ΠΑΝΕΠΙΣΤΗΜ ΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΜΣ ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ & ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ιδιωτικότητα στα Smartphones: Μοντέλα Αδειών Πρόσβασης και Ταξινόμηση Προσωπικών Δεδομένων

Ματίνα Τσαβλή

ΑΜ: MTE 1334

Επιβλέπων: Κωνσταντίνος Λαμπρινουδάκης

Κατεύθυνση: Ασφάλεια Ψηφιακών Συστημάτων

Πειραιάς, 2016

Ιδιωτικότητα στα Smartphones: Μοντέλα Αδειών Πρόσβασης και Ταξινόμηση Προσωπικών Δεδομένων

Ματίνα Τσαβλή

Πειραιάς, 2016

Πνευματικά δικαιώματα

Εγκρίθηκε από τα Μέλη της Τριμελούς Εξεταστικής Επιτροπής:

Πρώτος Εξεταστής (Επιβλέπων)	Κωσταντίνος Λαμπρινουδάκης Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά
Δεύτερος Εξεταστής	
Τρίτος Εξεταστής	
Ημερομηνία Έγκρισης	
Βαθμός	

Περίληψη

Στόχος: Η παρούσα μελέτη έχει ως κύριο στόχο να διερευνήσει θέματα ασφάλειας και ιδιωτικότητας, τα οποία έχουν προκύψει από τα μοντέλα αδειών (permission models) των λειτουργικών συστημάτων των smartphones. Στα πλαίσια αυτής της έρευνας, παρέχεται ένα μοντέλο ταξινόμησης των προσωπικών δεδομένων των χρηστών, τα οποία χρησιμοποιούνται κατά τη διάρκεια της χρήσης smartphone, μελετώνται τα μοντέλα αδειών χρήστη, καθώς και οι επιπτώσεις της αλματώδους αύξησης των αιτημάτων για παραχώρηση περισσότερων αδειών, τόσο από τη σκοπιά του χρήστη όσο και από τη σκοπιά του προγραμματιστή. Στη συνέχεια ερευνάται η ιδιωτικότητα που παρέχουν οι εφαρμογές στους χρήστες τους και προτείνεται μια ακολουθία διορθωτικών μέτρων ενάντια στη διάβρωση της ιδιωτικότητας του χρήστη.

Μεθοδολογία/Προσέγγιση: Η μεθοδολογία για την παρούσα έρευνα αναπτύχθηκε σε δύο βασικούς άξονες: ο πρώτος αφορά τα είδη των προσωπικών δεδομένων και ο δεύτερος περιλαμβάνει τις άδειες πρόσβασης που χρησιμοποιούν οι εφαρμογές για να αποκτήσουν πρόσβαση σε αυτά. Για την πρώτη περίπτωση, αρχικά μελετήθηκαν τα είδη των προσωπικών δεδομένων που χρησιμοποιούνται στις φορητές έξυπνες συσκευές και σχεδιάστηκε μια ταξινόμησή τους ανάλογα με το ποια οντότητα μπορεί ή/και έχει πρόσβαση σε αυτά. Στη δεύτερη περίπτωση, μελετήθηκε το υπάρχον μοντέλο αδειών πρόσβασης του Android, σχεδιάστηκε μια εφαρμογή Android ώστε να συλλεχθούν όλες οι άδειες πρόσβασης που προϋπάρχουν μέσα στο λειτουργικό σύστημα του Android, καθώς και ένα API σε γλώσσα προγραμματισμού Java, για να συλλεχθούν οι άδειες που ζητούν οι πιο δημοφιλείς εφαρμογές. Το δείγμα που συλλέχθηκε περιέχει περίπου 22.000 μοναδικές εφαρμογές, οι οποίες είναι διαθέσιμες σε Η.Π.Α. και Ελλάδα.

Πορίσματα: Στα δεδομένα που συλλέχθηκαν από το API εφαρμόστηκε ένα μοντέλο επικινδυνότητας για να εξαχθούν τα ερευνητικά συμπεράσματα. Τα αποτελέσματα της παρούσας έρευνας υποδεικνύουν ότι, παρά τα γεγονός ότι η παροχή άδειας πρόσβασης στα προσωπικά δεδομένα των χρηστών smartphone δεν είναι προβληματική ή παράνομη, τα υπάρχοντα λειτουργικά συστήματα των smartphones δεν παρέχουν ένα επαρκές επίπεδο προστασίας των προσωπικών αυτών δεδομένων.

Ερευνητικοί περιορισμοί: Η παρούσα προσέγγιση αφορά τη μελέτη του μοντέλου αδειών του Android, ωστόσο παρόμοια θέματα ασφάλειας και ιδιωτικότητας έχουν προκύψει και σε άλλα λειτουργικά συστήματα που είναι διαθέσιμα για smartphones. Αυτή η έρευνα βασίζεται αποκλειστικά στην απόκτηση προσωπικών δεδομένων του χρήστη από τρίτους μέσω της φυσιολογικής χρήσης του smartphone. Δεν εξετάζεται καθόλου το ενδεχόμενο απόκτησης των πληροφοριών με μεθόδους δικανικής, κατά τις οποίες η φυσική συσκευή φεύγει από τον έλεγχο του νόμιμου κατόχου της και υπόκειται σε διαδικασίες ανάσυρσης των δεδομένων της.

Επιπτώσεις: Οι προτεινόμενες λύσεις και προτάσεις αυξάνουν την επίγνωση των χρηστών smartphones, απαντούν σε μερικούς από τους προβληματισμούς που εγείρονται σχετικά με το θέμα της ιδιωτικότητας των προσωπικών δεδομένων των χρηστών smartphones, καθώς και περιορίζουν τα μειονεκτήματα που προκύπτουν από την χρήση smartphone συσκευών. Οι συστάσεις που παρουσιάζονται στην παρούσα έρευνα, αν υιοθετηθούν στην πράξη, θα ενδυναμώσουν τον έλεγχο των χρηστών πάνω στα προσωπικά τους δεδομένα και θα βελτιώσουν την ικανότητά τους να διαχωρίζουν τις έννομες εφαρμογές από τις κακόβουλες ή ενοχλητικές.

Λέξεις κλειδιά: Ιδιωτικότητα, προσωπικά δεδομένα, θέματα ασφάλειας, ταξινόμηση δεδομένων, smartphones, επίγνωση χρηστών, δικαιώματα χρηστών, μοντέλο αδειών, permission model, Android.

Πίνακας Περιεχομένων

Κατάλογος Πινάκων

Κατάλογος Γραφημάτων

1. Εισαγωγή

Με την αλματώδη αύξηση της χρήσης και των λειτουργικοτήτων των φορητών «έξυπνων» συσκευών (smartphones, tablets, καθώς και ο νέος όρος phablets, που περιγράφει τα υπερμεγέθη «έξυπνα» κινητά τηλέφωνα με μεγάλη υπολογιστική ισχύ), συνεχώς αναπτύσσονται όλο και πιο εξεζητημένα και περίπλοκα λειτουργικά συστήματα και εφαρμογές, τα οποία προσφέρουν στους χρήστες τους πληθώρα υπηρεσιών. Εκτός από τις παραδοσιακές λειτουργίες των συμβατικών κινητών τηλεφώνων, όπως τηλεφωνικές κλήσεις και αποστολή σύντομων μηνυμάτων, τα smartphones παρέχουν ποικιλία δυνατοτήτων, όπως για παράδειγμα υπηρεσίες παγκόσμιου συστήματος προσδιορισμού θέσης (GPS), υπηρεσίες ηλεκτρονικής αλληλογραφίας, καταγραφή βίντεο, πρόσβαση στον παγκόσμιο ιστό, καθώς επίσης και τη δυνατότητα εγκατάστασης εφαρμογών τρίτων (ο όρος third-party χρησιμοποιείται στη διεθνή βιβλιογραφία για να περιγράψει τις τρίτες οντότητες που εμπλέκονται στην δημιουργία εφαρμογών που δεν ανήκουν στο εγγενές λειτουργικό σύστημα). Τεράστιος όγκος ψηφιακών πληροφοριών των χρηστών δημιουργείται και αποθηκεύεται στα smartphones, όπως για παράδειγμα ίχνη τοποθεσίας, καταγραφές χρήσης, επαφές, φωτογραφίες, έγγραφα, στοιχεία κλήσεων και μηνύματα. Κάθε ένας τύπος ψηφιακών δεδομένων που δημιουργείται, εξυπηρετεί μια ακολουθία σκοπών που διακυμαίνεται από τον εμπλουτισμό των λειτουργικοτήτων των smartphones για να βελτιώσει την εμπειρία του χρήστη, έως την επεξεργασία και αποθήκευση των δεδομένων αυτών. Ακόμα και στην περίπτωση που το smartphone δεν είναι ενεργοποιημένο ή είναι σε κατάσταση αναμονής, παράγει προσωπικές πληροφορίες για τον χρήστη, όπως για παράδειγμα ίχνη τοποθεσίας, καταγραφές ημερομηνίας/ώρας της ενεργοποίησης/απενεργοποίησης του smartphone και άλλα.

Αυτά τα ψηφιακά δεδομένα συχνά συλλέγονται από το λειτουργικό σύστημα ή τις εφαρμογές σε διάφορες περιστάσεις και για διάφορες ανάγκες όπως για παράδειγμα για να υποστηρίξουν τις απαιτήσεις για τη λειτουργία τους, για να δημιουργήσουν ένα λεπτομερές προφίλ χρήστη ή για να αποκτήσουν γνώση για τις ανάγκες του χρήστη και τη συμπεριφορά του. Από τον χρήστη ζητείται να δώσει τη συγκατάθεσή του σε αυτές τις εφαρμογές για να τους εγκριθεί η πρόσβαση στα προσωπικά του δεδομένα, όπως καθορίζεται από το μοντέλο αδειών πρόσβασης[1] (permissions model) κάθε λειτουργικού συστήματος. Επί του

[1] Το μοντέλο αδειών κάθε λειτουργικού συστήματος καθορίζει τον τρόπο που είναι δομημένη η διαδικασία της εξουσιοδότησης των εφαρμογών. Κάθε λειτουργικό σύστημα καθορίζει κάποιο αριθμό αδειών (permissions) που μπορεί να χρησιμοποιηθεί από τις

παρόντος, δεν υπάρχει ένα γενικό εφαρμόσιμο πλαίσιο που χαρακτηρίζει το μοντέλο αδειών πρόσβασης, το οποίο να καθορίζει τους όρους, τις συνθήκες και τους σκοπούς για τη συλλογή και επεξεργασία των προσωπικών δεδομένων των χρηστών. Ωστόσο, ένα τέτοιο πλαίσιο πρόκειται να στοιχειοθετηθεί και να ενισχυθεί στη συμμόρφωσή του με το νόμο. Σύμφωνα με τους σχετικούς κανονισμούς της Ευρωπαϊκής Ένωσης, τα προσωπικά δεδομένα προστατεύονται και η επεξεργασία τους ρυθμίζεται από την Οδηγία 96/46/ΕC[2]. Τα δεδομένα που χαρακτηρίζονται ως δεδομένα επικοινωνίας/κίνησης (καταγραφές χρήσης, τοποθεσίας, διάρκειας κλήσεων κλπ.) επίσης προστατεύονται από το επικοινωνιακό απόρρητο και από κανόνες οι οποίοι είναι ενσωματωμένοι στην Οδηγία 2002/58/ΕC[3].

Ωστόσο, παρά το γεγονός ότι υπάρχει νομικό πλαίσιο σε πολλές χώρες, το οποίο καθορίζει πως πρέπει να γίνεται η διαχείριση των προσωπικών δεδομένων, φαίνεται πως υπάρχει έλλειψη διαφάνειας σχετικά με τον τρόπο που γίνονται τα αιτήματα για παραχώρηση αδειών πρόσβασης. Αμφισβητούμενη είναι επίσης η νομιμότητα αυτών των αιτημάτων, καθώς και η αντίστοιχη συλλογή των δεδομένων. Εξάλλου, έχει διαγνωστεί η τάση των χρηστών και των σχεδιαστών των εφαρμογών (οι προγραμματιστές που αναπτύσσουν το λογισμικό) να μειώνεται το ενδιαφέρον τους για τα θέματα ασφάλειας και ιδιωτικότητας και να αποφεύγουν τις ενέργειες που θα μπορούσαν να τους προφυλάξουν από περιστατικά ασφάλειας. Οι χρήστες πλέον έχουν κουραστεί από την ανάγκη να αποδέχονται όλο και περισσότερα αιτήματα πρόσβασης από τις εφαρμογές, όπως περιγράφεται στην έρευνα του Felt κα. (2012), στην οποία οι συγγραφείς παρουσιάζουν μια προσέγγιση της προσοχής, της αντίληψης και της συμπεριφοράς των χρηστών, ως «προειδοποιητική κόπωση», επειδή σταδιακά χάνουν το ενδιαφέρον τους για την προστασία της ιδιωτικότητας των προσωπικών τους δεδομένων. Παράλληλα, οι σχεδιαστές των εφαρμογών προσπαθούν να ανταποκριθούν στην μεγάλη πολυπλοκότητα των μοντέλων αδειών πρόσβασης των λειτουργικών συστημάτων και να αναπτύξουν καλογραμμένες και ασφαλείς εφαρμογές. Στην έρευνα του Balebako κα. (2014), οι συγγραφείς καταλήγουν στο γεγονός ότι οι σχεδιαστές των

εφαρμογές. Οι εφαρμογές, όταν εγκαθίστανται στο smartphone, ζητούν από τον χρήστη να τους εγκρίνει την πρόσβαση στα προσωπικά δεδομένα του μέσω των αιτημάτων για άδειες.

[2] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών , EEL281 της 23.11.1995, σ. 31

[3] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου , της 12 ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), EEL201 της 31.07.2002, σ. 37

εφαρμογών έχουν ελλιπή γνώση για τα μέτρα ιδιωτικότητας και παίρνουν αποφάσεις επί τούτου.

Αφ' ετέρου, οι χρήστες γίνονται όλο και πιο ενσυνείδητοι στα θέματα της ιδιωτικότητας και ένας μεγάλος αριθμός εργαλείων με στόχο την ενδυνάμωση της προστασίας της ιδιωτικότητας για χρήστες σε κινητά δίκτυα έχει ήδη αναπτυχθεί και προσφέρεται στις on-line αγορές εφαρμογών. Ένα αντιπροσωπευτικό εργαλείο είναι το TaintDroid[4], το οποίο εξετάζει διεξοδικά της ροές προσωπικών δεδομένων, αναλύοντας τις λειτουργίες της υποκείμενης εφαρμογής (Erck κα., 2010). Μια ακόμα ενδιαφέρουσα προσέγγιση παρουσιάζεται στην έρευνα του Sarma κα. (2012), στην οποία γίνεται εκτίμηση των κινδύνων από την εγκατάσταση μιας εφαρμογής, βασισμένη στην κατηγορία και στις άδειες πρόσβασης σε δεδομένα που ζητάει.

Οι λόγοι οι οποίοι ώθησαν τη συγγραφέα να ασχοληθεί με αυτόν τον τομέα και για τους οποίους προέβη στη συγγραφή της παρούσας έρευνας, ήταν η επισήμανση της αναγκαιότητας για την ενίσχυση της προστασίας των προσωπικών δεδομένων και η ανάγκη για καλλιέργεια κουλτούρας ασφάλειας στους χρήστες φορητών συσκευών. Επιβάλλεται να αναλογιστεί κανείς τις κοινές πρακτικές των διαφόρων πλατφορμών και λειτουργικών συστημάτων έξυπνων φορητών συσκευών, καθώς και αυτές των σχεδιαστών που αναπτύσσουν εφαρμογές και να τονιστεί η ανάγκη για αποτελεσματική προστασία των ροών των προσωπικών δεδομένων. Πιο συγκεκριμένα, λόγω της ποικιλομορφίας των πηγών των δεδομένων και της αξίας των προσωπικών πληροφοριών, η παρούσα έρευνα προτείνει μια ταξινόμηση των δεδομένων βασισμένη στις οντότητες που έχουν ή μπορούν να ζητήσουν πρόσβαση στα προσωπικά δεδομένα των χρηστών. Η έρευνα έχει γίνει με βάση τα smartphones, αλλά τα συμπεράσματά της είναι εφαρμόσιμα στο σύνολο των έξυπνων φορητών συσκευών, όπως tablets, PDAs, phablets.

Η μεθοδολογία για την παρούσα έρευνα αναπτύχθηκε σε δύο βασικούς άξονες: ο πρώτος αφορά τα είδη των προσωπικών δεδομένων και ο δεύτερος περιλαμβάνει τις άδειες πρόσβασης που χρησιμοποιούν οι εφαρμογές για να αποκτήσουν πρόσβαση σε αυτά. Για την πρώτη περίπτωση, αρχικά μελετήθηκαν τα είδη των προσωπικών δεδομένων που χρησιμοποιούνται στις φορητές έξυπνες συσκευές και σχεδιάστηκε μια ταξινόμησή τους ανάλογα με το ποια οντότητα μπορεί ή/και έχει πρόσβαση σε αυτά. Στη δεύτερη περίπτωση, μελετήθηκε το υπάρχον μοντέλο αδειών πρόσβασης του Android, σχεδιάστηκε μια εφαρμογή Android και ένα API σε γλώσσα προγραμματισμού Java, ώστε να συλλεχθούν όλες οι άδειες πρόσβασης που προϋπάρχουν μέσα στο λειτουργικό σύστημα του Android και αυτές που ζητούν οι εφαρμογές, αντίστοιχα. Το δείγμα που συλλέχθηκε περιέχει περίπου 22.000

[4] Το TaintDroid είναι ένα εργαλείο για υπολογιστή που προσφέρει έλεγχο για την ιδιωτικότητα του χρήστη σε πραγματικό χρόνο.

μοναδικές εφαρμογές, οι οποίες είναι διαθέσιμες σε Η.Π.Α. και Ελλάδα. Πιο συγκεκριμένα, η παρούσα έρευνα περιλαμβάνει τα εξής:

- Ανάλυση μοντέλων αδειών πρόσβασης για το Android.
- Κατηγοριοποίηση των προσωπικών δεδομένων των χρηστών έξυπνων φορητών συσκευών ανάλογα με τις οντότητες που έχουν ή/και μπορούν να έχει πρόσβαση σε αυτά.
- Δημιουργία βάσης δεδομένων με τις άδειες πρόσβασης που ζητούν οι εφαρμογές (για μεγάλο αριθμό εφαρμογών).
- Εξαγωγή και παρουσίαση στατιστικών στοιχείων για τις άδειες πρόσβασης που ζητούν οι εφαρμογές.
- Εξαγωγή συμπερασμάτων με βάση τα στατιστικά αποτελέσματα.

Η παρούσα ερευνητική εργασία οργανώνεται ως εξής: Στο Κεφάλαιο 2 περιγράφονται οι απαιτήσεις προστασίας της ιδιωτικότητας για τη συλλογή και την επεξεργασία των προσωπικών δεδομένων. Στο Κεφάλαιο 3 μελετώνται τα μοντέλα αδειών πρόσβασης, με εστίαση στο μοντέλο που εφαρμόζει το Android λειτουργικό σύστημα, ενώ έπειτα παρουσιάζονται δύο από τα πιο σημαντικά μειονεκτήματα του μοντέλου αδειών πρόσβασης του Android[5], καθώς και οι επιπτώσεις των αλλεπάλληλων αιτημάτων των εφαρμογών για ολοένα περισσότερες παραχωρήσεις πρόσβασης, είτε από την πλευρά του χρήστη, είτε από αυτή του προγραμματιστή. Στο Κεφάλαιο 4 παρουσιάζεται η ταξινόμηση των δεδομένων των smartphones, ανάλογα με τις οντότητες που έχουν ή αιτούνται πρόσβαση στα προσωπικά δεδομένα του χρήστη, η οποία υλοποιήθηκε στα πλαίσια της παρούσας έρευνας. Το Κεφάλαιο 5 αναλύει το Play Store proprietary API που σχεδιάστηκε για τις ανάγκες της παρούσας έρευνας: η μεθοδολογία που ακολουθήθηκε στο σχεδιασμό του, τα εργαλεία που χρησιμοποιήθηκαν και το δείγμα το οποίο συλλέχθηκε μέσω της χρήσης του. Το Κεφάλαιο 6 περιλαμβάνει τα αποτελέσματα της ανάλυσης των εφαρμογών που συλλέχθηκαν από το API, καθώς και την ανάλυση επικινδυνότητας που εφαρμόστηκε στις παραπάνω εφαρμογές, για να δείξει τους προβληματισμούς ασφάλειας και ιδιωτικότητας που εγείρονται στο σημερινό οικοσύστημα εφαρμογών. Εν τέλει, στο Κεφάλαιο 7 αναλογιζόμαστε πάνω στους τρόπους κατά τους οποίους γίνεται η διαχείριση των προσωπικών δεδομένων και προτείνουμε λύσεις για την αντιμετώπιση της παρούσας κρίσιμης κατάστασης των προβληματισμών που έχουν εγερθεί από πλευράς ιδιωτικότητας και ασφάλειας.

[5] Το Android είναι λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας το οποίο τρέχει τον πυρήνα του λειτουργικού Linux.

2. Απαιτήσεις Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Τα smartphones δεν είναι μόνο απλά εργαλεία επικοινωνίας· συνδυάζουν χαρακτηριστικά των συμβατικών κινητών τηλεφώνων και λειτουργικότητες ηλεκτρονικών υπολογιστών. Τα smartphones φιλοξενούν πληθώρα ετερογενών δεδομένων, τα οποία έχουν δημιουργηθεί από διάφορες hardware ή software πηγές και ως εκ τούτου συνιστούν μια πολύ πλούσια συλλογή προσωπικών πληροφοριών. Λόγω της μεγάλης τους δημοφιλίας και διείσδυσής τους, αποτελούν πλέον αναπόσπαστο κομμάτι της καθημερινότητας και επεμβαίνουν σε αυτή, καθώς και στην αντίστοιχη ιδιωτικότητα. Ο εντοπισμός ενός χρήστη κινητής συσκευής με τη χρήση των πληροφοριών που δίνονται από τις εφαρμογές εμπλέκει την ιδιωτικότητα των προσωπικών του δεδομένων καθώς και το απόρρητο των επικοινωνιών (Μυλωνάς κα. 2013).

Οι προγραμματιστές που αναπτύσσουν εφαρμογές για έξυπνες φορητές συσκευές έχουν συχνά ελλιπή γνώση των έννομων υποχρεώσεών τους. Όσον αφορά τους χρήστες της Ευρωπαϊκής Κοινότητας, η συλλογή και επεξεργασία προσωπικών δεδομένων πρέπει πρώτα να συμμορφώνεται με τις Οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Σύμφωνα με τους όρους της Οδηγίας 95/46/ΕΚ, ο νόμος προστασίας προσωπικών δεδομένων εφαρμόζεται επίσης και στην περίπτωση που ο προγραμματιστής που ανέπτυξε την εφαρμογή ή το ηλεκτρονικό κατάστημα που την παρέχει είναι εγκατεστημένο εκτός της ευρωπαϊκής επικράτειας αν κάνουν χρήση εξοπλισμού μέσα στα όρια της ευρωπαϊκής επικράτειας.

Η Οδηγία 95/46/ΕΚ καθορίζει τη δίκαια και νόμιμη μεταχείριση των προσωπικών δεδομένων. Βασική πράξη της ισχύουσας νομοθεσίας της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα, η οδηγία 95/46/ΕΚ, εκδόθηκε το 1995 με γνώμονα δύο στόχους: την προστασία του θεμελιώδους δικαιώματος στην προστασία των δεδομένων και τη διασφάλιση της ελεύθερης ροής δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών. Σύμφωνα με την οδηγία αυτή:

- ως <δεδομένα προσωπικού χαρακτήρα> νοείται κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί,
- <το πρόσωπο στο οποίο αναφέρονται τα δεδομένα> ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων

στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη,

- ως <υπεύθυνος της επεξεργασίας> νοείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα,
- όταν οι στόχοι και ο τρόπος της επεξεργασίας καθορίζονται από νομοθετικές ή κανονιστικές διατάξεις, εθνικές ή κοινοτικές, ο <υπεύθυνος της επεξεργασίας> ή τα ειδικά κριτήρια για τον ορισμό του μπορούν να καθορίζονται από το εθνικό ή το κοινοτικό δίκαιο, και
- ως <εκτελών την επεξεργασία> νοείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Συμπληρώθηκε από την απόφαση-πλαίσιο 2008/977/ΔΕΥ[6] ως γενική πράξη σε επίπεδο Ένωσης για την προστασία των δεδομένων προσωπικού χαρακτήρα στους τομείς της αστυνομικής και της δικαστικής συνεργασίας σε ποινικές υποθέσεις. Οι σχεδιαστές των εφαρμογών για φορητές συσκευές αποτελούν τους υπεύθυνους της επεξεργασίας και έχουν ως υποχρέωση να παρέχουν στους χρήστες περιεκτικές και κατανοητές πληροφορίες που αφορούν την ταυτότητά τους, τον σκοπό της συλλογής των δεδομένων, καθώς επίσης και τους πιθανούς αποδέκτες των δεδομένων. Επιπλέον, πρέπει να υπάρχει μια νομική βάση για τη συλλογή δεδομένων, όπως ορίζεται στην οδηγία για την προστασία των προσωπικών δεδομένων. Τα δομικά στοιχεία που συνθέτουν μια τέτοια βάση είναι: η συγκατάθεση του χρήστη[7], η σωστή εκτέλεση της σύμβασης ή της συλλογής για την επίτευξη ενός σκοπού με έννομο συμφέρον που επιδιώκει ο υπεύθυνος της επεξεργασίας ή κάποια τρίτη οντότητα (ο όρος third-party χρησιμοποιείται και σε αυτήν την περίπτωση στην διεθνή βιβλιογραφία για να περιγράψει τη μεταφορά δεδομένων από τους υπεύθυνους της επεξεργασίας σε κάποια τρίτη οντότητα για επεξεργασία, και ως εκ τούτου παίρνει το ρόλο του εκτελούντος την επεξεργασία). Ανεξαρτήτως νομικής βάσης, οι σχεδιαστές των εφαρμογών οφείλουν να

[6] Απόφαση-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, της 27ης Νοεμβρίου 2008, για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις, EEL350 της 30.12.2008, σ. 60 (η «απόφαση-πλαίσιο»).

[7] Ως <συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα> νοείται κάθε δήλωση βουλήσεως, ελευθέρας, ρητής και εν πλήρη επίγνωση, με την οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

συμμορφώνονται με τις βασικές αρχές της προστασίας δεδομένων (όπως αυτές υιοθετούνται στο αρ. 4 του Ν.2472/1997[8]):

- **Αρχή του σκοπού:** αποτελεί το βασικότερο κριτήριο και προσδιορίζει σε σημαντικό βαθμό το περιεχόμενο και των άλλων αρχών. Αυτό οφείλεται κατά κάποιο τρόπο στο ότι αποκλείει την πολυλειτουργική συλλογή και χρήση των προσωπικών δεδομένων, τη βασική δηλαδή δυνατότητα και συγχρόνως το μεγαλύτερο κίνδυνο που προκύπτει κυρίως από την αυτοματοποιημένη επεξεργασία τους. Συγκεκριμένα, σύμφωνα με την αρχή αυτή, τα δεδομένα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για σκοπούς, οι οποίοι:
  - έχουν καθοριστεί και αποσαφηνιστεί πλήρως από πριν
  - είναι νόμιμοι, και
  - προσδιορίζουν τη συγκεκριμένη μόνο συλλογή και επεξεργασία και δεν μεταβάλλονται κατά τη διάρκεια τους.
- **Αρχή της αναγκαιότητας**: η επεξεργασία επιτρέπεται, εφόσον ο σκοπός της δεν μπορεί να επιτευχθεί με εξ ίσου αποτελεσματικά αλλά λιγότερο επαχθή για το άτομο μέσα.
- **Αρχή της αναλογικότητας:** το έννομο συμφέρον του υπεύθυνου επεξεργασίας πρέπει να υπερέχει καταφανώς, σε κάθε συγκεκριμένη περίπτωση των δικαιωμάτων και συμφερόντων των υποκειμένων των δεδομένων και να μη βλάπτει τις προσωπικές τους ελευθερίες.
- **Αρχή της περιορισμένης συλλογής:** τα προσωπικά δεδομένα δεν πρέπει να είναι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας**.**
- **Αρχή της περιορισμένης διατήρησης στο χρόνο:** τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια ης περιόδου που απαιτείται για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους.

Οι εφαρμογές για φορητές συσκευές αιτούνται πρόσβαση στα προσωπικά δεδομένα των χρηστών για να τους παρέχουν κάποια υπηρεσία, αλλά επίσης για διαφήμιση, ανάλυση δεδομένων και άλλους δευτερεύοντες σκοπούς. Πολλές εφαρμογές συχνά συλλέγουν δεδομένα, συμπεριλαμβανομένου ευαίσθητων δεδομένων, βιομετρικών στοιχείων, δεδομένα τοποθεσίας ή ιστορικά φυλλομετρήσεων (Urban κα., 2012). Οι πιο σημαντικές ανησυχίες για την ιδιωτικότητα των προσωπικών δεδομένων πηγάζουν από την έλλειψη διαφάνειας, και αντίστοιχα, ενσυναίσθησης για την ύπαρξη, το είδος και την έκταση της

[8] Ν. 2472/1997 - Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

επεξεργασίας στην οποία υποβάλλονται (αρ. 29 Ομάδα Εργασίας Προστασίας Δεδομένων, 2013).

Αυτή η κατάσταση επιδεινώνεται λόγω της αμέλειας που δείχνουν οι σχεδιαστές των εφαρμογών για τις αρχές του σκοπού και της αναλογικότητας. Τα δεδομένα συλλέγονται και αποθηκεύονται για ένα σύνολο ακαθόριστων επιπλέον σκοπών και συχνά δεν είναι επαρκή, σχετικά και αναλογικά σε σχέση με την λειτουργικότητα της εφαρμογής.

Παράλληλα, το οικοσύστημα της ανάπτυξης εφαρμογών χαρακτηρίζεται από το μεγάλο βαθμό κατακερματισμού μεταξύ των πολλών συμμετεχόντων, συμπεριλαμβανομένων των σχεδιαστών εφαρμογών, των ιδιοκτητών εφαρμογών, των app stores, των κατασκευαστών λειτουργικών συστημάτων και συσκευών και άλλων τρίτων που υπάρχει περίπτωση να εμπλέκονται στη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα από έξυπνες συσκευές, όπως οι πάροχοι αναλύσεων και διαφημίσεων. Ως αποτέλεσμα, η πληθώρα των εμπλεκομένων που συμμετέχουν σε αυτή τη διαδικασία, η ταχέως αναπτυσσόμενη χρήση για έρευνα αγοράς και διαφήμιση, η αντίστοιχα μεγάλη συγκέντρωση και ευρεία διανομή των προσωπικών δεδομένων και η «έλλειψη ουσιαστικής συγκατάθεσης» (αρ. 29 Ομάδα Εργασίας Προστασίας Δεδομένων, 2013) αποτελούν τους σοβαρότερους κινδύνους για την προστασία των δεδομένων των τελικών χρηστών[9]. Είναι πράγματι αμφίβολο αν τα υπάρχοντα μοντέλα αδειών πρόσβασης συμμορφώνονται με τις απαιτήσεις της συγκατάθεσης των τελικών χρηστών.

[9] Κείμενο εργασίας της «Ομάδας Προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα» που έχει συσταθεί σύμφωνα με το αρ. 29 της Οδηγίας 95/46/ΕΚ με τίτλο: Γνώμη 02/2013 για τις εφαρμογές των έξυπνων συσκευών

3. Μοντέλα Αδειών Πρόσβασης

Κοινή απαίτηση όλων των σύγχρονων πληροφοριακών συστημάτων είναι η προστασία της πληροφορίας κατά τη διακίνησή της μέσα σε αυτά. Δεδομένης της ανάγκης προστασίας των ψηφιακών δεδομένων από μη εξουσιοδοτημένους χρήστες είναι απαραίτητη κάποια γλώσσα έκφρασης της επιθυμητής πολιτικής ελέγχου προσπέλασης[10] των υπολογιστικών πόρων, καθώς και συγκεκριμένων μηχανισμών για την εφαρμογή και παρακολούθηση της πολιτικής αυτής. Ο έλεγχος προσπέλασης απαιτεί την ύπαρξη μιας σειράς μηχανισμών ελέγχου προσπέλασης, οι οποίοι εξασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα και την εξουσιοδότηση. Οι μηχανισμοί αυτοί, είναι άμεσα εξαρτημένοι από τις συγκεκριμένες λειτουργίες προσπέλασης που υποστηρίζουν τα λειτουργικά συστήματα. Τα σύγχρονα λειτουργικά συστήματα προσφέρουν λειτουργίες προσπέλασης που είναι προσανατολισμένες στις συγκεκριμένες ανάγκες κάθε ανεξάρτητου χρήστη. Οι μηχανισμοί ελέγχου προσπέλασης, σε συνδυασμό με άλλους μηχανισμούς ασφάλειας, προστατεύουν το σύστημα από μη εξουσιοδοτημένη προσπέλαση στα δεδομένα εκείνα, τα οποία επηρεάζουν την ασφάλεια του συστήματος και είναι αποθηκεμένα στη μνήμη ή σε άλλο τμήμα του.

Ο μηχανισμός ελέγχου προσπέλασης που χρησιμοποιούν τα σύγχρονα λειτουργικά συστήματα είναι η εξουσιοδότηση «Βασισμένη σε Ρόλους»[11]. Ως ρόλος ορίζεται ένα σύνολο από ενέργειες/ευθύνες οι οποίες σχετίζονται με κάποια συγκεκριμένη λειτουργία του λειτουργικού συστήματος. Ο έλεγχος πρόσβασης δεν βασίζεται στην ταυτότητα των υποκειμένων/οντοτήτων (Πολιτική Διακριτικού Ελέγχου Προσπέλασης)[12] ή στη διαβάθμιση των υποκειμένων/οντοτήτων (Πολιτική Υποχρεωτικού Ελέγχου Προσπέλασης)[13], αλλά στο ρόλο που έχει ένα υποκείμενο/οντότητα μια δεδομένη χρονική στιγμή (Καλλονιάτης, 2015).

Το μοντέλο ελέγχου προσπέλασης RBAC αποτελεί ίσως την πληρέστερη λύση στην αντιμετώπιση του ελέγχου προσπέλασης για τα σύγχρονα πληροφοριακά συστήματα. Στην περίπτωση του Android έχει προταθεί μια γενική υλοποίηση του RBAC σαν αυτόνομη υπηρεσία, αλλά και μια προσέγγιση του τρόπου ανάπτυξης μηχανισμών ελέγχου προσπέλασης με σαφή διαχωρισμό μεταξύ της λήψης

[10] Ο όρος «έλεγχος προσπέλασης» αφορά τους συγκεκριμένους μηχανισμούς που υλοποιεί κάποιο υπολογιστικό σύστημα, με σκοπό να προστατεύσει από μη εξουσιοδοτημένη προσπέλαση τα δεδομένα και τους μη διαμοιρασμένους πόρους, οι οποίοι επηρεάζουν την ασφάλεια πόρων του συστήματος.
[11] RBAC – Role based Access Control
[12] DAC Discretionary Access Control
[13] MAC Mandatory Access Control

αποφάσεων εξουσιοδότησης και του μηχανισμού επιβολής ελέγχου προσπέλασης (Rohrer κα., 2012).

3.1. Το Μοντέλο Αδειών Πρόσβασης του Android

Ο έλεγχος προσπέλασης στις έξυπνες φορητές συσκευές υποστηρίζεται μέσω των μοντέλων αδειών πρόσβασης. Κάθε λειτουργικό σύστημα έχει δημιουργήσει το δικό του μηχανισμό αδειών προσπέλασης, ο οποίος καθορίζεται από τις προδιαγραφές και πολιτικές ασφάλειας που εφαρμόζονται. Το Android είναι ένα λειτουργικό σύστημα το οποίο εφαρμόζει διαχωρισμό προνομίων, και στο οποίο κάθε εφαρμογή τρέχει με μια ξεχωριστή ταυτότητα συστήματος (Linux αναγνωριστικό χρήστη και ομάδας). Μέρη του συστήματος διαχωρίζονται επίσης σε διαφορετικές ταυτότητες. Το Linux εκ τούτου απομονώνει τις εφαρμογές τη μια από την άλλη και από το σύστημα.

Οι Android εφαρμογές είναι κατά βάση γραμμένες σε Java και XML και τρέχουν μέσα στο περιβάλλον εκτέλεσης Android Runtime (ART)[14]. Ωστόσο, αρκετές εφαρμογές, συμπεριλαμβανομένου βασικές υπηρεσίες και εφαρμογές του Android, είναι μητρικές (εγγενείς) ή περιλαμβάνουν μητρικές βιβλιοθήκες. Αμφότερα το περιβάλλον εκτέλεσης και οι μητρικές εφαρμογές τρέχουν μέσα στο ίδιο περιβάλλον ασφάλειας, το οποίο περιέχεται μέσα στο περιβάλλον λειτουργίας εφαρμογών (Application Sandbox). Σκοπός του sandboxing είναι να βελτιωθεί η ασφάλεια απομονώνοντας μια εφαρμογή για να αποφευχθεί σε κακόβουλο λογισμικό, εισβολείς, πόρους του συστήματος ή άλλες εφαρμογές να αλληλεπιδράσουν με την προστατευόμενη εφαρμογή[15]. Έχοντας υιοθετήσει τον τρόπο λειτουργίας του Linux, το περιβάλλον λειτουργίας των εφαρμογών του Android, απομονώνει τα δεδομένα και την εκτέλεση του κώδικα των εφαρμογών από τις άλλες εφαρμογές. Το Android δίνει σε κάθε εφαρμογή ένα μοναδικό

[14] Η τεχνολογία του ART εισήχθη πρώτη φορά στην έκδοση Android 4.4 «KitKat», η οποία τη συμπεριελάμβανε ως εναλλακτικό περιβάλλον εκτέλεσης, κρατώντας ωστόσο τον Dalvik ως την προεπιλεγμένη εικονική μηχανή. Στην επόμενη έκδοση λογισμικού Android 5.0 «Lollipop», ο Dalvik αντικαταστάθηκε εξολοκλήρου από την τεχνολογία ART. Το περιβάλλον ART εκτελεί μετασχηματισμό του bytecode της εφαρμογής σε μητρική οδηγίες που αργότερα εκτελούνται από το περιβάλλον εκτέλεσης της συσκευής.

[15] Το sandboxing των εφαρμογών είναι αμφιλεγόμενης σημασίας καθώς η πολυπλοκότητά του μπορεί να προκαλέσει περισσότερα προβλήματα ασφάλειας από αυτά που σχεδιάστηκε να αποτρέψει. Το sandbox πρέπει να περιλαμβάνει όλα τα αρχεία που χρειάζεται η εφαρμογή για να εκτελεστεί, το οποίο μπορεί να επίσης να δημιουργήσει προβλήματα μεταξύ των εφαρμογών που χρειάζεται να αλληλεπιδράσουν. Για παράδειγμα, αν ένας προγραμματιστής αναπτύξει μια εφαρμογή που χρειάζεται να αλληλεπιδράσει με τις επαφές της συσκευής, λόγω του sandboxing αυτή η εφαρμογή θα έχανε σημαντική λειτουργικότητα.

αναγνωριστικό χρήστη (UID) και την τρέχει σαν ξεχωριστή διεργασία. Μόνο οι διεργασίες με ίδιο αναγνωριστικό χρήστη μπορούν να διαμοιράζονται πόρους, άρα, εφόσον κάθε αναγνωριστικό ανατίθεται μοναδικά, αυτό σημαίνει ότι καμία άλλη εφαρμογή δεν έχει πρόσβαση στους ίδιους πόρους.

Πιο εξειδικευμένες δυνατότητες ασφάλειας παρέχονται μέσω του μηχανισμού αδειών πρόσβασης, ο οποίος επιβάλει περιορισμούς σε ειδικές λειτουργίες που μπορεί να εκτελέσει μια διεργασία, και μέσω των αδειών URI[16], με τις οποίες επιτυγχάνεται παραχώρηση πρόσβασης για έναν ειδικό σκοπό μόνο και σε συγκεκριμένα δεδομένα.

Οι άδειες συστήματος χωρίζονται σε επιμέρους επίπεδα προστασίας (Android, 2015). Τα δύο πιο σημαντικά επίπεδα προστασίας είναι οι κανονικές και οι επικίνδυνες άδειες, καθώς είναι και αυτά που επηρεάζουν περισσότερο το χρήστη:

- Οι **κανονικές άδειες** (normal) καλύπτουν περιοχές στις οποίες η εφαρμογή χρειάζεται άδεια πρόσβασης σε δεδομένα ή πόρους του συστήματος έξω από το περιβάλλον λειτουργίας της (sandbox), αλλά σε σημεία όπου είναι πολύ μικρός ο κίνδυνος για τα προσωπικά δεδομένα του χρήστη ή τη λειτουργία των υπόλοιπων εφαρμογών. Μια τέτοια άδεια είναι η άδεια ρύθμισης της ζώνης ώρας. Αν μια εφαρμογή χρειάζεται αυτήν την άδεια, αυτόματα το σύστημα εγκρίνει την πρόσβαση στην εφαρμογή.
- Οι **επικίνδυνες άδειες** (dangerous) καλύπτουν περιοχές όπου η εφαρμογή ζητάει άδεια πρόσβασης σε δεδομένα ή πόρους του συστήματος, τα οποία περιλαμβάνουν προσωπικά δεδομένα του χρήστη, ή θα μπορούσαν να επηρεάσουν τα αποθηκευμένα δεδομένα ή τη λειτουργία των υπόλοιπων εφαρμογών. Αν μια εφαρμογή δηλώνει ότι χρειάζεται να της χορηγηθεί μια επικίνδυνη άδεια, τότε ο χρήστης θα πρέπει ρητά να της χορηγήσει την άδεια. Στον Πίνακα 1 (Android Developers, 2015), φαίνονται οι επικίνδυνες άδειες, καθώς και η ομάδα αδειών στην οποία ανήκουν.
- Για να ανήκει μια άδεια στο επίπεδο **αδειών με υπογραφές** (signature), η εφαρμογή που τη ζητάει θα πρέπει να έχει υπογραφθεί με το ίδιο πιστοποιητικό που έχει η εφαρμογή που το δήλωσε. Αυτό σημαίνει ότι οι εφαρμογές θα πρέπει να έχουν σχεδιαστεί από την ίδια εταιρεία. Αν τα πιστοποιητικά συμπίπτουν, το σύστημα αυτόματα παραχωρεί την άδεια χωρίς να ενημερώσει το χρήστη ή να ζητήσει ρητή έγκριση. Συνήθως αυτές οι εφαρμογές είναι προεγκατεστημένες.

[16] Uniform Resource Identifier (URI) permissions: αποτελούν άδειες ειδικού σκοπού με τις οποίες επιτυγχάνεται συνεργασία ανάμεσα στις εφαρμογές. Ένα τυπικό παράδειγμα αποτελεί η χρήση του ηλεκτρονικού ταχυδρομείου. Αν το URI μιας επισυναπτόμενης εικόνας σε ένα mail δοθεί στην εφαρμογή προβολής εικόνων, αυτή η εφαρμογή κανονικά δεν θα πρέπει να έχει άδεια να ανοίξει την εικόνα από τη στιγμή που δεν έχει άδεια πρόσβασης στα δεδομένα της εφαρμογής του ηλεκτρονικού ταχυδρομείου.

- **Άδεια συστήματος ή υπογραφής** (signatureOrSystem) είναι το επίπεδο των αδειών των εφαρμογών που έχουν εγκατασταθεί με δικαιώματα υπερχρήστη (root). Αυτού του επιπέδου οι άδειες παραχωρούνται μόνο σε εφαρμογές που είναι στο system image του Android ή έχουν υπογραφεί με το ίδιο πιστοποιητικό με την εφαρμογή που δήλωσε την άδεια. Η χρήση αυτού του επιπέδου αδειών θα πρέπει να αποφεύγεται, καθώς το αμέσως προηγούμενο επίπεδο καλύπτει σε μεγάλο βαθμό αυτές τις περιπτώσεις, ανεξάρτητα με το που ακριβώς έχουν εγκατασταθεί οι εφαρμογές. Αυτό το επίπεδο αδειών θα πρέπει να δηλώνεται μόνο σε περιπτώσεις που πολλαπλοί πάροχοι έχουν εφαρμογές μέσα στο system image και χρειάζονται να διαμοιραστούν συγκεκριμένα χαρακτηριστικά επειδή πρέπει να γίνουν build μαζί.
- **Άδεια ανάπτυξης** (development): αναφέρεται σε άδειες που προορίζονται μόνο για σχεδιαστές εφαρμογών και στις οποίες η ROM πρέπει να έχει υπογραφθεί με ένα σχεδιαστικό κλειδί (development key).

Πίνακας 1. Επικίνδυνες άδειες και ομάδες αδειών

Α/Α	Ομάδα Αδειών (Permissions Groups)	Άδεια (Permission)
1	Ημερολόγιο	READ_CALENDAR WRITE_CALENDAR
2	Κάμερα	CAMERA
3	Επαφές	READ_CONTACTS WRITE_CONTACTS GET_ACCOUNTS
4	Τοποθεσία	ACCESS_FINE_LOCATION ACCESS_COARSE_LOCATION
5	Μικρόφωνο	RECORD_AUDIO
6	Τηλέφωνο	READ_PHONE_STATE CALL_PHONE READ_CALL_LOG WRITE_CALL_LOG ADD_VOICEMAIL USE_SIP PROCESS_OUTGOING_CALLS
7	Αισθητήρες	BODY_SENSORS
8	SMS	SEND_SMS RECEIVE_SMS READ_SMS RECEIVE_WAP_PUSH RECEIVE_MMS
9	Αποθήκευση	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE

Το πρόβλημα που προκύπτει από αυτή την ταξινόμηση είναι ότι μια ομάδα αδειών (permission group) δύναται να περιέχει τόσο βασικές όσο και επικίνδυνες άδειες. Για παράδειγμα:

- **Τοποθεσία:** Μια εφαρμογή που ζητάει κατά προσέγγιση την τοποθεσία του χρήστη μέσω του κινητού δικτύου επικοινωνιών, δύναται να αποκτήσει την ακριβή τοποθεσία του μέσω του GPS της συσκευής.
- **SMS:** Μια εφαρμογή που χρειάζεται μόνο να λαμβάνει μηνύματα, μπορεί τώρα να έχει άδεια να λαμβάνει μηνύματα στο παρασκήνιο, με το ενδεχόμενο να χρεώνει το χρήστη.
- **Τηλέφωνο:** Μια εφαρμογή η οποία ζητάει να διαβάσει το αρχείο με τις κλήσεις, μπορεί τώρα να έχει άδεια να δρομολογεί εξερχόμενες κλήσεις και να καλεί χωρίς να ρωτάει το χρήστη.
- **Αποθήκευση (Φωτογραφίες/Αποθηκευτικά Μέσα/Αρχεία):** Μια εφαρμογή που ζητάει άδεια να διαβάσει τα περιεχόμενα του USB ή του SD αποθηκευτικού μέσου, έχει τώρα άδεια να διαμορφώσει όλο τον εξωτερικό αποθηκευτικό χώρο της συσκευής.
- **Κάμερα/Μικρόφωνο:** Μια εφαρμογή που ζητάει άδεια να βγάλει φωτογραφίες και βίντεο, πλέον έχει την άδεια καταγραφής ήχου. Η εφαρμογή θα μπορούσε να ακούει το χρήστη ακόμα και όταν ο χρήστης χρησιμοποιεί άλλες εφαρμογές ή η οθόνη του είναι κλειστή.

Από τον χρήστη ζητείται να δώσει την συγκατάθεσή του όταν μια εφαρμογή αιτείται πρόσβαση σε ένα νέο permissions group. Ωστόσο, αν έχει ήδη δώσει στην εφαρμογή έστω και μια από τις άδειες της ομάδας αυτής, η εφαρμογή από εκεί και πέρα μπορεί να χρησιμοποιήσει όλες τις άδειες της ομάδας. Ήδη πολλές εφαρμογές ζητούν περισσότερες άδειες από αυτές που χρειάζονται για να λειτουργήσουν σωστά, αλλά τώρα μπορούν να αποκτήσουν ακόμα περισσότερες άδειες που δε χρειάζονται (Hoffman, 2015).

3.2. Αλλαγές στο Μοντέλο Αδειών Android 6.0 (Marshmallow)

Κάθε λειτουργικό σύστημα έχει δομήσει το μηχανισμό αδειών πρόσβασής του διαφορετικά, το οποίο παρέχει μεγάλες και ετερογενείς λίστες με άδειες για να διαχειριστεί την πρόσβαση των εφαρμογών στον αχανή όγκο προσωπικών δεδομένων που υπάρχουν στις έξυπνες φορητές συσκευές. Οι λίστες αυτές είναι κάθε άλλο παρά στατικές και δύναται να αλλάξουν σημαντικά με κάθε νέα ενημέρωση του λειτουργικού.

Πίνακας 2. Αριθμός αδειών ανά έκδοση του Android[17]

Έκδοση	Κυκλοφόρησε	API Level	Όνομα	Αριθμός Αδειών
Android 6.0	Αύγουστος 2015	23	Marshmallow	131
Android 5.1	Μάρτιος 2015	22	Lollipop	191
Android 4.4	Οκτώβριος 2013	19	Kitkat	172

Για παράδειγμα, η έκδοση 4.4 του λειτουργικού συστήματος Android, υποστηρίζει περισσότερες από 170 διαφορετικές άδειες για τον έλεγχο της πρόσβασης των εφαρμογών στους πόρους της έξυπνης συσκευής, ενώ η έκδοση 5.1 ακόμα περισσότερες. Η τελευταία έκδοση Android 6.0 Marshmallow, εκτός από τον αριθμό και το είδος των αδειών, άλλαξε και όλη τη φιλοσοφία του μοντέλου αδειών που χρησιμοποιούσε και υιοθέτησε ένα μοντέλο παρεμφερές στα πρότυπα του iOS λειτουργικού συστήματος των iPhones. Αξίζει επίσης να σημειωθεί ότι στην επίσημη σελίδα του Android, οι άδειες που καταργήθηκαν δεν αναφέρονται καν, ενώ παράλληλα η σελίδα που περιγράφει αναλυτικά όλες οι αλλαγές μεταξύ των εκδόσεων είναι κάθε άλλο παρά ευανάγνωστη και εύχρηστη[18]. Επιπλέον, υπενθυμίζεται πως από όλες αυτές τις άδειες, μόνο οι επικίνδυνες ζητούν άδεια πρόσβασης από τον χρήστη, και αυτές δεν άλλαξαν σε αυτές τις εκδόσεις.

Οι αλλαγές στον μηχανισμό του μοντέλου των αδειών στο Android 6.0 (API level 23), συνοψίζονται ως εξής:

- Ο χρήστης χορηγεί άδειες στις εφαρμογές κατά τη διάρκεια της λειτουργίας της εφαρμογής και όχι κατά την εγκατάστασή της. Αυτή η προσέγγιση βελτιώνει τη

[17] Τα αποτελέσματα προέκυψαν από καταμέτρηση των διαθέσιμων αδειών στις αντίστοιχες εκδόσεις λειτουργικού στη συσκευή Android 5.1 WVGA. Για το σκοπό αυτό αναπτύχθηκε ένα πρωτότυπο εφαρμογής, το οποίο καλεί τον Package Manager του συστήματος. Περισσότερες πληροφορίες για την εφαρμογή που αναπτύχθηκε μπορούν να βρεθούν στο Παράρτημα.

[18] Η σελίδα που περιγράφει όλες τις αλλαγές ανάμεσα στις διάφορες εκδόσεις των API βρίσκεται στην τοποθεσία: http://developer.android.com/sdk/api_diff/23/changes.html

διαδικασία της εγκατάστασης, εφόσον ο χρήστης δεν χρειάζεται να χορηγήσει άδειες κατά την εγκατάσταση ή την αναβάθμιση της εφαρμογής.

- Ο χρήστης πλέον έχει τη δυνατότητα να εγκρίνει ή να απορρίπτει συγκεκριμένες άδειες από το σύνολο αυτών που ζητάει μια εφαρμογή. Για παράδειγμα, αν κάποιος χρήστης θέλει να στείλει ένα ηχητικό μήνυμα με την εφαρμογή WhatsApp, θα του ζητηθεί για μια και μοναδική φορά να παραχωρήσει άδεια χρήσης του μικροφώνου. Άρα, η ρύθμιση των αδειών θα γίνεται όταν η εφαρμογή θελήσει πρόσβαση για πρώτη φορά σε κάποιο πόρο της κινητής συσκευής.
- Επιπλέον, ο χρήστης μπορεί να επανεξετάσει τις άδειες που έχει παραχωρήσει από τις «Ρυθμίσεις» ή να δει τις άδειες κατηγοριοποιημένες ανά τύπο και ανά εφαρμογή που τις χρησιμοποιεί. Ο χρήστης μπορεί μετέπειτα να αλλάξει τις ρυθμίσεις των εφαρμογών, ακόμα και αν έχουν σχεδιαστεί για πιο παλιά έκδοση του Android και επομένως δεν ζητήσουν άδεια πρόσβασης για κάποιον πόρο[19]. Τις περισσότερες φορές, οι εφαρμογές συνεχίζουν να λειτουργούν κανονικά αν ο χρήστης ανακαλέσει κάποια άδεια που τους έχει παραχωρήσει στο παρελθόν. Ωστόσο, σε μερικές σπάνιες περιπτώσεις, η εφαρμογή μπορεί να καταρρεύσει ή να μην λειτουργεί κανονικά. Για παράδειγμα, αν ο χρήστης ανακαλέσει την άδεια χρήσης της κάμερας σε μια εφαρμογή που βγάζει φωτογραφίες, η εφαρμογή θα φαίνεται ότι δεν λειτουργεί, χωρίς να ειδοποιήσει το χρήστη ότι χρειάζεται να της παραχωρήσει άδεια πρόσβασης στην κάμερα. Όπως και να έχει, αν ο χρήστης αντιμετωπίσει οποιοδήποτε πρόβλημα σχετικό με τις άδειες της εφαρμογής, μπορεί να επιστρέψει στις «Ρυθμίσεις» και να χορηγήσει τις άδειες που ανακάλεσε.
- 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 η οποία θέλει να μπορεί να διαβάζει τα εισερχόμενα SMS μηνύματα απαιτεί την άδεια «READ_SMS». Όταν ο χρήστης εγκαθιστά την εφαρμογή από το Play Store, θα δει ότι ζητάει άδεια για όλη την ομάδα των SMS αδειών, τη στιγμή που όλες οι υπόλοιπες άδειες δεν χρησιμοποιούνται ζητάει άδεια για όλη την ομάδα των SMS αδειών. Αν λοιπόν χορηγήσει την άδεια αυτή, παράλληλα χορηγεί και όλες τις σχετικές με αυτή άδειες. Αυτή η εφαρμογή μπορεί στην επόμενη αναβάθμιση να θέλει να υποστηρίζει και λειτουργίες αποστολής SMS μηνυμάτων, όμως όταν ο χρήστης επιλέξει να γίνει η αναβάθμισή της, δεν θα προτραπεί να

[19] Οι παλιές εφαρμογές που δεν είχαν σχεδιαστεί με βάση τα νέα χαρακτηριστικά του μοντέλου αδειών του Android, υποθέτουν ότι τους παραχωρείται πρόσβαση σε οποιαδήποτε πόρο και αν ζητήσουν.

παραχωρήσει εκ νέου άδεια για να στέλνει SMS μηνύματα, άρα δεν θα ενημερωθεί καν, ενώ παράλληλα η εφαρμογή θα έχει τη δυνατότητα να στέλνει SMS[20] (Hoffman, 2015).

3.3. Μειονεκτήματα Μοντέλων Αδειών Πρόσβασης

Τα μοντέλα αδειών πρόσβασης των σύγχρονων λειτουργικών συστημάτων έξυπνων φορητών συσκευών είναι σε μεγάλο βαθμό ανεπαρκή για να διαφυλάξουν την ιδιωτικότητα των χρηστών τους, όπως αυτή καθορίζεται από το ευρωπαϊκό νομικό πλαίσιο. Οι σχεδιαστές των εφαρμογών πρέπει να συμμορφώνονται με τις απαιτήσεις συγκατάθεσης οι οποίες αναφέρονται στην οδηγία για τα προσωπικά δεδομένα (αρ. 5 παρ.3 της 2002/58/EC) αν παρέχουν υπηρεσίες σε χρήστες που ζουν στην Ευρωπαϊκή Οικονομική Ζώνη, ανεξάρτητα της τοποθεσίας που βρίσκεται ο πάροχος. Σύμφωνα με το νόμο, η χρήση ηλεκτρονικών τηλεπικοινωνιακών δικτύων για την αποθήκευση πληροφοριών ή για την απόκτηση άδειας πρόσβασης σε πληροφορίες αποθηκευμένες σε τερματικό εξοπλισμό ενός συνδρομητή ή χρήστη επιτρέπεται μόνο στην περίπτωση που ο συνδρομητής ή χρήστης έχει προμηθευθεί ξεκάθαρες και κατανοητές πληροφορίες, μεταξύ άλλων το σκοπό της επεξεργασίας, καθώς επίσης του έχει προσφερθεί το δικαίωμα να αρνηθεί οποιαδήποτε επεξεργασία από τον υπεύθυνο της επεξεργασίας.

Ακόμα και στην περίπτωση που ο νόμος απαιτεί από το χρήστη την ελεύθερη συναίνεση και μετά από ενημέρωση (ΣΜΕ) ως νομικό λόγο για να αποθηκεύσει πληροφορίες ή να λάβει πρόσβαση σε ήδη αποθηκευμένες πληροφορίες, η ενημέρωση του χρήστη δεν είναι πάντα κατανοητή και ξεκάθαρη. Η Ομάδα Εργασίας για την Προστασία των Προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Data Protection Working Party), η οποία αποτελείται από αντιπροσώπους των Ευρωπαϊκών Αρχών Προστασίας Δεδομένων, υπογραμμίζει ότι η μικρή οθόνη δεν αποτελεί δικαιολογία. Εξάλλου, η συγκατάθεση έχει μειωθεί στη διαδικασία «just click submit» (Ciocchetti, 2008), καθώς το καθεστώς συγκατάθεσης είναι στην ουσία του τύπου «όλα ή τίποτα» (Egelman κα., 2013), το οποίο δεν αφήνει περιθώριο στους χρήστες να δηλώσουν τις επιλογές τους και τις προτιμήσεις τους.

Η παρούσα έρευνα μελετάει το μοντέλο αδειών πρόσβασης του λειτουργικού συστήματος του Android, ωστόσο παρόμοια θέματα εγείρονται και σε άλλα

[20] Ο μόνος τρόπος με τον οποίο μπορεί να αποφευχθεί κάτι τέτοιο είναι να απενεργοποιήσει ο χρήστης τις αυτόματες ενημερώσεις και να επιβεβαιώνει χειροκίνητα τις άδειες κάθε φορά που μια εφαρμογή ζητάει αναβάθμιση. Από την άλλη, αυτό ενέχει τον κίνδυνο να καταλήξει να χρησιμοποιεί παλαιότερες εκδόσεις των εφαρμογών, το οποίο μπορεί να προκαλέσει και προβλήματα ασφάλειας.

λειτουργικά συστήματα, όπως το iOS και το Windows Mobile. Ξεκινώντας, η συγγραφέας παραθέτει μια σύντομη περιγραφή των αντιπροσωπευτικών γνωστών θεμάτων του μοντέλου αδειών πρόσβασης του Android, και έπειτα επικεντρώνεται στα δύο πιο σημαντικά μειονεκτήματα, τα οποία δεν έχουν συζητηθεί επαρκώς έως σήμερα. Σε αυτό το σημείο είναι σημαντικό να αναφέρουμε ότι η έρευνα βασίζεται σε συσκευές στις οποίες ο χρήστης δεν έχει πάρει δικαιώματα υπερχρήστη τους συστήματος (root), καθώς αυτό θα εισήγαγε περισσότερους κινδύνους διαρροής δεδομένων σε τρίτες οντότητες.

Στο Android μέχρι την προηγούμενη έκδοσή του, όταν μια εφαρμογή ξεκινούσε την εγκατάστασή της, προέτρεπε το χρήστη να εγκρίνει τις άδειες που ζητούσε. Ο χρήστης δεν είχε κανένα δικαίωμα διαπραγμάτευσης για συγκρότηση των επιλογών πρόσβασης και χρήσης. Για παράδειγμα, αν μια εφαρμογή πυξίδας ζητούσε άδεια να διαβάσει πληροφορίες από συγκεκριμένους αισθητήρες αλλά και τις επαφές του χρήστη, ο χρήστης δεν μπορούσε να επιτρέψει πρόσβαση μόνο στις άδειες που σχετίζονταν με τη λειτουργικότητα της εφαρμογής. Στην νέα έκδοση του Android αυτό αλλάζει, φαινομενικά προς όφελος των χρηστών. Πλέον ο χρήστης μπορεί να δώσει άδεια πρόσβασης σε μια συγκεκριμένη ομάδα αδειών και να απορρίψει την πρόσβαση σε κάποια άλλη. Έπειτα, όπως συζητήθηκε σε προηγούμενη ενότητα, αν μια εφαρμογή έχει σχεδιαστεί για πιο παλιά έκδοση του Android, δεν θα ζητήσει καμία συγκατάθεση από το χρήστη, αλλά αντιθέτως θα υποθέσει πως έχει πρόσβαση σε όποιο πόρο και να ζητήσει. Ο χρήστης θα πρέπει από μόνος του να ανατρέξει στις «Ρυθμίσεις» και να επανεξετάσει τις άδειες πρόσβασης χειροκίνητα.

Μερικές άδειες θα ήταν πολύ πιο αποτελεσματικές αν μπορούσαν να υποστηρίξουν μια δομή ελέγχου πρόσβασης περισσότερο αναλυτική και ξεκάθαρη. Στην έρευνα του Jeon κα. (2012), γίνεται αξιολόγηση μιας τέτοιας προσέγγισης για τις άδειες των εφαρμογών. Για παράδειγμα, μια εφαρμογή η οποία χρειάζεται να συνδεθεί σε μια συγκεκριμένη τοποθεσία στο διαδίκτυο για να παρέχει μια συγκεκριμένη λειτουργικότητα, θα έπρεπε να της επιτραπεί η πρόσβαση μόνο στην συγκεκριμένη τοποθεσία, αντί σε όλο το Ίντερνετ.

Στη μελέτη των Wei κα. (2012), μελετάται η εξέλιξη των αδειών και της χρήσης τους στο οικοσύστημα του Android από την έναρξη της κυκλοφορίας του το 2008. Μια βασική διαπίστωση είναι ότι το μοντέλο αδειών πρόσβασης του Android έχει γίνει πολύπλοκο και δύσκολο και για τους χρήστες και για τους σχεδιαστές των εφαρμογών να το καταλάβουν. Μια επιπρόσθετη παρατήρηση είναι ότι οι άδειες δεν γίνονται όλο και πιο λεπτομερείς και ξεκάθαρες και ότι σε γενικές γραμμές, ολόκληρη η πλατφόρμα του Android δεν πορεύεται σε μια προσέγγιση η οποία θα εμπλουτίσει την εμπιστευτικότητα και ιδιωτικότητα των προσωπικών δεδομένων από την πλευρά του χρήστη.

Ένα τεχνικό θέμα με αρνητικές επιπτώσεις στην αποτελεσματικότητα του μοντέλου ασφάλειας είναι ότι μερικές άδειες ομαδοποιούνται με τέτοιο τρόπο που

δυσχεραίνει την εύλογη συμφωνία μεταξύ χρηστών και εφαρμογών. Λιγότερο ευαίσθητα δεδομένα ομαδοποιούνται με κρίσιμες πληροφορίες προσωπικού χαρακτήρα. Για παράδειγμα, μια εφαρμογή ξυπνητηριού χρειάζεται να γνωρίζει πότε η συσκευή είναι εν μέσω κλήσης, ώστε να μην χτυπήσει και ενοχλήσει τη συνομιλία, καθώς επίσης και πότε η συσκευή είναι κλειστή, ώστε να την ενεργοποιήσει και να χτυπήσει. Αυτές οι λειτουργίες παρέχονται με την άδεια «READ_PHONE_STATE». Ωστόσο, η ίδια άδεια παρέχει πρόσβαση σε ευαίσθητα δεδομένα προσωπικού χαρακτήρα, όπως το IMEI[21] της συσκευής, το IMSI[22], το ICCID[23] κ.λπ., καθώς και σε αρχεία κλήσεων κ.α. Δηλαδή, μια οποιαδήποτε εφαρμογή ξυπνητηριού μπορεί να ξέρει το τηλέφωνο του χρήστη, τη χώρα, τον τηλεπικοινωνιακό του πάροχο, καθώς επίσης και όλους αυτούς που τον καλούν, τα στοιχεία των κλήσεων κ.α.

Παρόλο που η άδεια «READ_PHONE_STATE» είναι μια από τις πιο κρίσιμες από πλευράς ιδιωτικότητας, υπάρχει άλλο ένα τεχνικό θέμα που σχετίζεται με αυτή την άδεια. Για λόγους οπισθόδρομης συμβατότητας, οποιαδήποτε εφαρμογή που υποστηρίζει παλαιότερες εκδόσεις του Android, πρέπει να ζητάει αυτήν την άδεια επειδή στις πρώτες εκδόσεις του Android χορηγούταν από προεπιλογή στις εφαρμογές. Οι σχεδιαστές των εφαρμογών δεν έχουν άλλη επιλογή εάν επιθυμούν οι εφαρμογές τους να μπορούν να χρησιμοποιηθούν από παλαιότερες εκδόσεις του Android.

Κατ' αυτόν τον τρόπο, αρκετές εφαρμογές ζητούν αυτή την άδεια χωρίς ουσιαστικά να χρειάζονται κάποιο από τα προσωπικά δεδομένα που συλλέγονται μέσω αυτής. Αυτό αποτελεί μια πρακτική που παραβιάζει μια θεμελιώδη αρχή του ευρωπαϊκού νόμου για την προστασία των προσωπικών δεδομένων, την αρχή της αναλογικότητας, την οποία αναφέραμε στο Κεφάλαιο 2. Από τη μεριά των χρηστών είναι αδύνατο να διακρίνουν αν και πώς οι εφαρμογές θα χρησιμοποιήσουν τα δεδομένα που συλλέγονται νόμιμα από αυτή την άδεια, καθώς επίσης να αντιληφθούν και να εκτιμήσουν αν αυτά τα δεδομένα είναι απαραίτητα για να λειτουργήσει σωστά η εφαρμογή που τα ζητάει, ή αν θα χρησιμοποιηθούν για να εξυπηρετήσουν διαφημιστικούς σκοπούς για παράδειγμα.

Ένα άλλο ζήτημα είναι η πολυπλοκότητα των αδειών. Για παράδειγμα, στη μελέτη των Vidas κα. (2011), οι συγγραφείς απευθύνονται στην πολυπλοκότητα του μοντέλου των αδειών πρόσβασης και προτείνουν ένα βοηθητικό πρόγραμμα για να

[21] Το IMEI είναι το ακρωνύμιο των λέξεων International Mobile Equipment Identifier (διεθνή αναγνωριστικό αριθμό κινητής συσκευής) και συνοδεύει υποχρεωτικά κάθε συσκευή κινητής τηλεφωνίας (είναι η ταυτότητά της κάθε συσκευής).

[22] International Mobile Subscriber Identity, είναι το μοναδικό αναγνωριστικό συνδρομητή και δίνει πληροφορίες για την χώρα και τον τηλεπικοινωνιακό πάροχο.

[23] Το Integrated Circuit Card ID αποτελεί το σειριακό αριθμό της κάρτας SIM.

υποστηρίξουν τους προγραμματιστές των εφαρμογών στην εναρμόνιση των αιτημάτων αδειών πρόσβασης με τις ανάγκες των εφαρμογών τους.

Εν τέλει, θα πρέπει να υπογραμμιστούν δύο μειονεκτήματα του μοντέλου αδειών πρόσβασης των λειτουργικών συστημάτων των έξυπνων φορητών συσκευών, τα οποία δεν έχουν τονιστεί επαρκώς μέχρι σήμερα:

- Το πρώτο μειονέκτημα είναι η καταφανής αποτυχία του μοντέλου αδειών πρόσβασης που υπάρχει στο οικοσύστημα του Android να υποστηρίξει επαρκώς τα δικαιώματα των χρηστών, αναφορικά με την προστασία των προσωπικών τους δεδομένων. Οι έξυπνες φορητές συσκευές μεταφέρουν έναν τεράστιο όγκο (ευαίσθητων) προσωπικών δεδομένων των ιδιοκτητών τους. Στο παρόν πλαίσιο αδειοδότησης του Android, η εφαρμογή απλά ζητάει άδειες πρόσβασης σε δεδομένα, χωρίς να καθορίζει το σκοπό και τους όρους της πρόσβασης στα δεδομένα αυτά. Συνεπώς, τα θεμελιώδη δικαιώματα των χρηστών, όπως το δικαίωμα της ενημέρωσης για το σκοπό της πρόσβασης στα προσωπικά τους δεδομένα, απλά αγνοούνται από το οικοσύστημα των φορητών συσκευών και τις ισχύουσες πρακτικές της αγοράς.
- Το δεύτερο μειονέκτημα αφορά στο αν μια εφαρμογή έχει δικαίωμα να μεταδώσει τα προσωπικά δεδομένα εκτός της συσκευής. Προφανώς αυτή η άδεια αποτελεί ποιοτικό χαρακτηριστικό των όρων και των συνθηκών που αναφέρθηκαν παραπάνω, αλλά λόγω της μεγάλης του σημασίας αξίζει να αναφερθεί ξεχωριστά. Μια εφαρμογή που ζητάει προσωπικά δεδομένα από μια κινητή συσκευή διαφέρει από τις web ή desktop εφαρμογές, οι οποίες τρέχουν σε μια πλατφόρμα που ανήκει στον χρήστη. Επακριβέστερα, όταν μια εφαρμογή ζητάει πρόσβαση σε προσωπικά δεδομένα, θα πρέπει να δηλώνεται ξεκάθαρα αν αυτές οι πληροφορίες θα παραμείνουν μέσα στην συσκευή ή θα μεταφερθούν εκτός της συσκευής. Για παράδειγμα, αν μια εφαρμογή ζητάει πληροφορίες για την ηλικία και το φύλο του χρήστη απλά για να προσαρμόσει τη διεπαφή χρήστη στην αντίστοιχη ηλικιακή κλάση, τότε δεν υπάρχει λόγος να μεταφερθεί αυτή η πληροφορία εκτός της συσκευής, και συνεπώς, δεν απειλείται σοβαρά η ιδιωτικότητα του χρήστη. Αν όμως η εφαρμογή σχεδιάζει να μεταδώσει αυτά τα δεδομένα οπουδήποτε εκτός της συσκευής, τότε αυτό το γεγονός θα πρέπει να δηλώνεται σαφώς στο αίτημα της άδειας πρόσβασης.

3.4. Επιδράσεις στη Συμπεριφορά Χρηστών και Προγραμματιστών

Η βαθμιαία διάβρωση της ιδιωτικότητας, η οποία προκλήθηκε από τα ολοένα και περισσότερα αιτήματα αδειών πρόσβασης που ζητούν οι εφαρμογές κατά την αναβάθμισή τους, είχε ανεπιθύμητα αποτελέσματα στη συμπεριφορά των χρηστών σε σχέση με την ασφάλεια. Ο West (2008) απαρίθμησε μια σειρά ψυχολογικών χαρακτηριστικών που πηγάζουν από ενέργειες σχετικές με την ασφάλεια, καθώς επίσης η έλλειψη κινήτρων του χρήστη είναι ένα από τα σημαντικότερα χαρακτηριστικά που επιδεικνύουν οι χρήστες. Καθώς ο χρήστης μπορεί να είναι προκατειλημμένος στο να μην κάνει ενέργειες για την ενίσχυση της ιδιωτικότητάς του - σε αυτή την περίπτωση αναβαθμίσεις λογισμικού - είναι λογικό να περιμένει κανείς πως αυτές οι εκφυλιστικές ως προς την ιδιωτικότητα αναβαθμίσεις των εφαρμογών ενισχύουν την αδρανή στάση του χρήστη, ή ακόμα και του παρέχουν άλλοθι για να μην προβεί σε αυτές τις αναβαθμίσεις. Συμπερασματικά, η τάση των εφαρμογών να ζητούν περισσότερα προσωπικά δεδομένα από αυτά που χρειάζονται μπορεί να καταλήξει σε δυσάρεστες καταστάσεις. Για παράδειγμα, μπορεί να οδηγήσει στη σύγκλιση ή ακόμα και τον εκφυλισμό της συμπεριφοράς των χρηστών που είναι ενήμεροι για τα θέματα ιδιωτικότητας και αυτών που ασυνείδητα δίνουν τη συγκατάθεσή τους για να γίνουν διαθέσιμα τα προσωπικά τους δεδομένα σε τρίτους.

Η επιλογή των χρηστών να μην κάνουν τις αναβαθμίσεις λογισμικού που ζητούν οι εφαρμογές δύναται να αποτελέσει κίνδυνο όχι μόνο για τα προσωπικά δεδομένα των ίδιων των χρηστών, αλλά και για δεδομένα που είναι διαθέσιμα σε ένα εταιρικό δίκτυο. Η νέα τάση Bring-Your-Own-Device (BYOD), η οποία εξελίχθηκε τα τελευταία χρόνια στο σύγχρονο επιχειρηματικό περιβάλλον λόγω της ανάγκης για φορητότητα, απαιτεί μια ολιστική προσέγγιση όσον αφορά την ασφάλεια και τη διαχείριση των πληροφοριών που ανταλλάσσονται πάνω από ένα εταιρικό δίκτυο. Με βάση αυτή την τάση, οι φορητές συσκευές και τα δεδομένα στα οποία έχουν πρόσβαση, οδηγούν στην παραγωγικότητα και την αποτελεσματικότητα των στελεχών. Τα στελέχη χρησιμοποιούν οποιεσδήποτε εφαρμογές χρειάζονται για συγχρονισμό και διαμοιρασμό αρχείων, κράτηση σημειώσεων, επικοινωνία και πολλά ακόμη με στόχο τη μεγιστοποίηση απόδοσης στην εργασία. Επιπλέον, τα στελέχη έχουν τη δυνατότητα να χρησιμοποιούν τις ίδιες φορητές συσκευές και εκτός του προστατευόμενου (με τοίχος προστασίας) εσωτερικού δικτύου της εταιρίας, εκεί όπου περιμετρικός έλεγχος ασφάλειας δεν εφαρμόζεται, ενώ παράλληλα η ποικιλομορφία των σημερινών φορητών συσκευών, μπορεί να αποτελέσει πονοκέφαλο για τους υπεύθυνους ασφάλειας της εταιρίας. Ωστόσο, αν η φορητή συσκευή που χρησιμοποιεί κάποιο στέλεχος δεν είναι ιδιοκτησία της εταιρίας αλλά του χρήστη, υπάρχει ο κίνδυνος να εισαχθεί ακόμα και κακόβουλο λογισμικό στο εταιρικό δίκτυο, εφόσον ο διαχειριστής του δικτύου δεν θα έχει

επαρκή έλεγχο στη συγκεκριμένη συσκευή. Συμπερασματικά, οι πόροι που διαμοιράζονται είναι εταιρικοί και η ανάγκη για προστασία των εταιρικών δεδομένων μπορεί να είναι καθοριστικής σημασίας για την ίδια την εταιρία, καθώς μια και μόνο συσκευή αρκεί για να προκαλέσει ένα περιστατικό ασφάλειας σε όλο το εταιρικό δίκτυο.

Επομένως, αν ο πάροχος της εφαρμογής επιθυμεί να συλλέγει και να επεξεργάζεται τα προσωπικά δεδομένα των χρηστών της, μπορεί να επηρεάσει ακόμα και την ασφάλεια της εταιρίας για την οποία εργάζεται ο χρήστης. Εξάλλου, η αυξημένη πολυπλοκότητα του μοντέλου αδειών πρόσβασης με βάση το οποίο οι εφαρμογές οργανώνονται και λειτουργούν, μπορεί να προκαλέσει ακούσια ή ηθελημένα κάποιο περιστατικό ασφάλειας. Οι σχεδιαστές των εφαρμογών δεν είναι πάντα πλήρως καταρτισμένοι για το σχεδιασμό των εφαρμογών ή μπορεί να μην συνειδητοποιούν την ανάγκη της εφαρμογής της αρχής του ελαχίστου προνομίου (least privilege principle)[24]. Αντιθέτως, προτιμούν να συμπεριλάβουν περισσότερες άδειες από αυτές που πραγματικά χρειάζονται για να αποφύγουν χρονοβόρα αντιμετώπιση προβλημάτων και εντοπισμό σφαλμάτων στην περίπτωση που η εφαρμογή παρουσιάζει προβληματική λειτουργικότητα λόγω των περιοριστικών πολιτικών στις άδειες πρόσβασης. Επιπλέον, σε έρευνα που πραγματοποιήθηκε σε 141.372 εφαρμογές, η πλειοψηφία των σχεδιαστών εφαρμογών για smartphones δεν χρησιμοποιούν τις σωστές άδειες και είτε υπερκαλύπτουν είτε δεν ανταποκρίνονται στις απαιτήσεις ασφάλειας των εφαρμογών τους (Johnson, 2012).

Σε αυτό το σημείο πρέπει να τονιστεί ότι η παραχώρηση πρόσβασης στα προσωπικά δεδομένα των χρηστών φορητών συσκευών δεν είναι εξ ορισμού ούτε προβληματική ούτε παράνομη. Αντιθέτως, οι λειτουργικότητες πολλών εφαρμογών απαιτούν πρόσβαση σε ευαίσθητα προσωπικά δεδομένα χρηστών. Εξάλλου, ακόμα και οι χρήστες που έχουν επίγνωση της ιδιωτικότητάς τους εκτιμούν την αξία των εφαρμογών και αποδέχονται την εμπορευματοποίηση των προσωπικών τους δεδομένων ως το τίμημα που πρέπει να πληρώσουν σε αντάλλαγμα για τη δωρεάν χρήση των εφαρμογών αυτών - οι δωρεάν εφαρμογές συνήθως ζητούν περισσότερες άδειες πρόσβασης από ότι οι εφαρμογές επί πληρωμή (Pearce κα., 2012). Ωστόσο, οποιαδήποτε δημοσιοποίηση προσωπικών δεδομένων χρηστών φορητών συσκευών πρέπει να συμμορφώνεται με τους ευρωπαϊκούς κ.λπ. κανονισμούς για την προστασία των προσωπικών δεδομένων καθώς επίσης και οι πρακτικές που εφαρμόζονται από τους παρόχους των λειτουργικών συστημάτων και των εφαρμογών οφείλουν να προστατεύουν αποτελεσματικά τα δικαιώματα των χρηστών σε σχέση με το λόγο και τον τρόπο χρήσης των προσωπικών τους δεδομένων.

[24] Στο πλαίσιο αυτής της αρχής απαιτείται να διασφαλιστεί πως οι εφαρμογές λαμβάνουν το ελάχιστο δυνατό σύνολο αδειών χρήσης που απαιτείται για την εκτέλεση κάθε διεργασίας που καλείται από αυτήν.

4. Ταξινόμηση Δεδομένων σε Φορητές Συσκευές

Κάθε smartphone αποτελείται από ένα πλήθος στοιχείων και δομών, τα οποία, όταν συνδυαστούν, παρέχουν μια σειρά λειτουργικοτήτων στο χρήστη. Αυτά τα δομικά στοιχεία είναι υλικοί πόροι, υπηρεσίες δικτύου, πληροφοριακά δεδομένα και υπηρεσίες εφαρμογών και αποτελούν το ενεργητικό του smartphone. Αυτά τα δομικά στοιχεία μπορούν να κατηγοριοποιηθούν σε τέσσερις ξεχωριστούς τύπους (Theocharidou κα., 2012):

- συσκευή,
- συνδεσιμότητα,
- εφαρμογές και
- δεδομένα.

Στο δομικό στοιχείο «Συσκευή» ανήκουν όλα τα υλικά συστατικά της συσκευής. Αυτά είναι η φυσική συσκευή και ο πόροι της, όπως επεξεργαστής, μνήμη, σκληρός δίσκος, αισθητήρες, οθόνη, μπαταρία, κάμερα κ.λπ..

Το δομικό στοιχείο «Συνδεσιμότητα» αναφέρεται σε όλες τις τεχνολογίες που χρησιμοποιούνται για να παρέχουν τηλεπικοινωνιακές υπηρεσίες κινητού δικτύου. Αυτές είναι:

- το παγκόσμιο σύστημα για τηλεπικοινωνιακές υπηρεσίες,
- οι ασύρματες υπηρεσίες δικτύων προσωπικής περιοχής (Wireless Personal Area Networks),
- οι ασύρματες υπηρεσίες τοπικού και μητροπολιτικού δικτύου,
- οι υπηρεσίες δικτύου κυψέλης και
- οι υπηρεσίες επικοινωνίας κοντινού πεδίου (Near Field Communication).

Το δομικό στοιχείο των «Εφαρμογών» αναφέρεται σε όλες τις εφαρμογές που υπάρχουν εγκατεστημένες στη φορητή συσκευή. Αυτές οι εφαρμογές μπορεί να είναι είτε προεγκατεστημένες από τον κατασκευαστή του λειτουργικού συστήματος ή τον πάροχο τηλεπικοινωνιακών υπηρεσιών, είτε μπορεί να είναι εφαρμογές τρίτων που εγκατέστησε ο ίδιος ο χρήστης.

Τέλος, το δομικό στοιχείο των «Δεδομένων» είναι όλες οι πληροφορίες που αποθηκεύονται και χρησιμοποιούνται σε μια φορητή συσκευή. Αυτά τα δεδομένα μπορούν να είναι επαφές, οικονομικά στοιχεία, ιστορικό κλήσεων, πληροφορίες τοποθεσίας, ιστορικό χρήσης, εικόνες κ.λπ., και μπορούν να κατηγοριοποιηθούν περαιτέρω σε δεδομένα προσωπικά, οικονομικά, επιχειρησιακά, ιατρικά, συνδεσιμότητας ή αυθεντικοποίησης.

Ανάλογα με την πηγή τους, τα δεδομένα μπορούν να κατηγοριοποιηθούν ως εξής (Mylonas, 2008):

- Δεδομένα μηνυμάτων: δεδομένα που προέρχονται από τις υπηρεσίες μηνυμάτων του παρόχου (SMS, EMS, MMS), άμεσα μηνύματα και μηνύματα ηλεκτρονικού ταχυδρομείου. Αυτή η κατηγορία περιλαμβάνει αρχεία καταγραφής μηνυμάτων που περιλαμβάνουν τον αποστολέα, τον αποδέκτη, την ώρα και ημερομηνία της παράδοσης, επισυναπτόμενα αρχεία κ.ο.κ.
- Δεδομένα συσκευής: όλα τα δεδομένα της συσκευής και του λειτουργικού συστήματος που δεν σχετίζονται με εφαρμογές τρίτων (επαφές, φωτογραφίες, IMEI, Wi-Fi MAC Address, το αναγνωριστικό της συσκευής κ.α.)
- Δεδομένα της κάρτας (U)SIM: Αυτά τα δεδομένα περιλαμβάνουν συγκεκριμένες πληροφορίες για να αναγνωρίζεται μοναδικά ο χρήστης από τον τηλεπικοινωνιακό πάροχο, όπως το μοναδικό αναγνωριστικό συνδρομητή (IMSI), κομμάτι του οποίου αποτελεί ο αριθμός συνδρομητή (MSIN), και το σειριακό αριθμό της κάρτας SIM (ICCID). Η κάρτα SIM περιλαμβάνει τους μηχανισμούς για τη ροή εργασιών του λειτουργικού συστήματος, την αυθεντικοποίηση του χρήστη, τον αλγόριθμο για την κρυπτογράφηση των δεδομένων. Το σύστημα αρχείων είναι στην μόνιμη (persistent) μνήμη και μπορεί να αποθηκεύσει επαφές, μηνύματα κειμένου και ρυθμίσεις υπηρεσιών δικτύου.
- Δεδομένα εφαρμογών: όλα τα δεδομένα που είναι προσπελάσιμα από τις εφαρμογές και είναι απαραίτητα για την εκτέλεσή τους. Αυτά μπορούν να είναι αρχεία που περιέχουν τις ρυθμίσεις τους, αρχεία καταγραφών ή προσωρινά δεδομένα.
- Δεδομένα ιστορικού χρήσης: όλα τα αρχεία καταγραφής σχετίζονται με τη χρήση της φορητής συσκευής. Αυτά είναι τα αρχεία καταγραφής κλήσεων, το ιστορικό περιήγησης στο ίντερνετ, το ιστορικό σύνδεσης σε δίκτυα και το αρχείο καταγραφής συμβάντων του λειτουργικού συστήματος.
- Δεδομένα αισθητήρων: όλα τα δεδομένα που σχετίζονται με τους αισθητήρες του smartphone. Αυτά είναι τα δεδομένα τοποθεσίας, τα δεδομένα θερμοκρασίας, τα δεδομένα κατεύθυνσης, τα δεδομένα δόνησης κ.α. Οι πιο σημαντικοί αισθητήρες που υπάρχουν σε σχεδόν όλα τα smartphones είναι η κάμερα, το μικρόφωνο, το GPS, η πυξίδα και το επιταχυνσιόμετρο.
- Δεδομένα που εισάγει ο χρήστης: αυτά τα δεδομένα παράγονται από την αλληλεπίδραση του χρήστη με το smartphone. Για παράδειγμα, σε αυτή την κατηγορία ανήκει η πληκτρολόγηση, τα πατήματα κουμπιών,

οι κινήσεις και χειρονομίες του χρήστη. Ως χειρονομίες μπορούν να χαρακτηριστούν τα συρσίματα, τα χτυπήματα, τα αγγίγματα, τα διπλά χτυπήματα, οι επαφές και τα κουνήματα και οποιαδήποτε γενικά αλληλεπίδραση μπορεί να έχει ένας χρήστης με το smartphone.

Οι παραπάνω πηγές δεδομένων μπορούν να διαχειριστούν πολλά είδη πληροφοριών, όπως προσωπικές, επιχειρησιακές, αυθεντικοποίησης, οικονομικές, ιατρικές και συνδεσιμότητας. Ανάλογα με την κατηγορία στην οποία ανήκουν τα δεδομένα, κάποια από τα δεδομένα είναι πιο κρίσιμα από άλλα. Για παράδειγμα, οι εφαρμογές μπορούν να διαχειρίζονται όλους του τύπους των δεδομένων, συμπεριλαμβανομένου ευαίσθητων δεδομένων, όπως τα ιατρικά. Σε αυτό το σημείο αξίζει αν σημειωθεί πως η πρόσβαση στις κατατμήσεις του συστήματος (system partitions) είναι περιορισμένη από προεπιλογή στο λειτουργικό σύστημα Android. Αυτό συμβαίνει κυρίως για να προστατέψει κακόβουλες ή κακώς σχεδιασμένες εφαρμογές να επηρεάσουν την σταθερότητα και αξιοπιστία του λειτουργικού συστήματος. Η πρόσβαση στις κατατμήσεις του συστήματος επιτυγχάνεται με ξεκλείδωμα της συσκευής (rooting[25]).

Διαφορετικές οντότητες μπορούν να έχουν πρόσβαση σε διαφορετικά δεδομένα στις φορητές συσκευές. Μια λίστα από αυτές τις οντότητες οι οποίες μπορούν ή/και έχουν πρόσβαση σε πληροφορίες του χρήστη στα smartphones είναι η εξής:

(1) Φορητή συσκευή: μπορεί να έχει πρόσβαση στα δεδομένα της συσκευής και των αισθητήρων.
(2) Λειτουργικό σύστημα: μπορεί να έχει πρόσβαση στα δεδομένα μηνυμάτων, συσκευής, εφαρμογών, ιστορικού χρήσης, αισθητήρων, σε δεδομένα που εισάγει ο χρήστης και σε κάποια από τα δεδομένα της κάρτας SIM.
(3) Εφαρμογές: η λειτουργικότητα της εφαρμογής καθορίζει ποια δεδομένα θα είναι προσπελάσιμα από την εφαρμογή. Σύμφωνα με τη λειτουργικότητα, εφαρμόζεται μια γενική κατηγοριοποίηση. Αυτές οι εφαρμογές μπορεί να είναι:
    - Παιχνίδια – έχουν πρόσβαση σε δεδομένα αισθητήρων και σε δεδομένα που εισάγει ο χρήστης.
    - Περιεχομένου και πολυμέσων (μουσική, φωτογραφίες και βίντεο, ηχογράφηση, βιβλία κ.α.) – μπορούν να έχουν πρόσβαση σε δεδομένα συσκευής, αισθητήρων και σε δεδομένα που εισάγει ο χρήστης.

[25] Με τον όρο «rooting» στο Android, περιγράφεται η διαδικασία η οποία έχει ως σκοπό να επιτρέψει στο χρήστη να επεμβαίνει σε όλα τα partitions της συσκευής και όχι μόνο σε αυτό του χρήστη, το οποίο και είναι επιτρεπόμενο εξ' αρχής. Μέσω του «rooting» ο χρήστης έχει πλήρη έλεγχο στις ρυθμίσεις και τα χαρακτηριστικά της συσκευής. Για να αποκτήσει πρόσβαση στα υπόλοιπα partitions πρέπει να ξεκλειδώσει τον bootloader. Έτσι μπορεί να αντικαταστήσει την κονσόλα recovery που βρίσκεται στο ομώνυμο partition και, μέσω αυτής, να εγκαταστήσει την εφαρμογή superuser η οποία διαχειρίζεται τα δικαιώματα υπερχρήστη (root) στο λειτουργικό.

- Βασικές λειτουργίες και εργαλεία (εργαλεία τηλεφώνου, χάρτες, πλοήγηση, εξατομίκευση) – μπορούν να έχουν πρόσβαση σε δεδομένα αισθητήρων.
- Κοινωνική δικτύωση, επικοινωνία και τρόπος ζωής (VoIP τηλεφωνία, ιστολόγια, άμεσα μηνύματα, κοινωνικά δίκτυα, αγορές, ειδήσεις, δίκτυα διαφήμισης, αθλήματα, διασκέδαση, υγεία) – μπορούν να έχουν πρόσβαση σε δεδομένα μηνυμάτων, συσκευής, κάποια από τα U(SIM) δεδομένα, δεδομένα ιστορικού χρήσης και δεδομένα που εισάγει ο χρήστης.
- Προσωπική παραγωγικότητα, εκπαίδευση και επιχειρηματικότητα (τραπεζικές εφαρμογές, μετάφραση, εφαρμογές γραφείου, ημερολόγιο κ.α.) – μπορούν να έχουν πρόσβαση σε δεδομένα ιστορικού χρήσης και αισθητήρων.

Οι εφαρμογές περιήγησης στο διαδίκτυο συνδυάζουν χαρακτηριστικά και της κατηγορίας «Βασικών λειτουργιών και εργαλείων» και «Προσωπικής παραγωγικότητας, εκπαίδευσης και επιχειρηματικότητας». Αυτές οι υβριδικές λειτουργικότητες εφαρμόζονται γιατί ακόμα και αν έχει το πιο δημοφιλές λειτουργικό σύστημα προεγκατεστημένη την εφαρμογή για την περιήγηση στο διαδίκτυο, ο χρήστης μπορεί να εγκαταστήσει όποια άλλη επιθυμεί. Αυτές οι λειτουργικότητες επιτρέπουν την πρόσβαση σε αρχεία ιστορικού περιήγησης, σε GPS δεδομένα και σε δεδομένα εκτέλεσης εφαρμογών. Όλες οι εφαρμογές έχουν πρόσβαση στα δεδομένα που σχετίζονται με τη χρήση τους, όπως για παράδειγμα αρχεία καταγραφής συμβάντων και αρχεία ρυθμίσεων, αλλά δεν μπορούν να προσπελάσουν δεδομένα άλλων εφαρμογών.

(4) Τηλεπικοινωνιακός πάροχος: Οι πάροχοι των υπηρεσιών συλλέγουν εισερχόμενες/εξερχόμενες κλήσεις, μηνύματα, δεδομένα τοποθεσίας και δεδομένα σχετικά με τη χρήση του ίντερνετ (ελέγχεται η συχνότητα με την οποία τσεκάρουν οι χρήστες το email τους, η συχνότητα και διάρκεια της πρόσβασης στο ίντερνετ κ.α.). Μπορούν να έχουν πρόσβαση σε δεδομένα μηνυμάτων, στα δεδομένα της κάρτας U(SIM), στο ιστορικό χρήσης και σε δεδομένα αισθητήρων.

Στον πίνακα 3 παρουσιάζεται η πρόσβαση των οντοτήτων στους διάφορους τύπους δεδομένων.

Πίνακας 3. Ταξινόμηση προσωπικών δεδομένων ανάλογα με τις οντότητες που μπορούν ή/και έχον πρόσβαση στα δεδομένα[26]

Πηγές δεδομένων / *Οντότητες*	*Μηνύματα*	*Συσκευή*	*(U)SIM Κάρτα*	*Εφαρμογές*	*Ιστορικό Χρήσης*	*Αισθητήρες*	*Εισόδου Χρήστη*
Φορητή Συσκευή		✓				✓	
Λειτουργικό Σύστημα	✓	✓	~	✓	✓	✓	✓
Τύπος Εφαρμογής A. Παιχνίδια				*		✓	✓
B. Περιεχόμενο και πολυμέσα		✓		*		✓	✓
C. Βασικές λειτουργίες & εργαλεία			~	*		✓	
D. Κοινωνική δικτύωση, επικοινωνία & τρόπος ζωής	✓	✓	~	*	✓	✓	✓
E. Προσωπική παραγωγικότητα, εκπαίδευση & επιχειρηματικότητα				*	✓	✓	
Τηλεπικοινωνιακός Πάροχος	✓		✓		✓	✓	

[26] Το ✓ απεικονίζει πρόσβαση στα δεδομένα, το ~ απεικονίζει μερική πρόσβαση, το * απεικονίζει πρόσβαση μόνο στα δεδομένα που σχετίζονται με τη λειτουργία των εφαρμογών αυτών)

5. Play Store Proprietary API

5.1.Μεθοδολογία

Για τις ανάγκες τις παρούσας έρευνας σχεδιάστηκε μια βάση δεδομένων με σκοπό την εξαγωγή συμπερασμάτων σχετικά με την χρήση των αδειών προσπέλασης του μοντέλου του Android από τις εφαρμογές[27]. Η βάση δεδομένων περιέχει στοιχεία από περισσότερες από 15.000 εφαρμογές ανά χώρα (22.000 μοναδικές εφαρμογές συνολικά), οι οποίες διατίθενται στους χρήστες μέσω του Play Store σε Ελλάδα και Η.Π.Α.

Για να γίνει δυνατή η συλλογή των απαραίτητων στοιχείων που απαιτούνταν για τη βάση δεδομένων, σχεδιάστηκε και υλοποιήθηκε ένα proprietary API, το οποίο κάνει τη συλλογή των απαιτούμενων δεδομένων με επαναλαμβανόμενα POST Requests στην επίσημη σελίδα του Play Store και στο τέλος εξάγει τα αποτελέσματα σε φύλλο εργασίας excel. Τα απαιτούμενα δεδομένα για τη βάση δεδομένων είναι τα εξής:

- αναγνωριστικό εφαρμογής,
- κόστος εφαρμογής,
- άδειες πρόσβασης που ζητάει η εφαρμογή.

Τα υπάρχοντα APIs που κυκλοφορούν στο διαδίκτυο κρίθηκαν ακατάλληλα για την επιθυμητή διαδικασία καθώς είτε είναι παλιά και δεν έχουν συντηρηθεί για να υποστηρίζουν τις αλλαγές που εισήγαγε πρόσφατα η Google στη σελίδα του Play Store, είτε δεν υποστηρίζουν τη συλλογή των αδειών πρόσβασης των εφαρμογών. Ως αποτέλεσμα, η υλοποίηση ενός νέου proprietary μηχανισμού, ο οποίος θα είχε την επιθυμητή λειτουργικότητα και θα εξήγαγε τα επιθυμητά δεδομένα κρίθηκε απαραίτητη.

Επιπλέον, στην επίσημη σελίδα του Play Store υπάρχουν διαθέσιμες Android εφαρμογές οι οποίες ενδείκνυνται για μια τέτοια διαδικασία, μπορούν δηλαδή να φέρουν όλες τις άδειες που χρειάζεται κάποια συγκεκριμένη εφαρμογή. Η πληροφορία όμως με αυτό τον τρόπο δεν είναι εύκολα διαχειρίσιμη, καθώς κάθε φορά κατεβάζουν τις άδειες για μια και μόνο εφαρμογή και θα απαιτούσε να γίνει αυτή η διαδικασία αρκετές χιλιάδες φορές για να εξαχθούν οι άδειες από χιλιάδες εφαρμογές. Επιπλέον, οι εφαρμογές αυτές θα κατέβαζαν τις πληροφορίες που θα ήταν διαθέσιμες για τη χώρα που έχει δηλώσει ο χρήστης ότι ανήκει, άρα

[27] Πληροφορίες για το προγραμματισμό του API αναφέρονται στο Παράρτημα Β της παρούσας εργασίας.

πληροφορίες για την ίδια εφαρμογή σε διαφορετική χώρα θα ήταν αδύνατο να παρθούν. Αξίζει επίσης να σημειωθεί ότι δεν θα απαιτούνταν επιπλέον προσπάθεια για να εξαχθεί αυτή η πληροφορία από την εφαρμογή σε βάση δεδομένων. Όπως αποδεικνύεται λοιπόν, ο καταλληλότερος και αποδοτικότερος τρόπος να ανασυρθούν αυτές οι πληροφορίες ήταν να δημιουργηθεί εκ νέου ένα API, το οποίο θα υποστήριζε όλες τις παραπάνω λειτουργικότητες, ενώ ταυτόχρονα θα ελάττωνε το χρόνο και το υπολογιστικό κόστος που απαιτούνταν.

Η επεξεργασία των δεδομένων αυτών καταλήγει στη δημιουργία πινάκων με στατιστικά δεδομένα για να υποστηρίξουν τη διεξαγωγή συμπερασμάτων. Επιπλέον, στα δεδομένα αυτά εφαρμόστηκε και μια μελέτη επικινδυνότητας για την εξαγωγή επιπλέον χρήσιμων συμπερασμάτων.

5.2. Εργαλεία

Για το σχεδιασμό και την υλοποίηση του Play Store proprietary API χρησιμοποιήθηκαν τα ακόλουθα εργαλεία:

- Το eclipse, ένα ολοκληρωμένο περιβάλλον ανάπτυξης (IDE), το οποίο περιέχει ένα χώρο εργασίας (workspace) και ένα επεκτάσιμο σύστημα plugins για την προσαρμογή του περιβάλλοντος. Μπορεί να χρησιμοποιηθεί για την ανάπτυξη εφαρμογών σε πολλές γλώσσες προγραμματισμού με τη χρήση plugins.
- Η Java, η XML και η JSON ως γλώσσες προγραμματισμού.
- Το Microsoft Excel για τη δημιουργία πινάκων, την ανάλυση των δεδομένων και τη δημιουργία γραφημάτων.

Ως είσοδο το API δέχεται τα μοναδικά αναγνωριστικά των εφαρμογών που θέλουμε να κατεβάσουμε τις πληροφορίες και ως έξοδο παίρνουμε τις άδειες που χρησιμοποιούν και το κόστος τους.

5.3. Δείγμα

Από το σύνολο των εφαρμογών που είναι διαθέσιμες στο Play Store επιλέχθηκαν οι 600 πιο δημοφιλείς ανά κατηγορία και τιμή (οι 300 πιο δημοφιλείς δωρεάν και οι 300 πιο δημοφιλείς που έχουν κάποιο αντίτιμο).

Στο σημείο αυτό αξίζει να σημειωθεί πως το Play Store δίνει πληροφορίες για τις πιο δημοφιλείς εφαρμογές με βάση τη χώρα που έχει δηλώσει ο χρήστης στο προφίλ του. Αν δεν δηλωθεί χώρα προέλευσης, τότε δεν προβάλλονται καθόλου

στις διαθέσιμες εφαρμογές οι εφαρμογές επί πληρωμή[28]. Για το λόγο αυτό ακολουθήθηκαν δυο διαφορετικές προσεγγίσεις:

- συλλογή των δημοφιλέστερων εφαρμογών για την Ελλάδα και
- συλλογή των δημοφιλέστερων εφαρμογών για τις Η.Π.Α. (μέσω της χρήσης proxy).

Ως εκ τούτου, τα στατιστικά αποτελέσματα εξήχθησαν εις διπλούν, και η ίδια ανάλυση διεξάχθηκε δύο φορές, μια για κάθε χώρα.

Πίνακας 4. Συνοπτικά στοιχεία για τις εφαρμογές ανάλογα τη χώρα

	Εφαρμογές	**Μ.Ο. Τιμών**	**Μ.Ο. Αδειών**	**Κατηγορίες**
Η.Π.Α.	14,314	$ 3.41	5.14	28
Ελλάδα	14,892	€ 3.54	4.12	28
Συνολικά[29]	21,933	~	4.53	28

Μέσος όρος τιμής δεν μπορεί να υπολογιστεί για δύο διαφορετικές χώρες επειδή είναι δυνατό σε δύο διαφορετικές χώρες μια εφαρμογή να έχει διαφορετική τιμή. Για παράδειγμα η εφαρμογή «Minecraft: Pocket Edition» έχει €6,99 στην Ελλάδα, ενώ στις Η.Π.Α. έχει $6,99 αλλά λόγω ισοτιμίας νομισμάτων δεν αντιστοιχεί στο ίδιο ποσό.

Λόγω της ισοτιμίας μπορούμε να υπολογίσουμε το μέσο όρο τιμής των εφαρμογών που είναι διαθέσιμες στις Η.Π.Α. με βάση τη σημερινή ισοτιμία νομισμάτων ($1 = €0.915). Σε επόμενους πίνακες η μετατροπή έχει γίνει για να διευκολυνθεί η σύγκριση τιμών.

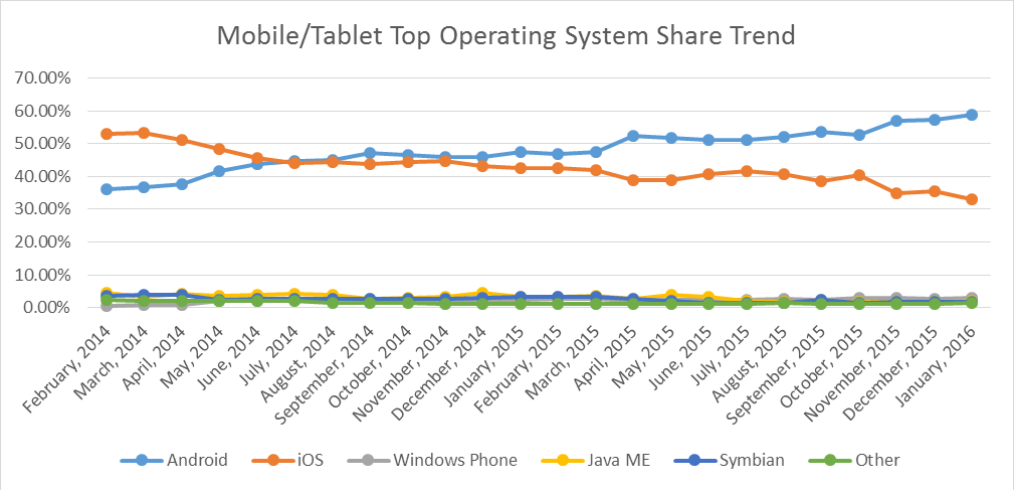
[28] Για να μην υπάρχουν δεδομένα χώρας προέλευσης του χρήστη χρησιμοποιήθηκε ο TOR Browser, αλλά οι μόνες εφαρμογές που ήταν διαθέσιμες ήταν οι εφαρμογές που ήταν δωρεάν. Για τις ανάγκες της παρούσας εργασίας οι εφαρμογές επί πληρωμή χρειάζονται οπωσδήποτε για ανάλυση, οπότε αυτή η προσέγγιση απορρίφθηκε.

[29] Ο συνολικός αριθμός των εφαρμογών που μελετήθηκαν δεν είναι ίσος με το άθροισμα των εφαρμογών των Η.Π.Α. και της Ελλάδας καθώς έχουν αφαιρεθεί οι διπλοεγγραφές.

6. Παρουσίαση Στατιστικών Δεδομένων

6.1. Στατιστικά για τη Χρήση του Android

Με βάση τα τελευταία στοιχεία για το μερίδιο αγοράς του Android στην παγκόσμια αγορά (NetMarketShare, 2016), το Android κυριαρχεί στο χώρο των λειτουργικών συστημάτων για φορητές έξυπνες συσκευές. Στη δεύτερη θέση έρχεται το iOS της Apple, ενώ τα Windows Phone, Java ME και Symbian συνολικά καταλαμβάνουν λιγότερο από το 10% της αγοράς λειτουργικών συστημάτων για κινητά τηλέφωνα.

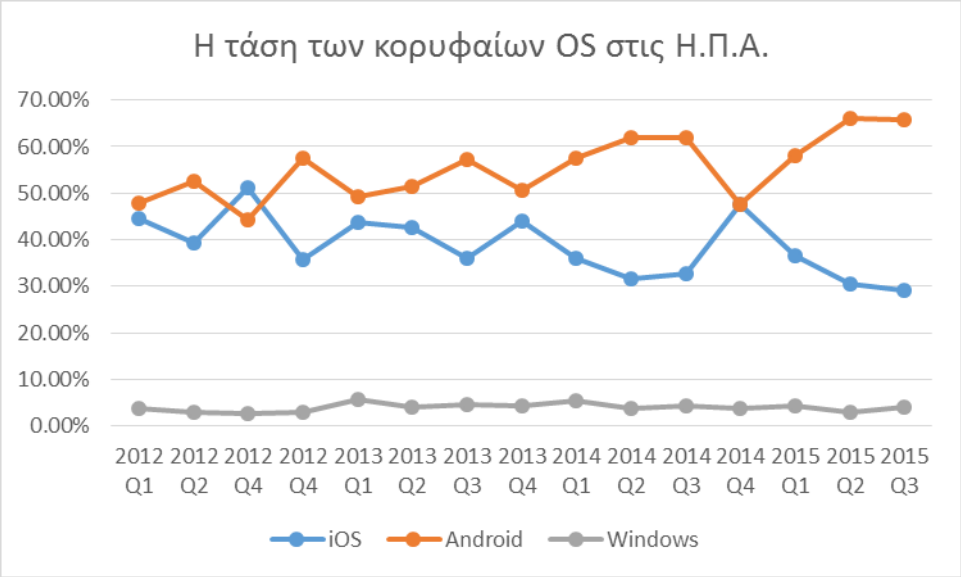


Εικόνα 1. Η τάση των κορυφαίων λειτουργικών συστημάτων για έξυπνες φορητές συσκευές σε παγκόσμιο επίπεδο

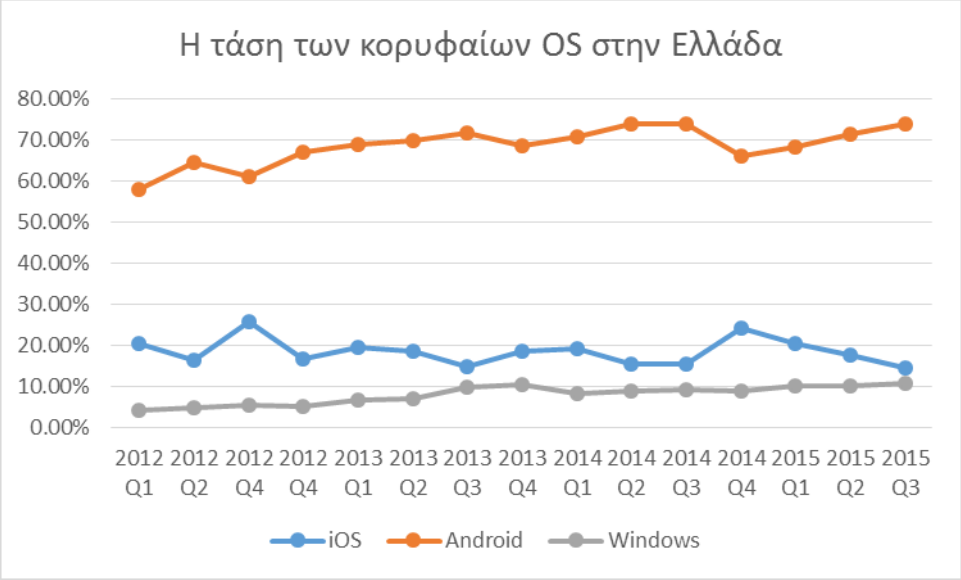
Η μεγάλη αύξηση της δημοτικότητας του Android στην παγκόσμια αγορά οφείλεται εκτός των άλλων και λόγω της χρήσης του στα smartphones και tablets των εταιρειών Samsung, Huawei, Xiaomi, Lenovo και ZTE, τα οποία έκαναν το Android κυρίαρχο της αγοράς. Οι κατασκευαστές αυτών των συσκευών κατέχουν τεράστιο μερίδιο αγοράς, καθώς εκτός από τις αναβαθμισμένες λειτουργικότητες που παρέχουν έχουν είναι και πιο προσιτά σε τιμές από τα iPhone. Από την άλλη, η δημοτικότητά του προσελκύει επίσης πολλούς προγραμματιστές κακόβουλων εφαρμογών.

Στις Η.Π.Α. μέχρι το τέταρτο τρίμηνο του 2013 οι καμπύλες δημοτικότητας των Android και iOS συνέκλιναν σημαντικά, μετά αυξήθηκε η δημοτικότητα του Android μέχρι το τέταρτο τρίμηνο του 2014, οπότε και συνέκλινε και πάλι η δημοτικότητά

τους. Αυτές οι συγκλήσεις δικαιολογούνται λόγω τη κυκλοφορίας των νέων iPhone στην αγορά.



Εικόνα 2. Η τάση των κορυφαίων λειτουργικών συστημάτων για έξυπνες φορητές συσκευές στις Η.Π.Α.

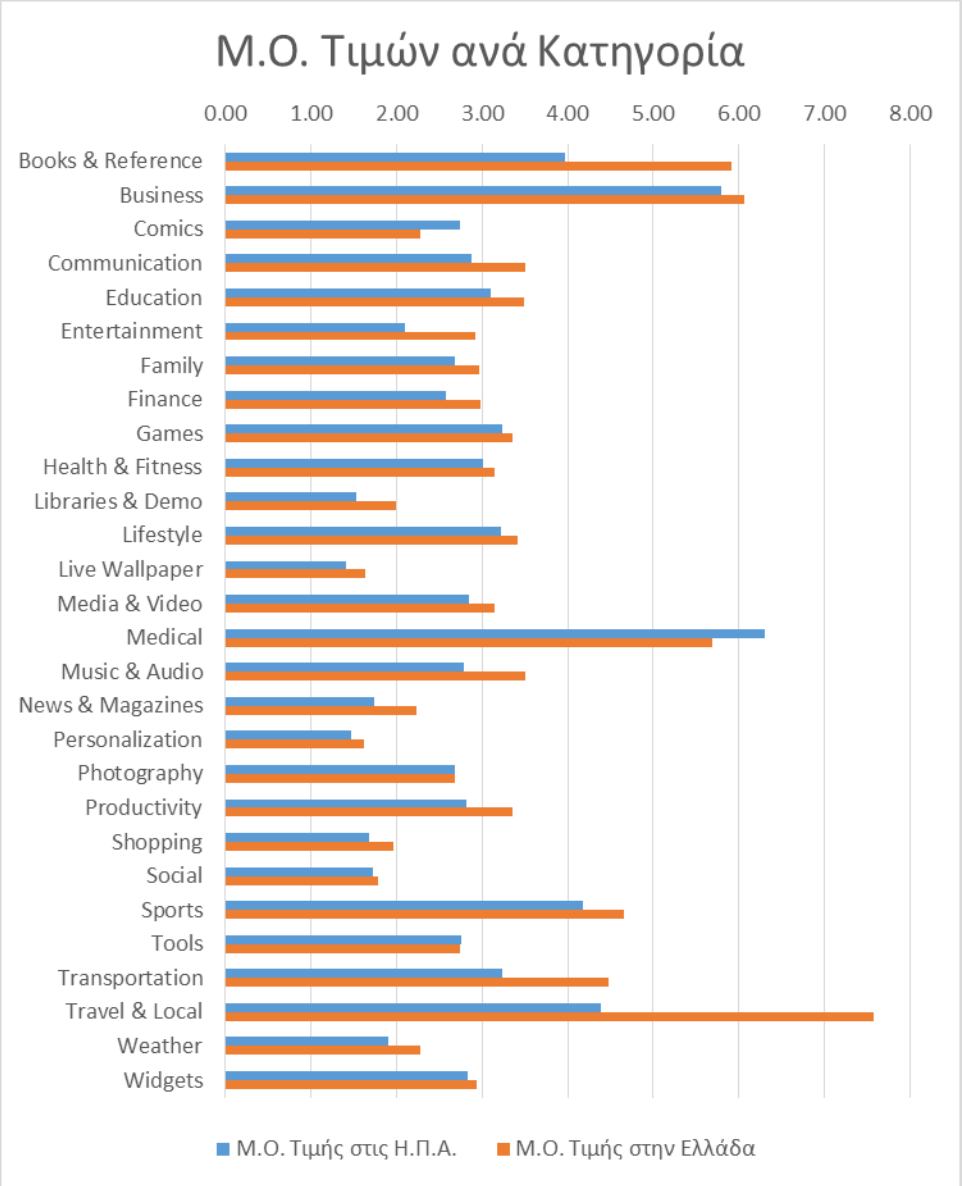


Εικόνα 3. Η τάση των κορυφαίων λειτουργικών συστημάτων για έξυπνες φορητές συσκευές στην Ευρώπη[30]

[30] Στοιχεία από πέντε χώρες: Γερμανία, Ηνωμένο Βασίλειο, Ισπανία, Γαλλία και Ιταλία.

6.2. Στατιστικά για τις Άδειες Πρόσβασης

Όλα τα δεδομένα που παρουσιάζονται σε αυτήν την ενότητα έχουν συγκεντρωθεί μέσω του API που υλοποιήθηκε για την παρούσα έρευνα.



Εικόνα 4. Μέσος όρος τιμών[31] των εφαρμογών ανά κατηγορία σε Η.Π.Α. και Ελλάδα

[31] Για να αποτυπωθεί σωστά η νομισματική αναλογικότητα των τιμών έγινε μετατροπή των τιμών των διαθέσιμων εφαρμογών στις Η.Π.Α. από δολάρια σε ευρώ ($1 = €0.915).

Πίνακας 5. Οι κατηγορίες με βάση το Play Store και ο αριθμός των εφαρμογών που μελετήθηκαν[32]

Α/Α	Κατηγορία	Η.Π.Α.		Ελλάδα	
		Αρ. Εφ.	Μ.Ο. Τιμών (€)	Αρ. Εφ.	Μ.Ο. Τιμών (€)
1	Books & Reference	600	4,34	600	5,92
2	Business	600	6,34	600	6,06
3	Comics	340	3,00	375	2,28
4	Communication	600	3,14	600	3,50
5	Education	600	3,39	600	3,49
6	Entertainment	600	2,29	600	2,92
7	Family	600	2,94	600	2,96
8	Finance	562	2,81	600	2,98
9	Games	600	3,53	600	3,36
10	Health & Fitness	600	3,29	600	3,15
11	Libraries & Demo	354	1,67	387	1,99
12	Lifestyle	600	3,52	600	3,41
13	Live Wallpaper	600	1,54	600	1,63
14	Media & Video	600	3,12	600	3,15
15	Medical	600	6,88	600	5,69
16	Music & Audio	600	3,05	600	3,51
17	News & Magazines	374	1,90	441	2,23
18	Personalization	600	1,61	600	1,62
19	Photography	600	2,94	600	2,68
20	Productivity	600	3,08	600	3,36
21	Shopping	367	1,83	410	1,96
22	Social	482	1,89	600	1,78
23	Sports	600	4,57	600	4,66
24	Tools	600	3,02	600	2,74
25	Transportation	495	3,53	600	4,48
26	Travel & Local	600	4,79	600	7,58
27	Weather	504	2,09	587	2,28
28	Widgets	600	3,09	495	2,93
	Σύνολο	**14.314**	**3,24**	**14.892**	**3,54**

[32] Ο μέσος όρος τιμής όλων των προσφερόμενων εφαρμογών δεν είναι ίσος με το μέσο όρο των επιμέρους μέσων όρων ανά κατηγορία. Αυτό συμβαίνει γιατί στο γενικό μέσο όρο έχουν αφαιρεθεί οι διπλοεγγραφές (υπάρχει η πιθανότητα μερικές εφαρμογές να ανήκουν σε περισσότερες από μια κατηγορίες).

Πίνακας 6. Οι 30 πιο απαιτητικές εφαρμογές σε άδειες στις Η.Π.Α.[33]

Α/Α	Όνομα Εφαρμογής	Κατηγορία	Τύπος	Αρ. Αδ.
1	Parallel Space-Multi Accounts	Tools	free	104
2	hike messenger	Communication	free	68
3	ZERO Launcher pro,smart,boost	LiveWallpaper	free	60
4	SideSync	Productivity	free	56
5	Antivirus Booster & Cleaner	Tools	free	56
6	GO Launcher-Theme,Wallpaper	LiveWallpaper	free	53
7	Security & Power Booster -free	Productivity	free	53
8	CM Security Antivirus AppLock	LiveWallpaper	free	52
9	Google	Tools	free	52
10	AVG AntiVirus FREE for Android	Widgets	free	52
11	AntiVirus PRO Android Security	Communication	paid	51
12	Tablet AntiVirus Security FREE	Productivity	free	50
13	Tablet AntiVirus Security PRO	Productivity	paid	49
14	Automagic * Automation	Tools	paid	49
15	QQ International - Chat & Call	Communication	free	48
16	Private Text Messaging & Calls	Communication	free	48
17	Cloud Space of CM Security	LiveWallpaper	free	48
18	Kaspersky Internet Security	Tools	free	47
19	C Launcher Speedy Brief Launch	Personalization	free	46
20	CM Swipe (Lite Launcher)	Productivity	free	46
21	360 Security - Antivirus Boost	Tools	free	46
22	Signal Private Messenger	Communication	free	45
23	Free Phone Calls, Free Texting	Social	free	45
24	AVX - Voice Assistant	Communication	paid	44
25	Tasker	Tools	paid	44
26	TIM Protect Segurança	Productivity	free	44
27	Next Lock Screen	Productivity	free	44
28	DU Speed Booster & Antivirus	Tools	free	44
29	Viber	Widgets	free	44
30	Verizon Messages	Widgets	free	44

Σύμφωνα με τον παραπάνω πίνακα, παρατηρείται ότι οι εφαρμογές με τις περισσότερες απαιτήσεις σε άδειες είναι δωρεάν. Συμπερασματικά, οι εφαρμογές επί αντιτίμου είναι πιο προσεκτικές στις άδειες που αιτούνται σε σχέση με τις δωρεάν εφαρμογές.

[33] Ο πλήρης πίνακας με τις άδειες και τις περιγραφές τους παρουσιάζεται στο Παράρτημα Β.

Πίνακας 7. Οι 30 πιο απαιτητικές εφαρμογές σε άδειες στην Ελλάδα

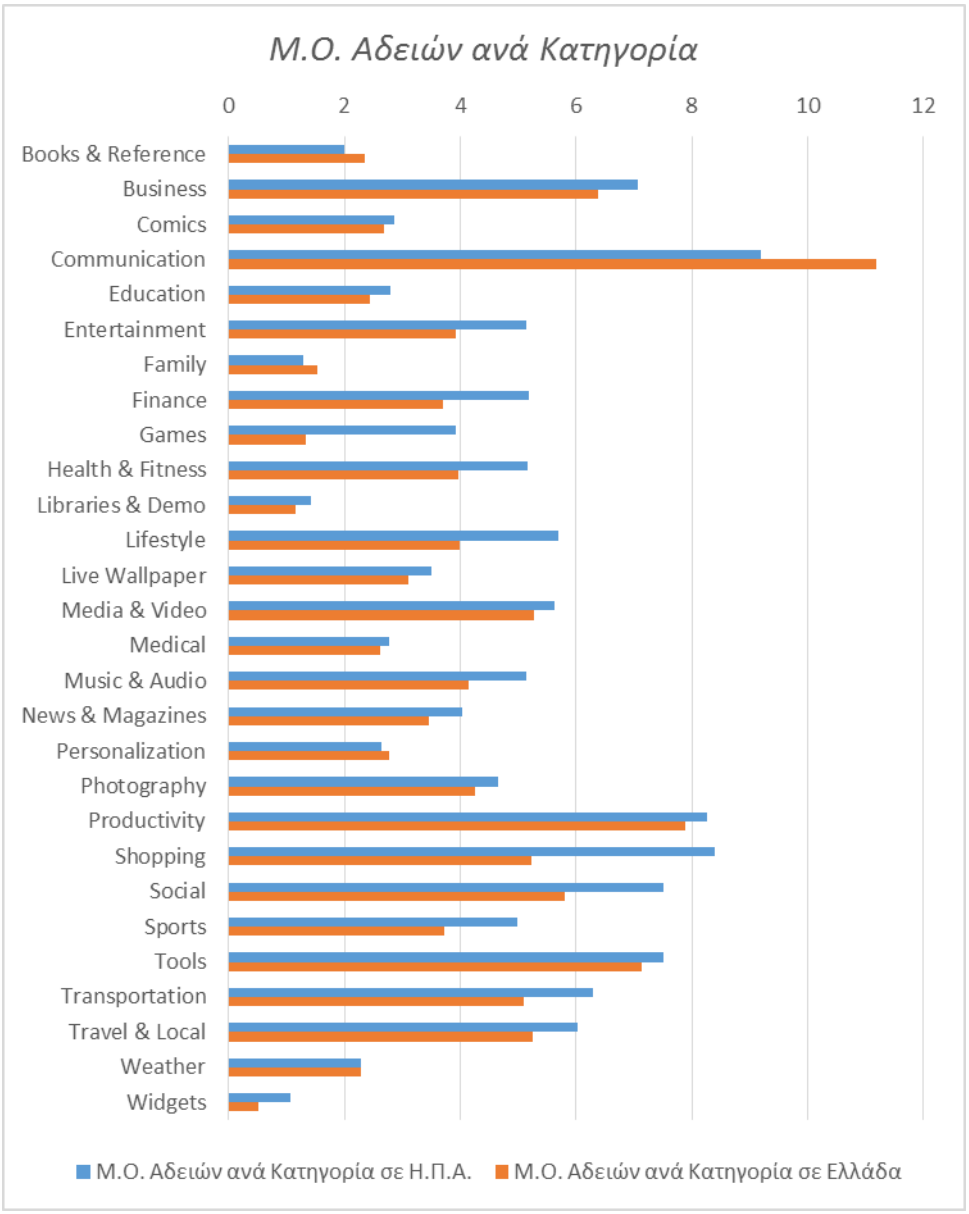
Α/Α	Όνομα εφαρμογής	Κατηγορία	Τύπος	Αρ.Αδ.
1	MLS Updater	Productivity	free	124
2	hike messenger	Communication	free	68
3	ZERO Launcher pro,smart,boost	LiveWallpaper	free	60
4	SideSync	Productivity	free	56
5	GO Launcher-Theme,Wallpaper	LiveWallpaper	free	53
6	Security & Power Booster -free	Productivity	free	53
7	AVG AntiVirus FREE for Android	Communication	free	52
8	CM Security Antivirus AppLock	LiveWallpaper	free	52
9	Google	Tools	free	52
10	AntiVirus PRO Android Security	Communication	paid	51
11	Tablet AntiVirus Security FREE	Productivity	free	50
12	Tablet AntiVirus Security PRO	Productivity	paid	49
13	Automagic * Automation	Tools	paid	49
14	QQ International - Chat & Call	Communication	free	48
15	Cloud Space of CM Security	LiveWallpaper	free	48
16	Avast Anti-Theft	Tools	free	48
17	Kaspersky Internet Security	Tools	free	47
18	C Launcher Speedy Brief Launch	Personalization	free	46
19	CM Swipe (Lite Launcher)	Productivity	free	46
20	360 Security - Antivirus Boost	Tools	free	46
21	AMC Security - Antivirus Boost	Tools	free	46
22	Signal Private Messenger	Communication	free	45
23	TalkU Free Calls +Free Texting	Communication	free	45
24	Tasker	Tools	paid	44
25	Viber	Communication	free	44
26	Vodafone Call+ & Message+	Communication	free	44
27	Next Lock Screen	Productivity	free	44
28	TIM Protect Segurança	Productivity	free	44
29	DU Speed Booster & Antivirus	Tools	free	44
30	GO Locker - theme & wallpaper	LiveWallpaper	free	43

Πίνακας 8. Οι άδειες που ζητούνται περισσότερο στις Η.Π.Α. και το ποσοστό των εφαρμογών που τις ζητούν

Α/Α	Αναγνωριστικό Όνομα Άδειας	Αρ. Εμφάνισης	Ποσοστό Εμφάνισης
1	INTERNET	5626	39.30%
2	ACCESS_NETWORK_STATE	5307	37.08%
3	READ_EXTERNAL_STORAGE	5174	36.15%
4	WRITE_EXTERNAL_STORAGE	5071	35.43%
5	WAKE_LOCK	4072	28.45%
6	ACCESS_WIFI_STATE	3030	21.17%
7	READ_PHONE_STATE	2994	20.92%
8	VIBRATE	2968	20.73%
9	GET_ACCOUNTS	2915	20.36%
10	c2dm.permission.RECEIVE	2600	18.16%
11	ACCESS_FINE_LOCATION	2499	17.46%
12	ACCESS_COARSE_LOCATION	2358	16.47%
13	RECEIVE_BOOT_COMPLETED	2186	15.27%
14	CAMERA	1805	12.61%
15	READ_CONTACTS	1294	9.04%
16	vending.BILLING	1288	9.00%
17	GET_TASKS	1164	8.13%
18	READ_GSERVICES	1135	7.93%
19	USE_CREDENTIALS	1135	7.93%
20	RECORD_AUDIO	1117	7.80%
21	BLUETOOTH	948	6.62%
22	WRITE_SETTINGS	857	5.99%
23	CHANGE_WIFI_STATE	801	5.60%
24	SYSTEM_ALERT_WINDOW	756	5.28%
25	CALL_PHONE	719	5.02%
26	MODIFY_AUDIO_SETTINGS	688	4.81%
27	BLUETOOTH_ADMIN	632	4.42%
28	MANAGE_ACCOUNTS	547	3.82%
29	INSTALL_SHORTCUT	512	3.58%
30	READ_CALL_LOG	480	3.35%

Πίνακας 9. Οι άδειες που ζητούνται περισσότερο στην Ελλάδα και το ποσοστό των εφαρμογών που τις ζητούν

Α/Α	Αναγνωριστικό Όνομα Άδειας	Αρ. Εμφάνισης	Ποσοστό Εμφάνισης
1	INTERNET	5091	34.18%
2	ACCESS_NETWORK_STATE	4773	32.05%
3	READ_EXTERNAL_STORAGE	4708	31.61%
4	WRITE_EXTERNAL_STORAGE	4599	30.88%
5	WAKE_LOCK	3537	23.75%
6	VIBRATE	2636	17.70%
7	READ_PHONE_STATE	2604	17.48%
8	ACCESS_WIFI_STATE	2595	17.42%
9	GET_ACCOUNTS	2443	16.40%
10	ACCESS_FINE_LOCATION	2058	13.82%
11	RECEIVE_BOOT_COMPLETED	2005	13.46%
12	c2dm.permission.RECEIVE	1986	13.34%
13	ACCESS_COARSE_LOCATION	1947	13.07%
14	CAMERA	1503	10.09%
15	vending.BILLING	1196	8.03%
16	READ_CONTACTS	1156	7.76%
17	RECORD_AUDIO	1021	6.86%
18	GET_TASKS	972	6.53%
19	USE_CREDENTIALS	960	6.45%
20	READ_GSERVICES	857	5.75%
21	WRITE_SETTINGS	850	5.71%
22	BLUETOOTH	814	5.47%
23	SYSTEM_ALERT_WINDOW	767	5.15%
24	CHANGE_WIFI_STATE	726	4.87%
25	MODIFY_AUDIO_SETTINGS	636	4.27%
26	CALL_PHONE	590	3.96%
27	BLUETOOTH_ADMIN	529	3.55%
28	INSTALL_SHORTCUT	515	3.46%
29	READ_CALL_LOG	489	3.28%
30	MANAGE_ACCOUNTS	475	3.19%



Εικόνα 5. Μέσος όρος αδειών ανά κατηγορία σε Η.Π.Α. και Ελλάδα

Πίνακας 10. Μέσος όρος αδειών ανά κατηγορία σε Η.Π.Α. και Ελλάδα

Α/Α	Κατηγορία	Μ.Ο. Αδειών	
		Η.Π.Α.	**Ελλάδα**
1	Books & Reference	2.00167	2.36333
2	Business	7.07500	6.39000
3	Comics	2.86176	2.69333
4	Communication	9.19333	11.18000
5	Education	2.79667	2.44833
6	Entertainment	5.13500	3.93500
7	Family	1.29333	1.52333
8	Finance	5.19039	3.70333
9	Games	3.93167	1.34000
10	Health & Fitness	5.16167	3.96333
11	Libraries & Demo	1.42938	1.15762
12	Lifestyle	5.68667	4.00167
13	Live Wallpaper	3.50667	3.11000
14	Media & Video	5.62333	5.27667
15	Medical	2.76667	2.62333
16	Music & Audio	5.14333	4.14500
17	News & Magazines	4.03476	3.46939
18	Personalization	2.64500	2.78000
19	Photography	4.65833	4.25833
20	Productivity	8.27000	7.88500
21	Shopping	8.38965	5.22927
22	Social	7.51037	5.80333
23	Sports	4.99833	3.73167
24	Tools	7.50333	7.13500
25	Transportation	6.29091	5.10833
26	Travel & Local	6.03667	5.25833
27	Weather	2.28175	2.27768
28	Widgets	1.06000	0.52121

Πίνακας 11. Οι 30 άδειες που ζητούνται λιγότερο στις Η.Π.Α.

Α/Α	Αναγνωριστικό Όνομα Άδειας	Αρ. Εμφ.	Ποσοστό Εμφ.
1	WRITE_GSERVICES	3	0.021%
2	ACCESS_CHECKIN_PROPERTIES	3	0.021%
3	MANAGE_DEVICE_ADMINS	3	0.021%
4	googleapps.permission.GOOGLE_AUTH.YouTubeUser	3	0.021%
5	MANAGE_USB	3	0.021%
6	BACKUP	2	0.014%
7	providers.tv.permission.READ_EPG_DATA	2	0.014%
8	providers.tv.permission.WRITE_EPG_DATA	2	0.014%
9	MOVE_PACKAGE	2	0.014%
10	SET_TIME	2	0.014%
11	STATUS_BAR_SERVICE	2	0.014%
12	CONFIGURE_WIFI_DISPLAY	2	0.014%
13	Hotword detection Permission	2	0.014%
14	BIND_DREAM_SERVICE	1	0.007%
15	BIND_TEXT_SERVICE	1	0.007%
16	BIND_INPUT_METHOD	1	0.007%
17	WRITE_VOICEMAIL	1	0.007%
18	READ_VOICEMAIL	1	0.007%
19	HARDWARE_TEST	1	0.007%
20	ACCESS_KEYGUARD_SECURE_STORAGE	1	0.007%
21	GET_APP_OPS_STATS	1	0.007%
22	ACCESS_NOTIFICATION_POLICY	1	0.007%
23	ACCESS_ALL_EXTERNAL_STORAGE	1	0.007%
24	SET_ALWAYS_FINISH	1	0.007%
25	MASTER_CLEAR	1	0.007%
26	BIND_VOICE_INTERACTION	1	0.007%
27	GTALK_SERVICE	1	0.007%
28	ACCESS_CACHE_FILESYSTEM	1	0.007%
29	READ_CELL_BROADCASTS	1	0.007%
30	BIND_REMOTEVIEWS	1	0.007%

Πίνακας 12. Οι 30 άδειες που ζητούνται λιγότερο στην Ελλάδα

Α/Α	Αναγνωριστικό Όνομα Άδειας	Αρ. Εμφ.	Ποσοστό Εμφ.
1	BIND_TEXT_SERVICE	2	0.013%
2	MOVE_PACKAGE	2	0.013%
3	DIAGNOSTIC	2	0.013%
4	googleapps.permission.GOOGLE_AUTH.YouTubeUser	2	0.013%
5	CONFIGURE_WIFI_DISPLAY	2	0.013%
6	MASTER_CLEAR	2	0.013%
7	BIND_REMOTEVIEWS	2	0.013%
8	FORCE_BACK	2	0.013%
9	CHANGE_BACKGROUND_DATA_SETTING	1	0.007%
10	BIND_DREAM_SERVICE	1	0.007%
11	SEND_RESPOND_VIA_MESSAGE	1	0.007%
12	WRITE_VOICEMAIL	1	0.007%
13	READ_VOICEMAIL	1	0.007%
14	BIND_NFC_SERVICE	1	0.007%
15	GET_APP_OPS_STATS	1	0.007%
16	BIND_VPN_SERVICE	1	0.007%
17	SIGNAL_PERSISTENT_PROCESSES	1	0.007%
18	BRICK	1	0.007%
19	SET_POINTER_SPEED	1	0.007%
20	SET_TIME	1	0.007%
21	ACCESS_CACHE_FILESYSTEM	1	0.007%
22	MANAGE_APP_TOKENS	1	0.007%
23	SET_ACTIVITY_WATCHER	1	0.007%
24	READ_INPUT_STATE	1	0.007%
25	ACCESS_CHECKIN_PROPERTIES	1	0.007%
26	SET_ANIMATION_SCALE	1	0.007%
27	STATUS_BAR_SERVICE	1	0.007%
28	ACCESS_NOTIFICATION_POLICY	1	0.007%
29	Hotword detection Permission	1	0.007%
30	BIND_VOICE_INTERACTION	1	0.007%

6.3. Μελέτη Επικινδυνότητας

Λόγω της μεγάλης του δημοτικότητας, το Android προσελκύει πολλούς προγραμματιστές κακόβουλων εφαρμογών, όπως τα Geinimi (Symantec, 2011)), DroidKungFu (Jiang, 2010) and AnserverBot (Jiang, 2010). Οι κακόβουλες εφαρμογές εξαπλώνονται γρήγορα στην αγορά του Android και μπορούν να προκαλέσουν οικονομική ζημία ή διαρροή προσωπικών δεδομένων στους χρήστες των έξυπνων φορητών συσκευών.

Οι περισσότερες κακόβουλες εφαρμογές είναι διαθέσιμες σε αγορές τρίτων για Android εφαρμογές, καθώς για να δημοσιευθούν στην επίσημη αγορά του Android, στο Play Store, περνούν από έλεγχο. Βέβαια, αυτό δεν αποκλείει την ύπαρξη κακόβουλων εφαρμογών και στην επίσημη σελίδα του Play Store.

Επιπλέον, πέρα από τις κακόβουλες εφαρμογές, οι οποίες έχουν σχεδιαστεί εξαρχής για να εκμεταλλευτούν τους χρήστες των έξυπνων φορητών συσκευών, υπάρχουν και οι εφαρμογές οι οποίες εγείρουν προβληματισμούς ασφάλειας και ιδιωτικότητας. Σε αυτές τις εφαρμογές ανήκουν οι εφαρμογές οι οποίες ζητούν πολλές παραπάνω άδειες από αυτές που χρειάζονται για να προσφέρουν τις λειτουργικότητες που θέλουν και έχουν σχεδιαστεί έτσι είτε ακούσια είτε εκούσια. Για παράδειγμα, μια εφαρμογή μπορεί να θεωρηθεί ότι εγείρει προβληματισμούς ασφάλειας είτε επειδή χρησιμοποιεί μια επικίνδυνη άδεια, είτε επειδή χρησιμοποιεί ένα συνδυασμό απλών αδειών, ο οποίος μπορεί να εγείρει κάποιο προβληματισμό ασφάλειας.

Αξίζει σε αυτό το σημείο να σημειωθεί πως αν μια εφαρμογή κατηγοριοποιηθεί ως κάποιου βαθμού επικινδυνότητας επειδή εγείρει κάποιο προβληματισμό ασφάλειας, αυτό δεν σημαίνει πως είναι κακόβουλη.

Οι απαιτούμενες άδειες από κάθε εφαρμογή οφείλουν να δηλώνονται στο Android manifest, οπότε η δήλωσή τους αποτελεί ένα χρήσιμο και αποτελεσματικό τρόπο για να αποκαλυφθούν οι πιθανοί κίνδυνοι. Σύμφωνα με τη διεθνή βιβλιογραφία, τα αποτελέσματα των ερευνών γύρω από τις δηλωμένες άδειες των εφαρμογών έχουν δείξει πως άδειες όπως οι INTERNET, READ_PHONE_STATE, ACCESS_NETWORK_STATE και WRITE_EXTERNAL_STORAGE ζητούνται συχνά και στις κακόβουλες και στις καλοήθεις εφαρμογές (Liang & Du, 2014). Από την άλλη, άδειες όπως οι READ_SMS, WRITE_SMS, SEND_SMS και RECEIVE_SMS ζητούνται σε συντριπτικά μεγαλύτερο βαθμό από τις κακόβουλες, αλλά σπανίως στις καλοήθεις.

Αρχικά θα παρουσιαστούν οι προβληματισμοί ασφάλειας και τα στατιστικά που προκύπτουν από την εφαρμογή της μελέτης στο δείγμα που συγκεντρώθηκε από το API που σχεδιάστηκε και στη συνέχεια θα παρουσιαστούν οι πιο επικίνδυνες εφαρμογές με βάση το μοντέλο των Liang και Du, στην έρευνα «Permission-

Combination-based Scheme for Android - Mobile Malware Detection» (Liang και Du, 2014).

6.3.1. Προβληματισμοί ασφάλειας & ιδιωτικότητας

Ο σχεδιασμός του χάρτη αδειών και προβληματισμών ασφάλειας που εγείρουν έχει γίνει έχοντας μελετήσει τις έρευνες των Liang και Du, καθώς και την έρευνα του site «IzzyOnDroid» (IzzySoft, 2015) για τους συνδυασμούς αδειών.

Αξίζει να σημειωθεί ότι η άδεια για απλή πρόσβαση σε δίκτυα δεν αποτελεί προβληματισμό ασφάλειας, καθώς περισσότερες από τα ¾ του συνόλου των δωρεάν εφαρμογών χρησιμοποιούν αυτή την άδεια για τις διαφημίσεις.

Επιπλέον, επισημαίνεται πως ο συνδυασμός αδειών που θεωρείται επικίνδυνος για μια εφαρμογή δύναται να είναι απαραίτητος για τη λειτουργία μιας άλλης. Για παράδειγμα, αν μια εφαρμογή ξυπνητηριού ζητάει πρόσβαση στην τοποθεσία και στο internet, εγείρονται προβληματισμοί ασφάλειας, ενώ αν το ζητάει μια εφαρμογή εύρεσης και αξιολόγησης εστιατορίων, θεωρείται καλοήθης χρήση. Συνεπώς τα αποτελέσματα που παρουσιάζονται στους παρακάτω πίνακες, δεν εξετάζουν το κριτήριο της σχετικότητας της εφαρμογής με την άδεια που ζητάει, καθώς αυτό το συμπέρασμα δεν δύναται να προκύψει με τρόπο αυτοματοποιημένο.

Πίνακας 13. Εφαρμογές που εγείρουν τις περισσότερες ανησυχίες ασφάλειας στις Η.Π.Α.

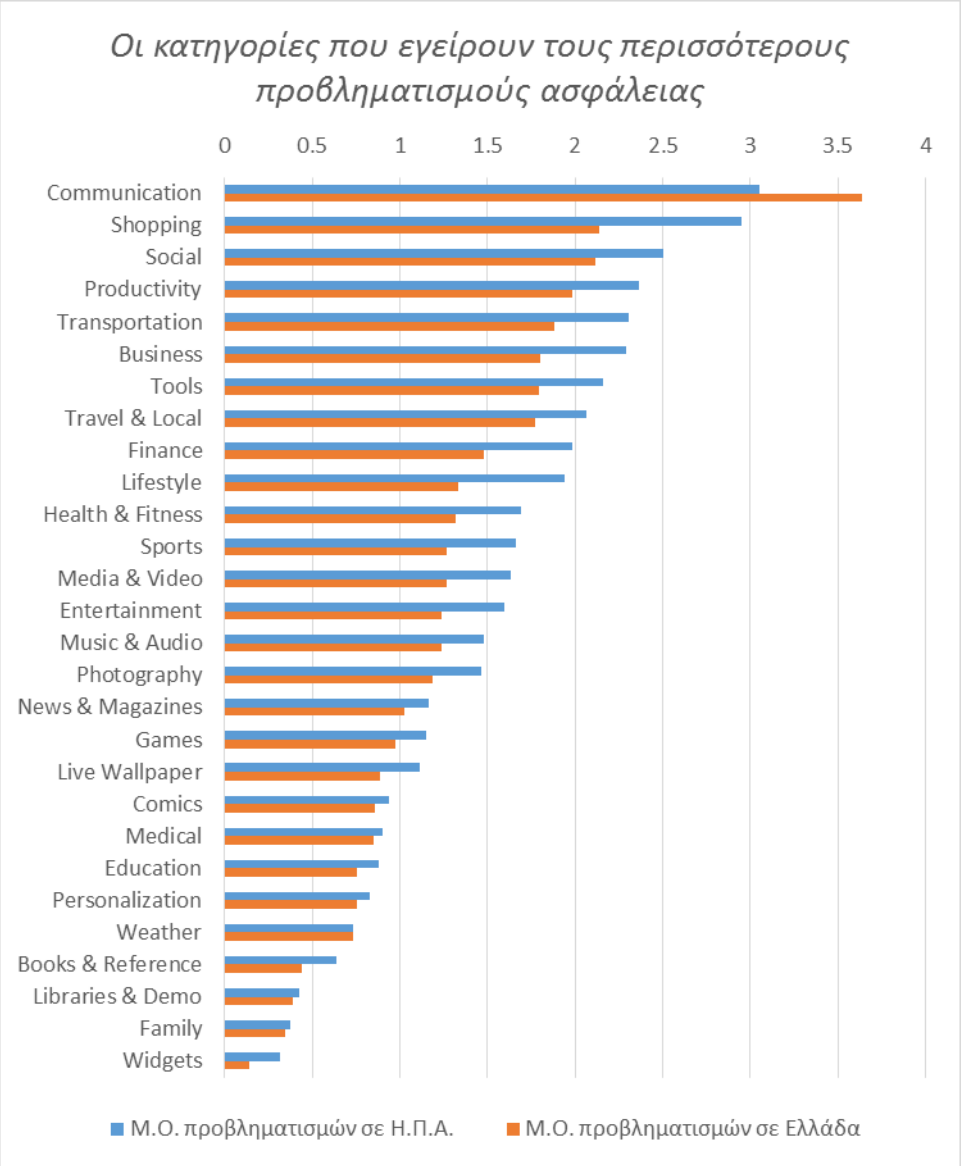
Α/Α	Όνομα Εφαρμογής	Κατηγορία	Τύπος	Αρ. Προβ.
1	AntiVirus PRO Android Security	Communication	paid	14
2	Tablet AntiVirus Security PRO	Productivity	paid	14
3	Automagic * Automation	Tools	paid	14
4	Vault-Hide SMS, Pics & Videos	Business	free	14
5	Private Text Messaging & Calls	Communication	free	14
6	CM Security Antivirus AppLock	LiveWallpaper	free	14
7	GO Launcher-Theme,Wallpaper	LiveWallpaper	free	14
8	ZERO Launcher pro,smart,boost	LiveWallpaper	free	14
9	GO Locker - theme & wallpaper	LiveWallpaper	free	14
10	Cortana	Productivity	free	14
11	Tablet AntiVirus Security FREE	Productivity	free	14
12	AirDroid: File Transfer/Manage	Tools	free	14
13	Parallel Space-Multi Accounts	Tools	free	14
14	Viber	Widgets	free	14
15	AVG AntiVirus FREE for Android	Widgets	free	14
16	AIVC (Alice) - Pro Version	Communication	paid	13
17	Tasker	Tools	paid	13
18	Coco	Communication	free	13
19	hike messenger	Communication	free	13
20	Signal Private Messenger	Communication	free	13
21	WF Mobile Merchant Phone	Finance	free	13
22	Assistant (Siri Alternative)	Lifestyle	free	13
23	CM Locker (Secure & Boost)	LiveWallpaper	free	13
24	Cloud Space of CM Security	LiveWallpaper	free	13
25	C Launcher Speedy Brief Launch	Personalization	free	13
26	Security & Power Booster -free	Productivity	free	13
27	Mobizen : Screen Recorder	Productivity	free	13
28	Next Lock Screen	Productivity	free	13
29	Arrow Launcher	Productivity	free	13
30	Dragon Mobile Assistant	Productivity	free	13

Πίνακας 14. Εφαρμογές που εγείρουν ανησυχίες ασφάλειας στην Ελλάδα

Α/Α	Όνομα Εφαρμογής	Κατηγορία	Τύπος	Αρ. Προβ.
1	AntiVirus PRO Android Security	Communication	paid	14
2	Tablet AntiVirus Security PRO	Productivity	paid	14
3	Automagic * Automation	Tools	paid	14
4	Vault-Hide SMS, Pics & Videos	business	free	14
5	Viber	Communication	free	14
6	AVG AntiVirus FREE for Android	Communication	free	14
7	Vodafone Call+ & Message+	Communication	free	14
8	UppTalk WiFi Calling & Texting	Communication	free	14
9	CM Security Antivirus AppLock	LiveWallpaper	free	14
10	GO Launcher-Theme,Wallpaper	LiveWallpaper	free	14
11	GO Locker - theme & wallpaper	LiveWallpaper	free	14
12	ZERO Launcher pro,smart,boost	LiveWallpaper	free	14
13	Luxury Clock CM Locker Theme	Personalization	free	14
14	Tablet AntiVirus Security FREE	Productivity	free	14
15	MLS Updater	Productivity	free	14
16	AirDroid: File Transfer/Manage	Tools	free	14
17	AIVC (Alice) - Pro Version	Communication	paid	13
18	Tasker	Tools	paid	13
19	GO SMS Pro	Communication	free	13
20	Signal Private Messenger	Communication	free	13
21	Free Calls & Text by Mo+	Communication	free	13
22	TalkU Free Calls +Free Texting	Communication	free	13
23	ZERO SMS - Fast & Free Themes	Communication	free	13
24	PHONE for Google Voice & GTalk	Communication	free	13
25	hike messenger	Communication	free	13
26	Coco	Communication	free	13
27	ZERO Dialer & Contacts & Block	Communication	free	13
28	Assistant (Siri Alternative)	Lifestyle	free	13
29	CM Locker (Secure & Boost)	LiveWallpaper	free	13
30	Cloud Space of CM Security	LiveWallpaper	free	13

Πίνακας 15. Οι κατηγορίες που εγείρουν τους περισσότερους προβληματισμούς ασφάλειας στις Η.Π.Α.

Α/Α	Κατηγορία	Αρ. Προβλ.	Μ.Ο. Προβλ.
1	Communication	1831	3.0517
2	Shopping	1083	2.9510
3	Social	1206	2.5021
4	Productivity	1418	2.3633
5	Transportation	1142	2.3071
6	Business	1375	2.2917
7	Tools	1294	2.1567
8	Travel & Local	1239	2.0650
9	Finance	1114	1.9822
10	Lifestyle	1166	1.9433
11	Health & Fitness	1013	1.6883
12	Sports	998	1.6633
13	Media & Video	978	1.6300
14	Entertainment	958	1.5967
15	Music & Audio	886	1.4767
16	Photography	877	1.4617
17	News & Magazines	437	1.1684
18	Games	691	1.1517
19	Live Wallpaper	667	1.1117
20	Comics	319	0.9382
21	Medical	541	0.9017
22	Education	527	0.8783
23	Personalization	499	0.8317
24	Weather	368	0.7302
25	Books & Reference	306	0.6400
26	Libraries & Demo	151	0.4266
27	Family	225	0.3750
28	Widgets	190	0.3167



Εικόνα 6. Οι κατηγορίες που εγείρουν τους περισσότερους προβληματισμούς ασφάλειας

Πίνακας 16. Οι κατηγορίες που εγείρουν τους περισσότερους προβληματισμούς ασφάλειας στην Ελλάδα

Α/Α	Κατηγορία	Αρ. Προβλ.	Μ.Ο. Προβλ.
1	Communication	2184	3.6400
2	Productivity	1281	2.1350
3	Tools	1268	2.1133
4	Business	1191	1.9850
5	Social	1131	1.8850
6	Transportation	1081	1.8017
7	Shopping	735	1.7927
8	Travel & Local	1064	1.7733
9	Media & Video	890	1.4833
10	Lifestyle	799	1.3317
11	Photography	793	1.3217
12	Finance	762	1.2700
13	Health & Fitness	762	1.2700
14	Entertainment	745	1.2417
15	Sports	744	1.2400
16	Music & Audio	712	1.1867
17	News & Magazines	451	1.0227
18	Live Wallpaper	585	0.9750
19	Medical	533	0.8883
20	Personalization	515	0.8583
21	Comics	320	0.8533
22	Education	454	0.7567
23	Weather	442	0.7530
24	Books & Reference	439	0.7317
25	Family	265	0.4417
26	Games	233	0.3883
27	Libraries & Demo	133	0.3437
28	Widgets	70	0.1414

Πίνακας 17. Οι πιο ανησυχητικοί προβληματισμοί ασφάλειας στις Η.Π.Α.

Α/Α	Κατηγορία	Περιγραφή	Αρ. Εφ.	Ποσοστό
1	Πρόσβαση σε δίκτυα	Μπορεί να αποκτηθεί πρόσβαση σε δίκτυα	5683	39.70%
2	Λογαριασμοί	Μπορούν να μεταδοθούν στοιχεία λογαριασμών	3294	23.01%
3	Ταυτότητα	Μπορούν να μεταδοθούν αναγνωριστικά δεδομένα	2889	20.18%
4	Τοποθεσία	Μπορούν να μεταδοθούν στοιχεία τοποθεσίας	2879	20.11%
5	Καταγραφές	Μπορούν να μεταδοθούν video, φωτογραφίες, ηχογραφήσεις	2266	15.83%
6	Εφαρμογές	Μπορούν να μεταδοθούν στοιχεία εφαρμογών	2264	15.82%
7	Προσωπικά δεδομένα	Μπορούν να μεταδοθούν προσωπικά δεδομένα	1464	10.23%
8	Δίκτυο	Μπορούν να αλλάξουν οι συνδέσεις δικτύου	1259	8.80%
9	Κόστος	Μπορούν να προκληθούν κόστη	954	6.66%
10	Spam	Μπορούν να τοποθετηθούν spam	437	3.05%
11	Παραποίηση πληροφοριών	Μπορούν να παραποιηθούν πληροφορίες	388	2.71%
12	Μηνύματα	Μπορούν να μεταδοθούν περιεχόμενα μηνυμάτων	372	2.60%
13	Ασφάλεια	Μπορούν να αλλάξουν οι ρυθμίσεις ασφάλειας	366	2.56%
14	Σύνταξη Μηνυμάτων	Μπορούν να συνταχθούν μηνύματα	194	1.36%

Πίνακας 18. Οι πιο ανησυχητικοί προβληματισμοί ασφάλειας στην Ελλάδα.

Α/Α	Κατηγορία	Περιγραφή	Αρ. Εφ.	Ποσοστό
1	Πρόσβαση σε δίκτυα	Μπορεί να αποκτηθεί πρόσβαση σε δίκτυα	5155	34.61%
2	Λογαριασμοί	Μπορούν να μεταδοθούν στοιχεία λογαριασμών	2737	18.38%
3	Ταυτότητα	Μπορούν να μεταδοθούν αναγνωριστικά δεδομένα	2476	16.63%
4	Τοποθεσία	Μπορούν να μεταδοθούν στοιχεία τοποθεσίας	2396	16.09%
5	Καταγραφές	Μπορούν να μεταδοθούν video, φωτογραφίες, ηχογραφήσεις	1890	12.69%
6	Προσωπικά δεδομένα	Μπορούν να μεταδοθούν προσωπικά δεδομένα	1285	8.63%
7	Δίκτυο	Μπορούν να αλλάξουν οι συνδέσεις δικτύου	1101	7.39%
8	Εφαρμογές	Μπορούν να μεταδοθούν στοιχεία εφαρμογών	931	6.25%
9	Κόστος	Μπορούν να προκληθούν κόστη	805	5.41%
10	Spam	Μπορούν να τοποθετηθούν spam	445	2.99%
11	Ασφάλεια	Μπορούν να αλλάξουν οι ρυθμίσεις ασφάλειας	404	2.71%
12	Παραποίηση πληροφοριών	Μπορούν να παραποιηθούν πληροφορίες	386	2.59%
13	Μηνύματα	Μπορούν να μεταδοθούν περιεχόμενα μηνυμάτων	371	2.49%
14	Σύνταξη Μηνυμάτων	Μπορούν να συνταχθούν μηνύματα	200	1.34%

6.3.2. Οι εν δυνάμει επικίνδυνες εφαρμογές

Ο παρακάτω πίνακας περιλαμβάνει την ανάλυση των Liang και Du, στην έρευνα «Permission-Combination-based Scheme for Android - Mobile Malware Detection» (Liang & Du, 2014), όπως εφαρμόστηκε για k=6 στο δείγμα που εξάχθηκε από το API που σχεδιάστηκε για τις ανάγκες της παρούσας έρευνας. Οι δύο πρώτες στήλες του πίνακα που ακολουθεί περιλαμβάνουν το ποσοστό των εφαρμογών, οι οποίες αιτούνται τους παρακάτω συνδυασμούς αδειών και που σύμφωνα με το δείγμα των συγγραφέων είναι είτε κακόβουλες, είτε καλοήθεις.

Πίνακας 19. Επικίνδυνοι συνδυασμοί αδειών και τα ποσοστά εμφάνισής τους

Α/Α	Συνδυασμός Αδειών	Κακόβουλες (%)	Καλοήθεις (%)	Play Store API (%)	
				Η.Π.Α.	Ελλάδα
1	ACCESS_NETWORK_STATE ACCESS_WIFI_STATE INTERNET READ_PHONE_STATE READ_SMS WRITE_SMS	38.25	2.56	0.89	0.83%
2	ACCESS_NETWORK_STATE INTERNET READ_PHONE_STATE READ_SMS WRITE_EXTERNAL_STORAGE WRITE_SMS	29.84	3.1	1.03	1.00%
3	ACCESS_NETWORK_STATE INTERNET READ_PHONE_STATE READ_SMS VIBRATE WRITE_SMS	29.76	3.1	0.87	0.85%
4	ACCESS_NETWORK_STATE INTERNET READ_PHONE_STATE READ_SMS SEND_SMS WRITE_SMS	28.97	2.56	0.89	0.86%
5	ACCESS_NETWORK_STATE INTERNET READ_PHONE_STATE READ_SMS RECEIVE_SMS SEND_SMS	28.73	3.1	1.08	0.91%

6.4. Λοιπά Στατιστικά Στοιχεία

Ο τελευταίος πίνακας περιλαμβάνει γενικά στατιστικά στοιχεία για τις διαθέσιμες εφαρμογές στο Play Store.

Πίνακας 20. Γενικά στατιστικά στοιχεία για τις εφαρμογές στις Η.Π.Α.

Κριτήρια	Η.Π.Α.		Ελλάδα	
	Αρ. Εμφάνισης	Ποσοστό Εμφάνισης	Αρ. Εμφάνισης	Ποσοστό Εμφάνισης
Δωρεάν apps με in-app billing ("Freemium")	985	6.88%	871	5.85%
Apps επί πληρωμή με in-app billing	303	2.12%	325	2.18%
Apps που δεν ζητούν καμία άδεια	8895	62.14%	10290	69.09%
Apps που ζητούν 1-5 άδειες	626	4.37%	768	5.16%
Apps που ζητούν 6-10 άδειες	2170	15.16%	2161	14.51%
Apps που ζητούν 11-20 άδειες	2665	18.62%	2158	14.49%
Apps που ζητούν 21-30 άδειες	388	2.71%	356	2.39%
Apps που ζητούν περισσότερες από 30 άδειες	163	1.14%	162	1.09%
Apps που δεν εγείρουν καμία ανησυχία[34]	9107	63.62%	10633	71.40%
Apps που εγείρουν 1-5 ανησυχίες	4566	31.90%	4313	28.96%
Apps που εγείρουν 6-10 ανησυχίες	1078	7.53%	821	5.51%
Apps που εγείρουν περισσότερες από 10 ανησυχίες	130	0.91%	128	0.86%

[34] Ο πίνακας με τους προβληματισμούς ασφάλειας περιγράφονται στο Παράρτημα Β.

7. Συμπεράσματα

Είναι πολύ ανησυχητικό το γεγονός ότι τα υπάρχοντα λειτουργικά συστήματα έξυπνων φορητών συσκευών δεν παρέχουν ένα ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων των χρηστών τους, καθώς επίσης και το γεγονός ότι είναι πιθανό να έχουν σχεδιαστεί εξ αρχής συνειδητά με ευπάθειες.

Όπως φαίνεται στον Πίνακα 3, τα δεδομένα αισθητήρων είναι τα πιο κρίσιμα δεδομένα, καθώς μπορούν να διαβαστούν από κάθε οντότητα που έχει πρόσβαση στο smartphone. Επιπλέον, η οντότητα που φαίνεται να είναι η πιο απειλητική είναι το λειτουργικό σύστημα, το οποίο μπορεί να έχει πρόσβαση σε όλα τα προσωπικά δεδομένα ενώ παράλληλα έχει διαγνωστεί με σοβαρές ευπάθειες.

Πληθώρα ενδιαφερουσών ιδεών έχουν προταθεί στη σύγχρονη βιβλιογραφία για την αντιμετώπιση των παραπάνω προβληματισμών, όπως τα fine-grained permissions και η καλύτερη κατηγοριοποίηση των αδειών σε ομάδες. Αν αυτές οι ιδέες υιοθετηθούν και υλοποιηθούν στην πράξη, μπορούν να βελτιώσουν σημαντικά την υπάρχουσα κατάσταση και να μετριάσουν τους προβληματισμούς ιδιωτικότητας που εγείρονται. Έχοντας αυτή την προοπτική κάνουμε τις παρακάτω προτάσεις:

- Τα μοντέλα αδειών πρόσβασης των έξυπνων φορητών συσκευών θα πρέπει να προσαρμοστούν για να συμμορφώνονται με τις απαιτήσεις του νομικού πλαισίου για την προστασία των προσωπικών δεδομένων, όσον αφορά στην διαφάνεια προς το χρήστη, την ρητή συγκατάθεση, τον περιορισμό του σκοπού, την σαφήνεια και αναλογικότητα σε σχέση με την έκταση και τη διάρκεια της επεξεργασίας. Για παράδειγμα, όταν μια εφαρμογή ζητάει την άδεια «`READ_PHONE_STATE`», θα πρέπει τουλάχιστον να δηλώσει τον τρόπο με τον οποίο πρόκειται να χρησιμοποιήσει κάθε ένα από τα επηρεαζόμενα δεδομένα, για πόσο χρονικό διάσημα, ότι θα τα έχει αποθηκευμένα σε ασφαλή τοποθεσία κατά τη διάρκεια αυτής της περιόδου, και τέλος, ότι θα τα διαγράψει μετά το πέρας της επεξεργασίας.
- Για κάθε προσωπική πληροφορία που ζητείται από μια εφαρμογή, θα πρέπει να δηλώνεται ξεκάθαρα αν αυτά τα δεδομένα (ή το αποτέλεσμα της επεξεργασίας τους) πρόκειται να μεταδοθούν εκτός της έξυπνης φορητής συσκευής ή αν θα χρησιμοποιηθούν αποκλειστικά μέσα στη συσκευή. Αν κάποια πληροφορία μεταδοθεί εκτός της συσκευής, τότε η μετάδοσή της, η αποθήκευσή της και η επεξεργασία της θα πρέπει να συμμορφώνεται με τις απαιτήσεις του νομικού πλαισίου της προστασίας προσωπικών δεδομένων.

Αμφότερες οι παραπάνω προτάσεις είναι τεχνικά εφικτές να υλοποιηθούν και θα ενδυνάμωναν τον έλεγχο των χρηστών πάνω στα προσωπικά τους δεδομένα. Χωρίς μάλιστα να επιβαρύνουν τους νόμιμους παρόχους των εφαρμογών. Εξάλλου, τέτοιου είδους μέτρα θα βελτίωναν την ικανότητα των χρηστών να ξεχωρίσουν καλοήθεις (benign) από κακόβουλες (malware) ή απροσδιόριστης επικινδυνότητας (grayware) εφαρμογές. Παρά την ύπαρξη εργαλείων όπως το TaintDroid που αναφέρθηκε νωρίτερα, το οποίο μπορεί να χρησιμοποιήσει ένας έμπειρος χρήστης για να καταλάβει τους κινδύνους χρήσης μιας εφαρμογής, δεν υπάρχει κάποιος καθιερωμένος τρόπος για τις εφαρμογές και τις υπόλοιπες οντότητες του οικοσυστήματος των έξυπνων φορητών συσκευών να τις δεσμεύει σε διαφανείς και υπεύθυνες πρακτικές σε σχέση με την ιδιωτικότητα των χρηστών τους. Οι παραπάνω προτάσεις αποτελούν έναν τρόπο να υποστηριχθεί αυτή η λειτουργικότητα εγγενώς μέσα στο λειτουργικό σύστημα, μαζί με την υποχρέωση των εφαρμογών να δηλώνουν γιατί και με ποιον τρόπο θα διαχειριστούν τα προσωπικά δεδομένα των χρηστών.

Μια άλλη πρόταση για να περιοριστεί η δυσανάλογα μεγάλη λίστα των αδειών πρόσβασης που αιτούνται οι εφαρμογές είναι να ενδυναμωθούν οι συμπεριφορές και στάσεις των καταναλωτών που επιδεικνύουν σκεπτικότητα στα αδικαιολόγητα ή/και υπερβολικά αιτήματα αδειών ή στην έλλειψη διαφάνειας. Αυτό θα μπορούσε να γίνει πράξη αν σχεδιαζόταν ένα σύστημα βασισμένο στις απόψεις των χρηστών για τις εφαρμογές το οποίο θα είχε ένα χρονικό αιτημάτων αδειών πρόσβασης για κάθε εφαρμογή, ώστε οι χρήστες να μπορούν να ενημερωθούν επαρκώς και να αποφασίσουν για το αν θα εγκαταστήσουν κάποια εφαρμογή ή αν θα κάνουν την αναβάθμισή της, βασισμένη πάνω το σεβασμό που δείχνει ο πάροχος της εφαρμογής για τα προσωπικά τους δικαιώματα. Όπως και με τα περισσότερα κοινωνικά δίκτυα, η αξία τους ακολουθεί το νόμο του Μέτκαλφ[35], άρα για να έχει αντίκτυπο αυτή η πρόταση απαιτείται δέσμευση και συνδρομή ενός μεγάλου αριθμού τελικών χρηστών. Αν η επεξεργασία των δεδομένων αποδειχθεί πως είναι πηγή εσόδων, οι υπηρεσίες που διαφυλάττουν την ιδιωτικότητα θα μπορούσαν να λειτουργήσουν ως ανταγωνιστικό πλεονέκτημα για τους ενσυνείδητους σε θέματα ιδιωτικότητας σχεδιαστές εφαρμογών.

[35] Νόμος του Μέτκαλφ: αξία ενός δικτύου είναι περίπου ίση με το τετράγωνο του αριθμού των ανθρώπων που το χρησιμοποιούν.

Παράρτημα Α

Στα πλαίσια της παρούσας έρευνας αναπτύχθηκε ένα πρωτότυπο εφαρμογής, το οποίο χρησιμοποιήθηκε για να εντοπίσει όλες τις άδειες του λειτουργικού συστήματος. Οι εκδόσεις του Android στις οποίες εφαρμόστηκε ο έλεγχος των αδειών είναι η Kitkat (Android 4.4.2 API level 19), η Lollipop (Android 5.5.1 API level 22) και η Marshmallow (Android 6.0 API level 23). Η συσκευή στην οποία εκτελέστηκε η εφαρμογή είναι η Android 5.1 WVGA 800[36].

Η λήψη των διαθέσιμων αδειών έγινε με κλήση στην κλάση του Package Manager. Η συνάρτηση που υλοποιήθηκε παρατίθεται παρακάτω:

```
void getAllInstalledAppPermissions() {
     PackageManager pm = getPackageManager();
     List<ApplicationInfo> packages =
pm.getInstalledApplications(PackageManager.GET_META_DATA);

  for (ApplicationInfo applicationInfo : packages) {
       Log.i(TAG + "getAllInstalledAppPermissions", "App: "
                  + applicationInfo.name + " Package: "
                  + applicationInfo.packageName);

       try {
              PackageInfo packageInfo = pm.getPackageInfo(
                           applicationInfo.packageName,
                           PackageManager.GET_PERMISSIONS);

// Get Permissions
              String[] requestedPermissions =
packageInfo.requestedPermissions;

              if (requestedPermissions != null) {
                     for (int i = 0; i <
requestedPermissions.length; i++) {
                           Log.i(TAG, requestedPermissions[i]);
                     }
              }
       } catch (NameNotFoundException e) {
              e.printStackTrace();
       }
}
}
```

Παράθεση Κώδικα 1. Η συνάρτηση `getAllInstalledAppPermissions()`

[36] Αυτή η συσκευή είναι εικονική συσκευή του Android SDK, η οποία επιτρέπει στους σχεδιαστές των εφαρμογών να αναπτύξουν εφαρμογές ανεξάρτητα από το μοντέλο της συσκευής που θα εκτελεστούν.

Η συνάρτηση `getAllInstalledAppPermissions()` καλεί τη συνάρτηση `PackageManager.GET_PERMISSIONS()`, η οποία επιστρέψει τις άδειες που υπάρχουν στο αρχείο manifest.

Η εφαρμογή αυτή χρειάζεται για να λειτουργήσει δύο άδειες:

- READ_LOGS
- WRITE_EXTERNAL_STORAGE

```
<uses-permission android:name="android.permission.READ_LOGS"/>
    <uses-permission
      android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

Παράθεση Κώδικα 2. Οι άδειες της εφαρμογής

Αυτές οι άδειες θα πρέπει να δηλωθούν μέσα στο manifest της εφαρμογής.

Παράρτημα Β

Όπως αναφέρθηκε και στο κείμενο της έρευνας, η ιστοσελίδα του Play Store είναι κάθε άλλη άλλο παρά εύχρηστη για τη συλλογή μαζικών δεδομένων με τρόπο αυτοματοποιημένο. Για αυτό το λόγο ήταν επιτακτική η ανάγκη να μελετηθεί και να αναλυθεί ώστε να βρεθεί μια κατάλληλη λύση για τις ανάγκες της παρούσας έρευνας.

```
public JSONObject makeHttpRequest(String url, String method,
List<NameValuePair> params) {
	// Making HTTP request
	makingHttpRequest(url, method, params);
	createReader();
	// try parse the string to a JSON object
	parseStringToJsonObject();
	// return JSON String
	return jObj;
}

private void makingHttpRequest(String url, String method,
		List<NameValuePair>params) {
	try {
		if (method == "POST") {
			makeHTTPrequestPOST(url, params);
		}
		else if (method == "GET") {
			makeHTTPrequestGET(url, params);
		}
	} catch (UnsupportedEncodingException e) {
		e.printStackTrace();
	} catch (ClientProtocolException e) {
		e.printStackTrace();
	} catch (IOException e) {
		e.printStackTrace();
	}
}

private void makeHTTPrequestPOST(String url, List<NameValuePair>
params)
		throws UnsupportedEncodingException, IOException,
		ClientProtocolException {
	DefaultHttpClient httpClient = new DefaultHttpClient();
	HttpPost httpPost = new HttpPost(url);
	httpPost.setEntity(new UrlEncodedFormEntity(params));

	HttpResponse httpResponse = httpClient.execute(httpPost);
	HttpEntity httpEntity = httpResponse.getEntity();
	is = httpEntity.getContent();
}
```

Παράθεση Κώδικα 3. Οι απαραίτητες συναρτήσεις για το POST request

Πίνακας 21. Πλήρης κατάλογος αδειών με τις περιγραφές τους

A/A	Αναγνωριστικό Άδειας	Περιγραφή
1	ACCESS_ALL_DOWNLOADS	access all system downloads
2	ACCESS_ALL_EXTERNAL_STORAGE	access external storage of all users
3	ACCESS_CACHE_FILESYSTEM	access the cache filesystem
4	ACCESS_CHECKIN_PROPERTIES	Access check-in properties
5	ACCESS_COARSE_LOCATION	Approximate location (network-based)
6	ACCESS_DOWNLOAD_MANAGER	Access download manager.
7	ACCESS_FINE_LOCATION	Precise location (GPS and network-based)
8	ACCESS_KEYGUARD_SECURE_STORAGE	Access keyguard secure storage
9	ACCESS_LOCATION_EXTRA_COMMANDS	Access extra location provider commands
10	ACCESS_NETWORK_STATE	View network connections
11	ACCESS_NOTIFICATION_POLICY	access notifications
12	ACCESS_SURFACE_FLINGER	Access SurfaceFlinger
13	ACCESS_WIFI_STATE	View Wi-Fi connections
14	ACCOUNT_MANAGER	Act as the AccountManagerService
15	ADD_VOICEMAIL	Add Voicemail
16	AUTHENTICATE_ACCOUNTS	Create accounts and set passwords
17	BACKUP	Control system backup and restore
18	BATTERY_STATS	Read battery statistics
19	BIND_ACCESSIBILITY_SERVICE	Bind to an Accessibility Service
20	BIND_APPWIDGET	Choose Widgets
21	BIND_DEVICE_ADMIN	Interact with device admin
22	BIND_DREAM_SERVICE	bind to a dream service
23	BIND_INPUT_METHOD	Bind to an Input Method
24	BIND_NFC_SERVICE	Bind NFC Service
25	BIND_NOTIFICATION_LISTENER_SERVICE	Bind Notification Listener Service
26	BIND_REMOTEVIEWS	Bind to a widget service
27	BIND_TEXT_SERVICE	Bind to a Text Service
28	BIND_VOICE_INTERACTION	manage voice keyphrases
29	BIND_VPN_SERVICE	Bind to a VPN service

30	BIND_WALLPAPER	Bind to wallpaper
31	BLUETOOTH	Pair with Bluetooth devices
32	BLUETOOTH_ADMIN	Access Bluetooth settings
33	BLUETOOTH_PRIVILEGED	allow Bluetooth pairing by Application
34	BODY_SENSORS	body sensors (like heart rate monitors)
35	BRICK	Permanently disable phone
36	BROADCAST_PACKAGE_REMOVED	Send package removed broadcast
37	BROADCAST_SMS	Send SMS-received broadcast
38	BROADCAST_STICKY	Send Sticky Broadcasts
39	BROADCAST_WAP_PUSH	Send WAP-PUSH-received broadcast
40	c2dm.permission.RECEIVE	Receive data from Internet
41	CALL_PHONE	Directly call phone numbers
42	CALL_PRIVILEGED	Directly call any phone numbers
43	CAMERA	Take pictures and videos
44	CAPTURE_AUDIO_OUTPUT	Capture audio output
45	CAPTURE_SECURE_VIDEO_OUTPUT	Capture Secure Video Output
46	CAPTURE_VIDEO_OUTPUT	Capture Video Output
47	CHANGE_BACKGROUND_DATA_SETTING	Change background data usage setting
48	CHANGE_COMPONENT_ENABLED_STATE	Enable or disable app components
49	CHANGE_CONFIGURATION	Change system display settings
50	CHANGE_NETWORK_STATE	Change network connectivity
51	CHANGE_WIFI_MULTICAST_STATE	Allow Wi-Fi Multicast reception
52	CHANGE_WIFI_STATE	Connect and disconnect from Wi-Fi
53	CHANGE_WIMAX_STATE	Change WiMAX state
54	CLEAR_APP_CACHE	Delete all app cache data
55	CLEAR_APP_USER_DATA	Delete other apps´ data
56	CONFIGURE_WIFI_DISPLAY	configure Wifi displays
57	control_incall_experience	control_incall_experience
58	CONTROL_LOCATION_UPDATES	Control Location Updates
59	DELETE_CACHE_FILES	Delete other apps´ cache
60	DELETE_PACKAGES	Delete apps
61	DIAGNOSTIC	Read/write to resources owned by diag

62	DISABLE_KEYGUARD	Disable your screen lock
63	DOWNLOAD_WITHOUT_NOTIFICATION	Download files without notification
64	DUMP	Retrieve system internal state
65	email.ACCESS_PROVIDER	Access email provider data
66	EXPAND_STATUS_BAR	Expand/collapse status bar
67	FLASHLIGHT	Control flashlight
68	FORCE_BACK	force app to close
69	FORCE_STOP_PACKAGES	Force stop other apps
70	GET_ACCOUNTS	Find accounts on the device
71	GET_APP_OPS_STATS	Retrieve app ops statistics
72	GET_PACKAGE_SIZE	Measure app storage space
73	GET_TASKS	Retrieve running apps
74	GET_TOP_ACTIVITY_INFO	get current app info
75	GOOGLE_AUTH	View configured accounts
76	GOOGLE_AUTH.mail	Google mail
77	GOOGLE_AUTH.wise	Google Spreadsheets
78	GOOGLE_AUTH.writely	Google Docs
79	googleapps.permission.GOOGLE_AUTH.ALL_SERVICES	access all Google services
80	googleapps.permission.GOOGLE_AUTH.youtube	YouTube
81	googleapps.permission.GOOGLE_AUTH.YouTubeUser	YouTube usernames
82	GTALK_SERVICE	Google Talk Service
83	HARDWARE_TEST	Test Hardware
84	Hotword detection Permission	Hotword detection
85	im.permission.READ_ONLY	read instant messages
86	INJECT_EVENTS	Press keys and control buttons
87	INSTALL_PACKAGES	Directly install apps
88	INSTALL_SHORTCUT	Install Shortcuts
89	INTERACT_ACROSS_USERS	Interact Across Users
90	INTERACT_ACROSS_USERS_FULL	Full license to interact across users
91	INTERNAL_SYSTEM_WINDOW	Internal System Window
92	INTERNET	Full network access
93	KILL_BACKGROUND_PROCESSES	Close other apps
94	launcher.WRITE_SETTINGS	write Home settings and shortcuts
95	MANAGE_ACCOUNTS	Add or remove accounts
96	MANAGE_APP_TOKENS	Manage App Tokens

97	MANAGE_DEVICE_ADMINS	add or remove a device admin
98	MANAGE_DOCUMENTS	Manage Documents
99	MANAGE_USB	Manage preferences and permissions for USB devices
100	MANAGE_USERS	manage users
101	MASTER_CLEAR	reset system to factory defaults
102	MEDIA_CONTENT_CONTROL	control media playback and metadata access
103	MODIFY_AUDIO_SETTINGS	Change your audio settings
104	MODIFY_PHONE_STATE	Modify Phone State
105	MOUNT_FORMAT_FILESYSTEMS	Erase USB storage
106	MOUNT_UNMOUNT_FILESYSTEMS	Access USB storage filesystem
107	MOVE_PACKAGE	Move app resources
108	NFC	Control Near Field Communication
109	PACKAGE_USAGE_STATS	Update component usage statistics
110	PERSISTENT_ACTIVITY	Make app always run
111	PROCESS_OUTGOING_CALLS	Reroute outgoing calls
112	providers.tv.permission.READ_EPG_DATA	readEpgData
113	providers.tv.permission.WRITE_EPG_DATA	writeEpgData
114	READ_ATTACHMENT	Read email attachments
115	READ_CALENDAR	Read calendar events plus confidential information
116	READ_CALL_LOG	Read Call Logs
117	READ_CELL_BROADCASTS	READ_CELL_BROADCASTS
118	READ_CONTACTS	Read your contacts
119	READ_EXTERNAL_STORAGE	Read the contents of your usb storage
120	READ_FRAME_BUFFER	Read Frame Buffer
121	READ_GSERVICES	Read Google service configuration
122	READ_HISTORY_BOOKMARKS	Read your Web bookmarks and history
123	READ_INPUT_STATE	Record what you type and actions that you take
124	READ_LOGS	Read sensitive log data
125	READ_PHONE_STATE	Read phone status and identity
126	READ_PROFILE	Read your own contact card
127	READ_SETTINGS	Read Home settings and shortcuts

128	READ_SMS	Read your text messages (SMS or MMS)
129	READ_SOCIAL_STREAM	Read your social stream
130	READ_SYNC_SETTINGS	Read sync settings
131	READ_SYNC_STATS	Read sync statistics
132	READ_USER_DICTIONARY	Read terms you added to the dictionary
133	READ_VOICEMAIL	read voicemail
134	REBOOT	Reboot
135	RECEIVE_BOOT_COMPLETED	Run at startup
136	RECEIVE_MMS	Receive text messages (MMS)
137	RECEIVE_SMS	Receive text messages (SMS)
138	RECEIVE_WAP_PUSH	Receive text messages (WAP)
139	RECORD_AUDIO	Record audio
140	REORDER_TASKS	Reorder running apps
141	SEND_DOWNLOAD_COMPLETED_INTENTS	Send download notifications.
142	SEND_RESPOND_VIA_MESSAGE	Send respond-via-message events
143	SEND_SMS	Send SMS messages
144	SET_ACTIVITY_WATCHER	Monitor and control all app launching
145	SET_ALARM	Set an alarm
146	SET_ALWAYS_FINISH	Force background apps to close
147	SET_ANIMATION_SCALE	Modify global animation speed
148	SET_DEBUG_APP	Enable app debugging
149	SET_ORIENTATION	Change screen orientation
150	SET_POINTER_SPEED	Change pointer speed
151	SET_PREFERRED_APPLICATIONS	Set preferred Apps
152	SET_PROCESS_LIMIT	Limit number of running processes
153	SET_TIME	Set Time
154	SET_TIME_ZONE	Set time zone
155	SET_WALLPAPER	Set Wallpaper
156	SET_WALLPAPER_HINTS	Adjust your wallpaper size
157	SHUTDOWN	Partial shutdown
158	SIGNAL_PERSISTENT_PROCESSES	Send Linux signals to apps
159	STATUS_BAR	Enable/Disable status bar
160	STATUS_BAR_SERVICE	Status bar
161	SUBSCRIBED_FEEDS_READ	Read subscribed feeds
162	SUBSCRIBED_FEEDS_WRITE	Write subscribed feeds

163	SYSTEM_ALERT_WINDOW	Draw over other apps
164	TRANSMIT_IR	Use IR Transmitter
165	UNINSTALL_SHORTCUT	Uninstall shortcuts
166	UPDATE_APP_OPS_STATS	modify app ops statistics
167	USE_CREDENTIALS	Use accounts on the device
168	USE_SIP	Make/receive Internet calls
169	vending.BILLING	In-app billing
170	VIBRATE	Control vibration
171	WAKE_LOCK	Prevent device from sleeping
172	WRITE_APN_SETTINGS	Change/intercept network settings and traffic
173	WRITE_CALENDAR	Add or modify calendar events and send email to guests without owners
174	WRITE_CALL_LOG	Write call log
175	WRITE_CONTACTS	Modify your contacts
176	WRITE_EXTERNAL_STORAGE	Modify or delete the contents of your USB storage
177	WRITE_GSERVICES	Write GServices
178	WRITE_HISTORY_BOOKMARKS	Write web bookmarks and history
179	WRITE_MEDIA_STORAGE	Modify/delete internal media storage contents
180	WRITE_PROFILE	Modify your own contact card
181	WRITE_SECURE_SETTINGS	Modify secure system settings
182	WRITE_SETTINGS	Modify system settings
183	WRITE_SMS	Edit your text messages (SMS or MMS)
184	WRITE_SOCIAL_STREAM	Write to your social stream
185	WRITE_SYNC_SETTINGS	Toggle sync on and off
186	WRITE_USER_DICTIONARY	Add words to user-defined dictionary
187	WRITE_VOICEMAIL	write voicemails

Πίνακας 22. Συνδυασμοί αδειών που εγείρουν προβληματισμούς ασφάλειας

Α/Α	Κατηγορία	Περιγραφή	Συνδυασμός Αδειών
1	Λογαριασμοί	Μπορούν να μεταδοθούν στοιχεία λογαριασμών	INTERNET & (GET_ACCOUNTS | READ_GSERVICE | AUTHENTICATE_ACCOUNTS | USE_CREDENTIALS)
2	Εφαρμογές	Μπορούν να μεταδοθούν στοιχεία εφαρμογών	INTERNET & (GET_TASKS)
3	Κόστος	Μπορούν να προκληθούν κόστη	SEND_SMS | CALL_PHONE | MODIFY_PHONE_STATE | PROCESS_OUTGOING_CALLS | WRITE_APN_SETTINGS
4	Παραποίηση πληροφοριών	Μπορούν να παραποιηθούν πληροφορίες	RECEIVE_MMS | RECEIVE_SMS
5	Ταυτότητα	Μπορούν να μεταδοθούν αναγνωριστικά δεδομένα	INTERNET & (READ_PHONE_STATE)
6	Τοποθεσία	Μπορούν να μεταδοθούν στοιχεία τοποθεσίας	INTERNET & (ACCESS_COARSE_LOCATION | ACCESS_FINE_LOCATION | ACESS_LOCATION_EXTRA_COMMANDS)
7	Μηνύματα	Μπορούν να μεταδοθούν περιεχόμενα μηνυμάτων	INTERNET & (READ_ATTACHMENT | READ_SMS)
8	Δίκτυο	Μπορούν να αλλάξουν οι συνδέσεις δικτύου	BLUETOOTH_ADMIN | CHANGE_NETWORK_STATE | CHANGE_WIFI_STATE | CHANGE_WIMAX_STATE
9	Πρόσβαση σε δίκτυα	Μπορεί να αποκτηθεί πρόσβαση σε δίκτυα	BLUETOOTH | INTERNET
10	Προσωπικά δεδομένα	Μπορούν να μεταδοθούν προσωπικά δεδομένα	INTERNET & (READ_CALENDAR | READ_CALL_LOG | READ_CONTACTS | READ_HISTORY_BOOKMARKS | READ_PROFILE | READ_SOCIAL_STREAM | READ_USER_DICTIONARY)
11	Spam	Μπορούν να τοποθετηθούν spam	INSTALL_SHORTCUT | SET_WALLPAPER
12	Καταγραφές	Μπορούν να μεταδοθούν video, φωτογραφίες, ηχογραφήσεις	INTERNET & (CAMERA | RECORD_AUDIO)
13	Ασφάλεια	Μπορούν να αλλάξουν οι ρυθμίσεις ασφάλειας	DISABLE_KEYGUARD
14	Σύνταξη Μηνυμάτων	Μπορούν να συνταχθούν μηνύματα	WRITE_SMS

Βιβλιογραφία

Ξενόγλωσση

(1) Android Developers, “Security Tips”, διαθέσιμο: http://developer.android.com/training/articles/security-tips.html, τελευταία προσπέλαση: 17/01/2016.
(2) Android Developers, “System Permissions”, διαθέσιμο: http://developer.android.com/guide/topics/security/permissions.html, τελευταία πρόσβαση: 17/01/2016.
(3) Android, “Security”, διαθέσιμο: https://source.android.com/security/, τελευταία προσπέλαση: 17/01/2016.
(4) Balebako, R., Marsh, A., Lin, J., Hong, J. and Cranor, L. F. (2014), “The Privacy and Security Behaviors of Smartphone App Developers”, Workshop on Usable Security (USEC 2014), San Diego, CA.
(5) Enck, W., Gilbert, P., Chun, B., Cox, L.P., Jung, J., McDaniel, P. and, Sheth, A.N. (2010), “TaintDroid - An Information Flow Tracking System for Real-Time Privacy Monitoring on Smartphones”, Proceedings of the 9th USENIX conference on Operating systems design and implementation, p.1-6, Vancouver, BC, Canada.
(6) European Parliament (1995), “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, Official Journal of the EC, 23, 6.
(7) Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D. (2012), “Android permissions: User attention, comprehension, and behavior”, In Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM, p. 3.
(8) IzzySoft (2015), “IzzyOnDroid”, διαθέσιμο: StripSearch helps you find apps by permission, τελευταία προσπέλαση: 17/01/2016.
(9) Hoffman, C. (2015), “Android’s App Permissions Were Just Simplified - Now They’re Much Less Secure”, διαθέσιμο: http://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure/, τελευταία προσπέλαση: 17/01/2016.
(10) Hoffman, C. (2015), “How to Manage App Permissions on Android 6.0”, διαθέσιμο: http://www.howtogeek.com/230683/how-to-manage-app-permissions-on-android-6.0/, How-to-Geek, τελευταία πρόσβαση: 17/01/2016.
(11) Jeon, J., Micinski, K.K., Vaughan, J.A., Fogel, A., Reddy, N., Foster, J.S. and Millstein, T. (2012), “Dr. Android and Mr. Hide: fine-grained permissions in android applications”, In Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '12), ACM, New York, NY, USA, 3-14.
(12) Jiang, X., “Anserverbot,” http://www.csc.ncsu.edu/faculty/jiang/ AnserverBot/, 2011.
(13) Jiang, X., “Droidkungfu,” http://www.csc.ncsu.edu/faculty/jiang/DroidKungFu.html, 2011.

(14) Johnson, R., Wang, Z., Gagnon, C., Stavrou, A. (2012), "Analysis android applications' permissions", In Proceedings of the 6th International Conference on Software Security and Reliability.
(15) Mylonas, A. (2008), "Smartphone spying tools", MSc Thesis, Royal Holloway, University of London.
(16) Rohrer, F., Zhang, Y., Chitkushev, L., and Zlateva, T. (2012), "Poster: Role based access control for android (rbaca)", Technical report, Boston University, MA USA, διαθέσιμο: https://www.acsac.org/2012/program/posters/poster09.pdf, τελευταία προσπέλαση: 17/01/2016.
(17) Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., and& Molloy, I. (2012), "Android permissions: a perspective combining risks and benefits", In Proceedings of the 17th ACM symposium on Access Control Models and Technologies, ACM, New York, USA, pp. 13-22.
(18) Sims, G. (2012), "How secure is Android?", διαθέσιμο: http://www.androidauthority.com/secure-android-90523/, τελευταία προσπέλαση: 17/01/2016.
(19) Symantec, "Geinimi," https://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99, 2010.
(20) Theoharidou, M., Mylonas, A. and Gritzalis, D. (2012), "A risk assessment method for smartphones", In Proc. of the 27th IFIP Information Security and Privacy Conference, Springer (AICT 376), p.443-456.
(21) Tsavli, M., Efraimidis, P. , Katos, V., Mitrou, L. (2015), "Reengineering the user: privacy concerns about personal data on smartphones", Information & Computer Security, Vol. 23 Iss: 4, pp.394 – 405.
(22) Vidas, T., Christin, N. and Cranor, L. (2011), "Curbing android permission creep", In Proceedings of the Web, Vol. 2.
(23) Wei, X., Gomez, L., Neamtiu, I., and Faloutsos, M. (2012), "Permission evolution in the android ecosystem", In Proceedings of the 28th Annual Computer Security Applications Conference, ACM, New York, NY, USA, pp. 31-40.
(24) West, R. (2008), "The Psychology of Security", Communications of the ACM, Vol. 51, No. 4, pp. 34-41.

Ελληνική

(25) Καλλονιάτης Χρήστος, Μηχανισμοί Ελέγχου Προσπέλασης, Σημειώσεις στα πλαίσια του μαθήματος «Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας», Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας, Πανεπιστήμιο Αιγαίου, διαθέσιμο:, τελευταία πρόσβαση: 17/01/2016.
(26) Ομάδα Εργασίας για την Προστασία των Προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, Γνώμη 02/2013 για τις εφαρμογές των έξυπνων συσκευών, αρ. 29 της Οδηγίας 95/46/ΕΚ, διαθέσιμο: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_el.pdf, τελευταία προσπέλαση: 17/01/2016.