Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστήμων

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Δικαιώματα Εφαρμογών Smartphones και Παραβιάσεις

Μιχάλης Συμεού

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Μάϊος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Δικαιώματα Εφαρμογών Smartphones και Παραβιάσεις

Μιχάλης Συμεού

Επιβλέπων Καθηγητής
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάϊος 2019

Περίληψη

Η χρήση των smartphones είναι αναμφισβήτητα ένα από τα πλέον αυξανόμενα πεδία της εφαρμοσμένης πληροφορικής. Η ανάγκη για εφαρμογές που να βοηθούν στη καθημερινότητα των χρηστών και την διασκέδαση τους (game apps), έχει προσελκύσει αρκετούς developers με εκατομμύρια εφαρμογές διαθέσιμες για εγκατάσταση στα smartphones .

Μεγάλη όμως είναι και η ανάγκη για την ασφάλεια των προσωπικών δεδομένων του χρήστη λόγω του όγκου των πληροφοριών που συλλέγει η κάθε κινητή συσκευή. Μια πολιτική προστασίας η οποία έχει θεσπιστεί για την ασφάλεια αυτών των δεδομένων και την οποία θα εξετάσουμε στην παρούσα διατριβή, είναι η άδεια δικαιωμάτων στο λειτουργικό Android. Οι άδειες δικαιωμάτων, έχουν ως σκοπό να προστατέψουν τα προσωπικά στοιχεία του χρήστη με την ενημέρωση του, ζητώντας του έγκριση για χρησιμοποίηση των προσωπικών του δεδομένων.

Η εκπόνηση της διατριβής αυτής, έχει ως στόχο να διερευνήσει αν οι εφαρμογές απαιτούν πρόσβαση σε δεδομένα τα οποία χρειάζονται για την σωστή λειτουργία τους και αν υπερβαίνουν των δικαιωμάτων τους, χρησιμοποιώντας πόρους και πληροφορίες εν αγνοία του χρήστη.

Το πρώτο μέρος, είναι η μελέτη κατάλληλων εφαρμογών που θα εγκατασταθούν στο λογισμικό για την συλλογή δεδομένων σχετικά με τις άδειες που χρησιμοποιούν. Για αυτό το μέρος της μεθοδολογίας μας, θα χρειαστούν είκοσι εφαρμογές για να μπορέσει το δείγμα να είναι αντιπροσωπευτικό. Στο δεύτερο μέρος, οι ίδιες εφαρμογές θα αποσυναρμολογηθούν, θα αφαιρεθούν από το κώδικα τα δικαιώματα που ζητούν και θα επανεγκατασταθούν, για να ελεγχθεί η λειτουργία τους χωρίς τις άδειες χρήσης.

Αποδεικνύεται ότι οι εφαρμογές πράγματι ζητούν περισσότερες άδειες χρήσης από ότι χρειάζονται χωρίς αυτό να σημαίνει ότι έχουν κακόβουλο στόχο.

Summary

The use of smartphones is undoubtedly one of the most growing fields of applied computing. The need for apps to help and entertain everyday users has attracted many developers with millions of applications available for installation on smartphones.

However, the need for the security of the user's personal data is also great, due to the amount of information collected by each mobile device. A security policy that has been enacted for the security of this data, and which we will look at in this thesis, is the permission for Android operating system. Permissions are intended to protect the user's personal information by informing him of his permission to use his or her personal data.

The purpose of this dissertation is to investigate whether applications require access to the data they need for their proper functioning and if they exceed their rights by using resources and information without the user's knowledge.
The first part is the study of suitable applications that will be installed in the software to collect data about the licenses they use. For this part of our methodology, twenty applications will be needed to enable the sample to be representative. In the second part, the same applications will be dismantled, the requested permissions will be removed from the code and will be reinstalled to check their operation without the licenses.

It turns out that applications actually ask for more licenses than they need without that meaning they have a malicious target.

Ευχαριστίες

Ένα μεγάλο ευχαριστώ το οφείλω στην επιβλέπουσα καθηγήτρια μου κ. Αδαμαντίνη Περατικού για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα, την συνεχή υποστήριξη, επίβλεψη αλλά και άψογη συνεργασία. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την κατανόηση και την ηθική υποστήριξη σε όλη την διάρκεια του μεταπτυχιακού μου.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

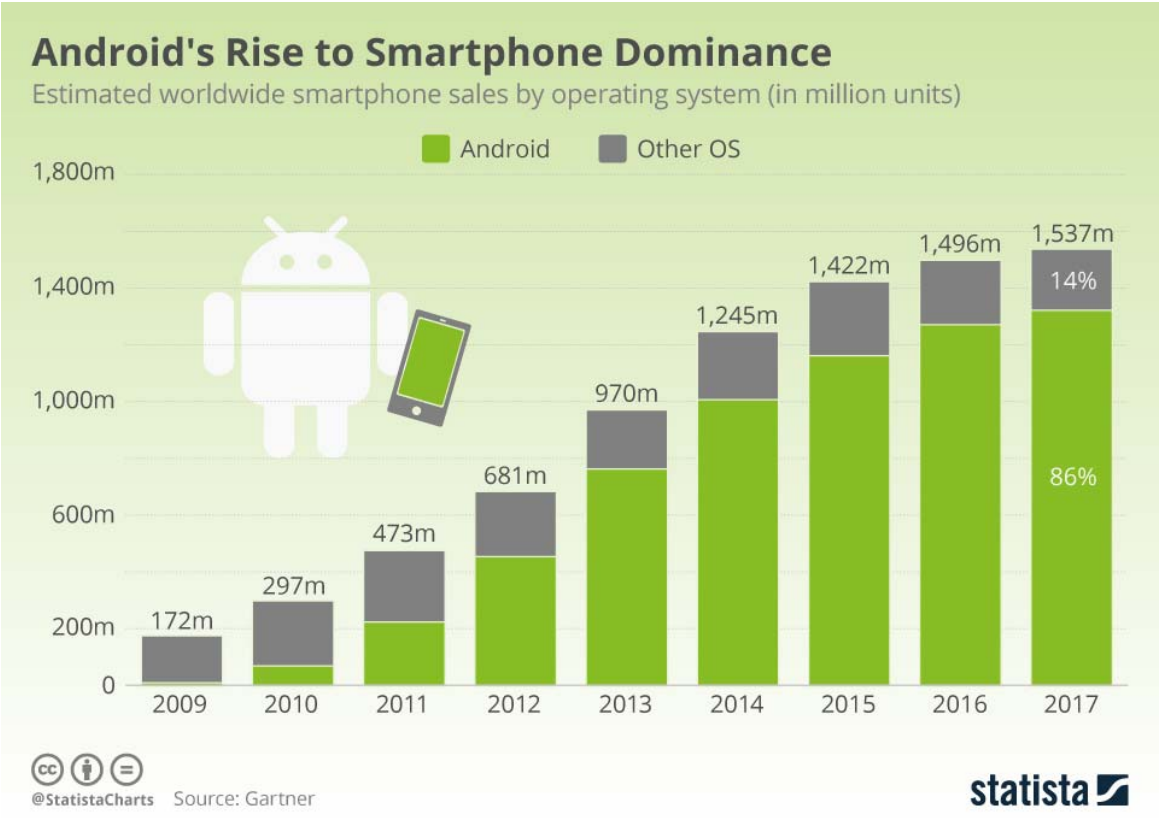
Σε μια εποχή όπου η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς το κομμάτι των έξυπνων κινητών τηλεφώνων γνωρίζει την μεγαλύτερη άνθιση. Η συνεχόμενη εξέλιξη τους έχει καταστήσει για πολλούς μη αναγκαία την χρήση του προσωπικού υπολογιστή αφού πλέον ένα smartphone μπορεί να εξυπηρετήσει όλες τις καθημερινές τους ανάγκες.

Τα smartphone έχουν καταφέρει, μέσω της συνεχόμενης βελτίωσης τους, να αποτελούν ένα βασικό και αναπόσπαστο κομμάτι της καθημερινότητας μας αφού μέσω αυτών οι χρήστες μπορούν εκτός από την επικοινωνία μέσω κλήσεων και sms, να πλοηγηθούν στο διαδίκτυο, να χρησιμοποιήσουν κοινωνικά δίκτυα, να πραγματοποιήσουν οικονομικές συναλλαγές, να διαχειρίζονται την ηλεκτρονική τους αλληλογραφία αλλά και να χρησιμοποιηθούν για ψυχαγωγία όπως για παράδειγμα με ηλεκτρονικά παιχνίδια. Αυτοί είναι και οι λόγοι που μέχρι το 2017 είχαν γίνει περισσότερες από 5 δισεκατομμύρια μοναδικές συνδέσεις όπου αντιστοιχεί στο 66% του παγκόσμιου πληθυσμού ενώ υπολογίζεται μέχρι το 2025 να φτάσει το 71% [16].

Όλες αυτές οι λειτουργίες των έξυπνων τηλεφώνων δημιουργούν ένα τεράστιο όγκο πληροφοριών και προσωπικών δεδομένων του χρήστη μαζεμένο σε μια μόνο συσκευή. Αυτές οι πληροφορίες, όπως για παράδειγμα ο εντοπισμός θέσης ή κωδικοί email, αποτελούν πόλο έλξης για κακόβουλους χρήστες οι οποίοι αν καταφέρουν να τα υποκλέψουν στην συνέχεια μπορεί να τα χρησιμοποιήσουν για δικούς τους σκοπούς. Οι συνέπειες σε πιθανή υποκλοπή μπορεί να έχουν οικονομικό, επαγγελματικό ή ακόμα και προσωπικό κόστος.

Το λειτουργικό σύστημα Android έχοντας ποσοστό 88% αποτελεί το δημοφιλέστερο σύστημα στα κινητά τηλέφωνα [17]. Στο ηλεκτρονικό της κατάστημα υπάρχουν πάνω από 2,5 εκατομμύρια εφαρμογές είτε δωρεάν είτε επί πληρωμή [18]. Δυστυχώς η μεγάλη

βάση χρηστών και η δημοτικότητα του[19] έχει επιφέρει την αύξηση των επιθέσεων και την αύξηση των κακόβουλων προγραμμάτων σε σύγκριση με τα άλλα λειτουργικά.



Εικόνα 1.1: Ποσοστό πωλήσεων Smartphones [19]

Η Google ως ιδιοκτήτρια εταιρεία του λειτουργικού Android έχει θεσπίσει ορισμένες πολιτικές προστασίας για την ασφάλεια αυτών των δεδομένων όπως τις άδειες δικαιωμάτων. Οι άδειες δικαιωμάτων είναι ένα μοντέλο ασφαλείας το οποίο επιτρέπει στις εφαρμογές να αξιοποιούν λειτουργίες του τηλεφώνου και ταυτόχρονα να προστατεύει τους χρήστες από κακόβουλο λογισμικό. Το λειτουργικό Android μέσω αυτών των χαρακτηριστικών του προσπαθεί να μειώσει τις πιθανές επιπτώσεις που μπορεί να προκύψουν από κάποιο κακόβουλο λογισμικό. Ο τρόπος που το επιτυγχάνει αυτό είναι η ενημέρωση και η απαίτηση αποδοχής του χρήστη για τις λειτουργίες που χρειάζεται η εκάστοτε εφαρμογή. Οι λειτουργίες αυτές μπορούν να περιλαμβάνουν εκτέλεση κλήσεων, αποστολή μηνυμάτων και πρόσβαση σε προσωπικά δεδομένα του χρήστη όπως διευθύνσεις, email κ.α.

Οι άδειες δικαιωμάτων για εφαρμογές από τρίτους στο λειτουργικό Android, χωρίζονται σε τέσσερα επίπεδα προστασίας. Τις κανονικές άδειες (normal permissions), τις επικίνδυνες άδειες (dangerous permission), τις άδειες υπογραφής και τις ειδικές άδειες

(special permissions) οι οποίες ωστόσο, χρησιμοποιούνται σπάνια. Οι κανονικές άδειες, δίνονται αυτόματα από το λειτουργικό αφού δεν έχουν άμεση σχέση με τα δεδομένα του χρήστη. Οι επικίνδυνες άδειες, αφορούν προσωπικά δεδομένα όπως π.χ. επαφές και πρέπει να τις εγκρίνει ο χρήστης για να αποκτήσουν πρόσβαση[21]. Αυτές οι άδειες χωρίζονται σε ομάδες που αφορούν ένα υποσύνολο αδειών, όπως για παράδειγμα η ανάγνωση επαφών και η εγγραφή επαφών ανήκουν στην ομάδα επαφές. Όταν το πρόγραμμα ζητήσει άδεια για ανάγνωση επαφών και δοθεί η έγκριση από τον χρήστη, τότε η εφαρμογή μπορεί να αποκτήσει έγκριση αυτόματα από το σύστημα και για την εγγραφή επαφών αφού ανήκουν στην ίδια ομάδα[22].

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

Η σημασία της ασφάλειας στα smartphones έχει οδηγήσει σε πλήθος ερευνών. Από την αρχή της εμφάνισης τους στην αγορά, έρευνες όπως του Shabtai et al.[13] ανέφεραν ότι πλέον τα κινητά θα αποτελούν πόλο έλξης για κακόβουλα λογισμικά λόγω και των προσωπικών πληροφοριών που αποθηκεύουν. Ο ίδιος μελέτησε και αξιολόγησε τους μηχανισμούς ασφάλειας του Android. Η έρευνα του έδειξε πως παρόλο που αυτοί οι μηχανισμοί ήταν καλά σχεδιασμένοι εντούτοις εντόπισε διάφορα θέματα ένα από τα οποία είναι και η κατάχρηση αδειών χρήσης.

Η έρευνα της Felt et al.[09] είχε ως επίκεντρο τις άδειες χρήσης του Android και κατά πόσο είναι αποτελεσματικές για την προστασία των χρηστών. Εξετάστηκε η συχνότητα των αιτημάτων άδειας από εφαρμογές μέσα από το επίσημο Play store. Τα αποτελέσματα έδειξαν ότι το τρόπος που το Android χρησιμοποιεί τις άδειες χρήσης έχει καλύτερα αποτελέσματα σε σχέση με άλλα μοντέλα permissions. Ωστόσο η συχνή εμφάνιση των επικίνδυνων αδειών μπορεί να παραπλανήσει το χρήστη και να προχωρήσει σε εγκατάσταση χωρίς να γνωρίζει αν η εφαρμογή είναι κακόβουλη ή όχι.

Αρκετοί ερευνητές έχουν δημιουργήσει μηχανισμούς για να ελέγχουν τις άδειες χρήσης και να τις ταξινομούν. Ένα από αυτά είναι το Kirin. Το Kirin[12] διαβάζει τις απαιτούμενες άδειες της εφαρμογής κατά την εγκατάσταση και τις ελέγχει σε σχέση με ένα σύνολο κανόνων ασφάλειας. Βασίζεται αποκλειστικά στο ποιες άδειες ζητούνται και όχι στο πως εφαρμόζονται αυτές οι άδειες. Ο Barrera et al. [02] χρησιμοποίησε αλγόριθμο SOM (Self-Organizing Map) για να αναλύσει το μοντέλο αδειών του Android και να διαπιστώσει πως εφαρμόζεται και τυχόν αδυναμίες του. Κατάληξε πως ορισμένες άδειες δεν είναι αρκετά σαφής όπως π.x INTERNET και χρησιμοποιούνται αρκετά συχνά.

Ένα ακόμη εργαλείο για έλεγχο κατά πόσο οι εφαρμογές χρησιμοποιούν υπερβολικές άδειες έχει δημιουργηθεί από τους Vidas et al[15]. Το εργαλείο αξιολογεί μια εφαρμογή Android για τις απαιτούμενές άδειες και ενημερώνει τον προγραμματιστή σχετικά με τα ελάχιστα στοιχεία ελέγχου που απαιτούνται για την ορθή εκτέλεση. Παρόμοιο εργαλείο είναι και το Stowaway[7] το οποίο ελέγχει για υπερβολικές άδειες χρήσης μέσα σε εφαρμογές. Με την μελέτη αυτή, μέσα από σχεδόν χίλιες εφαρμογές, διαπιστώθηκε ότι περισσότερο από το ένα τρίτο των εφαρμογών χρησιμοποιεί υπερβολικές άδειες χρήσης,

Σε μια πρόσφατη μελέτη των Bagheri H et al. [13], δημιουργήθηκε ένα μοντέλο με γλώσσα προγραμματισμού Alloy για την αυτοματοποιημένη ανάλυση αδειών του λειτουργικού Android. Μετα την ανάλυση του μοντέλου διαπιστωθήκαν τρωτά σημεία στο σύστημα μέσω αδειών χρήση τρίτων.

2.1 Android

Το Android είναι ένα λειτουργικό σύστημα για φορητές συσκευές όπως κινητά και tablet, το οποίο αρχικά αναπτύχθηκε από την Android Inc. στις αρχές του 2000 και στην συνέχεια αγοράστηκε από την Google το 2005 [11]. Το Νοέμβριο του 2007 εταιρείες τηλεπικοινωνίων όπως sprint και T-Mobile, κατασκευής υλικού όπως η HTC, η Sony, η Samsung, συμπεριλαμβανομένου και της Google δημιουργούν την Open Handset Alliance με σκοπό την ανάπτυξη ανοικτής πλατφόρμας για κινητές συσκευές[26]. Εκτός από συσκευές κινητής τηλεφωνίας και tablet, το λειτουργικό Android χρησιμοποιείται σε τηλεοράσεις, αυτοκίνητα, ρολόγια χειρός και άλλα.

Το Android από την αρχή της λειτουργίας του μέχρι τώρα μετρά αρκετές κύριες εκδόσεις και περισσότερες υποεκδόσεις. Η κάθε έκδοση η οποία παίρνει την κωδική ονομασία ενός γλυκού φέρνει εκτός από αισθητικές βελτιώσεις και λειτουργικές βελτιώσεις διορθώνοντας και αρκετά σφάλματα. Από τις 6 Αυγούστου 2018 είμαστε στην τελευταία έκδοση Android η οποία έχει την κωδική ονομασία Pie.

Κωδικη Ονομασια	Αριθμος Εκδοσης	Ημερομηνια κυκλοφοριας
(No codename)	1	23-Sep-08
Petit Four	1.1	9-Feb-09
Cupcake	1.5	27-Apr-09
Donut	1.6	15-Sep-09
Eclair	2.0 – 2.1	26-Oct-09
Froyo	2.2 – 2.2.3	20-May-10
Gingerbread	2.3 – 2.3.7	6-Dec-10
Honeycomb	3.0 – 3.2.6	22-Feb-11
Ice Cream Sandwi	4.0 – 4.0.4	18-Oct-11
Jelly Bean	4.1 – 4.3.1	9-Jul-12
KitKat	4.4 – 4.4.4	31-Oct-13
Lollipop	5.0 – 5.1.1	12-Nov-14
Marshmallow	6.0 – 6.0.1	5-Oct-15
Nougat	7.0 – 7.1.2	22-Aug-16
Oreo	8.0 – 8.1	21-Aug-17
Pie	**9**	6-Aug-18

Πίνακας 2.1.1: Εκδόσεις Android[25]

Το λειτουργικό Android αποτελείται από μια στοίβα λογισμικού η οποία χωρίζεται σε επίπεδα όπου κάθε επίπεδο περιλαμβάνει ένα αριθμό προγραμμάτων.

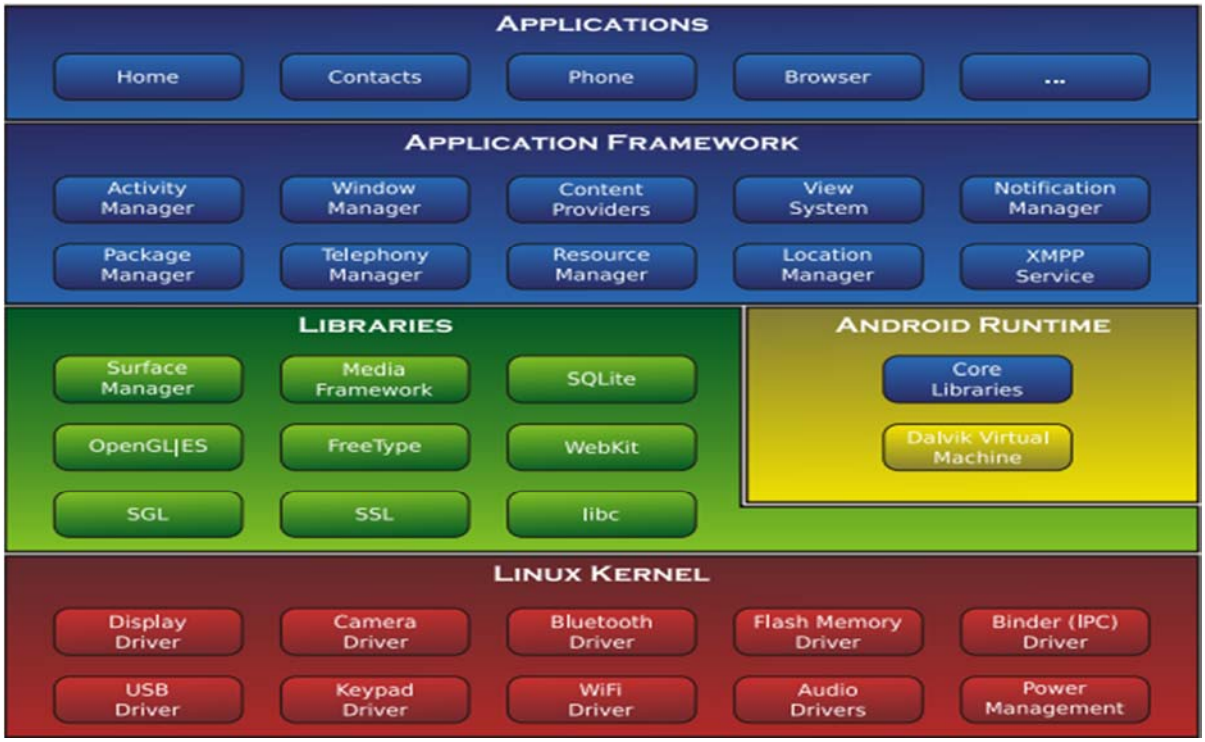
Το πρώτο επίπεδο που είναι και το πιο χαμηλό είναι ο πυρήνας του Linux(Linux Kernel). Ο πυρήνας δεν αλληλοεπιδρά με τους χρήστες και τους προγραμματιστές αλλά αποτελεί την καρδιά του συστήματος. Είναι υπεύθυνος για βασικές υπηρεσίες συστήματος όπως ασφάλεια, διαχείριση ενέργειας, μνήμης και οδηγούς συσκευών.

Το επόμενο επίπεδο είναι το επίπεδο βιβλιοθηκών (Native Libraries Layer) το οποίο φέρουν ένα σύνολο από βιβλιοθήκες σε μορφή C/C++ που χρησιμοποιούνται για τον χειρισμό διαφορετικών τύπων δεδομένων από την συσκευή. Στο ίδιο επίπεδο βρίσκεται και το επίπεδο εκτέλεσης (Android Runtime). Το επίπεδο περιλαμβάνει επίσης ένα σύνολο βασικών βιβλιοθηκών Java. Οι προγραμματιστές εφαρμογών Android δημιουργούν τις εφαρμογές τους χρησιμοποιώντας τη γλώσσα προγραμματισμού Java. Περιλαμβάνει επίσης την εικονική μηχανή Dalvik (Dalvik Virtual Machine).

Το ακριβώς επόμενο επίπεδο είναι το επίπεδο πλαισίου εφαρμογών (Application Framework). Οι εφαρμογές μας αλληλοεπιδρούν με αυτά τα τμήματα της αρχιτεκτονικής του Android. Τα προγράμματα αυτά διαχειρίζονται βασικές λειτουργίες της συσκευής όπως τον διαχειριστή πόρων (Resource Manager) για να επιτρέπεται η πρόσβαση από τις εφαρμογές σε δεδομένα άλλων εφαρμογών. Υπάρχουν ακόμα διαχειριστές

ειδοποιήσεων και διαχειριστές δραστηριοτήτων όπου ο πρώτος επιτρέπει την προβολή ειδοποιήσεων στη μπάρα κατάστασης και ο δεύτερος διαχειρίζεται τον κύκλο ζωής των εφαρμογών.

Τέλος υπάρχει το υψηλότερο επίπεδο στην στοίβα το επίπεδο εφαρμογών (Application Layer). Σε αυτό το επίπεδο βρίσκεται το σύνολο των βασικών εφαρμογών όπως είναι τα μηνύματα, επαφές, ημερολόγιο και άλλα.



Εικόνα 2.1.1: Επίπεδα Android [14]

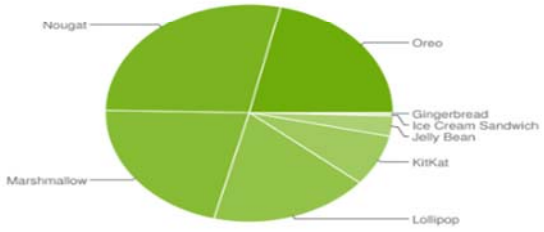
Ένας από τους λόγους που το συγκεκριμένο λογισμικό είναι τόσο διαδεδομένο είναι επειδή αποτελείται από ένα λειτουργικό σύστημα ανοιχτού κώδικα για κινητές συσκευές το οποίο διαχειρίζεται και επιβλέπει η Google. Στον επίσημο ιστότοπο πηγαίου κώδικα Android (Android Open Source Project)[20] προσφέρονται χρήσιμες πληροφορίες και ο κώδικας που απαιτείται, για να εξασφαλίσουν την συμβατότητα μεταξύ των συσκευών για διατήρηση του οικοσυστήματος υγιές και λειτουργικό για όλους τους χρήστες όπως και για την δημιουργία παραμετροποιήσιμων παραλλαγών Android για διάφορες ηλεκτρονικές συσκευές.

Το αποτέλεσμα του λειτουργικού ως έργο ανοιχτού κώδικα είναι να μπορεί να μεταφερθεί σε σχεδόν οποιαδήποτε συσκευή και να έχει δημόσια τεκμηρίωση που είναι

διαθέσιμη σε όλους (στα αγγλικά στο source.android.com και στα Κινέζικα στη διεύθυνση source.android.google.cn). Επίσης κάθε κατασκευαστής κινητών τηλεφώνων μπορεί να προσθέσει ή να αφαιρέσει λειτουργίες στο λειτουργικό και να το τροποποιήσει ανάλογα με τις δυνατότητες της συσκευής πραγματοποιώντας αλλαγές τόσο στο user interface όσο και στην υποστήριξη υλικού.

Αυτό είναι και ένα από τα μεγαλύτερα προβλήματα του λειτουργικού Android. Σε αυτές τις αλλαγές όπως επίσης και στο θέμα κόστους για παλαιότερες και φθηνότερες συσκευές οφείλεται η μεγάλη καθυστέρηση στη υιοθέτηση της τελευταίας έκδοσης του λειτουργικού στις συσκευές από τους κατασκευαστές ή ακόμη και η καθόλου ενημέρωση των συσκευών. Όπως φαίνεται και από την εικόνα 3 από επίσημα στοιχεία του Play store στις 26 Οκτωβρίου 2018 υπήρχαν σε χρήση 8 εκδόσεις Android με κυριότερες τις 4 τελευταίες που είναι η έκδοση 5 (Lollipop) με ποσοστό 17,9%, η έκδοση 6 (Marshmallow) με ποσοστό 21,3%, η έκδοση 7(Nougat) με ποσοστό 28,2% και η έκδοση 8-8.1(Oreo) με ποσοστό 21,5%.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.2%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.1%
4.2.x		17	1.5%
4.3		18	0.4%
4.4	KitKat	19	7.6%
5.0	Lollipop	21	3.5%
5.1		22	14.4%
6.0	Marshmallow	23	21.3%
7.0	Nougat	24	18.1%
7.1		25	10.1%
8.0	Oreo	26	14.0%
8.1		27	7.5%



Data collected during a 7-day period ending on October 26, 2018 (update coming soon: data feed under maintenance).
Any versions with less than 0.1% distribution are not shown.

Εικόνα 2.1.2: Εκδόσεις του Λειτουργικού Android[23]

Το αποτέλεσμα αυτής της πρακτικής είναι πολλές συσκευές να μένουν εκτεθειμένες σε διάφορα κενά ασφαλείας που διορθώνονται σε πιο νέες εκδόσεις αλλά επίσης δημιουργεί μια πολυπλοκότητα για τους προγραμματιστές των εφαρμογών αφού θα πρέπει οι εφαρμογές τους να είναι συμβατές με όλες τις εκδόσεις αν θέλουν να έχουν το μεγαλύτερο μέρος της αγοράς.

2.2 Android Stores

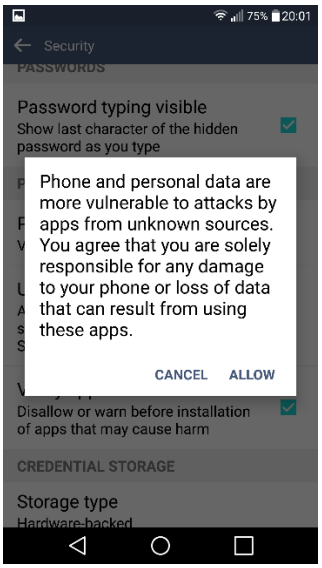
Για την εγκατάσταση των εφαρμογών στο λειτουργικό Android γίνεται με δυο κυρίως τρόπους. Ο ένας από το επίσημο κατάστημα εφαρμογών και δεύτερος απευθείας από την συσκευή αφού έχει κατέβει από κάποια ιστοσελίδα ή ένα μη επίσημο κατάστημα με εφαρμογές.

Το επίσημο κατάστημα εφαρμογών του Android διαχειρίζεται από την Google και ονομάζεται Google Play. Υπάρχουν εκατομμύρια εφαρμογές διαθέσιμες για λήψη είτε δωρεάν είτε επι πληρωμή από τους χρήστες. Το Google Play λειτουργεί επίσης ως κατάστημα ψηφιακών μέσων, προσφέροντας μουσική, βιβλία, ταινίες και τηλεοπτικά προγράμματα. Το Google Play κυκλοφόρησε στις 6 Μαρτίου 2012, συγκεντρώνοντας το Android Market, το Google Music και το eBookstore Google κάτω από το εμπορικό σήμα της Google.

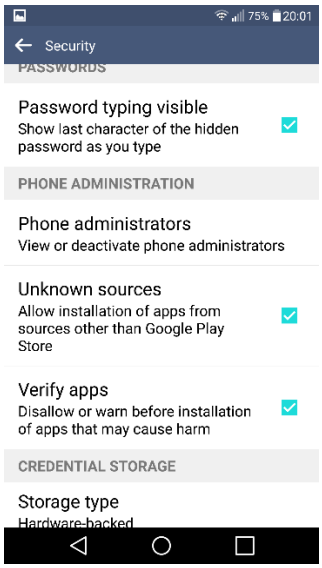
Το κατάστημα Google Play το 2016 είχε πάνω από 82 δισεκατομμύρια λήψεις εφαρμογών ενώ το 2017 πάνω από 3,5 εκατομμύρια εφαρμογές έχουν δημοσιευτεί και ήταν προσβάσιμες από τους χρήστες. Βάση της ανοικτής αγοράς του Android καμία εφαρμογή δεν επαληθεύεται από ειδικούς ασφαλείας. Αυτό αποτελεί θέμα ανησυχίας εφόσον είναι εύκολος στόχος από τους προγραμματιστές να ενσωματώσουν κακόβουλο λογισμικό σε εφαρμογές που εγκρίνονται και φορτώνονται στο κατάστημα για να μεταφορτωθεί στην συνέχεια από χρήστες, με ποικίλους βαθμούς σοβαρότητας.

Αυτή η τεχνική ονομάζεται repackaging. Είναι μια από τις πολλές τεχνικές διείσδυσης κακόβουλου κώδικα. Επιλέγονται διάφορες δημοφιλείς εφαρμογές από το Google Play, αποσυναρμολογούνται με την χρήση διαφόρων εργαλείων reverse engineering όπως Apktool, και αφού προστεθεί ο κακόβουλος κώδικας γίνεται η επανασυναρμολόγηση της εφαρμογής και διανέμεται μέσω ανεπίσημων ηλεκτρονικών καταστημάτων τα οποία έχουν λιγότερη ασφάλεια.

Παρόλο που το επίσημο κατάστημα προσφέρει εκατομμύρια εφαρμογές αρκετές από αυτές μπορεί να μην είναι διαθέσιμες λόγω διάφορων περιορισμών όπως συσκευής ή γεωγραφικής περιοχής. Για αυτό το λόγο οι χρήστες προβαίνουν σε λήψεις εφαρμογών από εναλλακτικά καταστήματα. Αυτά τα καταστήματα εκτός του ότι φιλοξενούν μεγάλο αριθμό εφαρμογών, προσφέρουν δωρεάν εφαρμογές οι οποίες κανονικά θα χρειάζονταν πληρωμή, επιπρόσθετα προσφέρουν έκπτωση σε εφαρμογές υψηλής ποιότητας ή παρέχουν άλλες προσφορές εξοικονόμησης χρημάτων. Η εγκατάσταση των εφαρμογών από ανεπίσημα καταστήματα είναι απενεργοποιημένη από προεπιλογή στο λειτουργικό Android. Παρόλα αυτά δίνεται στο χρήστη η δυνατότητα να ενεργοποιήσει αυτό το χαρακτηριστικό μέσα από τις ρυθμίσεις [33]. Ο λόγος που η Google ενσωμάτωσε αυτό το χαρακτηριστικό στο λειτουργικό είναι επειδή, όπως αναφέρεται και το μήνυμα που εμφανίζεται όταν το ενεργοποιήσουμε, δεν μπορεί να εγγυηθεί την ασφάλεια μας από άγνωστα προγράμματα.



Εικόνα 2.2.1: Μήνυμα ασφαλείας



Εικόνα 2.2.2: Ενεργοποίηση Εγκατάστασης Αγνώστων Πηγών

2.3 Permissions

Λόγω του όγκου των πληροφοριών που συλλέγει η κάθε κινητή συσκευή αλλά και την ανάγκη των χρηστών για προστασία των προσωπικών τους δεδομένων η Google έχει θεσπίσει ορισμένες πολιτικές προστασίας για την ασφάλεια αυτών των δεδομένων όπως τις άδειες δικαιωμάτων.

Το λειτουργικό σύστημα του Android χρησιμοποιεί την τεχνική Sandbox για να εκτελέσει τις εφαρμογές του με ασφάλεια. Η τεχνική Sandbox είναι ένας μηχανισμός ασφαλείας ο οποίος εκτελεί τις εφαρμογές σε μια απομονωμένη περιοχή του συστήματος με περιορισμένους πόρους στο σύστημα μας [12]. Στην περίπτωση που μελετάμε, το λειτουργικό Android επιτρέπει την πρόσβαση σε διάφορα δεδομένα και υλικά αφού τα ζητήσει η εφαρμογή μέσω των αδειών δικαιωμάτων [27]. Ακολούθως το σύστημα αξιολογεί την άδεια που απαιτεί η εφαρμογή και αν εμπίπτει στην κατηγορία κανονικής άδειας εγκρίνεται αυτόματα ενώ αν εμπίπτει στην κατηγορία επικίνδυνη ενημερώνει τον χρήστη για την έγκριση της ή την απόρριψη της [28].

Αυτές οι άδειες δικαιωμάτων είναι απαραίτητες για να δουλέψει σωστά μια εφαρμογή αν απαιτεί υλικά και πρόσβαση σε πόρους οι οποίοι δεν είναι διαθέσιμοι στα προκαθορισμένα από το λειτουργικό. Ανάλογα με το επίπεδο προστασίας της κάθε άδειας το σύστημα καθορίζει και τα αντίστοιχα επίπεδα πρόσβασης [05].

Υπάρχουν 4 επίπεδα προστασίας τα οποία χωρίζονται ως εξής:

- Τις κανονικές άδειες (normal permissions), τις επικίνδυνες άδειες (dangerous permission), τις άδειες υπογραφής και τις ειδικές άδειες (special permissions). Οι κανονικές άδειες είναι χαμηλού ρίσκου και παραχωρούνται αυτόματα από το σύστημα. Μερικές άδειες χαμηλού ρίσκου είναι για παράδειγμα το SET_WALLPAPER η οποία δίνει την δυνατότητα στην εφαρμογή να αλλάξει το φόντο εργασίας και το INTERNET η οποία δίνει πρόσβαση στο διαδίκτυο.

- Οι επικίνδυνες άδειες έχουν να κάνουν ως επι το πλείστων με δικαιώματα πρόσβασης στα προσωπικά δεδομένα του χρήστη ή και χειρισμού της συσκευής με τρόπο που μπορεί να βλάψει δεδομένα του συστήματος ή άλλες εφαρμογές. Μερικές επικίνδυνες άδειες χρήσης είναι το SMS και το PHONE. Με τις συγκεκριμένες άδειες μια εφαρμογή μπορεί να διαβάσει τα μηνύματα και τις επαφές, να πραγματοποιήσει κλήσεις και αποστολή μηνυμάτων και να διαγράψει αρχεία.

- Για τις άδειες υπογραφής το σύστημα παρέχει αυτά τα δικαιώματα κατά την εγκατάσταση, αλλά μόνο όταν η εφαρμογή που επιχειρεί να χρησιμοποιήσει μια

άδεια υπογράφεται από το ίδιο πιστοποιητικό με την εφαρμογή που καθορίζει την άδεια. Από το Android 8 (Oreo) και μετά ορισμένες άδειες υπογραφής είναι το BIND_NFC_SERVICE και το BIND_PRINT_SERVICE.

- Η τελευταία κατηγορία ειδικές άδειες είναι ιδιαίτερα ευαίσθητες και οι περισσότερες εφαρμογές δεν χρειάζεται να τις χρησιμοποιήσουν.

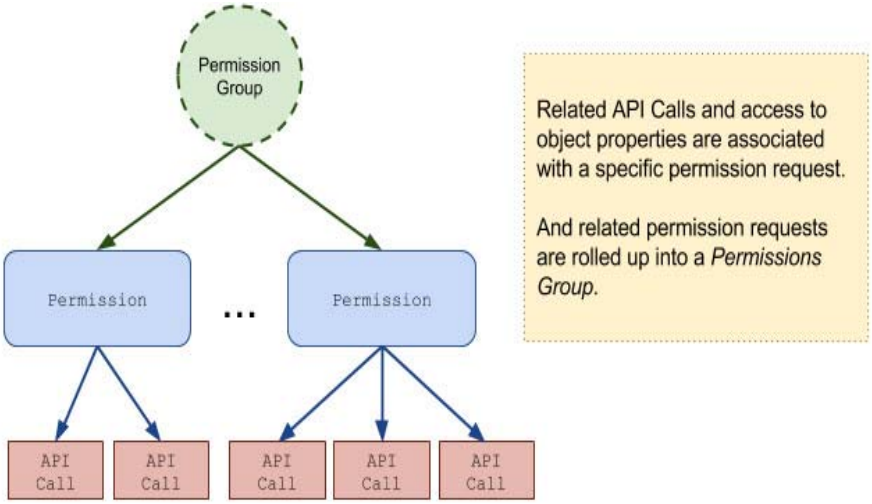
Για να μπορέσουν οι εφαρμογές να χρησιμοποιήσουν οποιαδήποτε από αυτές τις άδειες πρέπει να το δηλώσουν σε ένα αρχείο το AndroidManifest.xml. Σε αυτό το αρχείο το οποίο αναγκαστικά θα πρέπει να υπάρχει αναφέρονται βασικές πληροφορίες σχετικά με την εφαρμογή όπως το όνομα του πακέτου της εφαρμογής, τα χαρακτηριστικά εξοπλισμού και λογισμικού που απαιτούνται για να λειτουργήσει και επίσης τα δικαιώματα που χρειάζεται η εφαρμογή για να απόκτηση πρόσβαση σε δεδομένα ή άλλες εφαρμογές. Στην εικόνα 6 βλέπουμε ένα παράδειγμα για το πως μια εφαρμογή ζητά άδεια χρήσης για SMS που ανήκει στην κατηγορία επικίνδυνες άδειες. Στην συγκεκριμένη περίπτωση κατά την εκκίνηση της εφαρμογής το σύστημα θα εμφανίσει μήνυμα προς το χρήστη αν επιτρέπει την πρόσβαση για αποστολή μηνύματος ενώ σε αντίθετη περίπτωση που η άδεια χρήσης άνηκε στην κανονική κατηγορία το σύστημα θα της παραχωρούσε αυτόματα το δικαίωμα χωρίς να χρειάζεται να ενημερώσει και να έχει την έγκριση του χρήστη.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
          package="com.example.snazzyapp">

    <uses-permission android:name="android.permission.SEND_SMS"/>

    <application ...>
        ...
    </application>
</manifest>
```

Εικόνα 2.3.1: Παράδειγμα αρχείου AndroidManifest.xml[30]

Η οργάνωση των permissions γίνεται σε ομάδες που σχετίζονται με τις λειτουργίες ή τις δυνατότητες μια συσκευής. Με αυτό το τρόπο τα αιτήματα αδειών αντιμετωπίζονται

σαν ομάδα και μια ομάδα αντιστοιχεί σε πολλές άδειες δικαιωμάτων στο AndroidManifest. Για παράδειγμα όταν ζητηθεί η άδεια SEND_SMS και η άδεια READ_SMS στο χρήστη θα εμφανιστεί μήνυμα για έγκριση της ομάδας SMS. Έτσι πετυχαίνει την πιο προσιτή και απλή προσέγγιση προς τον χρήστη για πιο ξεκάθαρες επιλογές, χωρίς να τον μπερδεύει με περίπλοκα και τεχνικά ζητήματα [31].



Εικόνα 2.3.2: Άδεια Δικαιωμάτων σε Ομάδες[31]

Όλες οι άδειες μπορεί να ανήκουν σε ομάδες ανεξάρτητα από το επίπεδο προστασίας τους αλλά μόνο οι ομάδες που περιέχουν άδειες με επίπεδο προστασίας επικίνδυνο μπορεί να επηρεάσει την εμπειρία χρήσης. Από την έκδοση 6.0 και μετά, όπου έχουν γίνει αλλαγές στο τρόπο διαχείρισης των permissions όπως θα εξηγηθεί και πιο κάτω, αν δεν υπάρχει κάποια έγκριση για μια άδεια που ανήκει σε μια ομάδα τότε το σύστημα θα ενημερώσει το χρήστη για να εγκρίνει την πρόσβαση. Η ενημέρωση αυτή δεν επεξηγεί ακριβώς την άδεια που χρειάζεται μέσα σε αυτή την ομάδα, για παράδειγμα αν χρειάζεται την άδεια READ_CONTACTS θα ζητηθεί άδεια από τον χρήστη για πρόσβαση στις επαφές. Αν έχει δοθεί η πρόσβαση στην συγκεκριμένη άδεια και στην συνέχεια η εφαρμογή ζητήσει άδεια και για WRITE_CONTACTS τότε θα παραχωρηθεί αυτόματα από το σύστημα αφού ανήκει στην ίδια ομάδα.

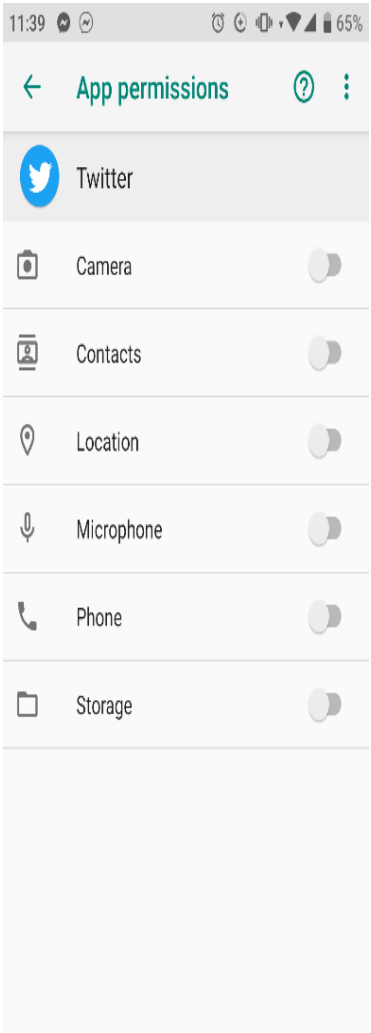
Table 1. Dangerous permissions and permission groups.

Permission Group	Permissions
CALENDAR	• READ_CALENDAR • WRITE_CALENDAR
CALL_LOG	• READ_CALL_LOG • WRITE_CALL_LOG • PROCESS_OUTGOING_CALLS
CAMERA	• CAMERA
CONTACTS	• READ_CONTACTS • WRITE_CONTACTS • GET_ACCOUNTS
LOCATION	• ACCESS_FINE_LOCATION • ACCESS_COARSE_LOCATION
MICROPHONE	• RECORD_AUDIO
PHONE	• READ_PHONE_STATE • READ_PHONE_NUMBERS • CALL_PHONE • ANSWER_PHONE_CALLS • ADD_VOICEMAIL • USE_SIP
SENSORS	• BODY_SENSORS
SMS	• SEND_SMS • RECEIVE_SMS • READ_SMS • RECEIVE_WAP_PUSH • RECEIVE_MMS
STORAGE	• READ_EXTERNAL_STORAGE • WRITE_EXTERNAL_STORAGE

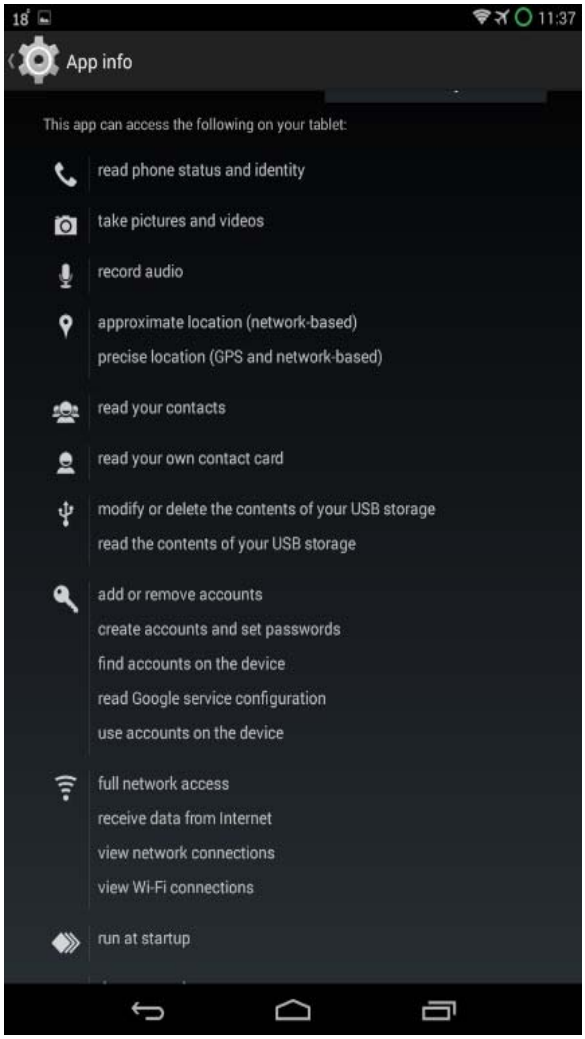
Εικόνα 2.3.3: Άδεια Δικαιωμάτων σε Ομάδες [22]

Όπως έχει προαναφερθεί κάθε νέα έκδοση φέρει αισθητικές αλλαγές αλλά και λειτουργικές. Ο τρόπος χειρισμού των permissions είναι μια από αυτές τις αλλαγές. Σύμφωνα το άρθρο Android Permissions: User Attention, Comprehension, and Behavior 2012 [08], η Google δεν επιτηρεί και ούτε περιορίζει τις εφαρμογές του Android αλλά χρησιμοποιεί τις άδειες δικαιωμάτων ούτως ώστε να ενημερώσει τους χρήστες για πιθανή παραβίαση των ιδιωτικών τους στοιχείων από κακόβουλες εφαρμογές. Στο παρών άρθρο αναφέρεται η παλιά μέθοδος αποδοχής των αδειών ασφαλείας κατά την εγκατάσταση της εφαρμογής , οι οποίες εμφανίζονταν σε μία λίστα χωρίς ο χρήστης να μπορεί να απορρίψει κάποια συγκεκριμένη. Αυτό συνέβαινε μέχρι την έκδοση 5.0(lollipop). Με την έκδοση Android 6.0 (Marshmallow) όμως έχει αλλάξει ο τρόπος παραχώρησης των αδειών δικαιωμάτων όπου εμφανίζονται κατά την λειτουργία της εφαρμογής μόνο οι επικίνδυνες άδειες και ξεχωριστά η μια από την άλλη [04]. Επιπλέον υπάρχει και η επιλογή μέσα από το μενού ρυθμίσεων, ο χρήστης να μπορεί να παραχωρήσει ή να ανακαλέσει οποιαδήποτε άδεια χρήσης ξεχωριστά[29]. Για παράδειγμα οι εικόνες 2.3.4 και 2.3.5 δείχνουν τα permissions τα οποία απαιτεί η εφαρμογή twitter και πως τα διαχειρίζεται η κάθε έκδοση Android. Η έκδοση 9 (Pie) η

οποία συνεχίζει την ίδια πρακτική από την έκδοση 6 και μετά μας επιτρέπει να επιλέξουμε την κάθε άδεια ξεχωριστά ενώ στη έκδοση 4.4.4 (KitKat) αφού έχουν εγκριθεί όλες αναγκαστικά κατά την εγκατάσταση τότε δεν μπορούμε να παρέμβουμε και να τις ανακαλέσουμε.



Εικόνα 2.3.4: Εφαρμογή σε Android 9



Εικόνα 2.3.5: Εφαρμογή σε Android 4.4.4

2.4 Κακόβουλο λογισμικό στα Android

Η πιο διαδεδομένη απειλή ασφαλείας είναι η κατάχρηση των υπηρεσιών από κακόβουλα λογισμικά. Οι καταχρήσεις αυτές περιλαμβάνουν αποστολή μηνυμάτων χωρίς την έγκριση ή την γνώση του χρήστη προς αριθμούς με υψηλές χρεώσεις. Επιπρόσθετα οι ανεπιθύμητες διαφημίσεις είναι αποτέλεσμα κακόβουλου λογισμικού όπως επίσης και η αποστολή προσωπικών δεδομένων σε άγνωστους παραλήπτες. Η Google υποστηρίζει ότι το Android είναι πιο ασφαλές από ότι ισχυρίζονται εταιρίες ασφαλείας οι οποίες

μεγαλοποιούν τον κίνδυνο για να αυξήσουν τις πωλήσεις λογισμικών ασφαλείας. Ερευνά της εταιρίας F-secure έδειξε ότι μόνο το 0.1% του κακόβουλου λογισμικού προέρχεται από το Google Play store [34] επιβεβαιώνοντας την Google που πιστεύει ότι τα πραγματικά κακόβουλα λογισμικά είναι σπάνια.

Όπως προαναφέρθηκε ακόμη ένα μεγάλο πρόβλημα ασφάλειας είναι ο κατακερματισμός (fragmentation) του Android. Οι προμηθευτές δεν υποστηρίζουν την ανανέωση και ενημέρωση παλαιοτέρων συσκευών στην τελευταία διαθέσιμη έκδοση Android, η οποία επιδιορθώνει διάφορα σφάλματα που βρίσκονται στο πυρήνα του λειτουργικού συστήματος, καθιστώντας τις ευάλωτες.

Τα κακόβουλα λογισμικά εκμεταλλεύονται τα τυχόν σφάλματα που υπάρχουν στο λειτουργικό για παραβίαση των δεδομένων και εκμετάλλευση των πόρων της συσκευής. Ορισμένα κακόβουλα λογισμικά παρουσιάζονται πιο κάτω[01].

- Backdoors: Το Backdoor malware είναι ένα είδος κακόβουλου λογισμικού που εκμεταλλεύεται τα δικαιώματα διαχειριστή (root) για να εγκαταστήσει άλλα κακόβουλα λογισμικά και να τους χορηγήσει δικαιώματα διαχειριστή χωρίς να γίνονται αντιληπτά από προγράμματα ασφάλειας. Σε μια τέτοια περίπτωση τα κακόβουλα λογισμικά αποκτούν πλήρη έλεγχο της συσκευής.

- Worms: Αναπαράγουν λειτουργικά αντίγραφα του εαυτού τους με σκοπό την μόλυνση συσκευών μέσω δίκτυο. Σε αντίθεση με τους ιούς, οι οποίοι απαιτούν την εξάπλωση ενός μολυσμένου αρχείου, τα Worms είναι αυτόνομο λογισμικό. Για να εξαπλωθούν, εκμεταλλεύονται μια ευπάθεια στο σύστημα είτε χρησιμοποιούν κάποιο είδος κοινωνικής μηχανικής για να εξαπατήσουν τους χρήστες να τα εκτελέσουν.

- Trojan: Ονομάζεται Δούρειος Ίππος (Trojan) εξαιτίας την εμφάνισης τους ως νόμιμο λογισμικό. Με την εγκατάσταση και την ενεργοποίηση τους έχουν πρόσβαση σε προσωπικές πληροφορίες χωρίς ο χρήστης να το γνωρίζει, προχωρώντας σε υποκλοπή δεδομένων

- Bots: Παρέχουν αυτοματοποιημένες υπηρεσίες και μπορεί να χρησιμοποιούν για καλές ή κακόβουλες ενέργειες. Το κακόβουλο λογισμικό έχει σχεδιαστεί για να μολύνει ένα υπολογιστή και να ενωθεί σε ένα κεντρικό υπολογιστή. Μπορούν να καταγράψουν πληροφορίες όπως καταγραφή πληκτρολογίου, συλλογή και ανάλυση στοιχείων και επιθέσεις DoS (Denial of Services.)

- Ransomware: Τα Ransomware είναι ένας τύπος κακόβουλου λογισμικού που απειλεί να δημοσιεύσει τα δεδομένα του θύματος ή να εμποδίσει την πρόσβαση σε αυτό, εκτός εάν καταβληθούν λύτρα. Ενώ μερικά απλά ransomware μπορούν να κλειδώσουν το σύστημα με τρόπο που δεν είναι δύσκολο για ένα έμπειρο άτομο να αντιστραφεί, το πιο προηγμένο κακόβουλο λογισμικό χρησιμοποιεί μια τεχνική που ονομάζεται κρυπτοβολική εκβίαση, η οποία κρυπτογραφεί τα αρχεία του θύματος, καθιστώντας τα απρόσιτα και απαιτεί την πληρωμή λύτρων για να τα αποκρυπτογραφήσει .

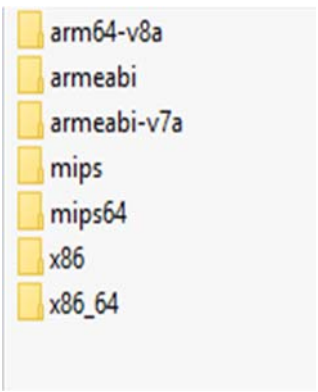
2.5 Αρχεία APK

Οι εφαρμογές Android διανέμονται και εγκαθίστανται με τη μορφή εφαρμογής (APK), τα οποία συνήθως αναφέρονται ως αρχεία APK. Τα αρχεία APK είναι αρχεία που περιλαμβάνουν τόσο κώδικα εφαρμογής όσο και πόρους, καθώς και το αρχείο δήλωσης εφαρμογής. Μπορούν επίσης να περιλαμβάνουν υπογραφή κώδικα. Η μορφή APK είναι μια επέκταση της μορφής Java JAR, 1 η οποία με τη σειρά της είναι μια επέκταση της δημοφιλούς μορφής αρχείου ZIP. Τα αρχεία APK έχουν τυπικά την επέκταση .apk και σχετίζονται με τον τύπο MIME της εφαρμογής / vnd.android.package-archive[10]. Επειδή τα αρχεία APK είναι συμπιεσμένα αρχεία και συμπεριφέρονται σαν αρχεία ZIP, μπορείτε εύκολα να εξεταστεί το τι περιέχουν, εξάγοντάς τα με ένα από τα πολλά προγράμματα συμπίεσης που υποστηρίζουν εξαγωγή από ZIP μορφή.

Εικόνα 2.5.1: Περιεχόμενα ενός APK

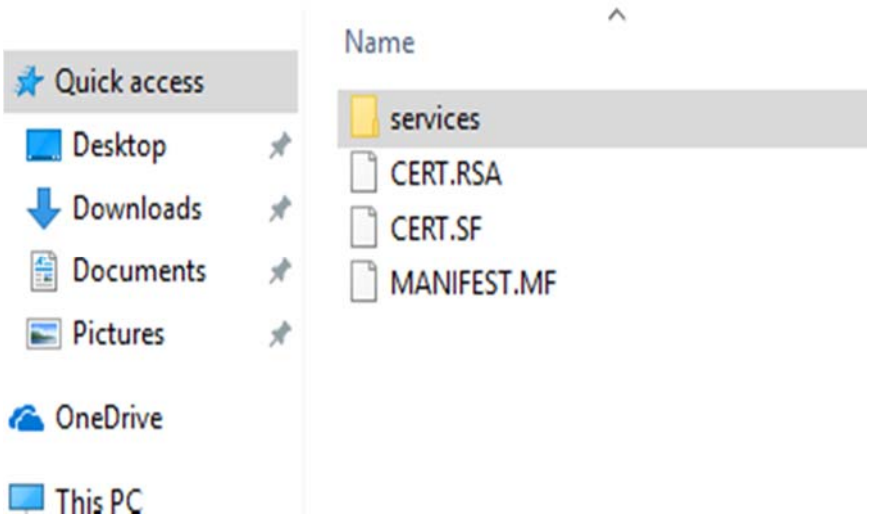
Κάθε αρχείο APK πρέπει να περιέχει ένα αρχείο AndroidManifest.xml το οποίο δηλώνει το όνομα του πακέτου της εφαρμογής, τις άδειες χρήσης, την έκδοση, τα στοιχεία του Developer και άλλα δεδομένα που θα πρέπει να αναφερθούν. Το αρχείο classes.dex περιέχει τον κώδικα της εφαρμογής και βρίσκεται σε μορφή DEX του Dalvik VM. Το αρχείο resources.arsc περιέχει συγκεντρωμένους πόρους σε δυαδική μορφή. Μπορεί να περιλαμβάνει εικόνες, συμβολοσειρές ή άλλα δεδομένα που χρησιμοποιούνται από το πρόγραμμα. Ο φάκελος assets χρησιμοποιείται για την συγκέντρωση αρχείων όπως μουσικής, γραμματοσειρές και εικόνες στην αρχική τους μορφή . Στην περίπτωση που οι δημιουργοί μια εφαρμογής χρησιμοποιήσουν κώδικα μέσω JNI (Java Native Interface) (Oracle |Introduction) για υποστήριξη και την λειτουργία σε πολλές και διαφορετικές πλατφόρμες τότε υπάρχει ο φάκελος lib με υποφακέλους για κάθε ξεχωριστή πλατφόρμα που υποστηρίζεται.

Εικόνα 2.5.2: Περιεχόμενα φακέλου assets



Εικόνα 2.5.3: Περιεχόμενα φακέλου lib

Διάφοροι πόροι όπως κινούμενες εικόνες, εικόνες και μενού που αναφέρονται απευθείας από τον κώδικα Android, είτε άμεσα χρησιμοποιώντας την κλάση android .content.res.Resources ή έμμεσα μέσω ανώτερου επιπέδου APIs, αποθηκεύονται στον φάκελο res σε ξεχωριστούς υποφακέλους για το καθένα. Τα αρχεία APK περιέχουν επίσης έναν φάκελο META-INF, ο οποίος περιέχει το αρχείο MANIFEST.MF και υπογραφές κωδικών οι οποίοι θα εξηγηθούν πιο κάτω.



Εικόνα 2.5.4: Περιεχόμενα φακέλου META-INF

Όλες οι εφαρμογές Android πρέπει να υπογράφονται από τον προγραμματιστή τους, συμπεριλαμβανομένων εφαρμογών συστήματος. Επειδή τα αρχεία APK Android αποτελούν επέκταση της μορφής πακέτου Java JAR, 8 η μέθοδος υπογραφής κώδικα που χρησιμοποιείται βασίζεται επίσης στην υπογραφή JAR. Το Android χρησιμοποιεί την υπογραφή APK για να βεβαιωθεί ότι οι ενημερώσεις για μια εφαρμογή προέρχονται από τον ίδιο δημιουργό και να δημιουργήσουν σχέσεις εμπιστοσύνης μεταξύ εφαρμογών. Και οι δύο αυτές δυνατότητες ασφαλείας εφαρμόζονται μέσω της σύγκρισης του πιστοποιητικού υπογραφής της τρέχουσας εγκατεστημένης εφαρμογής προορισμού με το πιστοποιητικό της ενημερωμένης έκδοσης ή σχετικής εφαρμογής.

Οι εφαρμογές συστήματος υπογράφονται από διάφορα κλειδιά ασφαλείας της πλατφόρμας. Τα διαφορετικά στοιχεία του συστήματος μπορούν να μοιράζονται πόρους και να τρέχουν μέσα στην ίδια διαδικασία όταν υπογράφονται με το ίδιο κλειδί πλατφόρμας. Τα κλειδιά πλατφόρμας παράγονται και ελέγχονται από όποιον διατηρεί την έκδοση Android εγκατεστημένη σε μια συγκεκριμένη συσκευή: κατασκευαστές

συσκευών, μεταφορείς, Google for Nexus συσκευές ή χρήστες για δικές τους εφαρμογές μέσων εκδόσεων Android.

Η υπογραφή κώδικα APK ή αλλιώς το πιστοποιητικό υπογραφής APK, χρησιμοποιείται και για ελέγχους κατά την διάρκεια της εγκατάστασης. Οι κύριοι λόγοι για την υπογραφή του κώδικα είναι η ακεραιότητα και η αυθεντικότητα. Όπως και σε όλα τα άλλα λειτουργικά πριν την εκτέλεση οποιασδήποτε εφαρμογής από τρίτους πρέπει να υπάρχει η επιβεβαίωση ότι ο κώδικας δεν έχει παραβιαστεί ή να πιστοποιείτε η αυθεντικότητα της πηγής της. Ένας από τους τρόπους για επιτύχει αυτός ο στόχος είναι με ένα σχέδιο ψηφιακής υπογραφής, το οποίο εγγυάται ότι μόνο η οντότητα που κατέχει το κλειδί υπογραφής μπορεί να παράγει έγκυρη υπογραφή κώδικα. Παρόλα αυτά το πιστοποιητικό υπογραφής δεν μπορεί να πιστοποιήσει ότι ο κώδικας είναι ασφαλής για να εκτελεστεί στην συσκευή μας. Επειδή η υπογραφή κώδικα Android βασίζεται σε υπογραφή Java JAR, χρησιμοποιεί δημόσια κλειδιά κρυπτογράφησης και πιστοποιητικά X.509 όπως πολλά προγράμματα υπογραφής κώδικα.

Η υπογραφή κώδικα Java εκτελείται σε επίπεδο αρχείου JAR. Τα αρχεία Jar manifest επαναχρησιμοποιούνται και επεκτείνονται για να προστεθεί μια υπογραφή. Το κύριο αρχείο δήλωσης JAR (MANIFEST.MF) έχει καταχωρήσεις με το όνομα κάθε αρχείου που υπάρχει στο APK με το κάθε hash που προκύπτει από την μέθοδο κρυπτογράφησης του για να δημιουργηθεί αυτή η υπογραφή. Για παράδειγμα στην εικόνα 15 είναι ένα δείγμα από τα περιεχόμενα του MANIFEST.MF.

```
Manifest-Version: 1.0
Created-By: singlejar

Name: AndroidManifest.xml
SHA-256-Digest: JqJkzZgldORBJNVquPMboITqAN2OXMhT5j2JptYlvMk=

Name: META-INF/services/com.google.protobuf.GeneratedExtensionRegistry
 Loader
SHA-256-Digest: Reh2kj7jH2f3e7PzQKvPS3IJWUNpqh+sXlpWabn+Gm4=

Name: android-support-multidex.version.txt
SHA-256-Digest: OuJRlNnX1srJFP8Td2Bv9F5nMX3O5iAgxf15egCfa+Q=

Name: assets/AEprec_100.emd
SHA-256-Digest: PWUMcRA6EImz4kkle4/4S0VoyeOQk3qvFAHhWGUqfrM=

Name: assets/AmaticSC-Bold.ttf
SHA-256-Digest: 02e+re5m77tlfSTT2PMPO2BjPplcjelzhVQc93XKu00=
```

Εικόνα 2.5.5: *Περιεχόμενα MANIFEST.MF*

Όπως φαίνεται και στην εικόνα 2.5.5 στο φάκελο META-INF υπάρχουν ακόμη δυο αρχεία που θα χρησιμοποιηθούν για να υλοποιηθεί η υπογραφή του κώδικα JAVA. Το αρχείο με επέκταση .SF, ένα αρχείο υπογραφής που περιλαμβάνει όλα τα αρχεία που θα υπογραφτούν, καθώς και την ψηφιακή υπογραφή που έχει επέκταση .RSA, .DSA ή .EC ανάλογα με τον αλγόριθμο που θα χρησιμοποιηθεί. Το αρχείο υπογραφής περιλαμβάνει το αρχείο MANIFEST.MF καθώς και όλα τα υπόλοιπα αρχεία που ήδη περιέχονται στο αρχείο MANIFEST.

```
Signature-Version: 1.0
Created-By: 1.0 (Android SignApk)
SHA-256-Digest-Manifest: IfOvW0AyTEUUZYa8tLrRSf0cFuHKIJsEdmylVCyKAlc=
X-Android-APK-Signed: 2, 3

Name: AndroidManifest.xml
SHA-256-Digest: +72iSRqc9uilOg/R7NhhMeNF3ISFiH9cMS1dR78ZQTY=

Name: META-INF/services/com.google.protobuf.GeneratedExtensionRegistry
 Loader
SHA-256-Digest: MX1PHKsrWkmOZFeJG6azRzbIPsCfE2tyR0pa8/mXD/g=

Name: android-support-multidex.version.txt
SHA-256-Digest: 6/lnFOH7mFVER94rAWcUmubglFFrHR7nf8+7zqQOgQs=

Name: assets/AEprec_100.emd
SHA-256-Digest: HZ9MATFX2YCjwAihknR57j3ZiwlGHUoWGAWu7dqPhjU=
```

Εικόνα 2.5.6: Περιεχόμενα αρχείου CERT.CF

Μέχρι την έκδοση JAVA 6 η προεπιλεγμένη έκδοση αλγορίθμου ήταν SHA-1 ενώ από την έκδοση 7 και μετά μπορεί να χρησιμοποιηθεί η έκδοση SHA-256 και SHA-512. Το λειτουργικό Android από την έκδοση 4.3 μπορεί να χρησιμοποιήσει και τους δυο αλγορίθμους.

Τα επίσημα εργαλεία JDK για την υπογραφή και την επαλήθευση JAR είναι οι εντολές jarsigner και keytool. Ένα αρχείο JAR έχει υπογραφεί χρησιμοποιώντας την εντολή jarsigner καθορίζοντας ένα αρχείο κλειδιού μαζί με το ψευδώνυμο του κλειδιού που χρησιμοποιείται για την υπογραφή (τα πρώτα οκτώ οι χαρακτήρες του ψευδώνυμου γίνονται το όνομα βάσης για το αρχείο μπλοκ υπογραφής, εκτός εάν έχει οριστεί η επιλογή -sigfile) και ο επιλεγμένος αλγόριθμος υπογραφής.

Η επαλήθευση αρχείου JAR εκτελείται χρησιμοποιώντας την εντολή jarsigner καθορίζοντας την επιλογή -verify. Η δεύτερη εντολή jarsigner πρώτα επαληθεύει το

μπλοκ υπογραφής και το πιστοποιητικό υπογραφής, διασφαλίζοντας ότι δεν έχει παραβιαστεί το αρχείο υπογραφής. Στη συνέχεια, επαληθεύει ότι κάθε digest στο αρχείο υπογραφής (CERT.SF) ταιριάζει με την αντίστοιχη ενότητα στο αρχείο manifest (MANIFEST.MF). (Ο αριθμός των καταχωρήσεων στο αρχείο υπογραφής δεν πρέπει να ταιριάζει με εκείνους που υπάρχουν στο αρχείο δήλωσης. Τα αρχεία μπορούν να προστεθούν στον καταχωρημένο JAR χωρίς να ακυρώνεται η υπογραφή του: αρκεί να μην έχει αλλάξει κανένα από τα αρχικά αρχεία, η επαλήθευση είναι επιτυχής.)

Τέλος, το jarsigner διαβάζει κάθε δηλωμένη καταχώρηση και ελέγχει ότι το αρχείο digest ταιριάζει με τα πραγματικά περιεχόμενα του αρχείου. Εάν έχει οριστεί μια δέσμη κλειδιών με την επιλογή -keystore, το jarsigner ελέγχει επίσης για να διαπιστώσει αν υπάρχει το πιστοποιητικό υπογραφής στην καθορισμένη δέσμη κλειδιών. Από την Java 7, υπάρχει μια νέα επιλογή περιορισμού που επιτρέπει την επικύρωση πρόσθετων πιστοποιητικών, συμπεριλαμβανομένου του ελέγχου της χρονικής εγκυρότητας και της επαλήθευσης της αλυσίδας πιστοποιητικών. Τα σφάλματα επικύρωσης αντιμετωπίζονται ως προειδοποιήσεις και αντικατοπτρίζονται στον κώδικα εξόδου της εντολής jarsigner.

Στην περίπτωση αυτής της μεταπτυχιακής διατριβής για υπογραφή των τροποποιημένων .apk αρχείων θα χρησιμοποιηθεί το uber-apk-signer.jar του οποίου η υπογραφή και η επαλήθευση φαίνεται στην εικόνα 2.5.7.

```
zipalign location: BUILT_IN
       C:\Users\panikos\AppData\Local\Temp\uapksigner-1325059971755619292\win-zipalign_25_0_0.exe559670008813662459.tmp

keystore:
       [0] 161a0018 C:\Users\panikos\AppData\Local\Temp\temp_3742587261289875769_debug.keystore (DEBUG_EMBEDDED)

01. reddit.apk

       SIGN
       file: C:\Users\panikos\.apkstudio\vendor\reddit.apk (24.86 MiB)
       checksum: 7b374003b61c6cd23b1fc9743afd6bff049aa37934ead557de0d8f87e2ba09a8 (sha256)
       - zipalign success
       - sign success

       VERIFY
       file: C:\Users\panikos\.apkstudio\vendor\reddit-aligned-debugSigned.apk (25.11 MiB)
       checksum: 264c0ca46ef1682aff3a4ec13377eaa49a1519a9d0fb20c7b71cdf8d90cff387 (sha256)
       - zipalign verified
       - signature verified [v1, v2]
              Subject: CN=Android Debug, OU=Android, O=US, L=US, ST=US, C=US
              SHA256: 1e08a903aef9c3a721510b64ec764d01d3d094eb954161b62544ea8f187b5953 / SHA256withRSA
              Expires: Thu Mar 10 22:10:05 EET 2044
```

Εικόνα 2.5.7: Υπογραφή και Πιστοποίηση apk αρχείου

2.6 Σκοπός της εργασίας

Η εκπόνηση της διατριβής αυτής, έχει ως στόχο να μελετήσει τα permissions που απαιτούνται από ένα αριθμό εφαρμογών και να διαπιστώσει αν οι εφαρμογές ζητούν τις άδειες που είναι αναγκαίες για την σωστή λειτουργία τους ή αν υπερβαίνουν τα δικαιώματα τους, χρησιμοποιώντας πόρους και πληροφορίες εν αγνοία του χρήστη.

Μέσω της πειραματικής διαδικασίας που θα ακολουθήσει, η παρούσα διατριβή καλείται να απαντήσει τα πιο κάτω ερευνητικά ερωτήματα

- Οι άδειες δικαιωμάτων είναι οι απαραίτητες για την σωστή λειτουργία της εκάστοτε εφαρμογής
- Αν εκτελούνται άδειες δικαιωμάτων εν αγνοία του ίδιου του χρήστη
- Αν παραβιάζονται τα δικαιώματα που εγκρίνει ο χρήστης και σε ποιο βαθμό

Κεφάλαιο 3
Σχεδιασμός

3.1 Λογισμικό και Υλικό

Για την Διπλωματική εργασία θα χρειαστεί να χρησιμοποιήσουμε ορισμένα 3rd. party προγράμματα τα οποία θα μας επιτρέψουν να πραγματοποιήσουμε αλλαγές στα δικαιώματα χρήσης στο AndroidManifest.xml.

Οι εφαρμογές για το Android είναι αρχεία σε μορφή apk. Στην ουσία το αρχείο apk είναι συμπιεσμένα πολλά αρχεία που σχετίζονται με την εκάστοτε εφαρμογή όπως ο κώδικα και διάφορα άλλα δεδομένα που χρειάζονται π.χ. γραφικά στοιχεία. Αν προσπαθήσουμε να χρησιμοποιήσουμε το WinRAR ή οποιοδήποτε άλλο διαδεδομένο πρόγραμμα για αποσυμπίεση του αρχείου για εξαγωγή των αρχείων θα παρατηρήσουμε ότι δεν εμφανίζονται σε μορφή κατανοητή ώστε να μπορούμε να τα επεξεργαστούμε. Αυτό συμβαίνει γιατί εκτός από συμπιεσμένα τα αρχεία έχουν δεχθεί και επεξεργασία από το λογισμικό προγραμματισμού για να γίνονται κατανοητά από το σύστημα[25] ή αλλιώς compiling .

Εικόνα 3.1.1: AndroidManifest μετά από εξαγωγή με WINRAR

Για να καταφέρουμε να εμφανίσουμε το AndroidManifest στην αρχική πηγή όπως είχε δημιουργηθεί από τον προγραμματιστή και στη συνέχεια να το τροποποιήσουμε πρέπει η εφαρμογή να γίνει decompile. Για decompiling και compiling των εφαρμογών θα χρησιμοποιήσουμε το πρόγραμμα apktool. Το πρόγραμμα apktool είναι ένα δωρεάν εργαλείο το οποίο χρησιμοποιείται για decompiling και αποσυμπίεση αρχείων apk, εμφανίζοντας όλα τα αρχεία σε ένα φάκελο έτσι ώστε να μπορούμε να τροποποιήσουμε τα αρχεία και να πραγματοποιήσουμε τις αλλαγές που θέλουμε. Το συγκεκριμένο πρόγραμμα βασίζεται στη γλώσσα προγραμματισμού java και μπορεί να βρεθεί στην σελίδα https://ibotpeaches.github.io/Apktool/ από όπου θα κατεβάσουμε το αρχείο σε μορφή .jar και θα το μεταφέρουμε στο φάκελο που βρίσκονται τα αρχεία apk τα οποία και θα τροποποιήσουμε. Οι εντολές που θα χρειαστούμε είναι η java -jar apktool.jar d "file.apk" και η java -jar apktool.jar b "foldername" -o file.apk. Η πρώτη εντολή αφορά την αποσυμπίεση (decompile) και δηλώνεται με το γράμμα d και ακολούθως το όνομα της εφαρμογής με την επέκταση. Για την συμπίεση του φακέλου που έχει προκύψει από την προηγουμένη εντολή χρησιμοποιείται η δεύτερη εντολή με το γράμμα b όπου ακολουθεί το όνομα του φακέλου και στην συνέχεια η επιλογή -o που δηλώνει το όνομα του αρχείου .apk που θα δημιουργηθεί.

Στην συνέχεια με το πρόγραμμα notepad++ θα προχωρήσουμε με τις αλλαγές μας στο AndroidManifest πριν να το μετατρέψουμε πάλι σε αρχείο apk. Το notepad++ είναι ένας δωρεάν επεξεργαστής κειμένου και κώδικα και είναι διαθέσιμο προς όλους στην ιστοσελίδα https://notepad-plus-plus.org/. Το εν λόγω πρόγραμμα θα μας βοηθήσει στο έλεγχο και τις αλλαγές που θα πραγματοποιήσουμε στο AndroidManifest.xml.

Το λειτουργικό Android απαιτεί ψηφιακή υπογραφή με πιστοποιητικό για να μπορέσει να γίνει εγκατάσταση στην συσκευή μας. Για να το πετύχουμε αυτό χρησιμοποιήσουμε το πρόγραμμα uber-signed-apk το οποίο μας επιτρέπει να προχωρήσουμε με τις δοκιμές μας. Το uber-signed-apk, που επίσης χρησιμοποιεί την γλώσσα προγραμματισμού java, είναι ένα εργαλείο που βοηθά στην υπογραφή και την πιστοποίηση πολλαπλών εφαρμογών Android (APK) είτε με πιστοποιητικά debug είτε με άλλα διαθέσιμα πιστοποιητικά. Το πρόγραμμα το βρίσκουμε στην ιστοσελίδα https://github.com/patrickfav/uber-apk-signer/releases/tag/v1.0.0 σε αρχείο .jar και το μεταφέρουμε στον ίδιο φάκελο που βρίσκονται τα αρχεία των εφαρμογών apk. Με την

εντολή “java -jar uber-signed-apk.jar -a file.apk” μπορούμε να χρησιμοποιήσουμε πιστοποιητικό debug για έλεγχο των εφαρμογών μας.

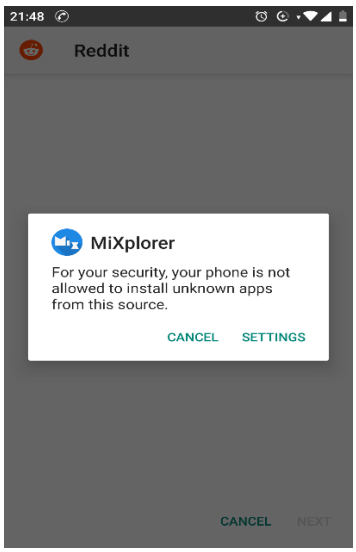
Σύμφωνα και με την βιβλιογραφία υπάρχουν αρκετοί τρόποι και προγράμματα για έλεγχο των δικαιωμάτων και σε αρκετές περιπτώσεις έχουν δημιουργηθεί προγράμματα από τους ερευνητές για περισσότερο έλεγχο όπως το Stowaway[7]. Παρόλα αυτά έχουν επιλεχθεί τα συγκεκριμένα τρία προγράμματα γιατί είναι δωρεάν και εύκολα προσβάσιμα από το κοινό, έχουν χαμηλές απαιτήσεις σε υπολογιστικές ανάγκες και λόγω της απλής λειτουργίας τους, που ανταποκρίνεται πλήρως στην σχετική έρευνα, είναι εύκολα στην χρήση.

Για έλεγχο των εφαρμογών θα χρησιμοποιηθεί το smartphone Xiaomi Mi A1 με έκδοση Android 9 η οποία είναι και η τελευταία έκδοση λειτουργικού android.

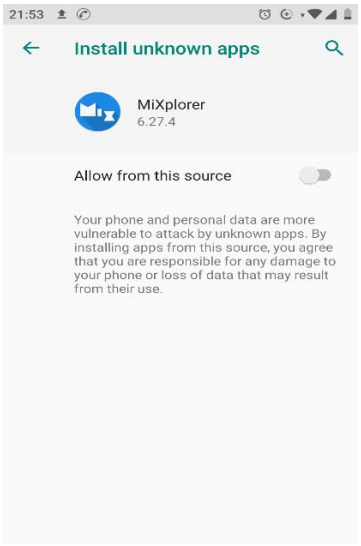
3.2 Πειραματική Διαδικασία

Σε αυτή την διαδικασία θα γίνει έλεγχος σε είκοσι εφαρμογές τις οποίες θα κατεβάσουμε από την ιστοσελίδα apkmirror.com. Οι εφαρμογές αυτές αφορούσαν διάφορες κατηγορίες όπως παιχνίδια single player, παιχνίδια multiplayer και εφαρμογές που είχαν σχέση με φωτογραφίες, ενημέρωση και forums. Τα αρχεία είναι σε μορφή .apk και είναι έτοιμα προς εγκατάσταση στο τηλέφωνο μας.

Με τον file explorer του κινητού μας βρίσκουμε τα αρχεία των εφαρμογών και προχωρούμε στην εγκατάσταση. Στην πρώτη εφαρμογή το λειτουργικό μας εμφανίζει μήνυμα ότι η συσκευή μας δεν επιτρέπει την εγκατάσταση και θα πρέπει να ενεργοποιήσουμε την εγκατάσταση εφαρμογών από άγνωστες πηγές μέσα από τις ρυθμίσεις όπως φαίνεται και στην εικόνα 3.2.1. Μέσα από τις ρυθμίσεις του λειτουργικού και το μενού apps & notification επιλέγουμε το special app access και δίνουμε έγκριση στο file explore μας για εγκατάσταση των εφαρμογών από άγνωστες πηγές. Μετα την έγκριση δεν θα ξαναπαρουσιαστεί το μήνυμα ασφαλείας.

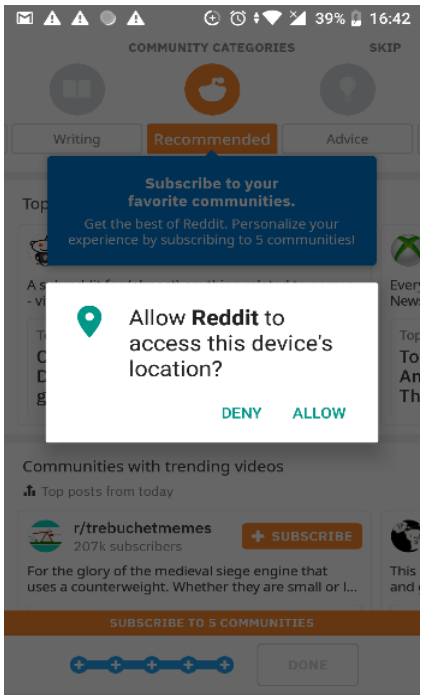


Εικόνα 3.2.1:*Μηνυμα ασφαλείας για άγνωστες πηγές*

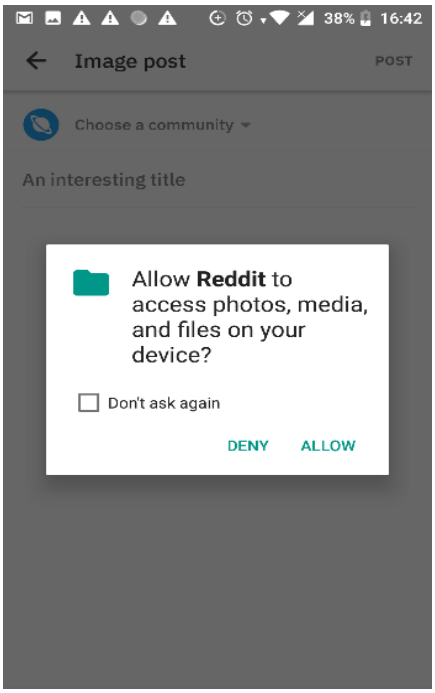


Εικόνα 3.2.2: *Έγκριση Άδειας Εγκατάστασης για άγνωστες πηγές*

Αρχικά εγκαθιστούμε την εκάστοτε εφαρμογή στη συσκευή και παρατηρούμε την εφαρμογή σε κανονική λειτουργία όπως τι δικαιώματα χρήσης ζητά και πως δουλεύει. Στο συγκεκριμένο παράδειγμα θα χρησιμοποιήσουμε την εφαρμογή Reddit. Μετά την εγκατάσταση η εφαρμογή μας ζητάει να παραχωρήσουμε δικαιώματα χρήσης σε τοποθεσία και σε μονάδα αποθήκευσης(αρχεία).



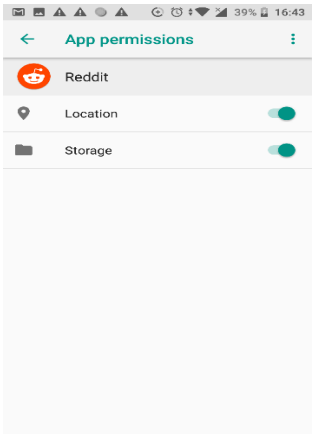
Εικόνα 3.2.3: Έγκριση Άδειας Δικαιωμάτων



Εικόνα 3.2.4: Έγκριση Άδειας Δικαιωμάτων

Σε περίπτωση που απορρίψουμε την έγκριση σε αυτά τα δικαιώματα χρήσης η εφαρμογή συνεχίζει να δουλεύει χωρίς όμως την δυνατότητα της αποθήκευση και δημοσίευση εικόνων αφού δεν έχει πρόσβαση στην μονάδα αποθήκευσης.

Στην συνέχεια δίνουμε την έγκριση μας και επιβεβαιώνουμε ότι η εφαρμογή αξιοποιεί όλες της τις δυνατότητες.



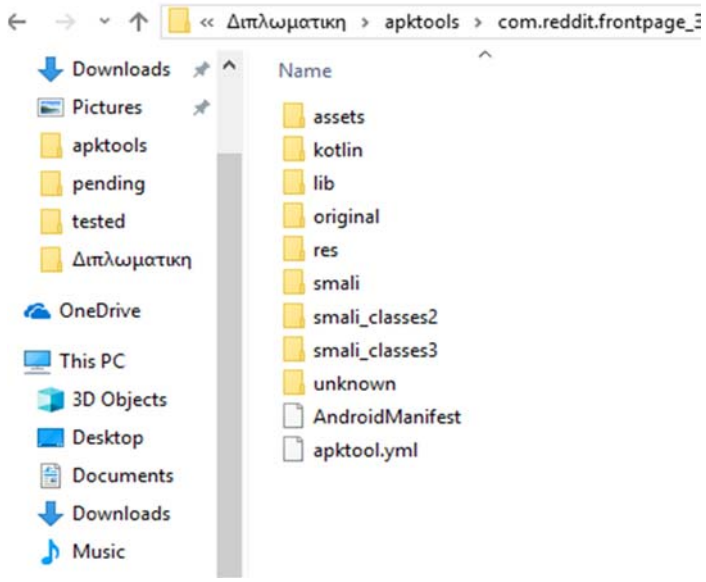
Εικόνα 3.2.5: Εμφάνιση των Αδειών Δικαιωμάτων

Αφού διαγράψουμε την εφαρμογή από το κινητό, μεταφέρουμε τις εφαρμογές στον υπολογιστή και με το πρόγραμμα apktool θα προχωρήσουμε σε decompile των apk. Με την χρήση του command prompt στο φάκελο όπου αποθηκεύσαμε τα αρχεία των εφαρμογών και το apktool.jar εισάγουμε την εντολή java -jar apktool.jar d “file.apk”.

```
C:\Users\panikos\.apkstudio\vendor>java -jar apktool.jar d "com.reddit.frontpage_3.15.0-220236_minAPI21(armeabi-v7a,x86)
(nodpi)_apkmirror.com.apk"
I: Using Apktool 2.3.4 on com.reddit.frontpage_3.15.0-220236_minAPI21(armeabi-v7a,x86)(nodpi)_apkmirror.com.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\panikos\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Εικόνα 3.2.6: Apktool Decompile

Όταν τελειώσει το decompile όλα τα αρχεία της εφαρμογής εμφανίζονται σε ένα φάκελο με την ονομασία της εφαρμογής όπου βρίσκεται και το αρχείο AndroidManifest.xml



Εικόνα 3.2.7: Φάκελος Αρχείων

Στη συνέχεια θα τρέξουμε το πρόγραμμα notepad++ και θα ανοίξουμε το αρχείο AndroidManifest.xml το οποίο έχει όλα τα δικαιώματα χρήσης που απαιτεί η εφαρμογή.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk,
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-feature android:name="android.hardware.camera" android:required="false"/>
    <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
    <uses-permission android:maxSdkVersion="22" android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
    <uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/>
    <uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/>
    <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="com.reddit.frontpage.permission.C2D_MESSAGE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="com.google.android.providers.gsf.permission.READ_GSERVICES"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
    <uses-permission android:name="com.sec.android.provider.badge.permission.READ"/>
    <uses-permission android:name="com.sec.android.provider.badge.permission.WRITE"/>
    <uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.htc.launcher.permission.UPDATE_SHORTCUT"/>
    <uses-permission android:name="com.sonyericsson.home.permission.BROADCAST_BADGE"/>
    <uses-permission android:name="com.sonymobile.home.permission.PROVIDER_INSERT_BADGE"/>
    <uses-permission android:name="com.anddoes.launcher.permission.UPDATE_COUNT"/>
    <uses-permission android:name="com.majeur.launcher.permission.UPDATE_BADGE"/>
    <uses-permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE"/>
    <uses-permission android:name="com.huawei.android.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.huawei.android.launcher.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.READ_APP_BADGE"/>
    <uses-permission android:name="com.oppo.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.oppo.launcher.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="me.everything.badger.permission.BADGE_COUNT_READ"/>
    <uses-permission android:name="me.everything.badger.permission.BADGE_COUNT_WRITE"/>
    <uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
```

Εικόνα 3.2.8: AndroidManifest.xml

Σε αυτή την περίπτωση θα απενεργοποιήσουμε μόνο το <uses-permission android:name= ”android.permission.WRITE_EXTERNAL_STORAGE”/> το οποίο αφορά την εγγραφή στην μνήμη του τηλεφώνου για να διαπιστώσουμε αν μπορούμε να χρησιμοποιήσουμε την δημοσίευση εικόνων. Η απενεργοποίηση γίνεται με την διαγραφή της συγκεκριμένης άδειας από το αρχείο μας και προχωρούμε στην αποθήκευση του.

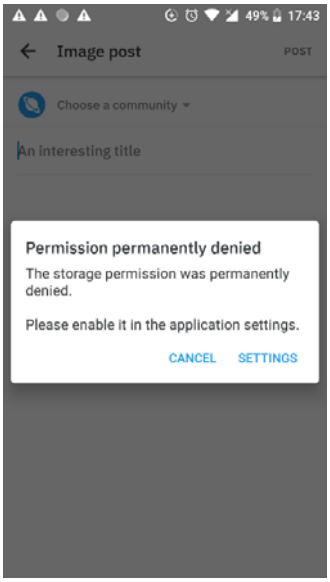
Με το apktool και την εντολή η java -jar apktool.jar b “foldername” -o file.apk κάνουμε compile το φάκελο σε αρχείο apk. Στην συνέχεια χρησιμοποιούμε το uber-apk-signer για να δημιουργηθεί ψηφιακή υπογραφή για να μπορούν να εγκατασταθούν οι εφαρμογές μας.

```
C:\Users\panikos\.apkstudio\vendor>java -jar apktool.jar b "com.reddit.frontpage_3.15.0-220236_minAPI21(armeabi-v7a,x86)
(nodpi)_apkmirror.com" -o reddit.apk
I: Using Apktool 2.3.4
I: Checking whether sources has changed...
I: Checking whether sources has changed...
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...

C:\Users\panikos\.apkstudio\vendor>java -jar uber-apk-signer.jar  -a reddit.apk
source:
       C:\Users\panikos\.apkstudio\vendor
zipalign location: BUILT_IN
       C:\Users\panikos\AppData\Local\Temp\uapksigner-1325059971755619292\win-zipalign_25_0_0.exe559670008813662459.tmp

keystore:
       [0] 161a0018 C:\Users\panikos\AppData\Local\Temp\temp_3742587261289875769_debug.keystore (DEBUG_EMBEDDED)

01. reddit.apk

       SIGN
       file: C:\Users\panikos\.apkstudio\vendor\reddit.apk (24.86 MiB)
       checksum: 7b374003b61c6cd23b1fc9743afd6bff049aa37934ead557de0d8f87e2ba09a8 (sha256)
       - zipalign success
       - sign success

       VERIFY
       file: C:\Users\panikos\.apkstudio\vendor\reddit-aligned-debugSigned.apk (25.11 MiB)
       checksum: 264c0ca46ef1682aff3a4ec13377eaa49a1519a9d0fb20c7b71cdf8d90cff387 (sha256)
       - zipalign verified
       - signature verified [v1, v2]
              Subject: CN=Android Debug, OU=Android, O=US, L=US, ST=US, C=US
              SHA256: 1e08a903aef9c3a721510b64ec764d01d3d094eb954161b62544ea8f187b5953 / SHA256withRSA
              Expires: Thu Mar 10 22:10:05 EET 2044

[Fri Oct 26 17:41:17 EEST 2018][v0.8.4]
```

Εικόνα 3.2.9: Apktool Compiling

Αφού το ξανατρέξουμε στο κινητό παρατηρούμε ότι δεν μας βγάζει πλέον την επιλογή για την μονάδα αποθήκευσης και μας εμφανίζει μήνυμα ότι είναι μόνιμα απενεργοποιημένη ακόμα και αν ενεργοποιηθεί μέσω των ρυθμίσεων. Έστω και αν εμείς

επιλέξαμε να αφαιρέσουμε μόνο την εγγραφή έχει απενεργοποιηθεί και η ανάγνωση στην μνήμη του τηλεφώνου.



Εικόνα 3.2.10: Απενεργοποίηση Άδειας Χρήσης

Αφού σημειωθούν οι διάφορες και οι παρατηρήσεις μας σχετικά με την συμπεριφορά της εφαρμογής, θα απεγκατασταθεί και θα επαναληφθεί η διαδικασία για κάθε μια από τις υπόλοιπες άδειες δικαιωμάτων.

Κεφάλαιο 4
Συλλογή Δεδομένων

4.1 Android Permissions

Το λειτουργικό σύστημα Android για να προστατέψει τους χρήστες και τα δεδομένα τους χρησιμοποιεί άδειες δικαιωμάτων τις οποίες πρέπει να αποκτήσουν οι εφαρμογές. Ανάλογα την επικινδυνότητα της εκάστοτε λειτουργίας το σύστημα μπορεί να παραχωρήσει την άδεια αυτόματα ή να ζητήσει την άδεια από το χρήστη.

Οι άδειες που δίνονται από το σύστημα ονομάζονται Normal Permissions και είναι οι άδειες οι οποίες δεν εμπεριέχουν τόσο κίνδυνο στο χρήστη ή στο σύστημα. Ένα παράδειγμα, είναι η αλλαγή του φόντου της οθόνης.

Οι επικίνδυνες άδειες δικαιωμάτων ή αλλιώς dangerous permissions είναι άδειες οι οποίες επηρεάζουν δεδομένα ή πηγές που αφορούν δεδομένα του χρήστη ή να επηρεάσουν την σωστή λειτουργία άλλων εφαρμογών. Για παράδειγμα η άδεια δικαιωμάτων για την αποστολή SMS θεωρείται επικίνδυνη.

4.2 Ανάλυση Permissions

Σε συνέχεια του πιο πάνω θα προχωρήσω σε μια ανάλυση των permissions που υπήρχαν στις εφαρμογές μας και στην διαβάθμιση του.

- android.permission.INTERNET: Επιτρέπει στις εφαρμογές να χρησιμοποιήσουν network sockets.
  Protection level: Normal

- android.permission.READ_EXTERNAL_STORAGE: Επιτρέπει στις εφαρμογές να διαβάζουν την εξωτερική μνήμη.

Protection Level: Dangerous

- android.permission.WRITE_EXTERNAL_STORAGE: Εεπιτρέπει στις εφαρμογές να γράψουν στην εξωτερική μνήμη. Όταν παραχωρηθεί αυτή η άδεια επιτρέπει έμμεσα και την Read_External_Storage.
  Protection Level: Dangerous

- android.permission.WAKE_LOCK: Αποτρέπει την συσκευή από το να σβήσει την οθόνη ή να μπει σε sleep mode.
  Protection Level: Normal

- android.permission.ACCESS_COARSE_LOCATION: Επιτρέπει στην εφαρμογή να έχει πρόσβαση στην κατά προσέγγιση τοποθεσία.
  Protection Level: Dangerous

- android.permission.ACCESS_FINE_LOCATION: Επιτρέπει στην εφαρμογή να έχει πρόσβαση σε ακριβή τοποθεσία.
  Protection Level: Dangerous

- android.permission.ACCESS_NETWORK_STATE: Επιτρέπει στην εφαρμογή να παίρνει πληροφορίες για τα δίκτυα.
  Protection Level: Normal

- android.permission.ACCESS_WIFI_STATE: Επιτρέπει στην εφαρμογή να παίρνει πληροφορίες για τα δίκτυα Wi-Fi.
  Protection Level: Normal

- android.permission.RECEIVE_SMS: Επιτρέπει στην εφαρμογή να λαμβάνει μηνύματα SMS.
  Protection Level: Dangerous.

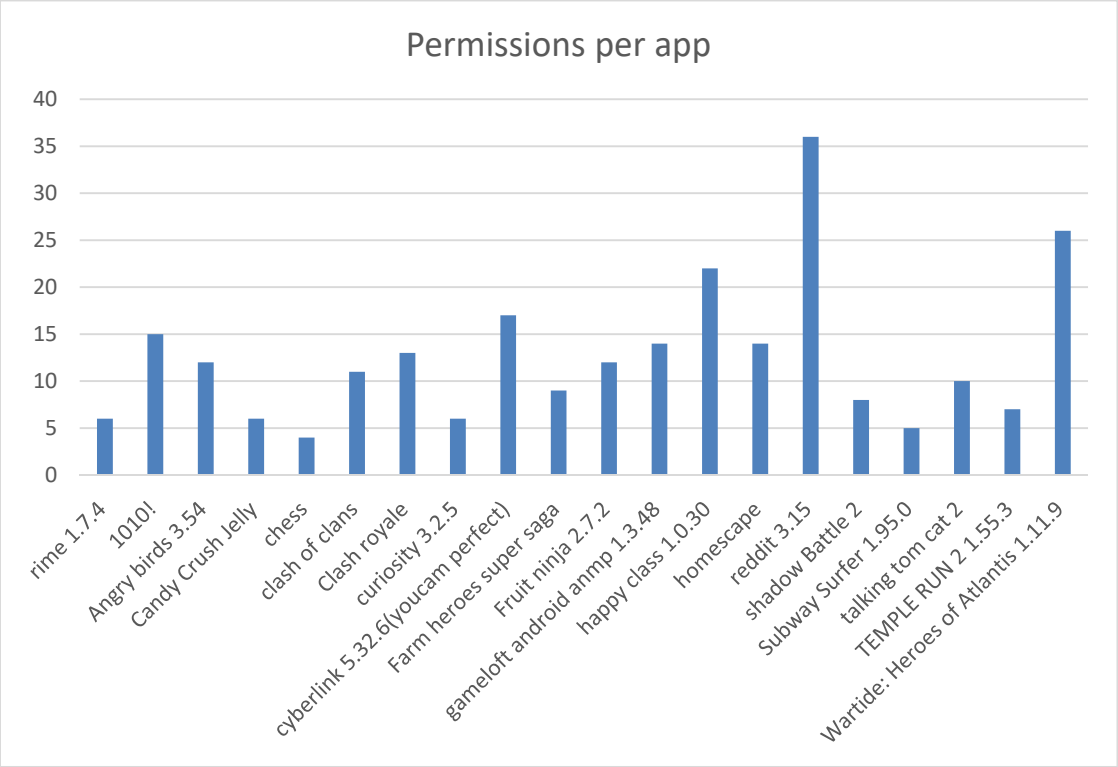
- android.permission.READ_SMS: Επιτρέπει στην εφαρμογή να στέλνει μηνύματα SMS.
  Protection Level: Dangerous.

- android.permission.CAMERA: Επιτρέπει στην εφαρμογή να χρησιμοποιήσει την κάμερα. Με αυτή την άδεια δικαιωμάτων έχει η εφαρμογή δικαίωμα να χρησιμοποιήσει όλα τα χαρακτηριστικά της κάμερα.
  Protection Level: Dangerous.

- android.permission.READ_PHONE_STATE: Επιτρέπει στην εφαρμογή να έχει πρόσβαση για ανάγνωση σε διάφορα δεδομένα που σχετίζονται με το τηλέφωνο, όπως αριθμός τηλεφώνου, χρόνος κλήσεων και στοιχεία δικτύου τηλεπικοινωνίων.
  Protection Level: Dangerous.

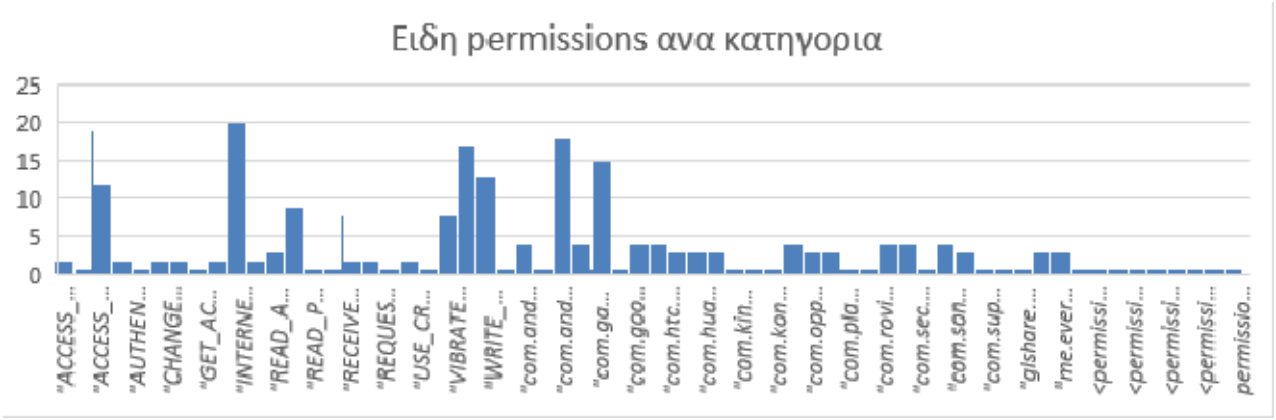
Οι εφαρμογές που θα αναλυθούν αφορούν κυρίως παιχνίδια multiplayer αλλά και single player,για να υπάρξει σύγκριση στις άδειες χρήσης που ζητούνται, προγράμματα κάμερας και επεξεργασίας φωτογραφίας αλλά και σε πρόγραμμα κοινωνικού δικτύου.

Αφού έχουν αναλυθεί οι εφαρμογές μας παρατηρήθηκε ο αριθμός δικαιωμάτων που ζητά η κάθε εφαρμογή όπως φαίνεται στο γράφημα πιο κάτω. Διαπιστώθηκε ότι όλες οι εφαρμογές ανεξαρτήτως μεγέθους ή είδους, παιχνίδι ή εφαρμογή χρειάζονται κάποια άδεια δικαιωμάτων.



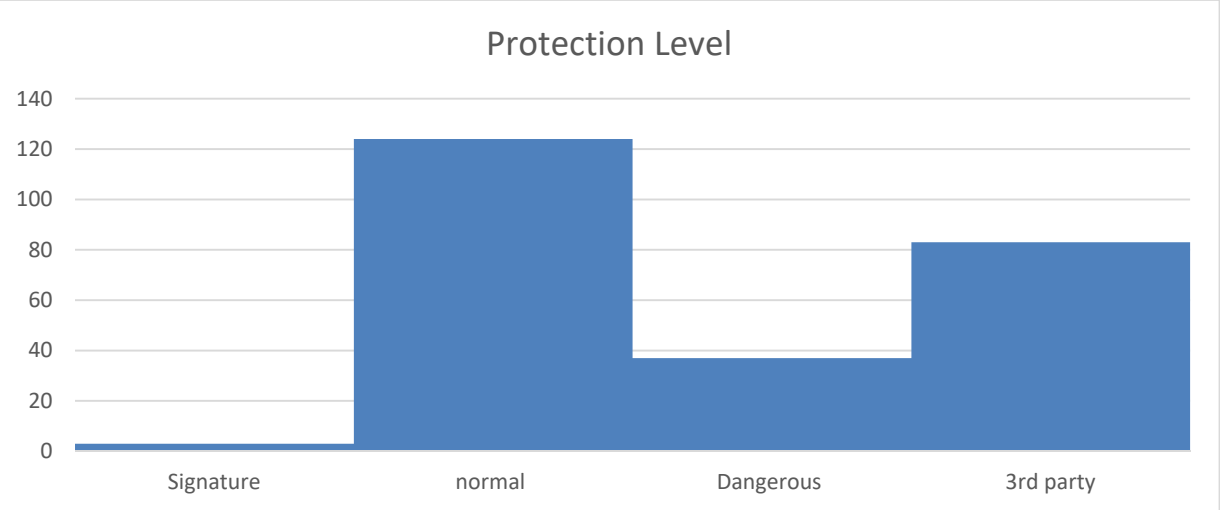
Γράφημα 4.2.1: Permissions per app

Οι 247 άδειες δικαιωμάτων που απαιτούνται συνολικά από όλες τις εφαρμογές χωρίζονται σε 68 κατηγορίες. Από το Γράφημα 2 παρατηρούμε ότι 20 αφορούν την άδεια Internet, δηλαδή την απαιτούν και οι 20 εφαρμογές μας, ενώ 19 απαιτούν την "Access_Network_State".



Γράφημα 4.2.2: Είδη permissions ανά κατηγορία

Στο πιο κάτω γράφημα παρατηρούμε τις άδειες δικαιωμάτων χωρισμένες ανά επίπεδο προστασίας. 124 άδειες εμπίπτουν στο επίπεδο προστασίας κανονικό ενώ στο επικίνδυνο μόνο 37. 83 άδειες δικαιωμάτων δεν αφορούν άδεια για χρήση κάποιων δεδομένων ή υλικών στη συσκευή μας αλλά για συνεργασία μεταξύ εφαρμογών όπως την αλλαγή κάποιου εικονιδίου σε εφαρμογές τρίτων.



Γράφημα 4.2.3: Protection Level

Οι 37 επικίνδυνες άδειες χρήσης χωρίζονται σε δώδεκα υποκατηγορίες σύμφωνα και τον πίνακα 2. Οι περισσότερες αφορούν την χρήση εγγραφής και ανάγνωσης εξωτερικής μνήμης ενώ τρεις από αυτές, οι άδειες χρήσης AUTHENTICATE_ACCOUNT, USE_CREDENTIALS,GET_ACCOUNTS από το Android 6 δεν χρησιμοποιούνται πλέον και μια, η άδεια χρήσης GET_TASKS έχει καταργηθεί από το Android 5.

Α/Α	Όνομα Άδειας Χρήσης	Εφαρμογές που τις χρησιμοποιούσαν
1	"android.permission.AUTHENTICATE_ACCOUNTS"/>	2
2	"android.permission.GET_TASKS"/>	2
3	"android.permission.MANAGE_ACCOUNTS"/>	2
4	"android.permission.USE_CREDENTIALS"/>	2
5	"android.permission.WRITE_EXTERNAL_STORAGE"/>	12
6	"android.permission.READ_EXTERNAL_STORAGE"/>	9
7	"android.permission.ACCESS_COARSE_LOCATION"/>	2
8	"android.permission.RECORD_AUDIO"/>	2
9	"android.permission.ACCESS_FINE_LOCATION"/>	1
10	"android.permission.CAMERA"/>	1
11	"android.permission.GET_ACCOUNTS"/>	1
12	"android.permission.READ_PHONE_STATE"/>	1

Πίνακας 4.2.1 Αναλυτικός Πίνακας Επικίνδυνων Αδειών Χρήσης

4.3 Ανάλυση Εφαρμογών μετά την αφαίρεση Permissions

1. Cyberlink (youcam perfect): Εφαρμογή για λήψη και επεξεργασία φωτογραφιών. Για πρώτο permission αφαιρέθηκε το android.permission.RECORD_AUDIO. Αυτό είχε ως αποτέλεσμα στην εγγραφή video να ζητάει η εφαρμογή ενεργοποίηση του AUDIO permission και να μην μπορεί να προχωρήσει. Στην συνέχεια αφαιρέσαμε το android.permission.RECEIVE_BOOT_COMPLETED όπου δεν παρατηρήθηκε κάποια διαφορά. Για τρίτη άδεια καταργήσαμε το android.permission.INTERNET και παρόλο που θεωρείται κανονική άδεια χρήσης και δεν χρειάζεται να εγκριθεί από τον χρήστη το market της εφαρμογής δεν μπορούσε να ενωθεί στο δίκτυο. Η επόμενη άδεια δικαιωμάτων που διαγράψαμε ήταν η

android.permission.READ_EXTERNAL_STORAGE. Παρατηρήσαμε όμως ότι η εφαρμογή ακόμη είχε πρόσβαση στα αρχεία μας. Σύμφωνα με το Android developer [22] όποια εφαρμογή δηλώσει permission το WRITE_EXTERNAL_STORAGE αποκτά αυτόματα και την ανάγνωση μνήμης. Έτσι αφαιρέθηκε και η άδεια WRITE_EXTERNAL_STORAGE και η εφαρμογή δεν είχε πλέον πρόσβαση. Οι επόμενες άδειες που αφαιρέθηκαν αφορούσαν το location και ήταν η android.permission.ACCESS.COARSE.LOCATION και ACCESS.FINE.LOCATION. Η εφαρμογή παρουσίαζε μήνυμα για ενεργοποίηση του Location και δεν μπορούσε να το χρησιμοποιήσει. Η εφαρμογή δεν σταμάτησε ποτέ να λειτουργεί ή να εμφανίσει κάποιο σφάλμα αλλά οπότε απενεργοποιούσαμε ένα permission η εφαρμογή έχανε και την συγκεκριμένη δυνατότητα.

2. Η δεύτερη εφαρμογή ήταν το Curiosity μια εφαρμογή η οποία προσφέρει άρθρα και ενημερωτικό υλικό ανάλογα με τα θέματα της επιλογής μας μέσω διαδικτύου. Παρόλο που οι άδειες που απαιτούσε ήταν όλες κανονικού επιπέδου, αφαιρέθηκε η άδεια VIBRATE. Κατά την δοκιμαστική λειτουργία πριν την αφαίρεση δεν φάνηκε να χρειάζεται αφού σε καμία στιγμή δεν χρησιμοποιήθηκε η δόνηση ενώ με την αφαίρεση της δεν υπήρξε κάποιο θέμα στην λειτουργία της. Για δεύτερο permission αφαιρέθηκε η άδεια ACCESS_NETWORK_STATE. Μια επίσης κανονικού επιπέδου άδεια χρήσης αλλά σημαντική αφού η εφαρμογή μας δουλεύει μέσω δικτύου. Στην συγκεκριμένη περίπτωση η εφαρμογή παρουσίασε σφάλμα και σε αναγκαστική διακοπή.
3. Για τρίτη εφαρμογή επιλέξαμε το Dungeon Hunters ένα multiplayer παιχνίδι. Αρχικά αφαιρέθηκε η επικίνδυνη άδεια χρήσης όπως το READ_EXTERNAL_STORAGE. Κατά την δοκιμή δεν υπήρξε κάποια διαφορά στην λειτουργία του. Έτσι αφαιρέθηκε και το δεύτερο επικίνδυνο permission το WRITE_EXTERNAL_STORAGE. Εκεί παρατηρήθηκε πως το παιχνίδι κατέβαζε ένα update αλλά στη έκδοση με τα αναιρεμένα permissions δεν μπορούσε να προχωρήσει στο κυρίως μενού ζητώντας να εγκατασταθεί το update. Στην συνέχεια αφαιρέθηκε και η κανονική άδεια χρήσης WAKE_LOCK για να συγκρίνουμε συμπεριφορές μεταξύ επικίνδυνης και κανονικής άδειας χρήσης. Σε αυτή την περίπτωση το παιχνίδι δεν ξεκινούσε καν και το λειτουργικό μας εμφάνιζε σφάλμα αναγκαστικής διακοπής.

4. Στη συνέχεια προχωρήσαμε με το παιχνίδι subway surfer. Ένα ακόμη παιχνίδι το οποίο είχε μόνο άδειες χρήσης κανονικού επιπέδου. Για αρχή διαγράφηκε η άδεια χρήσης WAKE_LOCK για να δούμε αν υπάρχουν τα ίδια αποτελέσματα όπως στην προηγουμένη εφαρμογή. Στο συγκεκριμένο παιχνίδι δεν υπήρξε κάποια αλλαγή ούτε στην λειτουργία αλλά ούτε και στο χρόνο για το σβήσιμο της οθόνης σε σχέση με την μη τροποποιημένη έκδοση. Η επόμενη άδεια χρήσης ήταν η GET_TASK όπου επίσης δεν υπήρξε κάποιο σφάλμα ή αλλαγή στην λειτουργία της εφαρμογής. Το επόμενο στάδιο ήταν η αφαίρεση της άδειας χρήσης INTERNET δηλαδή του διαδικτύου. Παρόλο που η εφαρμογή δεν χρειάζεται Internet για την βασική της λειτουργία παρα μόνο για το ηλεκτρονικό της κατάστημα, εντούτοις μετά την εμφάνιση του λογότυπου η εφαρμογή έκλεινε εμφανίζοντας πάλι το μήνυμα για αναγκαστική διακοπή.

5. Η επόμενη εφαρμογή ήταν Candy Crush jelly. Στην κανονική λειτουργία της παρατηρήθηκε ότι η οθόνη παρέμεινε ανοικτή όσο η εφαρμογή ήταν σε λειτουργία. Έτσι επιλέχθηκε η άδεια χρήσης WAKE_LOCK για να διαγραφεί. Ωστόσο δεν υπήρξε κάποια αλλαγή με την οθόνη να μένει μόνιμα ανοικτή. Ακολούθως διαγράφηκε η άδεια χρήσης ACCESS_WIFI_STATE η οποία χρειάζεται για να αντλεί πληροφορίες για τα δίκτυα WIFI. Πάλι όλες οι λειτουργίες του παιχνιδιού δούλευαν κανονικά χωρίς να παρουσιαστεί κάποιο πρόβλημα. Για τρίτη άδεια χρήσης αφαιρέθηκε το INTERNET. Η εφαρμογή εξακολουθούσε να δουλεύει αλλά με το τέλος του παιχνιδιού ενώ στην κανονική έκδοση μας εμφάνιζε πίνακα με την βαθμολογία των παικτών και την κατάταξη μας σε αυτή την περίπτωση απλά προχωρούσε στο επόμενο επίπεδο. Επίσης το εικονίδιο που φορτώνει το πίνακα Leaderboards με τις βαθμολογίες δεν δούλευε ενώ το εικονίδιο που φορτώνει πληροφορίες για την εφαρμογή μέσω διαδικτύου εμφάνιζε μήνυμα ότι δεν μπορεί να συνδεθεί στο internet και να ελέγξουμε την σύνδεση μας. Τελευταία άδεια χρήσης ήταν η ACCESS_NETWORK_STATE. Ένα ακόμη permission κανονικού επιπέδου το οποίο δεν απαιτεί έγκριση από τον χρήστη. Με την αφαίρεση του η εφαρμογή παρουσίασε σφάλμα και αναγκαστική διακοπή.

6. Στην έκτη εφαρμογή Wartide: Heroes of Atlantic υπήρχαν πολλά permissions τα οποία αφορούσαν κυρίως άδειες χρήσης για τρίτα προγράμματα όπως permissions για εμφάνιση εικονιδίων σε launchers. Μελετήθηκαν μόνο οι άδειες χρήσεις που

είχαν να κάνουν με το λειτουργικό Android. Αφαιρέθηκαν με την σειρά η άδεια χρήσης WAKE_LOCK και η άδεια χρήσης permission.C2D_message, άδεια που χρησιμοποιείτε για εμφάνιση μηνυμάτων στην μορφή ειδοποιήσεων. Δεν εμφανίστηκε καμία διαφορά κατά την δοκιμή και το παιχνίδι δεν φάνηκε να επηρεάζεται από την διαγραφή των αδειών. Ο χρόνος σβησίματος της οθόνης παρέμεινε ο ίδιος και πριν και μετά την αφαίρεση του WAKE_LOCK ο οποίος ήταν ο ίδιος με του συστήματος. Στην συνέχεια διαγράφηκε η επόμενη άδεια χρήσης που είχε σχέση με το λειτουργικό, το permission INTERNET. Η εφαρμογή ξεκινούσε κανονικά και μετά την εμφάνιση του λογότυπου η εφαρμογή εμφάνιζε σφάλμα "Download Error" στην διαδικασία μεταφόρτωσης δεδομένων από το διαδίκτυο.

7. Στο παιχνίδι Angry Birds, την έβδομη εφαρμογή που επιλέχθηκε για έλεγχο αφαιρέθηκαν ταυτόχρονα τα δυο επικίνδυνα permissions που υπήρχαν, το WRITE_EXTERNAL_STORAGE και READ_EXTERNAL_STORAGE. Παρόλο που υπήρχαν στο ANDROIDMANIFEST.xml ούτε στην αρχική μορφή ζητήθηκαν για έγκριση ούτε εμφάνισε κάποιο μήνυμα και δεν επηρέασαν την λειτουργία του παιχνιδιού μετά την αφαίρεση τους. Ούτε η επόμενη άδεια χρήσης READ_PHONE_STATE ζητήθηκε από τον χρήστη ενώ καμία διεργασία της εφαρμογής δεν χρειαζόταν πρόσβαση στα στοιχεία τηλεφώνου. Η ακύρωση της δεν προκάλεσε σφάλμα ούτε πρόβλημα στην λειτουργία του παιχνιδιού. Στην συνέχεια αφαιρέθηκαν με την σειρά το CHECK_LICENCE και το vending_BILLING που αφορούν για επικύρωση της εφαρμογής και για αγορές μέσω Google Play την χρήση πιστωτικής κάρτας. Δεν παρατηρήθηκε κάποιο σφάλμα και η αγορά προχώρησε κανονικά μέσα από το μενού του παιχνιδιού χωρίς να επηρεαστεί καθόλου από την άδεια χρήσης. Τελευταία άδεια χρήσης ήταν το INTERNET. Διαγράφηκε η άδεια χρήσης και η εφαρμογή ξεκίνησε κανονικά αλλά στην συνέχεια μετά από λίγα δευτερόλεπτα χρήσης η εφαρμογή κολλούσε, πράγμα που δεν συνέβαινε στην κανονική έκδοση.

8. Στην όγδοη εφαρμογή, το Shadow Battle 2 παρατηρήθηκε το ίδιο μοτίβο. Αφαιρέθηκε καταρχήν το permission vending.BILLING. Το παιχνίδι συνέχιζε να έχει πρόσβαση στο Google Play για αγορές μέσω διαδικτύου. Ακολούθησε η διαγραφή της άδειας χρήσης WAKE.LOCK. Και σε αυτή την περίπτωση και πριν και μετά η οθόνη έσβηνε στο όριο χρόνου που είχε ρυθμιστεί από το λειτουργικό άρα δεν

φάνηκε να επηρεάζει κάπως την εφαρμογή. Για τέλος αφήσαμε την άδεια INTERNET. Ήταν η μόνη άδεια χρήσης που παρατηρήθηκε αλλαγή στην σωστή λειτουργία όταν πραγματοποιήθηκε αναγκαστική διακοπή της εφαρμογής αμέσως μετά την εκκίνηση.

9. Ένατη εφαρμογή ήταν το clash of titans, ένα multiplayer παιχνίδι όπου έγινε για αρχή η αφαίρεση permissions όπως supercell.clashofclans.permission.C2D_MESSAGE και vending.BILLING. Καμία από τις δυο δεν είχε κάποια επίδραση στην σωστή λειτουργία αφού ακόμη και το store λειτουργούσε κανονικά. Μετά ακολούθησε η READ_EXTERNAL_MEMORY και στην συνέχεια η WRITE_EXTERNAL_MEMORY. Ενώ και οι δυο είναι επικίνδυνου επιπέδου άδειες χρήσης ποτέ δεν ζητήθηκαν για έγκριση στην επίσημη έκδοση, ούτε η αφαίρεση τους επηρέασε με κάποιο τρόπο την σωστή λειτουργία. Μια ακόμη άδεια χρήσης που διαγράφηκε ήταν το ACCESS_WIFI_STATE. Η δοκιμή και στην επίσημη έκδοση και στην τροποποιημένη έγινε με ανοικτό το WIFI στην πρώτη εκκίνηση της εφαρμογής και στην δεύτερη με κλειστό το WIFI. Και στις δυο περιπτώσεις με κλειστό το WIFI η εφαρμογή εμφάνιζε μήνυμα για ενεργοποίηση του. Το παιχνίδι σταμάτησε να λειτουργεί μόνο με την αφαίρεση του permission INTERNET. Όπως και στις άλλες περιπτώσεις μετά την εμφάνιση του λογότυπου η εφαρμογή έκλεινε χωρίς ειδοποίηση.

10. Στο Clash royal, ακόμη ένα multiplayer παιχνίδι της ιδίας εταιρίας με το πιο πάνω, υπήρχαν ακριβώς τα ίδια permissions. Επαναλάβαμε τα ίδια βήματα για να δούμε αν υπάρχει κάποια διαφορά στα αποτελέσματα. Αφαιρέθηκαν δηλαδή τα permissions για την ανάγνωση και εγγραφή της μνήμης χωρίς να υπάρξει κάποια διαφορά στην λειτουργία της. Το ίδιο συνέβη και με την αφαίρεση της άδειας χρήσης του ACCESS_WIFI_STATE που είτε υπήρχε είτε όχι το permission δεν υπήρξε κάποια διαφορά στην εφαρμογή. Με την διαγραφή του INTERNET υπήρξε το ίδιο πρόβλημα με την αναγκαστική διακοπή όπως και με τις προηγούμενες εφαρμογές.

11. Στο reddit, μια εφαρμογή συνδρομής σε διάφορα forum για συζήτηση απαιτείτε εγγραφή μέσω ηλεκτρονικού ταχυδρομείου. Με την δημιουργία λογαριασμού το όνομα του λογαριασμού εμφανιζόταν στους λογαριασμούς που υπήρχαν στις ρυθμίσεις της συσκευής. Αφαιρέθηκαν τα όλα τα δικαιώματα χρήσης που είχαν σχέση με πρόσβαση στα account της συσκευής δηλαδή οι άδειες χρήσης AUTHENTICATE_ACCOUNT, USE_CREDENTIALS, και GET_ACCOUNTS. Παρατηρήθηκε ότι η

εφαρμογή συνέχιζε να έχει πρόσβαση στους λογαριασμούς του τηλεφώνου για να αποθηκεύει τα στοιχεία του χρήστη. Σύμφωνα με το Android Developers από την έκδοση Android 6 και μετά δεν χρειάζονται οι πιο πάνω άδειες και αρκεί μόνο η υπογραφή πιστοποιητικού για πρόσβαση στους λογαριασμούς της εκάστοτε εφαρμογής. Ακολουθήσε η αφαίρεση των αδειών χρήσης ανάγνωσης και εγγραφής στη μνήμη και η αφαίρεση του INTERNET όπου η εφαρμογή δεν είχε πρόσβαση στα αρχεία μας ούτε στο διαδίκτυο.

12. Το Happy glass είναι ένα παιχνίδι puzzle το οποίο δεν είχε ιδιαίτερα permissions. Πριν την τροποποίηση του δοκιμάστηκε η λειτουργία με μόνες επιλογές την εκκίνηση νέου παιχνιδιού και την αγορά διαφόρων προϊόντων μέσω Google Play. Το ηλεκτρονικό κατάστημα δούλευε κανονικά αφού μας εμφάνιζε το ποσό αλλά και την πιστωτική κάρτα που είχαμε καταχωρημένη στο κατάστημα της Google. Αφού αφαιρέθηκε η άδεια χρήσης vending.Billing προσπαθήσαμε να ξαναπροχωρήσουμε στην αγορά κάποιου προϊόντος. Ούτε αυτήν την φορά όμως εμφανίστηκε σφάλμα στο ενσωματωμένο ηλεκτρονικό του κατάστημα και εξακολουθούσε να εμφανίζει τα στοιχεία της πιστωτικής κάρτας. Επίσης στην αρχική της μορφή η εφαρμογή ενημέρωνε τον χρήστη ότι θα αποστέλλει δεδομένα στην εταιρία για βελτιστοποίηση του παιχνιδιού και οι επιλογές που είχε ήταν να το εγκρίνει ή να το απορρίψει. Η επόμενη άδεια χρήσης για αφαίρεση ήταν το INTERNET έτσι ώστε να διαπιστώσουμε κατά πόσο μπορεί να προκαλέσει σφάλμα και παρόλο που το χρειάζεται για αποστολή δεδομένων του παιχνιδιού δεν παρουσιάστηκε κάποιο σφάλμα. Παρατηρήθηκε όμως ότι σταμάτησε η προβολή διαφημίσεων που παρουσιάζονταν ανάμεσα στα επίπεδα, όπως επίσης και ορισμένα mini-games που απαιτούσαν την προβολή διαφημίσεων για να κερδίσεις ορισμένα δώρα του παιχνιδιού είχαν απενεργοποιηθεί. Τέλος αφαιρέθηκαν τις άδειες WAKE_LOCK και VIBRATE όπου ούτε και αυτές είχαν κάποια εμφανή διαφορά στην εφαρμογή. Η οθόνη συνέχισε να σβήνει στο χρόνο που είχε οριστεί από το λειτουργικό ενώ η δόνηση συνέχισε να δουλεύει.

13. Ακόμη ένα παιχνίδι, το Fruit Ninja, είχε δηλωμένες άδειες χρήσης στο AndroidManifest.xml για ανάγνωση και εγγραφή της μνήμης. Στην κανονική λειτουργία της εφαρμογής δεν ζητήθηκαν από το χρήστη να τις εγκρίνει. Ήταν όμως άδειες επικίνδυνου επιπέδου έτσι ήταν οι πρώτες που διαγράφηκαν. Όπως ήταν

αναμενόμενο δεν παρουσιάστηκε κάποια δυσλειτουργία ούτε κάποιο μήνυμα που να μας ενημερώνει ότι δεν έχουν εγκριθεί και ότι χρειάζονται αυτές οι άδειες. Ακολούθησε η άδεια vending.Billing που αφορούσε το ηλεκτρονικό κατάστημα. Ούτε σε αυτή την περίπτωση υπήρξε κάποιο θέμα αφού λειτουργούσε κανονικά και μας εμφάνιζε όλα τα στοιχεία μας για να προχωρήσει η αγορά. Ούτε υπήρξε κάποια διαφορά στην λειτουργία της συσκευής. Ακολούθησαν οι άδειες διαδικτύου. Η πρώτη που αφαιρέθηκε ήταν το ACCESS_WIFI_STATE. Πάλι δεν υπήρξε κάποια αλλαγή αφού όταν επιλέγαμε κάτι από το μενού το οποίο είχε σχέση με το διαδίκτυο, είτε με το permission είτε όχι μας εμφάνιζε μήνυμα ότι να ελέγξουμε την σύνδεση μας. Αντιθέτως η μόνη άδεια που προκάλεσε την εφαρμογή να διακοπεί ήταν η αφαίρεση του INTERNET που ήταν η επόμενη άδεια που αφαιρέθηκε. Παρόλο που το παιχνίδι χρειάζεται το INTERNET για αγορές και δεν επηρεάζει το κυρίως μέρος του παιχνιδιού με την αφαίρεση του οδηγήθηκε σε αναγκαστική διακοπή.

14. Η επόμενη εφαρμογή που ερευνήθηκε ήταν το Temple Run 2 από το οποίο αφαιρέθηκε πρώτα η άδεια χρήσης vending.Billing για το ηλεκτρονικό κατάστημα. Το κατάστημα συνέχισε να λειτουργεί κανονικά όπως και στην κανονική έκδοση της εφαρμογής. Στην συνέχεια αφαιρέθηκε το permission ACCESS_NETWORK_STATE για να φανεί αν υπάρχει διαφορά στην λειτουργία της εφαρμογής. Δεν φάνηκε να επηρεάζει κάπως έτσι αφαιρέθηκε και η άδεια χρήσης ACCESS_WIFI_STATE. Η εφαρμογή εξακολουθούσε να δουλεύει κανονικά με όλα τα μενού και το κυρίως παιχνίδι να είναι λειτουργικό όπως και στην αρχική έκδοση. Ακολουθήσε η διαγραφή του διαδικτύου με το permission του INTERNET. Στην αρχική έκδοση όταν ξεκινούσε το παιχνίδι μας έκανε αυτόματα σύνδεση στο λογαριασμό μας στο Google Play όπου κρατούσε δεδομένα σχετικά με το παιχνίδι όπως σκορ, κατάταξη και σε τι επίπεδο του παιχνιδιού βρισκόμασταν. Με την αφαίρεση του INTERNET δεν φόρτωνε το λογαριασμό μας αλλά το παιχνίδι δούλευε κανονικά με μόνο πρόβλημα ότι δεν μπορούσε να φορτώσει το ηλεκτρονικό κατάστημα παρουσιάζοντας σφάλμα σύνδεσης.

15. Στην συνέχεια για την εφαρμογή RIME, ένα παιχνίδι τύπου escape room, αφαιρέθηκε αρχικά η άδεια για CHECK_LICENSE και η άδεια vending.Billing. Στην αρχική έκδοση υπήρχε η επιλογή για Donation με σύνδεση στο Google Play όπως και με τις προηγούμενες εφαρμογές. Η εφαρμογή συνέχισε να ενώνεται με το Google Play και

να ζητάει κωδικό για να προχωρήσει η αγορά ακριβώς όπως την αρχική έκδοση. Μέσα στο AndroidManifest.xml υπήρχε και η άδεια για WRITE_EXTERNAL_STORAGE η οποία ουδέποτε ζητήθηκε. Συνεχίσαμε με την αφαίρεση της για να διαπιστώσουμε κατά ποσό είναι αναγκαία στο παιχνίδι και αν πράγματι χρειάζεται. Δεν παρατηρήθηκε κάποιο σφάλμα στην εφαρμογή αφού όλα δούλευαν όπως στην κανονική έκδοση. Η επόμενη άδεια που αφαιρέθηκε ήταν πάλι το INTERNET. Το παιχνίδι ήταν single player με μόνη χρήση του διαδικτύου για προβολή διαφημίσεων και σύνδεση με το Google Play για τις δωρεές. Στο παιχνίδι υπήρχε η επιλογή για βοήθεια δίνοντας σου πληροφορίες για το επόμενο στάδιο αλλά πατώντας το ήταν αναγκαστική η προβολή διαφημίσεων για τριάντα δευτερόλεπτα. Με την αφαίρεση του INTERNET υπήρχε ο χρόνος των 30 δευτερολέπτων αλλά αντί για διαφήμιση υπήρχε μια μαύρη οθόνη. Επίσης στην επιλογή Donate εμφανιζόντανε το μήνυμα ότι δεν υπάρχει σύνδεση.

16. Το παιχνίδι με τις λιγότερες άδειες χρήσης ήταν το παιχνίδι Chess, ένα παιχνίδι σκακιού. Με μόλις τέσσερις άδειες χρήσης εκ των οποίων οι 2 αφορούσαν το διαδίκτυο, μια το WAKE_LOCK και μια για vending.Billing. Στο παιχνίδι υπήρχε η επιλογή αγοράς του για απομάκρυνση των διαφημίσεων, έτσι αφαιρέθηκε πρώτα το Vending.Billing αλλά δεν παρουσιάστηκε κάποιο θέμα και η αγορά προχωρούσε κανονικά. Στην συνέχεια αφαιρέθηκε και το WAKE_LOCK όπου ο χρόνος σβησίματος της οθόνης ήταν ο ίδιος και στις δυο περιπτώσεις, δηλαδή ο ίδιος με το χρόνο λειτουργικού. Προχωρήσαμε με την αφαίρεση του ACCESS_NETWORK_STATE όπου δοκιμάστηκε και με το WIFI ανοικτό και κλειστό. Τελευταίο έμεινε το permission του INTERNET που όπως και στην προηγούμενη εφαρμογή αντί για διαφημίσεις παρουσιάζει μια μαύρη οθόνη.

17. Η εφαρμογή Talking Tom Cat 2, ένα ψηφιακό κατοικίδιο, καταγράφει ήχο και αποθηκεύει βίντεο. Στην αρχική έκδοση το παιχνίδι ζητούσε έγκριση για καταγραφή ήχου και όταν προχωρούσαμε στην καταγραφή στιγμιότυπου ζητούσε έγκριση για ανάγνωση και εγγραφή στο μνήμη. Έτσι προτιμήθηκαν να αφαιρεθούν οι άδειες χρήσης καταγραφής ήχου, αποθήκευσης δεδομένων και διαδικτύου. Αρχικά αφαιρέθηκε η άδεια χρήσης επικίνδυνου επιπέδου RECORD_AUDIO. Η εφαρμογή μας ενημέρωνε ότι δεν είχε πρόσβαση στο μικρόφωνο και ζητούσε να το ενεργοποιήσουμε μέσα από τα Permissions του συστήματος. Αφού επιβεβαιώσαμε

ότι δεν μπορούσε να συνεχίσει με την καταγραφή ήχου, χωρίς όμως να παρουσιαστεί σφάλμα, συνεχίσαμε με την αφαίρεση του WRITE_EXTERNAL_MEMORY. Ούτε σε αυτή την περίπτωση εμφάνισε σφάλμα αλλά στην επιλογή αποθήκευση του βίντεο, η επιλογή ήταν απενεργοποιημένη χωρίς να ανταποκρίνεται σε οποιαδήποτε παρέμβαση του χρήστη. Τελευταία άδεια χρήσης για διαγραφή ήταν το INTERNET. Όπως και πολλές άλλες εφαρμογές το διαδίκτυο δεν είναι κύριο μέρος της λειτουργίας της. Περισσότερο αφορά αγορές μέσω Play Store και προβολή διαφημίσεων. Στο κυρίως μενού μετά την διαγραφή της άδειας, πολλά εικονίδια όπως το εικονίδιο των αγορών ή του διαμοιρασμού μέσω κοινωνικών δικτύων απουσίαζαν ενώ η εφαρμογή φαινόταν να δουλεύει κανονικά. Παρόλα αυτά μέσα σε λίγα λεπτά λειτουργίας κολλούσε με αποτέλεσμα να χρειάζεται ο χρήστης να την κλείσει.

18. Από το παιχνίδι 1010! αφαιρέθηκαν οι άδειες χρήσης για δόνηση, για πρόσβαση στο WIFI_STATE και INTERNET. Στην αφαίρεση του VIBRATE η εφαρμογή σταμάτησε να χρησιμοποιεί την δόνηση κάτι αναμενόμενο αλλά όχι αναγκαστικό όπως είχαμε δει και σε άλλες εφαρμογές. Με το permission ACCESS_WIFI_STATE δεν παρατηρήθηκε κάποια αλλαγή στην λειτουργία ενώ με την αφαίρεση του INTERNET σταμάτησαν να εμφανίζονταν οι διαφημίσεις.

19. Το παιχνίδι Homescape από πριν να αφαιρεθούν ακόμη τα permissions στην εκκίνηση μας ενημέρωνε ότι δεν είχε κατέβει από το επίσημο Play Store και πως για να προχωρήσουμε έπρεπε να γίνει εγκατάσταση από εκεί. Ήταν η πρώτη και μοναδική εφαρμογή που συναντήσαμε και είχε το συγκεκριμένο θέμα. Λόγω της ιδιαιτερότητας της αφαιρέθηκαν permissions όπως CHECK_LICENSE, SHARED_CONTENT.GOOGLE και REQUEST-INSTALL_PACKAGE σε μια προσπάθεια να παρακάμψουμε την επικύρωση της μέσω Play Store. Η εφαρμογή συνέχιζε να βγάζει το ίδιο σφάλμα ακόμη και όταν αφαιρέθηκαν όλα τα συγκεκριμένα permissions.

20. Για τελευταία εφαρμογή επιλέχθηκε το Farm Heroes Super Saga. Ένα ακόμη με παιχνίδι με την χρήση INTERNET να αποσκοπεί κυρίως στην αγορά επιπρόσθετου υλικού που θα βοηθήσει στην πρόοδο του παιχνιδιού. Στην συγκεκριμένη διαγράψαμε τις άδειες χρήσης WAKE_LOCK, permissions_C2D_MESSAGE όπου και

δεν παρατηρήθηκε καμία διαφορά. Το ίδιο και στην άδεια χρήσης ACCESS_WIFI_STATE. Με την αφαίρεση της άδειας του INTERNET η εφαρμογή παρουσίασε αναγκαστική διακοπή.

4.4 Αποτελέσματα

Από τις είκοσι εφαρμογές που έχουν ελεγχθεί οι εννέα έχουν παρουσιάσει αναγκαστική διακοπή της λειτουργίας τους από την εκκίνηση τους ενώ άλλες τρεις παρουσίασαν άλλα προβλήματα. Επτά εφαρμογές παρόλο που συνέχιζαν να λειτουργούν είχαν περιορισμένες δυνατότητες λόγω των αδειών χρήσης που αφαιρέθηκαν και μια δεν κατάφερε να ξεκινήσει αναγνωρίζοντας ότι δεν έγινε εγκατάσταση από το επίσημο Play Store.

Α/Α	Όνομα Εφαρμογής	Σφάλμα	Άδεια χρήσης που το προκάλεσε
1	Curiosity	Αναγκαστική διακοπή	ACCESS_NETWORK_STATE
2	Dungeon Hunters	Αναγκαστική διακοπή	WAKE_LOCK
3	Subway Surfer	Αναγκαστική διακοπή	INTERNET
4	Candy Crush	Αναγκαστική διακοπή	ACCESS_NETWORK_STATE
5	Shadow Battle 2	Αναγκαστική διακοπή	INTERNET
6	Clash of Titans	Αναγκαστική διακοπή	INTERNET
7	Clash Royal	Αναγκαστική διακοπή	INTERNET
8	Fruit Ninja	Αναγκαστική διακοπή	INTERNET
9	Farms Heroes Saga	Αναγκαστική διακοπή	INTERNET

Πίνακας 4.4.1: Εφαρμογές με Αναγκαστική Διακοπή

Όπως παρουσιάζεται και στον Πίνακα 3 και οι εννέα εφαρμογές που έχουν παρουσιάσει αναγκαστική διακοπή, έγινε αφαιρώντας μια κανονικού επιπέδου άδεια χρήσης. Παρόλο που τις περισσότερες τις επηρέασε η άδεια χρήσης του διαδικτύου εντούτοις παρατηρείτε ότι και άλλες άδειες επηρέασαν όπως η άδεια WAKE_LOCK και η ACCESS_NETWORK_STATE. Οι κανονικές άδειες χρήσης όπως έχει προαναφερθεί δεν χρειάζονται έγκριση από τον χρήστη και δίνονται αυτόματα από το σύστημα. Υπό κανονικές συνθήκες οι χρήστες δεν μπορούν να επέμβουν ούτε να τις ανακαλέσουν έτσι

πιθανόν οι προγραμματιστές να μην χρησιμοποίησαν δικλίδες ασφαλείας ή κάποια μέθοδο ελέγχου και για αυτό να παρουσίασαν αυτό το πρόβλημα.

Α/Α	Όνομα Εφαρμογής	Σφάλμα	Άδεια χρήσης που οδήγησε στο σφάλμα
1	Wartide: Heroes of Atlantic	Download Error	INTERNET
2	Angry Birds	Κολλούσε στο αρχικό μενού	INTERNET
3	Talking Tom Cat 2	Κολλούσε στο αρχικό μενού	INTERNET

Πίνακας 4.4.2: Εφαρμογές με διακοπή λειτουργίας

Οι επόμενες τρεις εφαρμογές ενώ στην αρχή φαινομενικά δούλευαν παρουσίασαν πρόβλημα στην κανονική λειτουργία τους, επίσης με άδειες κανονικής χρήσης. Η εφαρμογή Wartide: Heroes of Atlantic ξεκινούσε κανονικά αλλά στην πορεία εμφάνιζε σφάλμα διαδικτύου και δεν μπορούσε να προχωρήσει αφού χρειαζόταν να κατεβάσει από το διαδίκτυο μια ενημέρωση. Οι άλλες δυο εφαρμογές ενώ ξεκινούσαν και δούλευαν κανονικά κάποια στιγμή κολλούσαν χωρίς να ανταποκρίνονται. Χωρίς την αφαίρεση της συγκεκριμένης άδειας οι εφαρμογές δούλευαν κανονικά χωρίς κάποιο πρόβλημα.

Οι υπόλοιπες οκτώ εφαρμογές δεν παρουσίασαν τέτοιου είδους προβλήματα αλλά υπολειτουργούσαν ανάλογα της περίπτωσης των αδειών που αφαιρέθηκαν. Για παράδειγμα η εφαρμογή Cyberlink με την αφαίρεση των επικίνδυνων αδειών, ηχογράφησης, κάμερας, ανάγνωσης και εγγραφής της μνήμης, δεν μπορούσε να αξιοποιήσει τους συγκεκριμένους πόρους αλλά ποτέ δεν σταμάτησε να λειτουργεί.

Οι εφαρμογές οι οποίες απαιτούσαν άδειες χρήσης επικίνδυνου επιπέδου φαίνονται στο πιο κάτω πίνακα.

PERMISSIONS	ΕΦΑΡΜΟΓΕΣ											
	cyberlink	reddit	Subway Surfer	Dungeon Hunters	Angry birds	clash of clans	Clash royal	Fruit ninja	rime	talking tom cat 2	happy class	homescape
AUTHENTICATE_ACCOUNTS	✓	✓										
GET_TASKS	✓		✓									
MANAGE_ACCOUNTS	✓	✓										
USE_CREDENTIALS	✓	✓										
WRITE_EXTERNAL_STORAGE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
READ_EXTERNAL_STORAGE	✓	✓		✓	✓	✓	✓	✓		✓		✓
ACCESS_COARSE_LOCATION	✓	✓										
RECORD_AUDIO	✓									✓		
ACCESS_FINE_LOCATION	✓											
CAMERA	✓											
GET_ACCOUNTS		✓										
READ_PHONE_STATE								✓				

Πίνακας 4.4.3: Εφαρμογές με επικίνδυνες άδειες χρήσης

Οι δώδεκα από τις είκοσι εφαρμογές απαιτούσαν επικίνδυνες άδειες εγγραφής μνήμης ενώ οι εννέα από αυτές απαιτούσαν και ανάγνωση μνήμης. Η ανάγνωση μνήμης μέχρι την στιγμή που γράφεται αυτή η διπλωματική εργασία εγκρίνεται αυτόματα με την άδεια εγγραφής μνήμης, αν υπάρχει, αφού ανήκουν στην ίδια ομάδα αδειών. Η Google στην επίσημη σελίδα της[30] αναφέρει ότι όλες οι άδειες που χρειάζονται πρέπει να δηλώνονται ανεξαρτήτως αν ανήκουν στην ίδια ομάδα γιατί αυτό μπορεί να μην ισχύει σε μελλοντικές εκδόσεις του λειτουργικού. Αυτός είναι και ο λόγος που η αφαίρεση της ανάγνωσης μνήμης δεν προκάλεσε κανένα πρόβλημα στις εφαρμογές που αφαιρέθηκε.

Αντιθέτως στην αφαίρεση και των δυο αυτών αδειών χρήσης εμφανίστηκε περιορισμός στην λειτουργία τριών εφαρμογών. Στις δυο από αυτές την cyberlink και στο Reddit με την αποκοπή της πρόσβασης δεν μπορούσαν να φορτώσουν φωτογραφίες και άλλο υλικό από την μνήμη του τηλεφώνου ενώ η εφαρμογή Dungeon Hunters δεν μπορούσε να εγκαταστήσει ένα απαιτούμενο update. Οι υπόλοιπες εφαρμογές δεν εμφάνισαν κάποιο μήνυμα για έγκριση από τον χρήστη και με την αφαίρεση τους δεν αντιμετώπισαν κάποιο θέμα. Αυτό οφείλεται στο ότι από την έκδοση Android 4.4 και μετά οι εφαρμογές δεν χρειάζονται έγκριση για πρόσβαση στην μνήμη μέσα στο φάκελο όπου είναι η εφαρμογή.

Η αφαίρεση της άδειας ACCESS_COARSE_LOCATION αφορούσε μόνο δυο εφαρμογές εκ των οποίων μόνο η εφαρμογή Reddit παρουσίασε ένα μήνυμα για ενεργοποίηση του Location μέσα από τις ρυθμίσεις. Στην εφαρμογή cyberlink δεν υπήρξε τέτοιο μήνυμα αφού μας είχε ζητήσει να εγκριθεί το Location μέσω της άδειας ACCESS_FINE_LOCATION που ανήκει στο ίδιο group. Για να απενεργοποιηθεί εντελώς ο εντοπισμός τοποθεσίας από την εφαρμογή cyberlink αφαιρέθηκε και το ACCESS_FINE_LOCATION. Τότε η εφαρμογή ζήτησε να εγκριθεί η πρόσβαση στο Location χωρίς να υπάρχει η επιλογή.

Οι άδειες χρήσης RECORD_AUDIO και CAMERA με την αφαίρεση τους διέκοψαν την πρόσβαση στις εφαρμογές με αποτέλεσμα οι δυο αυτές εφαρμογές να χάσουν μέρος των δυνατοτήτων τους.

Η άδεια χρήσης READ_PHONE_STATE δεν ζητήθηκε από την εφαρμογή Angry Birds και ούτε επηρέασε καθόλου στην χρήση μετά την αφαίρεση.

Οι υπόλοιπες τέσσερις άδειες χρήσης επικίνδυνου επιπέδου είχαν καταργηθεί από προηγούμενες εκδόσεις Android έτσι δεν επηρέασαν καθόλου με την αφαίρεση τους.

Κεφάλαιο 5
Επίλογος

Στην παρούσα μεταπτυχιακή διατριβή ασχοληθήκαμε με τις άδειες χρήσης του λειτουργικού Android. Σκοπός μας ήταν να ελεγχθεί κατά πόσο οι εφαρμογές ζητούν τις αναγκαίες άδειες χρήσης ή αν υπάρχει κατάχρηση στα δικαιώματα που τους παραχωρεί ο χρήστης.

5.1 Συμπεράσματα

Αρχικά έχει περιγράφει το λειτουργικό Android και το επίσημο play store όπως και ο τρόπος εγκατάστασης εφαρμογών από ανεπίσημα ηλεκτρονικά καταστήματα. Στη συνέχεια έγινε μια επεξήγηση των permissions καθώς και η δομή ένα .apk αρχείου. Αναλύθηκαν τα αρχεία που περιλαμβάνονται στο .apk και η σημασία των αρχείων για την πιστοποίηση και την ψηφιακή υπογραφή κάθε αρχείου.

Για να επιτευχθεί ο σκοπός μας έχουμε χρησιμοποιήσει δυο δωρεάν Java προγράμματα, το apktool για το compile-decompile των εφαρμογών, και το uber-apk-signed για την υπογραφή πιστοποιητικών. Αφού εγκαταστάθηκαν οι επίσημες εφαρμογές και παρατηρήθηκαν οι λειτουργίες τους ακολούθως αφαιρέθηκαν από το σύστημα και εγκαταστάθηκαν με μειωμένες άδειες χρήσης για να συγκρίνουμε τις διάφορες.

Περισσότερη προσοχή έχει δοθεί στις επικίνδυνες άδειες χρήσης που μπορούν να έχουν πρόσβαση στα προσωπικά δεδομένα του χρήστη, ειδικά στις άδειες ανάγνωσης και εγγραφής της μνήμης. Παρατηρούμε ότι πολλές εφαρμογές παρόλο που τις περιέχουν στο Android Manifest δεν τις αξιοποιούν αλλά ούτε και τις αιτούνται από τον χρήστη για έγκριση. Στις υπόλοιπες εφαρμογές με την αναίρεση των συγκεκριμένων permissions δεν υπήρχε πρόσβαση στα αρχεία της συσκευής.

Με εξαίρεση την άδεια χρήσης READ_PHONE_STATE που υπήρχε στην εφαρμογή FRUIT NINJA , η οποία δεν ζητήθηκε και δεν επηρέασε με την αφαίρεση της, οι υπόλοιπες άδειες ανταποκρίνονται στις λειτουργίες των εφαρμογών και με την αφαίρεση τους επηρεάζονταν οι λειτουργίες που τις αφορούσαν. Επίσης είχαν εντοπιστεί permissions τα οποία πλέον δεν χρειάζονται στις σύγχρονες εκδόσεις Android.

Στις κανονικές άδειες χρήσης παρατηρήθηκε μεγαλύτερος αριθμός αδειών που δεν είχαν κάποια επίδραση στην λειτουργία των εφαρμογών, κάποιες από αυτές όμως επηρέασαν την λειτουργία των εφαρμογών ακόμη και στην εκκίνηση τους παρόλο που δεν ήταν αναγκαίες για την λειτουργία τους.

Συνοψίζοντας παρατηρούμε ότι το σύστημα που έχει θεσπιστεί με τις άδειες χρήσης όσο αφορά τις άδειες επικίνδυνου επιπέδου προσφέρει ένα καλό επίπεδο ασφάλειας. Η πρόσβαση σε πόρους ή δεδομένα που μπορούν να επηρεάσουν τα προσωπικά δεδομένα του χρήστη χρειάζεται έγκριση και με την απόρριψη ή την αφαίρεση της εκάστοτε άδειας η εφαρμογή παύει να έχει δικαιώματα χρήσης. Το ίδιο όμως δεν συμβαίνει με τις κανονικές άδειες χρήσης αφού δίνονται αυτόματα από το σύστημα χωρίς ο χρήστης να το γνωρίζει. Αυτό έχει ως αποτέλεσμα οι προγραμματιστές να το εκμεταλλεύονται και να ζητάνε περισσότερες από όσες χρειάζεται, χωρίς αυτό να σημαίνει ότι πρόκειται για κακόβουλο λογισμικό. Αρκετές φορές οι εφαρμογές προορίζονται για πολλές διαφορετικές εκδόσεις Android με διαφορετικό τρόπο χειρισμού των permissions. Έτσι αναγκαστικά υπάρχουν permissions τα οποία στις νεότερες εκδόσεις δεν χρειάζονται.

Όπως έχει αναφερθεί πιο πάνω, λόγω του αυξανόμενου αριθμού apps και λειτουργιών των έξυπνων τηλεφώνων όπως και με τις συνεχείς αλλαγές στο σύστημα χρήσης permissions με τις νεότερες εκδόσεις Android, το θέμα ασφάλειας στα smartphones αποτελούσε και αποτελεί κύριο θέμα μελέτης. Σύμφωνα με τις έρευνες Barrera D et al [02], Felt A.P [07] και τα αποτελέσματα της διατριβής είναι ξεκάθαρο ότι τα permissions χρειάζονται βελτιώσεις ειδικά στις κανονικές άδειες χρήσης. Μια πρόταση είναι τα συχνά χρησιμοποιούμενα δικαιώματα, όπως π.χ INTERNET, το οποίο αφορά μια γενική εικόνα, να διασπαστεί σε υποκατηγορίες με περισσότερες λεπτομέρειες στο πως θα το αξιοποιήσει η κάθε εφαρμογή ενώ τα οι σπάνιες άδειες να συρρικνωθούν σε πιο γενικές κατηγορίες. Η παροχή λεπτότερων λεπτομερειών για συχνές άδειες και ο συνδυασμός των σπάνιων δικαιωμάτων μπορεί να ενισχύσει τη σαφήνεια του μοντέλου άδειας χωρίς

να αυξάνει την πολυπλοκότητα (δηλαδή, διατηρώντας ένα σταθερό συνολικό αριθμό δικαιωμάτων) ως αποτέλεσμα των πρόσθετων δικαιωμάτων. Μια συμπληρωματική πρόταση είναι η καλύτερη τεκμηρίωση των δικαιωμάτων από τους δημιουργούς του λειτουργικού Android, έτσι ώστε να υπάρχει καλύτερη κατανόηση από τους προγραμματιστές για το ποια δικαιώματα χρειάζονται και ποια είναι περιττά.

Βιβλιογραφία

[01] Arshad, S., Shah, M.A., Khan, A. and Ahmed, M., 2016. Android malware detection & protection: a survey. Int. J. Adv. Comput. Sci. Appl, 7(2), pp.463-475.

[02] Barrera, D., Kayacik, H.G., Van Oorschot, P.C. and Somayaji, A., 2010, October. A methodology for empirical analysis of permission-based security models and its application to android. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 73-84). ACM.

[03] Bagheri, H., Kang, E., Malek, S. and Jackson, D., 2015, June. Detection of design flaws in the android permission protocol through bounded verification. In International Symposium on Formal Methods (pp. 73-89). Springer, Cham.

[04] D'Angelo, M. (2017). Correlating Sensitive Behaviours with User Interaction on Android. pages 8-10

[05] Elenkov N, Android Security Internal an In-Depth Guide to Android Security Architecture, 2015

[06] Enck, W., Ongtang, M. and McDaniel, P., 2009, November. On lightweight mobile phone application certification. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 235-245). ACM.

[07] Felt, A.P., Chin, E., Hanna, S., Song, D. and Wagner, D., 2011, October. Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 627-638). ACM

[08] Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D., 2012, July. Android permissions: User attention, comprehension, and behavior. In Proceedings of the eighth symposium on usable privacy and security (p. 3). ACM.

[09] Felt, A.P., Greenwood, K. and Wagner, D., 2011, June. The effectiveness of application permissions. In Proceedings of the 2nd USENIX conference on Web application development (pp. 7-7).

[10] Gustavo B., Juan C., Carlos L., Camila S.,(2018,August), A formal approach for the verification of the permission-based security model of Android, CLEI electronic journal, Volume 21, Number 2, Paper 3 (page 4)

[11] Khatoon, A., & Corcoran, P. (2017). Android permission system and user privacy — A review of concept and approaches. IEEE 7th International Conference on Consumer Electronics - Berlin. Berlin: IEEE.

[12] Ma, Z. (2013). Android Application Install-time Permission Validation and Run-time Malicious Pattern Detection. Arlington, Virginia, pages 3-4.

[13] Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y. and Dolev, S., 2009. Google android: A state-of-the-art review of security mechanisms. arXiv preprint arXiv:0912.5101.

[14] Van der Veen, V. (2013). Dynamic Analysis of Android Malware, page 10

[15] Vidas, T., Christin, N. and Cranor, L., 2011, May. Curbing android permission creep. In Proceedings of the Web (Vol. 2, pp. 91-96).

Ιστοσελίδες:

[16] Anon, (2019).[online]Available at: https://www.gsmaintelligence.com/research/?file=061ad2d2417d6ed1ab002da0dbc9ce22&download [Accessed 13 Apr. 2019]

[17] Mobile OS market share 2018 | Statista https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[18] Google Play Store: number of apps 2018 | Statista

https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[19] Infographic: Android's Rise to Smartphone Dominance
https://www.statista.com/chart/15561/smartphone-sales-by-os/

[20] Android Open Source Project
https://source.android.com

[21] Permissions overview | Android Developers
https://developer.android.com/guide/topics/permissions/overview

[22] Request App Permissions | Android Developers
https://developer.android.com/training/permissions/requesting

[23] Distribution dashboard | Android Developers
https://developer.android.com/about/dashboards

[24] Celebrating a Sweet Decade of Android
https://blog.google/products/android/celebrating-sweet-decade-android/

[25] Android version history
https://en.wikipedia.org/wiki/Android_version_history

[26] Android (operating system)
https://en.wikipedia.org/wiki/Android_(operating_system)

[27] Security tips | Android Developers
https://developer.android.com/training/articles/security-tips.html

[28] Request App Permissions | Android Developers
https://developer.android.com/training/permissions/requesting#declare-by-api-level

[29] Android 6.0 Changes | Android Developers

https://developer.android.com/about/versions/marshmallow/android-6.0-changes

[30] Permissions overview | Android Developers
https://developer.android.com/guide/topics/permissions/overview.html#normal-dangerous

[31] Permissions overview | Android Developers
https://developer.android.com/guide/topics/permissions/overview.html#permission-groups

[32] Tumbleson, C., & Wiśniewski, R. (n.d.). A tool for reverse engineering Android apk files. Ανάκτηση από https://ibotpeaches.github.io/Apktool/

[33] 10 Best Google Play Store Alternatives : Websites And Apps
https://fossbytes.com/10-google-play-store-alternatives/

[34] Report: 97% Of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe
https://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/#46fc50602d4f

[35] What Is the Difference: Viruses, Worms, Trojans, and Bots?
https://www.cisco.com/c/en/us/about/security-center/virus-differences.html#4

[36] Oracle |Introduction
https://docs.oracle.com/javase/7/docs/technotes/guides/jni/spec/intro.html#wp9502

Παράρτημα Α
Εικόνες

Παράρτημα Β
Γραφήματα

Παράρτημα Γ
Πίνακες