Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Ζητήματα Προστασίας Προσωπικών Δεδομένων σε «Έξυπνες» Εφαρμογές Εντοπισμού Θέσεως.

Στυλιανός Μονογιός

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ζητήματα Προστασίας Προσωπικών Δεδομένων σε «Έξυπνες» Εφαρμογές Εντοπισμού Θέσεως.

Στυλιανός Μονογιός

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

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

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2019

Περίληψη

Τα τελευταία χρόνια έχουμε παρακολουθήσει μια στροφή προς εξατομικευμένες εφαρμογές και υπηρεσίες που βασικό στοιχείο πολλών από αυτών είναι η δυνατότητα εξαγωγής της τρέχουσας τοποθεσίας και η πρόβλεψη της μελλοντικής θέσης των χρηστών με βάση τους ενσωματωμένους αισθητήρες των συσκευών. Ως εκ τούτου, υπάρχουν ανησυχίες σχετικά με την ιδιωτική ζωή γύρω από τις εφαρμογές, με τους χρήστες να μην γνωρίζουν εάν και ποια προσωπικά δεδομένα διαρρέουν κατά την χρήση τους. Ορισμένες εφαρμογές ίσως επιτρέπουν τη συγκεκαλυμμένη συλλογή και μετάδοση σε τρίτους των πληροφοριών τοποθεσίας ενός χρήστη την παρακολούθηση των επικοινωνιών του, όπως ευαίσθητα και προσωπικά δεδομένα. Η παρούσα Μεταπτυχιακή Διατριβή μελετά το βαθμό προστασίας προσωπικών δεδομένων, με βάση τις αλλαγές που υπεισέρχονται από το νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), μέσα από την χρήση «έξυπνων» εφαρμογών κινητών συσκευών και πιο συγκεκριμένα αυτών που καθιστούν δυνατό τον εντοπισμό της πραγματικής μας θέσης.

Για την διεκπεραίωση του ανωτέρου σκοπού θα αναλυθούν και θα παρουσιαστούν συνολικά πέντε δημοφιλείς εφαρμογές εντοπισμού θέσεως σε λειτουργικό σύστημα Android (Google Maps, Sygic GPS Navigation & Maps, TomTom GPS Navigation - Traffic Alerts & Maps, MAPS.ME, MapFactor GPS Navigation Maps). Για την εξέταση των εφαρμογών πραγματοποιείται Δυναμική Ανάλυση με τη χρήση δύο άλλων εφαρμογών, του Lumen Privacy Monitor και του Inspeckage-Android Package Inspector.

Τα αποτελέσματα της παρούσας Μεταπτυχιακής Διατριβής καταδεικνύουν ότι πράγματι, υφίσταται μία συνεχής και όχι πάντα διαφανής προς το χρήστη επικοινωνία μεταξύ εφαρμογών και βιβλιοθηκών τρίτων μερών, με συνακόλουθο αποτέλεσμα τη διαρροή προσωπικών και ευαίσθητών δεδομένων του χρήστη μέσω των ανωτέρω εφαρμογών. Επιπλέον παρουσιάζεται το φαινόμενο της «επίθεσης κλιμάκωσης προνομίων» των βιβλιοθηκών, συνέπεια του γεγονότος ότι οι βιβλιοθήκες κληρονομούν το σύνολο των δικαιωμάτων κάθε εφαρμογής. Τέλος, παρατηρήθηκε ότι οι εφαρμογές δεν πληρούν πάντα τα απαραίτητα κριτήρια ασφαλείας και διαφάνειας, με αποτέλεσμα τα προσωπικά δεδομένα του χρήστη να βρίσκονται έκθετα στα χέρια των επίδοξων υπηρεσιών παρακολούθησης και διαφήμισης.

Λέξεις Κλειδιά: Προσωπικά Δεδομένα, GDPR, Ιδιωτικότητα, Δημιουργία προφίλ, Location Based Services, Ground Positioning System, Δυναμική Ανάλυση, Third Parties Libraries.

Summary

Recently, we have seen a shift towards personalized applications and services. The vast majority of them have a common key element that is exporting the current location and predicting the future location of users based on built-in device sensors. This has leaded to the emerge of a number of concerns regarding privacy around applications, with users not knowing whether and what personal data is leaking during usage. Some applications may allow the covert collection and transmission of information to third-party sites by monitoring communications and by exposing sensitive and personal data. This Master Thesis examines the level of personal data protection, based on the changes introduced by the new GDPR, through the use of "smart" mobile applications, and in particular those that make it possible to identify our real time location.

Top five popular positioning applications on the Android operating system (Google Maps, Sygic GPS Navigation & Maps, TomTom GPS Navigation, MAPS.ME, and MapFactor GPS Navigation Maps) will be examined and presented. Dynamic Analysis is performed in order to test the above applications using two other applications the Lumen Privacy Monitor and the Inspeckage-Android Package Inspector.

The results of this Postgraduate Thesis demonstrate that there is a continuous and not always transparent to user communication between applications and third-party libraries, with the consequent leakage of personal and sensitive user data through the above applications. Additionally, the phenomenon of "privilege escalation attack" of libraries is a consequence of the fact that libraries inherit all the rights of each application. Finally, it has been noticed that applications do not meet the necessary security and transparency criteria. On the contrary, they expose the user's personal data to prospective tracking and advertising services instead.

Keywords: Personal Data, GDPR, Privacy, Profiling, Location Based Services, Ground Positioning System, Dynamic Analysis, Third Parties Libraries.

Ευχαριστίες

Με την ολοκλήρωση της Μεταπτυχιακής Διατριβής μου, θα ήθελα να ευχαριστήσω θερμά τον επιβλέπων καθηγητή μου Δρ. Κωνσταντίνο Λιμνιώτη για την επιστημονική ενίσχυση που μου παρείχε, την πολύτιμη βοήθειά του, την συνεχή επίβλεψη και καθοδήγηση του για την ολοκλήρωση της παρούσας εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω την σύζυγο μου και την οικογένεια μου για την κατανόηση τους και την αμέριστη συμπαράσταση τους, όχι μόνο για την ολοκλήρωση της εν λόγω διατριβής, αλλά και καθ΄ όλη την διάρκεια των μεταπτυχιακών μου σπουδών.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Ζούμε σε μια εποχή όπου η τεχνολογία αλλάζει από δευτερόλεπτο σε δευτερόλεπτο, είναι ένας κύκλος χωρίς αρχή, μέση και τέλος που συνεχώς διευρύνεται ανανεώνεται και ποτέ δεν σταματά να εξελίσσεται. Πλέον, η «επέλαση» της τεχνολογίας αντικατοπτρίζει κάθε πτυχή της καθημερινότητάς του σύγχρονου ανθρώπου. Η γρήγορη διάδοση της ασύρματης σύνδεσης στο διαδίκτυο και σε συνδυασμό με την ταχύτατη ανάπτυξη στον τομέα των τηλεπικοινωνιών, έχουν ως αποτέλεσμα την καθημερινή μας πρόσβαση σε όγκο και ποικιλία πληροφοριών που μόλις μια δεκαετία πριν ούτε καν είχαμε φανταστεί. Σε αυτή την έρευνα θα επικεντρωθούμε κυρίως στην εξέλιξη των «έξυπνων» συσκευών, οι οποίες μπήκαν στη ζωή μας τόσο ομαλά που μπόρεσαν όλες οι ηλικίες να εξοικειωθούν μαζί τους.

Οι «έξυπνες» συσκευές και ειδικότερα τα «έξυπνα» κινητά τηλέφωνα ή αλλιώς smartphones έχουν γίνει αναπόσπαστο κομμάτι στη ζωή κάθε ανθρώπου. Η δημοτικότητά τους οφείλεται κυρίως στη διαθεσιμότητα ενός ευρέος φάσματος εφαρμογών μέσω των λειτουργικών συστημάτων, όπως για παράδειγμα Android και iPhone OS, οι οποίες εμπλουτίζουν την καθημερινότητα και αυξάνουν τη χρηστικότητα. Το να μπορεί κανείς να έχει άμεση επικοινωνία σε όποιο μέρος του πλανήτη βρίσκεται ό,τι ώρα θέλει χωρίς καθόλου κόστος, το να μπορεί να κατευθυνθεί προς ένα σημείο που επιθυμεί με τη χρήση της τεχνολογίας εντοπισμού θέσεως, το

να μπορεί να φωτογραφηθεί, να επεξεργαστεί φωτογραφίες και βίντεο είναι ορισμένα από τα θετικά στοιχεία ενός smartphone.

Στον σημερινό κόσμο, οι χρήστες εξαρτώνται σε μεγάλο βαθμό από τα «έξυπνα» κινητά τους, σε σημείο που μερικές φορές ξεχνούν την αξία της ιδιωτικής ζωής, παραχωρώντας σε τρίτα μέρη προσωπικά δεδομένα. Αναμφίβολα, αυτό αποτελεί ένα τεράστιο πρόβλημα δεδομένου ότι στο εγγύς μέλλον, έως το 2020, εκτιμάται ότι θα υπάρχουν περίπου 50 δισεκατομμύρια συσκευές συνδεδεμένες στο Διαδίκτυο [1]. Ως εκ τούτου, υπάρχουν ανησυχίες σχετικά με την ιδιωτική ζωή γύρω από τις εφαρμογές, με τους χρήστες να μην γνωρίζουν εάν και ποια προσωπικά δεδομένα διαρρέουν κατά την χρήση τους. Ορισμένες εφαρμογές ίσως επιτρέπουν τη συγκεκαλυμμένη συλλογή και μετάδοση σε τρίτους των πληροφοριών τοποθεσίας ενός χρήστη την παρακολούθηση των επικοινωνιών του όπως κείμενα, ηλεκτρονικά μηνύματα και τηλεφωνήματα. Επιπλέον, πιθανόν οι πληροφορίες της υπηρεσίας εντοπισμού θέσης να μοιράζονται με άγνωστα τρίτα μέρη, πληροφορίες οι οποίες να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων όπως συνήθειες/προτιμήσεις του χρήστη, η συμπεριφορά του, η διάθεση του, με απώτερο σκοπό την δημιουργία προφίλ ενός χρήστη (profiling). Αποτελεί άξιων απορίας το ότι για να «κατεβάσει» ο χρήστης και να εγκαταστήσει οποιαδήποτε εφαρμογή χρειάζεται να αποκαλύψει προσωπικά στοιχεία, όπως τις επαφές στο κινητό του, τα μηνύματα και την τοποθεσία του και συνεπώς με ένα απλό «κλικ» στέλνουμε σε τρίτους πληροφορίες, όχι πάντα για σαφείς σκοπούς, μόνο και μόνο για να παίξει ένα παιχνίδι ή να μεταποιήσει μια φωτογραφία. Γιατί ως χρήστες το δεχόμαστε όμως; Είναι όλα "δούναι και λαβείν". Χρειάζεσαι μια εφαρμογή; Πρέπει να δώσεις πρόσβαση στα στοιχεία σου.

Ζητήματα προστασίας προσωπικών δεδομένων στον τομέα των «έξυπνων» εφαρμογών αποτελούν μία σύγχρονη νομική και τεχνολογική πρόκληση, καθότι ο «πυρετός» των νέων εφαρμογών για τις αγαπημένες μας έξυπνες συσκευές δεν έχει τέλος και δεδομένου ότι από τις 25 Μαΐου 2018 είναι σε εφαρμογή ο Γενικός Κανονισμός (ΕΕ) 2016/679 για την προστασία προσωπικών δεδομένων, ο οποίος θέτει πολλές υποχρεώσεις, για τις οποίες υπάρχουν πολλά ανοιχτά ερωτήματα ως προς το βαθμό στον οποίο υλοποιούνται. Ο Γενικός Κανονισμός πλέον αποτελεί ένα κοινό πλαίσιο ρυθμίσεων για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα προσωπικού χαρακτήρα των πολιτών της Ευρωπαϊκής Ένωσης, ανεξαρτήτως τόπου εγκατάστασης του οργανισμού που καθορίζει την επεξεργασία των δεδομένων.

Τα τελευταία χρόνια έχουμε παρακολουθήσει μια στροφή προς εξατομικευμένες εφαρμογές και υπηρεσίες που βασικό στοιχείο πολλών από αυτών είναι η δυνατότητα εξαγωγής της τρέχουσας τοποθεσίας και η πρόβλεψη της μελλοντικής θέσης των χρηστών με βάση τους ενσωματωμένους αισθητήρες των συσκευών. Οι εν λόγω καινοτόμες υπηρεσίες εστιάζουν στον εντοπισμό του κινητού του χρήστη με όσο το δυνατόν μεγαλύτερη ακρίβεια και στην αξιοποίηση της θέσης του, όπου και όποτε απαιτείται, ώστε να παρέχονται όλες οι διαθέσιμες πληροφορίες που αφορούν την γεωγραφική θέση του και/ή την γύρω περιοχή στην οποία ευρίσκεται ή κινείται, δηλαδή τον "γεωγραφικό χώρο" των ποικίλων δραστηριοτήτων του (οικονομικών, επιστημονικών, κοινωνικών κ.ά.).

1.1 Ερευνητικά Ερωτήματα

Η παρούσα μεταπτυχιακή διατριβή μελετά τον βαθμό προστασίας προσωπικών δεδομένών μέσα από την χρήση «έξυπνων» εφαρμογών κινητών συσκευών και πιο συγκεκριμένα αυτών που καθιστούν δυνατό τον εντοπισμό της πραγματικής μας θέσης. Θα παρουσιαστούν συνολικά πέντε δημοφιλείς εφαρμογές εντοπισμού θέσεως σε λειτουργικό σύστημα Android, οι οποίες θα εξεταστούν με τη χρήση άλλων εφαρμογών Δυναμικής Ανάλυσης, με απώτερο σκοπό να απαντηθούν τα ακόλουθα ερευνητικά ερωτήματα :

- Εφαρμόζονται μέτρα για την ασφάλεια των προσωπικών δεδομένων του χρήστη μέσα από τη χρήση των «έξυπνων» εφαρμογών προσδιορισμού θέσεως;
- Συλλέγεται και αποστέλλεται υπέρμετρη πληροφορία σε τρίτα μέλη;
- Κατά πόσον γίνεται επεξεργασία ερήμην του χρήστη των προσωπικών του δεδομένων με σκοπό τη δημιουργία προφίλ (profiling);

1.2 Δομή της Μεταπτυχιακής Διατριβής

Όπως αναφέρθηκε προηγουμένως ο βασικός άξονας της παρούσας Μεταπτυχιακής Διατριβής είναι να μελετήσει πέντε δημοφιλείς εφαρμογές για κινητές συσκευές λειτουργικού συστήματος Android, οι οποίες χρησιμοποιούν την υπηρεσία εντοπισμού τοποθεσίας του χρήστη, στα πλαίσια της μελέτης του βαθμού προστασίας των προσωπικών δεδομένων, ένεκα της νέας Ευρωπαϊκής

Οδηγίας GDPR (General Data Protection Regulation) για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα. Ως εκ τούτου η Μεταπτυχιακή Διατριβή λαμβάνει την παρακάτω δομή:

Στο Κεφάλαιο 2 ορίζεται και παρουσιάζεται η «έξυπνη» συσκευή ως ένα αναπόσπαστο κομμάτι της καθημερινότητας του κάθε ανθρώπου στον 21ο αιώνα, επεξηγώντας την αρχιτεκτονική του λειτουργικού συστήματος Android, που πλέον φέρεται από το μεγαλύτερο ποσοστό των κινητών συσκευών παγκοσμίως. Επίσης παρουσιάζεται το μοντέλο διαχείρισης των δικαιωμάτων του λειτουργικού συστήματος Android με σκοπό να γίνει κατανοητός ο τρόπος με τον οποίο το σύστημα αλληλοεπιδρά με τις εφαρμογές αλλά και η λογική που διέπει τις εφαρμογές.

Στο Κεφάλαιο 3 γίνεται μία εκτενής αναφορά στο νέο κανονισμό της Ευρωπαϊκής Ένωσης για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation - GDPR) και αντιπαραβάλλεται με την προηγούμενη σχετική οδηγία 95/46/ΕΚ για την Προστασία των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα. Αναφορά γίνεται και στην οδηγία 2002/58/ΕΚ για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα και την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών. Στην συνέχεια παρέχεται μια πιο λεπτομερής ανάλυση των κινδύνων ιδιωτικότητας μέσα από την συλλογή υπέρμετρης πληροφορίας, παρουσιάζοντας ποια είναι τα πιθανά προσωπικά δεδομένα που πιθανόν να διαρρέουν και τους τρόπους που αυτά πιθανόν να διαβιβάζονται σε τρίτα μέρη.

Στο Κεφάλαιο 4, λόγω και της νέας διάστασης που προσδίδεται στη χρηστικότητα των εφαρμογών που βασίζονται στην δυνατότητα προσδιορισμού της γεωγραφικής θέσης του χρήστη, ορίζεται η Υπηρεσία Προσδιορισμού Θέσης (LBS-Location Based Services) σε μία κινητή συσκευή. Ακολούθως παρουσιάζεται το Παγκόσμιο Σύστημα Προσδιορισμού Θέσης GPS (Global Positioning System) με σκοπό να γίνει ποιο κατανοητό πώς τα προσωπικά δεδομένα που διαρρέουν μέσα από της εφαρμογές με δυνατότητα στο προσδιορισμό της θέσης, μπορούν να παρουσιάσουν πτυχές της προσωπικής και ευαίσθητης πλευράς της ζωής μας.

Στο Κεφάλαιο 5 παρουσιάζεται η σημαντικότητα των εφαρμογών, των Android λειτουργικών συστημάτων όσο αφορά τον επιχειρηματικό τομέα. Επίσης αναλύεται η έννοια του όρου «Υπηρεσίες Τρίτων» ή “Third Parties Services” και γίνεται, μέσα από την παρουσίαση των ευρημάτων διάφορων μελετών, μια προσπάθεια κατανόησης της σχέσης Εφαρμογής-Υπηρεσίας Τρίτου.

Το Κεφάλαιο 6 αποτελεί την ραχοκοκαλιά της Μεταπτυχιακής Διατριβής καθότι παρουσιάζεται η Μεθοδολογία με την οποία προσεγγίστηκε η έρευνα για την προστασίας των προσωπικών δεδομένων μέσα από τις πέντε επιλεγμένες εφαρμογές. Συγκεκριμένα σχεδιάστηκε το περιβάλλον δοκιμών, αναλύθηκε η μέθοδος της δυναμικής ανάλυσης των εφαρμογών, παρουσιάστηκαν τα εργαλεία Lumen Privacy Monitor, το Xposed Framework και το Inspeckage- Android Package Inspector το οποίο αποτελεί ένα Xposed Module και περιεγράφηκε η ακριβής διαδικασία ανάλυσης.

Τέλος, στο Κεφάλαιο 7 παρουσιάζονται τα αποτελέσματα μέσα από την ανάλυση των εφαρμογών μας, με καταγραφή των συμπερασμάτων αλλά και των ενδεχόμενων μελλοντικών ερευνητικών βημάτων.

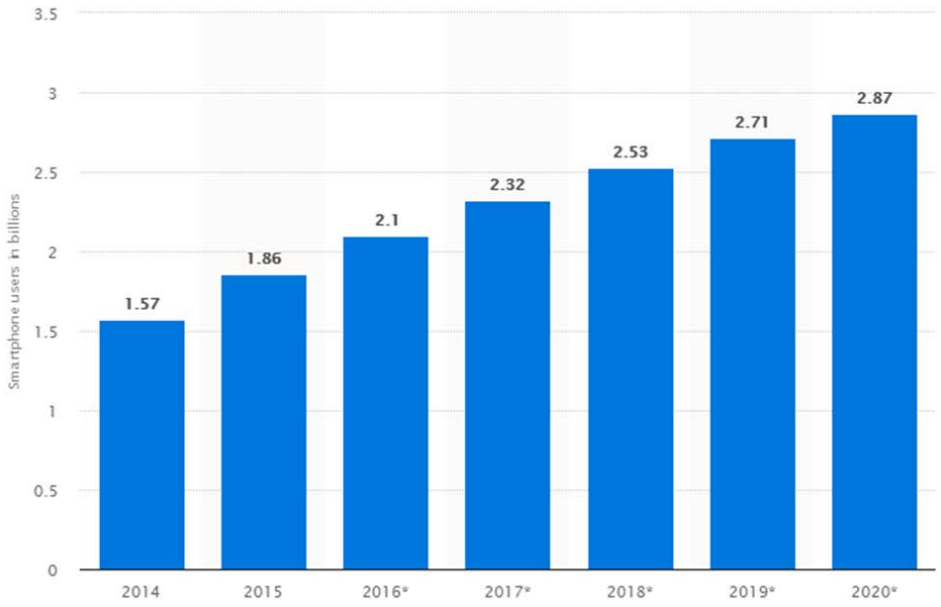
Κεφάλαιο 2
«Έξυπνες» Κινητές Συσκευές – Το Σύστημα Android

Η χρήση του smartphone έχει γίνει καθημερινή αναγκαιότητα για τους περισσότερους ανθρώπους σε οικονομικά προχωρημένες περιοχές του κόσμου, καθώς επιτρέπουν στους χρήστες να εκτελούν κοινωνικά και επιχειρηματικά καθήκοντα με απομακρυσμένο τρόπο (π.χ. πληρωμές, κοινωνική δικτύωση και παιχνίδια). Ένας παράγοντας κλειδί σε αυτό το είδος συμπεριφοράς είναι η αφθονία των κινητών εφαρμογών, ένας μεγάλος αριθμός των οποίων προσφέρονται δωρεάν. Επί του παρόντος Κεφαλαίου γίνεται μία εκτενής ανάλυση της έννοιας «έξυπνη συσκευή», επεξηγώντας την αρχιτεκτονική του λειτουργικού συστήματος Android, το οποίο αποτελεί το κυριότερο Λειτουργικό σύστημα στην εποχή που διανύουμε. Επίσης παρουσιάζεται το μοντέλο διαχείρισης των δικαιωμάτων του λειτουργικού συστήματος Android με σκοπό να γίνει κατανοητός ο τρόπος με τον οποίο το σύστημα αλληλοεπιδρά με τις εφαρμογές αλλά και η λογική που διέπει τις εφαρμογές

2.1 Έξυπνες Κινητές Συσκευές

Το smartphone ή με τον ελληνικό όρο έξυπνο τηλέφωνο, είναι ένα κινητό τηλέφωνο βασισμένο σε ένα λειτουργικό σύστημα με προηγμένη υπολογιστική ικανότητα σε σχέση με ένα συμβατικό κινητό τηλέφωνο. Ως στρατηγική του μάρκετινγκ, ο όρος Smartphone εισήχθη στην αγορά ως μια νέα κατηγορία κινητών τηλεφώνων που παρέχει ολοκληρωμένες υπηρεσίες βασισμένες στους τομείς της επικοινωνίας, της πληροφορικής και της κινητής τηλεφωνίας, όπως για παράδειγμα η φωνητική επικοινωνία, η ανταλλαγή μηνυμάτων, οι εφαρμογές διαχείρισης προσωπικών πληροφοριών και η δυνατότητα ασύρματης επικοινωνίας [1]. Είναι εξοπλισμένο με τις δυνατότητες προβολής φωτογραφιών, παιχνιδιών, αναπαραγωγής βίντεο, πλοήγησης, ενσωματωμένης κάμερας, αναπαραγωγής ήχου, εικόνας και εγγραφής, αποστολής/λήψης ηλεκτρονικού ταχυδρομείου, ενσωματωμένων εφαρμογών για κοινωνικές ιστοσελίδες και περιήγησης στο Διαδίκτυο με ασύρματη συνδεσιμότητα και πολλά άλλα.

Οι τελευταίες έρευνες δείχνουν ότι η δημοτικότητα των «έξυπνων» κινητών τηλέφωνων αυξάνεται στο ευρύ κοινό με γοργούς ρυθμούς. Αρχικά, χρησιμοποιούνταν κυρίως για επαγγελματικούς σκοπούς λόγω του κόστους τους , αλλά πλέον είμαστε περικυκλωμένοι από αυτά λόγω της μείωσης του κόστους τους σε συνδυασμό με την αύξηση των παροχών κινητών συσκευών. Επιπλέον, λόγω της γενικευμένης φύσης τους μπορούν να βρουν χρήση σε εκπαιδευτικά ιδρύματα, νοσοκομεία, δημόσιους χώρους, εμπορικά κέντρα κλπ. Πιο κάτω παρουσιάζεται ο αριθμός πωλήσεων κινητών συσκευών σε δισεκατομμύρια με την πάροδο του χρόνου.



Πίνακας 2.1: Μεταβολή του πλήθους των χρηστών «έξυπνων» συσκευών από το έτος 2014 έως το 2020 [3]

Τα λειτουργικά συστήματα που χρησιμοποιούνται από τις έξυπνες κινητές συσκευές περιλαμβάνουν, μεταξύ άλλων, το Android της Google, το iOS της Apple, το Symbian της Nokia, το BlackBerry OS της RIM, το Bada της Samsung, τα Windows Phone της Microsoft, το webOS της Hewlett-Packard, καθώς και ενσωματωμένες διανομές Linux όπως το Maemo και το MeeGo. Τέτοιου είδους λειτουργικά συστήματα μπορούν να εγκατασταθούν σε πολλά διαφορετικά μοντέλα κινητών τηλεφώνων και συνήθως κάθε συσκευή μπορεί να λάβει πολλές ενημερωμένες εκδόσεις λογισμικού λειτουργικού συστήματος κατά τη διάρκεια ζωής της [2].

2.2 Λειτουργικό Σύστημα Android

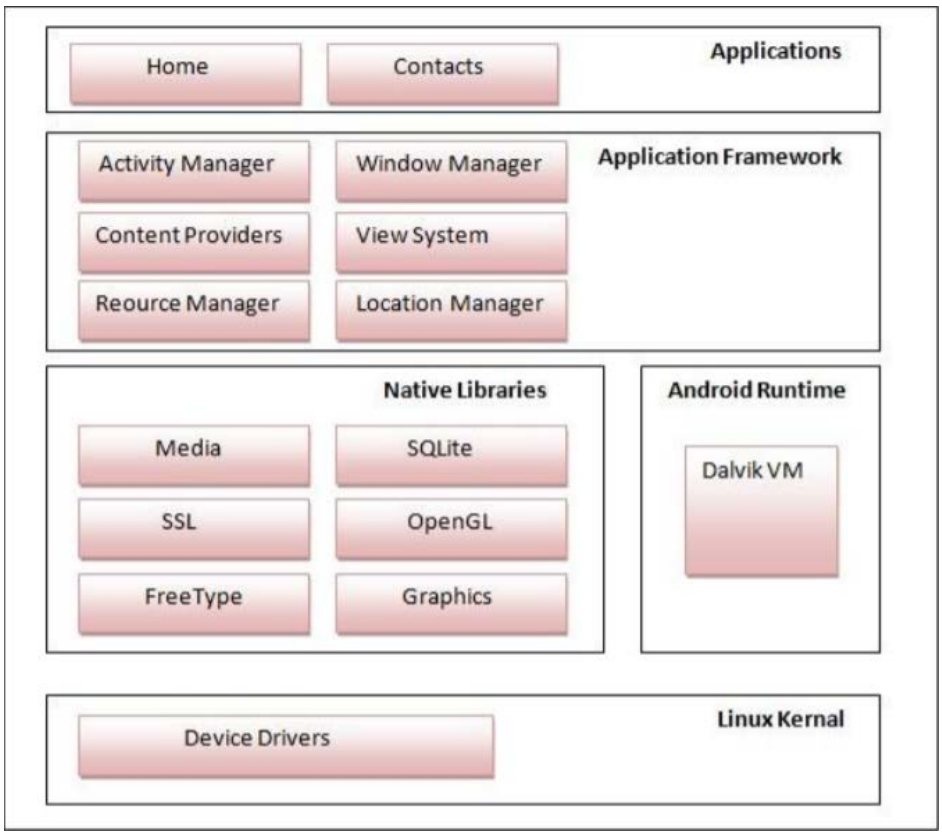
Όπως προαναφέρθηκε, το Android είναι ένα λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας το οποίο «τρέχει» τον πυρήνα του λειτουργικού Linux. Δημιουργήθηκε από την GOOGLE και επιτρέπει στους κατασκευαστές λογισμικού να συνθέτουν κώδικα με την χρήση της γλώσσας προγραμματισμού Java, ελέγχοντας την συσκευή μέσω βιβλιοθηκών λογισμικού ανεπτυγμένων από την Google. Το Android είναι μια ολοκληρωμένη στοίβα ανοιχτού κώδικα λογισμικού για φορητές συσκευές, που συνοδεύεται από λειτουργικό σύστημα και βασικές εφαρμογές που βασίζονται σε Linux και Java. Αποτέλεσμα αυτού το Android πλέον να έχει πολυάριθμους προγραμματιστές, οι οποίοι γράφουν εφαρμογές σε όλο τον κόσμο [4].

Το Android είναι συνήθως το πιο εξειδικευμένο λειτουργικό σύστημα για κινητές συσκευές που κατέχει μερίδιο αγοράς 75,39% σύμφωνα με τα τελευταία στατιστικά μηνός Μαρτίου 2019 και πάνω από 2.100.000 διαθέσιμες εφαρμογές στο κατάστημα αναπαραγωγής της Google το γνωστό Google Play. Το Google Play, παλαιότερα γνωστό ως Android Market, είναι μια πλατφόρμα διανομής ψηφιακών εφαρμογών για το Android, καθώς και ηλεκτρονικό κατάστημα που αναπτύχθηκε και διαχειρίζεται η Google. Η υπηρεσία επιτρέπει στους χρήστες να κατεβάζουν μουσική, βιβλία, περιοδικά, καταλόγους καθώς και εφαρμογές που κυκλοφορούν μέσω της Google.

Εικόνα 2.1: Μερίδιο αγοράς κινητών Λειτουργικών Συστημάτων παγκοσμίως [5].

2.2.1 Η Αρχιτεκτονική του Λειτουργικού Συστήματος Android

Το σύστημα της Google Android είναι ένα σύστημα, όπως προαναφέρθηκε, βασισμένο στο Linux που χρησιμοποιεί την αρχιτεκτονική στοίβας λογισμικού. Όπως φαίνεται στην Εικόνα 2.2, η αρχιτεκτονική του Android αποτελείται από τέσσερα στρώματα: τον πυρήνα (Linux Kernel), τις βιβλιοθήκες (Libraries) και το Android Runtime, το πλαίσιο εφαρμογών (Application framework) και τις εφαρμογές (Applications). Κάθε στρώμα σχετίζεται με την κατώτερη βαθμίδα/ενθυλάκωση, ενώ παρέχεται διεπαφή προς το άνω μέρος [4].



Εικόνα 2.2: Η αρχιτεκτονική του Λειτουργικού Συστήματος Android [4].

Στη συνέχεια παρουσιάζεται το κάθε στρώμα της αρχιτεκτονικής του λειτουργικού αυτού συστήματος.

Α) Εφαρμογές (Applications): Στο στρώμα αυτό περιέχονται όλες οι εφαρμογές του χρήστη όπως τα προγράμματα SMS, το ημερολόγιο, οι χάρτες πορείας, τα πρόγραμμα περιήγησης, οι επαφές, καθώς και άλλα. Όλα αυτά τα προγράμματα εφαρμογών σχεδιάζονται σε γλώσσα προγραμματισμού Java.

Β) Πλαίσιο εφαρμογών (Application Framework): Ο προγραμματιστής έχει τη δυνατότητα πρόσβασης σε όλα τα API (Application Interfaces) των βασικών προγραμμάτων. Το πλαίσιο εφαρμογών/Application Framework διευκολύνει την επαναχρησιμοποίηση των συστατικών των προγραμμάτων. Οποιαδήποτε άλλη εφαρμογή μπορεί εύκολα να απελευθερώσει τα λειτουργικά συστατικά της διαμέσου του Application Framework και άλλες εφαρμογές να έχουν πρόσβαση και να κάνουν χρήση αυτής της δυνατότητας. Επομένως οι χρήστες είναι σε θέση να υποκαταστήσουν τα συστατικά ενός προγράμματος με αυτόν τον συγκεκριμένο μηχανισμό επαναχρησιμοποίησης.

Το πλαίσιο Android περιλαμβάνει τις ακόλουθες βασικές υπηρεσίες [6]:

- Διαχείριση δραστηριοτήτων (Activity Manager) - Ελέγχει όλες τις πτυχές του κύκλου ζωής της εφαρμογής και της στοίβας δραστηριοτήτων.

- Παροχέας περιεχομένου (Content Providers) - Επιτρέπει στις εφαρμογές να δημοσιεύουν και να μοιράζονται δεδομένα με άλλες εφαρμογές.

- Διαχειριστής πόρων (Resource Manager) - Παρέχει πρόσβαση σε ενσωματωμένους πόρους χωρίς κώδικα, όπως κείμενα, ρυθμίσεις χρωμάτων και διατάξεις διασύνδεσης χρήστη.

- Διαχείριση ειδοποιήσεων (Notifications Manager) - Επιτρέπει στις εφαρμογές να εμφανίζουν ειδοποιήσεις στον χρήστη.

- Προβολή συστήματος (View System) - Ένα εκτεταμένο σύνολο προβολών που χρησιμοποιείται για τη δημιουργία διεπαφών χρήστη των εφαρμογών.

- Διαχείριση πακέτων (Package Manager) - Το σύστημα με το οποίο οι εφαρμογές είναι σε θέση να βρουν πληροφορίες σχετικά με άλλες εφαρμογές που είναι εγκατεστημένες στη συσκευή.

- Διαχείριση τηλεφωνίας (Telephony Manager) - Παρέχει τις υπηρεσίες τηλεφωνίας που είναι διαθέσιμες στη συσκευή, όπως η κατάσταση και οι πληροφορίες συνδρομητών.

- Διαχείριση τοποθεσίας (Location Manager) - Παρέχει πρόσβαση στις υπηρεσίες τοποθεσίας επιτρέποντας σε μια εφαρμογή να λαμβάνει ενημερώσεις σχετικά με τις αλλαγές τοποθεσίας.

Γ) Libraries And Google Android Runtime: Η βιβλιοθήκη χωρίζεται σε δύο συνιστώσες: Την Android Runtime καθώς και την Βιβλιοθήκη Android. Το Android Runtime στην πραγματικότητα αποτελείται από μια Java Core Library και την Dalvik εικονική μηχανή. Η εικονική μηχανή Dalvik είναι στην πραγματικότητα περιβάλλον εικονικής μηχανής και τείνει να κάνει κάποιες συγκεκριμένες βελτιώσεις για την κινητή συσκευή. Στην Dalvik VM (DVM) εκτελούνται όλες οι εφαρμογές του λειτουργικού συστήματος Android. Μέσω αυτής, η συσκευή είναι σε θέση να εκτελέσει πολλαπλά εικονικά μηχανήματα για αποδοτικότερη διαχείριση της ενέργειάς της. Συνεπώς η κάθε εφαρμογή εκτελείται καταλαμβάνοντας διαφορετική εικόνα του Dalvik VM κάθε

φορά. Για το σκοπό αυτό αρχεία τύπου Java μεταγλωττίζονται σε αρχεία τύπου .class μέσω του java compiler και στην συνέχεια αυτά τα αρχεία μεταγλωττίζονται σε αρχεία τύπου .dex. Τα αρχεία αυτά καταλήγουν στη DVM έτσι ώστε να παραχθεί ο κώδικας της εφαρμογής και να εκτελεστεί από την CPU. Τα αρχεία .apk περιέχουν αρχεία τύπου .dex τα οποία μπορούν να εκτελεστούν στη DVM. Αυτή η εικονική μηχανή δημιουργήθηκε για καλύτερη διαχείριση τόσο της μπαταρίας, όσο και της επεξεργαστικής ισχύος των κινητών τηλεφώνων. Από την έκδοση 4.4 υποστηρίζεται ο νέος συμβολομεταφραστής ART - «Android Runtime» ο οποίος όμως δεν είναι προεπιλεγμένος στην αρχική εγκατάσταση. Η κύρια διαφορά με τον προηγούμενο είναι ότι ο πρώτος μεταγλωττίζει τα αρχεία την στιγμή που τα εκτελεί σε αντίθεση με τον τελευταίο ο οποίος την υλοποιεί την παραπάνω διεργασία στην φάση εγκατάστασης.

Επίσης η βιβλιοθήκη συστήματος Google Android υποστηρίζει το πλαίσιο εφαρμογής (Application Framework) και αποτελεί συνήθως ένα σημαντικό σύνδεσμο που το συνδέει με τον Linux Kernel. Αυτή η βιβλιοθήκη συστήματος έχει αναπτυχθεί στην γλώσσα C ή C ++. Ορισμένες από τις βασικές βιβλιοθήκες παρατίθενται παρακάτω [6]:

- Βιβλιοθήκη System c - μια υλοποίηση της βασικής βιβλιοθήκης (libc) του συστήματος για ενσωματωμένες συσκευές που βασίζονται στο Linux.
- SQLite - Χρησιμοποιείται για την πρόσβαση σε δεδομένα που δημοσιεύονται από παρόχους περιεχομένου και περιλαμβάνει τις κλάσεις διαχείρισης βάσεων δεδομένων SQLite.
- SSL - Χρησιμοποιείται για την παροχή ασφάλειας στο διαδίκτυο.
- SGL - ο μηχανισμός γραφικών 2D.
- Libwebcore - μια σύγχρονη μηχανή αναζήτησης Ιστού που τροφοδοτεί τόσο τον browser του Android όσο και μια ενσωματωμένη προβολή ιστού.
- OpenGL - Χρησιμοποιείται για την παροχή διεπαφής Java στο API απεικόνισης γραφικών OpenGL/ES 3D.
- Πλαίσιο μέσων (Media framework) - Χρησιμοποιείται για την παροχή διαφορετικού κώδικα πολυμέσων που επιτρέπουν την εγγραφή και την αναπαραγωγή διαφορετικών μορφών πολυμέσων.

- Web Kit - Είναι ο μηχανισμός αναζήτησης που χρησιμοποιείται για την προβολή περιεχομένου στο διαδίκτυο ή περιεχομένου HTML.

Δ) Linux Kernel: Ο πυρήνας συστήματος της Google Android βασίζεται στον πυρήνα του Linux 2.6. Οι λειτουργίες όπως η εσωτερική αποθήκευση, η διαχείριση διεργασιών, το πρωτόκολλο επικοινωνιών μέσω διαδικτύου, η μονάδα δίσκου βάσης και άλλες βασικές υπηρεσίες βασίζονται επίσης στον πυρήνα του Linux.

2.2.2 Το Μοντέλο Διαχείρισης των Δικαιωμάτων του Λειτουργικού Συστήματος Android

Ο σκοπός μιας άδειας είναι να προστατεύσει το απόρρητο ενός χρήστη Android. Οι εφαρμογές Android πρέπει να ζητούν άδεια πρόσβασης σε προσωπικά δεδομένα χρήστη, όπως επαφές και SMS, καθώς και ορισμένες λειτουργίες του συστήματος, όπως κάμερα και διαδίκτυο. Ανάλογα με την λειτουργία κάθε εφαρμογής, το σύστημα μπορεί να χορηγήσει αυτόματα την άδεια ή μπορεί να ζητήσει από το χρήστη να εγκρίνει το αίτημα.

Ένα κεντρικό σημείο σχεδιασμού της αρχιτεκτονικής ασφαλείας του Android είναι ότι καμία εφαρμογή, από προεπιλογή, δεν έχει άδεια να εκτελέσει οποιεσδήποτε λειτουργίες που θα έχουν αρνητικές επιπτώσεις σε άλλες εφαρμογές, στο λειτουργικό σύστημα ή στον χρήστη. Αυτό περιλαμβάνει την ανάγνωση ή τη χρήση προσωπικών δεδομένων του χρήστη, όπως επαφές ή μηνύματα ηλεκτρονικού ταχυδρομείου, ανάγνωση ή γραφή αρχείων άλλης εφαρμογής, πρόσβασης στο δίκτυο, διατήρηση της αφύπνισης και ούτω καθεξής.

Μια εφαρμογή πρέπει να δημοσιοποιεί τα δικαιώματα που απαιτεί, συμπεριλαμβάνοντας τις ετικέτες <uses-permission> στο δηλωτικό της εφαρμογής (app manifest). Εάν η εφαρμογή εμφανίζει κανονικά δικαιώματα στο πρόγραμμά της, δηλαδή δικαιώματα που δεν δημιουργούν μεγάλο κίνδυνο για το απόρρητο του χρήστη ή τη λειτουργία της συσκευής, το σύστημα παρέχει αυτόματα αυτά τα δικαιώματα στην εφαρμογή σας. Πριν από το Android 6.0, τα δικαιώματα που αναφέρονται σε μια εφαρμογή έπρεπε να γίνουν αποδεκτά στο σύνολό τους κατά το χρόνο εγκατάστασης της. Από το Android 6.0 και έπειτα, τα δικαιώματα εξακολουθούν να παρατίθενται στο σύνολό τους στο δηλωτικό της εφαρμογής, αλλά ενδέχεται να γίνουν δεκτά ή να απορριφθούν

επιλεκτικά από τους χρήστες κατά τη διάρκεια της εγκατάστασης [7]. Επομένως αν η εφαρμογή αναφέρεται σε «επικίνδυνα» δικαιώματα, δηλαδή δικαιώματα που ενδέχεται να επηρεάσουν το απόρρητο του χρήστη ή την κανονική λειτουργία της συσκευής, ο χρήστης πρέπει να συμφωνήσει ρητά να παραχωρήσει αυτά τα δικαιώματα. Καταλήγοντας λοιπόν, ο τρόπος με τον οποίο το Android ζητά από τον χρήστη να εκχωρήσει επικίνδυνα δικαιώματα εξαρτάται από την έκδοση του Android που εκτελείται στη συσκευή του χρήστη και την έκδοση συστήματος που θα εγκατασταθεί και θα λειτουργήσει η εφαρμογή.

Αξίζει να σημειωθεί ότι οι άδειες δεν απαιτούνται μόνο για την λειτουργικότητα του συστήματος. Οι υπηρεσίες που παρέχονται από τις εφαρμογές μπορούν επίσης να επιβάλουν προσαρμοσμένα δικαιώματα για να περιορίσουν ποιος μπορεί να τις χρησιμοποιήσει [8]. Για παράδειγμα:

- Άδεια ενεργοποίησης δραστηριότητας (Activity permission enforcement): Οι άδειες που ισχύουν χρησιμοποιώντας το χαρακτηριστικό "δικαιώματα" του Android: στην ετικέτα <activity> του δηλωτικού περιορίζουν ποιος μπορεί να ξεκινήσει τη Δραστηριότητα.

- Εξουσιοδότηση επιβολής υπηρεσίας (Service permission enforcement): Οι άδειες που ισχύουν χρησιμοποιώντας το χαρακτηριστικό "δικαιώματα" του Android: στην ετικέτα <service> του δηλωτικού περιορίζουν ποιος μπορεί να ξεκινήσει ή να δεσμεύσει τη σχετική υπηρεσία.

- Εκτέλεση δικαιωμάτων εκπομπής (Broadcast permission enforcement): Οι δικαιώματα που ισχύουν χρησιμοποιώντας το χαρακτηριστικό "δικαιώματα" του Android: στην ετικέτα <receiver> περιορίζουν ποιος μπορεί να στείλει εκπομπές στο σχετικό BroadcastReceiver.

- Εξουσιοδότηση παροχέα περιεχομένου (Content Provider permission enforcement): Οι άδειες που ισχύουν χρησιμοποιώντας το χαρακτηριστικό "δικαιώματα" του Android: στην ετικέτα <provider> περιορίζουν ποιος μπορεί να έχει πρόσβαση στα δεδομένα σε έναν ContentProvider. Οι παροχείς περιεχομένου έχουν στη διάθεσή τους μια σημαντική πρόσθετη δυνατότητα ασφαλείας που ονομάζεται δικαιώματα URI, η οποία περιγράφεται στη συνέχεια. Σε αντίθεση με τα υπόλοιπα στοιχεία, υπάρχουν δύο χωριστά χαρακτηριστικά δικαιωμάτων που μπορείτε να ορίσετε: Android: readPermission περιορίζει τους χρήστες που διαβάζουν από τον παροχέα και το Android: η WritePermission περιορίζει ποιος μπορεί να γράψει σε αυτήν.

Στη συνέχεια παρουσιάζονται ομαδοποιημένα οι άδειες που απαιτούνται από τις πλείστες εφαρμογές. Οι άδειες οργανώνονται σε ομάδες που σχετίζονται με τις δυνατότητες ή τις λειτουργίες μιας συσκευής. Στο πλαίσιο αυτού του συστήματος ομαδοποίησης, τα αιτήματα αδειών αντιμετωπίζονται σε επίπεδο ομάδας και μια ενιαία ομάδα δικαιωμάτων αντιστοιχεί σε πολλά δικαιώματα στο δηλωτικό της εφαρμογής. Για παράδειγμα, η ομάδα SMS περιλαμβάνει τόσο τις READ_SMS όσο και τις δηλώσεις RECEIVE_SMS. Η ομαδοποίηση των δικαιωμάτων με αυτόν τον τρόπο επιτρέπει στον χρήστη να κάνει πιο σωστές και ενημερωμένες επιλογές, χωρίς να είναι συγκλονισμένοι από σύνθετες και τεχνικές αιτήσεις άδειας.

Permission Group	Descriptions
ACTIVITY_RECOGNITION	Χρησιμοποιείται για δικαιώματα που σχετίζονται με την αναγνώριση δραστηριότητας.
CALENDAR	Χρησιμοποιείται για δικαιώματα εκτέλεσης που σχετίζονται με το ημερολόγιο του χρήστη.
CALL_LOG	Χρησιμοποιείται για δικαιώματα που σχετίζονται με τις λειτουργίες τηλεφωνίας.
CAMERA	Χρησιμοποιείται για δικαιώματα που σχετίζονται με την πρόσβαση στην κάμερα ή τη λήψη εικόνων / βίντεο από τη συσκευή.
CONTACTS	Χρησιμοποιείται για δικαιώματα εκτέλεσης που σχετίζονται με επαφές και προφίλ σε αυτήν τη συσκευή.
MEDIA_AURAL	Χρησιμοποιείται για δικαιώματα που επιτρέπουν την πρόσβαση στη θέση της συσκευής.
MEDIA_VISUAL	Άδεια χρόνου εκτέλεσης που ελέγχει την πρόσβαση στην κοινόχρηστη οπτική συλλογή μέσων του χρήστη, συμπεριλαμβανομένων εικόνων και βίντεο.
PHONE	Χρησιμοποιείται για δικαιώματα που σχετίζονται με την πρόσβαση ήχου μικροφώνου από τη συσκευή.
SMS	Χρησιμοποιείται για δικαιώματα εκτέλεσης που σχετίζονται με τα μηνύματα SMS του χρήστη.
SENSORS	Χρησιμοποιείται για δικαιώματα που σχετίζονται με την πρόσβαση αισθητήρων σώματος ή περιβάλλοντος.
STORAGE	Αυτή η σταθερά καταργήθηκε στο επίπεδο API Q. Αφορά σε δυνατότητα εγγραφής και διαγραφής δεδομένων σε αποθηκευτικά μέσα εντός της συσκευής.

Πίνακας 2.2: Ομαδοποίηση δικαιωμάτων αναλόγως των λειτουργιών τους σε μία συσκευή.

Οι άδειες χωρίζονται σε επίπεδα προστασίας. Το επίπεδο προστασίας εξαρτάται από το ποια αιτήματα άδειας εκτέλεσης απαιτούνται [8]. Υπάρχουν τρία επίπεδα προστασίας που επηρεάζουν τις εφαρμογές τρίτων κατασκευαστών όπως πιο κάτω:

1. Κανονικά δικαιώματα (normal)

   Τα κανονικά δικαιώματα καλύπτουν περιοχές όπου η εφαρμογή σας χρειάζεται πρόσβαση σε δεδομένα ή πόρους έξω από το sandbox της εφαρμογής, αλλά όπου υπάρχει πολύ μικρός κίνδυνος για το απόρρητο του χρήστη ή για τη λειτουργία άλλων εφαρμογών. Για παράδειγμα, η άδεια για τη ρύθμιση της ζώνης ώρας είναι μια κανονική άδεια. Αν μια εφαρμογή δηλώνει στο δηλωτικό της ότι χρειάζεται κανονική άδεια, το σύστημα δίνει

αυτόματα στην εφαρμογή την άδεια κατά την ώρα εγκατάστασης. Το σύστημα δεν προτρέπει τον χρήστη να παραχωρήσει κανονικά δικαιώματα και οι χρήστες δεν μπορούν να ανακαλέσουν αυτά τα δικαιώματα.

2. Δικαιώματα υπογραφής (signature)

Το σύστημα παρέχει αυτά τα δικαιώματα εφαρμογής κατά την εγκατάσταση, αλλά μόνο όταν η εφαρμογή που επιχειρεί να χρησιμοποιήσει μια άδεια υπογράφεται από το ίδιο πιστοποιητικό με την εφαρμογή που καθορίζει την άδεια.

3. Επικίνδυνες άδειες (dangerous)

Τα επικίνδυνα δικαιώματα καλύπτουν περιοχές όπου η εφαρμογή θέλει δεδομένα ή πόρους που αφορούν τις προσωπικές πληροφορίες του χρήστη ή ενδέχεται να επηρεάσουν τα αποθηκευμένα δεδομένα του χρήστη ή τη λειτουργία άλλων εφαρμογών. Για παράδειγμα, η δυνατότητα ανάγνωσης των επαφών του χρήστη είναι επικίνδυνη άδεια. Εάν μια εφαρμογή δηλώνει ότι χρειάζεται επικίνδυνη άδεια, ο χρήστης πρέπει να δώσει ρητώς την άδεια στην εφαρμογή. Μέχρι ο χρήστης να εγκρίνει την άδεια, η εφαρμογή σας δεν μπορεί να παρέχει λειτουργίες που εξαρτώνται από αυτήν την άδεια ενδεχομένως και να μην λειτουργεί.

4. Ειδικά δικαιώματα (Special Permissions)

Υπάρχουν μερικά δικαιώματα που δεν συμπεριφέρονται σαν κανονικές και επικίνδυνες άδειες. Το WRITE_VOICEMAIL και το GET_ACCOUNTS είναι ιδιαίτερα ευαίσθητα, επομένως οι περισσότερες εφαρμογές δεν πρέπει να τις χρησιμοποιούν. Εάν μια εφαρμογή χρειάζεται ένα από αυτά τα δικαιώματα, πρέπει να δηλώσει την άδεια στο δηλωτικό και να στείλει μία σαφής ενημέρωση που ζητά την εξουσιοδότηση του χρήστη. Το σύστημα ανταποκρίνεται στην πρόθεση δείχνοντας μια λεπτομερή οθόνη ενημέρωσης στον χρήστη.

Από το Android 1 έως το 9 (επίπεδο 28 API), τα ακόλουθα δικαιώματα ταξινομούνται ως φαίνεται στον Πίνακα 2.3.

Δικαίωμα Βάση Δηλωτικού	Περιγραφή	Επίπεδο Προστασίας
ACCEPT_HANDOVER	Επιτρέπει σε μια εφαρμογή κλήσης να συνεχίσει μια κλήση που ξεκίνησε σε άλλη εφαρμογή. Ένα παράδειγμα είναι μια εφαρμογή κλήσεων βίντεο που θέλει να συνεχίσει μια φωνητική κλήση στο κινητό δίκτυο του χρήστη.	dangerous
ACCESS_CHECKIN_PROPERTIES	Επιτρέπει την πρόσβαση ανάγνωσης / εγγραφής στον πίνακα "Ιδιότητες" στη βάση δεδομένων checkin, για να αλλάξει τις τιμές που μεταφορτώνονται	Not for use
ACCESS_COARSE_LOCATION	Επιτρέπει σε μια εφαρμογή πρόσβαση σε κατά προσέγγιση τοποθεσία.	dangerous

ACCESS_FINE_LOCATION	Επιτρέπει σε μια εφαρμογή να αποκτά πρόσβαση σε ακριβή τοποθεσία.	dangerous
ACCESS_LOCATION_EXTRA_COMMANDS	Επιτρέπει σε μια εφαρμογή να αποκτά πρόσβαση σε πρόσθετες εντολές παρόχου τοποθεσίας.	normal
ACCESS_NETWORK_STATE	Επιτρέπει στις εφαρμογές την πρόσβαση σε πληροφορίες σχετικά με δίκτυα.	normal
ACCESS_NOTIFICATION_POLICY	Επιτρεπόμενη ένδειξη για τις εφαρμογές που επιθυμούν να έχουν πρόσβαση στην πολιτική ειδοποίησης.	normal
ACCESS_WIFI_STATE	Επιτρέπει στις εφαρμογές πρόσβαση σε πληροφορίες σχετικά με τα δίκτυα Wi-Fi.	normal
ACCOUNT_MANAGER	Επιτρέπει στις εφαρμογές να καλούν τους επαληθευτές λογαριασμού.	Not for use
ADD_VOICEMAIL	Επιτρέπει σε μια εφαρμογή να προσθέσει φωνητικά μηνύματα στο σύστημα.	dangerous
ANSWER_PHONE_CALLS	Επιτρέπει στην εφαρμογή να απαντά σε εισερχόμενη κλήση.	dangerous
BATTERY_STATS	Επιτρέπει σε μια εφαρμογή τη συλλογή στατιστικών στοιχείων μπαταριών	normal
BIND_ACCESSIBILITY_SERVICE	Πρέπει να απαιτείται από μια υπηρεσία AccessibilityService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature
BIND_APPWIDGET	Επιτρέπει σε μια εφαρμογή να ενημερώσει την υπηρεσία AppWidget σε ποια εφαρμογή μπορεί να έχει πρόσβαση στα δεδομένα του AppWidget.	Not for use
BIND_AUTOFILL_SERVICE	Πρέπει να απαιτείται από μια υπηρεσία AutofillService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_CARRIER_SERVICES	Η διαδικασία του συστήματος που επιτρέπεται να δεσμεύει τις υπηρεσίες σε εφαρμογές φορέα θα έχει αυτή την άδεια.	signature| privileged
BIND_CHOOSER_TARGET_SERVICE	Πρέπει να απαιτείται από μια υπηρεσία ChooserTargetService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_CONDITION_PROVIDER_SERVICE	Πρέπει να απαιτείται από την υπηρεσία ConditionProviderService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_DEVICE_ADMIN	Πρέπει να απαιτείται από το δέκτη διαχείρισης συσκευών, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να αλληλοεπιδράσει με αυτό.	signature
BIND_DREAM_SERVICE	Πρέπει να απαιτείται από μια DreamService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature
BIND_INCALL_SERVICE	Πρέπει να απαιτείται από μια InCallService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature| privileged
BIND_INPUT_METHOD	Πρέπει να απαιτείται από ένα InputMethodService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_MIDI_DEVICE_SERVICE	Πρέπει να απαιτείται από ένα MidiDeviceService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature
BIND_NFC_SERVICE	Πρέπει να απαιτείται από ένα HostApduService ή OffHostApduService για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature
BIND_NOTIFICATION_LISTENER_SERVICE	Πρέπει να απαιτείται από μια υπηρεσία NotificationListenerService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_PRINT_SERVICE	Πρέπει να απαιτείται από μια υπηρεσία PrintService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_QUICK_SETTINGS_TILE	Επιτρέπει σε μια εφαρμογή να δεσμεύει γρήγορα ρυθμίσεις τρίτου μέρους.	signature
BIND_REMOTEVIEWS	Πρέπει να απαιτείται από ένα RemoteViewsService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature
BIND_SCREENING_SERVICE	Πρέπει να απαιτείται από μια υπηρεσία CallScreeningService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature|privileged
BIND_TELECOM_CONNECTION_SERVICE	Must be required by a ConnectionService, to ensure that only the system can bind to it.	signature| privileged
BIND_TEXT_SERVICE	Πρέπει να απαιτείται από ένα TextService	signature
BIND_TV_INPUT	Πρέπει να απαιτείται από μια υπηρεσία TvInputService για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature| privileged
BIND_VISUAL_VOICEMAIL_SERVICE	Πρέπει να απαιτείται από μια σύνδεση VisualVoicemailService για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature| privileged
BIND_VOICE_INTERACTION	Πρέπει να απαιτείται από μια υπηρεσία VoiceInteractionService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_VPN_SERVICE	Πρέπει να απαιτείται από μια VpnService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να δεσμεύσει σε αυτό.	signature
BIND_VR_LISTENER_SERVICE	Πρέπει να απαιτείται από ένα VrListenerService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature
BIND_WALLPAPER	Πρέπει να απαιτείται από μια υπηρεσία WallpaperService, για να διασφαλιστεί ότι μόνο το σύστημα μπορεί να συνδεθεί σε αυτό.	signature| privileged
BLUETOOTH	Επιτρέπει στις εφαρμογές να συνδέονται με τις συνδεδεμένες συσκευές Bluetooth.	normal
BLUETOOTH_ADMIN	Επιτρέπει στις εφαρμογές να ανακαλύπτουν και να συνδυάζουν συσκευές Bluetooth.	normal
BLUETOOTH_PRIVILEGED	Επιτρέπει στις εφαρμογές να αντιστοιχούν συσκευές Bluetooth χωρίς αλληλεπίδραση χρήστη και να επιτρέπουν ή να απαγορεύουν την πρόσβαση στον τηλεφωνικό κατάλογο ή την πρόσβαση σε μηνύματα.	Not for use
BODY_SENSORS	Επιτρέπει σε μια εφαρμογή την πρόσβαση σε δεδομένα από αισθητήρες που χρησιμοποιεί ο χρήστης για να μετρήσει τι συμβαίνει στο σώμα του / της, όπως ο καρδιακός ρυθμός.	dangerous
BROADCAST_PACKAGE_REMOVED	Επιτρέπει σε μια εφαρμογή να μεταδίδει ειδοποίηση ότι ένα πακέτο εφαρμογής έχει καταργηθεί.	Not for use
BROADCAST_SMS	Επιτρέπει σε μια εφαρμογή να εκπέμπει ειδοποίηση παραλαβής SMS.	Not for use
BROADCAST_STICKY	Επιτρέπει σε μια εφαρμογή να εκπέμπει προειδοποιήσεις.	normal
BROADCAST_WAP_PUSH	Επιτρέπει σε μια εφαρμογή να εκπέμπει μια ειδοποίηση παραλαβής WAP PUSH.	Not for use

CALL_PHONE	Επιτρέπει σε μια εφαρμογή να ξεκινήσει μια τηλεφωνική κλήση χωρίς να περάσει από το περιβάλλον χρήστη για να επιβεβαιώσει την κλήση ο χρήστης.	dangerous
CALL_PRIVILEGED	Επιτρέπει σε μια εφαρμογή να καλέσει οποιονδήποτε αριθμό τηλεφώνου, συμπεριλαμβανομένων των αριθμών έκτακτης ανάγκης, χωρίς να περάσει από τη διεπαφή χρήστη Dialer για να επιβεβαιώσει ο χρήστης την κλήση.	Not for use
CAMERA	Απαιτείται να έχετε πρόσβαση στη συσκευή κάμερας.	dangerous
CAPTURE_AUDIO_OUTPUT	Επιτρέπει σε μια εφαρμογή να καταγράφει την έξοδο ήχου.	Not for use
CHANGE_COMPONENT_ENABLED_STATE	Επιτρέπει σε μια εφαρμογή να αλλάξει αν είναι ενεργοποιημένη ή όχι μια συνιστώσα εφαρμογής (εκτός από τη δική της).	Not for use
CHANGE_CONFIGURATION	Επιτρέπει σε μια εφαρμογή να τροποποιήσει την τρέχουσα διαμόρφωση, όπως η τοπική ρύθμιση.	dangerous
CHANGE_NETWORK_STATE	Επιτρέπει στις εφαρμογές να αλλάζουν κατάσταση συνδεσιμότητας δικτύου.	normal
CHANGE_WIFI_MULTICAST_STATE	Επιτρέπει στις εφαρμογές να εισέλθουν στη λειτουργία Wi-Fi Multicast.	normal
CHANGE_WIFI_STATE	Επιτρέπει στις εφαρμογές να αλλάζουν την κατάσταση σύνδεσης Wi-Fi.	normal
CLEAR_APP_CACHE	Επιτρέπει σε μια εφαρμογή να εκκαθαρίσει τις προσωρινές μνήμες όλων των εγκατεστημένων εφαρμογών στη συσκευή.	signature| privileged
CONTROL_LOCATION_UPDATES	Επιτρέπει την ενεργοποίηση / απενεργοποίηση ειδοποιήσεων ενημέρωσης τοποθεσίας από το ραδιόφωνο.	Not for use
DELETE_CACHE_FILES	Παλιά άδεια για τη διαγραφή αρχείων προσωρινής μνήμης μιας εφαρμογής, που δεν χρησιμοποιούνται πλέον.	-
DELETE_PACKAGES	Επιτρέπει σε μια εφαρμογή τη διαγραφή πακέτων.	Not for use
DIAGNOSTIC	Επιτρέπει τις εφαρμογές στο RW σε διαγνωστικούς πόρους.	Not for use
DISABLE_KEYGUARD	Επιτρέπει στις εφαρμογές να απενεργοποιούν το κλείδωμα πληκτρολογίου εάν δεν είναι ασφαλές.	normal
DUMP	Επιτρέπει σε μια εφαρμογή να ανακτά τις πληροφορίες απόστασης κατάστασης από υπηρεσίες συστήματος.	Not for use
EXPAND_STATUS_BAR	Επιτρέπει σε μια εφαρμογή να επεκτείνει ή να συμπτύξει τη γραμμή κατάστασης.	normal
FACTORY_TEST	Εκτελέστε ως εφαρμογή δοκιμής κατασκευαστή, τρέχοντας ως χρήστης root.	Not for use
FOREGROUND_SERVICE	Επιτρέπει σε μια κανονική εφαρμογή να χρησιμοποιεί το Service.startForeground.	normal
GET_ACCOUNTS	Επιτρέπει την πρόσβαση στη λίστα λογαριασμών στην Υπηρεσία Λογαριασμών.	Dangerous/ Special permission
GET_ACCOUNTS_PRIVILEGED	Επιτρέπει την πρόσβαση στη λίστα λογαριασμών στην Υπηρεσία Λογαριασμών.	dangerous
GET_AND_REQUEST_SCREEN_LOCK_COMPLEXITY	Επιτρέπει σε μια εφαρμογή να αποκτήσει την πολυπλοκότητα κλειδώματος οθόνης και να ζητήσει από τους χρήστες να ενημερώσουν την κλειδαριά οθόνης σε ένα ορισμένο επίπεδο πολυπλοκότητας.	normal
GET_PACKAGE_SIZE	Επιτρέπει σε μια εφαρμογή να εντοπίσει το χώρο που χρησιμοποιείται από οποιοδήποτε πακέτο.	normal
GET_TASKS	Αυτή η σταθερά αποκόπηκε στο επίπεδο API 21. Δεν ισχύει πλέον.	-
GLOBAL_SEARCH	Αυτή η άδεια μπορεί να χρησιμοποιηθεί στους παρόχους περιεχομένου για να επιτρέψει στο παγκόσμιο σύστημα αναζήτησης να έχει πρόσβαση στα δεδομένα του.	normal
INSTALL_LOCATION_PROVIDER	Επιτρέπει σε μια εφαρμογή να εγκαταστήσει έναν παροχέα τοποθεσίας στον Διαχειριστή τοποθεσίας.	Not for use
INSTALL_PACKAGES	Επιτρέπει σε μια εφαρμογή την εγκατάσταση πακέτων.	Not for use
INSTALL_SHORTCUT	Επιτρέπει σε μια εφαρμογή να εγκαταστήσει μια συντόμευση στο Launcher.	normal
INSTANT_APP_FOREGROUND_SERVICE	Επιτρέπει σε μια άμεση εφαρμογή τη δημιουργία υπηρεσιών προσκηνίου.	-
INTERNET	Επιτρέπει στις εφαρμογές να ανοίγουν υποδοχές δικτύου.	normal
KILL_BACKGROUND_PROCESSES	Επιτρέπει σε μια εφαρμογή να καλέσει το ActivityManager.killBackgroundProcesses (String).	normal
LOCATION_HARDWARE	Επιτρέπει σε μια εφαρμογή τη χρήση χαρακτηριστικών τοποθεσίας στο υλικό, όπως το geofencing api.	Not for use
MANAGE_DOCUMENTS	Επιτρέπει σε μια εφαρμογή να διαχειρίζεται την πρόσβαση σε έγγραφα, συνήθως ως μέρος ενός εργαλείου επιλογής εγγράφων.	Not for use
MANAGE_OWN_CALLS	Επιτρέπει μια εφαρμογή κλήσης η οποία διαχειρίζεται τις δικές της κλήσεις μέσω των αυτοδιαχειριζόμενων API ConnectionService.	normal
MASTER_CLEAR	Δεν χρησιμοποιείται από εφαρμογές τρίτων κατασκευαστών.	Not for use
MEDIA_CONTENT_CONTROL	Επιτρέπει σε μια εφαρμογή να γνωρίζει ποιο περιεχόμενο αναπαράγεται και ελέγχει την αναπαραγωγή του.	Not for use
MODIFY_AUDIO_SETTINGS	Επιτρέπει σε μια εφαρμογή να τροποποιεί τις συνολικές ρυθμίσεις ήχου.	normal
MODIFY_PHONE_STATE	Επιτρέπει την τροποποίηση της κατάστασης τηλεφωνίας - ενεργοποίηση, mmi κ.λπ.	Not for use
MOUNT_FORMAT_FILESYSTEMS	Επιτρέπει τη μορφοποίηση συστημάτων αρχείων για αφαιρούμενη αποθήκευση.	Not for use
MOUNT_UNMOUNT_FILESYSTEMS	Επιτρέπει την τοποθέτηση και την αποσυναρμολόγηση συστημάτων αρχείων για αφαιρούμενη αποθήκευση.	Not for use
NFC	Επιτρέπει στις εφαρμογές να εκτελούν λειτουργίες I / O μέσω NFC.	normal
NFC_TRANSACTION_EVENT	Επιτρέπει στις εφαρμογές να λαμβάνουν συμβάντα συναλλαγών NFC.	normal
PACKAGE_USAGE_STATS	Επιτρέπει σε μια εφαρμογή τη συλλογή στατιστικών στοιχείων χρήσης	normal
PERSISTENT_ACTIVITY	Αυτή η σταθερά καταργήθηκε στο επίπεδο API 15.	-

PROCESS_OUTGOING_CALLS	Επιτρέπει σε μια εφαρμογή να βλέπει τον αριθμό που καλείται κατά τη διάρκεια μιας εξερχόμενης κλήσης με την επιλογή να ανακατευθύνει την κλήση σε διαφορετικό αριθμό ή να διακόψει συνολικά την κλήση.	dangerous
READ_CALENDAR	Επιτρέπει σε μια εφαρμογή να διαβάσει τα δεδομένα ημερολογίου του χρήστη.	dangerous
READ_CALL_LOG	Επιτρέπει σε μια εφαρμογή να διαβάσει το αρχείο κλήσεων του χρήστη.	Dangerous/ Special permission
READ_CONTACTS	Επιτρέπει σε μια εφαρμογή να διαβάσει τα δεδομένα των επαφών του χρήστη.	dangerous
READ_INPUT_STATE	Αυτή η σταθερά έχει καταργηθεί στο επίπεδο API 16. Το API που χρησιμοποίησε αυτήν την άδεια έχει καταργηθεί.	Not for use
READ_LOGS	Επιτρέπει σε μια εφαρμογή να διαβάσει τα αρχεία καταγραφής συστήματος χαμηλού επιπέδου.	Not for use
READ_MEDIA_AUDIO	Επιτρέπει σε μια εφαρμογή να διαβάσει την κοινόχρηστη συλλογή ήχου του χρήστη.	dangerous
READ_MEDIA_IMAGES	Επιτρέπει σε μια εφαρμογή να διαβάσει τη συλλογή των κοινών εικόνων του χρήστη.	dangerous
READ_MEDIA_VIDEO	Επιτρέπει σε μια εφαρμογή την ανάγνωση της κοινόχρηστης συλλογής βίντεο του χρήστη.	dangerous
READ_PHONE_NUMBERS	Επιτρέπει την πρόσβαση ανάγνωσης στους αριθμούς τηλεφώνου της συσκευής.	dangerous
READ_PHONE_STATE	Επιτρέπει πρόσβαση μόνο στην ανάγνωση για την κατάσταση του τηλεφώνου, συμπεριλαμβανομένου του αριθμού τηλεφώνου της συσκευής, των πληροφοριών του κυψελοειδούς δικτύου, της κατάστασης οποιωνδήποτε συνεχιζόμενων κλήσεων και μιας λίστας οποιωνδήποτε PhoneAccounts που έχουν καταχωριστεί στη συσκευή.	Special permission
READ_SMS	Επιτρέπει σε μια εφαρμογή να διαβάζει μηνύματα SMS.	dangerous
READ_SYNC_SETTINGS	Επιτρέπει στις εφαρμογές να διαβάζουν τις ρυθμίσεις συγχρονισμού.	normal
READ_SYNC_STATS	Επιτρέπει στις εφαρμογές να διαβάζουν τα στατιστικά συγχρονισμού.	normal
READ_VOICEMAIL	Επιτρέπει σε μια εφαρμογή την ανάγνωση των φωνητικών μηνυμάτων στο σύστημα.	Signature |privileged
REBOOT	Απαιτείται να είναι δυνατή η επανεκκίνηση της συσκευής.	Not for use
RECEIVE_BOOT_COMPLETED	Επιτρέπει σε μια εφαρμογή να λάβει το Intent.ACTION_BOOT_COMPLETED που μεταδίδεται μετά την ολοκλήρωση της εκκίνησης του συστήματος.	normal
RECEIVE_MMS	Επιτρέπει σε μια εφαρμογή να παρακολουθεί εισερχόμενα μηνύματα MMS.	dangerous
RECEIVE_SMS	Επιτρέπει σε μια εφαρμογή να λαμβάνει μηνύματα SMS.	dangerous
RECEIVE_WAP_PUSH	Επιτρέπει σε μια εφαρμογή να λαμβάνει μηνύματα push WAP.	dangerous
RECORD_AUDIO	Επιτρέπει σε μια εφαρμογή να εγγράψει ήχο.	dangerous
REORDER_TASKS	Επιτρέπει σε μια εφαρμογή να αλλάζει τη σειρά Z των εργασιών.	normal
REQUEST_COMPANION_RUN_IN_BACKGROUND	Επιτρέπει την εκτέλεση μιας εφαρμογής συνοδευτικού στο παρασκήνιο.	normal
REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	Επιτρέπει σε μια εφαρμογή συνοδευτικό να χρησιμοποιεί δεδομένα στο παρασκήνιο.	normal
REQUEST_DELETE_PACKAGES	Επιτρέπει σε μια εφαρμογή να ζητά τη διαγραφή πακέτων.	normal
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	Η άδεια που πρέπει να διατηρεί μια εφαρμογή για να χρησιμοποιήσει το Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	normal
REQUEST_INSTALL_PACKAGES	Επιτρέπει σε μια εφαρμογή να ζητήσει την εγκατάσταση πακέτων.	signature
RESTART_PACKAGES	Αυτή η σταθερά έχει καταργηθεί στο επίπεδο API 15. Το API ActivityManager.restartPackage (String) δεν υποστηρίζεται πλέον.	-
SEND_RESPOND_VIA_MESSAGE	Επιτρέπει σε μια εφαρμογή (τηλέφωνο) να στείλει ένα αίτημα σε άλλες εφαρμογές για να χειριστεί τη δράση απάντησης μέσω μηνύματος κατά τις εισερχόμενες κλήσεις.	Not for use
SEND_SMS	Επιτρέπει σε μια εφαρμογή να στέλνει μηνύματα SMS.	dangerous
SET_ALARM	Επιτρέπει σε μια εφαρμογή να εκπέμπει μια πρόθεση να ορίσει ένα συναγερμό για τον χρήστη.	normal
SET_ALWAYS_FINISH	Επιτρέπει σε μια εφαρμογή να ελέγχει αν οι δραστηριότητες ολοκληρώνονται αμέσως όταν τοποθετούνται στο παρασκήνιο.	Not for use
SET_ANIMATION_SCALE	Τροποποιήστε τον συντελεστή κλίμακας σφαιρικής κίνησης.	Not for use
SET_DEBUG_APP	Ρυθμίστε μια εφαρμογή για εντοπισμό σφαλμάτων.	Not for use
SET_PREFERRED_APPLICATIONS	Αυτή η σταθερά αποκόπηκε στο επίπεδο API 15. Δεν είναι πλέον χρήσιμο, ανατρέξτε στην ενότητα PackageManager.addPackageToPreferred (String) για λεπτομέρειες.	-
SET_PROCESS_LIMIT	Επιτρέπει σε μια εφαρμογή να ορίζει το μέγιστο αριθμό διαδικασιών εφαρμογής (που δεν χρειάζονται) που μπορούν να εκτελούνται.	Not for use
SET_TIME	Επιτρέπει στις εφαρμογές να ρυθμίζουν το χρόνο του συστήματος.	Not for use
SET_TIME_ZONE	Επιτρέπει στις εφαρμογές να ορίσουν τη ζώνη ώρας του συστήματος.	Not for use
SET_WALLPAPER	Επιτρέπει στις εφαρμογές τη ρύθμιση της ταπετσαρίας.	normal
SET_WALLPAPER_HINTS	Επιτρέπει στις εφαρμογές να ορίσουν τις συμβουλές ταπετσαρίας.	normal
SIGNAL_PERSISTENT_PROCESSES	Αφήστε μια εφαρμογή να ζητήσει την αποστολή ενός σήματος σε όλες τις επίμονες διαδικασίες.	Not for use
SMS_FINANCIAL_TRANSACTIONS	Επιτρέπει στις οικονομικές εφαρμογές να διαβάζουν φιλτραρισμένα μηνύματα SMS.	dangerous

STATUS_BAR	Επιτρέπει σε μια εφαρμογή να ανοίγει, να κλείνει ή να απενεργοποιεί τη γραμμή κατάστασης και τα εικονίδια της.	Not for use
SYSTEM_ALERT_WINDOW	Επιτρέπει σε μια εφαρμογή τη δημιουργία παραθύρων χρησιμοποιώντας τον τύπο WindowManager.LayoutParams.TYPE_APPLICATION_OVERLAY, που εμφανίζεται πάνω από όλες τις άλλες εφαρμογές.	signature
TRANSMIT_IR	Επιτρέπει τη χρήση του πομπού IR της συσκευής, εάν υπάρχει.	normal
UNINSTALL_SHORTCUT	Μην χρησιμοποιείτε αυτό το δικαίωμα στην εφαρμογή σας.	-
UPDATE_DEVICE_STATS	Επιτρέπει σε μια εφαρμογή να ενημερώνει τα στατιστικά στοιχεία της συσκευής.	Not for use
USE_BIOMETRIC	Επιτρέπει σε μια εφαρμογή να χρησιμοποιεί βιομετρικές μορφές που υποστηρίζονται από συσκευές.	normal
USE_FINGERPRINT	Αυτή η σταθερά έχει εξαντληθεί στο επίπεδο API 28. Οι εφαρμογές θα πρέπει να ζητήσουν το USE_BIOMETRIC	normal
USE_FULL_SCREEN_INTENT	Απαιτείται για εφαρμογές που στοχεύουν το Build.VERSION_CODES.Q και επιθυμούν να χρησιμοποιούν προειδοποιήσεις πλήρους οθόνης ειδοποιήσεων.	dangerous
USE_SIP	Επιτρέπει σε μια εφαρμογή να χρησιμοποιεί υπηρεσία SIP.	dangerous
VIBRATE	Επιτρέπει την πρόσβαση στον δονητή.	normal
WAKE_LOCK	Επιτρέπει τη χρήση του PowerManager WakeLocks για να παραμείνει ο επεξεργαστής από τον ύπνο ή την οθόνη από την εξασθένιση.	normal
WRITE_APN_SETTINGS	Επιτρέπει στις εφαρμογές να γράφουν τις ρυθμίσεις apn και να διαβάζουν ευαίσθητα πεδία μιας υπάρχουσας ρύθμισης apn όπως χρήστη και κωδικό πρόσβασης.	Not for use
WRITE_CALENDAR	Επιτρέπει σε μια εφαρμογή να γράψει τα δεδομένα ημερολογίου του χρήστη.	dangerous
WRITE_CALL_LOG	Επιτρέπει σε μια εφαρμογή να γράφει (αλλά δεν διαβάζει) τα δεδομένα του αρχείου καταγραφής κλήσεων του χρήστη.	dangerous
WRITE_CONTACTS	Επιτρέπει σε μια εφαρμογή να γράψει τα δεδομένα επαφών του χρήστη.	dangerous
WRITE_EXTERNAL_STORAGE	Αυτή η σταθερά καταργήθηκε στο επίπεδο API Q. Αντικαταστάθηκε από νέες ομάδες άδειας με ισχυρά πληκτρολόγια στο Q.	normal
WRITE_GSERVICES	Επιτρέπει σε μια εφαρμογή την τροποποίηση του χάρτη υπηρεσιών της Google.	Not for use
WRITE_SECURE_SETTINGS	Επιτρέπει σε μια εφαρμογή να διαβάζει ή να γράφει τις ασφαλείς ρυθμίσεις συστήματος.	Not for use
WRITE_SETTINGS	Επιτρέπει σε μια εφαρμογή να διαβάζει ή να γράφει τις ρυθμίσεις του συστήματος.	Signature/ Special permission
WRITE_SYNC_SETTINGS	Επιτρέπει στις εφαρμογές να γράφουν τις ρυθμίσεις συγχρονισμού.	normal
WRITE_VOICEMAIL	Επιτρέπει σε μια εφαρμογή να τροποποιεί και να καταργεί υπάρχοντα μηνύματα φωνής στο σύστημα.	Signature| privileged

Πίνακας 2.3: Ομαδοποίηση δικαιωμάτων αναλόγως επιπέδων προστασίας.

Παρουσιάζεται λοιπόν, ότι η πλειοψηφία των εξεταζόμενων εφαρμογών κινητής τηλεφωνίας να απαιτεί πρόσβαση σε τεράστιο όγκο προσωπικών πληροφοριών που είναι αποθηκευμένες σε κινητές συσκευές, ενώ μόνο λίγες από αυτές λειτουργούν χωρίς συγκεκριμένες απαιτήσεις όσον αφορά την πρόσβαση σε προσωπικά δεδομένα [17]. Ο πιο περιζήτητος τύπος πρόσβασης είναι ο τύπος που επιτρέπει πρόσβαση σε "Φωτογραφία/Μέσα/Αρχεία", η οποία στην πράξη επιτρέπει την πρόσβαση σε κάθε αρχείο που είναι αποθηκευμένο στην συσκευή. Ο δεύτερος πιο περιζήτητος τύπος πρόσβασης σχετίζεται με δεδομένα σχετικά με τις συνδέσεις Wi- Fi, τα οποία με τη σειρά τους θα μπορούσαν να αποκαλύψουν πληροφορίες για όλες τις συνδεδεμένες συσκευές Wi-Fi, τη θέση του χρήστη κ.λπ. Ένα άλλο σημαντικό εύρημα είναι ότι οι χρήστες αξιολογούν εφαρμογές κινητής τηλεφωνίας χωρίς να λαμβάνουν υπόψη το επίπεδο πρόσβασης στα δεδομένα που απαιτείται από κάθε εφαρμογή κινητής τηλεφωνίας. Θα μπορούσε να υποστηριχθεί ότι οι χρήστες είτε δεν γνωρίζουν το επίπεδο της απαιτούμενης πρόσβασης σε δεδομένα από κινητές εφαρμογές είτε επιλέγουν να εγκαταστήσουν εφαρμογές για κινητά ανεξάρτητα από την απαιτούμενη πρόσβαση στα δεδομένα τους.

Κεφάλαιο 3
Προσωπικά Δεδομένα και Κίνδυνοι Ιδιωτικότητας

Τα βασικά νομικά και κανονιστικά θέματα σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω εφαρμογών για κινητά προέρχονται από το GDPR, καθώς και ορισμένες πτυχές της οδηγίας για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τον επικείμενο κανονισμό για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Στην συνέχεια εντοπίζονται και παρουσιάζονται επιλεγμένα νομικά και οργανωτικά ζητήματα που δημιουργούν προκλήσεις που ενδέχεται να προκαλέσουν κινδύνους στις εφαρμογές για κινητά.

3.1 Νομικό Πλαίσιο

3.1.1 Προσωπικά Δεδομένα

Ενώ οι χρήστες του διαδικτύου βασίζονται όλο και περισσότερο στη χρήση κινητών εφαρμογών για τις καθημερινές τους δραστηριότητες και ανάγκες, η επεξεργασία προσωπικών δεδομένων μέσω τέτοιων εργαλείων ενέχει σοβαρούς κινδύνους για την ασφάλεια των χρηστών και την ιδιωτική ζωή τους. Οι κίνδυνοι αυτοί προέρχονται κυρίως από την ποικιλία των δεδομένων και των αισθητήρων που υπάρχουν σε κινητές συσκευές, τη χρήση διαφορετικών τύπων αναγνωριστικών στοιχείων και την εκτεταμένη δυνατότητα παρακολούθησης των χρηστών, το περίπλοκο οικοσύστημα εφαρμογών για κινητά και οι περιορισμοί των προγραμματιστών εφαρμογών, καθώς και η εκτεταμένη χρήση τρίτων μερών. Για τους λόγους αυτούς, η εφαρμογή των βασικών αρχών προστασίας δεδομένων, όπως ορίζει ο Γενικός κανονισμός για την προστασία των δεδομένων (GDPR), αντιμετωπίζει σοβαρές προκλήσεις στις εφαρμογές για κινητά όσον αφορά τη διαφάνεια και τη συγκατάθεση, την προστασία δεδομένων από το σχεδιασμό και από προεπιλογή, καθώς και την ασφάλεια της επεξεργασίας [9].

Οι λόγοι για την προστασία των προσωπικών δεδομένων είναι πολύ σαφείς από το κανονιστικό πλαίσιο. Τα προσωπικά δεδομένα αφορούν μόνο φυσικά πρόσωπα. Με την ανάπτυξη της τεχνολογίας και του Διαδικτύου, τα προσωπικά δεδομένα γίνονται ολοένα και πιο εκτεθειμένα και προσβάσιμα σε όσους μπορούν να τα χρησιμοποιήσουν για δικούς τους, παράνομους σκοπούς. Τα κοινωνικά δίκτυα μπορούν να χαρακτηριστούν ως το βασικό παράδειγμα. Σύμφωνα με στατιστικές πληροφορίες αναφορικά με κοινωνικά μέσα δικτύωσης από το Φεβρουάριο του 2017, ο αριθμός των χρηστών κοινωνικών δικτύων, με προσωπικά δεδομένα, έφθασε τα 4,6 δισ. Αυτός ο αριθμός περιλαμβάνει επίσης τα λεγόμενα ψεύτικα προφίλ χρηστών που αντιπροσωπεύουν αντίγραφα πραγματικών προφίλ (προσώπων) που σκοπεύουν να τα βλάψουν χρησιμοποιώντας τα προσωπικά τους δεδομένα [10].

Για περίπου δύο δεκαετίες, το βασικό νομικό κείμενο για την προστασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση ήταν η Οδηγία 95/46/ΕΚ, η οποία είχε ενσωματωθεί στην έννομη τάξη κάθε Κράτους Μέλους. Πλέον, όπως περιγράφεται στη συνέχεια, η Οδηγία αυτή έχει καταργηθεί και αντικατασταθεί από τον Κανονισμό 2016/679 (ΕΕ) (Γενικός Κανονισμός Προστασίας Δεδομένων), γνωστός με το αρκτικόλεξο GDPR (General Data Protection Regulation). Ο

Κανονισμός αυτός έχει άμεση εφαρμογή, από τις 25 Μαΐου 2018, στα Κράτη-Μέλη της Ευρωπαϊκής Ένωσης.

Ως "προσωπικά δεδομένα" χαρακτηρίζεται οποιαδήποτε πληροφορία σχετίζεται με ένα φυσικό πρόσωπο που είτε έχει ταυτοποιηθεί ή είτε μπορεί να προσδιοριστεί μέσα από συγκεκριμένες πληροφορίες [9]. Με βάση τον νόμο περί προστασίας των δεδομένων προσωπικού χαρακτήρα, αναγνωρίσιμο άτομο (πρόσωπο στο οποίο αναφέρονται τα δεδομένα) είναι ένα άτομο που μπορεί να εντοπιστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε έναν ή περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, πνευματική, οικονομική, πολιτιστική ή κοινωνική του ταυτότητα [10]. Ο ορισμός των προσωπικών δεδομένων είναι ουσιαστικά ο ίδιος, τόσο στην Οδηγία 95/46/ΕΚ όσο και στον GDPR.

Πιο συγκεκριμένα, τα προσωπικά δεδομένα αντιπροσωπεύουν όλες τις πληροφορίες οι οποίες σχετίζονται με ένα άτομο. Τα δεδομένα μπορούν να περιλαμβάνουν το όνομα, το επώνυμο, τη διεύθυνση, τη διεύθυνση IP δικτύου, τη διεύθυνση MAC, τη διεύθυνση ηλεκτρονικού ταχυδρομείου, την τοποθεσία GPS, τον αριθμό τηλεφώνου, φωτογραφίες, βίντεο, την προσωπική ταυτότητα, τα βιομετρικά δεδομένα και άλλα δεδομένα σε σχέση με την προσωπική ταυτότητα του χρήστη [10].

Βιομετρικά δεδομένα ορίζονται ως τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά και βιολογικά, όπως δακτυλικά αποτυπώματα, γεωμετρία της παλάμης, ανάλυση της κόρης του ματιού, των χαρακτηριστικών του προσώπου, του DNA ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, όπως υπογραφή, φωνή, τρόπο πληκτρολόγησης, τρόπο βαδίσματος, τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου [11].

Ευαίσθητα δεδομένα (ή δεδομένα ειδικών κατηγοριών, όπως αποκαλούνται σε νομικά κείμενα) ορίζονται τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια, στην ερωτική ζωή, σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων [12]. Αξίζει να επισημανθεί ότι, με τον GDPR, στην ανωτέρω λίστα των ευαίσθητων δεδομένων προστίθενται και τα βιομετρικά δεδομένα, εφόσον χρησιμοποιούνται για ταυτοποίηση ατόμου, αλλά και τα γενετικά δεδομένα.

Εικόνα 3.1: Ποια είναι τα προσωπικά δεδομένα [10].

Ο όρος "επεξεργασία δεδομένων προσωπικού χαρακτήρα" αναφέρεται σε οποιαδήποτε ενέργεια ή σύνολο πράξεων που πραγματοποιούνται με δεδομένα προσωπικού χαρακτήρα, είτε αυτόματα είτε όχι, όπως συλλογή, καταγραφή, οργάνωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, διαβούλευση, χρήση, γνωστοποίηση μέσω μετάδοσης, διάδοση ή άλλη διάθεση, ευθυγράμμιση ή συνδυασμός, αποκλεισμός, διαγραφή ή καταστροφή [13].

Από νομική άποψη, υπάρχουν δύο βασικοί ρόλοι που συνεπάγονται συγκεκριμένες υποχρεώσεις προστασίας δεδομένων, δηλαδή τον υπεύθυνο επεξεργασίας δεδομένων και τον επεξεργαστή δεδομένων. Ο υπεύθυνος επεξεργασίας δεδομένων (data controller) είναι ο σημαντικότερος φορέας που πρέπει να συμμορφώνεται με τις κεντρικές νομικές υποχρεώσεις του GDPR όσον αφορά τη νόμιμη, δίκαιη και διαφανή επεξεργασία δεδομένων προσωπικού χαρακτήρα. Συνήθως, ο πάροχος εφαρμογών θα θεωρείται ως ο κύριος υπεύθυνος επεξεργασίας για την επεξεργασία προσωπικών δεδομένων, στο βαθμό που η εφαρμογή επεξεργάζεται τα προσωπικά δεδομένα των χρηστών για δικούς τους σκοπούς. Σε πολλές περιπτώσεις, ο προγραμματιστής της εφαρμογής μπορεί να είναι ο ίδιος με τον πάροχο της εφαρμογής, ενεργώντας ως υπεύθυνος επεξεργασίας δεδομένων. Αυτό όμως δεν συμβαίνει απαραίτητα.

Στο πλαίσιο του GDPR, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη το δικαίωμα προστασίας των δεδομένων κατά τις διαδικασίες ανάπτυξης και σχεδιασμού τους (αιτιολογική σκέψη 78 του GDPR). Παρόλο που οι εν λόγω οντότητες ενδέχεται να

μην υπόκεινται άμεσα στη ρύθμιση βάσει του GDPR, ενθαρρύνονται να διασφαλίζουν ότι οι υπεύθυνοι επεξεργασίας είναι σε θέση να εκπληρώσουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων. Στο πλαίσιο της κινητής τηλεφωνίας, αυτή η αιτιολογική σκέψη διακρίνεται σαφώς σε σχέση με τους προγραμματιστές εφαρμογών, τα καταστήματα εφαρμογών, τους παρόχους λειτουργικών συστημάτων, τους παρόχους βιβλιοθηκών και τους κατασκευαστές υλικού. Τουλάχιστον, οι προγραμματιστές εφαρμογών πρέπει να προγραμματίζουν την εφαρμογή με τέτοιο τρόπο ώστε να διασφαλίζεται η συμμόρφωση με το GDPR [9].

3.1.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και οι Βασικές Καινοτομίες του

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω εφαρμογών ρυθμίζεται πλέον από τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΕΕ) 2016/679 (GDPR), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018 και είναι το κύριο νομικό πλαίσιο προστασίας δεδομένων για όλα τα κράτη μέλη της ΕΕ, με την κατάργηση της ισχύουσας οδηγίας 95/46/ΕΚ για την προστασία των δεδομένων. Λαμβάνοντας υπόψη το περιβάλλον στο οποίο εγκρίθηκε η οδηγία για την προστασία των δεδομένων (1995) από τεχνολογική άποψη, ο λόγος για την έγκριση αυτού του νέου κανονισμού GDPR καθίσταται προφανής από τις τεχνολογικές εξελίξεις που έχουν έκτοτε επέλθει. Παράλληλα με την ενίσχυση όλων των αρχών, υποχρεώσεων και δικαιωμάτων προστασίας δεδομένων που κατοχυρώνονται στην οδηγία, ο GDPR περιλαμβάνει πρόσθετους μηχανισμούς προστασίας που επιτρέπουν στα άτομα να ελέγχουν καλύτερα τα προσωπικά τους δεδομένα, γεγονός που αποτελεί ιδιαίτερα πρόκληση για το διαδικτυακό και κινητό περιβάλλον [9].

Κάποιες εκ των καινοτομιών στη ρύθμιση προστασίας των προσωπικών δεδομένων που εισήχθησαν από το νέο Κανονισμό GDPR έχουν ως εξής (αν και κάποιες εξ αυτών προϋπήρχαν και απλά, με τον GDPR, ενισχύθηκαν):

- Δικαίωμα διαγραφής – δηλαδή ο κάθε χρήστης ο οποίος έχει εκχωρήσει άδεια σε τρίτους να επεξεργαστούν και να αποθηκεύσουν δεδομένα του, έχει κάθε δικαίωμα να απαιτήσει την διαγραφή τους – ενώ ο υπεύθυνος επεξεργασίας, αν ήδη τα έχει δημοσιοποιήσει σε άλλους, οφείλει να κάνει ενέργειες ενημέρωσης προς αυτούς για να τα διαγράψουν και οι ίδιοι αντιστοίχως

- Σαφής συγκατάθεση όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα (σαφής συναίνεση, η οποία προκύπτει με σαφή θετική ενέργεια του χρήστη),
- Δικαίωμα φορητότητας δεδομένων (π.χ. σε άλλο υπεύθυνο επεξεργασίας),
- Κοινοποίηση παραβίασης προσωπικών δεδομένων (εντός 72 ωρών) στην αρμόδια εποπτική Αρχή και, υπό προϋποθέσεις, και στα πρόσωπα των οποίων τα δεδομένα παραβιάστηκαν,
- Υποχρέωση (σε συγκεκριμένες περιπτώσεις) ορισμού υπεύθυνου προστασίας δεδομένων – ΥΠΔ (Data Protection Officer-DPO),
- Πρόστιμα τα οποία μπορούν να κυμαίνονται μέχρι και το 4% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως.

Στην Εικόνα 3.2 παρουσιάζονται κάποιες εκ των βασικών καινοτομιών στην εφαρμογή του GDPR. Πρέπει να σημειωθεί ότι η εφαρμογή του GDPR αναφέρεται μόνο σε προσωπικά δεδομένα.

Εικόνα 3.2: Βασικές Καινοτομίες του GDPR [10].

Όταν μιλάμε για την κατάχρηση δεδομένων με την σημερινή έννοια, όλα αρχίζουν με τη διαδικασία της σαφούς συμφωνίας για την επεξεργασία των προσωπικών δεδομένων. Το πρώτο πρόσωπο που έρχεται σε επαφή με το φυσικό πρόσωπο κατά τη διαδικασία παροχής των προσωπικών του δεδομένων είναι ο υπεύθυνος επεξεργασίας.

"Υπεύθυνος επεξεργασίας": είναι το φυσικό ή νομικό πρόσωπο, ο οργανισμός ή άλλος φορέας που καθορίζει το σκοπό και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Ο εκτελών την επεξεργασία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα κατόπιν έγκρισης του υπεύθυνου επεξεργασίας. Ο υπεύθυνος της

επεξεργασίας πρέπει να εξασφαλίσει τη σαφή, ρητή και ειδική συγκατάθεση του προσώπου από το οποίο θα συλλέγονται τα προσωπικά δεδομένα (αν και προβλέπονται και περιπτώσεις νόμιμης επεξεργασίας χωρίς τη συγκατάθεση)... Κάθε παραβίαση του απορρήτου (δικαιωμάτων και ελευθεριών) των δεδομένων προσωπικού χαρακτήρα πρέπει να κοινοποιείται στις αρμόδιες εποπτικές αρχές εντός 72 ωρών [10].

Το κύριο καθήκον του GDPR στο πλαίσιο της εφαρμογής όσο αφορά τον επιχειρηματικό τομέα, είναι οι επιχειρήσεις να γνωρίζουν πού βρίσκονται τα δεδομένα τους ανά πάσα στιγμή και για ποιο σκοπό μπορούν να χρησιμοποιηθούν. Ο σκοπός της επεξεργασίας πρέπει να είναι σαφής, θεμιτός και νόμιμος, ενώ δεδομένα που έχουν συλλεγεί για συγκεκριμένο σκοπό δεν μπορούν να χρησιμοποιηθούν για άλλο σκοπό. Το δικαίωμα διαγραφής είναι μία από τις κύριες καινοτομίες του GDPR και αναφέρεται στην απόσυρση (διαγραφή) προσωπικών δεδομένων, η οποία πρέπει να εκτελείται από τις επιχειρήσεις εντός της νόμιμης προθεσμίας. Το δικαίωμα διαγραφής το οποίο περιλαμβανόταν στην οδηγία της ΕΕ από το 1995 έχει τροποποιηθεί μέσω του GDPR και ορίζει τη διαδικασία με περισσότερες λεπτομέρειες. Το πρόσωπο έχει το δικαίωμα να ζητήσει τη διαγραφή των προσωπικών του δεδομένων και ο υπεύθυνος της επεξεργασίας υποχρεούται να συμμορφωθεί με το αίτημα αυτό, εάν και εφόσον τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα [10], καθώς επίσης και –όπως προαναφέρθηκε – να ενημερώσει κατάλληλα άλλους στους οποίους έχει δημοσιοποιήσει τα δεδομένα (για αυτό και το δικαίωμα αυτό στον GDPR αποκαλείται και ως δικαίωμα στη λήθη)

Όπως προαναφέρθηκε ο Γενικός Κανονισμός Προστασίας Δεδομένων τέθηκε σε ισχύ στις 25 Μαΐου 2018 και είναι δεσμευτικός για όλα τα κράτη μέλη της ΕΕ. Ωστόσο, ο κανονισμός εφαρμόζεται επίσης σε όλες τις χώρες εκτός των συνόρων της ΕΕ, δηλαδή σε εταιρείες οι οποίες παρέχουν υπηρεσίες σε κατοίκους της ΕΕ, ακόμα και αν η εγκατάσταση των εταιρειών αυτών δεν είναι σε κράτος μέλος. Αυτό σημαίνει ότι όλοι οι συνεργαζόμενοι με τα κράτη μέλη της ΕΕ πρέπει να τηρούν τους κανόνες τους.

Ο παρακάτω Πίνακας 3.1 δείχνει τη σύγκριση μεταξύ της προηγούμενης οδηγίας της ΕΕ για την προστασία των δεδομένων και της νέας GDPR.

Rules	EU Data Protection Directive from 1995	GDPR (EU 2016/769)
Right of access	+	+
Right to rectification	+	+
Right to erasure	+	+
Right to stop direct marketing	+	+
Right to be informed		+
Right to restriction of processing		+
Right to data portability		+
Right to object		+
Notification of personal data breaches (within 72 hours)		+
Obligation to appoint a data protection officer – DPO		+
Fines from 0.5 to 4% of total worldwide annual turnover		+

Πίνακας 3.1: Σύγκριση μεταξύ της προηγούμενης οδηγίας της ΕΕ για την προστασία των δεδομένων και της νέας.

3.1.3 Βασικά Νομικά και Κανονιστικά Ζητήματα

Η εφαρμογή του ευρωπαϊκού πλαισίου για την προστασία των δεδομένων ξεκινά με το ερώτημα κατά πόσον υπάρχει κάποια επεξεργασία των «προσωπικών δεδομένων». Σε ένα περιβάλλον εφαρμογών για κινητά όταν συλλέγονται δεδομένα σχετικά με μια κινητή συσκευή ή από την προσωπική φύση της χρήσης της κινητής συσκευής συνεπάγεται ότι τα δεδομένα αυτά πρέπει να θεωρούνται δεδομένα προσωπικού χαρακτήρα με βάση το GDPR. Έτσι, όχι μόνο τα δεδομένα στη συσκευή που είναι προσωπικά και ιδιωτικά από τη φύση τους, όπως εικόνες, μηνύματα, μηνύματα ηλεκτρονικού ταχυδρομείου κ.λπ., αλλά και δεδομένα που σχετίζονται με τη συσκευή, όπως αναγνωριστικά συσκευών, όπως η τοποθεσία της συσκευής και τα δεδομένα που σχετίζονται με τη χρήση της,

συμπεριλαμβανομένων των αρχείων καταγραφής (log files) που περιέχουν δεδομένα χρήσης που σχετίζονται με συγκεκριμένες εφαρμογές.

Μόλις ένας προγραμματιστής εφαρμογών συλλέξει και επεξεργαστεί τα δεδομένα από τη συσκευή του χρήστη, συμπεριλαμβανομένων των μεταδεδομένων που σχετίζονται με τη συσκευή και τη συμπεριφορά του χρήστη, ενεργοποιούνται όλες οι βασικές απαιτήσεις προστασίας δεδομένων GDPR. Εάν τα προσωπικά δεδομένα είναι πλήρως ανωνυμοποιημένα, το πλαίσιο προστασίας δεδομένων δεν ισχύει, διότι τα ανώνυμα προσωπικά δεδομένα δεν διακρίνονται από οποιοδήποτε άλλο είδος δεδομένων.

Τα ψευδωνυμοποιημένα δεδομένα είναι ένα νέο υποσύνολο προσωπικών δεδομένων που εισάγεται με σαφή νομικό ορισμό στο GDPR. Σύμφωνα με το GDPR, η «ψευδωνυμοποίηση» σημαίνει «επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπον ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδίδονται σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, υπό την προϋπόθεση ότι οι πρόσθετες αυτές πληροφορίες τηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν αποδίδονται σε φυσικό πρόσωπο που έχει ταυτοποιηθεί ή αναγνωριστεί». Ειδικότερα, τα ψευδωνυμοποιημένα δεδομένα εξακολουθούν να είναι δεδομένα προσωπικού χαρακτήρα και η διαδικασία ψευδωνυμοποίησης είναι ένα μέτρο που εισάχθηκε με βάση τον νέο κανονισμό GDPR [10].

Κατά την πρόσβαση σε ευαίσθητα (ειδικές κατηγορίες) δεδομένων όπως έχουν οριστεί, ισχύουν αυστηρότερες απαιτήσεις βάσει του άρθρου 9 του GDPR. Όταν η χρήση μιας εφαρμογής έχει ως αποτέλεσμα την επεξεργασία τέτοιων ευαίσθητων δεδομένων, για παράδειγμα σε εφαρμογές υγείας, συνήθως ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίσει ότι υπάρχει ρητή συγκατάθεση του χρήστη για την επεξεργασία αυτών των δεδομένων για συγκεκριμένους καθορισμένους σκοπούς. Είναι πιθανό ορισμένες πληροφορίες που επεξεργάζονται στο περιβάλλον κινητής τηλεφωνίας, όπως εικόνες, μηνύματα, να περιέχουν δεδομένα που πρέπει να χαρακτηρίζονται ως ευαίσθητα δεδομένα βάσει του άρθρου 9 GDPR. Οι εικόνες δεν θεωρούνται γενικά ευαίσθητα δεδομένα, αλλά οι εικόνες των προσώπων μπορούν να αποκαλύψουν τη φυλετική ή εθνική καταγωγή τους, τα ιδιωτικά μηνύματα των ανθρώπων μπορούν να αποκαλύψουν τις πεποιθήσεις και τις νοοτροπίες καθώς και την κατάσταση της υγείας τους. Το ίδιο μπορεί να ισχύει και για τα μεταδεδομένα, τα οποία συλλέγονται με την πάροδο του

χρόνου, μπορούν να παράσχουν ένα μοναδικά διεισδυτικό προφίλ των χρηστών. Ενώ τα δεδομένα θέσης δεν περιλαμβάνονται στη λίστα ειδικών κατηγοριών δεδομένων, η επεξεργασία των δεδομένων θέσης γενικά θεωρείται ότι απαιτεί ιδιαίτερη προσοχή στο ζήτημα της αναγκαιότητας και της αναλογικότητας και τα μεγάλα κινητά λειτουργικά συστήματα έχουν εφαρμόσει ειδικούς μηχανισμούς για τη διαφάνεια των δεδομένων θέσης και τη συγκατάθεση των χρηστών [14].

Τέλος, όταν τα ευαίσθητα δεδομένα του χρήστη αποστέλλονται μέσω τηλεπικοινωνιακών υπηρεσιών όπως το Διαδίκτυο, εφαρμόζεται η Ευρωπαϊκή Οδηγία 2002/58/ ΕΚ (η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Η παρούσα οδηγία υποχρεώνει αυτούς που συλλέγουν δεδομένα από τον χρήστη να ενημερώνουν τους χρήστες σχετικά με τους τρίτους που θα λάβουν τα δεδομένα αυτά και τους υποχρεώνει να ζητούν τη συγκατάθεσή τους όποτε σκοπεύουν να χρησιμοποιήσουν τα δεδομένα για σκοπούς διαφορετικούς από τον αρχικό σκοπό για τον οποίο συλλέχθηκαν [15].

Σύμφωνα με το άρθρο 5 παράγραφος 3 της Ευρωπαϊκή Οδηγία 2002/58/ ΕΚ [16] που αφορά στο απόρρητο των επικοινωνιών αναφέρει ότι, «Τα κράτη μέλη μεριμνούν ώστε η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση προσβάσεως σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη να επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας, και ο υπεύθυνος ελέγχου των δεδομένων τού παρέχει το δικαίωμα να αρνείται την επεξεργασία αυτή. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή η διευκόλυνση της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής». Συνεπώς, για πρόσβαση στον τερματικό εξοπλισμό του χρήστη – όπως είναι μία «έξυπνη» συσκευή – τυγχάνει εφαρμογής κατ' αρχάς η εν λόγω Οδηγία (η οποία έχει ενσωματωθεί στην εθνική νομοθεσία σε κάθε Κράτος-Μέλος).

3.1.4 Αρχές Προστασίας Δεδομένων

Όπως αναλύθηκε πιο πάνω, οι εφαρμογές για κινητά θέτουν συγκεκριμένους κινδύνους για την ασφάλεια και την ιδιωτικότητα, τόσο λόγω της φύσης τους, όσο και του γενικού

πλαισίου ανάπτυξης των εφαρμογών για κινητά. Για τον λόγο αυτόν οι βασικές αρχές προστασίας δεδομένων, όπως ορίζονται στο άρθρο 5 του GDPR, μπορούν να αντιμετωπίσουν σοβαρές προκλήσεις στον τομέα των εφαρμογών για κινητά. Οι βασικές αρχές είναι οι εξής και αναλύονται πιο κάτω [9]:

- «Νομιμότητα, δικαιοσύνη και διαφάνεια»: Τα δεδομένα προσωπικού χαρακτήρα διεκπεραιώνονται με σεβασμό της δικαιοσύνης και της διαφάνειας έναντι του υποκειμένου των δεδομένων και με την τήρηση της απαίτησης για θεμιτό λόγο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

- «Περιορισμός σκοπού": Όταν μια εφαρμογή επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, πρέπει να έχει συγκεκριμένο νόμιμο σκοπό και πρέπει να ενημερώνει σχετικά το υποκείμενο των δεδομένων. Περαιτέρω επεξεργασία για άλλους σκοπούς επιτρέπεται μόνο με βάση ένα συγκεκριμένο σύνολο κριτηρίων βάσει του GDPR (άρθρο 6 παράγραφος 4).

- «Ελαχιστοποίηση δεδομένων»: Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκή, συναφή και να περιορίζονται σε ότι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

- «Ακρίβεια»: Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται. Επιπλέον, πρέπει να λαμβάνεται κάθε εύλογο μέτρο ώστε να διασφαλίζεται ότι τα δεδομένα που είναι ανακριβή διαγράφονται ή διορθώνονται χωρίς καθυστέρηση, λαμβανομένων υπόψη των σκοπών για τους οποίους υποβάλλονται σε επεξεργασία.

- «Περιορισμός αποθήκευσης»: Τα δεδομένα προσωπικού χαρακτήρα διατηρούνται υπό μορφή που επιτρέπει τον προσδιορισμό των προσώπων στα οποία αναφέρονται τα δεδομένα για χρονικό διάστημα που δεν υπερβαίνει τα αναγκαία για τους σκοπούς, για τους οποίους τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία. Τα προσωπικά δεδομένα μπορούν να αποθηκεύονται για μεγαλύτερες χρονικές περιόδους, για λόγους αρχειοθέτησης δημόσιου συμφέροντος ή για στατιστικούς σκοπούς (άρθρο 89 GDPR).

- «Ακεραιότητα και εμπιστευτικότητα»: Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να εξασφαλίζει την κατάλληλη ασφάλεια, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή βλάβη. Ενόψει αυτού, οι ελεγκτές δεδομένων εφαρμόζουν κατάλληλα τεχνικά ή οργανωτικά μέτρα.

- «Αρχή της Λογοδοσίας»: Οι υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία, όπως είναι οι οργανισμοί, οι φορείς, οι επιχειρήσεις, που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα, οφείλουν βάση του νέου Κανονισμού, να διαμορφώνουν τις διαδικασίες τους, τα τεχνικά αλλά και τα οργανωτικά τους συστήματά κατά τέτοιο τρόπο ώστε να μπορούν να αποδεικνύουν ενώπιον των εποπτικών αρχών, ότι είναι πλήρως συμμορφωμένοι. Αποτελεί ένα μηχανισμό εγγύησης της τήρησης των αρχών που διέπουν την επεξεργασία προσωπικών δεδομένων αφού μετατοπίζει το «βάρος της απόδειξης», όσον αφορά τη νομιμότητα της επεξεργασίας και τη συμμόρφωση με τον ΓΚΠΔ, από τις αρχές προστασίας δεδομένων στους ίδιους τους υπευθύνους επεξεργασίας ή τους εκτελούντες.

3.2 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Δεδομένου ότι η ανάλυση δεδομένων έχει γίνει η νέα τάση στην οικονομία του Διαδικτύου, όλοι οι σχετικοί ενδιαφερόμενοι συμμετέχουν σε "αγώνα" για την απόκτηση όλο και περισσότερων δεδομένων σχετικά με τη μέση συμπεριφορά των πολιτών. Και τι μπορεί να είναι μια καλύτερη πηγή δεδομένων προσωπικού χαρακτήρα από το κινητό τηλέφωνο, το οποίο κυριολεκτικά περιέχει λεπτομερείς πληροφορίες για τις καθημερινές δραστηριότητες, τις επιθυμίες, τις ιδιοτροπίες και τις κοινωνικές επαφές ενός χρήστη. Προφανώς η "ελεύθερη" χρήση των εφαρμογών κινητών τηλεφώνων έρχεται σε ένα σημαντικό κρυφό κόστος που είναι, αρκετά συχνά, η απεριόριστη πρόσβαση σε όλα τα είδη προσωπικών δεδομένων που είναι αποθηκευμένα στο κινητό τηλέφωνο του χρήστη [17]. Τι πραγματικά όμως συμβαίνει; Όπως θα αναλυθεί στην συνέχεια, η επεξεργασία προσωπικών δεδομένων μέσω τέτοιων εργαλείων δεν είναι πάντα διαφανής ή ελεγχόμενη από τους χρήστες. Δυστυχώς, η κατανόηση του τρόπου λειτουργίας των εφαρμογών είναι συχνά πολύπλοκη λόγω του δυναμικού τους περιβάλλοντος, της επαναχρησιμοποίησης των βιβλιοθηκών λογισμικού και της διασύνδεσης με διαφορετικά δίκτυα

και συστήματα, ως αποτέλεσμα να καθιστούν ακόμα πιο δύσκολη την εκτίμηση των χαρακτηριστικών τους όσον αφορά την ιδιωτική ζωή και την ασφάλεια.

Οι κίνδυνοι ιδιωτικότητας και προστασίας των εφαρμογών κινητής τηλεφωνίας προέρχονται κυρίως από δύο διαστάσεις:

- τη φύση τους, ως λογισμικό που εκτελείται σε ιδιωτικές κινητές συσκευές και
- τις ιδιαιτερότητες του περιβάλλοντος ανάπτυξης και διανομής κινητών συσκευών.

Στην συνέχεια παρέχεται μια πιο λεπτομερής ανάλυση των σχετικών κινδύνων ιδιωτικότητας μέσα από την χρήση εφαρμογών κινητής τηλεφωνίας.

1. Ποικιλία δεδομένων και πολλαπλοί αισθητήρες

Οι κινητές συσκευές μπορούν τυπικά να έχουν πρόσβαση σε διάφορους τύπους προσωπικών/ευαίσθητων δεδομένων όπως αυτά ορίστηκαν πιο πάνω, που παρέχονται από χρήστες μέσω διαφόρων εφαρμογών για κινητά. Βέβαια, οι βασικές συσκευές χειρός ενσωματώνουν πολλούς και διάφορους αισθητήρες όπως για παράδειγμα μικρόφωνο, φωτογραφική μηχανή, επιταχυνσιόμετρο, GPS, Wifi κ.λπ. που παράγουν πολύ προσωπικά δεδομένα και συνεπώς πιθανόν να έχουν απροσδόκητες επιπτώσεις στο ιδιωτικό απόρρητο. Στην περίπτωση αυτή, έχει αποδειχθεί ότι οι χρήστες μπορούν εύκολα να ταυτοποιηθούν και να επικυρωθούν από σήματα κίνησης που έχουν αποκτηθεί από τις έξυπνες κινητές συσκευές τους, όπως αδρανειακά σήματα που παρέχονται από τα περισσότερα εμπορικά κινητά τηλέφωνα [18].

Στις μέρες μας πλέον οι έξυπνες κινητές συσκευές περιέχουν υλικό GPS (Global Positioning System), το οποίο μπορεί να εντοπίσει με ακρίβεια τη θέση ενός χρήστη με αποτέλεσμα να μπορούν γεωγραφικά να εντοπιστούν και φυσικά να παρακολουθηθούν. Μια εκτίμηση της τοποθεσίας ενός χρήστη μπορεί επίσης να ληφθεί από άλλες πηγές, όπως τα κοντινά δίκτυα Wi-Fi και οι πύργοι κυψελών κινητής τηλεφωνίας [7]. Οι βιβλιοθήκες τρίτων μελών – δηλαδή έτοιμες βιβλιοθήκες λογισμικού τις οποίες ενσωματώνουν οι προγραμματιστές όταν αναπτύσσουν εφαρμογές, προς διευκόλυνσή τους - μπορούν να παρακολουθούν, προς γνώση των μελών αυτών που αναπτύσσουν τις βιβλιοθήκες, τις κινήσεις των χρηστών για να καθορίσουν το πού ζουν, εργάζονται και κινούνται με βάση την τοποθεσία τους σε διάφορες χρονικές στιγμές της μέρας. Συνεπώς μπορεί ο καθένας να συμπεράνει

το γεγονός ότι το χαρακτηριστικό αυτό μπορεί να έχει ως αποτέλεσμα σημαντική ζημιά στην ιδιωτική ζωή των χρηστών. Στην πραγματικότητα, πολλές πιθανώς ευαίσθητες προσωπικές πληροφορίες μπορούν να μαζευτούν για ένα άτομο από το ίχνος κινητικότητας τους [14].

Οι χρήστες συνηθίζουν όλο και περισσότερο στη δυνατότητα φωνητικού ελέγχου, υποστηριζόμενου από παράγοντες φωνητικής ανάλυσης όπως το Siri, το Google Now ή το Cortana. Ωστόσο, έχουν λιγότερη επίγνωση του γεγονότος ότι η λειτουργία φωνητικού ελέγχου πραγματοποιείται από μια συσκευή που ακούει τα πάντα - τουλάχιστον για να αντιδράσει σε ορισμένους όρους ελέγχου όπως "Hey Siri", "Okay Google", "Hey Cortana " ή "Hi Bixby" - και ως εκ τούτου έχει πρόσβαση σε όλες τις ομιλούμενες επικοινωνίες του χρήστη.

2. Προσωπική συσκευή και Συνεχής σύνδεση στο διαδίκτυο

Είναι ευρύτατα διαδεδομένο το γεγονός ότι οι χρήστες συχνά βλέπουν τις έξυπνες κινητές συσκευές ως επέκταση του εαυτού τους και τείνουν να τις θεωρούν αξιόπιστες, πολύ προσωπικές και τις οποίες δεν μοιράζονται με κανέναν. Εκτός από αυτό, οι εν λόγω συσκευές είναι σχεδόν πάντα ενεργοποιημένες, μεταφέρονται από τον χρήστη τους σχεδόν παντού και συνδέονται συνεχώς με ένα δίκτυο. Ιδιαίτερα σημαντικό θεωρείται το γεγονός ότι τα κινητά συνδέονται με διαφορετικά, ενδεχομένως κακόβουλα δίκτυα, τα οποία εισάγουν νέους κινδύνους ασφάλειας και ιδιωτικής ζωής [19] . Συνήθως αποθηκεύουν πολλά προσωπικά δεδομένα για μεγάλο χρονικό διάστημα. Κατά συνέπεια αυτό τις καθιστά τέλειους στόχους για τους μεσίτες δεδομένων, τους διαφημιστές ή τους ιχνηλάτες και μπορεί να οδηγήσει σε συνεχή παρακολούθηση των χρηστών.

3. Διαφορετικοί τύποι αναγνωριστικών

Οι κινητές συσκευές περιέχουν πολλά διαφορετικά είδη αναγνωριστικών [9] όπως αναγνωριστικό υλικού συσκευής IMEI (International Mobile Equipment Identity), αποθηκευμένα αρχεία ή και δακτυλικά αποτυπώματα που μπορούν να χρησιμοποιηθούν από τις εφαρμογές. Οι De Monjoye et al. έδειξαν ότι τέσσερα χωροχρονικά σημεία, που ενδεχομένως προέρχονται από μία έξυπνη κινητή συσκευή, αρκούν για να αποτυπώσουν τα δακτυλικά αποτυπώματα και συγκεκριμένα να αναγνωρίσουν με μοναδικό τρόπο το 95% των ατόμων [20]. Τα περισσότερα από αυτά τα αναγνωριστικά, όπως τα αποτυπώματα συμπεριφοράς, είναι μόνιμα και δύσκολα μπορούν να αλλάξουν.

4. Δημιουργία "προφίλ" και Δικαιώματα πρόσβασης εφαρμογών

Όπως θα αναλυθεί λεπτομερώς στο Κεφάλαιο 5, οι φορητές συσκευές μπορούν να παρακολουθούνται φυσικά μέσω των ασύρματων διεπαφών τους από τρίτους για τη δημιουργία φυσικών "προφίλ" των χρηστών. Φυσικά, πολλά τρίτα μέρη πραγματοποιούν παρακολούθηση μεταξύ διαφορετικών τομέων δραστηριότητας, δηλαδή συνδυάζουν τα φυσικά και τα διαδικτυακά προφίλ των χρηστών κινητής τηλεφωνίας από διάφορες εφαρμογές [21]. Αυτή η παρακολούθηση μεταξύ διαφορετικών τομέων δραστηριότητας μπορεί να προσφέρει μια πληρέστερη εικόνα της συμπεριφοράς του χρήστη και εισάγει νέους κινδύνους για την ιδιωτικότητα και την ασφάλεια προσωπικών δεδομένων του. Η παρακολούθηση ενός χρήστη μέσω των συσκευών του ή η παρακολούθηση μεταξύ των εφαρμογών του από τρίτα μέρη , όπου μια εφαρμογή προσπαθεί να εντοπίσει/παρακολουθήσει τις άλλες εγκατεστημένες εφαρμογές στην συσκευή, αναπτύσσουν επίσης πρακτικές που εισάγουν νέες και σοβαρές ανησυχίες για την προστασία της ιδιωτικής ζωής [22].

Ένας χρήστης μπορεί να δώσει σε μία εφαρμογή την άδεια να συλλέξει την τοποθεσία του και σε μια άλλη εφαρμογή να έχει πρόσβαση στις επαφές του. Εάν όμως και οι δύο εφαρμογές χρησιμοποιούν την ίδια βιβλιοθήκη τρίτου μέρους (third-party library), ο προγραμματιστής της βιβλιοθήκης θα μπορέσει να συνδέσει αυτά τα δύο στοιχεία μαζί [23]. Παραδείγματος χάριν, αποδείχθηκε ότι τα γνωρίσματα του χρήστη, όπως η θρησκεία, η κατάσταση της σχέσης του, οι χώρες που τον ενδιαφέρουν και αν ο χρήστης είναι γονέας μικρών παιδιών, μπορεί να προβλεφθεί από εφαρμογές για κινητά [24].

Αναλυτικότερα, διάφορα δεδομένα επικοινωνίας μπορούν να χρησιμοποιηθούν για την δημιουργία προφίλ ενός χρήστη. Από τα αρχεία καταγραφής κλήσεων και τα μηνύματα, ένας τρίτος μπορεί να καθορίσει τους στενούς φίλους του χρήστη και με την ανάλυση του συναισθήματος φωνής, μπορεί επίσης να είναι σε θέση να καθορίσει ποια επαφή είναι ο/η σύζυγος του χρήστη. Επίσης, η ανάλυση μηνυμάτων κειμένου μπορεί να βοηθήσει στην αποκάλυψη των ενδιαφερόντων ενός χρήστη. Η ένταση, η διάρκεια και ο χρόνος των τηλεφωνικών κλήσεων μπορούν να σχηματίσουν μια εικόνα για το αν ένας χρήστης είναι πολύ κοινωνικός ή όχι [7].

Είναι σαφές ότι η λίστα εφαρμογών που είναι εγκατεστημένες σε μια συσκευή μπορεί να είναι χρήσιμη για την κατανόηση των ενδιαφερόντων ενός χρήστη. Όπως έχουμε προαναφέρει, οι πληροφορίες σχετικά με τη χρήση της εφαρμογής μπορούν να

αποκαλύψουν το επίπεδο σπουδαιότητας καθενός από αυτά τα ενδιαφέροντα για τον χρήστη [7]. Εάν τα δεδομένα χρήσης των εφαρμογών συνδυάζονται με δεδομένα τοποθεσίας, μπορεί να προβληθεί μια ευρύτερη εικόνα ενός χρήστη. Παραδείγματος χάριν, ένας χρήστης που εκτελεί αυτήν την περίοδο μια εφαρμογή χρονομέτρου, δεν παρέχει ως πληροφορία κάποια σημαντική γνώση, αλλά όταν συνδυάζεται με δεδομένα θέσης ένας διαφημιζόμενος μπορεί να καθορίσει ότι ο χρήστης χρησιμοποιεί την εν λόγω εφαρμογή στο γυμναστήριο. Κατά συνέπεια, αυτός ο χρήστης μπορεί να είναι στόχος για διαφημίσεις σχετικά με προϊόντα γυμναστικής και σχετικά.

Κάποιος θα μπορούσε να υποστηρίξει ότι οι εφαρμογές προσπαθούν να ειδοποιήσουν τους χρήστες ζητώντας άδεια για πρόσβαση σε δεδομένα τηλεφώνου πριν από την εγκατάσταση. Ως εκ τούτου, θα έλεγε κανείς ότι οι χρήστες γνωρίζουν πλήρως το τι επεξεργασία θα συμβεί και παρέχουν προς τούτο συγκατάθεση μόνο αν το επιθυμούν. Ωστόσο, αυτή η άδεια εμφανίζεται με τη μορφή μίας μόνο σελίδας που μοιάζει με το «παράθυρο» που περιέχει τους όρους άδειας χρήσης πριν από την εγκατάσταση του επιτραπέζιου λογισμικού. Εν τούτοις , στις περισσότερες περιπτώσεις ο χρήστης δεν έχει καμία δυνατότητα να τροποποιήσει τα δικαιώματα που απαιτούνται από την εφαρμογή για κινητά. Δεδομένου ότι δεν υπάρχουν άλλα μέτρα για την ευαισθητοποίηση των χρηστών όσον αφορά την εκμετάλλευση των ιδιωτικών δεδομένων τους, οι χρήστες είναι περισσότερο από πρόθυμοι να πιέσουν το κουμπί "Εγκατάσταση" αγνοώντας το γεγονός πρόσβασης της εφαρμογής σε προσωπικά του δεδομένα [17] . Περαιτέρω, όπως προαναφέρθηκε, ο χρήστης δεν μπορεί να ελέγξει το τι πληροφορίες μπορεί να συλλέγονται από τρίτα μέλη που αναπτύσσουν βιβλιοθήκες λογισμικού – ακριβώς γιατί μία βιβλιοθήκη μπορεί να χρησιμοποιείται σε πολλές διαφορετικές εφαρμογές, συγκεντρώνοντας έτσι το υπερσύνολο όλων των δεδομένων στα οποία αποκτά πρόσβαση η κάθε εφαρμογή ξεχωριστά.

5. Περιορισμένη φυσική ασφάλεια

Οι συσκευές χειρός είναι συχνά μικρές φυσικές συσκευές, οι οποίες είναι δύσκολο να ασφαλιστούν. Μπορούν εύκολα να κλαπούν ή να καταστραφούν, γεγονός που μπορεί να έχει αντίκτυπο στην εμπιστευτικότητα, αλλά και στη διαθεσιμότητα των δεδομένων. Αξίζει να τονιστεί ότι οι εφαρμογές για κινητά αναπτύσσονται συχνά από ένα άτομο ή μια μικρή ομάδα ατόμων, με δυστυχώς περιορισμένους πόρους και τεχνογνωσία για θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής των χρηστών. Είναι επομένως δύσκολο για

τους προγραμματιστές να υιοθετήσουν τις τελευταίες τεχνικές λύσεις και μέτρα προστασίας της ιδιωτικής ζωής.

6. Αγορά εφαρμογών

Οι εφαρμογές διανέμονται συχνά μέσω συγκεκριμένων αγορών εφαρμογών, οι οποίες ενδέχεται να διαδραματίσουν σημαντικό ρόλο στην ασφάλεια και την προστασία της ιδιωτικής ζωής των χρηστών των εν λόγω εφαρμογών. Ένα κατάστημα εφαρμογών συνήθως δεν παρέχει μόνο πρόσβαση σε εφαρμογές, αλλά ταυτόχρονα παρέχει πληροφορίες για εφαρμογές και συλλέγει και εμφανίζει αξιολογήσεις χρηστών. Επίσης, ένα κατάστημα εφαρμογών μπορεί να πραγματοποιεί ελέγχους ασφαλείας σε κάθε παρεχόμενη εφαρμογή, προκειμένου να αποτρέψει τη διανομή κακόβουλων ή ψεύτικων εφαρμογών. Λόγω του σημαντικού ρόλου που διαδραματίζει η διανομή εφαρμογών, οι πάροχοι υπηρεσιών καταστημάτων εφαρμογών θα μπορούσαν να φιλτράρουν εφαρμογές που εμφανίζουν εμφανείς κινδύνους ασφάλειας. Δυστυχώς τα καταστήματα εφαρμογών παραμένουν ανεξέλεγκτα και η πρόσβαση στις δυνατότητες διανομής τους από προμηθευτές εφαρμογών και προγραμματιστές εφαρμογών παραμένουν ασαφής.

7. Διαδικτυακά κοινωνικά δίκτυα

Πολλές εφαρμογές δίνουν τη δυνατότητα σε έναν χρήστη να μοιράζεται τα δεδομένα του, συγκεντρωτικά και μη, με άλλους επιλεγμένους χρήστες για λόγους σύγκρισης ή για στατιστικούς σκοπούς, όπως σε ένα κοινωνικό δίκτυο. Αυτό το χαρακτηριστικό φέρει τον κίνδυνο διαρροής προσωπικών δεδομένων και εισάγει νέους κινδύνους για την προστασία της ιδιωτικής ζωής και της ασφάλειας που πρέπει να ληφθούν υπόψη.

3.3 Τρόποι Διαρροής Προσωπικών Δεδομένων σε Έξυπνη Κινητή Συσκευή Android.

Η συλλογή δεδομένων και η εξαγωγή νέων πληροφοριών ή γνώσεων από αυτήν μέσω της τεχνικής εξόρυξης δεδομένων μέσω μίας εφαρμογής, δεν είναι νέα [25]. Όπως προαναφέρθηκε στο προηγούμενο Κεφάλαιο, το μάρκετινγκ βάσεων δεδομένων (Database marketing) χρησιμοποιεί την εξόρυξη δεδομένων για την ανάπτυξη μοντέλων συμπεριφοράς των πελατών. Τα τυπικά εμπόδια στην πρόσβαση σε αυτές τις πληροφορίες είναι τεχνικά, δηλαδή εάν τα δεδομένα δεν μπορούν να συλλεχθούν τότε δεν μπορούν να αξιοποιηθούν. Ωστόσο, η σημερινή

κοινωνία των πληροφοριών σημειώνει τεράστια πρόοδο στην ικανότητα συλλογής δεδομένων από διαφορετικές πηγές.

3.3.1 Κατηγορίες Προσωπικών Δεδομένων που Πιθανόν να Διαρρέουν

Υπάρχουν διαφορετικές κατηγορίες ιδιωτικών δεδομένων τα όποια είναι διαθέσιμα σε εφαρμογές σε έξυπνες κινητές συσκευές Android. Σε κάθε κατηγορία αναφερόμαστε σε σχετικές λειτουργίες του Android API και περιγράφουμε πώς επιτυγχάνεται η συλλογή των ιδιωτικών δεδομένων. Αυτό δεν είναι ασήμαντο εφόσον υπάρχουν διάφοροι τρόποι ανάκτησης δεδομένων από Android API και κατά συνέπεια, τύποι πηγών πληροφοριών όπως [26]:

- Δεδομένα τοποθεσίας

  Συνήθως, τα δεδομένα θέσης μπορούν να ανακτηθούν είτε από δέκτη GPS που είναι διαθέσιμος στις περισσότερα πλέον έξυπνες κινητές συσκευές, είτε μπορεί να προσεγγιστεί με βάση τη θέση του χρησιμοποιημένου σταθμού βάσης κυψελοειδές δίκτυού (3G,4G) είτε από το σταθμό βάσης WLAN (Wireless Local Area Network). Η κατηγορία LocationManager παρέχει πρόσβαση σε δεδομένα τοποθεσίας και υποστηρίζει διάφορους παρόχους, όπως δέκτη GPS ή δίκτυο κινητής τηλεφωνίας. Η μέθοδος getLastKnownLocation επιστρέφει ένα αντικείμενο θέσης που αντιπροσωπεύει την τελευταία θέση x που έχει αποκτηθεί από ένα συγκεκριμένο πάροχο. Εναλλακτικά, η πρόσβαση στα δεδομένα τοποθεσίας μπορεί να αποκτηθεί χρησιμοποιώντας την εντολή location listener η οποία μπορεί να παρακολουθήσει μέσω μίας εφαρμογής την τοποθεσία του τηλεφώνου. Η εφαρμογή μπορεί να αντικαταστήσει τη μέθοδο location changed (Location Location) που καλείται από το πλαίσιο αυτής για να την ενημερώσει την σχετικά με μια νέα θέση x που περιέχεται στη παράμετρο της θέσης. Η παρακολούθηση ενεργοποιείται με την κλήση της εντολής requestLocationUpdate.

- Μοναδικοί προσδιοριστές ταυτότητας

  Ένα κινητό τηλέφωνο αποθηκεύει αρκετά μοναδικά αναγνωριστικά στοιχεία όπως η διεθνής ταυτότητα κινητού εξοπλισμού (IMEI – International Mobile Equipment Identity), η οποία είναι παγκοσμίως μοναδική για κάθε κινητό τηλέφωνο με βάση το GSM (Global System of Mobile Communication) την Διεθνής ταυτότητα συνδρομητών κινητής τηλεφωνίας (IMSI – International Mobile Subscriber Identity), η οποία είναι παγκοσμίως μοναδική για κάθε συνδρομητή υπηρεσιών GSM. Αυτά τα μοναδικά αναγνωριστικά μπορούν να χρησιμοποιηθούν για την ταυτοποίηση των συσκευών και των συνδρομητών

με μεγάλη ακρίβεια. Η εντολή Telephony Manager μπορεί να παρέχει πρόσβαση σε τέτοια αναγνωριστικά.

Identifier	Description	Attribute
GAID	User-resettable 32-digit alphanumeric identifier	Pseudonymous
Android ID	64-bit number randomly generated when device is set up for the first time [5]	Semi-permanent
IMEI	15-digit decimal identifier representing GSM or LTE device	Permanent
IMSI	15-digit decimal identifier representing mobile subscriber identity	Permanent
MAC address	48-bit number assigned to the device's Wi-Fi network interface	Permanent

Εικόνα 3.3: Μοναδικά αναγνωριστικά κινητής συσκευής Android [27].

- Κατάσταση κλήσεων

Οι εφαρμογές Android μπορούν να παρακολουθήσουν την τρέχουσα κατάσταση του κινητού τηλεφώνου. Οι εφαρμογές ενημερώνονται σχετικά με το έναρξη και λήξη εισερχόμενων και εξερχόμενων κλήσεων. Η εντολή PhoneStateListener μπορεί να χρησιμοποιηθεί από μερικές εφαρμογές για την παρακολούθηση των εισερχόμενων τηλεφωνικών κλήσεων. Κατά την χρήση της εντολής, η εφαρμογή αντικαταθιστά την εντολή με τη μέθοδο CallStateChanged, η οποία καλείται από το πλαίσιο της εφαρμογής εάν η κατάσταση της κλήσης αλλάξει. Η παράμετρος incomingNumber περιέχει τον αριθμό τηλεφώνου της εισερχόμενης κλήση. Η παρακολούθηση ενεργοποιείται καλώντας τη μέθοδο TelephonyManager.listen.

- Στοιχεία αυθεντικοποίησης.

Το Android παρέχει ένα ενιαίο σύστημα σύνδεσης, όπου οι εφαρμογές του μπορούν να αιτηθούν πιστοποιητικά (tokens) αυθεντικοποίησης από το λειτουργικό σύστημα AndroidOS για πρόσβαση σε λογαριασμούς και σε διαδικτυακές υπηρεσίες χωρίς να είναι απαραίτητο ο χρήστης να εισαγάγει τα διαπιστευτήρια. Η εντολή AccountManager χρησιμοποιείται για να αποκτήσει ένα πιστοποιητικό (token) αυθεντικοποίησης ταυτότητας για έναν λογαριασμό χρήστη που είναι αποθηκευμένος στη κινητή συσκευή. Εάν ο χρήστης αποθηκεύσει τον κωδικό πρόσβασης για κάποιο λογαριασμό στο τηλέφωνο ή έχει ήδη αποθηκευτεί προσωρινά ένα πιστοποιητικό ελέγχου ταυτότητας, ο χρήστης δεν θα ενημερωθεί σχετικά με το αίτημα και το πιστοποιητικό θα παρασχεθεί στο

παρασκήνιο. Ένα πιστοποιητικό ταυτοποίησης μπορεί να ζητηθεί με τη μέθοδο getAuthToken που επιστρέφει ένα AccountManagerFuture.

- Στοιχεία επικοινωνίας και ημερολογίου

Τα έξυπνα τηλέφωνα Android χρησιμοποιούνται σχεδόν πάντοτε για τη διαχείριση προσωπικών πληροφοριών και κατά συνέπεια αποθηκεύουν διευθύνσεις και αριθμούς τηλεφώνου καθώς και ραντεβού. Αυτά τα δεδομένα παρέχονται συνήθως από έναν παροχέα περιεχομένου και μπορούν να προσεγγιστούν με ερωτήσεις που χρησιμοποιούν σύνταξη τύπου SQL για να λάβουν τα ανακτημένα δεδομένα. Ένα ερώτημα μπορεί να εκτελεστεί, για παράδειγμα με τις μεθόδους Activity.managedQuery ή ContentResolver.query.

3.3.2 Διαβίβαση Προσωπικών Πληροφοριών

Όσο οι προσωπικές πληροφορίες αποθηκεύονται σε κάποια μεταβλητή μιας εφαρμογής Android, τόσο περισσότερες πιθανότητες δημιουργούνται να διαρρέουν προς τα έξω. Παρακάτω προσδιορίζονται διάφοροι τρόποι διαρροής πληροφοριών [28]

- Επικοινωνία SMS

Μια εφαρμογή μπορεί να στείλει πληροφορίες σε άλλα τηλέφωνα ή οργανισμούς χρησιμοποιώντας την υπηρεσία smsManager. Με την μέθοδο getDefault() συσκευάζονται οι ιδιωτικές πληροφορίες σε ένα μήνυμα. Το μήνυμα μπορεί να σταλεί στον προορισμό του με την μέθοδο sendTextMessage () και sendMultipart- Μέθοδος TextMessage ()

- Επικοινωνία δικτύου

Οι εφαρμογές Android μπορούν να έχουν πρόσβαση στο Διαδίκτυο μέσω πολλών διαφορετικών API (Applications Interfaces). Μπορούν επίσης να έχουν πρόσβαση στο διαδίκτυο μέσω της μεθόδου socket. Η μέθοδος socket (String dstName, int dstPort) δημιουργεί μια νέα υποδοχή συνεχούς ροής (socket) η οποία είναι συνδεδεμένη με τον κεντρικό υπολογιστή προορισμού (ο διακομιστής της εφαρμογής) αφού ρυθμιστούν οι παράμετροι dstName και dstPort. Το dstName είναι η IP (Internet Protocol) διεύθυνση του διακομιστή προορισμού και το dstPort είναι ο αριθμός της θύρας του διακομιστή προορισμού.. Στην συνέχεια με τη μέθοδο getOutputStream μια ροή εξόδου ανακαλείται από ένα ανοιχτό socket, η οποία χρησιμοποιείται για εγγραφή στην ανοικτή σύνδεση του δικτύου. Στη συνέχεια, τα γραπτά δεδομένα μεταδίδονται στον προορισμό.

Από τα ανωτέρω, γίνεται σαφές ότι σε ολόκληρο το «οικοσύστημα» των έξυπνων εφαρμογών συντελείται διαρκώς μίας εκτενής επεξεργασία προσωπικών δεδομένων, από διάφορους εμπλεκόμενους (παρόχους λειτουργικών συστημάτων, προγραμματιστές εφαρμογών, τρίτα μέλη που αναπτύσσουν βιβλιοθήκες λογισμικού). Το γεγονός αυτό επιτείνει τους κινδύνους στα να συσσωρεύεται, σε κάποιο από τα εν λόγω μέλη, περισσότερη πληροφορία από ό,τι θα έπρεπε, πιθανότατα και ερήμην των χρηστών – πληροφορία η οποία μπορεί να χρησιμοποιηθεί περαιτέρω για άλλους σκοπούς. Με άλλα λόγια, ακριβώς λόγω της φύσης του περιβάλλοντος στο οποίο λειτουργούν οι «έξυπνες» συσκευές, ελλοχεύουν σοβαροί κίνδυνοι ιδιωτικότητας.

Κεφάλαιο 4
Εφαρμογές με Δικαιώματα Πρόσβασης στη Τοποθεσία

Είναι κοινά παραδεκτό το γεγονός ότι η δημοτικότητα των έξυπνων κινητών συσκευών οφείλεται στη διαθεσιμότητα ενός ευρέος φάσματος εφαρμογών, οι οποίες εμπλουτίζουν την καθημερινότητα και αυξάνουν τη χρηστικότητα. Μια νέα διάσταση που προδίδεται στη χρηστικότητα των εν λόγω εφαρμογών βασίζεται στην δυνατότητα προσδιορισμού της γεωγραφικής θέσης του χρήστη. Ως αποτέλεσμα των τελευταίων στατιστικών μελετών, μεγάλη δημοτικότητα παρουσιάζουν οι εφαρμογές οι οποίες χρησιμοποιούν την δυνατότητα εντοπισμού της θέσης του χρήστη με απώτερο σκοπό την καθοδήγησή του και την παροχή πληροφοριών τοποθεσίας. Όπως παρουσιάζεται και στο διαδίκτυο και συγκεκριμένα σε σελίδα στατιστικών στοιχείων , η οποία παρουσιάζει στατιστικά στοιχεία σχετικά με την εμβέλεια της αγοράς από τις πιο δημοφιλείς κατηγορίες εφαρμογών Android παγκοσμίως, τον Ιούνιο του 2018, παρατηρούμε ότι η κατηγορία Maps & Navigation κατέχει ένα αρκετά σεβαστό ποσοστό της τάξης του 18,67% [36]. Οι υπηρεσίες βασισμένες στην τοποθεσία (LBS-Location Based Services) χρησιμοποιούνται

από εφαρμογές πληροφοριών ή ψυχαγωγίας εγκατεστημένες σε κινητές συσκευές όπως φορητοί υπολογιστές, κινητά τηλέφωνα ή tablet. Μπορούν να καθορίσουν την τοποθεσία των χρηστών μέσω των συσκευών τους λαμβάνοντας τις πληροφορίες θέσης τους μέσω του Παγκόσμιου συστήματος εντοπισμού θέσης (GPS- Global Positioning System) [13].

4.1 Υπηρεσίες Βασισμένες στη Τοποθεσία και Προσωπικά Δεδομένα

Οι υπηρεσίες βάσει τοποθεσίας (LBS-Location Based Services) χρησιμοποιούν γεωγραφικά δεδομένα σε πραγματικό χρόνο από κινητή συσκευή ή smartphone για την παροχή πληροφοριών, ψυχαγωγίας ή ασφάλειας. Οι υπηρεσίες αυτές είναι αρκετά δημοφιλείς στις πλατφόρμες κινητών υπολογιστικών συσκευών, όπως το Android. Ωστόσο, θα μπορούσαν επίσης να οδηγήσουν σε διαρροή πλήθους προσωπικών πληροφοριών σχετικά με τον ιδιοκτήτη του τηλεφώνου, εάν χρησιμοποιούνται από κακόβουλα λογισμικά. Έχει παρατηρηθεί ότι ένας αυξημένος αριθμός κακόβουλων εφαρμογών Android χρησιμοποιεί το LBS για να αποκτήσουν τοποθεσίες χρηστών και να τις μεταδώσουν σε εισβολείς χωρίς την έγκριση των χρηστών, προκαλώντας παραβίαση της ιδιωτικής ζωής τους [28].

Πιο συγκεκριμένα τα συστήματα παρακολούθησης τοποθεσίας (LBS) χρησιμοποιούνται όλο και περισσότερο από τις επιχειρήσεις για να παρέχουν νέες υπηρεσίες στους πελάτες. Επιπροσθέτως, χρησιμοποιούνται από κυβερνητικές οντότητες για τον εντοπισμό πιθανών εγκληματιών και, ως εκ τούτου, για τη βελτίωση της ασφάλειας των κοινοτήτων. Παρόλα αυτά μέσω του LBS παρατηρείται διαρροή προσωπικών δεδομένων που όμως δεν αποτελεί κατ' ανάγκην παραβίαση της ιδιωτικής ζωής. Είναι γνωστό ότι μέσω της χρήσης LBS διαρρέουν προσωπικά δεδομένα σχετικά με τις τοποθεσίες μας. Ειδικότερα, όταν οι πληροφορίες τοποθεσίας συνδυάζονται με προσωπικά αναγνωριστικά, τότε έχει ως αποτέλεσμα την πιθανή παραβίαση του ιδιωτικού απορρήτου [13]. Σε αυτές τις περιπτώσεις, θα έπρεπε να είναι αναγκαία η συναίνεσητου χρήστη για την εξισορρόπηση των δικαιωμάτων ιδιωτικής ζωής των ατόμων έναντι των δικαιωμάτων ελευθερίας των επιχειρήσεων και των δικαιωμάτων ασφάλειας των κοινοτήτων.

Η εκμετάλλευση της τοποθεσίας δίνει τη δυνατότητα για αναζήτηση συγκεκριμένου πλαισίου και στοχευμένο μάρκετινγκ (διαφήμιση). Πράγματι, οι υπηρεσίες βάσει τοποθεσίας προσφέρουν μια

νέα διάσταση στο κλασικό μάρκετινγκ βάσεων δεδομένων αποκαλύπτοντας τη φυσική τοποθεσία. Παρόλο που αυτό επιτρέπει βελτιωμένες υπηρεσίες ή εμπειρίες, είναι επίσης δυνατές περισσότερες δραστηριότητες μάρκετινγκ προσανατολισμένες στις φυσικές τοποθεσίες που επισκέπτεται ο χρήστης [25]. Επιπλέον, η διαρροή πληροφοριών θέσης είναι ένα συχνό φαινόμενο για τις νόμιμες και μη εφαρμογές. Υπάρχουσες έρευνες δείχνουν ότι 27 από τις 50 πιο διαδεδομένες βιβλιοθήκες διαφήμισης, αποκτούν πληροφορίες θέσης των χρηστών για να προβάλλουν διαφημίσεις με βάση αυτή [29].

Είναι απαραίτητο να επισημανθεί ότι ένας αυξημένος αριθμός κακόβουλων εφαρμογών Android χρησιμοποιούν το LBS για την απόκτηση θέσεων των χρηστών και τη μετάδοσή τους σε τρίτα μέρη χωρίς την έγκριση αυτών, προκαλώντας παραβίαση της ιδιωτικής τους ζωής. Ως εκ τούτου, παλαιότερα αναπτύχθηκε ένα εργαλείο ανίχνευσης διαρροών πληροφοριών που ονομάζεται Brox [28]. Το Brox χρησιμοποιεί ένα πλαίσιο ανάλυσης ροής δεδομένων εξοπλισμένο με τεχνικές ευαίσθητες στην ροή, ευαίσθητες στο περιβάλλον και βασίζεται σε εσωτερικές διαδικασίες, για την ανίχνευση της διαδρομής διαρροής των πληροφοριών σε κακόβουλες εφαρμογές Android.

Παρόλο που η FTC (Ομοσπονδιακής Επιτροπής Εμπορίου των Ηνωμένων Πολιτειών Αμερικής) πρότεινε σε εταιρείες να εξετάσουν το ενδεχόμενο να προσφέρουν ένα μηχανισμό DNT (Do Not Track) για χρήστες smartphone, η πρόληψη της διαρροής δεδομένων τοποθεσίας εξακολουθεί να αποτελεί πρόκληση στην πράξη λόγω της ύπαρξης κακόβουλων εφαρμογών. Ένα καλό παράδειγμα είναι η πρόσφατα ανακαλυφθείσα κακόβουλη εφαρμογή Secret Tracking [30], η οποία λαμβάνει τις πληροφορίες θέσης του χρήστη από το GPS και στη συνέχεια στέλνει τις πληροφορίες μέσω SMS με μυστικό τρόπο. Για την αντιμετώπιση του προβλήματος αυτού, ο C. Gibler παρουσίασε το AndroidLeaks [31], ένα αυτόματο εργαλείο για την ανίχνευση πιθανών διαρροών απορρήτου στο σύστημα Android. Το AndroidLeaks εφαρμόζει με επιτυχία το υπάρχον πλαίσιο ανάλυσης Java στις εφαρμογές του Android μεταφράζοντάς τες σε αρχείο τύπου JAR. Εκτός απ' αυτό ο M. Grace παρουσίασε επίσης ένα κλιμακωτό και ακριβές πλαίσιο ανίχνευσης κακόβουλου λογισμικού, το RiskRanger, βασισμένο σε εφαρμογές φιλτραρίσματος βάση της συμπεριφοράς τους [32]. Παρόλα αυτά τα αποτελέσματά του μπορεί να είναι ανακριβή επειδή χρησιμοποιεί μόνο την προσπελάσιμη ανάλυση, χωρίς να λαμβάνει υπόψη την ανάλυση της φθοράς.

Σύμφωνα με το περιεχόμενο της διαρροής μπορούμε να κατηγοριοποιήσουμε τη διαρροή δεδομένων σχετικών με GPS πληροφορίες σε δύο τύπους.

1. Διαρροή μόνο πληροφοριών GPS των συσκευών.

2. Διαρροή όχι μόνο πληροφοριών GPS αλλά και άλλων προσωπικών δεδομένων, όπως μοναδικούς προσδιοριστές της συσκευής (π.χ IMEI) και αριθμούς τηλεφώνων.

Παράλληλα σύμφωνα με τον τρόπο ενεργοποίησης της διαρροής, διαιρούμε τη συμπεριφορά της διαρροής απορρήτου σε τρεις τύπους [28].

1. Η συμπεριφορά που προκαλείται από την αλληλεπίδραση του χρήστη με την εφαρμογή.

2. Η συμπεριφορά που ενεργοποιείται αυτόματα από τις υπηρεσίες που εκτελούνται στο παρασκήνιο (background).

3. Και η συμπεριφορά που ενεργοποιείται αυτόματα από υπηρεσίες στο παρασκήνιο και αλληλεπίδραση χρήστη.

Γεγονός αποτελεί ότι οι προγραμματιστές κακόβουλου λογισμικού Android προτιμούν να γράψουν την κακόβουλη εφαρμογή με πιο περίπλοκο μοντέλο δομής δεδομένων και πιο περίπλοκη λογική [28]. Αυτό απαιτεί, ο αναλυτής να αυξήσει την ικανότητα που απαιτείται για να χειριστεί την κατάσταση αυτή. Σύμφωνα με μια πρόσφατη έκθεση, το κακόβουλο λογισμικό Android χρησιμοποιεί περισσότερες τεχνικές για να αποφύγει την ανίχνευση, συμπεριλαμβανομένης της δυναμικής φόρτωσης κώδικα, της κρυπτογράφησης και της εκμετάλλευσης εγγενών κωδικών.

4.2 Global Positioning System

Το GPS (Global Positioning System), είναι παγκόσμιο σύστημα εντοπισμού γεωγραφικής θέσης, ακίνητου ή κινούμενου χρήστη, το οποίο βασίζεται σε ένα "πλέγμα" εικοσιτεσσάρων δορυφόρων της Γης, εφοδιασμένων με ειδικές συσκευές εντοπισμού, οι οποίες ονομάζονται "πομποδέκτες GPS". Οι πομποδέκτες αυτοί παρέχουν ακριβείς πληροφορίες για τη θέση ενός σημείου, το υψόμετρό του, την ταχύτητα και την κατεύθυνση της κίνησης του. Επίσης, σε συνδυασμό με ειδικό λογισμικό χαρτογράφησης μπορούν να απεικονίσουν γραφικά τις πληροφορίες αυτές [33].

Αναλυτικότερα ένα Global Positioning System (GPS) χρησιμοποιεί έναν αστερισμό δορυφόρων GPS που περιστρέφουν τη γη. Αυτοί οι δορυφόροι μεταδίδουν μηνύματα σε ραδιοσυχνότητες που αποτελούνται από το χρόνο του μηνύματος και από τις πληροφορίες τροχιάς. Ένας δέκτης GPS μετρά τους χρόνους διέλευσης των μηνυμάτων από τέσσερις δορυφόρους για να καθορίσει την απόστασή του από κάθε δορυφόρο και έτσι να υπολογίσει τη θέση του. Στις Ηνωμένες Πολιτείες, οι αξιωματούχοι επιβολής του νόμου χρησιμοποιούν την τεχνολογία GPS για την παρακολούθηση ύποπτων εγκληματικών ενεργειών χωρίς βεβαίως την επίγνωσή τους. Για παράδειγμα, μπορεί να επισυνάψουν στο αυτοκίνητο του υπόπτου μια συσκευή (Trackstick, ™) η οποία είναι ένα σύστημα καταγραφής δεδομένων GPS ενσωματωμένη στο GoogleEarth [13].

Η χρήση του συστήματος Global Positioning System (GPS) είναι πολύ επωφελής μέσω των κινητών συσκευών, καθιστώντας τη ζωή του χρήστη πιο εύκολη, π.χ. βρίσκοντας σημεία ενδιαφέροντος κοντά, όπως πρατήρια καυσίμων, υπεραγορές, εστιατόρια κλπ. Παρόλα αυτά, η τοποθεσία του χρήστη μπορεί να χρησιμοποιηθεί για άλλους σκοπούς και, ως εκ τούτου, να προκύπτουν θέματα ιδιωτικού απορρήτου. Από τεχνική άποψη, η τοποθεσία προσδιορίζεται είτε εσωτερικά από τη συσκευή είτε εξωτερικά μέσω αλληλοεπιδρώντων συστημάτων και δικτύων. Οι προκύπτουσες πληροφορίες θέσης μπορούν να αποθηκευτούν και να χρησιμοποιηθούν υπό διάφορες συνθήκες και οι εφαρμογές μπορούν να παρακολουθήσουν τη θέση του χρήστη χωρίς τη συγκατάθεσή του και τελικά να το καταχραστούν για παράδειγμα με σκοπό την αποστολή ανακατευθυνόμενης δημοσιότητας ή ακόμα και την καταγραφή των θέσεων του χρήστη [34].

Αξίζει να τονιστεί ότι το GPS χρησιμοποιείται από ορισμένες χώρες οι οποίες απαιτούν όλα τα μηχανοκίνητα οχήματα τους να έχουν συσκευές GPS έτσι ώστε να ελέγχουν και να παρακολουθούν τις αποστάσεις που ταξιδεύουν, με αποτέλεσμα, να μπορούν να εισπράττουν φόρους από τους αυτοκινητιστές, ανάλογα με τα χιλιόμετρα και να πληρώνουν για την κατασκευή και συντήρηση των αυτοκινητοδρόμων[13]. Αυτοί οι φόροι βάσει των χιλιομέτρων που διανύουν τα οχήματα θα αντικαταστήσουν τους φόρους καυσίμων, των οποίων τα έσοδα μειώνονται καθώς ο αριθμός των ηλεκτρικών και υβριδικών αυτοκινήτων αυξάνεται. Επιπλέον, το GPS χρησιμοποιείται από επιχειρήσεις, όπως υπηρεσίες παράδοσης πακέτων, για την παρακολούθηση εργαζομένων που ταξιδεύουν σε πολλαπλές τοποθεσίες κατά τη διάρκεια κάθε εργάσιμης ημέρας. Ακόμη ορισμένοι εργοδότες χρησιμοποιούν το ιστορικό τοποθεσίας των εργαζομένων για να συμπεράνουν τις προθέσεις τους ή για να οικοδομήσουν σχέσεις κοινωνικής δικτύωσης . Επειδή όμως οι συσκευές GPS ενσωματώνονται συχνά στα κινητά τηλέφωνα, τα άτομα ενδέχεται να μην γνωρίζουν ότι οι τοποθεσίες τους καταγράφονται όταν τα κινητά τους τηλέφωνα είναι ενεργοποιημένα.

4.2.1 Μέθοδοι Εξαγωγής Τοποθεσίας

Οι μέθοδοι για την εξαγωγή τοποθεσίας μιας κινητής συσκευής μπορούν να κατηγοριοποιηθούν στις ακόλουθες δύο προσεγγίσεις [35]:

«Host Based», δηλαδή βασισμένο στον κεντρικό υπολογιστή: Σε αυτήν την προσέγγιση, μια εγκατεστημένη εφαρμογή μπορεί να εξαγάγει τη θέση της συσκευής εξετάζοντας ενσωματωμένους αισθητήρες. Οι τοπικοί αισθητήρες μπορούν να παρέχουν δεδομένα θέσης που περιλαμβάνουν πληροφορίες hotspot (Wi-Fi) όπως SSID και BSSID, συνδεδεμένα με το τηλεφωνικό δίκτυο, καθώς και GPS . Η θέση μπορεί επίσης να συναχθεί με τη χρήση διαφόρων επιπτώσεων από πλευράς καναλιών, όπως με την χρήση ανάλυσης διακύμανσης τροφοδοσίας.

«Network Based», δηλαδή βασισμένο στο δίκτυο: Με αυτήν την προσέγγιση, η θέση της κινητής συσκευής μπορεί να ληφθεί με τη χρήση του τριγωνισμού μέσα από τους πύργους κινητής τηλεφωνίας, οι οποίοι παρέχουν ασύρματο διαδίκτυο στις κινητές συσκευές που παρέχουν κάρτα SIM.

4.2.2 GPS και Προσωπικά Δεδομένα

Τα τηλέφωνα με δυνατότητα GPS έχουν συμβάλει στη δημιουργία μιας νέας εποχής αποκάλυψης πληροφοριών και είναι πιθανό να εμφανιστούν νέες υπηρεσίες, οι οποίες ενθαρρύνουν τους ανθρώπους να αποκαλύπτουν πού βρίσκονται ανά πάσα στιγμή. Αν και αυτές οι υπηρεσίες είναι αναμφισβήτητα χρήσιμες, τα φαινομενικά αβλαβή δεδομένα μπορεί να μην αποκαλύπτουν μόνο πού βρισκόμαστε αλλά μπορούν να εκθέσουν πτυχές της ιδιωτικής ζωής μας που με την πρώτη ματιά μπορεί να μην είναι εμφανείς. Επιπλέον είναι δυνατό να συγκεντρωθούν είδη πληροφοριών με την πάροδο του χρόνου και να χρησιμοποιηθούν τεχνικές εξόρυξης δεδομένων για την εξαγωγή ενός "προφίλ συμπεριφοράς" από τα δεδομένα που έχουν διαρρεύσει [25]. Προβλήματα θα μπορούσαν να προκύψουν εάν, για παράδειγμα, οι πληροφορίες αυτές χρησιμοποιούνται από τρίτους για να διαφοροποιήσουν τις υπηρεσίες τους ή τις τιμές που αφορούν το άτομο, σε ορισμένες περιπτώσεις σε βάρος τους. Αυτό συμβαίνει ιδιαίτερα επειδή ο τελικός χρήστης μπορεί να μην έχει ιδέα ότι αυτό συμβαίνει ή μάλιστα πώς συμβαίνει.

Πρόσφατες Έρευνες ανέφεραν υψηλό ποσοστό διαρροής προσωπικών δεδομένων από δημοφιλείς εφαρμογές σε αβέβαια κανάλια επικοινωνίας χωρίς την ευαισθητοποίηση των χρηστών. Συγκεκριμένα, οι εν λόγω μελέτες έδειξαν ότι τα δεδομένα θέσης από τα πιο δημοφιλείς

προσωπικά αναγνωρίσιμες πληροφορίες διαρροής , καθώς το 10% των πιο δημοφιλών εφαρμογών διαγράφει δεδομένα θέσης σε απλό κείμενο . Στην πραγματικότητα, σύμφωνα με την Trend Micro, η άδεια θέσης αναγνωρίστηκε ως η πιο «κακοποιημένη» άδεια εφαρμογής Android [35].Τα δεδομένα τοποθεσίας μπορούν να μεταδοθούν μέσω της κίνησης δικτύου σε πολλές μορφές, όπως: σαφείς γεωγραφικές συντεταγμένες, ονόματα πόλεων ή σημεία ενδιαφέροντος, δίκτυα Wi-Fi (BSSID) και δεδομένα κυψελοειδούς δικτύου (Cell ID).

Με βάση τα πιο πάνω αυτό σημαίνει ότι οι συσκευές με δυνατότητα GPS μπορούν να παρακολουθούν επίμονα το σημείο όπου ο χρήστης πηγαίνει, με αποτέλεσμα την δημιουργία προφίλ του χρήστη με βάση τα δεδομένα που έχουν διαρρεύσει. Στην περίπτωση της παρακολούθησης πολλών χρηστών, μπορούν επίσης να συναχθούν κοινωνικές και επιχειρηματικές σχέσεις. Το πλεονέκτημα για τον χρήστη είναι ότι, για παράδειγμα, όταν ταξιδεύει σε μια νέα πόλη, ο χρήστης μπορεί να ζητήσει από την υπηρεσία ατομικές ειδικές αλλά και αφηρημένες ερωτήσεις: "Πού είναι τα εστιατόρια που θα ήθελα;" κλπ. Το μειονέκτημα είναι ότι τα δεδομένα που χρησιμοποιούνται για τη δημιουργία αυτών των προφίλ αναδεικνύουν αναπόφευκτα πολύ περισσότερα για τον χρήστη [25].

Προκειμένου να χρησιμοποιηθούν τα ίχνη θέσης ως σημαντική πηγή πληροφοριών, είναι επιτακτική η ανάλυση των δεδομένων και η συγκέντρωσή τους σε ομάδες τοποθεσιών που είναι σημαντικές για τον χρήστη, όπως το σπίτι, τα ψώνια ή το χώρο εργασίας του. . Αυτές οι θέσεις είναι επίσης γνωστές ως τα σημεία ενδιαφέροντος των χρηστών (POI-Point of Interest). Η πιο συνηθισμένη προσέγγιση για την εξαγωγή των POI χρηστών από τα ίχνη τοποθεσίας είναι η συγκέντρωση των ιχνών θέσης με κατώτατα όρια απόστασης και χρόνου με αποτέλεσμα να δημιουργηθεί ένα σύμπλεγμα το οποίο να ελέγχει εάν ο χρήστης έχει μείνει στον ίδιο χώρο για αρκετό χρόνο [35].

Με τον υπολογισμό της συχνότητας των επαναλαμβανόμενων PoI, κατατάχθηκαν οι θέσεις κλειδιά για κάθε χρήστη [25]. Αυτά δίνονται και αναλύονται περαιτέρω πιο κάτω:

- Τόπος κατοικίας και εργασίας: Εάν εξετάσουμε τον τρόπο δημιουργίας των POI, είναι προφανές ότι οι βασικές τοποθεσίες είναι εκείνες που επισκέπτονται συχνά και έτσι θα προσελκύσουν ένα "σύμπλεγμα" σημείων PoI. Ειδικότερα, η αναγνώριση της ακριβούς θέσης μπορεί να παρεμποδιστεί από την ασαφή συσσώρευση των σημείων δεδομένων PoI. Σε ορισμένες περιπτώσεις, η αποχώρηση και επιστροφή από ένα κτίριο εργασίας αρκετές φορές κατά τη διάρκεια της ημέρας μπορεί να είναι συνηθισμένο και έτσι θα

εγγραφεί πολλές φορές ανά (εργάσιμη) ημέρα. Η χρήση χρονικών δεδομένων μπορεί επίσης να χρησιμεύσει για την αποκάλυψη της ταυτότητας ορισμένων PoIs-για παράδειγμα, η τοποθεσία που συμβαίνει συχνότερα πρώτο και τελευταίο πράγμα κατά τη διάρκεια της ημέρας είναι πιθανό να είναι η κατοικία.

- Φύλο: Πολύ λίγες πληροφορίες μπορούν να σχετίζονται με το φύλο. Βέβαια, παρόλο που η επίσκεψη σε συγκεκριμένα καταστήματα ή η πραγματοποίηση συγκεκριμένων αγορών μπορεί να είναι ένας δείκτης ως προς φύλο του ατόμου, εν τούτοις αυτές οι πληροφορίες μπορεί να προέρχονται από το γεγονός ότι ο χρήστης συνοδεύεται από μέλος του αντίθετου φύλου. Χωρίς συγκεκριμένους δείκτες, όπως η χρήση μιας συγκεκριμένης δημόσιας τουαλέτας ή η είσοδος σε ένα ειδικό για το φύλο περιβάλλον, το οποίο δεν εμφανίζεται σε αυτά τα δεδομένα, δεν μπορεί να αποδοθεί σε κάποιον με απόλυτη εμπιστοσύνη το φύλο του.

- Κοινωνική κατάσταση: Υπάρχουν πολλοί δείκτες κοινωνικής κατάστασης στα δεδομένα. Πρώτον, ένας βασικός είναι η περιοχή στην οποία βρίσκεται η κατοικία των χρηστών. Δεδομένου ότι αυτό προσδιορίζεται εύκολα από τα δεδομένα θέσης και δεδομένης της αυξανόμενης διαθεσιμότητας των γεω-δημογραφικών πόρων του διαδικτύου. Ένα άλλο μέτρο της κοινωνικής κατάστασης είναι οι άνθρωποι με τους οποίους ένας χρήστης κοινωνικοποιείται - αυτό είναι ιδιαίτερα χρήσιμο αν αυτοί οι άνθρωποι είναι ήδη «ταυτοποιημένοι». Στην περίπτωση αυτής της μελέτης, αναζητώντας περιπτώσεις όπου δύο χρήστες βρίσκονταν σε στενή εγγύτητα μεταξύ τους, θα μπορούσε να συναχθεί μια κοινωνική ή επιχειρηματική σχέση.

- Οικογενειακή ζωή: Η δημιουργία της οικογενειακής κατάστασης ή η ύπαρξη παιδιών στην οικογένεια αποκτά ενδιαφέρον. Από τα δεδομένα GPS, προκείπτουν συγκεκριμένοι προσδιοριστές .Για παράδειγμα, οι συχνές επισκέψεις σε νηπιαγωγείο και πάρκα δείχνουν ότι μικρά παιδιά εμπλέκονται με τον εν λόγω χρήστη. Η έλλειψη αναγνωρίσιμου τόπου εργασίας για τον χρήστη μπορεί να υποδηλώνει ανεργία. Για άλλους χρήστες, οι μη δομημένες και σταθερές ώρες εργασίας υποδηλώνουν απλούς ανθρώπους. Αυτά αποτελούν κάποιους προσδιοριστές οικογενειακής κατάστασης.

Μέσα από την εν λόγω έρευνα και από τις θέσεις κλειδιά αναλύονται επίσης κάποια πιο ευαίσθητα δεδομένα για τον χρήστη όπως:

- Θρησκεία: Όπως πολλές από τις πληροφορίες που προκύπτουν από τα δεδομένα θέσης, μπορεί να είναι δυνατόν να διαπιστωθεί με κάποιο βαθμό βεβαιότητας ότι ένα άτομο έχει συγκεκριμένη θρησκεία εάν υπάρχουν ορισμένοι δείκτες. Με άλλα λόγια μπορεί να είναι δυνατή η ταξινόμηση ενός ατόμου βάσει θρησκεύματος, αλλά δεν είναι δυνατόν να ταξινομηθεί ένα άτομο ως μη έχον θρησκεία. Επειδή οι περισσότερες βασικές θρησκείες χαρακτηρίζονται από συγκεκριμένες συμπεριφορές, οι οποίες διεξάγονται σε συγκεκριμένες και αναγνωρίσιμες τοποθεσίες, για παράδειγμα, μια εκκλησιαστική υπηρεσία της Κυριακής ή περιοδικές κλήσεις προς προσευχή σε ένα τζαμί, οι σχέσεις μεταξύ ενός ατόμου και μιας θρησκείας είναι εύκολο να γίνουν.

- Υγεία: Οι συχνές επισκέψεις σε γραφείο γιατρού, σε νοσοκομεία ή μιας ειδικής κλινικής υγείας είναι πιθανώς ένας δείκτης για ένα θέμα υγείας, αν και όχι απαραίτητα αυτό του ατόμου που παρακολουθείται, καθώς μπορεί να συνοδεύει ένα άλλο. Αντίστροφα, η μη επισκεψιμότητα σε οδοντίατρους ή οπτικούς, σε τακτική βάση, θα μπορούσε να αποτελέσει ένδειξη ότι δεν υπάρχει κάποιο ζήτημα όσον αφορά την υγεία. Άλλα μοτίβα κίνησης μπορεί να αποτελούν ένδειξη υποκείμενων ιατρικών προβλημάτων. Η σωματική άσκηση που λαμβάνει ένα άτομο συνδέεται άμεσα με παράγοντες κινδύνου που σχετίζονται με ασθένειες όπως οι καρδιακές παθήσεις. Η άσκηση μπορεί να είναι αρκετά εμφανής στα δεδομένα θέσης με το περπάτημα ή το τρέξιμο καθώς και με τις επισκέψεις σε γυμναστήρια.

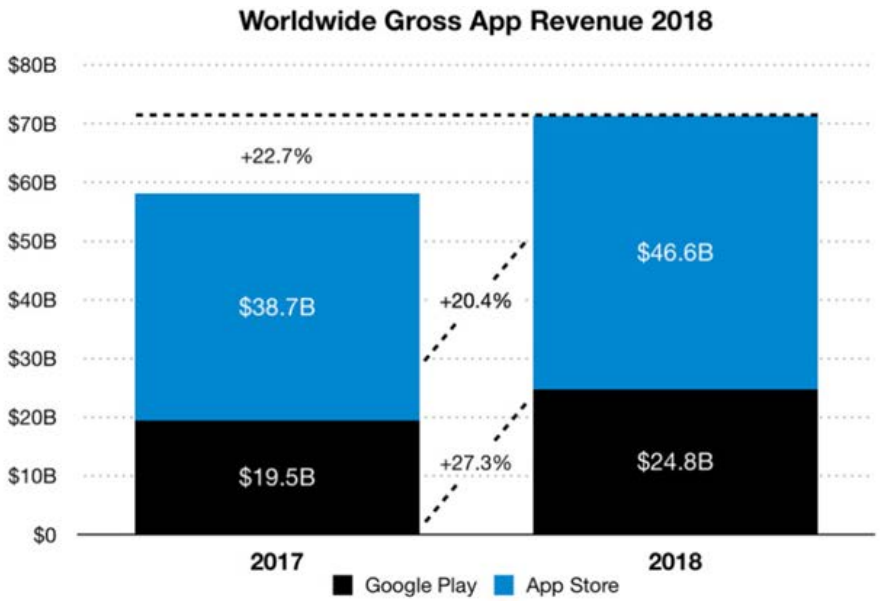
- Πράξη αδικήματος: όπως προαναφέρθηκε στο κεφάλαιο 3, τα δεδομένα που αφορούν αδικήματα, ποινικές καταδίκες ή μέτρα ασφαλείας μπορούν να θεωρηθούν ευαίσθητα. Η απόδειξη της τοποθεσίας θα μπορούσε να είναι χρήσιμη για την επιβεβαίωση ενός αδικήματος ως απόδειξη ότι βρίσκεστε σε μια τοποθεσία κατά τη διάρκεια του. Εντούτοις, σε ορισμένες περιπτώσεις, μπορεί να είναι άμεση απόδειξη ότι έχει διαπραχθεί αδίκημα. Ενώ η εντοπισμένη διακύμανση των δεδομένων GPS είναι πιθανώς υπερβολικά μεγάλη ώστε να υποδεικνύει ένα αδίκημα ταχύτητας σε μικρή απόσταση, κατά μέσο όρο σε μεγάλη απόσταση, μπορεί να είναι αρκετά ακριβές.

- Σεξουαλική ζωή: πράγματι με τη χρήση των δεδομένων θέσης μπορεί να γίνει ο προσδιορισμός των ερωτικών προτιμήσεων ενός ανθρώπου (π.χ. η παρουσία του σε συγκεκριμένο μέρος, σε συγκεκριμένο χρόνο μπορεί να αποκαλύπτει δεδομένα ερωτικής ζωής).

Είναι προφανές ότι μια τεράστια ποσότητα πληροφοριών σχετικά με το άτομο είναι κρυμμένη στα διαθέσιμα δεδομένα από την συνεχή παρακολούθηση των χρηστών. Παρόλα αυτά, είναι σαφές ότι σταθερά συμπεράσματα σχετικά με ορισμένες προσωπικές και ευαίσθητες πληροφορίες, όπως η οικογενειακή ζωή, η υγεία και η εμπιστοσύνη των δεδομένων, μπορεί να προέρχονται μόνο από τη συλλογή δεδομένων για μήνες, ακόμη και χρόνια [25]. Περαιτέρω, πρέπει να ληφθεί υπόψη ότι ακόμη και αν προκύψουν εσφαλμένα συμπεράσματα για κάποιο πρόσωπο από την επεξεργασία των ως άνω πληροφοριών – π.χ. αν γίνει εκτίμηση των θρησκευτικών του πεποιθήσεων λόγω κάποιων συνηθειών σχετικά με την τοποθεσία του, οι οποίες όμως συνήθειες είναι «τυχαίες» και γίνονται για άλλους, και όχι για θρησκευτικούς, λόγους – ενδέχεται και σε αυτήν την περίπτωση το άτομο να έχει δυσμενείς επιπτώσεις (π.χ. να υποστεί διακρίσεις).

Κεφάλαιο 5
Εφαρμογές Τρίτων Μελών: Ζητήματα Ιδιωτικότητας

Οι υπηρεσίες τρίτων (Third Parties Services), αποτελούν αναπόσπαστο κομμάτι του οικοσυστήματος κινητών συσκευών: διευκολύνουν την ανάπτυξη εφαρμογών και ενεργοποιούν λειτουργίες όπως η ανάλυση, η ενοποίηση κοινωνικών δικτύων και η δημιουργία εσόδων από εφαρμογές μέσω διαφημίσεων. Σύμφωνα πάντοτε με στατιστικές μελέτες, τα κέρδη από τις Android εφαρμογές η οποίες προέρχονται από το Google Play έχουν ανέλθει στα 24,8 δις για το 2018, οπότε και μιλάμε για ένα τεράστιο ποσοστό κερδών.



Εικόνα 5.1: Παγκόσμια ακαθάριστα έσοδα εφαρμογών για το 2017-2018 [37].

Ωστόσο, λόγω της γενικής αδιαφάνειας που εν τέλει χαρακτηρίζει τα κινητά συστήματα, οι υπηρεσίες αυτές είναι επίσης σε μεγάλο βαθμό «αόρατες» στους χρήστες. Αυτό έχει αρνητικές συνέπειες για το ιδιωτικό απόρρητο των χρηστών, καθώς οι υπηρεσίες τρίτων μπορούν ενδεχομένως να παρακολουθούν χρήστες χωρίς ή με την συγκατάθεσή τους, ακόμη και σε πολλαπλές εφαρμογές [15].

5.1 Οι Υπηρεσίες Τρίτων Μελών (Third Parties Services)

Πολλοί προγραμματιστές εφαρμογών για κινητά ενσωματώνουν στις εφαρμογές τους υπηρεσίες τρίτων μερών (Third-Parties) για διάφορους σκοπούς, όπως τη συντήρηση των εφαρμογών (π.χ. αναφορές σφαλμάτων), υπηρεσίες ανάλυσης, δοκιμές και τη διαφήμιση. Επιπλέον, οι εφαρμογές αυτές (βιβλιοθήκες τρίτων μελών – third party libraries) “κληρονομούν” το σύνολο των δικαιωμάτων χρήσης που ζητούνται από την εφαρμογή, επιτρέποντάς τους να έχουν πρόσβαση σε πληθώρα πολύτιμων δεδομένων του χρήστη, συχνά πέρα από αυτά που χρειάζονται για την παροχή της αναμενόμενης υπηρεσίας στον τελικό χρήστη, ειδικά εάν η ίδια βιβλιοθήκη χρησιμοποιείται από πολλαπλές εφαρμογές με διαφορετικά δικαιώματα.

Συγκεκριμένα οι βιβλιοθήκες τρίτων βασίζονται στα δικαιώματα χρήσης των εφαρμογών που τις χρησιμοποιούν, μερικά από τα οποία μπορεί να είναι ευαίσθητα για το απόρρητο των πληροφοριών του χρήστη. Ενώ οι πλατφόρμες για κινητά επιτρέπουν συνήθως στους χρήστες να χορηγούν ή να απενεργοποιούν δικαιώματα για κάθε εφαρμογή, αυτό παρουσιάζει αρκετές αδυναμίες. Πρώτον, οι χρήστες συνήθως παραμένουν απληροφόρητοι ότι με τη χορήγηση αδειών σε μια εφαρμογή οι πληροφορίες τους μπορούν να συλλεχθούν από υπηρεσίες τρίτων, μέσω αυτής. Δεύτερον, οι χρήστες δεν ενημερώνονται για τις εφαρμογές που μοιράζονται τις ίδιες υπηρεσίες τρίτου μέρους, με αποτέλεσμα να παρουσιάζεται διαρροή υπέρμετρης πληροφορίας μέσω της αλληλοκάλυψης που προσφέρεται κατά την χορήγηση αδειών μεταξύ των εφαρμογών [29]. Αυτή η έλλειψη διαφάνειας σημαίνει ότι το οικοσύστημα υπηρεσιών τρίτων παραμένει μυστηριώδες για τους χρήστες, τους ερευνητές και τις ρυθμιστικές αρχές σε βαθμό που δεν γνωρίζουμε ούτε καν την ταυτότητα των μεγάλων παρόχων υπηρεσιών.

Αξίζει να σημειωθεί ότι οι περισσότερες υπηρεσίες τρίτων μελών, με εξαίρεση τις υπηρεσίες διαδικτυακής διαφήμισης, λειτουργούν στο παρασκήνιο και δεν παρέχουν οπτικές ενδείξεις μέσα στις εφαρμογές, παρακολουθώντας αποτελεσματικά τους χρήστες χωρίς τη γνώση ή τη σαφή συγκατάθεσή τους παραμένοντας ουσιαστικά αόρατες. Η γενική έλλειψη διαφάνειας στα κινητά συστήματα δεν επιτρέπει στους χρήστες να εντοπίζουν τις υπηρεσίες τρίτων που χρησιμοποιούν οι εφαρμογές τους, πόσο μάλλον να γνωρίζουν σε ποιο βαθμό αυτές οι υπηρεσίες είναι σε θέση να συλλέγουν, να συσχετίζουν και να συγκεντρώνουν τα προσωπικά τους δεδομένα από εφαρμογές και πλατφόρμες. Ως αποτέλεσμα, τόσο οι τελικοί χρήστες όσο και οι προγραμματιστές δεν γνωρίζουν πώς λειτουργούν αυτές οι υπηρεσίες σε επίπεδο δικτύου και πώς χειρίζονται τα ευαίσθητα δεδομένα μόλις τα δεδομένα εγκαταλείψουν τη συσκευή. Για παράδειγμα τα δεδομένα μπορεί να μοιράζονται ή να πωλούνται σε άλλα τρίτα μέρη, συμπεριλαμβανομένων συμβεβλημένων διαφημιστικών υπηρεσιών και μεσιτών δεδομένων. Παρά τις τεράστιες ερευνητικές προσπάθειες που διεξάγουν ακαδημαϊκοί και ρυθμιστικοί φορείς για να ενισχύσουν τη διαφάνεια, υπάρχει έλλειψη γνώσης όσον αφορά την κατανόηση σε επίπεδο εταιρειών που κατέχουν αυτές τις υπηρεσίες, πως λειτουργούν, των σχέσεων τους με εταίρους τους και ποιες είναι οι πολιτικές απορρήτου κατανομής των δεδομένων [15]. Ορισμένες από αυτές τις υπηρεσίες ισχυρίζονται ρητά ότι δεν πωλούν τα δεδομένα τους σε τρίτους, αλλά οι μητρικές εταιρείες τους επιτρέπουν

την ανταλλαγή δεδομένων μεταξύ θυγατρικών στην πολιτική απορρήτου τους - π.χ. το Facebook Graph API μπορεί να μοιράζεται τα δεδομένα του με τις διαφημίσεις του Facebook. Άλλοι, δηλώνουν ρητά ότι διατηρούν το δικαίωμα να μοιράζονται συγκεντρωτικά, μερικές φορές ακόμη και μη ανώνυμα, δεδομένα με τους "συντρόφους" τους, συχνά μη γνωστούς τρίτους [15].

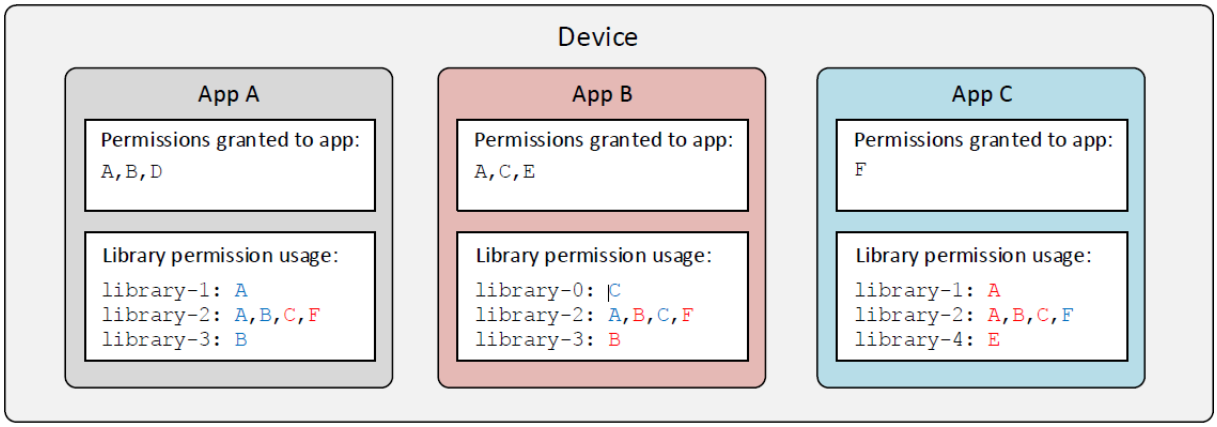
5.2 Η Σχέση Εφαρμογών και Υπηρεσιών Τρίτων Μελών

Όπως προαναφέρθηκε στο οικοσύστημα του Διαδικτύου, ένας μεγάλος αριθμός προγραμματιστών βασίζονται στις υπηρεσίες παρακολούθησης και διαφήμισης ATS (Advertising or Tracking Services), για τη δημιουργία εσόδων από τις εφαρμογές τους. Τα εργαλεία ελέγχου απορρήτου, όπως οι υπηρεσίες κατά της παρακολούθησης και οι αποκλεισμοί διαφημίσεων (Ad-Blocker), αποτέλεσαν πρόσφατα αντικείμενο πολλών συζητήσεων εξαιτίας τις ευρείας χρήσης τους και της παρέμβασής τους στην οικονομική βιωσιμότητα των εφαρμογών για κινητά και των ηλεκτρονικών υπηρεσιών [39]. Ενώ οι προγραμματιστές εφαρμογών μερικές φορές αναγνωρίζουν το γεγονός ότι ένας μεγάλος αριθμός χρηστών τους δεν επιθυμούν να παρακολουθούνται και τους προσφέρουν έναν τρόπο απενεργοποίησης στοχευμένων διαφημίσεων, με την αγορά πληρωμένων εκδόσεων των ίδιων εφαρμογών, πολλές εφαρμογές με πληρωμή εξακολουθούν να περιλαμβάνουν υπηρεσίες τρίτου μέρους, όπως υπηρεσίες ανάλυσης που συλλέγουν μοναδικά αναγνωριστικά [15].

Σε μελέτες, περιγράφεται μια καινοφανής και δυνητικά καταστροφική περίπτωση η η οποία εγείρει ζητήματα προστασίας δεδομένων λόγω μίας, κατά κάποιον τρόπο «επίθεσης κλιμάκωσης προνομίων» (privilege escalation attack) που μπορεί να εκτελεστεί από βιβλιοθήκες τρίτων. Αυτή η επίθεση, η οποία ονομάζεται «συμπαιγνία βιβλιοθηκών» (Intra-Libraries Collusion - ILC), συμβαίνει όταν μια ενιαία βιβλιοθήκη που είναι ενσωματωμένη σε περισσότερες από μία εφαρμογές σε μια συσκευή, αξιοποιεί το συνδυασμένο σύνολο δικαιωμάτων που διαθέτει για να συλλέξει δεδομένα του χρήστη σε, τελικά, υπέρμετρο βαθμό [7]. Η δυνατότητα συμπαιγνιών βιβλιοθηκών σε μία συσκευή, υπάρχει επειδή οι βιβλιοθήκες αποκτούν τα ίδια προνόμια με την εφαρμογή που τις χρησιμοποιεί/φιλοξενεί. Οι εφαρμογές Android, όπως προαναφέρθηκε, «συσκευάζονται» ως αρχεία τύπου .apk, τα οποία είναι συμπιεσμένα αρχεία που περιέχουν όλους τους πόρους που απαιτούνται από την εφαρμογή. Αυτό σημαίνει ότι

όλες οι βιβλιοθήκες που χρησιμοποιούνται από μια εφαρμογή καταρτίζονται στην ίδια δυαδική εφαρμογή για διανομή. Το μοντέλο ασφαλείας Android δεν υποστηρίζει το διαχωρισμό των δικαιωμάτων μεταξύ των εφαρμογών και των ενσωματωμένων βιβλιοθηκών τους. Ως εκ τούτου, όχι μόνο οι βιβλιοθήκες κληρονομούν τα δικαιώματα που έχουν χορηγηθεί στις εφαρμογές υποδοχής τους, αλλά και οι προγραμματιστές των ίδιων των εφαρμογών υποδοχής υποχρεώνονται μερικές φορές να δηλώσουν πρόσθετα δικαιώματα για την υποστήριξη ενσωματωμένων βιβλιοθηκών.

Ερευνητές χρησιμοποιώντας λίστες εφαρμογών από περισσότερες από 30.000 συσκευές, παρατηρήσαν ότι αρκετές δημοφιλείς βιβλιοθήκες κοινωνικής δικτύωσης, διαφήμισης και αναλύσεων είναι σε θέση να εκμεταλλευτούν την προαναφερθείσα μέθοδο συμπαιγνιών βιβλιοθηκών [7]. Περίπου το 57,6% των συσκευών που μελετήθηκαν είχαν τουλάχιστον μία βιβλιοθήκη που θα μπορούσε να επωφεληθεί από την ILC. Αυτές οι βιβλιοθήκες θα μπορούσαν να έχουν πρόσβαση σε δύο ή περισσότερα πρόσθετα δικαιώματα σε 30,8% των περιπτώσεων. Κάνοντας μια μελέτη περίπτωσης για τις βιβλιοθήκες διαφημίσεων, έδειξαν ότι οι βιβλιοθήκες διαφήμισης διαρρέουν ευαίσθητα δεδομένα από μια συσκευή έως και 2,4 φορές την ημέρα και ότι ο μέσος χρήστης έχει αποστέλλει τα προσωπικά δεδομένα σε 1,7 διαφορετικούς διακομιστές διαφημίσεων την ημέρα. Για παράδειγμα στην εικόνα 5.2 οι βιβλιοθήκες μπορούν να χρησιμοποιούν κάποια δικαιώματα, τα οποία απεικονίζονται με μπλε χρώμα, επειδή έχουν παραχωρηθεί στην εφαρμογή, ενώ τα δικαιώματα με κόκκινο χρώμα δεν είναι διαθέσιμα για τις βιβλιοθήκες εντός αυτής της εφαρμογής. Συνολικά, η βιβλιοθήκη-2 έχει πρόσβαση σε συνολικά τέσσερα δικαιώματα στη συσκευή.



Εικόνα 5.2: Ένα παράδειγμα για το πώς θα μπορούσε να συμβεί στην πράξη συμπαιγνία βιβλιοθηκών (ILC) [7].

Επιπροσθέτως πολλές βιβλιοθήκες χρησιμοποιούν δυναμική φόρτωση κώδικα, όπου ο εκτελέσιμος κώδικας ανακτάται από το Διαδίκτυο και φορτώνεται δυναμικά από τη βιβλιοθήκη, αποτρέποντας έτσι την κλιμακούμενη στατική ανάλυση από ερευνητές. Η ύπαρξη λοιπόν δυναμικών τεχνικών προγραμματισμού και παρατήρησης επιτρέπει στους προγραμματιστές της βιβλιοθήκης να εκτελούν αμφισβητούμενο κώδικα στις συσκευές μειώνοντας παράλληλα την πιθανότητα να ανακαλυφθούν. Ήδη, έχει παρατηρηθεί δυνητικά επιβλαβής κώδικας στις βιβλιοθήκες, επηρεάζοντας εκατοντάδες χιλιάδες εφαρμογές σε όλο το οικοσύστημα κινητών συσκευών [7].

Κάθε εφαρμογή δηλώνει στατικά τα ευαίσθητα δεδομένα και τις λειτουργίες που απαιτεί σε ένα δηλωτικό, το οποίο παρουσιάζεται στο χρήστη κατά την εγκατάσταση της. Ωστόσο, δεν είναι σαφές στον χρήστη σε ποιο βαθμό τα ευαίσθητα δεδομένα χρησιμοποιούνται μετά την εγκατάσταση της εφαρμογής. Μια εφαρμογή χαρτών, για παράδειγμα, θα απαιτήσει πρόσβαση στο Internet για τη λήψη ενημερωμένων πλακιδίων χαρτών, πληροφοριών για διαδρομές και εκθέσεις κυκλοφορίας. Θα χρειαστεί επίσης πρόσβαση στην τοποθεσία του τηλεφώνου για να ρυθμίσει τον προβαλλόμενο χάρτη και να δώσει κατευθύνσεις σε πραγματικό χρόνο. Η λειτουργικότητα της εφαρμογής απαιτεί την αποστολή δεδομένων θέσης στον διακομιστή χαρτών, η οποία είναι αναμενόμενη και αποδεκτή δεδομένου του σκοπού της εφαρμογής. Ωστόσο, εάν η εφαρμογή υποστηρίζεται από διαφημίσεις, μπορεί επίσης να διαρρεύσει δεδομένα τοποθεσίας στους διαφημιζόμενους για στοχευμένες διαφημίσεις, γεγονός που μπορεί να θέσει σε κίνδυνο την ιδιωτικότητα του χρήστη. Δεδομένου ότι μόνο οι πληροφορίες που παρουσιάζονται σήμερα στους χρήστες είναι μια λίστα με τα απαιτούμενα δικαιώματα, ένας χρήστης δεν θα μπορεί να πει πώς η εφαρμογή χαρτών χειρίζεται τις πληροφορίες θέσης της.

Για την αντιμετώπιση αυτού του προβλήματος, παρουσιάστηκε το AndroidLeaks [40], ένα στατικό πλαίσιο ανάλυσης για την αυτόματη εξάλειψη πιθανών διαρροών ευαίσθητων πληροφοριών σε εφαρμογές Android. Στην εν λόγω μελέτη αξιολογήθηκε η αποτελεσματικότητα του AndroidLeaks σε 24.350 εφαρμογές Android. Το AndroidLeaks διαπίστωσε 57.299 πιθανές διαρροές απορρήτου σε 7.414 εφαρμογές Android, από τις οποίες έχουν ελεγχθεί με μη αυτόματο τρόπο ότι 2.342 αιτήσεις διαχέουν ιδιωτικά δεδομένα, όπως πληροφορίες τηλεφώνου, τοποθεσία GPS, δεδομένα WiFi και ηχογράφηση με το μικρόφωνο. Το AndroidLeaks εξέτασε αυτές τις εφαρμογές σε 30

ώρες, γεγονός που υποδηλώνει ότι είναι σε θέση να κλιμακωθεί σε όλο και μεγαλύτερο αριθμό διαθέσιμων εφαρμογών.

Συμπληρωματικά, σε άλλη μελέτη περιγράφεται το TaintDroid [41], μια επέκταση στην πλατφόρμα Android κινητού τηλεφώνου που παρακολουθεί τη ροή δεδομένων ευαίσθητων πληροφοριών μέσω εφαρμογών, που σκοπό έχουν την παρακολούθηση και την υποκλοπή προσωπικής πληροφορίας. Το TaintDroid υποθέτει ότι οι εν λόγω εφαρμογές που έχουν εξεταστεί δεν είναι αξιόπιστες και παρακολουθεί σε πραγματικό χρόνο πώς αυτές οι εφαρμογές έχουν πρόσβαση και μπορούν να χειραγωγήσουν τα προσωπικά δεδομένα των χρηστών. Η ανάλυση της συμπεριφοράς των εφαρμογών απαιτεί επαρκείς πληροφορίες σχετικά με ποια δεδομένα φεύγουν από μία συσκευή και που αποστέλλονται. Έτσι, το TaintDroid θεωρεί αυτόματα τα δεδομένα ως ευαίσθητα, εφαρμόζοντας ετικέτες σε αυτά που διαδίδονται μέσω προγραμμάτων, αρχείων και μηνυμάτων. Όταν τα δεδομένα μεταφέρονται μέσω του δικτύου εγκαταλείποντας το σύστημα, το TaintDroid καταγράφει τις ετικέτες των δεδομένων, την εφαρμογή που είναι υπεύθυνη για τη μετάδοση των δεδομένων και τον προορισμό τους. Τέτοιου είδους ανατροφοδότηση σε πραγματικό χρόνο δίνει στους χρήστες και τις υπηρεσίες ασφαλείας μεγαλύτερη εικόνα τι κάνουν οι κινητές εφαρμογές εντοπίζοντας τις εν λόγω κακές εφαρμογές.

Στην μελέτη με το TaintDroid χρησιμοποιήθηκαν 30 τυχαία επιλεγμένες, δημοφιλείς εφαρμογές Android που χρησιμοποιούν τοποθεσία, φωτογραφική μηχανή ή δεδομένα μικροφώνου. Μέσω του TaintDroid επισημάνθηκαν 105 περιπτώσεις στις οποίες μεταδόθηκαν προσωπικά δεδομένα, στις οποίες οι 37 ήταν σαφώς νόμιμες. Το TaintDroid αποκάλυψε επίσης ότι 15 από τις 30 εφαρμογές ανέφεραν τοποθεσίες χρηστών σε διακομιστές διαφήμισης. Επτά εφαρμογές συγκέντρωσαν το αναγνωριστικό της συσκευής (HardwareID) και, σε ορισμένες περιπτώσεις, τον αριθμό τηλεφώνου και το αριθμό κάρτας SIM (IMSI). Συνολικά, τα δύο τρίτα των εφαρμογών στη μελέτη χρησιμοποιούσαν ευαίσθητα δεδομένα.

Η διαβίβαση προσωπικών δεδομένων από μόνη της δεν συνεπάγεται κατ' ανάγκη διαρροή απορρήτου. Ένας καλύτερος δείκτης μπορεί να θεωρηθεί το γεγονός εαν η μετάδοση γίνεται από πρόθεση του χρήστη ή όχι. Όταν η μετάδοση δεν προορίζεται από το χρήστη, είναι πιθανότερο να υπάρξει διαρροή απορρήτου. Το πρόβλημα είναι πώς μπορεί να προσδιοριστεί εάν η μετάδοση προορίζεται από τον χρήστη. Ως πρώτη λύση στην μελέτη , παρουσιάζεται το πλαίσιο ανάλυσης AppIntent [42]. Για κάθε μετάδοση

δεδομένων, το AppIntent μπορεί να παρέχει αποτελεσματικά μια ακολουθία χειρισμών GUI που αντιστοιχούν στην ακολουθία συμβάντων που οδηγούν στη μετάδοση δεδομένων, βοηθώντας έτσι έναν αναλυτή να προσδιορίσει εάν η μετάδοση δεδομένων ξεκινά με τη συγκατάθεση του χρήστη ή όχι. Παρουσιάστηκε η αξιολόγηση του AppIntent με ένα σύνολο από 750 κακόβουλων εφαρμογών, καθώς και 1.000 κορυφαίες δωρεάν εφαρμογές από το Google Play. Στα πειραματικά αποτελέσματα, 252 εφαρμογές είχαν διαρροή ευαίσθητων δεδομένων, μεταξύ των οποίων 224 εφαρμογές περιείχαν ανεπιθύμητη μετάδοση από τον χρήστη, ενώ άλλες 28 εφαρμογές περιείχαν μόνο μετάδοση δεδομένων που προορίζεται από το χρήστη. Επιπλέον, ότι το AppIntent μπορεί αποτελεσματικά να διαχωρίσει τις εφαρμογές που διαρρέουν πραγματικά την ιδιωτικότητα του χρήστη από αυτές που δεν το κάνουν. Σημαντικό είναι το γεγονός ότι η μετάδοση δεδομένων των αναγνωριστικών συσκευών και των αριθμών τηλεφώνου είναι πολύ συνηθισμένη, αλλά συνήθως δεν παρατηρείται από τους περισσότερους χρήστες κινητών συσκευών. Μεταξύ της ανιχνευθείς μη ακούσιας μετάδοσης δεδομένων στα δύο επιλεγμένα σύνολα δεδομένων, οι περισσότερες περιπτώσεις είναι η μετάδοση αναγνωριστικών συσκευών ή αριθμών τηλεφώνου. Επιπλέον, διαπίστωσαν ότι όχι μόνο τα αναγνωριστικά συσκευής και οι αριθμοί τηλεφώνου είναι γραμμένα σε αρχεία καταγραφής (log files) Android, αλλά και οι τοποθεσίες και οι επαφές των χρηστών αποθηκεύονται προσωρινά σε αρκετές περιπτώσεις. Αυτά τα καταγεγραμμένα δεδομένα μπορούν να χρησιμοποιηθούν από κακόβουλες εφαρμογές που κλέβουν το αρχείο καταγραφής Android.

Σε μία άλλη μελέτη παρουσιάζεται η πρώτη διαχρονική μελέτη σχετικά με τη χρήση δημοφιλών εφαρμογών Android και των ενημερωμένων εκδόσεων τους και τη διαρροή προσωπικών δεδομένων των χρηστών με την πάροδο του χρόνου [43]. Διαπίστωσαν ότι οι πληροφορίες που μοιράζονται με άλλα μέρη αλλάζουν με την πάροδο του χρόνου, με τις ακόλουθες τάσεις: (1) η ιδιωτικότητα τείνει να επιδεινώνεται σε όλες τις εκδόσεις. (2) οι τύποι των συγκεντρωμένων PII (Personally Identifiable Information) αλλάζουν σε όλες τις εκδόσεις, περιορίζοντας τη γενικευσιμότητα των μελετών μονής έκδοσης, (3) Η υιοθέτηση του HTTPS είναι σχετικά αργή σε εφαρμογές για κινητά, (4) τα τρίτα μέρη όχι μόνο παρακολουθούν τους χρήστες διαδεδομένα, αλλά συγκεντρώνουν επίσης επαρκείς πληροφορίες για ένα χρήστη.

Κεφάλαιο 6
Μεθοδολογία

Η παρούσα διατριβή, όπως αναφέραμε στην εισαγωγή, μελετά δημοφιλείς εφαρμογές παρακολούθησης τοποθεσίας ως προς τα δεδομένα που συλλέγουν ή/και αποστέλλουν σε τρίτα μέλη, με απώτερο στόχο να διερευνηθεί αφενός αν γίνεται επεξεργασία δεδομένων ερήμην του χρήστη και αφετέρου αν τρίτα μέλη (π.χ. διαφημιστικά δίκτυα) συλλέγουν υπέρμετρη πληροφορία που δύναται να οδηγήσει σε εξαγωγή συμπερασμάτων για τη προσωπική ζωή του χρήστη. Επομένως στο παρόν κεφάλαιο θα παρουσιαστούν οι τρόποι με τους οποίους μπορεί να αναλυθεί μία εφαρμογή και τα εργαλεία τα οποία συμβάλουν στην δημιουργία του περιβάλλοντος δοκιμών.

6.1 Δημιουργία Περιβάλλοντος Δοκιμών

6.1.1 Τρόποι Ανάλυσης Εφαρμογών

Η μία εκ των δύο μεθόδων ανάλυσης εφαρμογών είναι η στατική ανάλυση. Η στατική ανάλυση είναι μια τεχνική για την ανίχνευση κακόβουλης συμπεριφοράς με την ανάλυση των τμημάτων του κώδικα. Αυτή η τεχνική εκτελείται χωρίς να εκτελείται η εφαρμογή σε έναν εξομοιωτή ή συσκευή Android. Ωστόσο, αυτή η τεχνική έχει ένα σημαντικό μειονέκτημα, της παραμόρφωσης του κώδικα και της δυναμικής φόρτωσής του. Τα πλεονεκτήματα της στατικής ανάλυσης είναι ότι το κόστος του υπολογισμού είναι χαμηλό, λιγότερο χρονοβόρο και απαιτεί χαμηλότερη κατανάλωση πόρων. Υπάρχουν δύο κύριες τρόποι χρήσης για την ανίχνευση στατικής ανάλυσης, η ανίχνευση κακής χρήσης (Misuse Detection) και ανωμαλίας (Anomaly Detection) στον κώδικα ενός προγράμματος. Η τεχνική κακόχρηστίας είναι επίσης γνωστή ως τεχνική ανίχνευσης με βάση την υπογραφή. Μια εφαρμογή ανιχνεύεται ως κακόβουλο πρόγραμμα αν η υπογραφή ενός προγράμματος ταιριάζει με μια ακολουθία οδηγιών ή πολιτικών. Η τεχνική εντοπισμού ανωμαλιών βασίζεται σε αλγόριθμους μηχανικής μάθησης για την ανίχνευση κακόβουλων συμπεριφορών. Χαρακτηριστικά που προέρχονται από γνωστά κακόβουλα προγράμματα χρησιμοποιούνται για την εκπαίδευση του μοντέλου και την πρόβλεψη ενός άγνωστου κακόβουλου λογισμικού.

Στόχος της έρευνας είναι η αποτίμηση της συμπεριφοράς των εφαρμογών οι οποίες χρησιμοποιούν συστήματα εντοπισμού θέσεως. Για να επιτευχθεί αυτό και να παραχθούν τα οποιαδήποτε αποτελέσματα δεν επαρκεί ο στατικός έλεγχος των εφαρμογών μας αλλά ο έλεγχος κατά την χρήση τους. Επομένως απαιτείται η χρήση της δυναμικής ανάλυσης. Η δυναμική ανάλυση είναι μια τεχνική ανίχνευσης που αποσκοπεί στην αξιολόγηση της συμπεριφοράς λογισμικού εκτελώντας την εφαρμογή σε ένα πραγματικό περιβάλλον. Ουσιαστικά η δυναμική ανάλυση των εφαρμογών Android αφορά στην ανάλυση εφαρμογών σε πραγματικό χρόνο, με σκοπό τον εντοπισμό τρωτών σημείων επιπέδου εφαρμογής και σε συνδυασμό με το χειρισμό της εφαρμογής κατά την εκτέλεσή της. Επιπλέον με αυτή τη μέθοδο ανάλυσης παρακολουθείται η κλήση του συστήματος και η πρόσβαση σε ευαίσθητες πληροφορίες κατά το χρόνο εκτέλεσης της εφαρμογής. Το κύριο πλεονέκτημα αυτής της τεχνικής είναι ότι ανιχνεύει τη δυναμική φόρτωση κώδικα και καταγράφει τη συμπεριφορά της εφαρμογής κατά τη διάρκεια του χρόνου εκτέλεσης. Αυτή η τεχνική αποτυγχάνει να προσδιορίσει την ποσότητα του κώδικα που εκτελείται κατά την εκτέλεση της εφαρμογής. Υπάρχει πιθανότητα οι εφαρμογές να μην μπορέσουν να εκτελέσουν τον κακόβουλο κώδικα κατά την καταγραφή των λειτουργιών. Επιπλέον, αυτή η τεχνική είναι δύσκολο να εφαρμοστεί σε σύγκριση με τη στατική ανάλυση, λόγω των γενικών εξόδων εκτέλεσης της εφαρμογής.

6.1.2 Εργαλεία Ανάλυσης των Εφαρμογών

Οι εφαρμογές κινητής τηλεφωνίας όπως έχουμε προαναφέρει, έχουν γίνει όλο και πιο βασικές στην καθημερινή μας ζωή, προσφέροντας ποικίλες υπηρεσίες και υπηρεσίες κοινής ωφέλειας, που τις πλείστες φορές προσφέρονται χωρίς κόστος. Παρά το γεγονός ότι αναθέτουμε στις εφαρμογές οικειοθελώς μια πληθώρα πληροφοριών που τους επιτρέπουν να διεκπεραιώνουν αυτές τις υπηρεσίες, οι οποίες επίσης εξαρτώνται από τις αμέτρητες καθημερινές μας αλληλεπιδράσεις, εμείς γνωρίζουμε ελάχιστα για το τι μοιράζονται μαζί με τρίτους και τι κάνουν με τα δεδομένα μας. Πολλοί προγραμματιστές εφαρμογών για κινητά ενσωματώνουν στις εφαρμογές τους υπηρεσίες τρίτων μερών. Οι υπηρεσίες τρίτων αποτελούν αναπόσπαστο κομμάτι του κινητού οικοσυστήματος καθότι διευκολύνουν την ανάπτυξη εφαρμογών και ενεργοποιούν λειτουργίες όπως η ανάλυση, η ενοποίηση κοινωνικών δικτύων και η δημιουργία εσόδων από εφαρμογές μέσω διαφημίσεων. Ωστόσο, λόγω της γενικής αδιαφάνειας που δυστυχώς διέπει σε μεγάλο βαθμό τα κινητά συστήματα, οι υπηρεσίες αυτές είναι επίσης σε μεγάλο βαθμό αόρατες στους χρήστες. Αυτό έχει αρνητικές συνέπειες για την ιδιωτικότητα των χρηστών, καθώς οι υπηρεσίες τρίτων μπορούν ενδεχομένως να παρακολουθούν χρήστες χωρίς τη ρητή συγκατάθεσή τους, ακόμη και σε πολλαπλές εφαρμογές. Οι υπηρεσίες τρίτων μελών, όπως αναφέρθηκε στο Κεφάλαιο 5, «κληρονομούν» το σύνολο των δικαιωμάτων χρήσης που ζητούνται από την εφαρμογή κατά την εγκατάστασή της, επιτρέποντάς τους να έχουν πρόσβαση σε πληθώρα πολύτιμων δεδομένων του χρήστη, συχνά πέρα από αυτά που χρειάζονται για την παροχή της αναμενόμενης υπηρεσίας στον χρήστη, ειδικά εάν η ίδια βιβλιοθήκη χρησιμοποιείται από πολλαπλές εφαρμογές με διαφορετικά δικαιώματα. Για παράδειγμα μία εφαρμογή η οποία μπορεί να ζητά από τον χρήστη δικαίωμα χρήσης της τοποθεσίας του αποστέλλοντάς την σε ένα Α τρίτο μέρος και μία άλλη εφαρμογή να ζητά από τον χρήστη δικαίωμα χρήσης των επαφών του και να τις μοιράζεται επίσης με το Α μέλος.

Αυτό έχει άμεσες συνέπειες για την ιδιωτική ζωή των χρηστών. Ωστόσο, οι περισσότερες υπηρεσίες τρίτου μέρους, με εξαίρεση τις υπηρεσίες διαδικτυακής διαφήμισης, λειτουργούν στο παρασκήνιο και δεν παρέχουν οπτικές ενδείξεις μέσα στις εφαρμογές, παρακολουθώντας αποτελεσματικά τους χρήστες χωρίς τη γνώση ή τη συγκατάθεσή τους. Η γενική έλλειψη διαφάνειας στα κινητά συστήματα δεν επιτρέπει στους χρήστες να εντοπίζουν τις υπηρεσίες τρίτων που χρησιμοποιούν οι εφαρμογές τους, πόσο μάλλον να γνωρίζουν σε ποιο βαθμό αυτές οι υπηρεσίες είναι σε θέση να συλλέγουν, να συσχετίζουν και να συγκεντρώνουν τα προσωπικά τους δεδομένα και την ηλεκτρονική τους δραστηριότητα σε εφαρμογές και πλατφόρμες. Ως αποτέλεσμα, τόσο οι τελικοί χρήστες όσο και οι προγραμματιστές δεν γνωρίζουν πώς λειτουργούν

αυτές οι υπηρεσίες σε επίπεδο δικτύου, εάν και πώς χειρίζονται τα προσωπικά (ίσως και ευαίσθητα)δεδομένα και μόλις τα δεδομένα εγκαταλείψουν τη συσκευή, είτε τα μοιράζονται (είτε τα πωλούν) με άλλα τρίτα συμπεριλαμβανομένων συμβεβλημένων διαφημιστικών υπηρεσιών, ακόμη και μεσίτες δεδομένων. Παρά τις τεράστιες ερευνητικές προσπάθειες που διεξάγουν ακαδημαϊκοί και ρυθμιστικοί φορείς για να φωτίσουν αυτό το «οικοσύστημα», υπάρχει έλλειψη γνώσης όσον αφορά την κατανόηση όσο αφορά την κλίμακα των εταιρειών που κατέχουν αυτές τις υπηρεσίες, των εταιρικών σχέσεων τους και ποιες είναι οι πολιτικές απορρήτου και κατανομής δεδομένων που χρησιμοποιούν.

Έτσι λοιπόν βασικός άξονας της έρευνάς μας είναι η εύρεση, η μελέτη και η συσχέτιση των τρίτων μελών και των πληροφορίων που αυτές μοιράζονται μέσα από της εκχωρημένες άδειες που οι ίδιες οι εφαρμογές που ερευνούμε, εξασφάλισαν από τον χρήστη κατά την εγκατάστασή τους. Για το σκοπό αυτό έγινε η χρήση των παρακάτω εργαλείων.

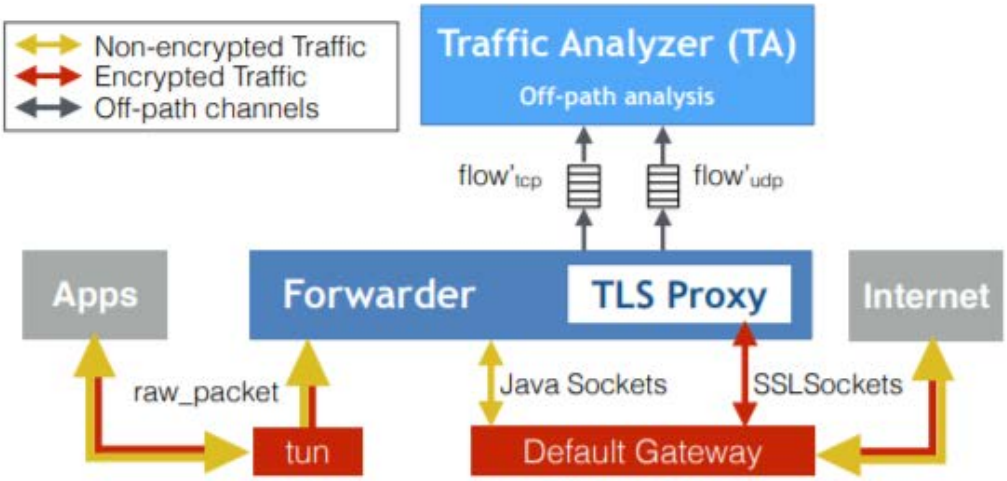
1. Lumen Privacy Monitor

Το Lumen Privacy Monitor είναι μια εφαρμογή Android που στοχεύει στην προώθηση της διαφάνειας και της ευαισθητοποίησης των χρηστών, ενημερώνοντας τους σχετικά με τον τρόπο χειρισμού των ευαίσθητων δεδομένων τους, όπως τα μοναδικά αναγνωριστικά στοιχεία (Unique Identifiers-UID) και τα προσωπικά αναγνωρίσιμα στοιχεία (Personally Identifiable Information -PII). Το πρόγραμμα αυτό δημιουργήθηκε κάτω από την «ομπρέλα» του προγράμματος ICSI Haystack. Το πρόγραμμα ICSI Haystack δημιουργήθηκε από ερευνητές του Πανεπιστημίου της Καλιφόρνιας, του Διεθνούς Ινστιτούτου Πληροφορικής (ICSI) στο Berkeley των ΗΠΑ και του IMDEA Networks το οποίο εδρεύει στην Ισπανία. Το έργο Haystack χρηματοδοτείται από το Εθνικό Ίδρυμα Επιστημών (National Science Foundation -NSF) και το Data Transparency Labs (DTL). Ο στόχος του έργου αυτού είναι να κατανοήσουμε καλύτερα το οικοσύστημα εφαρμογών για κινητά και τις επιπτώσεις του στην ασφάλεια και το ιδιωτικό απόρρητο των χρηστών, βοηθώντας παράλληλα τους μεμονωμένους χρήστες να καταλάβουν ποιοι οργανισμοί και εφαρμογές συλλέγουν προσωπικές πληροφορίες από τις συσκευές τους. Εγκαθιστώντας και εκτελώντας το Lumen, συλλέγονται πληροφορίες σχετικά με τη συμπεριφορά των εφαρμογών, τον τύπο πληροφοριών που διαρρέουν οι εφαρμογές και τον οργανισμό που συλλέγει αυτές τις πληροφορίες.

Έτσι λοιπόν για να ξεπεράσουμε τους περιορισμούς των υφιστάμενων μεθόδων ανάλυσης εφαρμογών για κινητά, εκμεταλλευόμαστε το Lumen Privacy Monitor, μια εφαρμογή για κινητά που παρέχει στους χρήστες και στους ερευνητές τη δυνατότητα να κατανοήσουν την

κυκλοφορία δικτύου που παράγεται από όλες τις εφαρμογές, ενώ χρήστης και εφαρμογές λειτουργούν εξ ολοκλήρου στο χώρο του χρήστη και χωρίς να απαιτείται πρόσβαση σε root. Είναι διαθέσιμο δωρεάν στο Google Play και μας παρέχει ανώνυμα, αλλά πλούσια δεδομένα της επισκεψιμότητας των εφαρμογών από τους χρήστες του. Στην πραγματικότητα παρεμβάλλεται ως ενδιάμεσο λογισμικό μεταξύ των εφαρμογών και της διασύνδεσης δικτύου. Το Lumen εκμεταλλεύεται την άδεια VPN του Android για τη δρομολόγηση μεταδιδόμενων πακέτων μέσω μιας διαδικασίας που εκτελείται στο χώρο του χρήστη. Τρέχοντας τοπικά στο τηλέφωνο του χρήστη, το μπορεί να παρακολουθεί άμεσα το κρίσιμο περιβάλλον των εφαρμογών, όπως για παράδειγμα το προσδιορισμό της ταυτότητας της συγκεκριμένης εφαρμογής που δημιουργεί την κυκλοφορία, την κατάσταση συσκευής (π.χ. τη γεωγραφική θέση, οθόνη και την κατάσταση του ραδιοφώνου), πληροφορίες σχετικά με τον χρήστη (π.χ. λογαριασμοί, μηνύματα, πρόσφατες κλήσεις και λίστες επαφών) και την κίνηση δικτύου που σχετίζεται άμεσα με τις δραστηριότητες των χρηστών. Επιπλέον το Haystack-Lumen προαιρετικά παρακολουθεί την κρυπτογραφημένη κίνηση μέσω ενός τοπικού πληρεξούσιου TLS (TLS proxy) που εξ αρχής εγκαθίσταται στο κινητό τηλέφωνο. Αυτό επιτρέπει την επιτόπια επιθεώρηση πακέτων για την καλύτερη κατανόηση των συμπεριφορών εφαρμογής, όπως για παράδειγμα η μετάδοση των δεδομένων προσωπικού χαρακτήρα. Ο προκύπτων συνδυασμός κίνησης δικτύου, δραστηριότητας εφαρμογής και λεπτομερών μεταδεδομένων επιτρέπει στο Lumen να παρουσιάσει στοιχεία για να χαρακτηρίσει την επισκεψιμότητα και την απόδοση του κινητού τηλεφώνου, να αξιολογήσει την ασφάλεια των εφαρμογών και να εντοπίσει διαρροές απόρρητου περιεχομένου. Απόρρητο περιεχόμενο λογίζεται το περιεχόμενο που αφορά προσωπικά και ευαίσθητα δεδομένα του χρήστη τα οποία μεταδίδονται σε τρίτα και πιθανόν σε περαιτέρω μέλη, για την επεξεργασία τους προς δημιουργία ενός προφίλ χρήστη με απώτερο σκοπό την στοχευμένη διαφήμιση [37].

Στην Εικόνα 6.1 παρουσιάζεται η αρχιτεκτονική του Haystack, επισημαίνοντας τα διαφορετικά στοιχεία του συστήματος και τη διαδικασία προώθησης δεδομένων για ένα εξερχόμενο πακέτο που δημιουργήθηκε από μια τοπική εφαρμογή. Οι συμπαγείς γραμμές αντιπροσωπεύουν την πραγματική διαδρομή προώθησης για κυκλοφορία που παράγεται από εφαρμογές κινητών, ακόμη και αν έχουν κρυπτογραφηθεί, ενώ η οι διακεκομμένες γραμμές αντιπροσωπεύουν την off-line διαδρομή που χρησιμοποιείται για την προστασία της ιδιωτικής ζωής και ανάλυση απόδοσης.



Εικόνα 6.1: Η Αρχιτεκτονική Haystack [37].

Ενώ είναι προφανές ότι ένα μεγάλο μέρος των εφαρμογών για κινητά έχουν υιοθετήσει το TLS ως το προεπιλεγμένο πρωτόκολλο ασφαλείας των δεδομένων επικοινωνίας, το Lumen χρησιμοποιεί έναν διακομιστή μεσολάβησης MITM (man-in-the-middle) για την κυκλοφορία TLS με τη συγκατάθεση του χρήστη. Κατά την εγκατάσταση, εξηγεί το σκοπό της εκτέλεσης της παρακολούθησης TLS και ζητά από τον χρήστη την άδεια να εγκαταστήσει ένα αυτό-υπογεγραμμένο πιστοποιητικό CA στο χώρο των έμπιστων πιστοποιητικών. .

Κατά την εγκατάσταση του προγράμματος ζητείται από τον χρήστη η συγκατάθεση για αρκετές άδειες (permissions) όπως αυτές παρουσιάζονται πιο κάτω [38]:

- Ανάκτηση εφαρμογών που εκτελούνται (Retrieve running apps): Αυτό το δικαίωμα επιτρέπει στο Lumen να αναγνωρίζει τις εφαρμογές που είναι υπεύθυνες για μια συγκεκριμένη ροή, να αποκτά τα σχετικά μεταδεδομένα (π.χ. Όνομα εφαρμογής, Όνομα πακέτου και εικονίδιο εφαρμογής) και τα δικαιώματά τους.

- Εύρεση λογαριασμών στη συσκευή (Find accounts on the device): Αυτό το δικαίωμα επιτρέπει στο Lumen να αναγνωρίζει εφαρμογές που διαρρέουν κάποιο από τους διαμορφωμένους λογαριασμούς σας στη συσκευή σας.

- Διαβάζει τις επαφές (Read contacts): Αυτό το δικαίωμα επιτρέπει στο Lumen να δει αν κάποια από τις εφαρμογές αποστέλλει τη λίστα επαφών του χρήστη σε έναν απομακρυσμένο διακομιστή. Αυτή η άδεια μπορεί να προκαλέσει ψευδή θετικά αποτελέσματα (false positive alarms) στην αναγνώριση των ιδιωτικών διαρροών.

- Την κατά προσέγγιση και ακριβή τοποθεσία (βάσει δικτύου και GPS): Αυτό το δικαίωμα επιτρέπει στο Lumen να γνωρίζει την τοποθεσία του χρήστη για να διαπιστώσει εάν κάποια από τις εφαρμογές την μεταδίδει σε ένα διακομιστή σε απευθείας σύνδεση (προφανώς, η άδεια αυτή είναι απολύτως απαραίτητη για τους σκοπούς της παρούσας έρευνας).

- Διαβάζει τα μηνύματά (SMS ή MMS): Αυτό το δικαίωμα επιτρέπει στο Lumen να δει αν κάποια από τις εφαρμογές του χρήστη διαρρέει τα μηνύματά του.

- Διαβάζει την κατάσταση και την ταυτότητα του τηλεφώνου (Read phone status and Identity): Αυτό το δικαίωμα επιτρέπει στο Lumen να αποκτά μοναδικούς αριθμούς UIDs όπως το IMEI, ένα από τα μοναδικά αναγνωριστικά για κινητά, που συνήθως ζητούνται από εφαρμογές για λόγους παρακολούθησης. Αυτή η άδεια επιτρέπει επίσης στο Lumen να γνωρίζει την κατάσταση της συνδεσιμότητας του χρήση για να ανακάμψει μετά από περιόδους αποσύνδεσης ή αποτυχιών.

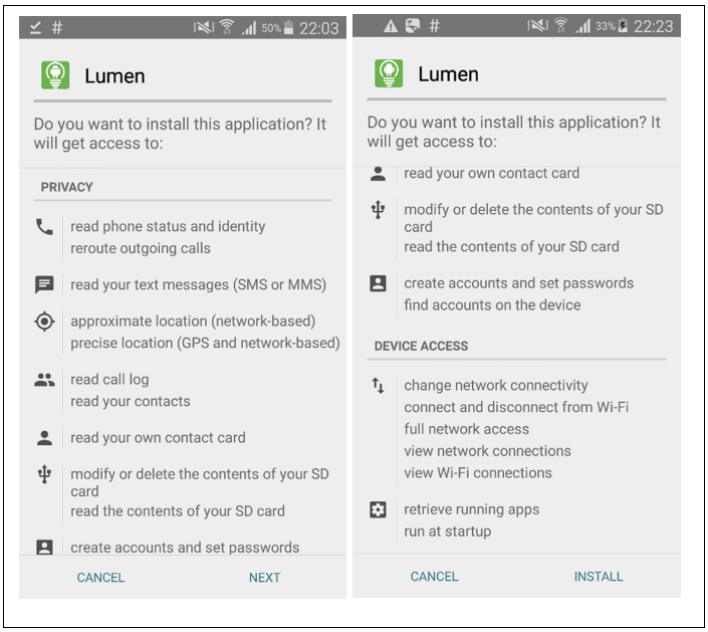
- Διαβάζει / Τροποποιεί ή διαγράφει τα περιεχόμενα του χώρου αποθήκευσης της κάρτας μνήμης (Read/Modify or delete the contents of your SD storage): Αυτή η άδεια επιτρέπει στο Lumen να αποθηκεύει πληροφορίες στην sdcard. Δεν διαβάζει καμία πληροφορία από αυτήν.

- Προβολή συνδέσεων Wi-Fi και σύνδεση και αποσύνδεση από Wi-Fi: Αυτό το δικαίωμα επιτρέπει στο Lumen να εντοπίσει αν οι εφαρμογές διαρρέουν πληροφορίες σχετικές με το WiFi, όπως το SSID (Service Set IDentifier) δικτύου. Αυτή η άδεια επιτρέπει επίσης να γνωρίζει την κατάσταση της συνδεσιμότητας για να ανακάμψει μετά από περιόδους αποσύνδεσης ή αποτυχιών. Επιπλέον, αυτή η άδεια επιτρέπει να αναγνωρίσει πιο εξελιγμένες διαρροές. Για παράδειγμα, το Lumen σαρώνει για γειτονικά AP (Access Points, SSID και διευθύνσεις MAC) για να προσδιορίσει εάν άλλες εφαρμογές διαχέουν την κατά προσέγγιση τοποθεσία μας με πιο διακριτικό τρόπο.

- Πλήρης πρόσβαση στο δίκτυο (Full network access): Όπως οποιαδήποτε εφαρμογή δικτύου, το Lumen χρειάζεται πρόσβαση στο Internet.

- Προβολή συνδέσεων δικτύου και αλλαγή σύνδεσης στο δίκτυο (View network connections and change network connectivity): Το Lumen απαιτεί επίσης από το

BIND_VPN_PERMISSION να αποκόπτει, να παρακολουθεί και να αναλύει τον την κυκλοφορία μας τοπικά.



Εικόνα 6.2: Άδειες που απαιτούνται για τη εγκατάσταση του Lumen Privacy Monitor.

2. Xposed Framework

Το Xposed είναι ένα από τα πιο ισχυρά και περιζήτητα εργαλεία που κάθε προηγμένος χρήστης του Android θέλει να εκμεταλλευτεί. Αυτό το εργαλείο έχει μερικές πολύ σημαντικές δυνατότητες που επιτρέπουν σε έναν χρήστη να προσαρμόσει το κινητό του τηλέφωνο σύμφωνα με τις απαιτήσεις του. Ένα κανονικό τηλέφωνο Android δεν έχει ορισμένες λειτουργίες που επιθυμεί να έχει ένας έμπειρος χρήστης Android στη συσκευή του. Επομένως για να προσαρμοστεί μία συσκευή στις απαιτήσεις κάθε χρήστη, πρέπει να εγκατασταθεί το Xposed Framework.

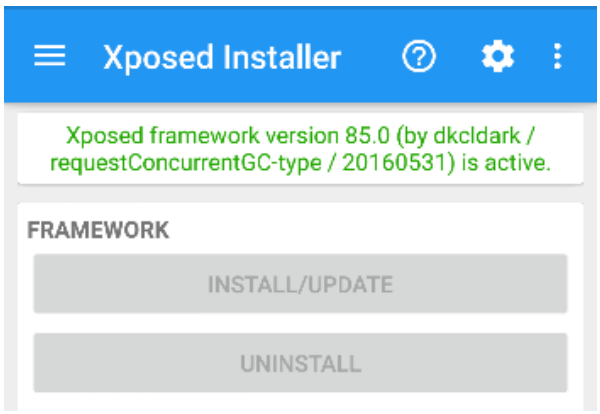
Η βασική προϋπόθεση για τη χρήση του πλαισίου είναι το τηλέφωνό πρέπει να είναι Root. Όπως έχει προαναφερθεί το Android βασίζεται στο Linux και ο χρήστης root (superuser) είναι κάτι παρόμοιο με τον διαχειριστή στα Windows. Με αυτήν την ιδιότητα έχουμε πρόσβαση σε ολόκληρο το λειτουργικό σύστημα και μπορούμε να κάνουμε τα πάντα. Στην Android συσκευή μας από προεπιλογή δεν έχουμε τέτοιου είδους πρόσβαση. Το αποτέλεσμα, εκτός των άλλων, είναι ότι και πολλές χρήσιμες εφαρμογές μέσα στο Play Store δεν λειτουργούν χωρίς root στο Android. Ο λογαριασμός του υπερχρήστη προϋπάρχει μέσα στην συσκευή μας. Ωστόσο, το λειτουργικό της Google, αλλά και αρκετοί κατασκευαστές, δεν μας επιτρέπουν να

αποκτήσουμε τέτοια δικαιώματα. Με το root στο Android παρακάμπτουμε αυτούς τους περιορισμούς και αποκτούμε την πλήρη πρόσβαση, αυξάνοντας έτσι και τις δυνατότητες της συσκευής. Οι λόγοι για τους οποίους κάνουμε Root τη συσκευή συνοψίζονται ως εξής:

- Έχουμε απόλυτο έλεγχο σε όλες τις λειτουργίες της συσκευής.
- Έχουμε μεγαλύτερη διάρκεια μπαταρίας.
- Μας δίνει δυνατότητες για προσαρμοσμένη ROM, που βελτιώνει την εμφάνιση και την αίσθηση του λειτουργικού συστήματος.
- Προσδίδει αύξηση στην ταχύτητα της συσκευής.
- Περισσότερες χρήσιμες εφαρμογές.
- Δυνατότητα διαγραφής των προ εγκατεστημένων εφαρμογών.
- Δυνατότητες Over/underclocking.
- Μπορούμε να πάρουμε πλήρες Backup με όλες τις ρυθμίσεις της συσκευής.

Συνεχίζοντας πρέπει να σημειωθεί ότι το Xposed Framework δεν κάνει πολλά από μόνο του. Επιτρέπει να κάνουμε αλλαγές στο σύστημα και σε εφαρμογές, χωρίς όμως να χρειάζεται να κάνουμε decompile-recompile τα .apk. Επίσης επιτρέπει να εγκαταστήσουμε άλλες εφαρμογές/modules με λειτουργικότητα επιπέδου συστήματος. Αυτός είναι ο λόγος για τον οποίο το Xposed framework θεωρείται ένα από τα καλύτερα εργαλεία ανάλυσης για τη συσκευή Android. Οι τροποποιήσεις που μπορούν να γίνουν στο τηλέφωνο είναι διαθέσιμες μέσω ορισμένων modules, οι οποίες μπορούν να θεωρηθούν ως εφαρμογές που μπορούν να εγκατασταθούν μέσω του Xposed Framework. Κάθε μία από αυτές τις μονάδες έχει ορισμένους συγκεκριμένους ρόλους. Για παράδειγμα, αν θέλουμε να αυξήσουμε τον χρόνο αναμονής της μπαταρίας του τηλεφώνου σας, θα χρειαστεί να εγκαταστήσετε τη μονάδα AMPLIFY BATTERY EXTENDER. Το Xposed Framework παρέχει σε χρήστες που έχουν κάνει Root τις συσκευές τους εκατοντάδες νέες δυνατότητες, χαρακτηριστικά και features παραμετροποίησης [40].

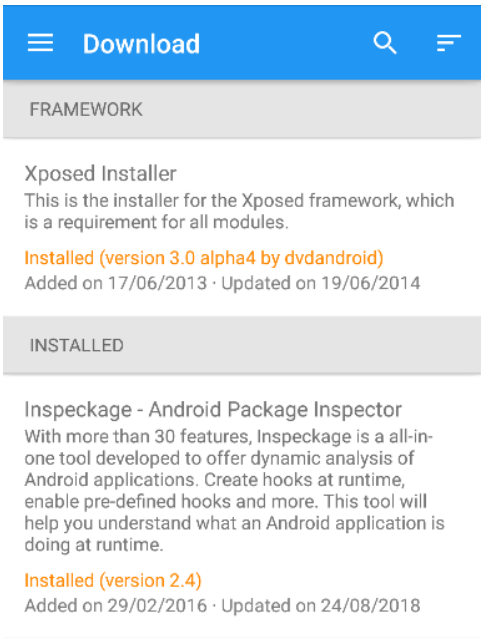
Έχοντας λοιπόν, κάνει root την συσκευή μας, κατεβάζουμε το .apk του Xposed Installer στην σωστή του έκδοση, η οποία εξαρτάται από την έκδοση του Android. Για τους σκοπούς της έρευνάς μας θα χρησιμοποιήσουμε την συσκευή SAMSUNG Galaxy S4 για την εγκατάσταση η οποία διαθέτει λογισμικό Lollipop 5.0.1. Επομένως επιλέξαμε την έκδοση Xposed Installer v. 3.0 alpha 4. Το Xposed Installer θα μας εγκαταστήσει το Xposed Framework έκδοσης 85.0.



Εικόνα 6.3: Επιτυχής εγκατάσταση του Xposed Framework

3. Xposed Modules

Υπάρχουν εκατοντάδες Xposed Modules για να καλύπτουν όλες τις "αλλαγές" που μπορεί να θέλουμε στις συσκευές μας. Θα αναφερθούμε ενδεικτικά στο Module που θα χρησιμοποιήσουμε το οποίο είναι το Inspeckage- Android Package Inspector.



Εικόνα 6.4: Επιτυχής εγκατάσταση του Inspeckage-Android Package Inspector.

Το Inspeckage είναι μια απλή εφαρμογή με έναν εσωτερικό διακομιστή HTTP που παρέχει μια φιλική διεπαφή ιστού και αναπτύχθηκε ως μονάδα του Xposed Framework. Μπορούμε να το εκτελέσουμε χωρίς το Xposed πλαίσιο, αλλά το 80% των δυνατοτήτων του εξαρτάται από το Xposed Framework, επομένως συνιστάται η παρουσία του πλαισίου στη συσκευή [41]. Το Inspeckage είναι ένα εργαλείο που αναπτύχθηκε για να προσφέρει δυναμική ανάλυση

εφαρμογών Android. Το Inspeckage μας βοηθά να καταλάβουμε τι κάνει μια εφαρμογή Android κατά το χρόνο της εκτέλεσης της. Κατά την επιθεώρηση θα μας επιτραπεί να αλληλοεπιδράσουμε με ορισμένα στοιχεία της εφαρμογής, όπως δραστηριότητες και παρόχους και να εφαρμόσουμε ορισμένες ρυθμίσεις στο Android. Επίσης το εργαλείο επιτρέπει την παράκαμψη της κρυπτογραφημένης κίνησης παρεμποδίζοντας την επαλήθευση του πιστοποιητικού ασφαλείας SSL, ακόμη και αν το πιστοποιητικό είναι "καρφωμένο" μέσα στην εφαρμογή [42]. Δεδομένου ότι η δυναμική ανάλυση εφαρμογών Android αποτελεί βασικό μέρος πολλών δοκιμών ασφάλειας εφαρμογών για κινητά, η ανάγκη ενός εργαλείου που μπορεί να μας βοηθήσει να κάνουμε δοκιμές είναι πραγματικότητα μέσω του Inspeckage.

Με το Inspeckage, μπορούμε να περισυλλέξουμε ποσότητα πληροφοριών σχετικά με τη συμπεριφορά της εφαρμογής όπως [43]:

1. Συλλογή πληροφοριών τις εφαρμογής όπως (Package Information):
    - Απαιτούμενα δικαιώματα.
    - Δικαιώματα εφαρμογών.
    - Κοινόχρηστες βιβλιοθήκες.
    - Εξαγόμενες και Μη Εξαγόμενες Δραστηριότητες, Παροχείς περιεχομένου, Δέκτες και Υπηρεσίες Broadcast.
    - Ελέγχει αν η εφαρμογή είναι debuggable.
    - Έκδοση, UID και GID.
    - κλπ.
2. Με τη χρήση των Hooks

    Τα Hooks ουσιαστικά, είναι ένα σημείο στον κώδικα που σας επιτρέπει να συνδέεστε σε μια ενότητα για να παρέχετε διαφορετική συμπεριφορά ή να αντιδράτε όταν συμβαίνει κάτι. Με τα hooks, μπορούμε να δούμε τι κάνει η εφαρμογή σε πραγματικό χρόνο όσο αφορά:
    - Κοινόχρηστες προτιμήσεις (Shared Preferences).
    - Σειρά εκτέλεσης κώδικα (Serialization)
    - Κρυπτογραφία.
    - Hashes.
    - SQLite (Το SQLite είναι μια βάση δεδομένων SQL ανοικτού κώδικα που αποθηκεύει τα δεδομένα σε ένα αρχείο κειμένου σε μια συσκευή).
    - Το HTTP.

- Σύστημα αρχείων (File System)
- WebView (Το Android WebView είναι ένα στοιχείο συστήματος για το λειτουργικό σύστημα Android που επιτρέπει στις εφαρμογές Android να προβάλλουν περιεχόμενο από τον ιστό απευθείας μέσα σε μια εφαρμογή).
- IPC (inter-process Communication-επικοινωνία μεταξύ διαδικασιών αναφέρεται συγκεκριμένα στους μηχανισμούς που παρέχει ένα λειτουργικό σύστημα για να επιτρέψει στις διεργασίες να διαχειρίζονται κοινά δεδομένα).

3. Ενέργειες

Με το Xposed είναι δυνατή η εκτέλεση ενεργειών όπως να:

- Ξεκινήσουμε οποιαδήποτε δραστηριότητα.
- Καλέσουμε οποιονδήποτε πάροχο.
- Απενεργοποιήσουμε την FLAG_SECURE η οποία αντιμετωπίζει το περιεχόμενο του παραθύρου ως ασφαλές, εμποδίζοντας το να εμφανίζεται σε στιγμιότυπα οθόνης ή να προβάλλεται σε μη ασφαλείς οθόνες.
- Παρακάμψουμε το πιστοποιητικό ασφαλείας SSL.
- Ξεκινούμε, σταματούμε και επανεκκινούμε την εφαρμογή.
- Αντικαταστούμε τις παραμέτρους και την τιμή επιστροφής.

4. Ψηφιακό Αποτύπωμα (Fingerprint)

Το ψηφιακό αποτύπωμα του μηχανήματος ή το αποτύπωμα του προγράμματος περιήγησης είναι πληροφορίες που συλλέγονται για μια απομακρυσμένη υπολογιστική συσκευή με σκοπό την ταυτοποίηση. Μία συσκευή μπορεί να ταυτοποιηθεί μοναδικά από ένα σύνολο πληροφοριών που «εκπέμπει» ενώ ο χρήστης τη χρησιμοποιεί (π.χ. καθώς πλοηγείτε στο Διαδίκτυο) και, άρα, υπ' αυτήν την έννοια, αυτές οι πληροφορίες συνιστούν ένα ψηφιακό αποτύπωμα της συσκευής. Τέτοιες πληροφορίες μπορεί να απαρτίζονται από τα εξής:

- ID διαφήμισης όπως το GAID (Google Advertising ID), διεύθυνση MAC, IMEI, έκδοση, μάρκα, τρόπος κατασκευής κλπ.

5. Τοποθεσία
   - Αλλαγή θέσης GPS

6. Πρόσθετα
   - Λήψη μίας εφαρμογής.
   - Προβολή του δέντρου καταλόγου της εφαρμογής.
   - Λήψη των αρχείων της εφαρμογής.

- Κατεβάζουμε την έξοδο που δημιουργείται από τα άγκιστρα/hooks σε μορφή αρχείου κειμένου.
- Πραγματοποιούμε μια λήψη στιγμιότυπου οθόνης.
- Στέλνουμε κείμενο στο πρόχειρο του Android.

6.2 Περιβάλλον Δοκιμών

Θα πραγματοποιηθεί δυναμική ανάλυση συνολικά πέντε (5) εφαρμογών με κατάλληλα εργαλεία λογισμικού τα οποία είναι το Lumen Privacy Monitor και το Inspeckage, προκειμένου να «ανιχνευτούν» σε πραγματικό χρόνο οι ροές δεδομένων από την οποιαδήποτε συσκευή του χρήστη. Το πείραμα ξεκίνησε την 1η Φεβρουαρίου 2019 και διήρκησε 2 μήνες. Όλοι οι συμμετέχοντες και τα ανενεργά κινητά τηλέφωνα βρίσκονταν εντός της ευρύτερης περιοχής της Κυπριακής Δημοκρατίας. Για τη πρόσβαση στο διαδίκτυο χρησιμοποιήθηκε το οικιακό δίκτυο κάθε χρήστη αλλά και το δίκτυο κινητής (4G). Ακόμη και για τις ανενεργές κινητές συσκευές χρησιμοποιήθηκε η μέθοδος hotspot μέσω δικτύου κινητής, με σκοπό την συμμετοχή τους «εν κινήσει». Για το σκοπό αυτό επιλέχθηκαν 5 δημοφιλείς εφαρμογές πλοήγησης/εντοπισμού θέσεως οι οποίες είναι:

1. Google Maps (v 10.12.1)
2. Sygic GPS Navigation & Maps (17.7.0)
3. TomTom GPS Navigation - Traffic Alerts & Maps (v 1.17.1)
4. MAPS.ME (v 9.0.7)
5. MapFactor GPS Navigation Maps (v 4.0.109)

Αφού επιλέχθηκαν οι ανωτέρω εφαρμογές έγιναν εγκατάσταση σε 5 κινητές συσκευές με λειτουργικό σύστημα Android ως αναφέρονται στον πίνακα.

Α/Α	Κατασκευαστής	Όνομα Μοντέλου	Κωδικός Μοντέλου	Έκδοση Λειτουργικού
1	SAMSUNG	Galaxy CORE 2	SM-G355HN	KitKat 4.4.2
2	SAMSUNG	Galaxy S3 neo	GT-I9301I	KitKat 4.4.2
3	SAMSUNG	Galaxy S4	GT-I9515	Lollipop 5.0.1
4	SAMSUNG	Galaxy S6	SM-G920X	Nougat 7.0
5	SAMSUNG	Galaxy S8	SM-G950F	Oreo 8.0

Πίνακας 6.1: Στοιχεία συσκευών που συμμετέχουν στο πείραμα.

6.3 Ανάλυση εφαρμογών

6.3.1 Ανάλυση με το Lumen Privacy Monitor

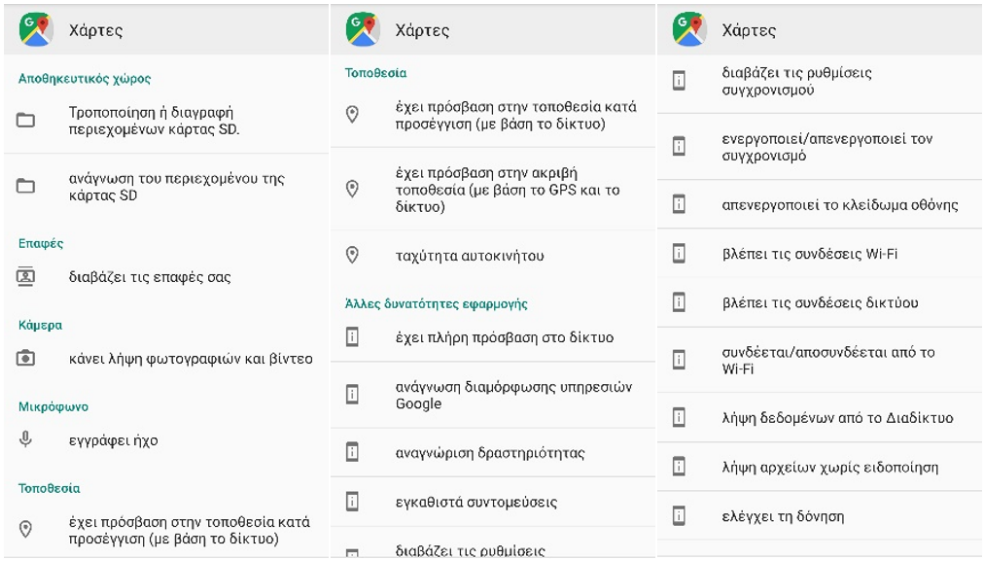
Μετά την εγκατάσταση των εφαρμογών μας σε κάθε κινητή συσκευή προχωρήσαμε στην λήψη της εφαρμογής Lumen Privacy Monitor από την ιστοσελίδα https://www.haystack.mobi/. Μετά από επικοινωνία με την ομάδα ανάπτυξης του " The Haystack Project" μας ενημέρωσαν ότι η έκδοση της εφαρμογής που βρίσκεται δημόσια μέσω του Google Play δεν λειτουργεί σωστά στην αναγνώριση της διαρροής των δεδομένων θέσης, επομένως έγινε λήψη της εφαρμογής μέσα από την ιστοσελίδα του προγράμματος. Στην σελίδα αυτή αναφέρονται όλα τα στοιχεία και οι πληροφορίες που αφορούν το πρόγραμμα δυναμικής ανάλυσης Lumen Privacy Monitor. Αφού γίνει η λήψη της εφαρμογής τότε εγκαταστάθηκε στις 4 από τις 5 συσκευές μας και συγκεκριμένα σε όλες πλην της συσκευής με A/A 3. Οι συσκευές υπ' αριθμόν 4 και 5 ανήκαν σε ενεργούς χρήστες κινητής συσκευής, δηλαδή σε κινητές συσκευές οι οποίες διέθεταν κάρτα SIM και χρησιμοποιούνταν καθημερινά ως ενεργές. Οι συσκευή υπ' αριθμόν 1 διέθετε κάρτα SIM αλλά δεν άνηκε σε ενεργό χρήστη. Τέλος η συσκευή υπ' αριθμόν 2 δεν διέθετε κάρτα SIM και δεν άνηκε σε κάποιο ενεργό χρήστη. Ουσιαστικά οι συσκευές 1 και 2 δεν ανήκαν σε κάποιο ενεργό χρήστη αλλά χρησιμοποιούνταν ανά τακτά χρονικά διαστήματα. Τέλος η συσκευή υπ' αριθμόν 3 χρησιμοποιήθηκε μόνο με σκοπό να ελεγχθούν οι εφαρμογές μας από το πρόγραμμα Δυναμικής Ανάλυσης Inspeckage.

Μετά από επικοινωνία που είχαμε με την ομάδα ανάπτυξης του " The Haystack Project" μας ενημέρωσαν επίσης ότι από την έκδοση Android 7 και μετά πιθανόν το πιστοποιητικό TLS που εγκαθίσταται από το πρόγραμμά μας, πιθανόν να μην θεωρηθεί έμπιστο και επομένως να μην γίνεται σωστά η αποκοπή του και, άρα, η πλήρης παρουσίαση των διαρροών δεδομένων. Επιπλέον μας ανάφεραν ότι οι περισσότερες εφαρμογές χρησιμοποιούν κωδικοποίηση για να φορτώσουν τα δεδομένα, ακόμα και για την τοποθεσία και λόγω του ότι αποτελούνται από μία μικρή ομάδα ερευνητών δεν έχουν προλάβει ακόμα να αναπτύξουν διορθώσεις για την εφαρμογή.

Η κάθε εφαρμογή λοιπών κατά την εγκατάστασή της ζήτησε πρόσβαση μέσω των "αδειών πρόσβασης" σε αρκετά δεδομένα της συσκευής, κάποιες βέβαια θα μπορούσαν να θεωρηθούν ως υπερβολικές αν κρίνουμε από τον σκοπό της κάθε εφαρμογής. Πιο κάτω παρουσιάζονται οι άδειες πρόσβασης που ζητήθηκαν από κάθε εφαρμογή στην κινητή συσκευή Samsung Galaxy S8. Σε αυτό το σημείο αξίζει να σημειωθεί ότι κάποιες εφαρμογές ζήτησαν, σε κάθε συσκευή και λόγω διαφορετικής έκδοσης λειτουργικού, ελαφρώς διαφοροποιημένες άδειες πρόσβασης. Για

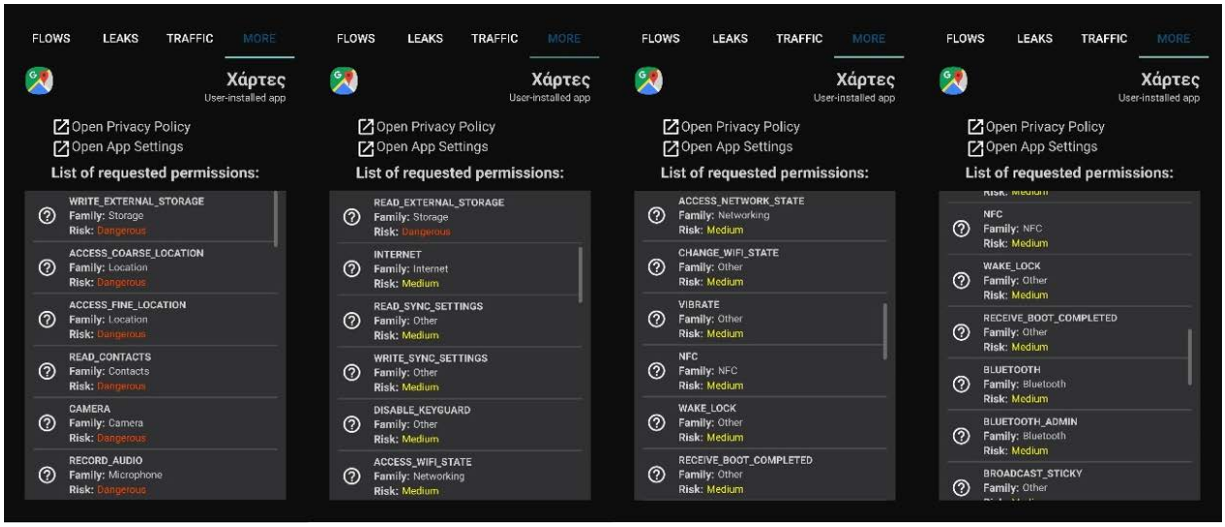
παράδειγμα στην εφαρμογή Google Maps, στα Core 2 και S3 υπολείπονται 2 επικίνδυνες άδειες, όπως το CAMERA και το RECORD_AUDIO, ενώ προσθέτουν την GET_ACCOUNTS, σε σχέση με το S8. Οι άδειες τροποποιούνται ελαφρώς, αναλόγως της έκδοσης της εφαρμογής και του λειτουργικού που φέρει η κάθε συσκευή.

1. Google Maps (v 10.12.1)

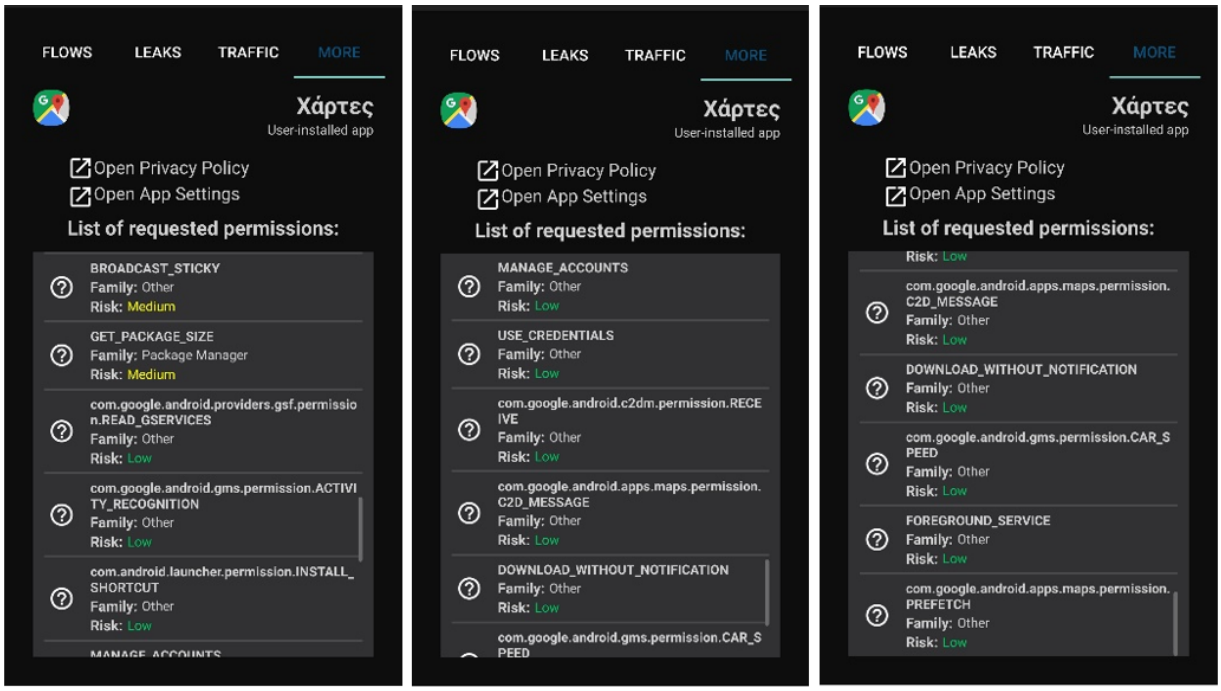


Εικόνα 6.5: Άδειες που απαιτούνται για την εγκατάστασης του Google Maps στην κινητή συσκευή Samsung Galaxy S8.

Στην εικόνα 6.5 παρουσιάζονται οι άδεις πρόσβασης που η εφαρμογή Google Maps ζητά από τον χρήστη της κινητής συσκευής Samsung Galaxy S8 (Oreo). Το πρόγραμμα Lumen Privacy Monitor έρχεται ταξινομεί τις πιο πάνω άδειες σε επίπεδα επικινδυνότητας ως Dangerous με κόκκινο χρώμα, ως Medium με κίτρινο χρώμα και ως Low με πράσινο χρώμα, όπως φαίνεται στην εικόνα.

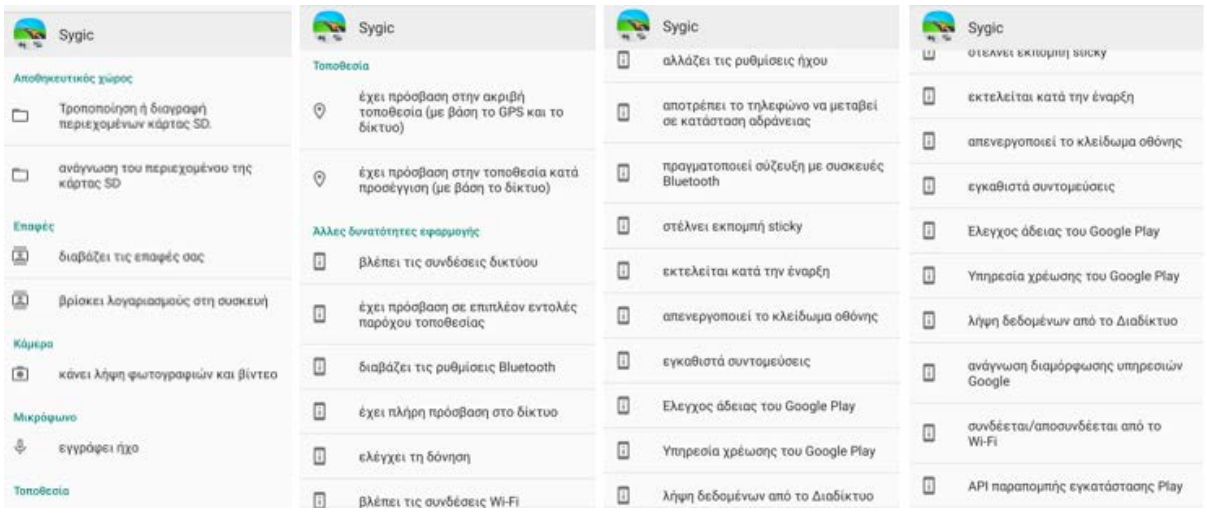


Εικόνα 6.6: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του Google Maps, μέσα από το Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.



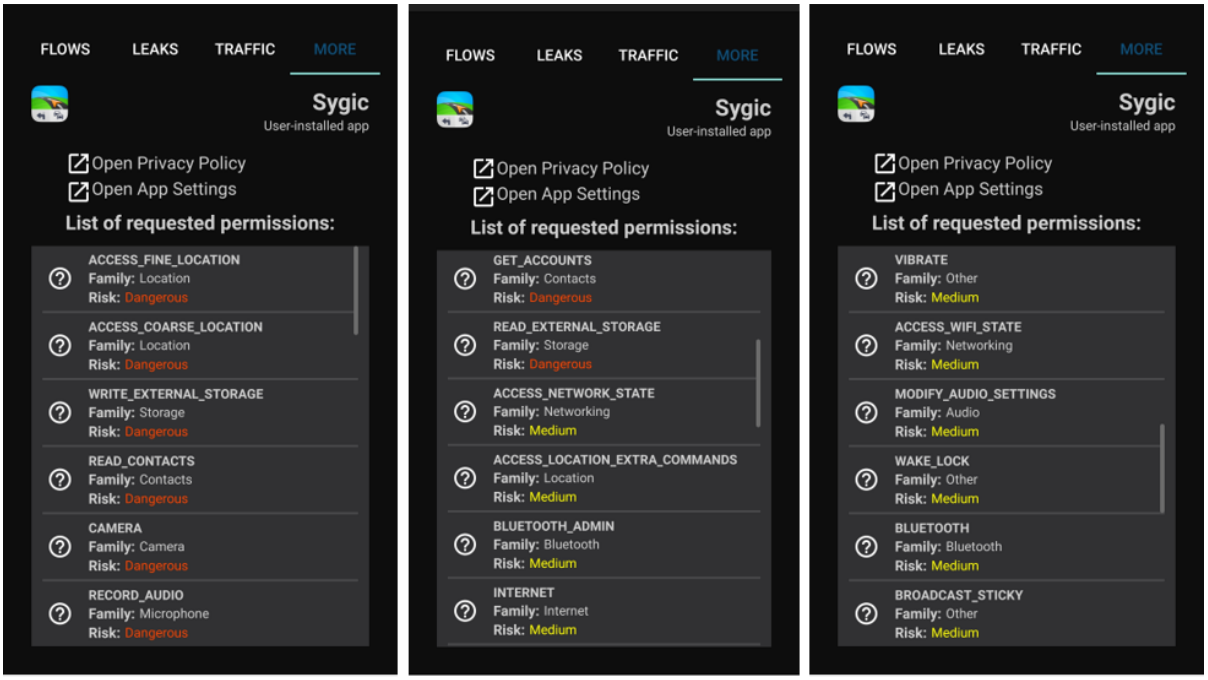
Εικόνα 6.7: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του Google Maps, μέσα από το Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.

2. Sygic GPS Navigation & Maps (17.7.0)

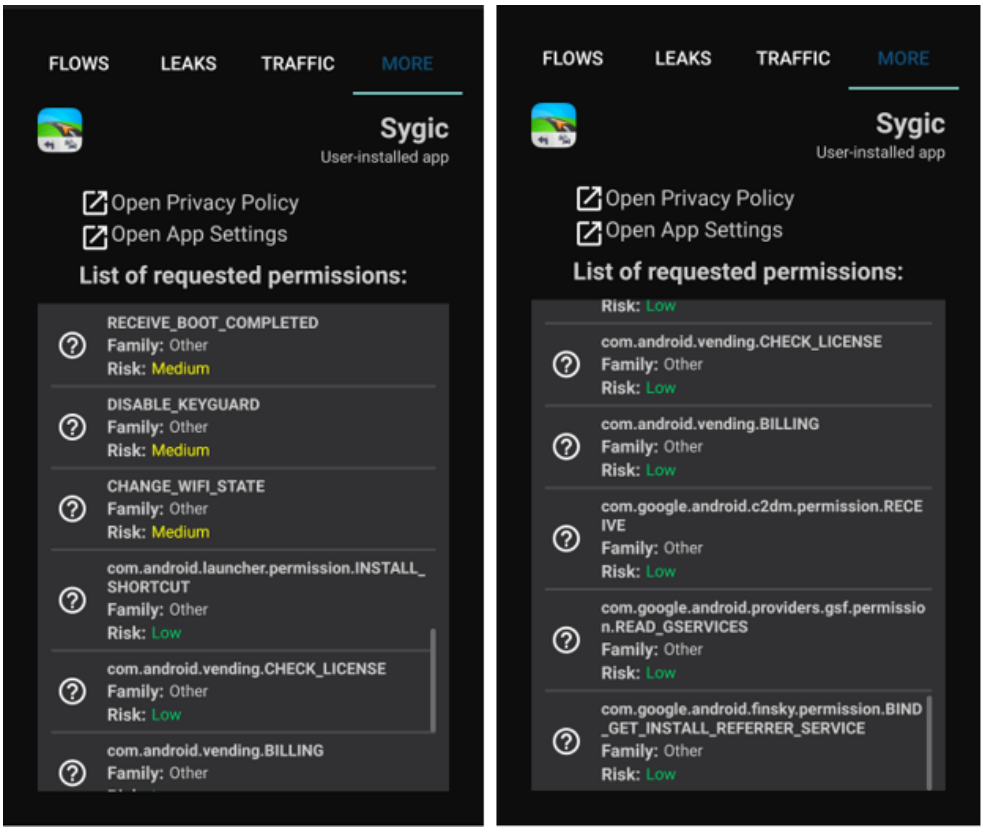


Εικόνα 6.8: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του Sygic στην κινητή συσκευή Samsung Galaxy S8.

Το πρόγραμμα Lumen Privacy Monitor έρχεται με τη σειρά του και ταξινομεί τις πιο πάνω άδειες σε επίπεδα επικινδυνότητας.

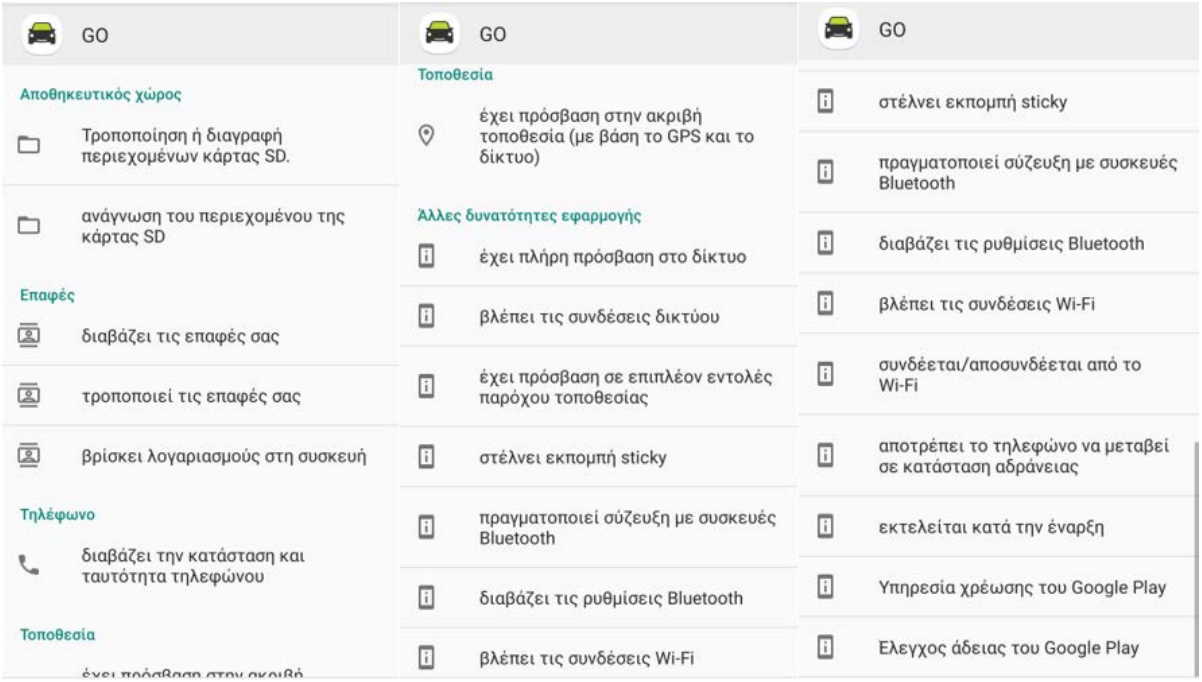


Εικόνα 6.9: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του Sygic, μέσα από το Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.

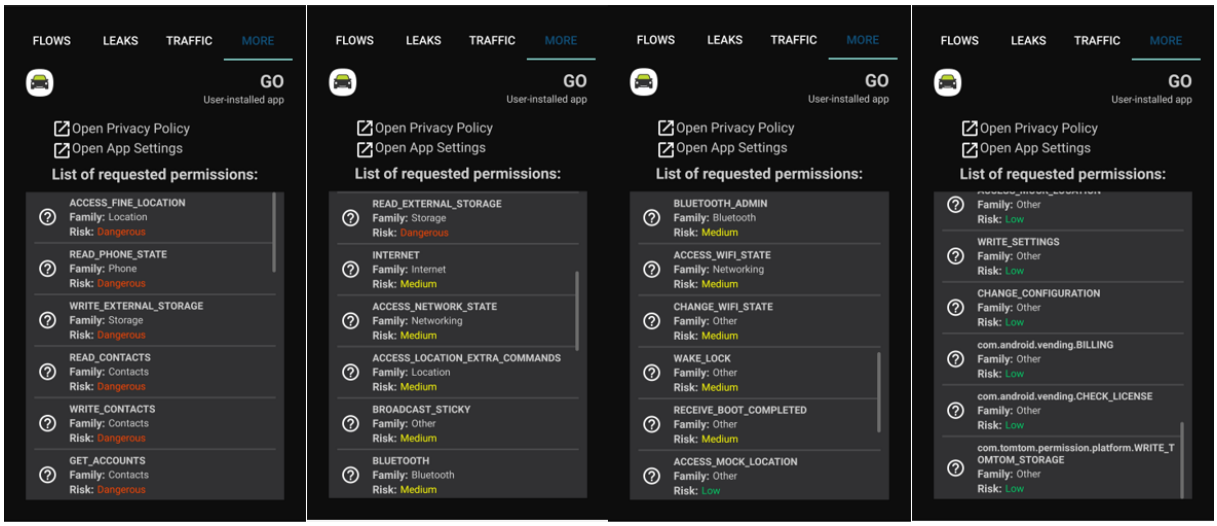


Εικόνα 6.10: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του Sygic, μέσα από το Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.

3. TomTom GPS Navigation - Traffic Alerts & Maps (v 1.17.1)

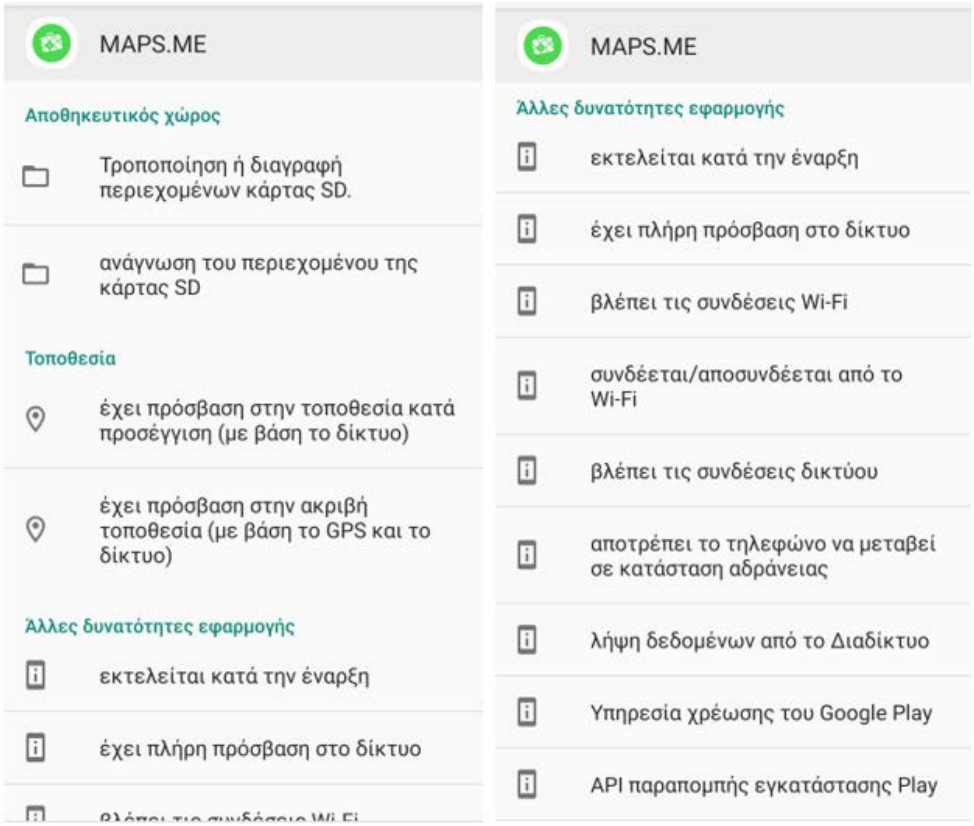


Εικόνα 6.11: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του TomTom GPS Navigation στην κινητή συσκευή Samsung Galaxy S8.

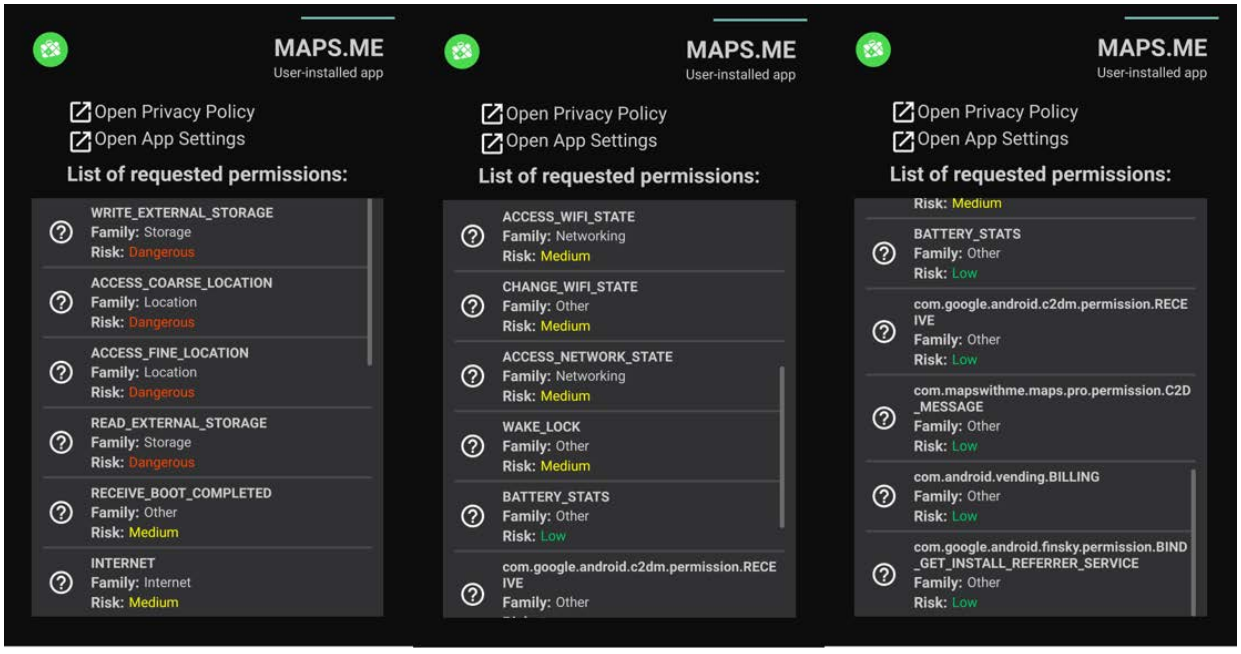


Εικόνα 6.12: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του TomTom GPS Navigation, μέσα από το Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.

4. MAPS.ME (v 9.0.7)

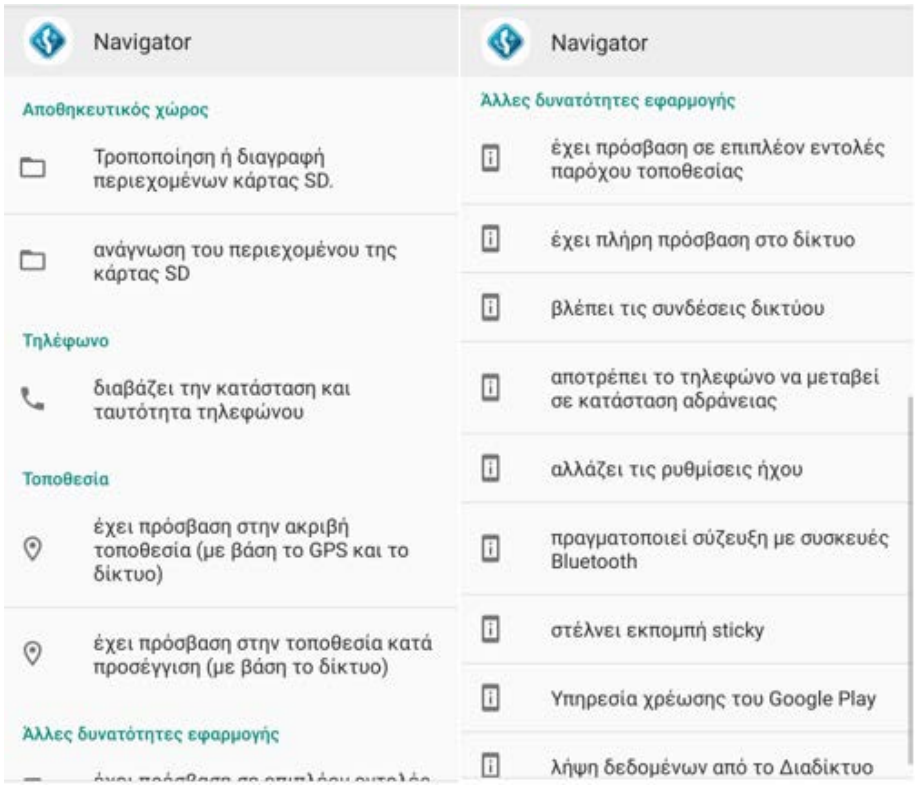


Εικόνα 6.13: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του MAPS.ME στην κινητή συσκευή Samsung Galaxy S8.

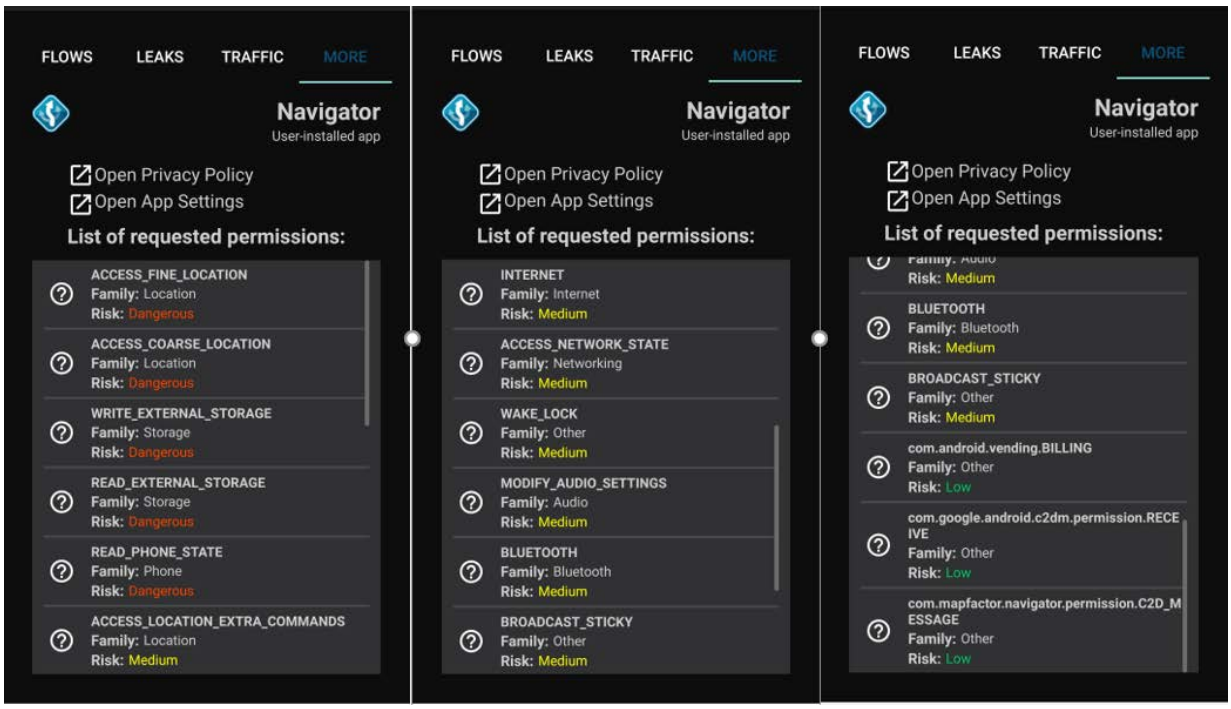


Εικόνα 6.14: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του MAPS.ME, μέσα από Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.

5. MapFactor GPS Navigation Maps (v 4.0.109)



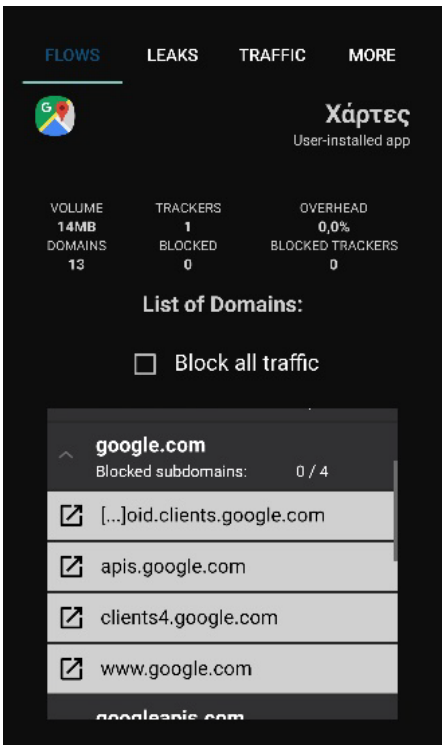
Εικόνα 6.15: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του MapFactor GPS Navigation στην κινητή συσκευή Samsung Galaxy S8.



Εικόνα 6.16: Αναλυτικά οι άδειες που απαιτούνται για την εγκατάστασης του MapFactor GPS Navigation, μέσω του Lumen Privacy Monitor στην κινητή συσκευή Samsung Galaxy S8.

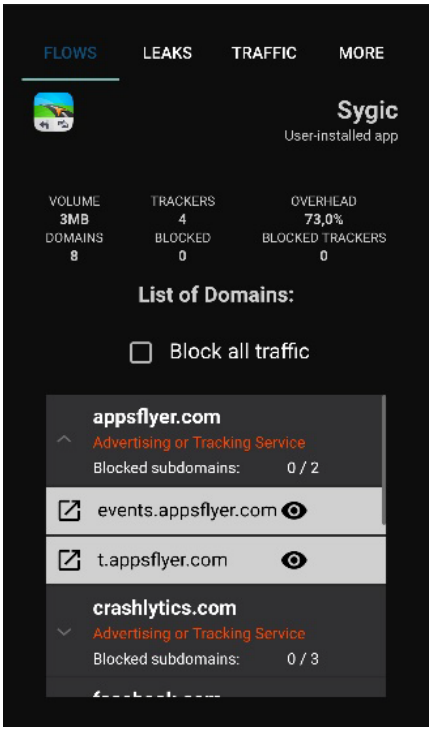
Στη συνέχεια καταγράψαμε για κάθε εφαρμογή τις λίστες οι οποίες αναγράφουν τους τομείς (Domains) που η ίδια επικοινωνεί και στέλνει ή λαμβάνει δεδομένα. Οι τομείς οι οποίοι παρουσιάζονται σε κάθε εικόνα είναι οι υπηρεσίες με τις οποίες επικοινωνεί μία εφαρμογή αλλά και οι προαναφερθείσες υπηρεσίες τρίτων (Trackers) που με τις οποίες γίνεται ανταλλαγή δεδομένων. Επιπλέον επιλέγοντας κάθε τομέα μπορούμε να δούμε με ποιους υποτομείς έχει στην πραγματικότητα επικοινωνία η εφαρμογή, πέρα τον κεντρικών βασικών τομέων. Πέραν των πιο πάνω, το Lumen Privacy Monitor παρέχει τη δυνατότητα προσδιορισμού του κατά πόσον ένας τομέας θεωρείται ATS (Advertising or Tracking Service), δηλαδή μία υπηρεσία τρίτου που σκοπό έχει τον εντοπισμό του χρήστη μέσω ιχνηλάτησής του, την και την παροχή διαφημίσεων σε αυτόν. Τέλος αποκαλύπτει σε μορφή ποσοστού τις γενικές ροές πληροφοριών (overhead) αλλά και συνολικά ως ποσότητα δεδομένων (Volume), που προκαλούνται από τις διαφημίσεις, τις συνδέσεις παρακολούθησης (tracking) και τις διαρροές δεδομένων των εφαρμογών. Τη λίστα αυτή την βρίσκουμε στο «FLOWS» για κάθε εφαρμογή και την παρουσιάζουμε εν μέρη στις πιο κάτω εικόνες:

1. Google Maps (v 10.12.1)



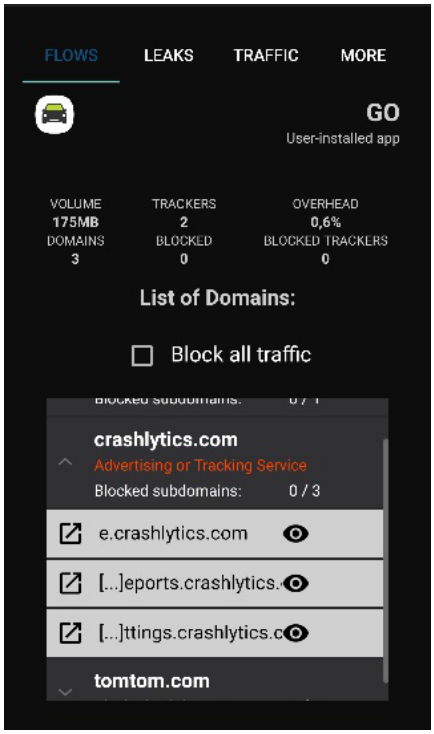
Εικόνα 6.17: Δείγμα τομέων, υποτομέων, συνολικού ποσοστού overhead και τιμής volume, που επικοινωνεί το Google Maps, μέσα από το Lumen Privacy Monitor.

2. Sygic GPS Navigation & Maps (17.7.0)



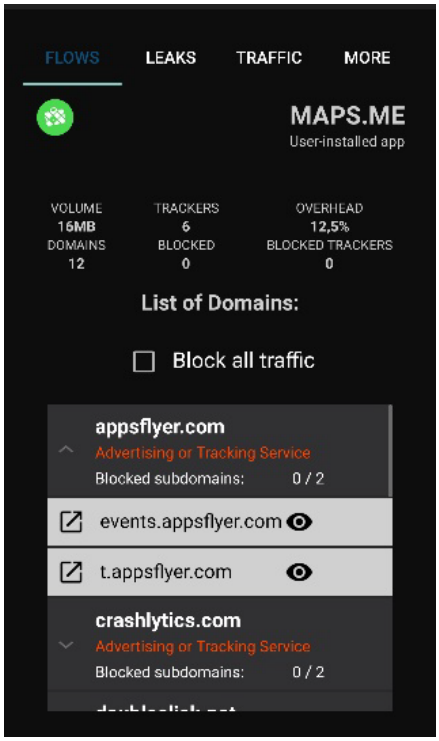
Εικόνα 6.18: Δείγμα τομέων, υποτομέων, συνολικού ποσοστού overhead και τιμής volume, που επικοινωνεί το Sygic μέσα, από το Lumen Privacy Monitor.

3. TomTom GPS Navigation - Traffic Alerts & Maps (v 1.17.1)



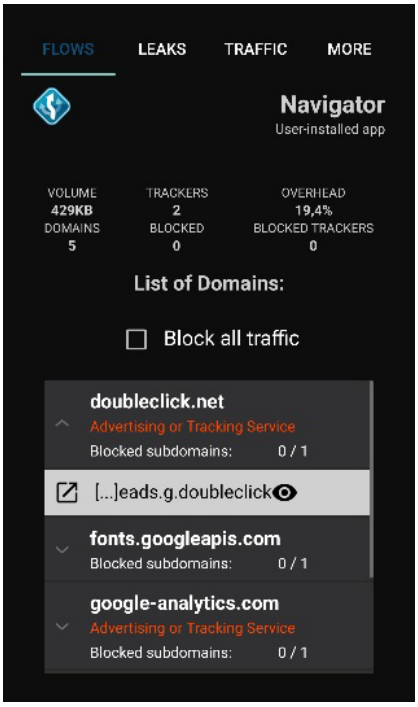
Εικόνα 6.19: Δείγμα τομέων, υποτομέων, συνολικού ποσοστού overhead και τιμής volume, που επικοινωνεί το TomTom GPS Navigation, μέσα από το Lumen Privacy Monitor.

4. MAPS.ME (v 9.0.7)



Εικόνα 6.20: Δείγμα τομέων, υποτομέων, συνολικού ποσοστού overhead και τιμής volume, που επικοινωνεί το MAPS.ME, μέσα από το Lumen Privacy Monitor.

5. MapFactor GPS Navigation Maps (v 4.0.109)

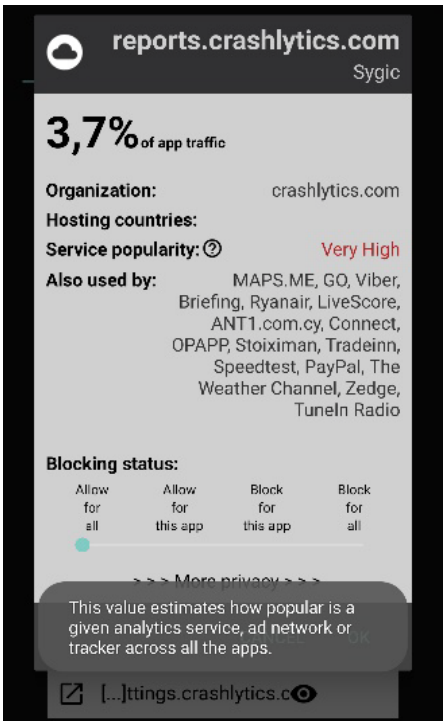


Εικόνα 6.21: Δείγμα τομέων, υποτομέων, συνολικού ποσοστού overhead και τιμής volume, που επικοινωνεί το MapFactor GPS Navigation, μέσα από το Lumen Privacy Monitor.

Πέραν τις παρουσίασης των τομέων με τους οποίους μία εφαρμογή επικοινωνεί το Lumen μπορεί να μας παρουσιάσει αναλυτικά έναν προς έναν τους τομείς και τους υπό τομείς προσφέροντάς μας πληροφορίες σχετικά με:

- Το ποσοστό επικοινωνίας που χρησιμοποιήθηκε από την εφαρμογή, για σκοπούς επικοινωνίας με τον κάθε τομέα.
- Το σε ποιόν πραγματικά ανήκει ο κάθε υποτομέας.
- Σε ποια χώρα φιλοξενείται ο εν λόγω τομέας.
- Το επίπεδο επικινδυνότητας κάθε υπηρεσίας/τομέα το οποίο υπολογίζει πόσο δημοφιλής είναι μια δεδομένη υπηρεσία ανάλυσης, ένα δίκτυο διαφημίσεων ή ένας ιχνηλάτης (tracker) σε όλες τις εφαρμογές.
- Από ποιες άλλες εφαρμογές χρησιμοποιείται ο τομέας.

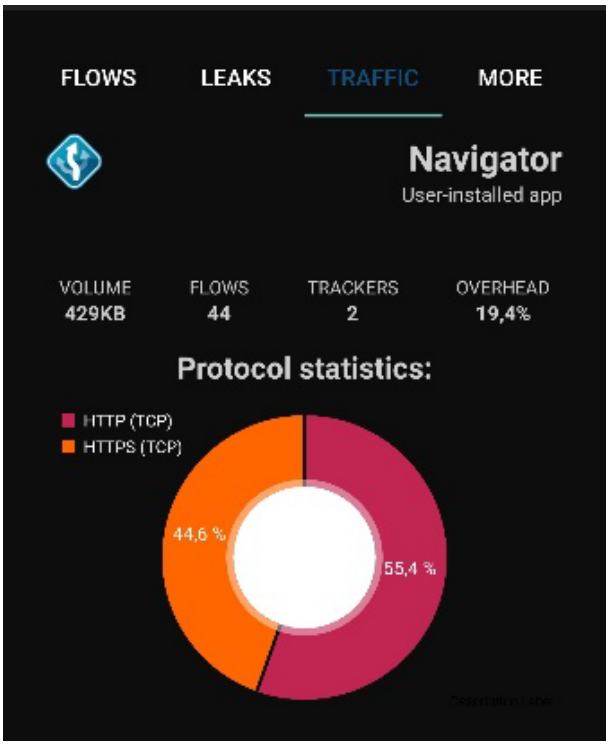
Τέλος μας παρέχει την δυνατότητα να επιλέξουμε το επίπεδο πρόσβασης του εν λόγω τομέα στην εφαρμογή μας (Blocking Status).



Εικόνα 6.22: Παρουσίαση τομέα reports.crashlytics.com, μέσα από το Lumen Privacy Monitor.

Οι εφαρμογές ενδέχεται μερικές φορές να διαρρέουν πληροφορίες όχι μόνο προς τους δικούς τους διακομιστές αλλά και σε διαφημιστικά δίκτυα στο διαδίκτυο ή σε άλλες υπηρεσίες παρακολούθησης μέσω διαδικτύου που αποκομίζουν οικονομικό όφελος από τα μεταδεδομένα

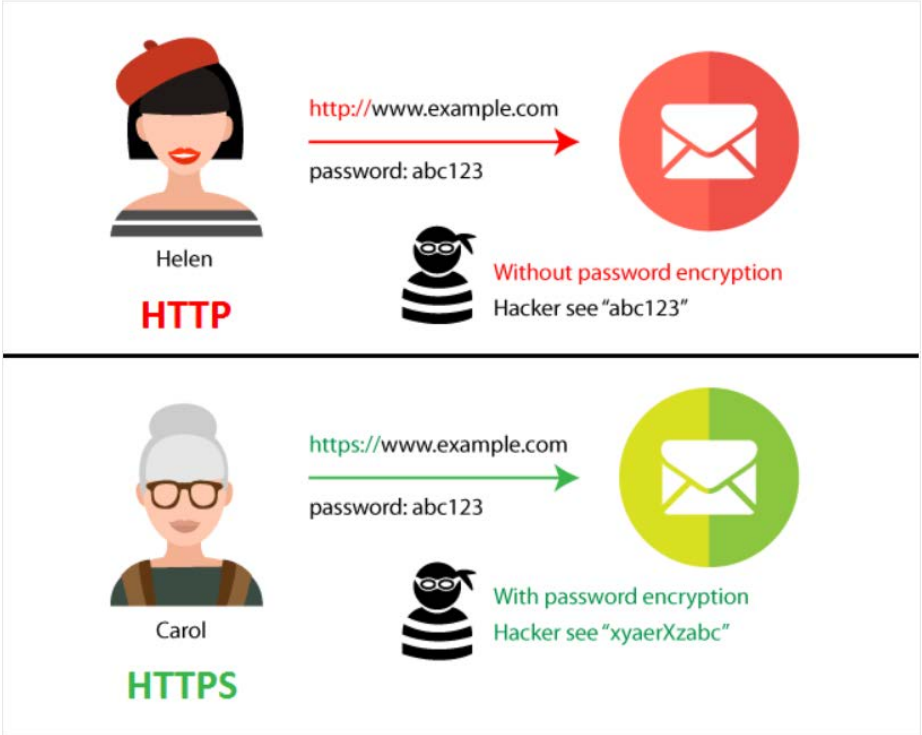
μας. Το Lumen αναλύει την επισκεψιμότητα του κινητού και παράγει αναφορές σχετικά με τα μοντέλα επισκεψιμότητας και τα ιδιωτικά δεδομένα που συλλέγονται από την κάθε εφαρμογή και υπηρεσία σε απευθείας σύνδεση. Στη συνέχεια το πρόγραμμα δυναμικής ανάλυσης των εφαρμογών μας παρουσιάζει τα πρωτόκολλα διαδικτύου που χρησιμοποιήθηκαν για την αποστολή των δεδομένων μεταξύ μίας εφαρμογής και του κάθε τομέα συνολικά.



Εικόνα 6.23: Τα πρωτόκολλα αποστολής δεδομένων στο δίκτυο για την εφαρμογή MapFactor GPS Navigation.

Το HTTP, ορίζεται ως Hyper Text Transfer Protocol (Πρωτόκολλο Μεταφοράς Υπέρ-Κειμένου) και είναι η τεχνολογία που επιτρέπει τους υπερσυνδέσμους και τη φυλλομέτρηση εν γένη, ουσιαστικά χωρίς αυτό δεν υπάρχει πλοήγηση στο διαδίκτυο [44]. Η τεχνολογία αυτή είναι που χρησιμοποιείται για την επικοινωνία μεταξύ των σέρβερ του διαδικτύου και των χρηστών. Το HTTPS είναι το ίδιο στην ουσία με το HTTP, όπως φαίνεται κι από το όνομά του, με την διαφορά της προσθήκης του Secure (Ασφαλές), που σημαίνει ότι έχει επιπλέον μια βαθμίδα ασφαλείας SSL (Secure Sockets Layer). Το SSL λοιπόν, που πλέον έχει μετονομαστεί σε TLS, είναι ένα ισχυρό σύστημα ασφαλούς και αδιαπέραστης κρυπτογράφησης που κάνει τα δεδομένα μας μη προσβάσιμα σε παρείσακτους κατά τη μεταφορά τους μέσω του Internet. Και τα δύο πρωτόκολλα κάνουν χρήση του TCP . Το πρωτόκολλο User Datagram Protocol (UDP) είναι μέρος της σουίτας πρωτοκόλλων του Internet. Το UDP χρησιμοποιείται για την αποστολή σύντομων μηνυμάτων

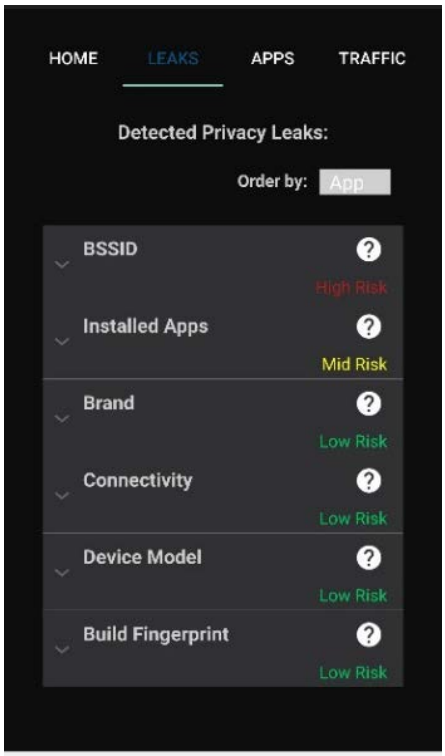
που ονομάζονται datagrams αλλά συνολικά, είναι ένα αναξιόπιστο πρωτόκολλο καθότι δεν απαιτεί σύνδεση. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Χρησιμοποιείται όταν η "γρήγορη" παράδοση των πακέτων είναι πιο σημαντική από την "ακριβή" παράδοση, π.χ. στη μετάδοση ομιλίας και βίντεο. Αντιθέτως, το πρωτόκολλο TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία



Εικόνα 6.24: Η κύρια διαφορά μεταξύ των πρωτοκόλλων Http και Https [45].

Μπορούμε να χρησιμοποιήσουμε το Lumen για να καταλάβουμε πού συνδέονται οι εφαρμογές μας, πόσο μεγάλη επισκεψιμότητα έχουν για σκοπούς διαφήμισης και παρακολούθησης και ποια δεδομένα μοιράζονται με τρίτους. Τέλος το Lumen Privacy Network μας παρουσιάζει όλα τα προσωπικά δεδομένα που διέρρευσε η συσκευή μας μέσω των εφαρμογών. Η λίστα των πληροφοριών διαρροής παρουσιάζεται με το όνομα "LEAKS". Κάθε διαρροή ονοματίζεται και ταξινομείται σε τρία επίπεδα επικινδυνότητας, αναλόγως του δεδομένου που διαρρέει. Τα τρία επίπεδα είναι όπως και στον τομέα των δικαιωμάτων πρόσβαση το "High Risk" με κόκκινο χρώμα,

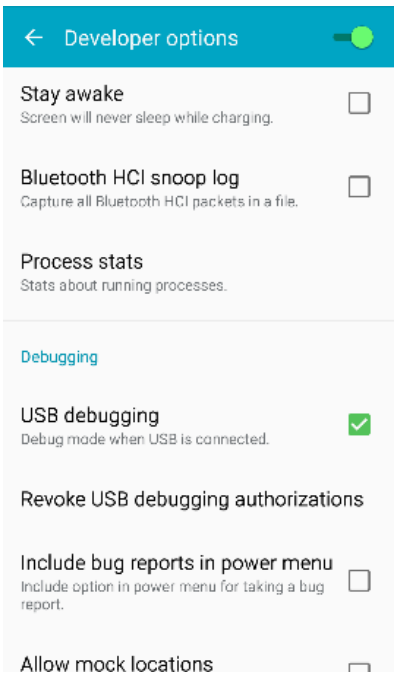
όπου παρουσιάζει της διαρροές υψηλού κινδύνου, το “Mid Risk” με κίτρινο χρώμα, όπου παρουσιάζονται διαρροές μεσαίου κινδύνου και το “Low Risk” με πράσινο χρώμα, όπου παρουσιάζονται διαρροές με χαμηλού επιπέδου επικινδυνότητας.



Εικόνα 6.25: Δείγμα διαρροών μέσα από το πλήθος των εφαρμογών μίας συσκευής.

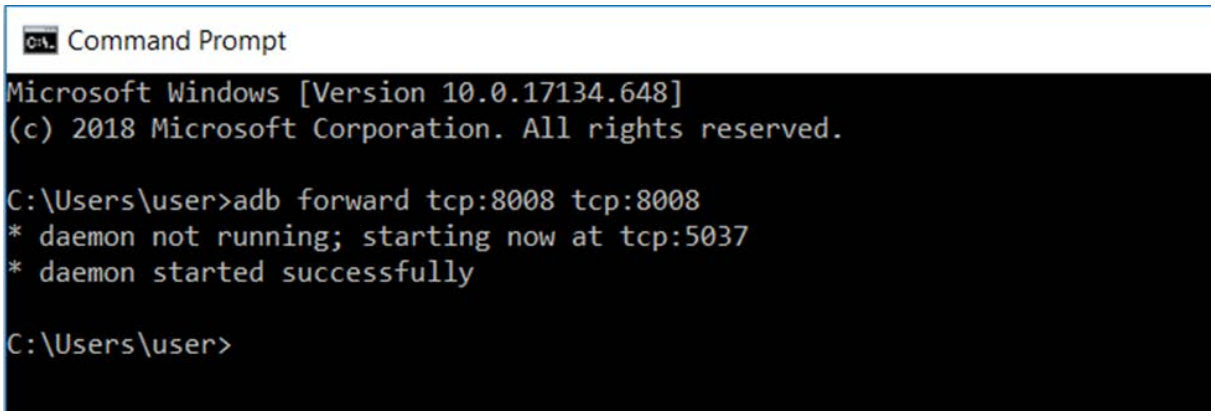
6.3.2 Ανάλυση με το Inspeckage

Για την ανάλυση μίας εφαρμογής με τη χρήση του προγράμματος δυναμικής ανάλυσης Inspeckage απαιτείται αρχικά η σύνδεση του κινητού τηλεφώνου με ένα υπολογιστή μέσω καλωδίου USB. Η συσκευή η οποία θα χρησιμοποιηθεί είναι το Samsung Galaxy S4, το οποίο όπως προαναφέρθηκε είναι Root και έχει επιλεχθεί το “USB debugging” από το Developer Options.



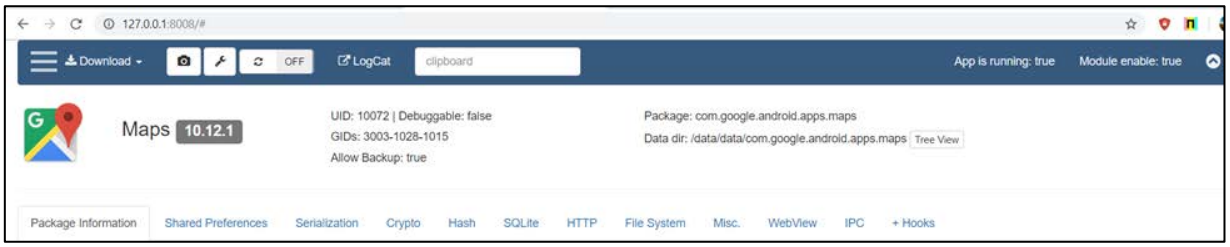
Εικόνα 6.26: Επιλογή USB debugging.

Αφού το κινητό συνδεθεί με τον ηλεκτρονικό υπολογιστή ανοίγουμε το περιβάλλον του Command Prompt και καταχωρούμε την εντολή "adb forward tcp:8008 tcp:8008" με σκοπό να ενεργοποιηθεί η σύνδεση των δύο συσκευών στην πόρτα 8008.



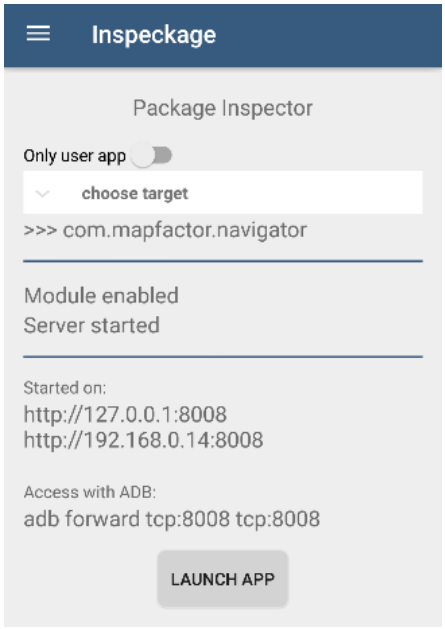
Εικόνα 6.27: Εκτέλεση σύνδεσης μέσα από το Command Prompt.

Αφού ενεργοποιηθεί η σύνδεση επιλέγουμε το φυλλομετρητή Google Chrome και πληκτρολογούμε στη γραμμή σελίδας την http://127.0.0.1:8008. Με αυτό τον τρόπο ενεργοποιείται το πρόγραμμα μέσω υπολογιστή.



Εικόνα 6.28: Παρουσίαση του γραφικού περιβάλλοντος του Inspeckage μέσω φυλλομετρητή .

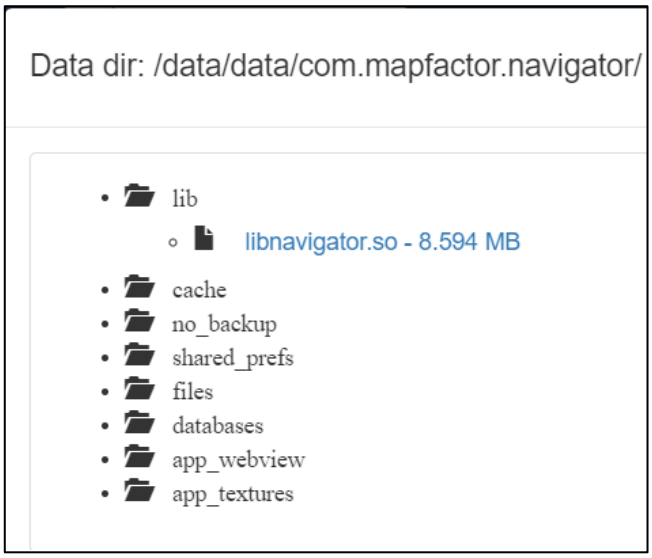
Για να ξεκινήσει η ανάλυση μίας εφαρμογής, η οποία έχει επιλεχθεί μέσα από το κομβίο "choose target", επιλέγουμε το κομβίο "Launch App" από την εφαρμογή του Inspeckage στο κινητό τηλέφωνο.



Εικόνα 6.29: Παρουσίαση του γραφικού περιβάλλοντος της εφαρμογής του Inspeckage.

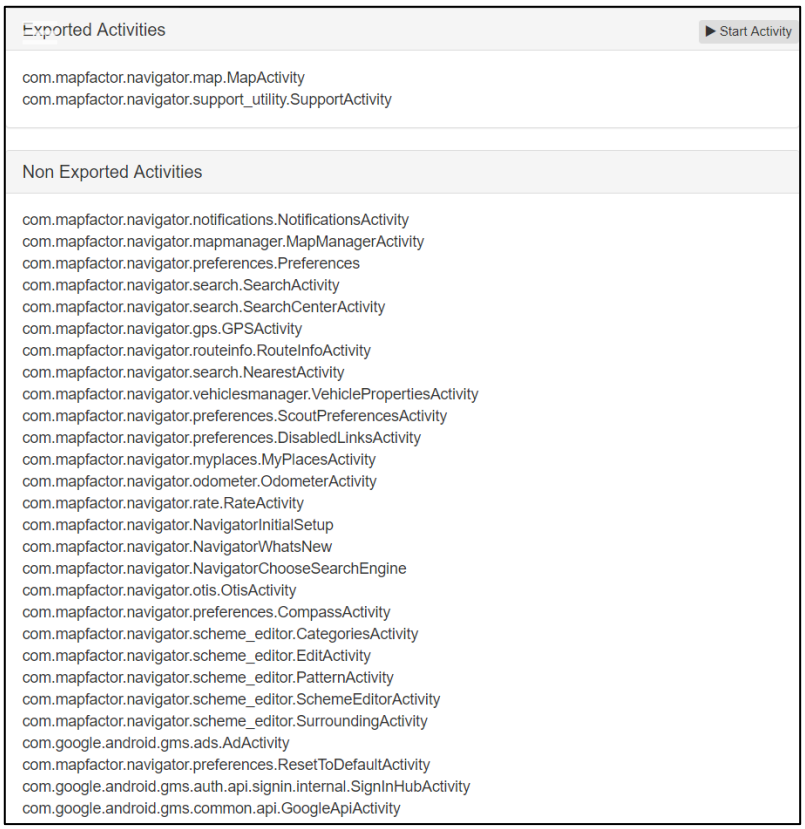
Με την πρόσβαση στο περιβάλλον της εφαρμογής, μέσω του Chrome, βλέπουμε τις βασικές πληροφορίες μίας εφαρμογής, όπως για παράδειγμα την έκδοση της εφαρμογής, τους μοναδικούς αριθμούς UID και GIDs και το αν είναι ή όχι debuggable μια εφαρμογή. Επίσης παρουσιάζονται όλες οι λειτουργίες και πληροφορίες που αναφέρθηκαν πιο πάνω κατά την παρουσίαση του προγράμματος δυναμικής ανάλυσης Inspeckage.

Μέσω του Inspeckage μπορούμε να δούμε ποια δεδομένα «φορτώνονται» κατά την εκκίνηση της εφαρμογής. Τα δεδομένα αυτά είναι ορατά μέσω αρχείων τύπου xml. Από την επιλογή «Tree View» μπορούμε να δούμε μια λίστα με τα directories της εφαρμογής.



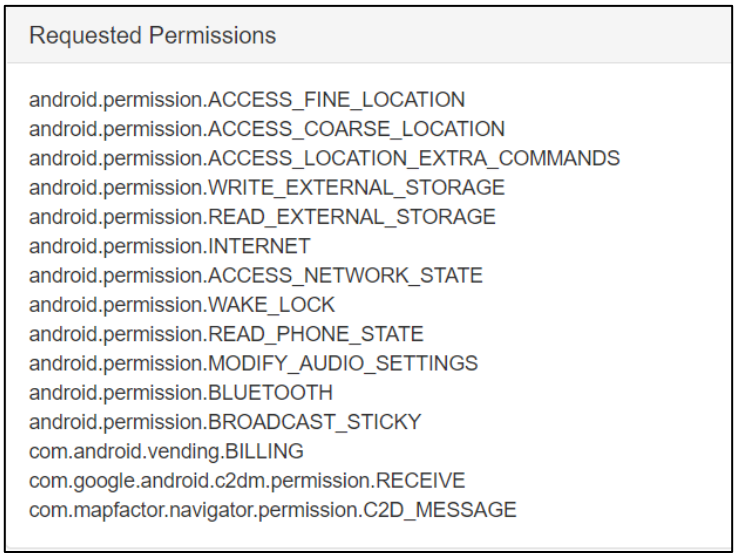
Εικόνα 6.30: Παρουσίαση των Directories μέσω του Tree View της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.

Η επόμενη εικόνα 6.30 μας δείχνει τις Exported και τις μη Exported διεργασίες της εφαρμογής και από το κουμπί Start Activity μπορούμε να ενεργοποιήσουμε όποια επιθυμούμε και να δούμε πώς θα συμπεριφερθεί η εφαρμογή.



Εικόνα 6.31: Παρουσίαση των εξαγόμενων και μη διεργασιών της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.

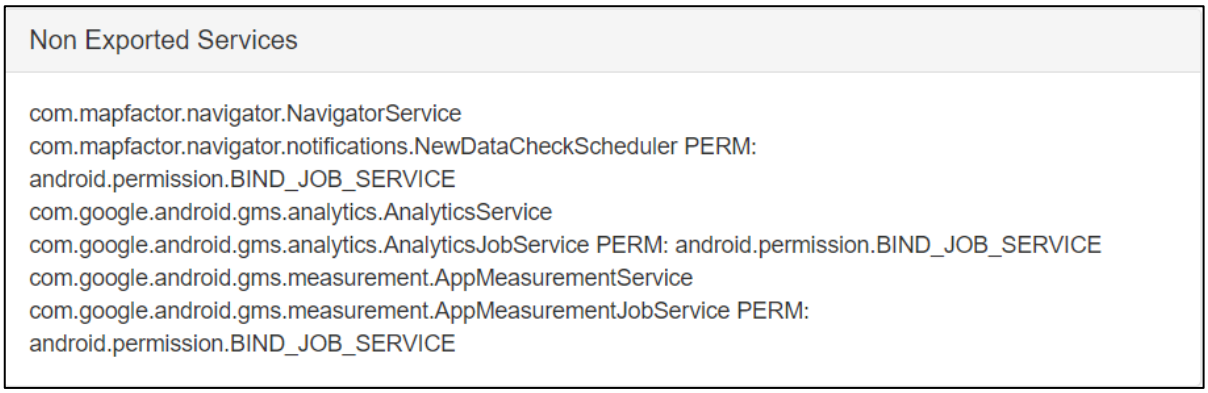
Παρουσιάζονται επίσης όλα τα δικαιώματα που χρησιμοποιεί η εφαρμογή κατά την εκτέλεσή της.



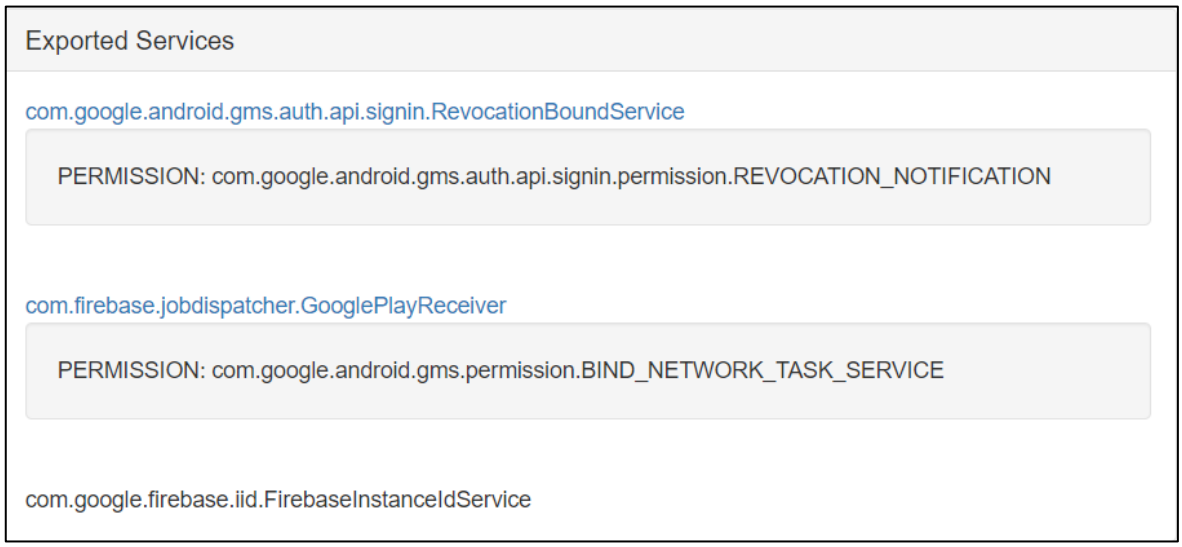
Εικόνα 6.32: Παρουσίαση των απαιτούμενων αδειών για την εγκατάσταση της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.

Η υπηρεσία (service) είναι ένα στοιχείο εφαρμογής (application component) που μπορεί να εκτελεί εργασίες στο παρασκήνιο και δεν παρέχει διεπαφή χρήστη. Ένα άλλο στοιχείο της εφαρμογής μπορεί να ξεκινήσει μια υπηρεσία και συνεχίζει να εκτελείται στο παρασκήνιο, ακόμη και αν ο χρήστης μεταβαίνει σε άλλη εφαρμογή. Επιπρόσθετα, ένα στοιχείο μπορεί να δεσμεύσει μια υπηρεσία για να αλληλοεπιδράσει μαζί του και να πραγματοποιήσει ακόμη και επικοινωνία μεταξύ διαδικασιών (IPC). Για παράδειγμα, μια υπηρεσία μπορεί να χειριστεί συναλλαγές δικτύου, να παίξει μουσική, να εκτελέσει I/O αρχείων ή να αλληλοεπιδράσει με έναν παροχέα περιεχομένου, όλα από το παρασκήνιο. Στις εικόνες 6.33 και 6.34 μπορούμε να διακρίνουμε τις εξαγόμενες και μη υπηρεσίες της εφαρμογής όπως επίσης και τις άδειες που τους παραχωρούν το δικαίωμα να τρέχουν. Μία εξαγόμενη υπηρεσία είναι η υπηρεσία εκτελεί κάποια λειτουργία που είναι αξιοσημείωτη για τον χρήστη, δηλαδή ο χρήστης μπορεί να την παρατηρήσει. Για παράδειγμα, μια εφαρμογή ήχου θα χρησιμοποιεί μια υπηρεσία για την αναπαραγωγή ενός ηχητικού κομματιού και ο χρήστης θα μπορεί να ακούσει τον ήχο. Οι υπηρεσίες αυτές πρέπει να εμφανίζουν μια ειδοποίηση και συνεχίζουν να εκτελούνται ακόμα και όταν ο χρήστης δεν αλληλοεπιδρά με την εφαρμογή.

Στον αντίποδα οι μη εξαγόμενες υπηρεσίες ή υπηρεσίες παρασκηνίου, εκτελούν μια ενέργεια που δεν παρατηρείται άμεσα από το χρήστη. Για παράδειγμα, εάν μια εφαρμογή χρησιμοποίησε μια υπηρεσία για να συμπιέσει το αποθηκευτικό χώρο της.



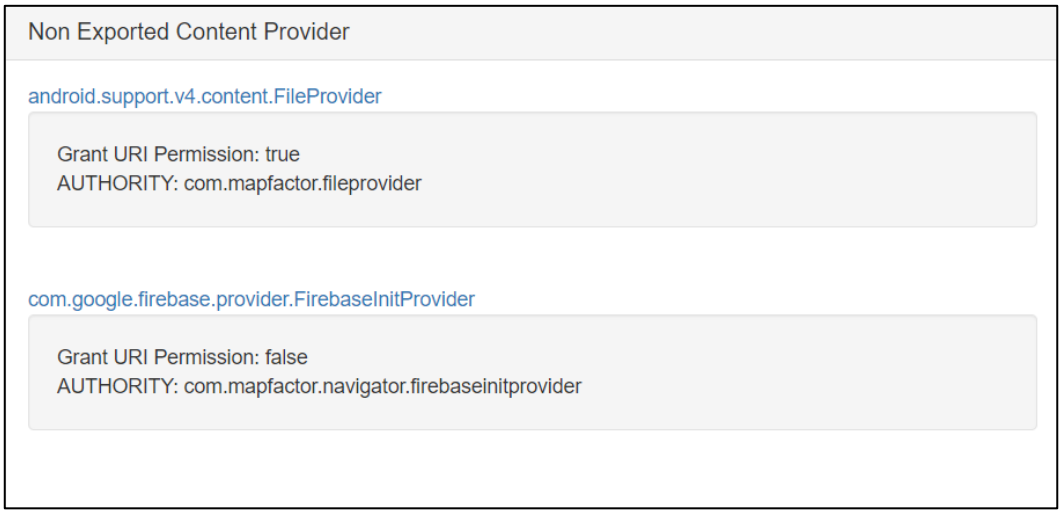
Εικόνα 6.33: Παρουσίαση των μη εξαγόμενων υπηρεσιών της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.



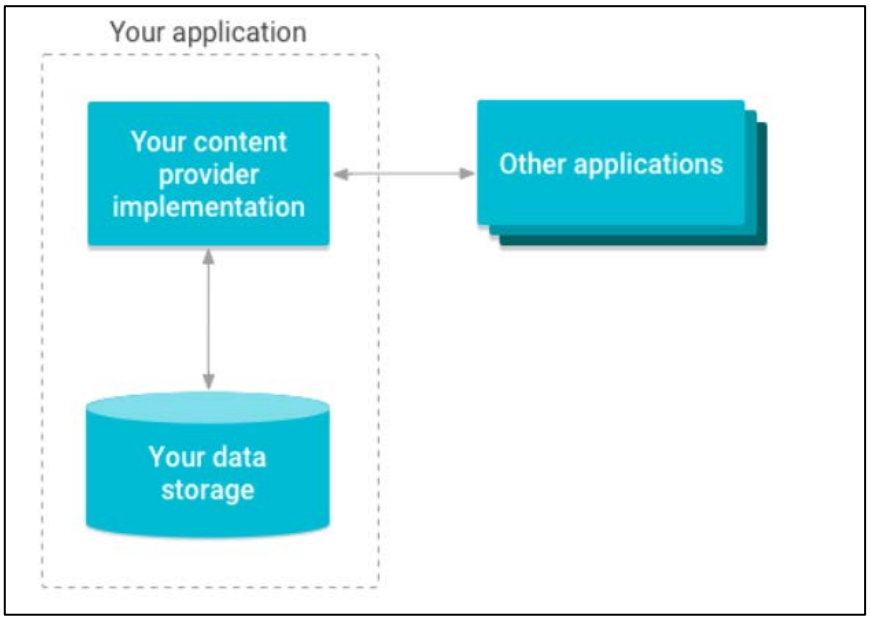
Εικόνα 6.34: Παρουσίαση των εξαγόμενων υπηρεσιών της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.

Στη συνέχεια μπορούμε να πάρουμε πληροφορίες σχετικά με τους μη εξαχθέντες παροχείς περιεχομένου για την εφαρμογή. Οι πάροχοι περιεχομένου μπορούν να βοηθήσουν μια εφαρμογή να διαχειριστεί την πρόσβαση σε δεδομένα που αποθηκεύονται από μόνα τους, αποθηκευμένα από άλλες εφαρμογές και να παρέχει έναν τρόπο να μοιράζονται δεδομένα με άλλες εφαρμογές [46]. Ενσωματώνουν τα δεδομένα και παρέχουν μηχανισμούς για τον καθορισμό της ασφάλειας των δεδομένων. Οι πάροχοι περιεχομένου είναι η τυπική διασύνδεση που συνδέει δεδομένα σε μία διαδικασία με κώδικα που εκτελείται σε άλλη διαδικασία. Η εφαρμογή ενός παρόχου περιεχομένου έχει πολλά πλεονεκτήματα. Το πιο σημαντικό είναι ότι μπορείτε να διαμορφώσετε

έναν παροχέα περιεχομένου για να επιτρέψετε σε άλλες εφαρμογές να έχουν ασφαλή πρόσβαση και να τροποποιούν τα δεδομένα της εφαρμογής μας.



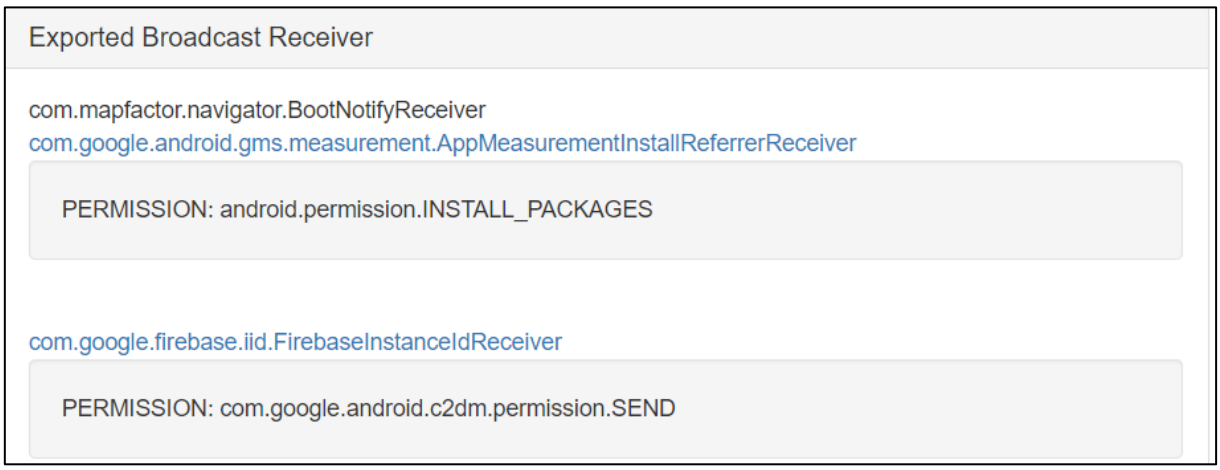
Εικόνα 6.35: Παρουσίαση των μη εξαγόμενων παροχέων περιεχομένου της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.



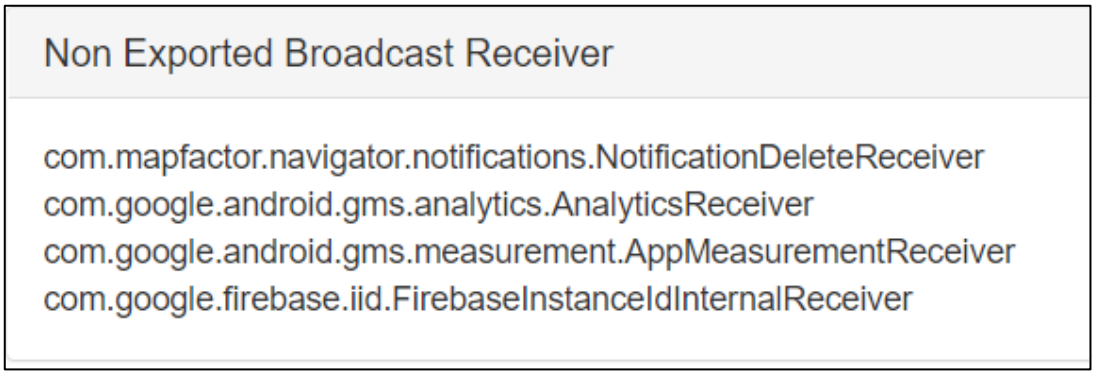
Εικόνα 6.36: Επισκόπηση του τρόπου με τον οποίο οι πάροχοι περιεχομένου διαχειρίζονται την πρόσβαση στην αποθήκευση [46].

Επιπλέον λαμβάνουμε πληροφορίες σχετικά με τους λήπτες εκπομπής μηνυμάτων. Οι εφαρμογές Android μπορούν να στέλνουν ή να λαμβάνουν μηνύματα εκπομπής από το σύστημα Android και

άλλες εφαρμογές Android, παρόμοια με το μοτίβο σχεδιασμού δημοσίευσης-εγγραφής. Αυτές οι εκπομπές αποστέλλονται όταν συμβαίνει κάποιο γεγονός ενδιαφέροντος [47]. Για παράδειγμα, το σύστημα Android πραγματοποιεί εκπομπές μηνυμάτων όταν λαμβάνουν χώρα διάφορα συμβάντα του συστήματος, όπως όταν το σύστημα εκκινήσει ή η συσκευή ξεκινήσει να φορτίζει. Οι εφαρμογές μπορούν επίσης να στείλουν προσαρμοσμένες εκπομπές, για παράδειγμα, να ειδοποιήσουν άλλες εφαρμογές για κάτι που μπορεί να τους ενδιαφέρουν (για παράδειγμα, έχουν ληφθεί κάποια νέα δεδομένα). Οι εφαρμογές μπορούν να εγγραφούν για να λαμβάνουν συγκεκριμένες εκπομπές. Όταν αποστέλλεται μια εκπομπή, το σύστημα δρομολογεί αυτόματα τις εκπομπές σε εφαρμογές που έχουν εγγραφεί για να λαμβάνουν αυτόν τον συγκεκριμένο τύπο εκπομπής. Σε γενικές γραμμές, οι εκπομπές μπορούν να χρησιμοποιηθούν ως σύστημα ανταλλαγής μηνυμάτων μεταξύ των εφαρμογών και εκτός της κανονικής ροής χρηστών.



Εικόνα 6.37: Παρουσίαση των εξαγόμενων ληπτών σημάτων εκπομπής της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.

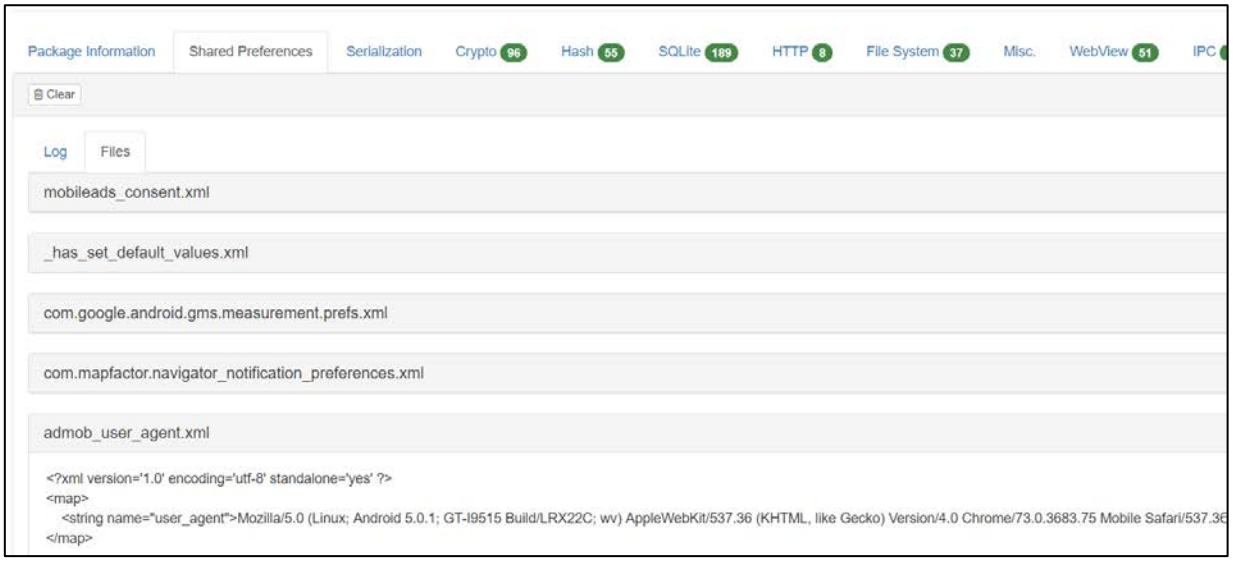


Εικόνα 6.38: Παρουσίαση των μη εξαγόμενων ληπτών σημάτων εκπομπής της εφαρμογής MapFactor GPS Navigation, μέσω του Inspeckage.

Στη συνέχεια θα δούμε παραδείγματα κάποιων διαρροών προσωπικών και μη δεδομένων μέσα από τη χρήση του προγράμματος Inspeckage το οποίο εκτελεί δυναμική ανάλυση στην εφαρμογή μας. Μέσω λοιπόν, του Shared Preferences και εξετάζοντας τα Files παρατηρήσαμε ότι το πρόγραμμα πλοήγησης Navigator εξάγαγε κάποια προσωπικά και μη δεδομένα από τη συσκευή όπως για παράδειγμα:

- το είδος του πυρήνα,
- την έκδοση του λογισμικού Android που χρησιμοποιούμε,
- το μοντέλο της συσκευής μας,
- το αποτύπωμά της συσκευής μας,
- Η πλατφόρμα που χρησιμοποιεί το πρόγραμμα περιήγησης (AppleWebKit/537.36),
- Λεπτομέρειες πλατφόρμας περιήγησης (KHTML, like Gecko),
- Το πρόγραμμα περιήγησης και την έκδοση του.

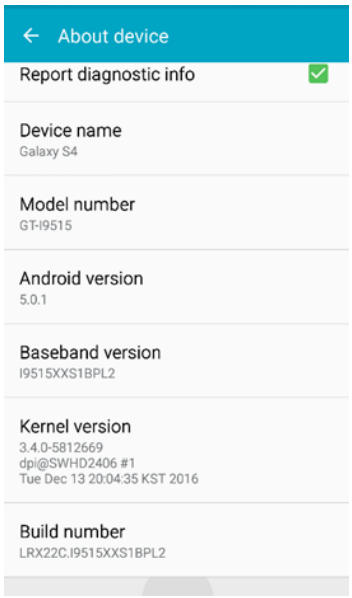
Τα δεδομένα αποστέλνονται στο admob. Το AdMob είναι μια εταιρεία διαφήμισης για κινητά που ιδρύθηκε από τον Omar Hamoui το 2006. Το όνομα AdMob είναι στην ουσία η συντομογραφία του "advertising on mobile" ή "διαφήμιση στο κινητό".



Εικόνα 6.39: Παρουσίαση προσωπικών δεδομένων που διαρρέουν μέσω της εφαρμογής MapFactor GPS Navigation, μέσα από το “Shared Preferences” του Inspeckage.

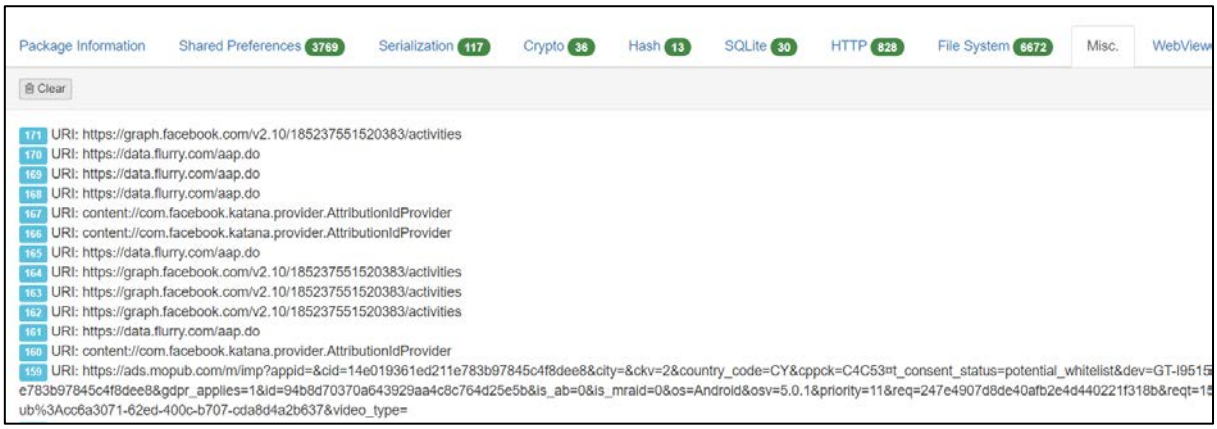
Το Google AdMob διευκολύνει τους προγραμματιστές να κερδίζουν χρήματα από τις εφαρμογές τους για κινητά με διαφημίσεις υψηλής ποιότητας. Το AdMob μεγιστοποιεί την αξία κάθε εμφάνισης συνδυάζοντας την παγκόσμια ζήτηση διαφημιζόμενων, τις καινοτόμες μορφές διαφημίσεων και την προηγμένη τεχνολογία δημιουργίας εσόδων από εφαρμογές. Οι διαφημίσεις

δημιουργούνται και πληρώνονται από διαφημιζόμενους που θέλουν να προωθήσουν τα προϊόντα ή τις υπηρεσίες τους σε χρήστες εφαρμογών. Το AdMob συνεργάζεται με διαφημιζόμενους που πληρώνουν για την προβολή διαφημίσεων που σχετίζονται με τους χρήστες.



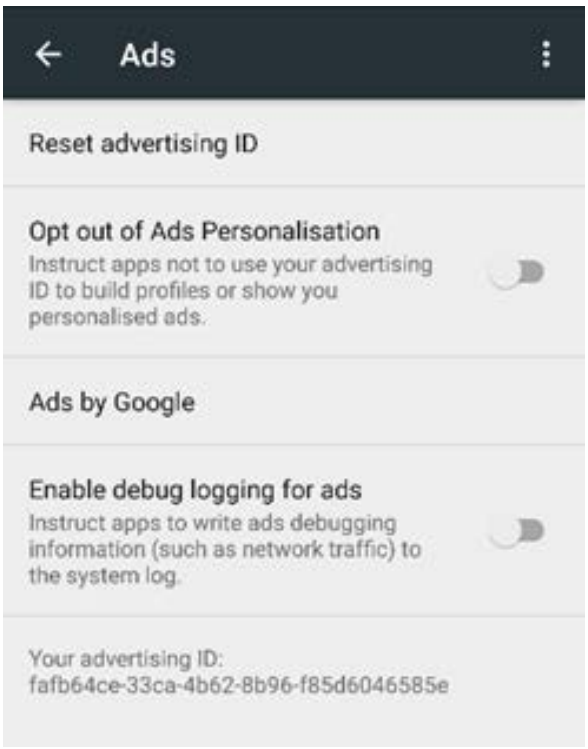
Εικόνα 6.40: Παρουσίαση στοιχείων συσκευής Samsung S4 που μπορεί να αποτελέσουν και προσωπικά δεδομένα.

Στη πιο κάτω εικόνα 6.41, η οποία προέρχεται από τον τομέα Misc. (διάφορα), μπορούμε να διακρίνουμε 3 από τους Third parties trackers με τους οποίους, στη συγκεκριμένη περίπτωση, η εφαρμογή MAPS.ME επικοινωνεί ανταλλάσσοντας δεδομένα. Η ανταλλαγή δεδομένων «εγκρίθηκε», όπως προαναφέρθηκε, μέσω των άδειών που ο χρήστης εκχώρησε στην εφαρμογή μη γνωρίζοντας ούτε με ποιους επικοινωνεί αλλά ούτε και το είδος των δεδομένων που πρόκειται να ανταλλαχθεί μεταξύ τους. Στην εικόνα αυτή λοιπόν βλέπουμε την εφαρμογή να επικοινωνεί με τομείς όπως το flurry.com, το facebook.com και το ads.mopub.com. Με τον τελευταίο τομέα παρατηρούμε ότι ανταλλάσσει πληροφορία όπως τη χώρα στην οποία βρίσκεται η συσκευή, το μοντέλο της συσκευής, το λειτουργικό που τρέχει η συσκευή και την έκδοση του.



Εικόνα 6.41: Παρουσίαση προσωπικών δεδομένων που διαρρέουν μέσω της εφαρμογής MAPS.ME και τομέων επικοινωνίας της, μέσα από το "Misc." του Inspeckage.

Επίσης και στις εικόνες 6.43 και 6.44, οι οποίες προέρχονται από το Shared Preferences, βλέπουμε ότι υπάρχει επικοινωνία με τους τομείς appsflyer.com και flurry.com και διαρροή του GAID (Google Advertising ID) ως "advertiserId" και "advertising_id". Το αναγνωριστικό Διαφήμισης της Google είναι ένα μοναδικό αναγνωριστικό-μοναδικός αριθμός μεγέθους 32-bit και το συναντάμε σε όλα τα κινητά με λειτουργικό Android που έχουν εγκαταστήσει το Google Play Store. Επιτρέπει σε κινητές εφαρμογές που εκτελούνται στο λειτουργικό σύστημα Android, να συλλέγουν δεδομένα σχετικά με συγκεκριμένους πελάτες, προκειμένου να βελτιωθεί τόσο η εξατομίκευση όσο και η ανάλυση των πελατών, με σκοπό να βοηθήσει τους διαφημιστές να στοχεύσουν με τις διαφημίσεις τους, πιθανούς πελάτες, σε περιβάλλον εφαρμογών για κινητά και να με οικονομικά αποδοτικό τρόπο. Το Google Advertising ID παρέχει στους προγραμματιστές ένα απλό και τυποποιημένο σύστημα για να συνεχίσουν να δημιουργούν έσοδα από τις εφαρμογές τους. Επιτρέπεται όμως στους χρήστες να επαναφέρουν το αναγνωριστικό τους ή να αποκλείσουν τις εξατομικευμένες διαφημίσεις (παλαιότερα γνωστές ως διαφημίσεις βάσει ενδιαφέροντος) στις εφαρμογές του Google Play. Το αναγνωριστικό αυτό και η δυνατότητα αναπροσαρμογής του δημιουργήθηκε με σκοπό την ανωνυμοποίηση των προσωπικών αναγνωριστικών ενός φυσικού προσώπου (αν και, με βάση το νομικό χαρακτηρισμό των ανώνυμων δεδομένων, η χρήση του GAID δεν συνιστά ανωνυμοποίηση).



Εικόνα 6.42: Παρουσίαση Google Advertising ID της συσκευής Samsung S4.

appsflyer-data.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <int name="appsflyerConversionDataRequestRetries" value="0" ></int>
   <long name="AppsFlyerTimePassedSincePrevLaunch" value="1555069363484" ></long>
   <int name="appsFlyerCount" value="16" ></int>
   <string name="sentSuccessfully">true</string>
   <int name="versionCode" value="1907" ></int>
   <string name="referrer">utm_source=google-play&utm_medium=organic</string>
   <string name="prev_event_value">{"action":"download"}</string>
   <long name="prev_event_timestamp" value="1553330643790" ></long>
   <string name="AF_INSTALLATION">1551302220949-8219539129563759837</string>
   <string name="appsFlyerFirstInstall">2019-02-27_211828+0000</string>
   <string name="savedProperties">{"advertiserId":"fafb64ce-33ca-4b62-8b96-f85d6046585e","logLe
8219539129563759837","AF_REFERRER":"utm_source=google-play&utm_medium=organic","KSAp
   <int name="appsFlyerInAppEventCount" value="8" ></int>
   <string name="prev_event_name">Downloader_Map_action_finished</string>
</map>
```

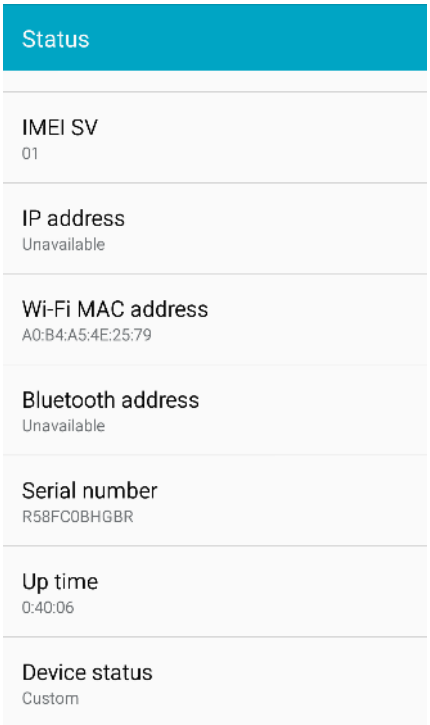
Εικόνα 6.43: Παρουσίαση προσωπικών δεδομένων (GAID) που διαρρέουν στο τομέα appsflyer.com μέσα από το "Shared Preferences" του Inspeckage.

FLURRY_SHARED_PREFERENCES.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <string name="advertising_id">fafb64ce-33ca-4b62-8b96-f85d6046585e</string>
   <string name="com.flurry.sdk.api_key">FP4MRV3698TD7JYF684V</string>
   <boolean name="ad_tracking_enabled" value="false" ></boolean>
   <boolean name="com.flurry.sdk.previous_successful_report" value="true" ></boolean>
   <long name="com.flurry.sdk.initial_run_time" value="1551302313613" ></long>
</map>
```

Εικόνα 6.44: Παρουσίαση προσωπικών δεδομένων (GAID) που διαρρέουν στο τομέα flurry.com μέσα από το "Shared Preferences" του Inspeckage.

Στον ίδιο πεδίο έρευνας του Inspeckage, το Shared Preferences, εντοπίσαμε διαρροές όπως είναι και η MAC διεύθυνση της συσκευής μας. Μια διεύθυνση MAC είναι ένας μοναδικός προσδιοριστής που αποδίδεται από τον κατασκευαστή σε ένα κομμάτι του υλικού του δικτύου.



Εικόνα 6.45: Παρουσίαση προσωπικών στοιχείων όπως την MAC Address του Samsung S4.

mytracker_prefs.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <string name="appVersionName">8.6.3-Google</string>
   <boolean name="preinstallRead" value="true" ></boolean>
   <string name="referrer">utm_source=google-play&utm_medium=organic</string>
   <long name="customEventsSkipped" value="0" ></long>
   <long name="rootedCheckTimestamp" value="1555013827825" ></long>
   <string name="mac">A0:B4:A5:4E:25:79</string>
   <string name="mrgsDeviceId">7a8e0a1893e4a85a97b9b7ea09f2f4a3</string>
   <string name="appId">36449940344140889901</string>
   <boolean name="isRooted" value="true" ></boolean>
   <long name="eventTimestampBase" value="1555013896" ></long>
   <string name="appVersion">1907</string>
   <long name="lastStopTimeStampSec" value="0" ></long>
   <boolean name="apiReferrerSent" value="true" ></boolean>
   <boolean name="referrerSent" value="true" ></boolean>
</map>
```

Εικόνα 6.46: Παρουσίαση προσωπικών δεδομένων (MAC Address) που διαρρέουν στο τομέα flurry.com, μέσα από το "Shared Preferences" του Inspeckage.

Κεφάλαιο 7
Αποτελέσματα-Συμπεράσματα

Στο προηγούμενο Κεφάλαιο παρουσιάστηκε η μεθοδολογία με την οποία προσεγγίσαμε την ανάλυση των εφαρμογών μας, παρουσιάζοντας τον τρόπο που μία δυναμική ανάλυση πραγματοποιείται αλλά και τα μέσα με τα οποία διεκπεραιώθηκε. Επίσης παρουσιάστηκε ο τρόπος με τον οποίο εξήχθησαν τα αποτελέσματα. Στο παρόν Κεφάλαιο θα παρουσιαστούν αναλυτικά τα αποτελέσματά μας προκειμένου να καταλήξουμε σε ασφαλή συμπεράσματα για το βαθμό διασφάλισης των δεδομένων προσωπικού χαρακτήρα, μέσα από τις πέντε εφαρμογές που αναλύθηκαν.

Αρχικά παρουσιάζεται η επικοινωνία με διάφορους τομείς, που η κάθε εφαρμογή επικοινώνησε, είτε για σκοπούς διαφήμισης, είτε για σκοπούς ανταλλαγής πληροφορίας στα πλαίσια της ορθής λειτουργίας της. Τα αποτελέσματα αυτά εξήχθησαν συνολικά μέσα από την χρήση των πέντε εφαρμογών στα πέντε κινητά τηλέφωνα. Τα δεδομένα εξάχθηκαν μέσα από το Lumen Privacy Monitor και το Inspeckage. Οι εφαρμογές αριθμούνται από το 1 έως το 5 ως εξής:

1. Google Maps (v 10.12.1)
2. Sygic GPS Navigation & Maps (17.7.0)

3. TomTom GPS Navigation - Traffic Alerts & Maps (v 1.17.1)
4. MAPS.ME (v 9.0.7)
5. MapFactor GPS Navigation Maps (v 4.0.109)

	Εφαρμογή				
Τομέας Διαδικτύου	**1**	**2**	**3**	**4**	**5**
app-measurement.com	✓				
google.com	✓				✓
googleapis.com	✓				✓
googleusercontent.com	✓				✓
gstatic.com	✓				✓
youtube.com	✓				
appsflyer.com		✓		✓	
crashlytics.com		✓	✓	✓	
facebook.com		✓		✓	
foursquare.com		✓			
infinario.com		✓			
sygic.com		✓			
uber.com		✓			
windows.net		✓			✓
adjust.com			✓		
tomtom.com			✓		
flurry.com				✓	
maps.me				✓	
mopub.com				✓	
my.com				✓	
pushwoosh.com				✓	
mapswithme.com				✓	
mail.ru				✓	
fbcdn.net				✓	
booking.com				✓	
mapfactor.com					✓
google-analytics.com	✓	✓			✓
googlesyndication.com					✓
googleadservices.com					✓
akamaized.net		✓			
Twitter.com		✓	✓	✓	
d30x8mtr3hjnzo.cloudfront.net				✓	
doubleclick.net				✓	✓

Πίνακας 7.1: Το σύνολο των τομέων που οι εφαρμογές μας επικοινωνούν.

Οι τομείς οι οποίοι παρουσιάζονται, αποτελούν τους βασικούς-κεντρικούς τομείς και όχι τους υποτομείς με τους οποίους μπορεί να επικοινώνησε μία εφαρμογή. Για παράδειγμα το facebook.com αντιπροσωπεύει τα graph.facebook.com, api.facebook.com, το lithium.facebook.com και αναλόγως συσκευής και λειτουργικού πιθανόν και άλλους υποτομείς. Παρατηρούμε ότι 11 τομείς επικοινωνούν με περισσότερες από μία εφαρμογές. Συγκεκριμένα 8 τομείς επικοινωνούν με 2 εφαρμογές και 3 τομείς επικοινωνούν με τρεις εφαρμογές παράλληλα. Παρατηρώντας λοιπόν

ποιες άδειες αποκτά ο κάθε τομέας, από την κάθε εφαρμογή με την οποία επικοινωνεί, καταλήγουμε στο συμπέρασμα ότι πράγματι πιθανών να γίνεται συλλογή υπέρμετρης πληροφορίας από κάποιους όπως είναι το crashlytics.com, το google-analytics.com ή ακόμα και το twitter.com.

Στη συνέχεια παρουσιάζονται οι τομείς οι οποίοι αξιολογήθηκαν από την εφαρμογή Lumen Privacy Monitor και από τις ιστοσελίδες https://whotracks.me/trackers/google_users.html και https://trustedsource.org/sources/index.pl?do=feedback&subdo=url&action=checksingle της McAfee, ως ATS (Advertising or Tracking Services) ή τομείς τρίτων.

	Εφαρμογή				
Advertising or Tracking Services	**1**	**2**	**3**	**4**	**5**
app-measurement.com	✓				
google.com	✓				✓
appsflyer.com		✓		✓	
crashlytics.com		✓	✓	✓	
foursquare.com		✓			
windows.net		✓			✓
adjust.com			✓		
facebook.com		✓		✓	
flurry.com				✓	
mopub.com				✓	
pushwoosh.com				✓	
google-analytics.com	✓	✓			✓
googlesyndication.com					✓
googleadservices.com					✓
akamaized.net		✓			
gstatic.com	✓				✓
infinario.com		✓			
fbcdn.net				✓	
d30x8mtr3hjnzo.cloudfront.net				✓	
mail.ru				✓	
googleusercontent.com	✓				✓
googleapis.com	✓				✓
Twitter.com		✓	✓	✓	
doubleclick.net				✓	✓

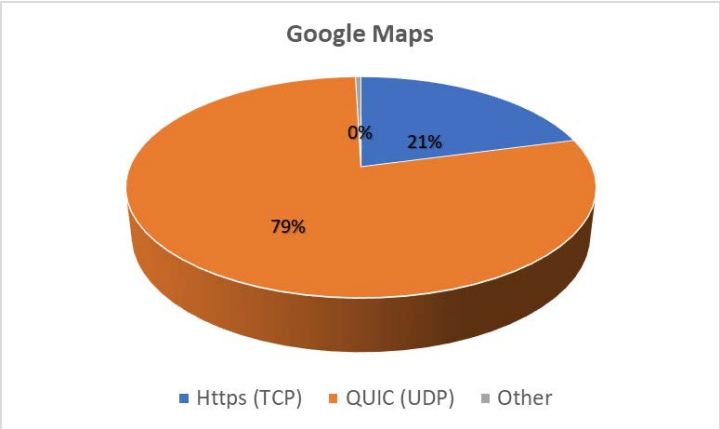
Πίνακας 7.2: Το σύνολο των τομέων αξιολογήθηκαν ως ATS.

Σύμφωνα με την πολιτική απορρήτου και των πέντε εφαρμογών, αναφέρεται ότι κατά την εγκατάσταση της εφαρμογής, είτε μέσω του Google Play ή άλλων καταστημάτων, συμφωνούμε και συνάπτουμε τη Συμφωνία Άδειας Τελικού Χρήστη (End User Licence Agreement-EULA). Σύμφωνα με την EULA, η εταιρεία είναι υποχρεωμένη να μας παρέχει τις Υπηρεσίες που αντιστοιχούν στις συγκεκριμένες λειτουργίες της συγκεκριμένης εφαρμογής. Οποιαδήποτε

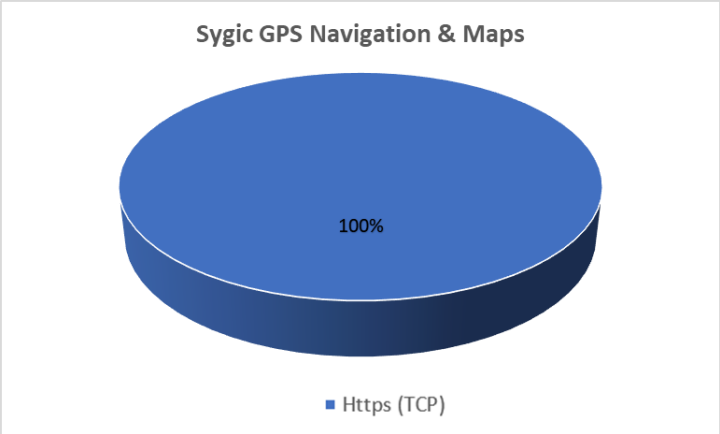
επεξεργασία που είναι απαραίτητη για την εκπλήρωση των υποχρεώσεών της από τη EULA, θεωρείται ξεχωριστός σκοπός επεξεργασίας και δεν υπόκειται σε χωριστή συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα. Γενικά, συλλέγονται τα προσωπικά μας δεδομένα απευθείας από εμάς, δηλαδή την πηγή, για παράδειγμα όταν αποφασίσουμε να κατεβάσουμε την εφαρμογή, να κάνουμε μια αγορά, να καταχωρήσουμε το λογαριασμό μας, να συμπληρώσουμε τη φόρμα συγκατάθεσης μάρκετινγκ, να επικοινωνήσουμε ή να χρησιμοποιήσετε τις Υπηρεσίες της εταιρείας. Η παροχή προσωπικών δεδομένων στην εταιρεία μπορεί να γίνει άμεσα, για παράδειγμα με τη συμπλήρωση της φόρμας εγγραφής, παραγγελίας ή συγκατάθεσης, αλλά μπορεί επίσης να συμβεί έμμεσα, για παράδειγμα, χρησιμοποιώντας τις εφαρμογές της, οι οποίες πρέπει να συλλέξουν δεδομένα για να λειτουργήσουν και για να σας παράσχουν με τις αιτούμενες υπηρεσίες. Για παράδειγμα, η εταιρεία αναφέρει «όταν χρησιμοποιείτε τις εφαρμογές πλοήγησης ή εντοπισμού, πρέπει να συλλέγουμε την ακριβή τοποθεσία, την ταχύτητα, πορείες κλπ.». Η παροχή προσωπικών δεδομένων από εμάς είναι εθελοντική ή παρουσιάζει είτε την απαίτηση σύναψης μιας σύμβασης είτε μιας συμβατικής απαίτησης (EULA). Ορισμένες επεξεργασίες δεδομένων προσωπικού χαρακτήρα ενδέχεται να απαιτούνται από το νόμο ή να απαιτούνται από την εταιρεία προκειμένου να επιδιώξει την σωστή της λειτουργία.

Αξιοσημείωτο όμως αποτελεί το γεγονός ότι καμία εφαρμογή δεν αναφέρει τους τομείς επικοινωνίας για την διεκπεραίωση των ανωτέρω λειτουργιών, πέραν των μητρικών τομέων, στα πλαίσια της διαφάνειας κατά την οποία, τα δεδομένα προσωπικού χαρακτήρα διεκπεραιώνονται με σεβασμό της δικαιοσύνης και της διαφάνειας έναντι του υποκειμένου των δεδομένων και με την τήρηση της απαίτησης για θεμιτό λόγο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Το υποκείμενο των δεδομένων, είτε προσωπικών είτε όχι, οφείλει να γνωρίζει και ποια δεδομένα του τυχαίνουν επεξεργασίας αλλά και από ποιους, με σκοπό να ασκήσει εάν και εφόσον το απαιτεί τα δικαιώματα του ως Ευρωπαίος πολίτης που υπάγεται στο γενικό κανονισμό για την προστασία δεδομένων (ΕΕ) 679/2016 (GDPR).

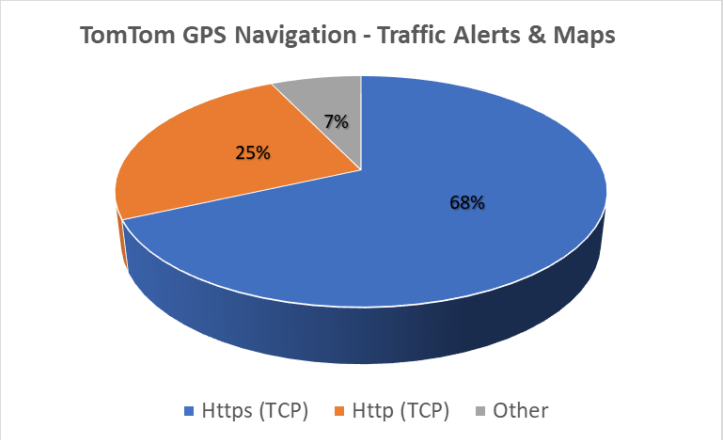
Στη συνέχεια παρουσιάζονται τα ποσοστά χρήσης των πρωτοκόλλων διαδικτύου Https, Http και Quic που η κάθε εφαρμογή χρησιμοποίησε κατά την επικοινωνία που είχε με τους τομείς που παρουσιάστηκαν στον Πίνακα 7.1. Τα αποτελέσματα αυτά εξάχθηκαν συνολικά μέσα από την χρήση των πέντε εφαρμογών στα τέσσερα κινητά τηλέφωνα. Τα δεδομένα και τα ποσοστά της διαδικτυακής επικοινωνίας για την κάθε εφαρμογή εξάχθηκαν μέσα από το Lumen Privacy Monitor.



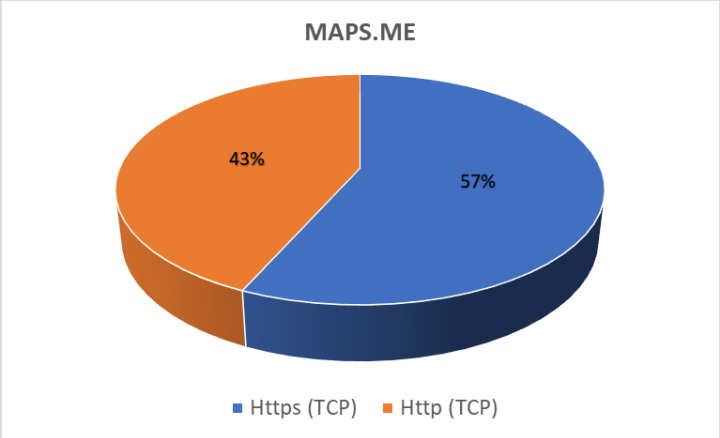
Σχήμα 7.1: Ποσοστά χρήσης πρωτοκόλλων της εφαρμογής Google Maps, μέσα από το Lumen Privacy Monitor.



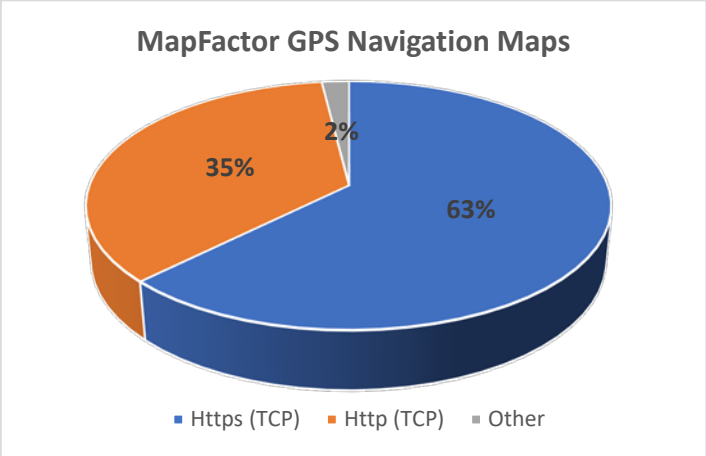
Σχήμα 7.2: Ποσοστά χρήσης πρωτοκόλλων της εφαρμογής Sygic GPS Navigation & Map, μέσα από το Lumen Privacy Monitor.



Σχήμα 7.3: Ποσοστά χρήσης πρωτοκόλλων της εφαρμογής TomTom GPS Navigation - Traffic Alerts & Maps, μέσα από το Lumen Privacy Monitor.



Σχήμα 7.4: Ποσοστά χρήσης πρωτοκόλλων της εφαρμογής MAPS.ME, μέσα από το Lumen Privacy Monitor.

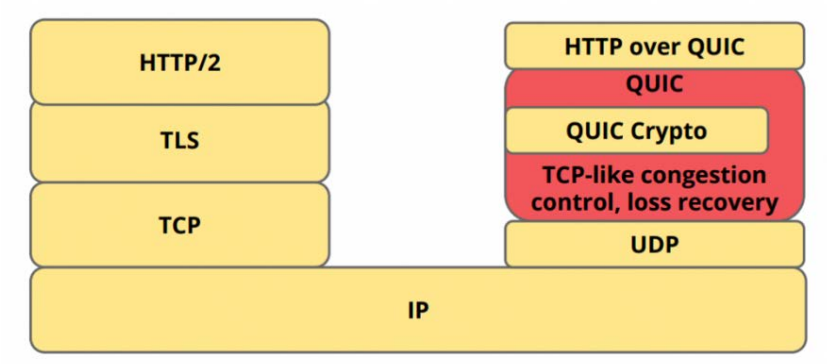


Σχήμα 7.5: Ποσοστά χρήσης πρωτοκόλλων της εφαρμογής MapFactor GPS Navigation Maps, μέσα από το Lumen Privacy Monitor.

Όπως προκύπτει, η εφαρμογή Sygic GPS Navigation & Maps αποστέλλει τα δεδομένα της κατά 100% με το ασφαλές πρωτόκολλο διαδικτύου Https. Πράγματι με την αποστολή όλων των δεδομένων, που χρησιμοποιήθηκαν σε κάθε επικοινωνία με τους τομείς, μέσα από το ασφαλές πρωτόκολλό TCP+TLS+HTTP εγγυάται στον χρήστη ότι όλα τα δεδομένα που βρίσκονται μέσα στο κανάλι επικοινωνίας δεν μπορούν να υποκλαπούν και να αναγνωριστούν όπως παρουσιάζεται και στην Εικόνα 6.24. Παρατηρείται επίσης ότι οι εφαρμογές TomTom GPS Navigation - Traffic Alerts & Maps, MAPS.ME και MapFactor GPS Navigation Maps δεν χρησιμοποιούν το Https σε όλο το εύρος των επικοινωνιών τους, γεγονός που υποδεικνύει μεγάλη πιθανότητα να εκτεθούν δεδομένα σε επιθέσεις MITM "Man in the Middle". Παρουσιάζεται επίσης σε κάποιες εφαρμογές η ποσότητα "Other", η

οποία πιθανόν να οφείλεται σε χειριστικά λάθη του χρήστη ή σε σφάλματα της εφαρμογής Lumen Privacy Monitor.

Συγχρόνως παρατηρούμε ότι η εφαρμογή Google Maps κάνει χρήση του πρωτοκόλλου Quic. Το QUIC (Quick UDP Internet Connections) είναι ένα πρωτόκολλο δικτύου επιπέδου μεταφοράς που σχεδιάστηκε από την Google [48]. Ο γενικός στόχος του είναι να μειωθεί η καθυστέρηση σε σύγκριση με εκείνη του TCP. Το QUIC είναι παρόμοιο με το TCP+TLS+HTTP/2 με τη διαφορά ότι εφαρμόζεται το UDP. Επειδή το TCP εφαρμόζεται στα χαμηλότερα επίπεδα μηχανημάτων (λειτουργικά συστήματα, firmware δρομολόγησης), οι αλλαγές στο TCP είναι σχεδόν αδύνατες δεδομένης της ποσότητας των αναβαθμίσεων που θα έπρεπε να γίνουν. Παρέχει βέβαια την ασφάλεια μέσω κρυπτογράφησης και αυθεντικοποίησης όσο και ο συνδυασμός των TCP+TLS+HTTP/2. Δεδομένου ότι το QUIC είναι χτισμένο πάνω από το UDP, δεν υφίστανται τέτοιοι περιορισμοί και μπορεί να ενσωματωθεί σε εφαρμογές κεντρικού υπολογιστή. Επομένως το QUIC φέρνει, τουλάχιστον, διπλάσια ταχύτητα σύνδεσης και μειώνει δραματικά την επίδραση της μεταβίβασης μεταξύ διαφορετικών δικτύων.



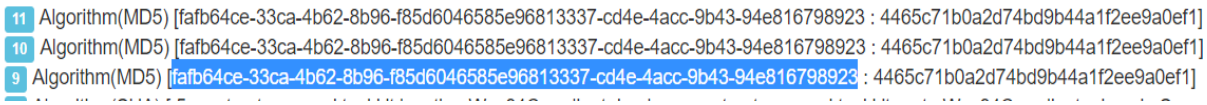
Εικόνα 7.1: Συσχέτιση λειτουργίας του TCP με το Quic [49].

Απόδειξη της χρήσης του πρωτοκόλλου TCP+TLS+HTTP μπορεί να αποτελέσει και το γεγονός ότι μέσα από την εφαρμογή Inspeckage και συγκεκριμένα τον τομέα Crypto, μπορέσαμε να εξάγουμε, τις λεπτομέρειες σχετικά με τον τρόπο που οι εφαρμογές, πλην της Google Maps, κρυπτογραφούν τα δεδομένα που αποστέλνονται μέσα από το κανάλι επικοινωνίας. Μπορέσαμε να εξάγουμε την μέθοδο κρυπτογράφησης και το είδος του κρυπτογραφικού αλγόριθμού που χρησιμοποιεί η κάθε εφαρμογή πλην της Google Maps και το παρουσιάζουμε ως ακολούθως:

Εφαρμογή	Μέθοδος Κρυπτογράφησης
Sygic GPS Navigation & Maps	AES/CBC/PKCS5Padding
TomTom GPS Navigation - Traffic Alerts & Maps	AES/GCM/No Padding
MAPS.ME	AES/CBC/PKCS5Padding
MapFactor GPS Navigation Maps	AES/CBC/PKCS5Padding

Πίνακας 7.4: Η μέθοδος κρυπτογράφησης ανά εφαρμογή.

Αξίζει να αναφερθούμε στο γεγονός ότι όλες οι εφαρμογές χρησιμοποιούσαν κρυπτογραφικούς συναρτήσεις κατακερματισμού των δεδομένων όπως για παράδειγμα η εφαρμογή TomTom GPS Navigation - Traffic Alerts & Maps στην Εικόνα 7.2.



Εικόνα 7.2: Παρουσιάζεται η διαδικασία κατακερματισμού του GAID με τον αλγόριθμο MD5, μέσα από το πεδίο "Hash" του Inspeckage.

Η παρατήρηση αυτή, της ύπαρξης των συναρτήσεων κατακερματισμού, δηλώνει ότι όλες οι εφαρμογές χρησιμοποιούν μία τεχνική «ψευδωνυμοποίησης», όπως αυτή εισήχθη ως έννοια στον GDPR, όπως αναφέρεται και στο Κεφάλαιο 3. Ουσιαστικά επιδιώκεται επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπον ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδίδονται σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, υπό την προϋπόθεση ότι οι πρόσθετες αυτές πληροφορίες τηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν αποδίδονται σε φυσικό πρόσωπο που έχει ταυτοποιηθεί ή αναγνωριστεί.

Εφαρμογή	Συνάρτηση Κατακερματισμού
Google Maps	SHA-1, MD5, SHA-256, SHA-512
Sygic GPS Navigation & Maps	SHA-1, MD5 και SHA-256
TomTom GPS Navigation - Traffic Alerts & Maps	SHA-1 και SHA-256
MAPS.ME	SHA-1 και MD5
MapFactor GPS Navigation Maps	SHA-1 και MD5

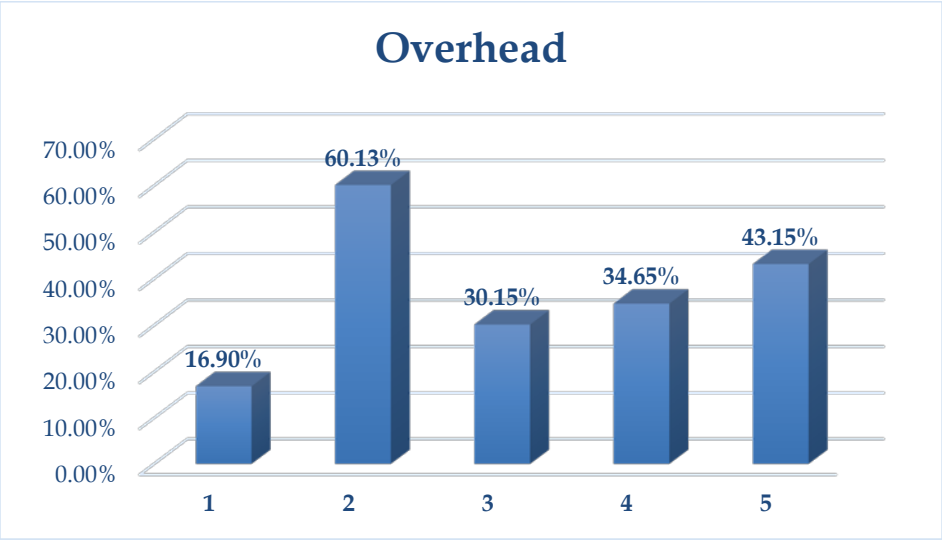
Πίνακας 7.5: Οι συναρτήσεις κατακερματισμού ανά εφαρμογή.

Ανατρέχοντας στις Πολιτικές απορρήτου της κάθε εφαρμογής παρατηρήσαμε ότι:

1. Η Google αναφέρει ότι όλα τα προϊόντα της σχεδιάζονται με ισχυρά χαρακτηριστικά ασφαλείας που προστατεύουν σε μόνιμη βάση τις πληροφορίες μας. Καταβάλλει μεγάλες προσπάθειες, για να προστατεύσει τους πελάτες και την Google από τυχόν μη εξουσιοδοτημένη πρόσβαση, παραποίηση, αποκάλυψη ή καταστροφή των πληροφοριών που έχουμε στην κατοχή μας, όπως για παράδειγμα την κρυπτογράφηση, για να διατηρήσουμε απόρρητα τα δεδομένα σας κατά τη μεταφορά τους.
2. Η Sygic αναφέρει ότι η εταιρεία είναι υποχρεωμένη να θεσπίσει μέτρα για να διασφαλιστεί το κατάλληλο επίπεδο ασφάλειας των προσωπικών δεδομένων. Παρόλο που τα μέτρα αυτά δεν απευθύνονται κατά κύριο λόγο στην επεξεργασία προσωπικών δεδομένων, ενδέχεται να απαιτηθεί η επεξεργασία των προσωπικών δεδομένων σε κάποιο βαθμό, προκειμένου να εφαρμοστούν τα μέτρα αυτά όπως για παράδειγμα κρυπτογράφηση, ψευδωνυμοποίηση, καταγραφή και δημιουργία αντιγράφων ασφαλείας, αναφορά σε σφάλματα, αναφορά παραβίασης/συμβάντων, έρευνες ασφαλείας και τεκμηρίωση, έλεγχος πρόσβασης ή και ανίχνευση βλαβερών περιεχομένων κ.λπ.
3. Η TomTom εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των Προσωπικών Δεδομένων από τυχαία ή παράνομη καταστροφή ή τυχαία απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση, ιδίως όταν η επεξεργασία συνεπάγεται τη διαβίβαση Προσωπικών Δεδομένων μέσω δικτύου και έναντι όλων των άλλων παράνομων μορφών επεξεργασία. Η TomTom το κάνει αυτό εξασφαλίζοντας ένα επίπεδο ασφάλειας που να ανταποκρίνεται στους κινδύνους που αντιπροσωπεύει η επεξεργασία και η φύση των Προσωπικών Δεδομένων που πρέπει να προστατευθούν.
4. Στην My.com λαμβάνουν τεχνικά, οργανωτικά και νομικά μέτρα, συμπεριλαμβανομένης, ενδεχομένως της κρυπτογράφησης, για να διασφαλίσουν ότι τα προσωπικά μας δεδομένα προστατεύονται από μη εξουσιοδοτημένη ή τυχαία πρόσβαση, διαγραφή, τροποποίηση, αποκλεισμό, αντιγραφή και διάδοση.
5. Τέλος η mapfactor.com αναφέρει ότι η συλλογή και η επεξεργασία των προσωπικών δεδομένων κάθε χρήστη γίνεται αποκλειστικά και μόνο στα πλαίσια της νέας Ευρωπαϊκής οδηγίας 2016/679, αναφέροντας ότι η προσωπική πληροφορία συνδέεται ανώνυμα.

Συμπερασματικά οι εφαρμογές επι το πλείστον, χρησιμοποιούν και ασφαλή πρωτόκολλα αλλά και μεθόδους ανωνυμοποίησης των δεδομένων που συλλέγουν. Δυστυχώς όμως δεν εφαρμόζεται αυτό στο σύνολο των δεδομένων και των επικοινωνιακών συνδέσεων μεταξύ εφαρμογών και τομέων πρώτων ή τρίτων μελών.

Ταυτόχρονα αποκαλύπτονται ποσοστιαία, ως προς τη συνολική επικοινωνία, οι γενικές ροές πληροφοριών (overhead) που προκαλούνται από τις διαφημίσεις (advertising), τις συνδέσεις παρακολούθησης (tracking) και τις διαρροές δεδομένων που εκτελούνται από τις εφαρμογές. Τα αποτελέσματα αυτά εξάχθηκαν συνολικά μέσα από την χρήση των πέντε εφαρμογών στα τέσσερα κινητά τηλέφωνα μέσω του Lumen Privacy Monitor. Στον πίνακα 7.6 λοιπόν, παρατηρούμε ότι τις λιγότερες διαρροές για σκοπούς διαφήμισης, παρακολούθησης και διαρροής δεδομένων παρουσιάζει η εφαρμογή Google Maps με ποσοστό 16,90%, ενώ τις μεγαλύτερες ροές δεδομένων παρουσιάζει η εφαρμογή Sygic GPS Navigation & Maps με ποσοστό 60,13%.



Πίνακας 7.6: Τα ποσοστά των γενικών ροών δεδομένων, ανά εφαρμογή στο σύνολο των υπό εξέταση συσκευών, με σκοπό την διαφήμιση, την παρακολούθηση και την διαρροή δεδομένων.

Στη συνέχεια θα παρουσιαστούν τα ευρήματα που μπορέσαμε να εξάγουμε μέσα από το Lumen Privacy Monitor και το Inspeckage, τα οποία αφορούν τις εφαρμογές στο σύνολο των υπό εξέταση κινητών συσκευών. Τα δεδομένα αυτά, τα οποία θεωρούνται προσωπικά δεδομένα, μεταφέρονται και σε πρώτα αλλά και σε τρίτα μέλη.

	Εφαρμογές		
Domain	**1**	**2**	**3**
google.com	Device Model		
facebook.com		Facebook Session ID	
infinario.com		GAID, Device Brand, Android ID,	
sygic.com		Device Model, Android ID, Android Version, Dropbox Version, Facebook Session ID	
tomtom.com			Device Model
appsflyer.com		GAID, Facebook Session ID	
Twitter.com		GAID	GAID
crashlytics.com		Facebook Session ID	
windows.net		Device Brand, Device Model, Android Version, GAID	

Πίνακας 7.7: Παρουσίαση των διαρροών σε κάθε τομέα μέσω των εφαρμογών στο σύνολο των υπό εξέταση συσκευών.

Στο σημείο αυτό αξίζει να σημειωθεί αρκετές διαρροές δεν μπορέσαμε να τις εντοπίσουμε καθότι, όπως προαναφέρθηκε, οι περισσότερες εφαρμογές και αναλόγως του λειτουργικού στο οποίο τρέχουν, χρησιμοποιούν κρυπτογράφηση εσωτερικά με αποτέλεσμα το TLS proxy, στο οποίο βασίζεται το Lumen, να μην μπορεί ουσιαστικά να υποκλέψει σε καθαρό κείμενο την πληροφορία παρα μόνο σε κρυπτοκείμενο.

	Εφαρμογές	
Domain	**4**	**5**
mapfactor.com		Build Fingerprint, Device Model
Server of HEG US Inc. (209.126.110.41)		Build Fingerprint, Device Model
pushwoosh.com	Country and City, HardwareID, Γλώσσα εφαρμογής	
google.com		Location
mapswithme.com	Device Model, Facebook Session ID, HardwareID,	
facebook.com	Facebook Session ID	
mopub.com	Counrty, Device Model, GAID, Android Version, Build Fingerprint, Type of kernel, Browser Type and Version,Facebook Session ID	
flurry.com	GAID, Country and City, Γλώσσα εφαρμογής	
appsflyer.com	GAID, Facebook Session ID	
Twitter.com	GAID	
windows.net		Device Model, OS and Version,GAID
crashlytics.com	GAID	
my.com	WiFi MAC Address	
admob.google.com		Android Version, Build Fingerprint, Type of kernel, Device Model, Browser Type and Version

Πίνακας 7.8: Παρουσίαση των διαρροών σε κάθε τομέα μέσω των εφαρμογών στο σύνολο των υπό εξέταση συσκευών.

Στη συνέχεια θα παρουσιαστούν τα δεδομένα τα οποία διέρρευσαν και τα οποία μπορούν να αποτελέσουν προσωπικά δεδομένα, με την ιδιότητα του μοναδικού προσδιοριστή ενός χρήστη.

- Device Model: αυτή η τιμή προσδιορίζει το μοντέλο της συσκευής και τον κατασκευαστή. Η εφαρμογή χρησιμοποιεί τυπικά αυτή την πληροφορία για την προσαρμογή του περιεχομένου στην οθόνη ή τη βελτίωση της αποτελεσματικότητας της διαφήμισης. Ωστόσο, αυτές οι πληροφορίες μπορούν επίσης να αποκαλύψουν πράγματα για την προσωπικότητα, τη γούστο, την οικονομική κατάσταση και τα δημογραφικά στοιχεία ενός χρήστη. Το επίπεδο επικινδυνότητας θεωρείτε χαμηλό.
- Android Version: παρουσιάζει την έκδοση του λειτουργικού του χρήστη που σε συνδυασμό με το μοντέλο και τον κατασκευαστή της συσκευής μπορεί να αποτελέσουν σημαντική πληροφορία για την προσαρμογή του περιεχομένου στην οθόνη ή τη βελτίωση της αποτελεσματικότητας της διαφήμισης. Το επίπεδο επικινδυνότητας θεωρείτε χαμηλό.
- Device Brand: Αυτή η τιμή προσδιορίζει τη μάρκα του τηλεφώνου. Όταν συνδυάζεται με άλλες πληροφορίες, μπορεί να χρησιμοποιηθεί για να εντοπίσει μοναδικά το χρήστη. Η εφαρμογή χρησιμοποιεί τυπικά αυτή την πληροφορία για την προσαρμογή του περιεχομένου στην οθόνη ή τη βελτίωση της αποτελεσματικότητας της διαφήμισης. Ωστόσο, αυτές οι πληροφορίες μπορούν επίσης να αποκαλύψουν πράγματα για την προσωπικότητα, τη γούστο, την οικονομική κατάσταση και τα δημογραφικά στοιχεία ενός χρήστη. Το επίπεδο επικινδυνότητας θεωρείτε χαμηλό.
- Google Advertising ID (GAID): Το αναγνωριστικό, όπως έχει αναφερθεί στο Κεφάλαιο 6, θεωρείτε ανωνυμοποιημένο μοναδικό αναγνωριστικό ενός χρήστη. Τι συμβαίνει όμως όταν το μοναδικό αυτό αναγνωριστικό συνδυάζεται με άλλα στοιχεία; Αυτό μπορεί να γίνει αναπροσαρμογή από τον χρήστη όποτε το θελήσει, αλλά τι πραγματικά συλλέγει η Google από τον χρήστη την στιγμή της αναπροσαρμογής του GAID; Το επίπεδο επικινδυνότητας θεωρείτε χαμηλό.
- Android ID: Αυτή η τιμή επιτρέπει στα δίκτυα διαφημίσεων και τους ιχνηλάτες να αναγνωρίζουν έναν χρήστη, μοναδικά ως χρήστη Google για σκοπούς παρακολούθησης ή διαφήμισης. Αυτό τους επιτρέπει να εντοπίζουν τον χρήστη μοναδικά ανάμεσα σε πλατφόρμες, όπως για παράδειγμα κατά την πλοήγηση του στο διαδίκτυο. Αυτή η τιμή θα οριστεί κατά την πρώτη εκκίνηση, είτε σε μια ολοκαίνουργια συσκευή είτε μετά από επαναφορά εργοστασιακών ρυθμίσεων. Το επίπεδο επικινδυνότητας θεωρείται υψηλό. Για αυτό το λόγο άλλωστε, από την έκδοση Oreo του Android και έκτοτε, καμία εφαρμογή

δεν έχει πρόσβαση στο Android ID (κάτι όμως που δεν ισχύει για τις παλαιότερες εκδόσεις).

infinario.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <long name="session_start" value="1555857932620" ></long>
   <string name="device_type">mobile</string>
   <string name="cookie">2988258f6ff64ef0</string>
   <string name="token">ea417e9a-718a-11e5-a4f8-44a84224c532</string>
   <long name="session_end" value="-1" ></long>
   <string name="google_advertising_id">fafb64ce-33ca-4b62-8b96-f85d6046585e</string>
   <string name="target">https://sygic-api.infinario.com</string>
   <string name="session_end_properties"></string>
</map>
```

Εικόνα 7.3: Παρατηρούμε ότι φορτώνεται το Android ID, το GAID στις παραμέτρους του infinario.com.

- Location: Η παράμετρος αυτή διαρρέει είτε σε μορφή συντεταγμένων με μεγάλη ακρίβεια είτε σε ποιο γενικευμένη μορφή όπως για παράδειγμα Χώρα και πόλη στην οποία δραστηριοποιείτε ο χρήστης. Το επίπεδο επικινδυνότητας θεωρείτε υψηλό.

camera.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <float name="bearing" value="0.0" ></float>
   <boolean name="tracking" value="false" ></boolean>
   <float name="tilt" value="0.0" ></float>
   <long name="timestamp" value="1555840206644" ></long>
   <float name="lat" value="34.680984" ></float>
   <float name="zoom" value="14.793555" ></float>
   <float name="lng" value="33.00652" ></float>
</map>
```

Εικόνα 7.4: Παρατηρούμε ότι φορτώνονται στοιχεία τοποθεσίας με τη μορφή συντεταγμένων στις παραμέτρους τις κάμερας του κινητού και αποστέλνονται στην Google.

- WiFi MAC Address: Οι εφαρμογές μπορούν να ζητήσουν πρόσβαση στις ρυθμίσεις συνδεσιμότητας για να προσαρμόσουν τη συμπεριφορά τους και για να βελτιώσουν την

απόδοση της τεχνολογίας δικτύου. Ωστόσο, όταν συνδυάζεται με άλλα στοιχεία όπως το όνομα του φορέα κινητής τηλεφωνίας σας, ο τύπος σύνδεσης, ο σταθμός βάσης ή το SSID μπορούν να αποκαλύψουν πολλές πληροφορίες σχετικά με εσάς και τον τρόπο συμπεριφοράς σας. Η WiFi Mac διεύθυνση αναγνωρίζει μοναδικά το σημείο πρόσβασης WiFi της κινητής συσκευής. Δίνει στους διαφημιστές και στις online υπηρεσίες πολλές πληροφορίες σχετικά με το χρήστη, τις δραστηριότητες του και τη θέση του. Τα πρώτα ψηφία της διεύθυνσης MAC προσδιορίζουν τον κατασκευαστή της συσκευής. Η αποκάλυψη μπορεί να συνδεθεί με την πραγματική ταυτότητά ενός χρήστη, καθώς μπορεί να είναι δυνατή η παρακολούθησή του χρησιμοποιώντας δεδομένα που συλλέγονται από δίκτυα WiFi ή μπορεί να χρησιμοποιηθεί για την παραποίηση της διεύθυνσης MAC μιας συσκευής για να αποκτηθεί πρόσβαση σε κάποια υπηρεσία. Το επίπεδο επικινδυνότητας θεωρείτε υψηλό.

- Build Fingerprint: Είναι μια τιμή που προσδιορίζει μοναδικά το λειτουργικό σύστημα Android και την έκδοση του. Οι εφαρμογές συνήθως χρησιμοποιούν αυτές τις πληροφορίες για την προσαρμογή του περιεχομένου στην οθόνη για τη βελτίωση της αποτελεσματικότητας της διαφήμισης. Ωστόσο, αυτές οι πληροφορίες, ειδικά όταν συνδυάζονται με άλλες διαρροές, μπορούν επίσης να αποκαλύψουν πράγματα για την προσωπικότητα, τη γούστο, την οικονομική κατάσταση και τα δημογραφικά στοιχεία ενός χρήστη. Το επίπεδο επικινδυνότητας θεωρείτε χαμηλό.
- Hardware ID: Αυτή η τιμή επιτρέπει στα δίκτυα διαφημίσεων και τους ιχνηλάτες να αναγνωρίζουν έναν χρήστη, μοναδικά ως χρήστη Google για σκοπούς παρακολούθησης ή διαφήμισης. Αυτό τους επιτρέπει να εντοπίζουν τον χρήστη μοναδικά ανάμεσα σε πλατφόρμες, όπως για παράδειγμα κατά την πλοήγηση του στο διαδίκτυο. Αυτό είναι το σειριακό στοιχείο της συσκευής, το οποίο παραμένει ακόμη και μια εργοστασιακή επαναφορά. Το επίπεδο επικινδυνότητας θεωρείτε υψηλό.
- Τέλος διαρρέουν πολλά στοιχεία τις συσκευής όπως ο τύπος του πυρήνα, ο τύπος και η έκδοση του φυλλομετρητή, η γλώσσα της εφαρμογής κλπ. Το επίπεδο επικινδυνότητας θεωρείτε χαμηλό.

Στους πίνακες 7.7 και 7.8 βλέπουμε ότι αρκετοί τομείς, εκ των οποίων οι πλείστοι ATS, υποκλέπτουν το Facebook session ID. Στην προσπάθεια μας να δούμε κατά πόσον οι εφαρμογές μέσω των τομέων επικοινωνίας τους προσπαθούν να εκτελέσουν διασταύρωση των στοιχείων που υποκλέπτουν με τις πλέον ολοκληρωμένες πηγές προσωπικών δεδομένων, όπως είναι τα μέσα κοινωνικής δικτύωσης πχ. Facebook, τρέξαμε παράλληλα με τις εφαρμογές, την εφαρμογή

του facebook. Το αποτέλεσμα ήταν να υποκλέπτεται ο μοναδικός αριθμός σύνδεσης. Ανατρέχοντας πίσω στον πίνακα 7.2 όπως έχουμε προαναφέρει αρκετοί τομείς επικοινωνούν με τις ίδιες εφαρμογές, αλλά πέραν τούτου μέσω του ICSI Haystack Panopticon https://www.haystack.mobi/panopticon/index.html παρατηρήσαμε ότι αρκετοί τομείς επικοινωνούν μεταξύ τους. Το ICSI Haystack Panopticon είναι ένας διαδραστικός χάρτης που φωτίζει την παρουσία ιχνηλατών τρίτων κατασκευαστών, όπως οι υπηρεσίες ανάλυσης και τα δίκτυα διαφημίσεων σε εφαρμογές Android. Ο χάρτης δημιουργείται χρησιμοποιώντας ανώνυμα δεδομένα που συλλέγονται μέσω των χρηστών της εφαρμογής Lumen Privacy Monitor για το Android. Για παράδειγμα λοιπόν, το twitter.com ως εφαρμογή, επικοινωνεί με το crashlytics.com και facebook.com ως υπηρεσία επικοινωνεί με το twitter ως εφαρμογή. Το ερώτημα όμως που προκύπτει είναι κατά πόσον οι τομείς που αρχικά επικοινωνούν με την κάθε εφαρμογή για την περισυλλογή πληροφοριών, στην τελική επικοινωνούν μεταξύ τους και ανταλλάζουν πληροφορία με αποτέλεσμα την πλήρη «αποκρυπτογράφηση» του χρήστη δημιουργώντας το προφίλ του με τη μέθοδο του «Cross-device tracking». Έτσι λοιπόν μέσω του μοναδικού αναγνωριστικού σύνδεσης στο Facebook θα μπορούσε για παράδειγμα, αν πράγματι ανταλλάζουν δεδομένα οι τομείς, το crashlytics.com να λάβει πλήρης στοιχεία για το ποιος είναι ένας χρήστης ζητώντας από το twitter.com, το οποίο υποκλέπτει μόνο το GAID και επικοινωνεί με το Facebook, τα στοιχεία σύνδεσης ενός χρήστη στο Facebook η και το αντίθετο. Επομένως λανθασμένα θεωρείται και η ψευδωνυμοποίηση ως ανωνυμοποίηση εφόσον το twitter.com πιθανόν να συνδέει το GAID με το Facebook session ID και μπορεί να σχηματίσει μια πλήρη εικόνα του χρήστη.

Επιπροσθέτως στον τον Πίνακα 7.2, όπου απεικονίζονται οι τομείς που αξιολογήθηκαν ως ATS, παρατηρούμε, όπως προαναφέραμε, ότι οι βιβλιοθήκες τρίτων υπάρχουν σε πάνω από μία εφαρμογές και φθάνουν μέχρι και τις τρείς εφαρμογές ανά συσκευή. Συνέπεια αυτού είναι το γεγονός ότι οι βιβλιοθήκες κληρονομούν το σύνολο των δικαιωμάτων κάθε εφαρμογής. Επομένως εδώ παρουσιάζεται, όπως αναφέρθηκε και στο κεφάλαιο 5, το φαινόμενο της «επίθεσης κλιμάκωσης προνομίων» των βιβλιοθηκών. Για παράδειγμα το crashlytics.com και το twitter.com επικοινωνούν με τις εφαρμογές 2, 3 και 4 από τις οποίες κληρονομεί τις άδειες όπως αυτές παρουσιάζονται στον πιο κάτω πίνακα 7.9.

	Εφαρμογές		
Permissions	**2**	**3**	**4**
Access_Fine _Location	✓	✓	✓
Access_Coarse_Location	✓		✓
Write_External_Storage	✓	✓	✓
Read_Contacts	✓	✓	
Camera	✓		
Record_Audio	✓		
Get_Accounts	✓	✓	
Read_Externatl_Storage	✓	✓	✓
Read_Phone_State		✓	
Write_Contacts		✓	

Πίνακας 7.9: Οι επικίνδυνες άδειες που χορηγούνται ανά εφαρμογή στην κινητή συσκευή Samsung Galaxy S8.

Εξετάζοντας τον πίνακα 7.9 παρατηρούμε λοιπόν, ότι μέσα από τρείς εφαρμογές εντοπισμού τοποθεσίας του χρήστη, οι βιβλιοθήκες crashlytics.com και twitter.com, κληρονομούν συνολικά δέκα επικίνδυνες άδειες (dangerous) εκ των οποίων οι 2 καλύπτονται μόνο από την εφαρμογή Sygic GPS Navigation & Maps (2) και άλλες 2 από την εφαρμογή TomTom GPS Navigation - Traffic Alerts & Maps (3). Οι υπόλοιπες άδειες αλληλοκαλύπτονται μεταξύ των 3 εφαρμογών. Αυτό είναι το φαινόμενο «συμπαιγνία βιβλιοθηκών».

Τέλος μέσα από τις διαρροές μας μπορούμε να διακρίνουμε το φαινόμενο αυτό, αλλά όχι σε μεγάλο βαθμό. Για παράδειγμα βλέπουμε το google.com να λαμβάνει από δυο εφαρμογές προσωπικά δεδομένα όπως η τοποθεσία και το μοντέλο της συσκευής μας, το twitter.com λαμβάνει το GAID από 3 εφαρμογές, το crashlytics.com λαμβάνει το GAID και το Facebook Session ID μέσα από 2 εφαρμογές και το windows.net λαμβάνει μέσα από 2 εφαρμογές, το μοντέλο και την κατασκευάστρια εταιρεία της συσκευής, την έκδοση του λειτουργικού και το GAID. Και λαμβάνοντας υπόψιν ότι αυτές ήταν οι διαρροές που εμείς μπορέσαμε να εντοπίσουμε και όχι οι εκ του πραγματικού συνόλου διαρροές, προκύπτει το ερώτημα «τελικά πράγματι συλλέγεται και αποστέλλεται υπέρμετρη πληροφορία σε τρίτα μέλη ;»

Κεφάλαιο 8
Επίλογος

Η παρούσα Μεταπτυχιακή Διατριβή μελέτησε τον βαθμό προστασίας προσωπικών δεδομένων, με βάση τις αλλαγές που υπεισέρχονται από το νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), μέσα από την χρήση «έξυπνων» εφαρμογών κινητών συσκευών και πιο συγκεκριμένα αυτών που καθιστούν δυνατό τον εντοπισμό της πραγματικής μας θέσης. Στόχος ήταν να γίνει μία εκτενής ανάλυση πέντε εφαρμογών και να εξεταστεί κατά πόσον προστατεύονται τα προσωπικά δεδομένα του χρήστη μέσα από τη χρήση των εφαρμογών, αν συλλέγεται και αποστέλλεται υπέρμετρη πληροφορία σε τρίτα μέλη και κατά πόσον γίνεται επεξεργασία ερήμην του χρήστη των προσωπικών του δεδομένων με σκοπό τη δημιουργία προφίλ (profiling). Με τη μέθοδο της Δυναμικής ανάλυσης και με την βοήθεια των Lumen Privacy Monitor και Inspeckage-Android Package Inspector μπορέσαμε να ερευνήσουμε σε βάθος τις 5 εφαρμογές παρατηρώντας τους τομείς (domains) επικοινωνίας, το επίπεδο αλληλεπίδρασης με τον χρήστη και πως τα ποιο πάνω επιδρούν στην προσωπική ζωή του χρήστη.

Τα αποτελέσματά μας βασίστηκαν στα προγράμματα Lumen Privacy Monitor και Inspeckage-Android Package Inspector τα οποία δημιουργήθηκαν και χρησιμοποιούνται ευρέως από την επιστημονική κοινότητα. Σε κάθε περίπτωση τα αποτελέσματά μας μέσω της τεχνικής εύρεσης,

της Δυναμικής Ανάλυσης, εναπόκεινται στην ακρίβεια που παρέχουν τα εν λόγω εργαλεία. Συνεπώς, η ακρίβεια των αποτελεσμάτων που παρέχονται από τα εν λόγω εργαλεία αποτελεί και έναν περιορισμό της έρευνας. Βέβαια, η συνδυαστική τους χρήση συντελεί στο να επιβεβαιωθεί η ακρίβεια των αποτελεσμάτων εφόσον κάποια αποτελέσματα συμπίπτουν και με τα δύο εργαλεία.

Τα αποτελέσματα της παρούσας Μεταπτυχιακής Διατριβής καταδεικνύουν ότι οι προγραμματιστές εφαρμογών και οι οργανισμοί που ρυθμίζουν τα καταστήματα εφαρμογών έχουν την ευθύνη να παρέχουν περισσότερη ασφάλεια, διαφάνεια και έλεγχο των εφαρμογών προς τους τελικούς χρήστες με μοναδικό σκοπό την προστασία της προσωπικής τους ζωής. Πιο συγκεκριμένα οφείλουν να ενημερώνουν τους χρήστες για όλους τους τομείς με τους οποίους επικοινωνεί η κάθε εφαρμογή αλλά επίσης και τι αποστέλλει και για ποιο σκοπό σε αυτούς τους τομείς. Επιπροσθέτως οφείλουν οι προγραμματιστές να εφαρμόζουν τα απαραίτητα μέτρα ασφαλείας των πληροφοριών που χρησιμοποιούν για τη λειτουργία των εφαρμογών τους, όπως για παράδειγμα τα πρωτόκολλα ασφαλείας κρυπτογράφησης https και μέτρα ψευδωνυμοποίησης ή ανωνυμοποίησης, προς αποφυγή διαρροής προσωπικών δεδομένων των χρηστών μέσα από επιθέσεις όπως MITM "man in the middle". Πέραν τούτου σε αυτή την εργασία, αναφέραμε μια καινοφανή και επικίνδυνη ευπάθεια, την πιθανή κλιμάκωση προνομίων μεταξύ βιβλιοθηκών. Το γεγονός ότι τα δικαιώματα μεταξύ των εφαρμογών και των ενσωματωμένων βιβλιοθηκών τους δεν διαχωρίζονται και επομένως επιτρέπεται στις βιβλιοθήκες να συγκεντρώνουν κρυφά πολλαπλές πηγές ευαίσθητων δεδομένων χρηστών αξιοποιώντας τα δικαιώματα που τους έχουν χορηγηθεί σε δύο ή περισσότερες εφαρμογές. Σημαντικό ρόλο έχουν και οι πάροχοι των λειτουργικών συστημάτων, οι οποίοι θα πρέπει να φροντίσουν έτσι ώστε να ενισχύουν την προστασία των δεδομένων των χρηστών, μην επιτρέποντας σε εφαρμογές την πρόσβαση σε μοναδικά αναγνωριστικά του χρήστη/συσκευής, τα οποία δεν αλλάζουν ποτέ με το χρόνο.

Επιπλέον, οι πληροφορίες που παρέχονται στο Google Play Store όσον αφορά τους τύπους απαιτούμενης πρόσβασης σε δεδομένα δεν είναι πλήρεις και σαφείς. Οι περιγραφές των τύπων πρόσβασης δεδομένων χαρακτηρίζονται από γενικεύσεις και επικαλύψεις. Μια πιο λεπτομερής και διαφανής περιγραφή σε συνδυασμό με την κατάλληλη αιτιολόγηση σε σχέση με τους λόγους για τους οποίους απαιτούνται συγκεκριμένοι τύποι πρόσβασης θα αυξήσει την εμπιστοσύνη των χρηστών κινητής τηλεφωνίας και θα απαγορεύσει την πρόσβαση και τη διαρροή των προσωπικών δεδομένων χωρίς πλήρη και σαφή άδεια χρήσης. Επιπλέον ένα από τα βασικά προβλήματα στο περιβάλλον κινητής τηλεφωνίας είναι ότι οι αρχιτεκτονικές εξουσιοδότησης δεν προβλέπουν τη δυνατότητα χορήγησης άδειας στην εφαρμογή και ολοκληρωμένων τρίτων

ξεχωριστά. Μερικές φορές, μια εφαρμογή μπορεί να ζητήσει πρόσβαση σε συγκεκριμένο τύπο δεδομένων στη συσκευή μόνο επειδή κάποιος τρίτος επιθυμεί ή πρέπει να αποκτήσει πρόσβαση σε αυτά τα δεδομένα. Τουλάχιστον, οι υποχρεώσεις διαφάνειας που αναφέρθηκαν παραπάνω απαιτούν από τους υπεύθυνους ανάπτυξης εφαρμογών να είναι πλήρως διαφανείς σχετικά με την επεξεργασία τρίτου που διευκολύνει η εφαρμογή και οι επιχειρήσεις επεξεργασίας πρέπει να έχουν επαρκή νομική βάση.

Η ανάλυσή μας αποκαλύπτει την ανάγκη για περαιτέρω διερεύνηση σε διάφορες κατευθύνσεις. Κατ' αρχάς, εύλογου απορίας αποτελεί και το εάν και πως πραγματικά επικοινωνούν δύο υπηρεσίες που συλλέγουν προσωπικά δεδομένα χρηστών και εάν πραγματικά μπορούν να σχηματίσουν μία πλήρη εικόνα για έναν χρήστη διασταυρώνοντας τα δεδομένα που συλλέγουν. Σε κάθε περίπτωση, μία τέτοια διασταύρωση στοιχείων, αν και σαφώς αθέμιτη από τη σκοπιά του νομικού πλαισίου προστασίας δεδομένων, είναι εφικτή όταν χρησιμοποιούνται, από διαφορετικά μέλη, κοινά αναγνωριστικά χρήστη/συσκευής: οι κίνδυνοι αυτοί δεν αντιμετωπίζονται επαρκώς αν χρησιμοποιείται απλά μία κρυπτογραφική συνάρτηση κατακερματισμού για παραγωγή ψευδωνύμων (κάτι που η έρευνά μας κατέδειξε ότι γίνεται στην πράξη). Συνεπώς, καθίσταται εξαιρετικά σημαντικό να αναπτυχθούν νέες τεχνολογίες προάσπισης τις ιδιωτικότητας οι οποίες να αντιμετωπίζουν αυτούς τους κινδύνους – συμπεριλαμβανομένων αποτελεσματικών τεχνικών ψευδωνυμοποίησης. Τέλος παρέχεται στις υπηρεσίες ATS η δυνατότητα να συλλέγουν πολλά στοιχεία συμπεριφοράς και προσωπικών δεδομένων από τους χρήστες μέσω της παρακολούθησης μεταξύ συσκευών. Λαμβάνοντας υπόψη ότι τα ανωτέρω αφορούν εφαρμογές εντοπισμού θέσης, γίνεται σαφές ότι η επέμβαση στην ιδιωτικότητα των χρηστών γίνεται ακόμα μεγαλύτερη, ακριβώς γιατί τα ανωτέρω δεδομένα συνδυάζονται και με τη γεωγραφική τοποθεσία του χρήστη. Επομένως είναι αναγκαία η έρευνα της συνολικής δυναμικής του οικοσυστήματος των ATS για κινητά και συγκεκριμένα του κατά πόσον οι υπηρεσίες αυτές συγκεντρώνουν, συνδέουν και αξιοποιούν προσωπικές πληροφορίες από διαφορετικές πλατφόρμες για να δημιουργήσουν ακριβή προφίλ χρηστών και για διαφημιστικούς σκοπούς.

Ελπίζουμε ότι τα ευρήματά μας θα πυροδοτήσουν και θα δώσουν μεγαλύτερη έμφαση στον δημόσιο διάλογο και θα οδηγήσουν σε ισχυρότερα ρυθμιστικά πλαίσια για την προστασία της ιδιωτικής ζωής των χρηστών.

Βιβλιογραφία

[1] Muhammad Sarwar, Tariq Rahim Soomro, "Impact of Smartphone's on Society," European Journal of Scientific Research, vol. 98, pp. 216-226, March 2013.

[2] "Number of smartphone users worldwide from 2014 to 2020 (inbillions)," https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Online]. [Accessed March 2019].

[3] "Smartphone," [Online]. Available: https://el.wikipedia.org/wiki/Smartphone. [Accessed March 2019].

[4] Palak Khanna, Amandeep Singh, "Google Android Operating System: A Review," International Journal of Computer Applications, vol. 147, no. 4, Αύγουστος 2016.

[5] "Mobile Operating System Market Share Worldwide," [Online]. Available: http://gs.statcounter.com/os-market-share/mobile/worldwide. [Accessed Μάρτιος 2019].

[6] M. Narmatha, S. Venkata KrishnaKumar, "Study on Android Operating System And Its Versions," International Journal of Scientific Engineering and Applied Science (IJSEAS), vol. 2, no. 2, Φεβρουάριος 2016.

[7] Vincent F. Taylor, Alastair Beresford and Ivan Martinovic, "Intra-Library Collusion: A Potential Privacy," 11 Aug 2017.

[8] "Permissions overview," [Online]. Available: https://developer.android.com/guide/topics/permissions/overview. [Accessed Μάρτιος 2019].

[9] ENISA-European Union Agency For Network and Information Security, Privacy and data protection in mobile applications:A study on the app development ecosystem and the technical implementation of GDPR, Νοέμβριος 2017.

[10] A.Skendzic, B. Kovacic, E.Tijan, "General Data Protection Regulation-Protection of Personal Data in an Organisation," Opatija Croatia, Μάϊος 2018.

[11] "ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016".

[12] Yavuz CANBAY, Mehtap ULKER, Seref SAGIROGLU, "Detection of Mobile Applications Leaking Sensitive Data," Turkey 2017.

[13] Jessa Liying Wang and Michael C. Loui, "Privacy and Ethical Issues in Location-Based Tracking Systems," IEEE 2009.

[14] S. Manoharan, "On GPS Tracking of Mobile Devices," in Fifth International Conference on Networking and Services, 2009.

[15] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, Phillipa Gill, "Apps, Trackers, Privacy, and Regulators:A Global Study of the Mobile Tracking Ecosystem," in Network and Distributed Systems Security (NDSS) Symposium, San Diego, CA, USA, February 2018.

[16] "ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002".

[17] Spyros E. Polykalas, George N. Prezerakos, Froso D. Chrysidou, Eleni D. Pylarinou, "Mobile apps and data privacy: when the service is free, the product is your data," Greece, 2017.

[18] M. Gadaleta and M. Rossi, IDNET: Smartphone-based Gait Recognition with Convolutional Neural Networks, 2016.

[19] Y. Zou, J. Zhu and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," 2016.

[20] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen and V. Blondel, "Unique in the Crowd: The Privacy Bounds of Human Mobility," 2013.

[21] D. Arp, E. Quiring and C. Wressneger, "Privacy Threats through Ultrasonic SideChannels on Mobile Devices," IEEE Security and Privacy, 2017.

[22] J. Achara, G. Acs and C. Castelluccia, "On the Unicity of Smartphone Applications," in 14th ACM CCS Workshop on Privacy in Electronic Society (ACM WPES), 2015.

[23] J. Achara, V. Roca, C. Castelluccia and A. Francillon, "MobileAppScrutinator: A Simple yet Efficient Dynamic Analysis Approach for Detecting Privacy Leaks across Mobile OSs," 2016.

[24] S. Seneviratne, A. Seneviratne, P. Mohapatra and A. Mahanti, "Predicting user traits from a snapshot of apps installed on a smartphone," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 18, no. 2, pp. 1-8, 2014.

[25] Mark N. Gasson, Eleni Kosta, Denis Royer, Martin Meints, and Kevin Warwick, "Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS,, vol. 41, no. 2, Μάρτιος 2011.

[26] Christopher Mann, Artem Starostin, "A Framework for Static Detection of Privacy Leaks in Android Applications," in 27th Symposium on Applied Computing (SAC): Computer Security Track, ACM 2011.

[27] Sooel Son, Daehyeok Kim, Vitaly Shmatikov, "What Mobile Ads Know About Mobile Users," in NDSS '16, San Diego, CA, USA, February 2016.

[28] Siyuan Ma, Zhushou Tang, Qiuyu Xiao, Jiafa Liu, Tran Triet Duong, Xiaodong Liny, Haojin Zhu, "Detecting GPS Information Leakage in Android Applications," in Globecom 2013 - Communication and Information System Security Symposium, 2013.

[29] "Market reach of the most popular Android app categories worldwide as of June 2018," [Online]. Available: https://www.statista.com/statistics/200855/favourite-smartphone-app-categories-by-share-of-smartphone-users/. [Accessed Μάρτιος 2019].

[30] M. C. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi, "Unsafe exposure analysis of mobile in-app advertisements," in 5th ACM conference on Security and Privacy in Wireless and Mobile Networks, 2012.

[31] ""Tecent, "Tecent found a malicious application call "secret tracking"," [Online]. Available: http://news.zol.com.cn/276/2764269.html.". [Accessed 2012].

[32] C. Gibler, J. Crussell, J. Erickson, and H. Chen, "Androidleaks: automatically detecting potential privacy leaks in android applications on a large scale," Trust and Trustworthy Computing, p. 291–307, 2012.

[33] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "Riskranker: scalable and accurate zero-day android malware detection," in ACM 10th international conference on Mobile systems, applications, and services, 2012.

[34] Rashmi Bajaj, Samantha Lalinda Ranaweera, Dharma P. Agrawal, "GPS: Location-Tracking Technology," Computing in Science & Engineering -Communications, pp. 92-94, Απρίλιος 2002.

[35] Marko Gašparović, Pedro Nicolau, Ana Marques, Catarina Silva, Luis Marcelino, "On Privacy in User Tracking Mobile Applications," 2016.

[36] Nir Sivan, Ron Bitton, Asaf Shabtai, "Analysis of Location Data Leakage in the Internet Traffic of Android-based Mobile Devices," Δεκέμβριος 2018.

[37] "Worldwide Mobile App Revenue," [Online]. Available: https://sensortower.com/blog/app-revenue-and-downloads-2018.

[38] Narseo Vallina-Rodriguez, Srikanth Sundaresan, Abbas Razaghpanah, Rishab Nithyanand, Mark Allman, Christian Kreibich1, Phillipa Gill, "Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem," 26 Oct 2016.

[39] R. Nithyanand, S. Khattak, M. Javed, N. Vallina-Rodriguez,M. Falahrastegar, J. E. Powles, E. De Cristofaro, H. Haddadi, and S. J. Murdoch, "Ad-blocking and counter blocking: A slice of the arms race," in USENIX FOCI, 2016.

[40] Clint Gibler, Jonathan Crussell, Jeremy Erickson, and Hao Chen, "AndroidLeaks: Automatically Detecting Potential Privacy Leaks In Android Applications on a Large Scale".

[41] William Enck, Peter Gilbert, Byung-Gon Chun, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones".

[42] Zhemin Yang, Min Yang, Yuan Zhang, Guofei Gu, Peng Ning, X. Sean Wang, "AppIntent: Analyzing Sensitive Data Transmission in Android for Privacy Leakage Detection," Berlin, Germany, 2013.

[43] Jingjing Ren, Martina Lindorfery, Daniel J. Dubois, Ashwin Raoz, David Choffnes and Narseo Vallina-Rodriguez, "Bug Fixes, Improvements, ... and Privacy Leaks:A Longitudinal Study of PII Leaks Across Android App Versions," in Network and Distributed Systems Security (NDSS) Symposium , San Diego, CA, USA, February 2018, .

[44] Abbas Razaghpanah, Narseo Vallina-Rodriguez, Srikanth Sundaresan, "Haystack: In Situ Mobile Traffc Analysis in User Space".

[45] "The ICSI Haystack Project:Privacy Policy and Requested App Permissions," [Online]. Available: https://haystack.mobi/privacy.html. [Accessed Μάρτιος 2019].

[46] "What is Xposed Framework & How to Install it on Rooted Android?," [Online]. Available: https://www.techrrival.com/xposed-framework/. [Accessed Μάρτιος 2019].

[47] "Android Package Inspector: Inspeckage," [Online]. Available: https://n0where.net/android-package-inspector-inspeckage. [Accessed 2019 Μάρτιος].

[48] Vasileios Chatzistefanou, Konstantinos Limniotis, "Anonymity in social networks:The case of anonymous social media," in 7th International Conference on E-Democracy - Privacy-Preserving, Secure, Intelligent E-Government Services, Athens, Greece, December 14th, 2017.

[49] "ac-pm/Inspeckage," [Online]. Available: https://github.com/ac-pm/Inspeckage. [Accessed Μάρτιος 2019].

[50] "Τι σημαίνουν τα « HTTP» και « HTTPS» στην αρχή μιας ηλεκτρονικής διεύθυνσης;," [Online]. Available: https://www.ired.gr/blog/item/3557-what-is-http-https.html. [Accessed 2019 Μάρτιος].

[51] "HTTP vs HTTPS: The Difference And Everything You Need To Know," [Online]. Available: https://seopressor.com/blog/http-vs-https/. [Accessed 2019 Μάρτιος].

[52] "Content providers," [Online]. Available: https://developer.android.com/guide/topics/providers/content-providers. [Accessed Μάρτιος 2019].

[53] "Broadcasts overview," [Online]. Available: https://developer.android.com/guide/components/broadcasts. [Accessed Μάρτιος 2019].

[54] "What is QUIC?," [Online]. Available: https://docs.google.com/document/d/1gY9-YNDNAB1eip-RTPbqphgySwSNSDHLq9D5Bty4FSU/edit.

[55] "QUIC vs. TCP+TLS—and why QUIC is not the next big thing," [Online]. Available: https://medium.com/@codavel/quic-vs-tcp-tls-and-why-quic-is-not-the-next-big-thing-d4ef59143efd.

[56] "SMARTPHONE APPLICATIONS DO NOT TRANSMIT DATA IN ISOLATION," [Online]. Available: https://citizenlab.ca/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/1-3/. [Accessed Μάρτιος 2019].