Ατομική Διπλωματική Εργασία

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΕΥΑΙΣΘΗΤΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ANDROID ΚΙΝΗΤΕΣ ΕΦΑΡΜΟΓΕΣ

Χριστιάνα Γιαπιντζάκη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Παρακολούθηση των προσωπικών
ευαίσθητων δεδομένων
στις Android κινητές εφαρμογές

Χριστιάνα Γιαπιντζάκη

Επιβλέπουσα Καθηγήτρια
Γεωργία Καπιτσάκη

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2019

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου Δρ. Γεωργία Καπιτσάκη η οποία μου παρείχε την δυνατότητα να ασχοληθώ και να εμβαθύνω τις γνώσεις μου όσον αφορά το συγκεκριμένο θέμα της παρούσας Ατομικής Διπλωματικής Εργασίας καθώς και για την εμπιστοσύνη που μου έδειξε καθ'όλη την διάρκεια εκπόνησης της εν λόγω εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου που χωρίς αυτούς δεν θα μπορούσα να ανταπεξέλθω στις δυσκολίες που αντιμετώπισα τα τελευταία τέσσερα χρόνια. Η παρούσα Ατομική Διπλωματική Εργασία είναι αφιερωμένη σε αυτούς ως ένδειξη εκτίμησης της αδιάκοπης ηθικής υποστήριξης και πίστης τους σε μένα.

Τέλος, θα ήθελα να ευχαριστήσω το Πανεπιστήμιο Κύπρου που με την ευκαιρία που μου πρόσφερε να φοιτήσω στον κλάδο της Πληροφορικής πλέον φεύγω πιο δυνατή και γεμάτη γνώσεις και εμπειρίες οι οποίες θα με συνοδεύουν σε όλο το υπόλοιπο της ζωής μου.

Περίληψη

Στα πλαίσια εκπόνησης της παρούσας ατομικής διπλωματικής εργασίας, αναπτύχθηκε η Android εφαρμογή PermExtractor με σκοπό την παρακολούθηση πρόσβασης αλλά και την έμμεση παροχή προστασίας σε ζητήματα ευαίσθητων προσωπικών δεδομένων σε Android κινητές εφαρμογές. Τόσο η παρακολούθηση πρόσβασης όσο και η παροχή προστασίας στα ζητήματα αυτά καθίστανται επιβεβλημένες αν αναλογιστεί κανείς το μέγεθος της χρήσης των smartphones, σε συνάρτηση με τους κινδύνους που κρύβει η εν λόγω χρήση.

Εισαγωγικά γίνεται μια αναφορά στο παρασκήνιο στο οποίο στηρίζεται η παρούσα εργασία και περιγράφεται ο στόχος που καλείται να εξυπηρετήσει. Ακολούθως, περιγράφεται η έννοια της ιδιωτικότητας και των προσωπικών ευαίσθητων δεδομένων των ανθρώπων, ενώ παράλληλα, παρουσιάζονται οι κίνδυνοι που ελλοχεύουν αναφορικά με αυτά.

Στην συνέχεια, αναλύεται η αρχιτεκτονική του Android συστήματος καθώς και οι τρόποι με τους οποίους παρέχει ασφάλεια στις εφαρμογές του. Περιγράφεται επιπλέον η δομή των APK αρχείων και αναφέρονται κάποια προβλήματα αναφορικά με την ασφάλεια στο Android.

Σε μεταγενέστερο στάδιο παρατείθεται μια περιγραφή των τεχνολογιών και των εργαλείων που χρησιμοποιήθηκαν κατά την ανάπτυξη της εφαρμογής PermExtractor αλλά και του τρόπου εκμετάλλευσης τους. Ακόμη, εξετάζονται μερικές παρόμοιες εφαρμογές με τον PermExtractor όπου λαμβάνει χώρα μια σύγκριση με αυτόν.

Σε τελικό στάδιο αναλύεται και παρουσιάζεται ο τρόπος με τον οποίο πραγματοποιήθηκε η υλοποίηση της εφαρμογής και περιγράφονται τα αποτελέσματα που εξήχθησαν από δοθέν ερωτηματολόγιο, συνοδευόμενα από κάποια γενικά συμπεράσματα αλλά και μελλοντικές εργασίες.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Γενική Εισαγωγή

Στην σημερινή κοινωνία είναι πλέον γεγονός πως η τεχνολογία λειτουργεί ως αναπόσπαστο κομμάτι της ζωής του ανθρώπου αφού εξαρτάται απο αυτήν για την διεκπεραίωση ορισμένων, αν όχι των περισσότερων εργασιών που είναι απαραίτητες για εκείνον. Αυτή η ραγδαία τεχνολογική ανάπτυξη, που παρακολουθείται τα τελευταία χρόνια, έχει προσδώσει στον άνθρωπο την ικανότητα να καταφέρνει σχεδόν οτιδήποτε επιθυμεί με γρήγορο και εύκολο τρόπο. Ταυτόχρονα, όμως, έχει οδηγήσει σε μια άνευ προηγουμένου διάδοση αρχείων και προσωπικών δεδομένων με απότελεσμα να είναι αδύνατο να γνωρίζουμε ποιος έχει πρόσβαση σε αυτά.

Μια από τις πιο αξιοσημείωτες ανακαλύψεις στον κόσμο της τεχνολογίας αποτελούν οι έξυπνες κινητές συσκευές από τις οποίες ο άνθρωπος είναι τόσο εξαρτημένος σε σημείο που βρίσκονται συνεχώς στην χούφτα του χεριού του. Καθημερινά, εκατομμύρια ανθρώπων έχουν την ευκαιρία να επιλέγουν την εγκατάσταση νέων εφαρμογών στις συκευές τους, μέσα από ένα συνεχώς αυξανόμενο εύρος, για σκοπούς επικοινωνίας, ψυχαγωγίας, αναζήτησης πληροφοριών κτλ. Οι εν λόγω εφαρμογές τις πλήστες φορές ισχυρίζονται πως είναι απαραίτητη η πρόσβαση σε διάφορες πληροφορίες που αφορούν τον χρήστη με σκοπό την ομαλή λειτουργία τους. Μεγάλο ποσοστό των πληροφοριών στις οποίες επιθυμούν πρόσβαση είναι τα προσωπικά ευαίσθητα δεδομένα των χρηστών.

Ο τρόπος με τον οποίο οι εφαρμογές ζητούν από τον χρήστη πρόσβαση σε πόρους της συσκευής του και στα προσωπικά του δεδομένα δεν είναι πάντα ξεκάθαρος αφού μπορεί να

παρουσιάζεται σε μορφή ενός μεγάλου κειμένου, για το οποίο δεν διαθέτει χρόνο ο χρήστης, ή και σε μορφή ενός πολύ σύντομου κειμένου με αποτέλεσμα ο χρήστης να μην αντιλαμβάνεται σε τι ακριβώς δίνει την έγκριση του. Ως αποτέλεσμα, πλούσιες ποσότητες προσωπικών δεδομένων ρέουν με ευκολία από τις κινητές συσκευές των χρηστών όχι μόνο προς μεγάλες δυνάμεις, όπως την Google και την Apple, αλλά και προς τρίτες επιχειρήσεις. Οι εν λόγω επιχειρήσεις τείνουν να συλλέγουν, να αναλύουν, να μοιράζονται, να εμπορεύονται και να χρησιμοποιούν δεδομένα δισεκατομμύριων ανθρώπων εισβάλλοντας στην ιδιωτικότητα τους και παράλληλα αφήνωντας τους ίδιους εν αγνοία.

1.2 Στόχος Διπλωματικής Εργασίας

Βάσει αυτών που αναφέρθηκαν παραπάνω αλλά και της έννοιας της ιδιωτικότητας ως ένα θεμελιώδες δικαίωμα του ανθρώπου είναι απαραίτητη η ύπαρξη διαδικασιών μέσα από τις οποίες ο χρήστης θα μπορεί να κατανοεί σε μεγαλύτερο βαθμό την έκταση πρόσβασης που έχουν οι εφαρμογές του στα προσωπικά του δεδομένα ώστε να προστατεύει καλύτερα τον εαυτό του και την ιδιωτικότητα του.

Στόχος της παρούσας ατομικής διπλωματικής εργασίας είναι η ανάπτυξη μιας Android εφαρμογής η οποία θα αναλύει τα APK αρχεία των εγκατεστημένων εφαρμογών του χρήστη με αποτέλεσμα να του παρουσιάζει με κατανοητό και φιλικό προς εκείνο τρόπο τα επικίνδυνα permissions που έχει πρόσβαση η κάθε μια. Ανάμεσα στα permissions αυτά θα βρίσκονται και κάποια τα οποία δηλώνονται μέσα στον κώδικα της εφαρμογής. Επιπρόσθετα, θα δίνει την ευκαιρία στον χρήστη να καθορίζει τις προτιμήσεις του όσον αφορά τα permissions που θεωρεί ο ίδιος ιδανικά για χρήση από τις εφαρμογές και θα τον ενημερώνει για το ποιες εφαρμογές είναι σύμφωνες με αυτά και ποιες όχι. Ακόμη, θα προτίνει στον χρήστη εναλλακτικές εφαρμογές οι οποίες θα είναι σύμφωνες με τις προτιμήσεις του.

1.3 Δομή Διπλωματικής Εργασίας

Κεφάλαιο 1: Σε αυτό το κεφάλαιο γίνεται μια γενική εισαγωγή στα πλαίσια του θέματος της παρούσας διπλωματικής εργασίας καθώς και περιγράφεται ο στόχος και η δομή της.

Κεφάλαιο 2: Στο συγκεκριμένο κεφάλαιο γίνεται μια εισαγωγή που συσχετίζει την έννοια της ιδιωτικότητας και της τεχνολογίας. Στην συνέχεια επεξηγούνται οι έννοιες της

ιδιωτικότητας, των προσωπικών και των ευαίσθητων δεδομένων. Τέλος, αναφέρονται οι κίνδυνοι που ελλοχεύουν όσον αφορά την ιδιωτικότητα των χρηστών της τεχνολογίας.

Κεφάλαιο 3: Στο κεφάλαιο αυτό παρουσιάζεται αναλυτικά η αρχιτεκτονική του Android συστήματος, η ασφάλεια που παρέχει στις εφαρμογές του και τα προβλήματα σχετικά με αυτή αλλά και περιγράφεται η δομή των APK αρχείων.

Κεφάλαιο 4: Σε αυτό το κεφάλαιο παρουσιάζονται κάποιες παρόμοιες εφαρμογές με αυτή που αναπτύχθηκε στα πλαίσια της παορούσας διπλωματικής εργασίας και γίνεται μια σύγκριση μεταξύ τους.

Κεφάλαιο 5: Στο συγκεκριμένο κεφάλαιο αναφέρονται οι τεχνολογίες και τα εργαλεία καθώς και ο τρόπος με τον οποίο χρησιμοποιήθηκαν κατά την ανάπτυξη της Android εφαρμογής.

Κεφάλαιο 6: Στο κεφάλαιο αυτό αναλύεται ο τρόπος υλοποίησης της Android εφαρμογής PermExtractor.

Κεφάλαιο 7: Σε αυτό το κεφάλαιο αναλύονται τα αποτελέσματα του ερωτηματολογίου αναφορικά με την εφαρμογή που αναπτύχθηκε ενώ ταυτόχρονα παρατείθονται κάποια γενικά συμπεράσματα και μελλοντικές εργασίες.

Κεφάλαιο 2

Ιδιωτικότητα

2.1 Εισαγωγή

Αναμφισβήτητα, ο 21ος αιώνας μπορεί να θεωρηθεί ως ο αιώνας των Big Data αφού η ραγδαία ανάπτυξη της τεχνολογίας προσφέρει πλέον την δυνατότητα αποθήκευσης και επεξεργασίας τεράστιας ποσότητας δεδομένων. Καθημερινά εκατομμύρια ανθρώπων βρίσκονται συνδεδεμένοι στις συσκευές τους κι αυτές μεταξύ τους μέσω του Internet of Things. Με σκοπό να χρησιμοποιήσουν τις συσκευές αυτές και να επιτελέσουν μια εργασία, οποιουδήποτε είδους, είναι απαραίτητη η παραχώρηση προσωπικών και ευαίσθητων δεδομένων των χρηστών.

Από την δημιουργία του Homo Sapiens, πριν 200.000 χρόνια μέχρι και σήμερα, η έννοια της ιδιωτικότητας δεν έχει επιδεχτεί κάποια αλλαγή [1]. Παραμένει ένα δικαίωμα το οποίο φέρει ο κάθε άνθρωπος και μπορεί να μεταφραστεί ως ένας τρόπος να ρυθμίζεται η πρόσβαση της κοινωνίας στα προσωπικά δεδομένα του. Μια αναφορά προερχόμενη από την TRUSTe / National Cyber Security Alliance (NCSA) [2], έδειξε πως οι περισσότεροι Αμερικανοί ανησυχούν σε μεγαλύτερο βαθμό για την προστασία των προσωπικών τους δεδομένων από το να χάσουν την κύρια πηγή εισοδήματός τους • γεγονός που ενισχύει την σημαντικότητα της ιδιωτικότητας για τους ανθρώπους.

Ο συνδυασμός της ραγδαίως αυξανόμενης δύναμης της τεχνολογίας και ταυτόχρονα της μειωμένης σαφήνειας της ιδιωτικότητας ως πράξη δημιουργούν προβλήματα που σχετίζονται άμεσα με το δίκαιο, την πολιτική και την ηθική [1].

Οι πρόσφατες εξελίξεις στην τεχνολογία της πληροφορίας απειλούν την προστασία της ιδιωτικής ζωής των ανθρώπων και έχουν προκαλέσει μείωση στον έλεγχο των προσωπικών

τους δεδομένων. Κυβερνήσεις αλλά και εμπορικές επιχειρήσεις εξασκούν την τεχνική της συλλογής δεδομένων με αποτέλεσμα την συσσώρευση τεράστιου όγκου πληροφοριών που αφορούν κοινούς πολίτες και την συμπεριφορά τους online. Οι επιδρομές αυτές στην ιδιωτικότητα ενός χρήστη μπορεί να σχετίζονται ακόμη και με την οικογένεια ή την κοινότητα του. Συνήθως οι κυβερνητικοί φορείς εφαρμόζουν τεχνικές με σκοπό την πρόσβαση σε δεδομένα τηλεφωνικών συνομιλιών, αναζητήσεων στο διαδίκτυο και ηλεκτρονικών πληρωμών ενώ οι εμπορικές επιχειρήσεις έχουν ως κύριο στόχο τα προσωπικά και κυρίως ευαίσθητα δεδομένα των πελατών τους με σκοπό την ανάπτυξη τους και την αύξηση του κέρδους τους [3].

Η ιδιωτικότητα είναι περίπλοκη οπουδήποτε κι αν εφαρμόζεται (Alan Westin 1968) [4], πόσο μάλλον στο οικοσύστημα των smartphones το οποίο αποτελεί μια σχετικά πρόσφατη ένταξη στον κόσμο της τεχνολογίας. Άρα, προφανώς, τα μέτρα και οι τεχνικές προστασίας που χρησιμοποιεί δεν έχουν τελειοποιηθεί ακόμη. Ένας παράγοντας που διαταράσσει την ύπαρξη αρμονικής σχέσης μεταξύ ιδιωτικότητας και smartphones είναι η συλλογή δεδομένων που επιτελούν τα smartphones αφού βρίσκονται συνεχώς σε λειτουργία και διαθέτουν μια μεγάλη ποικιλία αισθητήρων που επιτρέπουν την συγκέντρωση πιθανώς προσωπικών κι ευαίσθητων πληροφοριών των χρηστών. Ως αποτέλεσμα, η συλλογή αυτή κινεί υποψίες για το που αποθηκεύονται τα δεδομένα και ποιος έχει πρόσβαση σ'αυτά.

2.2 Ιδιωτικότητα και Προσωπικά δεδομένα

Η ιδιωτικότητα θεωρείται ένα από τα πιο σημαντικά ανθρώπινα δικαιώματα της σύγχρονης εποχής. Ορίζεται ως το δικαίωμα ενός ανθρώπου να ελέγχει την πρόσβαση στα προσωπικά του δεδομένα. Σχεδόν κάθε χώρα του κόσμου περιλαμβάνει το δικαίωμα της ιδιωτικότητας στο σύνταγμά της [5].

Στην απόφαση Vickery v Nova Scotia του Ανώτατου Δικαστηρίου του Καναδά [6], η ιδιωτικότητα χαρακτηρίστηκε ως δικαίωμα απόρρεον και συνυφασμένο με αυτό της αξιοπρέπειας του ατόμου. Αυτό το δικαίωμα έχει ουσιαστική σημασία για την αίσθηση ολοκλήρωσης κάθε ατόμου, τόσο μεμονωμένα όσο και ως μέλος της κοινωνίας. Χωρίς την έννοια της ιδιωτικότητας, είναι δύσκολο για ένα άτομο να κατέχει και να διατηρεί μια αίσθηση αυτοπεποίθησης ή να διατηρεί ανεξαρτησία πνεύματος και σκέψης.

Ο Samuel D. Warren και ο Louis Brandeis σε άρθρο τους [7] αναφορικά με την προστασία της ιδιωτικότητας εξέφρασαν έντονη αποδοκιμασία ως προς τις παρενοχλητικές δραστηριότητες των δημοσιογράφων εκείνων των ημερών. Οι συγγραφείς χρησιμοποίησαν την φράση "right to be left alone" βασιζόμενοι στο «δικαίωμα της προσωπικότητας του ατόμου». Η δημοσίευση του άρθρου των Warren και Brandeis ήταν η αφορμή για να ξεκινήσει ένας διάλογος περί ιδιωτικότητας που εμπεριέκλειε ισχυρισμούς για το δικαίωμα των ατόμων να ελέγχουν την έκταση στην οποία τρίτα άτομα έχουν πρόσβαση στα δεδομένα τους, καθώς και για το δικαίωμα της κοινωνίας να γνωρίζει τους πολίτες της.

Η έννοια της ιδιωτικότητας μπορεί να χωριστεί σε έναν αριθμό μορφών τις οποίες έλαβε κατά την ιστορική της εξέλιξη[8][10]:

- Informational/Tort privacy: Αυτή η μορφή αφορά το δικαίωμα ενός ατόμου να ασκεί άμεσο ή έμμεσο έλεγχο στην πρόσβαση σε πληροφορίες που αφορούν τον εαυτό του, σε καταστάσεις στις οποίες άλλοι έχουν δυνατότητα αποκτήσης πληροφοριών για το άτομο αυτό και σε τεχνολογίες που μπορούν να χρησιμοποιηθούν ως μέσο για τη δημιουργία, επεξεργασία ή διάδοση πληροφοριών του ατόμου.
- Constitutional/Decisional privacy: Αυτή η μορφή αφορά την ελευθερία που έχει το κάθε άτομο να παίρνει αποφάσεις, για θέματα προσωπικά, χωρίς την ανάμειξη άλλων ατόμων. Πιο συγκεκριμένα, αφορά την ελευθερία λήψης σημαντικών αποφάσεων που φτάνουν στον πυρήνα του ποιοι είμαστε, πως ορίζουμε τον εαυτό μας και πως συμπεριφερόμαστε[3].
- Bodily privacy: Αυτή η μορφή αφορά την προστασία του ανθρώπου ως φυσική υπόσταση από επεμβατικές διαδικασίες όπως γενετικές δοκιμές και δοκιμές φαρμάκων.
- Communications privacy: Αυτή η μορφή αφορά την διαφύλαξη του απορρήτου όσον αφορά τηλεφωνικές κλήσεις, ηλεκτρονικά μηνυμάτα και άλλους τρόπους επικοινωνίας.
- Territorial privacy: Αυτή η μορφή αφορά τον καθορισμό ορίων εισβολής στο εγχώριο και άλλο περιβάλλον του ατόμου, όπως ο χώρος εργασίας του ή ο δημόσιος χώρος.[9]

Προσωπικά δεδομένα, ως ορίζονται από το Data Protection Act 1998 (DPA)[11], νοούνται τα δεδομένα τα οποία σχετίζονται με ένα ζωντανό άτομο το οποίο μπορεί να προσδιοριστεί είτε από αυτά είτε από τον συνδιασμό αυτών των δεδομένων και άλλων πληροφοριών που διαθέτει στα χέρια του ο διαχειριστής τους. Παραδείγματα προσωπικών δεδομένων αποτελούν τα εξής; ημερομηνία γέννησης, σεξουαλική προτίμηση, τοποθεσία, θρησκεία, αλλά και διεύθυνση IP του υπολογιστή του ατόμου.

Τα ευαίσθητα δεδομένα [11] είναι ένα υποσύνολο των προσωπικών δεδομένων και περιλαμβάνουν φυλετική ή εθνοτική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή ιδιότητα μέλους σε συνδικαλιστικές οργανώσεις, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα σχετικά με την υγεία ή δεδομένα σχετικά με τη σεξουαλική ζωή ενός ατόμου ή τον σεξουαλικό προσανατολισμό.

2.3 Κίνδυνοι Ιδιωτικότητας

Η ανάπτυξη των κοινωνικών δικτύων, του οικοσυστήματος των smartphones καθώς και της διαδικτυακής διαφήμισης έχει καταστήσει ένα μεγάλο ποσοστό επιχειρήσεων ικανό να παρακολουθεί, να καταγράφει και να ακολουθεί πολλές πτυχές της ζωής των ανθρώπων. Ως αποτέλεσμα, όλες οι συμπεριφορές, οι κινήσεις, οι κοινωνικές σχέσεις, οι αδυναμίες, οι προτιμήσεις, τα ενδιαφέροντα και οι προσωπικές στιγμές των χρηστών τυγχάνουν αξιολόγησης και ανάλυσης σε πραγματικό χρόνο.

Τρανταχτό παράδειγμα αποτελούν τα smartphones, τα οποία καθώς βρίσκονται συνεχώς στο χέρι των ιδιοκτητών τους, μεταδίδουν μεγάλες ποσότητες πληροφορίας που αφορούν την καθημερινή ζωή των χρηστών στην Google και στην Apple. Οι πληροφορίες αυτές τις περισσότερες φορές μεταβιβάζονται ακόμη και σε τρίτες επιχειρήσεις [12].

Ένα τεράστιο σύνολο διασυνδεδεμένων βάσεων δεδομένων, που αποτελείται όχι μόνο από μεγάλους παίκτες όπως το Facebook και την Google αλλά και από χιλιάδες άλλες εταιρείες από διάφορες βιομηχανίες, συλλέγουν, αναλύουν, μοιράζονται, εμπορεύονται και χρησιμοποιούν δεδομένα δισεκατομμύριων ανθρώπων. Μεγάλο μέρος της διαδικασίας αυτής πραγματοποιείται στο παρασκήνιο [13]. Έτσι, οι περισσότεροι καταναλωτές αδυνατούν να κατανοήσουν την πλήρη έκταση και τις μορφές εταιρικής ψηφιακής παρακολούθησης, καθώς και την διαδικασία του profiling που υπόκεινται. Πιο συγκεκριμένα, οι χρήστες τείνουν να μην γνωρίζουν ποιες προσωπικές πληροφορίες και συμπεριφορές τους συλλέγονται ή πώς επεξεργάζονται τα δεδομένα αυτά. Αγνοούν παράλληλα σε ποιους μοιράζονται ή πωλούνται οι εν λόγω πληροφορίες, ποια συμπεράσματα εξάγονται από τη διαδικασία ανωτέρω και ποιες αποφάσεις λαμβάνονται βασιζόμενες σε αυτά.

Δυστυχώς, δεν καταβάλλεται καμία προσπάθεια από την μεριά των επιχειρήσεων ώστε να βοηθήσουν τους χρήστες να κατανοήσουν καλύτερα τις διαδικασίες που εφαρμόζονται στα προσωπικά τους δεδομένα. Συνεπώς, παραμένουν στο σκοτάδι ενώ την ίδια στιγμή παραβιάζεται σε μεγάλο βαθμό η ιδιωτικότητα τους.

Κεφάλαιο 3

Εισαγωγή στο Android

3.1 Android Αρχιτεκτονική

Σχήμα 1

Το Android OS είναι αναμφίβολα η πιο διαδεδομένη τεχνολογία, όσον αφορά τον κόσμο των έξυπνων τηλεφωνικών συσκευών, αφού αντιπροσωπεύει το 85.9% [14] του παγκόσμιου μεριδίου αγοράς. Παρουσιάστηκε, αρχικά, από την Android Inc. ενώ στην συνέχεια, εξαγοράστηκε από την Google και κυκλοφόρησε ως το Android Open Source Project (AOSP). Πλέον, αποτελεί μια ανοιχτή πλατφόρμα λογισμικού με ανοικτού κώδικα λειτουργικό σύστημα, δίνοντας την ευκαιρία ανάπτυξης λογισμικού ή ακόμα και εμπλουτισμού του πηρύνα του λειτουργικού συστήματος του Android, στους ενδιαφερόμενους προγραμματιστές.

Στο σχήμα 1, απεικονίζεται το Android Software Stack, το οποίο απαρτίζεται από πέντε κύρια στρώματα: το Linux Kernel layer, το Hardware Abstraction Layer, το Runtime layer, το Framework layer and το Application layer. Στο Runtime layer συμπεριλμβάνεται κι ένα ακόμη συστατικό, τα Native C/C++ Libraries. [15][16]

Ξεκινώντας από κάτω προς τα πάνω, το Linux Kernel θεωρείται το πρώτο κύριο στρώμα της Android αρχιτεκτονικής. Αυτό το στρώμα παρέχει βασικές υπηρεσίες, όπως διαχείριση διαδικασιών, μνήμης και αρχείων. Επιπρόσθετα, έχει την ευθύνη για συγκεκριμένα hardware drivers, όπως το Wi-Fi και το Bluetooth. Το Linux Kernel έχει σχεδιαστεί για να είναι ευέλικτο με πολλά συστατικά του Android που βασίζονται σε μεγάλο βαθμό στη διαθεσιμότητα συγκεκριμένου υλικού σε μια συγκεκριμένη συσκευή.

Το Android χρησιμοποιεί το Linux Kernel ως τον πηρύνα του λειτυργικού του συστήματος. Επιπλέον, κυκλοφορεί κατώ από δύο διαφορετικές άδειες ανοιχτού κώδικα. Το Linux Kernel κυκλοφορεί υπό το General Public License (GPL) και η πλατφόρμα Android, εξαιρουμένου του Linux Kernel, διαθέτει άδεια χρήσης Apache Software License (ASL).

Το Hardware Abstraction Layer (HAL) αποτελεί το δεύτερο στρώμα της Android αρχιτεκτονικής. Παρέχει τυποποιημένες διασυνδέσεις που προβάλλουν τις δυνατότητες του υλικού μιας Android συσκευής στο high-level Java API framework. Το HAL αποτελείται από μια ποικιλία με library modules. Καθένα, από αυτά τα modules, υλοποιεί μια διεπαφή για ένα συγκεκριμένο hardware component, όπως η κάμερα ή το Bluetooth. Σε περίπτωση που ένα framework θελήσει να έχει πρόσβαση στο υλικό της συσκευής, τότε το σύστημα του Android φορτώνει το αντίστοιχο library module για το εν λόγω hardware component [17].

Το Android Runtime (ART) είναι ένα ακόμα στρώμα του Android Software Stack. Ο ρόλος του είναι η διάθεση των βασικών βιβλιοθηκών Java οι οποίες προσφέρουν πλήρεις

δυνατότητες προγραμματισμού σε γλώσσα Java και του DVM (Dalvik Virtual Machine), το οποίο χρησιμοποιεί το Linux-based kernel για να παρέχει ένα περιβάλλον που θα φιλοξενήσει μια εφαρμογή Android. Το Android Runtime είναι σχεδιασμένο με τέτοιο τρόπο ώστε να μπορεί να τρέχει πολλαπλές εικονικές μηχανές σε συσκευές χαμηλής μνήμης. Αυτό πραγματοποιείται με την εκτέλεση αρχείων DEX, μια μορφή bytecode που έχει σχεδιαστεί ειδικά για το Android και έχει βελτιστοποιηθεί για ελάχιστη χρήση μνήμης.

Τα Native Libraries βρίσκονται στο ίδιο επίπεδο της στοίβας με το Android Runtime. Πρόκειται για βιβλιοθήκες, γραμμένες σε γλώσσα C/C++, οι οποίες ασχολούνται με τα πιο βαριά καθήκοντα, παρέχοντας έτσι πολλή δύναμη στην πλατφόρμα Android. Αυτές οι βιβλιοθήκες καλούνται μέσω διεπαφής Java. Στην πραγματικότητα, ένας τυπικός προγραμματιστής εφαρμογών Android έχει πρόσβαση σε αυτές τις βιβλιοθήκες αποκλειστικά μέσω των core libraries του ART που είναι βασισμένες σε Java. Οι βιβλιοθήκες C/C++ συμπεριλαμβάνουν μια γκάμα λειτουργιών, όπως τη σχεδίαση γραφικών 2D και 3D, την επικοινωνία SSL (Secure Sockets Layer), τη διαχείριση βάσεων δεδομένων SQLite, η αναπαραγωγή ήχου και βίντεο.[18]

Το Application Framework layer βρίσκεται πάνω από αυτό των Native Libraries. Το συγκεκριμένο στρώμα παρέχει σημαντικά Application programming interface (APIs) και high-level services που βρίσκονται σε μορφή κλάσεων της Java. Αυτά τα APIs μπορούν να χρησιμοποιηθούν από όλους τους προγραμματιστές για τη δημιουργία εφαρμογών Android. Διαχωρίζονται σε διάφορους τύπους και κάθε τύπος έχει το δικό του κύκλο ζωής και σκοπό που περιγράφει τον τρόπο με τον οποίο το στοιχείο θα δημιουργηθεί και θα καταστραφεί. Οι πιο σημαντικοί τύποι που προσφέρονται είναι οι εξής: [17]

- View System: Χρησιμοποιείται για την κατασκευή του User Interface (UI) μιας εφαρμογής και διαθέτει lists, grids, text boxes, buttons, ακόμη κι έναν ενσωματωμένο web browser.
- Resource Manager: Παρέχει πρόσβαση σε πόρους όπως localized strings, graphics, and layout αρχεία.
- Notification Manager: Παρέχει την δυνατότητα εμφάνισης custom alerts στο status bar της συσκευής.
- Activity Manager: Διαχειρίζεται τον κύκλο ζωής των εφαρμογών και παρέχει ένα κοινό navigation back stack.
- Content Providers: Παρέχει την δυνατότητα σε μια εφαρμογή να έχει πρόσβαση στα δεδομένα άλλων εφαρμογών αλλά και να μοιράζεται η ίδια τα δικά της.

Το Application, το ανώτατο στρώμα του Application Software Stack, αποτελείται από όλες τις εφαρμογές με τις οποίες ο χρήστης μπορεί να αλληλεπιδράσει άμεσα. Στο στρώμα αυτό περιλαμβάνονται τόσο οι εφαρμογές του πυρήνα όσο και οι third-party εφαρμογές, όπως phone, contacts, games, home, browser κ.τ.λ. Οι εφαρμογές του συστήματος έχουν δύο χρήσεις. Αρχικά, λειτουργούν ως εφαρμογές για χρήστες, αλλά ταυτόχρονα, παρέχουν και βασικές δυνατότητες στις οποίες μπορούν να έχουν πρόσβαση οι προγραμματιστές από τις δικές τους εφαρμογές. Για παράδειγμα, αν μια third-party εφαρμογή θέλει να παραδώσει ένα μήνυμα SMS, δεν χρειάζεται ο προγραμματιστής να χτίσει μόνος του τη λειτουργία αυτή αφού μπορεί να καλέσει μια άλλη ήδη εγκατεστημένη εφαρμογή SMS και να παραδώσει εκείνη το μήνυμα στον παραλήπτη.

3.2 Ασφάλεια στο Android

Σύμφωνα με μια έρευνα που διεξήχθη από το Bitdefender τον Απρίλιο του 2017 [19], το ποσοστό των χρηστών που αποθηκεύουν τις προσωπικές και ιδιωτικές τους πληροφορίες στις κινητές τους συσκευές ανέρχεται στο 50%. Το γεγονός αυτό καθιστά πολύ σημαντική την ύπαρξη προστασίας, στις Android συσκευές, με σκοπό την αποφυγή περιστατικών κλοπής δεδομένων των χρηστών ή επίθεσης από κακόβουλα λογισμικά. Τα Android διαθέτουν κάποια κύρια χαρακτηριστικά τα οποία στοχεύουν στην διαφύλαξη της ασφάλειας των εφαρμογών των χρηστών. [20][21]

Ένα από αυτά τα χαρακτηριστικά αποτελεί η τεχνική του Sandboxing για την οποία και είναι υπεύθυνο το Dalvik Virtual Machine (VMM), στο Linux Kernel στρώμα της Android αρχιτεκτονικής. Κατά το Sandboxing, το Android δημιουργεί ένα πλαίσιο απομόνωσης για την κάθε εφαρμογή και τα δεδομένα αυτής. Μαζί με την εφαρμογή, εντός του Sandbox, περιορίζεται το Application Framework, τα Native Libraries, και το Android Runtime. Με αυτό τον τρόπο η καθε εφαρμογή τρέχει μέσα στο δικό της Linux process. Σε περίπτωση που μια κακόβουλη εφαρμογή θελήσει να αλληλεπιδράσει με άλλες εφαρμογές, χωρίς να αποκτήσει την έγκριση του χρήστη, ο μηχανισμός Sandbox παρεμβαίνει απαγορεύοντας τις αλληλεπιδράσεις της στο επίπεδο του process. Επειδή τα Sandbox των εφαρμογών βασίζονται στο Linux Kernel, τους προσδίδεται ανθεκτικότητα και δυσκολία ως προς το να γίνουν hacked. Ως αποτέλεσμα, αυξάνεται η ασφάλεια στο Linux Kernel επίπεδο.

Το Application signing [22] επιτρέπει στους προγραμματιστές να εντοπίζουν τον δημιουργό μιας εφαρμογής και να ενημερώνουν την δικής τους με εύκολο τρόπο. Ανήκει στην κατηγορία των χαρακτηριστικών που αυξάνουν την ασφάλεια του Android γεφυρώνοτας την

εμπιστοσύνη μεταξύ των τριών οντοτήτων; Google, προγραμματιστή και εφαρμογής. Αυτή η διαδικασία είναι το πρώτο βήμα για την τοποθέτηση μιας εφαρμογής στο Sandbox της. Το πιστοποιητικό που αποκτά μια εφαρμογή μετά το signing της, διατυπώνει ποιο αναγνωριστικό χρήστη συσχετίζεται με ποια εφαρμογή. Το Application signing διασφαλίζει ότι μία εφαρμογή δεν μπορεί να έχει πρόσβαση σε άλλη εφαρμογή παρά μόνο μέσω σαφώς καθορισμένου IPC.

Το Inter-Process Communication (IPC) αποτελεί έναν ασφαλή μηχανισμό επαναχρησιμοποίησης συστατικών και διάδοσης διάφορων δεδομένων μεταξύ των εφαρμογών σε μια Android συσκευή. Ο μηχανισμός αυτός επιτυγχάνει τον σκοπό του με την χρήση Intents και Binders. Το Intent [23] ορίζεται ως ένα σύστημα μηνυμάτων το οποίο χρησιμοποιείται από ένα Activity για να κάνει launch ένα άλλο μέσω της συνάρτησης startActivity(). Μια άλλη λειτουργία του Intent είναι πως επιτρέπει σε ένα Activity να ζητά τις υπηρεσίες οποιουδήποτε άλλου καταλλήλως καταχωρημένου Activity στη συσκευή για την οποία έχουν ρυθμιστεί τα κατάλληλα permissions. Όσον αφορά το Binder, πρόκειται για μια αφαιρετική οντότητα του Intent. Αποτελεί ένα μηχανισμό που πραγματοποιεί in-process and cross-process κλήσεις.

3.2.1 Android permissions

Όπως προαναφέρθηκε στο παραπάνω κεφάλαιο, η ασφάλεια αποτελεί κύριο χαρακτηριστικό στο οποίο βασίζεται ο τρόπος δημιουργίας της Android αρχιτεκτονικής. Έτσι, καμία εφαρμογή, από προεπιλογή, δεν έχει δικαίωμα να εκτελέσει οποιεσδήποτε λειτουργίες που θα έχουν κάποια επιπτώση σε άλλες εφαρμογές, στο λειτουργικό σύστημα ή στον χρήστη, χωρίς την συγκατάθεση του ίδιου. Οι λειτουργίες αυτές περιλαμβάνουν την ανάγνωση ή τη συγγραφή ιδιωτικών δεδομένων του χρήστη, άγνωση ή εγγραφή αρχείων άλλης εφαρμογής, πρόσβαση στο δίκτυο κτλ. Στο σημείο αυτό έρχονται να επέμβουν τα Android Permissions.[24]

Σκοπός της ύπαρξης των permissions στα Android είναι η προστασία της ιδιωτικότητας των χρηστών. Το μεγαλύτερο ποσοστό των permissions, που χρειάζεται μια εφαρμογή για να λειτουργήσει, βρίσκεται στο Manifest αρχείο της, έχωντας την μορφή που απεικονίζεται στο Σχήμα 2.

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

    <uses-permission android:name="android.permission.READ_CONTACTS" />
    ...
</manifest>
```

Σχήμα 2

Ταυτόχρονα, υπάρχει και μια μειονότητα permissions, η οποία καθορίζεται με έμμεσο τρόπο στον κώδικα κάποιων εφαρμογών. Αυτό, διατρέχει κίνδυνο πρόσβασης των εφαρμογών σε πληροφορίες που μπορεί να εκμεταλλευτούν με κακόβουλο τρόπο.

Τα Android permissions χωρίζονται σε διάφορα protection levels.[25] Το protection level επηρεάζει το αν θα προβεί το σύστημα σε εμφάνιση runtime permission request στην διαπροσωπία του χρήστη. Σε τέτοια περίπτωση, αυτός, παίρνει τον έλεγχο στα χέρια του, καθώς έχει την ευκαίρια να αποδέχεται ή να απορρίπτει την χρήση κάποιου permission από μια εφαρμογή. Υπάρχουν τέσσερα protection levels που έχουν επίδραση σε third-party εφαρμογές; Normal, Dangerous, Signature και SignatureOrSystem permissions.

Αρχικά, τα Normal permissions είναι υπεύθυνα για την πρόσβαση σε δεδομένα και πόρους, που βρίσκονται εκτός του Sandbox μιας εφαρμογής, σε περιπτώσεις όμως που δεν βάζουν σε κίνδυνο την ιδιωτικότητα του χρήστη αλλά και την λειτουργία των υπόλοιπων εφαρμογών. Για την χρήση ενός Normal permission από μια εφαρμογή είναι απαραίτητη η δήλωση του στο Manifest αρχείο της. Έτσι το σύστημα αυτόματα παραχωρεί στην εφαρμογή το συγκεκριμένο permission χωρίς την ανάγκη έγκρισης από τον χρήστη. Κάποια παραδείγματα normal permissions είναι τα εξής; ACCESS_NETWORK_STATE, ACCESS_NOTIFICATION_POLICY, ACCESS_WIFI_STATE, BLUETOOTH κτλ.

Τα Dangerous permissions είναι μια μια κατηγορία υψηλού ρίσκου για τον χρήστη αφού έχει ως στόχο την πρόσβαση σε δεδομένα ή πόρους που αφορούν τις προσωπικές του πληροφορίες και ταυτόχρονα μπορεί να επηρεάσει τα αποθηκευμένα δεδομένα του χρήστη ή τη λειτουργία άλλων εφαρμογών. Για την χρήση ενός Dangerous permission από μια εφαρμογή είναι απαραίτητη η δήλωση του στο Manifest αρχείο της, αλλά επίσης, και η έγκριση από τον χρήστη. Μέχρις ότου ο χρήστης εγκρίνει το permission, η εφαρμογή δεν μπορεί να παρέχει λειτουργίες που εξαρτώνται από αυτό το συγκεκριμένο permission.

Τα permission groups τα οποία θεωρούνται ως Dangerous από το Android είναι τα εξής:[26][27]

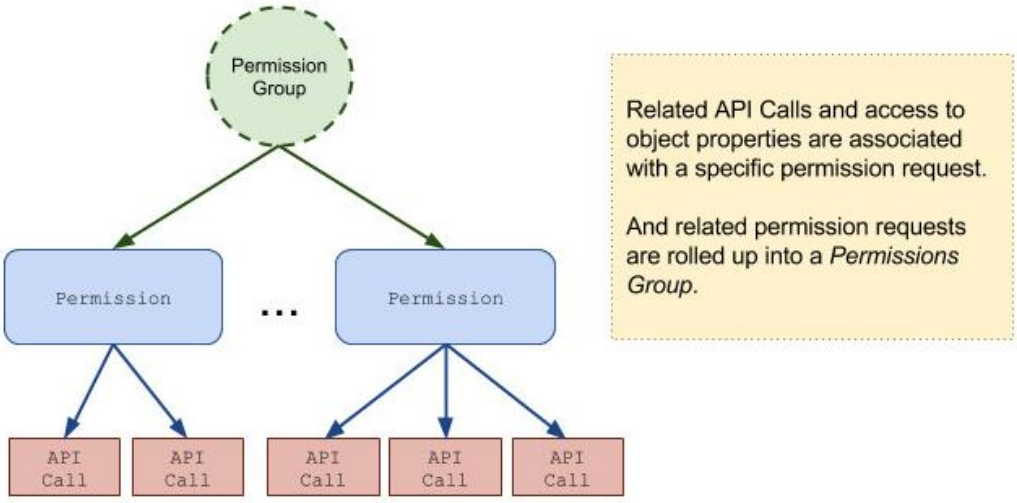
- Body Sensors – Επιτρέπουν την πρόσβαση σε δεδομένα που αφορούν την υγεία του χρήστη και τον αριθμό των βημάτων του καθώς και σε μετρητές καρδιακού ρυθμού, fitness trackers και άλλους αισθητήρες.
- Calendar – Επιτρέπει το διάβασμα, την δημιουργία, την επεξεργασία και την διαγραφή των διάφορων events του χρήστη, που βρίσκονται στο calendar του.
- Camera – Επιτρέπει την λήψη φωτογραφιών και εγγραφή βίντεο.
- Contacts – Επιτρέπει το διάβασμα, την δημιουργία και την επεξεργασία της λίστας επαφών του χρήστη. Επιπρόσθετα, έχει πρόσβαση στην λίστα όλων των λογαριασμών που χρησιμοποιούναι στη συσκευή του.
- Location – Επιτρέπει την πρόσβαση στην ακριβή τοποθεσία του χρήστη με χρήση GPS και στην κατά προσέγγιση τοποθεσία του με χρήση cellular data και Wi-Fi.
- Microphone – Επιτρέπει την εγγραφή ήχου, συμπεριλαμβανομένου και βίντεο.
- Phone – Επιτρέπει την πρόσβαση στον τηλεωνικό αριθμό του χρήστη και στα δεδομένα του δικτύου του, αφού είναι απαραίτητα για την πραγματοποίηση κλήσεων και VoIP, τον τηλεφωνητή, την ανακατεύθυνση κλήσεων και την επεξεργασία αρχείων καταγραφής κλήσεων.
- SMS – Επιτρέπει το διάβασμα, την λήψη και την αποστολή μηνυμάτων SMS και MMS.
- Storage – Επιτρέπει το διάβασμα και την εγγραφή αρχείων στο internal and external storage της συσκευής του χρήστη.

Το Signature protection level έχει σχέση με το application signing που αναφέρθηκε νωρίτερα. Ένα Signature permission χορηγείται από το σύστημα αυτόματα, χωρίς να ειδοποιεί τον χρήστη ή να ζητά τη ρητή έγκριση του, μόνο σε περίπτωση που η αιτούμενη εφαρμογή υπογράφεται με το ίδιο certificate με αυτό της εφαρμογής που έχει δηλωμένο το permission. Μια χρησιμότητα των permissions αυτού του επιπέδου αποτελεί η δυνατότητα δύο εφαρμογών, από τον ίδιο προγραμματιστή, να μοιράζονται δεδομένα χωρίς διακοπές και ενόχληση του χρήστη που τις έχει εγκαταστήσει στη συσκευή του.

Ένα SignatureOrSystem permission παρέχεται από το σύστημα μόνο σε εφαρμογές που περιλαμβάνονται στο Android Generic System Image (GSI) ή που έχουν υπογραφεί με το ίδιο certificate με την εφαρμογή που δηλώνει το permission. Είναι καλό να αποφεύγεται η χρήση των permissions που ανήκουν στο συγκεκριμένο επίπεδο, καθώς το Signature

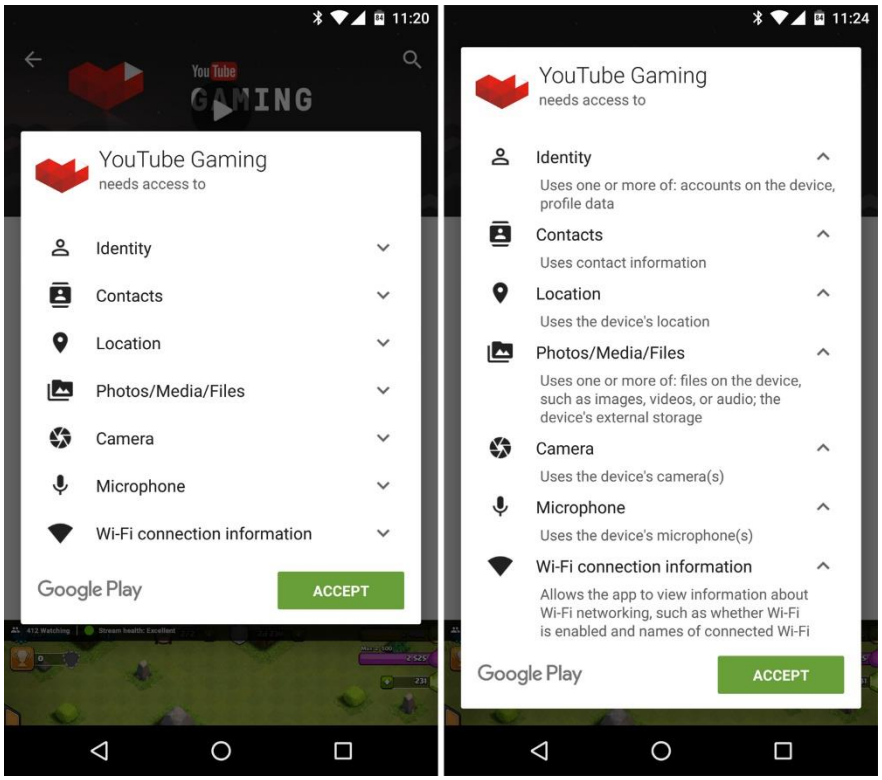
protection level είναι αρκετό για τις περισσότερες ανάγκες και εργασίες ανεξάρτητα από το που εγκαθίστανται οι εφαρμογές. Το SignatureOrSystem permission χρησιμοποιείται για ορισμένες ειδικές καταστάσεις όπου πολλοί προμηθευτές έχουν ενσωματωμένες εφαρμογές σε ένα system image και πρέπει να μοιράζονται συγκεκριμένα χαρακτηριστικά εξαιτίας του ότι είναι κατασκευασμένες μαζί.

Permissions, τα οποία είναι σχετικά μεταξύ τους, ομαδοποιούνται σε permission groups. Η ομαδοποίηση τους, με αυτόν τον τρόπο, επιτρέπει στον χρήστη να κάνει πιο σωστές και εύλογες επιλογές, χωρίς να είναι συγκλονισμένος από σύνθετες και τεχνικές αιτήσεις permissions. Επιπρόσθετα, επιτρέπει στον προγραμματιστή μιας εφαρμογής να ζητήσει μόνο την ελάχιστη απαιτούμενη ποσότητα permissions ανά πάσα στιγμή. Όταν μια εφαρμογή χρειάζεται ένα permission που ανήκει σε ένα συγκεκριμένο permission group (π.χ. READ_CONTACTS), το Android ζητά την έγκριση του χρήστη για την ομάδα υψηλότερου επιπέδου στην οποία ανήκει το permission (CONTACTS). Έτσι, όταν η εφαρμογή αργότερα χρειάζεται το permission WRITE_CONTACTS, το Android μπορεί αυτόματα να το παραχωρήσει χωρίς να το ζητήσει από τον χρήστη.[24]



Σχήμα 3

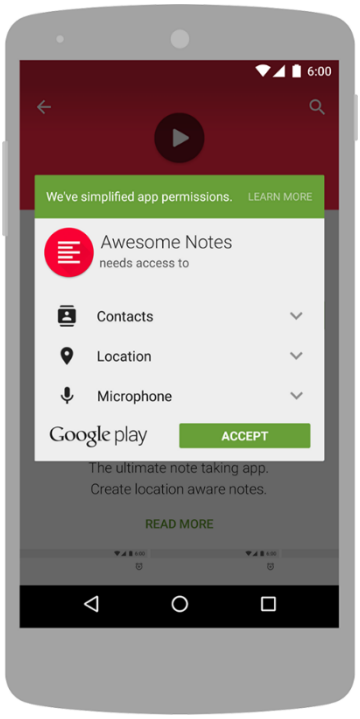
Όπως παρουσιάζεται στο Σχήμα 3, όταν ένας προγραμματιστής έχει σκοπό να ζητήσει ένα permission για την εφαρμογή του, πρέπει να αλληλεπιδράσει με τα APIs που αφορούν συνήθως το ίδιο το permission και όχι το permission group στο οποίο ανήκει.



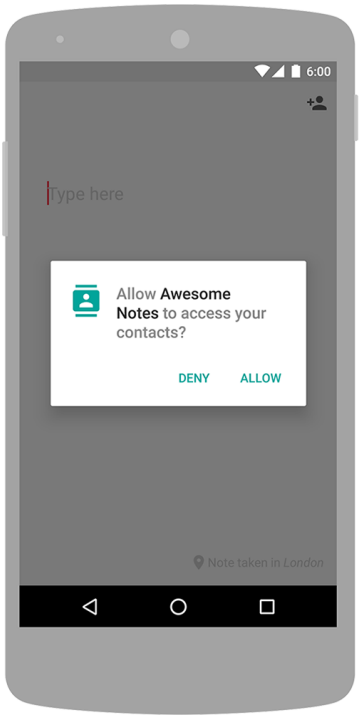
Σχήμα 4

Σε προηγούμενες κυκλοφορίες συσκευών από το Android Marshmallow (< Android 6.0 ή API 23), όλα τα permissions που απαιτούνται για την ομαλή λειτουργία μιας εφαρμογής καθορίζονται από τον προγραμματιστή στο Manifest file της. Κατά την εγκατάσταση της εφαρμογής το σύστημα ειδοποιεί τον χρήστη πως η εφαρμογή απαιτεί ένα συγκεκριμένο σύνολο permissions με σκοπό να δώσει την έγκριση του. Αυτός, με την σειρά του, έχει την δυνατότητα είτε να αποδεχτεί τα αιτούμενα permissions, πατώντας το κουμπί “ACCEPT”, είτε να τα απορρίψει, πατώντας το κουμπί back και ακυρώνοντας την εγκατάσταση της εφαρμογής ταυτόχρονα. Η διαδικασία που μόλις περιγράφτηκε παρουσιάζεται Σχήμα 5. Όταν μια εγκατεστημένη εφαρμογή πρόκειται να αναβαθμιστεί, υπάρχει περίπτωση να χρειάζεται νέα permissions. Ο τρόπος με τον οποίο ζητά αυτά τα permissions φαίνεται στο Σχήμα 4. Εάν ο χρήστης δεν θέλει να τα αποδεχτεί τότε ακυρώνεται η αναβάθμιση.

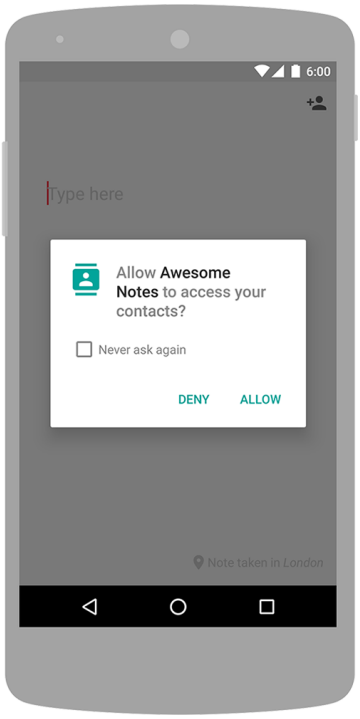
Το κύριο μειονέκτημα αυτής της προσέγγισης είναι ότι η Google δεν ελέγχει κατά πόσο μια εφαρμογή όντως χρειάζεται τα αιτούμενα permissions της για την ομαλή λειτουργία της ούτε ο χρήστης έχει την επιλογή να απορρίπτει ορισμένα permissions με αποτέλεσμα να αναγκάζεται να τα αποδεχτεί όλα, με σκοπό να χρησιμοποιήσει την εφαρμογή. Συνεπώς, οι προγραμματιστές μπορούν να προσθέτουν permissions τα οποία δεν απαιτούνται για τη λειτουργία μιας εφαρμογής, permissions τα οποία δεν εξυπηρετούν άλλο σκοπό παρά τη συλλογή δεδομένων, παραβιάζοντας το απόρρητο του χρήστη.



Σχήμα 5



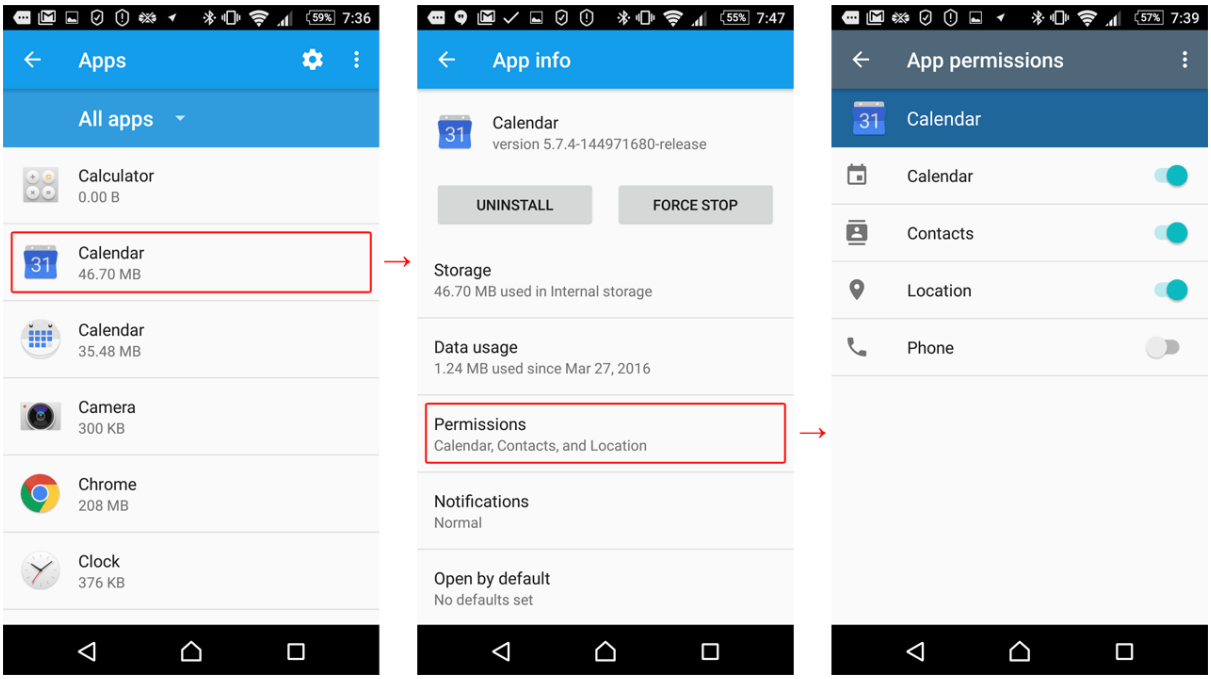
Σχήμα 6



Σχήμα 7

Με τη δημόσια κυκλοφορία του Android Marshmallow, η Google εισήγαγε την έννοια των runtime permissions στο Android, αλλάζοντας έτσι το τοπίο των permissions προς το καλύτερο. Σε συσκευές με έκδοση >= Android 6.0 ή API 23, ο χρήστης δεν ενημερώνεται πλέον για τα permissions που χρειάζεται μια εφαρμογή κατά την εγκατάσταση της στην συσκευή του. Αντί αυτού, η εφαρμογή ζητάει την έγκριση για ένα permission group την στιγμή που προσπαθεί ο χρήστης να χρησιμοποιήσει για πρώτη φορά την λειτουργία που το απαιτεί. Η διαδικασία αυτή πραγματοποιείται με τον τρόπο που παρουσιάζεται στο Σχήμα 6. Εμφανίζεται ένα system dialog στην οθόνη του χρήστη, που τον ειδοποιεί σχετικά με το permission group στο οποίο προσπαθεί να αποκτήσει πρόσβαση η εφαρμογή. Το παράθυρο περιλαμβάνει δύο κουμπιά, το “DENY” και το “ALOW”. Εάν ο χρήστης πατήσει το κουμπί “ALLOW” τότε η εφαρμογή έχει το δικαίωμα να χρησιμοποιεί το συγκεκριμένο permission group. Σε περίπτωση, όμως, που πατήσει το κουμπί “DENY”, την επόμενη φορά που ο χρήστης θα προσπαθήσει να χρησιμοποιήσει τη συγκεκριμένη λειτουργία θα εμφανιστεί το system dialog με μια επιπλέον επιλογή. Η εν λόγω επιλογή παρέχει δυνατότητα στο χρήστη να επιλέξει να μην ερωτάται στο μέλλον για την παροχή άδειας χρήσης του συγκεκριμένου permission group (Σχήμα 7).

Οι Android συσκευές με >= API 26, παρέχουν επίσης την επιλογή στο χρήστη να ενεργοποιεί και να απενεργοποιεί τα permission groups ένα-ένα μέσω των ρυθμίσεων του συστήματος. (Σχήμα 8)



Σχήμα 8

3.3 Δομή του Application Package Kit (APK)

Ένα Android Package Kit (APK) [28] [29] είναι ένα αρχείο σε μορφή συμπιεσμένου πακέτου με επέκταση .apk, που χρησιμοποιείται από το λειτουργικό σύστημα Android για τη διανομή και εγκατάσταση εφαρμογών σε κινητές συσκευές. Ακριβώς όπως τα συστήματα Windows (PC) χρησιμοποιούν ένα αρχείο .exe για την εγκατάσταση λογισμικού, έτσι και το σύστημα Android κάνει το ίδιο με το αρχείο .apk. Η πλειοψηφία των χρηστών απευθύνεται στο Google Play Store με σκοπό την εγκατάσταση μιας εφαρμογής στην συσκευή τους. Ταυτόχρονα, όμως, υπάρχουν και περιπτώσεις στις οποίες οι χρήστες πραγματοποιούν την παραπάνω εργασία με την λήψη του αρχείου .apk της εφαρμογής.

Ένα Android Package Kit περιλαμβάνει τα εξής συστατικά; classes.dex, res/, resources.arsc, AndroidManifest.xml, libs/, assets/ και META-INF/. (Σχήμα 9) [31]

- classes.dex: Μια Android εφαρμογή αποτελείται συνήθως από αρχεία με επέκταση .java, τα οποία μεταγλωττίζονται από το Java Virtual Machine (JVM) με αποτέλεσμα την δημιουργία αρχείων .class. Στην συνέχεια, αυτά τα αρχεία μετατρέπονται σε Dalvik executables (.dex) από το Dalvik Virtual Machine (DVM), πριν την εγκατάσταση της εφαρμογής στην συσκευή του χρήστη. Ο τρόπος σχεδίασης των

Dalvik executables εξυπηρετεί συστήματα τα οποία περιορίζονται από άποψη μνήμης και ταχύτητας επεξεργαστή.

- res/: Το res/ είναι ένας φάκελος που περιέχει τους περισσότερους πόρους XML (π.χ. layouts) και τα drawables (π.χ. PNG, JPEG) μιας εφαρμογής, σε φακέλους που καθορίζουν τα densities (π.χ. -mdpi, -hdpi), τα μεγέθη οθόνης (π.χ. -sw600dp, -large) και τις γλώσσες (π.χ. -en, -de, -pl). Ο φάκελος αυτός περιέχει τα στοιχεία που δεν μεταγγλωτίστηκαν στο αρχείό resources.arsc.

- resources.arsc: Ένα μερίδιο των πόρων μιας εφαρμογής (π.χ. XML αρχεία) μεταγλωττίζονται και προσθέτονται σε αυτό το αρχείο. Το resources.arsc κανονικά φυλάγεται χωρίς συμπίεση μέσα στο APK με σκοπό την γρηγορότερη πρόσβαση κατά τη διάρκεια της εκτέλεσης του.

- AndroidManifest.xml: Το AndroidManifest.xml είναι ένα αρχείο που κάθε Android εφαρμογή έχει στην κατοχή της καθώς περιλαμβάνει την περιγραφή σημαντικών πληροφοριών που αφορούν την ίδια την εφαρμογή. Αυτές οι πληροφορίες είναι χρήσιμες για τα Android build tools, το λειτουργικό σύστημα Android και φυσικά το Google Play Store. Κάποιες από τις πληροφορίες που είναι απαραίτητο να δηλώνονται στο συγκεκριμένο αρχείο είναι οι εξής:
    - Το package name της εφαρμογής καθώς και το ID της, το οποίο χρησιμοποιείται ως μοναδικό αναγνωριστικό για το σύστημα και το Google Play Store.
    - Τα συστικά της εφαρμογής τα οποία περιλαμβάνουν όλα τα activities, services, broadcast receivers και content providers.
    - Τα permissions τα οποία χρειάζεται η εφαρμογή για να έχει πρόσβαση σε προστατευόμενα μέρη του σύστηματος και άλλων εφαρμογών.
    - Τα χαρακτηριστικά υλικού και λογισμικού που απαιτούνται από την εφαρμογή για την ομαλή λειτουργία της.

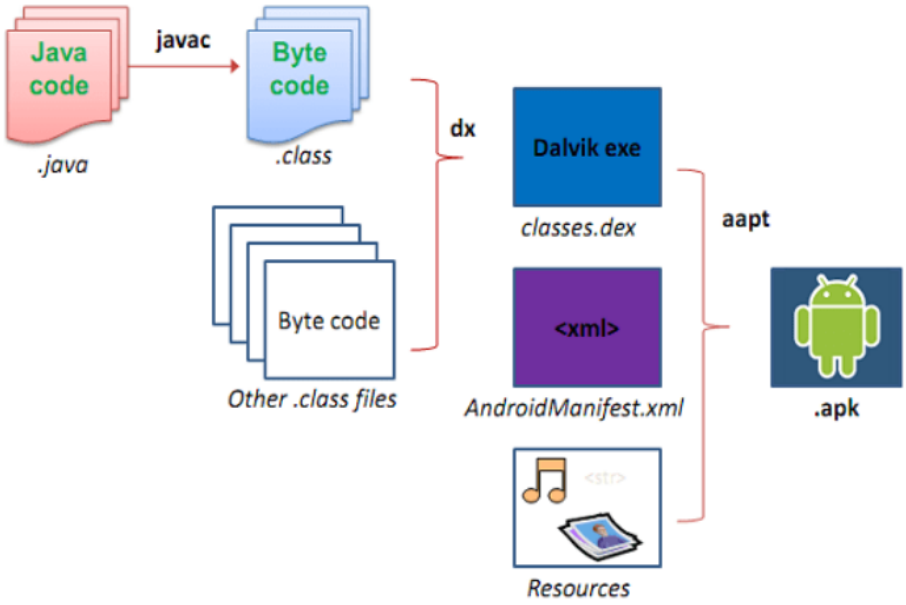
  Παρόμοια με άλλα XML αρχεία, το AndroidManifest.xml μετασχηματίζεται κατά τη μεταγλώττιση του σε αρχείο δυαδικής μορφής.

- libs/: Ο φάκελος libs/ περιέχει όλα τα native libraries μιας εφαρμογής, τοποθετημένα σε υποφακέλους οι οποίοι έχουν ονομαστεί με βάση το Application Binary Interface

(ABI) του CPU architecture που στοχεύουν. Για παράδειγμα, το armeabi αφορά τους επεξεργαστές ARM.

- assets/: Στον φάκελο assets/ τοποθετούνται διάφορα αρχεία τα οποία χρησιμοποιούνται σαν ακατέργαστα δεδομένα από την εφαρμογή και γι'αυτό τον λόγο δεν ανήκουν στα resources της. Παραδείγματα αρχείων αυτού του φακέλου είναι τα εξής; fonts, xml, text, αρχεία μουσικής και βίντεο. Με σκοπό την ανάγνωση και την χρήση των assets, γίνεται χρήση του AssetManager.

- META-INF/: Ο φάκελος META-INF/ περιέχει πληροφορίες για το manifest αρχείο και άλλα metadata που αφορούν το java package της εφαρμογής.
  - MANIFEST.MF: Περιέχει διάφορες πληροφορίες που χρησιμοποιούνται από το runtime περιβάλλον της Java κατά την φόρτωση του αρχείου jar της εφαρμογής. Κύριο μέρος των πληροφοριών αποτελεί η λίστα των ονομάτων των αρχείων του jar μαζί με τα SHA1 digests τους. (Σχήμα 10)
  - CERT.SF: Περιέχει όλη την λίστα των αρχείων του jar μαζί με τα SHA1 digests τους.
  - CERT.RSA: Περιλαμβάνει τα υπογραμμένα περιεχόμενα του αρχείου CERT.SF συνοδευμένα από το certificate τους.



Σχήμα 9

```
Manifest-Version: 1.0
Built-By: Generated-by-ADT
Created-By: Android Gradle 3.0.1

Name: AndroidManifest.xml
SHA1-Digest: +hyHktVNz+f2C+4ej4DdgQZv0jU=

Name: META-INF/INDEX.LIST
SHA1-Digest: nvBRGZAGJFSBbkDtKE9dogbdrNw=

Name: META-INF/ViberLibrary_release.kotlin_module
SHA1-Digest: o2H3+Ji0gffQ+23I88BZY6qYDMg=

Name: META-INF/android.arch.core_runtime.version
SHA1-Digest: OxxKFJcpzAROGjnfMbNijNv1+JU=
```

Σχήμα 10

3.4 Προβλήματα ασφάλειας στο Android

Η φιλοσοφία ανοιχτού κώδικα του Android παρέχει την δυνατότητα εγκατάστασης third-party εφαρμογών, τις οποίες μπορεί να ανακτήσει ο χρήστης μέσα από ανεπίσημα markets καθώς και από το Google Play Store. Αρκετά από τα Android markets δεν διαθέτουν πολιτικές αναφορικά με την ποιότητα των εφαρμογών που κυκλοφορούν. Ταυτόχρονα, το ίδιο το Android δεν προσφέρει κάποιου είδους εγγύηση για τυχούσες ζημιές που μπορεί να προκαλέσει μια εφαρμογή. Ως αποτέλεσμα, μερικοί προγραμματιστές, εκμεταλλεύονται την υφιστάμενη κατάσταση προς το συμφέρον τους, κυκλοφορώντας εφαρμογές κακόβουλου λογισμικού. Μέσω των κακόβουλων εφαρμογών αυτών, οι δημιουργοί τους εκμεταλλεύονται τυχόν ευάλωτα σημεία άλλων εφαρμογών ώστε να ανακτήσουν προσωπικά δεδομένα χρηστών, τα οποία στη συνέχεια δημοσιοποιούν, έχοντας ως απώτερο σκοπό να προκαλέσουν βλάβη σε κάποιο Android market ή και στην φήμη άλλου προγραμματιστή.

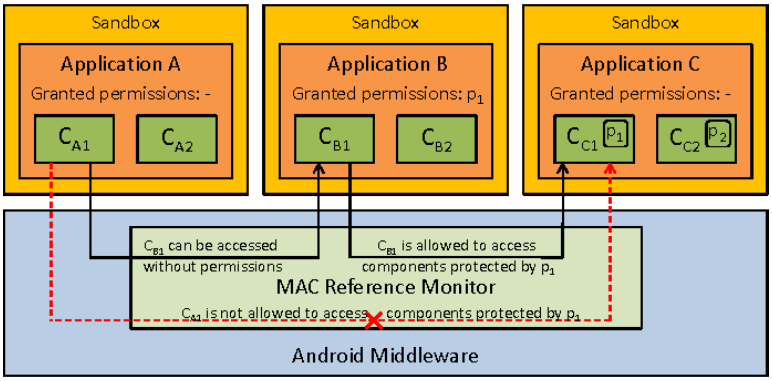
Ακολουθεί μια λίστα με τεχνικές που χρησιμοποιούνται από κακόβουλες εφαρμογές και αποτελούν μεγάλο κίνδυνο για το Android και φυσικά την ιδιωτικότητα των χρηστών του. [30]

- Privacy leakage ή personal-information theft: Αυτό το φαινόμενο παρατηρείται σε περιπτώσεις που οι χρήστες, εν αγνοία τους, επιτρέπουν σε κακόβουλες εφαρμογές την πρόσβαση σε ευαίσθητα δεδομένα τους, με την αποδοχή των dangerous permission groups που ζητούν οι εφαρμογές αυτές. Άρα είναι προφανές πως εναπόκειται στους ίδιους τους χρήστες ο τρόπος με τον οποίο θα χειριστούν τα permissions που ζητούνται από τις εφαρμογές που εγκαθιστούν στις συσκευές τους.

- Denial of Service attack (DOS): Πρόκειται για ένα είδος ηλεκτρονικής επίθεσης η οποία εξαντλεί τους πόρους μιας εφαρμογής παράγωντας ψηλό ή χαμηλό ρυθμό

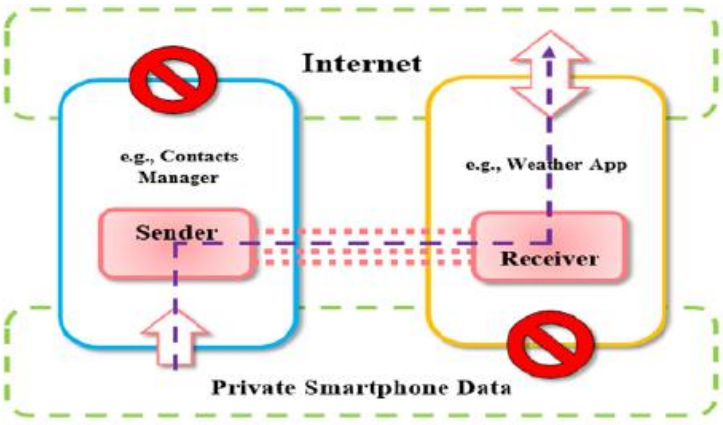
ποσοστό attack traffic. Με αυτό τον τρόπο ο χρήστης αδυνατεί να χρησιμοποιήσει την εφαρμογή κανονικά.

- Privilege escalation attack: Στη κατηγορία αυτή εμπίπτει οποιαδήποτε εκμετάλλευση υπάρχοντος σφάλματος σε μια εφαρμογή με σκοπό την πρόσβαση σε πόρους, με τους οποίους κανονικά δεν μπορεί να έρθει σε επαφή αφού είναι προστατευόμενοι από κάποια εφαρμογή ή χρήστη. Στο Σχήμα 11, παρουσιάζεται το συστατικό C_{A1} που μέσω ενός privilege escalation attack έχει πρόσβαση στο C_{c1}.



Σχήμα 11

- Application collusion attack: Πρόκειται για συνωμοσία εφαρμογών που έχουν ως σκοπό την παραβίαση κάποιας ασφάλειας που υπάρχει στο Android σύστημα. Ο τρόπος με τον οποίο οι εφαρμογές επιτυγχάνουν την εκτέλεση κακόβουλων δραστηριοτήτων και την πρόσβαση σε πόρους του συστήματος είναι η δημιουργία νέων ή η χρήση ήδη υπάρχοντων καναλιών επικοινωνίας μεταξύ τους. Στο Σχήμα 12, παρατηρούμε πως ο Contacts Manager έχει πρόσβαση μόνο στις επαφές του χρήστη. Ενώ το Weather Application έχει πρόσβαση μόνο στο δίκτυο. Έτσι μέσω ενός καναλιού επικοινωνίας ο Contacts Manager προωθεί τις επαφές στο Weather application ώστε αυτό να τα μεταφέρει σε κάποιον attacker. [35]



Σχήμα 12

Κεφάλαιο 4

Σχετικές εργασίες

4.1 Εισαγωγή

Οι κίνδυνοι που πηγάζουν από το συνεχώς αναπτυσσόμενο περιβάλλον των κακόβουλων Android εφαρμογών σχετίζονται άμεσα με τα προσωπικά δεδομένα των χρηστών και γενικότερα την ιδιωτικότητα τους. Αυτοί οι κίνδυνοι έχουν τραβήξει την προσοχή και έχουν προβληματίσει διάφορες ομάδες ερευνητών και προγραμματιστών με αποτέλεσμα να μελετήσουν εις βάθος το σύστημα του Android και να δημιουργήσουν εφαρμογές ή γενικότερα λογισμικό με σκοπό την προστασία των προσωπικών δεδομένων και την βελτίωση κατανόησης των χρηστών σε θέματα πρόσβασης από τα Android permissions. Στα επόμενα υποκεφάλαια περιγράφονται δύο εφαρμογές οι οποίες σχετίζονται σε μεγάλο βαθμό με το εν λόγω θέμα και με την εφαρμογή PermExtractor της παρούσας διπλωματικής εργασίας καθώς και συγκρίνονται με αυτή.

4.2 AppGuard [32][33]

Το AppGuard αποτελεί ένα εργαλείο βασισμένο στο inline reference monitoring (IRM), το οποίο επιτρέπει στον χρήστη να επιβάλλει λεπτομερείς πολιτικές ασφάλειας και ιδιωτικότητας σε third-party εφαρμογές.

Κάθε φορά που πραγματοποιείται η εγκατάσταση μιας εφαρμογής στην συσκευή ενός χρήστη, το σύστημα τον προτρέπει μέσω ειδοποίησης να το ασφαλίσει. Με το πάτημα της εν λόγω ειδοποίησης, ο χρήστης μεταφέρεται στην οθόνη όπου λαμβάνει μέρος η διαδικασία σάρωσης και επανεγγραφής της στοχευμένης εφαρμογής, η απεγκατάσταση της αυθεντικής εφαρμογής και η εγκατάσταση της τροποποιημένης. Μετά το τέλος της παραπάνω διαδικασίας, το AppGuard προτρέπει τον χρήστη να χορηγήσει στην νέα τροποποιημένη

εφαρμογή τα νέα permissions και να διαμορφώσει τις προκαθορισμένες πολιτικές ασφάλειας. Σημαντικό να αναφερθεί πως το AppGuard καταγράφει επίσης όλες τις σχετικές λειτουργίες με την ασφάλεια που πραγματοποιούνται από τις εφαρμογές. Έτσι, ο χρήστης ενημερώνεται γι'αυτές και πράττει ανάλογα στην ρύθμιση των πολιτικών διαμόρφωσης της κάθε εφαρμογής.

Ένα κύριο σημείο της υλοποίησης της συγκεκριμένης εφαρμογής είναι ο rewriter. Αρχικά, παίρνει το υπάρχον APK αρχείο μιας εφαρμογής, εξάγει το αντίστοιχο classes.dex αρχείο και το αποσυναρμολογεί. Αφού πραγματοποιηθεί η ανάλυση του τροποποιημένου κώδικα assembly, ο rewriter συγχωνεύει τους ελέγχους ασφαλείας που καθορίζονται από την προκαθορισμένη πολιτική στον υπάρχοντα κώδικα της εφαρμογής. Στο τέλος, επανασυναρμολογεί το αρχείο classes.dex και ανασυσκευάζει το APK αρχείο.

Η εφαρμογή αυτή δεν ανανεώνεται πλέον όμως μπορεί να χρησιμοποιηθεί ως βάση για τις μελλοντικές εργασίες της Android εφαρμογής PermExtractor αφού χρησιμοποιεί μια έξυπνη τεχνική για την τροποποίηση των permissions στις εφαρμογές του χρήστη βασιζόμενη σε κάποιες πολιτικές ασφάλειας.

Σχήμα 13

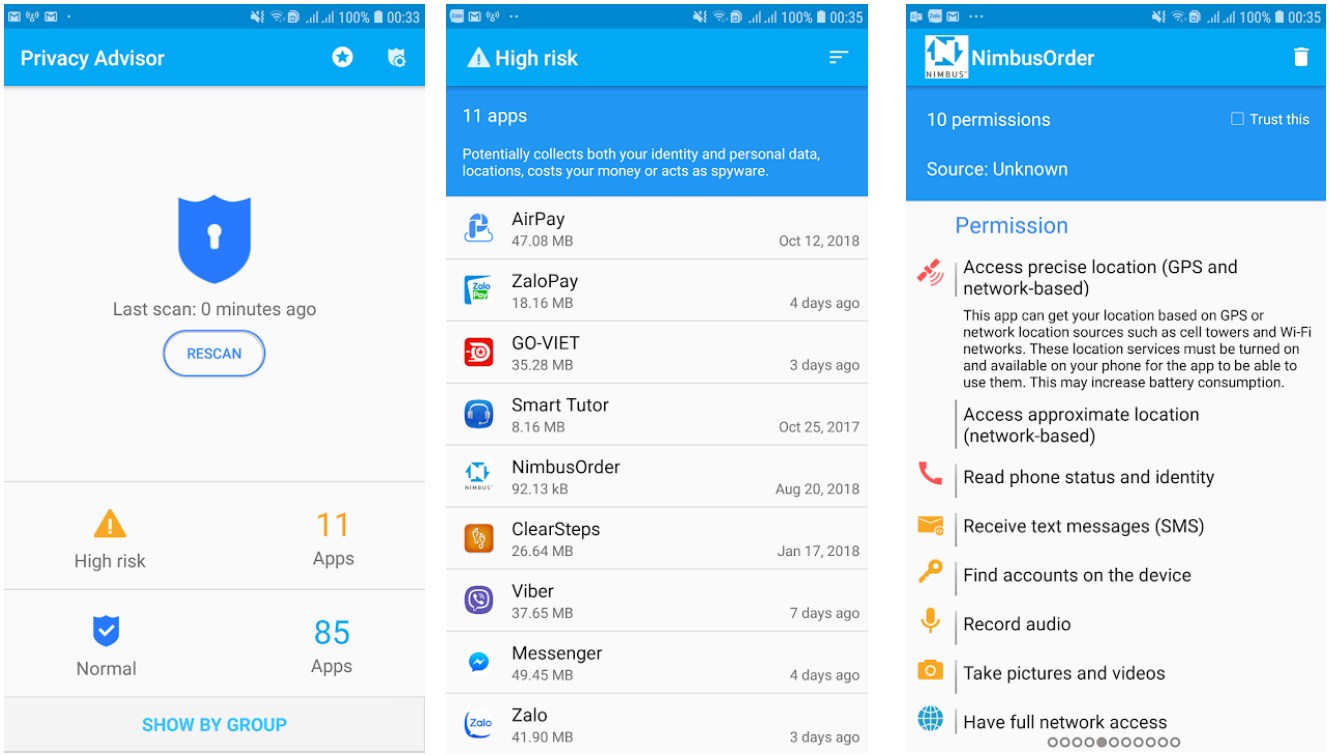
4.3 Privacy Advisor Pro (Checker Permissions) [34]

Το Privacy Advisor Pro αποτελεί μια Android εφαρμογή η οποία παρέχει την δυνατότητα στον χρήστη να ελέγξει λεπτομερώς τα permissions όλων των εφαρμογών της συσκευής του.

Η ανακάλυψη διάφορων εφαρμογών που χρησιμοποιούν κάποιο Ad Network είναι μια ακόμη λειτουργία της συγκεκριμένης εφαρμογής. Παράλληλα, διαθέτει επεξηγήσεις για τα σημαντικά permissions και εκθέτει εφαρμογές που έχουν ως στόχο την κατασκοπεία άλλων. Η εφαρμογή Privacy Advisor Pro έχει την δυνατότητα να πραγματοποιήσει σάρρωση των permissions μια εφαρμογής σε πραγματικό χρόνο και να διαχωρίσει τις εφαρμογές του χρήστη σε high-risk και normal. Στόχος της εφαρμογής, είναι η σάρωση και η ανακάλυψη των απειλών όσον αφορά τα προσωπικά δεδομένα των χρηστών.

Ο κώδικας της συγκεκριμένης εφαρμογής δεν βρίσκεται κάπου δημοσιευμένος οπότε δεν υπήρξε η δυνατότητα εξέτασης και κατανόησης του τρόπου υλοποίησης της.

Η εφαρμογή Privacy Advisor Pro είναι αρκετά παρόμοια με τον PermExtractor αφού έχει και αυτή ως στόχο την βελτίωση κατανόησης των χρηστών περί permissions στα Android και την διαφύλαξη της ιδιωτικότητας του. Ταυτόχρονα όμως, ασχολείται και με normal permissions κάτι το οποίο δεν είναι απαραίτητο, αφού δεν διατρέχουν κάποιο κίνδυνο για τον χρήστη. Επίσης, διαθέτει εντοπισμό εφαρμογών που χρησιμοποιούν κάποιο Ad Network ή API. Αυτό που παραλείπεται σε σύγκριση με τον PermExtractor, είναι κάποιου είδους app recommender ή τρόπος να ορίζει ο χρήστης τις προτιμήσεις του όσον αφορά τα permissions που χρησιμοποιούν οι εφαρμογές.



Σχήμα 14

Κεφάλαιο 5

Τεχνολογίες και εργαλεία

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζονται οι διάφορες γλώσσες προγραμματισμού καθώς και τα εργαλεία που χρησιμοποιήθηκαν με σκοπό την ανάλυση και την ανάπτυξη της Android εφαρμογής PermExtractor. Πιο συγκεκριμένα, αναλύεται ο τρόπος με τον οποίο βοήθησαν τα εργαλεία αυτά στην ανάπτυξη του συστήματος αλλά και ο τρόπος λειτουργίας των ιδίων. Όσον αφορά τις γλώσσες προγραμματισμού, καταγράφονται λίγα λόγια για την κάθε μια και το σημείο στο οποίο έγινε η χρήση τους μέσα στον κώδικα.

5.2 Γλώσσες Προγραμματισμού

5.2.1 Java/Kotlin

Η Java είναι μια αντικειμενοστρεφής γλώσσα προγραμματισμού της οποίας η γνώση είναι άκρως απαραίτητη για σκοπούς ανάπτυξης μιας εφαρμογής στο Android Studio (IDE). Θεωρείται μια ασφαλής γλώσσα εξαιτίας του ότι όλος ο κώδικας τρέχει εντός της JVM. Η JVM είναι μια εικονική μηχανή της οποίας ο σκοπός είναι να παρέχει στα Java προγράμματα την ευκολία να τρέχουν σε κάθε συσκευή και λειτουργικό σύστημα ενώ ταυτόχρονα

διαχειρίζεται την μνήμη που χρησιμοποιούν. Η Java διαθέτει ένα πλούσιο φάσμα λειτουργιών που συντηρούνται και ανανεόνται από την Oracle αλλά και ένα μεγάλο αριθμό κλάσεων και frameworks. Οι προγραμματιστές μπορούν να αξιοποιήσουν αυτές τις ιδιότητες στις εφαρμογές τους. [35-37]

Η Kotlin υποστηρίζεται επίσημα από την Google για ανάπτυξη Android εφαρμογών. Πρόκειται για μια cross-platform, γενικής χρήσης και statically-typed γλώσσα προγραμματισμού. Είναι σχεδιασμένη έτσι ώστε να μπορεί να διαλειτουργεί με την Java. Ταυτόχρονα, η έκδοση του JVM της standard lbrary της Kotlin βασίζεται στην class library της Java. Ένα πλεονέκτημα της αποτελεί η σύνταξη της η οποία είναι αρκετά συνοπτική σε σύγκριση με της Java. [38]

Στην παρούσα διπλωματική εργασία η Java καθώς και η Kotlin αποτελούν τις κύριες γλώσσες προγραμματισμού για την ανάπτυξη της εφαρμογής PermExtractor.

5.2.2 Python [39][40]

Η Python είναι μια υψηλού επιπέδου γλώσσα προγραμματισμού η οποία έχει ως κύρια χαρακτηριστικά της την ευκολία στο να την διαβάσει κάποιος αλλά και να γράψει κώδικα σε αυτήν, την φορητότητα της και το μεγάλο εύρος των βιβλιοθηκών που προσφέρει. Επιπρόσθετα, η συγκεκριμένη γλώσσα προγραμματισμού ανήκει στην κατηγορία Free/Libre and Open Source Software. Αυτό σημαίνει ότι ο πηγαίος κώδικας της είναι διαθέσιμος στο κοινό ώστε ο καθένας να μπορεί να τον τροποποιήσει και να τον διανέμει.

Ο κώδικας ενός από τα εργαλεία που χρησιμοποιήθηκαν στην παρούσα διπλωματική εργασία, του M-Perm Tool, είναι ανεπτυγμένος πάνω σε Python. Τα διάφορα πλεονεκτήματα της βοήθησαν στην κατανόηση της λειτουργίας του κώδικα του εργαλείου και στην προσαρμογή του στο τελικό σύστημα με σκοπό την εκμετάλλευση του.

5.2.3 PHP [41]

Η PHP – PHP Hypertext Preprocessor – αποτελεί μια από τις πιο διαδεδομένες τεχνολογίες στο Παγκόσμιο Ιστό, καθώς χρησιμοποιείται από ένα πολύ μεγάλο αριθμό εφαρμογών και ιστότοπων. Η ευρύτατη χρήση της είναι αποτέλεσμα της ευκολίας που παρουσιάζει ο προγραμματισμός με αυτή αλλά και το γεγονός πως είναι μια γλώσσα η οποία υπάρχει σχεδόν σε όλους τους διακομιστές. Η ιστορία της PHP ξεκινά από το 1994, όταν ένας

φοιτητής, ο Rasmus Lerdorf δημιούργησε ένα απλό script με όνομα php.cgi, για προσωπική του χρήση. Το script αυτό είχε σαν σκοπό να διατηρεί μια λίστα στατιστικών για τα άτομα που έβλεπαν το online βιογραφικό του σημείωμα. Έτσι, σήμερα έχουμε φτάσει μέχρι και την PHP 7 την οποία και χρησιμοποιούν οι περισσότεροι ιστότοποι.

Η συγκεκριμένη γλώσσα προγραμματισμού χρησιμοποιήθηκε ευραίως στην δημιουργία των web services. Ουσιαστικά, ήταν το μέσο επικοινωνίας της Java και των εργαλείων M-Perm Tool και Google Play Scraper. Εντός του κώδικα της PHP γινόταν εκτέλεση των εντολών των εργαλείων για την απόκτηση του επιθυμητού αποτελέσματος. Επιπλέον, ένας άλλος κύριως τρόπος χρήσης της ήταν η ένωση που είχε με την βάση δεδομένων MySql από όπου μπορούσε να ανακτά, να εισάγει, να διαγράφει και να ανανεώνει δεδομένα.

5.2.4 Node.js [42]

Το Node.js αποτελεί μια πλατφόρμα ανάπτυξης λογισμικού δημιουργημένη σε περιβάλλον Javascript. Η ανάπτυξη του προέκυψε από την ανάγκη του Ryan Dahl να βρει τον πιο αποδοτικό τρόπο να ενημερώνει τον χρήστη, σε πραγματικό χρόνο, για την κατάσταση ενός αρχείου που ανέβαζε στο διαδίκτυο. Το κύριο χαρακτηριστικό του Node είναι η επίτευξη ασύγχρονης επικοινωνίας μεταξύ των υπολογιστικών πόρων. Αυτή η επικοινωνία πραγματοποιείται με χρήση συμβάντων (events) που διαθέτει η Javascript και ονομάζονται callbacks.
Στην παρούσα διπλωματική εργασία, το δεύτερο εργαλείο που χρησιμοποιήθηκε αποτελεί ένα Node.js module το οποίο απαιτεί άλλα ήδη υπάρχοντα modules που είναι γραμμένα σε Node.js.

5.3 Βάση Δεδομένων

5.3.1 MySQL [43][44]

Η MySQL αποτελεί το πιο διαδεδομένο Open Source SQL σύστημα διαχείρισης βάσεων δεδομένων του οποίου η ανάπτυξη και διανομή πραγματοποιείται από την Oracle Corporation. Το όνομά της είναι ένας συνδυασμός του "My", το όνομα της κόρης του Michael Widenius του συνιδρυτή του συστήματος, και της "SQL", της συντομογραφίας του Structured Query Language. Η MySQL έχει ένα μεγάλο πλεονέκτημα, αφού είναι δωρεάν, είναι συνήθως διαθέσιμη σε κοινόχρηστα πακέτα φιλοξενίας και μπορεί εύκολα να εγκατασταθεί σε περιβάλλον Linux, Unix και Windows.

Στην παρούσα διπλωματική εργασία έγινε χρήση της phpMyAdmin, η οποία είναι ένα δωρεάν και ανοιχτού κώδικα εργαλείο διαχείρισης για την MySQL. Σκοπός της ήταν η αποθήκευση δεδομένων που αφορούν την Android εφαρμογή PermExtractor. Πιο συγκεκριμένα, εκεί βρίσκονταν οι εφαρμογές των χρηστών μαζί με τα requested permissions που ανεβρίσκονταν κατά την διαδικασία ανάλυσης.

5.4 Εργαλεία

5.4.1 M-Perm [45]

Το M-Perm είναι ένα εργαλείο ανίχνευσης, το οποίο δημιουργήθηκε με σκοπό τον εντοπισμό των δικαιωμάτων που καταχράζονται οι Android εφαρμογές. Το εργαλείο αυτό έχει την δυνατότητα να ανακαλύπτει τα δικαιώματα που χρησιμοποιούνται από τις εφαρμογές συμπεριλαμβανομένων των αιτούμενων επικίνδυνων δικαιωμάτων (dangerous requested permissions) αλλά και των third party permissions.

Είναι σημαντικό να αναφερθεί πως η επιλογή χρήσης του συγκεκριμένου εργαλείου έγινε βάσει του ότι μπορεί να εντοπίζει τα underprivileged permissions, κατά την ανάλυση, τα οποία δεν είναι ορισμένα στο Manifest αρχείο αλλά αναφέρονται με κάποιο τρόπο μέσα στον πηγαίο κώδικα της κάθε εφαρμογής.

Επιπρόσθετα, το M-Perm είναι γραμμένο στην γλώσσα προγραμματισμού Python και εφαρμόζει reverse engineering πάνω στο Application Package Kit (APK) αρχείο των εφαρμογών. Σε περίπτωση που το μέγεθος του APK αρχείου είναι μεγάλο, η διαδικασία του reverse engineering μπορεί να χρειαστεί κάποια λεπτά μέχρι να ολοκληρωθεί.

Η διαδικασία ανάλυσης του εργαλείου χωρίζεται σε δύο μέρη. Αρχικά, χρησιμοποιώντας την εντολή decompile, δημιουργεί το ασυμπίεστο αρχείο από το APK κάποιας εφαρμογής. Το δεύτερο μέρος, βασίζεται στα δεδομένα των αρχείων που παράχθηκαν προηγουμένως και με την εντολή analyze, παράγει δύο αρχεία txt μορφής, τα οποία περιέχουν τα ορισμένα permissions του Manifest αρχείου, τα third party permissions και τα overprivileged και underprivileged dangerous permissions.

5.4.2 Google-Play-Scraper [46]

Το Google-Play-Scraper αποτελεί ένα Node.js module του οποίου η λειτουργικότητα είναι οργανωμένη σε διάφορα Javascript αρχεία. Σκοπός του εργαλείου αυτού είναι η απόξεση δεδομένων από το Google Play Store.

Το κύριο στοιχείο που διαφοροποιεί την απόξεση δεδομένων [47] από την κανονική ανάλυση είναι το ότι η έξοδος προορίζεται για εμφάνιση σε έναν τελικό χρήστη και όχι για είσοδο σε άλλο πρόγραμμα. Η απόκρυψη δεδομένων ουσιαστικά συνεπάγεται την αφαίρεση συνήθως εικόνων ή δεδομένων πολυμέσων, μορφοποίησης εμφάνισης, περιττών ετικετών, σχολίων και άλλων πληροφοριών που είτε είναι ασήμαντα είτε εμποδίζουν την αυτοματοποιημένη επεξεργασία.

Το Google-Play-Scraper διαθέτει μια λίστα από μεθόδους τις οποίες μπορεί να εκμεταλλευτεί ένας προγραμματιστής με σκοπό να αποκτήσει το είδος των πληροφοριών που ζητά από το Google Play Store.

Οι μέθοδοι που παρέχει είναι οι εξής:

- app: Ανάκτηση λεπτομερούς περιγραφής μιας Android εφαρμογής.
- list: Ανάκτηση συγκεκριμένου μεγέθους λίστας που περιέχει εφαρμογές μιας κατηγορίας και συλλογής του Google Play.
- search: Ανάκτηση συγκεκριμένου μεγέθους λίστας που περιέχει εφαρμογές που εμφανίζονται με αναζήτηση μιας λέξης.
- developer: Ανάκτησης λίστας εφαρμογών από ένα συγκεκριμένο προγραμματιστή.
- suggest: Ανάκτηση πιθανών αναζητήσεων με βάση έναν όρο που εισήγαγε ο χρήστης.
- reviews: Ανάκτηση ανασκοπήσεων για μια συγκεκριμένη εφαρμογή.
- similar: Ανάκτηση λίστας που περιέχει παρόμοιες εφαρμογές με αυτή που εισήγαγε ο χρήστης.
- permissions: Ανάκτηση των permissions που χρησιμοποιεί μια εφαρμογή αλλά και των περιγραφών τους.
- categories: Ανάκτηση λίστας εφαρμογών μιας συγκεκριμένης κατηγορίας.

Στην παρούσα διπλωματική εργασία, έγινε χρήση του εργαλείου Google-Play-Store, με στόχο την δημιουργία μιας διαδικασίας που συνιστά στον χρήστη παρόμοιες εφαρμογές με εκείνες που έχει ήδη εγκατεστημένες στην συσκευή του, αλλά βρίσκονται εν αρμονία με τις προτιμήσεις του, όσον αφορά τα permission groups που χρησιμοποιούν.

Μέχρι στιγμής, δεν υπάρχει κάποιο επίσημο Google Application Programming Interface (API) στο διαδίκτυο το οποίο να μπορεί να χρησιμοποιηθεί με στόχο την ανάκτηση πληροφοριών από το Google Play Store. Υπάρχουν κάποια ανεπίσημα Android Market APIs τα οποία δεν είναι βοηθητικά αφού χρειάζονται οπωσδήποτε εισαγωγή του ονόματος και του κωδικού του χρήστη με σκοπό να λειτουργήσουν. Ως αποτέλεσμα, το εργαλείο Google-Play-Scraper θεωρήθηκε το πιο κατάλληλο για την λειτουργία που έπρεπε να προσθεθεί στην Android εφαρμογή PermExtractor.

Κεφάλαιο 6

Υλοποίηση Android εφαρμογής PermExtractor

6.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζεται ο τρόπος με τον οποίο αναπτύχθηκε η Android εφαρμογή PermExtractor. Όλες οι λειτουργίες της εφαρμογής στηρίζονται σε αποτελέσματα που αφορούν την χρήση permissions από τις εγκατεστημένες εφαρμογές του χρήστη και τα οποία ανακτήθηκαν μέσω των εργαλείων M-Perm Tool και Google-Play-Scraper. Μια από τις εν λόγω λειτουργίες αποτελεί η δυνατότητα να επιλέγει ο χρήστης τα ιδανικά για εκείνον permissions στα οποία επιθυμεί οι εφαρμογές της συσκευής του να έχουν πρόσβαση. Ο χρήστης έχει ανά πάσα στιγμή την δυνατότητα να αλλάξει τις προτιμήσεις του.

Επίσης, ο χρήστης έχει την ευκαιρία να αναλύει τις εγκατεστημένες εφαρμογές και να ενημερώνεται για τα permission groups τους αλλά και τα permissions του κάθε group. Για κάθε permission προσφέρεται η αντίστοιχη επεξήγηση του, με σκοπό ο χρήστης να κατανοεί σε μεγαλύτερο βαθμό σε ποια προσωπικά δεδομένα του μπορεί να έχει πρόσβαση η εφαρμογή που απαιτεί το συγκεκριμένο permission.

Το PermExtractor βασισμένο στις προτιμήσεις του χρήστη αναφορικά με τα permission groups, χρωματίζει τις ανελυμένες εφαρμογές με πράσινο όταν τα permissions τους είναι σύμφωνα με αυτά του χρήστη και με μπλε όταν ισχύει το αντίθετο. Οι εφαρμογές που δεν έχουν αναλυθεί ακόμη χρωματίζονται με άσπρο. Έτσι διευκολύνεται η ενημέρωση του

χρήστη και δεν είναι απαραίτητο το να ελέγξει ένα-προς-ένα τα permission groups της κάθε εφαρμογής.
Το app recommender, που προσφέρεται από την εφαρμογή, αποτελεί μια πολύ σημαντική λειτουργία αφού δίνει την δυνατότητα στον χρήστη να επιλέξει μια εφαρμογή που έχει εγκατεστημένη στη συσκευή του και να ενημερωθεί για άλλες παρόμοιες υποψήφιες που θα μπορούσε να κατεβάσει και οι οποίες είναι σύμφωνες με τις προτιμήσεις του χρήστη όσον αφορά τα permission groups που ζητούν για την λειτουργία τους.

Στα παρακάτω υποκεφάλαια θα παρουσιαστεί ο τρόπος που υλοποιήθηκε η κάθε διαδικασία της εφαρμογής καθώς και ο τρόπος που χρησιμοποιήθηκε το κάθε εργαλείο.

6.2 Δυναμική ανάλυση permissions των εφαρμογών

Για να πραγματοποιηθεί η συγκεκριμένη ανάλυση χρησιμοποιήθηκε το εργαλείο M-Perm το οποίο είναι υλοποιημένο σε γλώσσα προγραμματισμού Python. Η επιλογή του συγκεκριμένου M-Perm έγινε βάσει του ότι δύναται να εντοπίσει permissions τα οποία είναι επικύνδινα και δηλωμένα μέσα στον κώδικα της εφαρμογής με αποτέλεσμα την μη ενημέρωση του χρήστη για την ύπαρξη τους.

Το εν λόγω εργαλείο παίρνει σαν είσοδο ένα APK αρχείο οποιασδήποτε εφαρμογής και εφαρμόζει δύο ειδών διαδικασίες σ'αυτό. Η πρώτη διαδικασία είναι εκείνη του decompiling όπου ουσιαστικά το APK αρχείο αποσυμπιέζεται από την .zip μορφή του με σκοπό να εξερευνηθούν τα περιεχόμενα του. Ο κώδικας που πραγματοποιεί το decompiling βρίσκεται σε ένα script αρχείο, το apk-decompiler.sh, το οποίο χρησιμοποιεί τους dex2jar, procyon και apktool decompilers ώστε να μετατρέψει το APK αρχείο σε ευανάγνωστα αρχεία πηγαίου κώδικα. Η δεύτερη διαδικασία βασίζεται σε αρχεία που παράγονται από την πρώτη. Από όλα τα αρχεία επιλέγεται η χρήση του AndroidManifest.xml αλλά και των .java αρχείων που βρίσκονται στον φάκελο src του project μιας εφαρμογής.

Κατά την δεύτερη διαδικασία αναλύεται η εφαρμογή ώστε να αποκαλυφθούν όλες οι κατηγορίες των permissions που χρησιμοποιεί. Η δημιουργία μιας δενδρικής δομής με τα περιεχόμενα του AndroidManifest.xml αποτελεί το αρχικό βήμα της ανάλυσης καθώς, στην συνέχεια, ακολουθεί ο έλεγχος του minimum sdk της εφαρμογής με σκοπό να γνωρίζει το εργαλείο εάν δύναται να ολοκληρώση την διαδικασία ανάλυσης. Σε μεταγενέστερο στάδιο, εντοπίζονται τα requested και τα third-party permissions μέσα από διάσχιση της δενδρικής δομής manifest_tree. Ο διαχωρισμός τους πραγματοποιείται βάσει του ονόματος τους αφού

τα third-party ξεκινούν με την λέξη “com”. Με στόχο να ανακαλυφθούν τυχόντα permissions που δηλώνονται μέσα στον κώδικα, δημιουργείται ένα αντικείμενο της κλάσης Analyze. Το αντικείμενο αυτό διαπερνά τον πηγαίο κώδικα μιας εφαρμογής προσπαθώντας να διακρίνει αν υπάρχουν συναρτήσεις σχετικές με την χρήση permissions που δεν δηλώνονται στο αρχείο AndroidManifest.xml.

Αφού συλλεχθούν όλες οι απαραίτητες πληροφορίες σχετικά με τα permissions μιας εφαρμογής δημιουργούνται δύο αρχεία με επέκταση .txt. Στην μία αναφορά περιλαμβάνονται τα permissions κατηγοριοποιημένα αλλά και οι γραμμές κώδικα που τυχών συλλέχθηκαν. Παράλληλα, στην άλλη εμπερικλείονται εξ’ολοκλήρου οι γραμμές κώδικα που κάνουν αναφορά σε permissions καθώς και τα αντίστοιχα ονόματα αρχείων στα οποία εντοπίστηκαν.

```
# Parse manifest and validate API
manifest_tree = get_manifest_tree(source_path)
validate_minimum_sdk(manifest_tree)

# Collect permissions
package_name = get_package_name(manifest_tree)
permissions = get_requested_permissions(manifest_tree)
third_party_permissions = get_third_party_permissions(manifest_tree)

# Scrape the source
analyzer = Analyze(source_path, package_name, permissions, ignore, str(api))
source_report = analyzer.search_project_root()

# Analyze and print results
report = Report(package_name, permissions, third_party_permissions)
report.print_analysis(permissions, source_report)
```

Σχήμα 15

6.2.1 Χρήση ανάλυσης ως λειτουργία της εφαρμογής

Μια από τις κύριες λειτουργίες, που διαθέτει το σύστημα, είναι η παρουσίαση των dangerous permissions που χρησιμοποιεί η κάθε εφαρμογή που εγκαταστήθηκε από τον ίδιο τον χρήστη στην Android συσκευή του. Ο λόγος για τον οποίο επικεντρώνεται μόνο στα dangerous permissions είναι εμφανής μόνο και μόνο από την ονομασία τους αφού διατρέχουν κίνδυνο για την ακεραιότητα των προσωπικών δεδομένων του χρήστη και συνεπώς για την διατήρηση της ιδιωτικότητας του. Σκοπός της συγκεκριμένης λειτουργίας είναι η βαθύτερη κατανόηση του χρήστη σχετικά με την έκταση πρόσβασης κάθε εφαρμογής στα προσωπικά του δεδομένα και η ενημέρωση του για εφαρμογές που θεωρούνται ιδιαίτερα επικύνδινες.

Αρχικά, μέσω ενός PHP web service, η εφαρμογή PermExtractor αναζητά να μάθει εάν η εφαρμογή που επιλέχθηκε από τον χρήστη είναι ήδη ανελυμένη ή όχι. Η μέθοδος που ακολουθείται είναι η εξής:

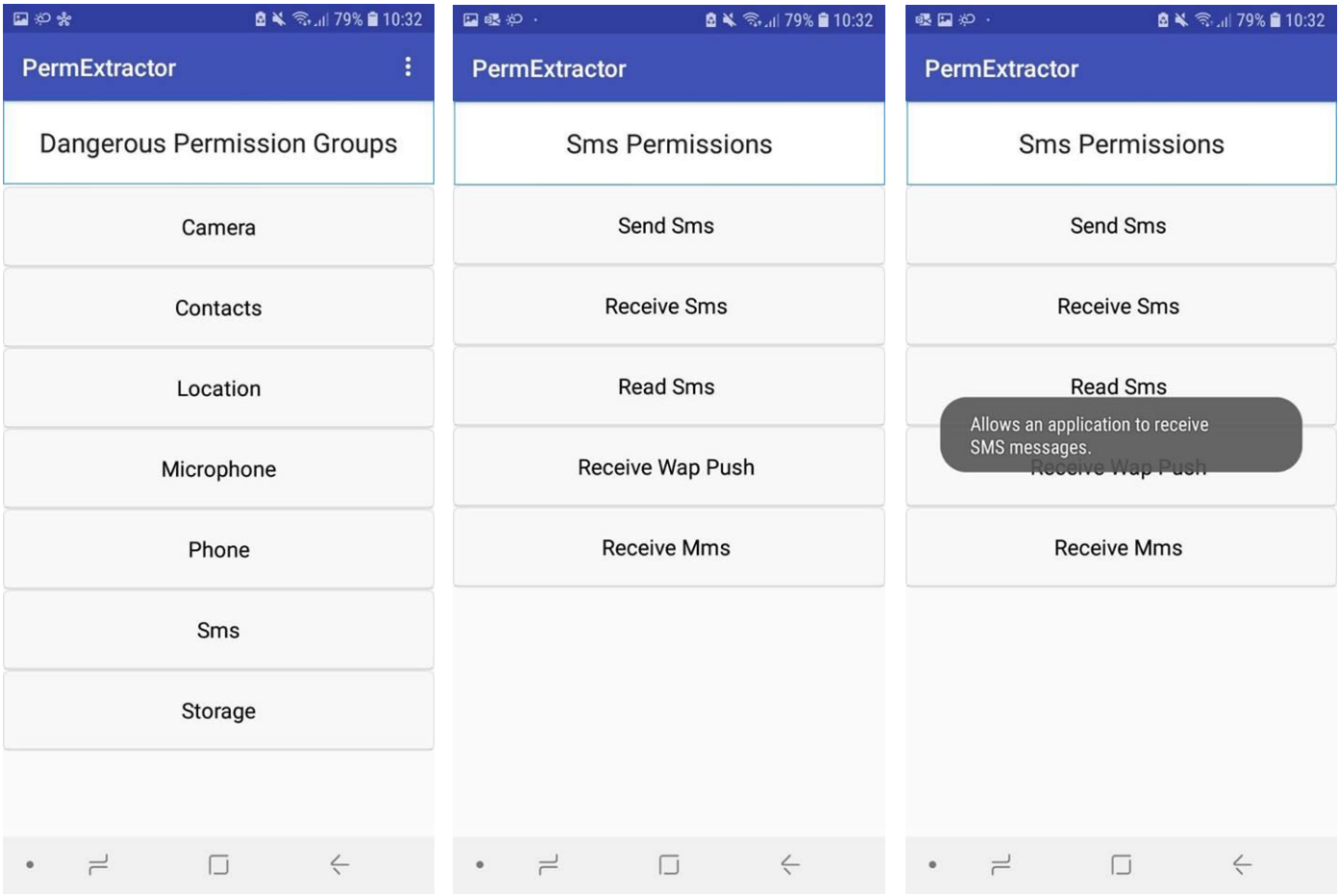
- Στέλλεται αρχικά το όνομα του APK, το version του και το όνομα του package του στο αρχείο getAnalyze.php.
- Το .php αρχείο μέσω queries, στην βάση δεδομένων MySQL, αναζητά να βρεί κάποια εγγραφή στον πίνακα apks της οποίας τα δεδομένα ταιριάζουν με αυτά που προήλθαν από την εφαρμογή PermExtractor.
    1. Σε περίπτωση που η αναζήτηση είναι επιτυχής, επιστρέφει σαν απάντηση τα permissions που βρίσκονται στην στήλη json_permissions.
    2. Σε περίπτωση που η αναζήτηση είναι ανεπιτυχής, επιστρέφει σαν απάντηση την φράση “Not Found.”.

Εάν ισχύει η περίπτωση (2) τότε είναι αναγκαία η εκτέλεση της διαδικασίας ανάλυσης που περιγράφηκε νωρίτερα. Με σκοπό την πραγματοποίηση της διαδικασίας είναι αναγκαία η ανάκτηση του APK αρχείου μιας εφαρμογής. Το εν λόγω αρχείο βρίσκεται σε ένα φάκελο των Android συσκευών από τον οποίο δεν επιτρέπεται η άμεση απόκτηση του. Έτσι, δημιουργείται ένα αντίγραφο του APK στον φάκελο Download ώστε να μεταφορτωθεί στον διακοσμιτή. Η μεταφόρτωση επιτυγχάνεται μέσω εγκαθίδρυσης Http url connection. Μετά ανοίγεται ένα stream όπου γράφονται όλα τα bytes του APK αρχείου και στέλλονται από την Android συσκευή στον διακοσμιτή. Εάν η απάντηση του διακοσμιτή είναι “File uploaded successfully”, τότε σειρά έχει η διαδικασία του decompiling και του analysing. Αυτές οι διαδικασίες εκτελούνται μέσω PHP web services, με την χρήση της συνάρτησης shell_exec().

Επιπρόσθετα, το δεύτερο web service συλλέγει από την αναφορά, που δημιουργείται στο τέλος της ανάλυσης, τις πληροφορίες που αφορούν τα over και under privileged dangerous permission groups και τα permissions που ανήκουν σε αυτά. Ο αλγόριθμος που ακολουθείται απαρτίζεται από διάφορες χρήσεις συναρτήσεων συμβολοσειρών και παρουσιάζεται στο Παράρτημα Α. Στο τέλος επιστρέφονται τα permissions σε μορφή json.

Η υλοποίηση των πιο πάνω PHP web services πραγματοποιείται μέσα σε κλάση που επεκτείνει την AsyncTask. Με την χρήση αυτής εκτελούνται όλες οι απαραίτητες λειτουργίες στο παρασκήνιο σε δευτερεύον νήμα. Αυτό αποτρέπει την διακοπή αλληλεπιδράσεων μεταξύ χρήστη-εφαρμογής. Επίσης, εξαιτίας του ότι το APK αρχείο κάποιων εφαρμογών έχει μεγάλο μέγεθος μπορεί να απαιτεί κάποια λεπτά εώς ότου ολοκληρωθεί η ανάλυση του. Έτσι, η AsyncTask ενημερώνει με notification πότε αρχίζει και πότε τελειώνει η ανάλυση για να μην είναι απαραίτητο να περιμένει ο χρήστης.

Αφού ο χρήστης αναλύσει μια εφαρμογή και έχει πρόσβαση στα dangerous permission groups και permissions αυτής, μπορεί να πατήσει πάνω σε αυτά με σκοπό να διαβάσει μια περιγραφή που επεξηγεί την χρησιμότητα τους. Αυτό έχει υλοποιηθεί με την χρήση της βιβλιοθήκης Volley και συγκεκριμένα της κλάσης StringRequest η οποία στέλνει στο web service το όνομα του permission κι αυτό με την σειρά του εντοπίζει την αντίστοιχη εγγραφή στον πίνακα permissions επιστρέφοντας την περιγραφή που βρίσκεται στην στήλη perm_descr. Αυτή η περιγραφή παρουσιάζεται στην εφαρμογή PermExtractor σε μορφή Toast.

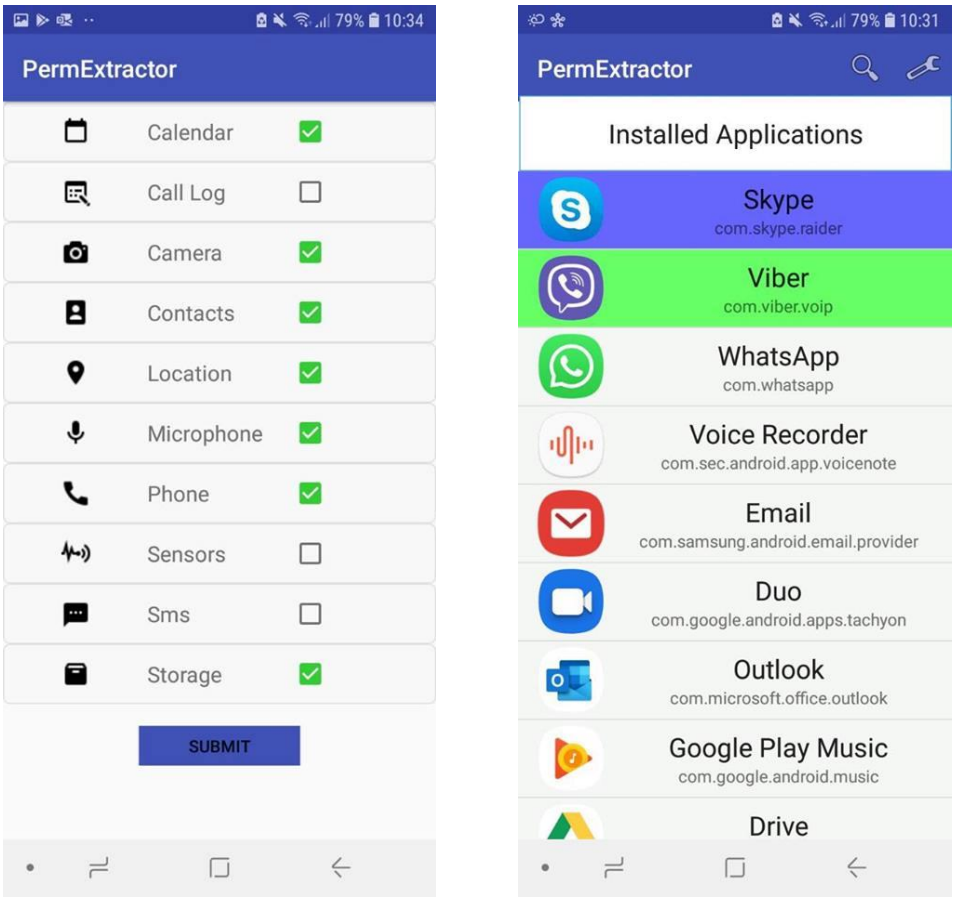


Σχήμα 16

6.3 Διαδικασία ορισμού προτιμήσεων χρήστη από κατάλογο με permission groups

Η συγκεκριμένη λειτουργία διαθέτει ένα κατάλογο με όλα τα ονόματα των dangerous permission groups του Android. Από αυτό τον κατάλογο ο χρήστης δύναται να επιλέξει όσα permission groups θεωρεί ο ίδιος ιδανικά να χρησιμοποιούνται από τις εγκατεστημένες εφαρμογές στην συσκευή του.

Ο τρόπος με τον οποίο αποθηκεύονται οι προτιμήσεις του χρήστη είναι μέσω εκμετάλλευσης των δυνατοτήτων της διεπαφής Shared Preferences που προσφέρει το Android Studio. Η συγκεκριμένη διεπαφή βεβαιώνει την παραμονή των προτιμήσεων του χρήστη σε σταθερή κατάσταση. Έτσι, δεν είναι αναγκαία η επιλογή νέων προτιμήσεων κάθε φορά που ο χρήστης επιστρέφει στην εφαρμογή αφού φυλάγονται αυτές της τελευταίας φοράς χρήσης της. Ταυτόχρονα, ο χρήστης έχει την δυνατότητα να τις τροποποιεί ανά πάσα στιγμή.



Σχήμα 17

6.4 Διαδικασία χρωματισμού εφαρμογών

Η συγκεκριμένη διαδικασία υλοποιείται με την χρήση της κλάσης StringRequest της βιβλιοθήκης Volley. Μέσω αυτής καλείται ένα PHP web service το οποίο εντοπίζει τα permission groups των ανελυμένων εφαρμογών στον πίνακα apks της βάσης δεδομένων και τα επιστρέφει σε json μορφή. Στην συνέχεια γίνεται σύγκριση των permission groups με αυτών που βρίσκονται αποθηκευμένα στα Shared Preferences.

- Σε περίπτωση που τα permission groups είναι υποσύνολο εκείνων των Shared Preferences, τότε σημαίνει πως η εφαρμογή είναι σύμφωνη με τις προτιμήσεις του χρήστη. Το layout της εφαρμογής χρωματίζεται με πράσινο.
- Σε περίπτωση που τα permission groups διαθέτουν groups τα οποία δεν συμπεριλαμβάνονται στις προτιμήσεις του χρήστη, τότε σημαίνει πως η εφαρμογή δεν είναι σύμφωνη με τις εν λόγω προτιμήσεις. Το layout της εφαρμογής χρωματίζεται με μπλε.

Το layout μιας μη ανελυμένης εφαρμογής χρωματίζεται πάντα με άσπρο.

6.5 Application recommender

Η υλοποίηση του application recommender βασίζεται στην χρήση του εργαλείου Google-Play-Scraper το οποίο είναι γραμμένο στη γλώσσα Node.js. Η διαδικασία υλοποίησης χωρίζεται σε δύο μέρη. Αρχικά, εντοπίζεται ένα σύνολο 50 εφαρμογών από το Google Play Store οι οποίες έχουν παρόμοια λειτουργικότητα με αυτή που έχει επιλέξει ο χρήστης. Στην συνέχεια, διαλέγονται, από το ανωτέρω σύνολο, οι εφαρμογές που ζητούν permission groups συμβατά με αυτά των προτιμήσεων του χρήστη και εμφανίζονται σε αυτόν. Τα δύο μέρη είναι υλοποιημένα με παρόμοιο τρόπο αφού το καθένα επιτελεί κλήση από την Android εφαρμογή σε ένα PHP web service από το οποίο εκτελείται μια Python εντολή μέσω της συνάρτησης shell_exec(). Στο επόμενο στάδιο, τα .py αρχεία πραγματοποιούν κλήση σε μια συγκεκριμένη συνάρτηση του Google-Play-Scraper με την χρήση της συνάρτησης muterun_js().

Το πρώτο μέρος χρησιμοποιεί την συνάρτηση similar() του εργαλείου η οποία δέχεται ως είσοδο το όνομα του package της εφαρμογής που έχει επιλέξει ο χρήστης. Ο τρόπος με τον οποίο εντοπίζονται παρόμοιες εφαρμογές είναι βασισμένος στην σύγκριση συγκεκριμένων πεδίων, που παρέχουν πληροφορίες αναφορικά με την κάθε εφαρμογή, με αυτών της εισόδου. Τα παραπάνω πεδία παρουσιάζονται στο Σχήμα 18.

```
const MAPPINGS = {
  title: [2],
  appId: [12, 0],
  url: {
    path: [9, 4, 2],
    fun: (path) => new url.URL(path, 'https://play.google.com').toString()
  },
  icon: [1, 1, 0, 3, 2],
  developer: [4, 0, 0, 0],
  developerId: {
    path: [4, 0, 0, 1, 4, 2],
    fun: extractDeveloperId
  },
  priceText: {
    path: [7, 0, 3, 2, 1, 0, 2],
    fun: (price) => price === undefined ? 'FREE' : price
  },
  free: {
    path: [7, 0, 3, 2, 1, 0, 2],
    fun: (price) => price === undefined
  },
  summary: [4, 1, 1, 1, 1],
  scoreText: [6, 0, 2, 1, 0],
  score: [6, 0, 2, 1, 1]
};
```

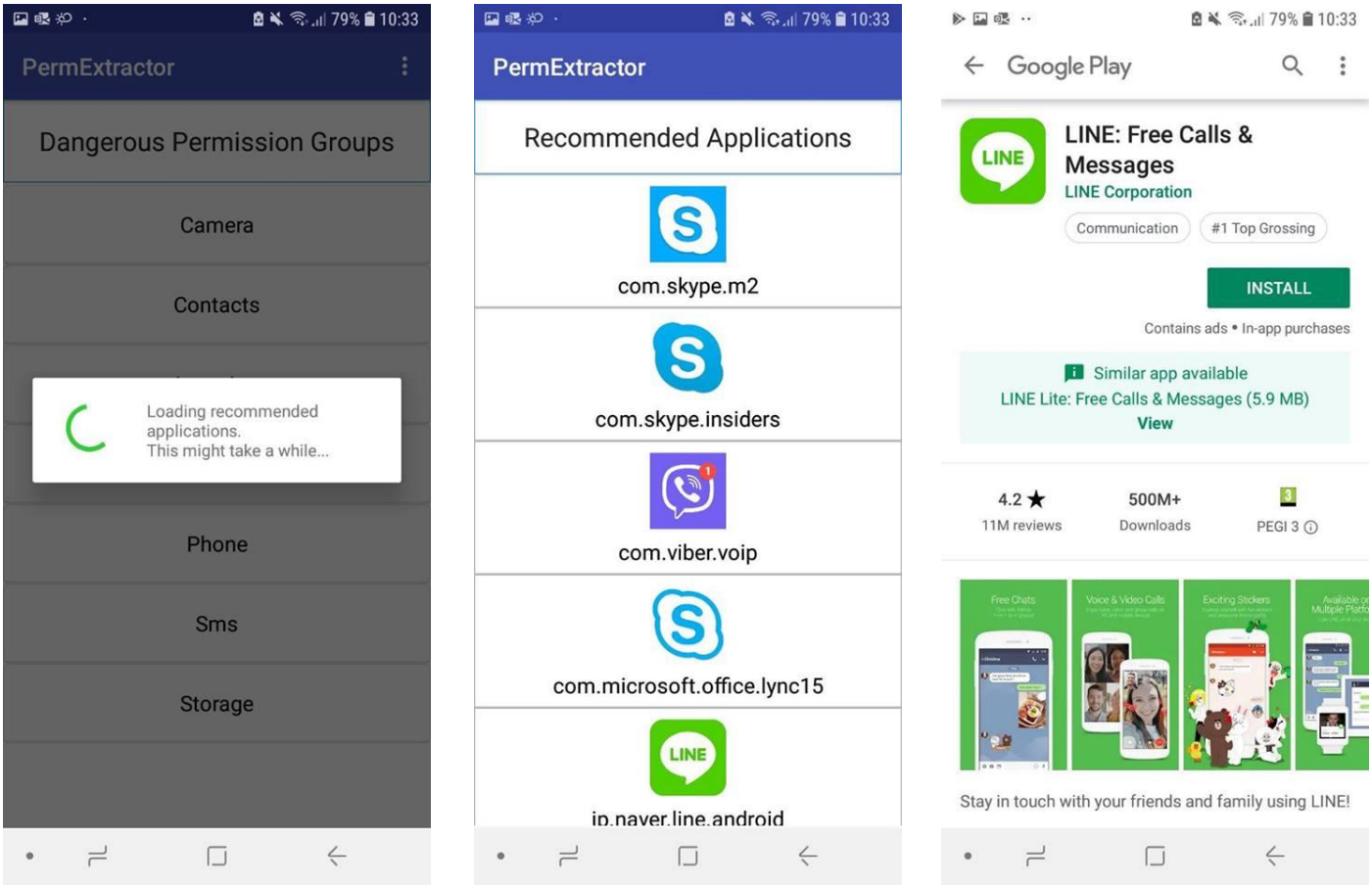
Σχήμα 18

Το δεύτερο μέρος της διαδικασίας χρησιμοποιεί την συνάρτηση permissions() του εργαλείου η οποία δέχεται ως είσοδο το όνομα του package κάθε εφαρμογής του συνόλου που ανακτήθηκε στο πρώτο μέρος. Μέσα στο PHP web service συγκρίνονται τα permission groups της εφαρμογής, που αποτελούν την έξοδο της συνάρτησης permissions(), με αυτά των Shared Preferences. Οι εφαρμογές που ζητούν permission groups τα οποία είναι ίδια με ή υποσύνολο των permission groups των Shared Preferences ωθούνται σε ένα πίνακα, ο οποίος στην πορεία μετατρέπεται σε json μορφή και επιστρέφεται στην εφαρμογή PermExtractor. Η μορφή json περιλαμβάνει το όνομα του package, το εικονίδιο και το URL της κάθε εφαρμογής.

Όταν ο χρήστης πατήσει πάνω σε μια από τις προτινόμενες εφαρμογές ενεργοποιείται η callback συνάρτηση onClick() του layout της. Εκεί δημιουργείται ένα Intent το οποίο μεταφέρει τον χρήστη στην ιστοσελίδα του Google Play Store όπου βρίσκεται η συγκεκριμένη εφαρμογή, βάσει του URL.(Σχήμα 19)

```
viewHolder.layoutApp.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        Intent viewIntent = new Intent( action: "android.intent.action.VIEW",
                Uri.parse(appItem.url));
        context.startActivity(viewIntent);
    }
});
```

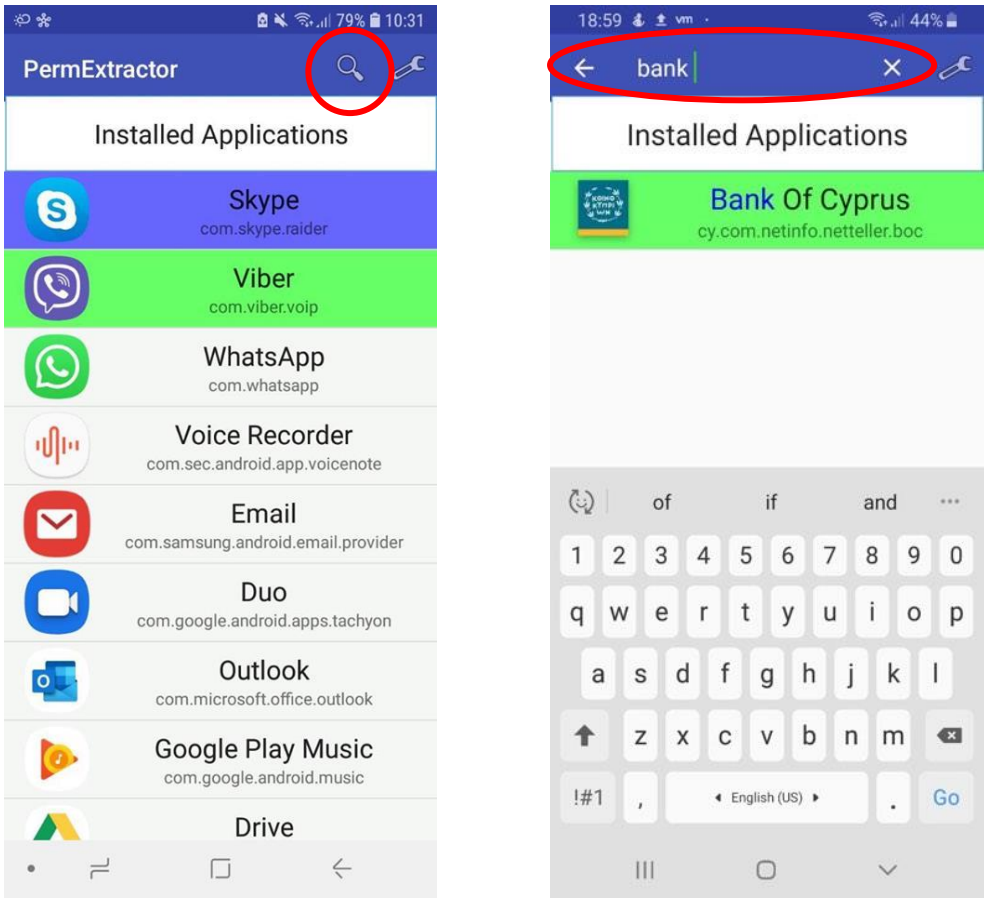
Σχήμα 19



Σχήμα 20

6.6 Διαδικασία αναζήτησης εγκατεστημένων εφαρμογών

Η διαδικασία αναζήτησης προσφέρει διευκόλυνση στον χρήστη για τον εντοπισμό μιας εγκατεστημένης εφαρμογής με σκοπό την αποφυγή του scrolling. Όταν ο χρήστης πληκτρολογήσει μια λέξη/φράση τότε ενεργοποιείται η callback συνάρτηση onQueryTextChange() ενός αντικειμένου τύπου SearchView. Η συγκεκριμένη συνάρτηση καλεί μια άλλη η οποία ανακαλύπτει τις εφαρμογές που εμπεριέχουν, το pattern που εισήγαγε ο χρήστης, στο όνομα τους ή στο όνομα του package τους και τις προσθέτει σε μια λίστα. Στην συνέχεια, παρουσιάζονται στην οθόνη της συσκευής, ενώ παράλληλα, γίνεται highlight το μέρος του ονόματος κάθε εφαρμογής που ταίριαξε με το pattern.

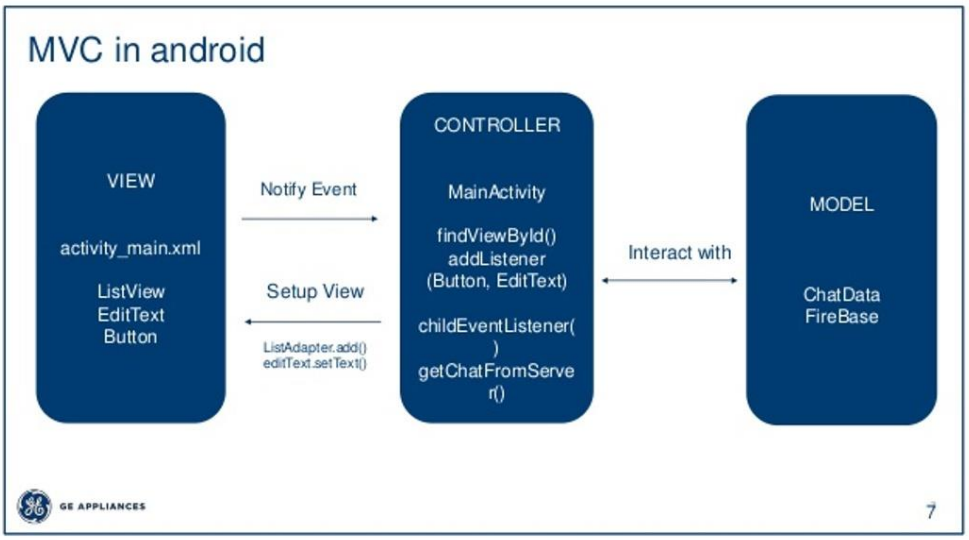


Σχήμα 21

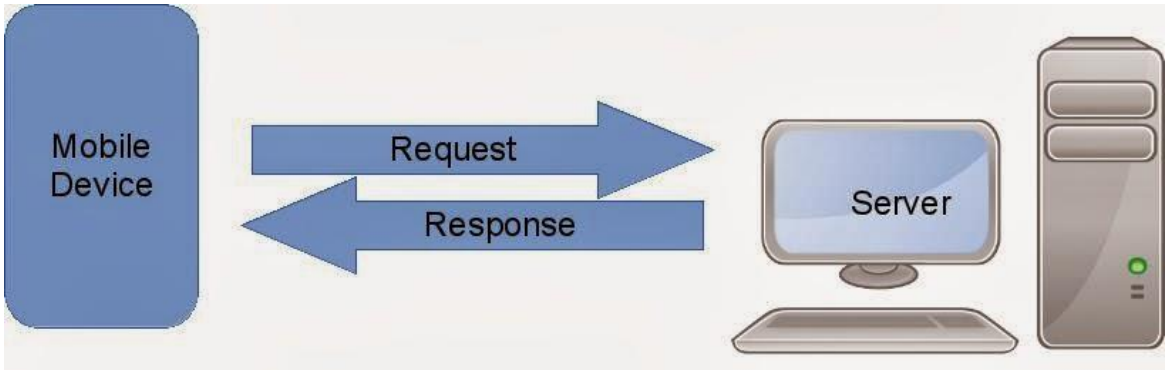
6.7 Αρχιτεκτονική συστήματος

Στην ανάπτυξη του συστήματος χρησιμοποιήθηκαν δύο είδη αρχιτεκτονικών. Από την στιγμή που η εφαρμογή δημιουργήθηκε μέσω του ολοκληρωμένου προγραμματιστικού περιβάλλοντος του Android Studio εννοείται πως έγινε χρήση της αρχιτεκτονικής Model-View-Controller (MVC) μιας και είναι ήδη υλοποιημένη μέσα σε αυτό. Το Model αντικατοπτρίζεται από τις κλάσεις που αφορούν την υλοποίηση της λογικής της εφαρμογής. Στην περίπτωση της εφαρμογής PermExtractor, οι κλάσεις που επεκτείνουν την AsyncTask, για παράδειγμα, αντιπροσωπεύουν σημαντικό μέρος της λογικής της εφαρμογής. Όσον αφορά το View, αποτελείται από όλα τα υπάρχοντα layouts, resources and built-in κλάσεις τα οποία και παρουσιάζονται στην οθόνη του χρήστη. Τέλος, ο Controller υποστηρίζεται από την ύπαρξη των Activities στο Android Studio ρόλος των οποίων είναι η σύνδεση μεταξύ View και Model μέσω της αντίδρασης σε διάφορα events που ενεργοποιούνται κατά την χρήση της εφαρμογής.(Σχήμα 22)

Η δεύτερη κατηγορία αρχιτεκτονικής που χρησιμοποιείται είναι αυτή του Client-Server. Στην περίπτωση της εφαρμογής PermExtractor, η ίδια αποτελεί τον Client ο οποίος μέσω των web services κάνει POST requests στον Server και αυτός επιστρέφει με την σειρά του το response του στο ανάλογο request. Η επικοινωνία μεταξύ τους επιτυγχάνεται με την εγκαθίδρυση Http URL Connection. (Σχήμα 23)



Σχήμα 22: Παράδειγμα MVC σε Android



Σχήμα 23: Παράδειγμα Client-Server
Αρχιτεκτονικής

Κεφάλαιο 7

Αποτελέσματα ερωτηματολογίου, γενικά συμπεράσματα και μελλοντική εργασία

7.1 Εισαγωγή

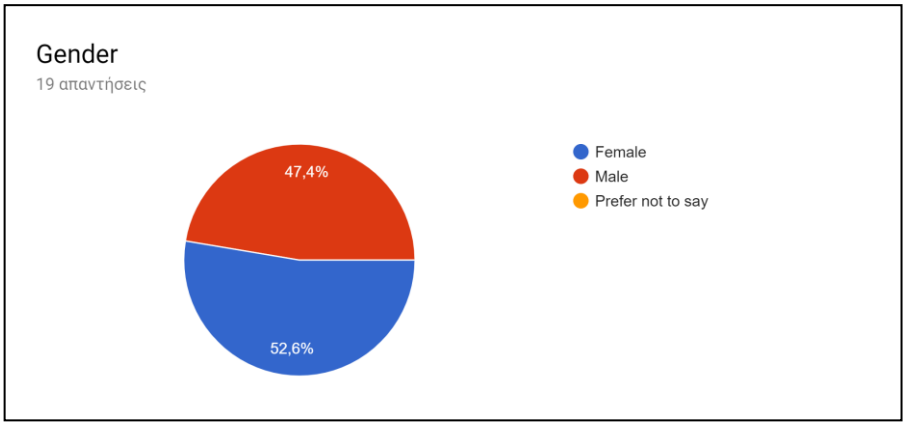
Μετά την υλοποίηση της, η εφαρμογή PermExtractor δόθηκε σε 19 κατόχους Android κινητών συσκευών με σκοπό να την εγκαταστήσουν και να την χρησιμοποιήσουν. Επιπρόσθετα, ζητήθηκε από τα άτομα αυτά να συμπληρώσουν ένα ερωτηματολόγιο που αφορούσε κυριώς την εμπειρία τους με το PermExtractor καθώς και τις γνώσεις τους περί ιδιωτικότητας και Android.

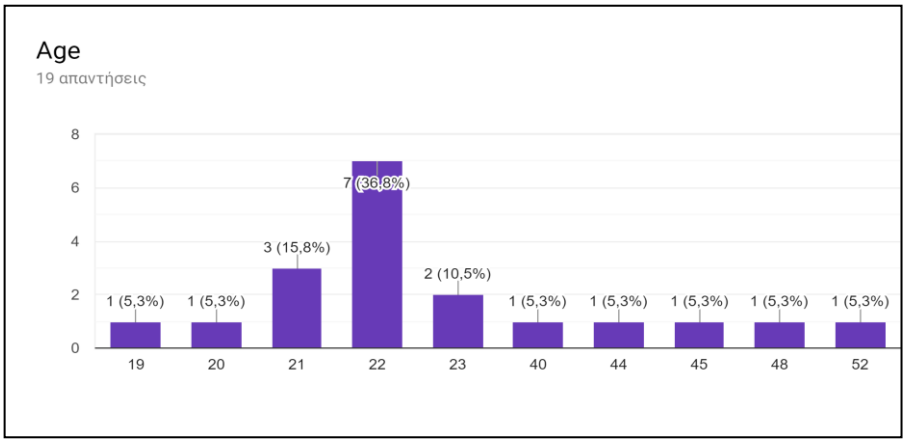
Σε αυτό το κεφάλαιο παρουσιάζονται τα αποτελέσματα των ερωτηματολογίων καθώς και η ανάλυση τους. Επίσης, παραθέτονται κάποια γενικά συμπεράσματα που εξήχθησαν κατά την διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας, την μελέτη άρθρων και γενικά πηγών σχετικών με την έννοια της ιδιωτικότητας και το Android σύστημα καθώς και την σχεδίαση, ανάπτυξη και αξιολόγηση της εφαρμογής PermExtractor. Στο τέλος, αναφέρονται κάποιες πιθανές μελλοντικές εργασίες που θα μπορούσαν να λάβουν μέρος ώστε να εξελιχθεί η εφαρμογή σε μια καλύτερη έκδοση της.

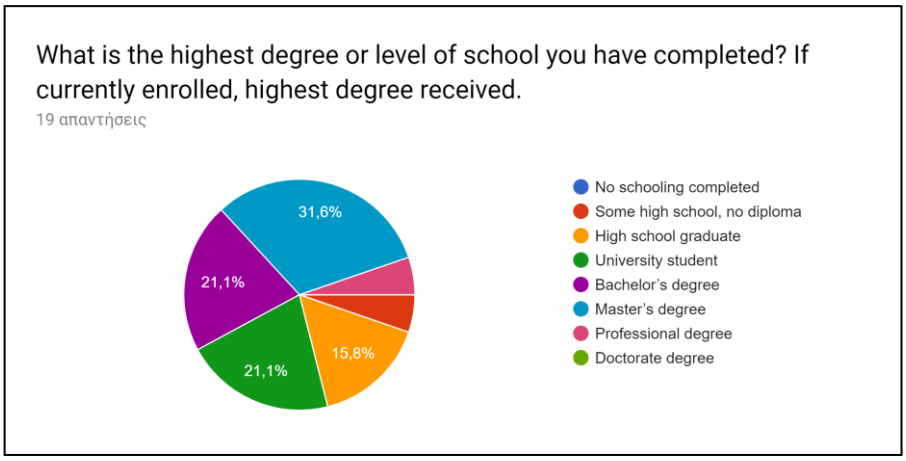
7.2 Παρουσίαση και ανάλυση αποτελεσμάτων

Όπως αναφέρθηκε νωρίτερα, το ερωτηματολόγιο που δημιουργήθηκε σχετικά με την παρούσα διπλωματική εργασία απαντήθηκε από 19 κατόχους Android κινητών συσκευών των οποίων οι ηλικίες κυμαίνονται από 19 μέχρι 52 χρονών. Το ερωτηματολόγιο χωρίζεται σε 4 κατηγορίες. Η πρώτη περιέχει δημογραφικές ερωτήσεις ενώ η δεύτερη περιλαμβάνει ερωτήσεις περί χρήσης των Android κινητών συσκευών. Επίσης, η τρίτη κατηγορία στοχεύει

στην ανάκτηση πληροφοριών σχετικά με το Android και την ιδιωτικότητα των χρηστών. Η τελευταία κατηγορία αφορά εξ'ολοκλήρου την αξιολόγηση της εμπειρίας των χρηστών με την εφαρμογή PermExtractor.



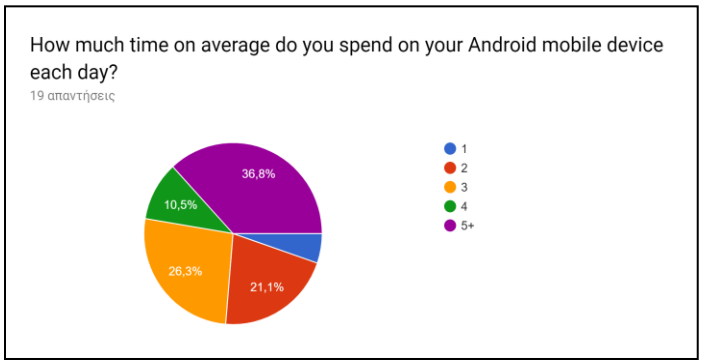




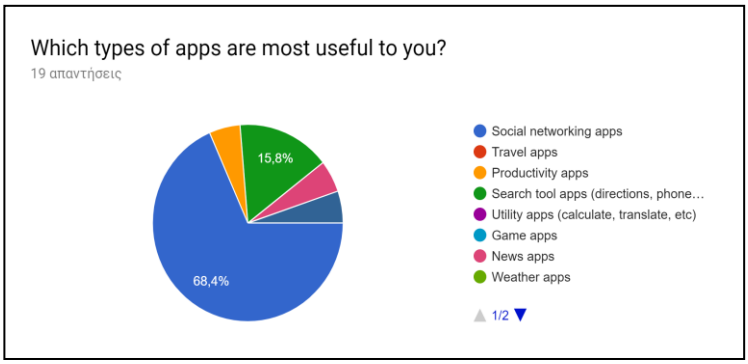
Είναι σημαντικό να υπογραμμιστεί πως οι συμμετέχοντες στην συγκεκριμένη έρευνα προέρχονται και από τα δύο φύλα, καθώς και από σχετικά μεγάλο εύρος ηλικιών, ενώ παράλληλα παρουσιάζουν διαφορές ως προς το επίπεδο εκπαίδευσης τους. Αποτελούν, δηλαδή, αντιπροσωπευτικό τμήμα του συνόλου του πληθυσμού και όχι στοχευμένη ομάδα αυτού. Ως αποτέλεσμα, έχουμε στην διάθεση μας μια ποικιλία απόψεων όσον αφορά την

χρήση των κινητών συσκευών, την ιδιωτικότητα των χρηστών και το Android καθώς και τον τρόπο αξιολόγησης της εφαρμογής PermExtractor.

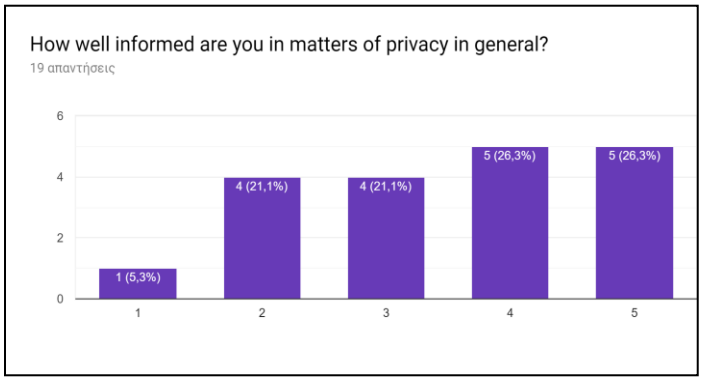
Ακολουθεί μια σειρά από διαγράμματα προερχόμενα από διάφορες κατηγορίες του ερωτηματολογίου και συνοδευμένα με διάφορα συμπεράσματα που απορρέουν από αυτά.



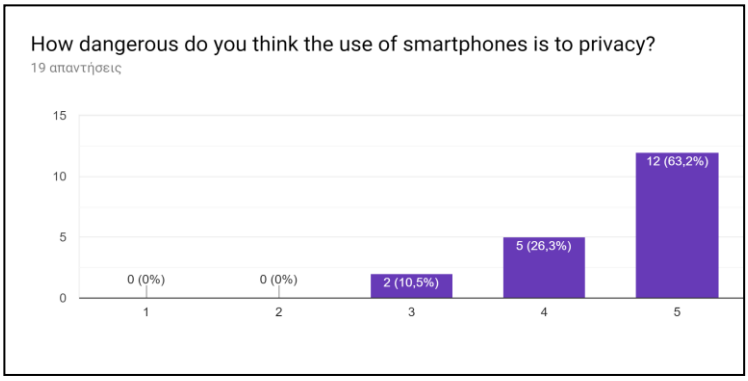
1



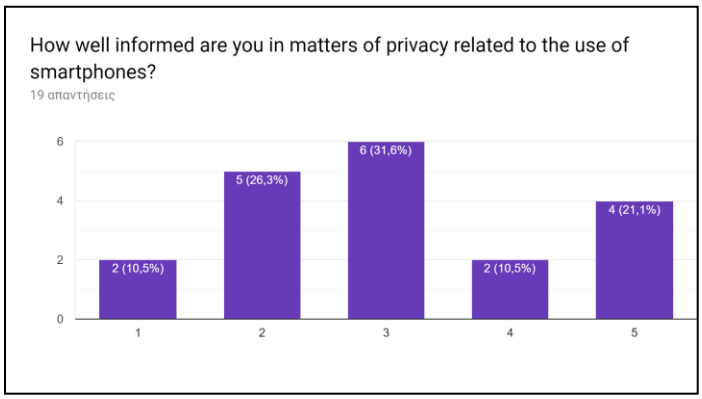
2



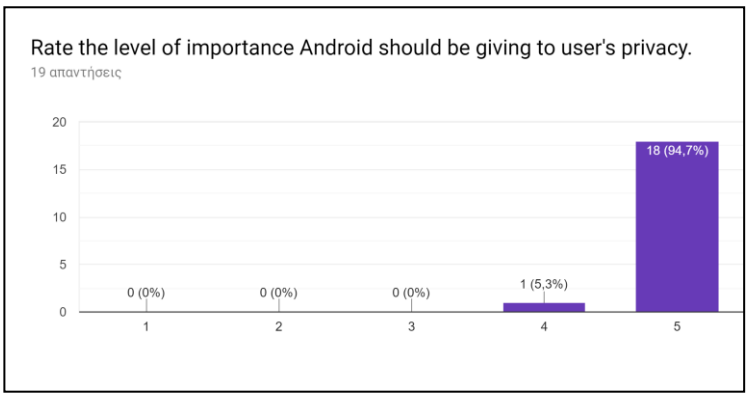
3



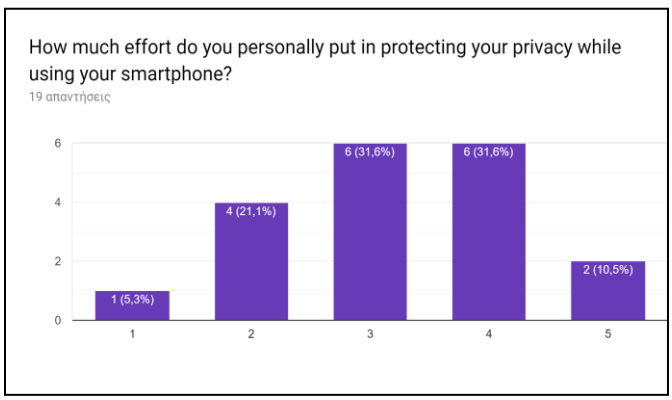
4



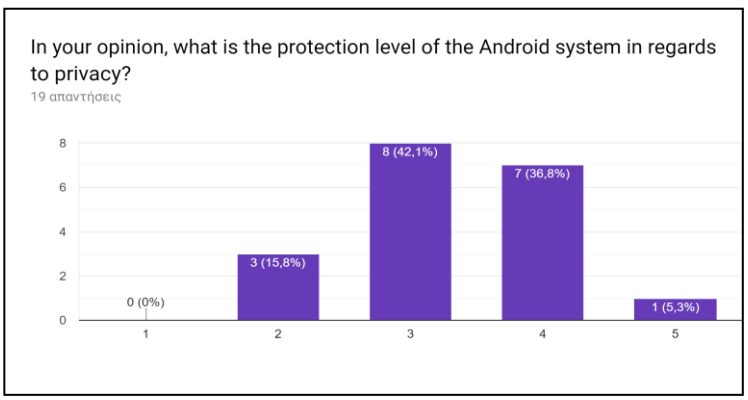
5



6



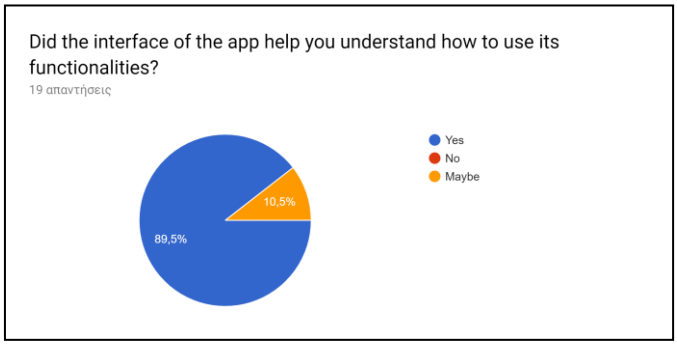
7



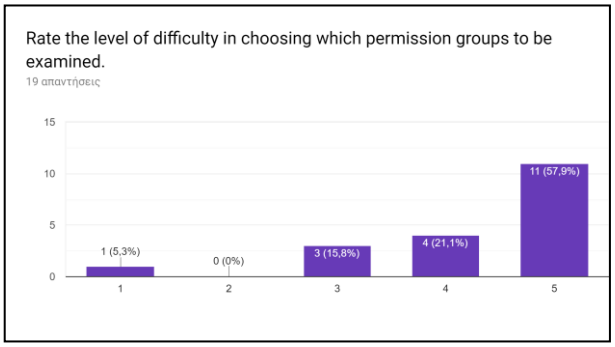
8

Αρχικά, ένα μεγάλο ποσοστό των χρηστών (63.2%) πιστεύει πως η χρήση των κινητών συσκευών απειλεί σε εξαιρετικό βαθμό την ιδιωτικότητα τους. Βάσει του διαγράμματος ..., σχεδόν το 50% των ατόμων, που έλαβαν μέρος στην έρευνα, χρησιμοποιεί την κινητή συσκευή του για 4-5 ώρες καθημερινώς. Ταυτόχρονα, το ποσοστό των ατόμων που βρίσκουν τις εφαρμογές κοινωνικής δικτύωσης πιο χρήσιμες ανέρχεται στο 68.4%. Συμπερασματικά, ένα μεγάλο ποσοστό των ανθρώπων τείνει να αφιερώνει περισσότερο από 1/6 της ημέρας του χρησιμοποιώντας κυρίως εφαρμογές κοινωνικής δικτύωσης οι οποίες ζητούν μεγάλες ποσότητες προσωπικών δεδομένων των χρηστών. Υπάρχει λοιπόν μια αντίφαση μεταξύ της επικινδυνότητας που προσδίδεται στη χρήση Android κινητών συσκευών και στην πραγματική χρήση αυτών, ιδίως δε των πλείονων επικίνδυνων εφαρμογών.

Το διάγραμμα 6 κάνει εμφανές πως η πλειονότητα των χρηστών (94.7%) θεωρεί ότι η πλατφόρμα Android πρέπει να δίνει ιδιαίτερη σημασία στην διατήρηση της ιδιωτικότητας τους. Όταν ερωτήθηκαν, όμως, οι χρήστες για την προσπάθεια που πιστεύουν πως καταβάλλεται από το Android σχετικά με την προστασία της ιδιωτικότητας τους, ένα μεγάλο ποσοστό (42.1%) απάντησε 3, που αντιστοιχεί με ‘μέτρια προσπάθεια’. Παράλληλα, στο διάγραμμα ... παρουσιάζεται πως οι περισσότεροι χρήστες (63.2%) δεν επιχειρούν οι ίδιοι να διαφυλάξουν την ιδιωτικότητα τους κατά την διάρκεια χρήσης των κινητών τους συσκευών. Συνεπώς, οι χρήστες κινητών συσκευών αναμένουν από την πλατφόρμα Android να αναλάβει τον ρόλο διαφύλαξης των προσωπικών τους δεδομένων και γενικά της ιδιωτικότητας τους, ενώ την ίδια στιγμή, δεν εντοπίζεται κάποια ιδιαίτερη προσπάθεια εκ μέρους των ιδίων. Ίσως στην περίπτωση των χρηστών, ένας από τους παράγοντες που συντείνει στην μη καταβολή αρκετής προσπάθειας είναι η άγνοια που τους διέπει όσον αφορά την διατήρηση ιδιωτικότητας κατά την χρήση των συσκευών τους. Το παραπάνω συμπέρασμα προέρχεται από τα αποτελέσματα του διαγράμματος 5.



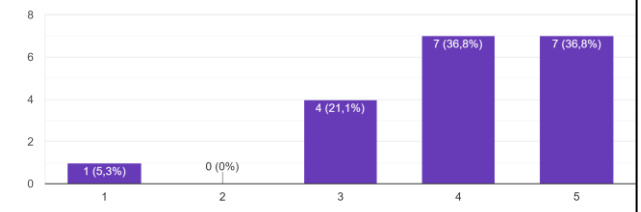
9



10

Rate the level of difficulty in understanding the meaning of permissions presented in the app.

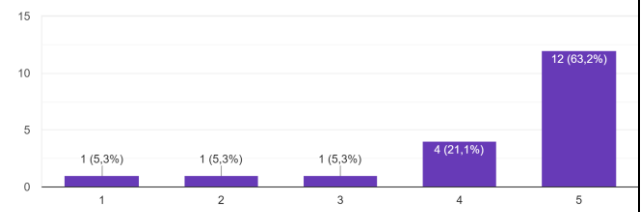
19 απαντήσεις



11

Rate the level of difficulty in understanding which apps are compatible with your preferences.

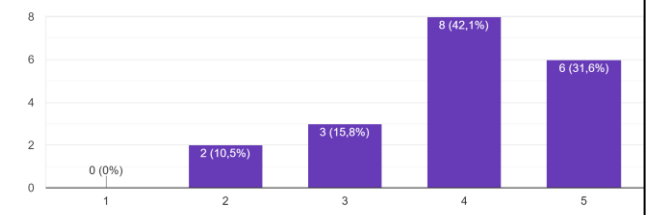
19 απαντήσεις



12

Rate the level of difficulty in viewing recommendations for your apps.

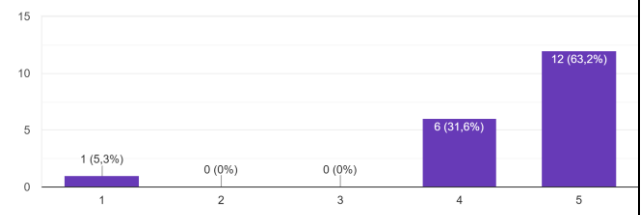
19 απαντήσεις



13

Rate the level of usefulness of the recommendation feature.

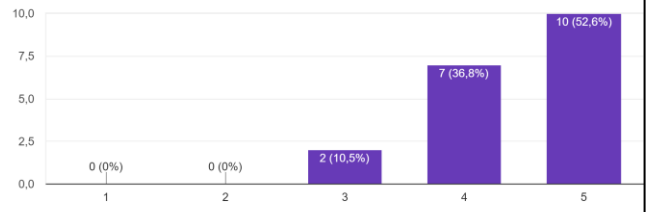
19 απαντήσεις



14

How would you rate the general usefulness of the app?

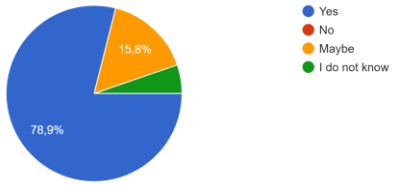
19 απαντήσεις



15

Do you think that this app contributes in providing a better understanding of what user data are accessed by installed apps?

19 απαντήσεις



16

Which feature of the app do you consider as the most useful and why?

11 απαντήσεις

Recommendations because it helps you find similar apps that uses only the specified permissions
Nothing in particular
The app recommendations due to my permission preferences
the recommendation feature as it allows you to find simillar apps with ur preferred permissions
Find permissions of other apps
Access type with Colour
Viewing the permissions of the already installed apps. It is important to know the personal data that is being accessed by the apps for privacy reasons.
Useful, Privacy issues
The recommendations because they provide alternatives that meet our privacy concerns
explaining each permission and permission group
Colours showing whether apps are compatible with my preferences or not

17

Όσον αφορά την εμπειρία των συμμετεχόντων με την Android εφαρμογή PermExtractor, το 89.5% πιστεύει πως η διαπροσωπεία βοηθάει στην κατανόηση του τρόπου χρήσης της εφαρμογής. Επιπρόσθετα, το ποσοστό των χρηστών που κατάλαβε αρκετά εώς και εξαιρετικά καλά την έννοια των permission groups ανέρχεται στο 73.6%, ενώ ταυτόχρονα, το ποσοστό των χρηστών που αντιλήφθηκε αρκετά εώς και εξαιρετικά καλά τον τρόπο ορισμού των προτιμήσεων του φτάνει το 79%. Ακόμη, το 63.2% των χρηστών βρήκε εξαιρετικά κατανοητό τον τρόπο χρωματισμού των εγκατεστημένων εφαρμογών.

Στο διάγραμμα 13, φαίνεται πως η πλειοψηφία των χρηστών δεν αντιμετώπισε κάποιο πρόβλημα όσον αφορά τον εντοπισμό του app recommender (73.7%). Ταυτόχρονα, ο app recommender αποτελεί την πιο χρήσιμη λειτουργια της εφαρμογής για τους χρήστες αφού προτείνει εναλλακτικές λύσεις σύμφωνες με τις προτιμήσεις τους, βάσει των απαντήσεων στην ερώτηση 17.

Γενικά, οι περισσότεροι χρήστες πιστεύουν ότι η εφαρμογή PermExtractor είναι αρκετά (36.8%) εώς και εξαιρετικά (52.6%) χρήσιμη για τους ίδιους καθώς και πολύ βοηθητική (78.9%) στην βελτίωση της κατανόησης τους σχετικά με την έκταση της πρόσβασης των εφαρμογών τους στα προσωπικά τους δεδομένα.

Όπως γίνεται εμφανές από τα αποτελέσματα των χρηστών, η εφαρμογή έχει επιτύχει τον στόχο της ως ένα μεγαλό βαθμό. Πιο ειδικά, συμβάλλει στην βελτίωση κατανόησης των χρηστών όσον αφορά την πρόσβαση που έχουν οι εφαρμογές στα προσωπικά δεδομένα τους. Αυτό επιτυγχάνεται κυρίως με τον φιλικό προς τον χρήστη τρόπο που παρουσιάζονται τα permission groups και τα permissions. Επιπρόσθετα, εξυπηρετεί έμμεσα στην διαφύλαξη της ιδιωτικότητας του χρήστη μιας και ο app recommender προσφέρει εναλλακτικές λύσεις ώστε οι χρήστες να εγκαθιστούν εφαρμογές στις συσκευές τους οι οποίε είναι σύμφωνες με τις προτιμήσεις τους σε permission groups.

7.3 Γενικά Συμπεράσματα

Η διαδικασία εκπόνησης της παρούσας διπλωματικής εργασίας, η οποία περιλαμβάνει την μελέτη διάφορων άρθρων και γενικά πηγών σχετικών με την έννοια της ιδιωτικότητας και το

Android σύστημα καθώς και την σχεδίαση, ανάπτυξη και αξιολόγηση της εφαρμογής PermExtractor, είχε ως αποτέλεσμα την εξαγωγή κάποιων γενικών συμπερασμάτων.

Η γρήγορη ανάπτυξη λογισμικού Android εφαρμογών δίνει την ευκαιρία σε όλους τους κατόχους Android κινητών συσκευών να επιλέξουν μέσα από ένα τεράστιο εύρος εφαρμογές που τους ενδιαφέρουν. Δυστυχώς ένα μεγάλο ποσοστό των χρηστών επιτρέπει στις εφαρμογές αυτές την πρόσβαση στα προσωπικά τους δεδομένα χωρίς να συνειδητοποιεί τον κίνδυνο που διατρέχει η ιδιωτικότητα του. Η πρόσβαση δύναται να παραχωρείται από τους ίδιους τους χρήστες εξαιτίας της έλλειψης κατανόησης περί permissions ή από τις ίδιες τις εφαρμογές εν αγνοία των χρηστών.

Έτσι, δημιουργήθηκε η Android εφαρμογή PermExtractor με στόχο την βελτίωση της κατανόησης των χρηστών περί πρόσβασης των εφαρμογών τους στα διάφορα permission groups, κάτι που επιτυγχάνεται με την φιλική προς τον χρήστη διαπροσωπεία του. Ακόμη ένας στόχος της εφαρμογής είναι η έμμεση διατήρηση της ιδιωτικότητας του χρήστη μέσω του app recommender. Ο recommender παροτρύνει την εγκατάσταση παρόμοιων εφαρμογών με αυτών που έχει ήδη ο χρήστης αλλά οι συγκεκριμένες ζητούν permission groups σύμφωνα με τις προτιμήσεις του. Σημαντικό είναι να σημειωθεί πως ο PermExtractor έχει την δυνατότητα να εντοπίζει και να ενημερώνει τον χρήστη για τυχών dangerous permissions που δύναται να δηλώνονται μέσα στον κώδικα των εφαρμογών και όχι στο αρχείο AndroidManifest.xml.

7.4 Μελλοντική εργασία

Στο μέλλον φαίνεται να υπάρχουν προοπτικές για την Android εφαρμογή PermExtractor ώστε να εξελιχθεί σε μια βελτιωμένη έκδοση του εαυτού της η οποία και θα παρέχει περισσότερες δυνατότητες στους χρήστες. Αυτό μπορεί να επιτευχθεί με την πρόσθεση κάποιων γραφικών παραστάσεων οι οποίες θα ενημερώνουν τον χρήστη για τα πιο περιζήτητα permission groups και permissions από τις εφαρμογές του ή ακόμα και για το ποιες εφαρμογές ζητούν permissions τα οποία δεν χρειάζονται πραγματικά για την ομαλή λειτουργία τους.

Επίσης, θα ήταν χρήσιμο για κινητές συσκευές Android 6.0+ να γίνεται εφικτή η διαχείριση και ρύθμιση των permissions που χρησιμοποιούνται από τις εφαρμογές μέσω του

PermExtractor. Αυτή η λειτουργία βρίσκεται ήδη μέσα στις Ρυθμίσεις των συσκευών Android 6.0+ όμως εάν υλοποιηθεί κάτι παρόμοιο στον PermExtractor θα τον μετατρέψει σε μια ολοκληρωμένη εφαρμογή που θα αφορά την ενημέρωση των χρηστών για τα permissions και την διαχείρηση αυτών.

Βιβλιογραφία

[1] How the Digital Age is Impacting Our Personal Privacy, Charles Okwe
https://medium.com/@cre8tivemediaservices/how-the-digital-age-is-impacting-our-personal-privacy-695326dd1455

[2] 2016 TRUSTe/NCSA Consumer Privacy Infographic - US Edition
https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/

[3] Privacy and Information Technology, Stanford Encyclopedia of Philosophy
https://plato.stanford.edu/entries/it-privacy/

[4] Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices, Arkady Yerukhimovich, Rebecca Balebako, Anne Boustead, Robert K. Cunningham, William Welser IV, Richard Housley, Richard Shay, Chad Spensky, Karlyn D. Stanley, Jeffrey Stewart, Ari Trachtenberg, Zev Winkelman.
https://pdfs.semanticscholar.org/60f2/f3fb8ea5e2dad60a1c4a40a620b3d1a84daf.pdf

[5] Τί είναι η ιδιωτικότητα; ξεχασμένος κι ατίθασος.
https://antiauthor.wordpress.com/2011/08/06/%CF%84%CE%AF%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9%CE%B7%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1/

[6] Vickery v Nova Scotia Supreme Court (Prothonotary) [1991] 1 SCR 671, 687.
https://www.scc-csc.ca/case-dossier/info/dock-regi-eng.aspx?cas=21598

[7] «The Right to Privacy», Samuel D. Warren & Louis Brandeis.
https://en.wikipedia.org/wiki/The_Right_to_Privacy_(article)

[8] Μορφές Ιδιωτικότητας, ξεχασμένος κι ατίθασος.
https://antiauthor.wordpress.com/2011/08/17/%CE%BC%CE%BF%CF%81%CF%86%CE%AD%CF%82%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1%CF%82/

[9] Introduction to Inquiry, Australian Privacy Law and Practice (ALRC Report 108). https://www.alrc.gov.au/publications/1.%20Introduction%20to%20the%20Inquiry/meaning-privacy

[10] D Banisar, Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments Privacy International. http://gilc.org/privacy/survey/intro.html

[11] GDPR: Personal Data and Sensitive Personal Data. https://www.burges-salmon.com/news-and-insight/legal-updates/gdpr-personal-data-and-sensitive-personal-data/

[12] Privacy and Security in Information Technology, Tyler Boone https://web.wpi.edu/Pubs/E-project/Available/E-project-053007-233726/unrestricted/TylerBoone.pdf

[13] How companies use personal data against people, Vienna, October 2017 Author: Wolfie Christl Contributors: Katharina Kopp, Patrick Urs Riechert Wolfie Christl. https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

[14] Android - Statistics & Facts https://www.statista.com/topics/876/android/

[15] Android Operating System Architecture, Umer Farooq https://www.researchgate.net/publication/326507076_Android_Operating_System_Architecture

[16] An Overview of the Android Architecture https://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture

[17] Android Architecture https://source.android.com/devices/architecture

[18] Platform Architecture
https://developer.android.com/guide/platform#linux-kernel

[19] US: Personal data stored on smartphones by 50 percent of users, Bitdefender.
https://www.bitdefender.com/news/us:-personal-data-stored-on-smartphones-by-50-percent-of-users-3368.html

[20] Android Application Install-time Permission Validation and Run-time Malicious Pattern Detection, Zhongmin Ma.
https://vtechworks.lib.vt.edu/bitstream/handle/10919/25238/Ma_Z_T_2014.pdf?sequence=1

[21] Smartphones and Android Internals, Faculty of San Diego State University.
https://kipdf.com/smartphones-and-android-internals-a-thesis-presented-to-the-faculty-of-san-diego_5ada0f617f8b9a528b8b45ed.html

[22] Application Signing
https://source.android.com/security/apksigning

[23] An Overview of Android Intents
https://www.techotopia.com/index.php/An_Overview_of_Android_Intents

[24] Permissions overview
https://developer.android.com/guide/topics/permissions/overview

[25] What are the different types of permissions in Android?
https://discussions.soti.net/thread/what-are-on-demand-permissions/

[26] Understanding Permissions in the Android World, Darshan Pania.
https://clevertap.com/blog/understanding-android-permissions/

[27] Understanding App Permissions.
https://guides.codepath.com/android/Understanding-App-Permissions

[28] #SmallerAPK, Part 1: Anatomy of an APK, Wojtek Kaliciński
https://medium.com/androiddevelopers/smallerapk-part-1-anatomy-of-an-apk-da83c25e7003

[29] What is an APK file and how do you install one? Nicholas Montegriffo
https://www.androidpit.com/android-for-beginners-what-is-an-apk-file

[30] Android Security: A Survey of Issues, Malware Penetration, and Defenses, Parvez Faruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti.
https://ieeexplore.ieee.org/document/6999911

[31] JAR-signed APK verification
https://source.android.com/security/apksigning/v2#v1-verification

[32] SRT AppGuard
http://www.srt-appguard.com/en/

[33] Backes, Michael, et al. "AppGuard–Enforcing User Requirements on Android Apps." Tools and Algorithms for the Construction and Analysis of Systems. Springer Berlin Heidelberg, 2013.
http://sps.cs.uni-saarland.de/publications/tacas2013.pdf

[34] Privacy Advisor Pro
https://play.google.com/store/apps/details?id=hugo.vn.privacyadvisor

[35] A Survey on Application Collusion Attacks on Android Permission-Mechanism, Dhaval Baraiya Prof. Hiteishi Diwanji.
https://www.academia.edu/20051067/A_Survey_on_Application_Collusion_Attacks_on_Android_Permission-Mechanism

[35] Java
https://el.wikipedia.org/wiki/Java

[36] Why is Java preferred for developing an Android app?
https://www.quora.com/Why-is-Java-preferred-for-developing-an-Android-app

[37] What is the JVM? Introducing the Java Virtual Machine
https://www.javaworld.com/article/3272244/what-is-the-jvm-introducing-the-java-virtual-machine.html

[38] Kotlin
https://en.wikipedia.org/wiki/Kotlin_(programming_language)

[39] Python
https://el.wikipedia.org/wiki/Python

[40] Features of Python Programming Language
https://data-flair.training/blogs/features-of-python/

[41] PHP
https://el.wikipedia.org/wiki/PHP

[42] Node.js
https://el.wikipedia.org/wiki/Nodejs

[43] MySQL
https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html

[44] phpMyAdmin
https://en.wikipedia.org/wiki/PhpMyAdmin

[45] M-Perm
https://mperm.github.io/index.html

[46] Google-Play-Scraper
https://github.com/facundoolano/google-play-scraper

[47] Data Scraping
https://en.wikipedia.org/wiki/Data_scraping

Παράρτημα Α

Link ερωτηματολογίου:
https://docs.google.com/forms/d/e/1FAIpQLSeXRnJRD0t-2_ToH-pqpEjJTcULrM3Dgs6GA6WalCY-NuQYfg/viewform

Απαντήσεις ερωτηματολογίου:
https://cgiap.cyend.com/QuestionnaireAnswers.csv.zip

CSV File με μερικά ανελυμένα APK αρχεία:
https://cgiap.cyend.com/apks.csv

APK file της εφαρμογής PermExtractor:
https://cgiap.cyend.com/permExtractor.apk