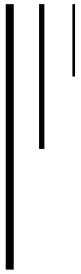


Πανεπιστήμιο Πειραιώς – Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

« **Ασφάλεια Ψηφιακών Συστημάτων** »

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Android Security**
Ονοματεπώνυμο Φοιτητή	**Ιωάννης Μαρινάκης**
Πατρώνυμο	**Ελευθέριος**
Αριθμός Μητρώου	**MTE 1116**
Επιβλέπων	**Χρήστος Ξενάκης,** Επίκουρος Καθηγητής

Ιούλιος 2013

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Περίληψη

Σήμερα διανύουμε μια περίοδο που συντελείται και μια μεγάλη αλλαγή στον τομέα των ηλεκτρονικών υπολογιστών. Παρατηρείται λοιπόν, μια σταδιακά μετάβαση από το τους επιτραπέζιους υπολογιστές στις κινητές συσκευές. Οι μοντέρνες φορητές συσκευές όπως τα smartphones και τα Tablet pc προσφέρουν την δυνατότητα επεξεργασίας κάθε στιγμή και οπουδήποτε.

Οι κινητές συσκευές διαδραματίζουν σπουδαίο ρόλο τόσο στην προσωπική όσο και στην επαγγελματική ζωή των χρηστών. Η χρήση ισχυρών επεξεργαστών , η σύνδεση σε wifi ή 4G δίκτυα, η ύπαρξη ισχυρών φωτογραφικών μηχανών και οθονών αφής είναι μόνο μερικά από τα χαρακτηριστικά των κινητών συσκευών, που επιτρέπουν στον χρήστη να κάνει σχεδόν τα πάντα.

Η ραγδαία όμως εξάπλωση των κινητών συσκευών δημιούργησε και μια πληθώρα νέων επιθέσεων από κακόβουλους εισβολείς που με στόχο το προσωπικό κέρδος, εξαπατούν τους χρήστες, κλέβουν ή και καταστρέφουν τα προσωπικά δεδομένα αυτών. Ο επιτιθέμενος είτε μέσω επιθέσεων διαδικτύου είτε μέσω μολυσμένων με κακόβουλο κώδικα εφαρμογών προσπαθεί να διεισδύσει στην ιδιωτική ζωή των χρηστών.

Το android είναι ένα λειτουργικό σύστημα που απευθύνεται σε κινητές συσκευές. Το συγκεκριμένο λειτουργικό έχει μεγάλη απήχηση στην αγορά καθώς καταλαμβάνει την πρώτη θέση στις προτιμήσεις των καταναλωτών. Όμως παρά τους μηχανισμούς ασφαλείας που διαθέτει, γίνεται ολοένα και μεγαλύτερος στόχος για τους κακόβουλους χρήστες σε όλο τον κόσμο.

Η κατανόηση του τρόπου λειτουργίας των επιθέσεων που πραγματοποιούνται στις κινητές συσκευές και η ευαισθητοποίηση από πλευράς χρηστών των κινδύνων στους οποίους είναι εκτεθειμένοι, είναι στοιχεία που οδηγούν στην καλύτερη θωράκιση των δεδομένων με αξία καθώς επίσης και στην αποτελεσματικότερη αντιμετώπιση των απειλών.

Abstract

Today we live in a transitional period from desktop computing to ubiquitous computing. Modern mobile devices, such as smartphones and tablet pc's, offer the capability of any time - any place computing. Mobile devices and applications have acquired critical importance both in our personal and professional lives. More than enough processing power, readable screen, powerful camera, Wi-Fi, 4G are some of the characteristics of a mobile device that allow users to do almost anything.

The rapid spread of mobile devices has created a plethora of attacks by malicious users who aim at personal gain, deceive users, and steal or destroy their personal data. The hacker either attacks via the Internet or via malware application trying to intrude into the privacy of the users. The android is an operating system targeting at mobile devices and has a great impact on the market; it is in fact a leader in consumer preferences. But despite the security mechanisms available, it is increasingly becoming a large target for hackers worldwide. An understanding of how the hacking on mobile devices is made and the awareness from users of the risks they are exposed to, can lead to a better protection of the valuable data as well as a more effective way to deal with threats.

Περιεχόμενα

Πίνακας Εικόνων

Εισαγωγή

Στις μέρες μας διανύουμε το χρυσό αιώνα των τεχνολογικών επιτευγμάτων. Ότι πριν από μερικές δεκαετίες φαινόταν απίθανο και ουτοπικό, σήμερα χάρη στην τεχνολογική εξέλιξη γίνεται πραγματικότητα. Η επικοινωνία έγινε ευκολότερη, η εκπαίδευση εμπλουτίστηκε, η ενημέρωση έγινε αμεσότερη, η ιατρική εξελίχθηκε και η βιομηχανική παραγωγή αναβαθμίστηκε. Ένα από τα μεγαλύτερα επιτεύγματα της τεχνολογικής προόδου είναι ο ηλεκτρονικός υπολογιστής. Ο ηλεκτρονικός υπολογιστής έφερε την επανάσταση στην καθημερινότητα των ανθρώπων σε όλο τον κόσμο. Πληθώρα λειτουργιών και υπηρεσιών τίθενται στη διάθεση εκατομμυρίων χρηστών επηρεάζοντας και γενικά αλληλεπιδρώντας τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο.

Σήμερα όμως διανύουμε και μια περίοδο που συντελείται και μια μεγάλη αλλαγή στον τομέα των ηλεκτρονικών υπολογιστών. Παρατηρείται λοιπόν μια σταδιακά μετάβαση από το τους επιτραπέζιους υπολογιστές στις κινητές συσκευές. Οι μοντέρνες φορητές συσκευές όπως τα smartphones και τα Tablet pc προσφέρουν την δυνατότητα επεξεργασίας κάθε στιγμή και οπουδήποτε. Αυτό μαρτυρούν και πολλές επίσημες έρευνες. Ενώ οι αποστολές συσκευών σε όλο τον κόσμο (συνδυασμένες αποστολές υπολογιστών, tablets, και κινητών τηλεφώνων) προβλέπεται να φτάσουν τα 2,35 δισεκατομμύρια μονάδες το 2013, σημειώνοντας 5,9% αύξηση από το 2012, οι παγκόσμιες αποστολές PC (επιτραπέζιοι και notebook) προβλέπεται να φθάσουν σε 305 εκατομμύρια μονάδες το 2013, σημειώνοντας μείωση 10,6% από το 2012, σύμφωνα με την Gartner. [1]

Worldwide Devices Shipments by Segment (Thousands of Units)

Device Type	2012	2013	2014
PC (Desk-Based and Notebook)	341,273	305,178	289,239
Ultramobile	9,787	20,301	39,824
Tablet	120,203	201,825	276,178
Mobile Phone	1,746,177	1,821,193	1901,188
Total	**2,217,440**	**2,348,497**	**2,506,429**

Εικόνα 1 - Παγκόσμιες πωλήσεις φορητών συσκευών και pc

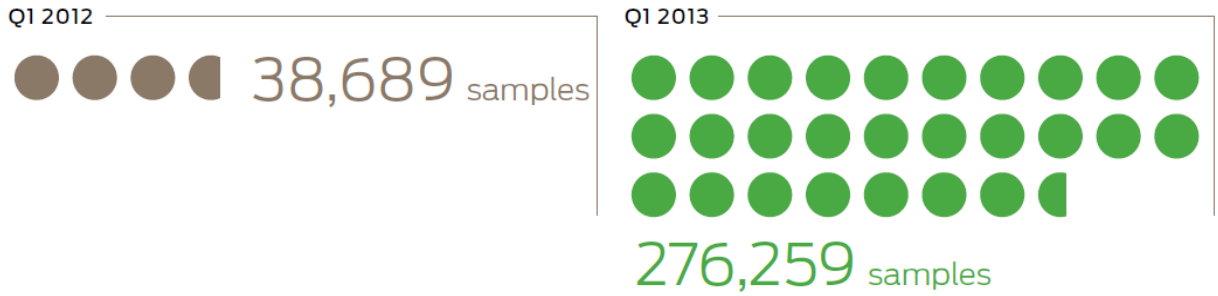
Η αγορά οδηγείται από τις πωλήσεις σε tablets, smartphones (Εικόνα 1). Οι αποστολές tablet αναμένεται να αυξηθούν κατά 67,9%, στα 202 εκατομμύρια μονάδες,

ενώ η αγορά κινητών συσκευών θα αυξηθεί κατά 4,3%, με όγκο πάνω από 1,8 δισεκατομμύρια μονάδες. Η απότομη πτώση των πωλήσεων PC που καταγράφεται στο πρώτο τρίμηνο ήταν αποτέλεσμα αλλαγής στις προτιμήσεις, τις ανάγκες και τις επιθυμίες των καταναλωτών. Οι καταναλωτές θέλουν ανά πάσα στιγμή, οπουδήποτε σύνδεση και κατανάλωση περιεχομένου (Mobile content), να δημιουργήσουν περιεχόμενο με ευκολία, καθώς και να έχουν τη δυνατότητα να μοιραστούν και να αποκτήσουν πρόσβαση σε αυτό το περιεχόμενο από ένα διαφορετικό χαρτοφυλάκιο προϊόντων.

Κινητό περιεχόμενο είναι οποιοσδήποτε τύπος των ηλεκτρονικών μέσων τα οποία είναι διαθέσιμα στις κινητές συσκευές, όπως ήχους κλήσης, τα γραφικά, παιχνίδια, ταινίες, και η πλοήγηση μέσω GPS. Οι ιδιοκτήτες των κινητών συσκευών μπορούν πλέον να χρησιμοποιούν τις συσκευές τους για να προγραμματίζουν τις συναντήσεις τους, να αποστέλλουν και λαμβάνουν μηνυμάτων κειμένου (SMS) η ηλεκτρονικού ταχυδρομείου (mail) , να ακούσουν μουσική, να βλέπουν βίντεο, να εξαργυρώνουν τα κουπόνια για αγορές, να διαχειριστούν έγγραφα, να πλοηγηθούν στο διαδίκτυο, να πάρουν οδηγίες κατεύθυνσης στο χάρτη, και ούτω καθεξής.

Όμως η ραγδαία ανάπτυξη της χρήσης των κινητών συσκευών είχε σαν αποτέλεσμα να οδηγήσει και στην αύξηση των κρουσμάτων ηλεκτρονικού εγκλήματος. Ολοένα και περισσότεροι κακόβουλοι χρήστες προσπαθούν να εκμεταλλευτούν τις ευπάθειες των συσκευών ή την άγνοια κινδύνου των χρηστών ώστε να αποκτήσουν πρόσβαση στις κινητές συσκευές. Οι κινητές συσκευές λόγω του σημαντικού ρόλου που διαδραματίζουν στη ζωή των χρηστών, περιέχουν μια πληθώρα προσωπικών και επαγγελματικών δεδομένων από προσωπικούς τηλεφωνικούς καταλόγους και αριθμούς τραπεζικών λογαριασμών έως σημαντικά εταιρικά έγγραφα. Η πρόσβαση κάποιου στα δεδομένα αυτά είναι σαν να του ανοίγεται μια πόρτα στην ιδιωτική ζωή του χρήστη.

Η εγκατάσταση μολυσμένων εφαρμογών με κακόβουλο λογισμικό, η απάτη με σκοπό την υπερχρέωση, η κλοπή της ηλεκτρονικής ταυτότητας και η παράνομη πρόσβαση σε ιδιωτικούς τραπεζικούς λογαριασμούς αποτελούν μόνο μερικές από μια μεγάλη λίστα επιθέσεων που έχουν μπορούν να εξαπολύσουν οι κακόβουλοι εισβολείς σε μια κινητή συσκευή. Τον Μάρτιο του 2013, η Juniper MTC παρατήρησε 614% αύξηση των malware εφαρμογών σε όλες τις κινητές πλατφόρμες σε σύγκριση με την ίδια χρονική περίοδο του προηγούμενου έτους. [2] Το σύνολο των εντοπισμένων malware εφαρμογών σε όλες τις πλατφόρμες αυξήθηκε από 38.689 στο τέλος του πρώτου τριμήνου του 2012 σε 276.259 στο τέλος του πρώτου τριμήνου του 2013 (Εικόνα 2).



Εικόνα 2 - Σύνολο εντοπισμένων malware εφαρμογών

Όλες αυτές λοιπόν οι επιθέσεις που στόχο έχουν να άρουν το απόρρητο των προσωπικών δεδομένων του χρήστη, δίνουν το έναυσμα για να ξεκινήσει μια ουσιαστική διερεύνηση των μέτρων ασφαλείας που παρέχουν οι σημερινές σύγχρονες κινητές συσκευές καθώς και τα αντίστοιχα λειτουργικά συστήματα που χρησιμοποιούν. Κενά ασφαλείας, παραλήψεις και καθυστέρηση αποστολής ενημέρωσης των εκδόσεων είναι μόνο μερικά από τα προβλήματα που εντοπίζονται και υπόκεινται άμεσης διόρθωσης από της κατασκευάστριες εταιρίες.

Πέρα όμως από τις τεχνικές και αυτοματοποιημένες μεθόδους ασφαλείας που προσφέρουν τα λειτουργικά συστήματα, μερίδιο ευθύνης για τη διασφάλιση των προσωπικών του δεδομένων φέρει και ο ίδιος ο χρήστης. Η άγνοια και η ελλιπής ενημέρωση του χρήστη για τους κινδύνους που διατρέχει η ιδιωτική του ζωή με τη χρήση κινητών συσκευών συχνά συνοδεύεται από παραβίασή της. Οι ευαισθητοποίησή τους σε θέματα ασφάλειας εν τέλει αποτελεί το κλειδί για μια αποτελεσματικότερη και όσο το δυνατό πληρέστερη διασφάλιση των δεδομένων που χρήζουν προστασίας.

Σκοπός

Σκοπός της εργασίας αυτής είναι να αναδειχτούν τα προβλήματα και οι ευπάθειες των κινητών συσκευών και των αντίστοιχων εφαρμογών τους ούτως ώστε να καταστεί δυνατή η δημιουργία συνείδησης σε θέματα ασφαλείας των προσωπικών δεδομένων. Η διαφύλαξη της ιδιωτικής ζωής έχει βαρύνουσα σημασία σε μια εποχή που τα δεδομένα κινούνται ελεύθερα και η πρόσβαση σε αυτά είναι πιο εύκολη παρά ποτέ άλλοτε.

Δομή της πτυχιακής εργασίας

Η Δομή της πτυχιακής εργασίας αποτελείτε από πέντε κεφάλαια τα οποία περιλαμβάνουν :

Στο 1^{ο} κεφάλαιο γίνεται μια αναφορά στις σύγχρονες φορητές συσκευές και στα σημαντικότερα (βάση πωλήσεων στην αγορά) λειτουργικά συστήματα που χρησιμοποιούν αυτές. Επιπλέον γίνεται αναφορά στις εφαρμογές που παρέχουν μέσων των market place τους οι κινητές αυτές πλατφόρμες.

Στο 2^{ο} κεφάλαιο δίνεται η αρχιτεκτονική δομή του Android OS, του πιο διαδεδομένου λειτουργικού συστήματος για κινητές συσκευές και των αντίστοιχων εφαρμογών που αυτό παρέχει.

Στο 3^{ο} κεφάλαιο πραγματοποιείται μια εκτενή ανάλυση στις απειλές που υπάρχουν σήμερα στις κινητές συσκευές και στη δομή της ασφάλεια του λειτουργικού συστήματος Android.

Στο 4^{ο} κεφάλαιο αναδεικνύεται η σημαντικότητα του mobile forensics αναλύοντας μια σχετική μελέτη σε Android λειτουργικό.

Στο 5^{ο} κεφάλαιο πραγματοποιούνται μια σειρά από επιθέσεις σε κινητές συσκευές που χρησιμοποιούν Android με απώτερο σκοπό να αναδειχτούν τα προβλήματα που υπάρχουν γύρω από την ασφάλεια.

Τέλος, στα συμπεράσματα δίνονται μια σειρά από ενέργειες που μπορεί να κάνει ο χρήστης προκειμένου να προστατευτεί από κακόβουλες επιθέσεις.

Κεφάλαιο 1° Κινητές Συσκευές

Εικόνα 3 - Διάφορες κινητές συσκευές

Μια κινητή πλατφόρμα (επίσης γνωστή ως κινητή συσκευή, συσκευή χειρός, υπολογιστής τσέπης) είναι ένας υπολογιστής μεγέθους τσέπης, που συνήθως αποτελείται από μια οθόνη με δυνατότητα αφής και/ή ένα μικροσκοπικό πληκτρολόγιο και ζυγίζουν λιγότερο από ένα κιλό. Η Samsung, Apple, HTC, LG, Research in Motion (RIM) και η Motorola Mobility είναι μερικά παραδείγματα κατασκευαστών που έχουν εστιάσει στην κατασκευή των φορητών συσκευών (Εικόνα 3). [3]

Στην περίπτωση ενός προσωπικού ψηφιακού υπολογιστή (PDA) όλη η αλληλεπίδραση με τον χρήστη γίνεται μέσω μιας οθόνης αφής. Τα έξυπνα κινητά (Smartphones) και τα PDAs είναι πολύ διαδεδομένα σε όσους έχουν ανάγκη την βοήθεια και την ευκολία μερικών πτυχών των κανονικών ηλεκτρονικών υπολογιστών, σε περιβάλλοντα που δεν θα ήταν δυνατό να χρησιμοποιηθούν ή να μεταφερθούν. Τέτοιες κινητές πλατφόρμες μπορούν να έχουν και μεγάλη επιχειρηματική αξία για τις επιχειρήσεις που τις χρησιμοποιούν καθώς προσφέρουν την δυνατότητα να σκανάρουν αντικείμενα όπως barcodes και έξυπνες κάρτες.

Μια φορητή υπολογιστική συσκευή διαθέτει ένα λειτουργικό σύστημα (OS), και μπορεί να τρέξει διάφορους τύπους λογισμικού εφαρμογών, γνωστούς και ως apps. Οι περισσότερες φορητές συσκευές μπορούν επίσης να έχουν δυνατότητα σύνδεσης με Wi-Fi, Bluetooth και 3G/4G δίκτυα. Η φωτογραφική μηχανή, η δυνατότητα αναπαραγωγής βίντεο ή αρχείων μουσικής καθώς και η δυνατότητα πλοήγησης με τη χρήση ενσωματωμένου δέκτη GPS είναι μερικά χαρακτηριστικά που συναντάμε στις συσκευές αυτές.

Ένας γενικός ορισμός που θα μπορούσε να δοθεί στις κινητές πλατφόρμες είναι μια ποικιλία συσκευών που επιτρέπουν στον χρήστη να έχει πρόσβαση σε δεδομένα και πληροφορίες όπου και αν αυτός βρίσκεται. Όμως οι δυνατότητες και η χρησιμότητά των

φορητών συσκευών δεν περιορίζονται ώστε να είναι σε θέσει καλύψουν διάφορους τομείς της αγοράς. Οι συσκευές αυτές λοιπόν, απευθύνονται τόσο σε επιχειρήσεις όσο και σε άτομα που θέλουν να καλύψουν προσωπικές τους ανάγκες. Στη συνέχεια παραθέτουμε τους κύριους εκπροσώπους των κινητών συσκευών.

1.1.1. Προσωπικός ψηφιακός βοηθός (PDA)

Εικόνα 4 - PDA

Ένας προσωπικός ψηφιακός βοηθός (PDA), επίσης γνωστός ως υπολογιστής παλάμης (Palmtop Computer) είναι μια φορητή συσκευή που λειτουργεί σαν προσωπικός διαχειριστής πληροφοριών (Εικόνα 4). Τα σημερινά PDA έχουν την δυνατότητα να συνδέονται στο διαδίκτυο και μέσω της οθόνης τους μπορούν να περιλαμβάνουν πρόγραμμα περιήγησης σε αυτό. Τα περισσότερα PDAs μπορούν να έχουν πρόσβαση στο Internet, intranets ή extranets μέσω Wi-Fi ή ασύρματα δίκτυα ευρείας ζώνης. Επίσης τα περισσότερα PDAs χρησιμοποιούν την τεχνολογία οθόνης αφής. [4]

Όμως τα σημερινά μοντέλα έχουν και άλλες δυνατότητες όπως το ότι έχουν μικρόφωνο και ακουστικό αλλά και ηχείο και όλα αυτά επιτρέπουν την χρήση τους ως κινητά τηλέφωνα αλλά και φορητά ηχοσυστήματα. Το πρώτο PDA κυκλοφόρησε το 1984 από την Psion, το Organizer II. Ακολούθησε το Series 3 από την Psion το 1991, το οποίο άρχισε να μοιάζει με το σημερινό γνώριμο ύφος των PDA. Είχε επίσης ένα πλήρες πληκτρολόγιο.

Ο όρος PDA χρησιμοποιήθηκε για πρώτη φορά τον Ιανουάριο του 1992 από τον πρόεδρο της εταιρίας Apple, John Sculley σε μια έκθεση ηλεκτρονικών συσκευών, την CES (Consumer Electronics Show) στο Las Vegas, και αναφερόταν στη συσκευή Apple Newton. Το 1994, η IBM παρουσίασε το πρώτο PDA με πλήρη λειτουργικότητα κινητού τηλεφώνου, το IBM Simon, το οποίο μπορεί επίσης να θεωρηθεί ως το πρώτο smartphone. Στη συνέχεια το 1996 η Nokia δημιούργησε το πρώτο κινητό τηλέφωνο με όλες τις λειτουργίες ενός PDA, το 9000 Communicator, το οποίο έγινε πρώτο σε πωλήσεις παγκοσμίως. Με την είσοδο στην αγορά αυτής της συσκευής δημιουργήθηκε ουσιαστικά ο όρος PDA τηλέφωνο. Παράλληλα την ίδια χρονιά κυκλοφόρησε και μια σειρά από προϊόντα PDA με το όνομα Palm. Σήμερα όλα τα PDA είναι ουσιαστικά και Smartphone. Τα PDA χωρίς λειτουργίες τηλεφώνου περιορίζονται πια σε πολύ χαμηλές πωλήσεις και δημιουργούνται για να καλύψουν συγκεκριμένες ανάγκες κυρίως στο τομέα της βιομηχανίας.

1.1.2. Personal Navigation Assistant (PNA)

Εικόνα 5 - PNA

Ένα PNA γνωστό και ως Personal Navigation Device (PND) είναι μια φορητή ηλεκτρονική συσκευή που συνδυάζει την ικανότητα εντοπισμού θέσης (π.χ. μέσω GPS) μαζί με λειτουργίες πλοήγησης (Εικόνα 5). Ο όρος PNA έχει τεθεί σε ευρεία χρήση με την αυξανόμενη δημοτικότητα των συστημάτων πλοήγησης των αυτοκινήτων. Τα πρώτα PNAs ήταν GPS μονάδες χειρός τα οποία απεικόνιζαν τη θέση του χρήστη πάνω σε έναν ηλεκτρονικό χάρτη. [5]

Η τελευταία γενιά των PNA έχουν εξελιγμένες λειτουργίες πλοήγησης και διαθέτουν μια ποικιλία από user interfaces, συμπεριλαμβανομένων των χαρτών, οδηγίες turn-by-turn και φωνητικές οδηγίες. Για την μείωση του συνολικού κόστους, πολλές εταιρίες κατασκευής PNAs έχουν ενσωματωμένο λειτουργικό σύστημα όπως τα Windows CE ή Embedded Linux και μέσα σε αυτά περιλαμβάνονται δημοφιλή προγράμματα πλοήγησης ,όπως το TomTom Navigator, I-GO 2006, Netropa IntelliNav iGuidance και ο Destinator. Αξίζει να σημειωθεί ότι το πρώτο PNA που κατασκευάστηκε ποτέ χρησιμοποιήθηκε από το στρατό των Ηνωμένων Πολιτειών.

1.1.3. Τα έξυπνα κινητά (smartphones)

Εικόνα 6 - Smartphone

Το smartphone είναι ένα κινητό τηλέφωνο που προσφέρει πιο προηγμένη υπολογιστική δυνατότητα και συνδεσιμότητα από ένα συμβατικό κινητό τηλέφωνο (Εικόνα 6). Ένα smartphone μπορεί να θεωρηθεί ως ένας προσωπικός υπολογιστής τσέπης με τις λειτουργίες κινητού τηλεφώνου. Τα κινητά τηλέφωνα διαθέτουν υλικολογισμικό ανάλογα με τον κατασκευαστή. Αν υποστηρίζουν λογισμικό τρίτων κατασκευαστών, είναι μόνο μέσω μιας σχετικά περιορισμένης πλατφόρμα, όπως η Java ή BREW. Το λογισμικό μέσω των πλατφορμών αυτών είναι συχνά λιγότερο ισχυρό και ολοκληρωμένο με άλλες λειτουργίες του τηλεφώνου καθώς επίσης και λιγότερο ενσωματωμένο στο κύριο περιβάλλον χρήστη του τηλεφώνου. [6]

Τα Smartphones αντίθετα, τρέχουν ένα πλήρες λογισμικό λειτουργικού συστήματος (OS), η ύπαρξη του οποίου μεγιστοποιεί τις δυνατότητες του υλικού των συσκευών, δίνοντας έτσι τη δυνατότητα στους χρήστες να έχουν μια καλύτερη αλληλεπίδραση με τη συσκευή τους. Επιπροσθέτως, παρέχουν πλατφόρμες στους προγραμματιστές ώστε να δημιουργήσουν μια πληθώρα προηγμένων εφαρμογών που μπορεί να εγκαταστήσει ο

χρήστης εύκολα στη συσκευή του. Αλλά και από πλευράς υλικού ένα smartphone διαφέρει άρδην από ένα κινητό τηλέφωνο. Η ύπαρξη υψηλής ανάλυσης οθόνων αφής, ψηφιακών φωτογραφικών μηχανών, βιντεοκαμερών, μονάδων πλοήγησης GPS αλλά και η ενσωμάτωση πανίσχυρων, σε πολλές περιπτώσεις, επεξεργαστών αναδεικνύουν τις τεράστιες δυνατότητες που προσφέρουν οι συσκευές αυτές.

Το πρώτο smartphone ονομάστηκε Simon, σχεδιάστηκε από την IBM το 1992 και εμφανίστηκε ως concept προϊόν, το ίδιο έτος στην COMDEX. Πρωτοεμφανίστηκε στο κοινό το 1993 και πωλήθηκε από τη BellSouth. Πέραν του ότι ήταν ένα κινητό τηλέφωνο, περιλάμβανε επίσης ένα ημερολόγιο, βιβλίο διευθύνσεων, παγκόσμιο ρολόι, αριθμομηχανή, σημειωματάριο, email, αποστολή και λήψη fax, και παιχνίδια. Το Simon διέθετε μια οθόνη αφής την οποία οι χρήστες χρησιμοποίησαν με τη βοήθεια μιας ακίδας ή απλώς με τα δάκτυλά τους. Με τα σημερινά δεδομένα, το Simon είναι ένα προϊόν περιορισμένων δυνατοτήτων. Ωστόσο, τα χαρακτηριστικά του για την εποχή εκείνη ήταν σε εξαιρετικά προχωρημένο στάδιο.

Όλα τα smartphones έχουν κάποια συγκεκριμένα χαρακτηριστικά που τα κάνουν να ξεχωρίζουν από τα απλά κινητά τηλέφωνα (Εικόνα 7) [7] [8]:

Εικόνα 7 - Κύρια χαρακτηριστικά των Smartphones

- **Λειτουργικό σύστημα**

Όπως αναφέρθηκε και προηγουμένως, ένα smartphone είναι βασισμένο σε ένα λειτουργικό σύστημα που του επιτρέπει να τρέχει προηγμένες εφαρμογές και να μεγιστοποιεί τις δυνατότητες της συσκευής. Στα εμπορικότερα λειτουργικά συστήματα

(OS) που χρησιμοποιούνται από τις σύγχρονες smartphones συσκευές συγκαταλέγονται το Android της Google, το iOS της Apple, το Symbian, το RIM της BlackBerry, Bada της Samsung, το Windows Phone της Microsoft, και το webOS της Hewlett-Packard. Εκτενέστερη ανάλυση για τα παραπάνω θα γίνει σε επόμενη ενότητα.

- **Εφαρμογές**

Η υποστήριξη των λειτουργικών συστημάτων των smartphones με πλατφόρμες για τους προγραμματιστές εφαρμογών οδήγησε σε μια εκρηκτική ανάπτυξη εφαρμογών παντός είδους. Ένα smartphone πλέον έχει την ικανότητα να πραγματοποιεί περισσότερα πράγματα. Για παράδειγμα, μπορεί να επιτρέπει τη δημιουργία και ανάγνωση Office εγγράφων, την επεξεργασία φωτογραφιών, τη δημιουργία λίστας τραγουδιών ή ακόμα και την παροχή οδηγιών για το πώς θα φτάσει ο χρήστης σε μια περιοχή μέσω GPS.

- **Πρόσβαση στο διαδίκτυο**

Η πλειοψηφία των smartphones μπορεί να έχει πρόσβαση στο διαδίκτυο, και μάλιστα με υψηλές ταχύτητες, χάρη στη μεγάλη ανάπτυξη των 3G ή 4G δικτύων και την προσθήκη υποστήριξης Wi-Fi σε πολλά από αυτά. Ακόμα και αν δεν προσφέρουν πρόσβαση με υψηλές ταχύτητες, παρέχουν τροποποιημένους browser που βελτιώνουν την ανταπόκριση ώστε να μπορεί ο χρήστης να επισκεφθεί τους αγαπημένους του ιστότοπους.

- **QWERTY πληκτρολόγιο**

Όλα τα smartphones περιλαμβάνουν ένα QWERTY πληκτρολόγιο. Αυτό σημαίνει ότι τα πλήκτρα είναι διατεταγμένα με τον ίδιο τρόπο που είναι σε ένα πληκτρολόγιο ενός προσωπικού υπολογιστή. Αντίθετα, στα κινητά τα πλήκτρα είναι διατεταγμένα σε αλφαβητική σειρά σε ένα αριθμητικό πληκτρολόγιο όπου κάθε φορά που πραγματοποιείται πάτημα του πλήκτρο αλλάζει το γράμμα που θα εισαχθεί. Το πληκτρολόγιο μπορεί να αποτελείται από πραγματικά κουμπιά ή να είναι εικονικό πάνω σε μια οθόνη αφής.

- **Μηνύματα**

Όλα τα κινητά τηλέφωνα μπορούν να στείλουν και να λάβουν γραπτά μηνύματα, όμως ένα smartphone είναι ικανό να διαχειρίζεται και e-mails. Επιπλέον, μπορεί να συγχρονίσει τον προσωπικό και επαγγελματικό e-mail λογαριασμό του χρήστη. Μερικά μπορούν να υποστηρίξουν πολλαπλούς e- mail λογαριασμούς ενώ άλλα παρέχουν πρόσβαση σε δημοφιλείς υπηρεσίες άμεσων μηνυμάτων όπως το MSN Messenger.

- **Ήχοι και Video**

Όλα τα μοντέρνα smartphones διαθέτουν υψηλής ανάλυσης οθόνες και ηχεία (σημερινά μοντέλα διαθέτουν ακόμα και full HD 1080p) δίνοντας τη δυνατότητα στις συσκευές αυτές να μετατρέπονται σε ένα πλήρες κέντρο ψυχαγωγίας καλύπτοντας έτσι της ανάγκες του χρήστη για διασκέδαση και όχι μόνο.

- **Camera**

Την ραγδαία ανάπτυξη της επεξεργαστικής ισχύς των συσκευών αλλά και γενικά του υλικού των συσκευών δεν θα μπορούσε να μην ακολουθήσει και η τεχνολογία των καμερών. Όλα τα σύγχρονα smartphones είναι εφοδιασμένα με υψηλής ανάλυσης ψηφιακές κάμερες και με την ανάπτυξη αντίστοιχων εφαρμογών προσφέρουν ποικίλες ευκολίες στους χρήστες. Μια κάμερα μπορεί να λειτουργήσει και σαν barcode scanner με την κατάλληλη εφαρμογή. Πολλές δε συσκευές διαθέτουν και δεύτερη camera για να υποστηρίξουν δημοφιλείς υπηρεσίες όπως video κλήση μέσω του Skype.

1.1.4. Tablets

Εικόνα 8 - Tablet

Μια ταμπλέτα (Tablet PC) είναι ένας ηλεκτρονικός υπολογιστής μεγέθους συνήθως 6 έως 10 ίντσες η οποία έχει ως βασικά χαρακτηριστικά αυτά ενός κανονικού Η/Υ και συνήθως περιλαμβάνει ένα πλήρες λειτουργικό σύστημα (Εικόνα 8) [9].

Ένα φορητό Tablet PC περιλαμβάνει μια οθόνη αφής ως κύρια μέθοδος εισόδου δεδομένων και είναι σχεδιασμένο έτσι ώστε να χρησιμοποιείται για προσωπική χρήση. Ο όρος Tablet PC έγινε γνωστός από μια παρουσίαση της Microsoft το 2001 όπου παρουσίασε το Microsoft Tablet PC. Η σειρά δεν είχε επιτυχία και απευθυνόταν σε μια εξειδικευμένη αγορά όπως νοσοκομεία και επιχειρήσεις. Επίσημα όμως το Tablet pc καθιερώθηκε το 2010, όταν η εταιρεία Apple κυκλοφόρησε το iPad, το οποίο χρησιμοποιεί την τεχνολογία οθόνης αφής παρόμοια με αυτή που χρησιμοποιείται στο iPhone. Το ipad έκανε παγκόσμια εμπορική επιτυχία ,θέτοντας της βάσεις ώστε σήμερα να κυκλοφορεί στην αγορά μια ευρεία γκάμα μοντέλων και προϊόντων προσωπικών ηλεκτρονικών υπολογιστών υποστηριζόμενα από διάφορα λειτουργικά συστήματα.

Οι ταμπλέτες χρησιμοποιούν εικονικά πληκτρολόγια και αναγνώριση γραφής έτσι ώστε να μπορούμε να εισάγουμε κείμενο, μέσω της οθόνης αφής. Όλες οι ταμπλέτες έχουν δυνατότητα ασύρματης σύνδεσης μέσω Wi-Fi, αλλά και ενσύρματα, στο διαδίκτυο. Η νέα γενιά ταμπλετών διαθέτει και υποδοχή για κάρτες sim, δίνοντας έτσι τη δυνατότητα στις συσκευές να συνδεθούν στο διαδίκτυο μέσω συνδέσεων 3G ή 4G των παρόχων κινητής τηλεφωνίας. Χρησιμοποιούν ακόμα την τεχνολογία του Bluetooth για

τη σύνδεση περιφερειακών και για την επικοινωνία με τις τοπικές συσκευές στη θέση της ενσύρματης USB σύνδεσης,

Το λογισμικό τους περιλαμβάνει εφαρμογές γραφείου, προγράμματα περιήγησης στο διαδίκτυο, παιχνίδια, αλλά από την στιγμή που τρέχουν ολοκληρωμένα λειτουργικά συστήματα (android, ios κ.α.), μπορούν ουσιαστικά να χρησιμοποιήσουν οποιοδήποτε εφαρμογή υποστηρίζει το λειτουργικό τους. Σήμερα τα Tablet που κυκλοφορούν στην αγορά τείνουν να έχουν τις ίδιες ακριβώς δυνατότητες με τα smartphones. Θα μπορούσε λοιπόν κάποιος να χαρακτηρίσει τις ταμπλέτες σαν smartphones με απλώς μεγαλύτερη οθόνη.

1.1.5. Πλεονεκτήματα φορητών συσκευών

Οι φορητές συσκευές διαθέτουν μια σειρά από λειτουργίες και χαρακτηριστικά που διευκολύνουν τόσο το χρήστη στην καθημερινότητά του. Αναλυτικά οι κινητές συσκευές προσφέρουν :

- **Mobility:** Οι κινητές συσκευές πέρα από το γεγονός ότι γίνονται ολοένα και μικρότερες παρέχουν και απεριόριστο βαθμό κινητικότητας στον χρήστη.
- **Universal:** Στόχος των κατασκευαστών κινητών συσκευών είναι να παράγουν μαζικά συσκευές που να καλύπτουν κάθε ανάγκη των χρηστών όσο εξεζητημένες και αν είναι αυτές.
- **Connection:** Το επίπεδο συνδεσιμότητας που παρέχεται από τις κινητές συσκευές είναι υψηλό καθώς έχουν την δυνατότητα να συνδέονται τόσο στις κεραίες του παρόχου του δικτύου τους οι οποίες μπορεί να βρίσκονται χιλιόμετρα μακριά όσο και σε δίκτυα μικρότερης εμβέλειας με κοντινότερες κεραίες (πχ WiFi). Επίσης, δεν είναι λίγες και οι εφαρμογές που λειτουργούν με τοπικές συνδέσεις από συσκευή σε συσκευή όπως (πχ Bluetooth).
- **Innovation:** Παρά το γεγονός ότι οι ανάγκες που πρέπει να καλύψουν οι κινητές συσκευές είναι ως επί των πλείστων κοινές για τους περισσότερους χρήστες, οι κατασκευαστές πρέπει να εισάγουν και καινοτομικά στοιχεία στις συσκευές τους δεδομένου ότι ο ανταγωνισμός είναι αυξημένος και στοχεύουν στο μεγαλύτερο δυνατό μερίδιο αγοράς.
- **Open:** Η πλατφόρμα του λειτουργικού συστήματος πρέπει να είναι ανοικτού κώδικα έτσι ώστε να μην περιορίζεται η ανάπτυξη εφαρμογών και η χρήση ανεξάρτητων ή/και διαφορετικών τεχνολογιών.

1.1.6. Περιορισμοί φορητών συσκευών

Παρά το γεγονός ότι οι φορητές συσκευές διευκολύνουν τους χρήστες στην επικοινωνία και την ανταλλαγή πληροφοριών εν κινήσει, παρατηρείται ότι υπάρχει μια σειρά από περιορισμούς και προβλήματα που δημιουργούνται από την χρήση τους. Αυτό οφείλεται κυρίως στο γεγονός ότι οι φορητές συσκευές μπήκαν στην καθημερινότητά των χρηστών σχετικά πρόσφατα και η τεχνολογία που σχετίζεται με αυτές τις συσκευές συνεχώς εξελίσσεται. Παρακάτω αναλύονται οι κυριότεροι από αυτούς τους περιορισμούς [10]:

- **Range & Bandwidth**: Η πρόσβαση στο Internet μέσω κινητών συσκευών είναι γενικά πιο αργή από αυτές των καλωδιακών συνδέσεων, χρησιμοποιώντας τεχνολογίες όπως το GPRS και EDGE, και πιο πρόσφατα τα HSDPA και HSUPA 3G και 4G δίκτυα. Αυτά τα δίκτυα είναι συνήθως διαθέσιμα εντός της εμβέλειας των πάροχων κινητής τηλεφωνίας. Μεγαλύτερη ταχύτητα παρέχουν τα ασύρματα τοπικά δίκτυα, αλλά έχουν πολύ περιορισμένο εύρος.

- **Security standards**: Όταν γίνεται εργασία μέσω της κινητής συσκευής, η σύνδεση σε δημόσια δίκτυα, απαιτεί προσεκτική χρήση του VPN. Η ασφάλεια είναι μείζον πρόβλημα, όσον αφορά τη χρήση κινητών συσκευών. Κάποιος μπορεί να επιτεθεί εύκολα στο VPN μέσω ενός τεράστιου αριθμού δικτύων που διασυνδέονται μέσω της γραμμής.

- **Power consumption**: Όταν μια πρίζα ή φορητή γεννήτρια δεν είναι διαθέσιμη, οι φορητούς υπολογιστές βασίζονται εξ ολοκλήρου στην ενέργεια της μπαταρίας. Η τεχνολογία των μπαταριών δεν έχει προχωρήσει το ίδιο σε σχέση με την τεχνολογία των επεξεργαστών και της μνήμης με αποτέλεσμα να υπάρχουν πλέον πολύ καλές φορητές συσκευές από άποψη υπολογιστικής ισχύος που υστερούν όμως στη διάρκεια ζωής της μπαταρίας Σε συνδυασμό με το μικρό τους μέγεθος, πολλές κινητές συσκευές, συχνά χρησιμοποιούν ασυνήθιστα ακριβές μπαταρίες προκειμένου να διασφαλίσουν την απαραίτητη διάρκεια ζωής της μπαταρίας.

- **Transmission interferences**: Ο καιρός, το έδαφος και το εύρος από το πλησιέστερο σημείο σήματος μπορούν να επηρεάσουν τη λήψη του σήματος. Σήραγγες, ορισμένα κτίρια, και γενικά στις αγροτικές περιοχές το σήμα είναι συχνά κακής ποιότητας.

- **Potential health hazards**: Οι άνθρωποι που χρησιμοποιούν κινητές συσκευές κατά την οδήγηση, συχνά αποσπούν την προσοχή τους και επομένως, θεωρείται πιο πιθανό να εμπλακούν σε τροχαία ατυχήματα. Τα κινητά τηλέφωνα μπορούν επίσης να επηρεάσουν ευαίσθητες ιατρικές συσκευές. Τα θέματα που αφορούν την ακτινοβολία των κινητών τηλεφώνων και την υγεία έχουν αυξηθεί.

- **Human interface with device**: Οι οθόνες και τα πληκτρολόγια τείνουν ολοένα να γίνουν μικρότερα, τα οποία μπορεί να δυσκολέψουν τους χρήστες. Εναλλακτικές μέθοδοι εισαγωγής, όπως η ομιλία ή την αναγνώριση γραφικού χαρακτήρα απαιτούν εκπαίδευση. Επιπροσθέτως, όταν ο χρήστης βρίσκεται εν κινήσει δεν έχει τη δυνατότητα να διαβάσει οδηγίες ή εγχειρίδια που απαιτούνται για την εκπλήρωση κάποιων συγκεκριμένων λειτουργιών. Η δυνατότητα να υπάρχει πρόσβαση στις εφαρμογές και στα δεδομένα τους με όσο το δυνατόν λιγότερα πατήματα κουμπιών είναι πολύ σημαντική στις φορητές συσκευές. Τα περιβάλλοντα διεπαφής πρέπει να είναι φιλικά προς τον χρήστη και ελκυστικά.
- **Limited storage**: Η πλειοψηφία των φορητών συσκευών έχει περιορισμένη χωρητικότητα σε μνήμη. Το πρόβλημα έχει αμβλυνθεί μέσω της επέκτασης της μνήμης με εξωτερικές κάρτες μεγάλης χωρητικότητας (π.χ. 8 GB) αλλά παραμένει ακόμα. Υπάρχουν εφαρμογές, συνήθως παιχνίδια, που είναι πολύ μεγάλες σε χωρητικότητα με το μέγεθός τους φτάνει ή και ξεπερνάει τα 300 MB. Όλα αυτά συντελούν στην εξάντληση της μνήμης της συσκευής αρκετά γρήγορα.

1.2. Λειτουργικά συστήματα για κινητές Συσκευές

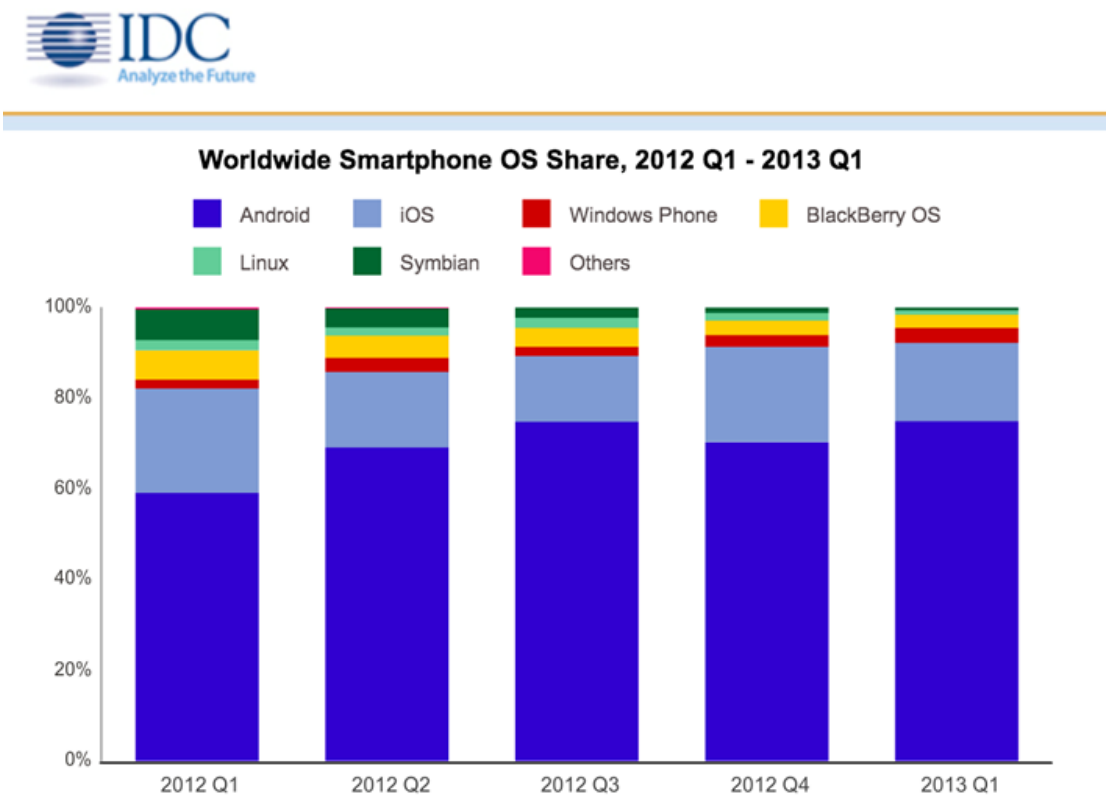
Το Mobile OS είναι το λειτουργικό σύστημα εκείνο που απευθύνεται αποκλειστικά στις κινητές συσκευές. Έχει τις ίδιες χαρακτηριστικές αρχές με ένα λειτουργικό σύστημα όπως τα Windows, τα Mac OS, τα Linux και άλλα, τα οποία ελέγχουν τους ηλεκτρονικούς υπολογιστές. Όμως αν και έχουν πολλά κοινά με τα προαναφερθέντα λειτουργικά, είναι κατά μια έννοια πιο ελαφρά, καθώς είναι φτιαγμένα ώστε να μπορούν να λειτουργούν με λιγότερους υπολογιστικούς πόρους ενώ έχουν να κάνουν περισσότερο με ασύρματες επικοινωνίες και τοπικά δίκτυα, με διαφορετικά αρχεία πολυμέσων και διαφορετικούς τρόπους εισαγωγής εντολών.

Αυτή η νέα γενιά λειτουργικών συστημάτων ρίχνει μεγάλο βάρος στην ανάπτυξη εφαρμογών από τρίτες εταιρίες αλλά και από ανεξάρτητους προγραμματιστές. Αυτός είναι και ο βασικός λόγος για τον οποίο όλα τα νέα λειτουργικά προμηθεύουν με τα δικά τους λογισμικά ανάπτυξης εφαρμογών οποιοδήποτε θέλει να ασχοληθεί και ενημερώνουν τους προγραμματιστές για τους τρόπους ανάπτυξης εφαρμογών σε αυτά. Κάθε κατασκευαστής έχει δημιουργήσει το δικό του market με χιλιάδες εφαρμογές καλύπτοντας έτσι ένα τεράστιο εύρος αναγκών του χρήστη.

Σήμερα με την ραγδαία ανάπτυξη των φορητών συσκευών υπάρχουν πολλές εταιρίες που κατασκευάζουν λειτουργικά συστήματα για αυτές. Βάση των στοιχείων που δίνει η αγορά , οι σημαντικότερες είναι το Android της Google, το IOS της Apple, το Symbian, το RIM της BlackBerry και το Windows Phone της Microsoft (Εικόνα 9). [11] Όλα όμως διέπονται από κάποια γενικά χαρακτηριστικά και παρουσιάζουν κάποιες

κοινές λειτουργίες ,που τα κάνει να ξεχωρίζουν από τα λειτουργικά συστήματα που απευθύνονται στους υπολογιστές. Τα χαρακτηριστικά αυτά είναι [12]:

- **Multitasking system:** Η ικανότητα δηλαδή να εκτελεί πολλαπλές εφαρμογές ταυτόχρονα καθώς και να ανταποκρίνονται σε ασύγχρονα γεγονότα.
- **Memory protection:** Η παροχή ενός ασφαλούς περιβάλλοντος για την εκτέλεση εφαρμογών χωρίς να διακυβεύεται η προστασία της ιδιωτικής ζωής των χρηστών καθώς επίσης και η ασφάλεια των δεδομένων.
- **Power conscious:** Μέρος της παραγωγής ενός λειτουργικού συστήματος που είναι φιλικό προς τις κινητές συσκευές είναι η δημιουργία μιας ενεργειακής συνείδησης, δηλαδή χρήσης όσο το δυνατόν λιγότερης ενέργειας, χωρίς να περιορίζεται ο χρήστης.
- **Extensible:** Η δυνατότητα που δίνεται σε τρίτες εταιρίες ώστε να αναπτύξουν εφαρμογές για το εκάστοτε λειτουργικό.
- **Support:** Υποστήριξη που παρέχεται μέσω μιας ευρεία ποικιλίας καναλιών επικοινωνίας.



Εικόνα 9 - Ποσοστά σε πωλήσεις των λειτουργικών συστημάτων για κινητές συσκευές

Σύμφωνα με τα στοιχειά που υπάρχουν ως τώρα και με την τάση στην αγορά την συγκεκριμένη περίοδο, είναι δεδομένη η αύξηση του ποσοστού των πωλήσεων Smartphone συσκευών σε σχέση με τα απλά κινητά τηλέφωνα. Τα λειτουργικά συστήματα για κινητές συσκευές είναι σήμερα σε ένα αρκετά προχωρημένο στάδιο, δυσανάλογο όμως της ραγδαίας ανάπτυξης των Smartphone συσκευών. Ήδη στην αγορά κυκλοφορούν συσκευές με πανίσχυρους τετραπύρηνους επεξεργαστές, με Full HD ανάλυση οθόνης και ψηφιακές φωτογραφικές μηχανές έως και 15MP. Παρόλη την σοβαρή προσπάθεια που έχει γίνει, τα λειτουργικά συστήματα ακόμα τρέχουν να προφτάσουν την εξέλιξη του υλικού. Ακολουθεί μια παρουσίαση των βασικών λειτουργικών συστημάτων που κατέχουν το μεγαλύτερο μερίδιο στην αγορά αυτή την στιγμή .

1.2.1. Symbian OS

Εικόνα 10 - Symbian OS logo

Το Symbian OS είναι λειτουργικό σύστημα για φορητές συσκευές, αποτελεί εξέλιξη του λειτουργικού συστήματος EPOC από την Psion (Εικόνα 11). Το Symbian OS δημιουργήθηκε με τη γλώσσα προγραμματισμού C++ από τη Symbian Ltd. Πριν το 2009 το Symbian OS υποστήριζε διαφορετικά περιβάλλοντα χρήστη. Όμως με την δημιουργία του Symbian Platform, το ίδιο έτος, τα 3 βασικά περιβάλλοντα χρήστη ενώθηκαν σε ένα, το οποίο εξαγοράστηκε από την Nokia και στην συνεχεία μετατράπηκε σε λογισμικό ανοικτού κώδικα. [6]

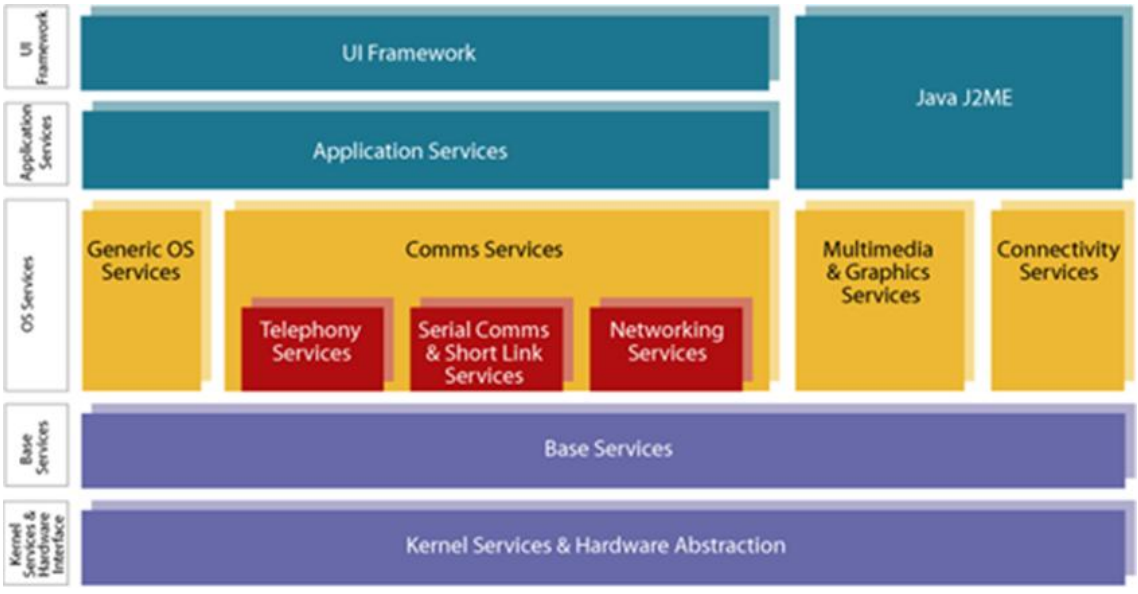
Αν και οι συσκευές με λογισμικό Symbian εξακολουθούν να πωλούνται σε μεγάλους αριθμούς στην αγορά, τα τελευταία χρόνια το μερίδιο του λειτουργικού αυτού συστήματος στην αγορά μειώνεται. Το τέλος της ανάπτυξης του λειτουργικού σηματοδοτήθηκε από την ανακοίνωση της Nokia το 2011 ότι βασικό λειτουργικό σύστημα για τις συσκευές της θα είναι πλέον το Microsoft Windows Phone OS.

Για την ανάπτυξη εφαρμογών στο περιβάλλον του λειτουργικού υπάρχει το Symbian SDK το οποίο χρησιμοποιεί ως γλώσσα προγραμματισμού την C++ σε συνδυασμό με το Qt, ένα Framework εφαρμογών που χρησιμοποιείται από πολλές πλατφόρμες. Μπορεί να χρησιμοποιηθεί είτε με το Qt Creator είτε με το Carbide, ένα παλιότερο IDE που χρησιμοποιείται για ανάπτυξη εφαρμογών Symbian. Ένας εξομοιωτής χρησιμοποιείται, για τη δοκιμή των εφαρμογών, που τρέχει τον κώδικα απευθείας αντί να προσομοιώνει την λειτουργία του κινητού τηλεφώνου. Οι Symbian συσκευές μπορούν επίσης να προγραμματιστούν χρησιμοποιώντας Python, Java ME, Flash Lite, Ruby,. NET, Web Runtime (WRT) Widgets και με την Standard C / C +. [13]

Το Symbian έχει μια αρχιτεκτονική microkernel, πράγμα που σημαίνει ότι συμπεριλαμβάνει τα ελάχιστα αναγκαία εντός του πυρήνα για να μεγιστοποιηθεί έτσι η αξιοπιστία, η διαθεσιμότητα και η ανταπόκρισή του. Περιέχει ένα scheduler ,τη διαχείριση μνήμης και τους οδηγούς των συσκευών. Όμως άλλες υπηρεσίες όπως η υποστήριξη της δικτύωσης ,της τηλεφωνίας και των filesystem τοποθετούνται στο Layer των υπηρεσιών.

Συνοπτικά η αρχιτεκτονική του λειτουργικού συστήματος Symbian παρουσιάζεται παρακάτω (Εικόνα 11) [12]:

- UI Framework Layer
- Application Services Layer
    - Java ME
- OS Services Layer
    - generic OS services
    - communications services
    - multimedia and graphics services
    - connectivity services
- Base Services Layer
- Kernel Services & Hardware Interface Layer



Εικόνα 11 - Αρχιτεκτονική Δομή του Symbian OS

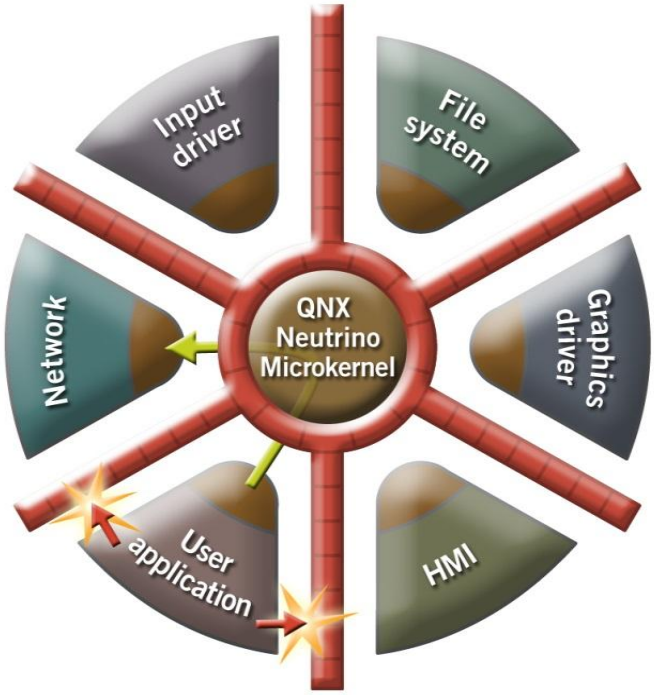
1.2.2. Blackberry OS

Εικόνα 12 - Blackberry 10 OS logo

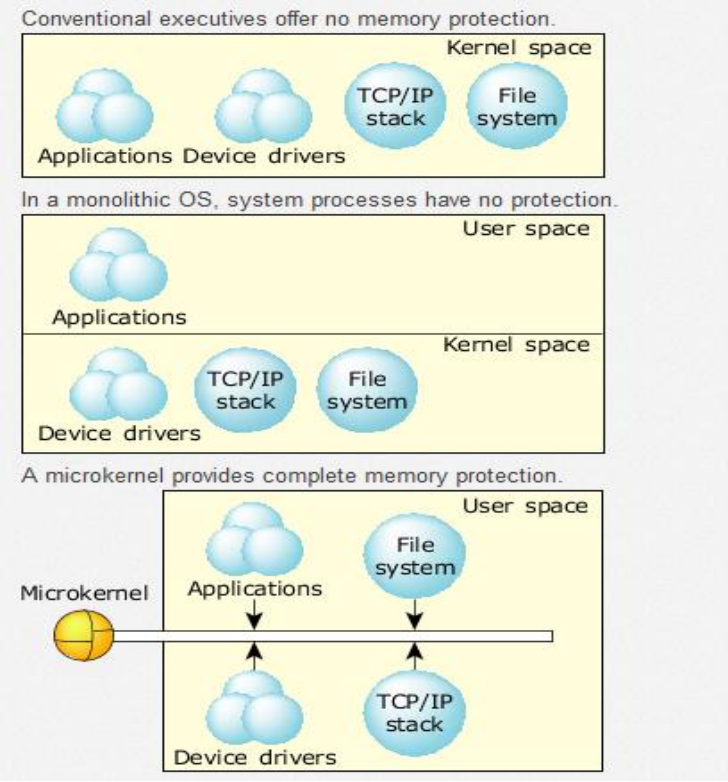
Το Blackberry OS ως κινητό λειτουργικό σύστημα πρώτο-εμφανίστηκε το 2005. Για την ανάπτυξη του υπεύθυνη είναι η εταιρία Research in Motion και χρησιμοποιείται στα smartphones Blackberry (Εικόνα 12). Το λειτουργικό αυτό σύστημα δίνει την δυνατότητα χρήσης πολλαπλών εφαρμογών ταυτόχρονα και είναι ειδικά φτιαγμένο ώστε να υποστηρίζει συγκεκριμένες συσκευές εισόδου δεδομένων που χρησιμοποιεί η Research in Motion στα κινητά της τηλέφωνα όπως το trackwheel και το trackball. [6]

Η πλατφόρμα Blackberry είναι αρκετά γνωστή για την υποστήριξή της σε εταιρικές εφαρμογές όπως Email και για αυτό το λόγο χρησιμοποιείται κυρίως σε εταιρικό επίπεδο. Αυτός ήταν εξάλλου και ο αρχικός στόχος του λειτουργικού. Τα τελευταία χρόνια έχει αυξήσει σε μεγάλο βαθμό την υποστήριξή του από τρίτες εταιρίες ανάπτυξης λογισμικού με αποτέλεσμα το ηλεκτρονικό κατάστημα πώλησης εφαρμογών του, το Blackberry Live να διαθέτει προς εγκατάσταση πάνω από 120.000 εφαρμογές. Για την ανάπτυξη εφαρμογών στην συγκεκριμένη πλατφόρμα χρησιμοποιείται το IDE (intergrated development environment) της Eclipse ενώ η γλώσσα προγραμματισμού είναι η C/C++ (σε παλαιότερες εκδόσεις ήταν η Java). Επιπλέον μπορεί να αναπτυχθούν εφαρμογές C και C ++ για το BlackBerry 10 χρησιμοποιώντας ένα Plug-in του BlackBerry Native Sdk για το Microsoft Visual Studio . [14]

Σήμερα το λειτουργικό που χρησιμοποιούν οι συσκευές της Blackberry βασίζεται στο QNX Neutrino Real Time Operating System (RTOS) (Εικόνα 13). Διαθέτει μια αρχιτεκτονική που ονομάζεται Micro πυρήνας. Αυτός διαφέρει από το Unix, MacOS και Windows που έχουν πολύ μεγαλύτερους, μονολιθικούς πυρήνες. Ακόμη και τα παλαιότερα Java-based λειτουργικά της BlackBerry βασίζονταν σε ένα μονολιθικό σύστημα. Η σχεδίαση λοιπόν του micro kernel προσφέρει ένα λειτουργικό σύστημα πιο εύκολα διατηρήσιμο, πιο ασφαλές, και πολύ πιο ευέλικτο. Το σύστημα λοιπόν διαθέτει ένα micro kernel και ένα διαχειριστή διαδικασιών. Όλα τα υπόλοιπα αποτελούν διαδικασίες που διαβιβάζονται στον επεξεργαστή προς εκτέλεση (Εικόνα 14). Προκειμένου δε η εν λόγω αρχιτεκτονική του συστήματος να αποφεύγει τα προβλήματα που αντιμετωπίζουν τα μονολιθικά συστήματα με τη λειτουργία των εφαρμογών και διαδικασιών στην ίδια μνήμη, χορηγεί εικονική μνήμη σε κάθε διαδικασία. Το γεγονός αυτό παρέχει περισσότερη ασφάλεια στα δεδομένα. [15]



Εικόνα 13 - Λειτουργία του QNX Neutrino Microkernel



Εικόνα 14 - Αρχιτεκτονική της λειτουργίας του Kernel στο Blackberry OS

1.2.3. Apple iOS

Εικόνα 15 - Apple iOS logo

Το iOS (γνωστό και ως iPhone OS) είναι το λειτουργικό σύστημα για κινητές πλατφόρμες της Apple (Εικόνα 15). Αν και αρχικά αναπτύχθηκε μόνο για το iPhone έχει από τότε επεκταθεί ώστε να υποστηρίζει και άλλες συσκευές της Apple όπως τα iPod Touch και iPad. Το συγκεκριμένο λειτουργικό σύστημα δεν υποστηρίζει άλλες συσκευές εκτός από αυτές της Apple. Ένα από τα μεγάλα πλεονεκτήματα του είναι το App Store το οποίο περιέχει περισσότερες από 500.000 εφαρμογές σύμφωνα με την τελευταία μέτρηση που έχει γίνει στα τέλη Μαΐου του 2012.

Το περιβάλλον χρήσης του είναι βασισμένο στην άμεση αλληλεπίδραση του χρήστη με την οθόνη αφής της συσκευής. Με αυτόν τον τρόπο ο χειρισμός γίνεται πολύ ευχάριστος, γρήγορος αλλά και απλός για τον χρήστη αφού μπορεί να αλληλεπιδρά με φυσικότητα με τα αντικείμενα που προβάλλονται στην οθόνη. Για παράδειγμα ο χρήστης μέσω της οθόνης αφής πολλαπλών σημείων μπορεί να χρησιμοποιεί διάφορες κινήσεις των δακτύλων του και να παίρνει άμεσα τα αποτελέσματα στην οθόνη.

Το iOS, για την ανάπτυξη εφαρμογών στο περιβάλλον του, χρησιμοποιεί το λογισμικό ανάπτυξης εφαρμογών iOS SDK το οποίο αναπτύχθηκε από την Apple και δόθηκε στους προγραμματιστές τον Φεβρουάριο του 2008. Τους δίνει την δυνατότητα να δημιουργήσουν εφαρμογές και να τις δοκιμάσουν σε ένα εξομοιωτή που ονομάζεται iPhone Simulator. Όμως για την εγκατάσταση μια εφαρμογής στη συσκευή, καθώς και για την πώληση της μέσω του App Store πρέπει ο χρήστης να είναι εγγεγραμμένος στο πρόγραμμα των προγραμματιστών iPhone. Ο δημιουργός μιας εφαρμογής μπορεί να την πουλήσει σε οποιαδήποτε τιμή πάνω από την μικρότερη επιτρεπτή τιμή (0.99 ευρώ) και να έχει κέρδος το 70% αυτής, με το υπόλοιπο 30% να αντιστοιχεί στο κέρδος της Apple. Εναλλακτικά, μπορεί να δίνει την εφαρμογή δωρεάν και να μην ζημιώνεται καθόλου από τα έξοδα κυκλοφορίας και διανομής, εκτός βεβαία από τα έξοδα εγγραφής. Το iOS SDK χρησιμοποιεί τον ίδιο πρόγραμμα γραφής κώδικα που χρησιμοποιεί και το Mac OS X, το Xcode, και περιλαμβάνει και τον iPhone Simulator, ένα πρόγραμμα που μπορεί να χρησιμοποιηθεί για να εξομοιώσει το πως θα φαίνονταν οι εφαρμογές και το πως θα δούλευαν αν έτρεχαν στο iPhone, και όλα αυτά από υπολογιστή του προγραμματιστή. Το SDK της Apple έχει ως απαιτήσεις συστήματος για να χρησιμοποιηθεί, έναν Intel Mac με λειτουργικό σύστημα Mac OS X Leopard ή και νεότερο. Άλλα λειτουργικά όπως τα Windows αλλά και παλιότερες εκδόσεις Mac OS X δεν υποστηρίζονται. [6] [16]

Η αρχιτεκτονική του λειτουργικού συστήματος ios αποτελείται από 4 στρώματα (Εικόνα 16). [17] Από τα τέσσερα διακριτά στρώματα τα δύο πρώτα είναι υψηλότερου επιπέδου τα οποία είναι πιο object-oriented στρώματα. Τα τελευταία δύο στρώματα

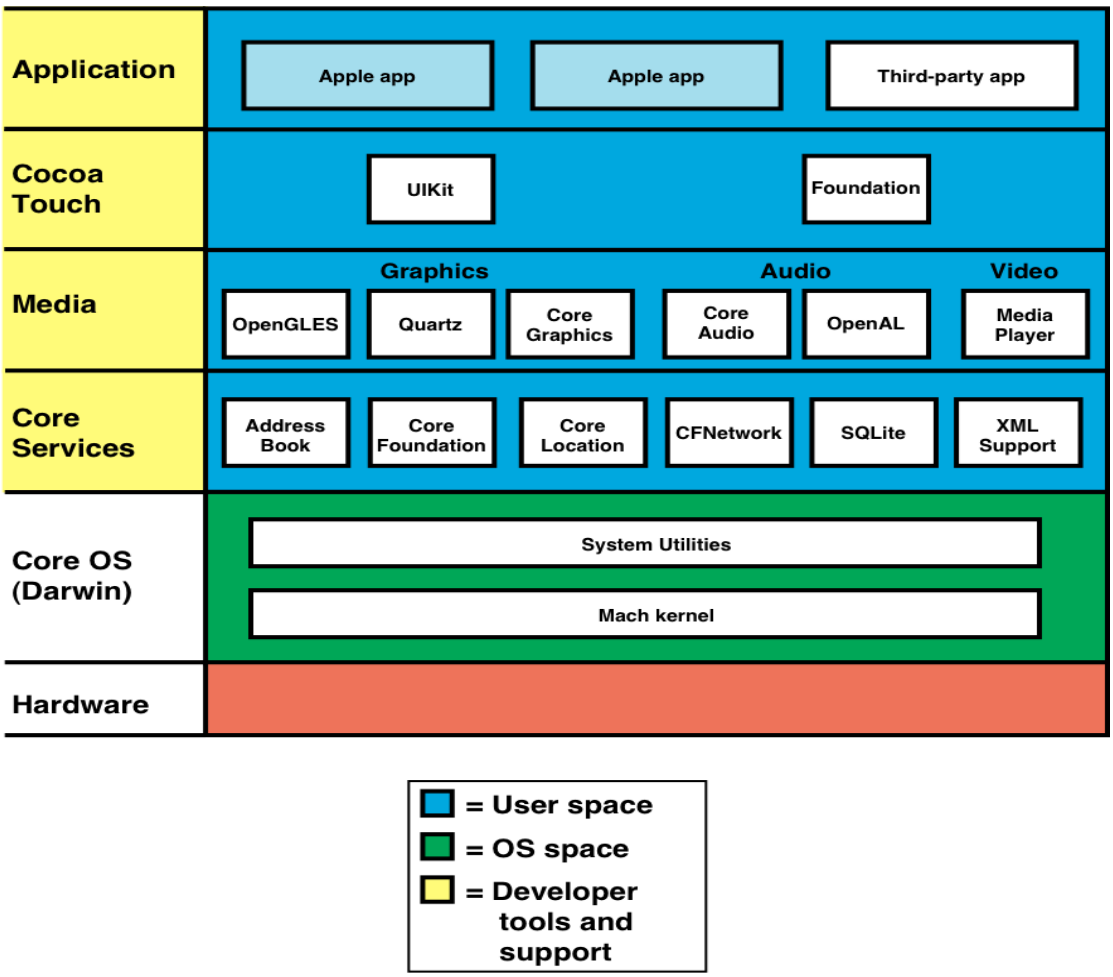
είναι χαμηλότερου επιπέδου και είναι ως επί το πλείστον συνδεδεμένα με το τμήμα του υλικού της συσκευής. Όλα τα στρώματα πρέπει να βασίζονται το ένα στο άλλο για την μέγιστη λειτουργικότητα και απόδοση της συσκευής. Το στρώμα Cocoa Touch είναι ένα από τα πιο σημαντικά στρώματα της αρχιτεκτονικής του συστήματος iOS και περιλαμβάνει το πλαίσιο UIKit, το οποίο χρησιμοποιείται ευρέως για την εκτέλεση πολλαπλών εργασιών, να πάρει την εντολή που πιέζει ο χρήστης στην οθόνη (ευαίσθητη είσοδο αφής) και να υποστηρίξουν την διαδικασία που θα οδηγήσει τελικά στην εφαρμογή iOS. Το ίδιο πλαίσιο μπορεί επίσης να χρησιμοποιηθεί για την πλατφόρμα OS X στην οποία ονομάζεται πλαίσιο Appkit.

Το στρώμα Media βοηθάει στην παροχή γραφικών, υποστήριξης ήχου και βίντεο για iOS εφαρμογές. Χρησιμοποιεί πυρήνα γραφικών, OpenGL ES, OpenAL, AV Foundation και Core Media τεχνολογίες. Τα στρώματα media επίσης διαθέτουν ένα μεγάλο αριθμό πλαισίων για να εκτελέσουν τα γραφικά και με οτιδήποτε σχετίζεται με τα Media. Διαθέτει ακόμα ένα πλαίσιο βιβλιοθήκης για να λειτουργήσουν οι φωτογραφίες και τα βίντεο από iOS συσκευές, ένα πυρήνα πλαίσιο εικόνας για τον έλεγχο της εικόνας, μέσω διαφόρων φίλτρων και τέλος ένα πυρήνα γραφικών για την κατασκευή 2D εικόνων.

Το στρώμα core Services είναι χρήσιμο ώστε να εκτελούνται οι απαραίτητες εργασίες των εφαρμογών iOS, όπως η iCloud αποθήκευση, η αγορά των εφαρμογών καθώς και η κεντρική αποστολή τους. Διαθέτει όμως ένα πιο σημαντικό συστατικό, το ARC, που σημαίνει αυτόματη αναφορά μέτρησης και είναι χρήσιμο για το σύστημα ήχου, βίντεο και αρχείων και τη διαχείριση της μνήμης. Το στρώμα core Services ως επί το πλείστον εξαρτάται από το πλαίσιο Foundation που λειτουργεί ως ένας μεσολαβητής μεταξύ των άλλων στρωμάτων ώστε να μοιράζονται κώδικα και δεδομένα μεταξύ τους οι βιβλιοθήκες και τα άλλα πλαίσια.

Το Core OS στρώμα υποστηρίζει κυρίως τα χαρακτηριστικά ασφαλείας και τη διασύνδεση με UNIX και Carnel περιβάλλοντα. Σε αυτό το στρώμα οι iOS εφαρμογές δεν έχουν καμία άμεση πρόσβαση. Ο πυρήνας του iOS είναι βασισμένος στο Darwin OS. Το Darwin είναι χτισμένο γύρω από XNU, ένα υβριδικό πυρήνα που συνδυάζει τρείς microkernel Mach, διάφορα στοιχεία του BSD (συμπεριλαμβανομένου του μοντέλου της διαδικασίας, στοίβας δικτύου, και εικονικό σύστημα αρχείων), και ένα object-oriented πρόγραμμα οδήγησης συσκευής που ονομάζεται I/O Kit. Το υβριδικό σχέδιο του πυρήνα συμβιβάζεται μεταξύ της ευελιξίας ενός microkernel και την απόδοση ενός μονολιθικού πυρήνα ,δημιουργώντας ένα πολύ ικανοποιητικό αποτέλεσμα.

Η αρχιτεκτονική του λειτουργικού συστήματος Apple iOS παρουσιάζεται παρακάτω [12].



Εικόνα 16 - Αρχιτεκτονική δομή του iOs

1.2.4. Windows Phone OS

Εικόνα 17 - Windows Phone OS logo

Το 2012 ανακοινώθηκαν τα Windows Phone 8, η δεύτερη γενιά του λειτουργικού συστήματος της Microsoft για φορητές συσκευές (Εικόνα 17). Το νέο λειτουργικό σύστημα περιλαμβάνει ένα εντελώς νέο περιβάλλον χρήσης το οποίο έχει δημιουργηθεί με μια γλώσσα σχεδίασης της ίδιας της εταιρίας, που ονομάζεται Metro. Παρέχει πλήρη υποστήριξη των υπηρεσιών της Microsoft όπως το Windows Live, το Zune, το Xbox Live και το Bing, αλλά και υπηρεσιών τρίτων εταιριών όπως το Facebook και τα Google Accounts. Αν και αυτή την στιγμή το νέο λειτουργικό βρίσκεται στα πρώτα του βήματα στην αγορά, μελλοντικά, μετά την συμφωνία με την Nokia, όπου θα χρησιμοποιείται ως το βασικό λειτουργικό στα κινητά τηλέφωνα της, δείχνει να είναι ικανό να ανταγωνιστεί τα άλλα 2 μεγάλα λειτουργικά συστήματα, το Android και το iOS. [18]

Το σύστημα των Windows 8 δεν είναι συμβατό με την αρχιτεκτονική λειτουργίας των Windows 7, το οποίο σημαίνει ότι οι χρήστες των Windows Phone 7 δεν θα είναι σε θέση να αναβαθμίσουν σε Windows 8. Ωστόσο, το σύστημα είναι συμβατό με τις εφαρμογές των Windows 7. Αυτό οφείλεται κυρίως στην προσπάθεια αντικατάστασης των Windows CE υπέρ του πυρήνα των Windows NT που έχει πολλά στοιχεία των Windows 8, πράγμα που καθιστά ευκολότερο για τους προγραμματιστές να μεταφέρουν εφαρμογές μεταξύ των δύο πλατφορμών. Επίσης υποστηρίζουν την NTFS μορφή δεδομένων.

Επιπλέον τα Windows Phone 8 λειτουργούν σε συσκευές με μεγαλύτερες οθόνες και multi-core επεξεργαστές, NFC, βελτιωμένη υποστήριξη αφαιρούμενων μέσων αποθήκευσης, επανασχεδιασμένη αρχική οθόνη που επιτρέπει την αλλαγή μεγέθους πλακιδίων σύμφωνα με τη σπουδαιότητα τους και νέο Wallet Hub. Επιπροσθέτως, τα Windows Phone 8 θα περιλαμβάνουν περισσότερες δυνατότητες που απευθύνονται στις επιχειρήσεις, όπως η διαχείριση της συσκευής, κρυπτογράφηση BitLocker, και τη δυνατότητα να δημιουργήσουν ένα ιδιωτικό Marketplace για τη διανομή εφαρμογών σε υπαλλήλους. Τα Windows Phone 8 θα υποστηρίζει επίσης over-the-air ενημερώσεις και όλες οι συσκευές με Windows Phone 8 λειτουργικό σύστημα θα λάβουν υποστήριξη λογισμικού για τουλάχιστον 36 μήνες μετά την απελευθέρωσή τους στην αγορά.

Για τον προγραμματισμό σε αυτή την πλατφόρμα, οι εφαρμογές πρέπει να βασίζονται ή στο XNA, ένα σετ εργαλείων της Microsoft με διαχειρίσιμο περιβάλλον ανάπτυξης εφαρμογών, ή σε μια συγκεκριμένη έκδοση του Silverlight που να υποστηρίζει τα Windows Phone. Για να υπάρχει η δυνατότητα σχεδίασης και δοκιμής εφαρμογών με το Visual Studio, η Microsoft προσφέρει τα Windows Phone Developer Tools ως επέκταση. Αυτό το σετ εργαλείων υποστηρίζει υπολογιστές που χρησιμοποιούν Windows Vista SP2 ή νεότερα.

Η αρχιτεκτονική των Windows NT μπορεί να χωριστεί σε δύο μέρη: Το επίπεδο του χρήστη και το επίπεδο του πυρήνα (Εικόνα 18). Το επίπεδο του χρήστη είναι το λιγότερο προνομιούχο επίπεδο των Windows NT και δεν έχει άμεση πρόσβαση στο υλικό καθώς και περιορισμένη πρόσβαση στη μνήμη. Αντίθετα το επίπεδο του πυρήνα είναι πιο προνομιούχο και έχει άμεση πρόσβαση στο υλικό και τη μνήμη. [19]

Το επίπεδο του χρήστη περιλαμβάνει:

- Εφαρμογές του τελικού χρήστη
- Environment Υποσυστήματα

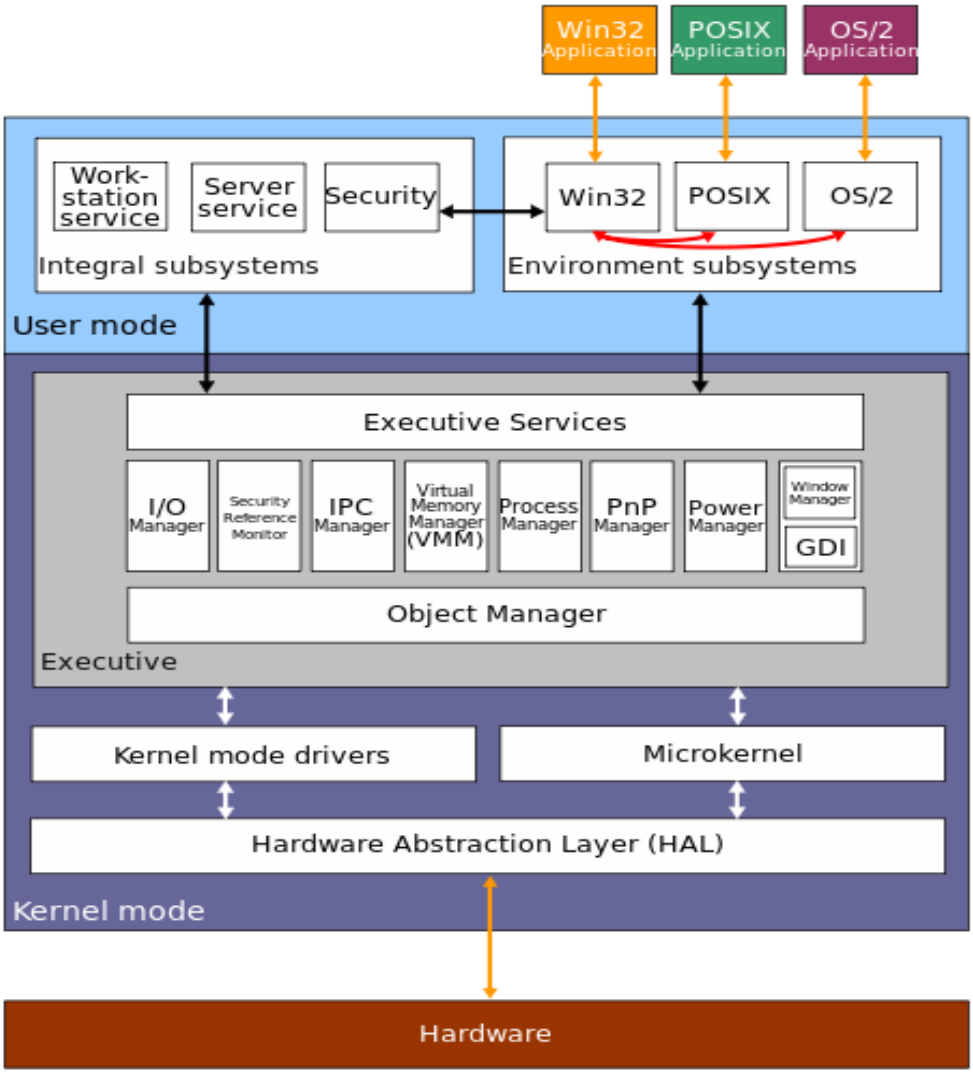
Το επίπεδο του πυρήνα περιλαμβάνει:

- NT Executive
- NT Kernel (microkernel)

- Επίπεδο αφαίρεσης υλικού (HAL)

Όπως και στο ios, ο πυρήνας του συστήματος αποτελεί ένα υβρίδιο microkernel και μονολιθικού συστήματος. Αυτό οφείλεται στο γεγονός ότι τα υποσυστήματα εξομοίωσης εκτελούνται στο επίπεδο λειτουργίας του χρήστη, αντί στο επίπεδο του πυρήνα, όπως συμβαίνει σε ένα μονολιθικό πυρήνα, και περαιτέρω, επειδή υλοποιούν μεγάλο αριθμό των σχεδιαστικών στόχων που μοιάζουν με τους στόχους του σχεδιασμού του Mach microkernel. Αντιστρόφως, ο λόγος που ο kernel των NT δεν είναι ένα σύστημα microkernel είναι επειδή τα περισσότερα από τα συστατικά του συστήματος εκτελούνται στον ίδιο χώρο διευθύνσεων με τον πυρήνας, όπως στην περίπτωση ενός μονολιθικού συστήματος.

Η αρχιτεκτονική του λειτουργικού συστήματος Windows NT παρουσιάζεται παρακάτω.



Εικόνα 18 - Αρχιτεκτονική δομή του Windows Phone OS

1.2.5. Android OS

Εικόνα 19 - Android OS logo

Το Android είναι λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας το οποίο τρέχει τον πυρήνα του λειτουργικού Linux (Εικόνα 19). Αρχικά αναπτύχθηκε από την Google και αργότερα από την Open Handset Alliance. Επιτρέπει στους κατασκευαστές λογισμικού να συνθέτουν κώδικα με την χρήση της γλώσσας προγραμματισμού Java ελέγχοντας την συσκευή μέσω βιβλιοθηκών λογισμικού ανεπτυγμένων από την Google. Τα Android αρχικά αναπτύχθηκαν από μια μικρή εταιρία λογισμικού η οποία εξαγοράστηκε από την Google. [20]

Η πρώτη παρουσίαση της πλατφόρμας Android έγινε τον Νοέμβριο του 2007, παράλληλα με την ανακοίνωση της ίδρυσης του οργανισμού Open Handset Alliance, μιας κοινοπραξίας 79 τηλεπικοινωνιακών εταιριών, εταιριών λογισμικού καθώς και κατασκευής hardware, οι οποίες είναι αφιερωμένες στην ανάπτυξη και εξέλιξη ανοιχτών προτύπων στις συσκευές κινητής τηλεφωνίας.

Η Google δημοσίευσε το μεγαλύτερο μέρος του κώδικα του Android υπό τους όρους της Apache License, μιας ελεύθερης άδειας λογισμικού. Μια μεγάλη κοινότητα προγραμματιστών ασχολείται με τον προγραμματισμό στο Android και με αυτό τον τρόπο αυξάνει τις δυνατότητες των συσκευών που το χρησιμοποιούν. Αυτή την στιγμή υπάρχουν πάνω από 200.000 εφαρμογές στο Android Market, το ηλεκτρονικό κατάστημα που έχει φτιάξει η Google, αν και υπάρχει και η δυνατότητα αγοράς εφαρμογών από τρίτες εταιρίες.

Από την στιγμή της εισόδου του στην αγορά το Android έχουν παρουσιάσει μια τεράστια αύξηση και στον αριθμό των συσκευών που το χρησιμοποιούν αλλά και του μεριδίου του στην αγορά, και αυτή την στιγμή θεωρείται το πιο διαδεδομένο λειτουργικό σύστημα για smartphones.

Για την ανάπτυξη εφαρμογών στο περιβάλλον του λειτουργικού χρησιμοποιείται το Android Software Development Kit το οποίο περιλαμβάνει ένα μεγάλο σετ από εργαλεία ανάπτυξης. Σε αυτό περιλαμβάνεται ένας debugger, βιβλιοθήκες, ένας εξομοιωτής, βιβλιογραφία, δείγματα κώδικα καθώς και σεμινάρια. Αυτή την στιγμή οι πλατφόρμες που υποστηρίζονται περιλαμβάνουν υπολογιστές που χρησιμοποιούν Linux (οποιαδήποτε μοντέρνα έκδοση), Mac OS X 10.4.9 ή νεότερο, Windows XP ή νεότερο. Το επίσημο περιβάλλον ανάπτυξης είναι το Eclipse με ταυτόχρονη χρησιμοποίηση των Android Development Tools αν και δίνεται η δυνατότητα χρησιμοποίησης οποιουδήποτε κειμενογράφου για την σύνταξη κώδικα Java ή XML και μέσω της γραμμής εντολών, η δημιουργία, κτίσιμο και debug εφαρμογών για Android αλλά και η δυνατότητα ελέγχου των συσκευών Android που έχουν συνδεθεί στον υπολογιστή. Με κάθε νέα έκδοση του

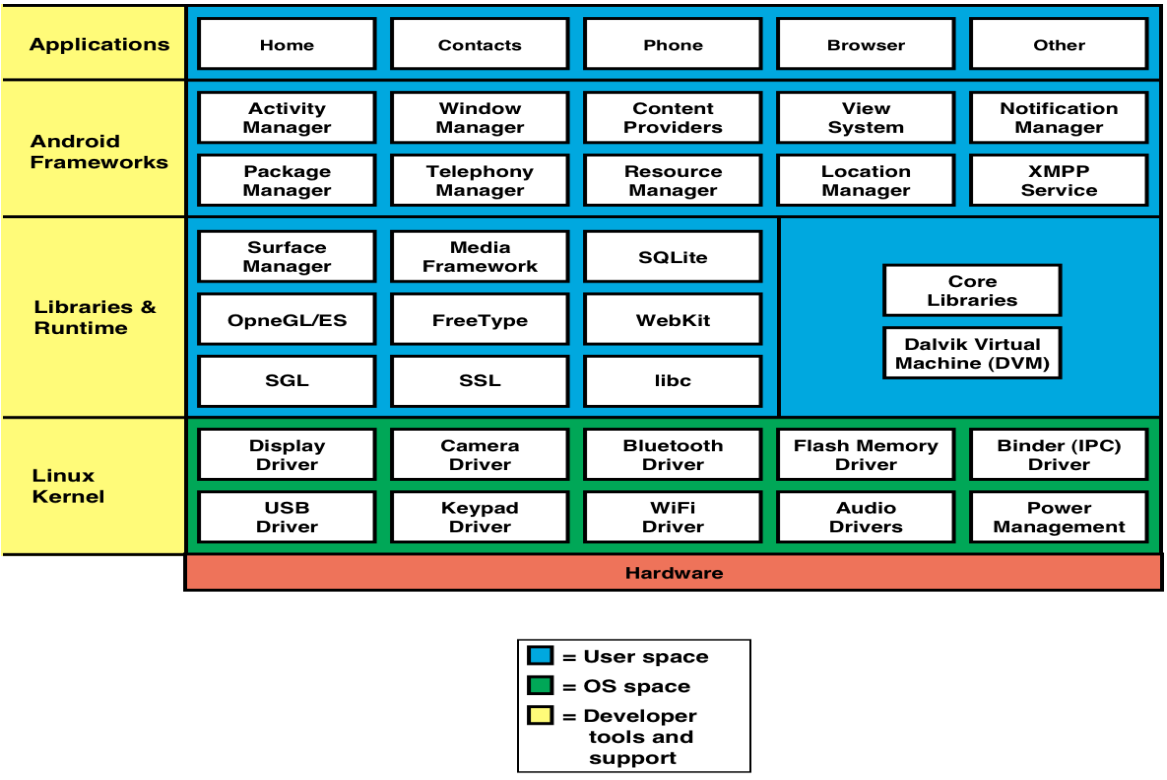
λειτουργικού συστήματος δημιουργείται και μια νέα έκδοση του SDK, με κάθε νέα έκδοση να μην σταματάει την υποστήριξη για ανάπτυξη εφαρμογών για την προηγούμενη έκδοση του λειτουργικού.

Όμως υπάρχουν και άλλοι τρόποι δημιουργίας εφαρμογών για το Android όπως το Native Development Kit το οποίο μπορεί να συντάξει βιβλιοθήκες γραμμένες σε C και άλλες γλώσσες προγραμματισμού σε κώδικα που χρησιμοποιούν οι επεξεργαστές ARM. Μια από τις καινοτομίες της πλατφόρμας Android είναι η δημιουργία εφαρμογών με το App Invertor, ένα περιβάλλον ανάπτυξης προγραμμάτων το οποίο βασίζεται σε Web τεχνολογίες και προορίζεται για νέους προγραμματιστές. Είναι κάτι που δείχνει τα προτερήματα ενός λειτουργικού που έχει τόσο ανοικτή αρχιτεκτονική.

Η αρχιτεκτονική του λειτουργικού συστήματος του Android αποτελείτε από 5 βασικά επίπεδα (Εικόνα 20). [12]

- Τον πυρήνα Linux (Linux Kernel)
- Τις εγγενείς και τις προηγμένες βιβλιοθήκες (Libraries)
- Τον χρόνο εκτέλεσης (Android Runtime)
- Το πλαίσιο εφαρμογής (Application Framework)
- Τις εφαρμογές (Applications)

Περαιτέρω ανάλυση ακολουθεί στο επόμενο κεφάλαιο.



Εικόνα 20 - Αρχιτεκτονική δομή του Android OS

1.3. Εφαρμογές για κινητές Συσκευές

Εικόνα 21 - Εφαρμογές κινητών συσκευών

Τα νέα λειτουργικά συστήματα σίγουρα έχουν αλλάξει τον τρόπο με τον οποίο χρησιμοποιούνται τα κινητά συστήματα τα τελευταία χρονιά αλλά ένα από τα πιο σημαντικά πράγματα που έχουν καταφέρει είναι η δημιουργία, μέσω αυτών, πολλών νέων και εντυπωσιακών εφαρμογών για τέτοιου είδους συστήματα (Εικόνα 21).

Οι εφαρμογές για κινητές πλατφόρμες είναι ένα μέρος της παγκόσμιας αγοράς κινητών συσκευών που μεγαλώνει και αναπτύσσεται ραγδαία. Αποτελούνται από λογισμικό που 'τρέχει' σε μια κινητή πλατφόρμα και εκτελεί συγκεκριμένες λειτουργίες για τον χρήστη του. Αυτές οι Mobile εφαρμογές χρησιμοποιούνται σε πλήθος μοντέλων κινητών τηλεφώνων, ακόμα και σε συσκευές χαμηλού κόστους στην αγορά. Στα νέα λειτουργικά συστήματα, μπορεί κάποιος να τις προμηθευτεί κατεβάζοντας τες από συγκεκριμένα ηλεκτρονικά καταστήματα εφαρμογών. Η ευρεία χρησιμοποίησή τους υπάρχει λόγω των πολλών λειτουργιών που μπορούν να πραγματοποιούν, που περιλαμβάνει από απλά περιβάλλοντα χρήσης για βασικές υπηρεσίες τηλεφωνίας και μηνυμάτων, μέχρι εξελιγμένες υπηρεσίες όπως τα βιντεοπαιχνίδια και εφαρμογές πολυμέσων.

Από τεχνικής άποψης, μπορούμε να τις χωρίσουμε σε κατηγορίες σε σχέση με το προγραμματιστικό περιβάλλον στο οποίο εκτελούνται:

- Εφαρμογές που τρέχουν στο περιβάλλον του λειτουργικού συστήματος όπως εφαρμογές που τρέχουν σε iOS, Android, Symbian OS, Windows Phone και Blackberry OS
- Εφαρμογές που τρέχουν σε Web/browser περιβάλλον όπως τα Webkit, Mozilla/Firefox, Opera Mini και RIM

- Άλλες πλατφόρμες και εικονικά συστήματα όπως τα Java/J2ME, BREW, Flash Lite και Silverlight

Από άποψη λειτουργιών μπορούμε να χωρίσουμε τις εφαρμογές για κινητές πλατφόρμες ως εξής:

- Εφαρμογές επικοινωνιών όπως Email, μηνυμάτων, περιήγησης στο διαδίκτυο, νέων και πληροφοριών και κοινωνικών δικτύων
- Εφαρμογές παράγωγης όπως ημερολόγια, αριθμομηχανές, σημειώσεων, υπενθυμίσεων, επεξεργασίας λέξεων, λογιστικών φύλλων, υπηρεσιών GPS και τραπεζικών υπηρεσιών
- Εφαρμογές πολυμέσων όπως γραφικών και εικόνας, παρουσίασης, αναπαραγωγής βίντεο, αναπαραγωγής ήχου και ροής δεδομένων ήχου και εικόνας
- Εφαρμογές παιγνιδιών όπως παζλ και στρατηγικής, τράπουλας και καζίνο, δράσης και περιπέτειας, αθλητικές και χόμπι.

Υπάρχουν καταστήματα εφαρμογών για όλα τα κύρια λειτουργικά συστήματα. Αυτά περιλαμβάνουν [20] [13] [6]:

- **Google Play:** περισσότερες από 800.000 εφαρμογές για Android συσκευές
- **Apple App Store**: πάνω από 900.000 διαθέσιμες εφαρμογές, 140.000 από αυτές ειδικά σχεδιασμένες για το iPad.
- **iTunes**: μουσική, videos, τηλεοπτικά shows, βιβλία και podcasts για χρήστες iPhone και iPad
- **BlackBerry App World**: περισσότερες από 250.000 εφαρμογές για BlackBerry Smartphones
- **Ovi Store**: πάνω από 10.000 εφαρμογές για Nokia Smartphones με λειτουργικό σύστημα Symbian
- **Windows Marketplace**: πάνω από 90.000 εφαρμογές για χρήστες Windows Phone

Τα τελευταία χρόνια οι εφαρμογές για κινητές πλατφόρμες έχουν εξελιχθεί ως ένα σημείο που προσφέρουν στον χρήστη μια πλούσια και γρήγορη εμπειρία χρήσης. Από αυτή την άποψη αυτές οι εφαρμογές έχουν χαρακτηριστικές διάφορες από την πλοήγηση σε ιστοσελίδες φτιαγμένες για κινητά συστήματα (Mobile Web) οπού ακόμα χαρακτηρίζονται από προβλήματα πρόσβασης αλλά και χαμηλές ταχύτητες στο δίκτυο κινητής τηλεφωνίας.

Κεφάλαιο 2° Android OS

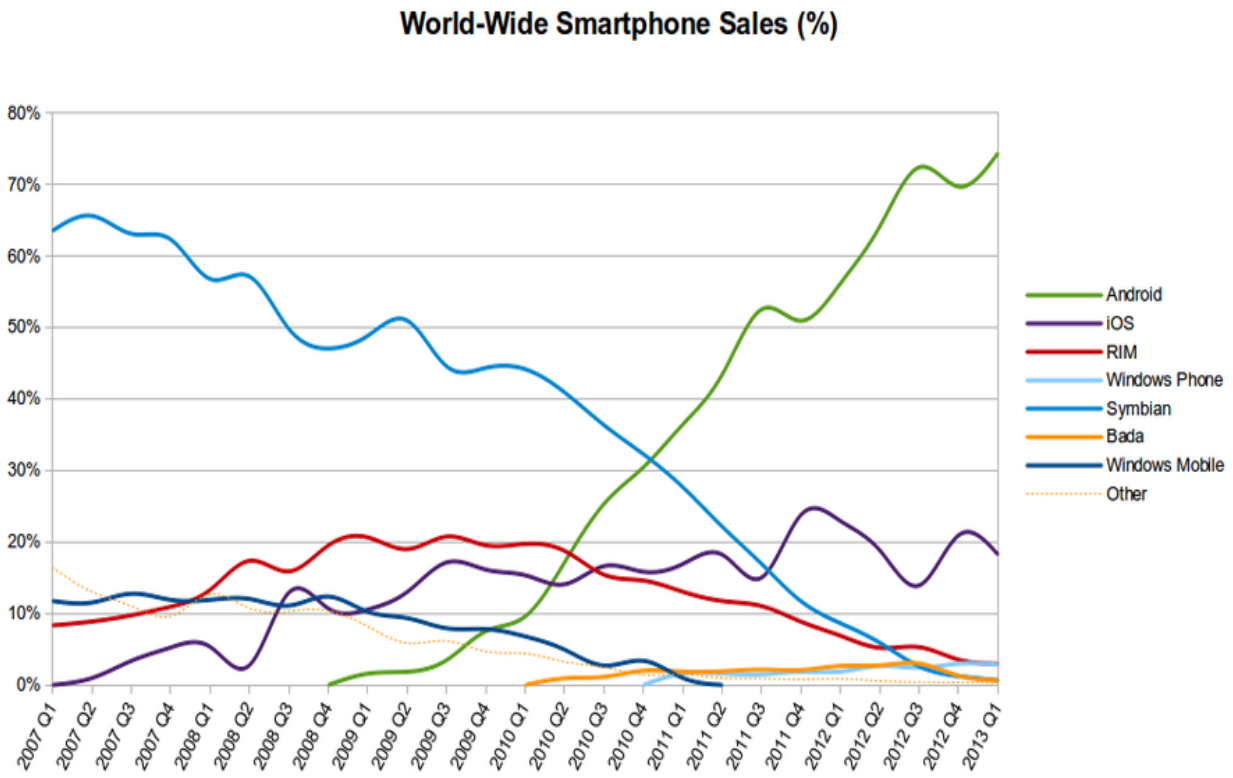
2.1. Ιστορική αναδρομή

Εικόνα 22 - Όλες οι εκδόσεις του Android OS

Το Android δημιουργήθηκε το 2003 στην Καλιφόρνια από τους Rubin, Miner, Sears και White. Αρχικός τους σκοπός ήταν να δημιουργήσουν ένα λειτουργικό σύστημα για smartphones. Αρχικά η ομάδα του Android λειτουργούσε μυστικά, αλλά η μεγάλη ανάπτυξη στο λειτουργικό ξεκίνησε μετά την εξαγορά του από την Google το 2005. Από τη χρονιά εκείνη μέχρι και το 2007 η Google δούλευε σιωπηλά πάνω στο Android κατοχυρώνοντας πατέντες και ψάχνοντας συνεργάτες. [20]

Το 2007 δημιουργήθηκε η Open Handset Alliance, ένας συνεταιρισμός που αποτελούνταν από τη Google, την HTC, την Samsung, την Qualcomm (κατασκευαστές επεξεργαστών) και άλλους με σκοπό να κάνουν το Android ένα ανοικτό λογισμικό και να κυκλοφορήσουν τα πρώτα smartphones με Android. Πράγματι, το πρώτο smartphone με λειτουργικό Android κυκλοφόρησε ένα χρόνο μετά από την HTC και ονομαζόταν HTC Dream. Από εκεί και μετά πρώτη η Samsung και δεκάδες άλλες εταιρείες υιοθέτησαν το Android ως λειτουργικό σύστημα για τις συσκευές που κατασκεύαζαν. Η αναφορά της Samsung δεν είναι τυχαία, αφού είναι η πρώτη εταιρεία στις πωλήσεις κινητών παγκοσμίως και η εξάπλωση του Android οφείλεται κατά μεγάλο βαθμό σε αυτήν.

Σήμερα το Android με τη σταθερή και διαρκώς ανοδική της πορεία έχει καταφέρει να είναι ο κυρίαρχος της αγοράς. Με βάση τα στοιχεία του πρώτου τριμήνου του 2013 , το Android καταλαμβάνει την πρώτη θέση σε αγορές με ποσοστό μεγαλύτερο του 75% παγκοσμίως (Εικόνα 23).



Εικόνα 23 - Παγκόσμιες πωλήσεις των mobile os

2.2. Οι διαφορετικές εκδόσεις του Android

Στη συνέχεια παρατίθενται όλες οι εκδόσεις του Android που έχουν κυκλοφορήσει έως σήμερα δίδοντας κάποια βασικά χαρακτηριστικά για την κάθε μία ξεχωριστά (Εικόνα 22). [21]

2.2.1. Android 4.1 Jelly Bean

Η έκδοση Jelly Bean, ανακοινώθηκε τον Ιούνιο του 2012 και προσθέτει μια σειρά από σημαντικά χαρακτηριστικά για το Android. Παραθέτουμε τα χαρακτηριστικά του Android 4.1.

- Google Now: ένα εργαλείο βοηθός που εμφανίζει τις σχετικές πληροφορίες με βάση το ιστορικό αναζήτησής και τα δεδομένα θέσης.
- Υψηλός ρυθμός περιήγησης μέσα στα μενού και τα home screens
- Προβολή φωτογραφιών γρήγορα περνώντας από την κάμερα σε προβολή αυτών ως filmstrips.

- Τα Widgets και τις εφαρμογές μπορεί ο χρήστης να τα μετακινήσει καθώς προσθέτει νέα.
- Οι ειδοποιήσεις τώρα περιλαμβάνουν περισσότερες πληροφορίες, όπως φωτογραφίες ή το θέμα στα μηνύματα ηλεκτρονικού ταχυδρομείου.
- Τα αποτελέσματα αναζήτησης μπορεί τώρα να εμφανίζουν απαντήσεις σε ερωτήματα, και όχι απλώς μια λίστα με Google συνδέσμους στο διαδίκτυο.
- Ένας νέος τρόπος κινήσεων για τη βελτίωση της προσβασιμότητας για τυφλούς χρήστες, επιτρέποντάς τους να περιηγηθούν στο UI χρησιμοποιώντας touch χειρονομίες, σε συνδυασμό με την παραγωγή ομιλίας.

2.2.2. Android 4.0 Ice Cream Sandwich

Η έκδοση Ice Cream Sandwich (ICS) ανακοινώθηκε στο Google I / O συνέδριο τον Μάιο 2011. Η έκδοση αυτή σχεδιάστηκε για να συγχωνεύσει την έκδοση Gingerbread για κινητά τηλέφωνα με την έκδοση Honeycomb, η οποία είχε σχεδιαστεί για τα table. Πλεονεκτήματα της έκδοσης Ice Cream Sandwich σε σχέση με την έκδοση Gingerbread:

- Ταχύτερο και πιο ομαλό πρόγραμμα περιήγησης.
- Η παρακολούθηση της κίνησης δεδομένων βοηθάει τον χρήστη να μην υπερβεί το όριο χρήσης δεδομένων που επιβάλλεται από τις εταιρίες κινητής τηλεφωνίας.
- Περισσότερος χώρος αποθήκευσης για τις εφαρμογές του χρήστη.
- Ένα νέο φιλικό προς το χρήστη action bar που αντικαθιστά το κουμπί του Μενού
- Αναγνώριση προσώπου για το ξεκλείδωμα του τηλεφώνου του χρήστη.
- Η ικανότητα να απορρίπτει ο χρήστης κλήσεις με προ-επιλεγμένα μηνύματα κειμένου

Ένα μειονέκτημα είναι το γεγονός ότι η έκδοση ICS δεν υποστηρίζει το Adobe Flash, αλλά δεν αποτελεί πλέον σημαντική έλλειψη καθώς η εταιρεία έχει ήδη επιβεβαιώσει ότι πρόκειται να το υποστηρίξει .

2.2.3. Android 3.0 και 3.1 Honeycomb

Η έκδοση Honeycomb του Android δημιουργήθηκε για να έχει εφαρμογή στις μεγάλες οθόνες των υπολογιστών tablet. Αυτή η έκδοση του Android είναι ένα ξεχωριστός κλάδος που απευθύνεται μόνο σε tablet, και δεν θα έχει εφαρμογή σε κινητά τηλέφωνα.

Το Android 3.1 ανακοινώθηκε το Μάιο του 2011, και προσθέτει σημαντικές βελτιώσεις για τον χρήστη της έκδοσης Honeycomb. Το Google αναφέρει ότι η έκδοση Honeycomb θα κάνει «τα στοιχεία UI να είναι πιο εύκολο να τα δούμε, να τα καταλάβουμε και τα χρησιμοποιήσουμε». Τα Widgets θα αποκτήσουν τη δυνατότητα μεγαλώνουν ή να μικραίνουν, για να ταιριάζουν στην οθόνη. Το Android 3.1 υποστηρίζει τους USB flash drives στα tablet για να μεταφέρει ο χρήστης αρχεία χωρίς σύνδεση σε υπολογιστή, καθώς και τα USB πληκτρολόγια, ποντίκια και χειριστήρια.

Χαρακτηριστικά:

- Ένα μπλε σχεδιασμός wireframe δίνει στην έκδοση Honeycomb μια εμπνευσμένη εμφάνιση.
- Η αρχική οθόνη φαίνεται να περιστρέφεται γύρω από ένα 3D καρουσέλ.
- Τα widgets είναι μεγαλύτερα και πιο τολμηρά ώστε να ταιριάζουν με το μέγεθος της οθόνης του tablet.
- Τα κουμπιά – στην αρχική οθόνη και πίσω - έχουν μεταφερθεί επί της οθόνης, ως εικονικά πλήκτρα που κινούνται ταυτόχρονα καθώς περιστρέφετε το tablet.
- Το μενού των εφαρμογών επανατοποθετείται στην άνω δεξιά γωνία. Υπάρχει επίσης ένα νέο κουμπί που εμφανίζει μια λίστα με τις τρέχουσες εφαρμογές, ορατές ως μικρογραφίες.
- Οι βασικές εφαρμογές, όπως το Gmail και το YouTube, σε μεγάλο βαθμό έχουν επανασχεδιαστεί ώστε να επωφεληθούν οι χρήστες του διαθέσιμου χώρου.
- Το πρόγραμμα περιήγησης στο διαδίκτυο εισάγει περιήγηση με καρτέλες, ένα χαρακτηριστικό γνωστό από τα desktop προγράμματα περιήγησης, όπως το Chrome. Υπάρχει επίσης η δυνατότητα ανώνυμης περιήγησης για να περιηγηθεί ο χρήστης ήσυχα.
- Τέλος, ένα μεγαλύτερο multi-touch πληκτρολόγιο επιτρέπει στον χρήστη να κρατήσει πατημένα πολλαπλά κλειδιά με προσωρινή εναλλαγή για παράδειγμα μεταξύ γραμμάτων και αριθμών.

2.2.4. Android 2.3 Gingerbread

Η έκδοση Gingerbread λανσαρίστηκε το Δεκέμβριο του 2010. Το NFC για πληρωμές και το SIP για κλήσεις μέσω διαδικτύου και τα δύο θέτουν τα θεμέλια για τις μελλοντικές εξελίξεις αν και δεν είναι πολύ διασκεδαστικά.

Το Android 2.3.3 όταν έφτασε στα τηλέφωνα τον Απρίλιο του 2011, πρόσθεσε μόνο ένα νέο χαρακτηριστικό - τη δυνατότητα για τηλέφωνα με single-core επεξεργαστές να τρέχουν εφαρμογές που έχουν σχεδιαστεί για dual-core επεξεργαστές. Το Android 2.3.4 πρόσθεσε ακόμα περισσότερες διορθώσεις σφαλμάτων. Παραθέτουμε τα χαρακτηριστικά του Android 2.3.:

- Τα στοιχεία του περιβάλλοντος εργασίας του χρήστη, όπως η γραμμή ειδοποιήσεων, μετατρέπονται από γκρι σε μαύρο χρώμα, σε μια προσπάθεια να αποφευχθεί το burn -in της οθόνης να και να αυξηθεί η διάρκεια ζωής της μπαταρίας.

- Οι συντομεύσεις του πληκτρολογίου στην οθόνη του κινητού τηλεφώνου αυξάνονται και ένας δείκτης βοηθά να επιλέξει ο χρήστης και να αντιγράψει κείμενο.

- Υποστήριξη για μια μπροστινή κάμερα για κλήσεις βίντεο και emo πορτρέτα.

- Χρήση download manager ώστε να μπορεί ο χρήστης να παρακολουθεί ότι έχει κατεβάσει.

2.2.5. Android 2.2 Froyo

Φτάνοντας στο Μάιο του 2010, η έκδοση Froyo εισήγαγε το Flash, το οποίο έχει γίνει μια από τις καθοριστικές διαφορές μεταξύ Android και του κύριου ανταγωνιστή της, το iPhone. Πλεονεκτήματα:

- Το Flash Player 10.1 ήρθε στο Android. Βίντεο, slideshow φωτογραφιών και audio streaming ξαφνικά έγιναν ορατά στο κινητό τηλέφωνο του χρήστη.

- Οι ρυθμίσεις του κινητού τηλεφώνου συνδέθηκαν με τις επαφές και το e-mail για την δημιουργία αντιγράφων ασφαλείας σε διακομιστές της Google και τα οποία αποκαθίσταται αυτόματα αν ο χρήστης επιλέξει ένα νέο Android τηλέφωνο.

- Παρέχει περισσότερες δυνατότητες για τη σύνδεση με το λογαριασμό Microsoft Exchange, συμπεριλαμβανομένου και της πρόσβασης στο Outlook στο βιβλίο διευθύνσεων. Επίσης, παρέχει την δυνατότητα στο τμήμα μηχανογράφησης να «ξεσκονίσει» από μακριά το τηλέφωνό.

- Στα σημεία πρόσβασης Wi-Fi hotspot επιτρέπετε ο χρήστης να μοιραστεί την 3G σύνδεση στο διαδίκτυο του τηλεφώνου του με άλλες συσκευές, μέσω Wi-Fi.

- Ταχύτερη περιήγηση στο διαδίκτυο, χάρη στις αλλαγές στο πρόγραμμα περιήγησης.

- Καλύτερη συμβατότητα Bluetooth στα ηχεία αυτοκινήτου, καθώς και η προσθήκη της κλήσης φωνής μέσω Bluetooth.

2.2.6. Android 2.0 και 2.1 Eclair

Η έκδοση Android 2.0 έφτασε, μόλις έναν μήνα μετά την έκδοση Donut, τον Νοέμβριο του 2009. Η έκδοση Eclair έφτασε και υποστηρίζει τον Microsoft Exchange server, τον οποίο οι περισσότερες επιχειρήσεις χρησιμοποιούν για το ηλεκτρονικό ταχυδρομείο τους. Η έκδοση Android 2.1 Eclair έφτασε τον Ιανουάριο του 2010. Η έκδοση αυτή διόρθωσε κάποια σφάλματα και πρόσφερε στους προγραμματιστές εφαρμογές με περισσότερες δυνατότητες, αλλά δεν πρόσθεσε νέα χαρακτηριστικά στους χρήστες. Παραθέτουμε τα χαρακτηριστικά του Android 2.1:

- Υποστήριξη ανταλλαγής, ώστε ο χρήστης να λαμβάνει τα Outlook e-mail του. Υπάρχει επίσης ένας ενιαίος φάκελος εισερχομένων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ωστόσο, ακόμη διατηρείται με POP και IMAP e-mail σε μια ξεχωριστή εφαρμογή στο Gmail.

- Η υποστήριξη πολλαπλών λογαριασμών Google παρέχει την δυνατότητα να φυλάσσονται όλα τα Gmail του χρήστη.

- Ρυθμίσεις της φωτογραφικής μηχανής συμπεριλαμβανομένης της υποστήριξης για flash, ψηφιακό zoom, ισορροπία λευκού και χρωματικά εφέ.

- Παρέχει την δυνατότητα αναζήτησης μέσα στα μηνύματα κειμένου και τα μηνύματα MMS.

- Η Multi-touch υποστήριξη στο πληκτρολόγιο της οθόνης βοηθά να εντοπίσει ο χρήστης το λάθος αμέσως. Το λεξικό ενσωματώνει τις επαφές, έτσι ώστε ο χρήστης να επιλέγει τα ονόματα των επαφών.

- Το πρόγραμμα περιήγησης στον διαδίκτυο ανανεώνεται με νέα γραμμή διευθύνσεων και μικρογραφίες για επιλογή στα bookmarks.

2.2.7. Android 1.6 Donut

Τον Οκτώβριο του 2009, εμφανίστηκε η έκδοση Donut. Προσέφερε λιγότερο σημαντικές βελτιώσεις, αλλά έφερε στα Android νέο πλήθος χρηστών, χάρη στην προσθήκη της υποστήριξης για CDMA - τεχνολογία που χρησιμοποιείται από ορισμένα αμερικανικά δίκτυα κινητής τηλεφωνίας. Παραθέτουμε τα χαρακτηριστικά του Android 1.6:

- Η λειτουργία αναζήτησης βοήθησε τους χρήστες να εντοπίσουν τις εφαρμογές και τις επαφές στο κινητό τους τηλέφωνο καθώς και να μεταβούν στην αναζήτηση στο διαδίκτυο.

- Υποστήριξη για μεγαλύτερης ανάλυσης οθόνη για τα Android τηλέφωνα διαφόρων μεγεθών.

- Στην πλοήγηση Google Maps προστίθεται δωρεάν το turn-by-turn sat-nav.

2.2.8. Android 1.5 Cupcake

Η χρήση ονομάτων γλυκών ξεκίνησε με το Cupcake, η πρώτη σημαντική αναβάθμιση για το Android, το οποίο έκανε την εμφάνιση του τον Μάιο του 2009. Η έκδοση Cupcake ήταν γεμάτη με νέα χαρακτηριστικά, αλλά ίσως το πιο σημαντικό ήταν το εικονικό πληκτρολόγιο, το οποίο άνοιξε το δρόμο για πλήκτρα, όπως το HTC Magic. Βασικά χαρακτηριστικά:

- Συντομεύσεις και widgets στην αρχική οθόνη σημαίνει ότι τα κινητά τηλέφωνα τώρα μπορούν να είναι προσαρμοσμένα στις ανάγκες του κάθε χρήστη.

- Ένα εικονικό πληκτρολόγιο επί της οθόνης θα μπορούσε να αντικαταστήσει το πληκτρολόγιο με αποτέλεσμα τα κινητά τηλέφωνα να είναι ελαφρύτερα και πιο λιτά.

- Προστέθηκε η εγγραφή βίντεο με κάμερα, καθώς και η δυνατότητα να ανεβάζονται τα βίντεο απευθείας στο YouTube.

- Το Stereo Bluetooth επιτρέπει στον χρήστη να ακούσει μουσική χωρίς καλώδια.

- Το πρόγραμμα περιήγησης στο διαδίκτυο παίρνει μεγάλη ώθηση με τη λειτουργία αντιγραφής και επικόλλησης.

2.2.9. Android 1.0 και 1.1

Το Android γεννήθηκε το 2008, εφαρμόστηκε στο T-Mobile G1. Το T-Mobile G1 κατασκευάστηκε από την HTC. Αυτή η πρώιμη έκδοση του Anroid είχε πολλές δυνατότητες, αλλά ταίριαζε καλύτερα σε gadgets.
Παρά το γεγονός ότι το G1 δεν μπορούσε να νικήσει την εκκολαπτόμενη iPhone της Apple στην βιομηχανία του στυλ, προσέφερε τα περισσότερα από τα κύρια χαρακτηριστικά του Android που γνωρίζουν και αγαπούν οι χρήστες. Χαρακτηριστικά:

- Το Android Market προσφέρει εφαρμογές χωρίς τους αυστηρούς κανόνες εισόδου του App Store της Apple, και παρέχει μια ποικιλία από εφαρμογές που κυμαίνονται από την υψηλή προς την πιο γελοία.

- Το πρόγραμμα περιήγησης της Android κάνει πιο ευχάριστη την περιήγηση στο διαδίκτυο μέσω του κινητού τηλέφωνου του χρήστη, χάρη στην ικανότητα να αποδώσει τις ιστοσελίδες γρήγορα και με ακρίβεια.

- Η Google Maps χρησιμοποιεί το GPS του κινητού τηλεφώνου και το Wi-Fi για να εντοπίσει τη θέση του χρήστη στον χάρτη, με αποτέλεσμα ο χρήστης ποτέ ξανά δεν θα χαθεί.

- Ο συγχρονισμός με τις επαφές του χρήστη, το e-mail και το ημερολόγιο του χρήστη σε απευθείας σύνδεση με την Google αρχικά έκανε τον χρήστη δύσπιστο όσον αφορά την ανταλλαγή όλων των δεδομένων με την Google, αλλά οι ανησυχίες για την προστασία της ιδιωτικής ζωής του χρήστη σύντομα νικήθηκαν από την ευκολία της πρόσβασης οπουδήποτε και από οπουδήποτε.

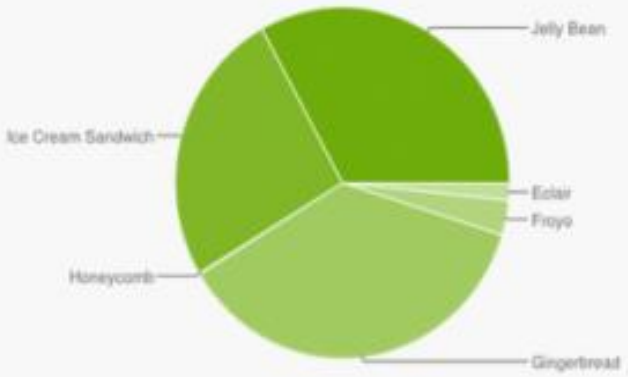
2.2.10. Στατιστικά των Εκδόσεων

Στις αρχές κάθε μήνα η Google δημοσιοποιεί τα αποτελέσματα από τις γνωστές στατιστικές της που αποκαλύπτουν τα ποσοστά χρήσης των διαφορετικών εκδόσεων του λειτουργικού Android. Οι στατιστικές βασίζονται στις ενεργές Android συσκευές, δηλαδή σε smartphones και tablets που έχουν πρόσφατα εισέλθει στο Google Play.

Για τον Μάιο, λοιπόν, η έκδοση 4.1 Jelly Bean του OS συνεχίζει να σημειώνει άνοδο με ποσοστό 33%. Αντίθετα, το Ice Cream Sandwich σημειώνει πτώση και είναι πλέον εγκατεστημένο στο 25,6 % των ενεργών Android συσκευών, γεγονός που φανερώνει ότι υπήρξαν αρκετές αναβαθμίσεις σε Jelly Bean μέσα στον προηγούμενο μήνα. Παρόλα αυτά, η έκδοση 2.3 Gingerbread του λειτουργικού παραμένει στην πρώτη θέση και είναι εγκατεστημένη στο 36,5% των Android συσκευών, αν και φαίνεται πώς υπάρχει μία σταθερή πτώση στα ποσοστά της. Παρακάτω μπορείτε να δείτε αναλυτικά τον πίνακα με τα ποσοστά των διαφορετικών εκδόσεων του OS: [22]

Version	Codename	API	Distribution
1.6	Donut	4	0.1%
2.1	Eclair	7	1.5%
2.2	Froyo	8	3.2%
2.3 - 2.3.2	Gingerbread	9	0.1%
2.3.3 - 2.3.7		10	36.4%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	25.6%
4.1.x	Jelly Bean	16	29.0%
4.2.x		17	4.0%

Data collected during a 14-day period ending on June 3, 2013.
Any versions with less than 0.1% distribution are not shown.

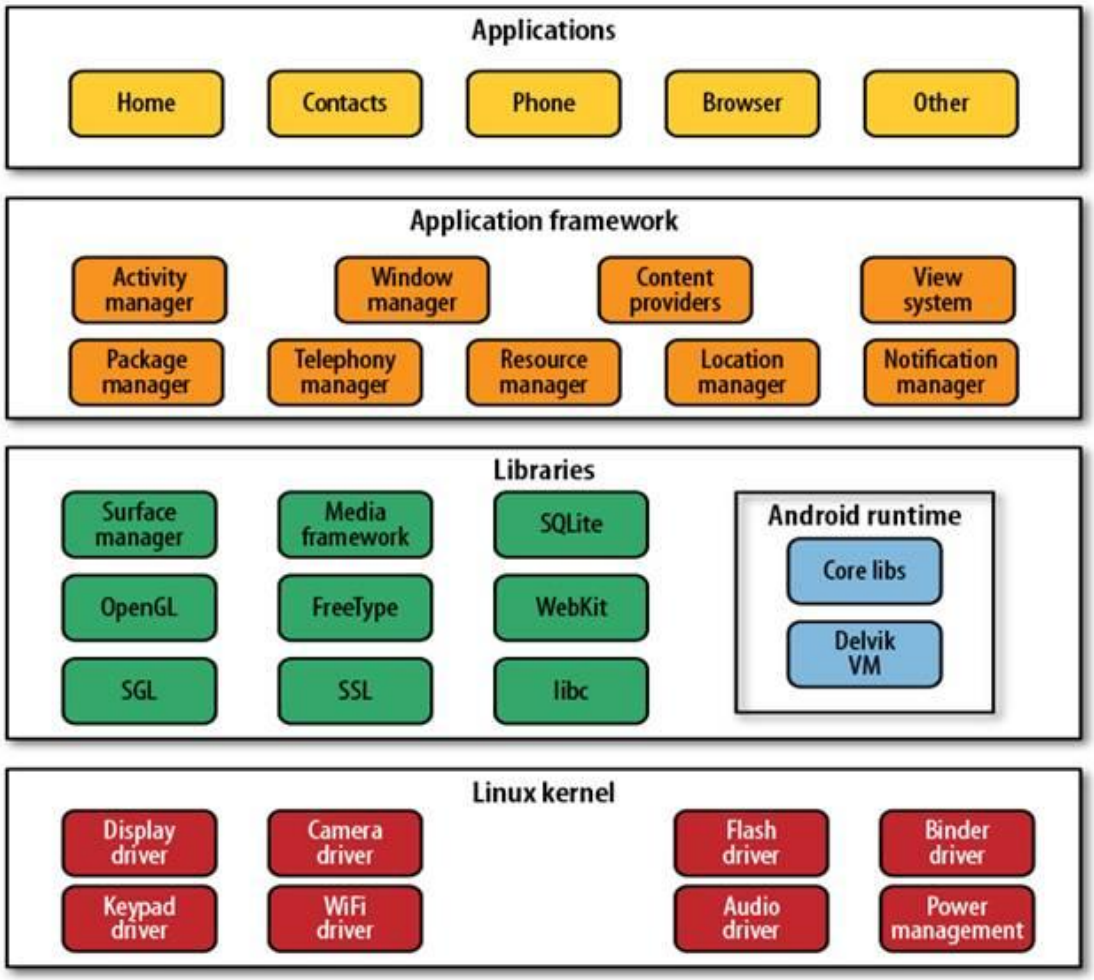


Εικόνα 24 - Ποσοστά χρήσης των εκδόσεων του Android

2.3. Αρχιτεκτονική δομή του Android

Το Android δεν είναι μόνο ένα λειτουργικό σύστημα. Είναι μια στοίβα λογισμικού η οποία αποτελείτε από το λειτουργικό σύστημα, τις υπηρεσίες διασύνδεσης με τις εφαρμογές (middleware) και τέλος από τις κύριες (core) εφαρμογές, μεταξύ αυτών, ενός email client, μιας εφαρμογής διαχείρισης SMS, ενός ημερολογίου, ενός browser, μιας εφαρμογής διαχείρισης επαφών, και άλλες οι οποίες έρχονται προεγκατεστημένες με την υπόλοιπη στοιβάδα λογισμικού του Android.

Στο παρακάτω σχεδιάγραμμα παρουσιάζεται μια οπτική αναπαράσταση της αρχιτεκτονικής αυτής.



Εικόνα 25 - Τα 5 επίπεδα της αρχιτεκτονικής δομής του Android

Όπως απεικονίζεται λοιπόν η αρχιτεκτονική του λειτουργικού συστήματος αποτελείτε από 5 βασικά επίπεδα . (Εικόνα 25). [23]

- Τον πυρήνα Linux (Linux Kernel)
- Τις εγγενείς και τις προηγμένες βιβλιοθήκες (Libraries)
- Τον χρόνο εκτέλεσης (Android Runtime)
- Το πλαίσιο εφαρμογής (Application Framework)
- Τις εφαρμογές (Applications)

2.3.1. Πυρήνας Linux (Linux Kernel)

Η βάση της στοίβας λογισμικού του Android είναι ο πυρήνας Linux. Ο τροποποιημένος πυρήνας του συστήματος βασίζεται στην έκδοση 2.6 (και στην έκδοση 3.0.1 για το

Android 4.0) του Linux Kernel, η οποία υποστηρίζει όλες τις κύριες λειτουργίες του λειτουργικού συστήματος. Οι λειτουργίες αυτές αφορούν διαχείριση μνήμης, διαχείριση διεργασιών, λειτουργίες δικτύου, ασφάλεια του λειτουργικού, και ένα σύνολο οδηγών υλικού (hardware drivers). Οι οδηγοί αυτοί είναι υπεύθυνοι για την επικοινωνία του software με το hardware της συσκευής. Ενδεικτικά ο πυρήνας του Android περιέχει:

- Οδηγό προβολής οθόνης Οδηγό
- Wifi και Bluetooth
- Οδηγό κάμερας

Ο πυρήνας του Android μπορεί να βασίζεται στον πυρήνα του Linux, αλλά διαφέρει αρκετά από αυτόν. Ο λόγος είναι οι αλλαγές στην αρχιτεκτονική που έχει κάνει η Google για να είναι ελαφρύτερος και βελτιστοποιημένος για χρήση σε κινητές συσκευές. Αυτό σημαίνει ότι παρότι το Android είναι κατά βάση Linux, επί της ουσίας είναι αρκετά δύσκολο να τρέξουν εφαρμογές ή να χρησιμοποιηθούν βιβλιοθήκες από τη μία πλατφόρμα στην άλλη.

2.3.2. Βιβλιοθήκες

Στο δεύτερο επίπεδο της στοίβας έχουμε τις βιβλιοθήκες του Android. Αυτές ουσιαστικά αποτελούν τα APIs που είναι διαθέσιμα στους προγραμματιστές για την ανάπτυξη των εφαρμογών. Οι βιβλιοθήκες από μόνες τους δεν αποτελούν εφαρμογές αλλά ενσωματώνονται και χρησιμοποιούνται από τις εφαρμογές για τις διάφορες λειτουργίες που παρέχει η καθεμία από αυτές. Ουσιαστικά αποτελούν ένα από τα δομικά υλικά των εφαρμογών, και άρα είναι αναπόσπαστο κομμάτι τους. Οι δυνατότητες των βιβλιοθηκών του Android γίνονται εμφανείς στους προγραμματιστές στην στοίβα του πλαισίου εφαρμογής. [20]

Το σύνολο σχεδόν των βιβλιοθηκών είναι γραμμένο σε C και C++, οι οποίες έχουν μεταγλωττιστεί για τη χρήση τους από το λειτουργικό. Μερικές από τις κύριες βιβλιοθήκες του Android είναι:

- **System C library:** μια ενσωμάτωση της standard βιβλιοθήκης συστήματος της C (libc) τροποποιημένη για κινητές συσκευές βασισμένες στο Linux.
- **Βιβλιοθήκες Πολυμέσων:** βασίζεται στο OpenCORE και υποστηρίζει αναπαραγωγή και εγγραφή πολλών δημοφιλών μέσων ήχου και εικόνας, όπως: MPEG4, H.264, MP3, AAC, AMR, JPG, και PNG

- **Surface Manager:** διαχειρίζεται την πρόσβαση στο υποσύστημα προβολής, και συνθέτει απρόσκοπτα δισδιάστατα και τρισδιάστατα επίπεδα γραφικών τα οποία προέρχονται από πολλαπλές εφαρμογές.
- **LibWebCore:** μια μοντέρνα μηχανή υποστήριξης πλοήγηση στο διαδίκτυο (browser engine) η οποία χρησιμοποιείτε και από τον ενσωματωμένο browser του Android αλλά και από τις WebViews που ενσωματώνονται στις εφαρμογές.
- **SGL:** η γνωστή μηχανή δισδιάστατων γραφικών
- **Βιβλιοθήκες 3D:** μια υλοποίηση βασισμένη στα APIs του OpenGL ES 1. Οι βιβλιοθήκες χρησιμοποιούν είτε τρισδιάστατη επιτάχυνση υλικού, όπου αυτή είναι διαθέσιμη, είτε μια υψηλά βελτιωμένη τρισδιάστατη επιτάχυνση λογισμικού σε περίπτωση που η πρώτη δεν είναι διαθέσιμη.
- **FreeType:** παρέχει ευκρίνεια γραφικών στα bitmaps και τις γραμματοσειρές των εφαρμογών του συστήματος.
- **SQLite:** μια πανίσχυρη αλλά και πολύ ελαφριά σχεσιακή βάση δεδομένων διαθέσιμη για όλες τις εφαρμογές

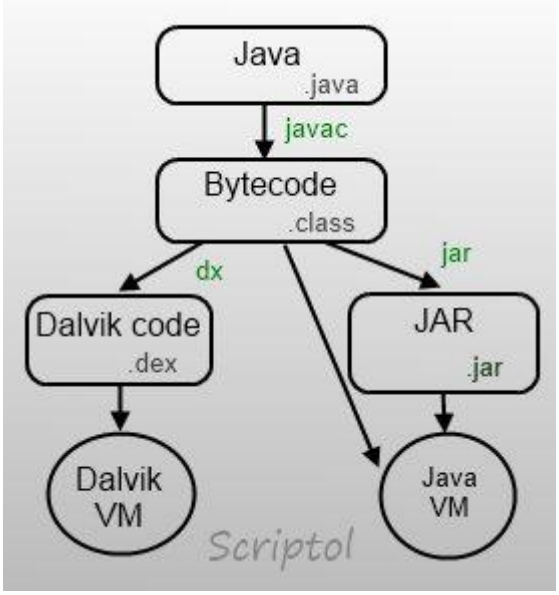
2.3.3. Χρόνος Εκτέλεσης Εφαρμογής (Android Runtime)

Ο χρόνος εκτέλεσης των εφαρμογών του Android, βρίσκεται στο ίδιο επίπεδο με τις κύριες βιβλιοθήκες και την μηχανή Dalvik. Εδώ βρίσκεται το κοινό σημείο επαφής μεταξύ των δυνατοτήτων που παρέχουν οι βιβλιοθήκες και του χρόνου εκτέλεσης της εικονικής μηχανής Dalvik η λειτουργία του οποίου, περιγράφεται παρακάτω.

2.3.3.1. Η εικονική μηχανή Dalvik

Σχεδόν το σύνολο των APIs του Android βασίζονται στη γλώσσα προγραμματισμού Java. Στην Java ως γνωστόν υπάρχει η λεγόμενη Java Virtual Machine στην οποία εκτελείτε ο κώδικας bytecode των εφαρμογών. Στο Android υπάρχει κάτι παρόμοιο και δεν είναι άλλο από την εικονική μηχανή Dalvik.

Η Dalvik λοιπόν είναι η εικονική μηχανή μέσω της οποίας τρέχουν οι εφαρμογές του Android. Κάθε εφαρμογή τρέχει μέσω τις δικής της εικονικής μηχανής στη δικιά της διεργασία και για αυτό το λόγο καμία εφαρμογή δεν έχει επαφή με την άλλη, ενώ εκτελούνται ταυτόχρονα. Η Dalvik δεν υποστηρίζει τον κώδικα bytecode, αντί αυτού οι κλάσεις της Java γίνονται compile σε αρχεία .dex ώστε να τρέξουν στην VM. Τα αρχεία dex ουσιαστικά αποτελούν συμπιεσμένα δεδομένα για εξοικονόμηση χώρου κατά την εκτέλεση (Εικόνα 26). [24]



Εικόνα 26 - Dalvik Virtual Machine

Το Android είναι από τη φύση του multitasking λειτουργικό σύστημα και για αυτό επιτρέπει στις εφαρμογές του να τρέχουν σε πολλά treads ταυτόχρονα και να απασχολούν πολλές διαδικασίες εάν αυτό είναι αναγκαίο. Για να γίνει αυτό εφικτό η μηχανή Dalvik είναι σχεδιασμένη για να έχει ελάχιστο αντίκτυπο στη χρήση της μνήμης. Χάρη στον λιτό της σχεδιασμό, το σύστημα είναι σε θέση να τρέχει πολλές εικονικές μηχανές ταυτόχρονα.

2.3.4. Πλαίσιο Εφαρμογής (Application Framework)

Το πλαίσιο εφαρμογής βρίσκεται στο τρίτο στρώμα της αρχιτεκτονικής του Android. Πρόκειται ουσιαστικά για μια ενσωματωμένη εργαλειοθήκη, που παρέχει ένα σύνολο υπηρεσιών για τις Android εφαρμογές. Όλες αυτές οι υπηρεσίες δίνουν τη δυνατότητα στους προγραμματιστές των εφαρμογών να αναπτύξουν καινοτόμες και πλούσιες σε υλικό, εφαρμογές. Οι προγραμματιστές έχουν στην διάθεση τους τη δυνατότητα ελέγχου του υλικού της συσκευής και μέσω αυτής μπορούν να αποκτήσουν πρόσβαση σε υπηρεσίες εντοπισμού, εκτέλεση διεργασιών παρασκηνίου, και πάρα πολλές ακόμη δυνατότητες. Ακόμα έχουν πρόσβαση σε όλα τα APIs μεταξύ αυτών και στα κύρια APIs που χρησιμοποιούν οι ενσωματωμένες εφαρμογές. Η δομή των εφαρμογών είναι τέτοια που ευνοείται η επαναχρησιμοποίηση δομικών συστατικών, και επίσης επιτρέπεται η χρήση των δυνατοτήτων τις μίας εφαρμογής από άλλες εφαρμογές, βέβαια κάτω από τις προδιαγραφές ασφάλειας του Android. Τα σημαντικότερα δομικά στοιχεία του πλαισίου εφαρμογών είναι: [23]

- **Σύστημα προβολών (View System):** αποτελεί ένα εκτενές σύνολο από αντικείμενα GUI τα οποία μπορούν να χρησιμοποιηθούν κατά το σχεδιασμό μιας εφαρμογής. Παραδείγματα προβολών είναι οι λίστες (listView), το πλέγμα (GridView), πεδία εισαγωγής κειμένου, κουμπιά, κλπ

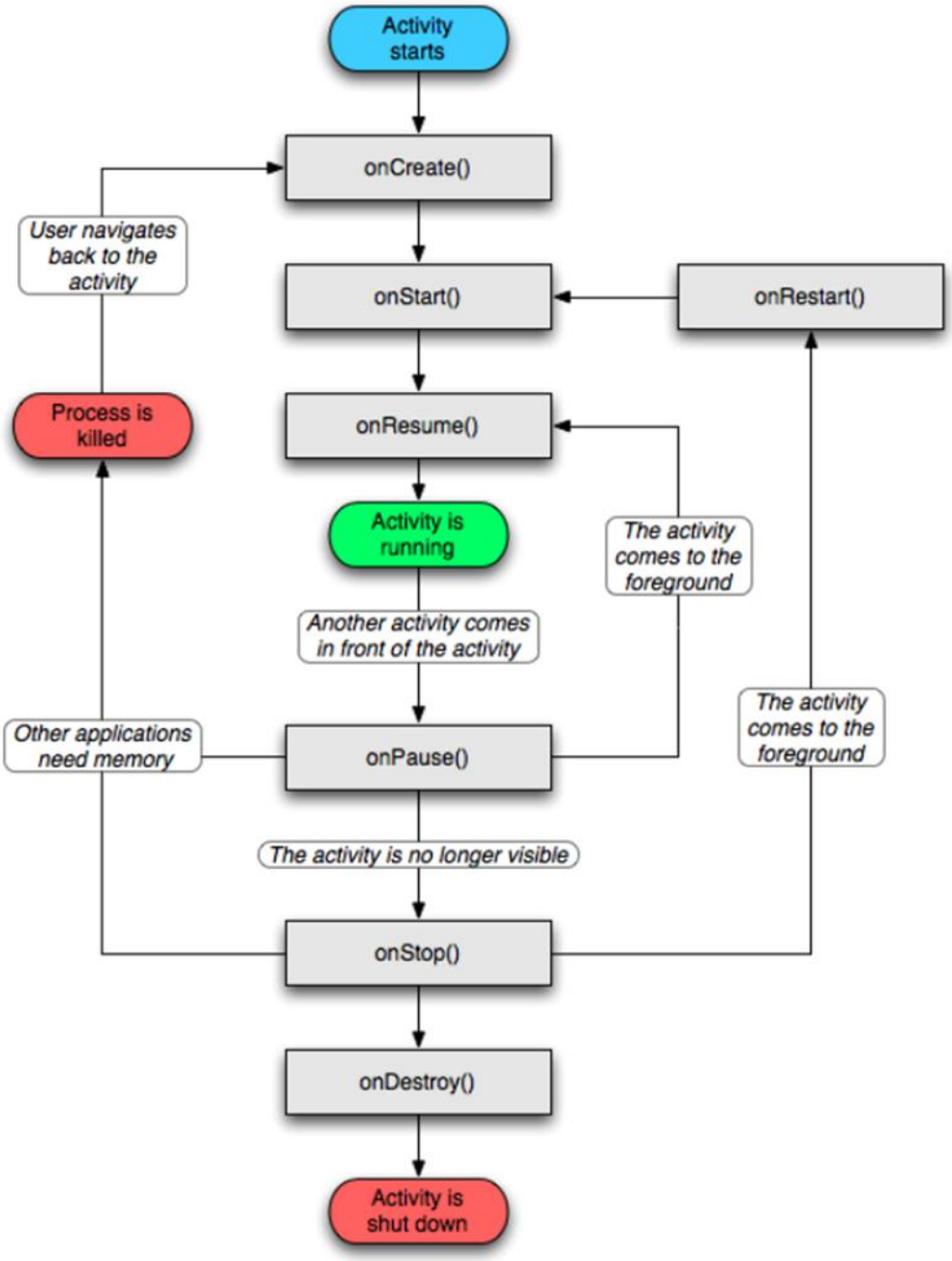
- **Πάροχος Περιεχομένου (Content Provider):** δίνει τη δυνατότητα στις εφαρμογές να μοιράζονται ή να ανταλλάσσουν δεδομένα μιας συγκεκριμένης μορφής η οποία ορίζεται από τον πάροχο. Παραδείγματα δεδομένων, είναι οι επαφές χρήστη και οι βάσεις δεδομένων των εφαρμογών.

- **Διαχειριστής Πόρων (Resource Manager):** παρέχει πρόσβαση σε υλικό το οποίο δεν είναι σε μορφή κώδικα όπως πχ, εικόνες, αρχεία xml, πίνακες χαρακτήρων, κλπ

- **Διαχειριστής Ειδοποιήσεων (Notification Manager):** δίνει στις εφαρμογές πρόσβαση στις υπηρεσίες ειδοποιήσεων χρήστη. Τέτοιες είναι οι ειδοποιήσεις στη notification bar, τα toast μηνύματα στο κάτω μέρος της οθόνης, η δόνηση του κινητού και η ενεργοποίηση της οθόνης, κλπ

- **Διαχειριστής Τοποθεσίας (Location Manager):** δίνει στις εφαρμογές τη δυνατότητα εντοπισμού της τοποθεσίας μη τη χρήση του GPS η των κεραιών των κυψελωτών δικτύων.

- **Διαχειριστής Δραστηριοτήτων (Activity Manager):** διαχειρίζεται τον κύκλο ζωής των δραστηριοτήτων και παρέχει δυνατότητα πλοήγησης από δραστηριότητα σε δραστηριότητα κρατώντας αποθηκευμένη στη μνήμη τη σειρά εκτέλεσης αυτών. Στο σχεδιάγραμμα (Εικόνα 27) φαίνεται λεπτομερώς ο κύκλος ζωής κάθε δραστηριότητας.



Εικόνα 27 - Κύκλος ζωής μιας Δραστηριότητας

2.4. Android File system

Ένας αποτελεσματικότερος τρόπος οργάνωσης των δεδομένων σε μια συσκευή γίνεται μέσο του συστήματος αρχείων (File System). Υπάρχουν διαφορετικοί τύποι συστήματος αρχείων για τους υπολογιστές και τις κινητές συσκευές. Η αποδοτικότητα του συστήματος αρχείων σε μια συσκευή μετράται από το πόσο γρήγορα μια εφαρμογή

μπορεί να διαβάσει, να γράψει αλλά και να ανακτήσει τα δεδομένα. Το Android βασίζεται στο σύστημα αρχείων του Linux και πολλά από αυτά χρησιμοποιούνται για την εκκίνηση και τη λειτουργία της συσκευής. Το Android χρησιμοποιεί EXT, FAT32 και τα YAFFS2 αρχεία για την εκκίνηση και την αποθήκευση δεδομένων. [25]

Τα FAT και FAT32, που είναι γνωστοί τύποι αφού χρησιμοποιούνται κυρίως από το λειτουργικό σύστημα Windows, υποστηρίζονται και από το Android κυρίως στην sd card. Παρόλο όμως που ο τύπος των αρχείων αυτών στερείται της ουσιαστικής ασφάλειας, συνεχίζει να χρησιμοποιείται ευρέως. Τα YAFFS2 (Yet Another Flash File System 2) είναι ένα σύστημα αρχείων σχεδιασμένο για τη μνήμη flash. Το πρόβλημα με τα YAFFS είναι ότι τα περισσότερα εργαλεία forensics που είναι διαθέσιμα στην αγορά, δεν είναι συμβατά με αυτό το σύστημα αρχείων. Όμως επισημαίνει ότι ορισμένες συσκευές που χρησιμοποιούν το λειτουργικό Android υποστηρίζουν ήδη τα EXT4. Αυτό οφείλεται πλέον στην ύπαρξη συσκευών που χρησιμοποιούν επεξεργαστές με διπλό πυρήνα , τη δυνατότητα πολυεπεξεργασίας και στη χρήση εξωτερικών καρτών μνήμης.

Η μνήμη για το σύστημα αρχείων YAFFS απευθύνεται σε μπλοκς (blocks) και κάθε μπλοκ περιέχει έναν καθορισμένο αριθμό σελίδων (pages) που ονομάζονται κομμάτια (chunks). Για τις Android συσκευές, κάθε μπλοκ έχει 64 κομμάτια και κάθε κομμάτι είναι 2KB. Επίσης, το μέγεθος του κάθε μπλοκ είναι 128KB. Το μπλοκ περιλαμβάνει επίσης μια 64 byte Out of Band (OOB) περιοχή που είναι η πρόσθετη έκταση για την αποθήκευση διαφόρων ετικετών (tags) και μεταδεδομένων (metadata). Όταν ένα μπλοκ διατίθεται για γράψιμο αποδίδεται μία αλληλουχία η οποία ξεκινά από το 1 και αυξάνεται με κάθε νέο μπλοκ. Οι δομές δεδομένων που αποθηκεύονται σε YAFFS2 αναφέρονται ως αντικείμενα. Αυτά τα αντικείμενα μπορεί να είναι αρχεία, κατάλογοι, συμβολικές συνδέσεις. Κάθε κομμάτι αποθηκεύει είτε σαν yaffs_ObjectHeader (object metadata) είτε σαν δεδομένα για το αντικείμενο. Η yaffs_ObjectHeader περιέχει διάφορες πληροφορίες όπως τον τύπο αντικειμένου, το μητρικό αντικείμενο , ένα checksum του ονόματος για να επιταχύνει την αναζήτηση, το όνομα του αντικειμένου, τα δικαιώματα και την ιδιοκτησία, πληροφορίες σχετικά με την MAC και το μέγεθος του αντικειμένου, αν αυτό είναι ένα αρχείο. Στην 64 byte Out-of-band περιοχή, τα YAFFS2 αποθηκεύουν κρίσιμες πληροφορίες για το κομμάτι, αλλά και μοιράζεται το χώρο με τις συσκευές Memory Technology Devices (MTD) του υποσυστήματος. Οι κρίσιμες YAFFS2 ετικέτες (tags) είναι:

- 1byte: Block State (0xFF αν είναι καλό μπλοκ, οποιαδήποτε άλλη τιμή για ένα κατεστραμμένο μπλοκ)
- 4byte: 32 bit chunk ID (το 0 υποδηλώνει κομμάτι που αποθηκεύει yaffs_ObjectHeader, αλλιώς τα δεδομένα)
- bytes: 32 bit object ID

- 2 bytes: Αριθμός μπλοκ δεδομένων σε αυτό το κομμάτι
- 4bytes: Αύξων αριθμός του παρόντος μπλοκ
- bytes: ECC tags (σε Android, χειρίζονται από τις MTD)
- 12 bytes: ECC για τα δεδομένα (σε Android, χειρίζονται από τις MTD)

Αν ένα αντικείμενο έχει αλλάξει, μια νέα yaffs_ObjectHeader θα δημιουργηθεί στη flash αφού η NAND μνήμη μπορεί να εγγραφεί μόνο μια φορά πριν από τη διαγραφή. Τα παλιά δεδομένα και οι κεφαλίδες εξακολουθούν να υπάρχουν, αλλά αγνοούνται στην δομή των αρχείων εξετάζοντας τις τιμές του αύξοντα αριθμό. Ομοίως, όταν ένα αρχείο διαγράφεται στο YAFFS, αυτό μετακινείται σε έναν ειδικό, κρυφό μη συνδεδεμένο (unlinked) χώρο ή αλλιώς διαγραμμένο κατάλογο. Το αρχείο παραμένει σε αυτόν τον κατάλογο μέχρις ότου όλα τα κομμάτια (chunks) στο αρχείο διαγράφονται. Για να επιτευχθεί αυτό, το σύστημα αρχείων καταγράφει τον αριθμό των κομματιών του συστήματος για το αρχείο και όταν φτάσει στο 0, τα απομεινάρια του αρχείου δεν υπάρχουν πια. Σε εκείνο το σημείο, δεν θα είναι πλέον δυνατό να εντοπιστεί το αντικείμενο στον " μη συνδεδεμένο " κατάλογο.

Επιπλέον όσον αναφορά το partitioning στις συσκευές Android, είναι διαφορετικό και εξαρτάται από τον εκάστοτε κατασκευαστή. Μια τυπική μορφή του διαχωρισμού στα επιμέρους partitions φαίνεται στην Εικόνα 28. Υπάρχουν συνήθως έξι partition στις Android συσκευές, το boot, cache, data, misc, recovery και το system.

[7.875122] 8 cmdlinepart partitions found on MTD device omap2-nand.0

[7.881866] Creating 8 MTD partitions on "omap2-nand.0":

[7.887451] 0x0000001c0000-0x000000340000 : "pds"

[7.894714] 0x000000620000-0x000000680000 : "misc"

[7.900939] 0x000000680000-0x000000a00000 : "boot"

[7.907989] 0x000000a00000-0x000000e80000 : "recovery"

[7.915740] 0x000000e80000-0x000009ae0000 : "system"

[7.956878] 0x000009ae0000-0x00000f780000 : "cache"

[7.986053] 0x00000f780000-0x00001fd40000 : "userdata"

[8.057373] 0x00001fd40000-0x00001ff40000 : "kpanic"

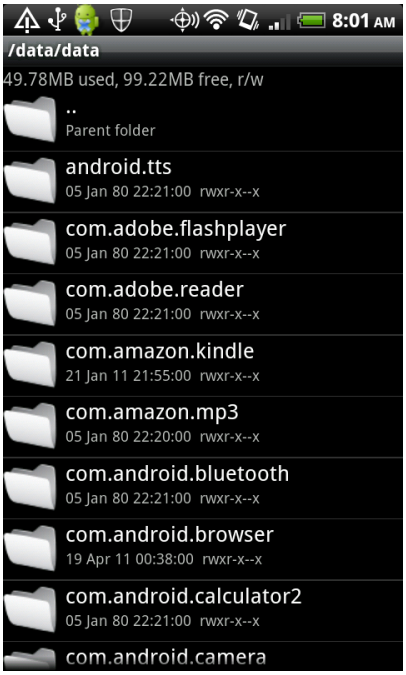
Εικόνα 28 - Τα Partition του Android

2.5. Αποθήκευσης Δεδομένων

Οι συσκευές Android αποθηκεύουν περισσότερα δεδομένα σε σύγκριση με οποιοδήποτε τυπική φορητή συσκευή. Το Android αποθηκεύει δεδομένα με πέντε διαφορετικές μεθόδους. Ιατροδικαστική εξεταστές αναζητά τα δεδομένα σε τέσσερις από τις πέντε μορφές. Οι πέντε μέθοδοι αποθήκευσης δεδομένων είναι : οι κοινές προτιμήσεις (shared preferences), η εσωτερική αποθήκη (internal storage), η εξωτερική αποθήκη (external storage), οι SQL lite δομές δεδομένων και το δικτύου (network).

Τα shared preferences επιτρέπουν σε έναν προγραμματιστή την αποθήκευση των ζευγαριών κλειδιού-τιμής των πρωταρχικών τύπων δεδομένων σε μια ελαφριά μορφή XML. Τα κοινόχρηστα αρχεία προτιμήσεων αποθηκεύονται στον κατάλογο των δεδομένων μιας εφαρμογής, τον shared_pref φάκελο. [25]

Οι συσκευές με Android αποθηκεύουν πολλά από τα δεδομένα στην εσωτερική μνήμη, όπως η NAND flash. Τα αρχεία των εφαρμογών αποθηκεύονται στον / datadata φάκελο (Εικόνα 29). Αυτός ο φάκελος είναι ορατός μόνο εάν κάποιος έχει αποκτήσει πρόσβαση με root (διαχειριστής) δικαιώματα. Η προεπιλεγμένη λειτουργία του Android είναι η αποθήκευση των δεδομένων των εφαρμογών στην εσωτερική μνήμη, χωρίς δικαίωμα πρόσβασης η μία στα δεδομένα της άλλης.



Εικόνα 29 - Φάκελος /datadata με τα αρχεία των Εφαρμογών

Κάθε συμβατή συσκευή με το Android υποστηρίζει μια κοινό εξωτερικό χώρο, που ο χρήστης μπορεί να χρησιμοποιήσει για να αποθηκεύσει τα αρχεία του. Τέτοιος χώρος μπορεί να είναι ένα αφαιρούμενο μέσο αποθήκευσης (όπως μια κάρτα SD) ή ένα εσωτερικό (μη αποσπώμενο) μέρος της συσκευής. Υπάρχουν όμως και περιπτώσεις όπου ένα Partition της εσωτερικής μνήμης που χρησιμοποιείται σαν εξωτερικός χώρος. Γενικά, τα αρχεία που αποθηκεύονται στην εξωτερική μνήμη είναι world-readable και μπορούν να τροποποιηθούν εύκολα από τον χρήστη.

Ως εξωτερικό μέσο αποθήκευσης συναντάται συνήθως οι sd cards, οι οποίες χρησιμοποιούν κυρίως FAT32. Όπως αναφέρθηκε και σε προηγούμενη ενότητα, αν και τα FAT32 φέρουν ιδιαίτερης προτίμησης ευρέως, δεν διαθέτουν κανένα μηχανισμό ασφαλείας σε σχέση με τους άλλους τύπους όπως inext3, ext4 και τα yaffs2.

Οι SQLite είναι μια δημοφιλής μορφή βάσης δεδομένων που εμφανίζεται σε πολλά κινητά συστήματα. Οι SQLite είναι πολύ ελαφρές και ευέλικτες παρέχοντας υψηλή ποιότητα καθώς επίσης και πολύ καλές ταχύτητες σε σύγκριση με άλλες μορφές βάσεων. Τα αρχεία SQLite συνήθως αποθηκεύονται στην εσωτερική αποθήκη στο / data / data / <packagename> / database. Τέλος ,όσον αναφορά το Δίκτυο, μπορεί να χρησιμοποιηθεί για την αποθήκευση και ανάκτηση δεδομένων .

2.6. Εφαρμογές

Το Android είναι εφοδιασμένο με ένα σύνολο εφαρμογών (applications) που περιλαμβάνει e- mail client, πρόγραμμα για αποστολή και λήψη SMS, ημερολόγιο,

χάρτες, περιηγητή διαδικτύου, κατάλογο επαφών, κλπ. Όλες οι εφαρμογές είναι γραμμένες σε Java. Η εκτέλεση των εφαρμογών είναι ένας σημαντικός στόχος των λειτουργικών συστημάτων και το Android παρέχει διάφορους τρόπους σε διαφορετικά επίπεδα για να συνθέσει, να εκτελέσει και να διαχειριστεί τις εφαρμογές. Για το σκοπό αυτό το Android διαφοροποιεί σαφώς τις ένοιες terms application, process, task και thread των εφαρμογών. Αυτή η ενότητα εξηγεί κάθε όρο αυτοτελώς, καθώς και τον συσχετισμό μεταξύ αυτών. [23]

2.6.1. Διαδικασίες και Threads

Πέντε τύποι Διαδικασία (process) διακρίνονται στο Android με σκοπό τον έλεγχο της συμπεριφοράς του συστήματος αλλά και των προγράμματα που εκτελούνται σε αυτό. Οι διάφοροι τύποι έχουν διαφορετικά επίπεδα σημασίας που είναι αυστηρά διατεταγμένα. Η προκύπτουσα ιεραρχία για τις κατηγορίες των διαδικασιών είναι (κατά υψίστης σημασία) : [23]

- **Foreground:** Μια διαδικασία που εκτελεί μια δραστηριότητα, μια υπηρεσία που παρέχει την δραστηριότητα, η εκκίνησης ή διακοπή της Υπηρεσίας ή η άμεση λήψη ενός BroadcastReceiver.

- **Visible:** Όταν μια διαδικασία έχει διακοπεί, αλλά εξακολουθεί να είναι ορατή δραστηριότητα ή υπηρεσία, δεσμεύεται σαν μια ορατή δραστηριότητα και δεν υπάρχει κανένα στοιχείο για αυτήν στο προσκήνιο (foreground), χαρακτηρίζεται ως ορατή διαδικασία.

- **Service:** Μια διαδικασία που εκτελεί μια υπηρεσία που ήδη έχει ξεκινήσει

- **Background:** Μια δραστηριότητα που δεν είναι πλέον ορατή καταχωρείται σαν μια διαδικασία στο παρασκήνιο (Background).

- **Empty:** Οι διαδικασίες αυτές δεν περιέχουν ενεργά στοιχεία μιας εφαρμογής και υπάρχει μόνο για σκοπούς προσωρινής αποθήκευσης.

Αν το σύστημα λειτουργεί με λίγη μνήμη διαθέσιμη, η σπουδαιότητα μιας διαδικασίας είναι εκείνη που θα καθορίσει την απόφαση του συστήματος σχετικά με το ποια διαδικασία θα σταματήσει οριστικά ώστε να ελευθερωθεί μνήμη. Ως εκ τούτου πρώτες πιθανότατα θα σταματήσουν οι κενές διαδικασίες ακολουθούμενες από τις διαδικασίες που βρίσκονται στο παρασκήνιο και ούτω καθεξής. Συνήθως είναι μόνο οι κενές διαδικασίες και αυτές του παρασκηνίου τερματίζονται έτσι ώστε η εμπειρία του χρήστη να παραμένει ανεπηρέαστη. Το σύστημα έχει σχεδιαστεί για να αφήσει τα πάντα άθικτα, όσο αυτό είναι δυνατό, σε οτιδήποτε σχετίζεται με ορατά στοιχεία όπως μια δραστηριότητα (Activity).

Οι διαδικασίες μπορούν να περιέχουν πολλαπλά threads, όπως είναι σύνηθες στα Linux συστήματα. Οι περισσότερες Android εφαρμογές αποτελούνται από πολλαπλά threads που διαχωρίζουν το περιβάλλον χρήστη (UI) από την είσοδο χειρισμό και I/O λειτουργίες καθώς επίσης και λειτουργίες με μεγάλες υπολογισμούς, εξ ου και η υποκείμενη διαδικασίες είναι multi-threaded. Τα threads που χρησιμοποιούνται σε επίπεδο εφαρμογής είναι τυποποιημένα Java threads που τρέχουν στην Dalvik VM .

2.6.2.Εφαρμογές και Εργασίες

Οι Android εφαρμογές εκτελούνται από τις διαδικασίες και τα threads που περιλαμβάνονται σε αυτές. Οι Εργασίες (Tasks) και η εφαρμογή συνδέονται μεταξύ τους στενά, δεδομένου ότι μια Εργασία μπορεί να θεωρηθεί ως μια εφαρμογή από τον χρήστη. Στην πραγματικότητα, οι Εργασίες είναι μια σειρά από δραστηριότητες ενδεχομένως πολλαπλών εφαρμογών. Οι Εργασίες ουσιαστικά είναι μια λογική αλληλουχία ενεργειών του χρήστη, π.χ. ο χρήστης ανοίγει μια εφαρμογή ηλεκτρονικού ταχυδρομείου με την οποία ανοίγει ένα συγκεκριμένο μήνυμα, το οποίο περιλαμβάνει έναν σύνδεσμο που ανοίγει μέσω ενός προγράμματος περιήγησης. Σε αυτό το σενάριο, η εργασία θα περιλαμβάνει δύο εφαρμογές (ταχυδρομείο και το πρόγραμμα περιήγησης) αφού υπάρχουν επίσης και δύο δραστηριότητες, της εφαρμογής mail και αυτής του πρόγραμμα περιήγησης. Ένα πλεονέκτημα των Εργασιών είναι η δυνατότητα που δίνουν στο χρήστη να πάει προς τα πίσω βήμα προς βήμα.

2.6.3. Εσωτερική Δομή των Εφαρμογών

Η δομή μιας εφαρμογής του Android βασίζεται σε τέσσερα διαφορετικά στοιχεία, τα οποία είναι: η Δραστηριότητα (Activity), η Υπηρεσία (Service), ο Δέκτης Μετάδοσης (BroadcastReceiver) και ο Πάροχος Περιεχόμενου **(**ContentProvider). Μια εφαρμογή δεν σημαίνει απαραίτητα ότι συνίσταται και από τα τέσσερα αυτά στοιχεία, αλλά για να παρουσιάσει μια γραφική απεικόνιση στον χρήστη θα πρέπει να υπάρχει τουλάχιστον μια Δραστηριότητα. [23]

Οι εφαρμογές μπορούν να ξεκινήσουν άλλες εφαρμογές ή συγκεκριμένα στοιχεία άλλων εφαρμογών με την αποστολή μιας πρόθεσης (Intent). Οι προθέσεις περιέχουν, μεταξύ άλλων, το όνομα της δράσης που πρέπει εκτελεστεί. Ο Διαχειριστής των προθέσεων (IntentManager) επιλύει τις εισερχόμενες προθέσεις και ξεκινάει τη σωστή εφαρμογή ή το αντίστοιχο στοιχείο της. Επιπλέον, η λήψη μιας πρόθεση μπορεί να φιλτράρεται από μια εφαρμογή.

Οι Υπηρεσίες και ο Δέκτης Μετάδοσης επιτρέπουν στις εφαρμογές να εκτελούν τις λειτουργίες τους στο παρασκήνιο και παρέχουν επιπλέον λειτουργικότητα σε άλλα στοιχεία. Από την άλλη πλευρά, ο Δέκτης Μετάδοσης μπορεί να προκληθεί από κάποιο

γεγονός και να τρέξει μόνο για λίγο, ενώ μια υπηρεσία μπορεί να τρέξει για ένα μεγάλο χρονικό διάστημα.

Ο πηγαίος κώδικας των στοιχείων της εφαρμογής καθώς και οι επιπλέον πόροι, όπως εικόνες, βιβλιοθήκες και τα άλλα απαραίτητα στοιχεία είναι τοποθετημένα σε ένα ενιαίο αρχείο .apk που αποτελεί το εκτελέσιμο της εφαρμογή Android.

2.6.3.1. AndroidManifest.xml

Όλες οι εφαρμογές του Android που τρέχουν στην Dalvik πρέπει να διαθέτουν ένα XML έγγραφο στον βασικό κατάλογό τους που ονομάζεται AndroidManifest.xml. Αυτό το έγγραφο χρησιμοποιείται από διάφορες λειτουργίες του λειτουργικού συστήματος για να αποκτήσουν σημαντικές πληροφορίες σχετικά με την εφαρμογή. Στο AndroidManifest υπάρχουν 23 προκαθορισμένοι τύποι πληροφοριών και καθορίζουν μεταξύ άλλων, το όνομα της εφαρμογής, τα συστατικά της, τις άδειες που απαιτούνται, τις βιβλιοθήκες που χρειάζεται και τα φίλτρα για τις προθέσεις και τον Δέκτη Μετάδοσης. Κατά τη διάρκεια της κατασκευής μιας εφαρμογής, το αρχείο κατέχει τις πληροφορίες ελέγχου για την υποστήριξη των προγραμματιστών.

2.6.3.2. Δραστηριότητες

Μια δραστηριότητα είναι μια ενιαία οθόνη της εφαρμογής όπως ένα παράθυρο του browser ή μια σελίδα των ρυθμίσεων. Περιέχει τα οπτικά στοιχεία της, δηλαδή τα εμφανή δεδομένα (όπως μια εικόνα) ή οτιδήποτε βοηθάει την αλληλεπίδραση με το χρήστη (όπως ένα κουμπί). Κάθε εφαρμογή μπορεί να έχει πολλαπλές δραστηριότητες, γιατί η μετάβαση μεταξύ των διαφορετικών δραστηριοτήτων ξεκινούν μέσω των προθέσεων.

Όλες οι δραστηριότητες είναι υποκατηγορίες στο android.app.Activity και ο κύκλος ζωής τους ελέγχεται από τις μεθόδους onXYZ(). Αυτή η έννοια είναι αναγκαία για το λειτουργικό σύστημα του Android όσον αναφορά το χειρισμό του multitasking και βοηθά την αντιμετώπιση συνθηκών χαμηλής μνήμης. Οι κύριες συναρτήσεις του είναι: η onCreate(), onDestroy(), onResume(), onPause() και η onRestart().

2.6.3.3. Πάροχος Περιεχόμενου

Η αποθήκευση και ανάκτηση των δεδομένων στις Android εφαρμογές γίνεται μέσω των παροχέων περιεχομένου. Αυτοί οι πάροχοι μπορούν επίσης να χρησιμοποιηθούν για την ανταλλαγή δεδομένων μεταξύ πολλαπλών εφαρμογών, δεδομένου του γεγονότος ότι η σχετική εφαρμογή κατέχει τα σωστά δικαιώματα πρόσβασης στα δεδομένα. Το Android διαθέτει προεπιλεγμένους παρόχους για παράδειγμα εικόνων, βίντεο, επαφών

και τις αντίστοιχες ρυθμίσεις οι οποίες μπορεί περιλαμβάνονται στο πακέτο android.provider.

Μια εφαρμογή υποβάλλει ερώτημα σε μια υπηρεσία επίλυσης περιεχομένου (ContentResolver) που επιστρέφει τον κατάλληλο παροχέα περιεχομένου. Όλοι οι πάροχοι έχουν πρόσβαση σε στοιχεία, όπως βάσεις δεδομένων με ένα ομοιόμορφο αναγνωριστικό πόρου (URI) για τον προσδιορισμό του φορέα παροχής, ένα όνομα πεδίου και τον τύπο δεδομένων του πεδίου αυτού. Οι εφαρμογές έχουν πρόσβαση στους πάροχος περιεχομένου μέσω μιας υπηρεσία επίλυσης περιεχομένου και ποτέ άμεσα στα δεδομένα. Αν η εφαρμογή θέλει να αποθηκεύσει δεδομένα που δεν πρέπει να μοιραστεί με άλλες, μπορεί να χρησιμοποιήσει μια τοπικό SQLite βάση δεδομένων.

2.6.3.4. Δραστηριότητες στο Παρασκήνιο

Οι Εφαρμογές μπορεί να χρειαστεί να εκτελέσουν κάποιες λειτουργίες υποστήριξης στο παρασκήνιο με ή χωρίς γραφικό περιβάλλον. Το Android παρέχει τον Δέκτης Μετάδοσης και τις υπηρεσίες για τους σκοπούς αυτούς. Αν πρέπει να πραγματοποιηθεί μόνο μια μικρή και σύντομη λειτουργία, προτιμάται ο Δέκτης Μετάδοσης ενώ για μεγάλες εργασίες προτιμάται η χρήση της Υπηρεσία.

Και στις δύο περιπτώσεις όμως δεν συνεπάγεται κατ 'ανάγκην ότι το στοιχείο του παρασκήνιου εκτελείται σαν ένα thread ή ακόμα και στη δική του διαδικασία, αφού το Android δεν επιτρέπει αυτό του είδος την συμπεριφορά. Για να μην παγώσει μια εφαρμογή που εκτελείται, η υπηρεσία ή ο Δέκτης Μετάδοσης συνήθως εκτελείται σε δικό του thread, αλλιώς το Android τείνει να σκοτώσει μια τέτοια μια εφαρμογή, η οποία φαίνεται ότι δεν ανταποκρίνεται. [23]

Ο Δέκτης Μετάδοσης ενεργοποιείται μέσω της μεθόδου η OnReceive () και μπορεί να ακυρωθεί από το αποτέλεσμα της μεθόδου αυτής. Αυτό καθιστά αναγκαία την χρήση μόνον σύγχρονων μεθόδων σε ένα δέκτη. Μια εκπομπή είναι συνήθως μη διατεταγμένη και αποστέλλεται σε όλους τους δέκτες που ταιριάζουν κατά την ίδια χρονική στιγμή. Αλλά μπορεί και να διαταχθεί όπου στην περίπτωση αυτή, το Android εκπέμπει σε ένα κάθε φορά δέκτη. Αυτός ο δέκτης εκτελείται, και μπορεί να διαβιβάσει ένα αποτέλεσμα στον επόμενη δέκτη ή μπορεί ακόμη και ματαιώσετε το σύνολο της εκπομπής.

Η υπηρεσία επιτρέπει σε μια εφαρμογή να εκτελεί μεγάλες εργασίες που εκτελούνται στο παρασκήνιο και να παρέχουν μέρος των λειτουργιών της σε άλλες εφαρμογές στο συστήματος. Μια υπηρεσία μπορεί να χρησιμοποιηθεί με δύο τρόπους, είτε είναι ξεκινήσει με μία εντολή ή να ξεκινήσει και να ελέγχεται από μια εισερχόμενη σύνδεση που κάνει χρήση της κλήσης απομακρυσμένης Διεργασίας (Remote Procedure Calls).

Κεφάλαιο 3° Ασφάλεια και Απειλές στο Android

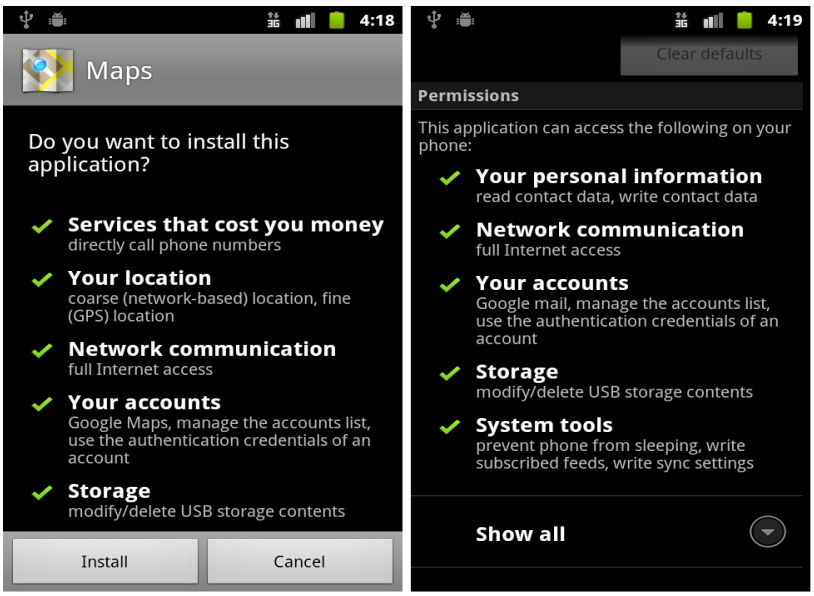
3.1. Ασφάλεια στο Android

Το σύστημα Android χρησιμοποιεί διάφορες μεθόδους για να παρέχει ασφάλεια στις συσκευές των χρηστών. Παρακάτω θα περιγράψουμε τα χαρακτηριστικά ασφαλείας που επηρεάζουν άμεσα τις εφαρμογές, τα οποία έχουν σημασία για τις κακόβουλες εφαρμογές , αφού θα πρέπει να προσπαθήσει να νικήσουν ή να παρακάμψουν.

3.1.1. Δικαιώματα

Το Android περιορίζει τις δυνατότητες των εφαρμογών που είναι εγκατεστημένες στη συσκευή ζητώντας ρητά από το χρήστη να επιτρέψει στην εφαρμογή να αποκτήσει πρόσβαση σε διάφορα μέρη του λειτουργικού συστήματος ή σε κάποια χαρακτηριστικά της συσκευής. Προκειμένου μια εφαρμογή να είναι σε θέση να χρησιμοποιήσει μία από αυτές τις δυνατότητες, θα πρέπει να της έχει χορηγηθεί η σχετική άδεια από το χρήστη κατά τη διάρκεια της εγκατάστασης, όπως φαίνεται στην εικόνα30. Το σύστημα έγκρισης είναι ολοκληρωμένο και παρέχει ένα καλό πλαίσιο για τον προσδιορισμό του είδους των πόρων που θα έχει πρόσβαση σε μόλις η εφαρμογή εγκατασταθεί σε μια συσκευή. [26]

Οι άδειες αποθηκεύονται σε ένα αρχείο που ονομάζεται manifest.xml που υπάρχει μέσα στα αρχεία της εφαρμογής, και δεν μπορεί να αλλάξει μετά την εγκατάστασή της. Εξαίρεση από τον κανόνα αυτό γίνεται όταν πραγματοποιείται κάποια ενημέρωση των εφαρμογών, αλλά ο χρήστης εξακολουθεί να υποχρεούται να εγκρίνει οποιαδήποτε νέα δικαιώματα, σε μια παρόμοια διαδικασία, όπως κατά την εγκατάσταση για πρώτη φορά.



Εικόνα 30 - Δικαιώματα ποτ απαιτούν τη συναίνεση του χρήστη

Η εκχώρηση των δικαιωμάτων έχει το χαρακτήρα όλα ή τίποτα. Αυτό σημαίνει ότι όταν ένας χρήστης εγκαθιστά μια εφαρμογή, θα πρέπει είτε να επιτρέψει στην εφαρμογή όλα τα δικαιώματα που αυτή απαιτεί είτε να απέχει από την εγκατάστασή της. Η λύση αυτή απομακρύνει την ανησυχία από τους κατασκευαστές για τη σωστή συμπεριφορά της εφαρμογής όταν θα προσπαθούσε να αποκτήσετε πρόσβαση σε χαρακτηριστικό που χρειαζόταν και δεν έχει την σχετική άδεια.

Τα δικαιώματα χωρίζονται σε τέσσερα επίπεδα προστασίας , η κανονική, επικίνδυνη, υπογραφή και signatureOrSystem. Τα επίπεδα αυτά έχουν χωριστεί με βάση την ζημιά ή το ενδεχόμενο κόστος που μπορεί να προκληθεί στον χρήστη, με τα περισσότερα από τα δικαιώματα να είναι χαρακτηρισμένα ως επικίνδυνα. Δικαιώματα που ανήκουν στο κανονικό (ονομάζεται επίσης ασφαλή) επίπεδο προστασίας, όπως η δόνηση και ο Ορισμός ταπετσαρίας, είναι δικαιώματα που θεωρείται ότι δεν υπάρχει κίνδυνος που να συνδέεται με αυτά. Το πρόγραμμα εγκατάστασης της Android δεν θα ζητήσει από τους χρήστες καμία άδεια για αυτά τα δικαιώματα. Ωστόσο το επικίνδυνο επίπεδο προστασίας, θα προκαλέσει προειδοποιήσεις που εμφανίζονται στο χρήστη πριν από την εγκατάσταση, και απαιτεί έγκριση του ώστε να χορηγηθεί άδεια στα συγκεκριμένα δικαιώματα.

Η υπογραφή και το επίπεδο προστασίας signatureOrSystem παρέχουν προστασία για τα πιο επικίνδυνων δικαιώματα. Τα δικαιώματα που περιλαμβάνονται στο επίπεδο της Υπογραφής, είναι διαθέσιμα μόνο σε μια εφαρμογή που έχει υπογραφεί με το ίδιο πιστοποιητικό, όπως το πιστοποιητικό που χρησιμοποιήθηκε για να υπογράψουν την εφαρμογή δηλώνοντας το συγκεκριμένο δικαίωμα. Ομοίως, το επίπεδο signatureOrSystem απαιτεί η εφαρμογή να είναι είτε μια εφαρμογή του συστήματος, δηλαδή ένα μέρος της εικόνας του συστήματος, είτε να υπογράφεται από το ίδιο πιστοποιητικό με εκείνο που χρησιμοποιήθηκε για την υπογραφή της έκδοση του Android που είναι εγκατεστημένο στη συσκευή. [26]

Ωστόσο, υπάρχουν ορισμένα προβλήματα με το σύστημα χορήγησης άδειας, αλλά αυτά σχετίζονται περισσότερο με την εφαρμογή των δικαιωμάτων και όχι με τα αυτά καθαυτά . Ουσιαστικά, το σύστημα άδειας μπορεί να παρακαμφθεί, όπως αποδεικνύεται από την Linberry et al. στην ομιλία τους στο Blackhat, όπου αποκάλυψε ότι το δικαίωμα *RECEIVE_BOOT_COMPLETED* δεν ελέγχεται στην πραγματικότητα. Αυτό σημαίνει ότι κάθε εφαρμογή θα μπορούσε να ρυθμιστεί να αρχίζει όταν το τηλέφωνο είναι ενεργοποιημένο και το σύστημα δεν θα μπορούσε πραγματικά να εξακριβώσει κατά πόσον η εφαρμογή είχε ζητήσει το συγκεκριμένο δικαίωμα. Αυτή τη στιγμή είναι άγνωστο αν αυτό επηρεάζει οποιαδήποτε άλλα δικαιώματα. Επιπλέον, σε ορισμένες περιπτώσεις, μια άσχετο δικαίωμα μπορεί να δώσει πρόσβαση ισοδύναμη με εκείνη ενός άλλου δικαιώματος.

3.1.2. Το Sandbox

Στο σύστημα Android κάθε εφαρμογή λειτουργεί αυτόνομα και είναι εφοδιασμένη με τη δική της UID. Η UID έρχεται να διαχωρίσει κάθε εφαρμογή στο δικό της sandbox, εμποδίζοντας την άμεση επικοινωνία μεταξύ τους. Κάθε εφαρμογή λοιπόν, τρέχει στο δικό της ιδιωτικό περιβάλλον και δεν είναι σε θέση να αποκτήσετε πρόσβαση σε άλλες εφαρμογές καθώς επίσης ούτε αυτή είναι προσβάσιμη από άλλες εφαρμογές άμεσα. Αυτό είναι χαρακτηριστικό ασφαλείας που προέρχονται από το περιβάλλον UNIX πάνω στο οποίο είναι βασισμένο το Android .

Όπως όμως διαπιστώνουμε από την εκχώρηση των δικαιωμάτων παραπάνω, ο κατασκευαστής της εφαρμογής μπορεί να ανοίξει ουσιαστικά την πύλη προς το sandbox, επιτρέποντας σε άλλες εφαρμογές να έχουν πρόσβαση στα χαρακτηριστικά της δηλώνοντας τα δικά τους δικαιώματα. Αυτό καθιστά δυνατή την αλληλεπίδραση με άλλες εφαρμογές, παρά την ύπαρξη του sandbox. Επιπλέον ο κατασκευαστής της εφαρμογής μπορεί να ζητήσει μια κοινόχρηστη UID. Με τη χρήση κοινόχρηστων UID, πολλαπλές εφαρμογές που υπογράφονται από τον κατασκευαστή, μπορούν να μοιράζονται το ίδιο sandbox. Εφαρμογές όμως που χρησιμοποιούν αυτή τη μέθοδο θα έχουν πρόσβαση σε κάθε δικαιώματα που έχει εκχωρηθεί στις υπόλοιπες, πράγμα που σημαίνει ότι εάν μία εφαρμογή έχει άδεια για την πρόσβαση στο internet και μια άλλη έχει δικαίωμα αποστολής sms, τότε και οι δύο εφαρμογές θα έχουν πρόσβαση στο Διαδίκτυο και να στέλνουν SMS. Επιπλέον κάθε εφαρμογή μπορεί να έχει πρόσβαση στις πληροφορίες της άλλης. Μια τέτοια λοιπόν λειτουργία είναι αρκετά ευέλικτη αλλά συνάμα και ανησυχητική για το λειτουργικό σύστημα της Android. [26]

3.1.3. Υπογραφή Εφαρμογής

Η πλατφόρμα Android απαιτεί τους κατασκευαστές να υπογράψουν τις εφαρμογές τους, πριν τους δοθεί η δυνατότητα εγκατάστασης σε μια συσκευή, χρησιμοποιώντας ένα αυτο-υπογεγραμμένο πιστοποιητικό. Το πιστοποιητικό αυτό εξασφαλίζει ότι ένας κακόβουλος προγραμματιστής δεν είναι σε θέση να μιμηθεί έναν άλλο νόμιμο. Το πιστοποιητικό παρέχει επίσης ένα επίπεδο εμπιστοσύνης μεταξύ του κατασκευαστή και του λειτουργικού συστήματος, δεδομένου ότι η διαδικασία υπογραφής ειδοποιεί το σύστημα εάν η εφαρμογή έχει τροποποιηθεί μετά την υπογραφή του κατασκευαστή.

3.1.4. Εξ αποστάσεων διακοπή μιας εφαρμογής

Η εφαρμογή του Google Play έχει τη δυνατότητα να αφαιρέσει εξ αποστάσεως εφαρμογές από τις συσκευές των χρηστών, όταν αυτές παραβιάζουν τη συμφωνία διανομής και τις πολιτικές δημιουργίας των εφαρμογών. Στις περισσότερες περιπτώσεις, οι εφαρμογές που παραβιάζουν αυτές τις συμφωνίες είναι κακόβουλες, και αυτή η δυνατότητα χρησιμοποιείται για να αφαιρεθεί το κακόβουλο λογισμικό ,αφού

πρώτα οι συγκεκριμένες έχουν απομακρυνθεί από το market. Η απομακρυσμένο όμως διακόπτη, είναι χρήσιμη μόνο για τις εφαρμογές που εγκαθίστανται μέσω του Google Play market. Εφαρμογές που είναι εγκατεστημένες μέσα από ανεπίσημες πηγές, δεν επηρεάζονται από αυτό το χαρακτηριστικό.

3.1.5. Προστασία των αρχείων του συστήματος

Το Android προστατεύει τα αρχεία του πυρήνα του λειτουργικού συστήματος, αποθηκεύοντάς τα σε ένα partition του σκληρού δίσκου που είναι μόνο προς ανάγνωση. Επιπλέον το sandboxing χαρακτηριστικό που αναφέρθηκε ανωτέρω, αποτρέπει τις εφαρμογές που είναι εγκατεστημένες στη συσκευή, να έχουν πρόσβαση στα αρχεία των άλλων, εκτός εάν τα αρχεία είναι εκτεθειμένα εσκεμμένα ή όχι από τον προγραμματιστή.

3.1.6. Google Bouncer

Η Google για να απαντήσει στις επικρίσεις σχετικά με την ασφάλεια του Google Play market, εισήγαγε ένα επιπρόσθετο επίπεδο ασφάλειας, που ονομάζεται Bouncer. Το Bouncer ελέγχει τις νέες εφαρμογές όταν αυτές αναρτώνται στο market, για να εντοπίσει ενδεχόμενων κακόβουλων εφαρμογών. Ακόμα φτάνει στο σημείο να προσομοιώσει την εφαρμογή που τρέχει σε μια συσκευή Android για ελέγχει την πλήρη συμπεριφορά της. Αυτό όμως είναι μια αυτοματοποιημένη διαδικασία που χρησιμοποιεί λίστες με τα χαρακτηριστικά των γνωστών και εντοπισμένων malware προγραμμάτων, πράγμα που σημαίνει ότι κάθε νέο κακόβουλο λογισμικό δεν θα μπορεί να ανιχνεύεται άμεσα από τον Bouncer. Ως παράδειγμα, η Trend Micro βρήκε αρκετές κακόβουλες εφαρμογές στο Android Market. [26]

3.1.7. Εφαρμογές Anti-virus

Οι εφαρμογές Anti-virus, είναι εφαρμογές που δημιουργούνται από εταιρείες τρίτων και αποσκοπούν στην πρόληψη κατά των κακόβουλων εφαρμογών, αποτρέπωντας αυτές να εγκατασταθούν σε μια συσκευή. Υπάρχουν πολλές εφαρμογές anti-virus στην αγορά, συμπεριλαμβανομένων των εφαρμογών που δημιουργούνται από τους κορυφαίους της αγοράς όπως η F-Secure και η Norton.

Η αποτελεσματικότητα αυτών των εφαρμογών έχει συζητηθεί, αλλά είναι προφανές ότι όπως και με τα αντίστοιχα λογισμικά στους υπολογιστές, η επιπρόσθετη ασφάλεια που παρέχουν είναι απαραίτητη σήμερα. Συχνά παρέχουν και δευτερεύουσες λειτουργίες, όπως η δυνατότητα απομακρυσμένης εκκαθάρισης καθώς επίσης και της ικανότητας να εντοπίσει τη συσκευή σε περίπτωση απώλειας ή κλοπής.

3.2. Target Value

Ο επιτιθέμενος σε ένα σύστημα έχει πάντα στόχο κάτι που έχει αξία (target value). Οι ενέργειές του μπορεί να βλάψουν μια επιχείρηση ή ένα πρόσωπο αποφέροντας στον ίδιο κάποιο κέρδος. Στόχος του είναι να αποκτήσει πληροφορίες που είναι εμπιστευτικές ή να τις αλλοιώσει πλήττοντας την ακεραιότητά τους ή αφαιρώντας τις να δημιουργήσει ένα πρόβλημα διαθεσιμότητας στους νόμιμους κατόχους. Ο επιτιθέμενος στη συνέχεια μπορεί να πουλήσει, διαρρεύσει, αναδιανείμει, καταστρέψει ή και να απειλήσει για τις παράνομα αποκτηθείσες πληροφορίες που διαθέτει, προκαλώντας οικονομικές ζημιές στα θύματα ή κλοπή της ταυτότητά τους. Επίσης, όσο αφορά μια εταιρεία μπορεί να βλάψει τη φήμη της και σε ορισμένες περιπτώσεις αυτό μπορεί να είναι χειρότερο από την απώλεια δεδομένων. [27]

Ιδιαίτερη όμως σημασία για την καλύτερη κατανόηση των επιθέσεων, είναι η γνώση ποιών πληροφοριών μπορούν να υποκλέψουν οι επιτιθέμενοι και που αυτές αντίστοιχα αποθηκεύονται μέσα στη συσκευή. Οι πολύτιμες λοιπόν πληροφορίες χωρίζονται σε δύο κατηγορίες δεδομένων, σε κατάσταση ηρεμίας (data at rest) και δεδομένα σε κίνηση (data in transit). Δεδομένα σε κατάσταση ηρεμίας, είναι ένας όρος που χρησιμοποιείται για να περιγράψει τα δεδομένα που είναι αποθηκευμένα σε διατηρήσιμη μνήμη. Τα δεδομένα σε μεταφορά από την άλλη πλευρά είναι ένας όρος που χρησιμοποιείται για να περιγράψει τα στοιχεία που είναι σε κίνηση, μέσω Wi-Fi, ή άλλων δικτύων ή βρίσκονται στη RAM.

Συγκεντρωτικά, ο παρακάτω κατάλογος αποτελεί μια επισκόπηση της κατηγοριοποίησης των πολύτιμων πληροφοριών που βρίσκονται μέσα σε μία συσκευή. [27]

- **Data at rest**

- Ιστορικό Επικοινωνίας
  - SMS/MMS
  - Ιστορικό κλήσεων
  - voice mail
  - Προσωπικά ή εταιρικά e-mail και οι επισυνάψεις τους
  - Instant Messenger ή άλλη επικοινωνία με τους εργαζομένους
- Άλλα ιστορικά
  - Ιστορικό web

- Ιστορικό αναζήτησης στο google
- youtube
- Ιστορικό παιχνιδιών και interactions

- Διαπιστευτήρια
  - Ονόματα χρηστών , κωδικοί πρόσβασης και πληροφορίες domain
  - Wi-Fi σημεία πρόσβασης, οι κωδικοί πρόσβασης και σχετικές πληροφορίες
  - Financial apps
- Tracking
  - geo-location
- Αρχεία
  - Εικόνες και Video
  - Δεδομένα στο ημερολόγιο
  - Εταιρικά στοιχεία που αποθηκεύονται στις συσκευές για λόγους ευκολίας

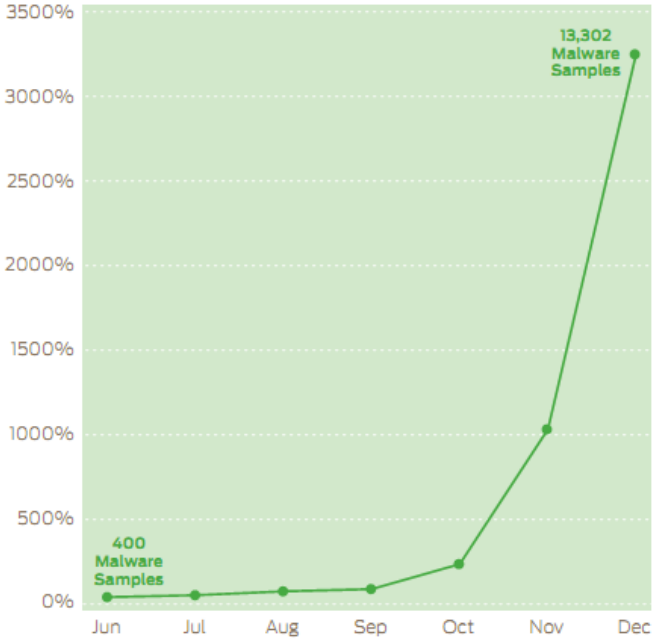
➢ **Data in transit**

- Κωδικοί Πρόσβασης
- Two-factor authentication
- επαναφορά του κωδικού πρόσβασης - απαντήσεις ασφαλείας
- Δεδομένα που εμφανίζονται αλλά δεν αποθηκεύονται μόνιμα ή σώζονται σε μη διατηρήσιμη μνήμη (πχ αριθμούς και υπόλοιπα τραπεζικών λογαριασμών)

3.3. Απειλές στις κινητές Συσκευές

Οι κινητές συσκευές και οι εφαρμογές που διαθέτουν έχουν αποκτήσει κρίσιμη σημασία τόσο στην προσωπική μας ζωή όσο και στην εργασία. Όχι μόνο είναι πανταχού παρών, αλλά επεκτείνονται σε ένα μεγάλο εύρος εφαρμογών από την ψυχαγωγία και τις διάφορες τραπεζικές συναλλαγές έως σε κρίσιμες επιχειρηματικές εφαρμογές. Το 2012, η παγκόσμιες πωλήσεις σε κινητά τηλέφωνα ανήλθαν στα 1.6 δισ. ευρώ και των Tablet Pc έφθασαν στα 660.9 εκ. ευρώ.

Ο τεράστιος όγκος των φορητών συσκευών που χρησιμοποιούνται σήμερα έχει δημιουργήσει ένα εντυπωσιακό φάσμα δυνατοτήτων για τους χρήστες δίνοντάς τους τη δυνατότητα να αλληλεπιδρούν και να διαχειρίζονται τις εργασίες τους και τα προσωπικά τους δεδομένα, ενώ κινούνται. Ωστόσο, αυτές οι ίδιες ευκαιρίες άνοιξαν επίσης τον δρόμο για τους hackers.



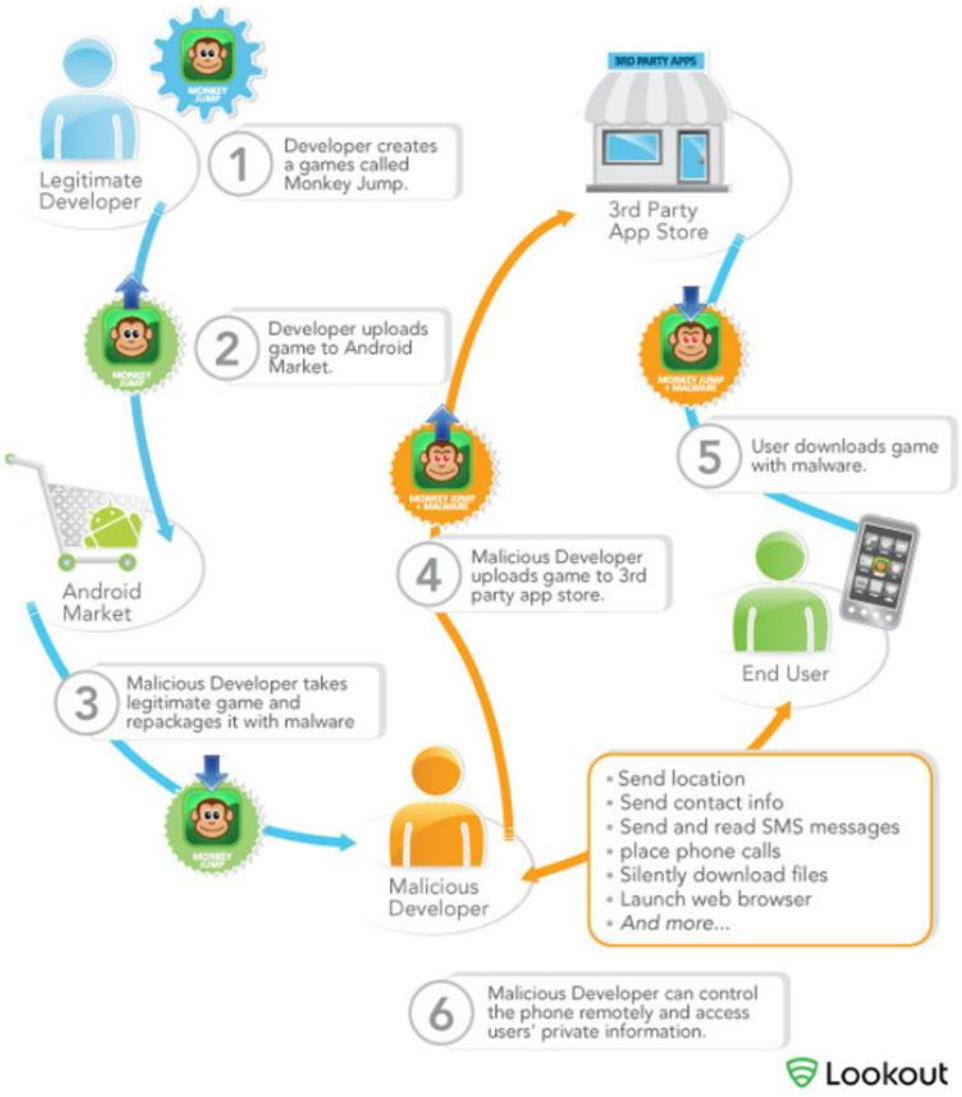
Εικόνα 31 - Αύξηση των Malware εφαρμογών

Το 2011, η Juniper Networks παρατήρησε ότι οι hackers διακινούν κακόβουλο λογισμικό με αυξανόμενο ρυθμό. Μόνο στην πλατφόρμα της Android, το κακόβουλο λογισμικό από τον Ιούνιο έως το Δεκέμβριο του 2011, αυξήθηκε κατά 3325% (Εικόνα 31) Αυτό κυρίως οφείλεται στο γεγονός ότι οι κατασκευαστές των λογισμικών των κινητών πλατφορμών δεν έχουν προλάβει να αναπτύξουν σημαντικούς μηχανισμούς ασφαλείας κατά του κακόβουλου λογισμικού. [2]

Επιπροσθέτως, η τεράστια ανάπτυξη ελεύθερων αγορών εφαρμογών στο διαδίκτυο χωρίς κανένα έλεγχο, βοήθησε στην εξάπλωση των μολυσμένων προγραμμάτων (Εικόνα 32). [28]

Επιπλέον, ειδικά στην περίπτωση της android, κυκλοφορούν πολλές custom version από διάφορους προγραμματιστές , αλλά και εκδίδονται πολλές τροποποιημένες εκδόσεις από τους κατασκευαστές των συσκευών, για λόγους καλύτερης συμβατότητας. Στις περιπτώσεις αυτές όμως, οι αναβαθμίσεις για την ασφάλεια που ακολουθούν την επίσημη έκδοση , μπορεί να μην γίνουν ποτέ ή μετά την πάροδο πολλών μηνών μέχρι να τροποποιηθούν κατάλληλα ,ώστε να είναι συμβατές. Τελικά είτε το κίνητρο είναι η κακή φήμη είτε η εταιρική κατασκοπεία ή το οικονομικό όφελος, οι hackers σήμερα είναι πιο εξελιγμένοι και κυνηγούν υψηλότερους στόχους στις επιθέσεις τους. Αυτό σημαίνει ότι οι ευαίσθητες πληροφορίες από τις επιχειρήσεις, τις κυβερνήσεις, τους πάροχους υπηρεσιών και τους χρήστες είναι σε μεγαλύτερο κίνδυνο.

Όπως και με υπολογιστές, υπάρχει μια ποικιλία απειλών για την ασφάλεια που μπορεί να επηρεάσει τις κινητές συσκευές. Οι απειλές χωρίζονται στις εξής κατηγορίες: application-based, web-based, με βάση το δίκτυο και φυσικές απειλές. [28]



Εικόνα 32 - κύκλος εξέλιξης μιας malware εφαρμογής

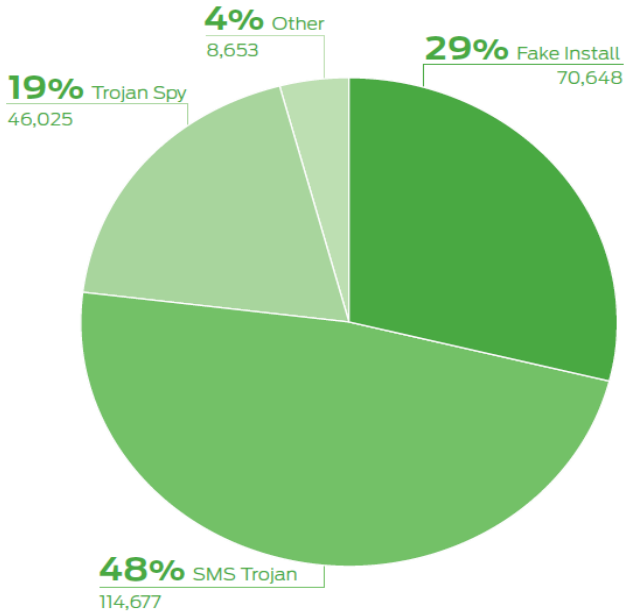
3.3.1. Application-based απειλές

Οι διαθέσιμες προς λήψη εφαρμογές παρουσιάζουν πολλά θέματα ασφαλείας για τις φορητές συσκευές, συμπεριλαμβανομένων τόσο του λογισμικού που έχει σχεδιαστεί ειδικά για να είναι κακόβουλο, όσο και το λογισμικό που μπορεί να αξιοποιηθεί για κακόβουλους σκοπούς. Οι Application-based απειλές γενικά, ταιριάζουν σε μία ή περισσότερες από τις ακόλουθες κατηγορίες:

- **Malware** είναι το λογισμικό που έχει σχεδιαστεί για να έχει κακόβουλη συμπεριφορά σε μια συσκευή. Για παράδειγμα, το κακόβουλο λογισμικό μπορεί να εκτελεστεί

χωρίς τη γνώση του χρήστη, όπως είναι η πραγματοποίηση χρεώσεων στο λογαριασμό του τηλεφώνου του χρήστη, την αποστολή ανεπιθύμητων μηνυμάτων στη λίστα επαφών του καθώς επίσης να δώσει σε έναν εισβολέα τη δυνατότητα εξ αποστάσεως διαχείρισης της συσκευής. Τα κακόβουλα προγράμματα μπορούν επίσης να χρησιμοποιηθούν για να κλέψουν προσωπικά δεδομένα από μια κινητή συσκευή, πράγμα που θα μπορούσε να οδηγήσει σε κλοπή ταυτότητας ή σε οικονομική απάτη. [28]

Υπάρχουν πολλά είδη κακόβουλου λογισμικού (malware) όπως, virus, worm, logic bomb, Trojan horse, backdoor (trapdoor), mobile code, exploits, downloaders, auto-rooter, kit (virus generator), Spammer programs, flooders, keyloggers, rootkit, zombie/bot, Adware, fake installer. Τα ποιο διαδεδομένα είναι τα sms Trojans και τα fake installer (Εικόνα 33). [2]



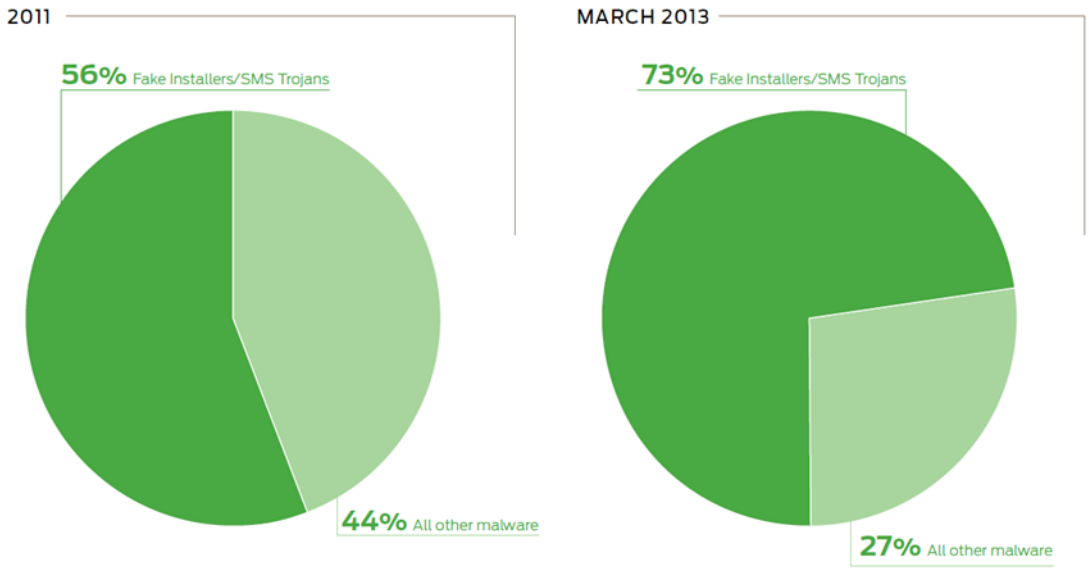
Εικόνα 33 - ποσοστά των διαφόρων malware

Τα **SMS Trojans**, τα οποία σύμφωνα με την έρευνα της Juniper MTC, αποτελούν το 36% των γνωστών κινητών κακόβουλων λογισμικών, τρέχουν στο παρασκήνιο της μολυσμένης εφαρμογής και στέλνουν κρυφά μηνύματα SMS σε αριθμούς πρόσθετου τέλους που ανήκουν στον εισβολέα. Μόλις σταλεί το μήνυμα, ο ιδιοκτήτης της συσκευής χρεώνεται αυτόματα. Οι ιδιοκτήτες αυτών των αριθμών επιπρόσθετης χρέωσης είναι γενικά ανώνυμοι.

Τον Οκτώβριο του 2011, η Juniper MTC ανακάλυψε ένα μεγάλο αριθμό κακόβουλων εφαρμογών που ονομάζονται **fake installers** σε αρκετά παράνομα καταστήματα εφαρμογών. Αυτές οι κακόβουλες εφαρμογές εκμεταλλεύονται την άγνοια των χρηστών και όχι τεχνικές αδυναμίες του λειτουργικού συστήματος. Αυτά τα

κακόβουλα προγράμματα λειτουργούν όπως τα SMS Trojans, όπου οι χρήστες χωρίς να το καταλάβουν συμφωνούν να στείλουν αυτόματα μηνύματα κειμένου με επιπρόσθετη χρέωση στους επιτιθέμενους κατά τη λήψη είτε πειρατικών εκδόσεων των εν τη πληρωμή εφαρμογών είτε εφαρμογών που θα μπορούσαν να βρεθούν δωρεάν στο επίσημο Android Market. [29]

Σε σύγκριση με μερικές από τις πιο πολύπλοκες παραλλαγές malware που εμφανίστηκαν το 2011, τα οποία απαιτούσαν σημαντικές επενδύσεις στην ανάπτυξη και τη διάδοσή τους, αυτό το κακόβουλο λογισμικό είναι ανοιχτό τόσο για αρχάριους όσο και για έμπειρους εγκληματίες , και παρουσιάζει μεγάλη ανάπτυξη στην αγορά εφαρμογών (Εικόνα 34). Επιπλέον, η χρήση των μηνυμάτων SMS με επιπρόσθετη χρέωση παρουσιάζει έναν εύκολο και γρήγορο τρόπο για άμεσο κέρδος έναντι των επιθέσεων που στοχεύουν στην παράνομη εξόρυξη και εκμετάλλευση προσωπικών δεδομένων. [2]



Εικόνα 34 - Αύξηση των κρουσμάτων Fake installer

Ένα παράδειγμα fake installer αποτελεί η πειρατική έκδοση της εφαρμογής Poweramp ,όπου ο χρήστης κατεβάζει την εφαρμογή από μια παράνομη αγορά με την υπόσχεση ότι θα μετατρέψει την δοκιμαστική έκδοση του προγράμματος σε κανονική (Εικόνα 35). Στην πραγματικότητα στέλνει μηνύματα κειμένου με επιπρόσθετη χρέωση στους επιτιθέμενους. Οι εφαρμογές αυτές υπογραμμίζουν την ανάγκη για τους καταναλωτές να είναι πολύ προσεκτικοί από πού λαμβάνουν ή να αγοράζουν τις εφαρμογές τους και τα καταστήματα εφαρμογών που χρησιμοποιούν. Επιπλέον, αν κάποια εφαρμογή ζητά από το χρήστη για πληρωμή μέσω SMS, θα πρέπει να δοθεί επιπλέον προσοχή. [2]

Εικόνα 35 - Poweramp fake installer

- **Το spyware λογισμικό** είναι σχεδιασμένο για τη συλλογή και χρήση δεδομένων χωρίς τη γνώση ή την έγκριση του χρήστη. Τα δεδομένα που συνήθως αλιεύονται, περιλαμβάνουν το τηλεφωνικό ιστορικό κλήσεων, μηνυμάτων κειμένου, στοιχεία τοποθεσίας, το ιστορικό περιήγησης στο διαδίκτυο, τη λίστα επαφών, email και φωτογραφίες της κάμερας. Το Spyware λογισμικό διαχωρίζεται γενικά σε δύο κατηγορίες: όταν είναι στοχευμένο και σχεδιασμένο ειδικά για την επιτήρηση ενός συγκεκριμένου προσώπου ή οργανισμού, ή όταν ο σκοπός του είναι να συγκεντρώσει στοιχεία για μια μεγάλη ομάδα ανθρώπων. Ανάλογα με το πώς χρησιμοποιείται λοιπόν, το spyware μπορεί να θεωρηθεί και ως μη κακόβουλο λογισμικό, όπως στην περίπτωση όπου οι γονείς χρησιμοποιώντας μηνύματα κειμένου ή εφαρμογές με στοιχεία τοποθεσίας, παρακολουθούν το τηλέφωνο του παιδιού τους.

Μία από τις πιο διάσημες περιπτώσεις των εμπορικών spyware ήταν ο CarrierIQ, που χρησιμοποιείται ευρέως από διάφορους κατασκευαστές κινητών συσκευών και εμπορικές εταιρίες. Ο CarrierIQ είχε τη δυνατότητα να καταγράφει ό, τι έγινε σε μια συσκευή, συμπεριλαμβανομένων των αναζητήσεων στο διαδίκτυο χρησιμοποιώντας το ασφαλές πρωτόκολλο HTTPS, και φέρεται να χρησιμοποιείται για την αύξηση της ικανοποίησης των πελατών με την καταγραφή στατιστικών στοιχείων των κλήσεις και άλλες παρόμοιες πληροφορίες. Το πρόβλημα ήταν όμως η εφαρμογή αυτή είχε δυνατότητες καταγραφής για πολύ περισσότερα, και δεν υπήρχε κανένας τρόπος για το μέσο χρήστη να απαλλαγεί από αυτήν. Επιπλέον, δεν υπήρχε τρόπος για τους χρήστες να γνωρίζουν ποιες πληροφορίες οι πωλητές έκριναν αναγκαίες για την βελτίωση των υπηρεσιών που προσέφεραν.

- **Απειλές κατά των Προσωπικών Δεδομένων** μπορεί να προκληθούν από τις εφαρμογές που δεν είναι κατ 'ανάγκη κακόβουλες (αν και μπορεί να είναι), αλλά συγκεντρώνουν ή χρησιμοποιούν περισσότερες ευαίσθητες πληροφορίες (π.χ.,

θέση, λίστες επαφών, προσωπικά στοιχεία) από ό, τι είναι αναγκαίες για τη λειτουργία τους.

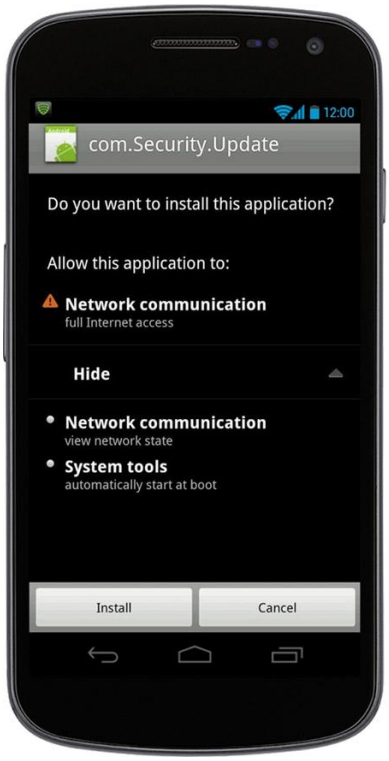
- **Ευάλωτες εφαρμογές** περιέχουν τρωτά σημεία λογισμικού που μπορούν να αξιοποιηθούν για κακόβουλους σκοπούς. Τέτοια τρωτά σημεία μπορεί συχνά να επιτρέψουν σε έναν εισβολέα να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, να εκτελεί ανεπιθύμητες ενέργειες, να σταματήσει μια υπηρεσία από την ορθή λειτουργία της καθώς επίσης να ενεργοποιήσει αυτόματα τη λήψη πρόσθετων εφαρμογών. Οι ευάλωτες εφαρμογές διορθώνονται συνήθως από κάποια ενημέρωση της εφαρμογής από τον κατασκευαστή.

3.3.2. Web-based απειλές

Επειδή οι κινητές συσκευές συχνά είναι συνεχώς συνδεδεμένες με το διαδίκτυο και χρησιμοποιούνται για την πρόσβαση σε web-based υπηρεσίες, οι web-based απειλές που αποτελούν ένα μεγάλο πρόβλημα για τους υπολογιστές αποτελούν εξίσου σημαντικό ζήτημα για τις κινητές συσκευές:

- **Απάτες Phishing** χρησιμοποιούν ιστοσελίδες ή άλλα περιβάλλοντα χρήστη που έχουν σχεδιαστεί για να ξεγελάσουν ένα χρήστη ώστε να παρέχει πληροφορίες, όπως τα στοιχεία σύνδεσης του λογαριασμού του, σε ένα κακόβουλο άτομο δίνοντας την ψευδαίσθηση ότι πρόκειται για νόμιμη υπηρεσία. Οι επιτιθέμενοι συχνά χρησιμοποιούν e-mail, μηνύματα κειμένου, το Facebook και το Twitter για να στείλουν συνδέσμους σε phishing ιστοσελίδες στους ανυποψίαστους χρήστες.

- **Drive-by downloads** αυτόματα αρχίζει να κατεβάζει μια εφαρμογή, όταν ένας χρήστης επισκέπτεται μια ιστοσελίδα. Σε ορισμένες περιπτώσεις, ο χρήστης πρέπει να δώσει τη συγκατάθεσή του για να ξεκινήσει η λήψη της εφαρμογή, ενώ σε άλλες περιπτώσεις η εφαρμογή μπορεί να ξεκινήσει αυτόματα. Ένα παράδειγμα αυτού του είδους των επιθέσεων αποτελεί ο CVE-2010-1807, ο οποίος επιτρέπει στον εισβολέα ,με μολυσμένο κώδικα που κρύβεται σε HTML αρχεία ,να προκαλέσει Denial of Service ή κατάρρευση κάποιων εφαρμογών. Επειδή το πρόγραμμα περιήγησης του Android δεν εγκαθιστά αυτόματα τις εφαρμογές, ένας εισβολέας θα πρέπει να πείσει τον χρήστη να κατεβάσει την εφαρμογή για να μολύνει με επιτυχία τη συσκευή με κακόβουλο λογισμικό. Παρακάτω παρουσιάζεται ένα παράδειγμα Drive-by downloads επίθεσης όπου ο hacker δίνει παραπλανητικό όνομα με στόχο να παραπλανήσει τον χρήστη και αυτός ανυποψίαστος να εγκαταστήσει την μολυσμένη εφαρμογή (Εικόνα 36). [28]



Εικόνα 36 - Drive-by downloads

- **Browser exploits** έχουν σχεδιαστεί για να επωφεληθούν των τρωτών σημείων σε ένα πρόγραμμα περιήγησης στο διαδίκτυο ή ενός λογισμικού που μπορεί να ξεκινήσει μέσω ενός web browser όπως Flash player, PDF reader, ή την προβολή εικόνων. Απλά με την επίσκεψη σε μια ιστοσελίδα, ένας ανυποψίαστος χρήστης μπορεί να προκαλέσει ένα exploit browser και να εγκαταστήσει ένα κακόβουλο λογισμικό ή να εκτελέσει άλλες ενέργειες σε μια συσκευή. [28]

3.3.3. Απειλές Δικτύου

Οι φορητές συσκευές υποστηρίζουν συνήθως τα δίκτυα κινητής τηλεφωνίας, καθώς και τα τοπικά ασύρματα δίκτυα. Υπάρχει μια σειρά από απειλές που μπορούν να επηρεάσουν αυτά τα δίκτυα:

- **Network exploits** εκμεταλλεύονται κενά λογισμικού στο λειτουργικό σύστημα της συσκευής ή σε άλλο λογισμικό που λειτουργεί σε τοπικά (π.χ., Bluetooth, Wi-Fi) ή κυψελωτά (π.χ., SMS, MMS) δίκτυα. Στις περιπτώσεις των Network exploits απειλών, συχνά δεν απαιτεί καμία παρέμβαση του χρήστη, πράγμα που τις καθιστά ιδιαίτερα επικίνδυνες όταν χρησιμοποιούνται για να διαδώσουν αυτόματα κακόβουλο λογισμικό.

Ιδιαίτερο ενδιαφέρον στην κατηγορία αυτών των απειλών έχουν η όχι και τόσο διαδεδομένες επιθέσεις μέσω Bluetooth. Η τεχνολογία Bluetooth απευθύνεται σε

προσωπικές κινητές συσκευές, όπως κινητά τηλέφωνα, PDA, laptop, κ.ά., γεγονός που δίνει μεγάλη βαρύτητα στην απειλή εντοπισμού της γεωγραφικής θέσης. Όσο η συσκευή εκπέμπει ραδιοσήματα ελλοχεύει ο κίνδυνος εντοπισμού της. Για να μπορέσει ένας επιτιθέμενος να εντοπίσει μια τέτοια συσκευή θα πρέπει να έχει στην κατοχή του κάποιο σταθερό αναγνωριστικό της συσκευής. Αν ο επιτιθέμενος καταφέρει να συσχετίσει αυτό το αναγνωριστικό με το φυσικό πρόσωπο στο οποίο ανήκει , η απειλή έχει πραγματοποιηθεί. Έτσι διαφαίνεται η ανάγκη υιοθέτησης μιας κατάστασης ανωνυμίας (anonymity state). Οι συσκευές που βρίσκονται σε αυτή την κατάσταση πρέπει να ανανεώνουν συχνά την διεύθυνσή τους. Υπάρχουν καταγεγραμμένα πέντε είδη επιθέσεων εντοπισμού θέσης:

1. Επίθεση παρακολούθησης κίνησης (traffic monitoring attack)
2. Επίθεση διερεύνησης (inquiry attack)
3. Επίθεση σελιδοποίησης (paging attack)
4. Επίθεση που βασίζεται στο user-friendly όνομα των συσκευών
5. Επίθεση αναπήδησης συχνοτήτων (frequency hopping attack)

- **Wi-Fi Hacking** Τα δημόσια Wi-Fi hotspots αντιπροσωπεύουν ένα πολύ εύκολο κανάλι για να εκμεταλλευτούν οι hackers. Με εργαλεία όπως FaceNiff και Firesheep, βρίσκοντας τους χρήστες σε ένα δίκτυο Wi-Fi, κλέβουν τα διαπιστευτήρια των χρηστών, και με τη χρήση αυτών, μπορούν να μιμηθούν ένα συνδεδεμένο χρήστη στο δίκτυο. Οι επιτιθέμενοι μπορούν να κλέβουν τους κωδικούς πρόσβασης, που οδηγεί σε οικονομικές συνέπειες και σε πολλές περιπτώσεις, κλοπή της ταυτότητας.
- **Wi-Fi Sniffing** μπορεί να θέσει σε κίνδυνο τα δεδομένα που αποστέλλονται από και προς μια συσκευή, εκμεταλλευόμενο το γεγονός ότι πολλές εφαρμογές και ιστοσελίδες δεν χρησιμοποιούν κατάλληλα μέτρα ασφαλείας, στέλνοντας τα στοιχεία τους σε απλό κείμενο (μη κρυπτογραφημένο). Με τον τρόπο αυτό μπορεί εύκολα να υποκλαπούν από οποιονδήποτε παρακολουθεί έναν ανασφαλές τοπικό ασύρματο δίκτυο. [28]

3.3.4. Φυσικές απειλές

Οι φορητές συσκευές σχεδιάστηκαν με κύριο χαρακτηριστικό τη λειτουργία σε όλη την καθημερινή ζωή των χρηστών. Η φυσική τους ασφάλεια λοιπόν, αποτελεί ένα σημαντικό ζήτημα.

- Χαμένες ή κλεμμένες συσκευές είναι από τα πιο διαδεδομένες απειλές. Η κινητή συσκευή είναι πολύτιμη όχι μόνο γιατί το hardware υλικό της, που μπορεί εκ νέου να

πωληθεί στη μαύρη αγορά, αλλά κυρίως λόγω των ευαίσθητων προσωπικών και εταιρικών πληροφοριών που μπορεί να περιέχει.

Παρακάτω παραθέτουμε συνοπτικά όλα τα παραπάνω. [27]

- Application-based threats
  - Malware (virus, worm, logic bomb, Trojan horse, backdoor (trapdoor), mobile code, exploits, downloaders, auto-rooter, kit (virus generator), Spammer programs, flooders, keyloggers, rootkit, zombie/bot, Adware)
  - Spyware
  - Privacy threats
  - Vulnerable applications
- Web-based Threats
  - Phising scams
  - Drive-by-downloads
  - Browser exploits
- Network Threats
  - Passive attacks
    - Traffic analysis, WI-FI sniffing
  - Active attacks
    - Masquerade (hijacking session)
    - Replay
    - Modification of messages (Man-in-the-middle)
    - Network exploits
    - Denial-of-service (DOS)
- Physical Threats
  - Χαμένες ή κλεμμένες συσκευές, μεταχειρισμένες που δεν έχουν καθαριστεί σωστά, κατάσχεση από τελωνιακούς υπαλλήλους ενώ είναι ανοικτή.

3.4. Rooting: Πλεονεκτήματα και μειονεκτήματα

Το Root ουσιαστικά δίνει σε ένα χρήστη το δικαίωμα πρόσβαση σε όλα τα αρχεία ενός συστήματος Android. Αυτός ο χρήστης λέγεται και superuser. Επιτρέπει δηλαδή στους χρήστες να εκτελούν λειτουργίες στη συσκευή που συνήθως δεν θα ήταν δυνατόν να πραγματοποιηθούν με τα φυσιολογικά δικαιώματα. Είναι το αντίστοιχο ακριβώς του administrator account σε ένα σύστημα windows. Μερικές από τις δυνατότητες που έχει κάποιος σαν superuser στη συσκευή είναι :

- Η καλύτερη διαχείριση της μνήμης της συσκευής
- Επανάκτηση διαγεγραμμένων αρχείων
- Δυνατότητα εγκατάστασης custom rom
- Πρόσβαση σε εφαρμογές που είναι φραγμένες στην Ελλάδα καθώς επίσης και εγκατάσταση εφαρμογών που απαιτούν την πρόσβαση σε αρχεία του συστήματος
- Διόρθωση προβλημάτων που έχουνε άμεση σχέση με τα αρχεία του λειτουργικού συστήματος
- Μεταφορά εφαρμογών στην κάρτα SD.
- overclock, undervolt
- πλήρης παραμετροποίηση του γραφικού περιβάλλοντος
- Ξεκλείδωμα από τον πάροχο

Τα δικαιώματα αυτά, μπορεί να χρησιμοποιηθούν για νόμιμους ή παράνομους σκοπούς. Η δίωξη ηλεκτρονικού εγκλήματος ή τα γραφεία εγκληματολογικών ερευνών μπορεί να χρησιμοποιήσουν τα δικαιώματα αυτά ώστε να εξάγουν δεδομένα από τη συσκευή. Επιπλέον, εφαρμογές συσχετισμένες με την ασφάλεια, χρησιμοποιούν το δικαίωμα του διαχειριστή προκειμένου να αποκτήσουν πρόσβαση σε κρυφά αρχεία και γενικά να έχουν τη δυνατότητα σε βάθος σάρωσης του συστήματος. Αν και η πρόσβαση root μπορεί να αυξήσει τον αριθμό των χαρακτηριστικών για μια εφαρμογή ή τις δυνατότητες της συσκευής, μπορεί να δημιουργήσει ταυτόχρονα υποβάθμιση του επιπέδου της ασφάλειας. Ένας χρήστης με κακόβολη συμπεριφορά, είναι πιθανόν να προσπαθήσει να παρακάμψει τους περιορισμούς του συστήματος και των αντίστοιχών δομών και πολιτικών ασφαλείας, αποκτώντας πρόσβαση στα δεδομένα της συσκευής. Επιπροσθέτως, μπορεί να θελήσει να αλλάξει τη δομή μιας εφαρμογής ή να δημιουργήσει μια νέα, εμφωλεύοντας κακόβουλο κώδικα με στόχο την αλλοίωση των αρχείων του λειτουργικού συστήματος. Η χρήση του rooting , βοηθάει προς την κατεύθυνση αυτή. Επίσης, μεταβάλλει ή αλλοιώνει τα μέρη της συσκευής (μια ενέργεια

που έρχεται σε αντίθεση με τις πρακτικές του forensic) και μπορεί να προκαλέσει σοβαρές βλάβες ,που ενδεχομένως να κοστίσουν και την ίδια την εγγύηση της συσκευής. Γενικά η χρήση του rooting δεν είναι ενδεδειγμένη σε χρήστες που δεν έχουν σαφή και ουσιαστική εμπειρία με τη διαχείριση των λειτουργικών συστημάτων. Για τον λόγο αυτό άλλωστε καμία κινητή πλατφόρμα δεν δίνει ποτέ επίσημα τα εν λόγω δικαιώματα.

3.5. Οι 10 μεγαλύτεροι κίνδυνοι στις κινητές συσκευές

Το 2011 η OWASP δημοσίευσε μια έρευνα σχετικά με του 10 μεγαλύτερους κινδύνους που διατρέχουν οι κινητές συσκευές. Αυτοί είναι [30]:

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

3.5.1. Insecure Data Storage

Πολλές εφαρμογές αποθηκεύουν ευαίσθητα δεδομένα σε κινητές συσκευές. Αυτά τα ευαίσθητα δεδομένα θα μπορούσαν να είναι για παράδειγμα, κωδικοί πρόσβασης που χρησιμοποιούνται για τον έλεγχο ταυτότητας των χρηστών. Ευτυχώς, αυτές οι πληροφορίες είναι κρυπτογραφημένες, αλλά μερικές φορές δεν είναι. Η ικανότητα που έχει ο χρήστης να αποθηκεύσει εύκολα και να συλλέγει πληροφορίες στην κάρτα SD καθιστά εύκολη για έναν κακόβουλο χρήστη ή μια εφαρμογή τη συλλογή ευαίσθητων δεδομένων. Αν για παράδειγμα, δεν γίνει κρυπτογράφηση στους κωδικούς πρόσβασης, είναι εύκολο να τους συλλέξει. Οι ευαίσθητες πληροφορίες δεν χρειάζεται να αποθηκευτούν στην κάρτα SD, αλλά θα μπορούσαν να αποθηκεύονται στη μνήμη. [31]

Εικόνα 37 - Insecure data storage

Ένα παράδειγμα φαίνεται στην εικόνα 37 [32]. Τα διαπιστευτήρια των αποθηκευμένων πληροφοριών ρυθμίζονται με το MODE_WORLD_READABLE που επιτρέπει σε κάθε εφαρμογή να έχει πρόσβαση και να διαβάσει τις πληροφορίες, γεγονός που δεν είναι καλό για την ασφάλεια του χρήστη.

3.5.2. Weak Server Side Controls

Μια εφαρμογή και ειδικότερα μια διαδικτυακή εφαρμογή ή μια cloud-based εφαρμογή μπορεί να επικοινωνεί και να λαμβάνει δεδομένα από έναν απομακρυσμένο server. Συνεπώς, είναι σημαντικό να διασφαλίσει αυτή την πλευρά. Από την πλευρά του server, υπάρχουν πολλές επιθέσεις που θα μπορούσαν να πραγματοποιηθούν. Ένας hacker θα μπορούσε, για παράδειγμα, για να αποκτήσει πρόσβαση σε μια κινητή συσκευή, να περάσει μέσω της επικοινωνία του server στη κινητή συσκευή. Δεδομένου ότι η κινητή συσκευή εμπιστεύεται τον server, ο hacker θα μπορούσε να διεισδύσει σχετικά εύκολα στην κινητή συσκευή.

3.5.3. Insufficient Transport Layer Protection

Πρόκειται για το πρόβλημα που προκύπτει από την έλλειψη ελέγχου του server. Χρησιμοποιώντας ελλιπή ή καθόλου κρυπτογράφηση των δεδομένων κατά τη μεταφορά αυτών ή αγνοώντας τα λάθη κατά την επικύρωση τους καθίστανται δυνατές οι MITM επιθέσεις, αλλοιώνοντας τα δεδομένα κατά τη μεταφορά τους. Οι κινητές συσκευές είναι στην πραγματικότητα πιο ευάλωτες σε επιθέσεις MITM καθώς το λουκέτο που εμφανίζεται πάντα όταν μια ιστοσελίδα είναι συνδεδεμένη με το SSL είναι πιο δύσκολο να το παρατηρήσει ο χρήστης χάρη στη μικρότερη οθόνη.

3.5.4. Client Side Injection

Αξιολογώντας τα δεδομένα εισόδου σε μια εφαρμογή Android μπορεί να αποτρέψει τα Client Side Injection. Για παράδειγμα, το XSS είναι επίσης διαθέσιμο σε κινητές

συσκευές και μαζί του είναι διαθέσιμες νέες δυνατότητες για τα smartphones. Ιδιαίτερα, ο κωδικός Injection 29 που εφαρμόστηκε σε smartphones θα μπορούσε, για παράδειγμα, να συγκεντρώνει στοιχεία επικοινωνίας ή άλλες προσωπικές πληροφορίες ακόμα και να στείλει μηνύματα κειμένου σε ακριβούς ξένους τηλεφωνικούς αριθμούς. Μια άλλη client Side_Injection επίθεση θα μπορούσε να είναι μέσω SQL injection. Δεδομένου ότι πολλές εφαρμογές έχουν ως βάση δεδομένων την SQL, η SQL injection θα μπορούσε να αποκαλύψει προσωπικές πληροφορίες ανάλογα με το τι είναι αποθηκευμένο στη βάση δεδομένων.

Οι Android εφαρμογές θα μπορούσαν να στείλουν αιτήσεις σε άλλες εγκατεστημένες εφαρμογές, έτσι ώστε για παράδειγμα η εγκατεστημένη εφαρμογή να θέλει να ανοίξει μια ιστοσελίδα χρησιμοποιώντας το προεπιλεγμένο πρόγραμμα περιήγησης στο διαδίκτυο. Αυτή η επικοινωνία ονομάζεται πρόθεση (Intent) και το ενσωματωμένο πρόγραμμα περιήγησης στο διαδίκτυο του Android πρόσφατα ανακαλύφθηκε ότι έχει μια ευπάθεια κατά το χειρισμό του Intents από άλλες εφαρμογές. Εάν το πρόγραμμα περιήγησης λάβει ένα Intents από javascript δεν θα ανοίξει ένα νέο παράθυρο, αλλά αντί αυτού θα χρησιμοποιήσει το παράθυρο που βλέπει ο χρήστης. Χάρη σε αυτό, κατέστει δυνατή η εκτέλεση JavaScript στην ιστοσελίδα που βλέπει ο χρήστης με αποτέλεσμα να κλέβει τα cookies. [33]

3.5.5. Poor Authorization and Authentication

Ορισμένες εφαρμογές που χειρίζονται την έγκριση και τον έλεγχο ταυτότητας χρησιμοποιούν τον αριθμό του κινητού τηλεφώνου, το IMEI (International Mobile Equipment Identity), το IMSI (International Mobile Subscriber Identity) ή το UUID (Universally Unique Identifier).

Όλοι αυτοί οι αριθμοί είναι εύκολο να τους βρει κανείς σε μια φορητή συσκευή και στη συνέχεια να τους διαβιβάσει με τη σωστή αξία βέβαια στον αποδέκτη και ο κακόβουλος χρήστης να αποκτήσει πρόσβαση. Ο αριθμός IMEI αποτελείται απο 15 ή 17 αριθμούς και οι πρώτοι 8 αριθμοί είναι συγκεκριμένοι, αφήνοντας στους εισβολείς 7 ή 9 αριθμούς αριστερά για να μαντέψουν. Οι προγραμματιστές επιλέγουν αυτόν τον έλεγχο ταυτότητας γιατί είναι εύκολο να τον εφαρμόσουν και νομίζουν ότι είναι αξιόπιστος. Η Πληκτρολόγηση του κωδικού σε μια φορητή συσκευή θα μπορούσε να είναι δύσκολη αλλά και ενοχλητική. Συνεπώς, οι προγραμματιστές επιλέγουν τον έλεγχο ταυτότητας με κάτι άλλο λιγότερο ασφαλές για τον χρήστη. Αυτό καθιστά όσο το δυνατόν πιο εύκολη για τον χρήστη την πρόσβαση σε μια φορητή συσκευή, αλλά με λιγότερη ασφάλεια. [30]

Εάν οι χρήστες μπορούν να επιλέγουν κωδικούς πρόσβασης, συνήθως επιλέγουν κωδικούς που είναι εύκολο να θυμούνται. Η απαγόρευση στους χρήστες να χρησιμοποιούν εύκολους κωδικούς πρόσβασης και αντίθετα να χρησιμοποιούν

αριθμούς ή ειδικούς χαρακτήρες στους κωδικούς πρόσβασης, είναι κάτι που πρέπει να εξεταστεί. Η καλύτερη φυσικά επιλογή θα μπορούσε να είναι η υποχρεωτική χρήση αριθμών και χαρακτήρων. [32]

3.5.6. Improper Session Handling

Οι session handling σε εφαρμογές πραγματοποιούνται με http cookies, O Auth tokens και Single Sign On (SSO) υπηρεσίες. Τα Hyper Text Transfer Protocol (HTTP) cookies αποστέλλονται εντός της HTTP απάντησης και περιέχουν τις τιμές για το όνομα, την αξία, την ημερομηνία λήξης, την έγκυρη Uniform Resource Locator (URL) διαδρομή, τον έγκυρο domain και αν τα cookies θα πρέπει να αποστέλλονται με ή χωρίς SSL. Αν τα cookies έχουν προγραμματιστεί να αποστέλλονται μόνο με το SSL, αυτό μειώνει τον κίνδυνο κάποιος άλλος να αποκτήσει τα cookies. Αυτά τα cookie πρέπει να σωθούν και αυτό οδηγεί σε μια άλλη απειλή, που αναφέρθηκε προηγουμένως, την insecure data storage. Μια άλλη προσέγγιση για την αποστολή cookies και χωρίς την αποθήκευση τους θα μπορούσε να γίνει στο πλαίσιο της διεύθυνσης URL. Αυτό βοηθά για την αποθήκευση πληροφοριών, έτσι ώστε η χρήση της υπηρεσίας να μπορεί να συνεχίσει από εκεί που σταμάτησε. Είναι ένας βολικός τρόπος για να θυμάται τις ρυθμίσεις όπως τα προϊόντα σε ένα καλάθι ή να ταυτοποιεί τους χρήστες κατά την περιήγηση τους μέσα σε μια εφαρμογή ή μεταξύ διαφόρων εφαρμογών. [34]

Το OAuth είναι ένα ανοικτό πρότυπο που επιτρέπει τη συνεργασία μεταξύ διαφορετικών εφαρμογών. Για παράδειγμα, ένας χρήστης χρησιμοποιεί μια εφαρμογή παιχνίδι και έχει μόλις ένα νέο ρεκόρ που θα ήθελε να το μοιραστεί με εύκολο τρόπο σε ένα κοινωνικό δίκτυο. Χωρίς το OAuth ο χρήστης θα έπρεπε να παρέχει το όνομα χρήστη και τον κωδικό πρόσβασης στο παιχνίδι, έτσι ώστε το παιχνίδι να συνδεθεί και στη συνέχεια να φορτώσει το νέο ρεκόρ στο κοινωνικό δίκτυο. Αντίθετα, αν το παιχνίδι χρησιμοποιεί το OAuth τότε ζητάει την άδεια από τον χρήστη για να φορτώσει τα δεδομένα στο κοινωνικό δίκτυο. Αυτή η άδεια θα πρέπει να χορηγείται από το χρήστη και ως εκ τούτου τα ονόματα χρηστών και οι κωδικοί πρόσβασης δεν αποκαλύπτονται. Το παιχνίδι λαμβάνει ένα διακριτικό που χρησιμοποιείται για να αποκτήσει πρόσβαση ο χρήστης και στη συνέχεια να φορτώσει το νέο ρεκόρ [35].

Το SSO είναι ένα χαρακτηριστικό που επιτρέπει στον χρήστη να συνδεθεί και να αποκτήσει πρόσβαση σε πολλαπλά συστήματα και εφαρμογές εφόσον ο χρήστης έχει την πρόσβαση που απαιτείται. Με την εφαρμογή αυτή ο χρήστης θα πρέπει να θυμάται έναν μόνο κωδικό πρόσβασης. (Opengroup. Single Sign-On).

Μια μεγάλη διαφορά μεταξύ των web εφαρμογών και των κινητών εφαρμογών είναι ότι έχουν συχνά πολύ περισσότερο κύρος. Οι χρήστες θέλουν κινητές συσκευές που να είναι βολικές στη χρήση και ως εκ τούτου δεν θέλουν να επαναλαμβάνουν τον έλεγχο ταυτότητας πολύ συχνά. Εάν ένας εισβολέας βρει αυτό το cookie και αρχίσει να το

χρησιμοποιεί, ο εισβολέας έχει περισσότερο χρόνο για να κάνει ζημιά. Το κόστος της υπομονής των χρηστών δεν θα πρέπει να είναι πιο σημαντικό από την ασφάλεια τους και ως εκ τούτου η εφαρμογή λιγότερου έγκυρου χρόνου για τα cookies. [32]

3.5.7. Security Decisions Via Untrusted Inputs

Οι εφαρμογές μπορούν να λαμβάνουν αποφάσεις μόνες τους για να εκπληρώσουν τις ανάγκες τους. Αυτό δημιουργεί μια απειλή για την ασφάλεια, όταν ο χρήστης δεν έχει δώσει το δικαίωμα αυτό στις εφαρμογές. Στο Android μια εφαρμογή μπορεί να ξεκινήσει μια πρόθεση η οποία θα μπορούσε να είναι είτε ρητή είτε σιωπηρή, και να ανοίξει τον δρόμο για XSS ευπάθειες, κατά την αναζήτηση υπηρεσιών. Αυτές οι προθέσεις, θα μπορούσαν να ανεβάσουν δεδομένα, να στείλουν sms ή διαγράψουν το περιεχόμενο του τηλεφωνικού κατάλογου χωρίς την άδεια του χρήστη. Αυτό συμβαίνει συχνά με κακόβουλες εφαρμογές που απαιτούν δικαιώματα, κατά την εγκατάσταση τους και ο χρήστης δεν νοιάζεται για τα δικαιώματα αυτά. Ο χρήστης χορηγεί ακριβώς όλα τα δικαιώματα επειδή είναι πρόθυμος να παίξει το νέο παιχνίδι που όλοι μιλούν για αυτό. Τα δικαιώματα αυτά θα μπορούσε να είναι δύσκολο να τα καταλάβει όταν ίσως απαιτείται περαιτέρω έγκριση όταν η εφαρμογή τρέχει και δημιουργεί μια συγκεκριμένη πρόθεση. [30]

3.5.8. Side Channel Data Leakage

Πρόκειται για διαρροή δεδομένων σε κάποιο χώρο της κινητής συσκευής η οποία δεν θα έπρεπε να είναι εκεί. Πληροφορίες μπορούν να αποθηκεύονται στη συσκευή ακούσια καθώς και ευαίσθητα δεδομένα τα οποία στη συνέχεια ονομάζονται κανάλι διαρροής δεδομένων.

Προγράμματα περιήγησης στο Web αποθηκεύουν στην cache στη φορητή συσκευή που θα μπορούσαν να περιλαμβάνουν ευαίσθητες πληροφορίες. Screenshots θα μπορούσαν να έχουν ληφθεί, ενώ οι χρήστες χρησιμοποιούν την εφαρμογή τραπεζικών συναλλαγών, αποκαλύπτοντας τραπεζικούς λογαριασμούς και χρηματικές συναλλαγές. Μηνύματα λάθους του συστήματος που δίνουν ενδείξεις για το πώς λειτουργεί μια εφαρμογή θα μπορούσαν να παρατηρηθούν, μαζί με σχόλια χρησιμοποιώντας το logcat το οποίο είναι ένα εργαλείο που παρέχει πληροφορίες εντοπισμού σφαλμάτων για Android εφαρμογές. [30]

Προσωρινοί κατάλογοι που χρησιμοποιούνται για την αποθήκευση αρχείων για την εφαρμογή θα μπορούσαν να περιέχουν ευαίσθητες πληροφορίες. Ανακτώντας τα δεδομένα της μνήμης με τον Dalvik Debug Monitor Server (DDMS) θα μπορούσε να αποκαλύψει ανεπιθύμητα δεδομένα, όπως tokens και τους κωδικούς πρόσβασης που χρησιμοποιεί η κινητή συσκευή.

3.5.9. Broken Cryptography

Οι εφαρμογές που αποθηκεύουν κάποιου είδους πληροφοριών, ιδίως σε κοινά μέσα, συχνά χρησιμοποιούν την κρυπτογράφηση, έτσι ώστε κανένας άλλος να μην μπορεί να δει τα στοιχεία. Ένας προγραμματιστής έχει τη δυνατότητα να χρησιμοποιήσει τις βιβλιοθήκες crypto αλλά συχνά τροποποιεί αυτές τις βιβλιοθήκες ή εφευρίσκει το δικό του αλγόριθμο κρυπτογράφησης. Η τροποποίηση βιβλιοθηκών crypto θα μπορούσε να δημιουργήσει τρωτά σημεία στις εφαρμογές και να κάνει έναν δικό του αλγορίθμου crypto που είναι καλός πολύ κακό. Πολλοί προγραμματιστές πιστεύουν ότι η κωδικοποίηση για παράδειγμα με base64 είναι ένας καλός τρόπος για την κρυπτογράφηση των δεδομένων, αλλά στην πραγματικότητα δεν είναι. Το ίδιο και με την σύγχυση όπου τα δεδομένα έχουν αλλάξει σε κάτι άλλο που δεν είναι τόσο κατανοητό ή σε σειρά όταν οι προγραμματιστές αλλάξουν τα δεδομένα σε άλλη μορφή. Η λήψη μιας εφαρμογής και εφαρμόζοντας reverse engineer σε αυτή θα αποκαλύψει το πώς η κρυπτογράφηση υλοποιήθηκε και αν είναι εύκολη, ένας εισβολέα δεν θα έχει κανένα πρόβλημα να αντιστρέψει τη διαδικασία και να αποκρυπτογραφήσει τα δεδομένα. [32]

3.5.10. Sensitive Information Disclosure

Αυτό αφορά τα ευαίσθητα δεδομένα που αποθηκεύονται ως αυστηρά κωδικοποιημένα ή ενσωματωμένα μέσα σε μια εφαρμογή σε σύγκριση με μια μη ασφαλή αποθήκευση δεδομένων σχετικά με την κινητή συσκευή για τη χρήση των εφαρμογών. Σχεδόν κάθε πρόγραμμα μπορεί να υποστεί reverse engineered παρέχοντας σχόλια για το πώς ο προγραμματιστής σκέφτεται. Πολλοί δεν πιστεύουν ότι αυτές οι πληροφορίες είναι προσβάσιμες, δεδομένου ότι είναι εντός του πηγαίου κώδικα, αλλά εν τέλη είναι .Τέτοιες πληροφορίες θα μπορούσε να είναι οτιδήποτε, όπως με ποιο τρόπο μια τεχνική κρυπτογράφησης λειτουργεί σε αυστηρά κωδικοποιημένους κωδικούς πρόσβασης, όπως στην εικόνα 38.

```
if (rememberMe)
    saveCredentials(userName, password);
//our secret backdoor account
if (userName.equals("all_powerful")
        && password.equals("iamsosmart"))
    launchAdminHome(v);
```

Εικόνα 38 - Sensitive information disclosure

Στην εικόνα 38. το όνομα χρήστη ισούται με το "all_powerful" και ο κωδικός πρόσβασης ισούται με "iamsosmart" και παρέχει πρόσβαση στην διαχείριση. [32]

Κεφάλαιο 4° Mobile forensics

Τα τελευταία χρόνια με την έξαρση του φαινομένου του ηλεκτρονικού εγκλήματος, ολοένα και περισσότεροι φορείς και επιχειρήσεις έχουν εστιάσει την προσοχή τους στον τομέα της ασφάλειας των δεδομένων τους. Οι κυβερνήσεις έχουν εξουσιοδοτήσει φορείς για τη διασφάλιση της ασφάλειας των απόρρητων κρατικών δεδομένων. Επιπλέον έχουν δημιουργήσει ειδικά σώματα, όπως η δίωξη ηλεκτρονικού εγκλήματος ,που είναι επιφορτισμένα με την εξιχνίαση υποθέσεων-εγκλημάτων που πραγματοποιούνται με σύγχρονους τεχνολογικούς τρόπους. Επίσης το Mobile Security έχει κεντρίσει το ενδιαφέρον και στις ιδιωτικές επιχειρήσεις για να προστατεύσουν τον εαυτό τους από απειλές όπως η εμπορική κατασκοπεία, οι οικονομικές απάτες, καθώς επίσης και οι κλοπές πνευματικής ιδιοκτησίας. Όμως και υποθέσεις προσωπικού ενδιαφέροντος όπως διαζύγια, διαμάχες επιμέλειας παιδιών αλλά και περιουσιακές διαφορές έχουν κερδίσει από την πρόοδο αυτού του τομέα. Όλα αυτά συνετέλεσαν στη σύσταση ενός νέου κλάδου ερευνών, της ψηφιακής δικανικής.

Ο όρος της ψηφιακής δικανικής (digital forensics) αρχικά χρησιμοποιήθηκε ως συνώνυμο του όρου της δικανικής υπολογιστών (computer forensics) αλλά επεκτάθηκε ο ορισμός του καλύπτοντας όλες τις συσκευές οι οποίες είναι ικανές να αποθηκεύσουν ψηφιακά δεδομένα, περιλαμβάνοντας κινητές συσκευές, βάσεις δεδομένων και δίκτυα, και αυτή τη στιγμή ο όρος μπορεί να χρησιμοποιηθεί ώστε να περιγράψει το σύνολο του κλάδου. Η ψηφιακή δικανική λοιπόν είναι η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση ,ανάλυση και παρουσίαση ψηφιακών αποδείξεων με τρόπο νόμιμα αποδεκτό. [27]

Ως εκ τούτου, τα είδη των ερευνών που θα επωφεληθούν από τη συλλογή των δεδομένων των χρηστών και την παρακολούθηση των smartphones είναι οι έρευνες των αρχών, οι εσωτερικές έρευνες εταιριών καθώς επίσης και ιδιωτικές έρευνες.

Στις έρευνες που διεξάγονται από τις διωκτικές αρχές που έχει εξουσιοδοτήσει το κράτος συνήθως εμπλέκονται μια σκηνή του εγκλήματος, ένα ακέραιο και ακριβές αντίγραφο των δεδομένων της συσκευής με τις αντίστοιχες διαδικασίες συντήρησής τους, καθώς και μια αυστηρή διαχείριση των αποδεικτικών στοιχείων έτσι ώστε οποιαδήποτε αποτελέσματα προκύπτει από την ανάλυση να είναι απόλυτα παραδεκτό στο δικαστήριο. Αντίθετα οι ιδιωτικές έρευνες πραγματοποιούνται από αδειούχους ερευνητές, συζύγους, γονείς, hackers, κλπ. και η έρευνα είναι κυρίως οικονομικής και νομική φύσεως ή αφορά προσωπικά θέματα.

Όσον αναφορά τις εσωτερικές έρευνες που πραγματοποιούνται στα πλαίσια ενός οργανισμού, διεξάγονται από εξειδικευμένο προσωπικό που εργάζεται σε αυτόν, καθώς και εξωτερικές εταιρίες, (π.χ. incident responders, ελεγκτές ασφαλείας, αναλυτές που διεξάγουν προληπτικούς ελέγχους κ.λπ.). Οι εν λόγω έρευνες εστιάζουν στη διερεύνηση

πιθανών παραβιάσεων της πολιτικής ασφαλείας, την κλοπής πνευματικής ιδιοκτησίας, καταχρήσεις, υπεξαιρέσεις, σαμποτάζ, κατασκοπεία, και άλλες καταγγελίες.

Για αντληθούν πολύτιμες πληροφορίες σε μια συσκευή smartphone κατά τη διεξαγωγή μιας έρευνας, απαιτείται συνήθως η φυσική πρόσβαση στη συσκευή. Μια εξαίρεση, αποτελεί το πρόγραμμα Encase Enterprise 4, το οποίο τον Οκτώβριο του 2012 παρουσίασε την εξ αποστάσεως forensic έρευνα σε Android συσκευές μέσω ενός δικτύου. Επιπροσθέτως, μερικά προγράμματα MDMS (Mobile Device Management) μπορούν να εκτελέσουν σε κάποιο βαθμό monitoring στη συσκευή. Υποθέτοντας ότι μια φορητή συσκευή επιτρέπει την ανάκτηση των δεδομένων της, οι ερευνητές μπορούν να χρησιμοποιήσουν μια ποικιλία εργαλείων για να λάβουν ένα λογικό ή φυσικό στιγμιότυπο της τρέχουσας κατάστασης της συσκευής. Τα λογικά στιγμιότυπα περιέχουν ένα dump των αρχείων ή φακέλων της συσκευής, ενώ το φυσικό στιγμιότυπο είναι bit-προς-bit αντίγραφα των τομέων ή σελίδων. Τα ακόλουθα εργαλεία είναι διαθέσιμα για την ανάκτηση πληροφοριών από το Android smartphones : [27]

- Android Debug Bridge
- AFLogical
- AFPhysical
- viaExtract
- Cellebrite UFED
- EnCase Neutrino
- Micro Systemation XRY
- Paraben Device Seizure
- AccessData MPE+.

Κάποια από τα εργαλεία που αναφέρονται παραπάνω είναι φορητές συσκευές hardware και άλλα είναι προϊόντα λογισμικού. Ωστόσο, κοινό σημείο αναφοράς όλων των παραπάνω είναι η απαίτηση για φυσική πρόσβαση στη συσκευή smartphone μέσω usb, ώστε να εκτελέσουν τις απαιτούμενες για την έρευνα εργασίες. Επιπλέον, πολλά από τα εργαλεία απαιτούν πρόσβαση στη συσκευή με root δικαιώματα. Επίσης, σχετική εργασία έχει δείξει ότι όταν δύο διαφορετικά εργαλεία στοχεύουν και εξάγουν το ίδιο σύνολο δεδομένων, τα αποτελέσματα είναι ελαφρώς διαφορετικά εξαιτίας των ποικίλων τεχνικών ανάκτησης που χρησιμοποιούνται σε κάθε εργαλείο. Για παράδειγμα ένα εργαλείο μπορεί να ανακτήσει κάποια μηνύματα sms που κάποιο άλλο δεν κατάφερε.

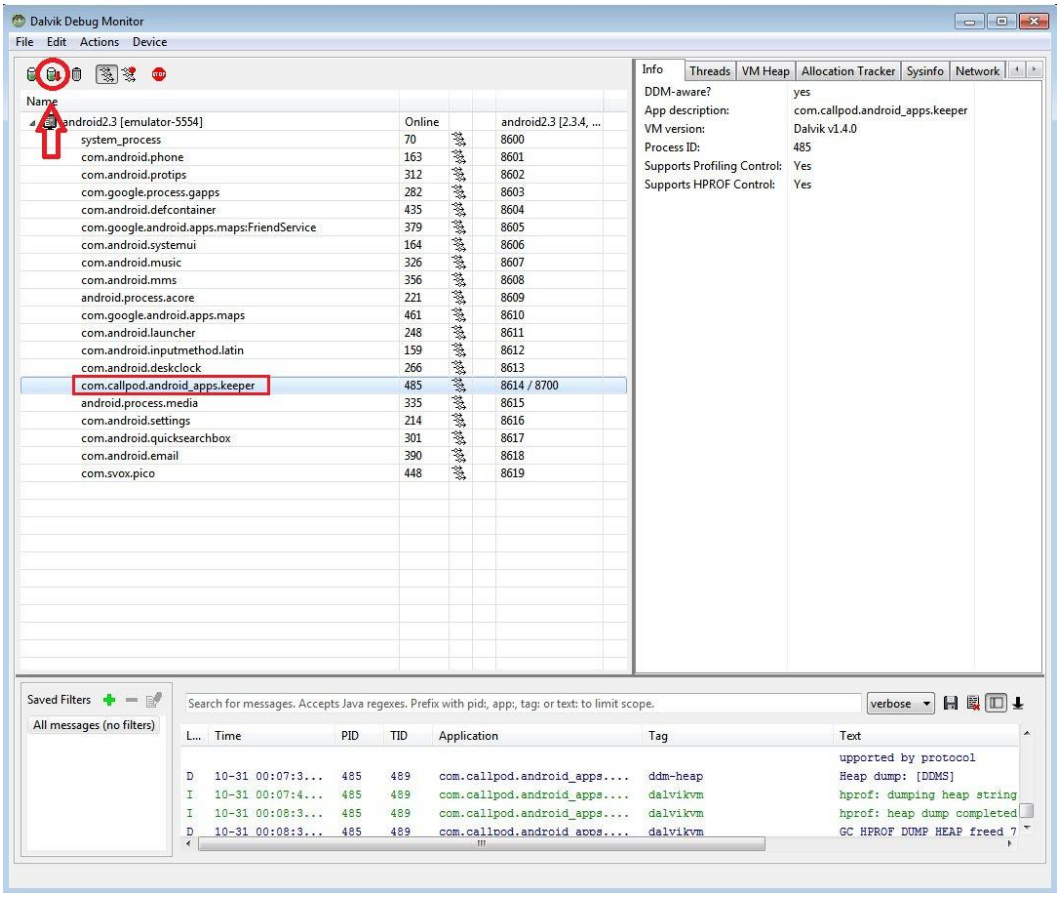
Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας δίνοντας κάποιες κατευθυντήριες γραμμές σχετικά με τα mobile forensics ομαδοποιεί τα δεδομένα των συσκευών που είναι πολύτιμα σε μια έρευνα. Αυτά τα σύνολα δεδομένων περιλαμβάνουν : [36]

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook information
- Appointment calendar information
- Text messages
- Dialed, incoming, and missed call logs
- Email
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging and Web browsing
- Electronic documents
- Location information.

Είναι λοιπόν κατανοητό ότι η περαιτέρω ανάπτυξη του λογισμικού των forensics εργαλείων είναι απαραίτητη. Όχι όμως μόνο για την βοήθεια που παρέχουν στις διωκτικές αρχές για την εξιχνίαση ηλεκτρονικών εγκλημάτων ή για την εξυπηρέτηση εταιριών για την πρόληψη κλοπών και καταχρήσεων. Τα εργαλεία αυτά έχουν και ένα ακόμα σημαντικό ρόλο. Σε πολλές περιπτώσεις αναδεικνύουν και τις ευπάθειες των λειτουργικών συστημάτων και των εφαρμογών που εκτελούνται σε αυτά. Ευπάθειες που εύκολα μπορεί να οδηγήσουν σε απώλεια προσωπικών δεδομένων κρίσιμου χαρακτήρα.

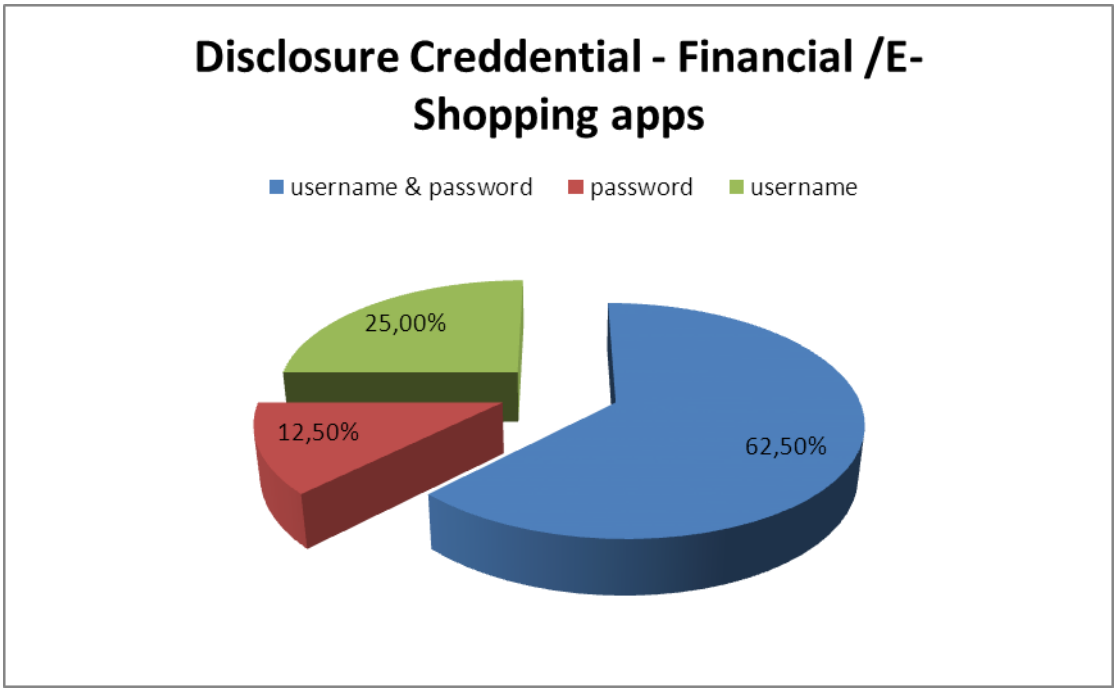
Ένα παράδειγμα δίνεται από μια ομάδα ερευνητών σε σχετική εργασία που πραγματοποιούσαν για το Πανεπιστήμιο του Πειραιά. Στην προσπάθεια να ανακτήσουν τα δεδομένα της μνήμης από μια συσκευή με Android λειτουργικό σύστημα, παρατήρησαν ότι κρίσιμες εφαρμογές , με σημαντικά data in motion δεδομένα του χρήστη (όπως username και password σε τραπεζικές εφαρμογές), παρέμεναν στη μνήμη και μάλιστα σε μορφή απλού κειμένου. [37] Εκτελώντας μια σειρά από πειράματα

με τη βοήθεια ενός εργαλείου του SDK της Google , το DDMS (Dalvik Debug Monitor Server) (Εικόνα 39), απέδειξαν ότι περίπου στο 62% των εφαρμογών που ελέγχθηκαν (τραπεζικές και ηλεκτρονικές αγορές) ανακτήθηκαν τα διαπιστευτήρια του χρήστη (Εικόνα 40). [37]



Εικόνα 39 - λειτουργία του DDMS

Τέτοιου είδους ευπάθειες, είτε αυτές προκύπτουν από σφάλματα στον κώδικα των προγραμματιστών των είτε από κενά ασφαλείας του λειτουργικού συστήματος, εκθέτουν τα προσωπικά δεδομένα του χρήστη. Αυτό μπορεί να οδηγήσει εύκολα σε οικονομικές απώλειες, αφού όπως αναφέρθηκε και παραπάνω, οι κακόβουλοι χρήστες καραδοκούν και εκμεταλλευόμενη την κάθε ευκαιρία θα προσπαθήσουν να αποκτήσουν κέρδος. Οι κατασκευαστές λοιπόν των εφαρμογών και του λειτουργικού συστήματος οφείλουν να θωρακίσουν τα προσωπικά δεδομένα των χρηστών και να τους παρέχουν τη μέγιστη δυνατή ασφάλεια.



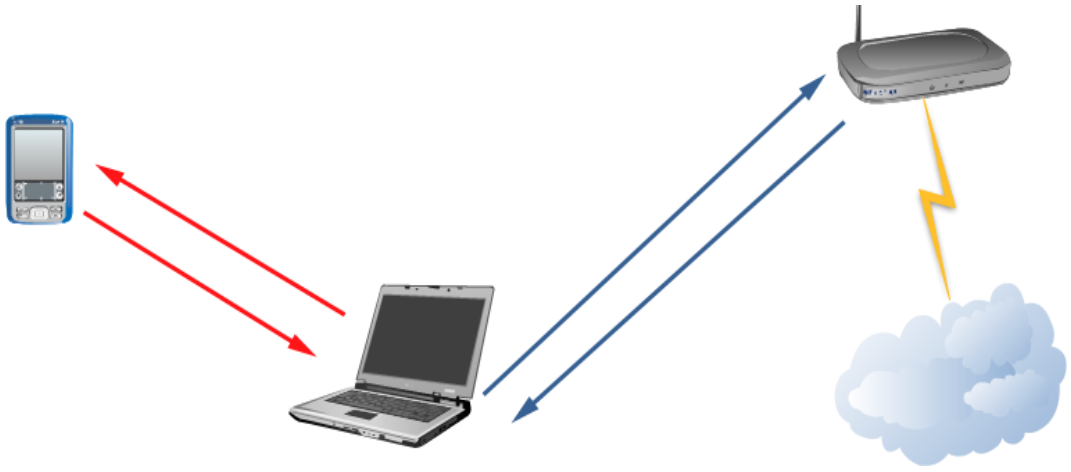
Εικόνα 40 - % αποτελέσματα ανάκτησης των credential

Κεφάλαιο 5° Σενάρια Επιθέσεων

Ακολουθούν μια σειρά από σενάρια επιθέσεων σε κινητές συσκευές με λειτουργικό Android.

5.1. Man In The Middle Attack - Sniffing Passwords

Στο σενάριο αυτό βρισκόμαστε σε ένα δημόσιο χώρο ή cafe που γνωρίζουμε ότι είναι wifi hot spot σημείο. Έχεις τι δυνατότητα να συνδεθείς όμως με τη χρήση κάποιου κωδικού που δίνεται από την καφετέρια ή αναγράφεται πάνω στην απόδειξη αγορών. Δημιουργούμε ένα δικό μας wifi δίκτυο με παρόμοιο όνομα με αυτού του καταστήματος χωρίς ασφάλεια. Το θύμα συνδέεται στο δικό μας δίκτυο και όλη πλέον η κίνηση των πληροφοριών πραγματοποιείται μέσα από τον υπολογιστή μας. Με ένα πρόγραμμα ανάλυσης της κυκλοφορίας στο δίκτυο υποκλέπτουμε όνομα και κωδικούς του θύματος - χρήστη σε γνωστές ιστοσελίδες παρακάμπτοντας την ασφάλεια .



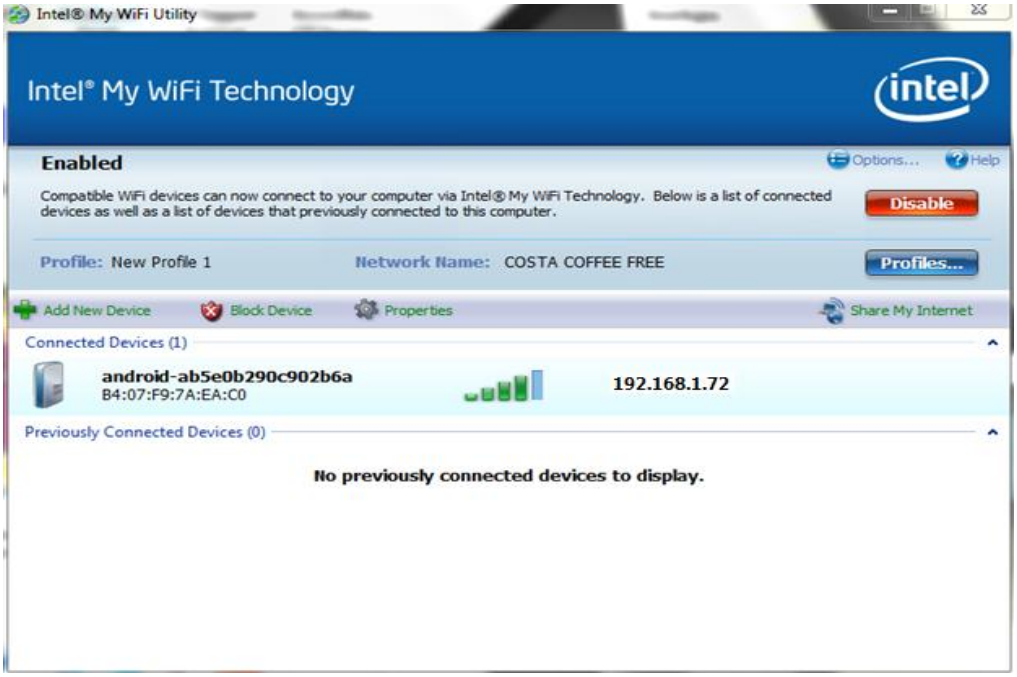
Εικόνα 41 - Σχέδιο της MITM επίθεσης

Θα χρειαστούμε :

- Backtrack 5 ή Linux.
- το SSLStrip
- Ettercap
- το Arpspoof (στο Backtrack 5 είναι εγκατεστημένο)
- Πρόγραμμα διαμοιρασμού πρόσβασης στο Internet

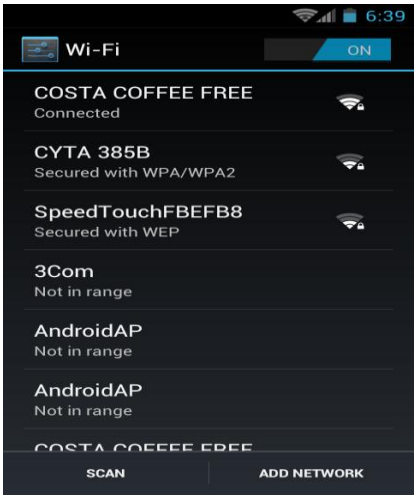
Βήματα Επίθεσης

1. Δημιουργούμε ένα WIFI Hot - Spot χωρίς ασφάλεια με μια πλαστή Επωνυμία. (πχ COSTA COFFEE FREE).



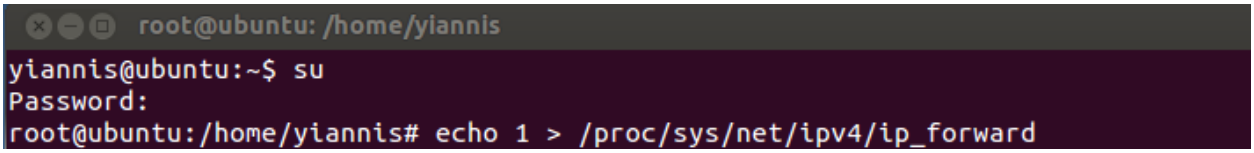
Εικόνα 42 - WiFi hot spot

2. Το θύμα συνδέεται από το Smartphone του στο δίκτυο μας.



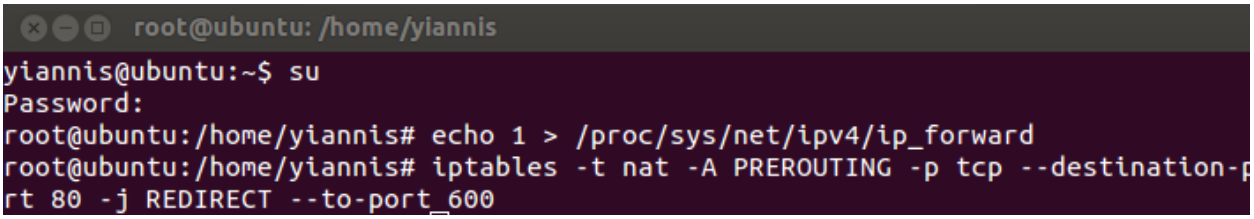
Εικόνα 43 - Σύνδεση στο μολυσμένο δίκτυο

3. Τρέχουμε την εντολή ***echo 1 > /proc/sys/net/ipv4/ip_forward*** ώστε ο υπολογιστής μας να μπει σε forward mode και να μας επιτρέψει να διαβιβάζουμε πακέτα άλλων υπολογιστών.



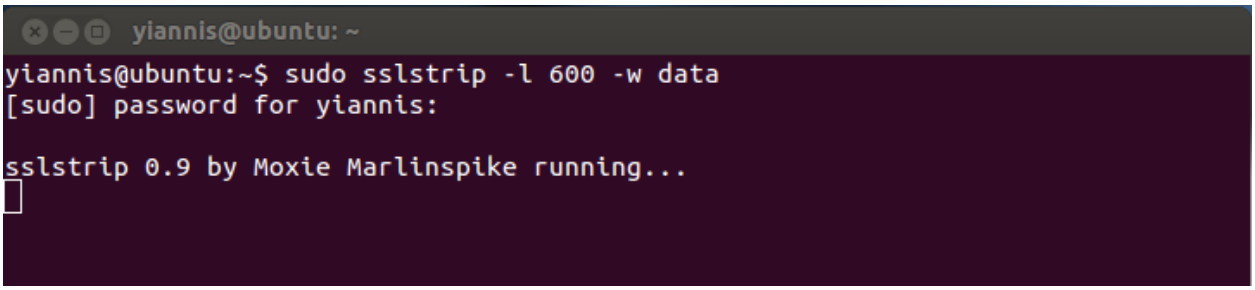
Εικόνα 44 - ip_forward

4. Τρέχουμε την εντολή ***iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 666*** που μας επιτρέπει να ανακατευθύνουμε την HTTP κυκλοφορία (port 80) στο πρόγραμμά μας SSLStrip (port 660)



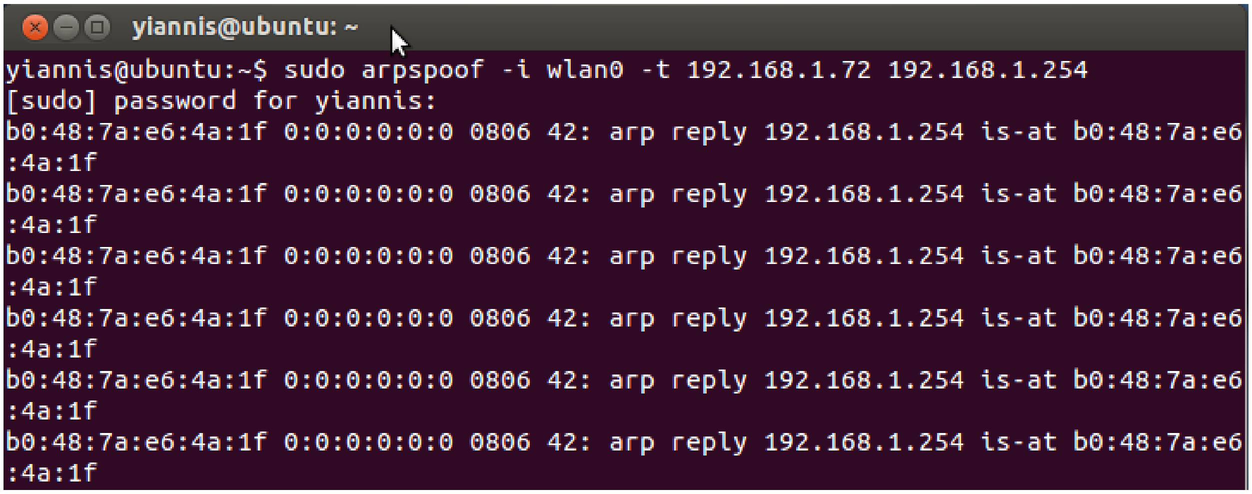
Εικόνα 45 - ανακατεύθυνση θύρας

5. Τρέχουμε την εντολή ***sudo sslstrip -l 660*** ώστε να τρέξει το SSLStrip και να εξουδετερώσει οποιαδήποτε σύνδεση HTTPS και την ανακατευθύνει στο πρωτόκολλο HTTP (μη ασφαλή σύνδεση).



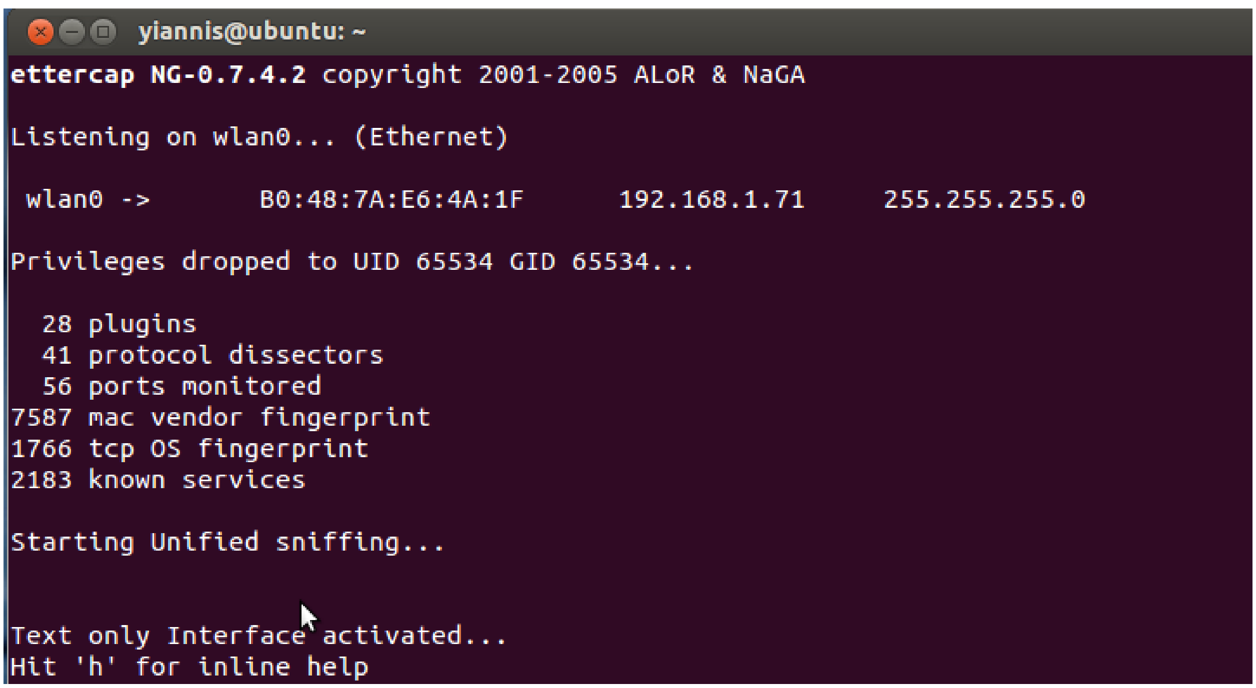
Εικόνα 46 - εκτέλεση του sslstrip

6. Σε νέο terminal τρέχουμε την εντολή ***arpspoof -i wlan0 -t 192.168.1.72 192.168.1.254*** . Με το ArpSpoof μολύνουμε το θύμα ώστε πλέον η κίνηση των πακέτων να γίνεται μέσα από εμάς.



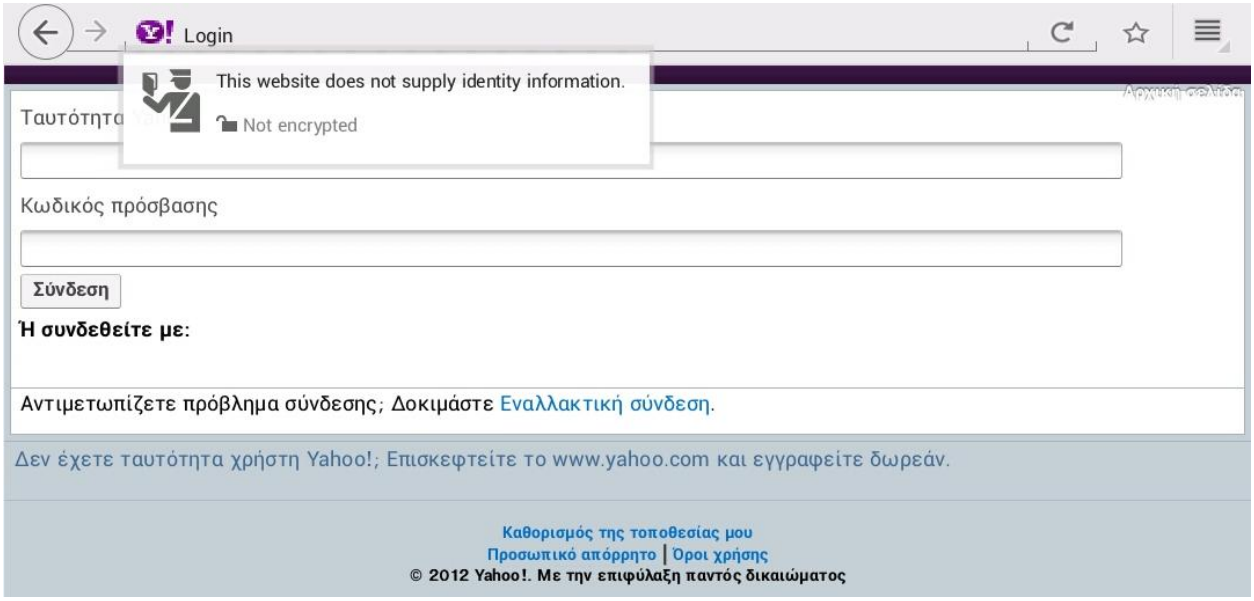
Εικόνα 47 - arpspoof

7. Σε νέο terminal τρέχουμε την εντολή ***ettercap -T -q -i wlan0 data*** όπου με το Ettercap κάνουμε ανάλυση των δεδομένων που κινούνται από το Smartphone του θύματος.

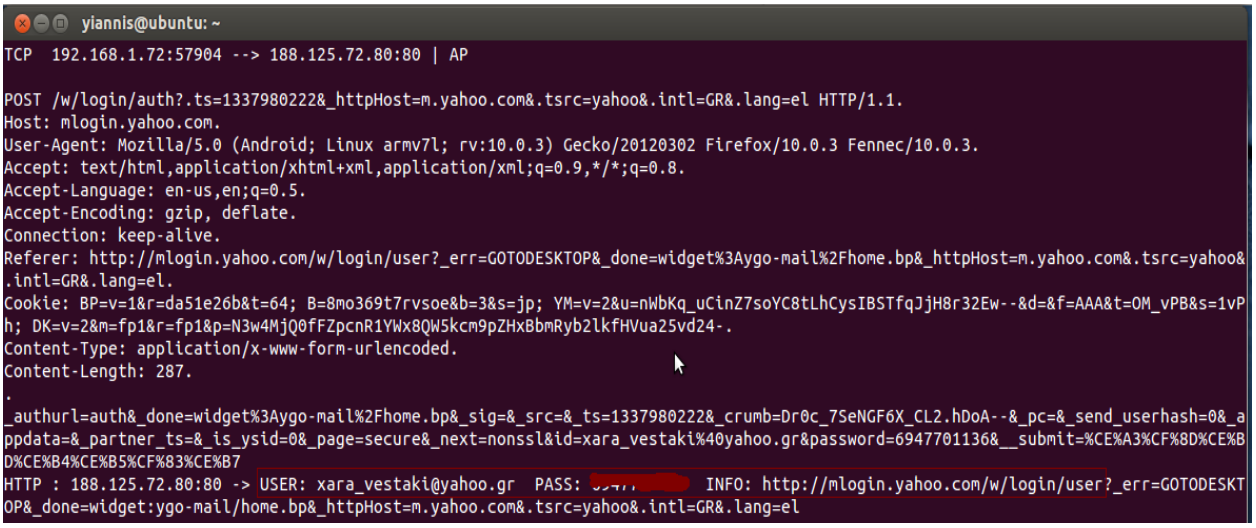


Εικόνα 48 - ettercap

8. Το θύμα προσπαθεί να συνδεθεί με το Yahoo και υποκλέπτουμε εύκολα το mail του καθώς και τον αντίστοιχο κωδικό πρόσβασής του.



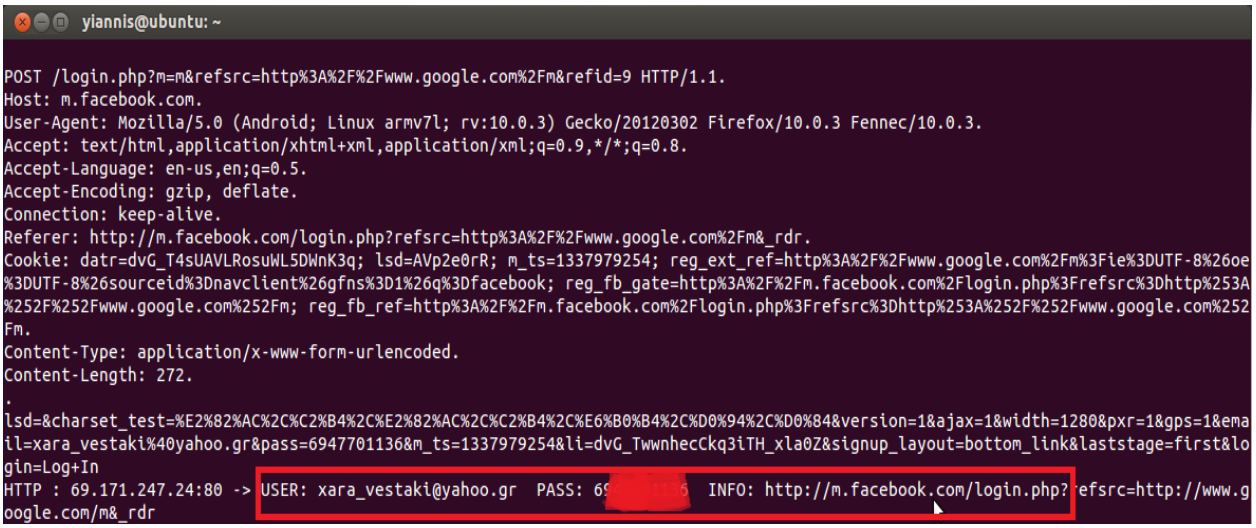
Εικόνα 49 - Σύνδεση στο Yahoo χωρίς ασφάλεια



Εικόνα 50 - Υποκλοπή των Credentials

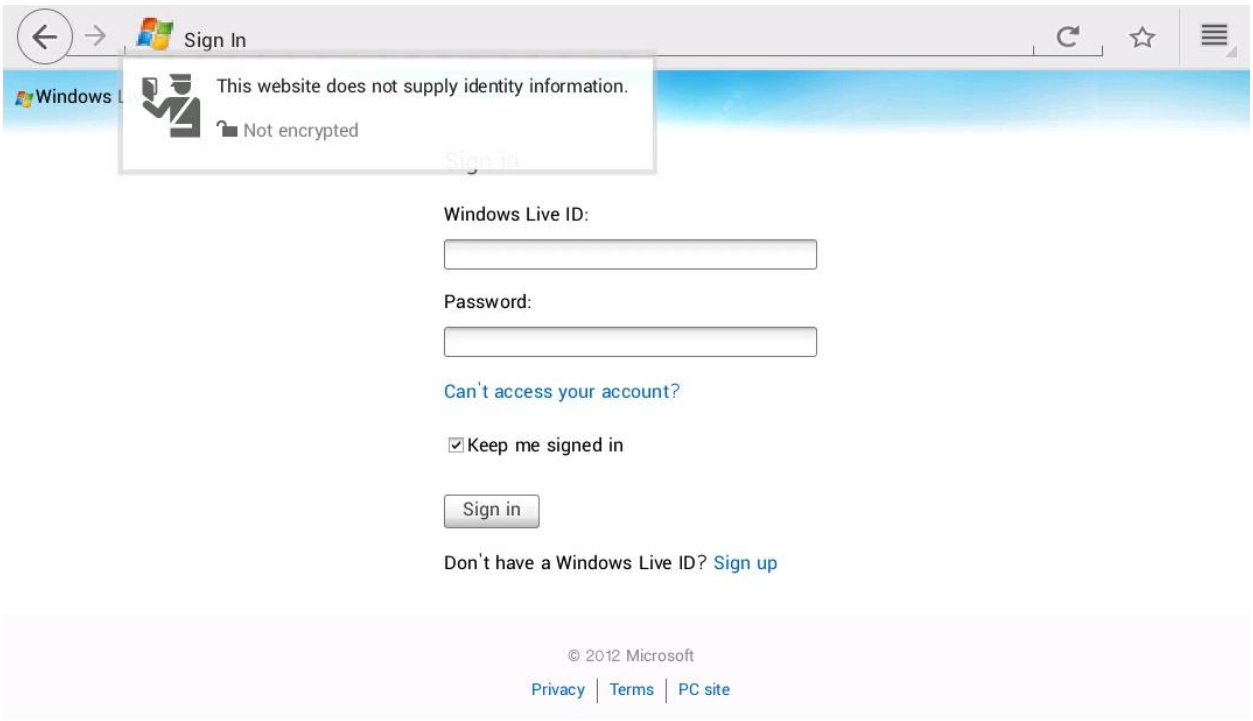
9. Το θύμα προσπαθεί να συνδεθεί με το Facebook και πάλι υποκλέπτουμε όνομα χρήστη και κωδικό πρόσβασης.

Εικόνα 51 - Σύνδεση στο Fasebook χωρίς ασφάλεια



Εικόνα 52 - Υποκλοπή των Credentials

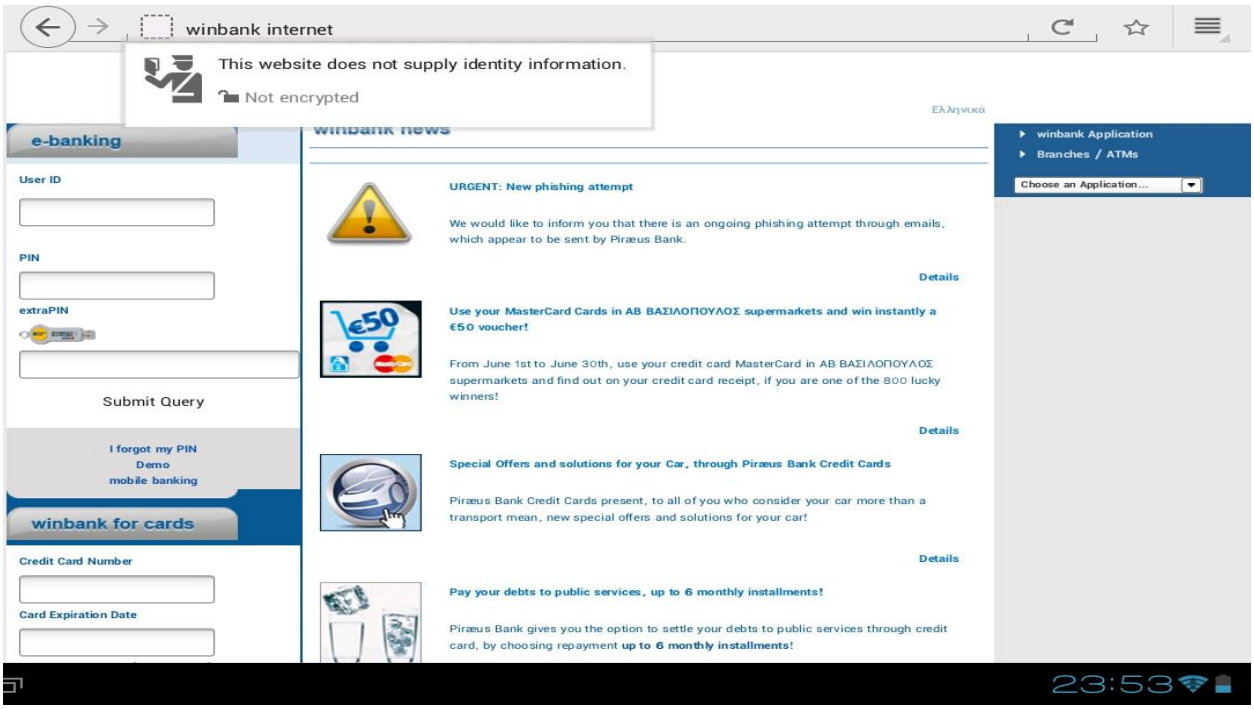
10. Το ίδιο συμβαίνει και με άλλες ιστοσελίδες όπως το Hotmail ,gmail και το e-banking της Τράπεζας Πειραιώς.



Εικόνα 53 - Σύνδεση στο Hotmail χωρίς ασφάλεια

Εικόνα 54 - Υποκλοπή των Credentials

Εικόνα 55 - Σύνδεση στο Gmail χωρίς ασφάλεια

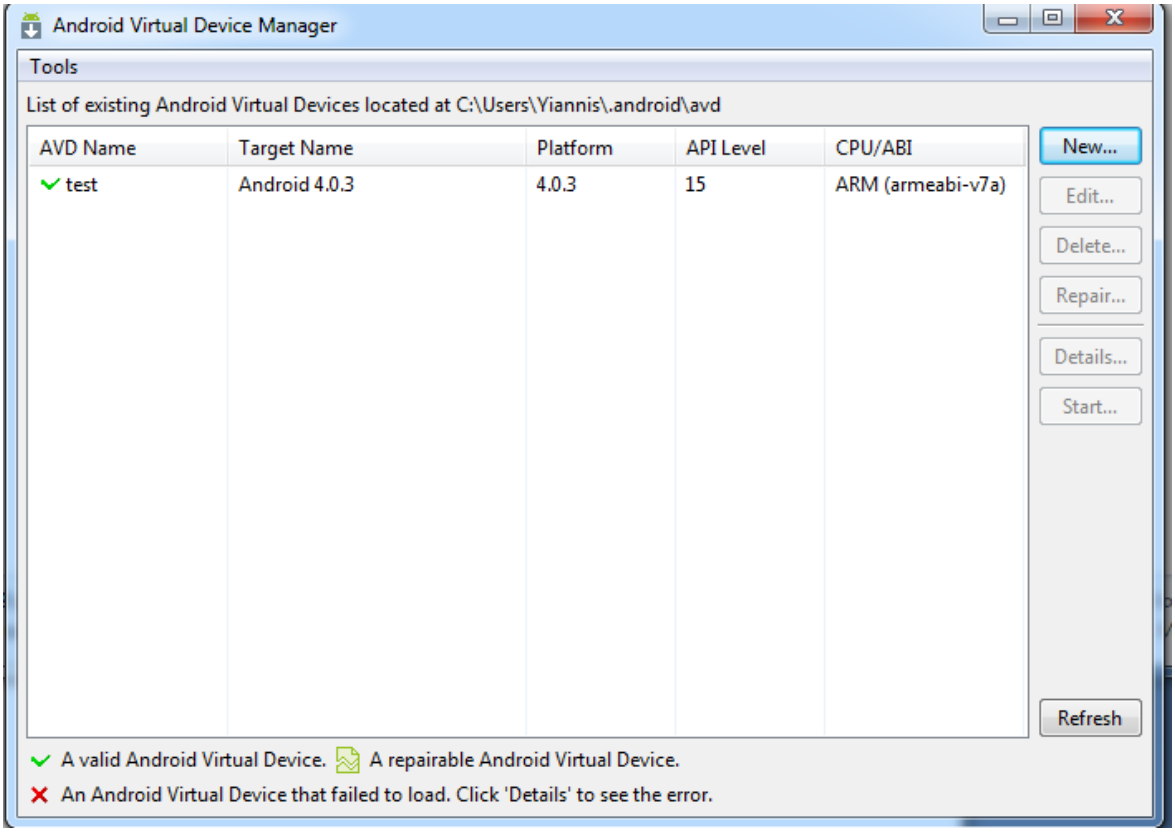


Εικόνα 56 - Σύνδεση στο Winbank χωρίς ασφάλεια

5.2 Εύρεση του κλειδιού κρυπτογράφησης από την Εφαρμογή

Αρχικά, θα δουλέψουμε πάνω σε μια πλατφόρμα εξομοίωσης του λογισμικού Android, την AVD - SDK. Αυτό μας δίνει την δυνατότητα να πειραματιστούμε σε περισσότερες εκδόσεις του λογισμικού και έτσι να παρατηρήσουμε ενδεχόμενες αλλαγές συμπεριφοράς αυτού.

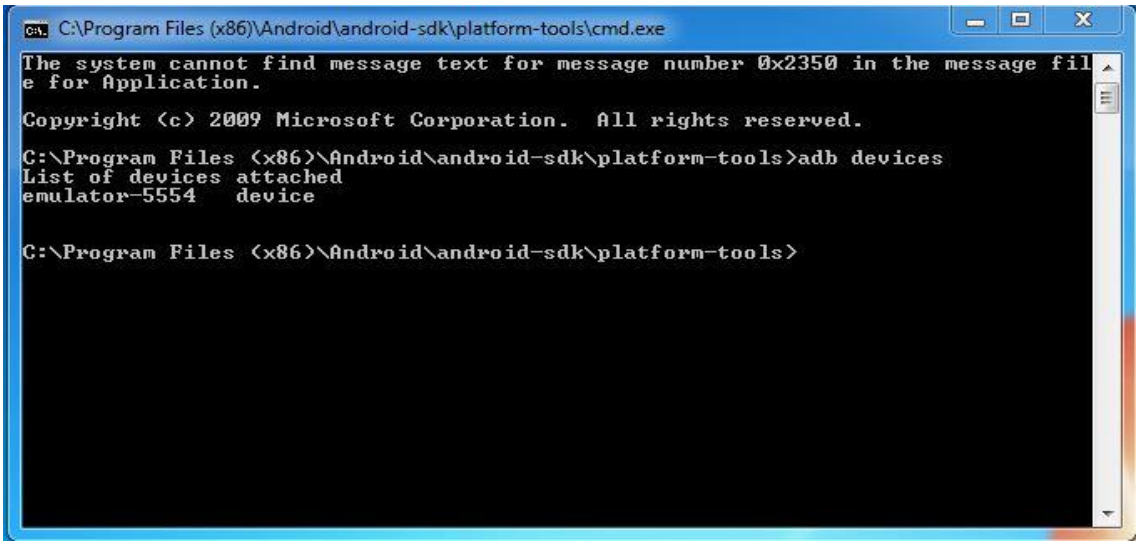
1. Αρχικά δημιουργούμε μια εξομοίωση συσκευής με Android στο AVD (πρέπει να έχουν εγκατασταθεί τα αντίστοιχα SDK tools της version) (Εικόνα 57)



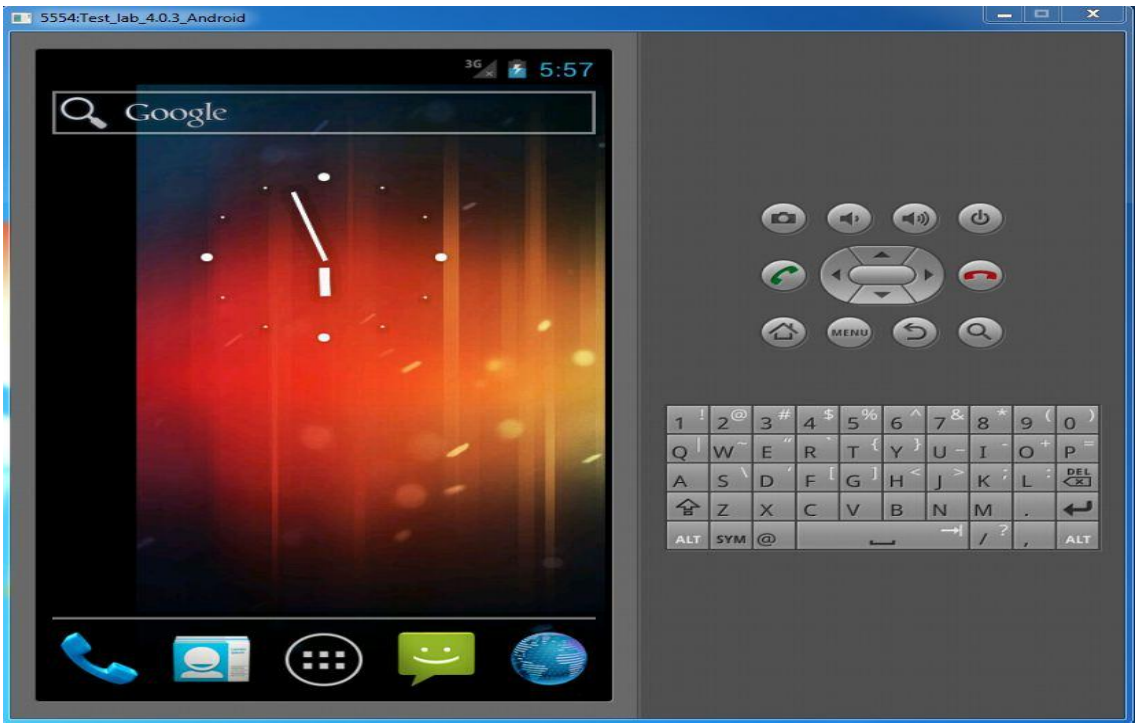
Εικόνα 57 - AVD

Στην εξομοίωσή μας χρησιμοποιούμε την πιο πρόσφατη version του Android, την 4.0.3.

Σε command prompt εκτελούμε ***adb devices*** για να επιβεβαιώσουμε ο εξομοιωτής είναι συνδεδεμένος. (Εικόνες 58,59)

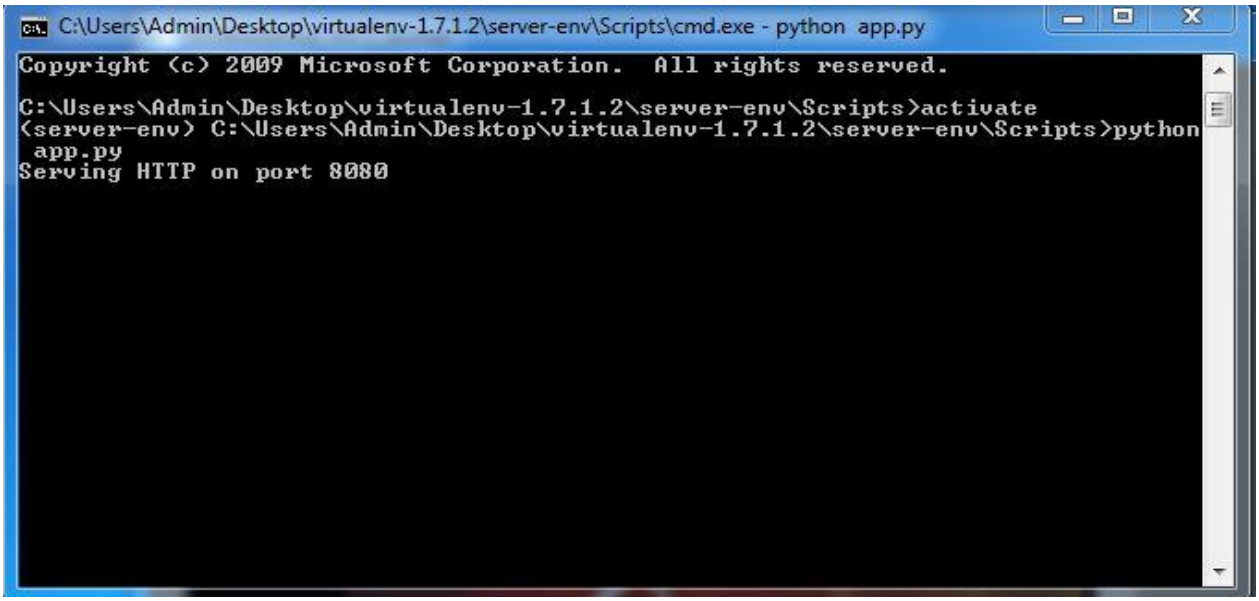


Εικόνα 58 - adb devices

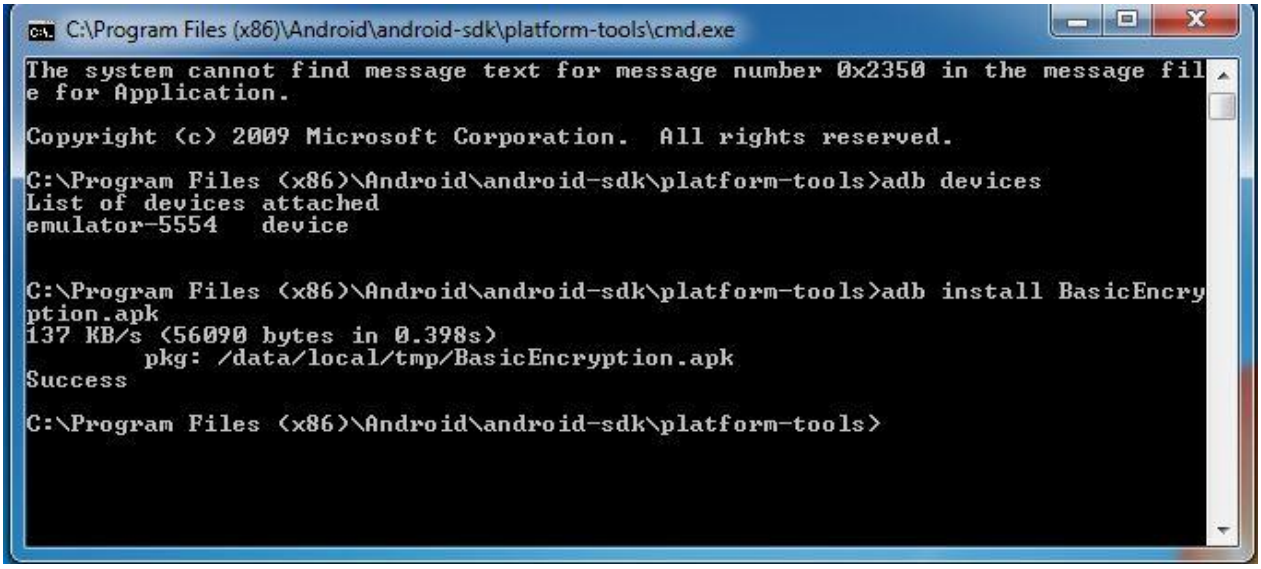


Εικόνα 59 - Εξομοίωση Android

2. Τρέχουμε το αρχείο python ***app.py*** για να ενεργοποιηθεί το HTTP στην θύρα 8080 (Εικόνα 60), και εγκαθιστούμε την εφαρμογή BasicEncryption.apk με την εντολή ***adb install BasicEncryption.apk*** (Εικόνα 61)



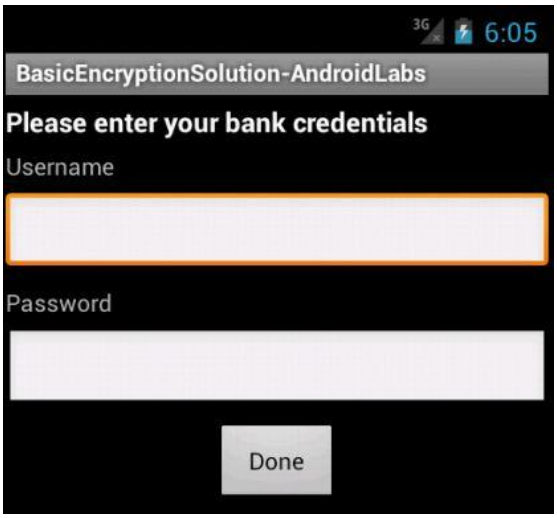
Εικόνα 60 - app.py



Εικόνα 61 - Εγκατάσταση Εφαρμογής

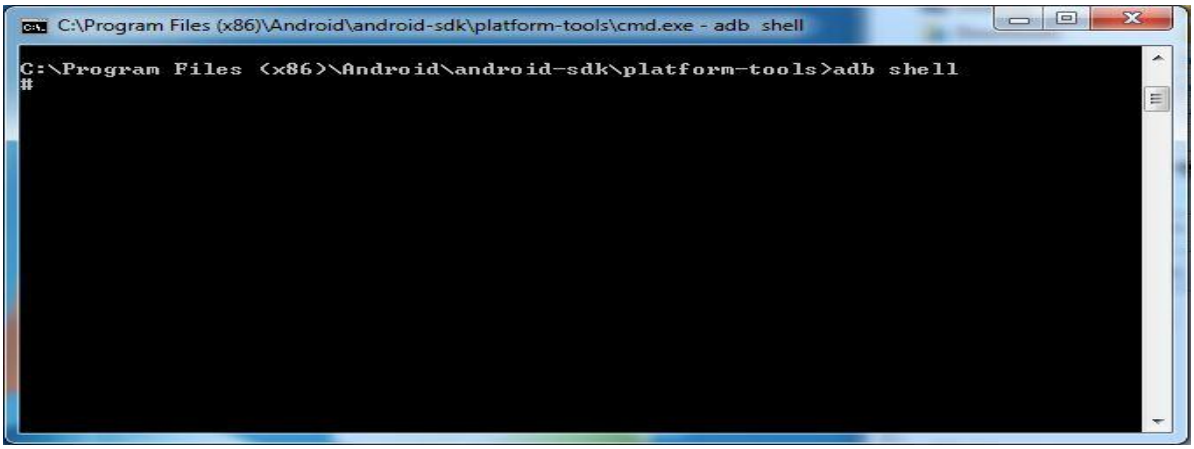
3.Ανοίγουμε την εφαρμογή από τον εξομοιωτή και δίνουμε Username και Password. (Εικόνες 62,63)

Εικόνα 62 - περιβάλλον Χρήστη



Εικόνα 63 - Εισαγωγή credentials

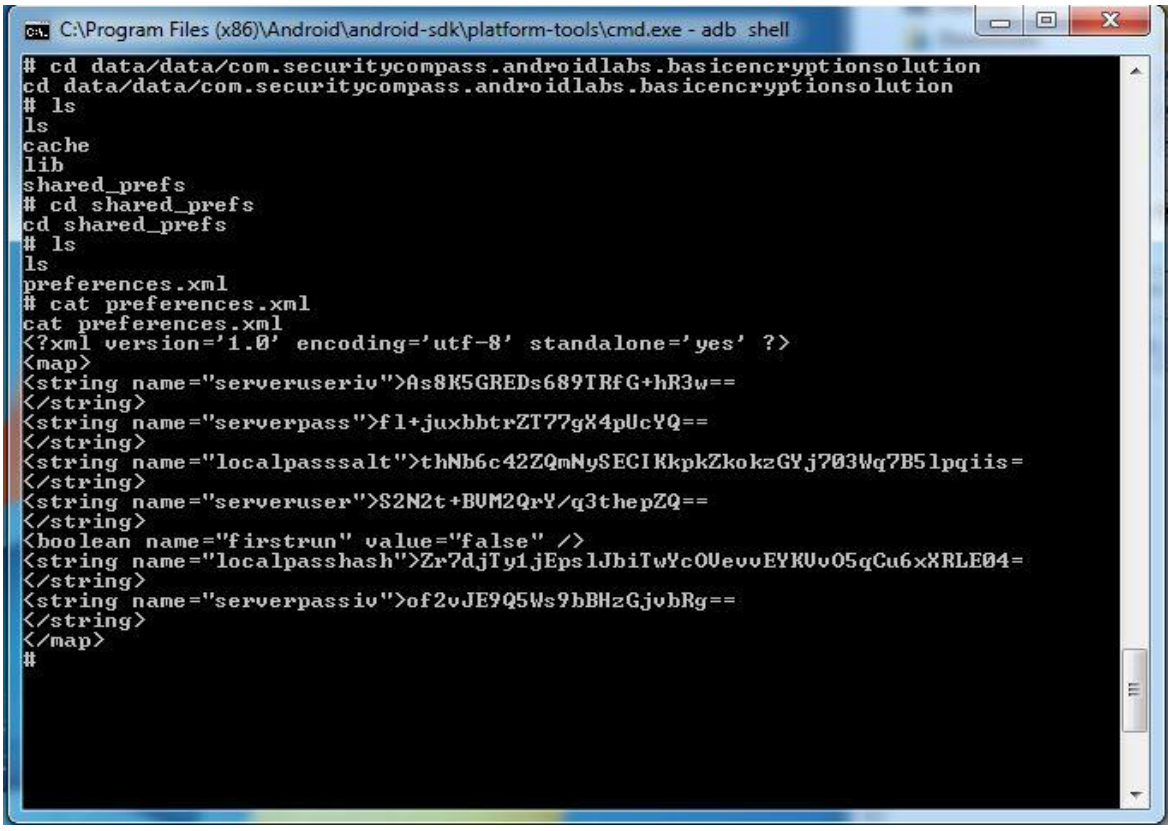
4. Ανοίγουμε ένα shell στον εξομοιωτή με την εντολή ***adb shell***. (Εικόνα 64)



Εικόνα 64 - adb shell

Πλοηγούμαστε στον κατάλογο *data/data/ com.securitycompass.androidlabs. basicencryptionsolution / shared_prefs*

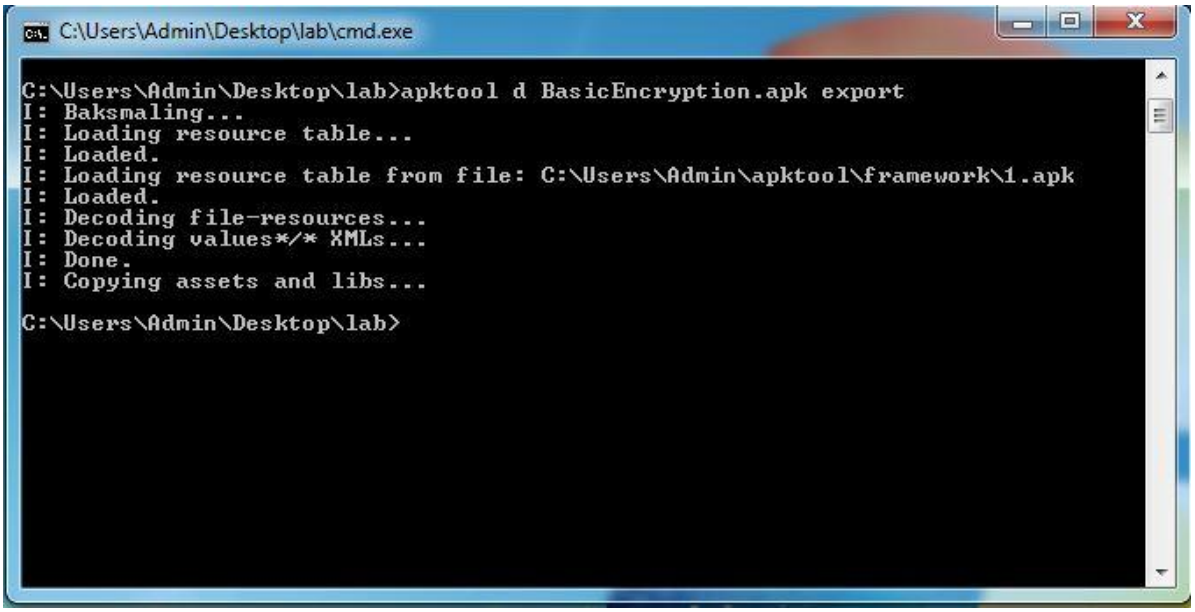
και ανοίγουμε το αρχείο preferences.xml. (Εικόνα 65) .Διαπιστώνουμε ότι το Username και το Password που δόθηκαν πριν είναι κρυπτογραφημένα.



Εικόνα 65 - preferences.xml

5. Στο στάδιο αυτό κάνουμε χρήση ενός πολύ δυνατού εργαλείου του Apktool. Είναι ένα εργαλείο για reverse engineering στις εφαρμογές Android. Μπορεί να αποκωδικοποιήσει τους πόρους σχεδόν στην αρχική του μορφή, και να τους ανακατασκευάσει αφού γίνουν κάποιες τροποποιήσεις. Καθιστά δυνατό τον εντοπισμό σφαλμάτων κώδικα smali, βήμα προς βήμα. Apktool θα απομεταγλωττίσει ή αποκωδικοποιήσει το apk αρχείο σε μορφή smali Android.

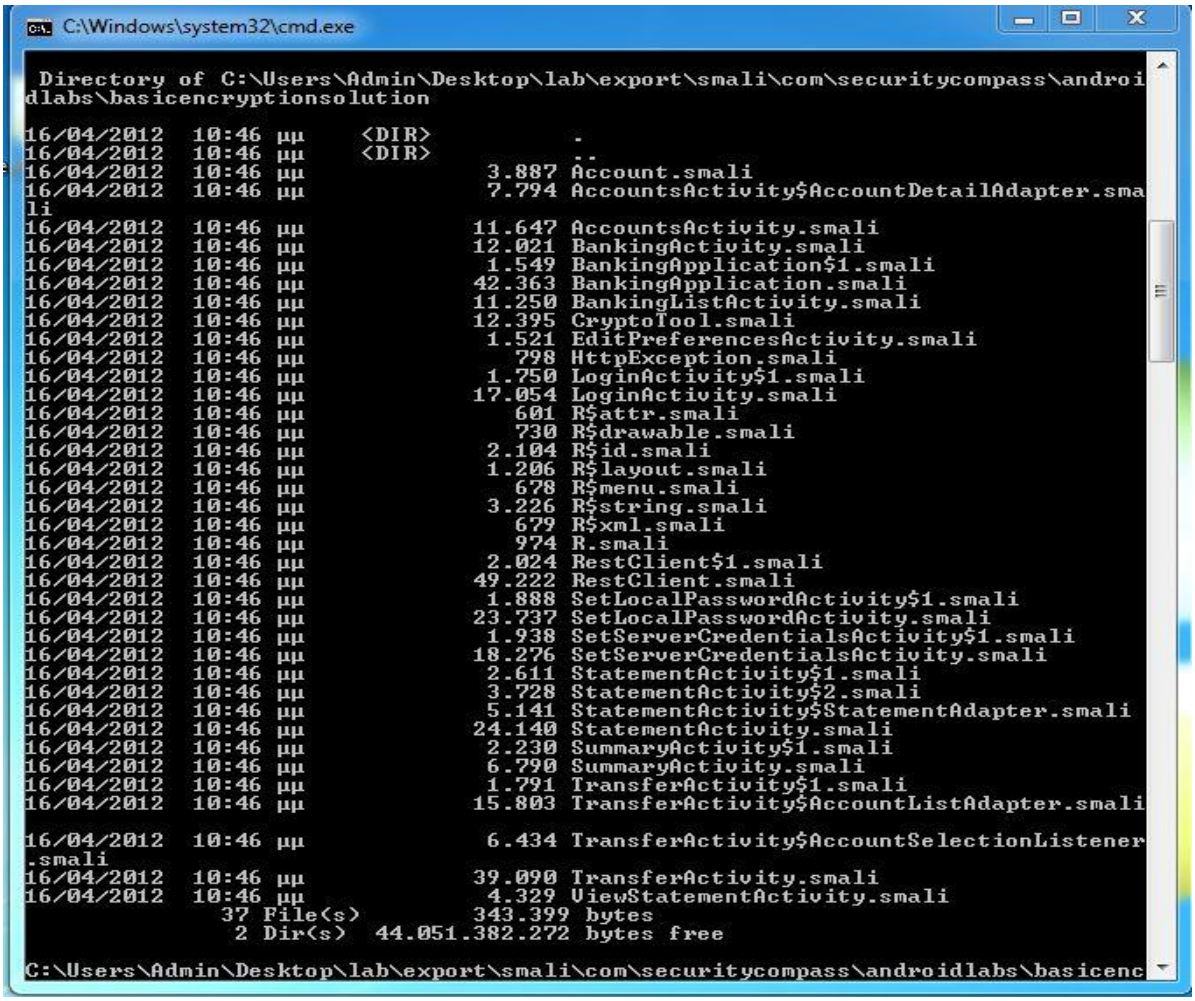
Εκτελούμε ***apktool d BasicEncryption.apk export*** και κάνουμε Export τα αρχεία της εφαρμογής μας. (Εικόνα 66)



Εικόνα 66 - apktool

Στη συνέχεια, πλοηγούμαστε στον κατάλογο *export/smali/ com/securitycompass/androidlabs/ basicencryptionsolution*

και ανακαλύπτουμε ότι υπάρχει ένα αρχείο με το όνομα *cryptotool.smali*. (Εικόνα 67)



Εικόνα 67 - cryptotool.smali

6. Ανοίγουμε το αρχείο *cryptotool.smali* με ένα απλό Notepad και διαπιστώνουμε ότι στην έβδομη σειρά βρίσκεται το κλειδί του AES. (Εικόνα 68).

CryptoTool.smali - Notepad

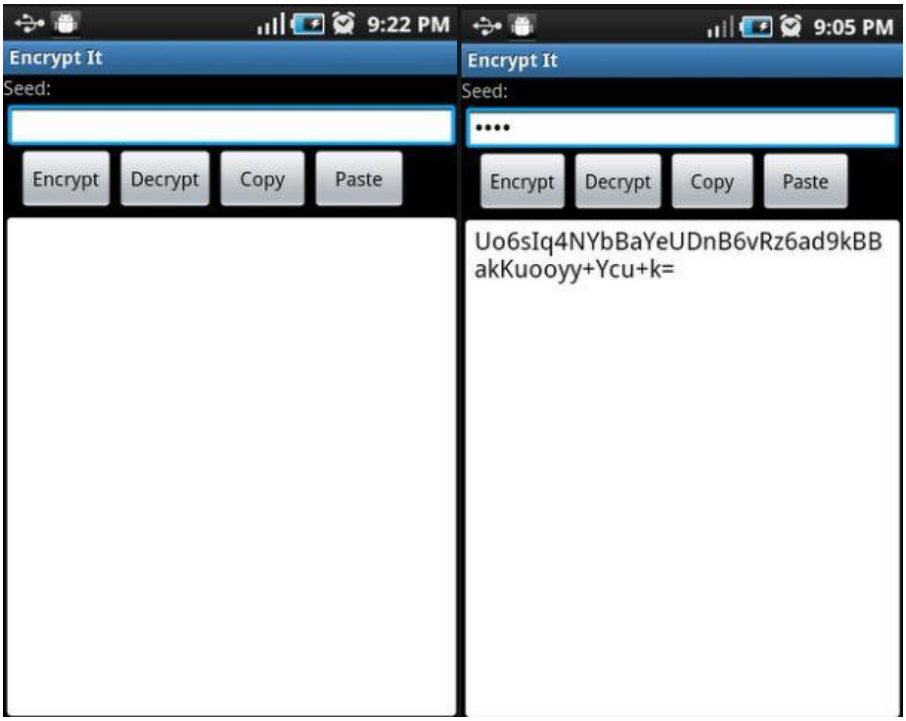
File Edit Format View Help

```
.class public Lcom/securitycompass/androidlabs/basicencryptionsolution/CryptoTool;
.super Ljava/lang/Object;
.source "CryptoTool.java"


# static fields
.field private static final CRYPTO_SPEC:Ljava/lang/String; = "AES/CBC/PKCS5Padding"

.field public static final DEFAULT_B64_KEY_STRING:Ljava/lang/String; = "T0xXpDs1lT9q36aPehvDnaX3EgaFlM4JKIGYvqTqld0="

.field private static final IV_BYTES:I = 0x10

.field private static final KEY_BITS:I = 0x100

.field private static final NUM_ITERATIONS:I = 0x3e8

.field private static final SALT_BYTES:I = 0x20


# direct methods
.method public constructor <init>()V
    .locals 0

    .prologue
    .line 42
    invoke-direct {p0}, Ljava/lang/Object;-><init>()V

    .line 44
    return-void
.end method


# virtual methods
.method public decodeB64(Ljava/lang/String;)[B
    .locals 1
    .parameter "b64String"

    .prologue
    .line 207
    const/4 v0, 0x0

    invoke-static {p1, v0}, Landroid/util/Base64;->decode(Ljava/lang/String;I)[B

    move-result-object v0

    return-object v0
.end method

.method public decryptB64String(Ljava/lang/String;[B[B)Ljava/lang/String;
    .locals 7
    .parameter "ciphertextB64"
    .parameter "key"
    .parameter "iv"
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Ljavax/crypto/NoSuchPaddingException;,
            Ljava/security/NoSuchAlgorithmException;,
            Ljava/security/InvalidAlgorithmParameterException;,
            Ljava/security/InvalidKeyException;,
            Ljavax/crypto/IllegalBlockSizeException;,
            Ljavax/crypto/BadPaddingException;
        }
    .end annotation

    .prologue
    .line 113
    const/4 v6, 0x0
```

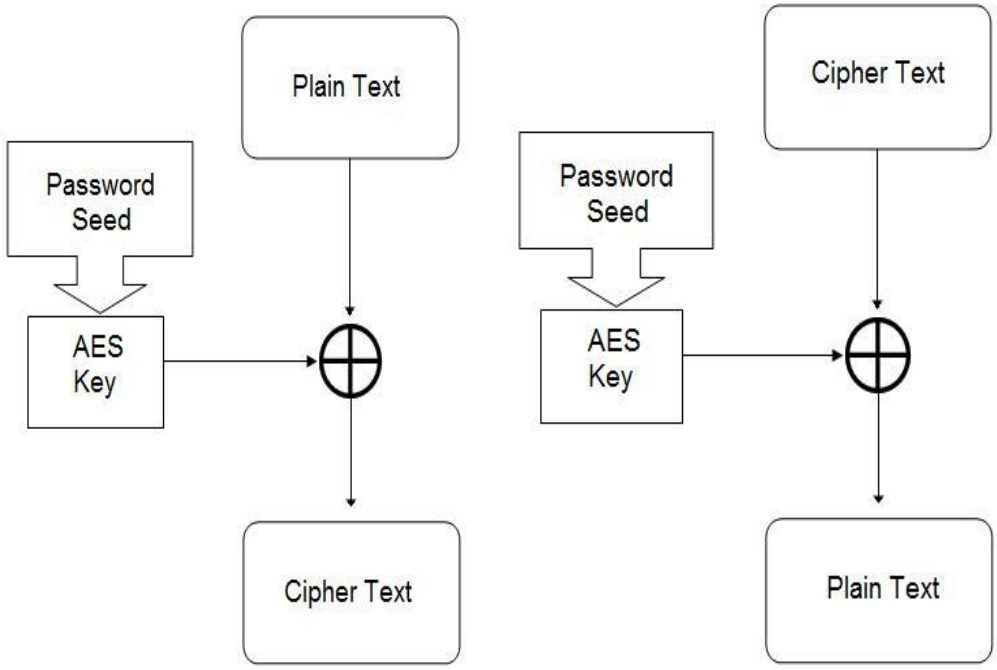
Εικόνα 68 - Εύρεση του κλειδιού

5.3. Εύρεση του Password Seed στην εφαρμογή Encrypt It

Η εφαρμογή Encrypt It κρυπτογραφεί μια συμβολοσειρά με αλγόριθμο AES χρησιμοποιώντας κλειδί μήκους 256bites. Ο χρήστης δίνει ένα αρχικό password, το οποίο αποτελεί το Initialization Vector και τη συμβολοσειρά προς κρυπτογράφηση. Πατώντας το κουμπί Encrypt η εφαρμογή κρυπτογραφεί τη συμβολοσειρά με το κλειδί που έχει δημιουργήσει και πατώντας το Decrypt αποκρυπτογραφεί τη συμβολοσειρά με το ίδιο κλειδί.

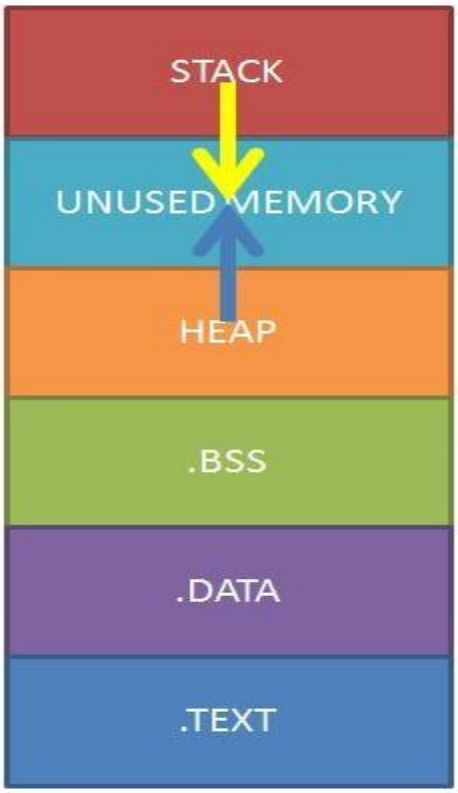


Εικόνα 69 - Η εφαρμογή Encrypt It



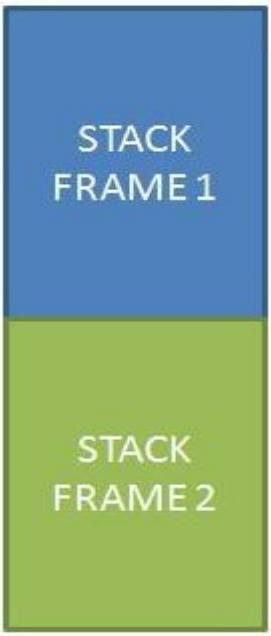
Εικόνα 70 - Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Κάθε διεργασία βρίσκεται στην ίδια εικονική μνήμη. Το λειτουργικό σύστημα δημιουργεί τη ψευδαίσθηση σε κάθε διεργασία ότι βρίσκεται μόνη της στη μνήμη και έχει στη διάθεσή της τους πόρους του συστήματος.



Εικόνα 71 - Η μνήμη της συσκευής

Όταν καλείται μια διεργασία δημιουργείται ένα stack frame. Επειδή όμως το πιο σύνηθες είναι μια διεργασία να καλεί μια άλλη διεργασία, δημιουργούνται πολλά stack frames το ένα κάτω από το άλλο.



Εικόνα 72 - Stack frames στη μνήμη

Παρακάτω φαίνεται η δομή του stack frame. Όταν καλείται η εφαρμογή Encrypt It δημιουργείται ένα stack frame. Δυο από τα ορίσματα της εφαρμογής είναι το Password Seed και η συμβολοσειρά (Plain Text). Καταφέρνοντας με κάποιο τρόπο να διαβάσουμε τα περιεχόμενα της μνήμης τη στιγμή που τρέχει η εφαρμογή, θα προσπαθήσουμε να ανακαλύψουμε το Password Seed.

Εικόνα 73 - Δομή ενός Stack frame

Η συσκευή που χρησιμοποιήθηκε είναι η Sony Ericcson Xperia X8, έχει εργοστασιακά έκδοση Android 2.1 και είναι rooted. Επιλέξαμε να κάνουμε το κινητό τηλέφωνο root για να αποφύγουμε τη διαδικασία απόκτησης δικαιωμάτων administrator σε αυτό με τεχνική privilege escalation. Η χρήση δικαιωμάτων administrator είναι απαραίτητη γιατί διαφορετικά δε θα είχαμε πρόσβαση στις διεργασίες και στη μνήμη που χρησιμοποιούν.

Εγκαθιστούμε στο κινητό την εφαρμογή Encrypt It από το Google Play. Δημιουργήσαμε έναν εικονικό υπολογιστή σε VMware με λειτουργικό Windows XP. Εγκαθιστούμε με τη σειρά:

1) JDK (Java Development Kit)
2) JRE (Java Runtime Environment)
3) Android SDK

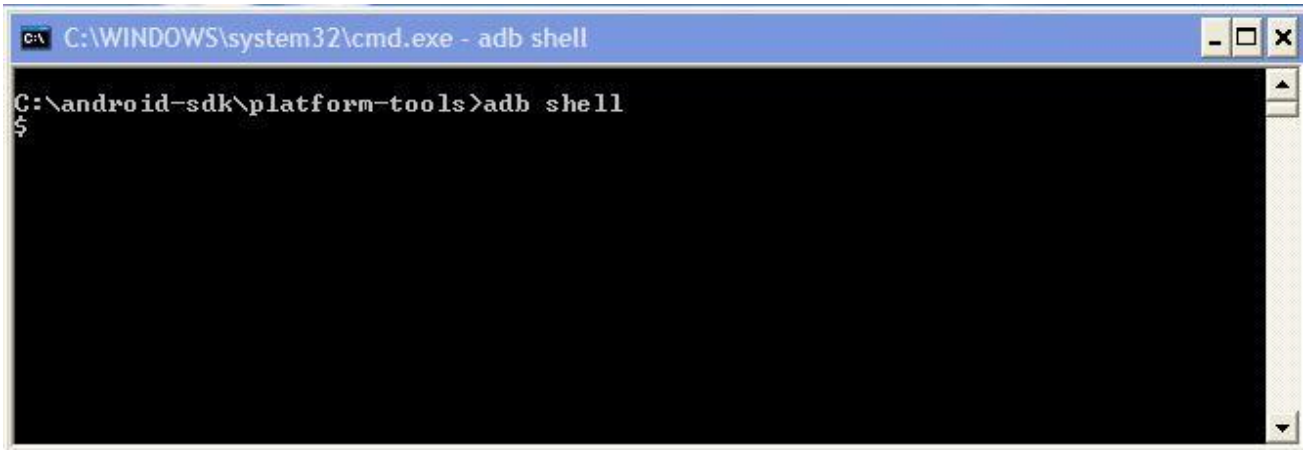
Όταν εγκατασταθεί το SDK πηγαίνουμε στο installation directory. Εγκαθιστούμε το πρόσθετο που αντιστοιχεί στην έκδοση Android του κινητού. Αφού το κινητό έχει Android 2.1 εγκαταστήσαμε τη 2.1 sdk. Συνδέουμε το κινητό με καλώδιο usb και εγκαθιστούμε τους κατάλληλους drivers.

Σε περιβάλλον command prompt χρησιμοποιούμε το εργαλείο ADB. Παρακάτω ακολουθούν βήμα βήμα οι εντολές που χρησιμοποιήσαμε για να φτάσουμε στο στόχο μας, την εύρεση δηλαδή του Password Seed του χρήστη.

1. Εντολή ***adb devices***. Δείχνει ποιες συσκευές είναι συνδεδεμένες με τον υπολογιστή.

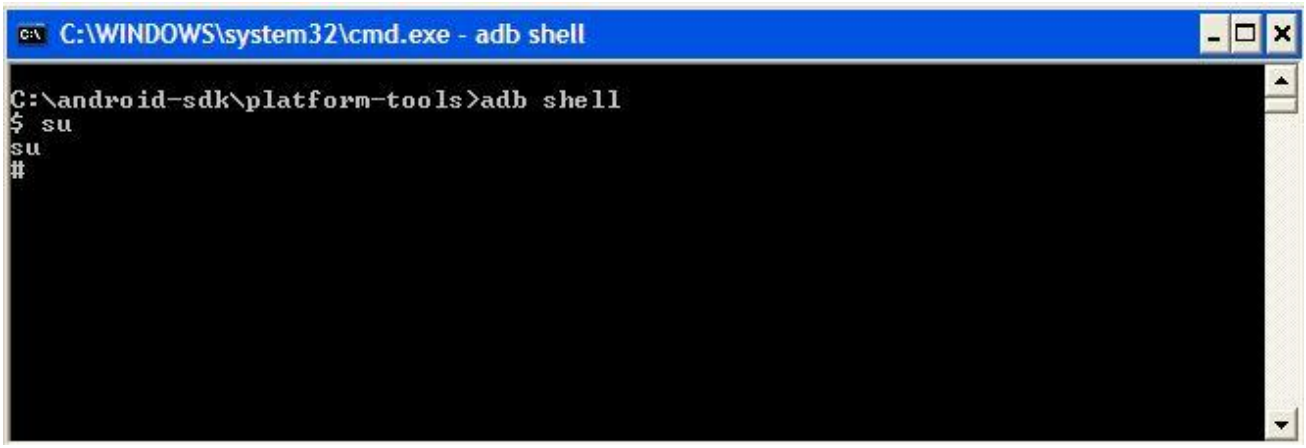
Εικόνα 74 - Συνδεδεμένες συσκευές

2. Εντολή ***adb shell***. Στο περιβάλλον command prompt ανοίγουμε ένα shell και έχουμε πρόσβαση στο κινητό τηλέφωνο.



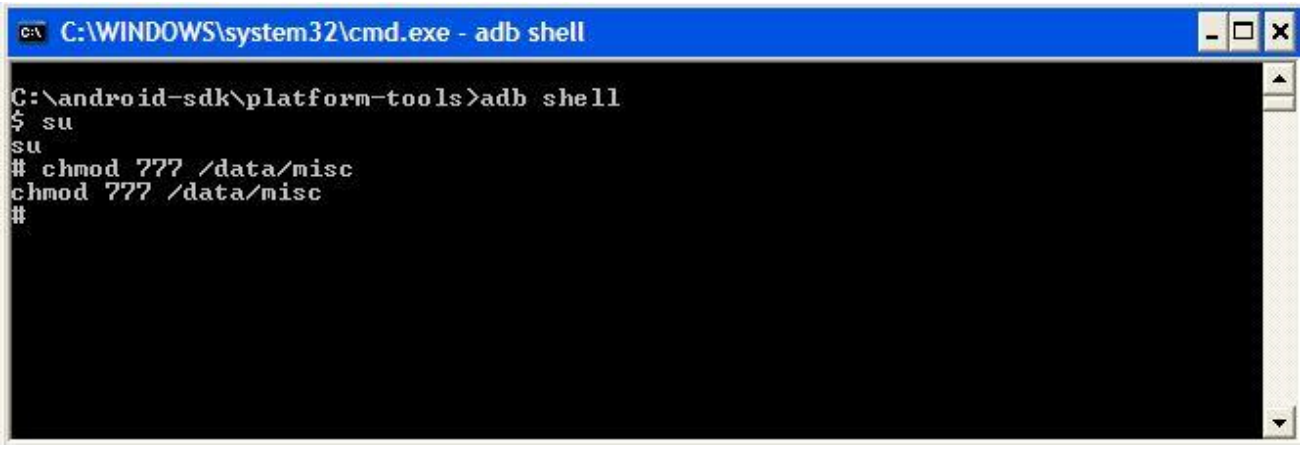
Εικόνα 75 - Shell για πρόσβαση στο κινητό

3.Εντολή ***su***. Αποκτούμε δικαιώματα super user έτσι ώστε να έχουμε τη δυνατότητα να αλλάξουμε δικαιώματα πρόσβασης σε φακέλους και αρχεία.



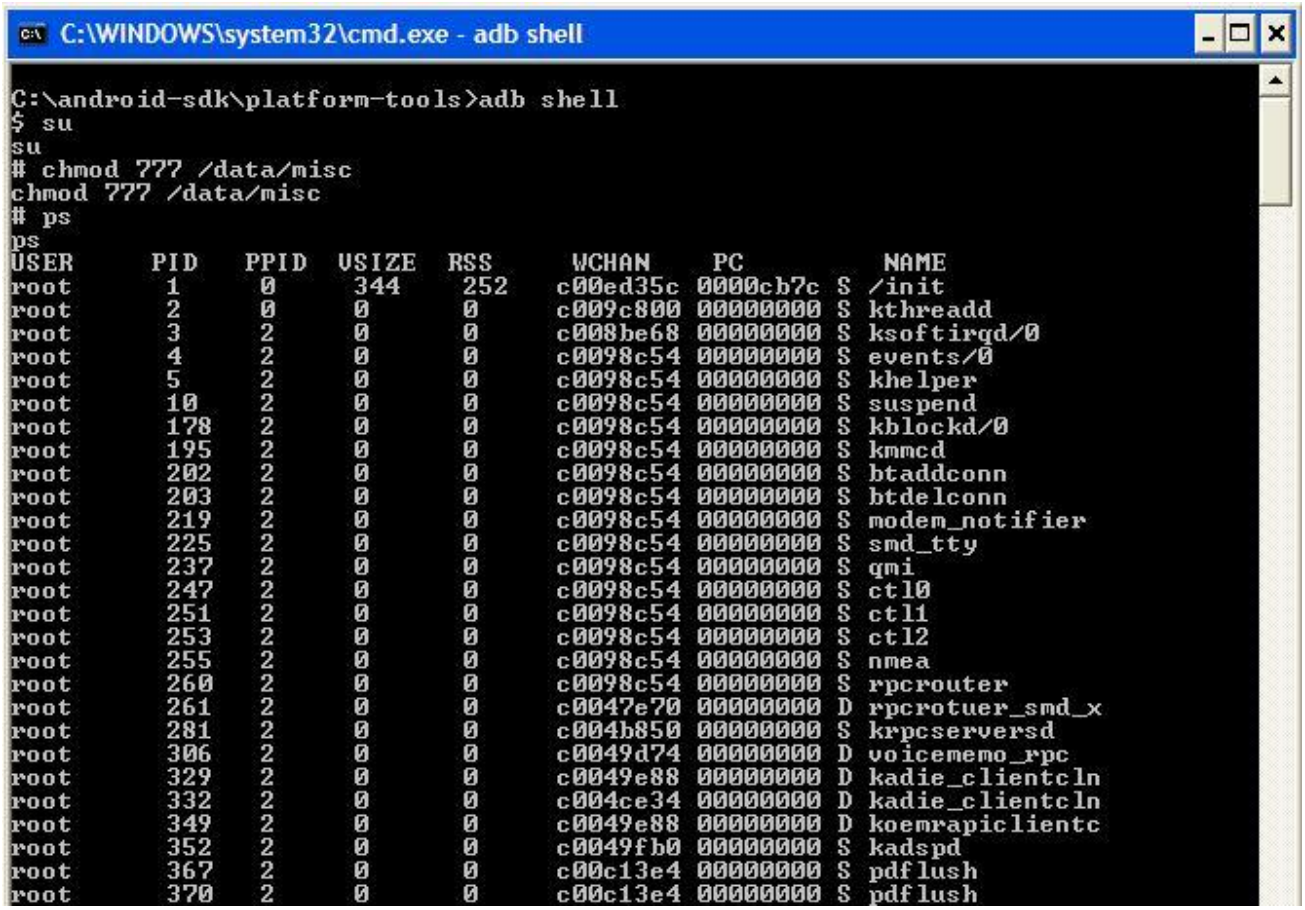
Εικόνα 76 - Απόκτηση προνομίων super user

4. Εντολή ***chmod 777 /data/misc***. Κάνουμε εγγράψιμο το φάκελο /data/misc.



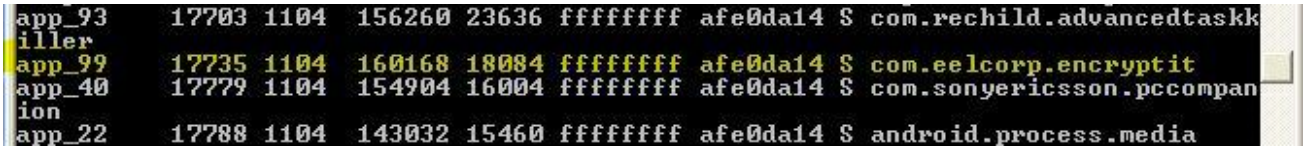
Εικόνα 77 - Αλλαγή στα δικαιώματα προσπέλασης του φακέλου /data/misc

5.Εντολή ***ps***. Εμφανίζει λίστα με τις διεργασίες που εκτελούνται εκείνη τη στιγμή στο κινητό τηλέφωνο. Εντοπίζουμε τη διεργασία Encrypt It Και σημειώνουμε το PID της.



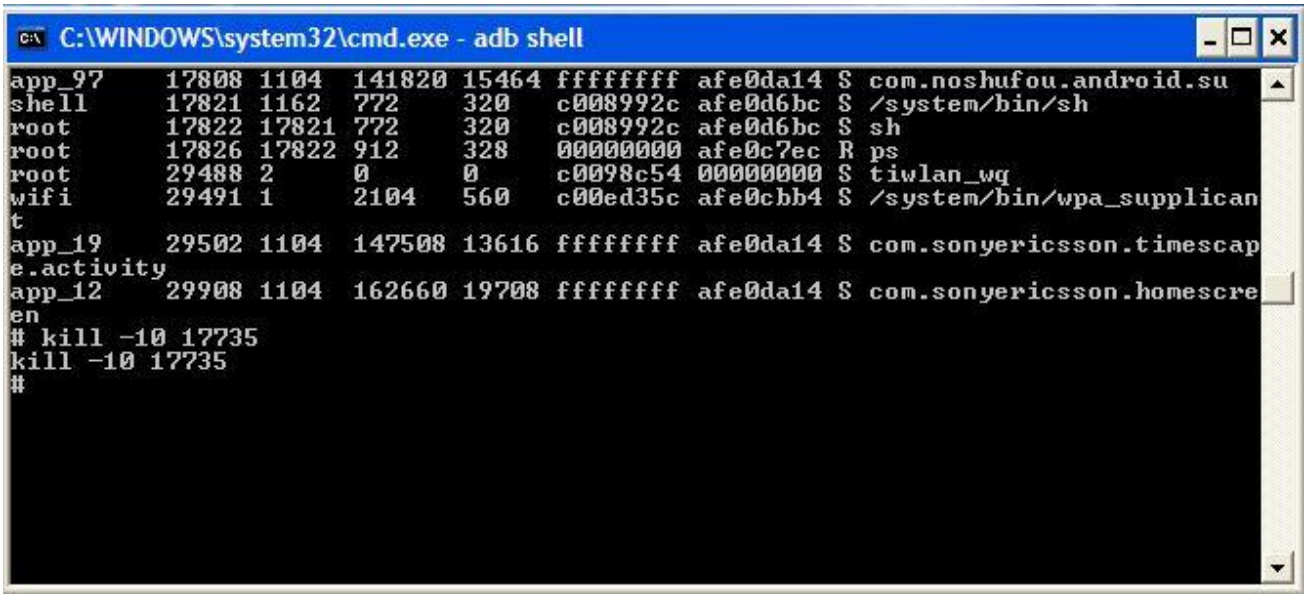
Εικόνα 78 - Η λίστα με τις διεργασίες

6. Εντοπίζουμε την εφαρμογή encrypt it και το PID της.

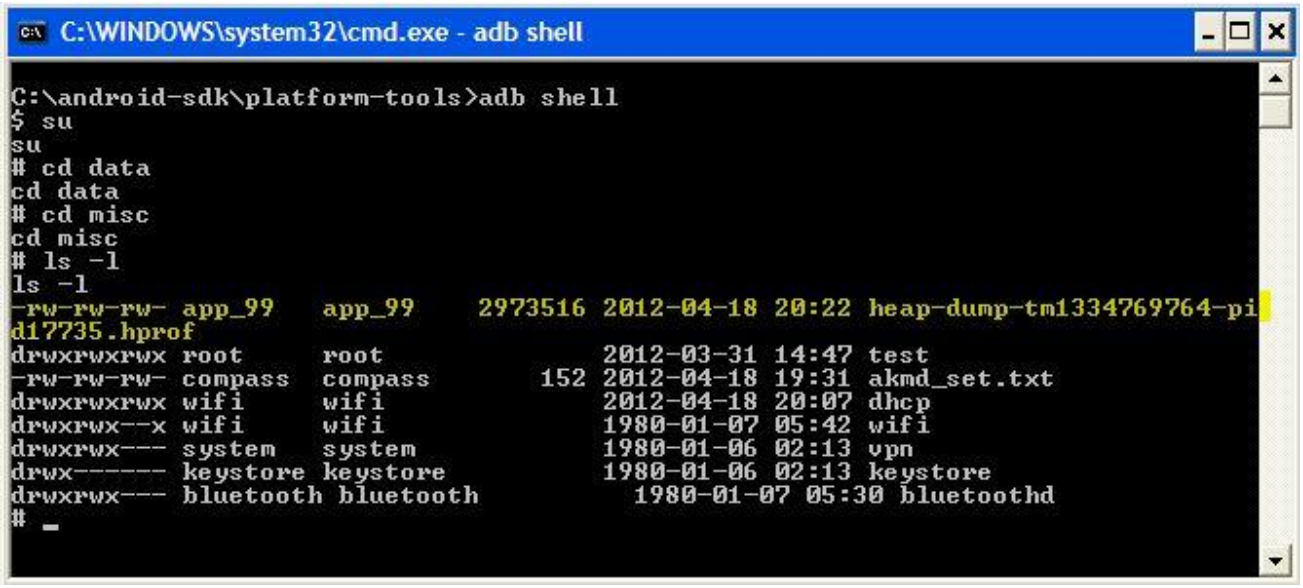


Εικόνα 79 - Εντοπισμός της εφαρμογής Encrypt It

7. Εντολή ***kill -10 17735***. Με την εντολή αυτή γίνεται dump η μνήμη της διεργασίας με αριθμό PID=17735 και δημιουργείται ένα αρχείο .hprof στο φάκελο /data/misc.

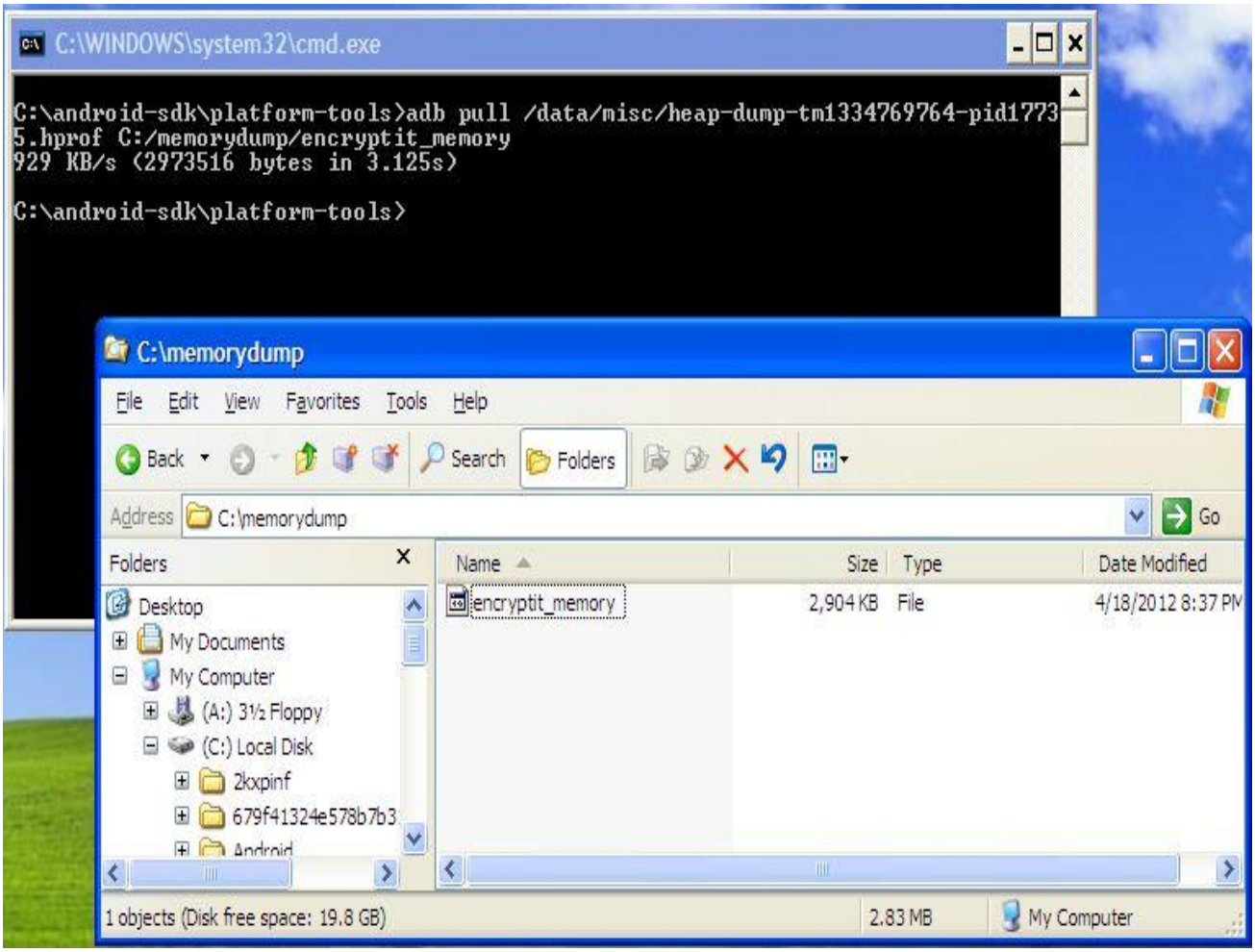


Εικόνα 80 -"Σκοτώνουμε" τη διεργασία και κάνουμε dump τη μνήμη της



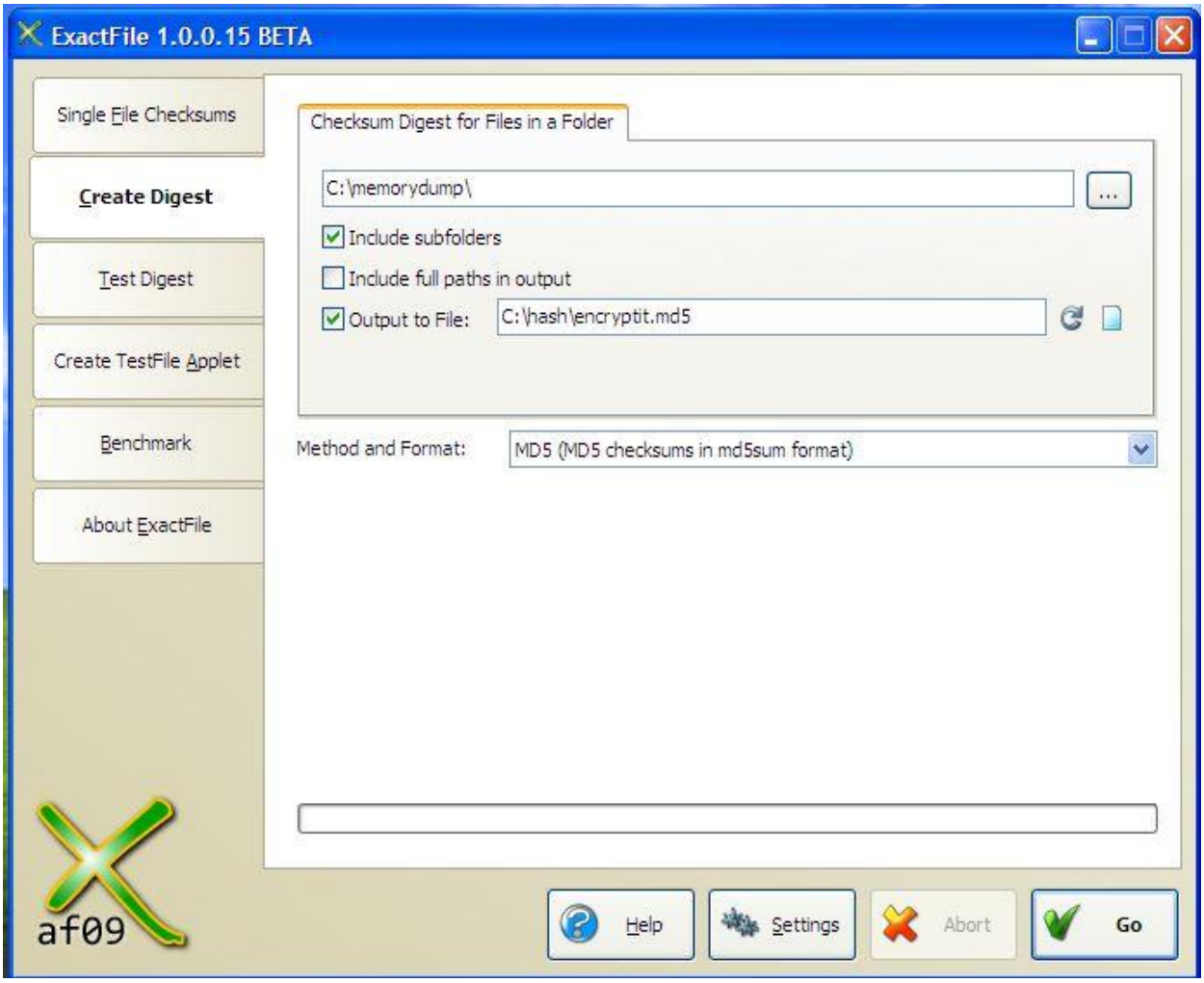
Εικόνα 81 - Το αποτέλεσμα του dump είναι ένα αρχείο στο φάκελο /data/misc

8. Εντολή ***adb pull data/misc/heap-dump-tm1334769764-pid17735.hprof C:/memorydump/encryptit_memory***. Μεταφέρουμε το αρχείο .hprof στο φάκελο c:/memomydump/ του υπολογιστή.

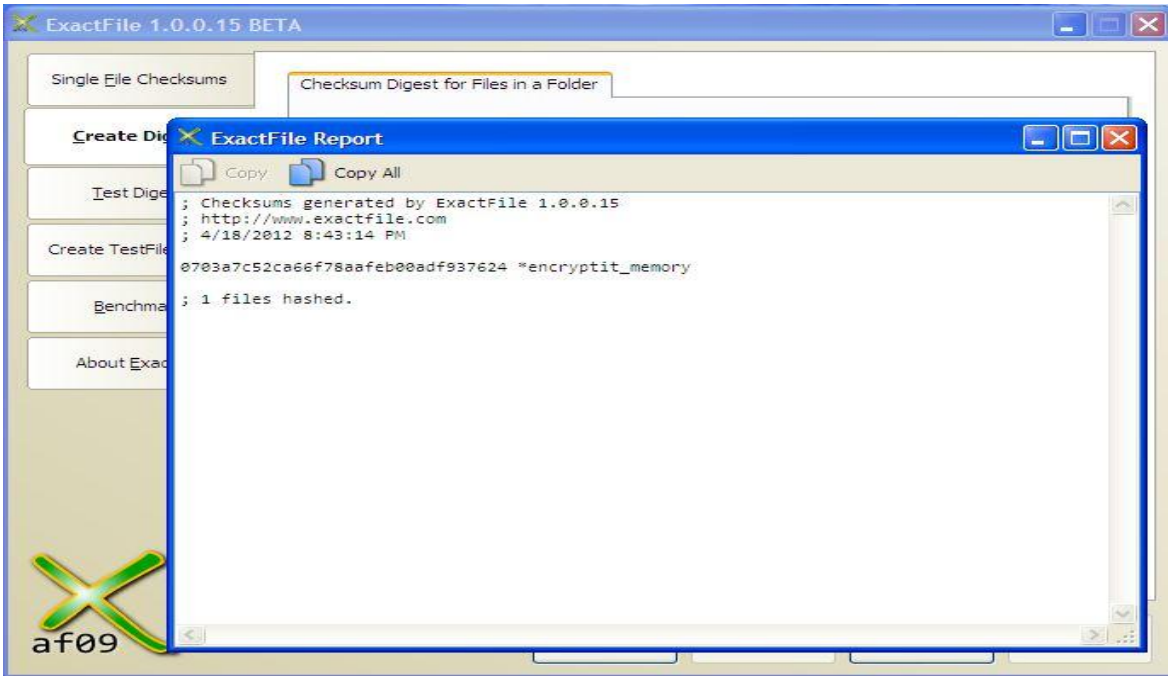


Εικόνα 82 - Μεταφορά του αρχείου στον υπολογιστή

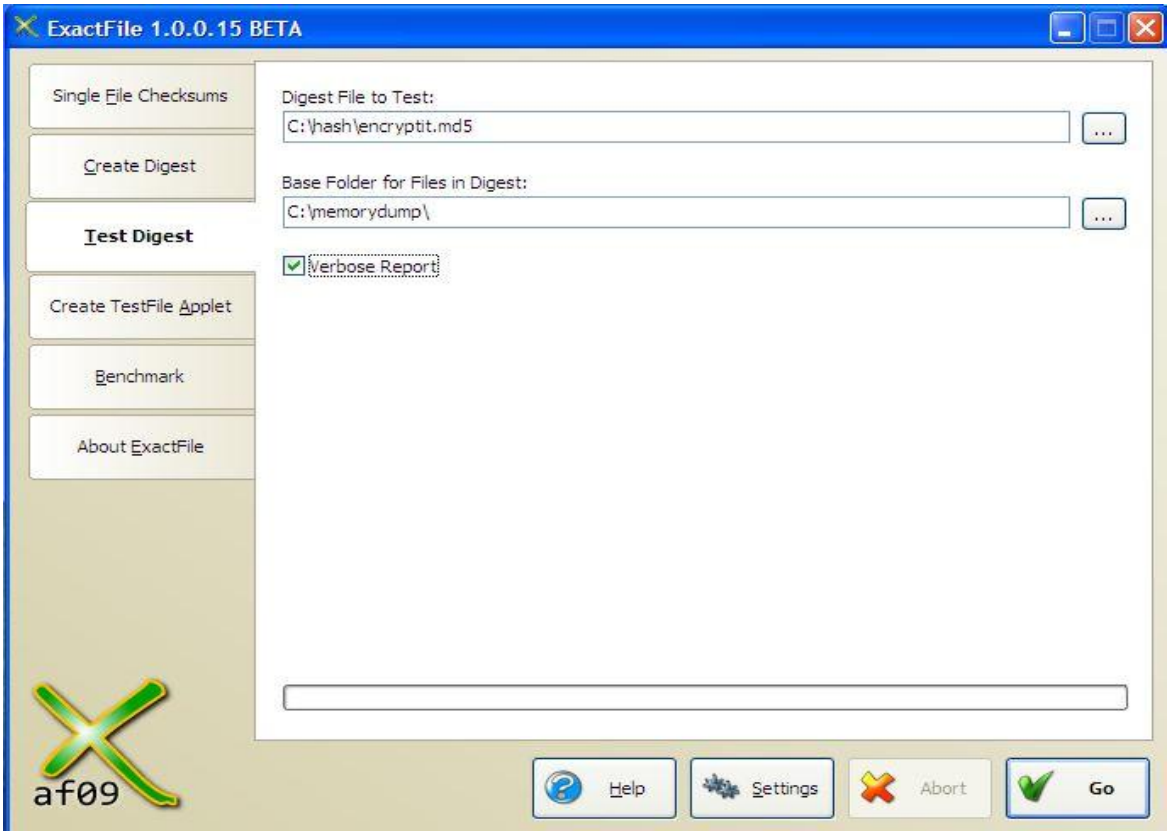
9. Χρησιμοποιώντας το πρόγραμμα **exactfile** δημιουργούμε ένα hash value για το αρχείο encryptit_memory.hprof. Αυτό γίνεται για να εξασφαλίσουμε την ακεραιότητα του αρχείου που συλλέξαμε από το κινητό τηλέφωνο κατά τη διάρκεια της επεξεργασίας και της έρευνας αργότερα.



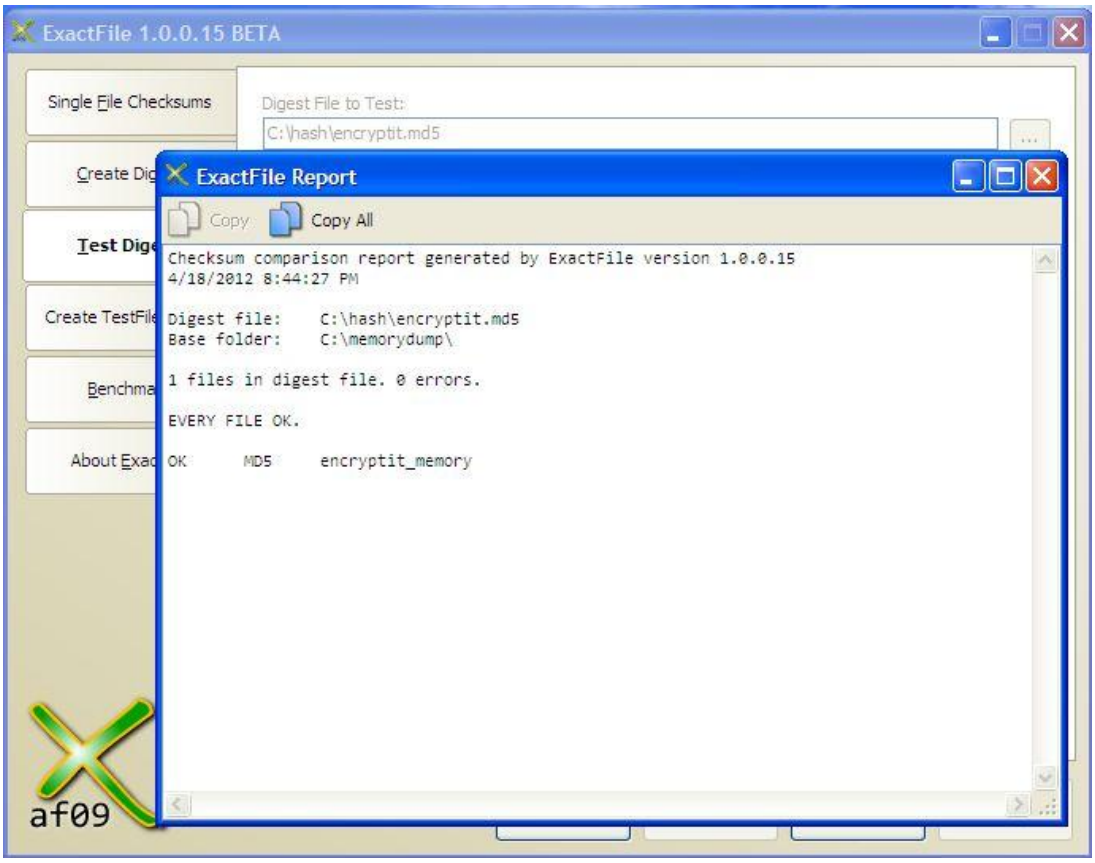
Εικόνα 83 - Δημιουργία MD5 hash value



Εικόνα 84 - Η MD5 hach value του αρχείου

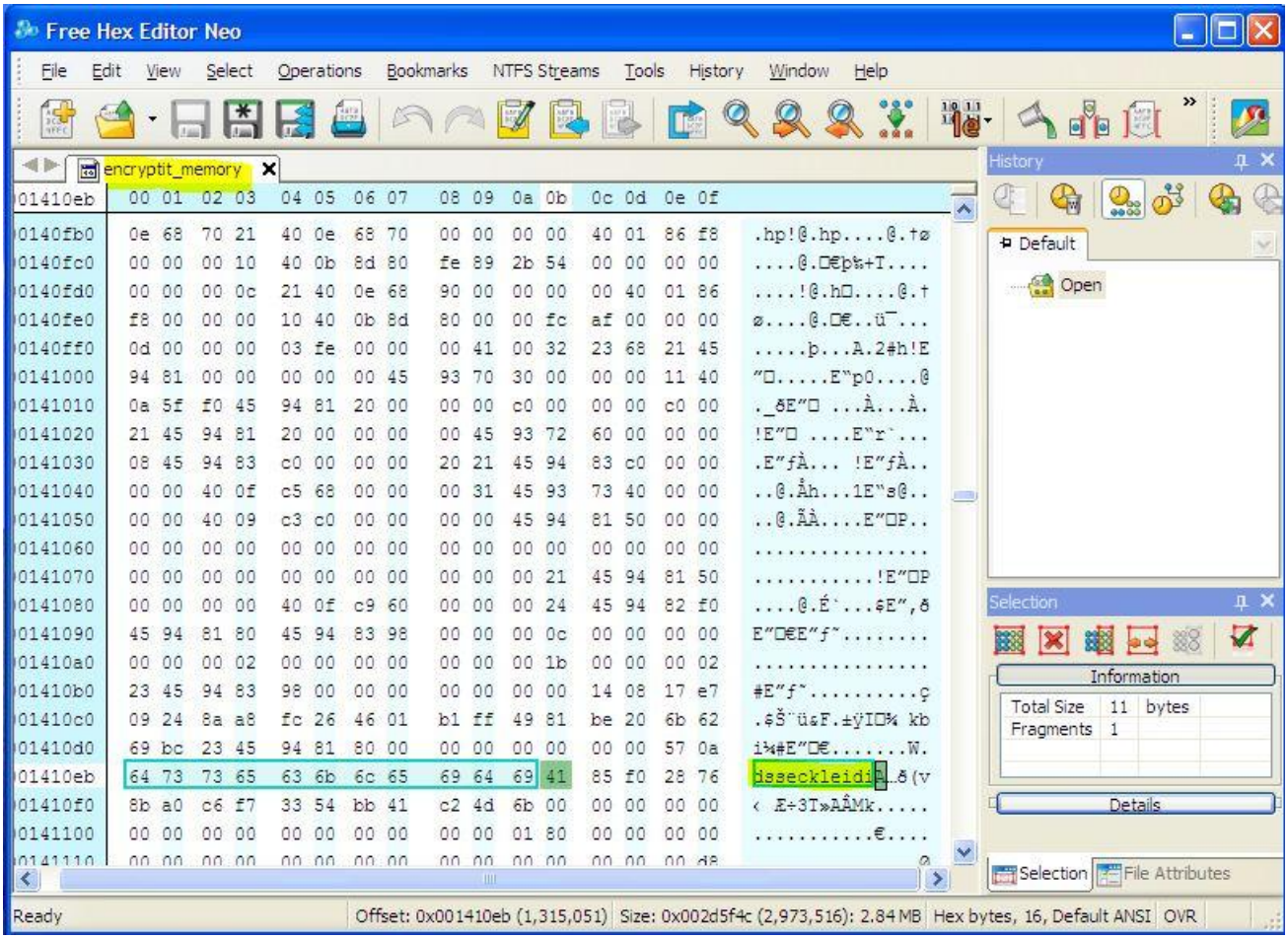


Εικόνα 85 - Επαλήθευση



Εικόνα 86 - Το αρχείο είναι ανέπαφο

10. Χρησιμοποιώντας ένα hex editor ανοίγουμε τα περιεχόμενα του αρχείου encryptit_memory.hprof και μετά από αναζήτηση ανακαλύπτουμε το Password Seed (dsseckleidi) σε μη κρυπτογραφημένη μορφή.



Εικόνα 87 - Αναζήτηση και εύρεση του password seed με τη χρήση hex editor

Οπότε γνωρίζοντας την εφαρμογή, το Password Seed και το Cipher Text μπορούμε να φτάσουμε στο Plain Text.

Συμπεράσματα

Από όλα όσα αναφέρθηκαν στα προηγούμενα κεφάλαια, γίνεται κατανοητό ότι οι φορητές συσκευές έχουν γίνει ένα αναπόσπαστο κομμάτι της καθημερινότητάς μας. Εκατομμύρια Χρήστες κάθε μέρα απολαμβάνουν τις ευκολίες που παρέχουν οι κινητές συσκευές. Η διασκέδαση, η επικοινωνία, οι οικονομικές συναλλαγές και η ενημέρωση είναι μόνο μερικοί από τους τομείς που καλύπτονται από μια τεράστια γκάμα εφαρμογών που είναι διαθέσιμες στην υπηρεσία των χρηστών.

Συνθέτοντας όμως την εικόνα της ραγδαίας ανάπτυξης της σύγχρονης τεχνολογίας ,δεν μπορούμε να παραλείψουμε και την αντίστοιχη αλματώδη εξέλιξη που υπάρχει στον τομέα των κακόβουλων χρηστών και προγραμμάτων. Ολοένα και περισσότεροι εισβολείς προσπαθούν να παραβιάσουν την ασφάλεια και να εισβάλουν απρόσκλητα στην προσωπική μας ζωή. Οι κακόβουλοι χρήστες έχοντας στόχο το προσωπικό κέρδος, εξαπατούν, κλέβουν και καταστρέφουν τα προσωπικά μας δεδομένα .

Καμία εφαρμογή και κανένα λογισμικό δεν πρόκειται ποτέ να παρέχει την απόλυτη ασφάλεια των δεδομένων μας. Χρειάζονται συντονισμένες κινήσεις για να προστατευτούμε. Η καθιέρωση σχετικής νοοτροπίας που δίνει ιδιαίτερη έμφαση στην ασφάλεια λειτουργεί προς την κατεύθυνση αυτή. Στη συνέχεια παραθέτουμε μια σειρά από ενέργειες που μπορεί να καθιερώσει ένας χρήστης ή μια εταιρία στις κινητές συσκευές, ώστε να προστατεύσει τα προσωπικά του δεδομένα από τους κακόβουλους εισβολείς. Σε ατομικό επίπεδο :

1. Αποφύγετε την απάτη των υπερχρεώσεων, ελέγχετε τακτικά το λογαριασμό του τηλεφώνου σας : Διαβάζετε πάντοτε την μηνιαίες καταστάσεις λογαριασμού του τηλέφωνο σας για ύποπτες χρεώσεις. Επικοινωνήστε με το φορέα σας αν έχετε εντοπίσει κάτι που πιστεύεται ότι είναι απάτη.

2. Ελέγξτε ξανά τις διευθύνσεις URL στο κινητό σας: Αφού κάνετε κλικ σε μια σύνδεση στο διαδίκτυο, να δοθεί ιδιαίτερη προσοχή στην διεύθυνση για να βεβαιωθείτε ότι ταιριάζει με την ιστοσελίδα που ισχυρίζεται ότι είναι, ειδικά αν σας ζητηθεί να καταχωρίσετε έναν λογαριασμό ή στοιχεία σύνδεσης.

3. Προστατέψτε τα προσωπικά σας δεδομένα, κατανοήστε την έννοια των δικαιωμάτων που απαιτούν οι εφαρμογές: Να είστε προσεκτικοί σχετικά με τη διαχείριση των αιτήσεων πρόσβασης σε προσωπικές πληροφορίες στο τηλέφωνό σας ή να αφήνετε τις εφαρμογές να έχουν πρόσβαση και να εκτελούν τις λειτουργίες του τηλεφώνου σας. Σιγουρευτείτε και να ελέγχετε τις ρυθμίσεις απορρήτου για κάθε εφαρμογή πριν την εγκαταστήσετε.

4. Να λειτουργείτε έξυπνα σχετικά με τις ρυθμίσεις της συσκευής: Κρατήστε τις συνδέσεις με το δίκτυο, όπως το WiFi, ή το Bluetooth κλειστές, όταν δεν είναι σε χρήση. Να είστε βέβαιοι ότι έχετε απενεργοποιήσει κάποιες ρυθμίσεις, όπως η λειτουργία εντοπισμού σφαλμάτων που μπορεί να ανοίξει στη συσκευή παράνομη πρόσβαση.

5. Εγκαταστήστε μια εφαρμογή ασφαλείας: Κατεβάστε μια εφαρμογή ασφαλείας που σαρώνει τις εφαρμογές που κατεβάζετε για malware και spyware, σας βοηθά να εντοπίσετε ένα χαμένη ή κλεμμένη συσκευής, και σας προστατεύει από επικίνδυνες ιστοσελίδες.

6. Ενημέρωση του τηλεφώνου και των εφαρμογών σας: Σιγουρευτείτε ότι θα κατεβάσετε και θα εγκαταστήσετε τις ενημερωμένες εκδόσεις του λογισμικού που χρησιμοποιεί η συσκευή σας αμέσως μόλις αυτές είναι διαθέσιμες. Το ίδιο ισχύει και για τις εφαρμογές.

Στο επίπεδο μιας εταιρίας:

1. Αύξηση της ευαισθητοποίησης των εργαζομένων: οι εργαζόμενοι πρέπει να κατανοήσουν τις απειλές και τους κινδύνους που υπάρχουν, έτσι ώστε να μπορούν να λαμβάνουν μέτρα προστασίας.

2. Προστατέψτε τα τηλέφωνα των εργαζομένων: Βεβαιωθείτε ότι κάθε τηλέφωνο είναι προστατευμένο με μια εφαρμογή ασφάλειας που εντοπίζει malware, σαρώνει τις εφαρμογές, και έχει την δυνατότητα του εξ αποστάσεως καθαρισμού της συσκευής.

3. Ενημέρωση τρωτών σημείων: Κρατήστε το λειτουργικό σύστημα των συσκευών των εργαζομένων ενημερωμένο και επιτρέψτε τις αυτόματες ενημερώσεις ή να δέχονται ενημερώσεις παροχής υπηρεσιών όταν ερωτηθούν. Να ενημερώνεστε διαρκώς για τα τρωτά σημεία του λογισμικού που δεν έχουν ακόμα επιδιορθωθεί. Τέλος το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας προσφέρει μια βάση δεδομένων των αδυναμιών της κάθε συσκευής.

Πράττοντας τα ανωτέρω ένας χρήστης μπορεί να προστατεύσει τα δεδομένα και την προσωπική του ζωή αποτελεσματικότερα. Δεν είναι κανόνες αλλά πρόκειται για βασικές ενέργειες που πρέπει ένας χρήστης να ενσωματώσει στην καθημερινότητά του ώστε να απολαμβάνει τα πλεονεκτήματα των κινητών συσκευών με ασφάλεια και να κάνει τη ζωή των κακόβουλων εισβολέων δύσκολη.

Βιβλιογραφία

[1] Gartner, Inc., "Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behavior," [Online]. Available: http://www.gartner.com/newsroom/id/2525515. [Accessed 5 06 2013].

[2] Juniper Networks, Inc., "Juniper Networks Third Annual Mobile Threats Report," Juniper Networks, Inc.,USA, 2013.

[3] Wikipedia, "Mobile device," [Online]. Available: https://en.wikipedia.org/wiki/Mobile_device. [Accessed 20 05 2013].

[4] Wikipedia, "Personal digital assistant," [Online]. Available: https://en.wikipedia.org/wiki/Personal_digital_assistant. [Accessed 24 05 2013].

[5] Wikipedia, "Personal navigation assistant," [Online]. Available: http://en.wikipedia.org/wiki/Personal_navigation_assistant. [Accessed 24 05 2013].

[6] Wikipedia, "Smartphone," [Online]. Available: http://en.wikipedia.org/wiki/Smartphone. [Accessed 11 06 2013].

[7] about.com, "What Makes a Smartphone Smart?," [Online]. Available: http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm. [Accessed 28 05 2013].

[8] http://www.boomwala.com, "SmartPhone Features," [Online]. Available: http://www.boomwala.com/2013/04/smartphone-features.html. [Accessed 02 06 2013].

[9] Wikipedia, "Tablet computer," [Online]. Available: http://en.wikipedia.org/wiki/Tablet_computer. [Accessed 05 06 2013].

[10] Wikipedia, "Mobile computing," [Online]. Available: https://en.wikipedia.org/wiki/Mobile_computing. [Accessed 25 05 2013].

[11] IDC, inc, "IDC - Press Release," [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24108913. [Accessed 12 06 2013].

[12] M. C, "Introduction to mobile operating system," [Online]. Available:

http://madhusudhanrc.blogspot.gr/2011/09/android-basic-interview-questions.html.

[13] Wikipedia, "Symbian," [Online]. Available: http://en.wikipedia.org/wiki/Symbian. [Accessed 08 05 2013].

[14] BlackBerry, "Fundamentals of the BlackBerry 10 OS," [Online]. Available: http://developer.blackberry.com/native/documentation/bb10/rtos.html. [Accessed 04 06 2013].

[15] QNX, "QNX Neutrino RTOS Secure Kernel," [Online]. Available: http://www.qnx.com/products/neutrino-rtos/secure-kernel.html. [Accessed 09 06 2013].

[16] K. Drexter, "DEVELOPE IPHONE APPS WITH IOS SYSTEM ARCHITECTURE," [Online]. Available: http://wickeddigital.blogspot.gr/2013/03/explore-ios-sdk-development-kit.html.

[17] Apple Inc, "About the iOS Technologies," [Online]. Available: http://developer.apple.com/library/ios/#documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/Introduction/Introduction.html. [Accessed 02 06 2013].

[18] Wikipedia, "Windows Phone," [Online]. Available: http://en.wikipedia.org/wiki/Windows_Phone. [Accessed 25 06 2013].

[19] Wikipedia, "Hybrid kernel," [Online]. Available: http://en.wikipedia.org/wiki/Hybrid_kernel. [Accessed 09 05 2013].

[20] Wikipedia, "Android (operating system)," [Online]. Available: http://en.wikipedia.org/wiki/Android_%28operating_system%29. [Accessed 05 06 2013].

[21] L. Westaway, "Android updates guide: All the features of every version," [Online]. Available: http://reviews.cnet.co.uk/mobile-phones/android-updates-guide-all-the-features-of-every-version-50003779/. [Accessed 26 06 2013].

[22] Android, "Platform Versions," [Online]. Available: http://developer.android.com/about/dashboards/index.html. [Accessed 28 06 2013].

[23] S. Brähler, Analysis of the Android Architecture, Germany: Karlsruhe Institute of Technology, 2010.

[24] Scriptol.com, "Dalvik, virtual machine of Android," [Online]. Available:

http://www.scriptol.com/programming/dalvik.php. [Accessed 04 06 2013].

[25] B. Anderson "Understanding the Android File Hierarchy" [Online]. Available:

http://www.all-things-android.com/content/understanding-android-file-hierarchy. [Accessed 28 06 2013].

[26] Android, "Android security overview," [Online]. Available: http://source.android.

com/tech/security/index.html. [Accessed 28 06 2013].

[27] A. Hoog, Android Forensics, USA: Syngress, 2011.

[28] Lookout, Inc, "Mobile Threat Report 2011," [Online]. Available: https://www.lookout.com/resources/reports/mobile-threat-report. [Accessed 18 06 2013].

[29] Lookout, Inc, "State of Mobile Security 2012," [Online]. Available: https://www.lookout.com/resources/reports/state-of-mobile-security-2012. [Accessed 07 06 2012].

[30] OWASP, "Top 10 Mobile Risks, Release Candidate v1.0," [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks. [Accessed 01 06 2013].

[31] OWASP, "Insecure Storage," [Online]. Available: https://www.owasp.org/index.php/Insecure_Storage. [Accessed 19 06 2013].

[32] J. Mannino, M. Zusman and L. Zach, "OWASP Top 10 Mobile Risks," [Online]. Available: http://www.slideshare.net/JackMannino/owasp-top-10-mobile-risks. [Accessed 19 06 2013].

[33] M. Backesy, S. Gerling and P. Styp-Rekowsky, A Local Cross-Site Scripting Attack against Android Phones, Germany: Saarland University, 2011.

[34] M. Chalandar, P. Darvish και A. Rahmani, A centralized cookie-based single sign-on in distributed systems, Information and Communications Technology, 2007.

[35] oauth, "Introduction," [Online]. Available: http://oauth.net/about/. [Accessed 30 06 2013].

[36] R. Ayers, "Mobile Device Forensics," [Online]. Available:

http://www.cftt.nist.gov/AAFS-MobileDeviceForensics.pdf. [Accessed 19 02 2013].

[37] D. Apostolopoulos, G. Marinakis, C. Ntantogian and C. Xenakis, Discovering authentication credentials in volatile memory of Android mobile devices, Greece: University of Piraeus, 2012.