γίνει έλεγχος ταυτότητας, στους χρήστες ενημερώνονται ότι η τράπεζα τους απαιτεί τώρα τη χρήση μιας νέας εφαρμογής smartphone ως μέτρο καταπολέμησης της απάτης (πόσο ειρωνικό).

Από τον χρήστη ζητείται ο αριθμό τηλεφώνου και το μοντέλο του/της, και αποστέλλεται ένα SMS, συνδεδεμένο με μια λήψη της εφαρμογής του κακόβουλου. Εάν αυτό δεν είναι αρκετά κακό, αυτόν τον κώδικα εμποδίζει ακόμη και τους χρήστες από την πρόσβαση σε λογαριασμούς τους έως ότου το κακόβουλο λογισμικό smartphone έχει εγκατασταθεί και παρέχει έναν κωδικό ενεργοποίησης.

Μερικοί χρηματοπιστωτικοί οργανισμοί απαιτούν πλέον προστασία από κακόβουλο λογισμικό για να τεθεί σε εφαρμογή πριν ο πελάτης εγγραφτεί για ηλεκτρονικές τραπεζικές συναλλαγές. Η κρυπτογράφηση όλων των δεδομένων σε μια κινητή συσκευή, και την εξασφάλιση της συσκευής με κωδικό PIN δημιουργεί ένας επιπρόσθετος περιορισμός σε περίπτωση που η συσκευή χαθεί ή κλαπεί.

Η δεύτερη πρόκληση είναι γύρω από τον έλεγχο ταυτότητας του χρήστη για της κινητές τραπεζικές εφαρμογής, ο αδύναμος κρίκος σε διαφορετικά αυτό που ήταν μια πολύ βολική υπηρεσία. Τους κωδικούς πρόσβασης χρηστών είναι εύκολο να μαντέψει κανείς εάν γνωρίζει τους κωδικούς πρόσβασης και τα κλειδιά του βασιλείου.

Οι περισσότεροι χρηματοπιστωτικοί οργανισμοί σήμερα απαιτούν έλεγχο ταυτότητας πολλών παραγόντων μέσω διακριτικά ασφάλειας και άλλους μηχανισμούς. Για twofactor authentication (2FA), δεν είναι μόνο αυτό που ξέρετε (δηλαδή, από έναν κωδικό πρόσβασης), αλλά επίσης κατέχετε (δηλαδή, είναι διακριτικό) που είναι απαραίτητο για την πρόσβαση ευαίσθητων πληροφοριών, προσθέτοντας ένα σημαντικό στρώμα της ασφάλειας. Αυτό μεταφέρει κάποιο κόστος σε ευκολία, αλλά αξίζει την προσπάθεια.

5.5 PUAs: Οι συγγραφείς επιδιώκουν να έχουν κέρδος αυξάνοντας τις εφαρμογές.

Παρόλα αυτά μέσω του malware, πιθανώς ανεπιθύμητες εφαρμογές (PUA) αναπτύσσονται στο Android, όπως μπορείτε να δείτε από την αθροιστική γραφική παράσταση που παρουσιάζει την ανάπτυξη PUA (εικόνα 5). Οι PUAs

είναι εφαρμογές Android που δεν χαρακτηριστούν αυστηρά ως κακόβουλα λογισμικά, αλλά παρόλα αυτά μπορεί να παρουσιάσει πολλούς κινδύνους,

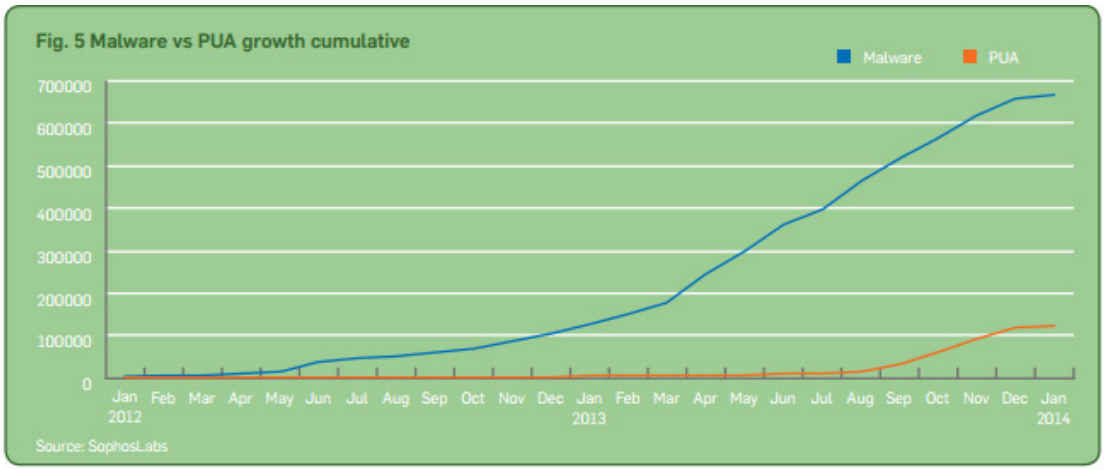
Πολλοί χρήστες μπορεί απρόσεκτα να εγκαταστήσουν εφαρμογές που συνδέονται με επιθετικής διαφήμισης δίκτυα, που μπορεί να ανιχνεύσει τις συσκευές και τις θέσεις τους, και μπορεί ακόμη να αιχμαλωτίσει στοιχεία επικοινωνίας. Αυτές οι εφαρμογές δημιουργούν εύκολα χρήματα παρέχοντας πορνογραφικές ή άλλες ακατάλληλες διαφημίσεις στους χρήστες.

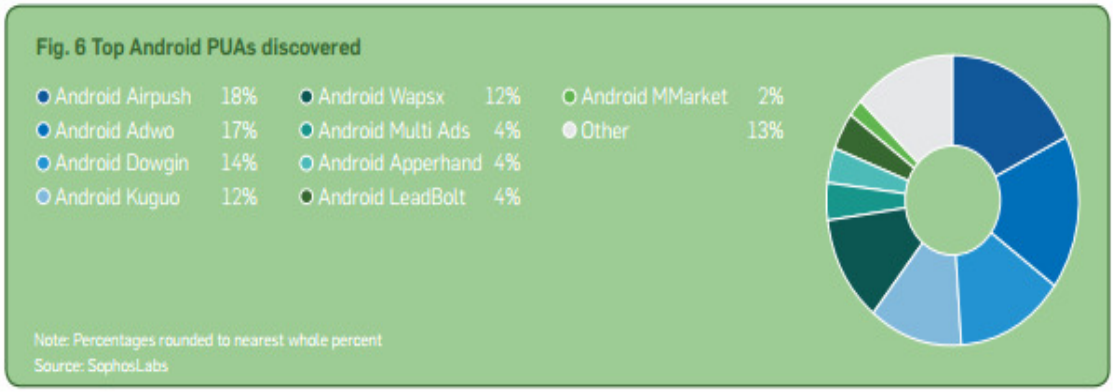
5.6 Εξασφάλιση Android

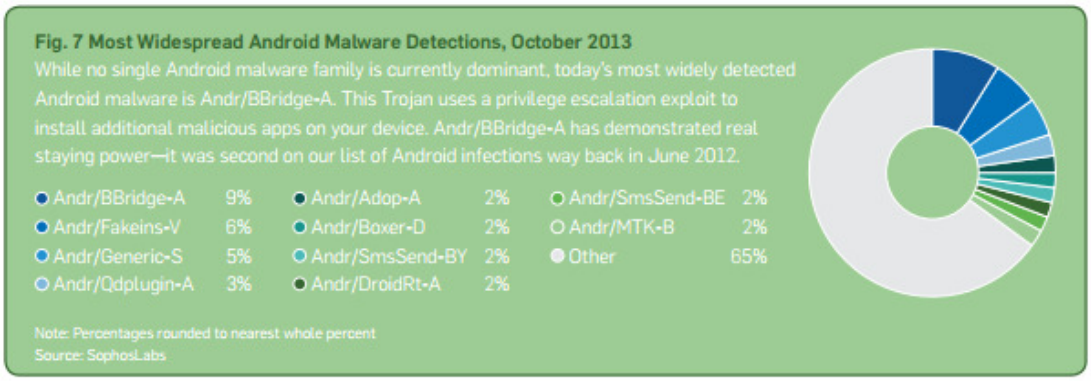
Η Google πρόσφατα έχει κάνει κάποια σημαντικά βήματα για την περαιτέρω εξασφάλιση της πλατφόρμας. Καταρχάς, το Android 4.3 εξάλειψε το χαρακτηριστικό γνώρισμα όπου τα πακέτα εφαρμογών (APK) λαμβάνονταν αυτόματα από τρίτες πηγές όταν το προεπιλεγμένο πρόγραμμα περιήγησης της εφαρμογής Android.

Δεύτερον, η Google έχει περιορίσει τον τρόπο ανάπτυξη της κυρίως όσον αφορά τα PUAs, που δεν είναι αλάνθαστα malware, αλλά συμπεριφέρονται με τρόπο που είναι πολύ πιο παρεμβατικός από ό, τι οι επιθυμίες των περισσότερων χρηστών.

Η Google έχει εντοπίσει αρκετές εφαρμογές και συμπεριφορές που δεν θα επιτρέπονται πλέον. Για παράδειγμα, οι προγραμματιστές δεν μπορούν πλέον να τοποθετήσουν τρίτες διαφημίσεις και συνδέσμους στην αρχική οθόνη, να αλλάζουν την αρχική σελίδα του browser ή να χρησιμοποιούν την περιοχή ειδοποιήσεων συστήματος για σκοπούς άσχετους με τους χρήσιμη λειτουργικότητα.







6. Κακόβουλο λογισμικό σε κινητά το 2014: τι να περιμένουμε

6.1 Κακόβουλο λογισμικό android που αναζητά νέους στόχους

Το 2013 SophosLabs είδε την αύξηση στα κακόβουλα λογισμικά android, όχι μόνο από την πλευρά του αριθμού των οικογενειών και των δειγμάτων, αλλά από τον αριθμό των συσκευών που επηρεάζονται σε παγκόσμιο επίπεδο. Ενώ αναμένονται ότι τα νέα χαρακτηριστικά ασφαλείας στην πλατφόρμα των andoid θα κάνει μια θετική αλλαγή στα ποσοστά μόλυνσης με την πάροδο του χρόνου, αφήνοντας περισσότερους χρήστες εκτεθειμένους στις επιθέσεις της απλής κοινωνικής μηχανικής.

Εγκληματίες θα συνεχίσουν να ανακαλύπτουν νέους οδούς για τα κακόβουλα λογισμικά Adroid. Αν και οι επιλογές σε αυτήν την πλατφόρμα είναι πιο περιορισμένες από τα Windows, οι συσκευές τηλεφώνου είναι ένα ελκυστικές για επιθέσεις που στοχεύουν στα κοινωνικά δίκτυα και στις πλατφόρμες. Για να μειώσουν τον κίνδυνο αυτό, εφαρμόζουν μια πολιτική BYOD που αποτρέπει μονόπλευρη φόρτωση των εφαρμογών του κινητού από άγνωστες πηγές και εντολές για προστασία κακόβουλων λογισμικών.

6.2 Κίνδυνος να διερεύσουν προσωπικές πληροφορίες από εφαρμογές σε κινητό και τα κοινωνικά δίκτυα.

Η ασφάλεια στα κινητά θα συνεχίσει να είναι ένα καυτό θέμα το 2014. Η συνεχιζόμενη έγκριση από αναδυόμενες εφαρμογές για την προσωπική και επιχειρηματική επικοινωνία διευρύνει τον χώρο των επιθέσεων, ιδιαίτερα για τις απάτες της κοινωνικής μηχανικής και τις προσπάθειες διαφυγής. Το βιβλίο διευθύνσεών και το γράφημά κοινωνικών συνδέσεων, είναι ένας θησαυρός για τους απατεώνες του κυβερνοχώρου όλων των ειδών, έτσι πρέπει να είστε προσεκτικοί με το ποιόν εμπιστεύεστε να έχει πρόσβαση σε αυτό και γιατί. Ο έλεγχος των εφαρμογών κινητών και διαδικτύου για τους επιχειρηματίες χρήστες θα βοηθήσει να μετριάσουν τον κίνδυνο αυτό.

6.3 Πρόσθετη ασφάλεια χρειάζεται να δομηθεί έτσι ώστε να αφαιρεθεί το βάρος από το χρήστη

Κινητές συσκευές χρησιμοποιούνται όλο και περισσότερο για τις τραπεζικές και άλλες online συναλλαγές. Δεδομένου ότι είναι προς το συμφέρον της τόσο των χρηματοπιστωτικών οργανισμών όσο και των τελικών χρηστών να αυξήσει αυτή την καθημερινή χρήση, φαίνεται πιθανό ότι τα πρόσθετα στρώματα ασφαλείας θα χρειαστούν να χτιστούν για να αφαιρεθεί σε κινητές συσκευές για να απαλλαχθούν από το φορτίο ασφαλείας του τελικού χρήστη και για να εφοδιαστεί με μια πραγματικά ασφαλή εμπειρία.

7. Οι 10 συμβουλές για την πρόληψη κακόβουλων λογισμικών σε κινητά.

Οι χρήστες μπορούν να λάβουν κάποια απλά βήματα για να προστατεύσουν τις συσκευές κινητής τηλεφωνίας τους. Οι παρακάτω 10 συμβουλές απευθύνονται σε οργανώσεις που χρειάζονται να εξασφαλίσουν την ασφάλεια των κινητών των χρηστών τους και την πρόληψη κακόβουλου λογισμικού σε κινητό εταιρείας ή BYOD συσκευές. Επίσης, πολλές από αυτές τις συμβουλές ισχύουν για καθημερινούς καταναλωτές, οι οποίοι πρέπει επίσης να προστατεύσουν τις προσωπικές συσκευές τους.

7.1 Ενημερώστε τους χρήστες σχετικά με τους κινδύνους στα κινητά.

Μια κινητή συσκευή είναι σαν ένας υπολογιστής και θα πρέπει να προστατεύεται σαν αυτόν. Οι χρήστες θα πρέπει να αναγνωρίζουν ότι εφαρμογές ή παιχνίδια μπορούσε να είναι κακόβουλα, και πάντα να εξετάζουν την πηγή. Μια καλή εμπειροτεχνική μέθοδος: Εάν μια εφαρμογή ζητά περισσότερες πληροφορίες από ό, τι πρέπει να κάνει τη δουλειά της, δεν θα πρέπει να το εγκαταστήσετε.

7.2 Εξετάστε την ασφάλεια του εναέριου σήματος δικτύων που χρησιμοποιούνται για πρόσβαση σε δεδομένα της εταιρείας.

Γενικά μιλώντας, για εναέρια δίκτυα (δηλαδή, Wi-Fi) είναι επισφαλείς. Για παράδειγμα, εάν ένας χρήστης έχει πρόσβαση σε εταιρικά δεδομένα χρησιμοποιώντας τη δωρεάν σύνδεση Wi-Fi τα δεδομένα μπορεί να εκτίθονται σε κακόβουλους χρήστες. Οι εταιρείες πρέπει να αναπτύσσουν πολιτική χρήση, να παρέχουν VPN τεχνολογία, και να απαιτούν από τους χρήστες να συνδέονται μέσω αυτών των ασφαλών σήραγγων.

7.3 Δημιουργήστε και επιβάλετε πολιτικές BYOD.

BYOD πρέπει να είναι μια κερδοφόρα για χρήστες και επιχειρήσεις, αλλά μπορεί να οδηγήσει σε πρόσθετο κίνδυνο. Αναρωτηθείτε: Πώς μπορώ να ελέγξω μια συσκευή που ανήκει στον χρήστη και διαχείστη, που απαιτεί πρόσβαση σε εταιρικό δίκτυο μου; Οι εργαζόμενοι είναι συχνά η καλύτερη άμυνα κατά της κλοπής των ευαίσθητων δεδομένων. Οι εργαζόμενοι, χρησιμοποιώντας τις δικές τους κινητές συσκευές πρέπει να ακολουθούν πολιτικές που κρατούν την επιχείρηση υποχωρητική με τις κανονιστικές απαιτήσεις.

7.4 Αποτροπή jailbreaking.

Jailbreaking είναι η διαδικασία της αφαίρεσης των περιορισμών ασφαλείας που επιβάλλεται από τον προμηθευτή του λειτουργικού συστήματος. 'Απόδραση' ή 'ρίζα' σημαίνει ότι αποκτάτε πλήρη πρόσβαση στο λειτουργικό σύστημα και τα χαρακτηριστικά. Αυτό σημαίνει, επίσης, σπάει το μοντέλο ασφαλείας και επιτρέπει όλες τις εφαρμογές, συμπεριλαμβανομένων και των κακόβουλων λογισμικών, να έχουν πρόσβαση στα δεδομένα που ανήκουν σε άλλες εφαρμογές.

7.5 Διατηρήστε την ομαλή λειτουργία της συσκευής για να ενημερωθεί.

Αυτό ακούγεται πιο εύκολο από ό, τι πραγματικά είναι. Στο οικοσύστημα του Android, οι ενημερώσεις μπορεί να μπλοκάρουν με διάφορους τρόπους: Από το Google (το οποίο αναβαθμίζει το λειτουργικό σύστημα) από τον κατασκευαστή του ακουστικού (το οποίο μπορεί να αποφασίσει να απελευθερώσει τις αναπροσαρμογές μόνο για τα τελευταία μοντέλα) ή από την κινητή υπηρεσία παροχής (η οποία δεν μπορεί να αυξηθεί το εύρος ζώνης στο δίκτυό τους για να υποστηρίξει τις ενημερώσεις). Χωρίς τη δυνατότητα να ενημερώσετε το Android OS, η συσκευή σας είναι ευάλωτη. Οι πάροχοι και οι κατασκευαστές κινητής τηλεφωνίας γνωρίζουν ποιες εκδόσεις και ενημερωμένες εφαρμόζονται και σε ποιες όχι.

7.6 Η κρυπτογράφηση της συσκευές σας.

Ο κίνδυνος απώλειας μιας συσκευής είναι ακόμα υψηλότερος από τον κίνδυνο μόλυνσης ενός κακόβουλου λογισμικού. Η προστασία των συσκευών με την πλήρη κρυπτογράφηση καθιστά εξαιρετικά δύσκολη

για κάποιον να διακόψει και να κλέψει τα δεδομένα. Η ρύθμιση ενός ισχυρού κωδικού πρόσβασης σε μια συσκευή, καθώς και για την κάρτα SIM, είναι αρκετό.

7.7 Η κινητή ασφάλεια πρέπει να εντάσσεται σε γενικό πλαίσιο ασφάλειας.

Χρειάζεται να επιτύχει μια ισορροπία ανάμεσα στην ελευθερία του χρήστη και την ευκολία διαχείρισης του περιβάλλοντος του. Εάν μια συσκευή δεν διατηρεί τις πολιτικές ασφάλειας, αυτό δεν θα πρέπει να συνδεθεί με το εταιρικό δίκτυο και την πρόσβαση εταιρικών δεδομένων. Τα τμήματα πρέπει να επικοινωνούν με ποιες συσκευές επιτρέπονται. Και θα πρέπει να μπορείτε να επιβάλλετε την πολιτική ασφαλείας σας χρησιμοποιώντας κινητή συσκευή εργαλεία διαχείρισης

7.8 Μπορείτε να εγκαταστήστε εφαρμογές που προέρχονται από αξιόπιστες πηγές? να εξετάστε μια επιχείρηση από κατάστημα εφαρμογών.

Πρέπει να επιτρέπετε μόνο την εγκατάσταση εφαρμογών που προέρχονται από αξιόπιστες πηγές, όπως Google Play και Apple App Store. Παρόλα αυτά οι εταιρείες θα πρέπει επίσης να θεωρούν την επιχείρηση εφαρμογών ως αποθήκευση για τη διανομή μιας εταιρικής εφαρμογής, τις εφαρμογές και τις κυρώσεις που θα υποστεί ο καταναλωτής. Τέλος ο πωλητής της επιλεγμένης ασφάλειάς σας μπορεί να βοηθήσει να δημιουργήσει μια εφαρμογή στο κατάστημα και να συμβουλεύσει το ποιες εφαρμογές είναι ασφαλείς.

7.9 Να παρέχει εναλλακτικές λύσεις ανταλλαγής-επιμερισμού.

Οι κινητοί χρήστες που θέλουν να αποθηκεύσουν δεδομένα μπορούν να έχουν πρόσβαση από οποιαδήποτε συσκευή, και μπορούν να χρησιμοποιούν υπηρεσίες χωρίς την έγκριση τους. Επίσης, οι επιχειρήσεις θα πρέπει να θεωρηθούν ως μια υπηρεσία ασφαλής αποθήκευσης που βασίζεται σε ανταλλαγή και φιλοξενία χρηστών με ασφαλή τρόπο.

7.10 Να ενθαρρύνουν τους χρήστες να εγκαταστήσουν αντί-κακόβουλο στις συσκευές τους.

Αν και το κακόβουλο λογισμικό υπάρχει για το iOS, BlackBerry και πλατφόρμες που υποστηρίζουν την Java έκδοση, αυτές τις διασυνδέσεις του λειτουργικού συστήματος δεν υποστηρίζουν anti-malware. Ωστόσο, ο κίνδυνος μόλυνσης είναι υψηλότερος για το Android, όπου είναι ήδη διαθέσιμο για το λογισμικό ασφάλειας. Σιγουρευτείτε ότι όλες οι συσκευές Android προστατεύονται από αντι-malware λογισμικό.

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΑΝΑΦΟΡΕΣ

[1] Βαρβαρίγος, Ε. Μπερμπερίδης, Κ. Κινητά Δίκτυα Επικοινωνιών, Πανεπιστημιακές Παραδόσεις. Πανεπιστήμιο Πατρών, 2004

[2] H. Holma, A. Toskala,"WCDMA for UMTS", 3rd Edition, John Wiley and Sons Ltd, England, 2004

[3] UMTS Forum – http://www.umts-forum.org/

[4]Asha Mehrotra «*GSM System Engineering*» , Artech House , 1997.

[5]Μ. Θεολόγου,«*Δίκτυα Κινητών και Προσωπικών Επικοινωνιών*», Εκδόσεις ΕΜΠ, Αθήνα 2002.

[6]Δημοσθένης Σούλης , «*Το Πανευρωπαϊκό Σύστημα Κινητής Τηλεφωνίας G.S.M. και η Εφαρμογή του στην Ελλάδα*», Αθήνα – Μάρτιος 1992.

[7]Antti Siitonen,«*GSM & GPRS*»,Lectures, November 2003,http://www.tml.hut.fi.

[8]Gunnar Heine, Holger Saqkob, «*GPRS: Gateway to Third Generation Mobile Networks*»,Artech House, 2003.

[9]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.

[10]3GPP TS *03.60*, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, Digital Cellular Telecommunications System (Phase 2+)General Packet Radio Service (GPRS) *Service Description*, *Stage 2* , September 2002, (Release 1998).

[11]Jian Cai, David J. Goodman, «*General Packet Radio Service in GSM*», IEEE Communications Magazine, October 1997, Rutgers University.

[12]Β. Μάγκλαρης, Τ. Χιώτης, Θ. Καρούνος, Φ. Σταματελόπουλος, «*Διαχείριση Δικτύων Υπολογιστών*», Εκδόσεις ΕΜΠ, Αθήνα 1994 .

[13] Juha Korhonen,"Introduction to 3G Mobile Communications", 2nd Edition, Artech House, 2003.

[14] H. Holma, A. Toskala,"WCDMA for UMTS", 3rd Edition, John Wiley and Sons Ltd, England, 2004.

[15] 3GPP. Medium Access Control (MAC) protocol specification. Technical specification, TS 25.321, version 7.0.0.

[16] Alexiou, A., Bouras, C., Igglesis, V. Performance Evaluation of UMTS for Mobile Internet Access. 12th Annual Meeting of the IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2004), Volendam, The Netherlands, 1 – 4, pp. 615 – 618.

[17] Alexiou, A., Bouras, C., Igglesis, V. Performance Evaluation of TCP over UMTS Transport Channels. 7th International Symposium on Communications Interworking – INTERWORKING 2004, Ottawa, Canada.

18. International Data Corporation; Apple Cedes Market Share in Smartphone Operating System Market as Android Surges and Windows Phone Gains, According to IDC; published 7 August 2013; http://www.idc.com/getdoc.jsp?containerId=prUS24257413

19. F-Secure Weblog; Sean Sullivan; Trojan:Android/Pincer.A; published 5 April 2013; http://www.f-secure.com/weblog/archives/00002538.html

20. Krebs on Security; Brian Krebs; Who Wrote the Pincer Android Trojan?; published 27 August 2013; http://krebsonsecurity.com/2013/08/who-wrote-the-pincer-android-trojan/

21. F-Secure Weblog; Sean Sullivan; Mobile Bot "Perkele Lite" [Android Only]; published 7 March 2013; http://www.f-secure.com/weblog/archives/00002519.html

22. Krebs on Security; Brian Krebs; A Closer Look: Perkele Android Malware Kit; published 19 August 2013; http://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/

23. Symantec; Andrea Lelli; Remote Access Tool Takes Aim with Android APK Binder; published 16 July 2013; http://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder

24. Symantec; First Malicious Use of 'Master Key' Android Vulnerability Discovered; published 23 July 2013; http://www.symantec.com/connect/blogs/first-malicious-use-master-key-android-vulnerability-discovered

25. Naked Security; Paul Ducklin; Android "Master Key" vulnerability - more malware exploits code verification bypass; published 9 August 2013; http://nakedsecurity.sophos.com/2013/08/09/android-master-key-vulnerability-more-malware-found-exploiting-code-verification-bypass/

26. InfoSecurity; More Exploits for Android 'MasterKey' Vulnerability Turn Up in the Wild; published 9 August 2013; http://www.infosecurity-magazine.com/view/33941/more-exploits-for-android-masterkey-vulnerability-turn-up-in-the-wild/

27. Threat Post; Dennis Fisher; Jeff Forristal on the Android Master-Key Vulnerability; published 5 August 2013; http://threatpost.com/jeff-forristal-on-the-android-master-key-vulnerability-2/101587

28. Nokia Developer News; Fred Patton; Changes to supported content types in the Nokia Store; published 4 October 2013; http://developer.nokia.com/Blogs/News/blog/2013/10/04/changes-to-supported-content-types-in-the-nokia-store/

29. F-Secure Weblog, Trojan:Android/Adrd.A, published 16 February 2011; http://www.f-secure.com/weblog/archives/00002100.html