Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ – ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΟΜΕΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Σχεδίαση και ανάπτυξη συστήματος πιστοποίησης χρήστη σε δίκτυο με βάση την SIM του κινητού τηλεφώνου»

Σπουδαστής:
ΙΑΚΩΒΟΥ Μάριος

ΕΠΙΒΛΕΠΩΝ ΣΕΠ: Δρ. Ι ΠΙΚΡΑΜΜΕΝΟΣ

-2013-

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Στα μέσα της δεκαετίας του 1990 υπήρχαν πολυάριθμα είδη δικτύων LAN και WAN, καθώς και πολυάριθμες στοίβες πρωτοκόλλων. Μέχρι το 2003, το μόνο ενσύρματο δίκτυο LAN σε εκτεταμένη χρήση είναι το Ethernet και ουσιαστικά όλα τα δίκτυα WAN είναι συνδεδεμένα στο Internet. Κατά τη διάρκεια του 20ου αιώνα οι βασικές τεχνολογίες ήταν η συλλογή, η επεξεργασία και η διανομή πληροφοριών. Μεταξύ των άλλων εξελίξεων είχαμε την εγκαθίδρυση των παγκόσμιων τηλεφωνικών δικτύων, την εφεύρεση του ραδιοφώνου και της τηλεόρασης, τη γένεση και την πρωτοφανή ανάπτυξη της βιομηχανίας των υπολογιστών και την εκτόξευση των τηλεπικοινωνιακών δορυφόρων.

Ως αποτέλεσμα της ραγδαίας τεχνολογικής προόδου, οι τεχνολογικοί αυτοί τομείς συγκλίνουν ταχύτητα και εξαφανίζονται οι διαφορές ανάμεσα στη συλλογή, τη μεταφορά, την αποθήκευση και την επεξεργασία των πληροφοριών. Οργανισμοί με εκατοντάδες γραφεία διάσπαρτα σε μία μεγάλη γεωγραφική περιοχή αναμένουν φυσιολογικά ότι θα μπορούν να εξετάζουν καθημερινά την τρέχουσα κατάσταση και των πιο απομακρυσμένων εγκαταστάσεων τους με το πάτημα ενός κουμπιού.

Παρόλο που η τεχνολογία των υπολογιστών είναι ακόμη νέα σε σύγκριση με άλλες βιομηχανίες οι υπολογιστές έχουν σημειώσει εντυπωσιακή πρόοδο σε πολύ μικρό χρονικό διάστημα. Κατά τα πρώτα είκοσι χρόνια της ύπαρξης τους, τα υπολογιστικά συστήματα ήταν ιδιαίτερα συγκεντρωτικά και λειτουργούσαν σε μεγάλα δωμάτια. Μια εταιρία μεσαίου μεγέθους ή ένα πανεπιστήμιο μπορεί να είχε έναν ή δύο υπολογιστές ενώ τα μεγάλα ιδρύματα είχαν το πολύ μερικές δεκάδες. Οι ιδέες ότι μέσα σε είκοσι χρόνια εξίσου ισχυροί υπολογιστές με μέγεθος μικρότερο από ένα γραμματόσημο θα παράγονταν μαζικά ξεπερνούσε κάθε φαντασία.

Η συγχώνευση των υπολογιστών και των επικοινωνιών είχε σημαντική επίδραση στον τρόπο οργάνωσης των υπολογιστικών συστημάτων. Η έννοια του κέντρου υπολογιστών σαν ένα δωμάτιο με ένα μεγάλο υπολογιστή στον οποίο οι χρήστες φέρνουν τη δουλειά τους για επεξεργασία είναι πλέον απαρχαιωμένη. Η δουλειά πλέον γίνεται από ένα μεγάλο πλήθος αυτόνομων αλλά διασυνδεδεμένων υπολογιστών. Αυτά τα συστήματα ονομάζονται δίκτυα υπολογιστών. Με τον όρο αυτό εννοούμε ένα σύνολο αυτόνομων υπολογιστών που είναι διασυνδεδεμένοι με

μία κοινή τεχνολογία. Δύο υπολογιστές λέμε ότι είναι διασυνδεδεμένοι εάν μπορούν να ανταλλάσσουν πληροφορίες. Η σύνδεση μπορεί να γίνεται είτε με χάλκινο σύρμα, είτε με οπτικές ίνες, με μικροκύματα, υπέρυθρες ακτίνες και τηλεπικοινωνιακούς δορυφόρους. Υπάρχουν δίκτυα σε διάφορα μεγέθη, σχήματα και μορφές. Να σημειώσουμε πως ούτε το Internet ούτε ο παγκόσμιος ιστός είναι δίκτυα υπολογιστών. Το internet δεν είναι ένα μόνο δίκτυο αλλά ένα δίκτυο δικτύων, ενώ ο ιστός είναι ένα κατανεμημένο σύστημα που λειτουργεί πάνω από το internet.

Υπάρχει αρκετή σύγχυση ανάμεσα σε ένα δίκτυο υπολογιστών και σε ένα κατανεμημένο σύστημα. Η βασική διαφορά είναι ότι ένα κατανεμημένο σύστημα έχει ένα σύνολο από ανεξάρτητους υπολογιστές και εμφανίζεται στους χρήστες σαν να ήταν ένα μοναδικό συνεκτικό σύστημα. Το σύστημα αυτό έχει συνήθως ένα βασικό μοντέλο ή υπόδειγμα το οποίο παρουσιάζεται στους χρήστες του. Πολλές φορές την ευθύνη υλοποίησης αυτού του μοντέλου την έχει ένα επίπεδο λογισμικού πάνω από το λειτουργικό σύστημα, το οποίο ονομάζεται ενδιάμεσο λογισμικό.

Στα δίκτυα υπολογιστών απουσιάζει η συνεκτικότητα, το μοντέλο και το λογισμικό που υπάρχει στα κατανεμημένα συστήματα. Οι χρήστες είναι εκτεθειμένοι στις πραγματικές μηχανές και δε γίνεται καμία προσπάθεια από το σύστημα έτσι ώστε οι μηχανές να παρουσιάζονται η να ενεργούν με συνεκτικό τρόπο. Αν οι μηχανές έχουν διαφορετικό υλικό και διαφορετικά λειτουργικά συστήματα αυτό είναι πλήρως ορατό από τους χρήστες. Αν κάποιος χρήστης θέλει να εκτελέσει ένα πρόγραμμα σε μία απομακρυσμένη μηχανή τότε αυτός θα πρέπει να συνδεθεί με τη συγκεκριμένη μηχανή για να το εκτελέσει εκεί.

Ουσιαστικά το κατανεμημένο σύστημα είναι ένα σύστημα λογισμικού χτισμένο πάνω σε ένα δίκτυο. Το λογισμικό δίνει στο δίκτυο έναν υψηλό βαθμό συνοχής και διαφάνειας. Κατά συνέπεια, η διάκριση ανάμεσα σε ένα δίκτυο και ένα κατανεμημένο σύστημα έγκειται στο λογισμικό και όχι στο υλικό τους.

Ωστόσο υπάρχει μία σημαντική επικάλυψη ανάμεσα στα δύο αυτά θέματα. Για παράδειγμα και τα κατανεμημένα συστήματα και τα δίκτυα υπολογιστών έχουν την ανάγκη μετακίνησης αρχείων από σημείο σε σημείο. Η διαφορά έγκειται στο ποιος ελέγχει τη μετακίνηση, το σύστημα ή ο χρήστης.

ΚΕΦΑΛΑΙΟ 1: ΔΙΚΤΥΑ

1.1. ΓΕΝΙΚΑ ΓΙΑ ΤΑ ΔΙΚΤΥΑ

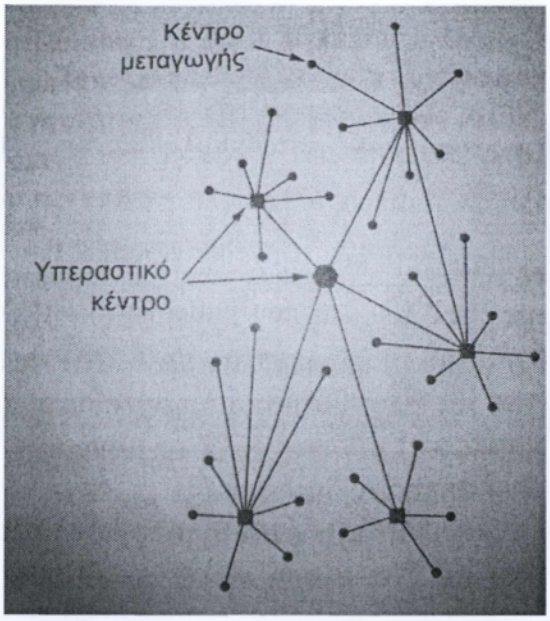
Ο τομέας της δικτύωσης υπολογιστών καλύπτει πολλά και διαφορετικά είδη δικτύων άλλα μεγάλα και άλλα μικρά, άλλα πολύ γνωστά και άλλα λιγότερο γνωστά. Τα δίκτυα αυτά έχουν διαφορετικούς στόχους, κλίμακες και τεχνολογίες. Μερικά παραδείγματα σχετικά με την ποικιλία που μπορούμε να συναντήσουμε στο πεδίο δικτύωσης υπολογιστών είναι: το Internet, που αποτελεί το πιο γνωστό δίκτυο , το ATM, το οποίο χρησιμοποιείται συχνά στον πυρήνα μεγάλων τηλεφωνικών δικτύων (από τεχνική άποψη το δίκτυο αυτό είναι πολύ διαφορετικό από το Internet), το Ethernet (το κυρίαρχο τοπικό δίκτυο), το IEEE 802.11, το πρότυπο για τα ασύρματα LAN.

1.1.1. Το Internet

Το Internet δεν είναι ένα απλό δίκτυο αλλά αποτελεί μία τεράστια συλλογή από διαφορετικά τοπικά δίκτυα που χρησιμοποιούν κάποια κοινά πρωτόκολλα και παρέχουν κάποιες κοινές υπηρεσίες. Είναι ένα ασυνήθιστο σύστημα, με την έννοια ότι δε σχεδιάστηκε από κανέναν. Για να το κατανοήσουμε καλύτερα, ας ξεκινήσουμε από την αρχή για να δούμε πως εξελίχθηκε και γιατί.

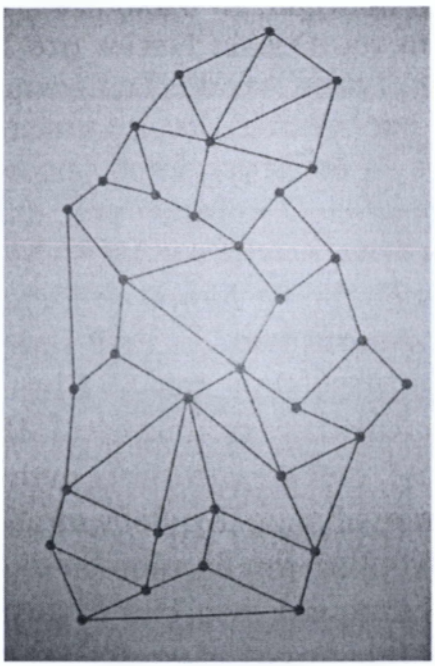
Η ιστορία αρχίζει στα τέλη της δεκαετίας του 1950. Στην ακμή του Ψυχρού Πολέμου παρουσιάστηκε η ανάγκη για τη δημιουργία ενός δικτύου διοίκησης και ελέγχου το οποίο θα μπορούσε να επιβιώσει σε έναν πυρηνικό πόλεμο. Εκείνη την εποχή όλες οι στρατιωτικές τηλεπικοινωνίες χρησιμοποιούσαν το δημόσιο τηλεφωνικό δίκτυο, το οποίο θεωρείτο ευπαθές. Ο λόγος για την πεποίθηση αυτή μπορεί να γίνει κατανοητός από την παρακάτω εικόνα. Στην εικόνα αυτή οι μαύρες κουκίδες αντιπροσωπεύουν κέντρα μεταγωγής, το καθένα από τα οποία συνδεόταν σε χιλιάδες τηλέφωνα. Αυτά τα κέντρα μεταγωγής ήταν με τη σειρά τους συνδεδεμένα σε κέντρα μεταγωγής ανώτερου επιπέδου (υπεραστικά κέντρα) σχηματίζοντας μια εθνική ιεραρχία με μικρό μόνο βαθμό πλεονασμού. Η ευπάθεια του συστήματος ήταν

ότι η καταστροφή λίγων επιλεγμένων περιφερειακών κέντρων μπορούσε να «θρυμματίσει» το σύστημα σε πολλές απομονωμένες νησίδες.



Εικόνα 1: Δομή του τηλεφωνικού συστήματος

Γύρω στο 1960 ο Paul Baran επινόησε την άκρως κατανεμημένη και ανεκτή σε βλάβες όπως φαίνεται στην παρακάτω εικόνα. Αφού οι διαδρομές ανάμεσα σε δύο οποιαδήποτε κέντρα μεταγωγής ήταν πια πολύ μεγάλες και δεν μπορούσαν να επιτρέψουν τη μετάδοση αναλογικών σημάτων χωρίς παραμόρφωση, ο Baran πρότεινε τη χρήση ψηφιακής τεχνολογίας μεταγωγής πακέτων σε ολόκληρο το σύστημα. Ο Baran σε πολλές αναφορές που έγραφε περιέγραφε με λεπτομέρεια της. Η ιδέα αυτή άρεσε στους αξιωματούχους του Πενταγώνου οι οποίοι ζήτησαν από την AT&T (το τότε εθνικό μονοπώλιο τηλεφωνίας των ΗΠΑ) να κατασκευάσει ένα πρωτότυπο. Η AT&Τα απέρριψε ασυζητητί τις ιδέες του Baran. Η μεγαλύτερη και πλουσιότερη εταιρεία στον κόσμο δεν ήταν προετοιμασμένη να επιτρέψει σε κάποιο νεαρό να της πει πώς να φτιάξει ένα τηλεφωνικό σύστημα. Είπαν λοιπόν ότι το δίκτυο του Baran δεν μπορούσε να κατασκευαστεί και η ιδέα θανατώθηκε.

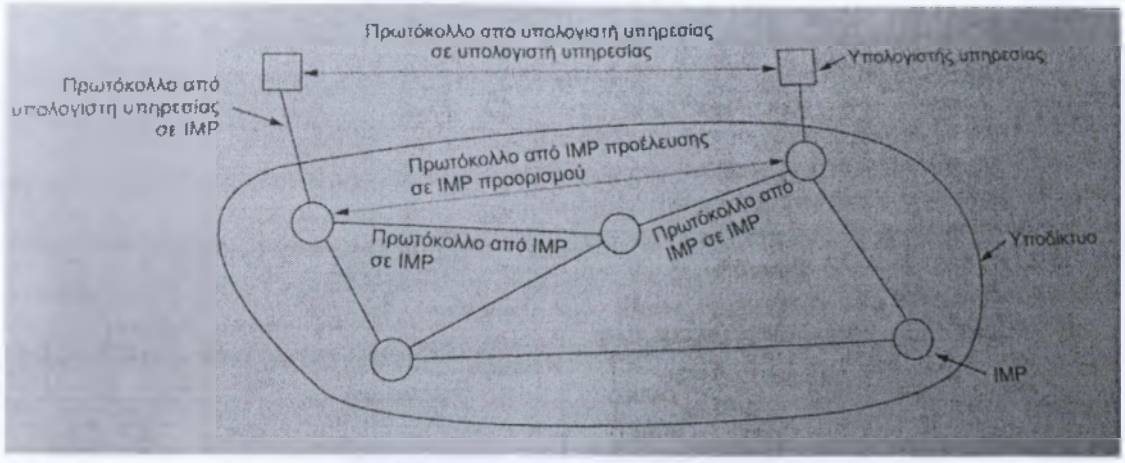


Εικόνα 2: Το κατανεμημένο σύστημα που πρότεινε ο Baran

Πέρασαν αρκετά χρόνια μέχρι να εξελιχθεί κάπως η τεχνολογία και για να κατανοήσουμε κάπως τα πράγματα ας γυρίσουμε πίσω τον Οκτώβριο του 1957 όταν η Σοβιετική Ένωση ξεπέρασε τις ΗΠΑ στο διάστημα με την εκτόξευση του πρώτου τεχνητού δορυφόρου, του Sputnik. Όταν ο πρόεδρος Αϊζενχάουερ προσπάθησε να βρει ποιος έφταιγε, έμεινε έκπληκτος όταν ανακάλυψε ότι ο Στρατός, το Ναυτικό και η Αεροπορία καυγάδιζαν για τον προϋπολογισμό έρευνας του Πενταγώνου. Η άμεση αντίδραση ήταν να δημιουργήσει ένα μόνο οργανισμό έρευνας για τα αμυντικά θέματα, την Υπηρεσία Προηγμένων Ερευνητικών Έργων ή ARPA (Advanced Research Projects Agency). Η ARPA δεν είχε ούτε ερευνητές ούτε εργαστήρια, στην πραγματικότητα δεν είχε τίποτα παραπάνω από ένα γραφείο και ένα μικρό προϋπολογισμό. Έκανε τη δουλειά της με το να απονέμει χρηματοδοτήσεις και συμβόλαια στα πανεπιστήμια και τις εταιρείες που είχαν ιδέες οι οποίες φαίνονταν στην υπηρεσία πολλά υποσχόμενες.

Στα πρώτα χρόνια η ARPA προσπαθούσε ακόμη να καθορίσει ποια θα έπρεπε να είναι η αποστολή της αλλά το 1967 η προσοχή του τότε διευθυντή της ARPA, του Luary Roberts, στράφηκε στη δικτύωση. Έτσι, ήρθε σε επαφή με διάφορους ειδικούς για να αποφασίσει τι να κάνει. Ένας από αυτούς, ο Wesley Clark πρότεινε τη

δημιουργία ενός υποδικτύου μεταγωγής πακέτων στο οποίο κάθε υπολογιστής υπηρεσίας θα είχε το δικό του δρομολογητή., όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 3: Η αρχική σχεδίαση του ARPANET

Μετά από κάποιον αρχικό σκεπτικισμό ο Roberts πείστηκε με την ιδέα αυτή και παρουσίασε ένα κάπως ασαφές άρθρο πάνω σε αυτή στο Συμπόσιο Αρχών Λειτουργικών Συστημάτων της ACM SIGOPS, που έγινε στο Γκάτλινμπεργκ του Τεννεσσί στα τέλη του 1967. Προς μεγάλη έκπληξη του Roberts, άλλο ένα άρθρο στο συνέδριο περιέγραφε ένα παρόμοιο σύστημα, τα οποίο δεν είχε μόνο σχεδιαστεί αλλά είχε υλοποιηθεί κιόλας υπό τη διεύθυνση του Donald Davies στο Εθνικό Εργαστήριο Φυσικής ή NPL (National Physical Laboratory) στην Αγγλία. Το σύστημα του NPL δεν ήταν εθνικής εμβέλειας αλλά έδειχνε ότι η μεταγωγή πακέτων μπορούσε να δουλέψει. Επιπρόσθετα, αναφερόταν σε παλαιότερες εργασίες του Baran που είχαν απορριφθεί. Ο Roberts έφυγε από το Γκάτλινμπεργκ αποφασισμένος να φτιάξει αυτό που αργότερα έγινε γνωστό ως ARPANET.

Το υποδίκτυο αποτελείται από υπολογιστές μίνι που ονομάζονταν Επεξεργαστές Μηνυμάτων Διασύνδεσης ή IMP (Interface Message Processors) οι οποίοι ήταν συνδεδεμένοι με γραμμές μετάδοσης των 56Kbps. Για να παρέχει υψηλή αξιοπιστία κάθε IMP συνδεόταν με τουλάχιστον άλλους δύο IMP. Το υποδίκτυο χρησιμοποιούσε αυτοδύναμα πακέτα (datagrams) έτσι αν καταστρέφονταν μερικές γραμμές και μερικοί IMP τα μηνύματα θα μπορούσαν να αναδρομολογηθούν αυτόματα μέσω εναλλακτικών διαδρομών.

Κάθε κόμβος του δικτύου αποτελούνταν από έναν IMP και έναν υπολογιστή υπηρεσίας και βρίσκονταν στο ίδιο δωμάτιο και ήταν συνδεδεμένοι με ένα μικρό καλώδιο. Ο υπολογιστής υπηρεσίας μπορούσε να στέλνει μηνύματα μεγέθους μέχρι 8063 bit στον IMP του, και αυτός με τη σειρά του τα τεμάχιζε σε πακέτα μεγέθους το πολύ 1003 bit και τα προωθούσε ανεξάρτητα προς τον προορισμό τους. Κάθε πακέτο λαμβανόταν πλήρως πριν προωθηθεί και έτσι το δίκτυο αυτό ήταν το πρώτο ηλεκτρονικό δίκτυο μεταγωγής με αποθήκευση και προώθηση.

Η ARPA προκήρυξε τότε ένα διαγωνισμό για την υλοποίηση του υποδικτύου. Δώδεκα εταιρίες υπέβαλαν προσφορές. Αφού εξέτασε όλες τις προσφορές η ARPA επέλεξε την BBN μια εταιρία παροχής συμβουλευτικών υπηρεσιών στο Κέμπριτζ της Μασαχουσέτης και το Δεκέμβριο του 1968 της έδωσε ένα συμβόλαιο για να υλοποιήσει το υποδίκτυο και να γράψει το λογισμικό του υποδικτύου. Η BBN αποφάσισε να χρησιμοποιήσει ως IMP ειδικά τροποποιημένους υπολογιστές μίνι Honeywell DDp-316 με 12K 16μπιτων λέξεων ως κύρια μνήμη. Οι IMP δεν είχαν δίσκους αφού τα κινούμενα μέρη θεωρήθηκαν αναξιόπιστα. Οι IMP διασυνδέονταν με γραμμές των 56 Kbps οι οποίες ήταν μισθωμένες από τις τηλεφωνικές εταιρίες.

Το λογισμικό διαιρέθηκε σε δύο μέρη: τα τμήματα υποδικτύου και υπολογιστή υπηρεσίας. Το λογισμικό του υποδικτύου αποτελούνταν από το άκρο του IMP για την σύνδεση από τον υπολογιστή υπηρεσίας προς τον IMP, το πρωτόκολλο από IMP σε IMP και από ένα πρωτόκολλο μεταξύ του IMP προέλευσης και του IMP προορισμού που σχεδιάστηκε για αύξηση της αξιοπιστίας.

Για να ενθαρρύνει την υιοθέτηση αυτών των νέων πρωτοκόλλων, η ARPA έδωσε πολλά συμβόλαια στην και στο Πανεπιστήμιο της Καλιφόρνιας στο Μπέρκλεϋ για να τα ενσωματώσουν στο Berkeley Unix. Οι ερευνητές του Μπέρκλεϋ ανέπτυξαν μία εύχρηστη σύνδεση εφαρμογών με το δίκτυο και έγραψαν πολλές εφαρμογές, βοηθητικά προγράμματα και εφαρμογές διαχείρισης για να διευκολύνουν τη δικτύωση.

Ο χρονισμός ήταν τέλειος. Πολλά πανεπιστήμια είχαν μόλις προμηθευθεί ένα δεύτερο και ένα τρίτο υπολογιστή VAX μαζί με ένα δίκτυο LAN για να τους διασυνδέσουν, αλλά δεν είχαν λογισμικό δικτύωσης. Όταν εμφανίστηκε το λειτουργικό σύστημα 4.2BSD, με το TCP/IP τις υποδοχές και πολλά βοηθητικά προγράμματα δικτύωσης, ολόκληρο το πακέτο υιοθετήθηκε άμεσα

Κατά τη δεκαετία του 1980 πρόσθετα δίκτυα, ειδικά δίκτυα LAN συνδέθηκαν με το ARPANET. Καθώς αυξανόταν η κλίμακα του δικτύου γινόταν όλο και πιο δύσκολη η ανεύρεση υπολογιστών υπηρεσίας, οπότε δημιουργήθηκε το Σύστημα Ονομάτων Περιοχών ή DNS (Domain Name System) ώστε να οργανώνει τις μηχανές σε περιοχές και να αντιστοιχίσει τα ονόματα των υπολογιστών υπηρεσίας σε διευθύνσεις IP. Από τότε το DNS έχει γίνει ένα γενικής χρήσης κατανεμημένο σύστημα βάσης δεδομένων που αποθηκεύει ποικίλες πληροφορίες σχετικά με την ονομασία.

1.1.2. Το NSFNET

Προς τα τέλη της δεκαετίας του 1970 το Εθνικό Ίδρυμα Επιστημών των ΗΠΑ ή NSF (National Science Foundation) είδε τον τεράστιο αντίκτυπο που είχε το ARPANET στην πανεπιστημιακή έρευνα καθώς επέτρεπε σε επιστήμονες από όλη τη χώρα να μοιράζονται δεδομένα και να συνεργάζονται σε ερευνητικά έργα. Το NSF σχεδίασε ένα διάδοχο του ARPANET ο οποίος ήταν ανοιχτός στις ερευνητικές ομάδες όλων των πανεπιστημίων

Το NSF χρηματοδότησε μερικά περιφερειακά δίκτυα που συνδέονταν στο δίκτυο κορμού επιτρέποντας σε χρήστες από χιλιάδες πανεπιστήμια, ερευνητικά εργαστήρια, βιβλιοθήκες και μουσεία να έχουν πρόσβαση σε οποιοδήποτε από τους υπερυπολογιστές και να επικοινωνούν μεταξύ τους. Το ολοκληρωμένο δίκτυο που περιελάμβανε το δίκτυο κορμού και τα περιφερειακά δίκτυα, ονομαζόταν NSFNET.

1.1.3. Χρήση του Internet

Το πλήθος των δικτύων, των μηχανών και των χρηστών που ήταν συνδεδεμένοι στο ARPANET αυξήθηκε ραγδαία μετά την καθιέρωση του TCP/IP ως επίσημου πρωτοκόλλου, την 1η Ιανουαρίου 1983. Όταν διασυνδέθηκαν το NSFNET και το ARPANET, η αύξηση έγινε εκθετική. Πολλά περιφερειακά δίκτυα συνδέθηκαν, ενώ έγιναν και συνδέσεις με δίκτυα στον Καναδά, την Ευρώπη και τις χώρες του Ειρηνικού.

Κάπου στα μέσα της δεκαετίας του 1980, ο κόσμος άρχισε να αντιμετωπίζει αυτή τη συλλογή δικτύων σαν ένα διαδίκτυο και αργότερα σαν το Διαδίκτυο ή Internet, αν και δεν έγινε ποτέ κάποια επίσημη τελετή εγκαινίων.

Ο συνδετικός ιστός του Internet είναι το μοντέλο αναφοράς TCP/IP και η στοίβα πρωτοκόλλων TCP/IP. Το TCP/IP επιτρέπει την παροχή μιας καθολικής υπηρεσίας και μπορεί να συγκριθεί με την υιοθέτηση μιας τυποποιημένης απόστασης ανάμεσα στις σιδηροτροχιές των τρένων το 19° αιώνα ή την υιοθέτηση ενός κοινού πρωτόκολλου σηματοδοσίας από όλες τις τηλεφωνικές εταιρίες.

Όταν λέμε ότι κάποιος είναι συνδεδεμένος στο Internet εννοούμε ότι μια μηχανή είναι συνδεδεμένη στο Internet αν εκτελεί τη στοίβα πρωτοκόλλων TCP/IP,έχει μία διεύθυνση IP σε όλες τις μηχανές του Internet. Η απλή ικανότητα να μπορεί να στέλνει και να λαμβάνει ηλεκτρονικό ταχυδρομείο δεν είναι αρκετή αφού το ηλεκτρονικό ταχυδρομείο μπορεί να διακινηθεί μέσω πυλών προς πολλά δίκτυα έξω από το Internet. Ωστόσο, αξίζει να σημειώσουμε ότι εκατομμύρια προσωπικοί υπολογιστές μπορούν να καλέσουν ένα φορέα παροχής υπηρεσιών Internet χρησιμοποιώντας ένα μόντεμ να λάβουν μία προσωρινή διεύθυνση IP και μετά να στείλουν πακέτα σε άλλους υπολογιστές υπηρεσίας στο Internet. Επομένως, θεωρούμε ότι αυτές οι μηχανές είναι συνδεδεμένες στο Internet για όσο χρονικό διάστημα είναι συνδεδεμένες στο Internet για όσο χρονικό διάστημα είναι συνδεδεμένες στο δρομολογητή του φορέα παροχής υπηρεσιών.

Από το 1970 έως και το 1990 το Internet και οι προκάτοχοι του είχαν τέσσερις κύριες εφαρμογές: Ηλεκτρονικό ταχυδρομείο, συζητήσεις, τηλεσύνδεση και μεταφορά αρχείων.

Μέχρι και τις αρχές της δεκαετίας του 1990, στο Internet βρίσκονταν κυρίως ακαδημαϊκοί, κρατικοί οργανισμοί και βιομηχανικοί ερευνητές. Μια νέα εφαρμογή, ο Παγκόσμιος Ιστός ή WWW (World Wide Web) άλλαξε τα πάντα και έφερε εκατομμύρια νέους, μη ακαδημαϊκούς χρήστες στο δίκτυο. Η εφαρμογή αυτή δεν άλλαξε κάποια από τις υπάρχουσες λειτουργίες αλλά τις έκανε ευκολότερες στη χρήση. Πατώντας σε ένα σύνδεσμο ο χρήστης μεταφέρεται άμεσα στη σελίδα προς την οποία δείχνει ο σύνδεσμος αυτός. Για παράδειγμα πολλές εταιρίες έχουν μια εισαγωγική σελίδα (home page) με καταχωρήσεις που δείχνουν σε άλλες σελίδες με στοιχεία προϊόντων, τιμοκαταλόγους, πωλήσεις, τεχνική υποστήριξη, επικοινωνία με υπαλλήλους, πληροφορίες για τους μετόχους και πολλά άλλα.

Πολλά άλλα είδη σελίδων έχουν εμφανιστεί σε πολύ σύντομο χρονικό διάστημα όπως χάρτες, πίνακες χρηματιστηριακών στοιχείων, κατάλογοι βιβλιοθηκών, μαγνητοφωνημένα ραδιοφωνικά προγράμματα ακόμη και σελίδες με συνδέσμους προς το πλήρες κείμενο πολλών βιβλίων για τα οποία έχουν λήξει τα πνευματικά δικαιώματα. Πολλοί άνθρωποι διαθέτουν προσωπικές σελίδες.

1.1.4. Ethernet

Το Ethernet είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης (LAN - Local area network, συντμ. LAN) υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα

Hardware

Το αρχικό Ethernet επέτρεπε ονομαστικούς ρυθμούς μετάδοσης δεδομένων της τάξης των 3 Mbps, μέσω ενός ομοαξονικού καλωδίου στο οποίο συνδέονταν οι επιμέρους υπολογιστές του δικτύου (σύνδεση token ring). Τη διασύνδεση αναλάμβανε μία κάρτα δικτύου Ethernet προσαρτημένη σε κάθε κόμβο, με κάθε κάρτα να χαρακτηρίζεται από μία μοναδική, εργοστασιακή 48-bit διεύθυνση MAC. Σήμερα η σύνδεση token ring έχει εγκαταλειφθεί ολοκληρωτικά και οι επιμέρους υπολογιστές του δικτύου συνδέονται ο καθένας σε ανεξάρτητη θύρα ενός router ή διανομέα. Έχουν εμφανιστεί νεότερες εκδόσεις του Ethernet οι οποίες χρησιμοποιούν είτε κοινά καλώδια χαλκού με αθωράκιστα (καλώδια UTP) ή θωρακισμένα (καλώδια STP) συνεστραμμένα ζεύγη αγωγών ή οπτικές ίνες:

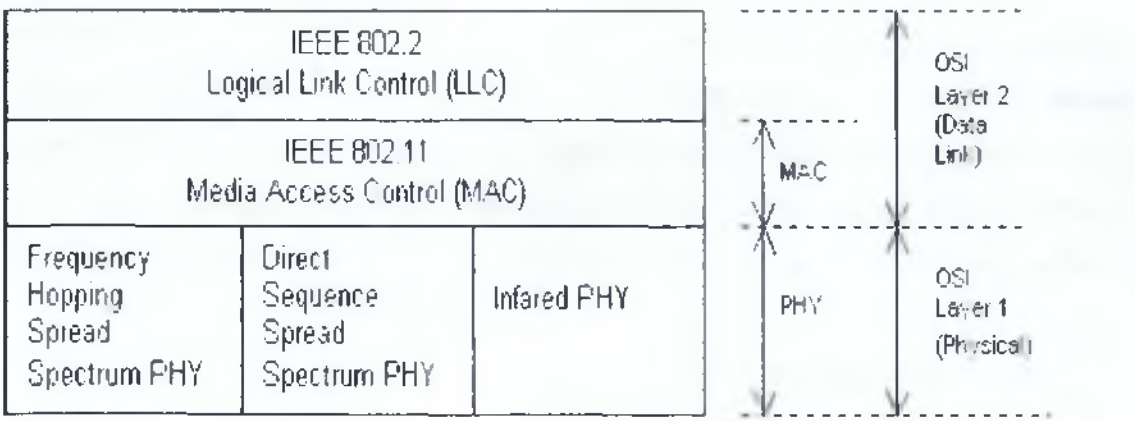
Ethernet (10MBps), όπου για τις συνδέσεις με χαλκό χρησιμοποιείται το πρότυπο 10BASE-T και για τις οπτικές ίνες το πρότυπο 10BASE-F(L). Η σύνδεση χαλκού είναι συμβατή με αυτή του Fast Ethernet.

Fast Ethernet (100 Mbps), όπου για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 100BASE-TX έναντι των ουσιαστικά εγκαταλελειμμένων 100BASE-T2, 100BASE-T4. Το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι το 100BASE-FX.

Επιπλέον, είναι δυνατή η αυτόματη ανίχνευση κυκλώματος 10BASE-T στην άλλη πλευρά του καλωδίου και η εν συνεχεία υποβάθμιση της ταχύτητας στα 10Mbps Gigabit Ethernet (1 Gbps), όπου για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 1000BASE-T.

1.1.5. Ασύρματα LAN: 802.11

Ένα ασύρματο LAN (WLAN) είναι συνήθως μία επέκταση ενός ενσύρματου LAN. WLAN συστατικά μετατρέπουν τα πακέτα δεδομένων σε ραδιοκύματα ή υπέρυθρους (IR) παλμούς φωτός και τα στέλνουν σε άλλες ασύρματες συσκευές ή σε ένα σημείο πρόσβασης που χρησιμεύει ως μια πύλη προς το ενσύρματο LAN. Τα περισσότερα δίκτυα WLANs σήμερα είναι βασισμένα στα πρότυπα IEEE 802.11 για ασύρματη επικοινωνία ανάμεσα σε συσκευές και σε ένα LAN. Η δομή ενός 802.11 WLAN παρουσιάζεται στην παρακάτω εικόνα:



Εικόνα 4: Η δομή ενός 802.11 WLAN

Το LLC [1] υπο-στρώμα εκτελεί τις εξής λειτουργίες:

1. διαχείριση της επικοινωνίας ζεύξης δεδομένων,
2. διεύθυνση του link
3. καθορισμός Πρόσβαση Υπηρεσίας Σημεία (Service Access Points (SAPs))
4. αλληλουχία ροής πακέτων δεδομένων

Το στρώμα MAC είναι ένα σύνολο πρωτοκόλλων που είναι υπεύθυνο για τη διατήρηση της τάξης στην χρήση ενός κοινόχρηστου μέσου. Διασφαλίζει ότι ο δέκτης είναι σε θέση να ανακτήσει τα πακέτα δεδομένων που έχουν αποσταλεί.

Όσον αφορά το φυσικό επίπεδο, η ασύρματη σύνδεση υποστηρίζει συνδεσιμότητα με μια χαλαρή έννοια του όρου σημείο-προς-σημείο επικοινωνίας. Η απουσία της αυστηρότητας στην έννοια του σημείου-προς-σημείο επικοινωνία βασίζεται στο γεγονός ότι πολλοί τρίτοι μπορούν να διεισδύσουν στο επικοινωνιακό κανάλι, χωρίς κατ 'ανάγκη να παρεμβαίνουν στη μετάδοση ή τη συναλλαγή που λαμβάνουν χώρα. Το MAC υπο-στρώμα, εξαιτίας του γεγονότος ότι είναι το τελευταίο επίπεδο των ψηφιακών δεδομένων επεξεργασίας, είναι σύνηθες να ενσωματωθεί σε μια κάρτα τσιπ κάρτα που ενσωματώνει και λειτουργίες κρυπτογράφησης,

1.1.6.: MAC επίπεδο

Οι ασύρματοι σταθμοί και το σημείο πρόσβασης προκειμένου να επικοινωνήσουν χρησιμοποιούν το ίδιο κανάλι , μια κοινή ραδιοσυχνότητα. Έτσι για να είναι δυνατή η ασύρματη επικοινωνία χρειάζεται ένας τρόπος, ένα πρωτόκολλο, που να καθορίζει τον τρόπο χρησιμοποίησης του μοναδικού καναλιού από πολλούς χρήστες. Χωρίς την παρουσία παρόμοιου μηχανισμού αξιόπιστη ασύρματη μετάδοση δεν θα ήταν δυνατή, αφού η εκπομπή του ενός θα έπεφτε πάνω στην εκπομπή των άλλων.

<u>Πρόσβαση των σταθμών στο φυσικό δίαυλο</u>

Ορίζονται δύο τρόποι πρόσβασης στο μέσο:

- DCF (Distribution Coordination Function) – Μηχανισμός Κατανεμημένου Συντονισμού

Αποτελείται βασικά από ένα μηχανισμό CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Σύμφωνα με αυτόν ένας σταθμός που επιθυμεί να εκπέμψει ανιχνεύει το ραδιοδίαυλο. Αν ο δίαυλος είναι ελεύθερος για ένα χρονικό διάστημα ο σταθμός εκπέμπει μετά από ένα τυχαίο χρονικό διάστημα. Χρησιμοποιείται επίσης ένας μηχανισμός επιβεβαίωσης λήψης. Αν ο αποστολέας δεν

δεχτεί το μήνυμα από το λήπτη θα υποθέσει ότι μία σύγκρουση πακέτων έγινε και θα γίνει επανεκπομπή του από το MAC επίπεδο.

- PCF (Point Coordination Function) – Μηχανισμός Σημειακού Συντονισμού

Προαιρετικός τρόπος πρόσβασης, χρησιμοποιείται για εφαρμογές πραγματικού χρόνου, όπου απαιτείται προνομιακή μεταχείριση έναντι της απλής μετάδοσης δεδομένων. Σε αυτό ρωτάται κάθε ένας σταθμός ξεχωριστά εάν έχει δεδομένα προς μετάδοση. Με αυτόν τον τρόπο ένας σταθμός μπορεί να αποκτήσει μεγαλύτερη προτεραιότητας πρόσβαση. Ο χρόνος μοιράζεται ανάμεσα στους δύο τρόπους πρόσβασης.

1.1.7.: WEP, Wired Equivalent Encryption

Αποσκοπεί να δώσει ένα ισοδύναμο βαθμό ασφαλείας με αυτόν ενός ενσύρματου δικτύου. Αποτελεί ένα στοιχειώδες μέτρο ασφαλείας σε ασύρματο δίκτυο. Ο χρήστης εισάγει το κλειδί κρυπτογράφησης που μπορεί να είναι 40-128bit. Το κλειδί αυτό χρησιμοποιείται για την αυθεντικοποίηση ασύρματων σταθμών που επιθυμούν να συνδεθούν και κατόπιν για την κρυπτογράφηση των δεδομένων. Το κλειδί κρυπτογράφησης είναι στατικό, με αποτέλεσμα αν κάποιος συλλέξει επαρκή αριθμό πακέτων να μπορεί να το βρει. Πρόσφατα, εγκρίθηκε το πρωτόκολλο CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) το οποίο χρησιμοποιεί τον αλγόριθμο AES για κρυπτογράφηση που είναι πολύ καλύτερο του RC4 που χρησιμοποιείται μέχρι τώρα. Το μειονέκτημα είναι ότι απαιτεί μεγαλύτερη επεξεργαστική ισχύ.

1.2.: ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ ΠΑΝΩ ΣΤΟ 802.11 ΠΡΩΤΟΚΟΛΛΟ

1.2.1. : Γενικά για τα πρωτόκολλα

Η πρόοδος στον τομέα των τηλεπικοινωνιών και της ψηφιακής επεξεργασίας σήματος μας έχει επιτρέψει να διακινούμε δεδομένα με ρυθμούς Gbps

(Δισεκατομύρια bit ανά δευτερόλεπτο) τόσο με ενσύρματες , όσο και με ασύρματες ζεύξεις. Η διαδικτύωση που συντελείται σήμερα μας επιτρέπει να ισχυριστούμε ότι σε μερικά χρόνια δεν θα υπάρχει αστική περιοχή χωρίς πρόσβαση στο διαδίκτυο. Για την καλύτερη κάλυψη των αναγκών των χρηστών σε ασύρματη επικοινωνία έχουν αναπτυχθεί διάφορα πρότυπα ασύρματης επικοινωνίας. Ενδεικτικά, αλλά όχι μόνο, έχουμε το Bluetooth, 802.11, GPRS/UMTS. Αυτά τα πρότυπα διαφέρουν στην περιοχή κάλυψης και στο ρυθμό μετάδοσης δεδομένων.

Αξίζει να αναφερθούμε στα δίκτυα WLAN . Τα δίκτυα WLAN λειτουργούν σύμφωνα με το πρότυπο 802.11 και έχουν το πλεονέκτημα ότι συνδυάζουν υψηλές ταχύτητες πρόσβασης με ικανοποιητική εμβέλεια κάλυψης. Ένας αρκετά σημαντικός τομέας είναι το AAA (authentication, authorization, accounting). Είναι δεόντως σημαντικό για ένα οποιοδήποτε δίκτυο επικοινωνιών είναι να έχει τα μέσα για να πιστοποιεί τους χρήστες που πρέπει, να τους εξουσιοδοτεί με τα κατάλληλα δικαιώματα και να έχει στατιστικά στοιχεία ώστε να μπορεί να διενεργήσει στατιστική ανάλυση των δεδομένων και να εφαρμόσει μοντέλο χρέωσης.

1.2.2. : Το πρωτόκολλο 802.11: Ιστορικά στοιχεία:

Το standard 802.11 είναι το πρώτο standard για WLAN (wireless local area network) και έως τώρα το μοναδικό που βρίσκεται στην αγορά. Η υλοποίηση του standard ξεκίνησε το 1987 σαν μέρος του IEEE 802.4 token bus standard με τον αριθμό γκρουπ IEEE 802.4L. Το IEEE 802.4 πρωτόκολλο είναι το αντίστοιχο των IEEE 802.3 και IEEE 802.5 τα οποία έχουν σχεδιαστεί με γνώμονα το βιομηχανικό περιβάλλον. Ένα από τα βασικά κίνητρα για την ανάπτυξη των WLAN's ήταν για να χρησιμοποιηθούν από τη βιομηχανία στην επικοινωνία μεταξύ διαφόρων μηχανημάτων. Για αυτό το λόγο μεγάλες εταιρείες όπως η GM (General Motors) συμμετείχαν ενεργά στην ανάπτυξη του 802.4L ειδικά κατά τα πρώτα στάδια της ανάπτυξης του. Το 1990 η ομάδα εργασίας του 802.4L μετονομάστηκε σε IEEE 802.11 δημιουργώντας ένα ανεξάρτητο 802.11 standard ώστε να ορίσει το φυσικό στρώμα και το MAC στρώμα για WLAN's. Το πρώτο IEEE 802.11 standard για ταχύτητες 1 και 2 Mbps ολοκληρώθηκε το 1997 υποστηρίζοντας DSSS , FHSS και φυσικό στρώμα διάχυτων υπέρυθρων ακτίνων (DFIR). Από την ολοκλήρωση αυτού

του standard , καινούργιες υλοποιήσεις του φυσικού στρώματος που υποστηρίζουν 11Mbps χρησιμοποιώντας CCK (IEEE 802.11b) και 54Mbps χρησιμοποιώντας ODFM (IEEE 802.11a) έχουν υλοποιηθεί. Και οι τρεις αυτές εκδόσεις του 802.11 μοιράζονται το ίδιο στρώμα MAC που χρησιμοποιεί CSMA/CA για αποθήκευση δεδομένων , μηχανισμό αίτησης αποστολής / αποδεκτής αποστολής (RTS/CTS) για να προσπεράσουν το πρόβλημα κρυμμένου τερματικού και έναν προαιρετικό μηχανισμό που λέγεται λειτουργία συντονισμού σημείων (PCF) για να υποστηρίξει εφαρμογές ευαίσθητες στην απόκριση χρόνου. Το IEEE 802.11 standard υποστηρίζει τόσο WLAN's βασισμένα στη λογική του πελάτη – εξυπηρετητή όσο και ad hoc δίκτυα με ισότιμους peers.

Το IEEE 802.11 standard ήταν το πρώτο standard ασύρματων δικτύων που είχε να αντιμετωπίσει την πρόκληση να ορίσει ένα συστηματικό standard για ασύρματα ευρυζωνικά δίκτυα. Σε σύγκριση με τα ενσύρματα δίκτυα τύπου LAN, τα WLANs λειτουργούν κάτω από αντίξοες συνθήκες μέσου μεταφοράς (αέρας) και έχουν μεγάλες απαιτήσεις σε φορητότητα και ασφάλεια. Το ασύρματο μέσο μεταφοράς έχει μεγάλους περιορισμούς στο εύρος ζώνης και περιοριστικούς κανονισμούς όσον αφορά τις συχνότητες που μπορεί να χρησιμοποιήσει. Επιπλέον , έχει το πρόβλημα της παρεμβολής από ανακλάσεις του σήματος (multipath fading). Το WLAN υπόκειται σε παρεμβολές από άλλα γειτονικά WLANs ή γενικά συσκευές ραδιοεπικοινωνίας ή μη (φούρνοι μικροκυμάτων , παλιά ασύρματα τηλέφωνα). Τα standard ασύρματης επικοινωνίας πρέπει να είναι σχεδιασμένα ώστε να υποστηρίζουν φορητότητα του χρήστη, χαρακτηριστικό που δεν υποστηρίζεται από κανένα άλλο standard τύπου LAN. Η ομάδα εργασίας του IEEE 802.11 έπρεπε να εξετάσει τη διαχείριση σύνδεσης, διαχείριση διασφάλισης σταθερότητας της σύνδεσης και διαχείριση εξοικονόμησης ενέργειας, κανένα από αυτά δεν υφίσταται σε κάποιο άλλο πρωτόκολλο της σειράς 802. Επίσης τα WLANs δεν έχουν φυσικά όρια (όριο του WLAN είναι τα σημεία όπου εξασθενεί τόσο το σήμα ώστε να είναι αδύνατη η πρόσβαση σε αυτό) και συνήθως επικαλύπτονται με γειτονικά WLANs έτσι η ομάδα που τυποποίησε τα standard έπρεπε να βρουν κάποιο τρόπο ώστε να οριστεί ένα ισχυρό επίπεδο ασφάλειας μεταξύ των ζεύξεων. Για όλους τους παραπάνω αναφερθέντες λόγους συν των διαφόρων ανταγωνιστικών standards χρειάστηκαν σχεδόν 10 χρόνια για την υλοποίηση του IEEE 802.11 χρόνος που είναι αρκετά μεγαλύτερος από αυτόν που απαιτήθηκε για άλλα standard τύπου 802 που

σχεδιάστηκαν για ενσύρματα μέσα. Μόλις παρουσιάστηκε το γενικό πλαίσιο χρειάστηκε αρκετά μικρότερος χρόνος για να αναπτυχθούν οι επεκτάσεις IEEE 802.11b και 802.11a .

1.2.3. : Προδιαγραφές 802.11

Το πρωτόκολλο 802.11 υποστηρίζει ρυθμούς μετάδοσης δεδομένων της τάξεως των 1Mbps και 2Mbps. Η μετάδοση του σήματος γίνεται είτε στην ISM ζώνη συχνοτήτων (2.4GHz – 2.4835GHz), είτε με υπέρυθρη ακτινοβολία μήκους κύματος 850nm. Για τη μετάδοση του σήματος στην ISM ζώνη χρησιμοποιείται διαμόρφωση FSK 2 – επιπέδων για ρυθμούς 1Mbps και FSK 4 – επιπέδων για ρυθμούς 2Mbps. Για την επικοινωνία μέσω υπερύθρων χρησιμοποιείται διαμόρφωση PPM (Pulse Position Modulation). Για μεγαλύτερη ανθεκτικότητα στον θόρυβο στενής ζώνης το σήμα κωδικοποιείται με μεθόδους απλωμένου φάσματος. Το πρωτόκολλο υποστηρίζει την μέθοδο εναλλαγής συχνότητας (FHSS) και ευθείας ακολουθίας (DSSS) για αυτό το σκοπό. Η μέγιστη εκπεμπόμενη ισχύς καθορίζεται από τους περιορισμούς που υπάρχουν για την χρήση της ISM ζώνης συχνοτήτων και περιορίζεται στα 20dBm ενώ η ευαισθησία του δέκτη, ορίζεται από το πρωτόκολλο, ότι πρέπει να είναι μικρότερη ή ίση των –80dBm για FER της τάξης του 3%.

1.2.4. IEEE 802.11b

Αναπτύχθηκε το 1999 και αποτελεί μια επέκταση στο αρχικό πρότυπο. Συγκεκριμένα υποστηρίζει μετάδοση επιπλέον σε ρυθμούς 5.5 και 11Mbps. Η μετάδοση γίνεται στη ζώνη συχνοτήτων των 2.4GHz. Είναι το πιο δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, όντας ένα αποτελεσματικό και δοκιμασμένο πρότυπο. Οι προσθήκες της 802.11b σε σχέση με την 802.11 αφορούν μόνο τον τρόπο μετάδοσης, ενώ ο τρόπος πρόσβασης των συσκευών και οι τρόποι λειτουργίας μένουν οι ίδιοι. Μία συσκευή που εργάζεται ακολουθώντας το 802.11b, υλοποιεί και τους τρόπους μετάδοσης του 802.11 και έτσι

είναι προς τα πίσω συμβατή με αυτό. Αυτή η ιδιότητα είναι σημαντική καθώς ο καταναλωτής δεν είναι αναγκασμένος να αλλάξει εξ ολοκλήρου τον εξοπλισμό του.

1.2.5. IEEE 802.11a

Το 1999 δημιουργήθηκε η επέκταση στο αρχικό πρότυπο που προβλέπει μετάδοση στη ζώνη συχνοτήτων των 5GHz με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας OFDM (Orthogonal Frequency Division Multiplexing) διαμόρφωση.

Η επέκταση αυτή αποσκοπούσε να καλύψει την ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Επιλέχθηκε η λειτουργία σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να μπορούν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί, αφετέρου ώστε να μην υπάρχει παρεμβολή από τις προηγούμενες συσκευές. Οι αντίστοιχες συσκευές είναι ασύμβατες με αυτές που εργάζονται με το 802.11b, αφού ο τρόπος μετάδοσης, αλλά και οι ραδιοσυχνότητες που χρησιμοποιούνται είναι διαφορετικές.

1.2.6.: IEEE 802.11g

Το 802.11g αποτελεί επέκταση στο 802.11b ώστε να υποστηρίζει μεγαλύτερους ρυθμούς. Έτσι εκτός από τους ρυθμούς μετάδοσης του 802.11b, υποστηρίζει και ρυθμούς μέχρι 54Mbps χρησιμοποιώντας OFDM διαμόρφωση. Οι αντίστοιχες συσκευές εργάζονται στη ζώνη συχνοτήτων των 2.4GHz, διατηρώντας συμβατότητα προς τα πίσω με το 802.11b.

ΚΕΦΑΛΑΙΟ 2: ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

2.1.: ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΚΙΝΗΤΗΣ

Οι υπηρεσίες που υποστηρίζονται από τα δίκτυα κινητών επικοινωνιών περιορίζονται από το ρυθμό μετάδοσης δεδομένων και από την ποιότητα της μετάδοσης αυτής. Έτσι στην αρχή, όπου η ποιότητα των υπηρεσιών και οι ρυθμοί μετάδοσης ήταν ιδιαίτερα χαμηλοί, οι συμπληρωματικές υπηρεσίες ήταν πολύ λίγες. Με την βελτίωση όμως των δύο αυτών παραγόντων, προκύπτει διαρκώς αυξανόμενη ζήτηση για νέες υπηρεσίες. Οι υπηρεσίες αυτές μπορούν να κατηγοριοποιηθούν σε τρεις μεγάλες κατηγορίες, αυτές με στόχο τις κοινωνικές επικοινωνίες και την ασφάλεια (όπως η βιντεοτηλεφωνία, η αποστολή φωτογραφιών, η γνωστοποίηση συναγερμών, ο εντοπισμός επείγοντος περιστατικού και άλλες), αυτές με σκοπό την εξοικονόμηση χρόνου και εξουσιοδότησης (όπως οι ηλεκτρονικές αγορές, οι ηλεκτρονικές τραπεζικές συναλλαγές, η αναζήτηση πληροφοριών στο διαδίκτυο, οι ηλεκτρονικές ειδήσεις, ο έλεγχος της κατοικίας, η πλοήγηση και άλλες) και αυτές για διασκέδαση (όπως τα ηλεκτρονικά στοιχήματα, τα διαδραστικά παιχνίδια, ηηλεκτρονική ενημέρωση για χόμπυ και άλλες). Η χρονική κατηγοριοποίηση των υπηρεσιών αυτών ανά περίοδο παρουσιάζεται συνοπτικά στη συνέχεια.

2.2.1: Υπηρεσίες πρώτης γενιάς

Στις υπηρεσίες πρώτης γενιάς (1G), μπορεί να συμπεριληφθεί μόνο η Υπηρεσία Φωνής και αυτή με ιδιαίτερα προβλήματα (συχνή διακοπή κλήσεων κατά την μετάβαση του χρήστη από τον χώρο κάλυψης μίας κυψέλης σε αυτόν μίας άλλης).

2.2.2: Υπηρεσίες δεύτερης γενιάς

Όσον αφορά τη δεύτερη γενιά υπηρεσιών (2G), με την πλήρη ψηφιακοποίηση των συστημάτων, έχουμε την βελτίωση της Υπηρεσίας Φωνής και την έλευση της

επαναστατικής Υπηρεσίας Σύντομων Μηνυμάτων (SMS). Η υπηρεσία αυτή χαρακτηρίζεται από το γεγονός ότι δεν απαιτεί σύνδεση από άκρη σε άκρη και επιτρέπει ανταλλαγή αλφαριθμητικών, περιορισμένου μεγέθους, μεταξύ των χρηστών. Τα μηνύματα αποθηκεύονται προσωρινά στο δίκτυο μέχρι να παραληφθούν από τους αποδέκτες τους. Ενώ αρχικά είχε δημιουργηθεί για να ενημερώνει τον χρήστη για φωνητικά μηνύματα, χρησιμοποιήθηκε για λόγους επικοινωνίας. Εξαιτίας της ζήτησης αυτής και της ανάγκης για πιο γρήγορη ανταλλαγή μηνυμάτων, αναπτύχθηκε η Βελτιωμένη Υπηρεσία Μηνυμάτων (EMS). Επιπλέον του αλφαριθμητικού, υποστηριζόταν και η αποστολή μικρών εικόνων και μελωδιών κλήσεων. Ο ρυθμός μετάδοσης δεδομένων στα 2G συστήματα, περιόριζε τις υπηρεσίες σε αυτό το μικρό αριθμό.

Με την έλευση των GPRS συστημάτων (2.5G) και τη βελτίωση του ρυθμού μετάδοσης, έχουμε για πρώτη φορά την Υπηρεσία Μηνυμάτων Πολυμέσων (MMS). Η υπηρεσία αυτή είναι βελτιωμένη έκδοση των προηγουμένων SMS και EMS υπηρεσιών αποστολής μηνυμάτων, με επιπλέον δυνατότητα την αποστολή εικόνων μεγαλύτερου μεγέθους, ήχων και βίντεο. Στην ίδια χρονική περίοδο έκαναν την εμφάνισή τους πρόδρομοι της Υπηρεσίας Ηλεκτρονικού Ταχυδρομείου (e-mail) για τον έλεγχο της ηλεκτρονικής αλληλογραφίας από το κινητό.

2.2.3: Υπηρεσίες τρίτης γενιάς

Η πραγματική επανάσταση στις υπηρεσίες όμως, ήρθε με τα συστήματα τρίτης γενιάς (3G). Λόγω του αρκετά υψηλού ρυθμού μετάδοσης και τη σαφή βελτίωση της ποιότητας των υπηρεσιών, έχουμε την εμφάνιση υπηρεσιών υψηλών απαιτήσεων. Η υπηρεσία Βίντεο Κλήσεων και υπηρεσίες αναπαραγωγής βίντεο σε πραγματικό χρόνο γίνονται πλέον πραγματικότητα και δίνουν τη δυνατότητα στον χρήστη να επικοινωνεί ζωντανά (με εικόνα) με απομακρυσμένους χρήστες αλλά και να ανταλλάσσει εκτός από εικόνες και βίντεο. Με την άφιξη των υπηρεσιών αυτών έγινε και η προσθήκη σε 3G συσκευές, ψηφιακής φωτογραφικής μηχανής, κάμερας και λογισμικών επεξεργασίας εικόνων και βίντεο. Την ίδια πορεία ακολούθησαν και οι υπηρεσίες αναπαραγωγής ήχου σε πραγματικό χρόνο καταλήγοντας στην

προσθήκη ραδιοφώνου στις κινητές συσκευές αλλά και λογισμικών επεξεργασίας ήχου και μελωδιών.

Από την πρώτη έκδοση του UMTS (Universal Mobile Telecommunications System release 99) έχουμε την εμφάνιση των υπηρεσιών θέσης (Location Based Services). Οι υπηρεσίες αυτές παρέχονται στους χρήστες των δικτύων κινητών και προσωπικών επικοινωνιών και η πληροφορία θέσης του χρήστη χρησιμοποιείται και προσθέσει αξία στις υπηρεσίες συνολικά. Η πληροφορία για τη θέση, αποτελείται από χωρικές συντεταγμένες X-Y που παράγονται από τις διάφορες τεχνολογίες εντοπισμού ή μπορεί και να εισάγεται από τον χρήστη ή το τερματικό αυτού. Το βήμα αυτό, έδωσε την δυνατότητα για την δημιουργία μια σειράς από νέες πρωτοποριακές υπηρεσίες οι οποίες μπορούν να κατηγοριοποιηθούν σε υπηρεσίες τοπικής πληροφόρησης (χρέωση κλήσης ανά περιοχή, τοπικός χρυσός οδηγός, πληροφορίες για τουριστικά μέρη, πληροφορίες για εστιατόρια και κινηματογράφους, τοπικά νέα και άλλα), σε υπηρεσίες προσανατολισμού και δρομολόγησης (ενημέρωση παρούσας κίνησης, επιλογή συντομότερης διαδρομής, καθοδήγηση δρομολογίου και άλλα), σε υπηρεσίες εμπορίου (κουπόνια από κοντινά καταστήματα, τοπικές ειδικές προσφορές και άλλα), σε υπηρεσίες για την ασφάλεια (έλεγχος θέσης οικογένειας, έλεγχος θέσης αυτοκινήτου και άλλα), σε υπηρεσίες διαχείρισης πόρων (διαχείριση προσωπικού, διαχείριση οχημάτων και άλλα), σε κοινωνικές υπηρεσίες και υπηρεσίες παιχνιδιών (αλληλοδραστικά παιχνίδια, αλληλεπίδραση με κοντινά στον χρήστη άτομα και άλλα) και σε υπηρεσίες έκτατης ανάγκης (προσδιορισμός θέσης σε επείγουσα κλήση, υπηρεσία E-911 και άλλα).

Η τελευταία έκδοση του UMTS περιλάμβανε την υπηρεσία ασύρματου δικτύου (WLAN) που παρέχει υψηλής ταχύτητας ασύρματη πρόσβαση στον παγκόσμιο ιστό (Internet). Με αφορμή την πρόσβαση στον παγκόσμιο ιστό, τελειοποιείται η υπηρεσία ηλεκτρονικού ταχυδρομείου (e-mail) και δόθηκε το έναυσμα για τη δημιουργία υπηρεσιών ηλεκτρονικού εμπορίου, υπηρεσιών τηλεμάθησης και υπηρεσιών διαδραστικών παιχνιδιών, εκμεταλλεύοντας την ασύρματη πρόσβαση στο διαδίκτυο.

Οι τελευταίες υπηρεσίες που έκαναν την εμφάνιση τους στη συγκεκριμένη περίοδο, είναι αυτές που συνδυάζουν περισσότερες από μία, ήδη υπάρχουσες, υπηρεσίες. Μια τέτοια κατηγορία υπηρεσιών, είναι οι υπηρεσίες εικονικών κοινοτήτων, οι οποίες αναμένεται να αποτελέσουν επέκταση των φυσικών

κοινοτήτων. Οι υπηρεσίες αυτές μπορούν να κατανοηθούν ως εικονικές κοινότητες στις οποίες προστίθενται οι υπηρεσίες κινητών επικοινωνιών. Στις υπηρεσίες αυτές ένα τερματικό μπορεί να δράσει τόσο ως αποδέκτης πληροφοριών όσο και ως αποστολέας αξιοποιώντας μία από τις υπάρχουσες τεχνολογίες σύνδεσης με άλλα τερματικά (WAN, SMS, MMS κ.ά.). Με τον τρόπο αυτό, δημιουργούνται κοινότητες από άτομα με κοινά ενδιαφέροντα, κοινή κατάσταση ή κοινή πορεία και με χρήση των υπηρεσιών αυτών, μπορούν να ανταλλάσσουν δεδομένα, πληροφορίες και οτιδήποτε άλλο, οποτεδήποτε.

Παρεμφερείς με τις υπηρεσίες κοινοτήτων είναι οι ανώνυμες υπηρεσίες. Οι υπηρεσίες αυτές κάνουν χρήση διαφόρων πληροφοριών που παρέχονται από το λογισμικό συσκευών τρίτης γενιάς και αξιοποιούν την πληροφορία αυτή σε άλλες υπάρχουσες υπηρεσίες (υπηρεσίες θερμοκρασίας ανά περιοχή, υπηρεσίες εύρεσης κυκλοφοριακής συμφόρησης ανά περιοχή και άλλες). Στις υπηρεσίες αυτές η πληροφορία δίνεται ανώνυμα από τερματικά που τυχαία βρίσκονται στην περιοχή ενδιαφέροντος μιας υπηρεσίας και προφανώς οι χρήστες των τερματικών αποδέχονται την ανάκτηση πληροφοριών από αυτούς.

2.2.4.: Τεχνολογία 3G - UMTS

Τα 3G συστήματα σχεδιάστηκαν να παρέχουν παγκοσμίως την δυνατότητα πραγματοποίησης πολλών εφαρμογών, όπως τηλεφωνία, αναζήτηση (paging) χρήστη, εφαρμογές σχετικά με μηνύματα, internet, broadband δεδομένα. Η διεθνής ένωση τηλεπικοινωνιών (International Telecommunication Union - ITU) ξεκίνησε την διαδικασία ορισμού του προτύπου για τα συστήματα 3ης γενιάς, αναφερόμενο ως International Mobile Telecommunications 2000 (IMT-2000). Στην Ευρώπη το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI: European Telecommunications Standards Institute) ήταν υπεύθυνο για την διαδικασία προτυποποίησης του UMTS. Το 1998 το 3GPP (Third Generation Partnership Project) ανέλαβε να συνεχίσει τις τεχνικές προδιαγραφές. Το 3GPP έχει πέντε κύριες περιοχές προτυποποίησης σχετικά με το UMTS: δίκτυο ασύρματης πρόσβασης(Radio Access Network), δίκτυο κορμού (Core Network), τερματικά (Terminals), θέματα υπηρεσιών και συστήματος.

UMTS υπηρεσίες

Το UMTS προσφέρει τηλεϋπηρεσίες (όπως ομιλία ή SMS) και άλλες υπηρεσίες φορέα, οι οποίες παρέχουν την δυνατότητα για μεταφορά πληροφοριών μεταξύ σημείων πρόσβασης.

Υπηρεσίες φορέα έχουν διαφορετικούς παράγοντες σχετικά με την ποιότητα της υπηρεσίας QoS (quality of service), τον ρυθμό μετάδοσης δεδομένων, τον χρόνο καθυστέρησης και το ρυθμό bit σφάλματος (bit error rate BER). Οι ρυθμοί δεδομένων είναι:

- 144 kbits/s σε αγροτικούς και δορυφορικούς
- 384 kbits/s σε αστικούς εξωτερικούς χώρους
- 2048 kbits/s σε εσωτερικούς χώρους και σε μικρούς εξωτερικούς χώρους

Οι υπηρεσίες με χρήση δικτύου UMTS ανήκουν σε διαφορετικές κλάσεις ποιότητας υπηρεσίας Qos (traffic classes). Αυτές είναι:

- συζητητική κλάση (conversational class: voice, video telephony, video gaming)
- streaming κλάση (multimedia, video on demand, webcast)
- διαδραστική κλάση (interactive class: web browsing, network gaming, database access)
- background κλάση (email, SMS, downloading)

Το UMTS βελτίωσε την ασφάλεια δικτύων και τις υπηρεσίες βασιζόμενες στην θέση των κινητών τερματικών.

Αρχιτεκτονική UMTS

Το δίκτυο UMTS αποτελείται από τρεις αλληλεπιδρώμενους τομείς:

- Δίκτυο κορμού (Core Network - CN)
- UMTS επίγειο δίκτυο ασύρματης πρόσβασης (UMTS Terrestrial Radio Access Network - UTRAN)
- Εξοπλισμός χρήστη (User Equipment - UE)

2.2.4: Υπηρεσίες τέταρτης γενιάς

Τα συστήματα τέταρτης γενιάς (4G), είναι υπό έρευνα IP-προσανατολισμένες υπηρεσίες πολυμέσων (IMS), υπηρεσίες τηλεοπτικής κάλυψης σε κινητά, υπηρεσίες

υψηλών απαιτήσεων βίντεο εφαρμογών και η επέκταση των υπαρχόντων υπηρεσιών με αυξημένη ζήτηση όπως αυτή των εικονικών κοινοτήτων και άλλων, βασισμένων στη θέση του χρήστη, υπηρεσιών.

Τι δυνατότητες προσφέρει το 4G δίκτυο;

Το δίκτυο 4ης γενιάς τεχνολογίας LTE (Long Term Evolution) βελτιώνει σημαντικά την εμπειρία των πελατών, παρέχοντας:

- Πολλαπλάσιες ταχύτητες πλοήγησης στο διαδίκτυο
- Χρήση προηγμένων multimedia εφαρμογών όπως HD Streaming και HD Video Conferencing
- Ταχύτατη αποστολή και λήψη μεγάλων αρχείων

Οι ταχύτητες είναι τέτοιες, που κατά μέσο όρο οι χρήστες μπορούν να κατεβάσουν μια ταινία HD μόλις σε 2-3 λεπτά!

Το δίκτυο 4G τεχνολογίας LTE (Long Term Evolution) προσφέρει μοναδική εμπειρία στο χρήστη με περισσότερο από 4 φορές υψηλότερη μέση ταχύτητα από το δίκτυο 3G.

Η μέση ταχύτητα πρόσβασης μέσω του δικτύου 3G της είναι περίπου 8 Mbps για την Ελλάδα. *(Τα στοιχεία αυτά πιστοποιούνται από τις πρόσφατες έρευνες των ανεξάρτητων εταιρειών, LCC και Commsquare, οι οποίες διενεργήθηκαν από το 4ο 3μηνο του 2011 έως και το Νοέμβριο του 2012.)*

Η ταχύτητα μετάδοσης δεδομένων εξαρτάται από τον τερματικό εξοπλισμό του χρήστη, την περιοχή που βρίσκεται ο συνδρομητής όπως επίσης και το πλήθος των συνδρομητών που κάνουν ταυτόχρονη χρήση στην περιοχή κάλυψης.

ΚΕΦΑΛΑΙΟ 3: GSM

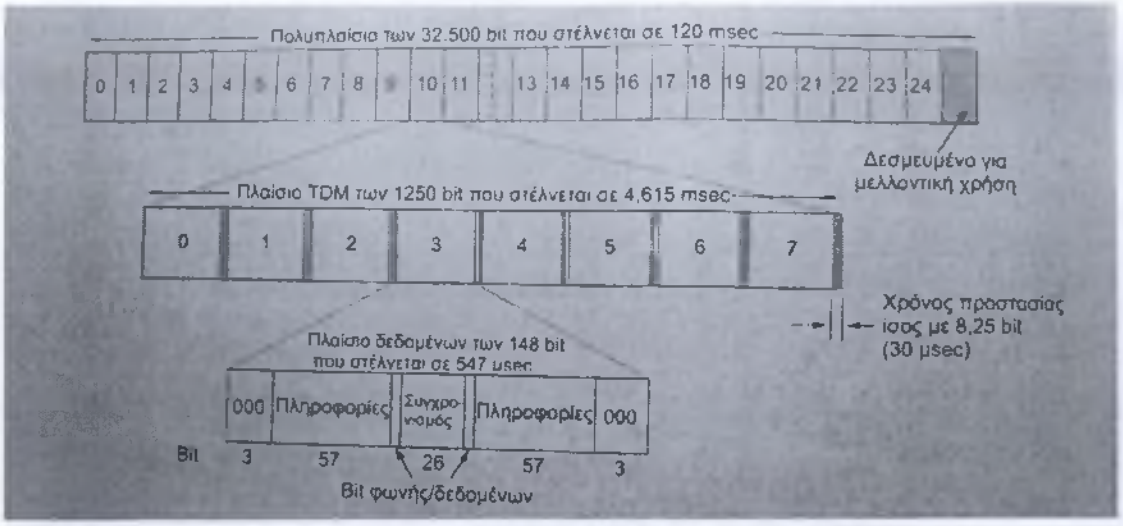
3.1. GSM: ΤΟ ΠΑΓΚΟΣΜΙΟ ΣΥΣΤΗΜΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Σχεδόν σε όλο τον κόσμο εκτός από την Ιαπωνία χρησιμοποιείται ένα σύστημα που ονομάζεται Παγκόσμιο Σύστημα Κινητών Επικοινωνιών ή GSM (Global System for Mobile Communications) το οποίο έχει αρχίσει να χρησιμοποιείται ακόμη και στις Η.Π.Α. σε περιορισμένη κλίμακα. Σε μια πρώτη προσέγγιση, το GSM είναι ένα κυψελωτό σύστημα. Χρησιμοποιείται πολυπλεξία με διαίρεση συχνότητας με κάθε κινητό να μεταδίδει σε μία συχνότητα και να λαμβάνει σε μία υψηλότερη συχνότητα (55 MHz παραπάνω για το GSM). Ένα ζεύγος συχνοτήτων διασπάται σε χρονικές υποδοχές που μοιράζονται σε περισσότερα από ένα κινητά, με πολυπλεξία με διαίρεση χρόνου. Τα κανάλια όμως του GSM παρουσιάζουν αρκετά μεγάλο εύρος (200kHz) παρέχοντας έτσι στο GSM πολύ υψηλό ρυθμό μετάδοσης δεδομένων ανά χρήστη.

Αξίζει να αναφέρουμε ότι μία ζώνη συχνοτήτων έχει εύρος 200 kHz όπως φαίνεται στην παρακάτω εικόνα. Ένα σύστημα GSM έχει 124 ζεύγη μονόδρομων καναλιών. Κάθε μονόδρομο κανάλι έχει εύρος 200 kHz και υποστηρίζει οκτώ χωριστές συνδέσεις χρησιμοποιώντας πολυπλεξία με διαίρεση χρόνου. Σε κάθε σταθμό που είναι τη δεδομένη στιγμή ενεργός εκχωρείται μια χρονική υποδοχή σε ένα ζεύγος καναλιών. Θεωρητικά μπορούν να υποστηριχθούν 992 κανάλια σε κάθε κυψέλη, πολλά όμως από αυτά δεν είναι διαθέσιμα, έτσι ώστε να αποφεύγονται οι διενέξεις συχνοτήτων με τις γειτονικές κυψέλες. Στην παρακάτω εικόνα οι οκτώ σκιασμένες χρονικές υποδοχές ανήκουν όλες στην ίδια σύνδεση, τέσσερις προς κάθε κατεύθυνση. Η μετάδοση και η λήψη δεν πραγματοποιούνται στην ίδια χρονική υποδοχή, επειδή οι πομποδέκτες του GSM δεν μπορούν ταυτόχρονα να μεταδίδουν και να λαμβάνουν και χρειάζονται χρόνο για να αλλάξουν κατάσταση. Αν ο κινητός σταθμός στον οποίο έχει εκχωρηθεί το ζεύγος συχνοτήτων 890,4/935,4 MHz και η χρονική υποδοχή 2 ήθελε να μεταδώσει προς το σταθμό βάσης, θα χρησιμοποιούσε τις τέσσερις χαμηλότερες σκιασμένες υποδοχές (καθώς και αυτές που ακολουθούν χρονικά), τοποθετώντας τα δεδομένα του σε κάθε υποδοχή μέχρι να σταλούν όλα τα δεδομένα.

Εικόνα 5: Το GSM χρησιμοποιεί 124 συχνότητες καναλιών, κάθε μία από τις οποίες χρησιμοποιεί ένα σύστημα TDM οκτώ υποδοχών.

Οι υποδοχές του TDM που φαίνονται στην παραπάνω εικόνα αποτελούν μέρος μιας πολύπλοκης ιεραρχίας πλαισίωσης. Κάθε υποδοχή TDM έχει μία συγκεκριμένη δομή, ενώ οι ομάδες πλαισίωσης TDM σχηματίζουν πολυπλαίσια (multiframes) επίσης με συγκεκριμένη δομή. Μια απλοποιημένη παραλλαγή της ιεραρχίας αυτής φαίνεται στην παρακάτω εικόνα. Στην εικόνα αυτή μπορούμε να δούμε ότι κάθε υποδοχή TDM αποτελείται από ένα πλαίσιο δεδομένων των 148 bit το οποίο καταλαμβάνει το κανάλι για 577 μsec (συμπεριλαμβανομένου ενός χρόνου προστασίας 30μsec μετά από κάθε υποδοχή). Κάθε πλαίσιο δεδομένων ξεκινά και τελειώνει με τρία bit 0, έτσι ώστε να διακρίνονται τα πλαίσια. Περιέχει επίσης δύο πεδία Πληροφοριών (Information) των 57 bit, με το καθένα να περιέχει ένα bit ελέγχου που δείχνει κατά πόσο το επόμενο πεδίο Πληροφοριών περιέχει φωνή ή δεδομένα. Ανάμεσα στα πεδία Πληροφοριών υπάρχει ένα πεδίο Συγχρονισμού των 26 bit, το οποίο χρησιμοποιείται από τον δέκτη για να συγχρονιστεί με τα όρια των πλαισίων του αποστολέα.



Εικόνα 6: Μέρος της δομής πλαισίωσης του GSM

Τα πλαίσια των δεδομένων μεταδίδονται σε 547 μsec, ο πομπός όμως μπορεί να στείλει ένα πλαίσιο δεδομένων μόνο κάθε 4,615 msec, αφού μοιράζεται το κανάλι με οκτώ άλλους σταθμούς. Αυτό δίνει μία μικτή ταχύτητα 33,854 kbps. Ωστόσο, η επιβάρυνση δαπανά μεγάλο ποσοστό του εύρους ζώνης, αφήνοντας τελικά ωφέλιμο φορτίο 24,7 kbps ανά χρήστη πριν τη διόρθωση σφαλμάτων. Μετά τη διόρθωση σφαλμάτων απομένουν 13 kbps για ομιλία παρέχοντας αρκετά καλή ποιότητα φωνής χρησιμοποιώντας όμως περισσότερο εύρος ζώνης.

Όπως μπορεί να φανεία από την παραπάνω εικόνα οκτώ πλαίσια δεδομένων σχηματίζουν ένα πλαίσιο TDM και 26 πλαίσια TDM σχηματίζουν ένα πολύπλάισιο διάρκειας 120 msec. Από τα 26 πλαίσια TDM ενός πολυπλαίσιου η υποδοχή 12 χρησιμοποιείται για έλεγχο και η υποδοχή είναι δεσμευμένη για μελλοντική χρήση, έτσι μένουν διαθέσιμες μόνο 24 υποδοχές για τους χρήστες.

Παρόλα αυτά εκτός από το πολυπλάισιο 26 υποδοχών όπως φαίνεαι στην παραπάνω εικόνα χρησιμοποιείται επίσης και ένα πολυπλαίσιο 51 υποδοχών. Μερικές από αυτές τις υποδοχές χρησιμοποιούνται για διάφορα κανάλια ελέγχου, τα οποία χρησιμεύουν στη διαχείριση του συστήματος. Το κανάλι ελέγχου εκπομπής (broadcast control channel) είναι μια συνεχής ροή εξόδου από τον σταθμό βάσης,η οποία περιέχει την ταυτότητα του σταθμού βάσης και την κατάσταση του καναλιού. Όλοι οι κινητοί σταθμοί παρακολουθούν την ισχύ του σήματος αυτού για να δουν αν έχουν μετακινηθεί σε μια νέα κυψέλη.

Το αφιερωμένο κανάλι ελέγχου (dedicated control channel) χρησιμοποιείται για ενημέρωση τοποθεσίας, καταχώριση και εγκαθίδρυση κλήσεων. Συγκεκριμένα, κάθε σταθμός βάης διατηρεί μια βάση δεδομένων με τους κινητούς σταθμούς που βρίσκονται την τρέχουσα στιγμή στη δικαιοδοσία του. Οι πληροφορίες που απαιτούνται για την τήρηση αυτής της βάσης δεδομένων στέλνονται στο αφιερωμένο κανάλι ελέγχου.

Τέλος υπάρχει το κοινό κανάλι ελέγχου (common control channel) το οποίο διαιρείται σε τρία λογικά υποκανάλια. Το πρώτο από αυτά τα υποκανάλια είναι το κανάλι ειδοποίησης (paging channel) το οποίο χρησιμοποιείται από το σταθμό βάσης για την ανακοίνωση εισερχόμενων κλήσεων. Κάθε κινητός σταθμός βάσης το παρακολουθεί συνεχώς για να εντοπίσει τυχόν κλήσεις στις οποίες θα πρέπει να απαντήσει. Το δεύτερο είναι το κανάλι τυχαίας προσπέλασης (random access channel) το οποίο επιτρέπει στους χρήστες να ζητούν να τους παραχωρηθεί μια υποδοχή στο αφιερωμένο κανάλι ελέγχου. Αν υπάρξει διένεξη σε δύο αιτήσεις, αυτές παραμορφώνονται και θα πρέπει να σταλούν ξανά. Χρησιμοποιώντας την υποδοχή στο αφιερωμένο κανάλι ελέγχου, ο σταθμός μπορεί στη συνέχεια να εγκαθιδρύσει μια κλήση. Η παραχώρηση της υποδοχής ανακοινώνεται στο τρίτο υποκανάλι, το κανάλι παραχώρησης πρόσβασης (access grant channel).

3.2. ΤΕΧΝΙΚΕΣ ΠΟΛΥΠΛΕΞΙΑΣ

- **Πολύπλεξη Διαίρεσης Συχνότητας (FDM: Frequency Division Multiplexing)**

Πρόκειται για την κλασική μέθοδο δημιουργίας καναλιών επικοινωνίας. Η FDM είναι μια μορφή πολυπλεξίας σήματος όπου πολλά σήματα βασικής ζώνης διαμορφώνουν διαφορετικά φέροντα κύματα σε διαφορετική συχνότητα και προστιθέμενα μαζί δημιουργούν ένα σύνθετο σήμα.

Οι κύριες φασματικές μπάντες που δημιουργούνται – για ανέβασμα και κατέβασμα δεδομένων – μπορούν περαιτέρω να διαιρεθούν σε μικρότερα κανάλια επικοινωνίας υψηλών ή χαμηλών ταχυτήτων. Ορισμένα υποκανάλια εξασφαλίζουν την χωρίς σφάλματα μετάδοση της φωνής (0 – 25 kHz), άλλα υποκανάλια

δεσμεύονται για τα δεδομένα αποστολής (ζώνη 25KHz με 138KHz) ενώ άλλα υποκανάλια δεσμεύονται για τα δεδομένα λήψης (ζώνη 138KHz έως 1.1MHz).

- **Πολύπλεξη Διαίρεσης Χρόνου (TDM, Time Division Multiplexing)**

Στην TDM, ο χρόνος μετάδοσης διαιρείται σε χρονικές θυρίδες ίσης διάρκειας και ο κάθε χρήστης μπορεί να χρησιμοποιήσει συγκεκριμένη χρονική θυρίδα για να εκπέμψει. Κατά τη διάρκεια της χρονικής θυρίδας, ο χρήστης έχει πρόσβαση σε όλο το διατιθέμενο εύρος ζώνης.

- **Πολύπλεξη Διαίρεσης Κώδικα (CDM, Code Division Multiplexing)**

Η Διαίρεση Πολύπλεξης Κώδικα (CDM) είναι μια τεχνική στην οποία κάθε κανάλι μεταδίδει τα δεδομένα του ως μια κωδικοποιημένη ακολουθία παλμών. Αυτή η κωδικοποιημένη μετάδοση τυπικά πραγματοποιείται με τη μετάδοση μιας μοναδικής χρονικά εξαρτημένης ακολουθίας παλμών, η οποία τοποθετείται μέσα στη μεταδιδόμενη πληροφορία και διαχωρίζει την κάθε ροή από τις υπόλοιπες που μπορεί να μεταδίδονται ταυτόχρονα στο ίδιο μέσο.

ΚΕΦΑΛΑΙΟ 4: ΚΡΥΠΤΟΓΡΑΦΙΑ, ΑΠΟΡΡΗΤΟ, ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

4.1 ΚΡΥΠΤΟΓΡΑΦΙΑ

4.1.1. Εισαγωγικά για την Κρυπτογραφία

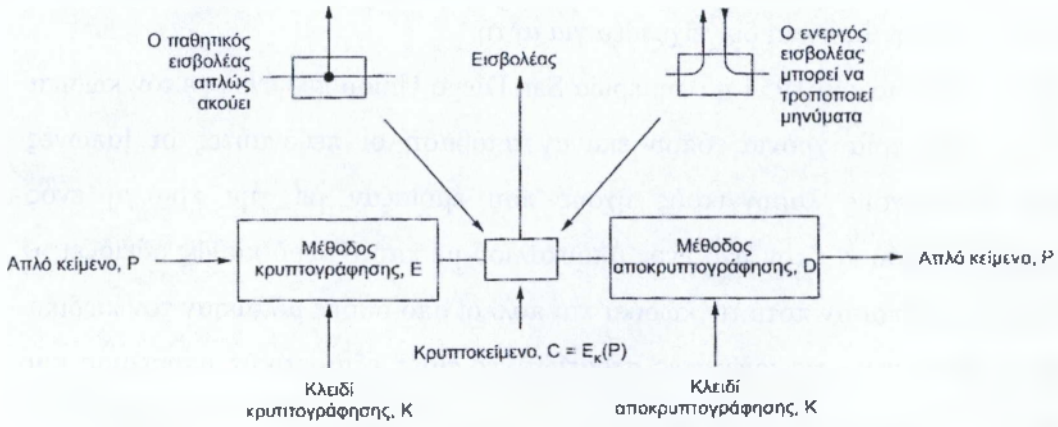
Η λέξη κρυπτογραφία (cryptography) προέρχεται από τις ελληνικές λέξεις «κρυφή γραφή». Έχει μεγάλη και εντυπωσιακή ιστορία που φτάνει χιλιάδες χρόνια πίσω. Οι επαγγελματίες κάνουν μία διάκριση ανάμεσα στην κρυπτογραφία και τους κώδικες. Η κρυπτογραφία ένας μετασχηματισμός χαρακτήρα προς χαρακτήρα ή bit προς bit, ο οποίος δεν ασχολείται με την γλωσσική δομή του μηνύματος. Αντίθετα, ο κώδικας (code) αντικαθιστά μία λέξη με μία άλλη λέξη ή ένα σύμβολο. Οι κώδικες δεν χρησιμοποιούνται πια αν και έχουν ένδοξη ιστορία. Ο πιο πετυχημένος κώδικας που επινοήθηκε ποτέ χρησιμοποιήθηκε από τις ένοπλες δυνάμεις των Η.Π.Α. κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου στον Ειρηνικό Ωκεανό.. Ο κώδικας χρησιμοποιούσε Ινδιάνους Ναβάχο οι οποίοι μιλούσαν μεταξύ τους χρησιμοποιώντας συγκεκριμένες λέξεις των Ναβάχο για τους στρατιωτικούς όρους. Η γλώσσα των Ναβάχο είναι ιδιαίτερα τονική, εξαιρετικά πολύπλοκη και δεν έχει γραπτή μορφή. Επίσης, κανείς στην Ιαπωνία δεν είχε ιδέα για αυτή.

Το Σεπτέμβριο του 1954 η εφημερίδα San Diego Union περιέγραψε τον κώδικα γράφοντας «Επί τρία χρόνια, όπου έκαναν απόβαση οι πεζοναύτες οι Ιάπωνες λάμβαναν περίεργους λαρυγγικούς ήχους που έμοιαζαν με την κραυγή ενός Θιβετιανού μοναχού και τον ήχο ενός μπουκαλιού με καυτό νερό καθώς αδειάζει ». Οι Ιάπωνες δεν έσπασαν ποτέ τιν κώδικα και πολλοί από όσους μιλούσαν τον κώδικα Ναβαχο τιμήθηκαν με τις ανώτατες στρατιωτικές τιμές εξαιρετικής υπηρεσίας και ανδρείας. Το γεγονός ότι οι Η.Π.Α. έσπασαν τον κώδικα των Ιαπώνων αλλά οι Ιάπωνες δεν έσπασαν ποτέ τον κώδικα Ναβαχο (Navajo) έπαιξε κρίσιμο ρόλο για τις αμερικανικές νίκες στον Ειρηνικό.

4.1.2. Λίγα λόγια για την κρυπτογραφία

Ιστορικά τέσσερις ομάδες ανθρώπων έχουν χρησιμοποιήσει και συνεισφέρει στην τέχνη της κρυπτογραφίας: ο στρατός, το διπλωματικό σώμα, όσοι τηρούν ημερολόγια και οι εραστές. Από όλους αυτούς τον πιο σημαντικό ρόλο τον είχε ο στρατός και ήταν εκείνος που διαμόρφωσε το συγκεκριμένο τομέα δια μέσου των αιώνων. Στους στρατιωτικούς οργανισμούς τα μηνύματα που πρέπει να κρυπτογραφηθούν δίνονται συνήθως σε χαμηλά αμειβόμενους κατώτερους υπαλλήλους κώδικα για κρυπτογράφηση και μετάδοση. Και μόνο ο όγκος των μηνυμάτων δεν επέτρεπε να πραγματοποιείται η δουλειά αυτή από μία ελίτ ειδικών.

Μέχρι την έλευση των υπολογιστών ένας από του κύριους περιορισμούς στην κρυπτογραφία ήταν η ικανότητα του υπαλλήλου κώδικα να εκτελεί τους απαιτούμενους μετασχηματισμούς συχνά στο πεδίο της μάχης και με λίγο εξοπλισμό. Ένας πρόσθετος περιορισμός ήταν η δυσκολία μετάβασης από μία κρυπτογραφική μέθοδο σε μία άλλη αφού κάτι τέτοιο απαιτεί εκ νέου εκπαίδευση μεγάλου πλήθους ανθρώπων. Ωστόσο, ο κίνδυνος να συλληφθεί ένας υπάλληλος κώδικα από τον εχθρό έκανε κρίσιμη τη δυνατότητα άμεσης αλλαγής της κρυπτογραφικής μεθόδου όταν κάτι τέτοιο χρειαζόταν. Έτσι δημιουργήθηκε το απλό μοντέλο της παρακάτω εικόνας.:



Εικόνα 7: Το μοντέλο της κρυπτογράφησης

Τα μοντέλα προς κρυπτογράφηση τα οποία αναφέρονται ωα απλό κείμενο μετασχηματίζονται από μία συνάρτηση που έχει ως παράμετρο ένα κλειδί. Στη συνέχεια η έξοδος της διαδικασίας κρυπτογράφησης που είναι γνωστή ως κρυπτοκείμενο μεταδίδεται συχνά με αγγελιοφόρο ή ραδιοκύματα. Υποθέτουμε ότι ο εχθρός ή ο εισβολέας ακούει και καταγράφει πιστά το πλήρες υποκείμενο. Ωστόσο, σε αντίθεση με τον επιθυμητό παραλήπτη δεν γνωρίζει ποιο είναι το κλειδί αποκρυπτογράφησης και έτσι δεν μπορεί να αποκρυπτογραφήσει εύκολα το κρυπτοκείμενο. Μερικές φορές ο εισβολέας μπορεί όχι μόνο να ακούει το κανάλι επικοινωνίας (παθητικός εισβολέας) αλλά και να καταγράφει τα μηνύματα και να τα αναπαράγει αργότερα, να εισάγει τα δικά του μηνύματα ή να τροποποιεί τα νόμιμα μηνύματα πριν φτάσουν στον παραλήπτη (ενεργός εισβολέας). Η τέχνη του σπασίματος των κρυπτογραφιών ονομάζεται κρυπτανάλυση (cryptanalysis) και η τέχνη της επινόησής τους (η κρυπτογραφία) είναι συλλογικά γνωστές ως κρυπτολογία (cryptology).

Θα χρησιμοποιούμε τον τύπο $C = E_K(P)$ για να δείχνουμε ότι η κρυπτογράφηση (encryption) του απλού κειμένου P με χρήση του κλειδιού K δίνει το κρυπτοκείμενο C. Παρόμοια το $P = D_K(C)$ παριστάνει την αποκρυπτογράφηση (decryption) του C για να λάβουν ξανά το απλό κείμενο. Συνεπώς, ισχύει ότι: $D_K(E_K(P)) = P$.

Η παράσταση αυτή υπονοεί ότι οι E και D είναι απλώς μαθηματικές συναρτήσεις. Το μόνο περίπλοκο σημείο είναι ότι και οι δυο είναι συναρτήσεις δύο παραμέτρων όπου έχουμε γράψει τη μία παράμετρο (το κλειδί) ως δείκτη και όχι ως παράμετρο ώστε να τη διακρίνουμε από το μήνυμα.

Ένας θεμελιώδης κανόνας κρυπτογραφίας είναι ότι πρέπει πάντα να υποθέτουμε ότι ο κρυπταναλυτής γνωρίζει μεθόδους που χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση. Με άλλα λόγια ο κρυπταναλυτής γνωρίζει ακριβώς πως λειτουργεί η μέθοδος κρυπτογράφησης E και η μέθοδος αποκρυπτογράφησης D. Η ποσότητα προσπάθειας που απαιτείται για την εφεύρεση, τη δοκιμή και την εγκατάσταση ενός νέου αλγορίθμου κάθε φορά που αποκαλύπτεται η παλιά μέθοδος έκανε πάντα μη πρακτική τη διατήρηση του αλγορίθμου κρυπτογράφησης μυστικού. Η εντύπωση ότι ο αλγόριθμος είναι μυστικός ενώ δεν είναι κάνει περισσότερο κακό παρά καλό.

Εδώ είναι που χρειάζεται το κλειδί. Το κλειδί είναι ένα σχετικά σύντομο αλφάβητο που επιλέγει μία από πολλές πιθανές κρυπτογραφήσεις. Σε αντίθεση με τη γενική μέθοδο η οποία μπορεί να αλλάζει μόνο κάποια χρονιά το κλειδί μπορεί να αλλάζει όσο συχνά απαιτείται. Άρα, το βασικό μοντέλο είναι μια σταθερή και δημόσια γνωστή γενική μέθοδος η οποία είναι παραμετροποιημένη από ένα μυστικό και εύκολα μεταβαλλόμενο κλειδί. Η ιδέα ότι ο κρυπταναλυτής γνωρίζει τους αλγορίθμους και ότι η μυστικότητα έγκειται αποκλειστικά στα κλειδιά ονομάζεται αρχή του Kerckhoff. Έτσι έχουμε:

Αρχή του Kerckhoff: «Όλοι οι αλγόριθμοι πρέπει να είναι δημόσιοι, μόνο τα κλειδιά είναι μυστικά.»

Η μη μυστικότητα του αλγορίθμου πρέπει να τονιστεί. Η προσπάθεια να . κρατηθεί κρυφός ο αλγόριθμος η οποία είναι γνωστή ως ασφάλεια μέσω ασάφειας δεν λειτουργεί ποτέ. Ένας αλγόριθμος θεωρείται αρκετά ανθεκτικός αν επί πέντε χρόνια μετά τη δημοσίευσή του κανείς δεν έχει καταφέρει να τον σπάσει.

Η πραγματική μυστικότητα έγκειται στο κλειδί. Επομένως το μήκος του κλειδιού είναι ένα βασικό σχεδιαστικό σύστημα. Όσο μεγαλύτερο είναι το μήκος τους κλειδιού τόσο υψηλότερος είναι ο παράγοντας εργασίας που πρέπει να αντιμετωπίσει ο κρυπταναλυτής. Ο παράγοντας εργασίας είναι εκθετικά ανάλογος ως προς το μήκος του κλειδιού. Η μυστικότητα παρέχεται από την ύπαρξη ενός ισχυρού αλλά δημόσιου αλγορίθμου και ενός μεγάλου κλειδιού.

Από τη μεριά του κρυπταναλυτή το πρόβλημα της κρυπτανάλυσης έχει τρεις βασικές παραλλαγές. Όταν έχει κάποια ποσότητα κρυπτοκειμένου αλλά όχι το απλό κείμενο αντιμετωπίζει το πρόβλημα μόνο του κρυποκειμένου. Όταν ο κρυπταναλυτής διαθέτει κάποια αντιστοιχισμένα ζεύγη κρυπτοκειμένου και απλού κειμένου το πρόβλημα ονομάζεται πρόβλημα γνωστού απλού κειμένου. Όταν ο κρυπταναλυτής έχει τη δυνατότητα να κρυπτογραφεί τμήματα απλού κειμένου της επιλογής του έχουμε το πρόβλημα του επιλεγόμενου απλού κειμένου.

4.2. ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Ως μια προσπάθεια ασφαλούς διανομής δημόσιων κλειδιών μπορούμε να φανταστούμε ένα κέντρο διανομής κλειδιών το οποίο είναι άμεσα διαθέσιμο 24 ώρες

τη μέρα για την παροχή δημόσιων κλειδιών κατόπιν αιτήσεως. Ένα από τα πολλά προβλήματα αυτής της επιλογής είναι ότι δεν μπορεί να κλιμακωθεί σε μεγάλες κλίμακες οπότε το κέντρο διανομής κλειδιών θα γίνει σύντομα σημείο συμφόρησης. Αν κάποτε αποτύχει το κέντρο η ασφάλεια στο Internet ξαφνικά θα παγώσει.

Για αυτούς τους λόγους έχει αναπτυχθεί μια διαφορετική λύση η οποία δεν απαιτεί να είναι κέντρο διανομής κλειδιών συνεχώς διαθέσιμο στο δίκτυο. Στην πραγματικότητα δεν χρειάζεται ούτε να βρίσκεται στο δίκτυο. Αυτό που κάνει το κέντρο είναι να πιστοποιεί τα δημόσια κλειδιά που ανήκουν σε άτομα, εταιρείες και άλλους οργανισμούς. Ένας οργανισμός που πιστοποιεί δημόσια κλειδιά ονομάζεται Αρχή Πιστοποίησης ή CA (Certified Authority).

Η αρχική δουλειά ενός πιστοποιητικού είναι να συσχετίζει ένα δημόσιο κλειδί με το όνομα του πρωταγωνιστή (ατόμου, εταιρίας, κ.τ.λ.). Τα ίδια τα πιστοποιητικά δεν είναι μυστικά ή προστατευμένα. Η τυπική λειτουργία του πιστοποιητικού είναι να συσχετίζει ένα δημόσιο κλειδί με έναν πρωταγωνιστή, ωστόσο το πιστοποιητικό μπορεί επίσης να χρησιμοποιηθεί για να συσχετίσει ένα δημόσιο κλειδί με μία ιδιότητα. Για παράδειγμα ένα πιστοποιητικό θα μπορούσε να λέει: «Αυτό το δημόσιο κλειδί ανήκει σε ένα άτομο άνω των 18 ετών». Επομένως θα μπορούσε να χρησιμοποιηθεί για να αποδείξει ότι ο ιδιοκτήτης του ιδιωτικού κλειδιού δεν είναι ανήλικος χωρίς όμως να αποκαλύπτει την ιδιότητα του ιδιοκτήτη. Τυπικά το άτομοα που θα είχε στην κατοχή του το πιστοποιητικό θα το έστελνε στην τοποθεσία Ιστού στον πρωταγωνιστή ή στη διεργασία που ενδιαφερόταν για την ηλικία του χρήστη. Τότε αυτή η διεργασία ή ο πρωταγωνιστής θα παρήγαγε έναν τυχαίο αριθμό και θα τον αποκρυπτογραφούσε με το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό. Αν ο ιδιοκτήτης ήταν σε θέση να το αποκρυπτογραφήσει και να το επιστρέψει τότε θα αποδεικνυόταν ότι ο ιδιοκτήτης είχε όντως την ιδιότητα που προσδιορίζεται από το πιστοποιητικό. Εναλλακτικά ο τυχαίος αριθμός θα μπορούσε να χρησιμοποιηθεί για την παραγωγή ενός κλειδιού συνδιάλεξης για τη μετέπειτα επικοινωνία.

Ένα άλλο παράδειγμα όπου ένα πιστοποιητικό μπορεί να περιέχει μια ιδιότητα είναι σε ένα αντικειμενοστραφές κατανεμημένο σύστημα. Κάθε αντικείμενο κανονικά προσφέρει διάφορες μεθόδους. Ο ιδιοκτήτης του αντικειμένου θα μπορούσε να παρέχει σε κάθε πελάτη ένα πιστοποιητικό το οποίο να δίνει ένα χάρτη ψηφίων με τις μεθόδους που επιτρέπεται να καλέσει ο πελάτης συσχετίζοντας το χάρτη ψηφίων με ένα δημόσιο κλειδί μέσω ενός υπογεγραμμένου πιστοποιητικού. Και σε αυτή την

περίπτωση αν ο ιδιοκτήτης μπορεί να αποδείξει ότι έχει στην κατοχή του το αντίστοιχο ιδιωτικό κλειδί, θα του επιτρέπεται να εκτελέσει τις μεθόδους του χάρτη ψηφίων. Η τεχνική αυτή έχει την ιδιότητα ότι η ταυτότητα του ιδιοκτήτη δε χρειάζεται να είναι γνωστή, γεγονός που είναι χρήσιμο σε περιπτώσεις όπου είναι σημαντική η προστασία του απορρήτου.

4.3.ΑΣΦΑΛΕΙΑ

Η προσθήκη της ασφάλειας δεν ήταν εύκολη υπόθεση επειδή ξέσπασε ένας πόλεμος σχετικά με το σημείο όπου θα έπρεπε να τοποθετηθεί. Οι περισσότεροι ειδικοί στην ασφάλεια πιστεύουν ότι για να υπάρχει πραγματική ασφάλεια, η κρυπτογραφία και οι έλεγχοι ακεραιότητας πρέπει να γίνονται στο επίπεδο εφαρμογών. Η διεργασία προέλευσης θα κρυπτογραφηθεί ή θα προστατεύει την ακεραιότητα των δεδομένων και μετά θα τα στέλνει στη διεργασία προορισμού όπου θα αποκρυπτογραφούνται ή θα επαληθεύονται. Όποια τροποποίηση και να γίνει ανάμεσα σε αυτές τις δύο διεργασίες συμπεριλαμβάνοντας και τροποποιήσεις μέσα σε κάποιο από τα λειτουργικά συστήματα θα μπορεί σε αυτή την περίπτωση να εντοπιστεί. Το πρόβλημα με αυτή την προσέγγιση είναι ότι απαιτεί την αλλαγή των εφαρμογών ώστε να ασχολούνται με την ασφάλεια. Επομένως, η αμέσως επόμενη καλύτερη προσέγγιση είναι να τοποθετηθεί η κρυπτογραφία στο επίπεδο μεταφοράς ή σε ένα επίπεδο ανάμεσα στο επίπεδο εφαρμογών και το επίπεδο μεταφοράς.

Η αντιτιθέμενη άποψη είναι ότι οι χρήστες δεν κατανοούν την ασφάλεια και επομένως δεν είναι σε θέση να τη χρησιμοποιήσουν σωστά και πώς κανένας δε θα ήθελε να τροποποιήσει τα υπάρχοντα προγράμματα με κανέναν τρόπο έτσι το επίπεδο του δικτύου πρέπει να πιστοποιεί την ταυτότητα ή να κρυπτογραφεί τα πακέτα χωρίς να αναμιγνύεται ο χρήστης. Έπειτα από χρόνια μαχών τελικά ορίστηκε ένα πρότυπο ασφαλείας επιπέδου δικτύου με σκοπό να βοηθά σε κάποιο βαθμό τους χρήστες που δεν είναι ενήμεροι για την ασφάλεια καθώς και το γεγονός ότι οι χρήστες οι οποίοι είναι ενήμεροι για την ασφάλεια να μην αποτρέπονται να κάνουν το σωστό.

Το αποτέλεσμα αυτού του πολέμου ήταν μία σχεδίαση που ονομάζεται ασφάλεια IP ή IPsec (IP security). Γενικά όλοι οι χρήστες δεν θέλουν

κρυπτογράφηση διότι είναι αρκετά δαπανηρή από άποψη υπολογιστική. Αντί να γίνει προαιρετική η κρυπτογράφηση αποφασίστηκε να γίνει υποχρεωτική αλλά να επιτρέπεται η χρήση κενού αλγορίθμου.

Η πλήρης σχεδίαση του IPsec είναι ένα πλαίσιο εργασίας για περισσότερες από μία υπηρεσίες, αλγορίθμους και επίπεδα λεπτομέρειας. Ο λόγος της ύπαρξης πολλαπλών υπηρεσιών είναι ότι δε θέλουν όλοι να πληρώσουν το κόστος για να έχουν όλες τις υπηρεσίες ανά πάσα στιγμή έτσι οι υπηρεσίες είναι διαθέσιμες κατόπιν επιλογής. Οι κύριες υπηρεσίες είναι η μυστικότητα, η ακεραιότητα δεδομένων και η προστασία από επιθέσεις αναπαραγωγής.

Ο λόγος ύπαρξης πολλών αλγορίθμων είναι ότι ένας αλγόριθμος που θεωρείται ασφαλής μπορεί να σπάσει κάποια στιγμή στο μέλλον. Αν το IPsec είναι ανεξάρτητο από τους αλγορίθμους το γενικό πλαίσιο μπορεί να επιβιώσει ακόμη και αν κάποιος συγκεκριμένος αλγόριθμος αργότερα σπάσει

Ένα κάπως απροσδόκητο χαρακτηριστικό του IPsec. Είναι ότι για να υπάρχει οποιαδήποτε ασφάλεια θα πρέπει να εγκαθιδρυθεί ένα κλειδί και να χρησιμοποιηθεί το κλειδί για κάποια χρονική περίοδο, ουσιαστικά αυτό είναι ένα είδος σύνδεσης. Η σύνδεση αυτή (η σύνδεση δηλ με την έννοια του IPsec) ονομάζεται συσχέτιση ασφαλείας ή SA (security association). Η SA είναι μια μονόδρομη σύνδεση ανάμεσα σε δύο άκρα, η οποία έχει αναγνωριστικό ασφαλείας που σχετίζεται με αυτή. Αν απαιτείται ασφαλής κίνηση και προς τις δύο κατευθύνσεις χρειάζονται δύο συσχετίσεις ασφαλείας. Τα αναγνωριστικά ασφαλείας μεταφέρονται στα πακέτα μέσω αυτών των ασφαλών συνδέσεων και χρησιμοποιούνται για την αναζήτηση κλειδιών και άλλων συναφών πληροφοριών οπότε επαρκεί ένα ασφαλές πακέτο.

Από τεχνική άποψη το IPsec έχει δύο βασικά μέρη:

- Το πρώτο μέρος αναγράφει δύο νέες κεφαλίδες που μπορούν να προστεθούν στα πακέτα για να μεταφέρουν το αναγνωριστικό ασφαλείας, τα δεδομένα ελέγχου ακεραιότητας και άλλες πληροφορίες
- Το δεύτερο μέρος το Πρωτόκολλο Συσχετίσεων Ασφαλείας και Διαχείρισης Κλειδιών Internet ή ISAKMP (Internet Security Association and Key Management Protocol) ασχολείται με τη διαχείριση κλειδιών.

4.3.1.:Ασφάλεια και Έξυπνες Κάρτες

Οι περισσότεροι παρατηρητές του κλάδου συμφωνούν ότι οι πολύ-συζητημένοι «Αυτοκινητόδρομοι Πληροφοριών» θα εξαπλωθούν ποιο γρήγορα στον επαγγελματικό κόσμο από ότι στον κόσμο των καταναλωτών. Ωστόσο, σε αμφότερες τις περιπτώσεις, οι εμπειρογνώμονες συμφωνούν ότι ένα ουσιαστικό συστατικό για τη συνολική επιτυχία τους θα είναι η μεγαλύτερη ασφάλεια. Όχι όμως μια κεντρική ασφάλεια, αλλά ευρέως διαθέσιμες υπηρεσίες ασφαλείας που θα απαιτηθούν για να ενθαρρύνουν τις επιχειρήσεις, μεγάλες ή μικρές, ακόμη και ιδιώτες, να διενεργούν συναλλαγές με άνεση και να έχουν εμπιστοσύνη στις πληροφορίες που θα έχουν ανά πάσα στιγμή στα χέρια τους.

Οι σύγχρονες απαιτήσεις για καλύτερη κρυπτογράφηση, βιομετρία, ευκολότερη και ταχύτερη προσαρμογή, και χειρισμό υψηλότερου εύρους ζώνης δεδομένων, ωθεί την βιομηχανία στην τεχνολογία των Έξυπνων Καρτών με ασφαλής επεξεργαστές και προηγμένες αρχιτεκτονικές. Ενισχυμένες αρχιτεκτονικές που ενσωματώνουν αριθμητικούς επεξεργαστές και υψηλή αποθηκευτική ικανότητα ενσωματωμένα σε μια έξυπνη κάρτα IC chip επιτρέπουν την ασφαλή λειτουργία των εφαρμογών που ικανοποιούν αυτές τις απαιτήσεις. Διάφορες μορφές της επικάλυψης IC θα οδηγήσει σε Έξυπνες Ετικέτες, Έξυπνους Τίτλους ή Έξυπνα Αυτοκόλλητα, υπονοώντας μια έκδοση συνημμένων Έξυπνων Καρτών, επιτρέποντας τη ορατότητα και την αποκέντρωση των πληροφοριών με τον πιο αποτελεσματικό τρόπο. Επιπροσθέτως, η χρήση των Barcodes θα μπορούσαν να συνδυαστούν με το ίδιο έξυπνο MEDIA, επιτρέποντας την καλύτερη αξιοποίηση των δύο τεχνολογιών. Η πολυάριθμη κρυπτογράφηση και οι μεθοδολογίες ασφάλειας που έχουν αναπτυχθεί για τέτοιες εφαρμογές συναλλαγών εμποδίζουν όμως την κατανόηση της προόδου αυτής της διαδικασίας. Η έλλειψη της γνώσης για την μεθοδολογία που ακολουθείται και για την λειτουργικότητα των μέσων που χρησιμοποιούνται για να πραγματοποιηθούν οι συναλλαγές, δημιουργεί τελικά δυσπιστία και δυσφορία, μειώνοντας τη συμμετοχή σε τέτοιου είδους συναλλαγές.

4.3.2.: Ασφαλές Περιβάλλον Έξυπνων Καρτών για το Απόρρητο και την Ασφάλεια των Κινητών.

Έξυπνη κάρτα είναι ένα καλύτερα προσαρμοζόμενο (best-fit) προϊόν όσον αφορά τα θέματα κινητικότητας των χρηστών, δεδομένου ότι συνδέεται με τον χρήστη. Ο κάτοχος της κάρτας μπορεί να την χρησιμοποιήσει οποτεδήποτε και οπουδήποτε θέλει, ενώ την ίδια στιγμή οι πληροφορίες χρήσης είναι αποκεντρωμένες στον ίδιο τον χρήστη. Η ικανότητα των έξυπνων καρτών να διατηρούν περιοχές πληροφοριών σύμφωνα με κλιμακούμενες απαιτήσεις ασφάλειας τις καθιστά επιλέξιμες ως μέσο προστασίας για την διασφάλιση της ιδιωτικής του ζωής ως χρήστη κινητής τηλεφωνίας. Η πρόσβαση στα συστήματα ασφάλειας των πληροφοριών επιτρέπεται ανάλογα με τα προνόμια του αιτούντος μέρους. Ο τελικός χρήστης διατηρεί τον απόλυτο έλεγχο κάθε συναλλαγής ακριβώς μέσα από τον ατομικό χειρισμό της έξυπνης κάρτας.

Το μειονέκτημα της τεχνολογίας της έξυπνης κάρτας είναι το σχετικά υψηλό κόστος και η μικρή μνήμη όπως και οι δυνατότητες επεξεργασίας όσον αφορά τις απαιτήσεις της επιβολής της ασφάλειας και της εφαρμογής συναλλαγών. Όντας ένα σχετικά αργό περιβάλλον αντίδρασης με περιορισμένο χώρο, είναι δύσκολο να διατηρήσει τις πληροφορίες του χρήστη, τις εφαρμογές και την ασφάλεια, όλα αυτά εντελώς υπό κάλυψη (κρυμμένα). Έτσι, κάποια συνεργασία με ένα άλλο ξένο σύστημα απαιτείται προκειμένου να επιτευχθούν οι απαιτήσεις μιας επιτυχούς ολοκληρωμένης συναλλαγής. Άρα αυτός είναι και ο μόνος τρόπος που οι έξυπνες κάρτες θα μπορούσαν να λειτουργήσουν.

Το ξένο (φιλόξενο) σύστημα μπορεί να είναι ένας υπολογιστής ή μια άλλη συσκευή με δυνατότητες επεξεργασίας που εξυπηρετούν την έξυπνη κάρτα. Η αλληλεπίδραση μεταξύ των δύο συσκευών, όπως και οι αρμοδιότητες τους θα πρέπει να είναι προσεκτικά σχεδιασμένες σύμφωνα με τις απαιτήσεις της εφαρμογής, ώστε να διατηρηθεί η μέγιστη απόδοση του συστήματος, μαζί με τη μέγιστη συμβατότητα μεταξύ άλλων διαφόρων συσκευών που θα λειτουργούν υπό την ομπρέλα της ίδιας εφαρμογής.

Διάφορες εφαρμογές εφαρμόζονται για την κινητή (μετακινούμενη) προστασία της ιδιωτικής ζωής και της ασφάλειας, κάποιες πιο απαιτητικές και κάποιες λιγότερο. Οι πιο απαιτητικές εφαρμογές αφορούν τα ευαίσθητα δεδομένα του χρήστη και ως εκ

τούτου απαιτούν έντονη φροντίδα για την διατήρηση της ιδιωτικής ζωής των χρηστών και την ασφάλεια. Εξελιγμένες διαδικασίες πρέπει να εφαρμόζονται για την προστασία των πληροφοριών των χρηστών με αποτέλεσμα την αναγκαιότητα μεγάλης μνήμης και επεξεργαστή υψηλών απαιτήσεων. Τέτοιες μεγάλες απαιτήσεις θα μπορούσαν να αποτελέσουν σημαντικό μειονέκτημα για την εφαρμογή της τεχνολογίας των ευφυών καρτών, όπως είναι σήμερα διαθέσιμες ανάλογα με τις απαιτήσεις της εκάστου εφαρμογής. Συστήματα ασφάλειας εντος της κάρτας είναι τυπικά σε αυτές τις περιπτώσεις, όπου η κάρτα θεωρείται πλέον ενεργή υπολογιστική συσκευή, με ή χωρίς την ενεργή διαχείριση της μνήμης της, που θα επέτρεπε την λήψη και εφαρμογή ειδικών προγραμμάτων.

Σημαντικό τμήμα της διαχείρισης και επεξεργασίας των δεδομένων πραγματοποιείται στο πλαίσιο της κάρτας αφήνοντας μόνο κρυπτογραφημένες απαντήσεις να περάσουν τα σύνορά της. Αλλά τι γίνεται με το χρόνο που απαιτείται για την επεξεργασία και απάντηση του μηνύματος; Τι συμβαίνει με το επικοινωνιακό μέρος της συναλλαγής και τα πρωτόκολλα που εμπλέκονται;

Οι λιγότερο απαιτητικές εφαρμογές είναι λιγότερο απαιτητικές για την τεχνολογία των έξυπνων καρτών, αλλά μπορεί να είναι τελικά πολύ απλές για να δικαιολογήσουν μια τέτοια δαπάνη. Άλλωστε οι έξυπνες κάρτες δεν είναι ακόμα τόσο φθηνές για να πεταχτούν μετά τη χρήση τους. Τα φιλόξενα συστήματα ασφαλείας που εφαρμόζονται σε τέτοιες περιπτώσεις αντιμετωπίζουν μια κάρτα ως έναν απλό φορέα δεδομένων.

Εξαιτίας αυτού, κάρτες μνήμης μπορούν να χρησιμοποιηθούν με οικονομικά ποιο αποδοτικό τρόπο. Όλη η προστασία των δεδομένων γίνεται από το σύστημα του ξενιστή, ενώ τα δεδομένα της κάρτας μπορούν να κρυπτογραφούνται. Α κοινή μέθοδος για την αύξηση της ασφάλειας είναι να γράψετε ένα κλειδί που περιέχει συνήθως μια ημερομηνία ή / και ώρα, μαζί με μια μυστική αναφορά σε ένα σύνολο των πλήκτρων του ξενιστή. Κάθε φορά που η κάρτα έχει ξαναγραφεί ο οικοδεσπότης μπορεί να γράψει μια αναφορά για τα κλειδιά, καθιστώντας με τον τρόπο αυτό κάθε μετάδοση διαφορετική. Η ασφάλεια μπορεί να αυξηθεί ακόμη περισσότερο με τη χρήση μιας έξυπνης κάρτας μνήμης που χρησιμοποιεί ένα μηχανισμό κωδικού πρόσβασης για την προστασία ενάντια μιας μη εξουσιοδοτημένης ανάγνωσης των δεδομένων.

Ένα ισχυρό σημείο της εφαρμογής μιας ολιστικής προσέγγισης σε θέματα ασφάλειας εντός (των ορίων) της έξυπνης κάρτας, είναι ότι οι συναλλαγές μπορούν να πραγματοποιηθούν και χωρίς σύνδεση όποτε είναι αναγκαίο. Η ύπαρξη ισχυρής ταυτότητας και οι αδιαπέραστες διαδικασίες συστημάτων ασφάλειας, όπως η τεχνική του Δημόσιου Κλειδιού Κρυπτογράφησης, επιτρέπει την ολοκλήρωση μιας συναλλαγής μεταξύ ενός τελικού χρήστη και ενός παρόχου, χωρίς την μεσολάβηση ενός διακομιστή ελέγχου ταυτότητας σε πραγματικό χρόνο. Επιπλέον, είναι δυνατόν να εκτελούνται παράλληλα στην ίδια έξυπνη κάρτα διάφορες εφαρμογές, ανεξάρτητες μεταξύ τους, καθώς η εφαρμοζόμενες μέθοδοι ασφαλείας θα διαφέρουν ανά περίπτωση και να απομονώσουν τις εφαρμογές, όπως και των συναφών τους δεδομένων. Ακόμη περισσότερο στο μέλλον, οι έξυπνες κάρτες μπορούν να γίνουν πλήρεις συσκευές διαδικτύου (Internet). Αφού μια έξυπνη κάρτα θα μπορούσε να αποτελέσει ένα νομικό πληρεξούσιο για τον τελικό χρήστη, θα μπορεί να ασκεί και επαγγελματικές δραστηριότητές στο Διαδίκτυο ακόμα και στη φυσική απουσία του ιδιοκτήτη του. Η ισχύς της εντολής εξαρτάται από την ψηφιακή υπογραφή της έξυπνης κάρτας και όχι από την παρουσία ή την απουσία του αγοραστή, ο αγοραστής διατηρεί όμως πάντα τον απόλυτο έλεγχο της κάρτας του με την επιλογή να συνδέεται ή να αποσυνδέσετε σε απευθείας σύνδεση με το διαδίκτυο.

Η ασφάλεια επηρεάζει και την επικοινωνία τμημάτων μεταξύ της έξυπνης κάρτας και της άλλης πλευράς της συναλλαγής. Η επικοινωνία μεταξύ της έξυπνης κάρτας και του συστήματος υποδοχής, όπως και μεταξύ του συστήματος υποδοχής με τον φορέα εκμετάλλευσης ή με την υπηρεσία ταυτοποίησης, η μεταξύ του συστήματος υποδοχής και του συστήματος της άλλης πλευράς, καθώς και μεταξύ των συγγενικών εφαρμογών είναι όλες ελέγξιμες σε ότι αφορά την ασφάλεια και την προστασία της ιδιωτικής ζωής και της επιβολής του νόμου. Δεδομένης της ήδη αναπτυχθείσας ασφάλειας για την επικοινωνία των τμημάτων των κάθετων συστημάτων όπως είναι τα δίκτυα κινητής τηλεφωνίας, πρέπει να ληφθεί μέριμνα ώστε να διατηρηθεί ο ρόλος και το κύρος κάθε πολυεπίπεδης προσέγγισης, καθώς και να καθοριστούν νέα πρότυπα ασφάλειας για τα τμήματα που επηρεάζονται άμεσα από τη συμμετοχή των έξυπνων καρτών σε διαδικασίες συναλλαγής. Μετά από όλα αυτά, έχοντας δημιουργήσει ένα πλήρως ασφαλές σύστημα με έναν όλα-σε-ένα μηχανισμό μέσα σε μια έξυπνη κάρτα, σε ένα καλά εναρμονισμένο περιβάλλον όπου οι αγοραστές και οι έμποροι θα μπορούν να συναλλάσσονται με επιτυχία ακόμη και

(offline) εκτός δικτύου, ποιος θα μπορούσε να είναι ο ρόλος του χειριστή; Υπάρχει ακόμα λόγος να χρησιμοποιώ το δίκτυο κινητής τηλεφωνίας από το τηλέφωνο μου όταν μπορώ να επικοινωνώ άμεσα με τον συγγενικό χρήστη; Η κατεδάφιση της πλανητικής τοπολογίας ανάμεσα σε μια κεντρική αρχή ελέγχου και των αποκεντρωμένων χρηστών μπορούν να εισάγουν παρενέργειες που θα πρέπει επίσης να διερευνηθούν και να δικαιολογηθούν. Οι απαιτήσεις των εφαρμογών και της τεχνολογίας δημιουργούν συγκεκριμένα αναμενόμενα χαρακτηριστικά της αντίδρασης της έξυπνης κάρτας σε μια συγκεκριμένη συναλλαγή. Ανεκτικές και μη ανεκτικές εφαρμογές θολώνουν την εικόνα ενός ολοκληρωμένου σχεδιασμού με παγκόσμια συμβατότητα, καθώς η τεχνολογία δημιουργεί συγκεκριμένους στόχους αντίδρασης στο μέχρι τώρα επικοινωνιακό περιβάλλον που έχει σχεδιαστεί. Παρόλα αυτά είναι σημαντικό να καθορίσουμε τις ελάχιστες απαιτήσεις της λειτουργίας επιλεγμένων εφαρμογών με σκοπό την ταξινόμηση των αρχών που θα οδηγήσουν στο σχεδιασμό των μελλοντικών συστημάτων ασφαλών έξυπνων καρτών.

Είναι σαφές ότι οι έξυπνες κάρτες μπορούν να παίξουν σημαντικό ρόλο για την προστασία του περιβάλλοντος της ιδιωτικής ζωής και ασφάλειας. τρέχουσα δυνατότητα αποθήκευσης της μνήμης τους, δικαιολογούν την εξωτερική φιλοξενία των πληροφοριών των χρηστών, μαζί με τα χαρακτηριστικά προστασίας που εφαρμόζονται σε αυτές. Η έλευση των δυνατοτήτων επεξεργασίας που παρέχουν οι έξυπνες κάρτες θα μπορούσαν να τις κάνει να συμμετάσχουν και στην κρυπτογραφία, μετατρέποντάς τις σε ένα ασφαλές κλειστό σύστημα. Μέχρι να συμβεί αυτό, Ίδη υπολογισμένες και Ίδη καθορισμένες αρχές ασφάλειας θα μπορούσαν να ανατεθούν σε έξυπνες κάρτες μαζί με τα χαρακτηριστικά των χρηστών, για ειδικές εφαρμογές όπως το e-banking. Κάποιες επιπλέον εφαρμογές των έξυπνων καρτών είναι διστακτικές (ποιο δύσκολες) , αφήνοντας χώρο για την συμμετοχή άλλων σχετικών τεχνολογιών, όπως οι έξυπνες ετικέτες και έξυπνες ταμπέλες ή ακόμα και οι ασύρματες έξυπνες κάρτες.

4.4. ΠΑΡΑΔΕΙΓΜΑ ΣΧΕΔΙΑΣΜΟΥ ΓΙΑ ΕΦΑΡΜΟΓΕΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

Υπάρχουν βασικά δύο διαφορετικοί τρόποιγια την υλοποίηση εφαρμογών σε έξυπνες κάρτες.

- Ο πρώτος τύπος της εφαρμογής βασίζεται σε αρχεία με καθορισμένες προϋποθέσεις πρόσβασης. Σε μια τέτοια υλοποίηση, οι απαραίτητες εντολές συμμορφώνονται γενικά με τις συνήθεις προδιαγραφές έξυπνες κάρτες, όπως ISO / IEC 7816-4.
- Ο άλλος τύπος της εφαρμογής βασίζεται σε κώδικα προγράμματος που εκτελείται σε έξυπνη κάρτα. Υπάρχουν πολλές διαφορετικές παραλλαγές αυτού του τύπου της εφαρμογής. Το πρόγραμμα - κώδικας μπορεί να εκτελεστεί απευθείας από τον επεξεργαστή στην έξυπνη κάρτα (native code), ή μπορεί να ερμηνεύεται.

Το ακόλουθο παράδειγμα επεξηγεί μία τυπική εφαρμογή των έξυπνων καρτών. Πρόκειται για εφαρμογή μεσαίου εύρους ηλεκτρονικής επεξεργασίας δεδομένων που δεν απαιτεί περίτεχνα σχέδια συστήματος. Συνήθως χρησιμοποιείται από μεσαίου μεγέθους επιχειρήσεις. Το background σύστημα που χρησιμοποιείται μπορεί να είναι ένα PC που βρίσκεται ένα ασφαλές περιβάλλον, το οποίο σημαίνει ότι το κόστος για την απόκτησή του καθώς και το λειτουργικό κόστος θα είναι πάρα πολύ χαμηλά.
Αυτό το απλό παράδειγμα δείχνει πώς μια τυπική εφαρμογή της έξυπνης κάρτας είναι κατασκευασμένη. Η κατασκευή εξηγείται βήμα προς βήμα. Το παράδειγμα βασίζεται στην αρχή της διανομής δεδομένων μεταξύ πολλών ατομικών, χωριστών συστημάτων
Έλεγχος της γνησιότητας ενός τερματικού - Η κατάσταση και οι στόχοι

Υπάρχουν περιπτώσεις στις οποίες θα πρέπει να είναι δυνατό για ένα χρήστη κάρτας να μπορεί να επαληθεύει την αυθεντικότητα ενός τερματικού. Ένα παράδειγμα είναι ένα τερματικό σε ένα σούπερ μάρκετ, στο οποία ο χρήστης πρέπει να εισάγει έναν κωδικό PIN μετά την εισαγωγή της κάρτας. Ένα πλαστό τερματικό θα μπορούσε να χρησιμοποιηθεί για να κατασκοπεύει το μυστικό κωδικό PIN. Αν η κάρτα στη συνέχεια κλαπεί από ένα πρόσωπο που γνωρίζει ήδη το PIN, ο κλέφτης θα μπορούσε να χρησιμοποιήσει για να κάνει αγορές με την κάρτα ή για να λάβει χρήματα από ένα μηχάνημα.

Το καλοκαίρι του 1997, χρησιμοποιήθηκε ένας πλαστό διανομέας μετρητών στο στο Μόναχο με τρόπο ώστε να συλλέγεται παράνομα η μαγνητική λωρίδα

δεδομένων και των συναφών κωδικών PIN. Αν οι έξυπνες κάρτες χρησιμοποιούνται, καλή προστασία έναντι αυτού του είδους της επίθεσης μπορεί να παρέχεται με ένα κατάλληλο σχεδιασμό εφαρμογής.

Απαιτήσεις

Είναι απαραίτητο να σχεδιάσουμε μία εφαρμογή η οποία θα επιτρέπει στο χρήστη κάρτας να αναγνωρίζει ένα πλαστό τερματικό έξυπνης κάρτας.

Προτεινόμενη λύση

Η προτεινόμενη λύση περιλαμβάνει την αποθήκευση ενός κωδικού πρόσβασης που είναι γνωστός μόνο στο χρήστη της κάρτας σε ένα αρχείο στην έξυπνη κάρτα. Αυτό το αρχείο μπορεί να διαβαστεί από το τερματικό μόνο αφού έχει πιστοποιηθεί με επιτυχία μέσω ενός μυστικού κλειδιού στην έξυπνη κάρτα.

Μετά από αυτή τη διαδικασία ελέγχου ταυτότητας, το τερματικό έχει τη δυνατότητα να διαβάσει τον κωδικό πρόσβασης από το αρχείο και να δείξει στην οθόνη του. Μόλις ο χρήστης της κάρτας βλέπει τον κωδικό πρόσβασης και επιβεβαιώσει ότι είναι σωστός, αυτός ή αυτή μπορούν να θεωρήσουν ότι το τερματικό είναι γνήσιο, δεδομένου ότι μόνο ο χρήστης γνωρίζει τον κωδικό πρόσβασης. Μόνο μετά αυτός ή αυτή αφού έχει επαληθεύσει τον κωδικό πρόσβασης, μπορεί να εισάγει το PIN που κάνει δυνατό το υπόλοιπο της συναλλαγής.

Η διαδικασία που περιγράφεται ανωτέρω συνιστάται στην προδιαγραφή DIN για κάρτες που φέρουν γερμανική υπογραφή, για παράδειγμα, προκειμένου να επιτραπεί στους χρήστες καρτών να καθορίσουν αν δημόσια τερματικά υπογραφής είναι αυθεντικά Πρέπει να αναφερθεί ένας σημαντικός περιορισμός της λύσης. Αυτό είναι ότι επιτρέπει ένα πλαστό τερματικό να αναγνωρίζεται, αλλά όχι να χειραγωγείται. Εάν το λογισμικό του τερματικού μπορούσε να τροποποιηθεί χωρίς να χαθεί το μυστικό κλειδί, θα ήταν για ένα χειραγωγούμενο τερματικό να πιστοποιεί σωστά αυτό το ίδιο χρησιμοποιώντας σωστά την την έξυπνη κάρτα και στη συνέχεια εμφανίζοντας τον κωδικό πρόσβασης. Ο περιορισμός αυτός θα πρέπει να λαμβάνεται υπόψη σε κάθε εφαρμογή στην οποία αυτή η τεχνική χρησιμοποιείται.

Ωστόσο, αυτό δεν είναι βασικά ένα κρίσιμο ζήτημα δεδομένου ότι ένα τερματικό που μπορεί να χειραγωγηθεί στο βαθμό αυτό θα επιτρέψει πολύ πιο εκτεταμένες μορφές επίθεσης πέρα από τους κωδικούς PIN.

Η προτεινόμενη λύση, η οποία παρουσιάζεται με τη μορφή συγκεκριμένων αρχείων και συνθηκών πρόσβασης παρουσιάζεται στον παρακάτω πίνακα αλλά, δεν

είναι μια πλήρης εφαρμογή της έξυπνης κάρτας. Αντ 'αυτού, είναι ένα είδος σχεδιασμού πρότυπο που μπορεί να συγχωνευθεί σε οποιαδήποτε επιθυμητή εφαρμογή. Για αυτό παρουσιάζουμε και ένα δεύτερο σχήμα όπου υπάρχουν κάποιες τροποποιήσεις και χρησιμοποιούνται διαφορετικές τιμές ή ακολουθίες εντολών. Το παράδειγμα αυτό προορίζεται κυρίως για να μεταφερθεί η βασική ιδέα για το πώς η γνησιότητα ενός τερματικού μπορεί να ελεγχθεί, και όχι για να χρησιμεύσει ως μια συγκεκριμένη εφαρμογή.

Key	Used for	Function	State transition
key 1	EXTERNAL AUTHENTICATE	Authentication of the terminal by the smart card	$x \rightarrow 1$
PIN	VERIFY CHV	Identification of the user	$1 \rightarrow 2$

Table 15.18 File tree and access conditions for testing the genuineness of a terminal (≥ 0: always, < 0: never)

File	FIC	Structure	Read	Write	File contents
EF 1	'0001'	transparent	$= 1$	$= 2$	password
EF 2	'0002'	linear fixed	< 0	< 0	key 1, PIN

Εικόνα 8: Κλειδιά που απαιτούνται για τον έλεγχο της γνησιότητας ενός τερματικού

Smart card		Terminal	User
	←	Reset	
ATR	→	IF ATR = OK THEN continue ELSE abort	
	↔	EXTERNAL AUTHENTICATE (with key 1)	
	↔	IF (authentication is successful) THEN continue ELSE abort	
	↔	SELECT FILE (EF 1)	
	↔	READ BINARY	*Output the content of the password file* IF (password correct) THEN terminal is genuine ELSE abort
	↔	VERIFY CHV	*Output* "Please enter PIN"

Εικόνα 9: Ακολουθία εντολών για τον έλεγχο της γνησιότητας ενός τερματικού

ΚΕΦΑΛΑΙΟ 5 : ΚΑΡΤΕΣ SIM

5.1.: ΕΙΣΑΓΩΓΙΚΑ ΓΙΑ ΤΙΣ ΚΑΡΤΕΣ SIM

Η ιδέα της έξυπνης κάρτας γεννήθηκε στη δεκαετία του 70 με την κατασκευή της μαγνητικής πιστωτικής κάρτας που είναι πρόγονος της σημερινής έξυπνης κάρτας. Την ιδέα για την έξυπνη κάρτα δημιούργησε η ανάγκη για μια πιστωτική κάρτα με ασφαλέστερο αποθηκευτικό μέσο από την μαγνητική ταινία. Την ασφάλεια την προσέφερε η κωδικοποίηση των δεδομένων και ο αποκλεισμός της αντιγραφής λόγω της υψηλής τεχνολογίας που απαιτεί η παραγωγή της.

Η γνωστή μας ΤΗΛΕΚΑΡΤΑ είναι μια μορφή κάρτας SIM με απλό προγραμματισμό. Αποκλειστική της λειτουργία είναι να μας παρέχει τηλεφωνική επικοινωνία συγκεκριμένης διάρκειας.

Το κοινό σημείο σ' όλες τις περιπτώσεις είναι η εσωτερική κατασκευή και η διαφορά τους ο προγραμματισμός.

Για τους λόγους λοιπόν της ασφάλειας και του αποκλεισμού της αντιγραφής, επιλέχθηκε η χρήση έξυπνης κάρτας και στα πλαίσια της κινητής τηλεφωνίας.

5.2. ΤΙ ΕΙΝΑΙ ΜΙΑ ΚΑΡΤΑ SIM;

Μια κάρτα SIM (subscriber identity module) είναι μια έξυπνη κάρτα (κάρτα με ενσωματωμένα ολοκληρωμένα κυκλώματα που μπορούν να επεξεργαστούν πληροφορίες) που αποθηκεύει με ασφάλεια το κλειδί για τον προσδιορισμό ενός συνδρομητή κινητής τηλεφωνίας, καθώς και πληροφορίες εγγραφής, προτιμήσεις και τα μηνύματα κειμένου. Η κάρτα αυτή έχει αποθηκευμένο το κλειδί που ταυτοποιεί το τηλεφωνικό αριθμό του χρήστη. Γενικά στη κάρτα αυτή αποθηκεύονται πληροφορίες σχετικά με την συνδρομή του χρήστη, το τηλεφωνικό του κατάλογο, το κατάλογο προτιμώμενων δικτύων για την περιαγωγή και τα γραπτά μηνύματα. Έτσι, επιτρέπεται στον χρήστη να διατηρεί τις πληροφορίες του όταν αλλάζει συσκευές τηλεφώνου. Ο χρήστης μπορεί επίσης να αλλάξει πάροχο έχοντας την ίδια τηλεφωνική συσκευή αλλά αλλάζοντας την κάρτα SIM.

Ισοδύναμο της κάρτας SIM στο UMTS Ισοδύναμο της κάρτας SIM στο UMTS είναι το Universal Subscriber Identity Module (USIM). *(Universal Mobile Telecommunications System (UMTS) είναι ένα σύστημα τρίτης γενιάς κινητής τηλεφωνίας για τα δίκτυα με βάση το πρότυπο GSM)*

Η κάρτα αυτή παρέχει την προσωπική κινητικότητα, έτσι ώστε ο χρήστης να έχει πρόσβαση στις υπό συνδρομή υπηρεσίες άσχετα με την συσκευή που χρησιμοποιεί. Επίσης, η κάρτα SIM, έχει, ως στατική πληροφορία που αφορά το δίκτυο και τον συνδρομητή, το IMSI (International Mobile Subscriber Identity), που χρησιμοποιείται για την ταυτοποίηση του χρήστη παγκοσμίως. Ακόμα, περιέχεται και ένα μυστικό κλειδί πιστοποίησης, το ki, που προστατεύει το χρήστη από υποκλοπές των συνομιλιών του με την κατάλληλη κρυπτογράφηση, καθώς και την προστασία από πρόσβαση στο δίκτυο άλλων ατόμων με χρέωση του νόμιμου χρήστη. Επίσης, στην SIM, υπάρχουν και πληροφορίες σχετικές με την συνδρομή των υπηρεσιών που παρέχονται, όπως είναι το SIM Toolkit, που δίνει εύκολη πρόσβαση σε εξειδικευμένες υπηρεσίες του δικτύου, π.χ. το SIM Toolkit MyCosmos της Cosmote.

Η κάρτα SIM αποθηκεύει πληροφορίες για την κατάσταση του δικτύου, όπως η τρέχουσα location area identity (LAI). Αν η συσκευή είναι απενεργοποιημένη και ενεργοποιείται ξανά τότε η συσκευή λάβει τα δεδομένα από την κάρτα SIM και θα ψάξει για την LAI.

Αυτό εξοικονομεί χρόνο, αποφεύγοντας να χρειάζεται να ψάξει όλη τη λίστα των συχνοτήτων που λογικά θα έκανε το τηλέφωνο. Κάθε SIM είναι μοναδικά πιστοποιημένη από το ICCID της [International Circuit Card ID].

Τα στοιχεία που είναι αποθηκευμένα στη κάρτα SIM προστατεύονται από έναν προσωπικό κωδικό, το PIN (Personal Identity Number), έτσι ώστε να μην μπορεί να χρησιμοποιηθεί η κάρτα από μη εξουσιοδοτημένα άτομα, παρά μόνο από τον νόμιμο κάτοχο της. Πρέπει όμως να τονιστεί ότι για κανένα λόγο δεν πρέπει ένας χρήστης να αφήνει την κάρτα SIM στα χέρια άλλων, όπως μπορεί να γίνει π.χ. όταν αφήνει την κινητή του συσκευή στο service, αφού υπάρχουν συσκευές που «σπάνε» το PIN, έτσι ώστε να έχουν πλήρη πρόσβαση στα στοιχεία της κάρτας. Έτσι, μπορεί να δημιουργηθεί ένας κλώνος της κάρτας με όλα τα δυσάρεστα αποτελέσματα για τον χρήστη, π.χ. ανεπιθύμητες χρεώσεις.

5.3.: International Mobile Subscriber Identity (IMSI)

IMSI[im-zee]: αρχικά των λέξεων International Mobile Subscriber Identity κινητής Πρόκειται για ένα μοναδικό αριθμό που σχετίζεται με όλους τους χρήστες κινητής τηλεφωνίας GSM και UMTS.

Ο αριθμός είναι αποθηκευμένος στην κάρτα SIM. Αποστέλλεται από το κινητό στο δίκτυο και χρησιμοποιείται για να εντοπιστούν και άλλες λεπτομέρειες του κινητού. Προκειμένου να αποφευχθεί το φαινόμενο οι συνδρομητές να εντοπίζονται και να παρακολουθούνται από ωτακουστές, το IMSI σπάνια αποστέλλεται και στη θέση του στέλνεται ένα τυχαίο TMSI(Temporary Mobile Subscriber Iden).

Ένα IMSI είναι συνήθως δεκαπέντε ψηφία. Ωστόσο, μπορεί να είναι μικρότερου μεγέθους

Τα πρώτα τρία ψηφία είναι ο κωδικός της χώρας (MCC- country code) και τα επόμενα ψηφία είναι ο κωδικός του δικτύου (MNC- network code). Η MNC μπορεί να είναι είτε δύο ψηφία σύνηθες π.χ. στην Ευρώπη) ή τρία ψηφία (σύνηθες στη Βόρεια Αμερική), τα υπόλοιπα ψηφία, μέχρι το μέγιστο μήκος είναι ο μοναδικός αριθμός συνδρομητή (MSIN - unique subscriber number) στο πλαίσιο της πελατειακής βάσης του δικτύου.

5.4.ΜΟΡΦΕΣ ΤΗΣ ΚΑΡΤΑΣ SIM

Ένας GSM κινητός σταθμός διαχωρίζεται σε δυο μέρη, ένα από τα οποία περιέχει το υλικό (hardware) και το λογισμικό (software) σχετικά με το interface ραδιομετάδοσης, και ένα άλλο το οποίο περιέχει τα δεδομένα που αφορούν το συνδρομητή: το Τμήμα Ταυτότητας του Χρήστη (Subscriber Identity Module - SIM). Η κάρτα SIM μπορεί είτε να είναι μια έξυπνη κάρτα η οποία να έχει το γνωστό μέγεθος των πιστωτικών καρτών, ή εναλλακτικά, μπορεί να "κοπεί" σε ένα μικρότερο μέγεθος που καλείται "ενσωματωμένη (plug-in) SIM". Αυτό το μικρότερο μέγεθος εισήχθηκε για να θέσει λιγότερους περιορισμούς στη σχεδίαση των συσκευών χειρός. Η κάρτα SIM είναι ένα είδος κλειδιού. Από τη στιγμή που θ' αφαιρεθεί από τη συσκευή, η τελευταία δεν μπορεί να χρησιμοποιηθεί πέραν από κλήσεις ανάγκης (αν

το επιτρέπει το δίκτυο), δηλ. με άλλα λόγια δεν μπορεί να χρησιμοποιηθεί για καμιά υπηρεσία που μπορεί να επηρεάσει το λογαριασμό του συνδρομητή.

Η δυνατότητα να μπορεί ν' αφαιρεί ο συνδρομητής την κάρτα SIM εμφανίζει πολλά πλεονεκτήματα γι' αυτόν πέρα από τον ρόλο της σαν κλειδί. Για παράδειγμα, αν ο κινητός σταθμός του χαλάσει και χρειάζεται επισκευή, ένας άλλος κινητός σταθμός μπορεί να χρησιμοποιηθεί, στο μεσοδιάστημα, στη θέση του. Συνάγουμε από αυτό ότι μπορούμε να αφαιρέσουμε την κάρτα SIM από έναν κινητό σταθμό και να την τοποθετήσουμε σ' έναν άλλο. Ένα άλλο παράδειγμα είναι η περίπτωση των χρηστών των πόλεων οι οποίοι έχουν μόνο μια συσκευή χειρός για λόγους οικονομίας. Όταν χρειαστεί, μπορούν να δανειστούν έναν ποιό ισχυρό κινητό σταθμό για να χρησιμοποιήσουν στην εξοχή, ή να νοικιάσουν έναν μόνιμο σταθμό αυτοκινήτου. Σ' όλες τις περιπτώσεις μπορούν να χρησιμοποιήσουν την δική τους κάρτα SIM, έτσι ώστε οι κλήσεις προς τον αριθμό πιστοποίησής τους να δρομολογούνται στη νοικιασμένη συσκευή και οι τηλεφωνικές χρεώσεις να πιστώνουν τον δικό τους λογαριασμό όπως και στην περίπτωση που οι τηλεφωνικές κλήσεις γίνονται από το δικό τους κινητό χειρός.

Η κάρτα SIM είναι επίσης η αποθήκη περισσότερης πληροφορίας που σχετίζεται με την τοπική παροχή υπηρεσιών στον χρήστη. Η κάρτα SIM μπορεί να προστατεύεται με έναν κωδικό αριθμό, έναν κώδικα PIN (Personal Identity Number - Προσωπικός Αριθμός Ταυτότητας), παρόμοιο με τους 4-ψήφιους PIN των πιστωτικών καρτών. Αντίθετα με τα PIN πολλών πιστωτικών καρτών, τα PIN στο GSM μπορούν να επιλεγούν από τον συνδρομητή. Η κάρτα SIM μπορεί επίσης να περιέχει μια λίστα από συντετμημένους αριθμούς κλήσης με το αντίστοιχο αλφαριθμητικό καρνέ (για το όνομα του ανταποκριτή για παράδειγμα) και τον τύπο της κλήσης (ομιλία, fax, κτλ). Η κάρτα SIM μπορεί επίσης να χρησιμοποιηθεί για ν' αποθηκεύει μικρά μηνύματα, συγκεκριμένα εκείνα που λαμβάνονται όταν ο χρήστης δεν είναι παρόν. Μια ποιό τεχνική εφαρμογή είναι η αποθήκευση μιας λίστας προτιμήσεων για την επιλογή του δικτύου όταν υπάρχουν πολλές επιλογές. Εφόσον ο χρήστης θα πρέπει να διαλέξει από ποιο δίκτυο θα λαμβάνει υπηρεσίες, για παράδειγμα όταν περνά τα διεθνή σύνορα μιας χώρας, η κάρτα SIM αποθηκεύει πληροφορίες για να κάνει αυτήν την εναλλαγή αυτόματα λαμβάνοντας υπόψη τις προτιμήσεις του χρήστη. Όταν συμβουλές χρέωσης πραγματικού χρόνου παρέχονται από τα δίκτυα, η κάρτα SIM θα πρέπει να είναι επίσης ικανή να αποθηκεύει αυτήν

την πληροφορία χρέωσης ώστε να κρατά τον συνδρομητή ενημερωμένο για τα έξοδά του.

Μια ενδιαφέρουσα ανάπτυξη για τον χρήστη είναι η δυνατότητα να διαβάζει και να τροποποιεί μέρος της πληροφορίας πιστοποίησης που είναι αποθηκευμένη στην κάρτα SIM. Αυτό μπορεί φυσικά να γίνει χρησιμοποιώντας το πληκτρολόγιο ενός κινητού σταθμού, αλλά μια πιο άνετη προσέγγιση θα μπορούσε επίσης να προσφερθεί χρησιμοποιώντας έναν αναγνώστη καρτών συνδεδεμένο με έναν προσωπικό υπολογιστή και σχετικό λογισμικό για εισαγωγή συντετμημένων αριθμών κλήσης, για συμπίεση μικρών μηνυμάτων στον υπολογιστή κτλ. Φυσικά, αυτό ισχύει μόνο για μέρος των δεδομένων που είναι αποθηκευμένα στην κάρτα SIM αφού η περισσότερη πληροφορία προστατεύεται από αλλαγές και σε μερικές περιπτώσεις ακόμα κι από ανάγνωση. Το πεδίο δράσεως της κάρτας SIM μπορεί να επεκταθεί και πέρα από τα όρια του GSM και η έννοια μιας κάρτας πολλαπλών εφαρμογών αναδύεται. Η συμβατότητα των προδιαγραφών της κάρτας SIM με διεθνώς αναγνωρισμένα πρότυπα του ISO σ' αυτό το πεδίο κάνει την εφαρμογή του GSM έναν καλό υποψήφιο για να συμπεριληφθεί σε μια κάρτα πολλαπλών εφαρμογών. Η έννοια της κάρτας SIM βρίσκεται ακόμα στα πρώτα της βήματα και αναπόφευκτα θα γίνει η βάση για μια καλύτερη συνεργασία μεταξύ του χρήστη και της συσκευής.

5.5.: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΠΕΡΙΓΡΑΦΗ – ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΚΑΡΤΑΣ SIM

Η κάρτα SIM είναι βασικά μια έξυπνη κάρτα που ακολουθεί τα πρότυπα του ISO και έχει αποθηκευμένες τις πληροφορίες που αφορούν τον συνδρομητή στο τμήμα του χρήστη του interface ραδιομετάδοσης. Οι λειτουργικότητές της, πέραν από την δυνατότητα αποθήκευσης πληροφοριών, σχετίζονται επίσης με τον τομέα της εμπιστευτικότητας. Ο υπόλοιπος κινητός σταθμός περιέχει όλα τα απαραίτητα μέσα μετάδοσης και σηματοδοσίας για προσπέλαση στο δίκτυο. Το interface μεταξύ της κάρτας SIM και του υπόλοιπου εξοπλισμού περιγράφεται λεπτομερώς στις προδιαγραφές και αναφέρεται απλά ως "SIM-ME" interface (ME - Mobile Equipment - Κινητός Εξοπλισμός). Λέγοντας "Κινητός Σταθμός" (MS) θα εννοούμε τον "Κινητό Εξοπλισμό" (ME) μαζί με την κάρτα SIM, εκτός από τις περιπτώσεις που ένας

κινητός σταθμός μπορεί να λειτουργήσει χωρίς την κάρτα SIM για επείγοντες κλήσεις όταν επιτρέπονται από το δίκτυο.

Η έννοια μιας κινητής συσκευής αποθήκευσης για δεδομένα του συνδρομητή έχει ανυπολόγιστης σημασίας συνέπειες. Σε προηγούμενα κυψελωτά συστήματα, εκτός του Γερμανικού C-δικτύου το οποίο εισήγαγε την έννοια της έξυπνης κάρτας όταν αυτή πέρασε στις επιτροπές του GSM, η πιστοποίηση του κινητού σταθμού απαιτούσε μια όχι τετριμμένη επέμβαση, μόνο από ειδικούς τεχνικούς και όχι από διοικητικούς υπαλλήλους. Αυτή η κατάσταση οδήγησε σε πολλά μειονεκτήματα. Ένας κινητός σταθμός μπορούσε να πουληθεί μόνο από ειδικευμένους εμπόρους, ικανούς όχι μόνο να εγκαταστήσουν τη συσκευή στο όχημα, αλλά και να δράσουν ως ένας μεσολαβητής ανάμεσα στον χρήστη και στον προμηθευτή υπηρεσιών για να πιστοποιήσει τη συσκευή. Αν τύχαινε ο σταθμός να χαλάσει, ήταν δύσκολο να εφοδιάσει τον χρήστη με έναν άλλο όσον καιρό διαρκούσε η επισκευή και σχεδόν αδύνατο να επιτρέψει στο χρήστη να κρατήσει τον ίδιο αριθμό καταλόγου όλον αυτόν τον καιρό.

Η αφαιρούμενη κάρτα SIM απλοποιεί αυτά τα θέματα και επίσης εισάγει και άλλα πλεονεκτήματα. Ένας βασικός χρήστης μπορεί φυσικά ν' αγοράσει μια κινητή συσκευή, αλλά μπορεί επίσης να την νοικιάσει ή να την μισθώσει για μια χρονική περίοδο και να την αλλάξει όπως αυτός επιθυμεί χωρίς πολύ διοίκηση. Αυτό που χρειάζεται είναι η δική του κάρτα SIM που μπορεί να ληφθεί από έναν διαχειριστή ή έναν παροχέα υπηρεσιών ανεξαρτήτως επιλογής συσκευής. Τα τελευταία βήματα της πιστοποίησης της κάρτας SIM μπορούν εύκολα να γίνουν μέσω ενός μικρού υπολογιστή και ενός απλού προσαρμογέα. Ο κινητός εξοπλισμός θα είναι για πώληση σε μια πολύ πιο ευρεία κλίμακα από ότι πριν καθόσον η απόκτησή του δεν θα χρειάζεται την παρέμβαση του διαχειριστή ή ενός παροχέα υπηρεσιών. Τα τηλέφωνα των αυτοκινήτων θα χρειάζονται βέβαια ακόμα εγκατάσταση στο όχημα αλλά τα φορητά ή χειρός θα ενθαρρύνουν τους χρήστες να αγοράζουν το κινητό τους από οποιοδήποτε κατάστημα.

Περισσότερα πλεονεκτήματα μπορούν να φανούν. Για παράδειγμα, τα νοικιασμένα αυτοκίνητα θα μπορούσαν να εφοδιαστούν με μια κινητή συσκευή που να μπορεί να χρησιμοποιηθεί με κάθε κάρτα SIM, είτε ιδιόκτητη είτε νοικιασμένη. Η αντίστροφη κατάσταση μπορεί επίσης να αποβεί προς όφελος των συνδρομητών αν όχι και των διαχειριστών: ένας συνδρομητής μπορεί ν' αλλάξει τον διαχειριστή που

τον εξυπηρετεί χωρίς αντικατάσταση του κινητού εξοπλισμού του (ΜΕ). Αλλά πάνω απ' όλα, αυτό το προσωπικό τσιπ ασφαλισμένο μέσα στην πλαστική θήκη του που καλείται κάρτα SIM, είναι το πρώτο τουβλάκι στο οικοδόμημα του προσωπικού τηλεπικοινωνιακού συστήματος δίνοντας τη δυνατότητα για ευρεία κινητικότητα μεταξύ των διαφορετικών τηλεπικοινωνιακών δικτύων.

5.6.: ΠΡΟΠΛΗΡΩΜΕΝΕΣ ΚΑΡΤΕΣ SIM

Επειδή οι πελάτες προτιμούν να γίνονται συνδρομητές στο πρώτο κατάστημα που συναντούν, αφήνοντας το πρακτορείο πωλήσεων να ασχοληθεί με την κάρτα τους SIM, είναι χρήσιμο για έναν διαχειριστή να προετοιμάσει όσο το δυνατόν περισσότερα πράγματα μπορεί εκ των προτέρων από την τελική περιγραφή.

Τυπικά, μέχρι τώρα, ο διαχειριστής διαχειριζόταν την πιστοποίηση και τα δεδομένα στις κάρτες SIM πριν την πραγματική επαφή με τον μέλλοντα συνδρομητή και μπορούσε ακόμα να μισο-συμπληρώσει τις αντίστοιχες εγγραφές στο HLR (Home Location Register - Καταχωρητή Οικείας Τοποθεσίας) το οποίο είναι μια βάση δεδομένων που περιέχει όλες τις πληροφορίες για τους χρήστες μιας περιοχής. Ο παροχέας υπηρεσιών έχει τότε στην κατοχή του έναν αριθμό από κάρτες SIM οι οποίες ήδη περιέχουν αποθηκευμένη μια IMSI (International Mobile Subscriber Identity - Διεθνής Ταυτότητα του Κινητού Συνδρομητή), το γνωστό μας διεθνή αριθμό τηλεφώνου, αλλά η οποία δεν μπορεί να χρησιμοποιηθεί σ' αυτό το στάδιο για λήψη υπηρεσιών (λόγω έλλειψης μιας κανονικής αρχικοποίησης στο HLR). Όταν δημιουργόταν η συνδρομή, ο παροχέας υπηρεσιών εισήγαγε τα δεδομένα που σχετίζονται με τον πελάτη στην δική του βάση δεδομένων και απέδιδε μια IMSI και μια κάρτα SIM στον νέο συνδρομητή. Κάτω από αυτό το σενάριο, ο παροχέας υπηρεσιών δεν χρειάζεται να εκτελέσει κάποια ενέργεια στην έτοιμη προς χρήση κάρτα SIM εκτός, πιθανώς, από το να τυπώσει το όνομα του συνδρομητή πάνω σ' αυτήν. Σε κάποια δίκτυα πωλήσεων, ο πελάτης μπορούσε να επιλέξει τον αριθμό καταλόγου του (τον MSISDN) μέσα από μια προτεινόμενη λίστα αριθμών.

Πρόσφατα όμως ανακοινώθηκε ότι εισήχθηκαν στην αγορά και προ-πληρωμένες (pre-paid) κάρτες SIM μέσω ενός ολοκληρωμένου πακέτου το οποίο

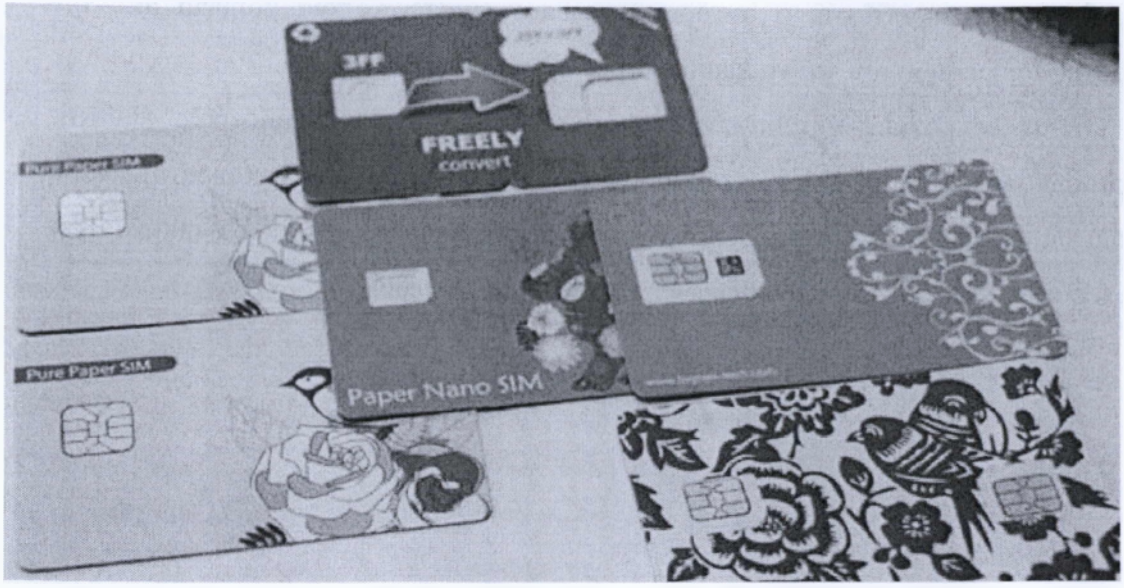
παρέχει τη δυνατότητα σε GSM κάρτες με εγκατεστημένη πίστωση να πωλούνται απευθείας στα μαγαζιά δίνοντας έτσι τη δυνατότητα στους εμπόρους να παρέχουν άμεση τηλεφωνική υπηρεσία αφού οι κάρτες είναι ήδη πληρωμένες από την εταιρεία. Το μυστικό είναι ότι, όπως και στις Τηλεκάρτες, οι κάρτες αυτές μπορούν να χρησιμοποιηθούν απευθείας από μια κινητή συσκευή διότι έχουν αποθηκευμένο έναν αριθμό από πιστωτικές μονάδες και είναι έγκυρες για ένα περιορισμένο χρονικό διάστημα. Μ' αυτές τις κάρτες δίνεται η δυνατότητα σε όποιον αγοράζει μια καινούργια κινητή συσκευή να έχει άμεση πρόσβαση σε μια τηλεφωνική υπηρεσία. Κάθε κάρτα έχει το δικό της λογαριασμό από τον οποίο αφαιρούνται μονάδες αυτόματα. Οι χρήστες μπορούν ακόμα να επικοινωνήσουν με μια υπηρεσία ψηφιακών απαντήσεων και να ρωτήσουν το υπόλοιπο του λογαριασμού τους. Το κινητό τηλέφωνο του ολοκληρωμένου πακέτου συνδέεται με την κάρτα μέσω ενός ειδικού κώδικα. Το πακέτο αυτό έχει επίσης μια απλή φόρμα, την οποία ο χρήστης πρέπει να στείλει στο διαχειριστή για να λάβει μια κανονική κάρτα SIM όταν λήξει η προθεσμία της προπληρωμένης κάρτας. Η νέα (κανονική) κάρτα SIM φθάνει μ' ένα ειδικό συνδιαστικό κλείδωμα (lock) το οποίο όταν εισαχθεί, ελευθερώνει τη γραμμή από την προπληρωμένη κάρτα.

Ο ρόλος του παροχέα υπηρεσιών για την φροντίδα του πελάτη δεν περιορίζεται μόνο στη συμπλήρωση νέων συνδρομών και στις αλλαγές τους. Πέρα από τον λογαριασμό, ο παροχέας υπηρεσιών πρέπει να εκτελέσει και ορισμένες υποχρεώσεις όπως βοήθεια στους πελάτες μετά την πώληση. Για παράδειγμα, η αναφορά για χαμένες κάρτες SIM πρέπει να χειριστεί γρήγορα και οι αντικαταστάσεις να προέρχονται με οποιαδήποτε IMSI, ενώ η IMSI της κλεμμένης κάρτας SIM απενεργοποιείται στο HLR. Ένα πρώτο επίπεδο προστασίας έναντι αθέμιτης χρήσης μιας κλεμμένης κάρτας SIM αποτελείται από το μπλοκάρισμα της ίδιας της κάρτας SIM, δηλ. την απαγόρευση κάθε προσπέλασης στο σύστημα όταν ένας λανθασμένος κώδικας PIN εισάγεται τρεις διαδοχικές φορές. Φυσικά, ο αφηρημένος αλλά νόμιμος ιδιοκτήτης της κάρτας SIM μπορεί περιστασιακά να πέσει ο ίδιος στην παγίδα. Για να αντιμετωπιστούν τέτοιες καταστάσεις, οι προδιαγραφές ορίζουν ένα Κλειδί Ξεμπλοκαρίσματος του PIN (το PUK - PIN Unblocking Key), διαφορετικό για κάθε PIN και το οποίο μπορεί να χρησιμοποιηθεί για να ξεμπλοκάρει την κάρτα SIM. Ανάλογα με την επιλογή του διαχειριστή, το PUK μπορεί να δοθεί στον συνδρομητή ή διαφορετικά να παραδοθεί μόνο στον παροχέα υπηρεσιών. Κι εδώ όμως οι

προσπάθειες είναι μετρημένες. Δέκα αποτυχημένες πληκτρολογήσεις σημαίνουν καταστροφή της κάρτας SIM, που στη συνέχεια πρέπει ν' αποκατασταθεί από το διανομέα, με κάποια οικονομική επιβάρυνση. Ο χρόνος αντικατάστασης, πάντως, είναι άμεσος και ο αριθμός κλήσεως παραμένει ο ίδιος. Ο κωδικός PUK είναι μοναδικός και δεν αλλάζει σε αντίθεση με τον PIN που αλλάζει. Στην άλλη (και ασφαλέστερη) περίπτωση, ο συνδρομητής θα χρειαστεί κάποια βοήθεια από τον παροχέα υπηρεσιών του για να ξεμπλοκάρει την κάρτα SIM του.

Η μελλοντική εξέλιξη θα είναι η εφαρμογή της νέας "πολυχρηστικής" έξυπνης κάρτας, που θα είναι συγχρόνως αριθμομηχανή, βάση δεδομένων και ταυτότητα και η οποία θα αποτελεί το μοναδικό μέσο για τις πάσης φύσεως εμπορικές, οικονομικές και άλλες συναλλαγές των ανθρώπων σε παγκόσμιο επίπεδο.

6.1.: ΧΑΡΤΙΝΕΣ ΚΑΡΤΕΣ SIM



Μια κινεζική εταιρεία τεχνολογίας και συγκεκριμένα η εταιρεία Beijing Big Ben Technology, αναπτύσσει περιβαλλοντικά φιλικές κάρτες SIM για κινητά, οι οποίες είναι φτιαγμένες από χαρτί. Η κινεζική εταιρεία παρουσίασε τις πρωτοποριακές κάρτες SIM στη Διεθνή Έκθεση Κινητής Τηλεφωνίας, που διοργανώνεται στη Βαρκελώνη.

Οι συμβατικές κάρτες SIM κατασκευάζονται από ανακυκλώσιμο πλαστικό και μέταλλο (τα σημεία επαφής).

Οι οικολογικές κάρτες SIM των Κινέζων είναι εξολοκλήρου από συνθετικές ίνες χαρτιού, οι οποίες ανακυκλώνονται πολύ ευκολότερα από το πλαστικό.

Η κινεζική εταιρεία *Beijing Big Ben Technology* κατασκευάζει χάρτινες κάρτες SIM εδώ και πέντε χρόνια και υποστηρίζει ότι κοστίζουν το ίδιο με τις πλαστικές. Τις χάρτινες κάρτες χρησιμοποιεί η Chine Mobile, αλλά η Big Ben φιλοδοξεί να προσελκύσει πελάτες σε όλο τον κόσμο που θέλουν να χτίσουν έμπρακτα ένα οικολογικό προφίλ. Επομένως, ευελπιστεί να διευρύνει σύντομα τη λίστα πελατών της, προσελκύοντας τηλεπικοινωνιακούς κολοσσούς παγκόσμιου βεληνεκούς που προσπαθούν να επιδείξουν ένα πιο φιλικό προς το περιβάλλον πρόσωπο.

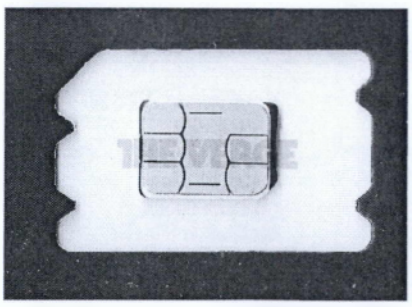
6.3.: Η ΚΑΡΤΑ SIM ΜΙΚΡΑΙΝΕΙ

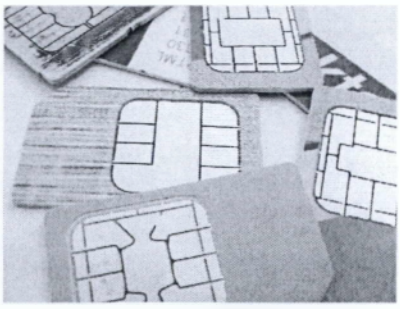
Το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (European Telecommunications Standards Institute – ETSI) προχώρησε στη δημιουργία ενός νέου προτύπου form factor που αφορά στις γνωστές κάρτες SIM, μεγέθους 40% μικρότερου από τη μικρότερη SIM που κυκλοφορεί σήμερα.

Η ανακοίνωση έγινε στο πλαίσιο της 55ης ετήσιας συνάντηση του ETSI, που διεξήχθη στην Οσάκα της Ιαπωνίας.

Ο χώρος (και γενικότερα το μέγεθος) αποτελεί ένα από τα σημαντικότερα προβλήματα στη σχεδίαση των σύγχρονων κινητών που ενσωματώνουν ολοένα και περισσότερα χαρακτηριστικά και είναι πλέον γενικά παραδεκτό ότι οι σημερινές κάρτες SIM καταλαμβάνουν σημαντικό κομμάτι αυτού του χώρου.

Το νέο form factor του ETSI (fourth form factor – 4FF) αφορά σε κάρτες SIM 40% μικρότερες από το μέγεθος των μικρότερων SIM που κυκλοφορούν σήμερα και, συγκεκριμένα, αναφέρεται σε διαστάσεις 12,3 (πλάτος) x 8,8 (ύψος) x 0,67 (πάχος) χιλιοστών. Μάλιστα, μπορεί να συσκευαστεί και να διανεμηθεί με τρόπο συμβατό με τους υπάρχοντες σχεδιασμούς SIM. με τη χρήση ειδικού αντάπτορα Η νέα κάρτα SIM θα προσφέρει την ίδια λειτουργικότερα με τις υπάρχουσες κάρτες, ενώ αξίζει να σημειωθεί ότι η κάρτα SIM είναι ένα από τα αδιαμφισβήτητα success stories στον χώρο των έξυπνων καρτών. Να σημειώσουμε ότι το πρότυπο που επιλέχτηκε είναι αυτό που πρότεινε η Apple





Η κάρτα SIM αποτελεί την πιο επιτυχημένη έκδοση "έξυπνης" κάρτας. Μέχρι σήμερα έχουν κατασκευαστεί πάνω από 25 δις κάρτες SIM, ενώ 4,5 δις παράγονται κάθε χρόνο!

Η νέα μικρότερη SIM υιοθετήθηκε ήδη από την ευρύτερη βιομηχανία που περιλαμβάνει τους σημαντικότερους παρόχους κινητής τηλεφωνίας και τους κατασκευαστές κινητών τηλεφώνων και καρτών παγκοσμίως. Το νέο σχέδιο αναμένεται σύντομα να δημοσιευθεί ως προδιαγραφή και να ανοίξει ο δρόμος για την παραγωγή της.

ΚΕΦΑΛΑΙΟ 7: NFC ΤΕΧΝΟΛΟΓΙΑ

7.1.:NFC ΕΙΣΑΓΩΓΙΚΑ

Η επικοινωνία κοντινού πεδίου (near field communication, NFC) αποτελεί μια πρότυπη τεχνολογία συνδεσιμότητας, η οποία διαδίδεται και εξελίσσεται ραγδαία με κύριο σκοπό τη λύση αρκετών προβλημάτων, σύγχρονων αλλά και μελλοντικών. Είναι μια μικρής εμβέλειας ασύρματη τεχνολογία, η οποία λειτουργεί στη συχνότητα των 13,56 MHz 56MHz (ενδεικτικά, ένα ασύρματο τηλέφωνο λειτουργεί σε συχνότητες κοντά στα 2GHz) και μεταφέρει δεδομένα με ρυθμό έως και 424 kbps (που μπορεί κάποιοι να τη θεωρήσουν χαμηλή, με αυτή την ταχύτητα σε ένα λεπτό θα έχουν μεταφερθεί 3,2MB περίπου το μέγεθος ενός «μικρού» τραγουδιού σε μορφή MP3), όμως αυτή η ταχύτητα αναμένεται να αυξηθεί μελλοντικά και έχει γίνει γνωστή κυρίως μέσω της χρήσης της από τα κινητά τελευταίας γενιάς (smartphones). Η κατανάλωση είναι μόλις στα 15mA (περίπου όση χρειάζεται ένα LED φωτάκι για να ανάψει) αν και ενδέχεται να είναι περισσότερη όταν υπάρχει εγγραφή δεδομένων. Η λειτουργία της βασίζεται στην επαφή ή στην προσέγγιση, σε απόσταση περίπου τεσσάρων με πέντε εκατοστών, της συσκευής που περιέχει το τσιπ NFC, σε κάποια άλλη συσκευή που περιλαμβάνει τον κατάλληλο αισθητήρα.

7.2. ΙΣΤΟΡΙΑ NFC

Η τεχνολογία αυτή δημιουργήθηκε το 2004 μετά από συνεργασία της Nokia, της Philips και της Sony, με την εξάπλωση της να είναι μεγαλύτερη των προσδοκιών και να μελετάται συνεχώς για περισσότερους τομείς της καθημερινότητας, όπως για παράδειγμα η γρήγορη ανάγνωση και εγγραφή δεδομένων, η χρήση εικονικών πιστωτικών καρτών, η πιστοποίηση οντοτήτων αλλά και η ενεργοποίηση υπηρεσιών.

Η τεχνολογία NFC συνδυάζει παλιότερες τεχνολογίες ασύρματης επικοινωνίας όπως το Bluetooth και η RFID, οι οποίες εναρμονίζονται ώστε να παρέχονται υπηρεσίες στους χρήστες στις παρακάτω ενδεικτικές περιπτώσεις:

- Έλεγχος πρόσβασης

- Ηλεκτρονικές συναλλαγές
- Ανταλλαγή και συλλογή πληροφοριών
- Νομιμότητα
- Πληρωμές
- Μεταφορές/Διαβιβάσεις
- Πιστοποιήσεις

Η τεχνολογία της επικοινωνίας κοντινού πεδίου πληροί τις προδιαγραφές των standard ISO/IEC 14443 A&B και Felica (ISO 18092) και προωθήθηκε κυρίως μέσω του NFC Forum (2004) στο οποίο συμμετέχουν 140 γνωστές εταιρίες και από άλλους οργανισμούς. Το NFC ορίζει τρεις κατηγορίες λειτουργίας:

- λειτουργία γρήγορης ανάγνωσης/εγγραφής (read/write mode, 48 Byte-9KB)
- λειτουργία Peer-to-Peer μέσω σύνδεσης δύο συσκευών ομότιμης σχέσης
- λειτουργία NFC καρτών εξομοίωσης που επιτρέπει στη συσκευή να συμπεριφέρεται στα πρότυπα μιας smartcard (μπρελόκ, αυτοκόλλητα, έξυπνες κάρτες με διαφορετική χωρητικότητα)

Η τεχνολογία NFC διαδίδεται με πολύ γρήγορους ρυθμούς λόγω της αξιοποίησης τους από τα έξυπνα κινητά (smartphones) Για αυτό το λόγο τον Νοέμβρη του 2011 οι 45 μεγαλύτερες εταιρίες κινητής τηλεφωνίας του κόσμου με κοινή τους ανακοίνωση δεσμεύτηκαν να υποστηρίξουν τις νέες κάρτες SIM που θα ενσωματώνουν την τεχνολογία NFC. Παρακάτω εμφανίζονται ονομαστικά οι τεχνολογίες NFC:

- **NDEF** (NFC Data Exchange Format)
- **RTD** (Record Type Definition)
- **NDEF** message
- **NDEF** record
- **NDEF** payload

Γενικότερα, η συγκεκριμένη τεχνολογία επιτρέπει σε συσκευές (κυρίως smartphones και tablets) να ανταλλάσσουν πληροφορίες μεταξύ τους ή με συγκεκριμένες «κάρτες» NFC με τον τρόπο περίπου που οι card readers διαβάζουν τις πιστωτικές κάρτες. Υπάρχουν πολλές πρακτικές εφαρμογές που είναι ήδη διαθέσιμες σε μερικές χώρες (περισσότερο στην Ιαπωνία), ενώ το NFC είναι ένα «ανοικτό πρότυπο» πράγμα που σημαίνει πως υπάρχει αρκετός χώρος για καινοτομία στις εφαρμογές τις εν λόγω τεχνολογίας.

7.3.: ΠΛΕΟΝΕΚΤΗΜΑΤΑ NFC

- Οι NFC αλληλεπιδράσεις είναι εύκολες και απλές καθώς δεν χρειάζεται παρά μόνο ένα απλό άγγιγμα.
- Η χρήση NFC είναι ιδανική για το ευρύτερο φάσμα των επιχειρήσεων καθώς είναι εύκολη στη χρήση, βελτιώνει την επικοινωνία μεταξύ των μελών της επιχείρησης.
- Η NFC τεχνολογία διευκολύνει την απλή και γρήγορη εγκατάσταση των ασύρματων τεχνολογιών όπως το Bluetooth και το WiFi.
- Είναι εγγενώς ασφαλής η χρήση καθώς οι μεταδόσεις είναι μικρής εμβέλειας (από ένα άγγιγμα σε μόλις λίγα εκατοστά). Επίσης σημαντικό χαρακτηριστικό είναι ότι δεν μπορεί να γίνει υποκλοπή δεδομένων ασύρματα.
- Βρίσκει εφαρμογή σε πολλές χρήσεις όπως στις πληρωμές, στα εισιτήρια, στη διαφήμιση, στις έξυπνες κάρτες, στην ανταλλαγή δεδομένων, στην κρυπτογράφηση παρουσίας και στον έλεγχο πρόσβασης.
- Αξιοποιεί τα κινητά τηλέφωνα ως μέσο αλληλεπίδρασης. Είναι ευρέως διαδεδομένα και τα κουβαλάμε πάντα μαζί μας, έχουν επεξεργαστή, έχουν συνήθως πρόσβαση στο διαδίκτυο, είναι διαδραστικά (πληκτρολόγιο, οθόνη αφής) και διαθέτουν ώριμα λειτουργικά συστήματα.

7.3.1.: Τελικά γιατί χρησιμοποιούμε το NFC όταν υπάρχει Bluetooth και το Wi-Fi;

Το Bluetooth και το Wi-Fi έχουν μεγαλύτερο εύρος σύνδεσης από το NFC. Αυτό σημαίνει πως υπάρχει μία θεωρητική ακτίνα που μπορούν να συνδεθούν δύο συσκευές η οποία ποικίλει από ένα μέτρο μέχρι εκατό μέτρα. Αυτό δημιουργεί δύο προβλήματα:

Εάν οι συσκευές είναι έτσι ρυθμισμένες ούτως ώστε να δέχονται συνδέσεις χωρίς κάποιο κωδικό (είναι δηλαδή «ελεύθερες») ο οποιοσδήποτε μπορεί να συνδεθεί και να πάρει πληροφορίες δημιουργώντας έτσι σημαντικά προβλήματα ασφαλείας.

Εάν υποθέσουμε ότι χρησιμοποιούμε κάποιο password προκειμένου να εξαλείψουμε το πρώτο πρόβλημα τότε αυτομάτως οι χρήστες θα πρέπει να

πλοηγηθούν στη συσκευή τους, και να εισάγουν το σωστό password πράγμα που σημαίνει ότι χάνεται ο παράγοντας «ευκολία».

Το NFC εξαλείφει και τα δύο αυτά προβλήματα απαιτώντας από τις δύο συσκευές να βρίσκονται αρκετά κοντά (μέχρι 20 εκατοστά) ενώ με το που γίνει η σύνδεση εμφανίζονται αυτόματα οι επιλογές στην οθόνη της συσκευής προκειμένου ο χρήστης να επιλέξει αυτό που θέλει εύκολα και γρήγορα.

7.4. ΜΕΙΟΝΕΚΤΗΜΑΤΑ

- Τα συστήματα NFC είναι εύκολο να υποκλαπούν. Οποιοσδήποτε είναι σε θέση να κλέψει τις προσωπικές πληροφορίες του καθενός πολύ εύκολα και αυτό γιατί δεν υπάρχει κάποιο αυστηρό μέτρο ασφαλείας. Μια προσθήκη θα μπορούσε να είναι ένα σύστημα αναγνώρισης προσώπου ή αναγνώρισης δακτυλικών αποτυπωμάτων.
- Η χρήση του NFC εκπέμπει ακτινοβολία.
- Ένα άλλο θέμα είναι ότι επειδή η λειτουργία του NFC γίνεται εξ αποστάσεως υπάρχει ο κίνδυνος απώλειας των δεδομένων.

7.5. ΕΦΑΡΜΟΓΕΣ ΤΟΥ NFC

7.5.1.: Πραγματικές εφαρμογές του NFC

- **Σαν RFID Scanner**

Μία συσκευή με NFC μπορεί να λειτουργήσει σαν ένα RFID Tag Scanner διαβάζοντας πληροφορίες που βρίσκονται με τη μορφή RFID tags (μικρά τσιπάκια λίγων χιλιοστών που περιέχουν πληροφορίες και που βρίσκονται οπουδήποτε υπό μορφή αυτοκόλλητου) σε αφίσες, φυλλάδια, διαφημίσεις και άλλα μέσα προβολής. Για παράδειγμα, φαντάσου πως πηγαίνεις σε ένα εστιατόριο και ακουμπάς το

smartphone ή το tablet σου στο μενού. Αυτομάτως στην οθόνη της συσκευής σου εμφανίζονται με διαδραστικό τρόπο τα πιάτα του εστιατορίου, τα σπέσιαλ της ημέρας, βίντεο με την παρασκευή του κάθε πιάτου και πολλά ακόμα.

- **Σαν πιστωτική κάρτα**

Το NFC μπορεί πολύ εύκολα να αντικαταστήσει την πιστωτική σου κάρτα με το τηλέφωνό σου. Μόλις οι πληροφορίες της κάρτας σου μεταφερθούν στη συσκευή σου (υπεύθυνη για αυτή τη διαδικασία θα είναι η τράπεζα), τότε μπορείς με ένα απλό άγγιγμα του smartphone σου να πληρώνεις σαν να είχες μαζί την πιστωτική σου κάρτα.

- **Σαν επαγγελματική κάρτα**

Η τεχνολογία NFC έχει ήδη αρχίσει να αντικαθιστά τις επαγγελματικές κάρτες. Το μόνο που χρειάζεται να κάνεις είναι να φέρεις κοντά δύο smartphones και αμέσως τα δεδομένα του ενός μεταφέρονται στην συσκευή του άλλου και αποθηκεύονται χωρίς να χρειάζεται να κάνεις τίποτα περισσότερο, άμεσα, εύκολα και γρήγορα.

- **Σύνδεση με Bluetooth και Wi-Fi**

Το NFC μπορεί να χρησιμοποιηθεί και σε συνδυασμό με τις συνδέσεις Bluetooth και Wi-Fi κάνοντές τες μια εύκολη διαδικασία. Φέρνοντας κοντά τις δύο συσκευές που θέλεις να ενώσεις μέσω Bluetooth αυτομάτως εμφανίζεται η επιλογή στην οθόνη των συσκευών και με ένα μόνο άγγιγμα οι συσκευές αυτές ενώνονται. Το ίδιο μπορεί να γίνει και για τη σύνδεση σε ένα Wi-Fi.

7.5.2.: Μελλοντικές εφαρμογές του NFC

Παρακάτω παρουσιάζονται μερικά παραδείγματα για το πώς μπορεί να εφαρμοστεί το NFC στο μέλλον.

- **Προσωπικές πληρωμές**

Αντί να δίνουμε χρήματα σε κάποιον, το μόνο που θα χρειάζεται να κάνουμε είναι να αγγίξουμε το κινητό μας με του άλλου και να του μεταφέρουμε το ποσό που επιθυμούμε

- **Κλειδί χωρίς... κλειδί**

Η συσκευή σου μπορεί να λειτουργήσει σαν κλειδί για το αυτοκίνητό μας, το σπίτι ή το χρηματοκιβώτιό σου. Βέβαια, προκειμένου να απωθηθούν διάφοροι «καλοθελητές» από το να μας κλέψουν το κινητό και να έχουν πρόσβαση στα πάντα, το NFC θα ξεκινάει τη διαδικασία πιστοποίησης η οποία θα ολοκληρώνεται με τον έλεγχο του προσώπου σου, ή της ίριδας του ματιού σου.

- **Κατάργηση της γραφειοκρατίας**

Παρόλο που μπορεί να φαντάζει ουτοπικό, το NFC μπορεί να χρησιμοποιηθεί για να αποθηκεύσουμε την ταυτότητά μας, την άδεια οδήγησης, το διαβατήριό μας και πολλά ακόμα. Ένα άγγιγμα μόνο αρκεί για την εκάστοτε υπηρεσία να παίρνουμε τις πληροφορίες που χρειαζόμαστε από τη συσκευή μας.

- **Υγεία και Ασφάλιση**

Οι γιατροί θα μπορούν να χρησιμοποιήσουν το NFC προκειμένου να ενημερωθούν για την υγεία των ασθενών τους. Οι ασθενείς θα έχουν «φορτώσει» τη συσκευή τους με πληροφορίες για την υγεία τους οι οποίες πληροφορίες θα συλλέγονται από συσκευές που θα είναι συνδεδεμένες πάνω τους και θα έχουν συγχρονιστεί με το smartphone τους. Ομοίως κάποιος που θα κάνει εισαγωγή σε ένα νοσοκομείο θα μπορεί να κάνει check-in κατά την είσοδό του, και αυτομάτως το σύστημα θα ενημερώνεται για το ιστορικό του.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η προστιθέμενη αξία που προσφέρουν οι έξυπνες κάρτες στο μηχανισμός ασφαλείας των ασύρματων συστημάτων όπως το IEEE 802.11 είναι ότι εισάγει ένα κρυφό επίπεδο που ενσωματώνει νοημοσύνη απορρήτου. Αυτό το μυστικό στρώμα είναι σε θέση να συνεργάζεται με όλα τα εμπλεκόμενα λειτουργικά στοιχεία (Χρήστης, μηχανισμός επιπέδου σύνδεσης δεδομένων, Υψηλότερος μηχανισμός επιπέδου) ως μεσολαβητής ελέγχου ταυτότητας. Αυτό βασίζεται στα χαρακτηριστικά του συστήματος ασφαλείας της έξυπνης κάρτας που επιτρέπουν διαβαθμισμένη πρόσβαση στα περιεχόμενά του συστήματος αρχείων για μια ποικιλία χρήστες. Ως εκ τούτου, το απόρρητο αυξάνεται και τα μυστικά αποκαλύπτονται μόνο με εγκεκριμένες διαδικασίες. Αυτό το επιπλέον επίπεδο δεν μπορεί να ανιχνευθεί ευθέως και επομένως η πολυπλοκότητα του συστήματος αυξάνεται και η προσπάθεια αυτών που προσπαθούν να παραβιάσουν το σύστημα ασφαλείας των έξυπνων καρτών γίνεται ακόμη πιο δύσκολη εξαιτίας προσπάθειες της πολυπλοκότητας αυτής.

Σχετικά με την κάρτα SIM αξίζει να σημειώσουμε ότι πρόκειται για μια έξυπνη κάρτα που αποθηκεύει με ασφάλεια το κλειδί για τον προσδιορισμό ενός συνδρομητή κινητής τηλεφωνίας, καθώς και πληροφορίες εγγραφής, προτιμήσεις και τα μηνύματα κειμένου και ταυτοποιεί το τηλεφωνικό αριθμό του χρήστη. Επιτρέπεται στον χρήστη να διατηρεί τις πληροφορίες του όταν αλλάζει συσκευές τηλεφώνου. Καθώς και να αλλάζει πάροχο έχοντας την ίδια τηλεφωνική συσκευή αλλά αλλάζοντας την κάρτα SIM. Η μελλοντική της εξέλιξη θα είναι η εφαρμογή μιας νέας "πολυχρηστικής" έξυπνης κάρτας, που θα είναι συγχρόνως αριθμομηχανή, βάση δεδομένων και ταυτότητα και η οποία θα αποτελεί το μοναδικό μέσο για τις πάσης φύσεως εμπορικές, οικονομικές και άλλες συναλλαγές των ανθρώπων σε παγκόσμιο επίπεδο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Tanebaum A. (μετάφραση: Ξυλωμένος Γ.), 2008, *Δίκτυα Υπολογιστών*, Κλειδάριθμος, Αθήνα

Rankl W., Effing W., 2003, *Smart Card Handbook*, Willey and Sons, Munich

ΑΡΘΡΟΓΡΑΦΙΑ

Giannis A. Pikrammenos, Vasilios Anagnostopoulos, (χ.χ.) *Bidirectional, Multi-Layer Peer-to-Peer Authentication in WLAN Network Using Smart Cards as Mediators*, Αθήνα

Giannis A. Pikrammenos, (χ.χ.), *Smart Media as the Secure Transactions Mediator of the future*, National Technical University of Athens, PhD, MBA

Giannis A. Pikrammenos, (χ.χ.), Sma*rt Card Secure Environments for Mobile Privacy and Security*, PhD., MBA

ΠΗΓΕΣ ΑΠΟ INTERNET

4G: The What, Why and When. The worldwide adoption and growth of wireless are the fastest technological achievements in history., 2012, Tellabs

Χάρτινες» οικολογικές κάρτες SIM για κινητά τηλέφωνα, 26/02/2013, www.skai.gr

http://en.wikipedia.org/wiki/