



Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Αυτοματοποιημένη συλλογή και ανάλυση Android εφαρμογών από το Google Play Automated collection and analysis Android applications from Google Play
Όνοματεπώνυμο Φοιτητή	Βαρθαλάμης Ευάγγελος
Πατρώνυμο	Αναστάσιος
Αριθμός Μητρώου	ΜΠΣΠ/ 13013
Επιβλέπων	κ. Κωνσταντίνος Πατσάκης Επίκουρος Καθηγητής

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)

(υπογραφή)

(υπογραφή)

Κωνσταντίνος Πατσάκης
Επίκουρος Καθηγητής

Ευθύμιος Αλέπης
Επίκουρος Καθηγητής

Γεώργιος Τσιχριντζής
Καθηγητής

Περίληψη

Από το 1995 άρχισε η ανάπτυξη μιας τεχνολογίας γνωστή ως κινητή τηλεφωνία. Σιγά σιγά κατάφερε και διαδόθηκε τόσο ώστε αναλογούσε μία συσκευή κινητής τηλεφωνίας σε κάθε κάτοικο της Γης. Οι συσκευές αρχικά ήταν ογκώδεις, μεγάλου βάρους και πολύ μικρής μονόχρωμης οθόνης. Ο ανταγωνισμός και η τάση έφεραν πολύ μικρότερες συσκευές ελαφρύτερες και έγχρωμων οθονών. Τα τελευταία χρόνια τα κινητά τηλέφωνα έχουν αντικατασταθεί από τα έξυπνα τηλέφωνα (smartphones) όπου η χρήση τους σαν συσκευές για ομιλία είναι ένα ελάχιστο ποσοστό δυνατοτήτων τους. Πλέον οι συσκευές είναι περισσότερο μικροί υπολογιστές και σε αυτό συνετέλεσε και η ανάπτυξη λειτουργικών όπου έδωσε όλες αυτές τις επιλογές στους χρήστες. Το λειτουργικό που έχει τη μεγαλύτερη ανταπόκριση τόσο στις συσκευές (επιλογή από τους κατασκευαστές) όσο και από τους τελικούς χρήστες είναι το Android της Google. Μαζί με το λειτουργικό αυτό, ξεκίνησε μία νέα προοπτική για τους προγραμματιστές, η ανάπτυξη εφαρμογών για κάθε ανάγκη των χρηστών του Android. Σήμερα έχει δημιουργηθεί ξεχωριστό κομμάτι στο λειτουργικό Android που έχει το όνομα Google Play και είναι το σημείο ανεύρεσης κάθε διαθέσιμης εφαρμογής (δωρεάν ή επί πληρωμής) για κάθε χρήστη με μόνες του υποχρέωσεις να διαθέτει κινητό που να «τρέχει» λειτουργικό της Google (Android) και έναν λογαριασμό gmail.

Εμείς θα κάνουμε λήψη αρκετών εφαρμογών από το Google Play, μαζί με τις πληροφορίες που μεταφέρουν (όγκος, κριτικές, πλήθος λήψεων κλπ) με σκοπό να δείξουμε από τον όγκο δεδομένων σε πόσες απαιτούνται ειδικές εγκρίσεις δικαιωμάτων επί των προσωπικών δεδομένων του χρήστη.

Summary

Since 1995, the development of a technology known as mobile telephony has begun. Slowly it was succeeded and spread so much that it attributed a mobile phone device to every inhabitant of the Earth. The devices were initially bulky, heavyweight and very monochrome. Competition and trend brought much smaller lighter and color monitors. In recent years mobile phones have been replaced by smartphones where their use as speech devices is a minimal percentage of their capabilities. Now the devices are more small computers, and the development of functionalities has also helped to give them all these choices to users. The most responsive operating device (both manufacturers) and end-users is Google's Android. Together with this, it launched a new perspective for developers, developing applications for every need of Android users. Today, a separate piece has been created in the Android operating system that has the Google Play name and is the point of finding any available app (free or paid) for each user in his own right to have a mobile running Google (Android) and a gmail account.

We will download several apps from Google Play along with the information they carry (volume, reviews, downloads, etc.) in order to show from the amount of data how much specific permissions are required on the user's personal data.

1 Ιστορικά στοιχεία

Το **smartphone** ή με τον ελληνικό όρο **έξυπνο τηλέφωνο**, είναι ένα κινητό τηλέφωνο βασισμένο σε ένα λειτουργικό σύστημα κινητής τηλεφωνίας με περισσότερο προηγμένη υπολογιστική ικανότητα και συνδεσιμότητα σε σχέση με ένα συμβατικό κινητό τηλέφωνο. Τα πρώτα smartphones συνδύαζαν τις λειτουργίες ενός προσωπικού ψηφιακού βοηθού (PDA) και ενός κινητού τηλεφώνου. Σε μεταγενέστερα μοντέλα προστέθηκαν οι λειτουργίες των φορητών media players, low-end compact ψηφιακές φωτογραφικές μηχανές, βιντεοκάμερες τσέπης, καθώς και μονάδες πλοήγησης GPS, με αποτέλεσμα την διαμόρφωση μιας πολυχρηστικής συσκευής. Πολλά σύγχρονα smartphones περιλαμβάνουν επίσης οθόνες αφής υψηλής ανάλυσης και web browsers που εμφανίζουν τυποποιημένες ιστοσελίδες, καθώς και βελτιστοποιημένες ιστοσελίδες για κινητά. Η πρόσβαση σε δεδομένα υψηλής ταχύτητας παρέχεται μέσω Wi-Fi και μέσω κινητών ευρυζωνικών υπηρεσιών. Τα τελευταία χρόνια, η ταχεία ανάπτυξη στην αγορά των εφαρμογών για κινητά και στο εμπόριο κινητών τηλεφώνων έχει γίνει οδηγός για την ευρεία υιοθέτηση των smartphones.

Τα λειτουργικά συστήματα (OS) των κινητών τηλεφώνων που χρησιμοποιούνται από τα σύγχρονα smartphones περιλαμβάνουν, μεταξύ άλλων, το Android της Google το IOS της Apple, το Symbian της Nokia το BlackBerry OS της RIM, το Bada της Samsung, τα Windows Phone της Microsoft το web OS της Hewlett-Packard καθώς και ενσωματωμένες διανομές Linux όπως το Maemo και το MeeGo. Τέτοιου είδους λειτουργικά συστήματα μπορούν να εγκατασταθούν σε πολλά διαφορετικά μοντέλα κινητών τηλεφώνων και συνήθως κάθε συσκευή μπορεί να λάβει πολλές ενημερωμένες εκδόσεις λογισμικού λειτουργικού συστήματος κατά τη διάρκεια ζωής της. Μερικά άλλα επερχόμενα λειτουργικά συστήματα είναι το Firefox OS της Mozilla, το Ubuntu Phone της Canonical Ltd's και το Tizen.

1.2 Λειτουργικό Σύστημα Android

Το **Android** είναι λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας (smartphones) το οποίο τρέχει τον πυρήνα του λειτουργικού Linux. Αρχικά αναπτύχθηκε από την Google και αργότερα από την Open Handset Alliance. Επιτρέπει στους κατασκευαστές λογισμικού να συνθέτουν κώδικα με την χρήση της γλώσσας προγραμματισμού Java, ελέγχοντας την συσκευή μέσω βιβλιοθηκών λογισμικού ανεπτυγμένων από την Google. Το Android είναι κατά κύριο λόγο σχεδιασμένο για συσκευές με Οθόνη αφής όπως τα έξυπνα τηλέφωνα και τα τάμπλετ, με διαφορετικό περιβάλλον χρήσης για τηλεοράσεις (Android TV), αυτοκίνητα (Android Auto) και ρολόγια χειρός (Android Wear). Παρόλο που έχει αναπτυχθεί για συσκευές με οθόνη αφής, έχει χρησιμοποιηθεί σε κονσόλες παιχνιδιών, ψηφιακές φωτογραφικές μηχανές, συνηθισμένους Η/Υ (π.χ. το HP Slate 21) και σε άλλες ηλεκτρονικές συσκευές.

Το Android είναι το πιο ευρέως διαδεδομένο λογισμικό στον κόσμο. Οι συσκευές με Android έχουν περισσότερες πωλήσεις από όλες τις συσκευές Windows, iOS και MacOS X μαζί.

Η πρώτη παρουσίαση της πλατφόρμας Android έγινε στις 5 Νοεμβρίου 2007, παράλληλα με την ανακοίνωση της ίδρυσης του οργανισμού Open Handset Alliance, μιας κοινοπραξίας 48 τηλεπικοινωνιακών εταιριών, εταιριών λογισμικού καθώς και κατασκευής hardware, οι οποίες είναι αφιερωμένες στην ανάπτυξη και εξέλιξη ανοιχτών προτύπων στις συσκευές κινητής τηλεφωνίας. Η Google δημοσίευσε το μεγαλύτερο μέρος του κώδικα του Android υπό τους όρους της Apache Licence, μιας ελεύθερης άδειας λογισμικού. Το λογότυπο για το λειτουργικό

σύστημα Android είναι ένα ρομπότ σε χρώμα πράσινου μήλου και σχεδιάστηκε από τη γραφίστρια Ιρίνα Μπλόκ.

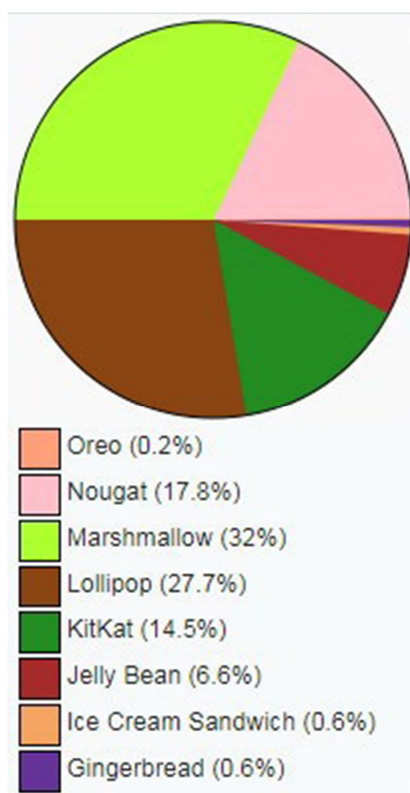
Η τελευταία έκδοση καλείται Android 8.0 Nougat και φέρνει σημαντικές αλλαγές.

1.3 Ιστορικό Ενημερώσεων

Παρόλο που το Android είναι ένα προϊόν ελεύθερου λογισμικού, ένα κομμάτι της ανάπτυξης του λογισμικού συνεχίζεται σε ιδιωτικό παρακλάδι. Για να έρθει αυτό το λογισμικό σε κοινή θέαση δημιουργήθηκε ένα παρακλάδι του μόνο ανάγνωσης, εν ονόματι "Cupcake". Το Cupcake συνήθως συγχέεται με τον τίτλο μιας ενημέρωσης, σε αντίθεση με όσα δηλώνει η ίδια η Google στην ιστοσελίδα ανάπτυξης του Android: "το Cupcake αποτελεί ακόμη ένα έργο σε εξέλιξη, όχι μια επίσημη έκδοση." Αξιοσημείωτες αλλαγές στο λειτουργικό Android θα παρουσιαστούν στο cupcake και περιλαμβάνουν αλλαγές στο σύστημα διαχείρισης των μεταφορτώσεων (download manager), το framework, Bluetooth, το λογισμικό συστήματος, το ραδιόφωνο και το σύστημα τηλεφωνίας, εργαλεία προγραμματισμού, το κυρίως σύστημα και διάφορες εφαρμογές, καθώς και πληθώρες διορθώσεις σφαλμάτων.

Στις 30 Απριλίου 2009, κυκλοφόρησε η επίσημη ενημέρωση έκδοσης 1.5 για το Android. Αποτελείται από πολλά νέα χαρακτηριστικά και βελτιώσεις στο γραφικό περιβάλλον:

- Δυνατότητα καταγραφής κινούμενης εικόνας με την χρήση της αντίστοιχης λειτουργίας του τηλεφώνου.
- Μεταφόρτωση αρχείων βίντεο στο YouTube και εικόνων στο Picasa κατευθείαν από το τηλέφωνο.
- Επανασχεδιασμένο λογισμικό πληκτρολογίου με λειτουργία αυτόματης συμπλήρωσης κειμένου.
- Δυνατότητα αυτόματης σύνδεσης ασύρματης συσκευής ακουστικού Bluetooth εφόσον εντοπιστεί σε μια συγκεκριμένη απόσταση.
- Νέα widgets και φάκελοι που μπορούν να τοποθετηθούν στην επιφάνεια εργασίας.
- Εφέ αλλαγής οθονών και μενού.
- Διευρυμένη λειτουργία αντιγραφής/επικόλλησης για να περιλαμβάνει δικτυακές διευθύνσεις.



Διάγραμμα 1 χρήσης εκδόσεων Android από τις συσκευές Smartphones

Από την πρώτη ημερομηνία έκδοσης του λειτουργικού Android στις 15 Σεπτεμβρίου 2009 στον παρακάτω πίνακα φαίνεται η εξέλιξη του μέχρι την τελευταία έκδοση 8.0. Η εξέλιξη του λειτουργικού έφερε βέβαια και προβλήματα αυξάνοντας τις απαιτήσεις των συσκευών που έκαναν χρήση του λειτουργικού αυτού. Οι αλλαγές ήταν πολλές πάντα με απώτερο σκοπό και στόχο την ευκολία του χρήστη έχοντας ως αποτέλεσμα την κάλυψη ακόμα μεγαλύτερου μεριδίου στην αγορά των κινητών τελευταίας τεχνολογίας smartphone. Μαζί με την εξέλιξη του λειτουργικού αναγκαστικά εξελίχθηκαν και οι εφαρμογές οι οποίες ακολούθησαν από την πρώτη έκδοση του λειτουργικού Android.

Οι εφαρμογές έπρεπε να εξελιχθούν και να βγάζουν καινούριες εκδόσεις ώστε να ακολουθούν το λειτουργικό προκειμένου να είναι δυνατή η λειτουργία τους. Οι ονομασίες των εκδόσεων του λειτουργικού έχουν σχέση πάντα με γλυκό αφήνοντας πάντα μία απορία για τον τρόπο εξεύρεσής τους.

Η αύξηση των απαιτήσεων αναγκάζει τους χρήστες σε αγορά νέων συσκευών δίνοντας μεγάλο μερίδιο στην αγορά ηλεκτρονικών συσκευών σε εταιρείες όπου κάνουν την εξέλιξη των συσκευών αγώνα δρόμου.

Έκδοση :	Κωδική Ονομασία :	Ημερομηνία	API level :	Διανομή
8.1	Oreo		27	
8.0		21 Αυγούστου 2017	26	0.2%

Έκδοση :	Κωδική Ονομασία :	Ημερομηνία	API level :	Διανομή
7.1	Nougat	4 Οκτωβρίου 2016	25	2.0%
7.0		22 Αυγούστου 2016	24	15.8%
6.0	Marshmallow	5 Οκτωβρίου 2015	23	32.0%
5.1	Lollipop	9 Μαρτίου 2015	22	21.0%
5.0		3 Νοεμβρίου 2014	21	6.7%
4.4	KitKat	31 Οκτωβρίου 2013	19	14.5%
4.3	Jelly Bean	24 Ιουλίου 2013	18	1.0%
4.2		13 Νοεμβρίου 2012	17	3.3%
4.1		9 Ιουλίου 2012	16	2.3%
4.0	Ice Cream Sandwich	16 Δεκεμβρίου 2011	15	0.6%
3.2	Honeycomb	15 Ιουλίου 2011	13	0%
2.3	Gingerbread	9 Φεβρουαρίου 2011	10	0.6%
2.2	Froyo	20 Μαΐου 2010	8	0%
2.0	Eclair	26 Οκτωβρίου 2009	7	-
1.6	Donut	15 Σεπτεμβρίου 2009	4	-

Πίνακας 1 εξέλιξης εκδόσεων Android

Το λειτουργικό android κατά την πρώτη εγκατάσταση σε κάθε συσκευή απαιτεί από τον χρήστη του την αποδοχή των όρων χρήσης του android προκειμένου να μπορέσει ο χρήστης να το χρησιμοποιήσει. Αυτό έφερε αλλαγές και στις εφαρμογές όπου μετά τις πρώτες τους εκδόσεις έφεραν την απαίτηση έγκρισης δικαιωμάτων.

Τα δικαιώματα αυτά και ο τρόπος που αυτά χρησιμοποιούνται έχουν γίνει αντικείμενο μελέτης πολλών ερευνητών κυρίως ως προς τον τρόπο που αυτά «επεμβαίνουν» στα δεδομένα της συσκευής μιας και αυτά είναι πολλές φορές προσωπικά.

2. Μια διαχρονική μελέτη της εφαρμογής Χρήση άδειας μέσω του Google Play Store των Vincent F. Taylor - Ivan Martinovic

2.1 Εισαγωγή

Το Android είναι το πιο δημοφιλές λειτουργικό σύστημα κινητής τηλεφωνίας με μερίδιο αγοράς 84,7% από το τρίτο τρίμηνο του 2015, υπερβαίνοντας το πλησιέστερο λειτουργικό iOS, με ποσοστό 13,1%. Αυτή η κυριαρχία τροφοδοτείται από μια μυριάδα προγραμματιστών εφαρμογών, συσκευών και καταναλωτών που υπάρχουν σε μια συμβιωτική σχέση γνωστή ως το οικοσύστημα Android. Ο Nielson αναφέρει ότι ο μέσος καταναλωτής χρησιμοποιεί πάνω από 26 διαφορετικές εφαρμογές ανά μήνα, ξοδεύοντας χρόνο περισσότερο από μία ώρα ανά ημέρα. Αυτή η έκρηξη στη χρήση smartphone έχει τροφοδοτηθεί, εν μέρει, από την ευκολία με την οποία οι τελικοί χρήστες μπορούν να αποκτήσουν εφαρμογές τρίτων μερών για να επεκτείνουν τη λειτουργικότητα των συσκευών τους. Οι αγορές εφαρμογών βρίσκονται στο επίκεντρο του οικοσυστήματος, λειτουργούν ως αποθήκες για πληθώρα εφαρμογών και παρέχουν βολικές δυνατότητες αναζήτησης και λήψης για να ικανοποιήσουν την όρεξη των καταναλωτών. Το Google Play Store είναι η μεγαλύτερη αγορά Android που μπορεί να υπερηφανεύεται για περισσότερες από 1.600.000 εφαρμογές.

Οι προγραμματιστές εφαρμογών δημιουργούν εφαρμογές και τις διαθέτουν είτε δωρεάν είτε επί πληρωμή. Οι δωρεάν εφαρμογές συνήθως περιέχουν διαφημίσεις για δημιουργία εσόδων, ενώ οι εφαρμογές που καταβάλλονται έχουν μια αρχική χρέωση που πρέπει να καταβληθεί στον προγραμματιστή, πριν να καταστεί δυνατή η χρήση της εφαρμογής αφού την κάνει λήψη. Για την προβολή διαφημίσεων (διαφημίσεων), οι εφαρμογές συνήθως περιλαμβάνουν βιβλιοθήκες διαφημίσεων, οι οποίες λαμβάνουν και προβάλλουν διαφημίσεις. Για τη μέγιστη δημιουργία εσόδων, οι διαφημίσεις στοχεύουν σε συγκεκριμένο χρήστη με βάση τις δημογραφικές πληροφορίες και τα ενδιαφέροντά του. Έτσι, οι εφαρμογές με πιο ευαίσθητη πρόσβαση στα δεδομένα ενός χρήστη μπορεί να είναι πιο κερδοφόρες για τους προγραμματιστές εφαρμογών, καθώς μπορούν να αξιοποιήσουν αυτά τα πρόσθετα δεδομένα για να βελτιώσουν το προφίλ των χρηστών και να πουλήσουν τα δεδομένα τους σε τρίτους.

2.2 Πρόβλημα Πεδίο εφαρμογής.

Το Android OS υιοθετεί μια προσέγγιση βασισμένη σε άδειες για την προστασία της πρόσβασης σε δεδομένα ιδιωτών χρηστών και σε ευαίσθητα API.

Υπάρχουν άδειες που χαρακτηρίζονται ως επικίνδυνες, δηλαδή εκείνες οι άδειες που προστατεύουν την πρόσβαση στα εμπιστευτικά δεδομένα ενός χρήστη.

Για το λόγο αυτό, εφεξής αναφερόμαστε σε επικίνδυνες άδειες ως απλά δικαιώματα. Τα δικαιώματα που απαιτούνται από μια εφαρμογή συνήθως σχετίζονται με την παροχή της λειτουργικότητας της εφαρμογής, αλλά κάποιες εφαρμογές είναι σκόπιμα υπερβολικά προνομιακές για να διευκολύνουν τη μεγαλύτερη πρόσβαση στα προσωπικά δεδομένα ενός χρήστη. Οι υπερβολικά προνομιούχες εφαρμογές απειλούν την ιδιωτική ζωή, ζητώντας

δικαιώματα πέραν των απαιτούμενων για λειτουργικότητα εφαρμογών και μπορεί επίσης να αποτελέσουν απειλή για την ασφάλεια σε περιπτώσεις όπως μια μπερδεμένη υποτακτική επίθεση.

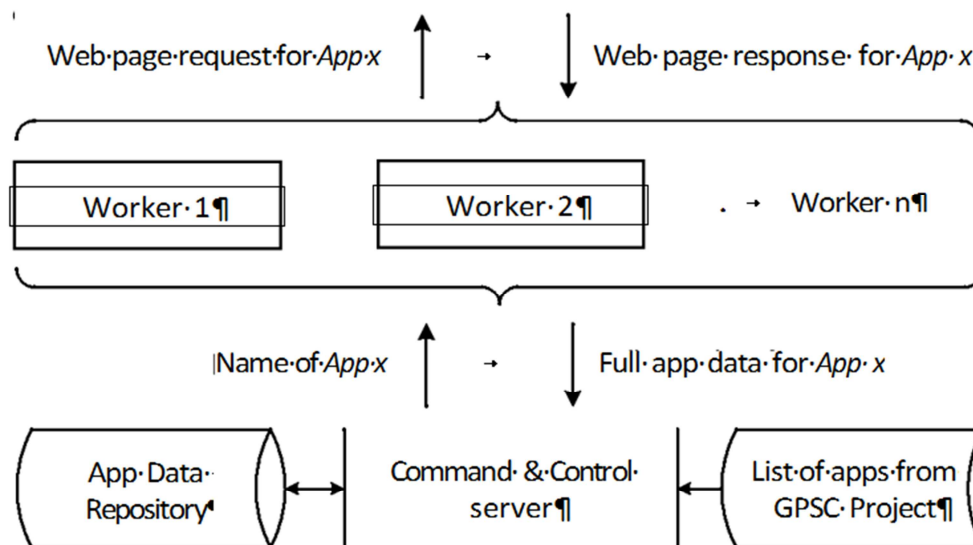
Από το Android 6.0 και έπειτα, οι χρήστες δεν είναι πλέον υποχρεωμένοι να αποδέχονται (ή να απορρίπτουν) τα δικαιώματα στο σύνολό τους κατά την εγκατάσταση, και μπορούν τώρα να αποδεχτούν (ή να απορρίπτουν) τις άδειες μεμονωμένα κατά τη διάρκεια εκτέλεσης. Αυτό προσφέρει πρόσθετο έλεγχο, αλλά πολλοί χρήστες εξακολουθούν να δέχονται αιτήσεις άδειας τυφλά λόγω συνήθειας ή έλλειψης κατανόησης.

Μελετώντας την εξέλιξη της άδειας εφαρμογής σε ολόκληρο το Google Play Store, είναι δυνατό να προσδιορίσουμε ποσοτικά την έκταση στην οποία πιθανότατα θα χαθεί η ιδιωτική ζωή / ασφάλεια, καθώς θα βγουν νέες εκδόσεις εφαρμογών στο σύνολο του Google Play Store.

Οι προηγούμενες ερευνητικές προσπάθειες εξέτασαν την εξέλιξη της άδειας στην ίδια την πλατφόρμα Android ή την εξέλιξη της χρήσης των αδειών σε βιβλιοθήκες διαφημίσεων Android, χωρίς να εξετάζουν τις αλλαγές στη χρήση των δικαιωμάτων σε επίπεδο εφαρμογών ή να ερευνήσει ολόκληρο το Google Play Store.

2.3 Επισκόπηση των αποτελεσμάτων ελέγχου

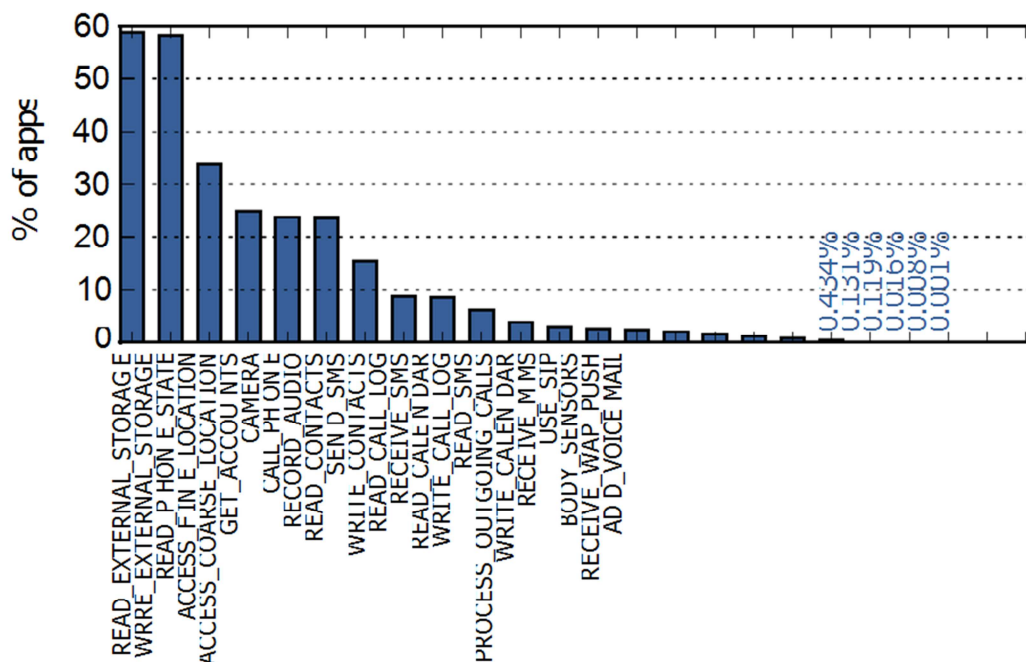
Στην παρούσα ενότητα ξεκινάνε οι Vincent F. Taylor - Ivan Martinovic με μια συνολική επισκόπηση των εφαρμογών και των αδειών στο Google Play Store, ακολουθούμενη από τη διαχρονική ανάλυση των δεδομένων. Για συντομία χρησιμοποιούν τους όρους Google Play Store και Store εναλλάξιμα.



Σχήμα 1 : Αρχιτεκτονική crawler βασισμένη σε cloud. Το Google Play Store Crawler (GPSC)

Το Google Play Store Project και το Google Play Store χρησιμοποιήθηκαν ως εξωτερικές πηγές δεδομένων.

Επικίνδυνα Δικαιώματα



Διάγραμμα 2: Επικράτηση χρήσης αδειών σε όλο το Google Play Store.

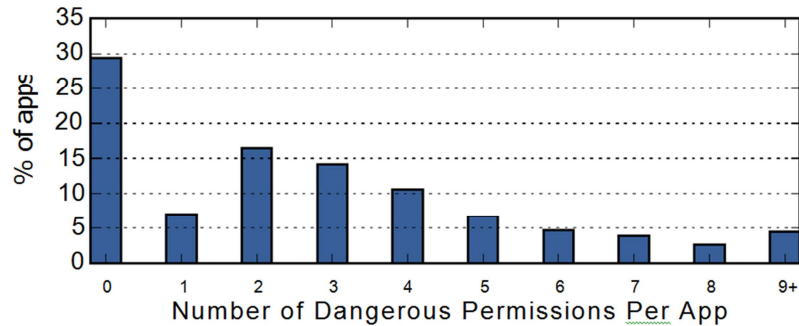
2.4 Γενική επισκόπηση

Για τη δημιουργία των ακόλουθων αποτελεσμάτων του Google Play Store, χρησιμοποιήθηκε το πιο πρόσφατο στιγμιότυπο κατά τη στιγμή της συγγραφής της μελέτης, δηλαδή το Μάρτιο του 2016.

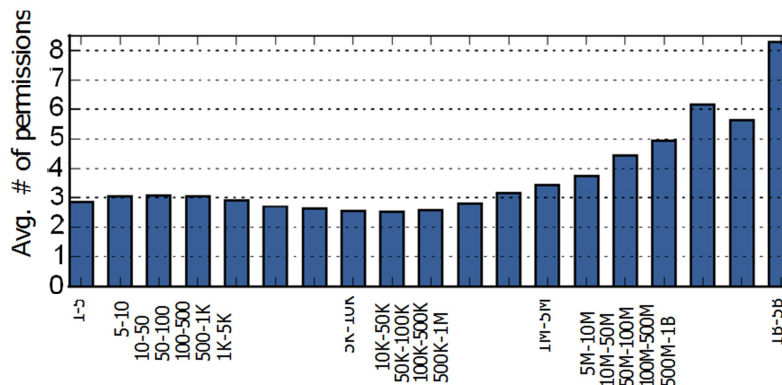
Το παραπάνω σχήμα δείχνει τη δημοτικότητα των δικαιωμάτων σε όλες τις εφαρμογές. Τα πιο δημοφιλή δικαιώματα αφορούν την ανάγνωση / εγγραφή σε εξωτερικό αποθηκευτικό χώρο σε μια συσκευή (58,9% / 58,3% αντίστοιχα), ανάγνωση της τρέχουσας κατάστασης της συσκευής (33,8%) και λήψη της ακριβούς θέσης του χρήστη (24,8%).

Το παραπάνω διάγραμμα δείχνει τον αριθμό των δικαιωμάτων που χρησιμοποιούνται σε όλες τις εφαρμογές. Ο μεγαλύτερος αριθμός εφαρμογών (29,4%) δεν χρησιμοποίησε δικαιώματα, ενώ η χρήση δύο (16,5%) και τριών (14,2%) συνολικών δικαιωμάτων ήταν πιο συνηθισμένη στις εφαρμογές που χρησιμοποίησαν δικαιώματα.

Μέχρι 1.000.000 λήψεις, η μέση εφαρμογή χρησιμοποίησε περίπου 2.5-3 δικαιώματα. Με εξαίρεση τις εφαρμογές που έχουν λήψεις 500 εκατομμυρίων-1 δισεκατομμυρίων, οι εφαρμογές με 10.000 λήψεις και άνω είχαν δικαιώματα χρήσης που αυξήθηκαν μονόπλευρα από 2,5 σε 8,3 ανά αποστολές, κατά μέσον όρο.3.2



Διάγραμμα 3: Αριθμός δικαιωμάτων που χρησιμοποιούνται ανά εφαρμογή στο Κατάστημα Google Play.



Διάγραμμα 4: Μέσος αριθμός αδειών χρήσης ανά κατηγορία εφαρμογής.

2.5 Αλλαγές στην Χρήση Εξουσιοδότησης

Ανέλυσαν τη χρήση της άδειας βάσει του αριθμού λήψεων μιας εφαρμογής. Οι εφαρμογές χωρίστηκαν σε τρεις κατηγορίες βάσει του συνολικού αριθμού λήψεών τους: 1-1K (χαμηλές λήψεις), 1K-1M (μεσαίες λήψεις) και 1M-5B (υψηλές λήψεις). Οι εφαρμογές προστίθενται συχνά και καταργούνται από το κατάστημα εφαρμογών, επομένως εξέτασαν μόνο τις εφαρμογές που υπήρχαν σε όλα τα στιγμιότυπα για ολόκληρη την περίοδο.

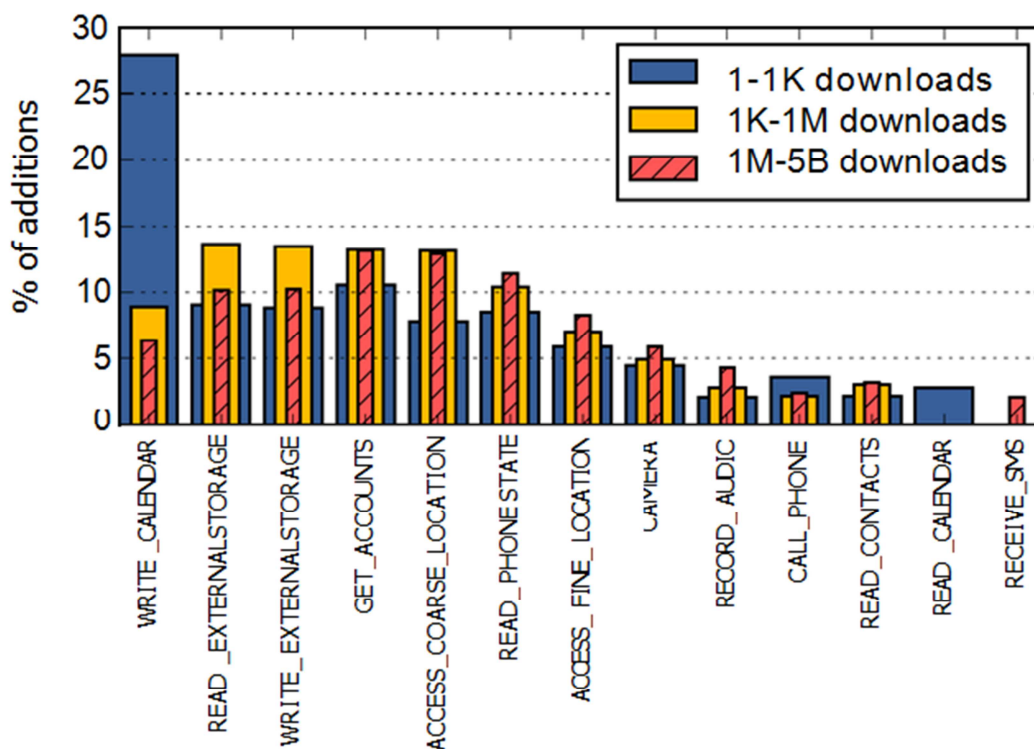
Πλήθος λήψεων	Οκτώβριος - 2014	Σεπτέμβριος - 2016	Διαφορά Αλλαγή
1-1K	3.13	3.16	+0.96%
1K-1M	2.37	2.45	+3.38%
1M-5B	3.40	3.58	+5.29%

Πίνακας 2: Μέση χρήση χρήσης (και ποσοστιαία αλλαγή) σε εφαρμογές κατά τη διάρκεια της διετούς περιόδου.

Ο παραπάνω πίνακας δείχνει τον τρόπο με τον οποίο άλλαξε η χρήση της άδειας χρήσης της εφαρμογής κατά τη διάρκεια της διετούς περιόδου. Σε όλα τα στιγμιότυπα, κάθε κατηγορία εφαρμογών είχε μια αύξηση στον μέσο αριθμό των δικαιωμάτων που χρησιμοποιήθηκαν.

Συνολικά, διαπιστώθηκε ότι οι εφαρμογές με λήψεις 1M-5B είχαν την υψηλότερη αύξηση στη μέση χρήση άδειας και την ποσοστιαία αλλαγή, από 3,40 σε 3,58, με αύξηση 5,29%. Οι εφαρμογές με λήψεις 1K-1M προχώρησαν από τη χρήση μέσων δικαιωμάτων 2,37 έως 2,45. Οι εφαρμογές με λήψεις 1-1K είχαν τη χαμηλότερη αύξηση στη χρήση άδειας, από 3,13 σε 3,16 κατά την εξεταζόμενη περίοδο.

Είναι ενδιαφέρον να σημειωθεί ότι οι εφαρμογές με λήψεις 1-1K χρησιμοποιούν περισσότερα δικαιώματα κατά μέσο όρο από τις εφαρμογές με downloads 1K-1M. Δυο πιθανοί λόγοι είναι ότι οι εφαρμογές με χαμηλά downloads χρησιμοποιούν άχρηστες άδειες, δηλαδή είναι υπερβολικά προνομιακές ή προσπαθούν να παρέχουν πρόσθετα χαρακτηριστικά (που απαιτούν πρόσθετα δικαιώματα) για να κερδίσουν μερίδιο αγοράς. Ενώ η συνολική αλλαγή στη μέση χρήση δικαιωμάτων χρήσης σε όλο το δείγμα είναι μικρή, υπενθυμίζετε στον αναγνώστη ότι αυτοί οι αριθμοί αντικατοπτρίζουν τη συνολική αλλαγή δικαιωμάτων σε μεγάλο αριθμό εφαρμογών, συμπεριλαμβανομένων πολλών εφαρμογών που δεν έχουν ενημερωθεί καθόλου. Πράγματι, στις λεπτομέρειες μεμονωμένων εφαρμογών, η προσθήκη πολλών δικαιωμάτων μεταξύ στιγμιότυπων δεν είναι ασυνήθιστη.



Διάγραμμα 5: Κατανομή των πιο συχνά προστιθέμενων δικαιωμάτων. Για λόγους σαφήνειας, παραλήφθηκαν άδειες που αντιστοιχούσαν σε λιγότερο από 2% των προσθηκών.

2.6 Κατάληξη αποτελεσμάτων

Στη δημοσίευση των Vincent F. Taylor και Ivan Martinovic, πραγματοποίησαν μια διαχρονική ανάλυση της άδειας εξέλιξης των εφαρμογών, λαμβάνοντας τριμηνιαία στιγμιότυπα του Google Play Store για μια περίοδο ενός έτους.

Η ανάλυσή τους έδειξε ότι ο μέσος αριθμός δικαιωμάτων που χρησιμοποιούνται από τις εφαρμογές αυξήθηκε κατά τη διάρκεια της περιόδου ενός έτους, ενώ οι λιγότερο δημοφιλείς εφαρμογές έχουν μεγαλύτερη αύξηση.

Παρατήρησαν ότι η πλειοψηφία των εφαρμογών δεν ενημερώνονται μεταξύ των στιγμιότυπων και εκείνων που ενημερώνονται, η πλειοψηφία δεν έχει αλλαγές στις απαιτήσεις αδειών τους. Ωστόσο, από τις εφαρμογές που έχουν αλλαγές στις απαιτήσεις των δικαιωμάτων τους, η πιο πιθανή αλλαγή είναι η προσθήκη μιας νέας άδειας.

Παρατήρησαν ότι περίπου δύο φορές περισσότερες εφαρμογές προσθέτουν νέα δικαιώματα, σε σχέση με τις εφαρμογές που καταργούν δικαιώματα.

Έκαναν δοκιμές και παρατήρησαν ότι οι δωρεάν εφαρμογές και οι δημοφιλείς εφαρμογές (εφαρμογές με περισσότερες από 1 εκατομμύριο λήψεις) ήταν πιο πιθανό να προσθέσουν νέα

δικαιώματα με την πάροδο του χρόνου. Η προσθήκη νέων δικαιωμάτων δεν είναι εγγενώς κακή, καθώς πολλές εφαρμογές έχουν νόμιμους λόγους να ζητήσουν πρόσθετη πρόσβαση σε δεδομένα χρήστη.

Ωστόσο, πολλές εφαρμογές είναι επίσης γνωστό ότι καταχρώνται τα παραχωρηθέντα δικαιώματά τους για σκοπούς δημιουργίας προφίλ χρηστών ή / και άμεσης κλοπής των δεδομένων τους. Παρατήρησαν μια τάση στο Google Play Store για τις εφαρμογές να προσθέτουν νέα δικαιώματα με την πάροδο του χρόνου.

Αναπτύσσοντας το φαινόμενο αυτό στην προσοχή της ερευνητικής κοινότητας, ελπίζουν να δημιουργήσουν επιπλέον ενδιαφέρον, έτσι ώστε να αναπτυχθούν κατάλληλες στρατηγικές για την ασφαλή αποθήκευση των ευαίσθητων δεδομένων των χρηστών, καθώς τα smartphones συνεχίζουν να αποτελούν ένα κρίσιμο κομμάτι της ζωής μας.

3 Ενημέρωση συμπεριφοράς στις αγορές εφαρμογών και επιπτώσεις στην ασφάλεια: Μια μελέτη περίπτωσης στο Google Play

Στη δημοσίευση των: Andreas Möller, Stefan Diewald, Luis Roalter, Florian Michahelles, Matthias Kranz, οι πλατφόρμες που σχετίζονται με πλατφόρμες, όπως το Apple App Store ή το Google Play (πρώην Android Market), αποτελούν σήμερα σημαντική πηγή, ίσως η μοναδική με τόσο μεγάλο πλήθος χρηστών, για τη διανομή εφαρμογών για κινητά.

Τον Μάρτιο του 2012, η Apple έφτασε συνολικά σε 25 δισεκατομμύρια downloads εφαρμογών iOS1. Μέχρι το 2011, 10 δισεκατομμύρια εφαρμογές Android είχαν ληφθεί συνολικά μέσω του Google Play. Οι χρήστες Smartphone εντοπίζουν τις εφαρμογές τους σε ένα μέρος και ενημερώνονται για τις διαθέσιμες ενημερώσεις (μέσω ενός συμβόλου σήματος στο εικονίδιο του App Store στο iOS ή ενός μηνύματος στη γραμμή ειδοποιήσεων στο Android). Ωστόσο, ούτε στο iOS ούτε στο Android, οι ενημερώσεις εφαρμογών εγκαθίστανται αυτόματα. Το Android έχει μια ρύθμιση για την εγκατάσταση ενημερώσεων χωρίς επιβεβαίωση, αλλά είναι απενεργοποιημένη από προεπιλογή.

Αυτή η εφαρμογή του μηχανισμού ενημέρωσης μπορεί να θεωρηθεί ως δυναμικός κίνδυνος για την ασφάλεια. Οι μη διορθωμένες τρύπες ασφαλείας αυξάνουν την ευπάθεια μιας συσκευής. Δεδομένου ότι οι χρήστες πρέπει να αναλάβουν την ευθύνη να διατηρούν το σύστημά τους ενημερωμένο, οι σημαντικές ενημερώσεις ενδέχεται να μην εγκατασταθούν έγκαιρα ή καθόλου. Ειδικά για εφαρμογές έρευνας ή στην αρχή της διάρκειας ζωής μιας εφαρμογής, είναι σημαντική η τακτική εγκατάσταση ενημερώσεων. Όντας σε κατάσταση ανάπτυξης, τέτοιες εφαρμογές συχνά είναι λιγότερο σταθερές και απαιτούν συχνότερες διορθώσεις. Μέχρι το τέλος του 2011, στο Google Play δημοσιεύθηκαν περισσότερες από 20.000 νέες εφαρμογές μηνιαίως, έτσι ώστε αυτό το φαινόμενο να επηρεάζεται πιθανώς από τον μεγάλο αριθμό εφαρμογών. Τα ελαττώματα ασφαλείας καθίστανται ακόμη πιο ασφαλή για τη νέα και επερχόμενη κατηγορία εφαρμογών που ενσωματώνουν το σπύρι ή το αυτοκίνητο (αποκαλούμενες εφαρμογές στο αυτοκίνητο), αφού στην περίπτωση αυτή όχι μόνο η ίδια η εφαρμογή, αλλά και η συνδεδεμένη συσκευή γίνεται ανασφαλής.

Ενώ η συμπερίληψη στο Apple App Store απαιτεί διαδικασία εξέτασης, το Google Play δεν υπόκειται σε περιορισμούς για τη μεταφόρτωση εφαρμογών. Ωστόσο, οι εφαρμογές σαρώνονται για ιούς και κακόβουλο λογισμικό και σε περίπτωση εντοπισμού πραγματοποιείται διαγραφή του κακόβουλου περιεχομένου. Αυτό είναι, ωστόσο, μόνο μια μέθοδος για να εντοπισθεί λογισμικό που προφανώς προσπαθεί να κάνει δημιουργήσει προβλήματα, αλλά όχι να εντοπίσει σφάλματα προγραμματισμού ή τρύπες ασφαλείας.

Η αυτόματη ανάλυση των προβλημάτων ασφαλείας κατά τη διαδικασία υποβολής σε ψηφιακούς χώρους της αγοράς έχει προταθεί με διάφορες προσεγγίσεις Di Cerbo κ.ά. όπου παρουσιάζουν μια μεθοδολογία για την ανάλυση της εγκληματολογικής κινητής τηλεφωνίας για την ανίχνευση εφαρμογών «ευάλωτου» (ή «κακόβουλου λογισμικού»).

Η μεθοδολογία βασίζεται στη σύγκριση του δικαιώματος ασφαλείας Android για κάθε εφαρμογή με ένα σύνολο μοντέλων αναφοράς, για εφαρμογές που διαχειρίζονται ευαίσθητα δεδομένα. Έτσι, η έρευνα των Andreas Möller, Stefan Diewald, Luis Roalter, Florian Michahelles, Matthias Kranz, επικεντρώνεται περισσότερο στην προστασία του χρήστη από κακόβουλες εφαρμογές ενώ οι υπόλοιπες επικεντρώνονται στην καταγραφή της (μη) συμμόρφωσης των χρηστών για την εγκατάσταση ενημερώσεων κώδικα ενός αξιόπιστου προγραμματιστή.

Έχει βρεθεί επίσης ότι οι εφαρμογές Android απαιτούν συχνά δικαιώματα που δεν χρειάζονται. Έτσι, έχουν προταθεί επεκτάσεις στο μοντέλο άδειας του Android, οι οποίες εστιάζουν ιδιαίτερα στη βελτίωση της (αρκετά πρώιμης) ακρίβειας των αδειών ή στην αφαίρεσή τους από την οπίσθια όψη με την επιτόπια παρακολούθηση αναφοράς. Λιγότερα δικαιώματα εγγενώς μειώνουν επίσης την πιθανότητα για σφάλματα σχετιζόμενα με την ασφάλεια.

3.1 Ενημέρωση Ανάλυσης Εγκατάστασης

Από τη στιγμή που το VMI Mensa ήταν διαθέσιμο για πρώτη φορά στο Google Play, έχουμε αποστείλει 21 ενημερώσεις. Για την ανάλυσή μας, χρησιμοποίησαν τα ενσωματωμένα εργαλεία στατιστικών στοιχείων της Κονσόλας προγραμματιστή Android στο Google Play.

Αυτά επιτρέπουν την παρακολούθηση του αριθμού των εγκαταστάσεων με την πάροδο του χρόνου, την παρακολούθηση των εκδόσεων εφαρμογών και πολλά άλλα. Όλα τα δεδομένα είναι ανώνυμα και δεν μπορούν να σχετίζονται με μεμονωμένους χρήστες. Όπως αναφέρθηκε προηγουμένως, οι ενημερώσεις μπορούν να εγκατασταθούν αυτόματα ή μη αυτόματα με επιβεβαίωση του χρήστη. Δεν είναι δυνατή η παρακολούθηση της ενεργοποίησης της αυτόματης ενημέρωσης στις συσκευές των χρηστών.

Για την ανάλυσή τους οι Andreas Möller, Stefan Diewald, Luis Roalter, Florian Michahelles, Matthias Kranz, εξέτασαν τις τελευταίες πέντε ενημερώσεις που δημοσιεύτηκαν στις 22 Δεκεμβρίου 2011, 17 Ιανουαρίου 2012, 26 Ιανουαρίου 2012, 24 Φεβρουαρίου 2012 και 02 Απριλίου 2012. Ο μέσος χρόνος μεταξύ των ενημερώσεων ήταν 26 ημέρες, κάτι που θεώρησαν ότι δεν αποτελεί αδικαιολόγητη προσπάθεια για την τακτική εγκατάστασή τους από τους χρήστες.

Όλες οι ενημερώσεις πρόσθεσαν νέες λειτουργίες στην εφαρμογή ή / και έλυσαν μικρά προβλήματα, αλλά κανένα δεν ήταν κρίσιμο για την ασφάλεια. Για κάθε ενημέρωση, παρατήρησαν πόσοι χρήστες κατέβασαν την ενημέρωση την πρώτη ημέρα δημοσίευσης και τις 6 συνεχόμενες ημέρες. Υπολόγισαν την αναλογία εγκατάστασης ενημέρωσης συσχετίζοντας τον αριθμό download με τον συνολικό αριθμό των εγκαταστάσεων ενεργών συσκευών στις αντίστοιχες ημέρες.

3.2 Ενημέρωση συμπεριφοράς

Ο παρακάτω δείχνει τα ποσοστά εγκατάστασης στην ημέρα δημοσίευσης των ενημερωμένων εκδόσεων (ημέρα 0) και τις έξι συνεχόμενες ημέρες (ημέρα 1 έως 6), κατά μέσο όρο για τις πέντε ενημερώσεις που εξετάστηκαν σε αυτή τη μελέτη.

Οι ακριβείς αναλογίες είναι πολύ παρόμοιες για όλες τις ενημερώσεις, γεγονός που υποδηλώνεται από τις χαμηλές τυπικές αποκλίσεις (βλ. Τελευταία στήλη του πίνακα). Κατά μέσο όρο, το 17,0% εγκατέστησε την ενημέρωση την ημέρα 0. Τις επόμενες ημέρες, οι αριθμοί συνεχώς και εκθετικά μειώνονται: το 14,6% εγκατέστησε την ενημέρωση την ημέρα 1, μόνο 7,8% την ημέρα 2 και 5,1% την ημέρα 3. Στις την 6η ημέρα, μόνο το 2,3% έλαβε την ενημέρωση.

Ημέρες από Δημοσίευση	Ποσοστό Εγκατάστασης	Τυπική απόκλιση
-----------------------	----------------------	-----------------

Ημέρα Δημοσίευσης	17.0%	2.7%
Ημέρα 1	14.6%	2.0%
Ημέρα 2	7.8%	1.3%
Ημέρα 3	5.1%	0.9%
Ημέρα 4	3.5%	0.7%
Ημέρα 5	2.8%	0.5%
Ημέρα 6	2.3%	0.4%
Σύνολο 7 ημερών	53.2%	2.7%

Πίνακας 3. Ποσοστό όλων των χρηστών που εγκατέστησαν μια ενημερωμένη έκδοση εντός 7 ημερών από τη δημοσίευσή της.

Μόνο λίγο περισσότερο από το ήμισυ όλων των χρηστών εγκατέστησαν μια πρόσφατη ενημέρωση εντός μιας εβδομάδας. Τα δεδομένα υπολογίστηκαν κατά μέσον όρο με βάση πέντε υποσυνειδητές ενημερώσεις που δημοσιεύθηκαν εντός 102 ημερών. Η τυπική απόκλιση σχετίζεται με τις πέντε μεμονωμένες ενημερώσεις που παρατηρήσαμε στην περίπτωση χρήσης.

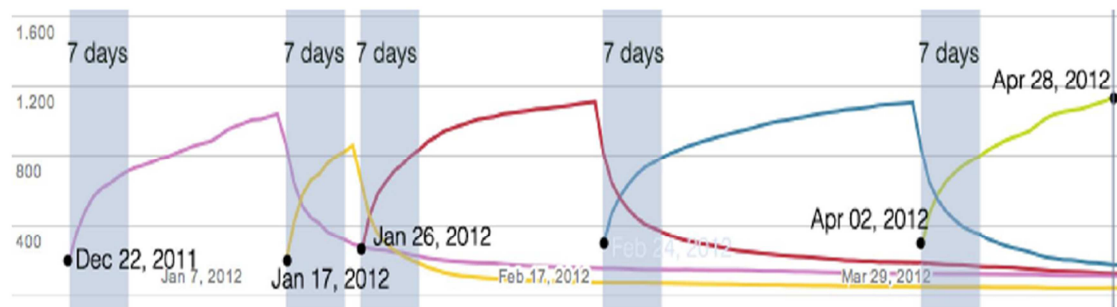
3.3 Διανομή έκδοσης

Εξέτασαν επίσης τη διανομή των τελευταίων πέντε εκδόσεων της εφαρμογής στις συσκευές των χρηστών, που απεικονίζονται με διαφορετικά χρώματα στο παρακάτω σχήμα. Οι περίοδοι επτά ημερών μετά την δημοσίευση μιας ενημέρωσης είναι ελαφρώς σκιασμένες για απεικόνιση. Η απεικόνιση δείχνει την εξάπλωση των νέων εκδόσεων λόγω σωρευτικών εγκαταστάσεων (εμφανίζονται με ένα απότομο γράφημα που ισοπεδώνει όλο και περισσότερο) και τη μείωση των παλαιότερων εκδόσεων. Επίσης είναι προφανές πόσο παραμένουν οι παλιές εκδόσεις (έως και τέσσερις εκδόσεις παλαιότερες από τις πιο πρόσφατες).

Για παράδειγμα, εξέτασαν τις 28 Απριλίου 2012, δηλαδή δύο εβδομάδες μετά τη δημοσίευση της τελευταίας ενημέρωσης: Μόνο το 56,4% όλων των χρηστών είχε εγκαταστήσει αυτή την τελευταία έκδοση (v.27). Οι προηγούμενες τέσσερις εκδόσεις ήταν ακόμα σε χρήση κατά 8,5% (v.26), 6,0% (v.25), 5,5% (v.24) και 2,1% (v.23). Το πιο σοβαρό, το 21,5% είχε ακόμα και παλαιότερες εκδόσεις εγκατεστημένες στις συσκευές τους την εποχή εκείνη.



Διάγραμμα 6. Οπτικοποίηση που αντιπροσωπεύει τον αριθμό των πέντε μεταγενέστερων λήψεων ενημέρωσης (κάθετος άξονας) με την πάροδο του χρόνου. Το γράφημα εμφανίζει τα μέγιστα στην ημέρα δημοσίευσης των ενημερωμένων εκδόσεων (ενδεχομένως εξαιτίας των ενεργοποιημένων αυτόματων ενημερώσεων) και στη συνέχεια μειώνεται εκθετικά. Τροποποιημένο διάγραμμα με βάση τα στατιστικά στοιχεία της κονσόλας προγραμματιστή Android.



Διάγραμμα 7. Οπτικοποίηση που αντιπροσωπεύει τον αριθμό των εγκαταστάσεων ανά εκδοχή (κάθετος άξονας). οι χρωματιστές γραμμές υποδεικνύουν τις πέντε τελευταίες εκδόσεις. Το διάγραμμα αποκαλύπτει πόσο παλιές εκδόσεις είναι ενεργοποιημένες στις συσκευές του χρήστη. Οι περίοδοι των 7 ημερών μετά την δημοσίευση μιας ενημέρωσης επισημαίνονται. Τροποποιημένο διάγραμμα με βάση τα στατιστικά στοιχεία της Κονσόλας προγραμματιστή Android.

3.4 Αποτελέσματα μελέτης 2012

Τα αποτελέσματα της μελέτης των Andreas Möller, Stefan Diewald, Luis Roalter, Florian Michahelles, Matthias Kranz, αποκαλύπτουν μια προβληματική επικαιροποίηση: Ακόμη και μία εβδομάδα μετά τη δημοσίευσή τους, οι ενημερώσεις εγκαταστάθηκαν μόνο από περίπου το 50% των χρηστών. Οι υπόλοιποι χρησιμοποίησαν διαφορετικές ξεπερασμένες εκδόσεις. το ένα πέμπτο ακόμη δεν εγκατέστησε ούτε μία από τις τελευταίες πέντε ενημερώσεις. Αυτό συνεπάγεται δύο δυνητικές ομάδες χρηστών: εκείνους που ενημερώνουν με υποδειγματικό

τρόπο, και εκείνους που μόλις και μετά βίας ενημερώνονται. Ως εκ τούτου, οι προγραμματιστές δεν πρέπει να κάνουν το λάθος να βασίζονται στην πεποίθηση ότι τουλάχιστον η προτελευταία έκδοση της εφαρμογής τους θα τρέξει στις περισσότερες συσκευές.

Αν αξιολογήσουν αυτό το αποτέλεσμα στη γενική συμπεριφορά ενημέρωσης, τα ευρήματά τους υποδηλώνουν μια κρίσιμη κατάσταση ασφάλειας. Οι αβλαβείς ενημερώσεις δυνατοτήτων στην μελέτη περιπτώσεώς τους θα μπορούσε να είναι σημαντικές διορθώσεις που σχετίζονται με την ασφάλεια σε άλλη εφαρμογή.

Κατά μέσο όρο, σχεδόν οι μισοί χρήστες θα χρησιμοποιούν μια ευάλωτη έκδοση εφαρμογής ακόμα και 7 ημέρες μετά τη δημοσίευση της ενημέρωσης κώδικα. Ο χρόνος από την ανίχνευση ενός κενού ασφαλείας στην τελική αποστολή ενημέρωσης δεν εξετάζεται καν εδώ.

Άλλοι λόγοι δείχνουν ότι η πραγματική κατάσταση επικαιροποίησης θα μπορούσε να είναι ακόμη χειρότερη από την υποδειγματική ανάλυση των περιπτώσεων. Ένας μεγάλος αριθμός εγκατεστημένων εφαρμογών θα μπορούσε να μειώσει περαιτέρω το ποσό των ενημερωμένων εφαρμογών, δεδομένου ότι θα χρειαστεί περισσότερος χρόνος για τις μεμονωμένες ενημερώσεις. Επιπλέον, το γεγονός ότι οι χρήστες υποτίθεται ότι ασχολούνται ιδιαίτερα με την εξεταζόμενη εφαρμογή τους θα μπορούσε να έχει επίσης αντίκτυπο στη συχνότητα επικαιροποίησης. Παρατηρείται μια ακόμα πιο κρίσιμη κατάσταση με εφαρμογές που δεν χρησιμοποιούνται τακτικά, αλλά για ποια ασφάλεια είναι κρίσιμη μόνο τότε (π.χ. για τις on-line τραπεζικές εφαρμογές). Απαιτείται λεπτομερής παρακολούθηση της χρήσης για την καλύτερη κατανόηση της σχέσης μεταξύ συχνότητας χρήσης και συμπεριφοράς ενημέρωσης.

Εξέτασαν επίσης τη συμπεριφορά των χρηστών σε περίπτωση προβλημάτων. Η εφαρμογή περιείχε ένα στοιχείο "Δώστε την γνώμη" στο μενού προτιμήσεων που επέτρεψε την αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου στους προγραμματιστές.

Στην περιγραφή της εφαρμογής στο Google Play, ζητήθηκε από τους χρήστες να τους δώσουν ανατροφοδότηση χρησιμοποιώντας αυτή τη λειτουργία. Συνέδεσαν επίσης μια σελίδα από την οποία οι χρήστες θα μπορούσαν να επικοινωνήσουν και με τους προγραμματιστές. Το συμπέρασμα τους έδειξε ότι λίγοι χρήστες χρησιμοποίησαν αυτές τις ευκαιρίες.

Μάλλον χρησιμοποίησαν τη λειτουργία αξιολόγησης στο Google Play. Για παράδειγμα, η λήψη του δεν λειτούργησε για μία ημέρα λόγω προβλήματος του διακομιστή. Οι χρήστες των εφαρμογών άφησαν αμέσως κακή βαθμολογία στο Google Play, αντιλαμβανόμενοι ότι η εφαρμογή δεν λειτουργεί πια. Προφανώς, δεν είχαν διαβάσει τα αιτήματα παροχής ανατροφοδότησης ανά μήνυμα ή δεν βρήκαν τον σύνδεσμο ανατροφοδότησης στην εφαρμογή.

Μια παρόμοια περίπτωση περιγράφει επίσης ότι δεν έχουν όλοι οι χρήστες το χρόνο και την υπομονή να διαβάσουν τα κείμενα περιγραφής στο Google Play: Ένας χρήστης σχολίασε ότι θα ήταν καλό να έχουμε αγγλική μετάφραση. Στην πραγματικότητα, η εφαρμογή είναι πλήρως εντοπισμένη σε 6 γλώσσες (μεταξύ των οποίων και στα αγγλικά) και οι τοπικές προσαρμογές προσαρμόζονται αυτόματα στη γλώσσα συστήματος της συσκευής. Ομοίως, ο χρήστης αξιολόγησε την εφαρμογή χειρότερα λόγω αυτής της καταγγελίας.

Για τους προγραμματιστές, οι παρατηρήσεις έχουν τρεις συνέπειες:

- Πρώτον, δείχνουν πόσο οι γρήγοροι χρήστες δίνουν κακές αξιολογήσεις, οι οποίες μπορεί να είναι προβληματικές, ειδικά για εμπορικές εφαρμογές - άλλες εργασίες ανέφεραν ότι οι κριτικές των χρηστών μπορεί να είναι σκληρές. Ως εκ τούτου, είναι σημαντικό να διατηρηθεί η εφαρμογή χωρίς προβλήματα και να παρέχονται έγκαιρες ενημερώσεις σε περίπτωση προβλημάτων.
- Δεύτερον, οι προγραμματιστές δεν μπορούν να βασίζονται στους χρήστες που διαβάζουν τις οδηγίες και χρησιμοποιούν τις ενσωματωμένες λειτουργίες ανατροφοδότησης.

Διαπίστωσαν ότι πρέπει να βρεθούν τρόποι περαιτέρω βελτίωσης αυτών των λειτουργιών και έμαθαν επίσης ότι η παρακολούθηση των αξιολογήσεων και των σχολίων στο Google Play είναι σημαντική. Διαφορετικά, σε ορισμένες περιπτώσεις, δεν θα μπορούσαν να γνωρίζουν πιθανά προβλήματα. Στην περίπτωση τους, σχετίζονταν με τη χρηστικότητα και τα δευτερεύοντα ζητήματα, αλλά θα μπορούσαν να είναι και σφάλματα ασφαλείας. Αυτό είναι ιδιαίτερα σημαντικό, αφού τα κενά ασφαλείας δεν συμβαδίζουν απαραίτητως με εφαρμογές που δεν ανταποκρίνονται ή δεν συντρίβουν και, συνεπώς, δεν καλύπτονται από τη λειτουργία ενσωματωμένης αναφοράς σφαλμάτων του Google Play.

- Τρίτον, ως πρώτο βήμα προς τη βελτίωση της ασφάλειας στις πλατφόρμες κινητής τηλεφωνίας και ενόψει των μερικές φορές δύσκολων μηχανισμών λήψης, ενθάρρυναν τους προγραμματιστές να υποστηρίζουν τους χρήστες στην ενημέρωση, π.χ. με ενσωματωμένους ελέγχους επικαιροποίησης στους χρήστες της εφαρμογής ή / και προώθησης τους στην αγορά της πλατφόρμας, όπως τις χρησιμοποιούν στις ερευνητικές εφαρμογές τους.

Κατόπιν αυτών θα γίνει στη διατριβή αυτή μία προσπάθεια να ληφθούν δεδομένα από το google play store, να γίνει ανάλυσή τους προκειμένου να δούμε πόσα δικαιώματα ανά εφαρμογή απαιτούνται δίνοντας έμφαση σε αυτά που έχουν περισσότερη διεισδυτικότητα στα δεδομένα του χρήστη όπως αυτά αποθηκεύονται στη συσκευή. Τα δεδομένα αυτά είναι προσωπικά αλλά η έγκριση που δίνεται τα καταστή άμεσα διαθέσιμα προς επεξεργασία και εκμετάλλευση.

4 Δεδομένα εφαρμογών Android (Play Store)

4.1 Ανάλυση κώδικα και τρόπος λειτουργίας

Σκοπός της διατριβής είναι η ανάλυση στατιστικών των εφαρμογών Android προκειμένου να μάθουμε τον αριθμό των χρηστών που έκαναν λήψη των εφαρμογών και την ικανοποίηση αυτών όσον αφορά τις υπηρεσίες της εφαρμογής που κατέβασαν. Για το σκοπό αυτό χρησιμοποιήσαμε ένα scrapy ή από τον ιστότοπο <https://github.com/manojps/google-play-apps-crawler-scrapy>.

Μετά από την τροποποίηση του κώδικα, διότι είχε σταματήσει να επιστρέφει αποτελέσματα, ο κώδικας πήρε την παρακάτω τελική κατάληξη.

```
# -*- coding: utf-8 -*-
from scrapy.contrib.spiders import CrawlSpider, Rule
from scrapy.contrib.linkextractors import LinkExtractor
from gplaycrawler.items import GplaycrawlerItem

class MySpider(CrawlSpider):
    name = "gplay"
    allowed_domains = ["play.google.com"]
    start_urls = ["https://play.google.com/store/apps/"]
    rules = (
        Rule(LinkExtractor(allow=('/store/apps/')),follow=True,callback='parse_link'),
        #Rule(LinkExtractor(allow=('/store/apps/'), deny=('/store/apps/details?')),follow=True),
        #Rule(LinkExtractor(allow=('/store/apps/details?')),follow=True,callback='parse_link')
    )

    def abs_url(url, response):
        """Return absolute link"""
        base = response.xpath('//head/base/@href').extract()
        if base:
            base = base[0]
        else:
            base = response.url
        return urlparse.urljoin(base, url)

    def parse_link(self,response):
```

```

item = GplaycrawlerItem()
if "details?id" in response.url:
    item["Link"] = response.url
    item["Item_name"] = ".join(response.xpath('//*[@class="document-
title"]/div/text()).extract())
    item["Updated"] = ".join(response.xpath('//*[@itemprop="datePublished"]/text()).extract())
    item["Author"] = ".join(response.xpath('//*[@itemprop="author"]/a/span/text()).extract())
    item["Filesize"] = ".join(response.xpath('//*[@itemprop="fileSize"]/text()).extract())
    item["Downloads"] =
".join(response.xpath('//*[@itemprop="numDownloads"]/text()).extract())
    item["Version"] = ".join(response.xpath('//*[@itemprop="softwareVersion"]/text()).extract())
    item["Compatibility"] =
".join(response.xpath('//*[@itemprop="softwareVersion"]/text()).extract())
    item["Content_rating"] =
".join(response.xpath('//*[@itemprop="contentRating"]/text()).extract())
    item["Author_link"] = ".join(response.xpath('//*[@class="dev-link']/@href).extract())
    item["Genre"] = ".join(response.xpath('//*[@itemprop="genre"]/text()).extract())
    item["Price"] = ".join(response.xpath('//*[@class="price buy id-track-
click"]/span[2]/text()).extract())
    item["Rating_value"] = ".join(response.xpath('//*[@class="score"]/text()).extract())
    item["Review_number"] = ".join(response.xpath('//*[@class="reviews-
num"]/text()).extract())
    item["Description"] = ".join(response.xpath('//*[@class="id-app-orig-desc"]/text()).extract())
    item["IAP"] = ".join(response.xpath('//*[@class="inapp-msg"]/text()).extract())
    item["Developer_badge"] = ".join(response.xpath('//*[@class="badge-
title"]/text()).extract())
    item["Physical_address"] = ".join(response.xpath('//*[@class="content physical-
address"]/text()).extract())
    item["Video_URL"] = ".join(response.xpath('//*[@class="play-action-container']/@data-
video-url').extract())
    item["Developer_ID"] = ".join(response.xpath('//*[@itemprop="author"]/a/@href).extract())
else:
    pass
return item

```

Σε αυτό περιλαμβάνονται όλες οι βιβλιοθήκες και τα απαραίτητα δεδομένα προκειμένου να δουλέψει το τροποποιημένο scrapy και να μας επιστρέψει τα αποτελέσματα που θα συλλέξει.

Η τελική μορφή των τροποποιημένων αρχείων όπου περιλαμβάνονται οι βιβλιοθήκες, αλλά και τα αρχεία για τη λειτουργία είναι η παρακάτω:

Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
spiders	23/9/2017 7:43 μμ	Φάκελος αρχείων	
__init__.py	18/9/2017 7:05 μμ	Αρχείο PY	0 KB
__init__.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	1 KB
items.py	18/9/2017 7:27 μμ	Αρχείο PY	1 KB
items.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	1 KB
pipelines.py	23/9/2017 7:41 μμ	Αρχείο PY	2 KB
pipelines.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	3 KB
README.md	18/9/2017 7:08 μμ	Αρχείο MD	2 KB
settings.py	20/9/2017 8:39 μμ	Αρχείο PY	1 KB
settings.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	1 KB

Στιγμιότυπο 1 των αρχείων όπου χρησιμοποιεί ο κώδικας.

Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
__init__.py	18/9/2017 7:05 μμ	Αρχείο PY	1 KB
__init__.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	1 KB
gplay.py	20/9/2017 9:05 μμ	Αρχείο PY	3 KB
gplay.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	4 KB
playcrawler.py	19/9/2017 6:05 μμ	Αρχείο PY	4 KB
playcrawler.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	4 KB
review_doesnt_work.py	18/9/2017 7:08 μμ	Αρχείο PY	4 KB
review_doesnt_work.pyc	23/9/2017 7:43 μμ	Αρχείο PYC	2 KB
scratch	23/9/2017 7:38 μμ	Αρχείο	2 KB

Στιγμιότυπο 2 των αρχείων του φακέλου Spiders

Για τη λήψη των εφαρμογών (apk) χρησιμοποιήθηκε ο κώδικας gplaycli.py που σαν αποτέλεσμα είναι να εκτελείται και ο κώδικας googleplay-ari όπου μαζί με είναι αναγκαία η χρήση του καθώς εκεί εκτελείται ο τρόπος για να συνδεθεί και να γίνει η συλλογή των δεδομένων από τη βάση του Google play.

Τα στοιχεία που απαιτούνται ώστε να γίνει η σύνδεση και η επιτυχημένη λήψη είναι τα εξής:

LANG

ANDROID_ID

GOOGLE_LOGIN

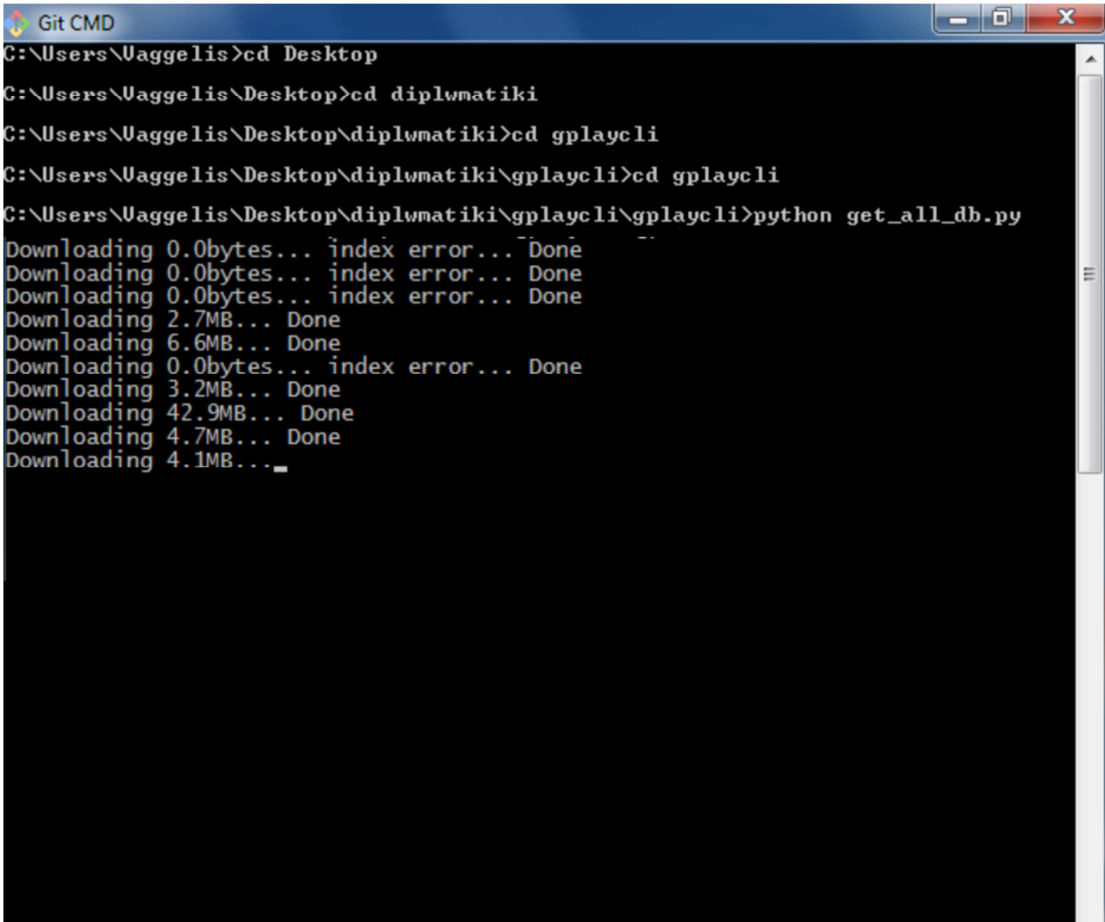
GOOGLE_PASSWORD

AUTH_TOKEN

4.1 Εκτέλεση κώδικα λήψης εφαρμογών

Για την εκτέλεση των αρχείων ρυθον και του κώδικα, εγκαταστήσαμε το ελεύθερο λογισμικό Anaconda2 και GIT

Έπειτα έγινε εκτέλεση του κώδικα μέσω του προγράμματος Git CMD, όπου μέσω των εντολών περιηγούμαστε στο φάκελο όπου βρίσκεται το αρχείο `get_all_db.py` και το καλέσαμε να εκτελέσει όλες τις εντολές του κώδικα. Τα αποτελέσματα φαίνονται παρακάτω:



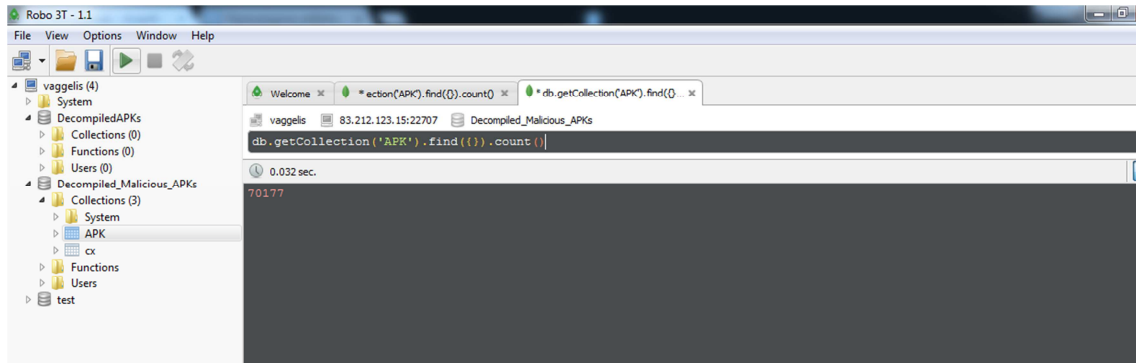
```
Git CMD
C:\Users\Uaggelis>cd Desktop
C:\Users\Uaggelis\Desktop>cd diplommatiki
C:\Users\Uaggelis\Desktop\diplommatiki>cd gplaycli
C:\Users\Uaggelis\Desktop\diplommatiki\gplaycli>cd gplaycli
C:\Users\Uaggelis\Desktop\diplommatiki\gplaycli\gplaycli>python get_all_db.py
Downloading 0.0bytes... index error... Done
Downloading 0.0bytes... index error... Done
Downloading 0.0bytes... index error... Done
Downloading 2.7MB... Done
Downloading 6.6MB... Done
Downloading 0.0bytes... index error... Done
Downloading 3.2MB... Done
Downloading 42.9MB... Done
Downloading 4.7MB... Done
Downloading 4.1MB... _
```

Στιγμιότυπο 3 εκτέλεση κώδικα

Καλώντας τον κώδικα του `get_all_db.py` ουσιαστικά κάνουμε χρήση των στοιχείων που έχουμε στο κομμάτι του `googleplay.api` προκειμένου να ξεκινήσει η λήψη των εφαρμογών. Όταν δεν πραγματοποιείται λήψη το μήνυμα «index error» μας ενημερώνει ότι δεν ήταν δυνατή η λήψη και ο πιο πιθανός λόγος είναι η έλλειψη στοιχείων πληρωμής καθώς πληθώρα εφαρμογών είναι επί πληρωμή.

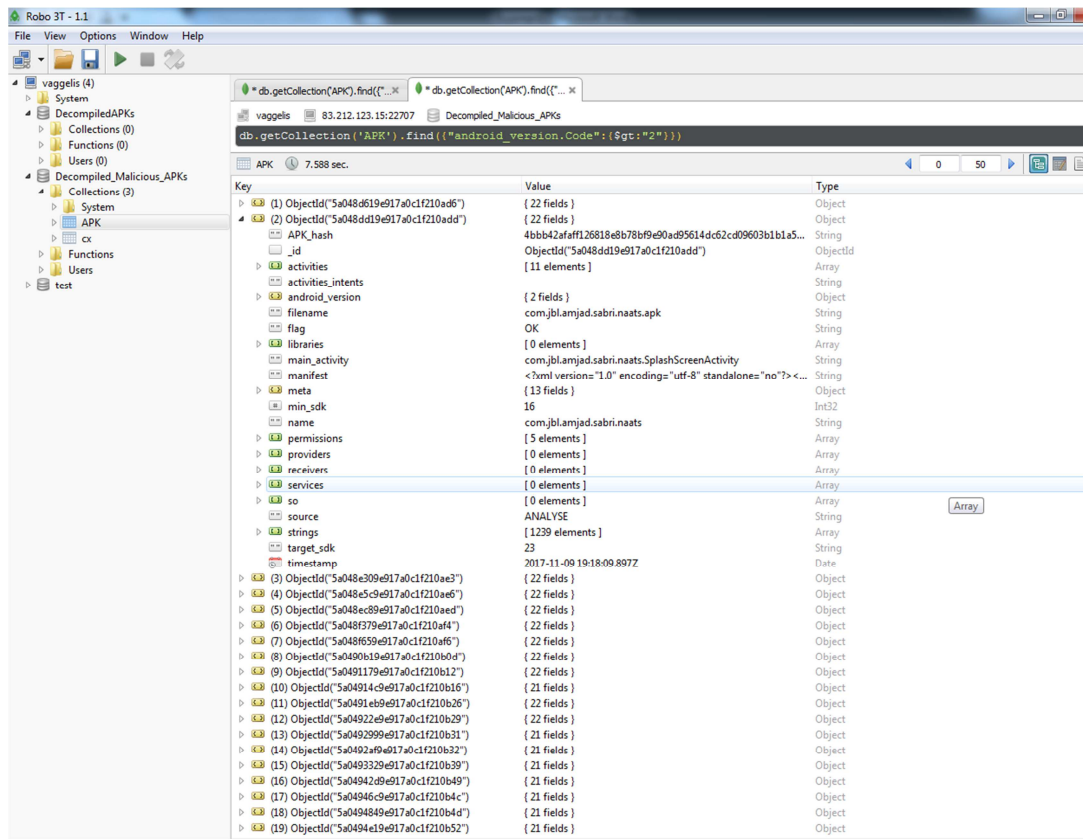
Τα στοιχεία πλέον κρατούνται σε ένα εικονικό μηχάνημα με στοιχεία σύνδεσης 83.212.123.15:22707 και η βάση δεδομένων είναι εφικτό να προσπελαστεί μέσω του προγράμματος `robotomongo`.

Το scrapy συνέλεξε τελικά πληροφορίες για **70177** εφαρμογές αφού δούλεψε για περίπου δεκαπέντε ημέρες, και τα αποθήκευσε στη βάση δεδομένων που βλέπουμε παρακάτω.



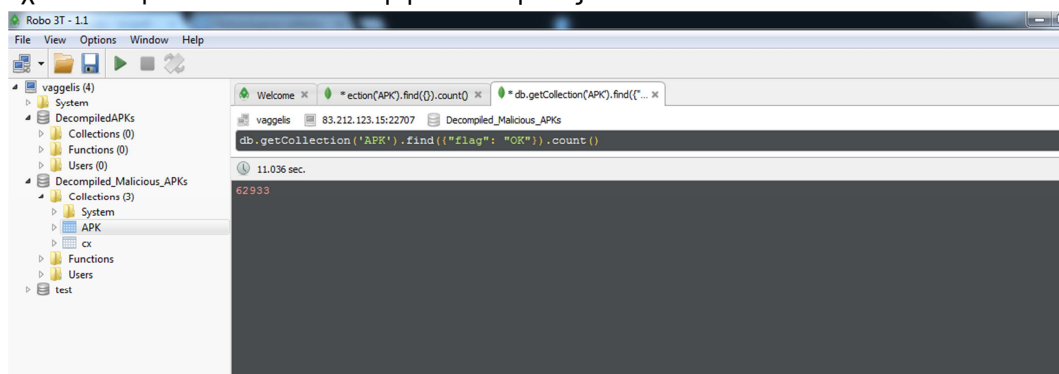
Στιγμιότυπο 4 εκτέλεση ερωτημάτων στη βάση

Κάθε εφαρμογή αποθηκεύτηκε στη βάση έχοντας τη θέση ενός αντικειμένου με περισσότερα στοιχεία καθένα από αυτό και τα πεδία που έχουν πλέον γεμίσει τη βάση φαίνονται στο παρακάτω στιγμιότυπο.



Στιγμιότυπο 5 Προβολή βάσης δεδομένων στον εικονικό υπολογιστή

Τα αντικείμενα, εφαρμογές και πληροφορίες αυτών, έχουν γεμίσει τη βάση και από τα επι συνόλω **70177** τα **62933** είναι αυτά όπου έχουν δεδομένα μέσα στους πίνακες και για το λόγο αυτό γίνεται ο έλεγχος μέσω του «flag» μιας σταθεράς η οποία καταχωρείται όταν οι πίνακες έχουν δεδομένα και είναι δυνατή η ανάλυσή τους.



Στιγμιότυπο 6 εκτέλεση ερωτημάτων στη βάση

Αυτοματοποιημένη συλλογή και ανάλυση Android εφαρμογών από το Google Play.

4.2 Εφαρμογές και τρόπος ανάδειξης.

Από το σύνολο των δεδομένων που λήφθηκαν και αποτελούν τη βάση δεδομένων θα μπορούμε να αντιληφθούμε τον τρόπο σκέψης των χρηστών, τι ζητάνε, τι επιλέγουν και να βγάλουμε κάποια συμπεράσματα όπου αν ακολουθηθούν από τον ιδιοκτήτες και προγραμματιστές των εφαρμογών να μπορέσουν αν προσελκύσουν περισσότερους χρήστες και εν τέλει να αυξήσουν το εισόδημά τους.

Σκοπός είναι να αντιληφθούμε τι θα μπορέσει να κάνει μία εφαρμογή πιο «ελκυστική» στον χρήστη. Οι εφαρμογές διακρίνονται καταρχάς σε δύο μεγάλες κατηγορίες τις δωρεάν και της επί πληρωμή. Από την ανάλυσή μας δεν είναι δυνατό να βγάλουμε αποτελέσματα για τις επί πληρωμή, αφού καμία τέτοια εφαρμογή δεν έχει ληφθεί στα δεδομένα μας, μιας και στα κριτήρια που ο κώδικάς μας χρησιμοποίησε στο Google Play ώστε να λάβουμε πρόσβαση για τη λήψη τους δεν περιελάμβανε κάποιο στοιχείο κάρτας ώστε να γίνει η χρέωση και εν συνεχεία η λήψη της εφαρμογής.

Οι δωρεάν εφαρμογές αρχικά είχαν σαν μόνο τρόπο είσπραξης εσόδων τις διαφημίσεις όπου αυτές καταλαμβάνουν κάποιο κομμάτι της οθόνης της εφαρμογής και πληρώνονται από το «click» των χρηστών πάνω στα διαφημιζόμενα στοιχεία.

Πολύ σύντομα όμως δημιουργήθηκε η ανάγκη από την Google αρχικά και μετά από τους προγραμματιστές να διατηρούνται στατιστικά ώστε να γίνεται διάκριση και διαφοροποίηση της τιμής αυτού του «click». Δηλαδή μία εφαρμογή που η ανταπόκριση από τους χρήστες είναι πολύ μεγάλη η τιμή που αυτή λαμβάνει είναι προφανώς μεγαλύτερη. Έτσι κάθε εφαρμογή πριν την επιλογή από το χρήστη, δίνει τη δυνατότητα σε αυτόν να γνωρίζει μία πληθώρα πληροφοριών ώστε να αποφασίσει ποια από αυτές θα κάνει λήψη και χρήση από τη συσκευή του.

Οι πληροφορίες αυτές είναι:

1. Οι κριτικές από τους προηγούμενους χρήστες, είτε με κάποια μονάδα μέτρησης αλλά και περιγραφικά ώστε να γίνεται στο μέγιστο βαθμό η πληροφόρησή του. Αυτό ανάγκασε τους προγραμματιστές να γίνουν πολύ προσεκτικοί με τις εκδόσεις καθώς οι απαιτήσεις των χρηστών είναι πλέον πάρα πολύ μεγάλες.
2. Ο αριθμός των λήψεων
3. Η κατηγορία όπου η εφαρμογή κατατάσσεται πχ παιχνίδια, εργαλεία κλπ
4. Η περιγραφή του προγραμματιστή όπου όσο καλύτερα περιγράφει τις λειτουργίες μπορεί να γίνει και η αιτία για την επιλογή από τον χρήστη.
5. Το μέγεθος λήψης αφού στις παλαιότερες συσκευές ο χώρος αποθήκευσης ήταν περιορισμένος.
6. Το νούμερο της έκδοσης καθώς για κάθε αλλαγή ή προσθήκη δημιουργείται μία νέα έκδοση και διατίθεται προς χρήση και αναγκαστικά και προς κριτική από τους χρήστες αν έχει κάποια βελτίωση.
7. Την έκδοση λειτουργικού που είναι συμβατή.

Μετά από δύο χρόνια λειτουργίας του Google Play (αρχικά ονομαζόταν Play Store) η Google αποφάσισε να κάνει μία ακόμα καινοτομία, αυτή της πρότασης στον χρήστη παρόμοιων εφαρμογών σε σχέση με αυτή, τα χαρακτηριστικά των οποίων εξετάζει. Τα κριτήρια που η Google αποφασίζει να κατατάσσει τις εφαρμογές είναι όλα τα παραπάνω που αναφέραμε και

πάντα σαν γνώμονα έχει να δώσει το καλύτερο αποτέλεσμα στον χρήστη και αυτός να είναι απόλυτα ικανοποιημένος ότι βρήκε την καλύτερη στην αναζήτησή του και τελικά έκανε λήψη της καλύτερης εφαρμογής όπου θα καλύψει όλες τις ανάγκες του.

Αυτό έχει φέρει τους προγραμματιστές σε έναν διαρκή αγώνα βελτίωσης των εφαρμογών τους, με τελικό αποδέκτη τον χρήστη όπου απολαμβάνει το καλύτερο αποτέλεσμα. Οι προγραμματιστές προκειμένου να μείνουν στην κορυφή των επιλογών της Google και αυτόματα των χρηστών είναι πολύ προσεκτικοί στο αποτέλεσμα που προσφέρουν μέσω των εφαρμογών τους, ανεβάζοντας το επίπεδο ψηλά και να επιβιώσουν οι καλύτεροι.

Από το 2014 οι καλύτερες δωρεάν εφαρμογές προχώρησαν σε μία ακόμα αλλαγή, αυτή της μετατροπής τους σε επί πληρωμή βγάζοντας εκδόσεις που απαιτούνταν χρήματα για να γίνει η λήψη τους και οι χρήστες απολάμβαναν αυτές χωρίς τις ενοχλητικές για μερικούς διαφημίσεις. Βλέποντας αυτή την εξέλιξη η «κούρσα» της πρωτιάς έγινε ακόμα πιο δύσκολη και πιο σκληρή αλλά πάντα με τελικό αποτέλεσμα την καλύτερη εφαρμογή για τον χρήστη.

4.3 Ανάλυση δεδομένων

Η ανάλυση των δεδομένων που πήραμε μας έδωσε στοιχεία για τα δικαιώματα που ζητάει μία εφαρμογή πριν ακόμα ληφθεί από τον χρήστη και γίνει εγκατάσταση στην έξυπνη συσκευή «smartphone».

Όπως είδαμε και στις προαναφερόμενες αναλύσεις, οι προγραμματιστές απαιτούν από τον χρήστη να εγκρίνει ένα πλήθος δικαιωμάτων επί των προσωπικών πολλές φορές δεδομένων του τηλεφώνου του χωρίς να ελέγχει τι δίνει.

Τα δικαιώματα αυτά κληρονομούνται και στις επόμενες εκδόσεις των εφαρμογών χωρίς να απαιτείται ξανά η έγκριση από τον χρήστη. Μοναδική περίπτωση έγκρισης είναι η τυχόν μεταβολή των δικαιωμάτων σε κάποια αναβάθμιση.

Στη συνέχεια εκτελέσαμε τον κώδικα q.py όπου κάνει έλεγχο των δεδομένων των εφαρμογών που έχουμε συλλέξει και μας επιστρέφει αποτελέσματα για τα δικαιώματα αυτά σε πόσες από τις ληφθείσες εφαρμογές γίνεται μνεία και ουσιαστικά ζητάνε την έγκριση για παράδειγμα στις επαφές, στην κάμερα, στο facebook και άλλα.

Ο κώδικας q.py τροποποιήθηκε ώστε να συνδέεται στη βάση του εικονικού υπολογιστή και να εκτελεί τα ερωτήματα εκεί. Ο τροποποιημένος κώδικας του q.py είναι ο παρακάτω:

```
#!/usr/bin/env python
# -*- coding: UTF-8 -*-

from pymongo import MongoClient
import pprint

client = MongoClient('83.212.123.15:22707')
db = client.Decompiled_Malicious_APKs
certs_depr= db.APK.find({"certificate":{"$regex": u"1024"}})
print certs_depr.count()
```



```

certs_ok= db.APK.find({"certificate":{"$regex": u"2048"}})
print certs_ok.count()
certs_md5= db.APK.find({"certificate":{"$regex": u"md5"}})
print certs_md5.count()
perms=[]
cnts=[]
for r in db.APK.find({"flag":"OK"}):
    apk_perms=r["permissions"]
    apk_perms=list(set(apk_perms))
    for p in apk_perms:
        if p in perms:
            idx=perms.index(p)
            cnts[idx]+=1
        else:
            perms.append(p)
            cnts.append(1)
for i in range(len(perms)):
    print perms[i],cnts[i]

```

```

#so
#for r in db.APK.find():
#    if len(r["so"])>0:
#        for j in range(len(r["so"])):
#            print r["name"]+"|"+r["so"][j][0],r["so"][j][1]

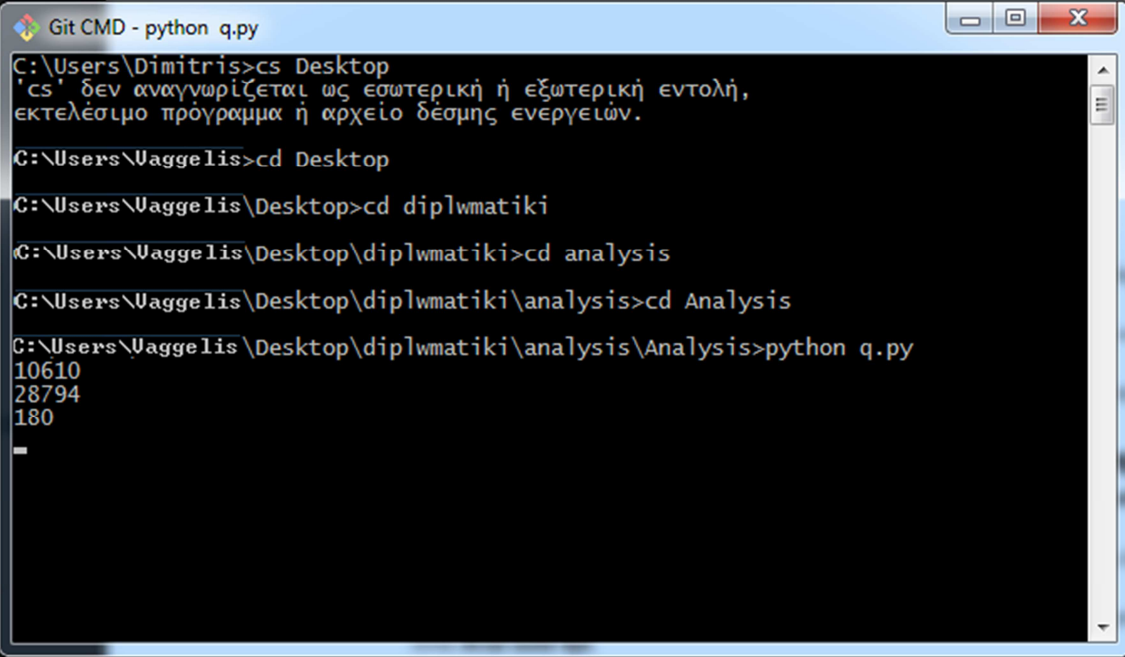
for r in db.APK.find({"so": {"$exists": True}}):
    try:
        if len(r["so"]) > 0:
            for j in range(len(r["so"])):
                print r["name"]+"|"+r["so"][j][0], r["so"][j][1]
    except KeyError:
        print "so array does not exist"

```

Αρχικά ο κώδικας έκανε έλεγχο και μας έβγαλε αποτελέσματα για τα πιστοποιητικά certs_depr, certs_ok και certs_md5 και τα αποτελέσματα βγήκαν σχεδόν άμεσα με πλήθος 10610, 28794 και 180 από το πλήθος των 62933 όπου έκανε έλεγχο.

Εκεί βλέπουμε ότι σε ποσοστό 18,86% οι εφαρμογές μας είχαν το πιστοποιητικό depr, σε ποσοστό 45.75% οι εφαρμογές μας είχαν το πιστοποιητικό ok και σε ποσοστό 0,29% οι εφαρμογές μας είχαν το πιστοποιητικό md5.

Ο αλγόριθμος MD5 είναι μια ευρέως χρησιμοποιούμενη λειτουργία κατακερματισμού που παράγει μια τιμή κατακερματισμού 128 bit. Παρόλο που το MD5 σχεδιάστηκε αρχικά για να χρησιμοποιηθεί ως κρυπτογραφική λειτουργία κατακερματισμού, έχει βρεθεί ότι είναι ευάλωτο από εκτεταμένες ευπάθειες. Μπορεί ακόμα να χρησιμοποιηθεί ως έλεγχος για την επαλήθευση της ακεραιότητας των δεδομένων, αλλά μόνο ενάντια στην ακούσια διαφθορά.



```
Git CMD - python q.py
C:\Users\Dimitris>cd Desktop
'cd' δεν αναγνωρίζεται ως εσωτερική ή εξωτερική εντολή,
εκτελέσιμο πρόγραμμα ή αρχείο δέσμης ενεργειών.
C:\Users\Uaggelis>cd Desktop
C:\Users\Uaggelis\Desktop>cd διπλωματική
C:\Users\Uaggelis\Desktop\διπλωματική>cd analysis
C:\Users\Uaggelis\Desktop\διπλωματική\analysis>cd Analysis
C:\Users\Uaggelis\Desktop\διπλωματική\analysis\Analysis>python q.py
10610
28794
180
-
```

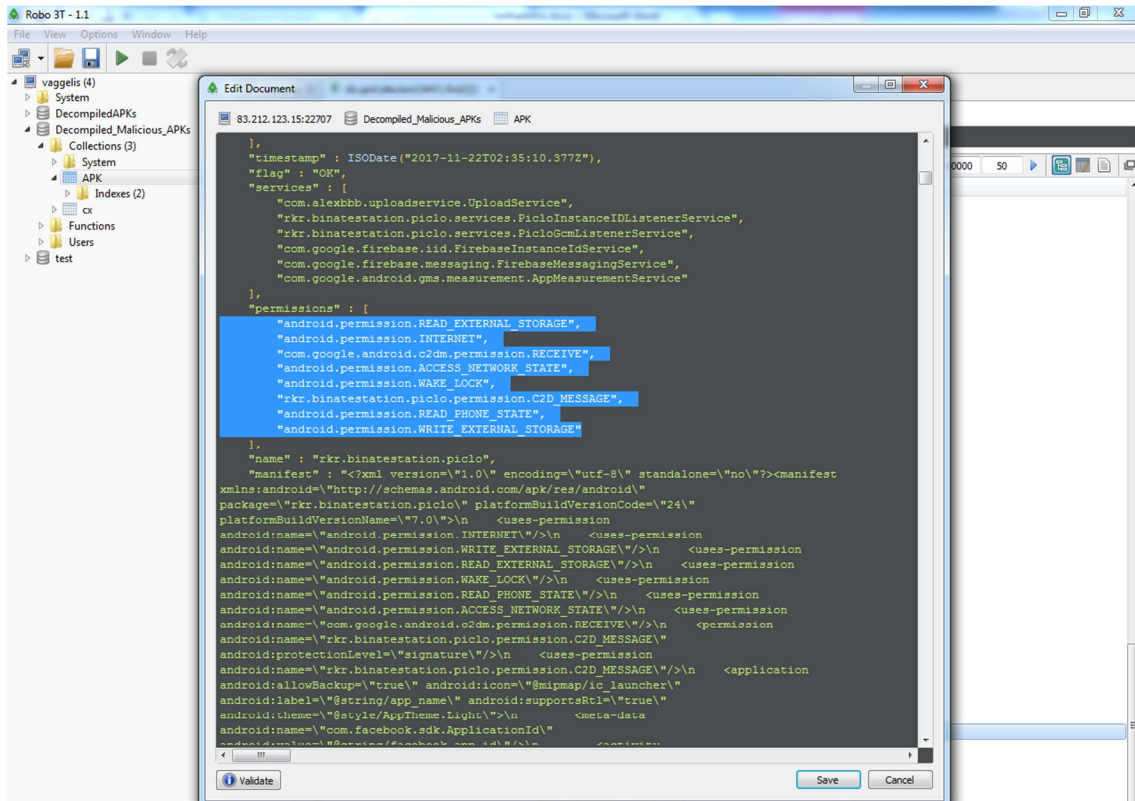
Στιγμιότυπο 7 εκτέλεση κώδικα

Στη συνέχεια μέσω του κώδικα προσπελαύνονται τα δεδομένα της βάσης με σκοπό να αναζητηθούν σε κάθε πίνακα πληροφοριών τα δικαιώματα που απαιτεί κάθε εφαρμογή από τον χρήστη. Παρακάτω φαίνονται κάποια από αυτά όπου μέσω της έγκρισης του χρήστη δίνεται η πρόσβαση από την ανάγνωση των επαφών, μέχρι τον έλεγχο της κάμερας. Στο σημείο αυτό η κάθε «αθώα» για εμάς εφαρμογή φαίνεται να μπορεί να είναι η αιτία παραβίασης των προσωπικών μας δεδομένων και η χρήση τους από οποιονδήποτε μπορεί να έχει πρόσβαση στην εφαρμογή ή να πληρώσει το ανάλογο αντίτιμο για να τα πάρει.

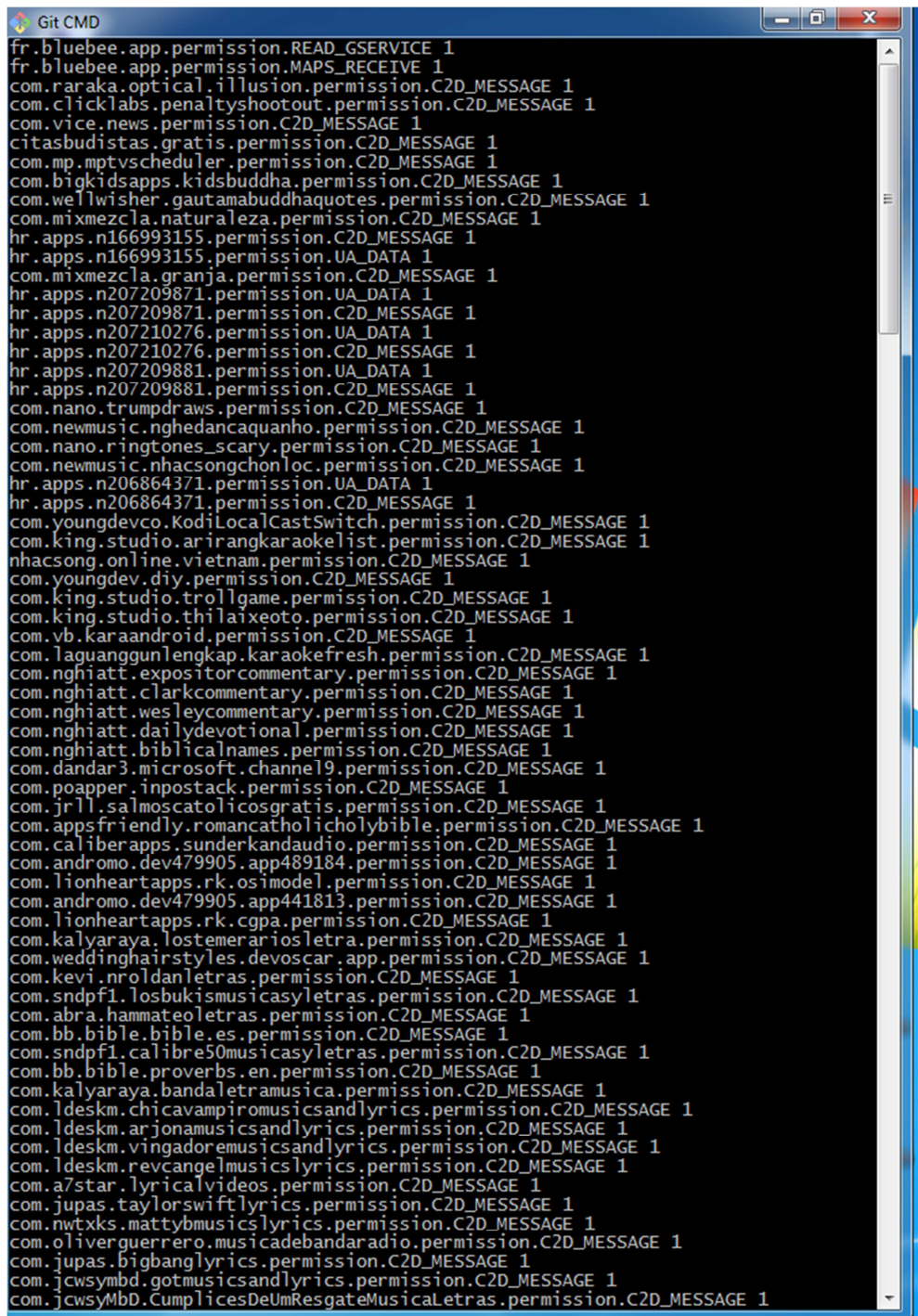
Τα δικαιώματα σε πάρα πολλές από τις εφαρμογές μας είναι κοινά πχ. Δυνατότητα πρόσβασης στο ασύρματο προσαρμογέα της συσκευής, πρόσβαση στο κατάλογο επαφών.

```
"android.permission.DISABLE_KEYGUARD",
"android.permission.ACCESS_NETWORK_STATE",
```

```
"android.permission.WAKE_LOCK",  
"android.permission.ACCESS_WIFI_STATE",  
"android.permission.INTERNET",  
"android.permission.WRITE_EXTERNAL_STORAGE"  
"android.permission.READ_EXTERNAL_STORAGE",  
"android.permission.INTERNET",  
"com.google.android.c2dm.permission.RECEIVE",  
"android.permission.WAKE_LOCK",  
"rkr.binatestation.piclo.permission.C2D_MESSAGE",  
"android.permission.READ_PHONE_STATE",  
"android.permission.CHANGE_NETWORK_STATE",  
"android.permission.RECEIVE_BOOT_COMPLETED",  
"android.permission.WRITE_SETTINGS",  
"com.google.android.c2dm.permission.RECEIVE",  
"android.permission.WAKE_LOCK",  
"android.permission.GET_TASKS",  
"android.permission.CHANGE_WIFI_STATE",  
"android.permission.RECORD_AUDIO",  
"android.permission.MOUNT_UNMOUNT_FILESYSTEMS",  
"android.permission.WRITE_EXTERNAL_STORAGE"  
"android.permission.VIBRATE"  
"android.permission.READ_CONTACTS"
```



Στιγμιότυπο 8 εμφάνισης δεδομένων βάσης

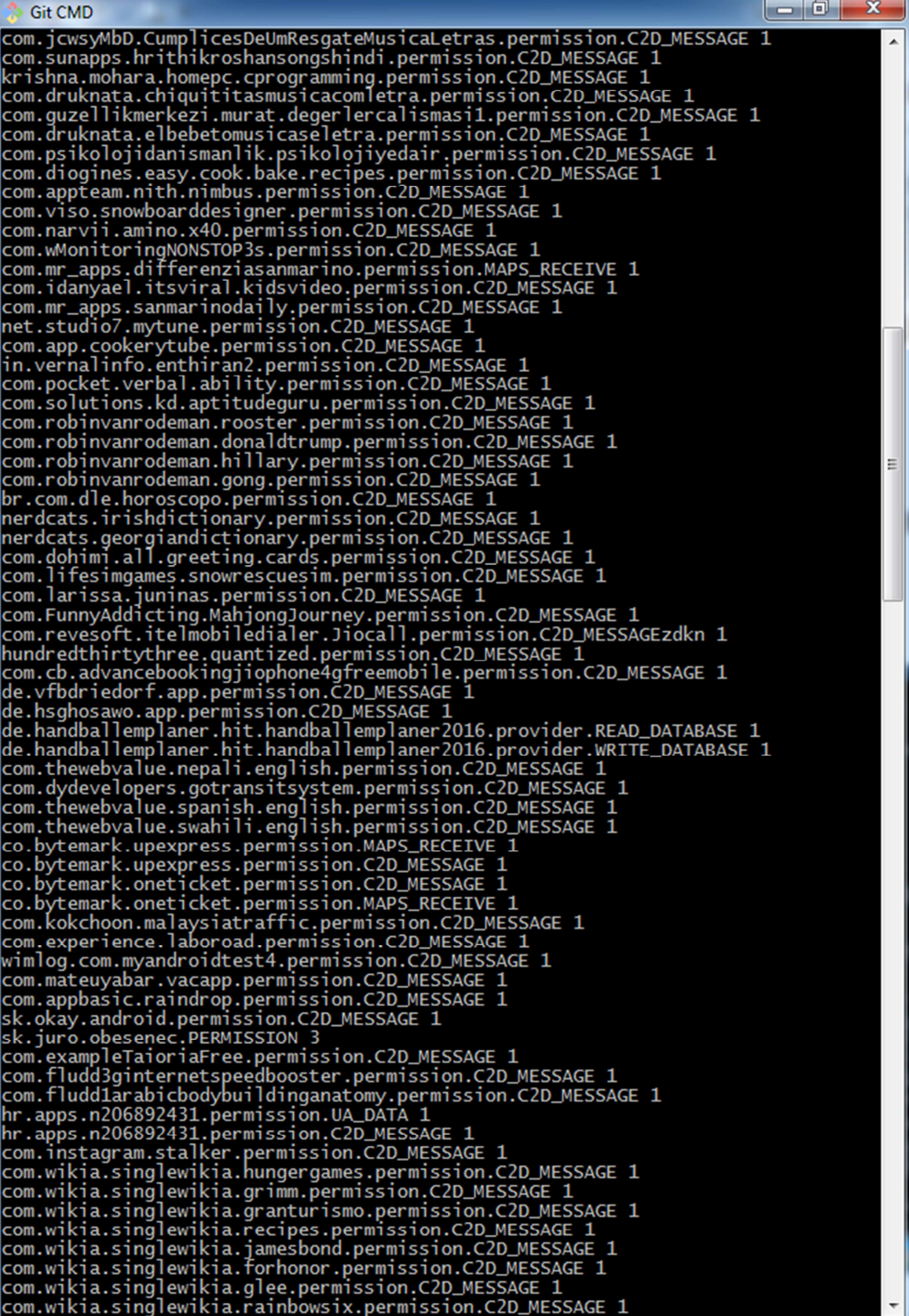


```

Git CMD
fr.bluebee.app.permission.READ_GSERVICE 1
fr.bluebee.app.permission.MAPS_RECEIVE 1
com.raraka.optical.illusion.permission.C2D_MESSAGE 1
com.clicklabs.penaltyshootout.permission.C2D_MESSAGE 1
com.vice.news.permission.C2D_MESSAGE 1
citasbudistas.gratis.permission.C2D_MESSAGE 1
com.mp.mptvscheduler.permission.C2D_MESSAGE 1
com.bigkidsapps.kidsbuddha.permission.C2D_MESSAGE 1
com.wellwisher.gautambuddhaquotes.permission.C2D_MESSAGE 1
com.mixmezcla.naturaleza.permission.C2D_MESSAGE 1
hr.apps.n166993155.permission.C2D_MESSAGE 1
hr.apps.n166993155.permission.UA_DATA 1
com.mixmezcla.granja.permission.C2D_MESSAGE 1
hr.apps.n207209871.permission.UA_DATA 1
hr.apps.n207209871.permission.C2D_MESSAGE 1
hr.apps.n207210276.permission.UA_DATA 1
hr.apps.n207210276.permission.C2D_MESSAGE 1
hr.apps.n207209881.permission.UA_DATA 1
hr.apps.n207209881.permission.C2D_MESSAGE 1
com.nano.trumpdraws.permission.C2D_MESSAGE 1
com.newmusic.nghedancaquanho.permission.C2D_MESSAGE 1
com.nano.ringtones_scary.permission.C2D_MESSAGE 1
com.newmusic.nhacsongchonloc.permission.C2D_MESSAGE 1
hr.apps.n206864371.permission.UA_DATA 1
hr.apps.n206864371.permission.C2D_MESSAGE 1
com.youngdevco.KodiLocalCastSwitch.permission.C2D_MESSAGE 1
com.king.studio.arirangkaraoke1st.permission.C2D_MESSAGE 1
nhacsong.online.vietnam.permission.C2D_MESSAGE 1
com.youngdev.diy.permission.C2D_MESSAGE 1
com.king.studio.trollgame.permission.C2D_MESSAGE 1
com.king.studio.thilaixeoto.permission.C2D_MESSAGE 1
com.vb.karaandroid.permission.C2D_MESSAGE 1
com.laguanggunlengkap.karaokefresh.permission.C2D_MESSAGE 1
com.nghiatt.expositorcommentary.permission.C2D_MESSAGE 1
com.nghiatt.clarkcommentary.permission.C2D_MESSAGE 1
com.nghiatt.wesleycommentary.permission.C2D_MESSAGE 1
com.nghiatt.dailydevotional.permission.C2D_MESSAGE 1
com.nghiatt.biblicalnames.permission.C2D_MESSAGE 1
com.dandar3.microsoft.channel9.permission.C2D_MESSAGE 1
com.poapper.inpostack.permission.C2D_MESSAGE 1
com.jrll.salmoscatolicosgratis.permission.C2D_MESSAGE 1
com.appsfriendly.romancatholicolybible.permission.C2D_MESSAGE 1
com.caliberapps.sunderkandaudio.permission.C2D_MESSAGE 1
com.andromo.dev479905.app489184.permission.C2D_MESSAGE 1
com.lionheartapps.rk.osimodel.permission.C2D_MESSAGE 1
com.andromo.dev479905.app441813.permission.C2D_MESSAGE 1
com.lionheartapps.rk.cgpa.permission.C2D_MESSAGE 1
com.kalyaraya.lostemerariosletra.permission.C2D_MESSAGE 1
com.weddinghairstyles.devoscar.app.permission.C2D_MESSAGE 1
com.kevi.nroldanletras.permission.C2D_MESSAGE 1
com.sndpf1.losbukismusicasyletras.permission.C2D_MESSAGE 1
com.abra.hammateoletras.permission.C2D_MESSAGE 1
com.bb.bible.bible.es.permission.C2D_MESSAGE 1
com.sndpf1.calibre50musicasyletras.permission.C2D_MESSAGE 1
com.bb.bible.proverbs.en.permission.C2D_MESSAGE 1
com.kalyaraya.bandaletramusica.permission.C2D_MESSAGE 1
com.ldeskm.chicavampiomusicsandlyrics.permission.C2D_MESSAGE 1
com.ldeskm.arjonamusicsandlyrics.permission.C2D_MESSAGE 1
com.ldeskm.vingadoremusicsandlyrics.permission.C2D_MESSAGE 1
com.ldeskm.revcangelmusiclyrics.permission.C2D_MESSAGE 1
com.a7star.lyricalvideos.permission.C2D_MESSAGE 1
com.jupas.taylorswiftlyrics.permission.C2D_MESSAGE 1
com.nwtxks.mattybmusiclyrics.permission.C2D_MESSAGE 1
com.oliverguerrero.musicadebandaradio.permission.C2D_MESSAGE 1
com.jupas.bigbanglyrics.permission.C2D_MESSAGE 1
com.jcwsymbd.gotmusicandlyrics.permission.C2D_MESSAGE 1
com.jcwsymbd.CumplicesDeUmResgateMusicalletras.permission.C2D_MESSAGE 1

```

Στιγμιότυπο 9 εκτέλεση κώδικα

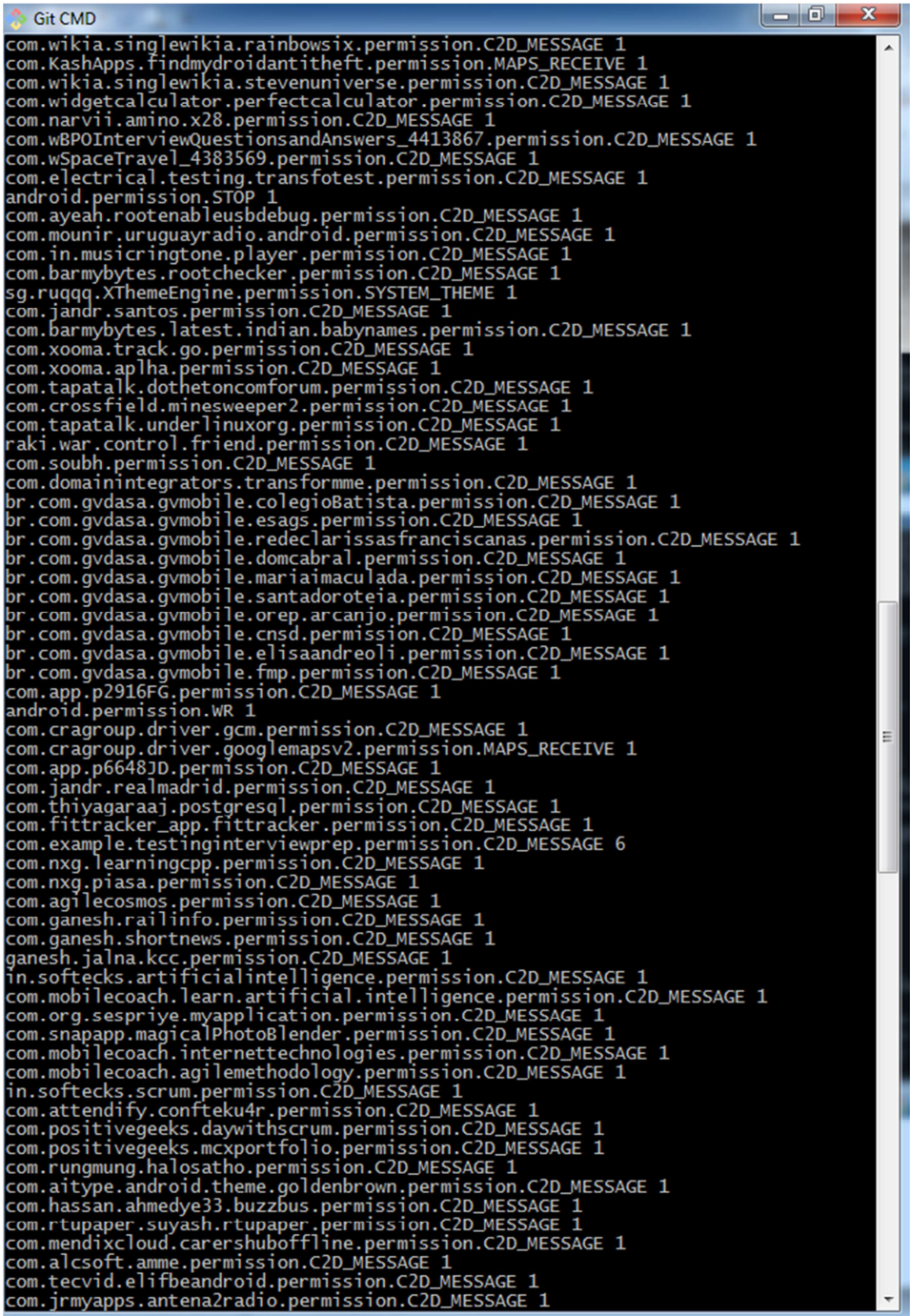


```

Git CMD
com.jcwsyMbd.CumplicesDeUmResgateMusicaLetras.permission.C2D_MESSAGE 1
com.sunapps.hrithikroshansongshindi.permission.C2D_MESSAGE 1
krishna.mohara.homepc.cprogramming.permission.C2D_MESSAGE 1
com.druknata.chiquititasmusicacomletra.permission.C2D_MESSAGE 1
com.guzellikmerkezi.murat.degerlercalismasi1.permission.C2D_MESSAGE 1
com.druknata.elbetetomusicaseletra.permission.C2D_MESSAGE 1
com.psikolojidanismanlik.psikolojiyedair.permission.C2D_MESSAGE 1
com.diogines.easy.cook.bake.recipes.permission.C2D_MESSAGE 1
com.appteam.nith.nimbus.permission.C2D_MESSAGE 1
com.viso.snowboarddesigner.permission.C2D_MESSAGE 1
com.narvii.amino.x40.permission.C2D_MESSAGE 1
com.wMonitoringNONSTOP3s.permission.C2D_MESSAGE 1
com.mr_apps.differenziasanmarino.permission.MAPS_RECEIVE 1
com.idanyael.itsviral.kidsvideo.permission.C2D_MESSAGE 1
com.mr_apps.sanmarinodaily.permission.C2D_MESSAGE 1
net.studio7.mytune.permission.C2D_MESSAGE 1
com.app.cookerytube.permission.C2D_MESSAGE 1
in.vernalinfo.enthiran2.permission.C2D_MESSAGE 1
com.pocket.verbal.ability.permission.C2D_MESSAGE 1
com.solutions.kd.apitudeguru.permission.C2D_MESSAGE 1
com.robinvanrodeman.rooster.permission.C2D_MESSAGE 1
com.robinvanrodeman.donaldtrump.permission.C2D_MESSAGE 1
com.robinvanrodeman.hillary.permission.C2D_MESSAGE 1
com.robinvanrodeman.gong.permission.C2D_MESSAGE 1
br.com.dle.horoscopo.permission.C2D_MESSAGE 1
nerdcats.irishdictionary.permission.C2D_MESSAGE 1
nerdcats.georgiandictionary.permission.C2D_MESSAGE 1
com.dohmi.all.greeting.cards.permission.C2D_MESSAGE 1
com.lifesimgames.snowrescuesim.permission.C2D_MESSAGE 1
com.larissa.juninas.permission.C2D_MESSAGE 1
com.FunnyAddicting.MahjongJourney.permission.C2D_MESSAGE 1
com.revesoft.itelmobiledialer.Jiocall.permission.C2D_MESSAGEzdkn 1
hundredthirtythree.quantized.permission.C2D_MESSAGE 1
com.cb.advancebookingjioophone4gfreemobile.permission.C2D_MESSAGE 1
de.vfbdriedorf.app.permission.C2D_MESSAGE 1
de.hsghosawo.app.permission.C2D_MESSAGE 1
de.handballplanner.hit.handballplanner2016.provider.READ_DATABASE 1
de.handballplanner.hit.handballplanner2016.provider.WRITE_DATABASE 1
com.thewebvalue.nepali.english.permission.C2D_MESSAGE 1
com.dydevelopers.gotransitsystem.permission.C2D_MESSAGE 1
com.thewebvalue.spanish.english.permission.C2D_MESSAGE 1
com.thewebvalue.swahili.english.permission.C2D_MESSAGE 1
co.bytemark.upexpress.permission.MAPS_RECEIVE 1
co.bytemark.upexpress.permission.C2D_MESSAGE 1
co.bytemark.oneticket.permission.C2D_MESSAGE 1
co.bytemark.oneticket.permission.MAPS_RECEIVE 1
com.kokchoon.malaysiatraffic.permission.C2D_MESSAGE 1
com.experience.laboroad.permission.C2D_MESSAGE 1
wimlog.com.myandroidtest4.permission.C2D_MESSAGE 1
com.mateuyabar.vacapp.permission.C2D_MESSAGE 1
com.appbasic.raindrop.permission.C2D_MESSAGE 1
sk.okay.android.permission.C2D_MESSAGE 1
sk.juro.obesenec.PERMISSION 3
com.exampleTaioriaFree.permission.C2D_MESSAGE 1
com.fludd3ginternetspeedbooster.permission.C2D_MESSAGE 1
com.fludd1arabicbodybuildinganatomy.permission.C2D_MESSAGE 1
hr.apps.n206892431.permission.UA_DATA 1
hr.apps.n206892431.permission.C2D_MESSAGE 1
com.instagram.stalker.permission.C2D_MESSAGE 1
com.wikia.singlewikia.hungergames.permission.C2D_MESSAGE 1
com.wikia.singlewikia.grimm.permission.C2D_MESSAGE 1
com.wikia.singlewikia.granturismo.permission.C2D_MESSAGE 1
com.wikia.singlewikia.recipes.permission.C2D_MESSAGE 1
com.wikia.singlewikia.jamesbond.permission.C2D_MESSAGE 1
com.wikia.singlewikia.forhonor.permission.C2D_MESSAGE 1
com.wikia.singlewikia.ilee.permission.C2D_MESSAGE 1
com.wikia.singlewikia.rainbowsix.permission.C2D_MESSAGE 1

```

Στιγμιότυπο 10 εκτέλεση κώδικα



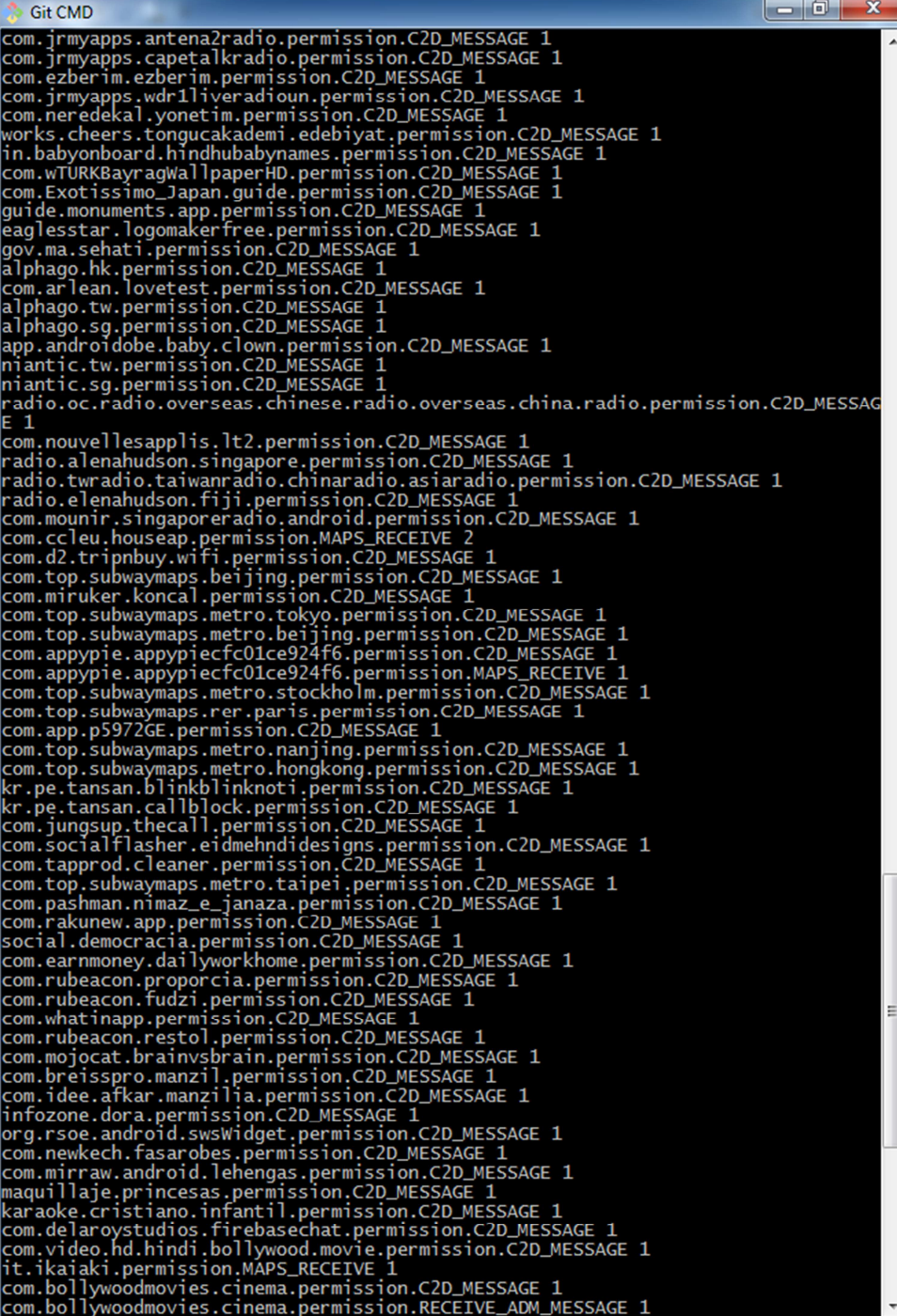
```

Git CMD
com.wikia.singlewikia.rainbowsix.permission.C2D_MESSAGE 1
com.KashApps.findmydroidantitheft.permission.MAPS_RECEIVE 1
com.wikia.singlewikia.stevenuniverse.permission.C2D_MESSAGE 1
com.widgetcalculator.perfectcalculator.permission.C2D_MESSAGE 1
com.narvii.amino.x28.permission.C2D_MESSAGE 1
com.wBPOInterviewQuestionsandAnswers_4413867.permission.C2D_MESSAGE 1
com.wSpaceTravel_4383569.permission.C2D_MESSAGE 1
com.electrical.testing.transfotest.permission.C2D_MESSAGE 1
android.permission.STOP 1
com.ayeah.rootenableusbdebug.permission.C2D_MESSAGE 1
com.mounir.uruguayradio.android.permission.C2D_MESSAGE 1
com.in.musicringtone.player.permission.C2D_MESSAGE 1
com.barmybytes.rootchecker.permission.C2D_MESSAGE 1
sg.ruqqq.XThemeEngine.permission.SYSTEM_THEME 1
com.jandr.santos.permission.C2D_MESSAGE 1
com.barmybytes.latest.indian.babynames.permission.C2D_MESSAGE 1
com.xooma.track.go.permission.C2D_MESSAGE 1
com.xooma.aplha.permission.C2D_MESSAGE 1
com.tapataalk.dotheoncomforum.permission.C2D_MESSAGE 1
com.crossfield.minesweeper2.permission.C2D_MESSAGE 1
com.tapataalk.underlinuxorg.permission.C2D_MESSAGE 1
raki.war.control.friend.permission.C2D_MESSAGE 1
com.soubh.permission.C2D_MESSAGE 1
com.domainintegrators.transformme.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.colegioBatista.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.esags.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.redeclarissasfranciscanas.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.domcabral.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.mariamaquilada.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.santadoroteia.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.orep.arcanjo.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.cnsd.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.elisaandreoli.permission.C2D_MESSAGE 1
br.com.gvdasa.gvmobile.fmp.permission.C2D_MESSAGE 1
com.app.p2916FG.permission.C2D_MESSAGE 1
android.permission.WR 1
com.cragroup.driver.gcm.permission.C2D_MESSAGE 1
com.cragroup.driver.googlemapsv2.permission.MAPS_RECEIVE 1
com.app.p6648JD.permission.C2D_MESSAGE 1
com.jandr.realmadrid.permission.C2D_MESSAGE 1
com.thiyagaraaj.postgresql.permission.C2D_MESSAGE 1
com.fittracker_app.fittracker.permission.C2D_MESSAGE 1
com.example.testinginterviewprep.permission.C2D_MESSAGE 6
com.nxg.learningcpp.permission.C2D_MESSAGE 1
com.nxg.piasa.permission.C2D_MESSAGE 1
com.agilecosmos.permission.C2D_MESSAGE 1
com.ganesh.railinfo.permission.C2D_MESSAGE 1
com.ganesh.shortnews.permission.C2D_MESSAGE 1
ganesh.jalna.kcc.permission.C2D_MESSAGE 1
in.softecks.artificialintelligence.permission.C2D_MESSAGE 1
com.mobilecoach.learn.artificial.intelligence.permission.C2D_MESSAGE 1
com.org.sespriye.myapplication.permission.C2D_MESSAGE 1
com.snapapp.magicalPhotoBlender.permission.C2D_MESSAGE 1
com.mobilecoach.internettechnologies.permission.C2D_MESSAGE 1
com.mobilecoach.agilemethodology.permission.C2D_MESSAGE 1
in.softecks.scrum.permission.C2D_MESSAGE 1
com.attendify.confteku4r.permission.C2D_MESSAGE 1
com.positivegeeks.daywithscrums.permission.C2D_MESSAGE 1
com.positivegeeks.mcxportfolio.permission.C2D_MESSAGE 1
com.rungmung.halosatho.permission.C2D_MESSAGE 1
com.aitype.android.theme.goldenbrown.permission.C2D_MESSAGE 1
com.hassan.ahmedye33.buzzbus.permission.C2D_MESSAGE 1
com.rtupaper.suyash.rtupaper.permission.C2D_MESSAGE 1
com.mendixcloud.carershuboffline.permission.C2D_MESSAGE 1
com.alcsoft.amme.permission.C2D_MESSAGE 1
com.tecvid.elifbeandroid.permission.C2D_MESSAGE 1
com.jrmyapps.antena2radio.permission.C2D_MESSAGE 1

```

Στιγμιότυπο 11 εκτέλεση κώδικα

Αυτοματοποιημένη συλλογή και ανάλυση Android εφαρμογών από το Google Play.



```

Git CMD
com.jrmyapps.antenaradio.permission.C2D_MESSAGE 1
com.jrmyapps.capetalkradio.permission.C2D_MESSAGE 1
com.ezberim.ezberim.permission.C2D_MESSAGE 1
com.jrmyapps.wdr11liveradioun.permission.C2D_MESSAGE 1
com.neredekal.yonetim.permission.C2D_MESSAGE 1
works.cheers.tongucakademi.edebiyat.permission.C2D_MESSAGE 1
in.babyonboard.hindhubbabynames.permission.C2D_MESSAGE 1
com.wTURKBayragwallpaperHD.permission.C2D_MESSAGE 1
com.Exotissimo_Japan.guide.permission.C2D_MESSAGE 1
guide.monuments.app.permission.C2D_MESSAGE 1
eaglesstar.logomakerfree.permission.C2D_MESSAGE 1
gov.ma.sehati.permission.C2D_MESSAGE 1
alphago.hk.permission.C2D_MESSAGE 1
com.arlean.lovetest.permission.C2D_MESSAGE 1
alphago.tw.permission.C2D_MESSAGE 1
alphago.sg.permission.C2D_MESSAGE 1
app.androidobe.baby.clown.permission.C2D_MESSAGE 1
niantic.tw.permission.C2D_MESSAGE 1
niantic.sg.permission.C2D_MESSAGE 1
radio.oc.radio.overseas.chinese.radio.overseas.china.radio.permission.C2D_MESSAG
E 1
com.nouvellesapplis.lt2.permission.C2D_MESSAGE 1
radio.alenahudson.singapore.permission.C2D_MESSAGE 1
radio.twradio.taiwanradio.chinaradio.asiaradio.permission.C2D_MESSAGE 1
radio.elenahudson.fiji.permission.C2D_MESSAGE 1
com.mounir.singaporeradio.android.permission.C2D_MESSAGE 1
com.ccleu.houseap.permission.MAPS_RECEIVE 2
com.d2.tripnbuy.wifi.permission.C2D_MESSAGE 1
com.top.subwaymaps.beijing.permission.C2D_MESSAGE 1
com.miruker.koncal.permission.C2D_MESSAGE 1
com.top.subwaymaps.metro.tokyo.permission.C2D_MESSAGE 1
com.top.subwaymaps.metro.beijing.permission.C2D_MESSAGE 1
com.appypie.appypiecf01ce924f6.permission.C2D_MESSAGE 1
com.appypie.appypiecf01ce924f6.permission.MAPS_RECEIVE 1
com.top.subwaymaps.metro.stockholm.permission.C2D_MESSAGE 1
com.top.subwaymaps.rer.paris.permission.C2D_MESSAGE 1
com.app.p5972GE.permission.C2D_MESSAGE 1
com.top.subwaymaps.metro.nanjing.permission.C2D_MESSAGE 1
com.top.subwaymaps.metro.hongkong.permission.C2D_MESSAGE 1
kr.pe.tansan.blinkblinknoti.permission.C2D_MESSAGE 1
kr.pe.tansan.callblock.permission.C2D_MESSAGE 1
com.jungsup.thecall.permission.C2D_MESSAGE 1
com.socialflasher.eidmehndidesigns.permission.C2D_MESSAGE 1
com.tapprod.cleaner.permission.C2D_MESSAGE 1
com.top.subwaymaps.metro.taipei.permission.C2D_MESSAGE 1
com.pashman.nimaz_e_janaza.permission.C2D_MESSAGE 1
com.rakunew.app.permission.C2D_MESSAGE 1
social.democracia.permission.C2D_MESSAGE 1
com.earnmoney.dailyworkhome.permission.C2D_MESSAGE 1
com.rubeacon.proporcia.permission.C2D_MESSAGE 1
com.rubeacon.fudzi.permission.C2D_MESSAGE 1
com.whatinapp.permission.C2D_MESSAGE 1
com.rubeacon.restol.permission.C2D_MESSAGE 1
com.mojocat.brainvsbrain.permission.C2D_MESSAGE 1
com.breisspro.manzil.permission.C2D_MESSAGE 1
com.idee.afkar.manzilia.permission.C2D_MESSAGE 1
infozone.dora.permission.C2D_MESSAGE 1
org.rsoe.android.swsWidget.permission.C2D_MESSAGE 1
com.newkech.fasarobes.permission.C2D_MESSAGE 1
com.mirraw.android.lehengas.permission.C2D_MESSAGE 1
maquillaje.princesas.permission.C2D_MESSAGE 1
karaoke.cristiano.infantil.permission.C2D_MESSAGE 1
com.delaroystudios.firebaseiochat.permission.C2D_MESSAGE 1
com.video.hd.hindi.bollywood.movie.permission.C2D_MESSAGE 1
it.ikakiaki.permission.MAPS_RECEIVE 1
com.bollywoodmovies.cinema.permission.C2D_MESSAGE 1
com.bollywoodmovies.cinema.permission.RECEIVE_ADM_MESSAGE 1

```

Στιγμιότυπο 12 εκτέλεση κώδικα

Αυτοματοποιημένη συλλογή και ανάλυση Android εφαρμογών από το Google Play.

Οι κυριότερες απαιτήσεις δικαιωμάτων τις οποίες ουσιαστικά παραχωρεί κάθε χρήστης δίνοντας πλήρη πρόσβαση σε αυτό που η εφαρμογή απαιτεί είναι οι παρακάτω:

String	ACCESS_CHECKIN_PROPERTIES Επιτρέπει την πρόσβαση ανάγνωσης / εγγραφής στον πίνακα "ιδιότητες" στη βάση δεδομένων checkin, για να αλλάξει τις τιμές που μεταφορτώνονται.
String	ACCESS_COARSE_LOCATION Επιτρέπει σε μια εφαρμογή να έχει πρόσβαση σε κατά προσέγγιση τοποθεσία.
String	ACCESS_FINE_LOCATION Επιτρέπει σε μια εφαρμογή πρόσβαση σε ακριβή τοποθεσία.
String	ACCESS_LOCATION_EXTRA_COMMANDS Επιτρέπει σε μια εφαρμογή να αποκτά πρόσβαση σε πρόσθετες εντολές παροχής παρόχου τοποθεσίας.
String	ACCESS_NETWORK_STATE Επιτρέπει στις εφαρμογές την πρόσβαση σε πληροφορίες σχετικά με δίκτυα.
String	ACCESS_NOTIFICATION_POLICY Άδεια σήμανσης για εφαρμογές που επιθυμούν να έχουν πρόσβαση στην πολιτική ειδοποιήσεων.
String	ACCESS_WIFI_STATE Επιτρέπει στις εφαρμογές πρόσβαση σε πληροφορίες σχετικά με τα δίκτυα Wi-Fi.
String	ACCOUNT_MANAGER Επιτρέπει στις εφαρμογές να πραγματοποιούν κλήσεις στους λογαριασμούς λογαριασμού λογαριασμών.
String	ADD_VOICEMAIL Επιτρέπει σε μια εφαρμογή να προσθέσει φωνητικά μηνύματα στο σύστημα.
String	ANSWER_PHONE_CALLS Επιτρέπει στην εφαρμογή να απαντά σε μια εισερχόμενη τηλεφωνική κλήση.
String	BATTERY_STATS Επιτρέπει σε μια εφαρμογή τη συλλογή στατιστικών στοιχείων μπαταρίας
String	BIND_ACCESSIBILITY_SERVICE Πρέπει να απαιτείται από μια υπηρεσία AccessibilityService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.
String	BIND_APPWIDGET Επιτρέπει σε μια εφαρμογή να ενημερώσει την υπηρεσία AppWidget σε ποια εφαρμογή μπορεί να έχει πρόσβαση στα δεδομένα του AppWidget.
String	BIND_AUTOFILL_SERVICE Πρέπει να απαιτείται από μια υπηρεσία AutofillService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_CARRIER_MESSAGING_SERVICE

	<i>Αυτή η σταθερά έχει καταργηθεί στο επίπεδο API 23. Χρησιμοποιήστε το BIND_CARRIER_SERVICES αντί αυτού</i>
String	BIND_CARRIER_SERVICES Η διαδικασία του συστήματος που επιτρέπεται να δεσμεύει τις υπηρεσίες σε εφαρμογές φορέα θα έχει αυτήν την άδεια.
String	BIND_CHOOSER_TARGET_SERVICE Πρέπει να απαιτείται από μια υπηρεσία ChooserTargetService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_CONDITION_PROVIDER_SERVICE Πρέπει να απαιτείται από την υπηρεσία ConditionProviderService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_DEVICE_ADMIN Πρέπει να απαιτείται από το δέκτη διαχείρισης συσκευών, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να αλληλεπιδράσει με αυτό.
String	BIND_DREAM_SERVICE Πρέπει να απαιτείται από μια υπηρεσία DreamService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_INCALL_SERVICE Πρέπει να απαιτείται από μια InCallService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_INPUT_METHOD Πρέπει να απαιτείται από ένα InputMethodService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_MIDI_DEVICE_SERVICE Πρέπει να απαιτείται από ένα MidiDeviceService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_NFC_SERVICE Πρέπει να απαιτείται από ένα HostApduService ή το OffHostApduService για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_NOTIFICATION_LISTENER_SERVICE Πρέπει να απαιτείται από μια υπηρεσία NotificationListenerService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_PRINT_SERVICE Πρέπει να απαιτείται από μια υπηρεσία PrintService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_QUICK_SETTINGS_TILE Επιτρέπει σε μια εφαρμογή να δεσμεύει τα πλακάκια γρήγορων ρυθμίσεων τρίτου μέρους.
String	BIND_REMOTEVIEWS Πρέπει να απαιτείται από μια υπηρεσία RemoteViewsService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.

String	BIND_SCREENING_SERVICE Πρέπει να απαιτείται από μια υπηρεσία CallScreeningService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_TELECOM_CONNECTION_SERVICE Πρέπει να απαιτείται από μια ConnectionService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_TEXT_SERVICE Πρέπει να απαιτείται από ένα TextService (π.χ.
String	BIND_TV_INPUT Πρέπει να απαιτείται από μια υπηρεσία TvInputService για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_VISUAL_VOICEMAIL_SERVICE Πρέπει να απαιτείται από μια σύνδεση VisualVoicemailService για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.
String	BIND_VOICE_INTERACTION Πρέπει να απαιτείται από μια υπηρεσία VoiceInteractionService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_VPN_SERVICE Πρέπει να απαιτείται από μια υπηρεσία VpnService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BIND_VR_LISTENER_SERVICE Πρέπει να απαιτείται από ένα VrListenerService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.
String	BIND_WALLPAPER Πρέπει να απαιτείται από μια υπηρεσία WallpaperService , για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.
String	BLUETOOTH Επιτρέπει στις εφαρμογές τη σύνδεση σε συνδυασμένες συσκευές Bluetooth.
String	BLUETOOTH_ADMIN Επιτρέπει στις εφαρμογές να ανακαλύπτουν και να συνδυάζουν συσκευές Bluetooth.
String	BLUETOOTH_PRIVILEGED Επιτρέπει στις εφαρμογές να αντιστοιχούν συσκευές Bluetooth χωρίς αλληλεπίδραση χρηστών και να επιτρέπουν ή να απαγορεύουν την πρόσβαση στον τηλεφωνικό κατάλογο ή την πρόσβαση σε μηνύματα.
String	BODY_SENSORS Επιτρέπει σε μια εφαρμογή την πρόσβαση σε δεδομένα από αισθητήρες που χρησιμοποιεί ο χρήστης για να μετρήσει τι συμβαίνει στο σώμα του / της, όπως ο καρδιακός ρυθμός.
String	BROADCAST_PACKAGE_REMOVED Επιτρέπει σε μια εφαρμογή να μεταδίδει ειδοποίηση ότι ένα πακέτο εφαρμογής έχει καταργηθεί.

String	BROADCAST_SMS Επιτρέπει σε μια εφαρμογή να εκπέμπει ειδοποίηση απόδειξης SMS.
String	BROADCAST_STICKY Επιτρέπει σε μια εφαρμογή να μεταδίδει sticky intentions.
String	BROADCAST_WAP_PUSH Επιτρέπει σε μια εφαρμογή να εκπέμπει μια ειδοποίηση παραλαβής WAP PUSH.
String	CALL_PHONE Επιτρέπει σε μια εφαρμογή να ξεκινήσει μια τηλεφωνική κλήση χωρίς να περάσει από τη διεπαφή χρήστη Dialer για να επιβεβαιώσει την κλήση ο χρήστης.
String	CALL_PRIVILEGED Επιτρέπει σε μια εφαρμογή να καλέσει οποιονδήποτε αριθμό τηλεφώνου, συμπεριλαμβανομένων των αριθμών έκτακτης ανάγκης, χωρίς να περάσει από τη διεπαφή χρήστη Dialer για να επιβεβαιώσει ο χρήστης την κλήση.
String	CAMERA Απαιτείται να έχετε πρόσβαση στη συσκευή κάμερας.
String	CAPTURE_AUDIO_OUTPUT Επιτρέπει σε μια εφαρμογή να καταγράψει την έξοδο ήχου.
String	CAPTURE_SECURE_VIDEO_OUTPUT Επιτρέπει σε μια εφαρμογή να συλλάβει ασφαλή έξοδο βίντεο.
String	CAPTURE_VIDEO_OUTPUT Επιτρέπει σε μια εφαρμογή να καταγράψει την έξοδο βίντεο.
String	CHANGE_COMPONENT_ENABLED_STATE Επιτρέπει σε μια εφαρμογή να αλλάξει αν είναι ενεργοποιημένη ή όχι μια συνιστώσα εφαρμογής (διαφορετική από τη δική της).
String	CHANGE_CONFIGURATION Επιτρέπει σε μια εφαρμογή να τροποποιήσει την τρέχουσα ρύθμιση παραμέτρων, όπως η τοπική ρύθμιση.
String	CHANGE_NETWORK_STATE Επιτρέπει στις εφαρμογές να αλλάζουν κατάσταση συνδεσιμότητας δικτύου.
String	CHANGE_WIFI_MULTICAST_STATE Επιτρέπει στις εφαρμογές να εισέλθουν στη λειτουργία Wi-Fi Multicast.
String	CHANGE_WIFI_STATE Επιτρέπει στις εφαρμογές να αλλάζουν την κατάσταση σύνδεσης Wi-Fi.
String	CLEAR_APP_CACHE Επιτρέπει σε μια εφαρμογή να εκκαθαρίσει τις προσωρινές μνήμες όλων των εγκατεστημένων εφαρμογών στη συσκευή.
String	CONTROL_LOCATION_UPDATES Επιτρέπει την ενεργοποίηση / απενεργοποίηση ειδοποιήσεων ενημέρωσης τοποθεσίας από το ραδιόφωνο.

String	DELETE_CACHE_FILES Επιτρέπει σε μια εφαρμογή τη διαγραφή αρχείων cache.
String	DELETE_PACKAGES Επιτρέπει σε μια εφαρμογή τη διαγραφή πακέτων.
String	DIAGNOSTIC Επιτρέπει τις εφαρμογές στο RW σε διαγνωστικούς πόρους.
String	DISABLE_KEYGUARD Επιτρέπει στις εφαρμογές να απενεργοποιούν το κλείδωμα πλήκτρων εάν δεν είναι ασφαλές.
String	DUMP Επιτρέπει σε μια εφαρμογή να ανακτά τις πληροφορίες απόστασης κατάστασης από υπηρεσίες συστήματος.
String	EXPAND_STATUS_BAR Επιτρέπει σε μια εφαρμογή να επεκτείνει ή να συμπύξει τη γραμμή κατάστασης.
String	FACTORY_TEST Εκτελέστε ως εφαρμογή δοκιμής κατασκευαστή, τρέχοντας ως χρήστης root.
String	GET_ACCOUNTS Επιτρέπει την πρόσβαση στη λίστα λογαριασμών στην Υπηρεσία Λογαριασμών.
String	GET_ACCOUNTS_PRIVILEGED Επιτρέπει την πρόσβαση στη λίστα λογαριασμών στην Υπηρεσία Λογαριασμών.
String	GET_PACKAGE_SIZE Επιτρέπει σε μια εφαρμογή να εντοπίσει το χώρο που χρησιμοποιείται από οποιοδήποτε πακέτο.
String	GET_TASKS <i>Αυτή η σταθερά αποκόπηκε στο επίπεδο API 21. Δεν ισχύει πλέον.</i>
String	GLOBAL_SEARCH Αυτή η άδεια μπορεί να χρησιμοποιηθεί στους παρόχους περιεχομένου για να επιτρέψει στο παγκόσμιο σύστημα αναζήτησης να έχει πρόσβαση στα δεδομένα του.
String	INSTALL_LOCATION_PROVIDER Επιτρέπει σε μια εφαρμογή να εγκαταστήσει έναν παροχέα τοποθεσίας στον Διαχειριστή τοποθεσίας.
String	INSTALL_PACKAGES Επιτρέπει σε μια εφαρμογή την εγκατάσταση πακέτων.
String	INSTALL_SHORTCUT Επιτρέπει σε μια εφαρμογή να εγκαταστήσει μια συντόμευση στο Launcher.
String	INSTANT_APP_FOREGROUND_SERVICE Επιτρέπει σε μια άμεση εφαρμογή τη δημιουργία υπηρεσιών προσκηνίου.
String	INTERNET Επιτρέπει στις εφαρμογές να ανοίγουν υποδοχές δικτύου.

String	KILL_BACKGROUND_PROCESSES Επιτρέπει σε μια εφαρμογή να καλέσει killBackgroundProcesses(String) .
String	LOCATION_HARDWARE Επιτρέπει σε μια εφαρμογή να χρησιμοποιεί λειτουργίες τοποθεσίας στο υλικό, όπως το geofencing api.
String	MANAGE_DOCUMENTS Επιτρέπει σε μια εφαρμογή να διαχειρίζεται την πρόσβαση σε έγγραφα, συνήθως ως μέρος ενός εργαλείου επιλογής εγγράφων.
String	MANAGE_OWN_CALLS Επιτρέπει σε μια εφαρμογή κλήσης η οποία διαχειρίζεται τις δικές της κλήσεις μέσω των αυτοδιαχειριζόμενων API ConnectionService .
String	MASTER_CLEAR Όχι για χρήση από εφαρμογές τρίτων κατασκευαστών.
String	MEDIA_CONTENT_CONTROL Επιτρέπει σε μια εφαρμογή να γνωρίζει ποιο περιεχόμενο αναπαράγεται και ελέγχει την αναπαραγωγή του.
String	MODIFY_AUDIO_SETTINGS Επιτρέπει σε μια εφαρμογή να τροποποιεί τις συνολικές ρυθμίσεις ήχου.
String	MODIFY_PHONE_STATE Επιτρέπει την τροποποίηση της κατάστασης τηλεφωνίας - ενεργοποίηση, mmi κ.λπ.
String	MOUNT_FORMAT_FILESYSTEMS Επιτρέπει τη μορφοποίηση συστημάτων αρχείων για αφαιρούμενη αποθήκευση.
String	MOUNT_UNMOUNT_FILESYSTEMS Επιτρέπει την τοποθέτηση και την αποσυναρμολόγηση συστημάτων αρχείων για αφαιρούμενη αποθήκευση.
String	NFC Επιτρέπει στις εφαρμογές να πραγματοποιούν λειτουργίες I / O μέσω NFC.
String	PACKAGE_USAGE_STATS Επιτρέπει σε μια εφαρμογή τη συλλογή στατιστικών στοιχείων χρήσης Η δήλωση της άδειας συνεπάγεται την πρόθεση χρήσης του API και ο χρήστης της συσκευής μπορεί να παραχωρήσει άδεια μέσω της εφαρμογής Ρυθμίσεις.
String	PERSISTENT_ACTIVITY <i>Αυτή η σταθερά καταργήθηκε στο επίπεδο API 9. Αυτή η λειτουργικότητα θα καταργηθεί στο μέλλον. μην χρησιμοποιείτε. Επιτρέψτε σε μια εφαρμογή να κάνει τις δραστηριότητές της επίμονες.</i>
String	PROCESS_OUTGOING_CALLS Επιτρέπει σε μια εφαρμογή να βλέπει τον αριθμό που καλείται κατά τη διάρκεια μιας εξερχόμενης κλήσης με την επιλογή ανακατεύθυνσης της κλήσης σε διαφορετικό αριθμό ή διακοπής της κλήσης συνολικά.
String	READ_CALENDAR

	Επιτρέπει σε μια εφαρμογή να διαβάσει τα δεδομένα ημερολογίου του χρήστη.
String	READ_CALL_LOG Επιτρέπει σε μια εφαρμογή να διαβάσει το αρχείο κλήσεων του χρήστη.
String	READ_CONTACTS Επιτρέπει σε μια εφαρμογή να διαβάσει τα δεδομένα των επαφών του χρήστη.
String	READ_EXTERNAL_STORAGE Επιτρέπει σε μια εφαρμογή να διαβάζει από εξωτερικό αποθηκευτικό χώρο.
String	READ_FRAME_BUFFER Επιτρέπει σε μια εφαρμογή να λαμβάνει λήψεις οθόνης και, γενικότερα, να έχει πρόσβαση στα δεδομένα προσωρινής αποθήκευσης πλαισίων.
String	READ_INPUT_STATE <i>Αυτή η σταθερά καταργήθηκε στο επίπεδο API 16. Το API που χρησιμοποίησε αυτήν την άδεια έχει καταργηθεί.</i>
String	READ_LOGS Επιτρέπει σε μια εφαρμογή να διαβάσει τα αρχεία καταγραφής συστήματος χαμηλού επιπέδου.
String	READ_PHONE_NUMBERS Επιτρέπει πρόσβαση ανάγνωσης στους αριθμούς τηλεφώνου της συσκευής.
String	READ_PHONE_STATE Επιτρέπει πρόσβαση μόνο για ανάγνωση στην κατάσταση του τηλεφώνου, συμπεριλαμβανομένου του αριθμού τηλεφώνου της συσκευής, των τρεχουσών πληροφοριών κυψελοειδούς δικτύου, της κατάστασης τυχόν συνεχιζόμενων κλήσεων και μιας λίστας οποιωνδήποτε PhoneAccount καταχωριστεί στη συσκευή.
String	READ_SMS Επιτρέπει σε μια εφαρμογή να διαβάζει μηνύματα SMS.
String	READ_SYNC_SETTINGS Επιτρέπει στις εφαρμογές να διαβάζουν τις ρυθμίσεις συγχρονισμού.
String	READ_SYNC_STATS Επιτρέπει στις εφαρμογές να διαβάζουν τα στατιστικά στοιχεία συγχρονισμού.
String	READ_VOICEMAIL Επιτρέπει σε μια εφαρμογή την ανάγνωση των φωνητικών μηνυμάτων στο σύστημα.
String	REBOOT Απαιτείται να είναι δυνατή η επανεκκίνηση της συσκευής.
String	RECEIVE_BOOT_COMPLETED Επιτρέπει σε μια εφαρμογή να λάβει το ACTION_BOOT_COMPLETED που μεταδίδεται μετά την ολοκλήρωση της εκκίνησης του συστήματος.
String	RECEIVE_MMS Επιτρέπει σε μια εφαρμογή να παρακολουθεί εισερχόμενα μηνύματα MMS.
String	RECEIVE_SMS

	Επιτρέπει σε μια εφαρμογή να λαμβάνει μηνύματα SMS.
String	RECEIVE_WAP_PUSH Επιτρέπει σε μια εφαρμογή να λαμβάνει μηνύματα push WAP.
String	RECORD_AUDIO Επιτρέπει σε μια εφαρμογή να εγγράψει ήχο.
String	REORDER_TASKS Επιτρέπει σε μια εφαρμογή να αλλάξει τη σειρά Z των εργασιών.
String	REQUEST_COMPANION_RUN_IN_BACKGROUND Επιτρέπει την εκτέλεση μιας εφαρμογής συνοδευτικού στο παρασκήνιο.
String	REQUEST_COMPANION_USE_DATA_IN_BACKGROUND Επιτρέπει σε μια εφαρμογή συνοδευτικό να χρησιμοποιεί δεδομένα στο παρασκήνιο.
String	REQUEST_DELETE_PACKAGES Επιτρέπει σε μια εφαρμογή να ζητά τη διαγραφή πακέτων.
String	REQUEST_IGNORE_BATTERY_OPTIMIZATIONS Η άδεια πρέπει να διατηρηθεί για να χρησιμοποιηθεί η ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS .
String	REQUEST_INSTALL_PACKAGES Επιτρέπει σε μια εφαρμογή να ζητήσει την εγκατάσταση πακέτων.
String	RESTART_PACKAGES <i>Αυτή η σταθερά restartPackage(String) στο επίπεδο API 8. Το API restartPackage(String) δεν υποστηρίζεται πλέον.</i>
String	SEND_RESPOND_VIA_MESSAGE Επιτρέπει σε μια εφαρμογή (τηλέφωνο) να στείλει ένα αίτημα σε άλλες εφαρμογές για να χειριστεί τη δράση απάντησης μέσω μηνύματος κατά τις εισερχόμενες κλήσεις.
String	SEND_SMS Επιτρέπει σε μια εφαρμογή να στέλνει μηνύματα SMS.
String	SET_ALARM Επιτρέπει σε μια εφαρμογή να εκπέμπει μια πρόθεση να ορίσει ένα συναγερμό για τον χρήστη.
String	SET_ALWAYS_FINISH Επιτρέπει σε μια εφαρμογή να ελέγχει εάν οι δραστηριότητες ολοκληρώνονται αμέσως όταν τοποθετούνται στο παρασκήνιο.
String	SET_ANIMATION_SCALE Τροποποιήστε τον συντελεστή κλίμακας παγκόσμιας κίνησης.
String	SET_DEBUG_APP Ρυθμίστε μια εφαρμογή για εντοπισμό σφαλμάτων.
String	SET_PREFERRED_APPLICATIONS <i>Αυτή η σταθερά καταργήθηκε στο επίπεδο API 7. Δεν είναι πλέον χρήσιμο, δείτε addPackageToPreferred(String) για λεπτομέρειες.</i>

String	SET_PROCESS_LIMIT Επιτρέπει σε μια εφαρμογή να ορίζει τον μέγιστο αριθμό διαδικασιών εφαρμογής (που δεν χρειάζονται) που μπορούν να εκτελούνται.
String	SET_TIME Επιτρέπει στις εφαρμογές να ρυθμίζουν το χρόνο του συστήματος.
String	SET_TIME_ZONE Επιτρέπει στις εφαρμογές να ρυθμίζουν τη ζώνη ώρας του συστήματος.
String	SET_WALLPAPER Επιτρέπει στις εφαρμογές τη ρύθμιση της ταπετσαρίας.
String	SET_WALLPAPER_HINTS Επιτρέπει στις εφαρμογές να ορίσουν τις συμβουλές ταπετσαρίας.
String	SIGNAL_PERSISTENT_PROCESSES Επιτρέπει σε μια εφαρμογή να ζητήσει την αποστολή ενός σήματος σε όλες τις επίμονες διαδικασίες.
String	STATUS_BAR Επιτρέπει σε μια εφαρμογή να ανοίγει, να κλείνει ή να απενεργοποιεί τη γραμμή κατάστασης και τα εικονίδια της.
String	SYSTEM_ALERT_WINDOW Επιτρέπει σε μια εφαρμογή τη δημιουργία παραθύρων χρησιμοποιώντας τον τύπο TYPE_APPLICATION_OVERLAY , που εμφανίζεται πάνω από όλες τις άλλες εφαρμογές.
String	TRANSMIT_IR Επιτρέπει τη χρήση του πομπού IR της συσκευής, εάν υπάρχει.
String	UNINSTALL_SHORTCUT Αυτή η άδεια δεν υποστηρίζεται πλέον.
String	UPDATE_DEVICE_STATS Επιτρέπει σε μια εφαρμογή να ενημερώνει τα στατιστικά στοιχεία της συσκευής.
String	USE_FINGERPRINT Επιτρέπει σε μια εφαρμογή να χρησιμοποιεί υλικό δακτυλικών αποτυπωμάτων.
String	USE_SIP Επιτρέπει σε μια εφαρμογή να χρησιμοποιεί υπηρεσία SIP.
String	VIBRATE Επιτρέπει την πρόσβαση στον δονητή.
String	WAKE_LOCK Επιτρέπει τη χρήση του PowerManager WakeLocks για να παραμείνει ο επεξεργαστής από τον ύπνο ή την οθόνη από την εξασθένιση.
String	WRITE_APN_SETTINGS Επιτρέπει στις εφαρμογές να γράφουν τις ρυθμίσεις APN.
String	WRITE_CALENDAR

	Επιτρέπει σε μια εφαρμογή να γράψει τα δεδομένα ημερολογίου του χρήστη.
String	WRITE_CALL_LOG Επιτρέπει σε μια εφαρμογή να γράφει (αλλά δεν διαβάζει) τα δεδομένα του αρχείου καταγραφής κλήσεων του χρήστη.
String	WRITE_CONTACTS Επιτρέπει σε μια εφαρμογή να γράψει τα δεδομένα επαφών του χρήστη.
String	WRITE_EXTERNAL_STORAGE Επιτρέπει σε μια εφαρμογή να γράφει σε εξωτερικό αποθηκευτικό χώρο.
String	WRITE_GSERVICES Επιτρέπει σε μια εφαρμογή την τροποποίηση του χάρτη υπηρεσιών της Google.
String	WRITE_SECURE_SETTINGS Επιτρέπει σε μια εφαρμογή να διαβάζει ή να γράφει τις ασφαλείς ρυθμίσεις συστήματος.
String	WRITE_SETTINGS Επιτρέπει σε μια εφαρμογή να διαβάζει ή να γράφει τις ρυθμίσεις του συστήματος.
String	WRITE_SYNC_SETTINGS Επιτρέπει στις εφαρμογές να γράφουν τις ρυθμίσεις συγχρονισμού.
String	WRITE_VOICEMAIL Επιτρέπει σε μια εφαρμογή να τροποποιεί και να καταργεί υπάρχοντα μηνύματα φωνής στο σύστημα.

Πίνακας 4: Κυριότερα δικαιώματα εφαρμογών android

Οι κυριότερες και πιο επικίνδυνες προσβάσεις στις συσκευές μας είναι οι κάτωθι:

1. Τοποθεσία (Location)
2. Κατάσταση και ταυτότητα τηλεφώνου (Phone status and identity)
3. Ανάγνωση και τροποποίηση των επαφών σας (Read and modify your contacts)
4. Παραχώρησης δικαιωμάτων που σχετίζονται με τα SMS και τα MMS
5. Παραχώρηση δικαιωμάτων σχετικά με λογαριασμούς χρηστών

Δεν υπάρχει επί του παρόντος κάποιος ενσωματωμένος τρόπος για να διαχειριστούμε τα δικαιώματα των εφαρμογών στην τελευταία έκδοση του Android, δεδομένου ότι η Google επέλεξε να αφαιρέσει την δυνατότητα AppOps από το Android 4.4.2 και έπειτα.

Συμπεράσματα

Τα δικαιώματα που εκχωρούν οι χρήστες στις εφαρμογές «ανοίγουν» πόρτες στους προγραμματιστές να έχουν πρόσβαση σε δεδομένα των συσκευών όπου γίνεται η χρήση. Τα δικαιώματα αυτά πολλές φορές είναι απορίας άξιον το λόγο που ζητούνται, αλλά αν ερευνηθεί ο βαθύτερος λόγος τότε θα καταλάβουμε ότι η γνώση των δεδομένων αυτών δίνει τη δυνατότητα σε πιο προσωποποιημένες διαφημίσεις και εφαρμογές.

Οι χρήστες πολλές φορές πριν αναζητήσουν μία εφαρμογή ή κάποιο αντικείμενο προς αγορά παρατηρούν ότι οι διαφημίσεις που περιβάλλουν σελίδες ή εφαρμογές, περιλαμβάνουν παρόμοια προϊόντα ή υπηρεσίες.

Στο μέλλον οι πληροφορίες για μεγάλο αριθμό ανθρώπων θα είναι πιο σημαντικές από οτιδήποτε άλλο. Υπάρχει και η άποψη ότι κάποια στιγμή μελλοντικά ένας μεγάλος πόλεμος θα γίνει για τις πληροφορίες.

Οι προγραμματιστές έχοντας αυτόν τον όγκο δεδομένων για τις προτιμήσεις των χρηστών που επέλεξαν την εφαρμογή τους μπορούν να τις μεταπωλήσουν και να λάβουν χρήματα πολλαπλάσια από τη χρήση των εφαρμογών τους και τις εισπράξεις από τις διαφημίσεις.

Οι hackers αναζητούν όγκο πληροφοριών και τις μεταπωλούν παίρνοντας μεγάλα χρηματικά ποσά.

Με λίγη επαγρύπνηση, είναι απολύτως δυνατό να ελαχιστοποιηθούν οι κίνδυνοι, μαθαίνοντας το πώς να διαχειρίζεσαι καλύτερα τα δικαιώματα εφαρμογών (και να γνωρίζεις το πώς να τα ανακαλέσεις, εάν κάτι τέτοιο είναι απαραίτητο). Τι πρέπει και μπορούμε να κάνουμε γι' αυτά .

Είναι δύσκολο να αρνηθεί κάποιος ότι, τουλάχιστον από προεπιλογή, οι ρυθμίσεις απορρήτου και ασφάλειας του Android είναι κάπως ελλιπείς. Ανάμεσα στην περιστασιακή σύγχυση με τις ονομασίες των παραχωρήσεων δικαιωμάτων και σε μια ανικανότητα για την χορήγηση δικαιωμάτων επιλεκτικά, αυτό είναι σίγουρα κάτι πάνω στο οποίο το Android θα πρέπει να αφιερώσει σημαντική προσοχή.

Ωστόσο, ακόμη και με αυτά τα θέματα παρόντα, παραμένει ακόμα απολύτως εφικτό το να βρεθεί κάθε χρήστης πάνω από τα πράγματα και να εξασφαλίσει την ασφάλεια των δεδομένων του με το να είναι σε συνεχή εγρήγορση σχετικά με τις εφαρμογές που εγκαθιστά και με τα δικαιώματα που παραχωρεί σε αυτές τις εφαρμογές.

Τελικό συμπέρασμα είναι ότι εμπεριέχετε στη συσκευή, είναι τα δεδομένα του χρήστη, είναι προσωπικά και αφού είναι μέσα στη δική του συσκευή αυτός θα πρέπει να έχει τον έλεγχο.

Βιβλιογραφία

1. <https://el.wikipedia.org/wiki/Smartphone>
2. <https://el.wikipedia.org/wiki/Android>
3. A Longitudinal Study of App - Permission Usage across the Google Play Store
Vincent F. Taylor - Ivan Martinovic
4. Update Behavior in App Markets and Security Implications: A Case Study in Google Play
Andreas Möller, Stefan Diewald, Luis Roalter, Florian Michahelles, Matthias Kranz
5. Causal Impact Analysis for App Releases in Google Play
William Martin, Federica Sarro and Mark Harman
6. <https://developer.android.com/reference/android/Manifest.permission.html>

Περιεχόμενα

Περίληψη	3
Summary	3
1 Ιστορικά στοιχεία	4
1.2 Λειτουργικό Σύστημα Android	4
1.3 Ιστορικό Ενημερώσεων	5
2. Μια διαχρονική μελέτη της εφαρμογής Χρήση άδειας μέσω του Google Play Store των Vincent F. Taylor - Ivan Martinovic.....	8
2.1 Εισαγωγή	8
2.2 Πρόβλημα Πεδίο εφαρμογής.	8
2.3 Επισκόπηση των αποτελεσμάτων ελέγχου	9
2.4 Γενική επισκόπηση	10
2.5 Αλλαγές στην Χρήση Εξουσιοδότησης	11
2.6 Κατάληξη αποτελεσμάτων	13
3 Ενημέρωση συμπεριφοράς στις αγορές εφαρμογών και επιπτώσεις στην ασφάλεια: Μια μελέτη περίπτωσης στο Google Play	15
3.1 Ενημέρωση Ανάλυσης Εγκατάστασης.....	16
3.2 Ενημέρωση συμπεριφοράς	16
3.3 Διανομή έκδοσης	17
3.4 Αποτελέσματα μελέτης 2012.....	18
4 Δεδομένα εφαρμογών Android (Play Store)	21
4.1 Ανάλυση κώδικα και τρόπος λειτουργίας	21
4.1 Εκτέλεση κώδικα λήψης εφαρμογών	23
4.2 Εφαρμογές και τρόπος ανάδειξης.....	27
4.3 Ανάλυση δεδομένων	28
Συμπεράσματα.....	47
Βιβλιογραφία	48
Περιεχόμενα	49
Περιεχόμενα Διαγραμμάτων	50
Περιεχόμενα Πινάκων.....	50
Περιεχόμενα Σχημάτων.....	50
Περιεχόμενα Στιγμιότυπων	51

Περιεχόμενα Διαγραμμάτων

Διάγραμμα 1 χρήσης εκδόσεων Android από τις συσκευές Smartphones	6
Διάγραμμα 2: Επικράτηση χρήσης αδειών σε όλο το Google Play Store.	10
Διάγραμμα 3: Αριθμός δικαιωμάτων που χρησιμοποιούνται ανά εφαρμογή στο Κατάστημα Google Play.	11
Διάγραμμα 4: Μέσος αριθμός αδειών χρήσης ανά κατηγορία εφαρμογής.	11
Διάγραμμα 5: Κατανομή των πιο συχνά προστιθέμενων δικαιωμάτων. Για λόγους σαφήνειας, παραλήφθηκαν άδειες που αντιστοιχούσαν σε λιγότερο από 2% των προσθηκών.	13
Διάγραμμα 6. Οπτικοποίηση που αντιπροσωπεύει τον αριθμό των πέντε μεταγενέστερων λήψεων ενημέρωσης (κάθετος άξονας) με την πάροδο του χρόνου. Το γράφημα εμφανίζει τα μέγιστα στην ημέρα δημοσίευσης των ενημερωμένων εκδόσεων (ενδεχομένως εξαιτίας των ενεργοποιημένων αυτόματων ενημερώσεων) και στη συνέχεια μειώνεται εκθετικά. Τροποποιημένο διάγραμμα με βάση τα στατιστικά στοιχεία της κονσόλας προγραμματιστή Android.	18
Διάγραμμα 7. Οπτικοποίηση που αντιπροσωπεύει τον αριθμό των εγκαταστάσεων ανά εκδοχή (κάθετος άξονας). οι χρωματιστές γραμμές υποδεικνύουν τις πέντε τελευταίες εκδόσεις. Το διάγραμμα αποκαλύπτει πόσο παλιές εκδόσεις είναι ενεργοποιημένες στις συσκευές του χρήστη. Οι περίοδοι των 7 ημερών μετά την δημοσίευση μιας ενημέρωσης επισημαίνονται. Τροποποιημένο διάγραμμα με βάση τα στατιστικά στοιχεία της Κονσόλας προγραμματιστή Android.	18

Περιεχόμενα Πινάκων

Πίνακας 1 εξέλιξης εκδόσεων Android	7
Πίνακας 2: Μέση χρήση χρήσης (και ποσοστιαία αλλαγή) σε εφαρμογές κατά τη διάρκεια της διετούς περιόδου.	12
Πίνακας 3. Ποσοστό όλων των χρηστών που εγκατέστησαν μια ενημερωμένη έκδοση εντός 7 ημερών από τη δημοσίευσή της.	17
Πίνακας 4: Κυριότερα δικαιώματα εφαρμογών android	46

Περιεχόμενα Σχημάτων

Σχήμα 1 : Αρχιτεκτονική crawler βασισμένη σε cloud. Το Google Play Store Crawler (GPSC)	9
---	---

Περιεχόμενα Στιγμιότυπων

Στιγμιότυπο 1 των αρχείων όπου χρησιμοποιεί ο κώδικας.	23
Στιγμιότυπο 2 των αρχείων του φακέλου Spiders	23
Στιγμιότυπο 3 εκτέλεση κώδικα	24
Στιγμιότυπο 4 εκτέλεση ερωτημάτων στη βάση	25
Στιγμιότυπο 5 Προβολή βάσης δεδομένων στον εικονικό υπολογιστή	26
Στιγμιότυπο 6 εκτέλεση ερωτημάτων στη βάση	26
Στιγμιότυπο 7 εκτέλεση κώδικα	30
Στιγμιότυπο 8 εμφάνισης δεδομένων βάσης	32
Στιγμιότυπο 9 εκτέλεση κώδικα	33
Στιγμιότυπο 10 εκτέλεση κώδικα	34
Στιγμιότυπο 11 εκτέλεση κώδικα	35
Στιγμιότυπο 12 εκτέλεση κώδικα	36