ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ιδιωτικότητα στο Android: Μελέτη αδειών πρόσβασης και πολιτικών ιδιωτικότητας εφαρμογών στο Android

ΣΥΓΓΡΑΦΕΑΣ: ΤΕΠΕΛΙΔΗΣ ΝΙΚΟΛΑΟΣ

ΑΜ: Π2013069

ΤΡΙΜΕΛΗΣ ΟΜΑΔΑ ΕΞΕΤΑΣΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ

ΤΣΩΧΟΥ ΑΓΓΕΛΙΚΗ (ΕΠΙΒΛΕΠΩΝ)

ΜΑΓΚΟΣ ΕΜΜΑΝΟΥΗΛ

ΚΟΥΡΟΥΘΑΝΑΣΗΣ ΠΑΝΑΓΙΩΤΗΣ

ΚΕΡΚΥΡΑ, 2019

Περίληψη

Σκοπός της συγκεκριμένης διπλωματικής εργασίας είναι η διερεύνηση και αξιολόγηση των θεμάτων ασφαλείας και ιδιωτικότητας των εφαρμογών στο λειτουργικό σύστημα Android. Για την επίτευξη του συγκεκριμένου σκοπού απαιτήθηκε η ανάλυση των αδειών πρόσβασης και των πολιτικών ιδιωτικότητας που χρησιμοποιούν οι εφαρμογές για να αποκτήσουν πρόσβαση στα προσωπικά δικαιώματα των χρηστών. Αναφορικά με τις άδειες πρόσβασης αναπτύχθηκε μια εφαρμογή που διαβάζει όλα τα δικαιώματα από δεκάδες εφαρμογές στο aptoide, μια ανεπίσημη ιστοσελίδα παροχής εφαρμογών στο Android, γεγονός που έχει ως στόχο την διερεύνηση του επιπέδου ασφαλείας τέτοιων ιστοσελίδων. Έπειτα, έγινε εισαγωγή των δεδομένων σε μια βάση δεδομένων για την εξαγωγή αποτελεσμάτων. Από τα αποτελέσματα που εξάχθηκαν, συμπεραίνουμε ότι οι εφαρμογές του aptoide, απαιτούν κατά μέσο όρο μεγάλο πλήθος δικαιωμάτων, ενώ παρατηρήθηκε και μεγάλο ποσοστό επικίνδυνων αδειών, που ελλοχεύουν κινδύνους για την ιδιωτικότητα των προσωπικών δεδομένων των χρηστών, γεγονός που δείχνει πως τουλάχιστον η συγκεκριμένη ανεπίσημη ιστοσελίδα δεν είναι η κατάλληλη για κατέβασμα εφαρμογών. Αναφορικά με τις πολιτικές ιδιωτικότητας που μελετήθηκαν από δέκα διάσημες εφαρμογές του play store (επίσημη ιστοσελίδα εφαρμογών της Google), διαπιστώθηκε πως καμία πολιτική ιδιωτικότητας δεν ήταν πλήρης βάσει των δικαιωμάτων που απαιτούσε η εφαρμογή, γεγονός που σίγουρα γεννάει προβληματισμούς. Τα παραπάνω συμπεράσματα αυξάνουν την επίγνωση των χρηστών σχετικά με την ιδιωτικότητα στο Android και απαντούν σε μερικούς από τους προβληματισμούς τους αναφορικά με τις άδειες πρόσβασης και τις πολιτικές ιδιωτικότητας. Έτσι έπειτα από την ανάγνωση της παρούσας εργασίας θα είναι σε θέση να διαχωρίζουν τις έννομες από τις κακόβουλες εφαρμογές, αλλά και θα διαπιστώσουν το επίπεδο ασφάλειας που προσφέρουν ανεπίσημες ιστοσελίδες συγκριτικά με την επίσημη ιστοσελίδα εφαρμογών της Google. Ωστόσο βάσει των όσων αναφέρθηκαν στην βιβλιογραφική επισκόπηση της παρούσας έρευνας, εκτός των δικαιωμάτων που απαιτούν οι εφαρμογές, έχει ευθύνη και το ίδιο το Android με το σύστημα δικαιωμάτων που παρέχει στους χρήστες, το οποίο παρουσιάζει αρκετά κενά. Τέλος η συγκεκριμένη εργασία πέρα από την συνεισφορά της στους χρήστες, δίνει κίνητρο και σε μελλοντικούς ερευνητές να αναλύσουν εφαρμογές και από άλλες ανεπίσημες ιστοσελίδες εκτός του aptoide για να υπάρξει μια πιο γενική και ολοκληρωμένη άποψη για τις ανεπίσημες ιστοσελίδες παροχής εφαρμογών.

Περιεχόμενα

Κατάλογος Πινάκων

1.Εισαγωγή

Η αλματώδης εξέλιξη της τεχνολογίας σε συνδυασμό με την ανάγκη των χρηστών για διευθέτηση όλων των εργασιών του από μια πλατφόρμα, η οποία θα χαρακτηρίζεται από φορητότητα και πλήθος λειτουργιών, οδήγησε στην δημιουργία των έξυπνων κινητών τηλεφώνων, κοινώς των smartphones. Τα smartphones εκτός των βασικών λειτουργιών που παρέχει ένα κινητό τηλέφωνο, όπως την λειτουργία τηλεφώνου, γραπτού μηνύματος και ραδιοφώνου, μπορεί να εκτελέσει ακόμα πιο σύνθετες. Ορισμένες από αυτές είναι το GPS(υπηρεσία παγκόσμιου συστήματος προσδιορισμού θέσης), καταγραφή βίντεο, πρόσβαση στον παγκόσμιο ιστό, δυνατότητα διαχείρισης ηλεκτρονικού ταχυδρομείου, αλλά και εγκατάσταση προγραμματισμένων εφαρμογών από τρίτες οντότητες (παιχνίδια, χρήσιμα εργαλεία, κοινωνικά δίκτυα). Για την εγκατάσταση και την λειτουργία, όμως, των παραπάνω εφαρμογών απαιτείται η χρήση κάποιου λειτουργικού συστήματος. Ένα τέτοιο λειτουργικό σύστημα είναι το Android. Το android είναι το πιο δημοφιλές λειτουργικό σύμφωνα με την προτίμηση του κόσμου, για αυτό και η έρευνα της παρούσας εργασίας θα γίνει σε αυτό, με σκοπό την πιο ολοκληρωμένη εξαγωγή συμπερασμάτων. Ωστόσο πολλές από τις εφαρμογές τρίτων προσώπων απαιτούν ορισμένες άδειες πρόσβασης από τον χρήστη (όπως πρόσβαση στην τοποθεσία, στις επαφές, στην κάμερα, στον αποθηκευτικό χώρο). Αυτά τα δεδομένα συλλέγονται από τις εφαρμογές είτε για να εκτελεστούν ορισμένες λειτουργίες της εφαρμογής (παροχή υπηρεσιών), είτε για να διευκολύνουν την περιήγηση του χρήστη στην εφαρμογή είτε για να δημιουργήσουν κάποιο προφίλ του χρήστη, σχετικά με τον τρόπο διαχείρισης της εφαρμογής, είτε για διαμοιρασμό σε συνεργάτες και τρίτες οντότητες (διαφημιστές, εκδότες κ.α.), σκοποί οι οποίοι αναφέρονται στην πολιτική ιδιωτικότητας κάθε εφαρμογής.

Η παρούσα εργασία σχετίζεται με τον τομέα της ασφάλειας και της ιδιωτικότητας σε εφαρμογές του λειτουργικού συστήματος Android, και πως αυτές έχουν πρόσβαση σε προσωπικά-ευαίσθητα δεδομένα των χρηστών. Η εργασία απευθύνεται σε χρήστες που ασχολούνται με την τεχνολογία και πιο συγκεκριμένα με χρήστες που έχουν στην κατοχή τους κινητή συσκευή με το λειτουργικό σύστημα Android. Επίσης απευθύνεται σε μελλοντικούς ερευνητές, δίνοντας τους κίνητρο για εξαγωγή παρόμοιων μελετών, ώστε να υπάρξει μια πιο ολοκληρωμένη άποψη στην συγκεκριμένη θεματολογία. Σκοπός της εργασίας είναι η διερεύνηση και αξιολόγηση των θεμάτων ασφαλείας και ιδιωτικότητας των εφαρμογών στο λειτουργικό σύστημα Android. Στόχοι της εργασίας είναι η εξαγωγή έμπιστων συμπερασμάτων σχετικά με τις άδειες πρόσβασης που απαιτούν δεκάδες εφαρμογές από μια ανεπίσημη ιστοσελίδα εφαρμογών για το Android, το aptoide και η ολοκληρωμένη εξαγωγή συμπερασμάτων αναφορικά με την πληρότητα των πολιτικών ιδιωτικότητας δέκα δημοφιλών εφαρμογών του play store σε σχέση με τις άδειες πρόσβασης που απαιτούν.

Το συγκεκριμένο ερευνητικό αντικείμενο είναι ιδιαίτερα σημαντικό στην σημερινή εποχή, διότι το διαδίκτυο διέπει αρκετούς κινδύνους και η ασφάλεια και η ιδιωτικότητα των προσωπικών-ευαίσθητων δεδομένων των χρηστών πρέπει να θεωρείται δεδομένη και όχι να βρίσκεται υπό αμφισβήτηση. Κάθε φορά που ο χρήστης χρησιμοποιεί μια εφαρμογή δεν μπορεί να είναι σίγουρος για τον τρόπο χρήσης των δεδομένων που δίνει ο ίδιος ή παίρνονται αυτοματοποιημένα από την εφαρμογή και οι τρόποι πειθούς των εφαρμογών (πολιτικές ιδιωτικότητας) δεν παρέχουν την απαραίτητη ασφάλεια στο χρήστη. Για αυτό η συγκεκριμένη εργασία υλοποιήθηκε, για να συνειδητοποιήσουν οι χρήστες ως ένα βαθμό το πλήθος των πληροφοριών που συλλέγονται από τις εφαρμογές μέσω των αδειών πρόσβασης

τους, αλλά και να κατανοήσουν πως οι πολιτικές ιδιωτικότητας δεν τους παρέχουν την απαραίτητη ασφάλεια, αφού οι ίδιες παρουσιάζουν αρκετές ελλείψεις και οι προγραμματιστές βασίζονται στην πεποίθηση ότι ο χρήστης δεν θα ασχοληθεί ή δεν θα συνειδητοποιήσει τα όσα γράφονται μέσα.

Η καινοτομία της παρούσας εργασίας σχετίζεται με την υλοποίηση μιας προγραμματιστικής εφαρμογής σε γλώσσα προγραμματισμού python, που θα εξάγει τις άδειες πρόσβασης των εφαρμογών του aptoide. Επιπλέον η χρήση της ιστοσελίδας του aptoide έγινε τόσο για τον λόγο ότι η συγκεκριμένη ιστοσελίδα δεν έχει μελετηθεί, καθώς όλες οι έρευνες αφορούσαν το play store, την επίσημη ιστοσελίδα που παρέχει η Google για κατέβασμα των εφαρμογών, όσο και για τον λόγο της ανάγκης σύγκρισης μιας ανεπίσημης ιστοσελίδας με την επίσημη για διαπίστωση των διαφορών και παροχή γνώσης στους χρήστες αναφορικά με τα επίπεδα ασφαλείας αυτών.. Τέλος, αναφορικά με τις πολιτικές ιδιωτικότητας, γίνεται ανάλυση των παρόντων πολιτικών ιδιωτικότητας των εφαρμογών, γεγονός που προσφέρει κάτι καινούργιο στην ήδη υπάρχουσα βιβλιογραφία.

Στα επόμενα κεφάλαια της εργασίας θα μελετηθεί η υπάρχουσα βιβλιογραφία αναφορικά με την ιδιωτικότητα και την ασφάλεια στο android όπως οι πολιτικές ιδιωτικότητας και το σύστημα δικαιωμάτων του android, ενώ θα υπάρχει βιβλιογραφική αναφορά στις άδειες πρόσβασης του android, τις αλλαγές στο android marsmallow, τους τύπους αδειών και σε μια έρευνα σχετικά με άδειες πρόσβασης στο Play Store, την οποία θα συγκρίνουμε με την παρούσα στο κεφάλαιο των αποτελεσμάτων της έρευνας. Έπειτα θα γίνει αναφορά στην μεθοδολογία που ακολουθήθηκε στην έρευνα που περιλαμβάνει την μελέτη των αδειών πρόσβασης δεκάδων εφαρμογών στο Aptoide με την χρήση μιας προγραμματιστικής υλοποιημένη σε γλώσσα προγραμματισμού python και την ανάλυση δέκα πολιτικών ιδιωτικότητας διάσημων εφαρμογών στο Android σε σχέση με τα δικαιώματα που συλλέγουν και τον τρόπο που τα χρησιμοποιούν. Τέλος ακολουθούν τα αποτελέσματα και τα συμπεράσματα της έρευνας, όπου θα διαπιστωθεί αν η συγκεκριμένη υλοποιήσει τους στόχους της.

2. Ανάλυση της υπάρχουσας βιβλιογραφίας

2.1. Ιδιωτικότητα

2.1.1. Πολιτικές ιδιωτικότητας σε ιστοσελίδες και εφαρμογές

Οι οργανισμοί οι οποίοι συλλέγουν και επεξεργάζονται προσωπικά δεδομένα διατυπώνουν τις πρακτικές τους υπό μορφή Πολιτικών Ιδιωτικότητας. Η πολιτική ιδιωτικότητας ενός οργανισμού μπορεί να είναι διατυπωμένη σε φυσική γλώσσα και διαθέσιμη μέσω της ιστοσελίδας του οργανισμού ή κωδικοποιημένη σε κάποια γλώσσα, συνήθως σε xml, που μπορεί να γίνει αντιληπτή από προγράμματα λογισμικού. Η πιο δημοφιλής προσέγγιση προς την δεύτερη κατεύθυνση που αναφέραμε είναι η Πλατφόρμα για τις Προτιμήσεις Ιδιωτικότητας (Platform for Privacy Preferences-P3P). Η πλατφόρμα P3P, που πρωτοπαρουσιάστηκε το 1997, έχει επηρεάσει σε μεγάλο βαθμό τις τεχνολογίες ελέγχου πρόσβασης που στοχεύουν στην προστασία της ιδιωτικότητας. Πιο συγκεκριμένα, η πλατφόρμα δίνει την δυνατότητα σε διαδικτυακές ιστοσελίδες να κωδικοποιούν και γνωστοποιούν τις πρακτικές τους αναφορικά με τη συλλογή και τη χρήση προσωπικών δεδομένων με χρήση της XML γλώσσας. Με αυτόν τον τρόπο δίνει η δυνατότητα σε πράκτορες χρηστών (user agents) να αποκτήσουν και να ερμηνεύσουν με αυτοματοποιημένο τρόπο την πολιτική ιδιωτικότητας της ιστοσελίδας και να διαπιστώσουν τον βαθμό συμφωνίας της με τις προτιμήσεις και τις απαιτήσεις του υποκειμένου των δεδομένων. [4]

Μελέτες επανειλημμένα έχουν δείξει ότι οι χρήστες ανησυχούν όλο και περισσότερο για την ιδιωτικότητα τους όταν συνδέονται στο διαδίκτυο. Έρευνα το 2011 έδειξε ότι το 70% των ερωτηθέντων ενδιαφέρεται για την ιδιωτικότητα του στο διαδίκτυο (Jupiter Research). Σε ξεχωριστή μελέτη το 69% των ερωτηθέντων δήλωσε ότι ανησυχεί για επιθέσεις κατά της ιδιωτικότητας και προσπαθεί να αναλάβει δράση για να τις αποφύγουν (Culnan, M. J. and Milne 2001). Σύμφωνα με άλλη έρευνα, το 91% των ιστοτόπων στις ΗΠΑ συλλέγει προσωπικές πληροφορίες και το 90% προσωπικά δεδομένα αναγνώρισης (Adkinson, W. F., Eisenach, J. A., and Lenard T. M. 2002). Λόγω του ενδιαφέροντος του κοινού και των πιέσεων από τις ρυθμιστικές αρχές κάθε ιστοσελίδα σχεδόν ανεβάζει μια πολιτική ιδιωτικότητας προσβάσιμη από όλους. Έρευνα που διεξήγαγε το Ίδρυμα Προόδου και Ελευθερίας, κατέληξε στο συμπέρασμα ότι το 77% του δείγματος (ιστοσελίδες υψηλής επισκεψιμότητας) έχουν δημοσιεύσει μια πολιτική ιδιωτικότητας (Adkinson, W. F., Eisenach, J. A., and Lenard T. M. 2002). Οι πολιτικές ιδιωτικότητας αποσκοπούν στην ενημέρωση των χρηστών σχετικά με τις επιχειρηματικές πρακτικές και χρησιμεύουν ως βάση στην λήψη αποφάσεων των χρηστών (αν τους ικανοποιήσουν ή όχι οι επιχειρηματικές πρακτικές). Υπάρχουν αρκετά προβλήματα με τις πολιτικές ιδιωτικότητας, με κύριο αυτό της αντίθεσης του τι θέλει η εταιρία να εισάγει στις πολιτικές ιδιωτικότητας και τι θέλουν οι χρήστες να γνωρίζουν σχετικά με τις επιχειρηματικές πρακτικές. Κύριος λόγος που διαφέρουν οι πολιτικές ιδιωτικότητας από ιστοσελίδα σε ιστοσελίδα είναι η έλλειψη ρυθμιστικής αρχής ή βιομηχανικών προτύπων όπως η γλώσσα που χρησιμοποιείται στις πολιτικές. Για αυτό είναι δύσκολη η σύγκριση μεταξύ πολιτικών [1]. Άλλο ένα φαινόμενο που παρατηρείται αφορά την αλλαγή της πολιτικής ιδιωτικότητας. Εφόσον οι πολιτικές ιδιωτικότητας δεν εντάσσονται στα πλαίσια κάποιου συμβολαίου, υπόκεινται σε αλλαγές χωρίς την ενημέρωση του καταναλωτή-χρήστη. Για παράδειγμα το Amazon.com υπέστη μια σημαντική τροποποίηση στην πολιτική απορρήτου της, δηλώνοντας ότι η εταιρεία θα

μπορούσα να ανταλλάξει προσωπικά δεδομένα με άλλες εταιρείες χωρίς φυσικά να ενημερώσει τον χρήστη για αυτήν την αλλαγή (CNN 2000) [2].

Πολιτικές ιδιωτικότητας και επικίνδυνα δικαιώματα στις εφαρμογές

Πολλές εφαρμογές στο Android συλλέγουν προσωπικές πληροφορίες χρηστών. Η Google χρειάζεται εφαρμογές που να διαχειρίζονται τα ευαίσθητα προσωπικά δεδομένα των χρηστών, χρησιμοποιώντας πολιτικές ιδιωτικότητας που να περιγράφουν εκτενώς τον τρόπο με τον οποίο μια εφαρμογή συλλέγει, χειρίζεται και διαμοιράζεται τις πληροφορίες των χρηστών (Google 2017). Ωστόσο πολλοί χρήστες δεν ενδιαφέρονται να διαβάσουν τις πολιτικές ιδιωτικότητας, όχι επειδή δεν νοιάζονται για την ιδιωτικότητα τους αλλά επειδή οι πολιτικές είναι συνήθως πολύ εκτενείς ή κάποιες πληροφορίες δεν αναγράφονται (Costante, E., Den Hartog, J. and Petkovic, M., (2011)). Είναι δύσκολο για τους χρήστες να γνωρίζουν ποια δεδομένα τους χρησιμοποιούνται από τις εφαρμογές Android, με αποτέλεσμα να μην μπορούν να εκτιμήσουν τους πιθανούς κινδύνους (Gibler, C., Crussell, J., Erickson, J. and Chen, H., (2012)).

Τα πιο σημαντικά δεδομένα μπορούν να υποκλαπούν κάνοντας χρήση των επικίνδυνων δικαιωμάτων του Android όπως τοποθεσία, επαφές, αποθηκευτικός χώρος κ.α. Σε έρευνα που διεξήγαγαν οι Rawan Baalous και Ronald Poet (2018) σε 73 πολιτικές ιδιωτικότητας αντίστοιχων εφαρμογών, διαπίστωσαν πως 128 τύποι πληροφορίας αντιστοιχούν σε επικίνδυνα δικαιώματα του Android. Στον πίνακα 1 φαίνεται η συχνότητα χρήσης του κάθε επικίνδυνου δικαιώματος από όλες τις εφαρμογές που εξετάστηκαν συνολικά. [3]

Privacy Policy's Terminology	Frequency
Personal information	74%
Phone number/s	34%
Location	30%
Location information	29%
Photo/s	27%
Contact information	26%
Personal data	23%
Telephone number/s	22%
Location data	16%
Address	15%

Πίνακας 1: Επικίνδυνα Δικαιώματα και συχνότητα εμφάνισης τους (Rawan Baalous και Ronald Poet (2018))

2.1.2. Νομοθεσία και αρχές προστασίας της ιδιωτικότητας

Ευρωπαϊκή προσέγγιση

Στην Ευρώπη, τόσο σε εθνικό όσο και σε υπερεθνικό επίπεδο, καταγράφεται το πρώτο νομοθετικό πλαίσιο, αναφορικά με την προστασία των προσωπικών δικαιωμάτων. Μέσα από τα πρώτα νομοθετικά κείμενα, τα οποία τα συναντάμε στα σκανδιναβικά κράτη, καθώς και στη Γερμανία και τη Γαλλία, στην δεκαετία του 1970, συνειδητοποίησαν την σημασία της επεξεργασίας προσωπικών πληροφοριών και τους κινδύνους που μπορούν να επιφέρουν. Η σύμβαση 108/28.1.1981 για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, του Συμβουλίου της Ευρώπης, αποτελεί την πρώτη ουσιαστική, έστω και ελλιπή, αρχή σχετικά με την προστασία προσωπικών δεδομένων, αποτελώντας το δεύτερο νομοθετικό πλαίσιο στην Ευρώπη. Η συγκεκριμένη Σύμβαση εκτός των ρυθμίσεων σχετικά με την επεξεργασία των δεδομένων (αρχή της αναλογικότητας, της ακρίβειας , αρχή του σκοπού), περιείχε ειδικούς κανόνες για τα ευαίσθητα δεδομένα και τα δικαιώματα των χρηστών. Παράλληλα, έθεσε κανόνες, οι οποίοι προστάτευαν τους χρήστες, σε περίπτωση διαρροής των πληροφοριών εκτός συνόρων της χώρας. Ωστόσο, η Σύμβαση δεν έκανε καμία αναφορά στην αναγκαιότητα πρόβλεψης μηχανισμών ανεξαρτήτου ελέγχου, κάτι που προστέθηκε στο πρωτόκολλο του 2001.

Ορόσημο στην προστασία των προσωπικών δεδομένων θεωρείται η κοινοτική οδηγία 95/46/ΕΚ με την οποία επιδιώχθηκε η εναρμόνιση των ευρωπαϊκών νομοθεσιών σε ένα υψηλό επίπεδο προστασίας. Έθεσε συγκεκριμένες προϋποθέσεις, ώστε να γίνει επιτρεπτή η επεξεργασία των δεδομένων των χρηστών. Πιο συγκεκριμένα, επεξεργασία των δεδομένων από το νομοθέτη μπορεί να γίνει α) σε περίπτωση που υπάρξει συγκατάθεση του χρήστη β) εντάσσεται στο πλαίσιο της εκπλήρωσης μια συμβατικής σχέσης γ) είναι αναγκαία για χρήση από το νόμο π.χ. για εξιχνίαση εγκλημάτων δ) αποσκοπεί στο συμφέρον του υποκειμένου των δεδομένων ε)εξυπηρετεί την εκπλήρωση έργου δημοσίου συμφέροντος στ) κρίνεται αναγκαία για την εκπλήρωση ενός έννομου συμφέροντος του υποκειμένου επεξεργασίας.

Ωστόσο, η εισαγωγή στις ψηφιακές τεχνολογίες και πιο συγκεκριμένα στις τηλεπικοινωνίες και στις ηλεκτρονικές επικοινωνίες, δημιούργησε νέες απαιτήσεις, αναφορικά με την διασφάλιση της προστασίας των δεδομένων των χρηστών. Έτσι, η κοινοτική οδηγία 95/46/ΕΚ συμπληρώθηκε από την οδηγία 97/66/ΕΚ για να διαφυλάξει την επεξεργασία δεδομένων των χρηστών και στον τηλεπικοινωνιακό τομέα. Η οδηγία αυτή αντικαταστάθηκε από την οδηγία 2002/58/ΕΚ για την προστασία υποκλοπής προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η οποία οδηγία τελεί υπό τροποποίηση, λόγω ύπαρξης προβλημάτων όπως οι διαδικτυακές διευθύνσεις (IP addresses) [4].

Ελληνικό Κανονιστικό πλαίσιο

Η Ελλάδα υπήρξε από τις πρώτες χώρες που μετέφεραν την κοινοτική οδηγία στο εσωτερικό δίκαιο. Το άρθρο 9Α του συντάγματος ορίζει ότι ο καθένας έχει δικαίωμα προστασίας από τη συλλογή την επεξεργασία και την χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει. Ο νόμος 2472/97 μετέφερε το ρυθμιστικό πλαίσιο της κοινοτικής οδηγίας για την προστασία δεδομένων (95/46/ΕΚ) στο εσωτερικό νομοθετικό πλαίσιο. Ο παραπάνω νόμος συμπληρώθηκε από το

νόμο 3471/06 για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ο οποίος νόμος αντικατέστησε τον 2774/1999. Ο νόμος αυτός, ενσωματώνοντας την οδηγία 2002/58/ΕΚ αποσκοπεί στην εισαγωγή ειδικών ρυθμιστικών διατάξεων, που αφορούν την διασφάλιση του απορρήτου και της ιδιωτικότητας των χρηστών από πρακτικές των παρόχων, όπως εγκατάσταση κακόβουλου λογισμικού παρακολούθησης [4]. Τον νόμο 3471/06 ήρθε να τροποποιήσει ο 3625/2007 και έπειτα ο 3917/2011. Τέλος ο νόμος 4139/2013 ήρθε να προσθέσει έναν νέο, πιο ολοκληρωμένο ορισμό στην έννοια των ευαίσθητων προσωπικών δεδομένων, ενώ νομιμοποιήθηκε η επεξεργασία των προσωπικών δεδομένων από τις δικαστικές-εισαγγελικές αρχές [8].

Γενικός Κανονισμός Προστασίας Δεδομένων

Ο κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, δηλαδή ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Ένωσης, ήρθε για να αντικαταστήσει την κοινοτική οδηγία 95/46/ΕΚ. Στο πλαίσιο του ΓΚΠΔ προσωπικά δεδομένα θεωρούνται οποιαδήποτε δεδομένα σχετίζονται με ένα άτομο όπως ονοματεπώνυμο, διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, δεδομένα τοποθεσίας ή διεύθυνση IP. Επιπλέον, ευαίσθητα προσωπικά δεδομένα όπως θρησκευτικές πεποιθήσεις και ο σεξουαλικός προσανατολισμός, υπάγονται σε επιπλέον προστασία. Οι εταιρείες που βρίσκονται εντός ευρωπαϊκής ένωσης έχουν να διαχειριστούν νέους αυστηρότερους κανόνες ως προς τον τρόπο που διαχειρίζονται τα δεδομένα των χρηστών, καθώς και αυστηρότερες ποινές σε περίπτωση που παραβιάσουν τους συγκεκριμένους κανόνες. Ο νόμος σχεδιάστηκε ώστε οι χρήστες να έχουν μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, επιβάλλοντας νέες υποχρεώσεις σε οργανισμούς που διαχειρίζονται αυτά τα δεδομένα. Πιο συγκεκριμένα οι πολίτες έχουν δικαίωμα να λαμβάνουν ξεκάθαρες πληροφορίες σχετικά με την οντότητα που επεξεργάζεται τα δεδομένα του, αλλά και τον λόγο για τον οποίο τα επεξεργάζεται, να έχουν πρόσβαση στα προσωπικά τους δεδομένα, τα οποία κατέχει ο οργανισμός, να διορθώνουν τα δεδομένα σε περίπτωση λαθεμένης γραφής τους από της εταιρία, να μεταφέρουν δεδομένα από έναν πάροχο υπηρεσιών σε έναν άλλο. Τέλος αλλάζουν οι κανόνες ως προς την συναίνεση των χρηστών, αφού πια οι εταιρείες δεν θα μπορούν να δικαιολογήσουν την έγκριση του χρήστη από μια πολιτική ιδιωτικότητας, η οποία συνήθως είναι και μακροσκελής και αρνείται να διαβάσει η πλειοψηφία του κόσμου [6]. Η Ελλάδα και η Σλοβενία αποτελούν τις μοναδικές χώρες της Ευρωπαϊκής Ένωσης που δεν έχουν επικαιροποίηση του παραπάνω νόμου και την μεταφορά του στην ελληνική έννομη τάξη [7].

Αρχές προστασίας προσωπικών δεδομένων

- **Αρχή του περιορισμούς της συλλογής (collection limitation principle)**: Πρέπει να υπάρχουν όρια στην συλλογή των προσωπικών δεδομένων, η συλλογή τους να συμμορφώνεται με την νομοθεσία, ενημερώνοντας τον χρήστη όπου αυτό απαιτείται.
- **Αρχή της ποιότητας των δεδομένων (data quality principle):** Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν και να χαρακτηρίζονται από πληρότητα και ακρίβεια
- **Αρχή προσδιορισμού του σκοπού (purpose specification principle)**: Ο σκοπός για τον οποίο συλλέγονται τα προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερα κατά την διάρκεια της συλλογής τους
- **Αρχή περιορισμού της χρήσης (use limitation principle):** Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον

προσδιορισμένο σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.

- **Αρχή της προστασίας της ασφάλειας (security safeguards principle):** Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες.
- **Αρχή της συμμετοχής του ατόμου (individual participation principle):** Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:
    1. Να ζητά από τον υπεύθυνο επεξεργασίας, σε περίπτωση που διατίθενται, δεδομένα που σχετίζονται με το εν λόγω άτομο
    2. Να το ανακοινώνονται τα δεδομένα μέσα σε σύντομο χρονικό διάστημα. Αν απαιτεί κόστος η ανακοίνωση τους, αυτό να μην είναι υπερβολικό.
    3. Σε περίπτωση που απορριφθούν αιτήσεις που αναφέρθηκαν στις δύο παραπάνω παραγράφους να δίνεται στο άτομο η δυνατότητα αμφισβήτησης και περαιτέρω διεκδίκησης των δεδομένων
    4. Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτόν
- **Αρχή της ευθύνης (accountability principle):** Κάθε υπεύθυνος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων. [5]

Στις παραπάνω βασικές αρχές για την προστασία των προσωπικών δεδομένων βασίστηκε, μεταξύ άλλων, και η ανάπτυξη της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ, η οποία αναφέρθηκε παραπάνω.

2.2. Ασφάλεια στο Android

2.2.1. Σύστημα δικαιωμάτων android

Σε αυτό το κεφάλαιο θα αναλύσουμε εκτενώς τον τρόπο με τον οποίο λειτουργεί το σύστημα δικαιωμάτων του Android. Πιο συγκεκριμένα:

Δομή API: Το Android API είναι χωρισμένο σε δύο μέρη. Το πρώτο μέρος αποτελείται από μια βιβλιοθήκη που βρίσκεται στον εικονικό χώρο κάθε εφαρμογής και το δεύτερο από μια εφαρμογή του API που τρέχει στις διαδικασίες του συστήματος. Η βιβλιοθήκη API εκτελείται με τα ίδια δικαιώματα που έχει και η εφαρμογή που πρέπει να εκτελεσθεί, ενώ η εφαρμογή API δεν έχει περιορισμούς στα δικαιώματα. Τα δύο μέρη (βιβλιοθήκη και εφαρμογή API) μπορούν να επικοινωνούν και να αλληλεπιδρούν μεταξύ τους. Κλήσεις API που διαβάζουν ή αλλάζουν την κατάσταση του τηλεφώνου εξαπλώνονται από την βιβλιοθήκη στην εφαρμογή του API στην διαδικασία του συστήματος. Οι κλήσεις API χωρίζονται σε τρία στάδια. Στο πρώτο στάδιο η εφαρμογή που τρέχει επικαλείται από την βιβλιοθήκη το δημόσιο API. Στο δεύτερο στάδιο επικαλείται μια ιδιωτική διεπαφή, τον μηχανισμό RPC [12], επίσης από την βιβλιοθήκη. Στο τρίτο στάδιο ο μηχανισμός RPC εκτελεί ένα αίτημα RPC με την διαδικασία του συστήματος, ζητώντας από ένα service του συστήματος να εκτελέσει μια συγκεκριμένη ενέργεια. Μια εφαρμογή μπορεί να

χρησιμοποιήσει Java reflections, δηλαδή ένα API που χρησιμοποιείται για την πρόσβαση ή την επεξεργασία μεθόδων και κλάσεων κατά την διάρκεια της εκτέλεσης της εφαρμογής [9].

Δικαιώματα: Για την επιβολή δικαιωμάτων στο σύστημα του Android, απαιτείται διάφορα τμήματα του συστήματος να επικαλούνται έναν μηχανισμό επικύρωσης δικαιωμάτων, ώστε να γίνει έλεγχος αν μια εφαρμογή που εκτελείται έχει συγκεκριμένη άδεια. Οι έλεγχοι αδειών τοποθετούνται στην εφαρμογή API στην διαδικασία του συστήματος. Όταν κριθεί απαραίτητο η εφαρμογή API καλεί τον μηχανισμό επικύρωσης δικαιωμάτων για να ελέγξει ότι η εφαρμογή έχει τα απαραίτητα δικαιώματα. Κάποιες φορές μπορεί και η βιβλιοθήκη να ελέγξει τα δικαιώματα, αλλά αυτοί οι έλεγχοι μπορεί να μην είναι έμπιστοι, αφού οι εφαρμογές μπορούν να τους παρακάμψουν επικοινωνώντας απευθείας με την διαδικασία του συστήματος μέσω του μηχανισμού RPC. Για αυτό το λόγο οι έλεγχοι δεν πρέπει να πραγματοποιούνται στην βιβλιοθήκη API, αλλά η εφαρμογή API να επικαλείται τον μηχανισμό επικύρωσης δικαιωμάτων. Ωστόσο κάποια δικαιώματα επιβάλλονται από τις ομάδες UNIX, αντί του μηχανισμού επικύρωσης δικαιωμάτων του Android. Μια εφαρμογή όταν εγκαθίσταται με τα δικαιώματα INTERNET, WRITE_EXTERNAL_STORAGE ή BLUETOOTH, εκχωρείται σε μια ομάδα Linux που έχει πρόσβαση στις σχετικές υποδοχές(sockets) και αρχεία. Κατά επέκταση ο πυρήνας του Linux είναι αυτός που αναλαμβάνει την πολιτική ελέγχου για αυτά τα δικαιώματα. Η βιβλιοθήκη API που όπως είπαμε παραπάνω τρέχει με τα ίδια δικαιώματα με την εφαρμογή μπορεί να έχει πρόσβαση απευθείας σε αυτά τα socket και τα αρχεία, χωρίς να απαιτείται η επίκληση της εφαρμογής API στην διαδικασία του συστήματος.

Intents: Το σύστημα intent χρησιμοποιείται και για εσωτερική και για εξωτερική επικοινωνία εντός της εφαρμογής. Ουσιαστικά πρόκειται για ένα αντικείμενο μηνύματος το οποίο μπορείς να χρησιμοποιήσεις για να ζητήσεις πρόσβαση σε ένα άλλο μέρος της εφαρμογής [10] . Για να αποτραπεί από τις εφαρμογές να στέλνουν intents συστήματος, το Android περιορίζει το ποιος έχει δικαίωμα να στείλει συγκεκριμένα Intents. Όλα τα intents στέλνονται μέσω της υπηρεσίας ActivityManagerService, η οποία είναι υπεύθυνη να υποβάλλει κάποιους περιορισμούς. Ένας περιορισμός που μπορεί να θέσει, είναι η αποστολή Intents από εφαρμογές που έχουν κάποια συγκεκριμένα δικαιώματα. Ένας άλλος περιορισμός που μπορεί να θέσει έχει να κάνει με το UID (Unique ID). Πιο συγκεκριμένα να επιτρέψει αποστολές μόνο μέσω διαδικασιών των οποίων το UID είναι ίδιο με του συστήματος. Ωστόσο σε αυτή την περίπτωση τα Intents δεν μπορούν να σταλούν από εφαρμογές, επειδή τα intents πρέπει να προέρχονται από την διαδικασία του συστήματος. Πολύ πιθανόν οι εφαρμογές να χρειάζονται κάποια δικαιώματα για να λάβουν intents. Το λειτουργικό σύστημα χρησιμοποιεί έναν μηχανισμό, θέτοντας ορισμένα δικαιώματα στο intent, για να περιορίσει τους παραλήπτες του intent [11].

2.2.2. Αδυναμίες του συστήματος δικαιωμάτων του Android

- Ύπαρξη κενών ασφαλείας στο αρχείο package.xml το οποίο διατηρεί τις πληροφορίες ρύθμισης πακέτου για κάθε εφαρμογή. Αυτές οι πληροφορίες διαχειρίζονται από μια υπηρεσία συστήματος που ονομάζεται PackageManager και αποτελεί μια από τις σημαντικότερες υπηρεσίες του συστήματος δικαιωμάτων. Οι πληροφορίες ρύθμισης πακέτου μιας εφαρμογής περιέχουν στοιχεία όπως τα δικαιώματα της εφαρμογής, την πιστοποίηση, το UID, την διαδρομή

κ.α. Κάθε μία από τις πληροφορίες ρύθμισης πακέτου χαρακτηρίζεται ως κόμβος <package> στο package.xml αρχείο. Το package.xml αρχείο, ως αρχείο του συστήματος ανήκει στον χρήστη που διαχειρίζεται το λειτουργικό και κανένας άλλος χρήστης δεν μπορεί να έχει πρόσβαση σε αυτό. Σε αυτό φυσικά συμβάλει το γεγονός ότι το σύστημα δικαιωμάτων είναι βασισμένο σε Linux που ελέγχει τον χρήστη που προσπαθεί να έχει πρόσβαση εκεί. Ωστόσο, στην περίπτωση που αποκτηθούν δικαιώματα διαχειριστή το σύστημα δικαιωμάτων αυτομάτως είναι μη έγκυρο και το αρχείο xml γίνεται προσβάσιμο από ένα κακόβουλο λογισμικό (malware), έχοντας την δυνατότητα να προσθέσει όποια δικαιώματα θελήσει στο ίδιο, αλλά και σε άλλες εφαρμογές.

- Κατά την εκκίνηση του συστήματος όλες οι εφαρμογές, είτε πρόκειται για εφαρμογές συστήματος είτε όχι, θα εγκατασταθούν εκ νέου από την αρχή. Για μία εφαρμογή εκτός συστήματος αν υπάρχει ο κόμβος <package>, τα δικαιώματα της εφαρμογής θα αποκτηθούν από τον κόμβο. Ωστόσο, αν ο κόμβος <package> έχει αφαιρεθεί, η εφαρμογή φαίνεται σαν να μην υπάρχει στο σύστημα. Τότε, η υπηρεσία PackageManager προσπαθεί να εγκαταστήσει εκ νέου την εφαρμογή και να δώσει δικαιώματα στην εφαρμογή χρησιμοποιώντας το αρχείο AndroidManifest.xml. Αυτός ο τρόπος λειτουργίας του λειτουργικού δίνει την δυνατότητα στο κακόβουλο λογισμικό να διαγράψει τον κόμβο <package> και να δώσει εντολή στην υπηρεσία PackageManager να εγκαταστήσει μια κακόβουλη έκδοση αυτού του κόμβου
- Ο έλεγχος ταυτότητας μια εφαρμογής συστήματος δεν είναι επαρκής. Οι εφαρμογές συστήματος είναι πιο σημαντικές από τις εφαρμογές που δεν ανήκουν στο σύστημα. Ωστόσο, δεν υπάρχει κάποια απαίτηση πιστοποίησης για τις εφαρμογές συστήματος. Επίσης οι εφαρμογές συστήματος έχουν μηχανισμό αυτόματης πιστοποίησης, γεγονός που καθιστά εφικτό να αντικατασταθούν από μια επιβλαβή εφαρμογή. Το κακόβουλο λογισμικό δεν είναι απαραίτητο να υπογραφεί από το ίδιο πιστοποιητικό που έχει η γνήσια εφαρμογή. Επιπλέον σε σχέση με τις τρίτες εφαρμογές, οι εφαρμογές συστήματος παίρνουν άμεσα τα δικαιώματα που τους αντιστοιχούν από το manifest αρχείο. Αυτό μπορεί να λειτουργήσει ως πλεονέκτημα στα κακόβουλα προγράμματα, καθώς μπορούν να υλοποιηθούν ώστε να λειτουργούν σαν εφαρμογή συστήματος. Το σύστημα δικαιωμάτων επεξεργάζεται τις εφαρμογές στον κατάλογο /system/app ως εφαρμογές συστήματος. Αν το κακόβουλο λογισμικό τοποθετηθεί στην παραπάνω διαδρομή, τότε μπορεί να λειτουργήσει ως εφαρμογή συστήματος, ανεξάρτητα από την εγκυρότητα των πιστοποιητικών που διαθέτει. [13]

Αν αναλογιστούμε τα όσα προαναφέρθηκαν οι επιτιθέμενοι μπορούν να εκτελέσουν διάφορες επιθέσεις κατά των δικαιωμάτων που απαιτούν είτε οι εφαρμογές συστήματος, είτε οι μη συστήματος. Αναλύοντας τα δεδομένα από τα δικαιώματα που απέκτησαν πρόσβαση, μπορούν να κλέψουν σημαντικά ιδιωτικά δεδομένα του χρήστη, τα οποία σίγουρα αν ήταν εν γνώσει του και στην κρίση του, δεν θα έδινε την άδεια να κλαπούν.

2.2.3. Repackaging εφαρμογών και third party markets

Τα τελευταία χρόνια έχει παρατηρηθεί μεγάλη αύξηση στα ανεπίσημα third-party android markets, κυρίως λόγω της μεγάλης ζήτησης από τους χρήστες. Ο κύριος λόγος που οι χρήστες επιλέγουν third party markets έναντι του google play store, είναι η δύναμη που έχει η Google σε κάθε λογαριασμό που δημιουργεί ο πελάτης για να έχει πρόσβαση στην ιστοσελίδα εφαρμογών της. Υπήρχαν αρκετές

περιπτώσεις που η Google χρησιμοποίησε κάποια “backdoor” για να διαγράψει εφαρμογές που είχε κατεβάσει ο χρήστης και τις θεωρούσε επιβλαβής. Σύμφωνα με εμπειρογνώμονες στο θέμα της ασφάλειας κανείς δεν θα πρέπει να έχει τόσο μεγάλη εξουσία στους πελάτες της (Keizer, 2011). Ταυτόχρονα όμως αυξήθηκε και ο αριθμός των πλαστών και κακόβουλων εφαρμογών. Σύμφωνα με έρευνα το 2012, μεταξύ 5% και 13% των εφαρμογών που κατέβηκαν από third party markets είχαν επεξεργαστεί από την επίσημη έκδοση της εφαρμογής με την τεχνική του repackaging (Zhou et al. 2012) [14]. Ουσιαστικά ο όρος repackaging είναι ένα είδος επίθεσης που παρατηρείται πολύ συχνά στο android. Οι επιτιθέμενοι επεξεργάζονται την αυθεντική εφαρμογή που υπάρχει στο google play store (το επίσημο market της google όπου ανεβαίνουν εκατομμύρια εφαρμογές) αποσυμπιέζοντας την, χρησιμοποιώντας την τεχνική του reverse engineer, προσθέτουν κάποιο επιβλαβές στοιχείο και ξανά συμπιέζουν την εφαρμογή και την ανεβάζουν σε κάποιο third party market. Οι χρήστες από την μεριά τους δεν μπορούν να κατανοήσουν την διαφορά της επίσημης εφαρμογής με την επεξεργασμένη, ειδικά όταν πρόκειται για έναν μέσο χρήστη ενός κινητού τηλεφώνου που στερείται αυτών των γνώσεων [15]. Ωστόσο υπάρχουν αρκετές τεχνικές, με τις οποίες μπορείς να διακρίνεις repackaged εφαρμογές. Η πιο εύκολη τεχνική, σχετίζεται με τα δικαιώματα των εφαρμογών. Οι repackaged εφαρμογές απαιτούν περισσότερα δικαιώματα από ότι οι επίσημες εφαρμογές. Οι επιτιθέμενοι όταν προσθέτουν διαφορετικές διαφημίσεις ή κάποιου άλλους είδους κακόβουλο λογισμικό, συνήθως προσθέτουν περισσότερα δικαιώματα στην εφαρμογή [16]. Όποτε ο χρήστης κάνοντας μια σύγκριση των δικαιωμάτων που απαιτεί η εφαρμογή από την επίσημη ιστοσελίδα εφαρμογών του android με την αντίστοιχη ιστοσελίδα ενός third party market μπορεί να διαπιστώσει αν το πλήθος των δικαιωμάτων της εφαρμογής που τον ενδιαφέρει διαφέρει από ιστοσελίδα σε ιστοσελίδα.

Παρότι των όσων ειπώθηκαν παραπάνω, τα third party markets, συνεχώς εξελίσσονται. Σύμφωνα με έρευνα του πανεπιστημίου Politecnico di Milano(2013), βρέθηκαν ογδόντα εννιά (89) διαφορετικά android markets χρησιμοποιώντας το εργαλείο AndroCracwl. Επιπλέον, είναι ενδιαφέρον να επισημάνουμε ότι η Κίνα είναι η χώρα με τα περισσότερα markets. Ο λόγος που παρατηρείται αυτό το φαινόμενο είναι πως η Κίνα αποτελεί την μόνη χώρα στο κόσμο που δεν επιτρέπεται το Google play store [14]. Αν αναλογιστούμε τον πληθυσμό της Κίνας λοιπόν η χρήση εναλλακτικών android market είναι πολύ σημαντική για την διασημότητα του λειτουργικού Android. Το μεγάλο πλήθος third-party markets, οδηγεί στην δημιουργία ολοένα και περισσότερων ανταγωνιστών στο χώρο. Το κάθε market προσπαθεί να εντυπωσιάσει με τις δυνατότητες του, ώστε να προσελκύσει όσο περισσότερο κόσμο μπορεί (όπως κριτικές της εφαρμογής, προτάσεις για παρόμοιες εφαρμογές, σύνθετη αναζήτηση εφαρμογών, έκδοση εφαρμογής, ημερομηνία τελευταίας αναβάθμισης, εμφανή δικαιώματα που απαιτεί η εφαρμογή κ.α.). Ωστόσο, τα περισσότερα markets δεν προσφέρουν πολιτικές ιδιωτικότητας ή οι πολιτικές ιδιωτικότητας δεν είναι ξεκάθαρες ως προς τον χρήστη. Επίσης μόνο λίγα από αυτά προσφέρουν σύστημα προστασίας adivirus για σάρωση των εφαρμογών που ανεβαίνουν στην ιστοσελίδα τους, με αποτέλεσμα πολλές από τις εφαρμογές να είναι «μολυσμένες» με malware. Σύμφωνα με έρευνα του Yi Ying Ng (2014) [14], η οποία επικεντρώθηκε κυρίως στην Κίνα, το 36% των εφαρμογών που αναλύθηκαν σε ανεπίσημα markets, διαπιστώθηκε πως ήταν ύποπτες. Οι προγραμματιστές ανεβάζοντας και διαγράφοντας συνεχώς τις εφαρμογές τους από τα third-party markets σε συνδυασμό με το μεγάλο πλήθος εφαρμογών που ανεβαίνουν στην ιστοσελίδα και την δυσκολία ανάλυσης του κώδικα όλων των εφαρμογών που ανεβαίνουν καθημερινά στην ιστοσελίδα, καταφέρνουν να επιτύχουν την άρνηση ενασχόλησης των ιδιοκτητών της ιστοσελίδας με το τρέχον πρόβλημα (Ng et al. 2014).

Ακόμα μια έρευνα που έχει ως στόχο την εκτενέστερη ανάλυση και αιτιολόγηση των όσων ειπώθηκαν στο κεφάλαιο μέχρι στιγμής έγινε από τους Sajal Rastogi, Kriti Bhushan, B. B. Gupta (2015) [16]. Οι ίδιοι κατεβάζοντας πενήντα εφαρμογές από το google play και το Mobogenie (ένα third-party market) αντίστοιχα, με πάνω από εκατό εκατομμύρια λήψεις η κάθε μία, συμπέραναν πως αν και πρόκειται για τις ίδιες εφαρμογές κάποιες από αυτές διέφεραν στα δικαιώματα. Πιο συγκεκριμένα διαπίστωσαν πως έξι από τις πενήντα εφαρμογές, ζητούσαν περισσότερα δικαιώματα από το Mobogenie σε σχέση με την επίσημη ιστοσελίδα της google, ενώ οι υπόλοιπες ζητούσαν ακριβώς το ίδιο πλήθος δικαιωμάτων. Αυτό μας οδηγεί στο συμπέρασμα ότι οι εφαρμογές που απαιτούσαν περισσότερα δικαιώματα από το Mobogenie είναι repackaged και είτε έχουν κάποιον επιβλαβές κώδικα, είτε κάποιες επιπλέον διαφημίσεις, είτε ορισμένες παραμετροποιήσεις στις παραμέτρους των χρημάτων που απαιτούνται για αγορές αντικειμένων ή δυνατοτήτων εντός της εφαρμογής.

Φυσικά, υπάρχει και η πλευρά των επίσημων προγραμματιστών των εφαρμογών, οι οποίοι επηρεάζονται από τα third party markets. Ας πάρουμε για παράδειγμα μια εφαρμογή που ο προγραμματιστής την προσφέρει δωρεάν και εισπράττει χρήματα από τις διαφημίσεις εντός της εφαρμογής. Αν ο χρήστης κατεβάσει την εφαρμογή από την επίσημη ιστοσελίδα εφαρμογών της google (google play store), τότε τα χρήματα τα εισπράττει όπως είναι λογικό ο προγραμματιστής. Ωστόσο, αν μια τρίτη οντότητα κάνει repackage την εφαρμογή και προσθέσει δικές του διαφημίσεις, γεγονός που αποτελεί το πιο συχνό φαινόμενο των repackaged εφαρμογών, τότε εφόσον ο χρήστης κατεβάσει την εφαρμογή από το third party market, στο οποίο ανέβηκε η συγκεκριμένη εφαρμογή τότε τα χρήματα τα εισπράττει η τρίτη οντότητα και όχι ο επίσημος προγραμματιστής της εφαρμογής. Το ίδιο συμβαίνει και όταν οι εφαρμογές (κυρίως παιχνίδια), ζητάνε χρήματα μέσω αγορών αντικειμένων εντός εφαρμογής. Ακόμα και όταν η εφαρμογή είναι εντελώς δωρεάν και ο επίσημος προγραμματιστής δεν έχει κάποιο κέρδος από αυτήν, η repackaged εφαρμογή θα επηρεάσει την φήμη του και οι χρήστες δεν θα εμπιστεύονται μελλοντικές εφαρμογές από αυτόν τον προγραμματιστή.

Marketplace	URL	Language
AndroidBlip	http://www.androidblip.com/	English
AppsLib	http://www.appslib.com/	English
F-Droid	http://www.f-droid.org	English
GetJar	http://m.getjar.com/	English
AppMarket	http://indiroid.com/	Turkish
Soc.io	http://soc.io/	English
Andiim3	http://andiim3.com	English
Android	http://androidis.ru	Russian
AndroidPhones.ru	http://android-phones.ru/category/files/	Russian
Anzhi	http://www.anzhi.com	Chinese
Aptoide	http://aptoide.com	English
Amazon AppStore	http://www.amazon.it/mobile-apps/b?node=1661660031	English
Hiapk	http://hiapk.com	Chinese
Opera Mobile Store	http://apps.opera.com/	English
Mikandi	http://mikandi.com	English
Myandroid.su	http://myandroid.su/index.php/catprog	Russian
Wandojia	http://wandoujia.com/	Chinese
Androidpit	http://www.androidpit.com	English
1Mobile	http://www.1mobile.com	English
92apk	http://www.92apk.com	Chinese
Android online	http://www.androidonline.net	Chinese
Appchina.com	http://www.appchina.com	Chinese
Appitalism	http://www.appitalism.com	English
Eomarket.com	http://www.eomarket.com	Chinese
Insyde Market	http://www.insydemarket.com	English
Nduoa	http://www.nduoa.com	Chinese
SlideMe	http://slideme.org	English
SjApk	http://www.sjapk.com	Chinese
Xda Developers	http://forum.xda-developers.com	English
4PDA	http://4pda.ru/forum/index.php?showforum=281	Russian
Softportal	http://www.softportal.com/dlcategory-1649.html	Russian
AppBrain	http://www.appbrain.com/	English
Apk gfan	http://apk.gfan.com/	Chinese
ProAndroid.net	http://www.proandroid.net/	Russian
Andapponline	https://www.andapponline.com/	English
AppsZoom	http://www.appszoom.com/	English
AndroLib	http://www.androlib.com/	English
Camangi	http://www.camangimarket.com/	English
ESDN	http://www.esdn.ws/mobile-applications-market	English
T-app	http://tapp.ru/	Russian
Jimi168	http://www.jimi168.com/	Chinese
Android MyApp	http://android.myapp.com	Chinese
D.cn	http://android.d.cn/	Chinese
Hami apps	http://hamiapps.emome.net/	Taiwanese
Lenovo	http://3g.lenovomm.com/	Chinese
Mobango	http://www.mobango.com	English
Nexva.com	http://nexva.com	English
Panda app	http://download.pandaapp.com	English
T-store	http://www.tstore.co.kr	Korean
Taobao	http://app.taobao.com	Chinese
Yandex	http://store.yandex.com/	Russian
BrotherSoft	http://android.brothersoft.com/	English
Mobo Market	http://store.moborobo.com	English
AppZil	http://www.appzil.com/	Korean
Freeware Lovers	http://www.freewarelovers.com/	English
Android Downloadz	http://www.androiddownloadz.com/	English
CoolApk	http://www.coolapk.com	Chinese
APKS	http://www.apk5.com/	Chinese
APK	http://apk.imobile.com.cn/	Chinese
Cooyo	http://www.cooyo.com/	Chinese
Aibala	http://www.aibala.com/	Chinese
AppVN	http://appstore.vn/android/	English
AppTomato	http://apptomato.com/	English
Mobogenie	http://www.mobogenie.com/	English
GetBazaar	http://getbazaar.com/en/	Arabic
RepoDroid	http://repodroid.com/	English
GetApk	http://getapk.co/	English
Samsung Galaxy App	http://samsungapps.sina.cn/main/getMain.as	English
189store	http://www.189store.com	Chinese
Baidu Mobile	http://as.baidu.com	Chinese
Sogou	http://app.sogou.com	Chinese
Zhushou 360	http://zhushou.360.cn	Chinese
25PP	http://apps.uc.cn	Chinese
CNMO	http://app.cnmo.com	Chinese
Removed Apps	http://www.removedapps.com	English
Appdh.com	http://www.appdh.com/	Chinese
Apps Apk	http://www.appsapk.com	English
Mobile Apk World	http://mobileapkworld.com	English
AndroidPit	https://www.androidpit.com/	English

Πίνακας 2:Third-Party Markets που βρέθηκαν το Σεπτέμβριο 2015 (W.J.Buchanan et al.(2017))

2.2.4. Δικαιώματα και διαχειριστής root

Στη σημερινή εποχή το λειτουργικό σύστημα Android αποτελεί το πιο διάσημο λειτουργικό για τις κινητές συσκευές. Για αυτό και η κλοπή προσωπικών δεδομένων με την εγκατάσταση κάποιου malware αποτελεί ο κύριος στόχος μια επίθεσης προς τις συγκεκριμένες συσκευές. Για να προστατευθούν οι χρήστες από αυτό το φαινόμενο το Android χρησιμοποιεί ένα μηχανισμό ασφαλείας για να προστατεύσει τους βασικούς πόρους του συστήματος. Αυτός ο μηχανισμός ονομάζεται σύστημα δικαιωμάτων [13]. Τα δεδομένα των χρηστών μπορούν να κλαπούν χρησιμοποιώντας είτε σένσορες (όπως η κάμερα και το μικρόφωνο), είτε επικοινωνιακά πρωτόκολλα (όπως το 3g και wifi). Ωστόσο όλοι οι πόροι από τους παραπάνω σένσορες και πρωτόκολλα είναι προστατευμένα από το σύστημα δικαιωμάτων του Android, γεγονός που επιτρέπει μόνο στις εφαρμογές που έχουν κάποιο από τα αντίστοιχα δικαιώματα να έχουν πρόσβαση στους συγκεκριμένους πόρους του συστήματος [17].

Εκτός από τα δικαιώματα όμως, και οι διαχειριστές-root μπορούν να έχουν πρόσβαση στους πόρους του συστήματος. Η συσκευή android που αγοράζει ο κάθε καταναλωτής είναι “Unroot” δηλαδή ο χρήστης δεν έχει δικαιώματα διαχειριστή στην συσκευή οπότε δεν μπορεί να παρέμβει στους πόρους του συστήματος. Ωστόσο, πολλοί είναι εκείνοι που θέλουν να αποκτήσουν πλήρης πρόσβαση στους πόρους του λειτουργικού, ώστε να έχουν ορισμένα πλεονεκτήματα όπως να απεγκαθιστούν εφαρμογές του συστήματος που δεν χρειάζονται, να δημιουργούν εφεδρικά αντίγραφα ασφαλείας των εφαρμογών και των αρχείων τους, να απενεργοποιήσουν τις διαφημίσεις από τις εφαρμογές και να εγκαθιστούν άλλα λειτουργικά συστήματα από τρίτες οντότητες. Σύμφωνα με έρευνα της NetQin(2012) [17] 23% των κινητών στην Κίνα έχουν γίνει root έστω μία φορά το πρώτο εξάμηνο του 2012, γεγονός που δείχνει πως πολλοί είναι αυτοί που έχουν ενθουσιαστεί από τις δυνατότητες που προσφέρει το root. Ωστόσο, υπάρχει ένα μεγάλο κενό ασφαλείας που ίσως δεν αναλογίζονται οι χρήστες όταν αποφασίζουν να αποκτήσουν δικαιώματα διαχειριστή στην συσκευή τους. Στις rooted συσκευές το malware μπορεί να τρέξει με δικαιώματα διαχειριστή, δηλαδή να προσπεράσει τον έλεγχο του συστήματος δικαιωμάτων και να έχει πρόσβαση στα ιδιωτικά δεδομένα του χρήστη όπως (μηνύματα, επαφές, κάμερα κ.α.) [17]. Σύμφωνα με έρευνα του YaJin Zhou et al. [13] ότι το 36,7% των malware επηρέασαν συσκευές που είχαν δικαιώματα διαχειριστή και απέκτησαν πρόσβαση σε προσωπικά δεδομένα του χρήστη. Έτσι για να μην μπορεί το Malware να έχει δικαιώματα πρόσβασης root πρέπει ο χρήστης να προβεί σε unroot της συσκευής. Με αυτόν τον τρόπο το malware δεν θα έχει πρόσβαση στους πόρους του συστήματος. Βέβαια και πάλι ο χρήστης δεν μπορεί να νιώθει προστατευμένος γιατί όπως θα δούμε στο επόμενο κεφάλαιο υπάρχουν κάποιες αδυναμίες στο σύστημα δικαιωμάτων που μπορούν να δημιουργήσουν κενά ασφαλείας στο λειτουργικό.

Πριν δούμε τις αδυναμίες του συστήματος δικαιωμάτων, ας εμβαθύνουμε στο πρόβλημα του root λίγο περισσότερο. Όπως είπαμε παραπάνω ο χρήστης μπορεί να προβεί όποια στιγμή θελήσει σε unroot της συσκευής. Εξάλλου, η διαδικασία επαναφοράς σε unroot κατάσταση διαρκεί κάτω από ένα λεπτό και είναι ιδιαίτερα εύκολη. Για αυτό το λόγο σύμφωνα με το [13], το malware πρέπει να συνεχίσει να λειτουργεί ακόμα και όταν το κινητό επανέλθει σε unroot κατάσταση. Για να επιτευχθεί αυτό κατά την διάρκεια του root να πραγματοποιηθούν δύο είδους επιθέσεις. Στην πρώτη να αλλοιωθούν αρχεία δεδομένων ώστε να υπάρχει πρόσβαση στα απαιτούμενα δικαιώματα και με αυτόν τον τρόπο να μπορεί το malware να περνάει τον έλεγχο ασφαλείας του συστήματος δικαιωμάτων όποτε θέλει ή να αλλοιωθεί ο κώδικας στα αρχεία του συστήματος δικαιωμάτων ώστε να διαγραφούν τυχόν περιορισμοί στην πρόσβαση.

2.2.5. Ο ρόλος του Linux User ID (UID) και η εκμετάλλευση του από Malwares

Κατά προεπιλογή κατά την εγκατάσταση μιας εφαρμογής, το Android δίνει ένα ξεχωριστό αναγνωριστικό στην εφαρμογή, το οποίο ονομάζεται User ID (ή UID) και η εφαρμογή τρέχει σαν ένας ανεξάρτητος χρήστης Linux. Ωστόσο το android δεν παρέχει κάποιο περιορισμό στις πιστοποιήσεις των εφαρμογών και επιτρέπει σε διαφορετικές εφαρμογές να έχουν το ίδιο UID, αν και σε αυτή την περίπτωση απαιτεί να έχουν υπογραφεί με το ίδιο πιστοποιητικό. Οι εφαρμογές με το ίδιο UID μπορούν να τρέξουν με τα ίδια δικαιώματα, να μοιράζονται τα δεδομένα τους, ακόμα και να τρέχουν στην ίδια διεργασία του συστήματος. Επίσης κάποιες εφαρμογές συστήματος μπορούν να μοιράζονται το ίδιο UID. Ωστόσο κάποιο Malware δεν μπορεί να μοιραστεί το ίδιο UID με άλλες εφαρμογές, επειδή τα πιστοποιητικά δεν αντιστοιχούν. Σε αντίθεση με το παραπάνω, αν μια εφαρμογή τηρεί ορισμένες προδιαγραφές, το σύστημα δικαιωμάτων του android δεν μπορεί να επικυρώσει το πιστοποιητικό υπογραφής της εφαρμογής και με αυτόν τον τρόπο το malware μοιράζεται το ίδιο UID με την εφαρμογή. Επίσης, σε περίπτωση που ο χρήστης του κινητού έχει δικαιώματα διαχειριστή στο λειτουργικό σύστημα (root) τα πράγματα γίνονται ακόμα πιο εύκολα για τον επιτιθέμενο. Όπως αναφέραμε παραπάνω, κατά την διάρκεια της εγκατάστασης μια εφαρμογής, δίνεται στην εφαρμογή ένα ξεχωριστό UID. Αυτό το ID είναι συνήθως πάνω από 10000. Από την στιγμή που θα δωθεί αυτό το ID στην εφαρμογή δεν μπορεί να αλλάξει. Ωστόσο όταν το λειτουργικό σύστημα είναι rooted, το UID της εφαρμογής μπορεί να αλλάξει σε 0, το οποίο είναι το UID του root. Με αυτόν τον τρόπο εφόσον είναι γνωστό το UID της εφαρμογής, το malware και πάλι μπορεί να μοιράζεται το ίδιο UID με την εφαρμογή. [17]

2.2.6. Ερευνητική προσέγγιση για τους λόγους χρήσης των δικαιωμάτων των εφαρμογών

Οι εφαρμογές του Android συχνά ζητούν πρόσβαση σε προσωπικά δεδομένα του χρήστης, όπως δεδομένα τοποθεσίας και λίστες επαφών. Αν και το Android απαιτεί από τους προγραμματιστές να δηλώνουν τι δικαιώματα χρησιμοποιεί η εφαρμογή που προγραμμάτισαν, δεν χρησιμοποιεί κάποιο μηχανισμό για να γίνει εμφανής ο τρόπος με τον οποίο χρησιμοποιούνται τα προσωπικά του δεδομένα. Αν το αναλύσουμε περαιτέρω, μια εφαρμογή μπορεί να χρησιμοποιήσει ένα δικαίωμα για πολλαπλούς σκοπούς. Για παράδειγμα μια εφαρμογή που απαιτεί πρόσβαση στην τοποθεσία, μπορεί να την χρησιμοποιήσει για πολλαπλούς λόγους όπως διαφήμιση, γεωγραφική θέση του χρήστη, αναζήτηση για κοντινούς προορισμούς. Οι χρήστες δεν μπορούν με κάποιον τρόπο να καταλάβουν πως και για ποιο λόγο χρησιμοποιείται ένα συγκεκριμένο προσωπικό του δεδομένο από την εφαρμογή.

Έρευνες προσπάθησαν να ανακαλύψουν μεθόδους ώστε να γεφυρώσουν αυτό το κενό που υπάρχει μεταξύ χρηστών και λειτουργίας της εφαρμογής. Ο Whyper (Pandita et al. 2013) εφάρμοσε τεχνικές επεξεργασίας φυσικής γλώσσας την περιγραφή των εφαρμογών για να συμπεράνει την χρήση των δικαιωμάτων. Chabada (Gorla et al. 2014) ομαδοποιούσε εφαρμογές σύμφωνα με τις περιγραφές τους, για να προσδιορίσει την απόδοση από κάθε ομαδοποίηση χρησιμοποιώντας το API. Ο Riskmon (Jing et al. 2014) δημιούργησε μια βασική γραμμή αξιολόγησης κινδύνου για κάθε χρήστη σύμφωνα με τις προσδοκίες του χρήστη και τις συμπεριφορές κατά τη διάρκεια εκτέλεσης αξιόπιστων εφαρμογών, η οποία μπορεί να χρησιμοποιηθεί για την εκτίμηση των κινδύνων χρήσης των ευαίσθητων πληροφοριών του χρήση και την ταξινόμηση εφαρμογών. Ο Amini et al. (2013) παρουσίασε ένα εργαλείο, το Gort, το

οποίο συνδύαζε το crowdsourcing (εξωτερική ανάθεση καθηκόντων σε εθελοντές χρήστες) και τη δυναμική ανάλυση, γεγονός που βοηθούσε τους χρήστες καταλάβουν ασυνήθιστες συμπεριφορές εφαρμογών. [18]

Οι Haoyu Wang, Yuanchun Li, Yao Guo, Yuvraj Agarwal, και Jason I. Hong. (2017) χρησιμοποίησαν την μέθοδο εξόρυξης κειμένου για να διαπιστώσουν τον σκοπό για τον οποίο χρησιμοποιούνται τα δικαιώματα στις εφαρμογές. Η εφαρμογή, στον Java κώδικα της, περιέχει κείμενο με διάφορα αναγνωριστικά, όπως ονόματα κλάσεων, ονόματα μεθόδων και ονόματα πεδίων. Αναλύοντας αυτά τα πεδία είναι εύκολο να συνειδητοποιήσει κανείς τι υλοποιεί ο κώδικας. Έτσι, αν βρεθεί κάποιος προσαρμοσμένος κώδικας (custom code) που χρησιμοποιεί το δικαίωμα της τοποθεσίας για παράδειγμα, και υπάρχει μέθοδος ή κλάση ή μεταβλητή με όνομα “photo” ή “tag” είναι πολύ πιθανόν η εφαρμογή να χρησιμοποιεί το δικαίωμα της τοποθεσίας για ανίχνευση θέσης. Στην συγκεκριμένη έρευνα χρησιμοποιήθηκαν τα δεδομένα από την τοποθεσία και από τις επαφές γιατί προηγούμενες έρευνες έδειξαν ότι οι χρήστες ανησυχούν περισσότερο για αυτά. Στην έρευνα λήφθηκαν υπόψιν 10 λόγοι για χρήση του δικαιώματος τοποθεσίας και 10 λόγοι για χρήση του δικαιώματος επαφών όπως φαίνονται στον Πίνακα 3. Επίσης, εξετάστηκε η συμπεριφορά από 460 περιπτώσεις που χρησιμοποιούσαν την τοποθεσία σε 305 επιλεγμένες εφαρμογές και από 560 περιπτώσεις που χρησιμοποιούσαν τις επαφές σε 317 εφαρμογές. Τα αποτελέσματα της έρευνας έδειξαν ότι σε 85% των περιπτώσεων κατάφεραν να διαπιστώσουν τον λόγο της χρήσης του δικαιώματος της τοποθεσίας και σε 94% των περιπτώσεων τον λόγο χρήσης της λιστας επαφών. Να τονίσουμε ότι στην έρευνα δεν συμπεριλήφθηκαν ενσωματωμένες βιβλιοθήκες τρίτων οντοτήτων. Μια τέτοια μέθοδος εξόρυξης κειμένου, εφόσον εμφανίζει μεγάλο ποσοστό επιτυχίας θα μπορούσε να αναπτυχθεί από τους προγραμματιστές του Play Store, ώστε να βοηθήσει τους χρήστες να συνειδητοποιήσουν πως χρησιμοποιούνται τα δικαιώματα των εφαρμογών και για ποιο λόγο. Βέβαια, μια τέτοια υλοποίηση ίσως δεν συμφέρει ούτε την google, ούτε τους προγραμματιστές των τρίτων εφαρμογών, επειδή μπορεί να υπάρξει μείωση στα κέρδη τους, αφού οι συνειδητοποιημένοι πια χρήστες ίσως να μην προβαίνουν σε κατέβασμα των εφαρμογών τους.

Τέλος σε έρευνα του ο Lin et al. (2012, 2014) κατηγοριοποίησε χειροκίνητα 400 διάσημες βιβλιοθήκες τρίτων οντοτήτων (third-party libraries) βασιζόμενος στην λειτουργικότητα τους και χρησιμοποίησε αυτές τις κατηγορίες για να καταλάβει τον λόγο της χρήσης των δικαιωμάτων από κάθε βιβλιοθήκη. Έτσι κατηγοριοποίησε τις βιβλιοθήκες σε 9 διαφορετικούς λόγους χρήσης τους όπως φαίνεται στον Πίνακα 3. [18]

Τύπος	Δικαιώματα	Λόγοι χρήσης
Λόγοι χρήσης των δικαιωμάτων σε βιβλιοθήκες τρίτων οντοτήτων (Lin et al 2012)	Όλα τα δικαιώματα	Advertising, analytics, social networking, utilities, development aid, social games, secondary market, payment, game engine
Λόγοι χρήσης των δικαιωμάτων σε προσαρμοσμένο κώδικα (Haoyu Wang, Yuanchun Li, Yao Guo, Yuvraj Agarwal, και Jason I. Hong. (2017))	Τοποθεσία	search nearby places, location-based customization, transportation information, recording, map and navigation, geosocial networking, geotagging, location spoofing, alert and remind, and location-based game
	Επαφές	backup and synchronization, contact management, blacklist, call and SMS, contact-based customization, email, find friends, record, fake calls and SMS, remind

Πίνακας 3: Σκοπός χρήσης των δικαιωμάτων στις εφαρμογές (Lin et al 2012) (Haoyu Wang, Yuanchun Li, Yao Guo, Yuvraj Agarwal, και Jason I. Hong. (2017))

2.3. Άδειες πρόσβασης στο Android

2.3.1. Επίπεδα προστασίας των αδειών πρόσβασης

Οι άδειες πρόσβασης χωρίζονται σε τρία επίπεδα προστασίας, τα οποία επηρεάζουν τις εφαρμογές τρίτων οντοτήτων.

- Κανονικές άδειες (normal): Οι κανονικές άδειες καλύπτουν περιοχές στις οποίες η εφαρμογή χρειάζεται άδεια πρόσβασης σε δεδομένα ή πόρους του συστήματος έξω από το περιβάλλον λειτουργίας της, αλλά σε σημεία όπου είναι πολύ μικρός ή μηδαμινός ο κίνδυνος για τα προσωπικά δεδομένα του χρήστη. Στον Πίνακα 4 φαίνονται όλα οι άδειες πρόσβασης οι οποίες μπορούν να χαρακτηριστούν ως κανονικές στην έκδοση Android 9 Pie (API level 28).
- Άδειες με υπογραφές (signature): Πρόκειται για άδειες πρόσβασης, οι οποίες χορηγούνται αν η εφαρμογή που αιτείται άδεια, υπογραφεί με το ίδιο πιστοποιητικό με την εφαρμογή που ορίζει την άδεια υπογραφής. Στον πίνακα 5 βλέπουμε τις άδειες πρόσβασης που μπορούν να χρησιμοποιήσουν εφαρμογές τρίτων οντοτήτων στο Android 8.1 Oreo (API level 27) και μπορούν να χαρακτηριστούν ως “signature”.
- Επικίνδυνες άδειες (dangerous): Πρόκειται για υψηλού ρίσκου άδειες πρόσβασης που επιτρέπουν στην εφαρμογή να έχει πρόσβαση σε προσωπικά δεδομένα του χρήστη ή να επηρεάσει την λειτουργικότητα από άλλες εφαρμογές, ακόμα και ολόκληρου του συστήματος. Στον Πίνακα 6 αναγράφονται όλες οι επικίνδυνες άδειες πρόσβασης. [19] [20]

ACCESS_LOCATION_EXTRA_COMMANDS
ACCESS_NETWORK_STATE
ACCESS_NOTIFICATION_POLICY
ACCESS_WIFI_STATE
BLUETOOTH
BLUETOOTH_ADMIN
BROADCAST_STICKY
CHANGE_NETWORK_STATE
CHANGE_WIFI_MULTICAST_STATE
CHANGE_WIFI_STATE
DISABLE_KEYGUARD
EXPAND_STATUS_BAR
FOREGROUND_SERVICE
GET_PACKAGE_SIZE
INSTALL_SHORTCUT
INTERNET
KILL_BACKGROUND_PROCESSES
MANAGE_OWN_CALLS
MODIFY_AUDIO_SETTINGS
NFC

READ_SYNC_SETTINGS
READ_SYNC_STATS
RECEIVE_BOOT_COMPLETED
REORDER_TASKS
REQUEST_COMPANION_RUN_IN_BACKGROUND
REQUEST_COMPANION_USE_DATA_IN_BACKGROUND
REQUEST_DELETE_PACKAGES
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
SET_ALARM
SET_WALLPAPER
SET_WALLPAPER_HINTS
TRANSMIT_IR
USE_FINGERPRINT
VIBRATE
WAKE_LOCK
WRITE_SYNC_SETTINGS

Πίνακας 4: Κανονικές άδειες [19]

BIND_ACCESSIBILITY_SERVICE
BIND_AUTOFILL_SERVICE
BIND_CARRIER_SERVICES
BIND_CHOOSER_TARGET_SERVICE
BIND_CONDITION_PROVIDER_SERVICE
BIND_DEVICE_ADMIN
BIND_DREAM_SERVICE
BIND_INCALL_SERVICE
BIND_INPUT_METHOD
BIND_MIDI_DEVICE_SERVICE
BIND_NFC_SERVICE
BIND_NOTIFICATION_LISTENER_SERVICE
BIND_PRINT_SERVICE
BIND_SCREENING_SERVICE
BIND_TELECOM_CONNECTION_SERVICE
BIND_TEXT_SERVICE
BIND_TV_INPUT
BIND_VISUAL_VOICEMAIL_SERVICE
BIND_VOICE_INTERACTION
BIND_VPN_SERVICE

BIND_VR_LISTENER_SERVICE
BIND_WALLPAPER
CLEAR_APP_CACHE
MANAGE_DOCUMENTS
READ_VOICEMAIL
REQUEST_INSTALL_PACKAGES
SYSTEM_ALERT_WINDOW
WRITE_SETTINGS
WRITE_VOICEMAIL

Πίνακας 5: Άδειες με υπογραφή [19]

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

Πίνακας 6: Επικίνδυνες άδειες [19]

2.3.2. Αλλαγές στην διαχείριση των αδειών πρόσβασης στο Android 6 Marsmallow

Μια από τις πιο σημαντικές αλλαγές που έγιναν από την Google στο Android 6 Marsmallow, το οποίο παρουσιάστηκε το 2015, και ισχύουν μέχρι και σήμερα στην τωρινή έκδοση που κυκλοφορεί (android 9 pie), αφορά στην διαχείριση των αδειών πρόσβασης. Μέχρι την έκδοση έξι(6) του Android ο χρήστης ήταν αναγκασμένος να υποδεχτεί όλες τις άδειες που απαιτούσε η εφαρμογή, με αποτέλεσμα να αποδέχεται άδειες που ο ίδιος δεν ήθελε να εγκρίνει, διότι πίστευε πως είτε αποκτηθεί πρόσβαση σε κάποια προσωπικά δεδομένα του είτε ήταν ασήμαντες για την λειτουργία της εφαρμογής. Αξίζει να αναφέρουμε ότι η πρόσβαση στα δικαιώματα εφαρμογών στις εκδόσεις πριν το Marshmallow, απαιτούσε root στη συσκευή. Μόνο έτσι μπορούσαμε να διαχειριστούμε τις άδειες όπως εμείς θέλαμε [22]. Από την έκδοση 6 του λειτουργικού αυτό το πρόβλημα διορθώθηκε και ως ένα βαθμό ο χρήστης μπορεί να αισθάνεται πιο ασφαλής, αφού πια χορηγεί τις άδειες που ο ίδιος θέλει μετά την εγκατάσταση της εφαρμογής και όχι κατά την διάρκεια της όπως συνέβαινε στις προηγούμενες εκδόσεις. Πλέον με το πρώτο άνοιγα της εφαρμογής μετά την εγκατάσταση εμφανίζεται ένα παράθυρο διαλόγου που ζητάει από τον χρήστη να εγκρίνει τις άδειες τις εφαρμογής μία προς μία και αυτός αποφασίζει ποιες θα επιτρέψει και ποιες όχι. Επίσης σε περίπτωση που παραχωρήσει κάποια άδεια που δεν θέλει μπορεί να ανατρέξει στις Ρυθμίσεις του κινητού και να την απενεργοποιήσει. Ωστόσο, αυτή η ενέργεια μπορεί να δημιουργήσει πρόβλημα σε κάποιες δυνατότητες της εφαρμογής, παρόλο που η εφαρμογή θα ανταποκρίνεται κανονικά. Για παράδειγμα σε μια εφαρμογή κάμερας αν ο χρήστης δεν δώσει άδεια στο μικρόφωνο της συσκευής, η ίδια δεν θα μπορεί να εγγράψει βίντεο με ήχο, γεγονός που δημιουργεί αυτομάτως πρόβλημα για την λειτουργία βίντεο της εφαρμογής, χωρίς όμως να δημιουργείται πρόβλημα σε άλλες δυνατότητες της όπως την φωτογραφία. Ωστόσο, αν και όσα αναφέρθηκαν δείχνουν να επωφελούν το χρήστη, υπάρχει ένα πρόβλημα που επηρεάζει αρνητικά την ιδιωτικότητα του χρήστη. Πιο συγκεκριμένα, οι εφαρμογές πλέον μπορούν να πάρουν άδεια χωρίς να τη ζητήσουν από τον χρήστη. Το Play Store έχει κατηγοριοποιήσει τις άδειες σε ομάδες σχετικών αδειών. Για παράδειγμα μια εφαρμογή που θέλει να διαβάζει τα αρχεία από τον εξωτερικό χώρο του κινητού (κάρτα μνήμης) απαιτεί την άδεια READ_EXTERNAL_STORAGE. Αν ο χρήστης κατά την διάρκεια της εγκατάστασης της εφαρμογής χορηγήσει αυτήν την άδεια στην εφαρμογή, ταυτόχρονα παραχωρεί όλες τις άδειες που σχετίζονται με την ομάδα STORAGE. Η συγκεκριμένη εφαρμογή μπορεί σε επόμενη αναβάθμιση να θέλει να εντάξει άδεια και για εγγραφή στον εξωτερικό χώρο χρησιμοποιώντας την άδεια WRITE_EXTERNAL_STORAGE που ανήκει επίσης στην ομάδα STORAGE. Ωστόσο ο χρήστης δεν θα προτραπεί να παραχωρήσει εκ νέου την άδεια εγγραφής στον εξωτερικό χώρο, ενώ παράλληλα η εφαρμογή θα μπορεί να εγγράψει φακέλους ή αρχεία στον εξωτερικό χώρο αποθήκευσης (Hoffman, 2015) [21]

2.3.3. Μειονεκτήματα των αδειών πρόσβασης

Η ιδιωτικότητα των δεδομένων των χρηστών συνεχώς αμφισβητείται στο λειτουργικό σύστημα Android από τους χρήστες και όχι άδικα. Μεγάλο μέρος της ευθύνης για την καταπάτηση των προσωπικών δεδομένων των χρηστών έχει το μοντέλο αδειών πρόσβασης που χρησιμοποιεί το android. Πιο συγκεκριμένα τα μειονεκτήματα των αδειών πρόσβασης είναι τα εξής:

- Αλλαγή του μοντέλου αδειών πρόσβασης ανάλογα με την έκδοση του λειτουργικού. Όπως αναφέραμε στο προηγούμενο κεφάλαιο στο Android Marsmallow έγιναν ορισμένες αλλαγές στον τρόπο διαχείρισης των αδειών πρόσβασης κάθε εφαρμογής που εγκαθιστά ο χρήστης μέσω του Play Store. Ωστόσο, χρήστες που βρίσκονται στην προηγούμενη έκδοση του λειτουργικού από την Marsmallow καθώς και προγενέστερες αυτής, είναι υποχρεωμένοι να δεχτούν όλες τις άδειες που απαιτεί κάθε εφαρμογή κατά την εγκατάσταση της, γεγονός που δημιουργεί μια αίσθηση ανασφάλειας στους χρήστες ως προς την ιδιωτικότητα τους.
- Μη υποστήριξη των δικαιωμάτων των χρηστών, αναφορικά με την προστασία των προσωπικών δεδομένων τους. Οι εφαρμογές ζητάνε ορισμένες άδειες πρόσβασης, χωρίς όμως να ενημερώνει τον χρήστη για την λειτουργικότητα της συγκεκριμένης άδειας και κυρίως τον σκοπό για τον οποίο την χρησιμοποιεί η εφαρμογή. Με αυτό τον τρόπο ένα από τα θεμελιώδη δικαιώματα των χρηστών, αυτό της ενημέρωσης του σκοπού της πρόσβασης στα προσωπικά δεδομένα τους, αγνοείται από το τρέχον σύστημα του λειτουργικού.
- Χρήση προσωπικών δεδομένων εκτός συσκευής (τρίτες οντότητες) χωρίς την ενημέρωση των χρηστών. Ο χρήστης δεν μπορεί να αντιληφθεί αν οι άδειες που ζητάει η εφαρμογή είναι απαραίτητες για την σωστή λειτουργία της εφαρμογής ή αν χρησιμοποιούνται για να εξυπηρετήσουν διαφημιστικούς σκοπούς για παράδειγμα. Φυσικά, αυτό δηλώνεται ή πρέπει να δηλώνεται ρητά στις πολιτικές ιδιωτικότητας κάθε εφαρμογής, αν και οι περισσότερες εφαρμογές δεν δηλώνουν τέτοιες πληροφορίες επίτηδες. Ακόμα και όταν δηλώνεται ρητά ο τρόπος διαχείρισης των δεδομένων του χρήστη στις πολιτικές ιδιωτικότητας, οι ίδιες ή δεν εμφανίζονται κατά το άνοιγμα της εφαρμογής ή βρίσκονται σε υπομενού της εφαρμογής και ο μέσος χρήστης είτε δεν γνωρίζει πώς να έχει πρόσβαση σε αυτές, είτε δεν τις διαβάζει, επειδή συνήθως είναι μακροσκελής. [21]

Αν αναλογιστούμε τα όσα αναφέρθηκαν σχετικά με τα μειονεκτήματα των αδειών πρόσβασης, συμπεραίνουμε ότι το μοντέλο αδειών του Android έχει σημαντικά κενά ασφαλείας ακόμα και μετά τις αλλαγές που έγιναν στο Android Marsmallow και θα πρέπει να προβεί σε αναδιάρθωση του συστήματος διαχείρισης των αδειών πρόσβασης. Βέβαια παρατηρώντας την διασημότητα του σε συνδυασμό με την αδιαφορία των χρηστών του , δύσκολα θα δούμε κάποια αλλαγή στο άμεσο μέλλον.

2.3.4. Ερευνητική Προσέγγιση: Μελέτη αδειών πρόσβασης εφαρμογών από το Google Play

Σε έρευνα που διεξήγαγε η Ματίνα Τσαβλή (Πειραιάς 2016) σχετικά με τις άδειες πρόσβασης σε 14.000 εφαρμογές του Google Play, συλλέγοντας όλα τα δικαιώματα που απαιτεί κάθε εφαρμογή με την χρήση προγραμματισμού συμπέρανε τα εξής (αναφέρονται μόνο οι πρώτες πέντε γραμμές κάθε πίνακα):

- Οι πιο απαιτητικές εφαρμογές σε άδειες στην Ελλάδα είναι οι Mls Updater, hike messenger, Zero Launcher pro smart boost, slidesync με 124,68,,60,56 και 53 απαιτούμενες άδειες αντίστοιχα.
- Οι άδειες που ζητούνται περισσότερο στην Ελλάδα είναι οι INTERNET, ACCESS_NETWORK_STATE, READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE και WAKE_LOCK με ποσοστά 34, 32, 31, 30 και 23 τις εκατό αντίστοιχα
- Οι άδειες που ζητούνται λιγότερο στην Ελλάδα είναι οι BIND_TEXT_SERVICE, MOVE_PACKAGE, DIAGNOSTIC, googleapps.permission.GOOGLE_AUTH.YouTubeUser, CONFIGURE_WIFI_DISPLAY όλες με ποσοστό 0,013%
- Οι χαμηλότεροι μέσοι όροι αδειών ανά κατηγορία παρατηρήθηκαν στις εξής κατηγορίες: Widgets, Libraries and Demo, Games, Family και Weather με τιμές 0,52, 1,15, 1,34, 1,52 και 2,27 αντίστοιχα ενώ οι υψηλότεροι στις κατηγορίες Communication, Productivity, Tools, Business και Social με τιμές 11,18, 7,88, 7,13, 6,39 και 5,80 αντίστοιχα. [21]

Φυσικά, όλα όσα προαναφέρθηκαν είναι ένα δείγμα της έρευνας που διεξάχθηκε, ώστε να μπορούμε να εξάγουμε ορισμένα συμπεράσματα. Έτσι από την συγκεκριμένη έρευνα μπορούμε να συμπεράνουμε:

- Δύο από τις άδειες που ζητούνται περισσότερο στην Ελλάδα από εφαρμογές του Play Store, οι READ_EXTERNAL_STORAGE και WRITE_EXTERNAL_STORAGE κατατάσσονται στις επικίνδυνες άδειες όπως αναφέρθηκαν σε προηγούμενο κεφάλαιο της βιβλιογραφικής επισκόπησης.
- Οι πιο απαιτητικές εφαρμογές σε άδειες στην Ελλάδα απαιτούν υπερβολικό πλήθος αδειών που σίγουρα δεν χρειάζονται, με αποτέλεσμα πολύ πιθανόν να έχει γίνει repackaging εφαρμογών (όπως είδαμε σε προηγούμενο κεφάλαιο) ή εξ αρχής η εφαρμογή να έχει προγραμματιστεί έτσι, είτε για λόγους εισαγωγής διαφημίσεων εντός της εφαρμογής, είτε εγκατάστασης κάποιου άλλου είδους κακόβουλου λογισμικού.
- Οι ψηλότεροι μέσοι όροι αδειών διαπιστώθηκαν σε κατηγορίες εφαρμογών όπως επικοινωνία, κοινωνικά δίκτυα και εργαλεία, στις οποίες παρατηρούνται εφαρμογές με μεγάλο πλήθος εγκαταστάσεων από τους χρήστες, γεγονός που δείχνει πως οι προγραμματιστές στοχεύουν σε εφαρμογές που έχουν ανάγκη οι χρήστες, ώστε να εξασφαλίσουν μεγαλύτερο κέρδος από διαφημίσεις ή να αποκτήσουν δεδομένα από όσο περισσότερους χρήστες μπορούν πουλώντας τα μετά σε μεγάλες εταιρείες.

Ο κύριος λόγος παράθεσης της παραπάνω έρευνας είναι η χρήση της στο κεφάλαιο 5 της παρούσας εργασίας (Αποτελέσματα έρευνας) ώστε να γίνει σύγκριση με τα αποτελέσματα που θα εξαχθούν για αυτήν.

3. Μεθοδολογία

3.1. Μελέτη των απαιτούμενων αδειών πρόσβασης των εφαρμογών στο Aptoide

3.1.1. Υλοποίηση προγραμματιστικής εφαρμογής

Για τις ανάγκες της παρούσας έρευνας σχεδιάστηκε μια βάση δεδομένων που είχε ως στόχο την εξαγωγή συμπερασμάτων αναφορικά με το πλήθος των αδειών πρόσβασης που απαιτεί η κάθε εφαρμογή από ένα third party market του Android, το Aptoide. Η βάση δεδομένων περιείχε στοιχεία από 2500 εφαρμογές, που διατίθενται μέσω του Ελληνικής ιστοσελίδας του Aptoide. Για την συλλογή των παραπάνω στοιχείων κρίθηκε απαραίτητη η δημιουργία μια προγραμματιστικής εφαρμογής, η οποία θα συλλέγει τα απαιτούμενα δεδομένα με επαναλαμβανόμενα POST REQUEST στην επίσημη ελληνική ιστοσελίδα του Aptoide. Τα πεδία που χρειάστηκαν να ενταχθούν στους πίνακες της βάσης δεδομένων είναι τα εξής:

- Όνομα εφαρμογής (στην βάση δεδομένων βρίσκεται ως “name”)
- Url (διεύθυνση) εφαρμογής (στην βάση δεδομένων βρίσκεται ως “url”)
- Άδειες πρόσβασης που απαιτεί κάθε εφαρμογή (στην βάση δεδομένων βρίσκεται ως “permi”)
- Πλήθος άδειων πρόσβασης κάθε εφαρμογής για ευκολότερη εύρεση αποτελεσμάτων (στην βάση δεδομένων βρίσκεται ως “numofpermi”)

Η απουσία έτοιμων βιβλιοθηκών για την εξαγωγή των δεδομένων από την ιστοσελίδα του Aptoide δημιούργησε την ανάγκη υλοποίησης προγραμματιστικής εφαρμογής από το μηδέν, ώστε να μπορέσουμε να εξάγουμε τα απαιτούμενα αποτελέσματα.

Οι λόγοι που επιλέχτηκε το Aptoide, ένα third party market για το Android, και όχι η επίσημη ιστοσελίδα εφαρμογών της Google για την εξαγωγή των αδειών πρόσβασης κάθε εφαρμογής είναι οι εξής:

- Η ύπαρξη αρκετών ερευνών αναφορικά με την επίσημη ιστοσελίδα εφαρμογών της Google, που αφορά τόσο τις άδειες πρόσβασης των εφαρμογών της, όσο και την διασημότητα των εφαρμογών. Έτσι, αποφασίστηκε να δημιουργηθεί έρευνα σε ένα ενναλακτικό android market, το Aptoide, που περιέχει επίσης πολύ μεγάλο πλήθος εφαρμογών.
- Η ανάγκη σύγκρισης της εμπιστευτικότητας του Google Play με ένα third party android market όπως το Aptoide, αναφορικά με τις άδειες που απαιτεί κάθε εφαρμογή και να συμπεράνουμε κατά πόσο οι χρήστες μπορούν να εμπιστευτούν ένα εναλλακτικό market για το κατέβασμα των εφαρμογών τους.

3.1.2. Εργαλεία

Για την υλοποίηση της προγραμματιστικής εφαρμογής και την εξαγωγή συμπερασμάτων για τις άδειες πρόσβασης των εφαρμογών του Aptoide χρησιμοποιήθηκαν τα εξής εργαλεία.

- **Python version 3.7.4**: Χρησιμοποιήθηκε η συγκεκριμένη γλώσσα προγραμματισμού, διότι προσφέρει ένα μεγάλο πλήθος έτοιμων βιβλιοθηκών είτε official είτε unofficial, που παρέχουν έτοιμο τον κώδικα για το σκοπό για τον οποίο γράφτηκαν, γεγονός που διευκολύνει τον χρήστη, αφού δεν απαιτείται από τον ίδιο να γράφει πολλές γραμμές κώδικα για να υλοποιήσει το επιθυμητό αποτέλεσμα. Επίσης, η συγκεκριμένη γλώσσα έχει ιδιαίτερα εύκολη σύνταξη, κατανοητή προς τον χρήστη και μεγάλο πλήθος βοηθημάτων τόσο για τις βιβλιοθήκες της, όσο και για την γενικότερη σύνταξη της γλώσσας, γεγονός που έχει συμβάλει σημαντικά στην μεγάλη διασημότητα της και την ολοένα και περισσότερη αποδοχή του κόσμου. Η έκδοση 3 της python σε σύγκριση με την έκδοση 2, έχει ορισμένες διαφορές κυρίως στο τομέα της σύνταξης, οπότε η συγκεκριμένη εφαρμογή ενδέχεται να παρουσιάζει προβλήματα αν «τρέξει» στην έκδοση 2. Η βιβλιοθήκη που χρησιμοποιήθηκε εκτενώς στο πρόγραμμα για να μπορέσουμε να εξάγουμε τις άδειες πρόσβασης στην βάση δεδομένων είναι η «Beautiful Soup», μέσω της οποίας καταφέραμε να αποκτήσουμε όλα τα δικαιώματα κάθε εφαρμογής μέσω του html κώδικα που είναι διαθέσιμος για κάθε εφαρμογή στην ιστοσελίδα του Aptoide. Φυσικά, χρησιμοποιήθηκαν και άλλες βιβλιοθήκες που ήταν εξίσου σημαντικές όπως η «requests» για εξαγωγή όλου του html κώδικα και η «urllib.request» για άνοιγμα της ιστοσελίδας κάθε εφαρμογής για να διαπιστώσουμε ότι είναι λειτουργική και δεν εμφανίζει κάποιο λάθος.
- **PostgreSQL version 11**: Χρησιμοποιήθηκε η συγκεκριμένη βάση δεδομένων, διότι είναι εύχρηστη, ανοικτού κώδικα (open source) και με πολλές δυνατότητες. Επίσης, στην τελευταία της έκδοση (έκδοση 11), η βάση δεδομένων μεταφέρεται σε web based περιβάλλον, δηλαδή είναι προσβάσιμη μέσω του browser, ενώ στις προηγούμενες εκδόσεις αποτελούσε ξεχωριστό παράθυρο του λειτουργικού συστήματος που έτρεχε. Αναφορικά με τον τρόπο που εισήχθησαν τα δεδομένα στην βάση, χρησιμοποιήθηκαν πίνακες, ένας για κάθε κατηγορία εφαρμογής ή παιχνιδιού με τα αναγνωριστικά που αναφέρθηκαν στην ενότητα 4.1.1 της παρούσας εργασίας. Επίσης για την υλοποίηση ορισμένων γενικών ερωτημάτων και όχι ερωτημάτων που αφορούσαν τις κατηγορίες των παιχνιδιών και των εφαρμογών, υλοποιήθηκε ένας πίνακας (allapps), που εμπεριέχει όλες τις εφαρμογές και τα παιχνίδια που μελετήθηκαν συνολικά μαζί με τα δικαιώματα τους (2595 εφαρμογές και παιχνίδια). Φυσικά απαιτήθηκε και η σύνδεση της βάσης δεδομένων με τον πηγαίο κώδικα για να μπορέσουν να εισαχθούν τα στοιχεία στους πίνακες. Έπειτα, υλοποιήθηκαν τα απαραίτητα sql ερωτήματα (Παράρτημα Β) για να εξαχθούν τα απαραίτητα συμπεράσματα που θέσαμε εξ αρχής ως στόχο.

3.1.3. Δειγματοληψία και περιορισμοί του πηγαίου κώδικα

Δείγμα

Από το σύνολο των εφαρμογών που υπάρχουν στην ιστοσελίδα του Aptoide, επιλέχθηκαν 2595 εφαρμογές, δείγμα επαρκές για την εξαγωγή ολοκληρωμένων συμπερασμάτων. Πιο συγκεκριμένα

επιλέχθηκαν οι 50 κορυφαίες εφαρμογές ή παιχνίδια από κάθε κατηγορία, από σύνολο 55 κατηγοριών που αντιστοιχούν στις δύο ενότητες. Ωστόσο, κάποιες από αυτές τις εφαρμογές έτυχε να μην ανοίγει η ιστοσελίδα τους και για αυτό το λόγο βγήκε το παραπάνω δείγμα. Σε αυτό το σημείο να τονιστεί ότι η επιλογή των εφαρμογών έγινε από την Ελληνική ιστοσελίδα του Aptoide. Σε άλλες χώρες που η ιστοσελίδα παρέχεται με άλλο domain name πολύ πιθανόν να είχαν εξαχθεί διαφορετικά συμπεράσματα λόγω διαφορετικής προτίμησης των χρηστών, γεγονός που θα οδηγούσε σε αλλαγές στην σειρά που παρουσιάζονται οι κορυφαίες εφαρμογές κάθε κατηγορίας έναντι του ελληνικού domain που χρησιμοποιήθηκε.

Περιορισμοί του πηγαίου κώδικα

Όπως αναφέραμε στην υποενότητα 4.1.2 χρησιμοποιήθηκε η γλώσσα προγραμματισμού Python για την υλοποίηση της προγραμματιστικής εφαρμογής. Επίσης, όπως αναφέρθηκε σημαντικό ρόλο στον κώδικα είχε και η βιβλιοθήκη «Beautiful Soup» που εισάχθηκε για να αποκτηθούν όλα τα δικαιώματα κάθε εφαρμογής ξεχωριστά. Ωστόσο η συγκεκριμένη βιβλιοθήκη μπορούσε να εισαχθεί και για την αυτοματοποιημένη αλλαγή κατηγορίας όταν ολοκληρώνονταν οι 50 εφαρμογές μιας κατηγορίας (για παράδειγμα η αναπήδηση από την action κατηγορία παιχνιδιών στην επόμενη, δηλαδή στην arcade), και να γίνει εξαντλητική αναζήτηση δικαιωμάτων των εφαρμογών και σε εκείνη την κατηγορία. Με αυτόν τον τρόπο, εισάγοντας απλά έναν επαναληπτικό βρόγχο, δεν θα απαιτούνταν να γραφτεί ο ίδιος κώδικας 60 φορές (όσες είναι οι κατηγορίες που μελετήθηκαν) και θα είχε εξοικονομηθεί πολύτιμος χρόνος για την υλοποίηση της εφαρμογής. Όμως, η βιβλιοθήκη είχε κάποιου είδους περιορισμό στο κώδικα της και δινόταν η δυνατότητα να γίνει αυτοματοποιημένα μόνο για 9 κατηγορίες από τις συνολικά 40 των εφαρμογών και 9 από τις συνολικά 20 των παιχνιδιών και έτσι αποφασίστηκε να μην χρησιμοποιηθεί ο συγκεκριμένος τρόπος και ο κώδικας να βασιστεί στο χειροκίνητο τρόπο για λόγους ομοιομορφίας. Ο αυτοματοποιημένος τρόπος μπορεί να επιτευχθεί εισάγοντας τις γραμμές κώδικα όπως φαίνονται στο Παράρτημα Α. Φυσικά, αν και ο συγκεκριμένος περιορισμός απαιτούσε την εισαγωγή περισσότερων γραμμών κώδικα, ο ίδιος είναι απόλυτα λειτουργικός. Μέρος του κώδικα που αφορά μια κατηγορία παρουσιάζεται στο Παράρτημα Α και όλος ο κώδικας διατίθεται μέσω ξεχωριστού αρχείου που παραδίδεται με την εργασία.

3.2. Μελέτη και ανάλυση πολιτικών ιδιωτικότητας δέκα δημοφιλών εφαρμογών στο Android αναφορικά με τα δεδομένα χρήστη που συλλέγουν

Σε αυτό το κεφάλαιο θα αναλύσουμε τις πολιτικές ιδιωτικότητας δέκα δημοφιλών εφαρμογών στο Android αναφορικά με τα δεδομένα χρήστη που συλλέγουν και με ποιον τρόπο τα χρησιμοποιούν. Πιο συγκεκριμένα επιλέχτηκαν οι εφαρμογές facebook, instagram, navigon, google earth, shazam, soundhoud, uc browser, mozilla firefox Τα κριτήρια με τα οποία επιλέχτηκαν οι παρακάτω εφαρμογές είναι :

- Ο βαθμός διάδοσης και χρήσης από τους χρήστες όλου του κόσμου.
- Η πιθανή χρήση επικίνδυνων δικαιωμάτων λόγω της μεγάλης διάδοσης τους όπως το δικαίωμα στην τοποθεσία, στην κάμερα, στο μικρόφωνο και στον εσωτερικό χώρο αποθήκευσης, γεγονός που κάνει την αξιολόγηση πιο αναγκαία και πιο ενδιαφέρουσα.

- Σύγκριση εφαρμογών των οποίων ανήκουν σε παρόμοια κατηγορία έτσι ώστε να κατανοήσουν οι χρήστες ποια από τις δυο εφαρμογές έχει την μεγαλύτερη πληρότητα-συσχέτιση, αναφορικά με τα δικαιώματα που απαιτεί(uc browser- google chrome, facebook- twitter, viber- whatsapp, e-radio- tunein radio, Netflix- kodi) (Κεφάλαιο 5 υποενότητα 5.5)

1. UC Broswer

Ο UC Broswer είναι ένας πολύ διαδεδομένος browser κυρίως στις android συσκευές. Αυτό που τον κάνει ξεχωριστό έναντι άλλων browser στο συγκεκριμένο λειτουργικό είναι η ταχύτητά του και η ελάχιστη επεξεργαστική ισχύ που απαιτεί με αποτέλεσμα να τρέχει απροβλημάτιστα σε όλες τις συσκευές ακόμα και στις low end(χαμηλών χαρακτηριστικών). Παρακάτω θα αναλύσουμε και την συγκεκριμένη πολιτική ιδιωτικότητας [23].

Διαβάζοντας εκτενώς την πολιτική ιδιωτικότητας του UC Broswer παρατηρούμε ότι η εφαρμογή συλλέγει αρκετά δεδομένα με αυτοματοποιημένο τρόπο. Πιο συγκεκριμένα συλλέγει:

- Πληροφορίες που αφορούν το Software, όπως την έκδοση του περιηγητή, την έκδοση του Android και την λίστα των εφαρμογών που έχει εγκατεστημένα ο χρήστης
- Πληροφορίες που αφορούν το Hardware, όπως το IMEI, την MAC διεύθυνση και πληροφορίες σχετικές με τον κατασκευαστή και το μοντέλο του κινητού
- Πληροφορίες που αφορούν το δίκτυο, όπως IP Address, διαχειριστή δεδομένων κινητής τηλεφωνίας και κατάσταση του δικτύου
- Ρυθμίσεις και χρήση, όπως ώρα και ημερομηνία, γλώσσα συστήματος, σφάλματα και αναφορές, ιστορικό του περιηγητή, ρυθμίσεις και τι πληκτρολογεί ο χρήστης στην μπάρα αναζήτησης
- Τοποθεσία (εφόσον την αποδεχτεί ο χρήστης)

Επίσης αναφέρει πως χρησιμοποιούνται cookies και άλλες παρόμοιες τεχνικές για να συλλέξουν πληροφορίες για την ημερομηνία και την ώρα που επισκέφθηκε ο χρήστης κάποια συγκεκριμένη ιστοσελίδα, καθώς και τι αναζήτησε σε αυτήν. Ακόμα, όπως αναφέρεται στην πολιτική ιδιωτικότητας, οι προγραμματιστές του UC Broswer μπορούν να συλλέγουν πληροφορίες από εξωτερικούς συνεργάτες ή άλλες τρίτες οντότητες και να τις συνδυάζουν με τις πληροφορίες που έχουν συλλέξει. Για παράδειγμα, αν ο χρήστης συνδεθεί με τον λογαριασμό Google ή Facebook, ενδέχεται να έχουν πρόσβαση στα στοιχεία των προφίλ των δύο παραπάνω λογαριασμών.

Σχετικά με τους τρόπους που χρησιμοποιεί τις πληροφορίες που συλλέγει η συγκεκριμένη εφαρμογή παραθέτει τους εξής:

- Για προστασία από κακόβουλο λογισμικό, για αυτόματη διόρθωση και συγκεκριμένες προτάσεις ιστοσελίδων ανάλογα την χρήση, για συγχρονισμό σελιδοδεικτών και άλλες ενέργειες που αφορούν την online αποθήκευση (cloud).
- Για βελτίωση των συγκεκριμένων δυνατοτήτων και της τεχνικής υποστήριξης των πελατών

- Για στατιστικούς λόγους και αναφορές για να παρακολουθείται η απόδοση και να ανιχνεύονται τεχνικά προβλήματα
- Για να εξαγωγή συγκεντρωτικών μη προσωπικών πληροφοριών όπως η τάση χρήσης
- Για τον εντοπισμό και την πρόληψη της απάτης

Επιπλέον ονομάζει μερικές διαφημιστικές πλατφόρμες, όπως το AdMob της Google, το Facebook Audience Network και το Intowow, με τις οποίες συνεργάζεται και τους διαμοιράζει της πληροφορίες που συλλέγει, τις οποίες αναφέραμε εκτενώς παραπάνω. Παράλληλα, γίνεται διαμοιρασμός των πληροφοριών του χρήστη, εφόσον ζητηθούν από τις δικαστικές αρχές ή γίνει αλλαγή στην ιδιοκτησία της επιχείρησης ή συγκεκριμένα της εφαρμογής, ενώ μη προσωπικά στοιχεία των χρηστών μπορούν να δοθούν σε εκδότες, διαφημιζόμενους ή συνδεδεμένους ιστοτόπους. Τέλος, επισημαίνεται ότι η πολιτική ιδιωτικότητας θα αναθεωρείται περιοδικά και ενδέχεται να διαφοροποιηθεί με ή χωρίς την προειδοποίηση του χρήστη.

2. Google Chrome

Ο Google Chrome είναι με διαφορά ο πιο δημοφιλής περιηγητής στο Android και αυτό αντικατοπτρίζεται πλήρως από το πλήθος λήψεων της εφαρμογής από την επίσημη ιστοσελίδα εφαρμογών της Google (Google Play). Για αυτό κρίθηκε απαραίτητη η μελέτη της πολιτικής ιδιωτικότητας του [24] και η σύγκριση της (Κεφάλαιο 5, Υποενότητα 5.5), με αυτήν του UC Broswer, την οποία μελετήσαμε παραπάνω.

Στην πολιτική ιδιωτικότητας, ο Chrome, αναφέρει ότι οι πληροφορίες του χρήστη αποθηκεύονται στο σύστημα της κινητής του συσκευής και όχι στους server της Google. Πιο συγκεκριμένα οι πληροφορίες που αποθηκεύονται στην κινητή συσκευή είναι:

- Πληροφορίες ιστορικού περιήγησης. Για παράδειγμα το Chrome αποθηκεύει τις διευθύνσεις URL των σελίδων που επισκέπτεται ο χρήστης, εικόνες και προσωρινό κείμενο, ενώ αν είναι ενεργοποιημένη η λειτουργία πρόβλεψης ενεργειών δικτύων αποθηκεύει και ορισμένες διευθύνσεις IP που συνδέονται με αυτές τις σελίδες.
- Προσωπικά στοιχεία και κωδικούς, για διευκόλυνση του χρήστη αναφορικά με φόρμες και είσοδο σε λογαριασμούς
- Cookies ή δεδομένα από ιστοσελίδες που επισκέπτεται ο χρήστης
- Δεδομένα από πρόσθετα
- Εγγραφές από τις λήψεις των χρηστών από ιστοσελίδες

Για να σταλθούν τα παραπάνω δεδομένα στην Google, πρέπει ο χρήστης να συνδεθεί στον λογαριασμό Google και να ενεργοποιήσει τον συγχρονισμό. Στην περίπτωση που τα δεδομένα αφορούν λογαριασμούς τραπεζών και πληροφορίες πιστωτικής κάρτας, αυτά δεν αποθηκεύονται στο λογαριασμό Google Payment εφόσον δεν δωθεί άδεια από το χρήστη. Επίσης αναφέρεται ότι τα δεδομένα είναι προστατευμένα όσο υπάρχουν στους Servers της Google.

Ο Chrome διαχειρίζεται με διάφορους τρόπους τα δεδομένα των χρηστών. Αναλυτικότερα οι τρόποι είναι οι εξής:

- Οι ιστοσελίδες που επισκέπτεται ο χρήστης με τον περιηγητή Google Chrome μπορούν με αυτοματοποιημένο τρόπο να αποκτήσουν πληροφορίες όπως την διεύθυνση IP του χρήστη και τα δεδομένα των Cookies. Αν ο chrome διαπιστώσει κάποια είδους επίθεση από κάποια τρίτη οντότητα σε ένα δίκτυο, τότε στέλνει πληροφορίες για αυτήν την σύνδεση στην Google για να διαπιστώσει τον τρόπο που λειτουργεί η επίθεση
- Ο Chrome δίνει την δυνατότητα στους χρήστες εφόσον εκείνοι το επιθυμούν να δώσει πληροφορίες σχετικά με την τοποθεσία τους σε άλλες ιστοσελίδες. Ωστόσο στο android εφόσον ο χρήστης δώσει το δικαίωμα της τοποθεσίας από τις ρυθμίσεις της εφαρμογής αυτή μπορεί να διαμοιραστεί αυτοματοποιημένα σε όλες τις ιστοσελίδες που την απαιτούν χωρίς την ειδοποίηση του χρήστη. Επίσης, ο περιηγητής της Google χρησιμοποιεί το Google Location Service για να υπολογίσει την τοποθεσία του χρήστη, χρησιμοποιώντας τα κοντινά wifi router και την διεύθυνση IP της συσκευής.
- Για την ενημέρωση του λογισμικού ο Chrome στέλνει πληροφορίες στην Google όπως την κατάσταση σύνδεσης, την ώρα, και υπολογίζει το πλήθος των συνδεδεμένων χρηστών στην εφαρμογή.
- Σε περίπτωση που δεν μπορεί ο χρήστης να συνδεθεί σε μια ιστοσελίδα, ο Chrome κάνει προτάσεις για παρόμοιες ιστοσελίδες. Ωστόσο για να παρέχει αυτές τις προτάσεις στέλνεται στην Google η διεύθυνση της ιστοσελίδας που προσπαθεί να προσπελάσει ο χρήστης.
- Για την αυτοματοποιημένη συμπλήρωση του username και του password σε μια φόρμα, στέλνονται στους server της Google περιορισμένα, ανώνυμα δεδομένα, κρυπτογραφώντας την διεύθυνση και τα δεδομένα της φόρμας. Επίσης, παρέχει ασφάλεια σε περίπτωση που δοθούν στοιχεία πιστωτικής κάρτας.
- Για την βελτίωση των παροχών που προσφέρει, ο Chrome στέλνει στατιστικά χρήσης και αναφορές μη ανταπόκρισης της εφαρμογής στην Google. Τα στατιστικά χρήσης περιέχουν πληροφορίες όπως τις ρυθμίσεις και την χρήση μνήμης του συστήματος, ενώ οι αναφορές μη ανταπόκρισης μπορεί να περιέχουν την διεύθυνση ή τις διευθύνσεις που χρησιμοποιεί ο χρήστης και άλλες προσωπικές πληροφορίες. Σε αυτήν την περίπτωση μπορεί να δοθούν κάποιες μη προσωπικές πληροφορίες σε τρίτες οντότητες όπως συνεργάτες, διαφημιστές και προγραμματιστές όπως αναφέρεται στην πολιτική ιδιωτικότητας.

3. Facebook

Το facebook είναι ένας ιστότοπος μέσα από τον οποίο ο χρήστης επικοινωνεί με άλλους χρήστες, μοιράζεται φωτογραφίες, τραγούδια , ιδέες ,απόψεις. Θεωρείται το πιο διάσημο κοινωνικό δίκτυο βάσει χρηστών και για αυτό κρίνεται απαραίτητο να μελετήσουμε την πολιτική ιδιωτικότητάς του [25].

Το Facebook, χωρίζει τις πληροφορίες που συλλέγει σε τρεις κατηγορίες. Πιο συγκεκριμένα:

1. **Πληροφορίες από ενέργειες στις οποίες ο χρήστης προβαίνει και κοινοποιεί**

- Κοινοποίηση περιεχομένου, ανταλλαγή μηνυμάτων η επικοινωνία με άλλους. Για παράδειγμα μεταδεδομένα όπως η τοποθεσία μιας φωτογραφίας που στάλθηκε ή ημερομηνία δημιουργίας ενός αρχείου ή πληροφορίες σχετικές με την κάμερα για παροχή προτάσεων φίλτρων. Όλα αυτά τα δεδομένα συλλέγονται
- Πληροφορίες για τα άτομα, τις σελίδες, τους λογαριασμούς και τις ομάδες με τις οποίες συνδέεται ο χρήστης
- Στοιχεία επικοινωνίας, σε περίπτωση που ο χρήστης θέλει να ανεβάσει, να συγχρονίσει ή να εισάγει από κάποια συσκευή όπως κατάλογο επαφών, ιστορικό κλήσεων ή ιστορικό SMS.
- Πληροφορίες όπως τα είδη περιεχομένου που βλέπει και αλληλεπιδρά ο χρήστης, τις ενέργειες του χρήστη, τα άτομα που αλληλεπιδρά, καθώς και την ώρα, την συχνότητα και τη διάρκεια των δραστηριοτήτων των χρηστών.
- Πληροφορίες σχετικές με τις αγορές ή τις συναλλαγές των χρηστών εντός της εφαρμογής όπως ο αριθμός της πιστωτικής κάρτας, στοιχεία επαλήθευσης λογαριασμού, πληροφορίες τιμολόγησης, η διεύθυνση αποστολής και τα στοιχεία επικοινωνίας
- Πληροφορίες από ενέργειες τρίτων οντοτήτων στον λογαριασμό ενός χρήστη όπως για παράδειγμα πότε κοινοποιούν ή σχολιάζουν μια φωτογραφία του χρήστη, πότε στέλνουν μήνυμα ή εισάγουν τα στοιχεία επικοινωνίας του.

2. **Πληροφορίες συσκευής**
    - Πληροφορίες όπως το λειτουργικό σύστημα, η έκδοση υλικού ή λογισμικού, το επίπεδο μπαταρίας, η ισχύς του σήματος, ο διαθέσιμος χώρος αποθήκευσης, ο τύπος του προγράμματος περιήγησης, τα ονόματα και οι τύποι εφαρμογών και αρχείων, τα πρόσθετα (Plugins)
    - Μοναδικά αναγνωριστικά και αναγνωριστικά συσκευών, όπως από παιχνίδια, εφαρμογές ή λογαριασμούς που χρησιμοποιεί ο χρήστης, αλλά και αναγνωριστικά οικογενειακών συσκευών.
    - Σήματα συσκευής, όπως σήματα Bluetooth και πληροφορίες σχετικά με κοντινά σημεία πρόσβασης σε δίκτυα WI-FI και πύργους κινητής τηλεφωνίας
    - Πληροφορίες που επιτρέπει ο χρήστης στο Facebook να λαμβάνει, όπως η δυνατότητα πρόσβασης στην τοποθεσία GPS, στην κάμερα ή στις φωτογραφίες
    - Πληροφορίες δικτύου και συνδέσεις, όπως το όνομα του παρόχου κινητής τηλεφωνίας, η γλώσσα, η ζώνη ώρας, ο αριθμός του κινητού τηλεφώνου, ι διεύθυνση IP και η ταχύτητα σύνδεσης.
    - Δεδομένα Cookie
3. **Πληροφορίες από συνεργάτες**
    - Οι διαφημιζόμενοι, οι προγραμματιστές εφαρμογών και οι εκδότες μπορούν να στέλνουν πληροφορίες στο Facebook μέσω του API και SDK και του Pixel του Facebook. ΟΙ συνεργάτες αυτοί μπορούν να παρέχουν πληροφορίες για τις δραστηριότητες του χρήστη εκτός Facebook, όπως πληροφορίες της συσκευής, τους ιστοτόπους που επισκέπτεται ο χρήστης, τις αγορές που κάνει και τις διαφημίσεις που βλέπει ο ίδιος, ανεξάρτητα αν ο χρήστης έχει λογαριασμό Facebook, κάνοντας χρήση του API του.

Τρόπος χρήσης των πληροφοριών

Το Facebook χρησιμοποιεί της πληροφορίες του χρήστη για του παρακάτω λόγους:

- Παροχή, εξατομίκευση και βελτίωση των προϊόντων
- Παροχή μετρήσεων, στατιστικών στοιχείων και άλλων επαγγελματικών υπηρεσιών
- Προώθηση προστασίας, ακεραιότητας και ασφάλειας
- Επικοινωνία με το χρήστη για προωθητικές ενέργειες ή για ευκολότερη λύση των προβλημάτων του.
- Έρευνα και καινοτομία προς όφελος του κοινωνικού συνόλου

Κοινοποίηση δεδομένων σε τρίτους συνεργάτες

- Συνεργάτες που χρησιμοποιούν τις υπηρεσίες αναλύσεων
- Διαφημιζόμενοι
- Συνεργάτες μετρήσεων
- Συνεργάτες που προσφέρουν αγαθά και υπηρεσίες στα προϊόντα του Facebook
- Προμηθευτές και πάροχοι υπηρεσιών
- Ερευνητές και ακαδημαϊκοί
- Επιβολή του νόμου ή νομικά αιτήματα

4.Twitter

Το Twitter είναι άλλο ένα διάσημο κοινωνικό δίκτυο και για αυτό το λόγο έχει ενδιαφέρον η μελέτη της πολιτικής του ιδιωτικότητας [26].

Όπως και το Facebook έτσι και το Twitter, διαχωρίζει τις πληροφορίες που συλλέγει σε κατηγορίες και πιο συγκεκριμένα σε πληροφορίες που διαμοιράζεται ο χρήστης με το twitter και σε πληροφορίες που παίρνονται αυτοματοποιημένα από την εφαρμογή.

Πληροφορίες που διαμοιράζεται ο χρήστης

- Βασικές πληροφορίες του λογαριασμού, όπως το όνομα χρήστη, τον κωδικό, τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή το κινητό του τηλέφωνο.
- Δημόσιες πληροφορίες όπως πληροφορίες του προφίλ του χρήστη, την ώρα και την ημερομηνία, τα λεγόμενα «Tweets» του χρήστη. Επίσης στις δημόσιες πληροφορίες εντάσσονται και σχόλια σε δημοσιεύσεις τρίτων ή πληροφορίες που αναρτήθηκαν από τρίτες οντότητες που αφορούν τον ίδιο τον χρήστη. Επίσης για την δημοσίευση αυτών των πληροφοριών σε άλλες ιστοσελίδες και εφαρμογές το Twitter χρησιμοποιεί το API του (application programming interface)
- Πληροφορίες επικοινωνίας, όπως την διεύθυνση ηλεκτρονικού ταχυδρομείου και το κινητό τηλέφωνο για πιστοποίηση και ασφάλεια του λογαριασμού
- Πληροφορίες από την υπηρεσία προσωπικών μηνυμάτων μεταξύ των χρηστών. Αυτές οι πληροφορίες μπορεί να είναι ιστότοποι που έχουν σταλεί σε προσωπικό μήνυμα και περιέχουν κάποιο κακόβουλο λογισμικό ή να είναι πληροφορίες σχετικές με την οντότητα που επικοινωνεί ένας χρήστης με έναν άλλον και την χρονική στιγμή που το κάνει, αλλά όχι πληροφορίες αναφορικά με το κείμενο που περιλαμβάνει οι συζητήσεις τους.
- Πληροφορίες πιστωτικής ή χρεωστικής κάρτας

Πληροφορίες που παίρνονται αυτοματοποιημένα από την εφαρμογή

- Πληροφορίες τοποθεσίας τις οποίες αποκτά μέσω της διεύθυνσης IP ή των ρυθμίσεων της συσκευής για να παρέχει υπηρεσίες στον χρήστη
- Διευθύνσεις που επισκέπτεται ο χρήστης από τα προωθητικά email που στέλνει το Twitter ή από τα «Tweets» που εμφανίζονται σε άλλες ιστοσελίδες ή κινητές εφαρμογές.
- Cookies
- Χρήση πληροφοριών του χρήστη για αποδοτικότερες διαφημίσεις που να σχετίζονται με τις ανάγκες του, παίρνοντας πληροφορίες από τους διαφημιστές
- Λήψη πληροφοριών χρήστη από τρίτες οντότητες που δεν είναι διαφημιστές, όπως συνεργάτες που συμβάλλουν στην ασφάλεια και βελτίωση του περιεχομένου της πλατφόρμας του Twitter.

Κοινοποίηση δεδομένων σε τρίτες οντότητες

- Παροχείς υπηρεσιών
- Σε διαφημιστές (Μη προσωπικά δεδομένα)
- Σε περίπτωση αλλαγής της ιδιοκτησίας της εφαρμογής
- Σε περίπτωση που απαιτηθούν για νομικούς λόγους ή από την κυβέρνηση

5.Viber

Το Viber είναι μια εφαρμογή κοινωνικής δικτύωσης, όπου ο χρήστης μπορεί να ανταλλάξει άμεσα μηνύματα, να πραγματοποιήσει βίντεο-κλήσεις και να στείλει μηνύματα σε άλλους χρήστες. Επιπλέον δίνεται η δυνατότητα επικοινωνίας με το πραγματικό κινητό τηλέφωνο του παραλήπτη, υπηρεσία όμως που προσφέρεται επί πληρωμή.

Μελετώντας την πολιτική ιδιωτικότητας [27] της εφαρμογής διαπιστώθηκαν τα εξής:

Πληροφορίες που συλλέγει το Viber

- Πληροφορίες λογαριασμού όπως όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, ημερομηνία γέννησης, εικόνα προφίλ, καθώς και τις επαφές του τηλεφώνου και το κινητό τηλέφωνο του χρήστη σε περίπτωση που ο ίδιος εγκρίνει την πρόσβαση σε αυτά.
- Πληροφορίες από κοινωνικά δίκτυα σε περίπτωση που ο χρήστης συνδεθεί με τον λογαριασμό Viber σε κοινωνικά δίκτυα τρίτων οντοτήτων όπως Facebook, Twitter, VK.
- Πληροφορίες κατάστασης χρήστη, παρέχοντας σε άλλους χρήστες την κατάσταση σύνδεσης, αν διαβάστηκε ή όχι κάποιο μήνυμα που παρέλαβε ο χρήστης, την διάρκεια κλήσης σε περίπτωση που αυτή πραγματοποιήθηκε. Φυσικά οι συγκεκριμένες πληροφορίες μπορούν να γίνουν αόρατες σε άλλους χρήστες, αν ο χρήστης προβεί σε τροποποίηση ρυθμίσεων. Σε περίπτωση που ο χρήστης χρησιμοποιήσει τις επεκτάσεις των μηνυμάτων ή προβεί σε κάποια αγορά εντός της εφαρμογής, εφαρμογή λαμβάνει πληροφορίες σχετικά με την αναζήτηση του χρήστη και τον τρόπο διαμοίρασης των στοιχείων που αγόρασε. Επιπλέον, συλλέγονται πληροφορίες σχετικά με τα προφίλ

χρηστών που επισκέφθηκε ο χρήστης και του περιεχομένου που είδε σε αυτά για βελτίωση των υπηρεσιών της εφαρμογής

- Πληροφορίες κινητής συσκευής, όπως το λειτουργικό σύστημα της συσκευής, τον περιηγητή αναζήτησης, το ασύρματο δίκτυο, τον πάροχο κινητής τηλεφωνίας και την τοποθεσία του χρήστη σε περίπτωση που αυτός το επιτρέψει
- Προσωπικές πληροφορίες όπως τα γραπτά μηνύματα και οι κλήσεις που πραγματοποιεί ο χρήστης δεν διαβάζονται ή ακούγονται από αυτούς που διαχειρίζονται τα προσωπικά δεδομένα των χρηστών και σε περίπτωση που σταλθούν επιτυχώς δεν αποθηκεύονται ούτε στους servers σύμφωνα με την πολιτική ιδιωτικότητας

Τρόπος χρήσης των δεδομένων από την εφαρμογή

- Για συγχρονισμό μεταξύ συσκευών
- Για πιο έγκυρη αναπαράσταση διαφημίσεων
- Για δημιουργία του προφίλ του χρήστη
- Για την επίτευξη επικοινωνίας με τους άλλους χρήστες
- Βελτίωση των υπηρεσιών σε μελλοντικές εκδόσεις της εφαρμογής
- Παροχή προσφορών
- Επεξεργασία των πληρωμών του χρήστη
- Σε περίπτωση που απαιτηθούν από το νόμο
- Αποτροπή απάτης και ανεπιθύμητων μηνυμάτων
- Επικοινωνία με τον χρήστη σε περίπτωση που αντιμετωπίζει κάποιο πρόβλημα

6.WhatsApp

Το WhatsApp είναι άλλη μία εφαρμογή κοινωνικής δικτύωσης εξίσου διάσημη με το Viber. Όπως είδαμε και σε άλλες εφαρμογές, έτσι και το WhatsApp διαχωρίζει τις πληροφορίες που συλλέγει σε τρεις κατηγορίες όπως αυτές αναφέρονται στην πολιτική ιδιωτικότητας [28] που είναι αναρτημένη στο διαδίκτυο. Πιο συγκεκριμένα:

Πληροφορίες που παρέχει ο χρήστης

- Πληροφορίες λογαριασμού όπως email, κινητό τηλέφωνο ή φωτογραφία προφίλ
- Μηνύματα όπως συνομιλίες, φωτογραφίες, βίντεο, ηχητικά μηνύματα, αρχεία και διαμοιρασμός τοποθεσίας. Όλα τα παραπάνω διαγράφονται απευθείας από τους servers της εταιρείας, ωστόσο σε κάποιες περιπτώσεις τα μηνύματα αποθηκεύονται κρυπτογραφημένα στους servers για ένα μικρό χρονικό διάστημα
- Πληροφορίες από υπηρεσίες πληρωμής
- Εξυπηρέτηση πελατών

Πληροφορίες που παίρνονται αυτοματοποιημένα από την εφαρμογή

- Πληροφορίες αναφορικά με την δραστηριότητα του χρήστη στις υπηρεσίες της εφαρμογής όπως η διάρκεια αλληλεπίδρασης με τους άλλους χρήστες, ποιες υπηρεσίες

χρησιμοποιεί περισσότερο ο χρήστης για παράδειγμα μηνύματα, κλήσεις ή πληροφορίες όπως τη εικόνα προφίλ, την ημερομηνία που ήταν τελευταία φορά διαθέσιμος ο χρήστης και το πότε επεξεργάστηκε τις πληροφορίες του προφίλ του.

- Πληροφορίες συσκευής και σύνδεσης όπως το λειτουργικό σύστημα, την έκδοση της εφαρμογής, το ποσοστό της μπαταρίας, το δίκτυο κινητής τηλεφωνίας, την διεύθυνση IP.
- Πληροφορίες τοποθεσίας σε περίπτωση που δώσει ο χρήστης το συγκεκριμένο δικαίωμα στην εφαρμογή για να μπορεί ο χρήστης να διακρίνει κοντινές τοποθεσίες ή τοποθεσίες που διαμοιράστηκε άλλος χρήστης μαζί του, αλλά και για λόγους διάγνωσης και αντιμετώπισης προβλημάτων των χρηστών. Για να καθοριστέι η θέση του χρησιμοποιείται η διεύθυνση IP, το GPS, το Bluetooth ή ακόμα και πληροφορίες από κοντινές συνδέσεις ασύρματου δικτύου (WI-FI).
- Cookies

Πληροφορίες από τρίτες οντότητες

- Πληροφορίες που παρέχουν άλλοι χρήστες σχετικά με τον χρήστη της εφαρμογής, μέσω της χρήσης της εφαρμογής όπως ο αριθμός κινητού τηλεφώνου, το όνομα κ.α.
- Πληροφορίες από επιχειρήσεις, με τις οποίες ο χρήστης συνδέεται χρησιμοποιώντας την εφαρμογή. Αυτές οι πληροφορίες αφορούν τον τρόπο με τον οποίο αλληλεπιδρά ο χρήστης με αυτές. Επίσης, οι επιχειρήσεις στο WhatsApp μπορούν να χρησιμοποιήσουν άλλες εταιρίες για να τους βοηθήσουν με την διαχείριση των πληροφοριών που συλλέγουν.
- Πληροφορίες από παροχείς τρίτης οντότητας με τους οποίους συνεργάζεται το WhatsApp όπως το Facebook

Τρόπος χρήσης των πληροφορίων του χρήστη

- Για παροχή και βελτίωση και παροχή των υπηρεσιών της εφαρμογής
- Ασφάλεια και προστασία του χρήστη
- Επικοινωνία με τον χρήστη για τις υπηρεσίες που προσφέρει η εφαρμογή και τους συνεργάτες του Facebook
- Μη χρήση των πληροφοριών για διαφημιστικούς λόγους από τρίτες οντότητες
- Επικοινωνία μεταξύ επιχειρήσεων που συνεργάζονται με την εφαρμογή
- Μετρήσεις και αναλύσεις

7.E-radio

Το e-radio είναι μια εφαρμογή που χρησιμοποιείται ευρέως στην Ελλάδα και περιέχει ένα μεγάλος πλήθος ραδιοφωνικών σταθμών από όλες τις πόλεις, τους οποίους ο χρήστης μπορεί να ακούσει απλά έχοντας πρόσβαση στο διαδίκτυο. Κρίθηκε απαραίτητο για την παρούσα έρευνα να συμπεριλάβουμε μια ελληνική εφαρμογή για να διαπιστώσουμε τι είδους δεδομένα συλλέγει και πως τα χρησιμοποιεί. Έπειτα θα εξετάσουμε και μια εφαρμογή που περιέχει ραδιοφωνικούς σταθμούς από

όλο τον κόσμο και να συγκρίνουμε τις δύο εφαρμογές (Κεφάλαιο 5, Υποενότητα 5.5). Μελετώντας την πολιτική ιδιωτικότητας [29] του E-radio διακρίνουμε τις εξής πληροφορίες που συλλέγει η εφαρμογή:

Πληροφορίες που δίνει ο χρήστης

- Πληροφορίες λογαριασμού σε περίπτωση που δημιουργήσει ο χρήστης όπως το όνομα, τη διεύθυνση ηλεκτρονικού ταχυδρομείου, ημερομηνία γέννησης, φύλο, τον κωδικό του λογαριασμού και τον ταχυδρομικό κώδικα.
- Πληροφορίες αν συμμετέχει σε διαγωνισμούς και έρευνες τις οποίες δεν διασαφηνίζει
- Πληροφορίες που δίνει ο χρήστης για να λαμβάνει προωθητικές ενέργειες, οι οποίες επίσης δεν αναφέρονται

Πληροφορίες που συλλέγονται αυτοματοποιημένα

- Πληροφορίες αναφορικά με τις δραστηριότητες ακρόασης και χρήσης της εφαρμογής όπως ραδιοφωνικούς σταθμούς, αγαπημένα, καλλιτέχνες, τραγούδια
- Πληροφορίες από κοινωνικά δίκτυα σε περίπτωση που συνδεθεί ο χρήστης με κάποιο λογαριασμό κοινωνικού δικτύου στην εφαρμογή
- Πληροφορίες από τον υπολογιστή ή το κινητό, όπως την διεύθυνση IP, το λειτουργικό σύστημα και άλλες software ή hardware πληροφορίες οι οποίες δεν αναφέρονται
- Πληροφορίες σχετικά με την τοποθεσία του χρήστη και πιο συγκεκριμένα την γενική γεωγραφική θέση του, την οποία χρησιμοποιεί για να παρέχει περιεχόμενο και υπηρεσίες που είναι παραμετροποιημένες για την συγκεκριμένη τοποθεσία.
- Cookies σε περίπτωση που τα έχει ενεργοποιημένα ο χρήστης

Χρήση των δεδομένων που συλλέγονται από την εφαρμογή

- Προσαρμογή των διαφημίσεων και του περιεχομένου που βλέπει ο χρήστης
- Βελτίωση της εμπειρίας του χρήστη στην ιστοσελίδα ή στην εφαρμογή
- Ικανοποίηση των αιτημάτων των χρηστών για συγκεκριμένα προϊόντα και υπηρεσίες, όπως αποστολή ενημερωτικών-διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και συμμετοχή σε δημοσκοπήσεις και διαγωνισμούς
- Για αποστολή περιεχομένου ανάλογα τις συνήθειες και την γεωγραφική θέση του χρήστη
- Για αποστολή πληροφοριών που αφορούν νέες δυνατότητες που προστέθηκαν στην εφαρμογή
- Παροχή τεχνικής υποστήριξης

Διαμοιρασμός πληροφοριών σε τρίτες οντότητες

- Πληροφορίες που συλλέγονται από τον λογαριασμό του χρήστη, εφόσον αυτός δημιουργήσει έναν
- Παροχή μόνο απαιτούμενων πληροφοριών (οι οποίες δεν αναφέρονται) σε εσωτερικούς συνεργάτες ή τρίτες οντότητες που συνεργάζεται το e-radio για την παροχή υπηρεσιών όπως διαχείριση πληροφοριών αλληλογραφίας, συντήρηση βάσεων δεδομένων,

επεξεργασία πληρωμών, επεξεργασία πληρωμών, αναλύσεις, προσαρμογή της διαφήμισης

- Διαμοιρασμός, μεταβίβαση ή και πώληση των στοιχείων σε περίπτωση συγχώνευσης της εταιρίας με άλλην, πτώχευσης, , πώλησης περιουσιακών στοιχείων ή μεταβίβαση της υπηρεσίας σε άλλον πάροχο. Επίσης, αναφέρεται ότι δεν είναι δυνατός ο έλεγχος του τρόπου με τον οποίο οι εν λόγω φορείς μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες
- Διαμοιρασμός πληροφοριών με θυγατρικές εταιρίες
- Διαμοιρασμός πληροφοριών με μέσα κοινωνικής δικτύωσης όπως το Facebook αν και αναφέρεται πως δεν διαμοιράζονται προσωπικές πληροφορίες
- Διαμοιρασμός πληροφοριών αν απαιτείται από το νόμο

8.TuneIn Radio

Το TuneIN Radio είναι άλλη μια εφαρμογή παροχής ραδιοφωνικών σταθμών από όλο τον κόσμο με την χρήση του διαδικτύου. Η πολιτική ιδιωτικότητας [30] μιας τέτοιας εφαρμογής παρουσιάζει αρκετό ενδιαφέρον, εφόσον αποτελεί την πιο διάσημη εφαρμογή ραδιοφώνου, αν ληφθούν υπόψιν οι λήψεις της. Πιο συγκεκριμένα η εφαρμογή συλλέγει και διαχειρίζεται τις πληροφορίες του χρήστη ως εξής:

Πληροφορίες που παρέχονται από τον χρήστη

- Πληροφορίες λογαριασμού σε περίπτωση που ο χρήστης δημιουργήσει, όπως όνομα ημερομηνία γέννησης, κωδικός πρόσβασης και διεύθυνση ηλεκτρονικού ταχυδρομείου. Σε περίπτωση που ο χρήστης εισέλθει στο σύστημα σαν εκφωνητής κάποιου ραδιοφωνικού σταθμού πρέπει να παρέχει πληροφορίες όπως το κινητό του τηλέφωνο, την διεύθυνση ζωντανής ροής του σταθμού και άλλες πληροφορίες σχετικά με τον σταθμό.
- Πληροφορίες πληρωμής όπως τον αριθμό πιστωτικής κάρτας σε περίπτωση που κάποιος χρήστης γίνει συνδρομητής σε κάποια υπηρεσία της εφαρμογής
- Πληροφορίες που παρέχει ο χρήστης επικοινωνώντας με το τμήμα εξυπηρέτησης πελατών
- Στοιχεία επικοινωνίας από συνεργάτες ή πωλητές που παρέχονται από τους ίδιους για την επίτευξη καλύτερης συνεργασίας
- Πληροφορίες που παρέχει ο χρήστης σε περίπτωση αίτησης εργασίας στο TuneIn, όπως αναφορές και βιογραφικά σημειώματα

Προσωπικές πληροφορίες που συλλέγονται από τρίτες οντότητες

- Πληροφορίες από κοινωνικά δίκτυα σε περίπτωση που συνδεθεί ο χρήστης στην εφαρμογή με έναν τέτοιο λογαριασμό όπως το Facebook
- Πληροφορίες που παρέχονται από άλλους χρήστες ή τους διαφημιστές της εφαρμογής

Προσωπικές πληροφορίες που συλλέγονται με αυτοματοποιημένο τρόπο

- Χρησιμοποιώντας της υπηρεσίες της εφαρμογής συλλέγονται πληροφορίες όπως οι ραδιοφωνικοί σταθμοί ή οι καλλιτέχνες που ακούει ο χρήστης, προφίλ χρηστών που επισκέπτεται ο χρήστης, τις αναζητήσεις, περιεχόμενο ή άτομα που ακολουθεί ο χρήστης στην εφαρμογή, τα σχόλια και το περιεχόμενο που αναρτάει.
- Τις επαφές του χρήστη που υπάρχουν στην συσκευή εφόσον δοθεί η άδεια από τον ίδιο
- Πληροφορίες τοποθεσίας του χρήστη με την συγκατάθεση του, χρησιμοποιώντας είτε το GPS της συσκευής είτε μέσω της διεύθυνσης IP. Η χρήση της τοποθεσίας σύμφωνα με την πολιτική απορρήτου γίνεται για λόγους παροχής ειδοποιήσεων, υπηρεσιών όπως την παροχή τοπικών ραδιοφωνικών σταθμών, αλλά και λόγους διαφήμισης.
- Πληροφορίες συσκευής όπως ο περιηγητής αναζήτησης, το λειτουργικό σύστημα της κινητής συσκευής και τα μοναδικά αναγνωριστικά των συσκευών
- Πληροφορίες widget: Όταν ο χρήστης συνδεθεί σε μια ιστοσελίδα που εμπεριέχει ένα TuneIn widget (όπως το TuneIn player και το TuneIn Follow Button), η εφαρμογή μπορεί να λάβει πληροφορίες σχετικά με την ιστοσελίδα όπως το όνομα της σελίδας, την διεύθυνση IP και άλλες πληροφορίες της συσκευής.
- Cookies

Χρήση των πληροφοριών από την εφαρμογή

- Εσωτερική χρήση και χρήση που σχετίζεται με τις υπηρεσίες της εφαρμογής
- Ανάλυση και βελτιστοποίηση των υπηρεσιών
- Επικοινωνία με τον χρήστη
- Διαφημίσεις
- Αποστολή προσαρμοσμένου περιεχομένου στις απαιτήσεις του κάθε χρήστη
- Συγκεντρωτικά δεδομένα για στατιστική ανάλυση και άλλους νομικούς σκοπούς
- Συνεργάτες και προμηθευτές
- Αξιολόγηση των αιτήσεων εργασίας στο TuneIn
- Χρήση των δεδομένων για προστασία των νόμιμων δικαιωμάτων της εφαρμογής

9.Netflix

Το Netflix είναι μια συνδρομητική πλατφόρμα, μέσω της οποίας ο χρήστης έχει πρόσβαση σε μεγάλο πλήθος ταινιών και σειρών που μπορεί να δει χωρίς να χρειαστεί να τις κατεβάσει στην συσκευή του. Παρακάτω θα μελετηθεί η πολιτική ιδιωτικότητας [31] της συγκεκριμένης εφαρμογής για να διαπιστωθεί ο τρόπος με τον οποίο συλλέγει και διαχειρίζεται τα δεδομένα εκατομμύρια χρηστών.

Πληροφορίες που παρέχει ο χρήστης

- Προσωπικές πληροφορίες με το πέρας της δημιουργίας του λογαριασμού χρήστη, όπως διεύθυνση ηλεκτρονικού ταχυδρομείου, τον ταχυδρομικό κώδικα, τον τρόπο πληρωμής της υπηρεσίας και τον αριθμό κινητού τηλεφώνου. Οι συγκεκριμένες πληροφορίες

παρέχονται επίσης και κατά την διάρκεια την επικοινωνίας με την εξυπηρέτηση πελατών ή συμμετοχής σε έρευνες και προωθητικές ενέργειες.

- Πληροφορίες που παρέχει ο χρήστης όταν υποβάλλει βαθμολογίες, τις προσωπικές του προτιμήσεις και τις ρυθμίσεις λογαριασμού.

Πληροφορίες που συλλέγονται με αυτοματοποιημένο τρόπο

- Πληροφορίες που σχετίζονται με την δραστηριότητα των χρηστών στο Netflix, όπως οι επιλογές τίτλων, το ιστορικό προβολών και τα ερωτήματα αναζήτησης
- Πληροφορίες από τις αλληλεπιδράσεις των χρηστών με τα email, τις ειδοποιήσεις και τα μηνύματα κειμένου που στέλνει η εταιρία
- Λεπτομέρειες της επικοινωνίας του χρήστη με την εξυπηρέτηση πελατών, όπως την ώρα την ημερομηνία, τον λόγο επικοινωνίας και σε περίπτωση τηλεφωνικής κλήσης τον αριθμό τηλεφώνου και την ηχογράφηση της κλήσης
- Αναγνωριστικά συσκευών τα οποία δεν αναφέρονται εκτενώς
- Χαρακτηριστικά συσκευών και λογισμικού όπως στοιχεία σύνδεσης, πηγή παραπομπής, διεύθυνση IP μέσω της οποίας η εταιρία εντοπίζει την τοποθεσία του χρήστη και το πρόγραμμα περιήγησης
- Πληροφορίες μέσω των Cookies

Πληροφορίες που συλλέγονται από συνεργάτες που αλληλεπιδρά ο χρήστης

Στους συνεργάτες που αλληλεπιδρά ο χρήστης περιλαμβάνονται ο πάροχος υπηρεσιών τηλεόρασης ή διαδικτύου ή οι πάροχοι συσκευών πολυμέσων με δυνατότητα «streaming» μέσω των οποίων είναι διαθέσιμη η υπηρεσία Netflix στις συσκευές τους ή οι πάροχοι κινητής τηλεφωνίας που παρέχουν υπηρεσίες στους χρήστες εισπράτοντας πληρωμές τις οποίες αποδίδουν στο Netflix ή οι πάροχοι ψηφιακών βοηθών. Οι πληροφορίες που συλλέγονται είναι:

- Ερωτήματα αναζήτησης από εντολές που δίνει ο χρήστης μέσω των ψηφιακών βοηθών
- Πληροφορίες ενεργοποίησης υπηρεσιών, όπως η διεύθυνση ηλεκτρονικού ταχυδρομείου και άλλων στοιχείων επικοινωνίας
- Αναγνωριστικά συσκευών που υποστηρίζουν την εμπειρία εγγραφής στην υπηρεσία Netflix και την διαδικασία διεκπεραίωσης πληρωμών των συνεργατών του χρήστη.

Πληροφορίες από άλλες πηγές

- Παρόχους υπηρεσιών που συμβάλλουν στην γνωστοποίηση της τοποθεσίας του χρήστη με την χρήση της διεύθυνσης IP του.
- Παρόχους υπηρεσιών πληρωμής που παρέχουν στην εταιρία στοιχεία πληρωμής ή ενημερώσεις αυτών.
- Παρόχους δεδομένων από τους οποίους η εταιρία λαμβάνει δημογραφικά δεδομένα και δεδομένα που σχετίζονται με τα ενδιαφέροντα των χρηστών

Γνωστοποίηση των πληροφοριών σε τρίτες οντότητες

- Στον όμιλο εταιρειών Netflix
- Στους παρόχους υπηρεσιών όπως άλλες εταιρίες και αντιπροσώπους
- Συνεργάτες
- Προωθητικές προσφορές
- Σε περίπτωση ανάγκης προστασίας του Netflix, γνωστοποιώντας της πληροφορίες όταν ζητηθούν από το νόμο ή τον εντοπισμό παράνομων δραστηριοτήτων κατά την χρήση της υπηρεσίας ή τυχόν παραβιάσεων των όρων χρήσης ή για προστασία των δικαιωμάτων, της ιδιοκτησίας ή της ασφάλειας της ετιαρίας.
- Σε περίπτωση μεταβίβαση της επιχείρησης σε τρίτους

10.Kodi

Το Kodi είναι άλλη μια πλατφόρμα παροχής υπηρεσιών οπτικοακουστικού περιεχομένου όπως ταινίες και σειρές. Δεν είναι τόσο διαδεδομένη όσο το Netflix, αλλά παρέχεται δωρεάν στους χρήστες. Ο λόγος για τον οποίο η συγκεκριμένη εφαρμογή δεν είναι τόσο διαδεδομένη στο ευρύ κοινό, σχετίζεται ίσως με την δυσχρηστία της αρχικής ρύθμισης της εφαρμογής, διότι ο χρήστης θα πρέπει να προβεί σε εγκαταστάσεις ορισμένων επεκτάσεων που έχουν δημιουργηθεί από τρίτους για να απολαύσουν τις δυνατότητες της εφαρμογής. Ωστόσο κρίθηκε απαραίτητη η μελέτη της συγκεκριμένης πολιτικής απορρήτου [32] για να διαπιστωθούν οι διαφορές ανάμεσα σε μια δωρεάν και μια επί πληρωμή εφαρμογή όπως είναι το Netflix.

Τρόποι συλλογής πληροφοριών του χρήστη

- Σε περίπτωση που ο χρήστης αποφασίσει να τις παρέχει όπως για παράδειγμα μέσω της χρήσης των forum
- Με αυτοματοποιημένο τρόπο μέσω του λογισμικού και των υπηρεσιών της εφαρμογής όπως στην περίπτωση που η εφαρμογή συνδεθεί με τους servers της εταιρίας για να αναβαθμίσει της επεκτάσεις που έχει εγκαταστήσει ο χρήστης
- Μέσω των Cookies που χρησιμοποιούνται στην ιστοσελίδα της εταιρίας

Ωστόσο είναι ορατό πως δεν αναφέρονται το είδος των πληροφοριών που συλλέγει η εφαρμογή, γεγονός που κάνει τους χρήστες που διαβάζουν την πολιτική απορρήτου επιφυλακτικούς για την ασφάλεια των δεδομένων τους.

Χρήση των πληροφοριών που συλλέγονται

- Παροχή και βελτίωση του λογισμικού και των υπηρεσιών

Γνωστοποίηση των πληροφοριών σε τρίτες οντότητες

- Στην περίπτωση που ζητηθούν από άλλους και δοθεί η άδεια από τον ίδιο το χρήστη να διαμοιραστούν.

- Για εκπαιδευτικούς σκοπούς, δημοσιεύοντας μη προσωπικές πληροφορίες για βελτίωση του λογισμικού και προώθηση του ανοικτού κώδικα
- Στην περίπτωση που απαιτηθούν από το νόμο
- Στην περίπτωση χρεοκόπησης ή πώλησης της εταιρίας σε τρίτη οντότητα

Είναι αναγκαίο να αναφερθεί ότι οι πολιτικές απορρήτου αναλύθηκαν ως προς τις πληροφορίες που συλλέγουν και ως προς τον τρόπο που τις χρησιμοποιούν ή τις διαμοιράζονται, και για αυτό το λόγο απαιτήθηκε η ανάγνωση των συγκεκριμένων κομματιών της πολιτικής και όχι ολόκληρου του κειμένου. Έτσι βάσει των πληροφοριών που συλλέχτηκαν, στο επόμενο κεφάλαιο (Αποτελέσματα Έρευνας), θα εξαχθούν ορισμένα συμπεράσματα για τον βαθμό στον οποίο οι παραπάνω πολιτικές έχουν εισάγει στα δικαιώματα που απαιτούν, τα όσα γράφονται στην πολιτική τους. Στη συνέχεια θα γίνει και σύγκριση των πολιτικών απορρήτου που ανήκουν στην ίδια κατηγορία όπως uc browser και google chrome, για να διαπιστωθεί ποια εφαρμογή από κάθε κατηγορία είναι πιο ασφαλής για τον χρήστη να εγκαταστήσει στο κινητό του τηλέφωνο.

4. Αποτελέσματα Έρευνας

4.1. Στατιστικά στοιχεία για τις άδειες πρόσβασης

Όνομα Κατηγορίας	Μέσος όρος δικαιωμάτων
Tools	34.04
Communication	33.34
Personalization	30.86
Social	28.04
Productivity	27.87
Shopping	26.34
Finance	25.58
Lifestyle	23.18
Health and Fitness	22.04
News and magazines	21.97
Dating	21.00
Business	20.91
Maps and navigation	20.62
Music and Audio	19.80
Transport	19.40
Travel and Local	19.29
Auto and Vehicles	18.92
Video Players and Editors	17.28
Entertainment	17.25
Photography	17.02
Art and Design	16.16
Casino games	15.35
Food and Drink	15.28
Parenting	14.81
House and Home	14.38
Weather	13.96
Media and Video	13.94

Education	13.18
Medical	13.04
Role Playing games	12.54
Trivia games	12.18
Action games	12.08
Sports	11.80
Events	11.67
Card games	11.43
Sports games	11.20
Word games	10.91
Multimedia	10.50
Comics	10.32
Music games	10.04
Arcade games	9.91
Racing games	9.82
Puzzle games	9.76
Casual games	9.50
Adventure games	9.48
Strategy games	9.31
Board games	9.14
Books and reference	9.06
Simulation games	8.98
Libraries and demo	8.88
Themes	8.35
Family games	7.14
Health	6.82
Educational games	6.66
Brain and puzzle games	4.37
Όλες οι εφαρμογές	**18.24**
Όλα τα παιχνίδια	**9.98**
Γενικός μέσος όρος	**15,39**

Πίνακας 7: Μέσος όρος αδειών ανά κατηγορία

Όνομα Άδειας	Αρ. Εμφάνισης	Ποσοστό Εμφάνισης
INTERNET	2534	97.64%
ACCESS NETWORK STATE	2483	95.68%
WAKE LOCK	2002	77.14%
WRITE EXTERNAL STORAGE	1827	70.40%
Google.c2dm. RECEIVE	1623	62.54%
ACCESS WIFI STATE	1620	62.42%
VIIBRATE	1293	49.82%
READ EXTERNAL STORAGE	1222	47.09%
INTALL REFERRER SERVICE	1145	44.12%
Android.vending.BILLING	1090	42.00%
RECEIVE BOOT COMPLETED	1029	39.65%
ACCESS FINE LOCATION	837	32.25%
ACCESS COARSE LOCATION	789	30.40%
READ PHONE STATE	781	30.09%
CAMERA	613	23.62%
GET ACCOUNTS	574	22.11%
RECORD AUDIO	445	17.14%
FOREGROUND SERVICE	429	16.53%
BLUETOOTH	415	15.99%
CHANGE WIFI STATE	371	14.29%
GET TASKS	368	14.18%
SYSTEM ALERT WINDOW	366	14.10%

READ CONTACTS	343	13.21%
USE CREDENTIALS	310	11.94%
Android.vending.CHECK LICENSE	297	11.44%
MODIFY AUDIO SETTINGS	296	11.40%
INSTALL SHORTCUT	252	9.71%
WRITE SETTINGS	250	9.63%
MANAGE ACCOUNTS	217	8.36%
CHANGE NETWORK STATE	193	7.43%

Πίνακας 8: Οι 30 άδειες που ζητούνται περισσότερο και το ποσοστό των εφαρμογών που τις ζητούν

Όνομα Άδειας	Αρ. Εμφάνισης	Ποσοστό Εμφάνισης
ACCESS FINE LOCATION	837	32.25%
ACCESS COARSE LOCATION	789	30.40%
READ PHONE STATE	781	30.09%
CAMERA	613	23.62%
GET ACCOUNTS	574	22.11%
RECORD AUDIO	445	17.14%
READ CONTACTS	343	13.21%
CALL PHONE	191	7.36%
READ CALENDAR	100	3.85%
WRITE CONTACTS	97	3.73%
WRITE CALENDAR	81	3.12%

READ SMS	78	3.00%
RECEIVE SMS	71	2.73%
SEND SMS	60	2.31%
READ CALL LOG	47	1.81%
WRITE CALL LOG	23	0.88%
PROCESS OUTGOING CALLS	18	0.69%
ANSWER PHONE CALLS	13	0.50%
RECEIVE MMS	13	0.50%
BODY SENSORS	11	0.42%
RECEIVE WAP PUSH	3	0.11%
USE SIP	3	0.11%
READ PHONE NUMBERS	3	0.11%
ADD VOICEMALL	0	0%

Πίνακας 9: Οι 24 επικίνδυνες άδειες και το ποσοστό των εφαρμογών που τις ζητούν

Όνομα Εφαρμογής	Αριθμός Αδειών
Alipay	237
Hide app, private dating, safe chat – privacyhider	181
Shareit	180
Phone Clone	166
Samsung Email	140
Parallel Space Lite- Dual App	132

Intelligent Hub	126
HTC Sense Home	117
Car Mode	106
Samsung Pay	106
Virus Cleaner 2019: Scan & Remove Virus, Antivirus	96
Phone Cleaner & Virus Cleaner -Super Phone Cleaner	96
Huawei Backup	96
Samsung Experience Service	95
Smart Things	92
Samsung Internet Browser	91
Huawei Health	90
Huawei Wallet	84
Kindle	81
Color Flash Launcher - Call Screen, Themes	81
Microsoft Launcher	80
Gallery	78
KingRoot	77
ME Launcher - Theme & 3D Wallpaper, Fast	75
Galaxy Apps	75
Amazon	75
MiLocker	74

Clean Master- Space Cleaner & Antivirus & Free Ram	74
Joy launcher - Live wallpaper	74
Phone	71

Πίνακας 10: Οι 30 πιο απαιτητικές εφαρμογές σε άδειες

Όνομα Εφαρμογής	Αριθμός Αδειών
Five Nights at Freddy's: SL	1
Candy Camera - Light Effects	1
Isha & Pawan	1
Drink Water	1
Hello Android	1
Terraria	1
Majotori	1
Cat Fishing	1
Tic Tac Toe	1
Peppa Pig: Sports Day	1
Google Maps Go – Directions, Traffic & Transport	1
MX Player Codec (Tegra3)	1
The Simpsons Game TRIVIA	1
Anti Mosquito	1
FastChallenge	1

LEGO® Juniors Create & Cruise	1
Age of Civilizations	1
Smart Watch	1
Awesome App	1
Five Nights at Freddy's 2 Demo	1
Poweramp Full Version Unlocker	1
Sound Search for Google Play	1
Grand Theft Auto - GTA	1
Age of Civilizations II	1
Daniel	1
Angry Neighbor	1
Color Days Widget	1
Beaming Service for Samsung	1
OpenCV Manager	1
ANYCARD	1

Πίνακας 11: Οι 30 λιγότερο απαιτητικές εφαρμογές σε άδειες

Από τους παραπάνω πίνακες μπορούμε να εξάγουμε τα εξής συμπεράσματα:

- Από τον πίνακα 1 συνειδητοποιούμε ότι οι μεγαλύτεροι μέσοι όροι παρατηρούνται στις κατηγορίες tools, communication, personalization, social και productivity, διότι οι προγραμματιστές των εφαρμογών γνωρίζουν την διασημότητα των συγκεκριμένων κατηγοριών, αφού οι ίδιες περιλαμβάνουν επεξεργαστές κειμένου, clouds, θέματα, κοινωνικά δίκτυα, εφαρμογές άμεσων μηνυμάτων, τις οποίες κάθε χρήστης θέλει να έχει στο κινητό του. Επίσης, οι εφαρμογές έχουν σχεδόν διπλάσιο μέσο όρο απαιτούμενων δικαιωμάτων από τα παιχνίδια, γεγονός που δικαιολογείται και από την διασημότητα των εφαρμογών έναντι των παιχνιδιών, αλλά και των περισσότερων δυνατοτήτων που προσφέρουν που οδηγεί και στην ανάγκη χρήσης χαρακτηριστικών όπως το η τοποθεσία, το Bluetooth, το δίκτυο και άλλα.
- Από τον πίνακα 2 είναι εμφανές πως σχεδόν όλες οι εφαρμογές που μελετήθηκαν στην παρούσα διπλωματική εργασία χρησιμοποιούν το δικαίωμα INTERNET και ACCESS NETWORK STATE, τα οποία δεν αποτελούν πρόβλημα για την ασφάλεια του χρήστη ή έχουν χαμηλό βαθμό επικινδυνότητας. Ωστόσο τα ποσοστά των αδειών READ-WRITE EXTERNAL STORAGE και ACCESS FINE-COARSE LOCATION είναι άκρως ανησυχητικά και βάζουν σε κίνδυνο τον χρήστη και τα δεδομένα του.
- Στον πίνακα 3 φαίνεται πως δύο από τα πιο σημαντικά δικαιώματα που επηρεάζουν την ασφάλεια του χρήστη (ACCESS COARSE-FINE LOCATION) χρησιμοποιούνται από περίπου ένα τρίτο των εφαρμογών που μελετήθηκαν, ποσοστό αρκετά μεγάλο, ενώ γενικότερα παρατηρούνται μεγάλα ποσοστά χρήσης επικίνδυνων αδειών από εφαρμογές του aptoide. Έτσι η ασφάλεια των εφαρμογών της συγκεκριμένης ιστοσελίδας μπορεί να αμφισβητηθεί.
- Τέλος από τους πίνακες 4 και 5 μπορούμε να επαληθεύσουμε ότι οι εφαρμογές χρησιμοποιούν περισσότερες άδειες από τα παιχνίδια. Επιπλέον στον πίνακα 4 διακρίνονται 10 εφαρμογές που απαιτούν παραπάνω από 100 άδειες, ενώ και οι 30 εφαρμογές ξεπερνάνε τις 70. Βάσει της λειτουργικότητας των συγκεκριμένων εφαρμογών δεν είναι λογική η χρήση τέτοιου πλήθους αδειών, γεγονός που πρέπει να προβληματίσει τον χρήση για τον τρόπο λειτουργίας τους.

4.2. Σύγκριση αποτελεσμάτων έρευνας με άδειες πρόσβασης εφαρμογών από το Google Play

Συγκρίνοντας την έρευνα που διεξάχθηκε στην συγκεκριμένη διπλωματική εργασία στην ιστοσελίδα του aptoide, με αυτήν της Ματίνας Τσαβλής (Πειραιάς 2016) που περιγράψαμε στην ενότητα 3.3.4, σχετικά με εφαρμογές στο Google Play μπορούμε να συμπεράνουμε τα εξής:

- Οι 4 από τις 5 κατηγορίες στους υψηλότερους μέσους όρους που παρατηρήθηκαν συμβαδίζουν. Ωστόσο οι μέσοι όροι του aptoide σε αυτές είναι πολύ μεγαλύτεροι από αυτοί του play store, γεγονός που δημιουργεί προβληματισμούς. Επιπλέον και στις κατηγορίες με τους χαμηλότερους μέσους όρους παρατηρείται μεγάλη διαφορά στα ποσοστά.
- Αναφορικά με τις άδειες που ζητούνται περισσότερο από τις εφαρμογές, παρατηρώντας τις 5 πιο συχνές παρατηρούμε και εδώ συσχέτιση των τεσσάρων. Ωστόσο, και σε αυτόν τον τομέα τα ποσοστά εμφάνισης στις εφαρμογές του aptoide είναι και πάλι πολύ μεγαλύτερα. Φυσικά, βλέποντας και τις 30 εγγραφές που καταγράφηκαν στις δύο έρευνες, στην περίπτωση του aptoide οι άδειες παρουσιάζονται με μεγαλύτερο ποσοστό.
- Φυσικά στον τομέα των εφαρμογών θα ήταν δύσκολο να υπάρχει συσχέτιση μεταξύ των δύο ερευνών. Βέβαια, είναι εμφανές πως στην περίπτωση του play store μόνο μία εφαρμογή ζητάει περισσότερες από 100 άδειες και οι επόμενες τέσσερις 68, 60, 56 και 53 αντίστοιχα, ενώ στην περίπτωση του aptoide παρατηρήθηκαν 10 εφαρμογές με τριψήφιο αριθμό αδειών και άλλες τόσες ζητούσαν περισσότερες από 80 άδειες.

Οι παραπάνω έρευνες διεξάχθηκαν σε διαφορετικό χρονικό σημείο (2016 έναντι 2019), σε διαφορετικές εφαρμογές και με διαφορετικό δείγμα. Ωστόσο, ακόμα και αν η σύγκριση δεν είναι απόλυτα έμπιστη, είναι εμφανές ότι οι εφαρμογές του aptoide απαιτούν περισσότερες άδειες στο σύνολο τους, ενώ παρατηρούνται υψηλά ποσοστά και στην χρήση των επικίνδυνων αδειών σε σχέση με τις εφαρμογές του Google Play. Όλα τα παραπάνω οδηγούν στο συμπέρασμα, ότι το aptoide δεν σέβεται σε μεγάλο βαθμό τον χρήστη και η ασφάλεια των δεδομένων των χρηστών είναι αμφίβολη. Όλα τα παραπάνω δεν έχουν σκοπό να επιδείξουν την «αθωότητα» του Google Play. Ωστόσο σίγουρα η επίσημη ιστοσελίδα της Google σέβεται περισσότερο τους πελάτες της και παρέχει καλύτερες υπηρεσίες από το aptoide.

4.3. Πληρότητα πολιτικών ιδιωτικότητας των δέκα εφαρμογών συγκριτικά με τα δικαιώματα που απαιτούν

1.Uc Browser

Μελετώντας τα δικαιώματα που απαιτεί η συγκεκριμένη εφαρμογή, παρατηρήθηκε ότι αυτά συσχετίζονται σε μεγάλο βαθμό με τα όσα αναγράφονται στην πολιτική ιδιωτικότητας αναφορικά με τα δεδομένα που συλλέγονται από την εταιρία. Πιο συγκεκριμένα, πληροφορίες όπως η ημερομηνία και ώρα η γλώσσα συστήματος, το ιστορικό του περιηγητή, η έκδοση του περιηγητή, η έκδοση του Android και η λίστα εφαρμογών που έχει εγκατεστημένες ο χρήστης δικαιολογούνται με τις άδειες modify system settings, read home settings, write και read web bookmarks and history και retrieve running apps. Επιπλέον πληροφορίες όπως η διεύθυνση IP, τα δεδομένα κινητής τηλεφωνίας, η κατάσταση του δικτύου και η τοποθεσία αναγράφονται στην λίστα δικαιωμάτων ως view netowork connections, change network connectivity, full network access και access- fine-coarse location. Ωστόσο, πληροφορίες που συλλέγονται όπως το IMEI και η MAC διεύθυνση, δεν αντιστοιχείται στην άδεια read phone state, η οποία είναι υπεύθυνη για αυτόν τον σκοπό. Τέλος, σχετικά με τις επικίνδυνες άδειες που αναγράφονται στην λίστα αδειών της εφαρμογής όπως η πρόσβαση στην κάμερα και τον αποθηκευτικό χώρο, δεν αναφέρεται στην πολιτική ιδιωτικότητας της εφαρμογής τι πληροφορίες συλλέγει η εταιρία από αυτές και πως τις χρησιμοποιεί. Έτσι αν και μεγάλο πλήθος των πληροφοριών που αναγράφονται στην πολιτική του uc browser αντιστοιχεί σε κάποια άδεια, υπάρχουν αρκετές σημαντικές ελλείψεις και η πολιτική απορρήτου δεν μπορεί να θεωρηθεί πλήρης σε αυτόν τον τομέα.

2. Google Chrome

Όπως είδαμε στην περιγραφή της πολιτικής ιδιωτικότητας του Chrome, οι πληροφορίες συλλέγονται μόνο όταν ο χρήστης συνδεθεί με τον λογαριασμό της google και ενεργοποιήσει τον συγχρονισμό της συσκευής. Αυτή η μέθοδος που χρησιμοποιεί ο chrome δικαιολογείται στην λίστα δικαιωμάτων με τις άδειες toggle sync on and off, read sync statistics, read sync settings, add or remove accounts και find accounts on the device. Επίσης, πληροφορίες που σχετίζονται με την τοποθεσία του χρήστη και το ιστορικό αναζήτησης αναφέρονται τόσο στην πολιτική, όσο και στην λίστα δικαιωμάτων (access fine-coarse location, read history). Ωστόσο, ο chrome, όπως και ο uc, έχει κάποιες ελλείψεις στην πολιτική ιδιωτικότητας. Ενώ στην λίστα δικαιωμάτων αναφέρονται ορισμένες επικίνδυνες άδειες όπως read contacts, record audio, access camera και read-write storage, δεν υπάρχει κάποια αντίστοιχη αναφορά στην πολιτική απορρήτου της εφαρμογής σχετικά με τι δεδομένα συλλέγονται από αυτές τις άδειες και με ποιον τρόπο χρησιμοποιούνται.

3. Facebook

Συγκρίνοντας την πολιτική απορρήτου του Facebook με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Ο κατάλογος επαφών το ιστορικό κλήσεων και το ιστορικό SMS που συλλέγει το Facebook σε περίπτωση που ο χρήσης θέλει να τα ανεβάσει, υπάρχουν στη λίστα δικαιωμάτων της εφαρμογής ως read call log, read contacts και read sms

- Πληροφορίες που συλλέγονται όπως το λειτουργικό σύστημα, το επίπεδο μπαταρίας, η ισχύς του σήματος και ο διαθέσιμος χώρος αποθήκευσης, αναγράφονται στις άδειες πρόσβασης ως modify system settings και read battery statistics
- Πληροφορίες σχετικά με σήματα Bluetooth και κοντινά σημεία πρόσβασης σε δίκτυα Wi-Fi και πύργους κινητής τηλεφωνίας επίσης αναφέρονται στην λίστα των απαιτούμενων δικαιωμάτων ως view wi-fi connections, view network connections, access Bluetooth setting και pair with Bluetooth devices
- Πληροφορίες που επιτρέπει ο χρήστης να λαμβάνει το Facebook όπως η δυνατότητα πρόσβασης στην τοποθεσία, στην κάμερα και στις φωτογραφίες, υπάρχουν ως κατοχυρωμένα δικαιώματα ως read-write storage, access camera, access coarse-fine location
- Πληροφορίες δικτύου και συνδέσεις όπως το όνομα του παρόχου κινητής τηλεφωνίας, ο αριθμός του κινητού τηλεφώνου, η διεύθυνση IP και η ταχύτητα σύνδεσης, συσχετίζονται στην λίστα των αδειών με την άδεια read phone status and identity
- Ωστόσο επικίνδυνες άδειες που αναγράφονται στην λίστα των δικαιωμάτων της εφαρμογής όπως read calendar και record audio δεν αναφέρονται στην πολιτική ιδιωτικότητας.

4.Twitter

Συγκρίνοντας την πολιτική απορρήτου του Twitter με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Πληροφορίες που παίρνονται μέσω της δημιουργίας λογαριασμού του χρήστη όπως το όνομα χρήστη, ο κωδικός και η διεύθυνση ηλεκτρονικού ταχυδρομείου, δικαιολογούνται με την χρήση της άδειας add or remove accounts
- Πληροφορίες τοποθεσίας που συλλέγονται από το Twitter, συσχετίζονται με την άδεια access fine-coarse location που είναι ορατή στις άδειες πρόσβασης
- Πληροφορίες πιστωτικής ή χρεωστικής κάρτας και διευθύνσεις που επισκέπτεται ο χρήστης από προωθητικά email που στέλνει η εταιρία ή από τα «Tweets» που εμφανίζονται σε άλλες ιστοσελίδες ή κινητές εφαρμογές συλλέγονται από το twitter. Τα παραπάνω δεδομένα δικαιολογούνται με την άδεια receive data from internet που υπάρχει μέσα στην λίστα της δημοφιλούς εφαρμογής.
- Αν και το κινητό τηλέφωνο αναφέρεται ως δεδομένο που προαιρετικά εισάγει ο χρήστης στην εφαρμογή και μάλιστα με γραπτό τρόπο, στην λίστα αδειών εντοπίστηκε η άδεια read phone status and identity που υλοποιεί την παραπάνω εργασία με αυτοματοποιημένο τρόπο. Όποτε το κινητό τηλέφωνο και πληροφορίες IMEI παρέχονται στην εταιρία παρά την θέληση του χρήστη
- Δεν αναφέρεται σε κανένα σημείο στην πολιτική ιδιωτικότητας τα δεδομένα που συλλέγονται αναφορικά με την εγγραφή ήχου, την πρόσβαση στην κάμερα, τον αποθηκευτικό χώρο και τις επαφές του χρήστη, παρότι αναγράφονται ως άδειες (read contacts, read-write storage, record audio, access camera)

5.Viber

Συγκρίνοντας την πολιτική απορρήτου του Viber με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Πληροφορίες λογαριασμού όπως όνομα διεύθυνση ηλεκτρονικού ταχυδρομείου μέσω της χρήσης των αδειών add or remove accounts και create accounts and set passwords, οι οποίες αναγράφονται στο αρχείο κειμένου που παρέχεται με τις άδειες.
- Πληροφορίες επαφών και κινητού τηλεφώνου σε περίπτωση που τις εγκρίνει ο χρήστης μέσω των αδειών read contacts και read phone status and identity, οι οποίες επίσης αναγράφονται
- Πληροφορίες από κοινωνικά δίκτυα σε περίπτωση που ο χρήστης συνδεθεί με τον λογαριασμό Viber σε κοινωνικά δίκτυα τρίτων οντοτήτων όπως Facebook και Twitter, ονομάζονται ως άδεια read data from internet.
- Πληροφορίες κινητής συσκευής, όπως το λειτουργικό σύστημα, το ασύρματο δίκτυο, τον πάροχο κινητής τηλεφωνίας και την τοποθεσία του χρήστη σε περίπτωση που ο ίδιος την επιτρέψει. Όλες αυτές οι πληροφορίες χαρακτηρίζονται από τις άδειες modify system settings, view wi-fi connections και view network connections, access fine-coarse location, οι οποίες είναι ορατές στο αρχείο καταγραφής των αδειών
- Πληροφορίες που λαμβάνονται μέσω ηχητικών μηνυμάτων ή κλήσεων, μέσω της άδειας record audio, δεν χρησιμοποιούνται από αυτούς που διαχειρίζονται αυτά τα δεδομένα στην εταιρία.
- Ωστόσο και σε αυτήν την εφαρμογή υπάρχει η δυνατότητα χρήσης της πρόσβασης στην κάμερα και τον αποθηκευτικό χώρο σε περίπτωση που εγκριθούν από τον χρήστη. Δεν αναφέρεται στην πολιτική ιδιωτικότητας τι στοιχεία συλλέγουν από αυτές τις άδειες και φυσικά ούτε τον τρόπο που τα διαχειρίζονται

6.WhatsApp

Συγκρίνοντας την πολιτική απορρήτου του WhatsApp με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Πληροφορίες λογαριασμού που συλλέγονται, συσχετίζονται με την άδεια find, add or remove accounts από το αρχείο καταγραφής των αδειών
- Πληροφορίες όπως το κινητό τηλέφωνο, το δίκτυο κινητής τηλεφωνίας και η διεύθυνση IP, συσχετίζονται με την άδεια read phone status and identity, η οποία αναγράφεται στις άδειες πρόσβασης της εφαρμογής
- Πληροφορίες συσκευής όπως το λειτουργικό σύστημα και το ποσοστό μπαταρίας, αντιστοιχίζονται με την άδεια Modify system setting
- Η τοποθεσία του χρήστη σε περίπτωση που δώσει ο ίδιος την έγκριση, καθορίζεται κάνοντας χρήση του GPS, του Bluetooth ή κοντινών συνδέσεων ασύρματου δικτύου (Wi-Fi). Όλα τα παραπάνω εντάσσονται ως δικαιώματα στην εφαρμογή (view Wi-Fi connections, access fine-coarse location, pair with Bluetooth devices)
- Ηχητικά μηνύματα, φωτογραφίες, βίντεο και αρχεία τα οποία σύμφωνα με την πολιτική απορρήτου διαγράφονται απευθείας από τους servers της εταιρίας, αντιστοιχίζονται με τις ανάλογες άδειες που αναφέρονται στο αρχείο καταγραφής δικαιωμάτων (record audio, read contents of storage, access camera, read storage).

- Δεν γίνεται αναφορά στην πολιτική ιδιωτικότητας για τις πληροφορίες που συλλέγει από την επικίνδυνη άδεια receive and send sms που χρησιμοποιεί η εφαρμογή σε περίπτωση που την εγκρίνει ο χρήστης

7.E-Radio

Συγκρίνοντας την πολιτική απορρήτου του E-Radio με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Πληροφορίες που συλλέγονται από κοινωνικά δίκτυα σε περίπτωση που ο χρήστης συνδεθεί με κάποιο λογαριασμό κοινωνικού δικτύου στην εφαρμογή. Αυτές οι πληροφορίες παίρνονται κάνοντας χρήση του δικαιώματος receive data from internet, το οποίο αναφέρεται στο αρχείο κειμένου που περιέχει τις άδειες.
- Πληροφορίες σχετικά με την τοποθεσία του χρήστη, αντιστοιχίζονται με τα δικαιώματα access coarse and fine location
- Η εφαρμογή κάνει χρήση της άδειας read phone state, η οποία είναι υπεύθυνη για την εύρεση του IMEI και του κινητού τηλεφώνου της συσκευής. Ωστόσο στην πολιτική ιδιωτικότητας δεν αναφέρεται σε κάποιο σημείο ότι συλλέγονται τα παραπάνω δεδομένα.
- Αν και συλλέγονται πληροφορίες λογαριασμού του χρήστη σε περίπτωση που ο ίδιος θελήσει να δημιουργήσει, δεν υπάρχει ανάλογο δικαίωμα που να δημιουργεί ή να διαχειρίζεται το λογαριασμό.
- Αναφορικά με πληροφορίες όπως το λειτουργικό σύστημα της συσκευής, επίσης δεν αναφέρεται ανάλογο δικαίωμα που να μπορεί να παρέχει αυτήν την πληροφορία στην εταιρία.
- Αν και αναφέρεται το δικαίωμα πρόσβασης στον αποθηκευτικό χώρο, δεν βρέθηκε κάποια αναφορά σε αυτό στην πολιτική ιδιωτικότητας που αναλύθηκε

8.TuneIn Radio

Συγκρίνοντας την πολιτική απορρήτου του TuneIn Radio με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Πληροφορίες όπως ο περιηγητής αναζήτησης ή πληροφορίες που σχετίζονται με το widget της εφαρμογής που εμπεριέχεται σε άλλες ιστοσελίδες συλλέγονται από την εταιρία. Αυτές οι πληροφορίες αντιστοιχίζονται στην άδεια receive data from internet, η οποία εμπεριέχεται στην εφαρμογή
- Πληροφορίες της τοποθεσίας του χρήστη χρησιμοποιώντας είτε το GPS είτε την διεύθυνση IP. Η συσχέτιση αυτών των πληροφοριών με τις άδειες πρόσβασης γίνεται μέσω των αδειών access fine and coarse location.
- Πληροφορίες συσκευής όπως το λειτουργικό σύστημα και τα μοναδικά αναγνωριστικά των συσκευών, αντιπροσωπεύονται από τις άδειες modify system settings και read phone status and identity αντίστοιχα. Ωστόσο, καμία από τις δύο άδειες δεν αναφέρεται σαν δικαίωμα, ενώ η δεύτερη αποτελεί και επικίνδυνη άδεια.
- Αν και αναγράφεται στην πολιτική απορρήτου ότι συλλέγονται οι επαφές της συσκευής με την συγκατάθεση του χρήστη, δεν γίνεται κάποια τέτοια αναφορά στο αρχείο αδειών

- Φυσικά υπάρχει και έλλειψη ενημέρωσης στην πολιτική ιδιωτικότητας αναφορικά με τα δεδομένα που συλλέγονται από την άδεια read and write on storage, την οποία χρησιμοποιεί η εφαρμογή

9.Netflix

Συγκρίνοντας την πολιτική απορρήτου του Netflix με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Πληροφορίες της τοποθεσίας του χρήστη, χρησιμοποιώντας μόνο την διεύθυνση IP του χρήστη. Για αυτές τις πληροφορίες χρειάζεται μόνο το δικαίωμα full network access (το οποίο περιλαμβάνεται), και όχι η χρήση του δικαιώματος access fine location, το οποίο δεν περιλαμβάνεται
- Πληροφορίες από τις αλληλεπιδράσεις των χρηστών με τα email, συσχετίζονται με το δικαίωμα find accounts on the device
- Τα αναγνωριστικά των συσκευών τα οποία δεν αναφέρονται εκτενώς στην πολιτική απορρήτου, αντιστοιχίζονται στην άδεια read phone status and identity. Πρόκειται για μια σημαντική και επικίνδυνη άδεια και η χρήση των αναγνωριστικών αυτών από την εταιρία θα έπρεπε να αναφέρεται αναλυτικά.
- Άλλα σημαντικά δικαιώματα που αναφέρονται στο αρχείο κειμένου των αδειών, όπως τα access phone storage και record audio, θα έπρεπε να δικαιολογούνται από την πολιτική ιδιωτικότητας, πράγμα που δεν γίνεται.

10.Kodi

Συγκρίνοντας την πολιτική απορρήτου του Kodi με τα δικαιώματα που απαιτεί διαπιστώθηκαν τα εξής:

- Δεν γίνεται κάποια αναφορά στην πολιτική ιδιωτικότητας, αναφορικά με τον τύπο των πληροφορίων που συλλέγονται στην εφαρμογή. Ωστόσο, μελετώντας ο αρχείο κειμένου καταγραφής των δικαιωμάτων της εφαρμογής παρατηρήθηκαν δικαιώματα όπως αυτό της πρόσβασης στον αποθηκευτικό χώρο ή της πλήρης πρόσβασης στο δίκτυο για τα οποία δεν παρουσιάζεται καμιά πληροφορία στην πολιτική. Φυσικά υπάρχουν και άλλα δικαιώματα που εμπεριέχει η εφαρμογή, αλλά δεν είναι τόσο σημαντικά ώστε να αναφερθούν.

Συμπερασματικά, είναι εμφανές όλες οι εφαρμογές έχουν έλλειψη είτε στον τομέα της πολιτικής ιδιωτικότητας βάσει των όσων αναγράφονται στα δικαιώματα της κάθε εφαρμογής, είτε το αντίστροφο. Φυσικά, σε κάθε εφαρμογή υπάρχουν και άλλα δικαιώματα, αλλά για την παρούσα έρευνα επικεντρωθήκαμε μόνο στα σημαντικά και επικίνδυνα για την ασφάλεια των χρηστών. Είναι ορατό ότι στις περισσότερες εφαρμογές που μελετήθηκαν δεν υπάρχουν αναφορές στην πολιτική ιδιωτικότητας σχετικά με τα δικαιώματα πρόσβασης στον αποθηκευτικό χώρο, κάμερας και εγγραφής ήχου που έχουν οι αντίστοιχες εφαρμογές, ενώ σε κάποιες παρατηρήθηκαν και ελλείψεις αναφοράς των δικαιωμάτων πρόσβασης στις επαφές και στα μοναδικά αναγνωριστικά (όπως αριθμός κινητού τηλεφώνου και IMEi). Όπως προαναφέραμε καμία εφαρμογή δεν παρουσιάζει πλήρης πολιτική ιδιωτικότητας αναφορικά με τα δεδομένα που συλλέγει. Ωστόσο, οι εφαρμογές που έχουν τα λιγότερα κενά, αποδείχτηκαν οι WhatsApp, Viber και Facebook. Παρότι και οι τρεις εφαρμογές συλλέγουν μεγάλο πλήθος δεδομένων η

πολιτική ιδιωτικότητας τους σχεδόν καλύπτει την αναφορά στις επικίνδυνες άδειες και για αυτό το λόγο θεωρούνται πιο ολοκληρωμένες. Αντίθετα οι εφαρμογές Twitter, Uc browser και Kodi παρουσιάζουν τις πιο ελλιπείς πολιτικές ιδιωτικότητας στον τομέα συλλογής των δεδομένων. Οι δύο πρώτες δεν αναγράφουν τον τρόπο που συλλέγουν ορισμένες πληροφορίες από σημαντικά δικαιώματα που χρησιμοποιούν, ενώ η τρίτη δεν αναφέρει καθόλου τι δεδομένα συλλέγει παρά μόνο τον τρόπο με τον οποίο τα συλλέγει (αυτοματοποιημένα, μέσω cookies, παροχή από τους χρήστες). Τέλος είναι αναγκαίο να αναφερθεί ότι οι πληροφορίες σχετικά με τα δικαιώματα κάθε εφαρμογής πάρθηκαν από την επίσημη ιστοσελίδα εφαρμογών της google (Google play).

4.4. Σύγκριση πολιτικών ιδιωτικότητας

1.UC Browser και Google chrome

Συγκρίνοντας τις δύο πολιτικές ιδιωτικότητας μπορούν να εξαχθούν τα εξής συμπεράσματα:

Αναφορικά **με τα δεδομένα που συλλέγουν**

- Πολλά από τα δεδομένα που συλλέγει ο google chrome αποθηκεύονται στην συσκευή του χρήστη και όχι στους servers της εταιρείας, όπως συμβαίνει στον UC Browser. Για να αποσταλούν τα συγκεκριμένα δεδομένα στην εταιρία πρέπει ο χρήστης να συνδεθεί με τον λογαριασμό Google που έχει και να ενεργοποιήσει τον συγχρονισμό.
- Ο UC Browser συλλέγει περισσότερα και πιο επικίνδυνα δεδομένα από τον Chrome
- Ευαίσθητα προσωπικά όπως προσωπικά στοιχεία μιας φόρμας αγοράς ή δεδομένα πιστωτικής κάρτας στέλνονται κρυπτογραφημένα στην Google, ενώ στον UC δεν αναφέρεται κάποιο σύστημα ασφαλείας. Βέβαια στην περίπτωση του UC δεν αναφέρεται ότι συλλέγονται τέτοιου είδους δεδομένα.

Αναφορικά με τον τρόπο χρήσης και διαμοίρασης των δεδομένων

- Και οι δύο εφαρμογές αναφέρουν πως χρησιμοποιούν τα δεδομένα για προσωπική χρήση και βελτίωση των υπηρεσιών που προσφέρουν στο χρήστη
- Και οι δύο εφαρμογές διαμοιράζουν τα δεδομένα σε τρίτες οντότητες. Στην περίπτωση του Chrome τα δεδομένα μπορεί να διαμοιραστούν σε συνεργάτες, διαφημιστές ή προγραμματιστές, ενώ στην περίπτωση του uc σε διάφορες διαφημιστικές πλατφόρμες που συνεργάζεται η εταιρία ή εκδότες.
- Ο UC αναφέρει πως διαμοιράζει τις πληροφορίες σε περίπτωση που ζητηθούν από τις δικαστικές αρχές ή σε περίπτωση αλλαγής της ιδιοκτησίας. Κάτι ανάλογο δεν αναφέρεται στην εφαρμογή της Google.

Συμπερασματικά, ο Google chrome συλλέγει μικρότερο πλήθος δεδομένων από το UC Browser, ενώ τα διαχειρίζεται και με καλύτερο τρόπο προσφέροντας κάποιο σύστημα κρυπτογράφησης σε ορισμένα από αυτά. Παράλληλα, ο Chrome, συλλέγει λιγότερο επικίνδυνα δεδομένα του χρήστη κάνοντας τον χρήστη να νιώθει περισσότερο ασφαλή στην χρήση του περιηγητή. Αναφορικά με τα τον τρόπο διαμοίρασης των αρχείων και οι δύο εφαρμογές κοινοποιούν τα δεδομένα σε τρίτες οντότητες, ενώ ο Uc browser αναφέρει και τον τρόπο διαχείρισης των δεδομένων σε περίπτωση αλλαγής της ιδιοκτησίας ή απαίτησης χρήσης

αυτών από τις δικαστικές αρχές, γεγονός που κάνει την πολιτική ιδιωτικότητας της εφαρμογής πιο ολοκληρωμένη σε αυτόν τον τομέα. Ωστόσο βλέποντας συνολικά τις δύο εφαρμογές θα λέγαμε πως ο Google Chrome είναι πιο ασφαλής εφαρμογή βάσει των όσων αναφέρονται στην πολιτική ιδιωτικότητας του.

2.Facebook και Twitter

Συγκρίνοντας τις δύο πολιτικές ιδιωτικότητας μπορούν να εξαχθούν τα εξής συμπεράσματα:

Αναφορικά με τα δεδομένα που συλλέγουν

- Και οι δύο εφαρμογές συλλέγουν πληροφορίες που διαμοιράζεται ο χρήστης με αυτές. Ωστόσο το Facebook συλλέγει ορισμένες επικίνδυνες για την ασφάλεια του χρήστη πληροφορίες που δεν συλλέγει το Twitter, όπως πληροφορίες σχετικά με την κάμερα για παροχή προτάσεων φίλτρων, τις επαφές, το ιστορικό των κλήσεων και των SMS του χρήστη.
- Το Facebook αναφέρει πως συλλέγει και αρκετές πληροφορίες συσκευής όπως το λειτουργικό σύστημα, μοναδικά αναγνωριστικά, σήματα Bluetooth και κοντινά σημεία πρόσβασης Wi-fi κ.α. Παρόμοιες αναφορές δεν υπάρχουν στην πολιτική ιδιωτικότητας του Twitter.
- Και οι δύο εφαρμογές παίρνουν πληροφορίες αναφορικά με τον χρήστη από τρίτες οντότητες όπως συνεργάτες και διαφημιστές.

Αναφορικά με τον τρόπο χρήσης και διαμοίρασης των δεδομένων

- Το Facebook αναφέρει με ποιον τρόπο διαχειρίζεται τα δεδομένα του χρήστη ενδοεταιρικά, ενώ το Twitter όχι.
- Και οι δύο εφαρμογές κοινοποιούν τα δεδομένα σε τρίτους συνεργάτες. Το Facebook τους ονομάζει, ενώ αντίθετα το Twitter προτιμά να μην τους αναφέρει αναλυτικά.

Συμπερασματικά, και οι δύο εφαρμογές συλλέγουν μεγάλο πλήθος δεδομένων με το Facebook, ωστόσο να συλλέγει περισσότερες και πιο επικίνδυνες. Βέβαια όπως είδαμε στην προηγούμενη ενότητα (Ενότητα 5.3) το Twitter δεν αναφέρει στην πολιτική ιδιωτικότητας αρκετά δεδομένα που συλλέγει βάσει των δικαιωμάτων που απαιτεί από τον χρήστη, οπότε δεν μπορεί να θεωρηθεί πιο έμπιστη στον τομέα αυτό. Αντιθέτως, το facebook, αν και συλλέγει μεγάλο πλήθος δεδομένων, ενημερώνει τον χρήστη για την πλειοψηφία αυτών, ώστε ο χρήστης να έχει μια σχεδόν ολοκληρωμένη άποψη για αυτό. Στον τομέα της χρήσης των δεδομένων επίσης το Twitter δεν αναφέρει το οτιδήποτε, ενώ στο τομέα της διαμοίρασης πάλι το Facebook είναι πιο συγκεκριμένο. Έτσι, το Facebook θεωρούμε πως έχει πιο πλήρη πολιτική ιδιωτικότητας και είναι πιο ειλικρινές προς τους πελάτες της.

3.Viber και WhatsApp

Συγκρίνοντας τις δύο πολιτικές ιδιωτικότητας μπορούν να εξαχθούν τα εξής συμπεράσματα:

Αναφορικά με τα δεδομένα που συλλέγουν

- Και οι δύο εφαρμογές συλλέγουν παρόμοιες πληροφορίες αναφορικά με τις πληροφορίες που παρέχει ο χρήστης και αυτές που συλλέγονται με αυτοματοποιημένο τρόπο από τις δύο εταιρίες. Η διαφορά φαίνεται στον τρόπο

που παρουσιάζονται οι πληροφορίες, όπου στο whatsapp είναι χωρισμένες σε αυτές που δίνει ο χρήστης και αυτές που παίρνονται αυτοματοποιημένα, ενώ στο viber υπάρχει ένα ενιαίο κείμενο και για τις δύο κατηγορίες.

- Το WhatsApp αναφέρει πληροφορίες που συλλέγονται από τρίτες οντότητες όπως από άλλους χρήστες της εφαρμογής, από επιχειρήσεις με τις οποίες ο χρήστης συνδέεται χρησιμοποιώντας την εφαρμογή, από συνεργάτες όπως το Facebook. Αντίθετα το Viber δεν αναφέρει τέτοιου είδους πληροφορίες.

Αναφορικά με τον τρόπο χρήσης και διαμοίρασης των δεδομένων

- Και οι δύο εφαρμογές αναφέρουν αναλυτικά με ποιους τρόπους χρησιμοποιούν τα δεδομένα που συλλέγουν από τους χρήστες

Συμπερασματικά και οι δύο εφαρμογές έχουν ορισμένες ελλείψεις στο τομέα της συλλογής πληροφοριών βάσει των όσων ειπώθηκαν στην προηγούμενη ενότητα (ενότητα 5.3) για αυτές, αλλά δεν παρουσιάζουν μεγάλες διαφορές, ενώ αναφορικά με τον τρόπο χρήσης των δεδομένων είναι και οι δύο εξίσου επεξηγηματικές.

4.E-Radio και TuneIn Radio

Συγκρίνοντας τις δύο πολιτικές ιδιωτικότητας μπορούν να εξαχθούν τα εξής συμπεράσματα:

Αναφορικά με τα δεδομένα που συλλέγουν

- Και οι δύο εφαρμογές συλλέγουν πληροφορίες που δίνει ο χρήστης χωρίς να είναι ιδιαίτερα επεξηγηματικές σε κάποιες από αυτές.
- Το TuneIn Radio συλλέγει πιο επικίνδυνες πληροφορίες από ότι το E-radio, όπως μοναδικά αναγνωριστικά (όπως IMEI) και ο κατάλογος επαφών.
- Το TuneIn Radio συλλέγει πληροφορίες και από τρίτες οντότητες όπως πληροφορίες από άλλους χρήστες ή διαφημιστές ή πληροφορίες από κοινωνικά δίκτυα σε περίπτωση που εισάγει κάποιον τέτοιο λογαριασμό μέσα στην εφαρμογή, ενώ το E-Radio δεν συλλέγει τέτοιες πληροφορίες.

Αναφορικά με τον τρόπο χρήσης των δεδομένων

- Και οι δύο εφαρμογές είναι σαφείς με ποιον τρόπο διαχειρίζονται τα δεδομένα των χρηστών.

Συμπερασματικά, το TuneIn Radio είναι πιο επικίνδυνη εφαρμογή για το χρήστη, διότι συλλέγει πιο επικίνδυνα δεδομένα. Ωστόσο το E-radio περιέχει μόνο ελληνικούς ραδιοφωνικούς σταθμούς και απευθύνεται μόνο σε χρήστες της χώρας μας.

5.Netflix και Kodi

Συγκρίνοντας τις δύο πολιτικές ιδιωτικότητας μπορούν να εξαχθούν τα εξής συμπεράσματα:

Αναφορικά με τα δεδομένα που συλλέγουν

- Το Netflix χωρίζει σε κατηγορίες τις πληροφορίες που συλλέγει και πιο συγκεκριμένα σε πληροφορίες που παρέχει ο χρήστης, πληροφορίες που συλλέγονται με

αυτοματοποιημένο τρόπο, πληροφορίες που συλλέγονται από συνεργάτες και πληροφορίες από άλλες πηγές, ενώ παράλληλα τις αναλύει κιόλας. Αντίθετα, το Kodi δεν αναφέρει καν τον τύπο των πληροφοριών που συλλέγει, γεγονός που από μόνο του κάνει τους χρήστες που διαβάζουν την πολιτική απορρήτου επιφυλακτικούς για την ασφάλεια των δεδομένων τους.

Αναφορικά με τον τρόπο γνωστοποίησης των δεδομένων

- Και οι δύο εφαρμογές να αναφέρουν σε ποιες οντότητες γνωστοποιούν τα δεδομένα του χρήστη. Εντύπωση προκαλεί το γεγονός ότι το Kodi γνωστοποιεί πληροφορίες σε περίπτωση που ζητηθούν από άλλους και δοθεί η άδεια από τον ίδιο τον χρήστη να διαμοιραστούν, δείχνοντας τον σεβασμό προς τον χρήστη. Επίσης η ίδια εφαρμογή δημοσιεύει μη προσωπικές πληροφορίες για εκπαιδευτικούς σκοπούς για βελτίωση του λογισμικού και προώθηση του ανοικτού κώδικα, γεγονός επίσης σπάνιο αναφοράς σε πολιτική ιδιωτικότητας.

Συμπερασματικά, η πολιτική ιδιωτικότητας του Netflix είναι πιο ολοκληρωμένη και πιο αναλυτική αναφορικά με τα δεδομένα που συλλέγονται. Εξάλλου, πρόκειται για μια εφαρμογή που παρέχει τις υπηρεσίες της επί πληρωμή, ενώ το Kodi είναι δωρεάν που σε επίπεδο παροχής ταινιών και σειρών θεωρείται πειρατεία. Έτσι το Netflix θεωρείται καλύτερη εφαρμογή τόσο για λόγους ασφάλειας των πληροφοριών όσο και για ηθικούς λόγους.

5. Συμπεράσματα

Η μεθοδολογία της παρούσας έρευνας χωρίστηκε σε δύο ενότητες. Η πρώτη ενότητα σχετίζονταν με την μελέτη των αδειών πρόσβασης δεκάδων εφαρμογών στο Aptoide, μέσω μια προγραμματιστικής εφαρμογής που υλοποιήθηκε, ενώ η δεύτερη αφορούσε την μελέτη δέκα πολιτικών ιδιωτικότητας διάσημων εφαρμογών του play store και την σύγκριση τους με τις άδειες που αυτές η κάθε μία από αυτές απαιτούσε. Αναλύοντας τις δύο παραπάνω ενότητες με τους τρόπους που αναφέρθηκαν παραπάνω καταλήξαμε στα εξής συμπεράσματα:

- Το Aptoide, βάσει του μέσου όρου και της επικινδυνότητας των δικαιωμάτων που απαιτούν, δεν θεωρείται έμπιστη ιστοσελίδα λήψης εφαρμογών σε σχέση με την επίσημη ιστοσελίδα εφαρμογών που προσφέρει η Google, παρότι το γεγονός ότι ο χρήστης μπορεί να κατεβάσει οποιαδήποτε εφαρμογή δωρεάν σε αντίθεση με τον ανταγωνιστή.
- Οι πολιτικές ιδιωτικότητας των εφαρμογών που μελετήθηκαν δεν παρουσιάστηκαν πλήρης, ως προς τον συλλογής των πληροφοριών σε σύγκριση με τις άδειες που απαιτούν, αφού σε όλες απουσίαζε τουλάχιστον μια αναφορά στην πολιτική απορρήτου για τον τρόπο που χρησιμοποιεί μια επικίνδυνη άδεια. Προφανώς υπήρχαν και άλλες ελλείψεις, αλλά αυτές αφορούσαν μη σημαντικές-επικίνδυνες άδειες και δεν δόθηκε η απαραίτητη σημασία.

Επιπλέον βάσει των όσων αναφέρθηκαν στην υποενότητα 2.2.1, ευθύνη για τον διαμοιρασμό των πληροφοριών του χρήστη δεν έχουν μόνο οι εφαρμογές αλλά και το λειτουργικό σύστημα του Android, και ο τρόπος με τον οποίο έχει υλοποιηθεί το σύστημα διαχείρισης δικαιωμάτων.

Ακόμα, θεωρούμε πως οι στόχοι που είχαμε θέσει στην αρχή της εργασίας υλοποιήθηκαν, διότι και το δείγμα των εφαρμογών που μελετήθηκαν ήταν επαρκές και οι πολιτικές ιδιωτικότητας και οι άδειες μελετήθηκαν λεπτομερώς ως προς τον τομέα της συλλογής πληροφοριών και της επικινδυνότητας αντίστοιχα.

Η συμβολή της εργασίας στην υπάρχουσα βιβλιογραφία είναι δεδομένη, αφού προσφέρει νέες πληροφορίες από ένα περιβάλλον που δεν έχει διερευνηθεί έως σήμερα, το aptoide και αναλύει τις πολιτικές ιδιωτικότητας κορυφαίων εφαρμογών που σχεδόν κάθε χρήστης χρησιμοποιεί κάποιες ή και όλες στο κινητό του τηλέφωνο. Έτσι οι μελλοντικοί ερευνητές της εργασίας θα έχουν στην διάθεση τους ένα ακόμα βοηθητικό εργαλείο που μπορεί να τους βοηθήσει σε κάποια μελλοντική τους έρευνα, ενώ οι αναγνώστες με την σειρά τους θα δουν από μια νέα οπτική γωνία τον τρόπο με τον οποίο συλλέγονται τα δεδομένα τους.

6. Μελλοντικές προσθήκες και έρευνες

Γενικότερα η παρούσα έρευνα καλύπτει τις απαραίτητες πληροφορίες που πρέπει να έχει ο χρήστης στην διάθεση του για να εξάγει τα απαραίτητα συμπεράσματα τόσο για την ιστοσελίδα του aptoide, όσο και για τις πολιτικές ιδιωτικότητας, όχι μόνο των δέκα εφαρμογών που μελετήθηκαν, αλλά ενός μεγάλους πλήθους αυτών, εφόσον καμία δεν τηρούσε όσα έπρεπε βάσει των δικαιωμάτων που απαιτούσε. Επίσης παρακολουθώντας τα όσα γράφτηκαν στην παρούσα έρευνα σχετικά με τις πολιτικές ιδιωτικότητας, ο χρήστης, θα είναι σε θέση να κατανοεί της πολιτικές απορρήτου των εφαρμογών και να αντιστοιχεί τα όσα αναγράφονται με τις άδειες που η εφαρμογή ζητάει. Ωστόσο, στην συγκεκριμένη έρευνα θα μπορούσαν να προστεθούν ορισμένα τμήματα, τόσο στον τομέα της προγραμματιστικής εφαρμογής όσο και σε αυτόν των πολιτικών ιδιωτικότητας. Στον τομέα της προγραμματιστικής εφαρμογής θα μπορούσαν να εξαχθούν επιπλέον συμπεράσματα από την βάση δεδομένων που υλοποιήθηκε, όπως εφαρμογές που έχουν τις περισσότερες επικίνδυνες άδειες ή κατηγορίες με τις πιο επικίνδυνες άδειες για την πιο αποδοτική εξαγωγή αποτελεσμάτων και την παροχή επιπλέον πληροφοριών στους χρήστες σχετικά με το aptoide. Στον τομέα των πολιτικών ιδιωτικότητας μπορεί να προστεθεί κάποιου είδους πρωτογενής έρευνα με την χρήση ερωτηματολογίου, μέσω του οποίου θα εξαχθούν συμπεράσματα για τον βαθμό στον οποίο οι χρήστες διαβάζουν τις πολιτικές ιδιωτικότητας των εφαρμογών, αλλά και τον βαθμό στον οποίο τις κατανοούν.

Παράλληλα μελλοντικοί ερευνητές μπορούν να λάβουν κίνητρα από την συγκεκριμένη διπλωματική και να δημιουργήσουν ανάλογες εργασίες σε άλλες ανεπίσημες ιστοσελίδες παροχής εφαρμογών στο Android ή να αναλύσουν ακόμα περισσότερες πολιτικές ιδιωτικότητας, ώστε να είμαστε σε θέση να εξάγουμε πληρέστερα συμπεράσματα. Επίσης, οι μελλοντικοί ερευνητές μπορούν να υλοποιήσουν σε πιο ολοκληρωμένο βαθμό σε μια ιστοσελίδα ανοικτού κώδικα, την μέθοδο εξόρυξης κειμένου από τον πηγαίο, που αναλύσαμε σε προηγούμενο κεφάλαιο (Κεφάλαιο 3, Υποενότητα 3.2.6), για να διαπιστώσουν τον σκοπό για τον οποίο χρησιμοποιούνται τα δικαιώματα στις εφαρμογές, εφόσον όπως αποδείχτηκε η συγκεκριμένη μέθοδος έχει μεγάλα ποσοστά επιτυχημένης αντιστοίχησης του κειμένου με τα δικαιώματα.

7. Βιβλιογραφία

1. Carlos Jensen, Colin Potts, Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices, Vienne Austria 2004 σελ. 1 βλέπε https://dl.acm.org/citation.cfm?id=985752
2. ANTHONY D. MIYAZAKI AND SANDEEP KRISHNAMURTHY, Internet Seals of Approval: Effects on Online PrivacyPolicies and Consumer Perceptions, The Journal of Consumer Affairs, Vol. 36, No. 1, 2002 σελ. 1 βλέπε https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-6606.2002.tb00419.x
3. Rawan Baalous, Ronald Poet, How Dangerous Permissions are Described in Android Apps' Privacy Policies?, 2018, βλέπε https://dl.acm.org/citation.cfm?id=3264477
4. Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας, Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών- Τεχνικά και Νομικά Θέματα, 2010 σελ. 95-96, 522-528
5. Γεώργιος Λιουδάκης, Κακλαμάνη Δήμητρα-Θεοδώρα, Προστασία Προσωπικών Δεδομένων Σε Έξυπνα Περιβάλλοντα, 2009, σελ. 29-31 βλέπε http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/8692
6. Κώστας Μαυραγάνης, Σε ισχύ ο νέος ευρωπαϊκός νόμος προστασίας δεδομένων, GDPR: Όσα πρέπει να γνωρίζετε, βλέπε https://www.huffingtonpost.gr/entry/se-ische-o-neos-eeropaikos-nomos-prostasias-dedomenon-gdpr-osa-prepei-na-ynorizete_gr_5b06a9efe4b07c4ea10585d4
7. Lawspot.gr, GDPR: Ελλάδα και Σλοβενία οι δύο τελευταίες χώρες χωρίς νέο Νόμο για τα προσωπικά δεδομένα, βλέπε https://www.lawspot.gr/nomika-nea/gdpr-ellada-kai-slovenia-oi-dyo-teleytaies-hores-horis-neo-nomo-gia-ta-prosopika-dedomena
8. ΝΟΜΟΣ 2472/1997 ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF σελ. 2,4
9. Reflection in Java, βλέπε https://www.geeksforgeeks.org/reflection-in-java/
10. Intents and Intent Filters, βλέπε https://developer.android.com/guide/components/intents-filters
11. Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner, Android Permissions Demystified, 2011, σελ. 3 βλέπε https://dl.acm.org/citation.cfm?id=2046779
12. Remote procedure calls, τελευταία τροποποίηση Μάρτιος 2019, βλέπε https://www.androidcookbook.info/android-system/remote-procedure-calls.html
13. Zhongwen Zhang, Before Unrooting your Android Phone, Patching up Permission System First!, 2015, σελ. 53-54, βλέπε https://link.springer.com/chapter/10.1007%2F978-3-319-15087-1_4
14. William J.Buchanana, Simone Chiale, Richard Macfarlane, A methodology for the security evaluation within third-party Android Marketplaces, 2017, σελ. 1-3, βλέπε https://www.sciencedirect.com/science/article/pii/S1742287617300245 (14)
15. Wenliang Du, Android Repackaging Attack Lab, 2018, σελ. 1 βλέπε http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Mobile/Android_Repackaging/Android_Repackaging.pdf (15)

16. Sajal Rastogi, Kriti Bhushan, B. B. Gupta, Measuring Android App Repackaging Prevalence based on the Permissions of App, 2015, σελ. 2-3, βλέπε https://www.sciencedirect.com/science/article/pii/S2212017316302626
17. Zhongwen Zhang Yuewu Wang, Jiwu Jing, Qiongxiao Wang, Lingguang Lei, Once Root Always a Threat: Analyzing the Security Threats of Android Permission System, 2014. Σελ. 366-369, βλέπε https://link.springer.com/chapter/10.1007/978-3-319-08344-5_23
18. HAOYU WANG, YUANCHUN LI and YAO GUO, YUVRAJ AGARWAL and JASON I. HONG, Understanding the Purpose of Permission Use in Mobile Apps, 2017, Σελ. 1-5, βλέπε https://dl.acm.org/citation.cfm?id=3086677
19. Android Developers, Permissions overview, βλέπε https://developer.android.com/guide/topics/permissions/overview
20. Zheran Fangac, Weili Han, Yingjiu Li, Permission based Android security: Issues and countermeasures, 2014, σελ. 2, βλέπε https://reader.elsevier.com/reader/sd/pii/S0167404814000261?token=245EF41C58931B3D0E8C5EB5481A807D3CDC50340866465872A9976488DC40871CB376B5249A58BD69B2AB2E66DB15B3
21. Ματίνα Τσαβλή, Ιδιωτικότητα στα Smartphones: Μοντέλα Αδειών Πρόσβασης και Ταξινόμηση Προσωπικών Δεδομένων, 2016, σελ. 29-34, 47-56, βλέπε http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9619/Tsavli_Matina.pdf?sequence=1&isAllowed=y
22. Άκης Τίγκας, Τι Είναι τα Δικαιώματα Εφαρμογών στο Android και Τι να Προσέχουμε, 2017, βλέπε https://www.pcsteps.gr/166366-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%B1-%CE%B4%CE%B9%CE%BA%CE%B1%CE%B9%CF%8E%CE%BC%CE%B1%CF%84%CE%B1-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CF%8E%CE%BD-%CF%83%CF%84%CE%BF-android/
23. Πολιτική Ιδιωτικότητας του UC Broswer βλέπε https://m.ucweb.com/company/privacy/
24. Πολιτική Ιδιωτικότητας του Google Chrome βλέπε https://www.google.com/intl/en/chrome/privacy/
25. Πολιτική Ιδιωτικότητας του Facebook βλέπε https://www.facebook.com/about/privacy/
26. Πολιτική Ιδιωτικότητας του Twitter βλέπε https://twitter.com/en/privacy
27. Πολιτική Ιδιωτικότητας του Viber βλέπε https://www.viber.com/terms/viber-privacy-policy/
28. Πολιτική Ιδιωτικότητας του WhatsApp βλέπε https://www.whatsapp.com/legal/#privacy-policy-information-we-collect
29. Πολιτική Ιδιωτικότητας του E-Radio βλέπε http://www.e-radio.gr/privacy.asp
30. Πολιτική Ιδιωτικότητας του TuneIn Radio βλέπε http://tunein.com/policies/privacy/
31. Πολιτική Ιδιωτικότητας του Netflix βλέπε https://help.netflix.com/legal/privacy
32. Πολιτική Ιδιωτικότητας του Kodi βλέπε https://kodi.tv/kodi-privacy-policy
33. Επίσημη ιστοσελίδα του Aptoide βλέπε https://gr.aptoide.com/

Παράρτημα Α

```
import requests
import psycopg2
import urllib.request
from urllib.parse import urlparse
from bs4 import BeautifulSoup ##Εισαγωγή απαραίτητων βιβλιοθηκών

conn = psycopg2.connect("dbname=aptoide user=postgres password=boss") ##Σύνδεση με την βάση δεδομένων
#ADVENTURE GAMES
result = requests.get("https://gr.aptoide.com/group/games/sub/adventure") ##Αίτηση του html κώδικα της συγκεκριμένης ιστοσελίδας
src = result.content
soup = BeautifulSoup(src, 'lxml')
i=0 ##Αρχικοποίηση του i
for h2_tag in soup.find_all('div',class_='apps-list-container'):
       links = h2_tag.findAll('a') ##Εύρεση όλων των tag "a" μέσα στην κλαση "apps-list-container" του html κώδικα
for a in links:
       mystring2 = a['href']
##Το href αναφέρεται σε ιστοσελίδες που περιέχονται μέσα στο "a" tag. Στην συγκεκριμένη περίπτωση οι 50 κορυφαίες εφαρμογές της κατηγορίας adventure και εκχωρούνται στην μεταβλητή "mystring2"
       try:
              if urllib.request.urlopen(mystring2).read(): ##Έλεγχος αν ανοίγει η κάθε ιστοσελίδα που περιλαμβάνει το "mystring2"
                     mystring = mystring2 ##Εκχώρηση της "mystring2" στην "mystring"
              duthgr = urllib.request.urlopen(mystring).read() ##Άνοιγα της ιστοσελίδας που περιέχεται στην "mystring" και εκχώρηση στην μεταβλητή "duthgr"
              soup2 = BeautifulSoup(duthgr, 'html.parser')
              for h3_tag in soup2.find_all('h1'): ##Εύρεση των "h1" tag που περιλαμβάνει τα ονόματα των εφαρμογών
                     appname = h3_tag.text ##Παίρνουμε μόνο το κείμενο που περιλαμβάνεται μέσα στο "h1" tag
                     print(appname) ##Εκτύπωση του κειμένου δηλαδή του ονόματος της εφαρμογής
              duthgr = urllib.request.urlopen(mystring).read()
              soup = BeautifulSoup(duthgr, 'html.parser')
              newshtml = soup.find_all('table',class_='table',id='app-view-information-table')
##Εύρεση της κλάσσης "table" με id "app-view-information-table" που περιλαμβάνει τα δικαιώματα που απαιτεί η κάθε εφαρμογή
              div=newshtml[1] ##Επειδή υπήρχαν δύο κλάσεις με το ίδιο όνομα παίρνουμε μόνο αυτήν που χρειαζόμαστε
              inner_text = div.text
              strings = inner_text.split("  ") ##Παίρνουμε μόνο το κείμενο των δικαιωμάτων
              for line in strings: ##Βρόγχος ώστε να βρει όλα τα δικαιώματα
                     print(line) ##Εκτύπωση των δικαιωμάτων
                     i=i+1 ##Μέτρηση των δικαιωμάτων
              cur = conn.cursor() ##Σύνδεση με την βάση
              cur.execute("INSERT INTO adventure_games(url,permi,numofperm,name) VALUES (%s,%s,%s,%s)", (mystring,inner_text,format(i),appname)) ##Εισαγωγή στοιχείων στην βάση
              i=0
       except: ##Σε περίπτωση που δεν ανοίξει κάποια ιστοσελίδα να μην σταματήσει να τρέχει ο κώδικας αλλά να βγάλει ένα κενό
              print("")
conn.commit() ##Εμφάνιση στοιχείων μέσα στην βάση
```

Κομμάτι του κώδικα που εντάχθηκε στην εργασία μαζί με την εισαγωγή των απαραίτητων σχολίων

```
result = requests.get("https://gr.aptoide.com/group/games") ##Αίτηση του html κώδικα στην γενική κατηγορία "παιχνίδια"
src = result.content
soup = BeautifulSoup(src, 'lxml')
links=[]
for htag in soup.find_all('h2'): ##Εύρεση όλων των "h2" tag στον html κώδικα
       links= htag.findAll('a') ##Παίρνουμε μόνο αυτά που γράφονται εντός του "a" tag
       for a in links:
              mystring4= a['href']
##Παίρνουμε συγκεκριμένα μόνο τις ιστοσελίδες που περιέχονται μέσα στο "a" tag Που περιλαμβάνει όλες τις κατηγορίες που υπάρχουν στην κατηγορία "παιχνίδια" με την χρήση του "href"
              tolink=("https://gr.aptoide.com"+mystring4) ##Επειδή οι ιστοσελίδες δεν είχαν το "https://gr.aptoide.com" και δεν θα μπορούσαν να ανοικτούν προστέθηκε η προηγούμενη εντολή
              print(tolink) ##Εκτύπωση των ιστοσελίδων
```

Βελτιωμένη εκδοχή του κώδικα

Εντάσσοντας τον παραπάνω της βελτιωμένης εκδοχής του κώδικα στον αρχικό κώδικα θα μπορούσαμε να εξάγουμε το ίδιο αποτέλεσμα με πολύ λιγότερο αριθμό γραμμών κώδικα, γλυτώνοντας πολύτιμο χρόνο. Ωστόσο η βελτιωμένη εκδοχή του κώδικα δεν μπορούσε να υλοποιηθεί λόγω περιορισμών της βιβλιοθήκης BeautifulSoup και για αυτό υλοποιήθηκε η πρώτη εκδοχή. Περισσότερες πληροφορίες υπάρχουν στο Κεφάλαιο 3, υποενότητα 3.1.3.

Παράρτημα Β

Τα SQL ερωτήματα που υλοποιήθηκαν για την εξαγωγή των απαραίτητων συμπερασμάτων όπως φαίνονται στους Πίνακες 7, 8, 9, 10, 11 της παρούσας εργασίας.

1. **Select count(permi) from allapps where permi like '%....%';** : Στις τελίτσες συμπληρώνεται το όνομα του δικαιώματος. Έπειτα από αρκετές δοκιμές διάφορων δικαιωμάτων βγαίνουν τα δικαιώματα με το μεγαλύτερο ποσοστό εμφάνισης όπως φαίνεται στον Πίνακα 8. Επίσης αν στο ίδιο ερώτημα τοποθετήσουμε μόνο τις επικίνδυνες άδειες θα εξάγουμε αποτελέσματα για τις πιο επικίνδυνες άδειες όπως φαίνεται στον Πίνακα 9.
2. **Select avg(numofperm) from table_name;** : Όπου table_name εννοούνται οι κατηγορίες κάθε εφαρμογής ή παιχνιδιού όπως αυτές αντιστοιχήθηκαν στους ανάλογους πίνακες μέσα στην βάση. Έτσι με αυτό το ερώτημα εξάγουμε αποτελέσματα για τον μέσο όρο των αδειών ανά κατηγορία όπως φαίνεται στον Πίνακα 7.
3. **Select name, numofperm from allapps order by numofperm desc;** : Με την παραπάνω εντολή εξάγουμε έναν πίνακα που που περιέχει το όνομα κάθε εφαρμογής που εισάχθηκε στην βάση δεδομένων και τον αριθμό των αδειών που απαιτεί σε φθίνουσα σειρά. Έπειτα επιλέξαμε τις πρώτες 30 εφαρμογές, οι οποίες είχαν τα περισσότερα δικαιώματα και τις τοποθετήσαμε στον Πίνακα 10. Αντίστοιχα, με το ερώτημα **Select name, numofperm from allapps order by numofperm asc;** προβάλαμε το πλήθος των δικαιωμάτων των εφαρμογών κατά αύξουσα σειρά και επιλέξαμε τις 30 πρώτες για την δημιουργία του Πϊνακα 11.