Ατομική Διπλωματική Εργασία

Εργαλείο Ανάλυσης Προστασίας Δεδομένων για Διαδικτυακές και Κινητές Εφαρμογές για γονείς και παιδιά

Παναγιώτης Γρούτας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ιανουάριος 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Εργαλείο για ανάλυση προστασίας δεδομένων
σε διαδικτυακές και κινητές
εφαρμογές για παιδιά/γονείς

Παναγιώτης Γρούτας

Επιβλέπων Καθηγητής
Καπιτσάκη Γεωργία

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

Ιανουάριος 2021

Ευχαριστίες

Για να υλοποιηθεί η παρούσα πτυχιακή εργασία με βοήθησαν σε μεγάλο βαθμό πολλά άτομα, πρακτικά και ψυχολογικά.

Αρχικά, θα ήθελα να ευχαριστήσω τη επιβλέπουσα καθηγήτρια της εργασίας, Δρ. Γεωργία Καπιτσάκη,η οποία οποιαδήποτε βοήθεια χρειαζόμουν, για υλικό ή ακόμη και για τον τρόπο που θα δούλευα για τη δημιουργία της εφαρμογής, μου το παρείχε άμεσα βοηθώντας με έτσι να διευρύνω τις γνώσεις μου για το συγκεκριμένο θέμα αλλά και τα υλικά που χρησιμοποίησα. Επίσης, είχαμε πολύ καλή επικοινωνία και οι συναντήσεις μας ήταν εποικοδομητικές.

Στη συνέχεια θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου που με στήριξαν κυρίως ψυχολογικά, αφού καθ' όλη τη διάρκεια των σπουδών μου αλλά και της εκπόνησης της διπλωματικής δεν σταμάτησαν να πιστεύουν σε εμένα και στις δυνατότητες μου.

Τέλος, θα ήθελα να ευχαριστήσω το Πανεπιστήμιο Κύπρου για τις εμπειρίες και τις γνώσεις που αποκόμισα κατά τη διάρκεια των σπουδών μου σε αυτό και θα μου χρησιμεύσουν σε όλη μου τη ζωή.

Περίληψη

Η παρούσα Ατομική Διπλωματική Εργασία (ΑΔΕ) είχε στόχο τη κατασκευή ενός εργαλείου που θα ενημερώνει τον χρήστη για τα permissions που χρησιμοποιεί μια εφαρμογή, τους πόρους δηλαδή, που αποτελούν μέρος των προσωπικών πληροφοριών του χρήστη και θα χρησιμοποιήσει η εφαρμογή. Οι εφαρμογές που μπορεί ο χρήστης να αναζητήσει, θα είναι είτε Android εφαρμογές είτε διαδικτυακές εφαρμογές HTML5. Το εργαλείο αυτό αποφασίστηκε να είναι μια Android εφαρμογή και να υλοποιηθεί σε περιβάλλον Android Studio. Το όνομα της εφαρμογής είναι AppPrivacyAnalyzer

Αρχικά, γίνεται μια γενική παρουσίαση για το στόχο και το περιεχόμενο της εφαρμογής και το θεωρητικό υπόβαθρο της. Επίσης, σε αυτό το κεφάλαιο επεξηγείται η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων του ανθρώπου στις ηλεκτρικές συσκευές με αναφορά στο GDPR.

Στα επόμενα δύο κεφάλαια παρουσιάζονται κάποιες προηγούμενες εργασίες που αφορούν την ιδιωτικότητα για Android και διαδικτυακές εφαρμογές καθώς και μία γενική εξήγηση του για το πως διαχειρίζονται τη προστασία δεδομένων αυτές οι εφαρμογές.

Στη συνέχεια, παρουσιάζεται η σχεδίαση και η ανάπτυξη του συστήματος και οι μέθοδοι και τα εργαλεία που χρησιμοποιήθηκαν.

Τέλος, γίνεται παρουσίαση αποτελεσμάτων μετά από χρήση της εφαρμογής από κάποιο αριθμό χρηστών.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Γενική Εισαγωγή

Καθημερινά, στη σημερινή κοινωνία παρατηρούμε ότι το μεγαλύτερο ποσοστό των ανθρώπων βρίσκονται μπροστά από ένα ηλεκτρονικό υπολογιστή ή διαρκώς με ένα κινητό στο χέρι. Η τεχνολογία πλέον είναι αναπόσπαστο κομμάτι της ζωής μας και καθοριστική για την εξέλιξη της αφού πολύ μεγάλο μέρος των εργασιών που εκτελεί καθημερινά ο μέσος άνθρωπος γίνεται μέσω αυτής. Τα δεδομένα που ρέουν καθημερινά στο διαδίκτυο μέσω της της τεχνολογίας είναι αμέτρητα, με μεγάλο αριθμό αυτών να αφορούν προσωπικά δεδομένα ανθρώπων. Αυτό καθιστά τη τεχνολογία επικίνδυνη αν δεν προσεχθεί, αφού δεν μπορούμε να ξέρουμε σε ποιον είναι ορατά αυτά τα δεδομένα.

Για προστασία του κόσμου από την απρόσκοπτη και ανεπιθύμητη διαρροή δεδομένων βλέπουμε τις εφαρμογές κινητών τηλεφώνων τα τελευταία χρόνια να ζητούν άδεια όσον αφορά τις πληροφορίες του χρήστη θα χρησιμοποιήσουν. Αυτό γίνεται επειδή οι συγκεκριμένες πληροφορίες συνήθως αφορούν προσωπικές πληροφορίες του χρήστη, όπως η χρήση των φωτογραφιών, η χρήση της τοποθεσίας και άλλα πολλά που θα αναφερθούν στη συνέχεια της εργασίας. Τα μηνύματα αυτά εμφανίζονται μετά της θέσπιση των γενικών κανόνων προστασίας δεδομένων (GDPR), για να εμφανίζεται με συντομία και κατανοητά προς όλους τους χρήστες, τι πληροφορίες ζητά η κάθε εφαρμογή. Έτσι είναι απαραίτητη, σε όλα τα λειτουργικά συστήματα, η συγκατάθεση του χρήστη για συλλογή κάποιας πληροφορίας.

Τα μηνύματα αυτά εμφανίζονται συνήθως κατά την εγκατάσταση κάποιας εφαρμογής ή κατά τη διεκπεραίωση κάποιας άλλης εργασίας της εφαρμογής. Συνήθως, όμως, οι χρήστες επειδή έχουν ως κύριο σκοπό την άμεση χρήση της εφαρμογής αγνοούν τα μηνύματα με αποτέλεσμα να διαρρέουν δεδομένα και πληροφορίες, τα οποία δεν επιθυμούν να διαρρεύσουν.

Στις διαδικτυακές εφαρμογές, ο πιο διαδεδομένος τρόπος συλλογής δεδομένων και πληροφοριών είναι τα cookies τα οποία και αυτά οι περισσότεροι χρήστες αγνοούν με ανεπιθύμητα αποτελέσματα. Επίσης οι διαδικτυακές εφαρμογές μπορεί να ζητούν ρητά τη χρήση κάποιον δεδομένων, όπως η χρήση κάμερας ή και του ημερολογίου. Στο διαδίκτυο όμως υπάρχουν ορισμένες κακόβουλες εφαρμογές που μπορεί οποιοσδήποτε χρήστης να κατεβάσει, οι οποίες συλλέγουν προσωπικά δεδομένα χωρίς καμιά προειδοποίηση.

1.2 Στόχος Ατομική Διπλωματικής Εργασίας

Στόχος της Διπλωματικής Εργασίας είναι να μειώσει τα προβλήματα που δημιουργούνται και αναφέρονται πιο πάνω δίνοντας έμφαση στους πιο άπειρους χρήστες όπως είναι οι γονείς και τα παιδιά. Θα πρέπει να υπάρχει κάποιος εύκολος τρόπος ούτως ώστε αυτοί οι χρήστες να καταλαβαίνουν με εύκολο τρόπο αν κάποια εφαρμογή θεωρείται επικίνδυνη για διαρροή προσωπικών πληροφοριών και παραβίαση της ιδιωτικότητας του ούτως ώστε να μπορεί να προστατευτεί.

Στη παρούσα εργασία αποφασίστηκε η ανάπτυξη μιας κινητής εφαρμογής από την οποία θα μπορεί κάποιος χρήστης να μάθει πληροφορίες για τις πληροφορίες που ζητά οποιαδήποτε εφαρμογή υπάρχει στο Google Play και να δει κατά πόσο αυτή η εφαρμογή χαρακτηρίζεται ως επικίνδυνη. Θα γίνετε ανάλυση των permissions που δηλώνονται στο manifest και αυτών που κρύβονται από τις κλήσεις βιβλιοθηκών.
Επίσης, θα γίνετε ανάλυση των permissions που χρησιμοποιεί μια διαδικτυακή εφαρμογή και αν αυτά μπορεί να είναι επικίνδυνα.

Έτσι θα δίνετε μια πλήρης εξήγηση στους χρήστες της εφαρμογής για το τι πληροφορίες ζητά κάθε εφαρμογή με σκοπό την εξασφάλιση της ιδιωτικότητας.

1.3 Δομή Ατομικής Διπλωματικής Εργασίας

Κεφάλαιο 1: Μια γενική εισαγωγή για θέματα ιδιωτικότητας αλλά και παρουσίαση του στόχους της διπλωματικής Εργασίας και της δομής της.

Κεφάλαιο 2: Σε αυτό κεφάλαιο γίνετε μια αναλυτική εξήγηση για θέματα ιδιωτικότητας και τους κινδύνους που διατρέχει

Κεφάλαιο 3: Σε αυτό το κεφάλαιο παρουσιάζεται η αρχιτεκτονική Android. Γίνετε μια γενική εξήγηση του τι είναι δίνοντας έμφαση στους κινδύνους που διατρέχουν τα προσωπικά δεδομένα των χρηστών αλλά και στα permissions permissions.

Κεφάλαιο 4: Σε αυτό το κεφάλαιο γίνετε αναφορά και παρουσίαση της γλώσσας σήμανσης HTML5 και πως αντιδρά σε θέματα ιδιωτικότητας.

Κεφάλαιο 5: Στο συγκεκριμένο κεφάλαιο γίνετε αναφορά στις γλώσσες προγραμματισμού αλλά και τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής.

Κεφάλαιο 6: Στο συγκεκριμένο κεφάλαιο αναλύεται ο τρόπος ανάπτυξης της Android εφαρμογής AppPrivacyAnalyzer

Κεφάλαιο 7: Στο συγκεκριμένο κεφάλαιο εξάγονται τα συμπεράσματα για την εφαρμογή και παρουσιάζεται η αξιολόγηση από δείγμα χρηστών και τα αποτελέσματα του ερωτηματολογίου που τους δόθηκε.

Κεφάλαιο 2

Ιδιωτικότητα και Προστασία Προσωπικών Δεδομένων

2.1 Εισαγωγή

Όπως αναφέρεται και στο προηγούμενο κεφάλαιο οι κίνδυνοι που υπάρχουν στο διαδίκτυο λόγω το μεγάλου όγκου δεδομένων που υπάρχει σε αυτό είναι τεράστιοι. Ανά πάσα στιγμή μπορούν να διαρρεύσουν προσωπικά μας δεδομένα στο διαδίκτυο και να μπορούν να έχουν πρόσβαση σε αυτά διάφοροι οργανισμοί και συστήματα. Με αυτά τα δεδομένα θα μπορούν να σχηματίσουν προσωπική εικόνα για το κάθε χρήστη που κατέχουν τα στοιχεία του. Με τη συνεχή αύξηση του πιο πάνω φαινομένου άρχισαν να ερευνώνται όροι όπως τη ιδιωτικότητας και της προστασίας προσωπικών δεδομένων.

Τον Ιούνιο του 2013 η εφημερίδα Gurdian δημοσίευσε μια σειρά από αρχεία που είχαν σχέση με την παρακολούθηση των πολιτών την Αμερικής από την NSA. Η NSA είχε φτιάξει ένα τεράστιο δίκτυο παρακολούθησης των πολιτών, χωρίς να πάρει εξουσιοδότηση από κάποιον φορέα.

2.2 Ορισμός Ιδιωτικότητας

Η Ιδιωτικότητα είναι το δικαίωμα του κάθε ανθρώπου να αποφασίζει ο ίδιος για το πότε, πως και μέχρι πότε θα διαρρέουν τα προσωπικά του δεδομένα και έχει αναγνωριστεί ως θεμελιώδες ανθρώπινο δικαίωμα[4]. Το δικαίωμα της Ιδιωτικότητας είναι πλέον αποδεκτό παγκόσμια αφού είναι Εισάχθηκε από την Οικουμενική Διακήρυξη

των Δικαιωμάτων του Ανθρώπου, από το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα, την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου, καθώς και από διάφορες άλλες διεθνείς και περιφερειακές συνθήκες που αφορούν τα ανθρώπινα δικαιώματα.

Ο Alan Westin, ένας από τους πρωτεργάτες του πεδίου, είχε δηλώσει [3] ότι «κανένας ορισμός της ιδιωτικότητας δεν είναι εφικτός, γιατί τα θέματα ιδιωτικότητας είναι εκ θεμελίων ζήτημα αξιών, συμφερόντων και εξουσίας».

Η Ιδιωτικότητα σύμφωνα με τους ειδικού χωρίζεται στις πιο κάτω κατηγορίες:[5]

- Πληροφοριακή Ιδιωτικότητα, είναι η ιδιωτικότητα που αναφέρεται στη προστασία των προσωπικών δεδομένων και την αποφυγή διαρροής τους στο διαδίκτυο χωρίς τη θέληση του ανθρώπου.

- Σωματική Ιδιωτικότητα , αφορά το δικαίωμα για έλεγχο της σωματικής ιδιωτικότητα ς, δηλαδή για το αν δίνει το δικαίωμα σε κάποιο να κάμει σωματικό έλεγχο.

- Τηλεπικοινωνιακή Ιδιωτικότητα , αφορά την ιδιωτικότητα της γραπτής ή ηχητική επικοινωνίας μεταξύ ανθρώπων και την προστασία από την παραβίαση συνομιλιών(τηλεφωνία, email, γραπτά μηνύματα κλπ)

- Εδαφική Ιδιωτικότητα , αναφέρεται στην οριοθέτηση του χώρου που κατέχει ένα άτομο και στην ιδιωτικότητα που έχει σε αυτό το χώρο, στη προστασία του για να μην παραβιάζεται.
- Ιδιωτικότητα προσωπικής συμπεριφοράς, σε αυτή την ανήκει η παράνομη φωτογράφιση αλλά και η προστασία από κριτικές για τις προσωπικές επιλογές κάποιου ατόμου.

2.3 Κίνδυνοι Ιδιωτικότητας

Σε κάθε βήμα της περιδιάβασής μας στο Διαδίκτυο “προσφέρουμε” προσωπικές πληροφορίες. Αυτές οι πληροφορίες είναι σαν ένα γρίφος που πρέπει να συμπληρωθεί για να αποκαλυφθεί η εικόνα μας. Η περιήγηση μας στο Διαδίκτυο έχει πολλά κοινά με

τη ζωή μας στο φυσικό κόσμο. Έτσι τίθενται κάποια πολύ σοβαρά ζητήματα: της προστασίας των προσωπικών μας δεδομένων, της ορθής και ηθικής επικοινωνίας με τη βοήθεια της τεχνολογίας και το γεγονός πως ότι και αν κάνουμε στο Διαδίκτυο αφήνει ίχνη.

Με αυτά τα ίχνη οι μεγάλες επιχειρήσεις συλλέγουν στοιχεία για του χρήστες δημιουργώντας μια εικόνα για κάθε χρήστη. Κάθε ένα από αυτό το ίχνος δίνει στοιχεία στις επιχειρήσεις αυτές για τις προτιμήσεις μας, τις τελευταίες μας αγορές ή ακόμη και τη τοποθεσία μας ούτως ώστε να μπορούν να μας πλασάρουν κάποιο προϊόν που μπορεί να μας δελεάσει περισσότερο. Όπως αναφέρεται και πιο πάνω οργανισμοί όπως η NSA αλλά και η CIA συλλέγουν συνεχώς στοιχεία για του πολίτες ΗΠΑ. Έτσι ο κάθε ένας από εμάς δυστυχώς θα πρέπει να γνωρίζει ότι πιθανόν να κατέχει λογαριασμό στις βάσεις δεδομένων αυτών των τεράστιων επιχειρήσεων και να είναι πιο προσεκτικός για το πως διαχειρίζεται τα προσωπικά του δεδομένα στο διαδίκτυο.

2.4 GDPR

Το GDPR (General Data Protection Regulation) εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο τον Απρίλιο του 2016 και τα επίσημα κείμενα και οι κανονισμοί της οδηγίας δημοσιεύθηκαν σε όλες τις επίσημες γλώσσες της ΕΕ τον Μάιο του 2016. Η νομοθεσία τέθηκε σε ισχύ σε ολόκληρη την Ευρώπη Ένωση στις 25 Μαΐου 2018.

Στον πυρήνα του, το GDPR είναι ένα νέο σύνολο κανόνων που έχουν σχεδιαστεί για να παρέχουν στους πολίτες της ΕΕ μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων. Αποσκοπεί στην απλοποίηση του ρυθμιστικού περιβάλλοντος για τις επιχειρήσεις, ώστε τόσο οι πολίτες όσο και οι επιχειρήσεις στην Ευρωπαϊκή Ένωση να μπορούν να επωφεληθούν πλήρως από την ψηφιακή οικονομία.

Οι μεταρρυθμίσεις έχουν σχεδιαστεί για να αντανακλούν τον κόσμο στον οποίο ζούμε τώρα, και φέρνουν νόμους και υποχρεώσεις - συμπεριλαμβανομένων εκείνων που αφορούν τα προσωπικά δεδομένα, το απόρρητο και τη συγκατάθεση - σε ολόκληρη την Ευρώπη σε ταχύτητα για την εποχή που συνδέεται με το Διαδίκτυο.

Βασικά, σχεδόν κάθε πτυχή της ζωής μας περιστρέφεται γύρω από δεδομένα. Από εταιρείες κοινωνικών μέσων, έως τράπεζες, εμπόρους λιανικής και κυβερνήσεις - σχεδόν κάθε υπηρεσία που χρησιμοποιούμε περιλαμβάνει τη συλλογή και ανάλυση των προσωπικών μας δεδομένων.

Ρόλος του GDPR

Συμβαίνουν αναπόφευκτα παραβιάσεις δεδομένων. Οι πληροφορίες χάνονται, κλέβονται ή απελευθερώνονται με άλλο τρόπο στα χέρια ανθρώπων που δεν είχαν ποτέ σκοπό να το δουν και αυτοί οι άνθρωποι έχουν συχνά κακόβουλη πρόθεση.
Σύμφωνα με τους όρους του GDPR, όχι μόνο οι οργανισμοί πρέπει να διασφαλίζουν ότι τα προσωπικά δεδομένα συλλέγονται νόμιμα και υπό αυστηρούς όρους, αλλά όσοι το συλλέγουν και διαχειρίζονται είναι υποχρεωμένοι να το προστατεύουν από κατάχρηση και εκμετάλλευση, καθώς και να σέβονται τα δικαιώματα των δεδομένων ιδιοκτήτες - ή αντιμετωπίζουν κυρώσεις επειδή δεν το κάνουν.

Το GDPR ισχύει για κάθε οργανισμό που λειτουργεί εντός της ΕΕ, καθώς και για οργανισμούς εκτός ΕΕ που προσφέρουν αγαθά ή υπηρεσίες σε πελάτες ή επιχειρήσεις στην ΕΕ. Αυτό σημαίνει τελικά ότι σχεδόν κάθε μεγάλη εταιρεία στον κόσμο χρειάζεται μια στρατηγική συμμόρφωσης με τον GDPR.

Το GDPR επιβάλλει τελικά νομικές υποχρεώσεις σε έναν επεξεργαστή για τη διατήρηση αρχείων προσωπικών δεδομένων και τον τρόπο επεξεργασίας τους, παρέχοντας πολύ υψηλότερο επίπεδο νομικής ευθύνης σε περίπτωση παραβίασης του οργανισμού.

Οι τύποι δεδομένων που θεωρούνται προσωπικά βάσει της ισχύουσας νομοθεσίας περιλαμβάνουν όνομα, διεύθυνση και φωτογραφίες. Το GDPR επεκτείνει τον ορισμό των προσωπικών δεδομένων έτσι ώστε κάτι σαν μια διεύθυνση IP να μπορεί να είναι προσωπικά δεδομένα. Περιλαμβάνει επίσης ευαίσθητα προσωπικά δεδομένα, όπως γενετικά δεδομένα και βιομετρικά δεδομένα, τα οποία θα μπορούσαν να υποβληθούν σε επεξεργασία για τον μοναδικό προσδιορισμό ενός ατόμου.

Κεφάλαιο 3

Λειτουργικό Σύστημα Android

3.1 Εισαγωγή

Το Android είναι ένα λειτουργικό σύστημα βασισμένο σε μια έκδοση του πυρήνα Kernel (Linux) και είναι σχεδιασμένο για συσκευές όπως τα κινητά τηλέφωνα, τα tablets αλλά και οι τηλεοράσεις. [6] Το android αναπτύχθηκε από μια κοινοπραξία προγραμματιστών γνωστών ως Open Handset Alliance και η πρώτη συσκευή με Android κυκλοφόρησε το 2008. Το Android είναι ένα ελεύθερο λογισμικό ανοικτού κώδικα, δηλαδή επιτρέπει στους χρήστες να αναπτύξουν δωρεάν τη δική τους εφαρμογή. Παρά τη πτώση του τα τελευταία χρόνια λόγω της εμφάνισης νέων λειτουργικών συστημάτων, διατηρεί τη πρωτιά στους χρήστες των smartphones, αφού το 72,92% των χρηστών έχουν συσκευή Android , δηλαδή περισσότεροι από 1,6 δισεκατομμύριά χρήστες. [7]

3.2 Αρχιτεκτονική Android

Το Android αποτελείται από ένα Kernel βασισμένο σε αυτόν του Linux με το middleware, τις βιβλιοθήκες και το APIs να είναι γραμμένα σε C και το software των εφαρμογών που τρέχει πάνω στο application framework που περιλαμβάνει βιβλιοθήκες συμβατές με την Java. Το Android χρησιμοποιεί τη εικονική μηχανή Dalvik. Η κύρια

πλατφόρμα του hardware είναι η ARM αρχιτεκτονική που χρησιμοποιείται σε 32-bits συστήματα.

Διάγραμμα 3.1 Android Software Stack[22]

Το Android είναι μια στοίβα στοιχείων λογισμικού (Android Software Stack) που χωρίζεται περίπου σε πέντε ενότητες και τέσσερα κύρια επίπεδα, όπως φαίνεται στο πιο πάνω διάγραμμα αρχιτεκτονικής.

Στο κάτω μέρος των επιπέδων βρίσκεται το Linux - Linux 3.6 που είναι ο πυρήνας που χρησιμοποιεί το Android. Αυτό παρέχει ένα επίπεδο αφαιρετηκότητας μεταξύ του υλικού της συσκευής παρέχοντας όλα τα απαραίτητα hardware προγράμματα όπως κάμερα, πληκτρολόγιο, οθόνη κ.λπ. Επίσης, ο πυρήνας χειρίζεται και άλλα πράγματα στα εξειδικεύετε το Linux, όπως η δικτύωση(wifi, Bluetooth).

Πάνω από τον πυρήνα του Linux υπάρχει ένα σύνολο βιβλιοθηκών που περιλαμβάνει τη μηχανή αναζήτησης Web ανοιχτού κώδικα WebKit, γνωστή ως βιβλιοθήκη libc, τη βάση δεδομένων SQLite που είναι ένα χρήσιμο αποθετήριο για αποθήκευση και κοινή

χρήση δεδομένων εφαρμογών, βιβλιοθήκες για αναπαραγωγή και εγγραφή ήχου και βίντεο, SSL βιβλιοθήκες που είναι υπεύθυνες για την ασφάλεια στο Διαδίκτυο κ.λπ.

Το τρίτο τμήμα της αρχιτεκτονικής είναι το Android Runtime. Αυτή η ενότητα παρέχει ένα βασικό στοιχείο που ονομάζεται Dalvik Virtual Machine, το οποίο είναι ένα είδος Java Virtual Machine ειδικά σχεδιασμένο και βελτιστοποιημένο για Android. Το Dalvik VM χρησιμοποιεί βασικά χαρακτηριστικά Linux όπως h διαχείριση μνήμης και multi-threading. Το Dalvik VM επιτρέπει σε κάθε εφαρμογή Android να λειτουργεί με τη δική της διαδικασία, με τη δική της παρουσία της εικονικής μηχανής Dalvik. Το Android Runtime Android παρέχει επίσης ένα σύνολο βασικών βιβλιοθηκών που επιτρέπουν στους προγραμματιστές εφαρμογών Android να γράφουν εφαρμογές Android χρησιμοποιώντας τυπική γλώσσα προγραμματισμού Java.

Το επίπεδο Application Framework παρέχει πολλές υπηρεσίες υψηλότερου επιπέδου σε εφαρμογές με τη μορφή κλάσεων Java. Οι προγραμματιστές εφαρμογών επιτρέπεται να κάνουν χρήση αυτών των υπηρεσιών στις εφαρμογές τους.

Το Android Framework παρέχει τις παρακάτω βασικές υπηρεσίες:

- Activity Manager ελέγχει τον κύκλο ζωής μια εφαρμογής και τη στοίβα δραστηριοτήτων.
- Content Providers επιτρέπει στις εφαρμογές την επικοινωνία με άλλες εφαρμογές, όπως η δημοσίευση και η κοινή χρήση δεδομένων.
- Recourse Manager παρέχει πρόσβαση σε μη ενσωματωμένους πόρους.
- Notification Manager επιτρέπει στις εφαρμογές την εμφάνιση ειδοποιήσεων στο χρήστη
- View System επιτρέπει τη δημιουργία διεπαφών με το χρήστη.

Στο πιο πάνω επίπεδο βρίσκονται οι εφαρμογές που μπορεί ο χρήστης να έχει άμεση πρόσβαση σε αυτές, με το να τις κατεβάσει στη δική του Android συσκευή. Παραδείγματα τέτοιων εφαρμογών είναι τα παιχνίδια, οι εφαρμογές κοινωνικής δικτύωσης, κάποιο πρόγραμμα περιήγησης στο διαδίκτυο και άλλα πολλά.[8]

3.3 Ασφάλεια στο Android

Λόγω της φύσης του Android είναι λογικό οι εφαρμογές που χρησιμοποιούν οι χρήστες καθημερινά να μην παρέχουν όλες την απαραίτητη ασφάλεια, αφού οποιοσδήποτε χρήστης μπορεί να δημιουργήσει τη δική του εφαρμογή. Με τη χρήση κάποιας εφαρμογής ο κάθε χρήστης μπορεί να αφήσει άθελα του να εκτεθούν προσωπικά του στοιχεία. Έτσι, το Android σχεδιάστηκε με τέτοιο τρόπο ούτως ώστε να παρέχει ασφάλεια στους χρήστες του μέσω κάποιων τεχνικών που χρησιμοποιεί.

Μια από αυτές τις τεχνικές είναι οι μηχανισμοί IPC (Interprocess Communication) που επιτρέπουν την επαλήθευση της ταυτότητας μιας εφαρμογής. Ο μηχανισμός αυτός γίνετε με τη χρήση Intent, Binder ή Messenger with a Service και BroadcastReceiver.[9]
Χρησιμοποιώντας intents, είναι δυνατόν για εμάς να μεταφέρουμε δεδομένα από τη μία δραστηριότητα στην άλλη, θέτοντας πρόσθετα σε ένα intent και καλώντας τη μέθοδο startActivity. Εάν η δραστηριότητα που αρχικοποιείται έχει το χαρακτηριστικό "process" στο μανιφέστο της, η δραστηριότητα θα ξεκινήσει με τη δική της διαδικασία, αλλά θα έχει πρόσβαση στα δεδομένα που της διαβιβάστηκαν με το επιπλέον intent. Δηλαδή έχει πρόσβαση σε ένα άλλο σωστά καταχωρημένο intent.

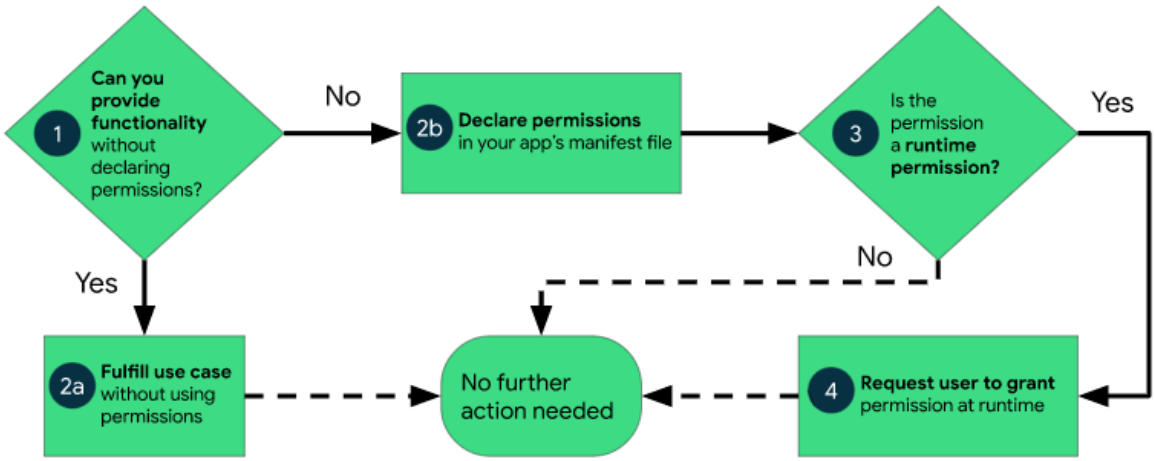
Μια άλλη τεχνική που προσφέρεται στο Android είναι το Application Signing[10]. Το Application Signing επιτρέπει στους προγραμματιστές να αναγνωρίζουν τον δημιουργό της εφαρμογής και να ενημερώνουν την εφαρμογή τους χωρίς να δημιουργούν περίπλοκες διεπαφές και δικαιώματα. Κάθε εφαρμογή που εκτελείται στην πλατφόρμα Android πρέπει να υπογράφεται από τον προγραμματιστή. Οι εφαρμογές που προσπαθούν να εγκαταστηθούν χωρίς να υπογραφούν απορρίπτονται είτε από το Google Play είτε από το πρόγραμμα εγκατάστασης του πακέτου στη συσκευή Android.

3.4 Android permissions

Τα permissions στις εφαρμογές βοηθούν στην υποστήριξη της ιδιωτικότητα ς και στη προστασία των δεδομένων του χρήστη περιορίζοντας τη πρόσβαση στα δεδομένα του

χρήστη, όπως είναι τα στοιχεία επικοινωνίας ή της παρούσας κατάστασης του, άλλα και αποτρέπουν τη χρήση στοιχείων όπως είναι η εγγραφή ήχου ή η χρήση κάμερας.

Τα περισσότερα permissions που χρειάζεται κάποια εφαρμογή για να μπορεί να λειτουργήσει είναι δηλωμένα στο manifest της κάθε εφαρμογής. Ορισμένα δικαιώματα, γνωστά ως δικαιώματα εγκατάστασης, εκχωρούνται αυτόματα κατά την εγκατάσταση της εφαρμογής σας. Άλλα δικαιώματα, γνωστά ως runtime permissions, απαιτούν από την εφαρμογή να προχωρήσει ένα βήμα παραπέρα και να ζητήσει την άδεια κατά το χρόνο εκτέλεσης της εφαρμογής.



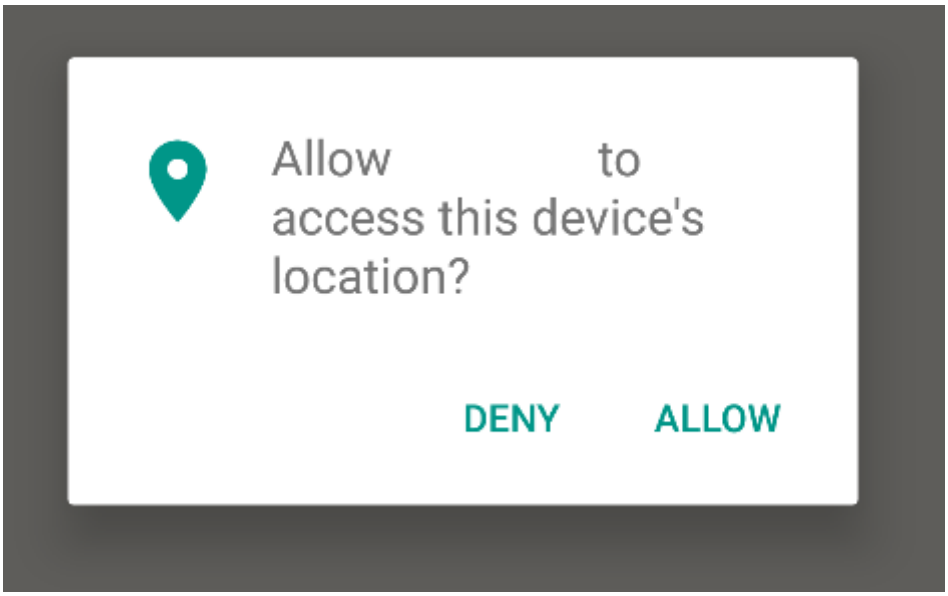
Διάγραμμα 3.2 Ροή δικαιωμάτων στο android.

Τα permissions χωρίζονται σε διάφορες κατηγορίες ανάλογα με το εύρος των περιορισμένων δεδομένων στα οποία μπορεί να έχει πρόσβαση η εφαρμογή αλλά και το εύρος των περιορισμένων ενεργειών, όταν το σύστημα δίνει στην εφαρμογή το συγκεκριμένο permission.

Τα install-time permissions παρέχουν στην εφαρμογή πρόσβαση σε περιορισμένα δεδομένα που επηρεάζουν ελάχιστα το σύστημα ή άλλες εφαρμογές. Όταν δηλώνονται τα συγκεκριμένα permissions, εκχωρούνται κατά την εγκατάσταση της εφαρμογής και παρουσιάζονται στο χρήστη με τη μορφή ειδοποίησης για άδεια εγκατάστασης της εφαρμογής όταν βλέπει τις λεπτομέρειες της πριν την εγκατάσταση.

Τα normal permissions αφορά δικαιώματα που επεκτείνονται πέρα από το περιβάλλον της εφαρμογής αλλά παρουσιάζουν πολύ χαμηλό κίνδυνο για το χρήστη. Άλλη κατηγορία είναι τα signature permissions (sign app - που αναφέρεται και πιο πάνω) και δηλώνονται αν η εφαρμογή έχει δηλώσει άδεια υπογραφής που έχει καθορίσει άλλη εφαρμογή, τότε παραχωρείται άδεια για εγκατάσταση της άλλης εφαρμογής.

Μια σημαντική κατηγορία είναι τα run-time permissions που αναφέρονται πιο πάνω και παρουσιάζονται στο χρήστη κατά τη χρήση της εφαρμογής και είναι γνωστά ως dangerous permissions. Εμφανίζονται στο χρήστη όταν προσπαθήσει να χρησιμοποιήσει μια συγκεκριμένη λειτουργία της εφαρμογής και αυτή η λειτουργία απαιτεί κάποια από τα δεδομένα του χρήστη, όπως φαίνεται και στην εικόνα πιο κάτω.



Εικόνα 3.1

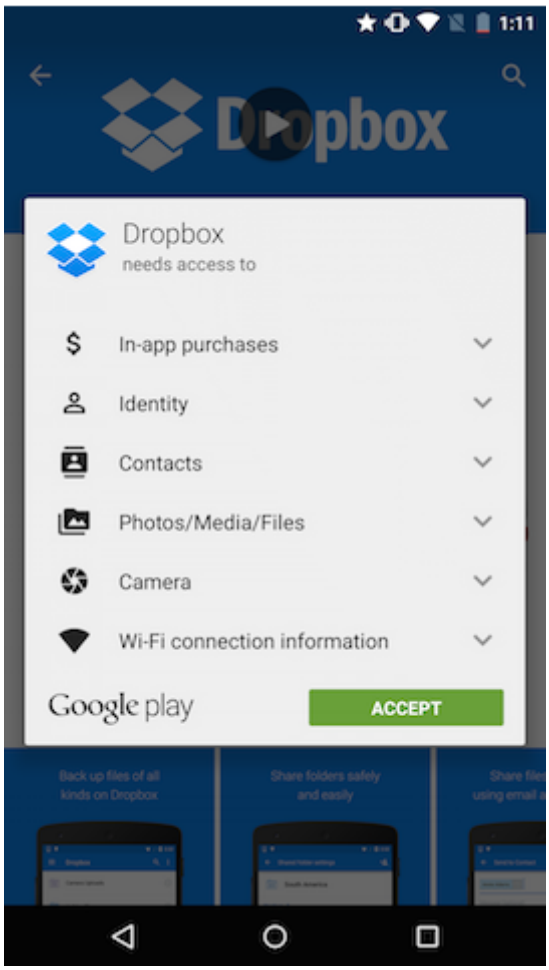
Στη συγκεκριμένη εικόνα (εικόνα 3.1) βλέπουμε ένα runtime permission, όπου ζητείται από το χρήστη η άδεια χρήσης της τοποθεσίας του.

Τέλος, υπάρχουν τα special permissions που αντιστοιχούν σε συγκεκριμένες λειτουργίες εφαρμογών. Μόνο η πλατφόρμα και οι OEM μπορούν να ορίσουν ειδικά δικαιώματα. Επιπλέον, η πλατφόρμα και οι OEM συνήθως ορίζουν ειδικά δικαιώματα όταν θέλουν να προστατεύσουν την πρόσβαση σε ιδιαίτερα ισχυρές ενέργειες, όπως η χρήση άλλων εφαρμογών.

Τα dangerous permissions που αναφέρονται πιο πάνω είναι τα «επικίνδυνα» για τον χρήστη δικαιώματα, δηλαδή αυτά που μπορούν να ζητήσουν πρόσβαση σε προσωπικά δεδομένα του χρήστη ή και σε άλλες εφαρμογές. Τα dangerous permissions δηλώνονται στο manifest και πρέπει να γίνουν αποδεκτά από το χρήστη για να μπορεί να χρησιμοποιήσει τη συγκεκριμένη λειτουργία της εφαρμογής. Τα dangerous permissions όπως ορίζονται από το Android φαίνονται πιο κάτω: [12]

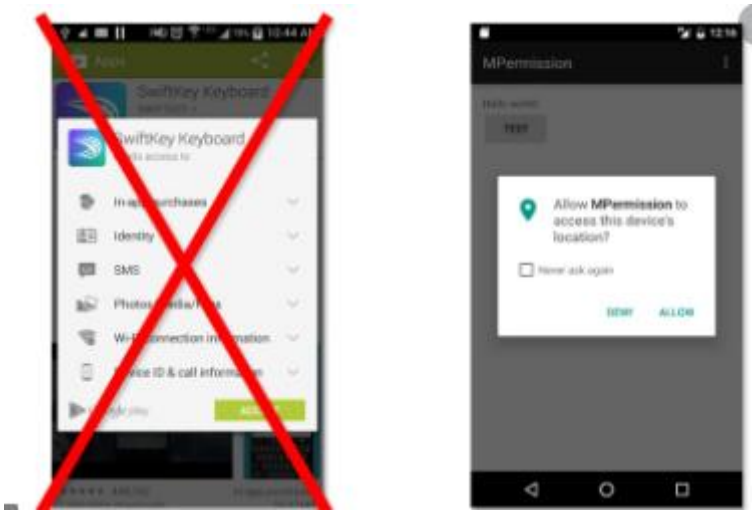
- CALENDAR - γίνετε αποδεκτή η χρήση του ημερολογίου, για διάβασμα, εγγραφή και διαγραφή δεδομένων από αυτό
- CAMERA – επιτρέπει τη χρήση της κάμερας.
- CONTACTS – επιτρέπει στην εφαρμογή να γράψει(write) ή να διαβάσει(read) στοιχεία από τις επαφές του χρήστη.
- RECORD_AUDIO – επιτρέπει τη χρήση του μικροφώνου για εγγραφή ήχου.
- LOCATION – επιτρέπει τη χρήση δεδομένων που αφορούν την τοποθεσία του χρήστη.
- CALL_PHONE – επιτρέπει τη πρόσβαση στα δεδομένα κινητής τηλεφωνίας του χρήστη.
- SMS- επιτρέπει τη λήψη και αποστολή μηνυμάτων.

Τα δικαιώματα ήταν πολύ πιο απλά πριν το Marshmallow (API 23).[13] Όλα τα δικαιώματα διεκπεραιώνονταν κατά την εγκατάσταση. Όταν ένας χρήστης προσπαθούσε να εγκαταστήσει μια εφαρμογή από το Google Play Store, παρουσιαζόταν στον χρήστη μια λίστα δικαιωμάτων που απαιτούσε η εφαρμογή. Ο χρήστης θα μπορούσε είτε να αποδεχτεί όλα τα δικαιώματα και να συνεχίσει για να εγκαταστήσει την εφαρμογή ή να αποφασίσει να μην εγκαταστήσετε την εφαρμογή. Ήταν μια προσέγγιση όλα ή τίποτα. Δεν υπήρχε τρόπος να παραχωρηθούν μόνο ορισμένα δικαιώματα στην εφαρμογή και κανένας τρόπος για τον χρήστη να ανακαλέσει ορισμένα δικαιώματα μετά την εγκατάσταση της εφαρμογής. Το μήνυμα που εμφανιζόταν στο χρήστη πριν την εγκατάσταση μια εφαρμογής φαίνεται στην πιο κάτω εικόνα.



Εικόνα 3.2

Η έκδοση Marshmallow επέφερε μεγάλες αλλαγές στο μοντέλο δικαιωμάτων. Εισήγαγε την έννοια των runtime permissions. Αυτά είναι δικαιώματα που ζητούνται κατά την εκτέλεση της εφαρμογής (αντί πριν από την εγκατάσταση της εφαρμογής). Μια άδεια μπορεί να δοθεί μετά την εγκατάσταση και αντίστοιχα απορριφθεί από τον χρήστη, δηλαδή τα εγκεκριμένα δικαιώματα, μπορούν επίσης να ανακληθούν αργότερα. Ο χρήστης στο Marshmallow μπορεί να κατεβάσει την εφαρμογή χωρίς να δώσει κάποια άδεια και όταν προσπαθήσει να χρησιμοποιήσει κάποια λειτουργεία της εφαρμογής που απαιτεί την έγκριση του για χρήση κάποιων δεδομένων θα του εμφανιστεί εκεί το ανάλογο μήνυμα. Αυτή η αλλαγή φαίνεται στο σχήμα πιο κάτω.



Εικόνα 3.3

Αυτό σημαίνει ότι υπάρχουν μερικά ακόμη πράγματα που πρέπει να ληφθούν υπόψη όταν υπάρχει χρήση δικαιωμάτων για μια εφαρμογή Marshmallow όπως ότι το targetSdkVersion πρέπει να είναι> = 23 η συσκευή σας πρέπει να τρέχει σε Marshmallow για να έχουμε το νέο μοντέλο δικαιωμάτων. Οι Android συσκευές με targetSdkVersion >= API 26, παρέχουν επίσης την επιλογή στο χρήστη να χειρίζεται τα permissions μέσω των ρυθμίσεων του συστήματος.

3.5 Κίνδυνοι ασφάλειας στο Android

Η ανοιχτή φύση του Android, η ευκολία με την οποία μπορούν να δημιουργηθούν εφαρμογές, και η μεγάλη ποικιλία των αγορών έξω από το Play Store, έχουν αυξήσει τα προβλήματα που αφορούν την ασφάλεια στο Android. Το λειτουργικό της Google έχει γίνει ο πιο ελκυστικός στόχος για τα κακόβουλα λογισμικά, τείνοντας να ξεπεράσει τα Windows στους φορητούς υπολογιστές.

Οι μεγαλύτεροι κίνδυνοι βρίσκονται στα malware. Πρόκειται για κακόβουλο λογισμικό, που έχει σχεδιαστεί με σκοπό την ανάληψη του ελέγχου στην Android συσκευή.Συνήθως αυτός ο κίνδυνος βρίσκεται μέσα στις εφαρμογές που κατεβάζουμε, ιδίως σε αυτές που βρίσκονται εκτός του Play Store. Το ανησυχητικό σε ότι αφορά τις mobile συσκευές, είναι ότι τα malware έχουν στοχοποιήσει ως επί το πλείστων το Android.

Παράδειγμα malware είναι τα Exploits που πρόκειται για ένα από τα μεγαλύτερα είδη απειλών. Αυτού του τύπου το κακόβουλο λογισμικό, εκμεταλλεύεται τα κενά στην ασφάλεια στο Android, που του επιτρέπουν την ολική πρόσβαση (root) στη συσκευή. Ένα τέτοιο κενό ασφάλειας ήταν το επικίνδυνο σφάλμα «Stagefright», που είχε θέσει σε κίνδυνο χιλιάδες Android συσκευές.

Από την άλλη, υπάρχουν οι κίνδυνοι που προκύπτουν από το διαδίκτυο αυτό συμβαίνει από τη συνεχή σύνδεση που υπάρχει με αυτό. Τα προβλήματα που προκύπτουν προέρχονται, όπως και στους υπολογιστές, όπως είναι μια απλή επίσκεψη σε μια ιστοσελίδα η οποία όμως κρύβει κάτι κακόβουλο. Παράδειγμα μια τέτοιας web απειλής είναι το Phishing που στοχεύει στο Android, όπως ακριβώς κάνει με τα PC και Mac. Στο Phishing γίνεται χρήση κείμενων, μηνυμάτων ηλεκτρονικού ταχυδρομείου, και των social media, για να ξεγελαστούν οι χρήστες και να παρέχουν ευαίσθητα δεδομένα.

Κεφάλαιο 4

HTML 5

4.1 Εισαγωγή

Το HTML (HyperText Markup Language) είναι η βασική γλώσσα σήμανσης για τη δημιουργία ιστοσελίδων και προβολής τους στο διαδίκτυο. Τα στοιχεία της αποτελούν τα βασικά δομικά στοιχεία των ιστοσελίδων. Το HTML αποτελείται από ετικέτες και στο browser εμφανίζονται κείμενο, πίνακες και άλλα στοιχεία σύμφωνα με αυτές.

Εικόνα 4.1

Το HTML 5[14] πρόκειται για μια νέα ανανεωμένη έκδοση του HTML. Πρόκειται για συνεργασία μεταξύ της Κοινοπραξίας Παγκοσμίου Ιστού (W3C) και της Ομάδας Εργασίας Ιστού (Hypertext Application Technology Technology Working Group) (WHATWG). Το HTML5 υποστηρίζει όλα τα προγράμματα περιήγησης ιστού, όπως

Firefox, Chrome, Safari και Opera. Επιπλέον, τα κινητά προγράμματα περιήγησης ιστού που είναι προεγκατεστημένα σε iPhones, iPads και Android έχουν επίσης εξαιρετική υποστήριξη για HTML5.

Σε αυτήν την έκδοση δίνεται μεγάλη έμφαση στην δημιουργία responsible ιστοσελίδων, σελίδων που προσαρμόζονται σε διαφορετικές συσκευές. Για τους χρήστες κινητών συσκευών (smartphones), που πιθανόν επισκέπτονται την ιστοσελίδα με περιορισμένο bandwidth και είναι αυτοί στους οποίους απευθύνεται κυρίως η τεχνική της responsive σχεδίασης, θα πρέπει η ιστοσελίδα όχι μόνο να ανταποκρίνεται στον περιορισμένο «χώρο» της οθόνης τους, αλλά και να την φορτώνει όσο το δυνατόν ταχύτερα.

Το HTML 5 παρέχει μια σειρά από νέες λειτουργίες. Μερικά από αυτά είναι τα ακόλουθα.

- Έντυπα 2.0 - Ενίσχυση φόρμουλων ιστού HTML. Υπάρχουν νέα χαρακτηριστικά για μια ετικέτα

- WebSocket - Παροχή τεχνολογίας αμφίδρομης επικοινωνίας για την εφαρμογή Ιστού.

- Καμβάς - Υποστηρίζει δισδιάστατες επιφάνειες σχεδίασης με πρόγραμμα JavaScript.

- Σύρετε και ρίξτε - Επιτρέπει τη μεταφορά και απόθεση στοιχείων από μια τοποθεσία σε άλλη τοποθεσία στην ίδια ιστοσελίδα.

- Βίντεο και ήχου - Επιτρέπει την ενσωμάτωση βίντεο και ήχου στην ιστοσελίδα χωρίς τη χρήση plugin τρίτων.

- Γεωγραφική θέση - Επιτρέπει στους νέους επισκέπτες να μοιράζονται τη θέση τους με την εφαρμογή Ιστού.

4.2 Privacy στο HTML5

Το διαδίκτυο έχει γίνει αναπόσπαστο κομμάτι στις ζωές των ανθρώπων, Καθημερινά τεράστιος αριθμός ανθρώπων σερφάρουν σε αυτό. Μπορεί το διαδίκτυο να προσφέρει πολλά καλά στον άνθρωπο αλλά συνάμα κρύβει και πολλούς κινδύνους. Ένας από τους κυριότερους κινδύνους είναι αυτός της διαρροής προσωπικών δεδομένων. Έτσι το HTML θα έπρεπε να δημιουργήσει και να παρέχει στους χρήστες κάποιους μηχανισμούς για προστασία προσωπικών δεδομένων τους.
Τα Web application συμπεριφέρονται διαφορετικά στο θέμα διατήρησης του απορρήτου από μια εφαρμογή που θα κατεβάζαμε σε περιβάλλον Android. Η πρόοδος του HTML5 διευκόλυνε σε μεγάλο βαθμό την απόκτηση δεδομένων που σχετίζονται με τον χρήστη μέσω προγραμμάτων περιήγησης στο Web (π.χ. τοποθεσία, επίπεδο μπαταρίας συσκευής, πληροφορίες δικτύου). Στα web app ένα API ειδοποιά το χρήστη ότι κάποια δεδομένα του συλλέγονται, όμως οι browsers έχουν διαφορετικούς τρόπους για ειδοποιούν, με συχνότερο τρόπο την ειδοποίηση στο πάνω μέρος του παράθυρου.[15]

Το privacy στο HTML5 βασίζετε στους πιο κάτω όρους.
Consent είναι η διαδικασία απόκτησης άδειας από το χρήστη για το API για πρόσβαση στη συσκευή. Η συγκατάθεση μπορεί να είναι σιωπηρή ή ρητή. Για παράδειγμα, εάν πατήσετε ένα κουμπί "Λήψη φωτογραφίας", δίνετε σιωπηρά άδεια στην εφαρμογή να χρησιμοποιεί την κάμερα. Από την άλλη πλευρά, εάν κάνετε κλικ στο κουμπί "Στείλτε μήνυμα ηλεκτρονικού ταχυδρομείου σε έναν φίλο", δεν δίνετε σιωπηρά το API επαφών για να στέλνετε spam σε όλους στη βάση δεδομένων των επαφών σας. Κάθε API HTML5 προϋποθέτει ότι απαιτείται ρητή άδεια από προεπιλογή, αλλά καθορίζει περιστάσεις στις οποίες η σιωπηρή άδεια είναι αποδεκτή.

Το Minimization είναι η προϋπόθεση ότι τα API συμβάλλουν στη συλλογή λιγότερων πληροφοριών που απαιτούνται για μια συγκεκριμένη διεργασία.

Control είναι η δυνατότητα του χρήστη να διαχειρίζεται τις επιλογές δικαιωμάτων. Οι χρήστες πρέπει να μπορούν να ανακαλέσουν την πρόσβαση ενός browse σε μια συσκευή αφού την έχουν παραχωρήσει.

4.3 Απειλές στο HTML5

- **Απειλές από κακόβουλο κώδικα**

Οι εφαρμογές HTML5 είναι πιο πιθανό να προσθέσουν κινδύνους ασφαλείας μέσω σφάλματος προγραμματιστή. Για παράδειγμα, η εκτέλεση κακόβουλου κώδικα αποστέλλεται αυτόματα μέσω Bluetooth, Wi-Fi ή μηνυμάτων κειμένου. Αυτός ο κακόβουλος κώδικας μπορεί να συλλάβει ευαίσθητες πληροφορίες και να εκθέσει την κινητή συσκευή του θύματος σε έναν εισβολέα. Το χειρότερο, ο κακόβουλος κώδικας μπορεί να εξαπλωθεί και να αναγκάσει την εφαρμογή να εκτελέσει ανεπιθύμητες εργασίες όπως αποστολή μηνυμάτων SMS. Καθώς η χρήση αυτής της πλατφόρμας αυξάνεται, οι αδυναμίες ασφαλείας της γίνονται ένα μεγαλύτερο πρόβλημα.

Με τη χρήση λανθασμένων API, οι προγραμματιστές κάνουν τις εφαρμογές ευάλωτες και ως εκ τούτου μπορούν να στείλουν κακόβουλο κώδικα στη μηχανή JavaScript για εκτέλεση. Η επιλογή των σωστών API είναι ζωτικής σημασίας για την αποφυγή αυτής της παραβίασης ασφάλειας.

Εκτός από το σφάλμα προγραμματιστή, κακόβουλος κώδικας μπορεί να εισαχθεί σε μια εφαρμογή μέσω εικόνων και αρχείων μουσικής , κωδικών QR, μετάδοσης Bluetooth και πεδίων SSID που μεταδίδονται μέσω Wi-Fi. Τα μηνύματα SMS που εμφανίζονται από την εφαρμογή μπορούν επίσης να περιέχουν κακόβουλο κώδικα.

- **Middleware**

Οι εφαρμογές HTML5 συχνά χρειάζονται ένα πλαίσιο ενδιάμεσου λογισμικού για να είναι πολλαπλές πλατφόρμες. Αυτό το μεσαίο λογισμικό είναι ένας από τους τρόπους με τους οποίους το JavaScript μπορεί να καλέσει το λειτουργικό σύστημα στη μητρική του γλώσσα. Αυτό το μεσαίο λογισμικό ευθύνεται για κακόβουλες επιθέσεις έγχυσης κώδικα γνωστές ως XSS (cross-site scripting) καθώς το Middleware δέχεται δεδομένα και κώδικα και εκτελεί το τελευταίο αυτόματα.

Ο κίνδυνος είναι μεγαλύτερος σε κινητές συσκευές λόγω των αδειών που δίνουμε σε εφαρμογές, όπως πρόσβαση σε λίστες επαφών, δεδομένα τοποθεσίας και κάμερες. Δεν

είναι μόνο εφαρμογές HTML5 που εκθέτουν τους χρήστες σε ζητήματα ασφαλείας, αλλά ένα πρόβλημα που επηρεάζει γενικά τις εφαρμογές.

- **Third Party Code**

Ένα άλλο ζήτημα ασφάλειας για προγραμματιστές στο HTML5 προέρχεται από τη χρήση κωδικών τρίτων. Το HTML5 είναι γνωστό ότι προσφέρει δυναμισμό στην ανάπτυξη ιστού με τη χρήση κωδικών τρίτων και αυτό ανοίγει πιθανές ευπάθειες για τον ιστότοπο. Στις προηγούμενες εκδόσεις της γλώσσας σήμανσης, η JavaScript είχε περιορισμένη χρήση για την υποβολή αιτημάτων που προέρχονται από τον τομέα. Για παράδειγμα, οι προηγούμενες εκδόσεις HTML δεν επέτρεπαν σε σελίδες από έναν τομέα να μεταβιβάζουν ή να έχουν πρόσβαση σε δεδομένα σε σελίδες από άλλον τομέα. Αυτό εμπόδισε έναν κακόβουλο ιστότοπο να ερμηνεύει τα δεδομένα από έναν νόμιμο ιστότοπο με τη μορφή αναδυόμενων παραθύρων. Στο HTML5, το JavaScript ζητά πόρους από διαφορετικούς τομείς με μια νέα μέθοδο γνωστή ως κοινή χρήση πόρων (CORS). Εδώ η JavaScript μπορεί να έχει πρόσβαση σε πληροφορίες από πολλούς τομείς ταυτόχρονα. Αυτό επιτρέπει σε έναν ιστότοπο να προσφέρει πληροφορίες από πολλούς τομείς ταυτόχρονα. Ωστόσο, το HTML5 δεν διαθέτει κανένα μηχανισμό για τον έλεγχο της προέλευσης του περιεχομένου. Αυτό προσφέρει μια μεγάλη ευκαιρία στους χάκερ να έχουν πρόσβαση σε πληροφορίες τόσο από τον διακομιστή όσο και από τους πελάτες.

4.4 Τρόποι Αντιμετώπισης

Οι σωστές στρατηγικές σχεδιασμού δεν πρέπει να περιέχουν καθόλου ή ελάχιστη αποθήκευση δεδομένων και να ελαχιστοποιούν τη λογική στον πελάτη, διατηρώντας κωδικούς πρόσβασης, διακριτικά, προφίλ ασφαλείας και διαπιστευτήρια στον διακομιστή. Η εστίαση πρέπει να είναι στην αλληλεπίδραση UI με τον διακομιστή. Είναι δυνατή η ανάπτυξη ασφαλών εφαρμογών HTML5 χωρίς να αφήνονται δεδομένα πίσω στην κρυφή μνήμη.

Οι προγραμματιστές πρέπει να γνωρίζουν τις πιο ισχυρές απειλές για την ασφάλεια των κινητών συσκευών και να προστατεύουν τις εφαρμογές τους. Ένας άλλος χρήσιμος

πόρος είναι η λεπτομερής κατευθυντήρια γραμμή για ασφαλή ανάπτυξη κινητών από το PCI SSC (Συμβούλιο Προτύπων Ασφάλειας Βιομηχανίας Κάρτας Πληρωμών).

Η τεχνολογία κινητής τηλεφωνίας σας πρέπει να παρέχει ένα πλαίσιο ελέγχου ταυτότητας και ισχυρές δυνατότητες ασφαλείας, όπως:

- Κρυπτογράφηση στη συσκευή
- Ασφαλής επικοινωνία πελάτη / διακομιστή
- Έλεγχος πρόσβασης
- Έλεγχος ταυτότητας εκτός σύνδεσης

Οι εφαρμογές πολλαπλών πλατφορμών είναι ένας από τους βαθμούς ανάπτυξης εφαρμογών για κινητά, αλλά ποτέ δεν συμβιβάζονται σε θέματα ασφάλειας και εμπειρίας χρήστη. Ένας τρόπος για να το επιτύχετε αυτό είναι να εστιάσετε στην ενοποίηση μεταξύ της εφαρμογής, των χαρακτηριστικών της πλατφόρμας cloud και των υπηρεσιών απομακρυσμένου ελέγχου ταυτότητας και να τις συνδυάσετε με τις βέλτιστες πρακτικές ασφαλείας που ισχύουν για την ανάπτυξη ιστού.

Κεφάλαιο 5

Τεχνολογίες και Εργαλεία

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα γίνει αναφορά στις τεχνικές που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής AppPrivacyAnalyzer. Η εφαρμογή αποφασίστηκε να είναι εφαρμογή Android, δηλαδή για κινητές συσκευές. Η εφαρμογή αναπτύχθηκε με τη βοήθεια του Android Studio. Θα γίνει αναφορά για τις γλώσσες προγραμματισμού που χρησιμοποιήθηκαν αλλά και πως χρησιμοποιήθηκαν κάποια εργαλεία για εκπλήρωση του στόχου της εφαρμογής.

5.2 Γλώσσες Προγραμματισμού

Java

Η Java είναι μια γλώσσα προγραμματισμού υψηλού επιπέδου που αναπτύχθηκε αρχικά από την Sun Microsystems και κυκλοφόρησε το 1995. Η Java λειτουργεί σε διάφορες πλατφόρμες, όπως Windows, Mac OS και διάφορες εκδόσεις του UNIX. [15] Στη παρούσα εργασία η Java ήταν απαραίτητη αφού για ανάπτυξη μιας εφαρμογής στο Android Studio είναι απαραίτητη.

Ο κώδικας της Java τρέχει σε μια εικονική μηχανή γνωστή ως Java Virtual Machine. Το JVM έχει δύο κύριες λειτουργίες: να επιτρέπει στα προγράμματα Java να εκτελούνται

σε οποιαδήποτε συσκευή ή λειτουργικό σύστημα και να διαχειρίζεται και να βελτιστοποεί τη μνήμη του προγράμματος.[6]

Python

Η Python είναι μία αντικειμενοστρεφής, γλώσσα προγραμματισμού υψηλού επιπέδου με δυναμική σημασιολογία. Οι ενσωματωμένες δομές δεδομένων υψηλού επιπέδου, σε συνδυασμό με τη δυναμική πληκτρολόγηση και τη δυναμική δέσμευση, την κάνουν πολύ χρήσιμη για την ταχεία ανάπτυξη εφαρμογών, καθώς και χρήσιμη για σύνδεση ήδη υπάρχοντών προγραμμάτων. Άλλο γεγονός που τη καθιστά ως μια καλή επιλογή είναι ο μεγάλος αριθμός βιβλιοθηκών που χρησιμοποιεί.

Στη παρούσα διπλωματική εργασία είναι γραμμένα σε python κάποια μικρά scripts που βοηθούν στη συνένωση των εργαλείων στο βασικό πρόγραμμα.

PHP

Η PHP είναι μια γλώσσα δέσμης ενεργειών από διακομιστή. που χρησιμοποιείται για την ανάπτυξη στατικών ιστότοπων ή δυναμικών ιστότοπων ή εφαρμογών Web [19]. Δημιουργήθηκε αρχικά από τον Δανό-Καναδό προγραμματιστή Rasmus Lerdorf το 1994 και συνεχίζει να αναπτύσσετε από το “The PHP Group”.

Έγινε χρήση της PHP για συνένωση του εργαλείο Google-Play-Scraber με το κώδικα Java αφού η εκτέλεση των εντολών που παρέχει το εργαλείο γίνετε σε κώδικα PHP. Μια πιο κλασική χρήση της PHP, που χρησιμοποιείται και στη συγκεκριμένη εφαρμογή είναι η ένωση με τη βάση δεδομένων που χρησιμοποιείται από το σύστημα.

Node.js

Το Node.js είναι ένα runtime περιβάλλον ανοιχτού κώδικα, πολλαπλών πλατφορμών, back-end, που εκτελεί κώδικα JavaScript . Αυτό που ξεχωρίζει τη συγκεκριμένη γλώσσα προγραμματισμού είναι ο τρόπος που λειτουργεί με τα callbacks του Javascript.

Ο κώδικας του εργαλείου Google-Play-Scraper που χρησιμοποιήθηκε στην εφαρμογή, είναι Node.js. Η απλότητα τη βοήθησε στη ευκολότερη χρήση του εργαλείου.

5.3 Βάση δεδομένων

MySQL

Η MySQL είναι ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων ανοιχτού κώδικα. Το όνομά του είναι ένας συνδυασμός του "My", του ονόματος της κόρης του συνιδρυτή Michael Widenius και του "SQL", της συντομογραφίας για τη Structured Query Language. Η MySql είναι το πλέον διαδεδομένο σύστημα διαχείρισης βάσεων δεδομένων και αυτό παρέχετε δωρεάν και σχεδόν σε όλα τα λειτουργικά συστήματα.

Για αποθήκευση δεδομένων που χρειάζονταν για την παρούσα διπλωματική εργασία και την Android εφαρμογή που δημιουργήθηκε μια βάση δεδομένων με χρήση της phpMyAdmin, η οποία είναι ένα δωρεάν και ανοιχτού κώδικα εργαλείο διαχείρισης για την MySQL.

5.4 Εργαλεία

google-play-scraper

Το Google-Play-Scraper είναι ένα εργαλείο που έχει ως σκοπό τη συλλογή δεδομένων από το Google Play. Αποτελεί ένα Node.js module και κάθε λειτουργεία του αποτελεί και ένα JavaScript αρχείο. Το συγκεκριμένο εργαλείο παρέχετε σε μορφή ανοιχτού κώδικα στο Github. [18]

Όπως αναφέρθηκε και πιο πάνω το Google-Play-Scraper αποτελείται από διάφορα JavaScript αρχεία τα οποία αποτελούν και μια μέθοδο η οποία εκτελεί μια διεργασία. Οι μέθοδοι που προσφέρονται είναι οι πιο κάτω:

- app: Ανακτά την πλήρη λεπτομέρεια μιας εφαρμογής.
- list: Ανακτά μια λίστα εφαρμογών από μία από τις συλλογές στο Google Play.

- search: Ανακτά μια λίστα εφαρμογών που είναι αποτελέσματα αναζήτησης βάσει του δεδομένου όρου.
- developer: Επιστρέφει τη λίστα εφαρμογών με το δεδομένο όνομα προγραμματιστή.
- suggest: Με δεδομένη μια συμβολοσειρά επιστρέφεται έως και πέντε πρόταση για την ολοκλήρωση ενός όρου ερωτήματος αναζήτησης.
- reviews: Με δεδομένη μια συμβολοσειρά επιστρέφεται έως και πέντε πρόταση για την ολοκλήρωση ενός όρου ερωτήματος αναζήτησης.
- similar:Επιστρέφει μια λίστα παρόμοιων εφαρμογών με αυτήν που καθορίστηκε.
- permissions: Επιστρέφει τη λίστα δικαιωμάτων στα οποία έχει πρόσβαση μια εφαρμογή.
- categories: Ανακτά μια πλήρη λίστα κατηγοριών που υπάρχουν από το αναπτυσσόμενο μενού στο Google Play.

Στόχος τη διπλωματικής εργασίας ήταν η ανεύρεση των permissions που χρησιμοποιεί μια εφαρμογή, άρα έγινε χρήση της μεθόδου permissions αφού ο χρήστης θα μπορεί να ψάξει τα στοιχεία για οπουδήποτε application χρειάζεται.

Κεφάλαιο 6

Υλοποίηση Εφαρμογής

6.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο θα γίνει επεξήγηση του πως αναπτύχθηκε η Android εφαρμογή AppPrivacyAnalyzer. Η εφαρμογή έχει ως στόχο να ενημερώνει τον εκάστοτε χρήστη για το τι permission χρησιμοποιεί μια εφαρμογή είτε αυτή είναι μια android εφαρμογή είτε είναι μια Android εφαρμογή είτε είναι μια Web εφαρμογή.

Ο χρήστης θα μπορεί να αναλύσει την εφαρμογή την οποία ψάχνει, δηλαδή θα του δίνετε επεξήγηση για το τι δεδομένα μπορεί να συλλέξει η εφαρμογή ανάλογα με τα permissions που ζητούνται. Αφού η εφαρμογή απευθύνεται σε γονιούς και παιδιά δίνετε μια πιο απλοϊκή επεξήγηση της επικινδυνότητας του κάθε permission δίνοντας βάση στα dangerous permissions. Ο χρήστης μπορεί να αναζητήσει οποιαδήποτε εφαρμογή θέλει από το Google Play με τη βοήθεια ενός search bar. Η αντίστοιχη λειτουργεία για web app γίνετε με τη βοήθεια του URL.

Μια άλλη λειτουργία που προσφέρει η εφαρμογή είναι ο εντοπισμός των permissions που χρησιμοποιούν οι ήδη εγκατεστημένες εφαρμογές. Αυτό γίνετε για να μπορεί ο

χρήστης να δει τι permissions έχει ήδη κάνει αποδεκτά από προηγουμένως. Η εφαρμογή δίνει μια απλή εξήγηση γι' αυτά τα permissions και για το κατά πόσο μπορεί να είναι επικίνδυνα για τα προσωπικά τους δεδομένα.

Η τελευταία λειτουργία που προσφέρεται είναι πολύ σημαντική αφού ο χρήστης αναζητώντας κάποια εφαρμογή που προσφέρεται του Google Play, θα μπορεί να δει αν τα permissions που ζητά αυτή η εφαρμογή, έχουν γίνει αποδεκτά από πριν για τη χρήση κάποιας άλλης εφαρμογής. Αυτό θα βοηθήσει το χρήστη αρχικά, να μπορεί πρώτον, να μην ελέγξει ενδελεχώς όλα τα permissions της εκάστοτε εφαρμογής αφού ήδη τα αποδέχτηκε και δεύτερον να καταλάβει αν αυτή η εφαρμογή είναι πιο οικεία σε αυτόν.

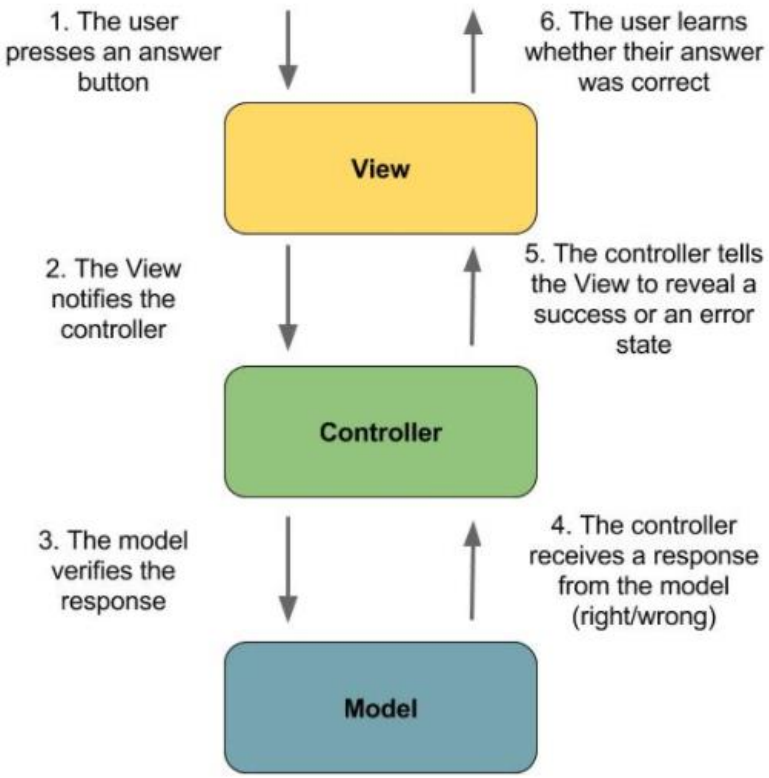
Στη συνέχεια, αρχικά θα γίνει επεξήγηση της αρχιτεκτονικής που χρησιμοποιήθηκε για ανάπτυξη της εφαρμογής και μετέπειτα θα γίνει εξήγηση του πως υλοποιήθηκε η κάθε λειτουργεία που προσφέρει η εφαρμογή AppPrivacyAnalyzer.

6.2 Αρχιτεκτονική Εφαρμογής

Όπως και στις περισσότερες Android εφαρμογές έτσι και στην AppPrivacyAnalyzer χρησιμοποιήθηκε για την ανάπτυξη της το μοντέλο αρχιτεκτονικής MVC (Model-View-Controler). Η τεχνική MVC χωρίζει τον κώδικα σε 3 συστατικά:[20]

- **Model**: περιέχει δεδομένα εφαρμογών και επιχειρηματική λογική (οι κανόνες του συστήματος). Για παράδειγμα, λογαριασμοί χρηστών, προϊόντα που πουλάτε, ένα σύνολο φωτογραφιών κ.λπ. Το model δεν γνωρίζει τη διεπαφή. Στην εφαρμογή AppPrivacyAnalyzer το Model αποτελούν οι κλάσεις της Java.
- **View**: είναι υπεύθυνο για ότι μπορεί να δει ο χρήστης στην οθόνη του και προσφέρει την αλληλεπίδραση του χρήστη με την εφαρμογή. Στην εφαρμογή AppPrivacyAnalyzer το View είναι υλοποιημένο με XML.
- **Controller:** είναι η σύνδεση μεταξύ της View και του Model, το οποίο διαχειρίζεται επίσης τη λογική της εφαρμογής. Ο Controller αντιδρά στην είσοδο του χρήστη και παρουσιάζει τα δεδομένα που ζητά ο χρήστης. Παίρνει κάποια

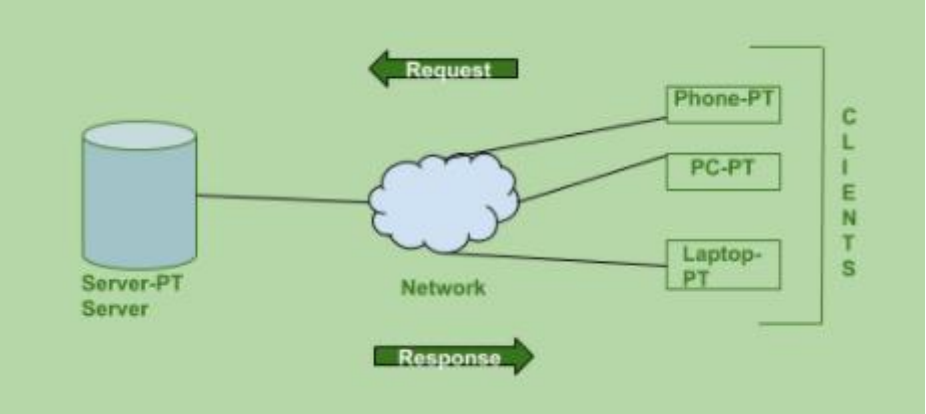
είσοδο από το View, ανακτά τα δεδομένα από το Model και τα παρουσιάζει ξανά μέσω του View.



Εικόνα 6.1 Λειτουργία MVC μοντέλου στη πράξη.

Εκτός όμως από την αρχιτεκτονική MVC που χρειάστηκε για το κτήσιμο της εφαρμογής στο Android, χρησιμοποιήθηκε και το μοντέλο αρχιτεκτονικής Client-Server για ανταλλαγή μηνυμάτων με τον server.

Το μοντέλο Client-Server είναι μια κατανεμημένη δομή εφαρμογών που χωρίζει εργασίες ή φόρτο εργασίας μεταξύ των παρόχων ενός πόρου ή υπηρεσίας, που ονομάζεται server και των αιτούντων υπηρεσιών που ονομάζονται client. Στην αρχιτεκτονική client-server, όταν ο client στέλνει ένα αίτημα για δεδομένα στον server μέσω του Διαδικτύου, ο server αποδέχεται τη ζητούμενη διαδικασία και παραδίδει τα πακέτα δεδομένων που ζητήθηκαν πίσω στον client. Οι client δεν μοιράζονται κανέναν από τους πόρους τους. Παραδείγματα μοντέλου client-server είναι το ηλεκτρονικό ταχυδρομείο, το World Wide Web κ.λπ.[21]



Εικόνα 6.2 Διάγραμμα λειτουργίας μοντέλου Client-Server

6.3 Android Permissions

Αποτελεί τη βασικότερη λειτουργία της εφαρμογής. Ο χρήστης μπορεί μέσω ενός Search Bar να αναζητήσει οποιαδήποτε εφαρμογή επιθυμεί από το Google Play. Στη συνέχεια αφού επιλέξει τη εφαρμογή που θέλει θα μπορεί να δει τα permissions που χρησιμοποιεί και ποια από αυτά τα permissions είναι επικίνδυνα.

Η λειτουργία αυτή χωρίζεται σε δύο υπολειτουργίες. Αρχικά, τη προσπάθεια να πάρουμε στοιχεία των εφαρμογών από το Google Play και στη συνέχεια με αυτά τα στοιχεία να μπορούμε να βρούμε τα permissions που χρησιμοποιούν οι εφαρμογές. Η υλοποίηση αυτων των υπολειτουργιών εξηγείται στα πιο κάτω υποκεφάλαια.

6.3.1 Αναζήτηση Εφαρμογής στο Google Play

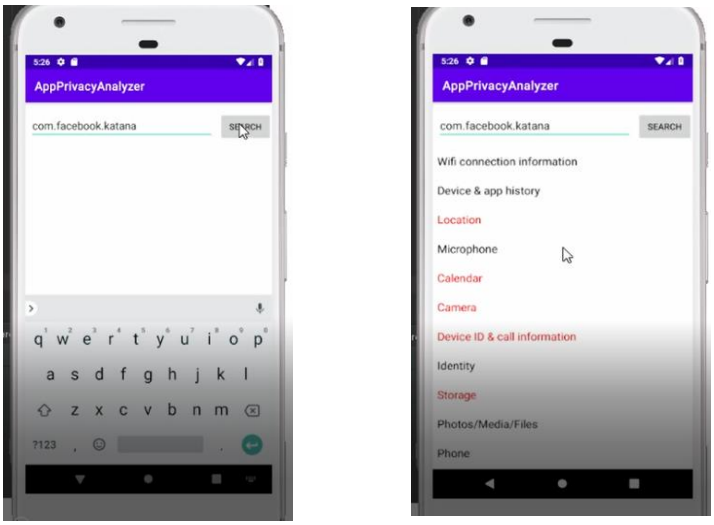
Στόχος αυτής της λειτουργίας είναι να συλλέξουμε στοιχεία από το Google Play που είναι η εφαρμογή όπου κάποιος χρήστης μπορεί να κατεβάσει οποιαδήποτε εφαρμογή επιθυμεί. Αυτό δεν μπορούσε να γίνει εύκολα κατορθωτό αφού το API του Google Play δεν είναι προσβάσιμο. Έτσι έγινε συγχρονισμός ενός search bar που δημιουργήθηκε στο Android Studio με αυτό του Google Play αυτός ο συγχρονισμός δεν είναι 100% επιτυχείς άρα δίνετε στο χρήστη η επιλογή να δώσει το όνομα της εφαρμογής που θέλει να αναλύσει ή και το όνομα του package της εφαρμογής. Στα μελλοντικά σχέδια της εφαρμογής είναι η επιδιόρθωση αυτού του προβλήματος ούτως ώστε να διευκολύνει τη διαδικασία εύρεση μιας εφαρμογής.

6.3.2 Εύρεση και επεξήγηση Permissions

Αφού πάρουμε με τη βοήθεια της πιο πάνω λειτουργίας παίρνουμε το όνομα μια εφαρμογής, δηλαδή το όνομα του package τότε μπορούμε να το χρησιμοποιήσουμε και με τη χρήση του εργαλείου Google-Play-Scraper να βρούμε τα permissions που χρησιμοποιεί. Ο τρόπος που υλοποιείται αυτή η λειτουργεία είναι με κλήση μέσω του κώδικα Java της Android εφαρμογής σε ένα PHP Web Server. Σε αυτό τον Server εκτελείται μια Python εντολή μέσω της εντολής shellexec(). Στη python μπορούμε να εκτελέσουμε ένα JavaScript αρχείο ενός Node.js εργαλείου μέσω της εντολής muterun_js(). Με αυτό το τρόπο επιτυγχάνεται η χρήση του εργαλείου Google-Play-Scraper.

Η λειτουργία υλοποιείται με τη χρήση της μεθόδου permissions() που δέχεται ως είσοδο το όνομα του package της εφαρμογής που έχει επιλέξει ο χρήστης. Αφού έχουμε τα permissions που παίρνουμε από τη μέθοδο στον PHP Web Server στον οποίο εκτελείται η εντολή τότε αποστέλλονται στον Java κώδικα και παρουσιάζονται στο χρήστη. Αν ο χρήστης θέλει τελικά να κατεβάσει την εφαρμογή του δίνετε η δυνατότητα μέσω ενός Intent και ένωσης του με το Google Play.

Τέλος, η εφαρμογή δίνει τη δυνατότητα στο χρήστη ποια από αυτά τα permissions θεωρούνται dangerous. Αυτό επιτυγχάνεται με σύγκριση των permissions που χρησιμοποιεί η εφαρμογή που επέλεξε ο χρήστης με τα dangerous permissions μέσω της Java.



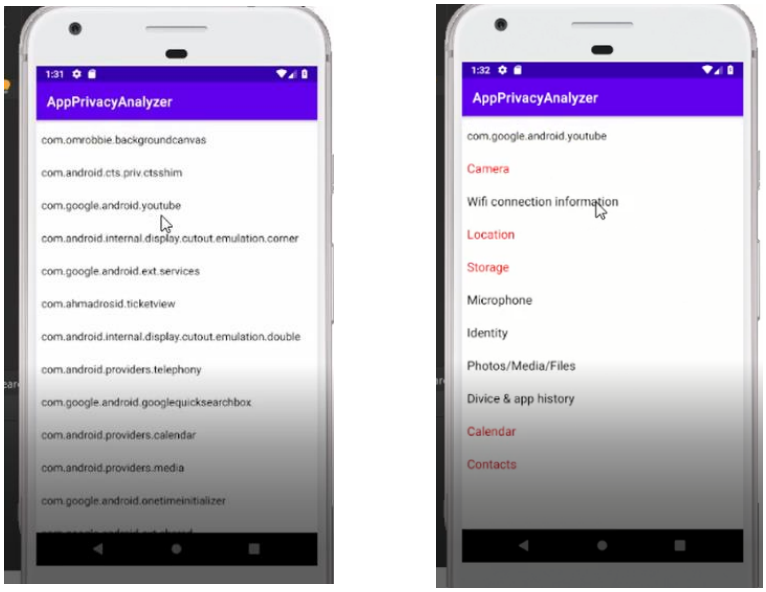
Εικόνα 6.3 Λειτουργία 1 Εύρεση Permissions

6.4 Permissions εγκατεστημένων εφαρμογών

Με αυτή τη λειτουργία θα μπορεί ο χρήστης να δει τις εφαρμογές που έχει εγκατεστημένες στη συσκευή του. Στη συνέχεια αφού επιλέξει μια συγκεκριμένη εφαρμογή θα μπορεί να δει τα permissions που χρησιμοποιεί.

Η εύρεση των εφαρμογών που είναι εγκατεστημένες στη συσκευή υπάρχουν σε μία σελίδα της εφαρμογής σε μορφή λίστας. Οι εφαρμογές αυτές συλλέγονται από τη συσκευή μέσω της μια κλάσης της Java. Στη σελίδα αυτή δίνετε η δυνατότητα στο χρήστη να αναζητήσει μια εφαρμογή ούτως ώστε να αποφεύγει την δια χειρός αναζήτηση(scroll down). Αυτό επιτυγχάνεται με τη χρήση ενός searchbar, έτσι ο χρήστης μπορεί να δακτυλογραφήσει το όνομα της εφαρμογής που ψάχνει και με τη χρήση της συνάρτησης onQueryTextChange() που παρέχετε στα SearchView εργαλεία, θα του εμφανιστεί η εφαρμογή που αντιστοιχεί στο όνομα που πληκτρολόγησε. Η εύρεση των εφαρμογών επιτυγχάνετε με τη χρήση μιας λειτουργίας του Android το package manager και της εντολής getInstalldesApplication.

Στη συνέχεια, αφού επιλέξει την εφαρμογή θα του εμφανιστούν τα Permissions που χρησιμοποιεί η συγκεκριμένη εφαρμογή. Αυτό θα γίνει πάλι με τη χρήση του εργαλείου Google-Play-Scraper όπως περιγράφεται πιο πάνω. Με χρήση της μεθόδου permissions() του εργαλείου που θα δεχθεί ως είσοδο το package της ήδη εγκατεστημένης εφαρμογής.



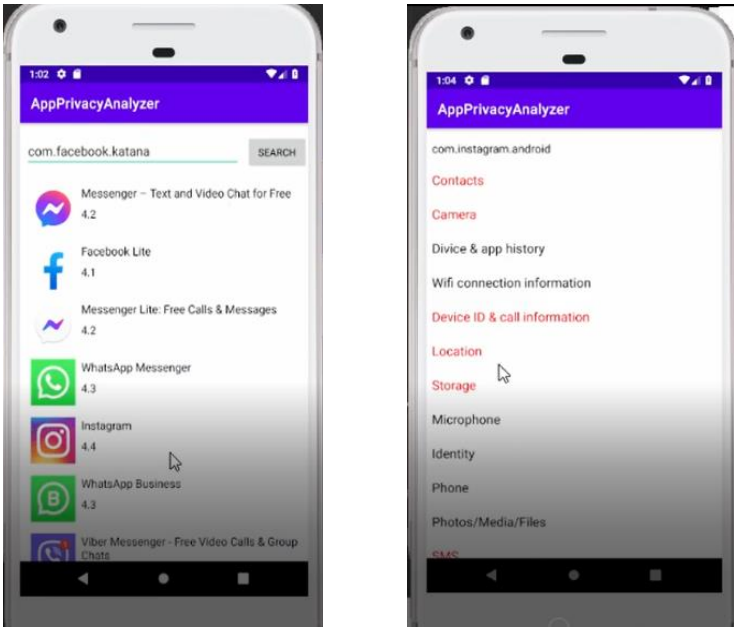
Εικόνα 6.4 Λειτουργία 2 Εύρεση Permissions Εγκατεστημένων Εφαρμογών

6.5 Σύγκριση Permissions εφαρμογών

Όπως αναφέρεται και πιο πάνω ο χρήστης θα μπορεί να ψάξει μια εφαρμογή από το Google Play και θα μπορεί να συγκρίνει αν τα permissions που ζητήθηκαν από ήδη εγκατεστημένες συσκευές. Αυτό επιτυγχάνετε βρίσκοντας όλα τα Permissions που έγιναν ήδη αποδεκτά από το χρήστη. Στη συνέχεια γίνετε σύγκριση των Permissions της εφαρμογής που αναζητήθηκε από το χρήστη με αυτά. Τα ίδια permissions παρουσιάζονται στον χρήστη σε μορφή λίστας.

Αν και δεν ήταν στα αρχικά πλάνα της εφαρμογής, μετά από έρευνα[23] που πραγματοποιήθηκε πάρθηκε η απόφαση να υλοποιηθεί και κάπως αντίστροφη λειτουργία με αυτή που περιγράφετε πιο πάνω. Αυτή η λειτουργία επιτρέπει στο χρήστη να επιλέξει μια εφαρμογή της επιθυμίας του και να συγκρίνει τα permission που χρησιμοποιεί με άλλες παρόμοιες εφαρμογές που υπάρχουν στο Google Play. Για υλοποίηση γίνετε χρήση του εργαλείου Google-Play-Scraper.

Η λειτουργία υλοποιείται με τη χρήση της μεθόδου similar() που δέχεται ως είσοδο το όνομα του package της εφαρμογής που έχει επιλέξει ο χρήστης αυτό μας εμφανίζει κάποιο αριθμό παρόμοιων εφαρμογών. Στη συνέχεια για να βρεθούν τα permissions της κάθε παρόμοιας εφαρμογής που βρέθηκε εκτελείται η μεθόδου permissions() με είσοδο το package κάθε εφαρμογής. Οι μέθοδοι του εργαλείου Google-Play-Scraper εκτελούνται σε PHP Web server όπως εξηγείται και πιο πάνω.
Στη συνέχεια, γίνετε σύγκριση στον PHP Web server των permissions των εφαρμογών αυτών με αυτά της εφαρμογής που επέλεξε ο χρήστης. Οι εφαρμογές που έχουν σύνολο ίδιων permissions επιστρέφονται στην εφαρμογή.



Εικόνα 6.5 Λειτουργία 3 Σύγκριση Permissions

6.6 Web εφαρμογές

Αποτελεί τη δεύτερη πιο βασική λειτουργία της εφαρμογής AppPrivacyAnalyzer. Ο χρήστης αφού εισάγει το URL της Web εφαρμογής που θέλει να δει τα δικαιώματα που ζητούνται από τη συγκεκριμένη εφαρμογή. Αυτό γίνετε με τη χρήση Permissions API όπου μέσω το API της κάθε εφαρμογής εντοπίζονται αν έγιναν request για Permissions.

Κεφάλαιο 7

Συμπεράσματα

7.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα γίνει μια ανασκόπηση των συμπερασμάτων της διπλωματικής εργασίας αλλά και ένα γενικό συμπέρασμα και μια ανασκόπηση για μελλοντική εργασία που μπορεί να γίνει στη συνέχεια.

Για εξαγωγή συμπερασμάτων δόθηκε η εφαρμογή σε κάποιο αριθμό χρηστών. Στη συνέχεια αυτοί οι χρήστες κλήθηκαν να απαντήσουν σε ένα ερωτηματολόγιο. Στο ερωτηματολόγιο κλήθηκαν να απαντήσουν σε ερωτήσεις για το τι γνωρίζουν για θέματα ιδιωτικότητας στις Android συσκευές αλλά και στις web εφαρμογές. Στο τέλος υπάρχουν ερωτήσεις σχετικές με το AppPrivacyAnalyzer. Τα αποτελέσματα παρουσιάζονται σε γραφήματα πιο κάτω.

7.2 Αποτελέσματα Ερωτηματολογίου

Μετά την ολοκλήρωση της, η εφαρμογή δόθηκε για δοκιμή σε 20 χρήστες Android συσκευών ηλικίας 18-41 ετών, έγινε αρχικά προσπάθεια οι χρήστες αυτοί να είναι παιδιά οι γονείς, όμως λόγω δυσκολιών που υπήρξαν, η εφαρμογή δόθηκε στον οικογενειακό μου κύκλο και σε φίλους. Μετά από χρήση της εφαρμογής κλήθηκαν να απαντήσουν σε ερωτηματολόγιο 30 ερωτήσεων. Το ερωτηματολόγιο χωριζόταν σε 5 μέρη. Περιλάμβανε ερωτήσεις δημογραφικού χαρακτήρα, ερωτήσεις για τον τρόπο

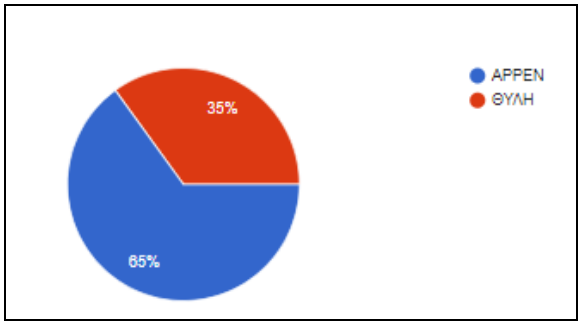
χρήσης Android συσκευών, την ασφάλεια και την ιδιωτικότητα που πιστεύουν ότι τους προσφέρει μια Android συσκευή και το διαδίκτυο και τέλος αξιολόγηση της εφαρμογής AppPrivacyAnalyzer.

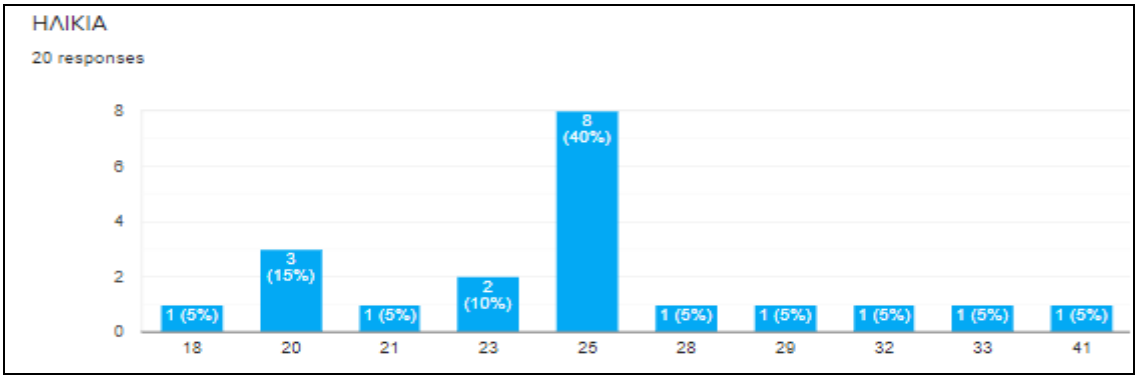
Το ερωτηματολόγιο δημιουργήθηκε με τη χρήση του Google Form και ήταν προσβάσιμο μέσω link. Όλες οι πληροφορίες δόθηκαν εμπιστευτικά, παρόλα αυτά ενθαρρύνθηκαν οι συμμετέχοντες να απαντήσουν με ακρίβεια.

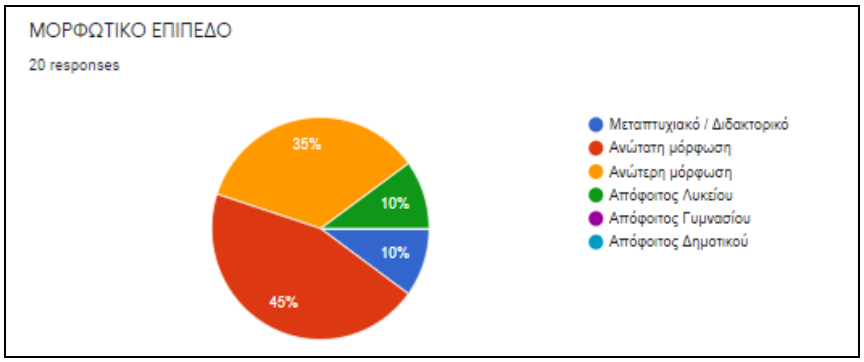
Σκοπός της μελέτης είναι να διερευνηθεί η χρησιμότητα της εφαρμογής AppPrivacyAnalyzer και κατά πόσο βοήθησε τους χρήστες να κατανοήσουν θέματα ιδιωτηκότητας και προστασίας προσωπικών δεδομένων.

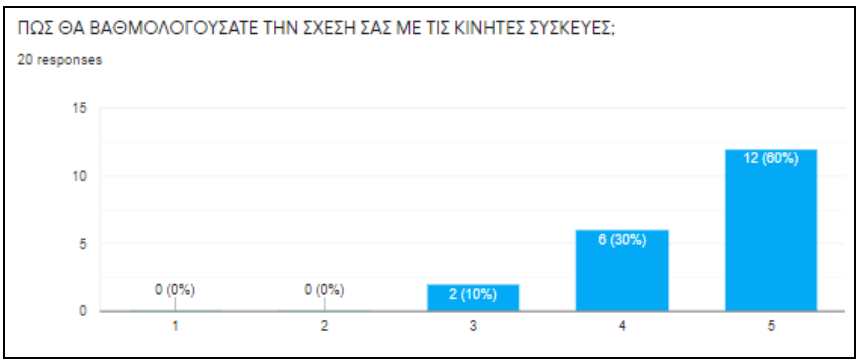
Η στατιστική ανάλυση των δεδομένων που συλλέχθηκαν έγινε με τη βοήθεια του Google Form όπως επίσης και οι γραφικές παραστάσεις τις οποίες παραθέτω στη συνέχεια.

Το δείγμα μας περιλαμβάνει κυρίως άρρενες με μέσω όρο ηλικίας τα 25,4 έτη, οι οποίοι στη συντριπτική τους πλειοψηφία σπουδάζουν ή αποφοίτησαν από μια ανώτερη ή ανώτατη σχολή. Οι περισσότεροι θεωρούν ότι η σχέση τους με τις κινητές τους συσκευές είναι αρκετά καλή.





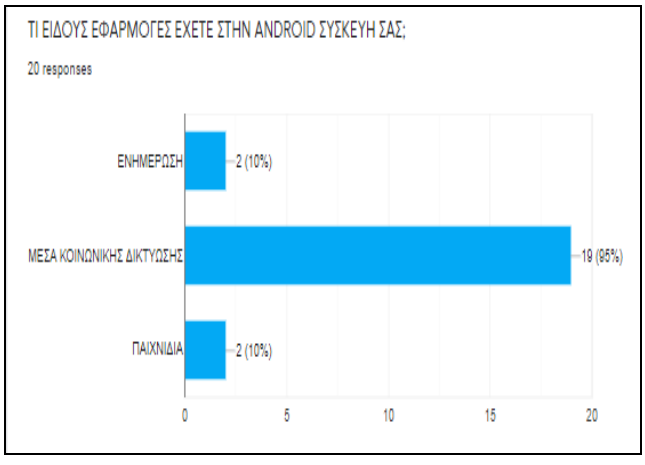


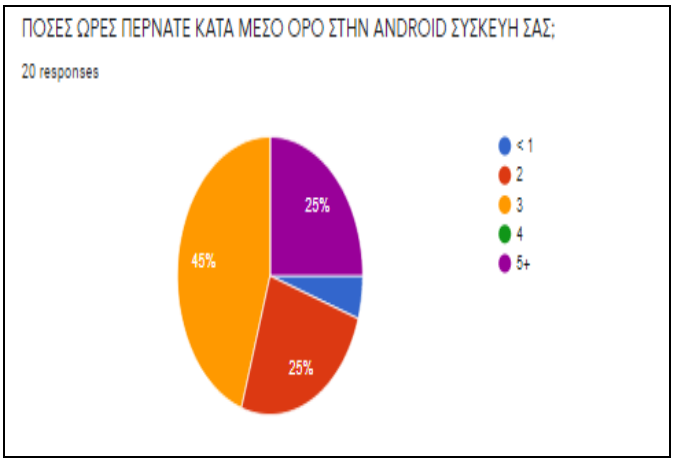


Γραφικές Παραστέσεις 7.1 Δημογραφικών Ερωτήσεων

Οι περισσότεροι χρησιμοποιούν (95%) τις Android συσκευές για περιήγηση στα μέσα κοινωνικής δικτύωσης. Αυτό καθίστατε εύλογο αν αναλογιστεί κανείς ότι πρόκειται για άτομα νεαρής ηλικίας. Οι λόγοι που επιλέγουν τα Android λογισμικά ποικίλουν, με τις δημοφηλέστερες να είναι η ευκολία στη χρήση, η αξιοπιστία και η μεγαλύτερη εξοικίωση.

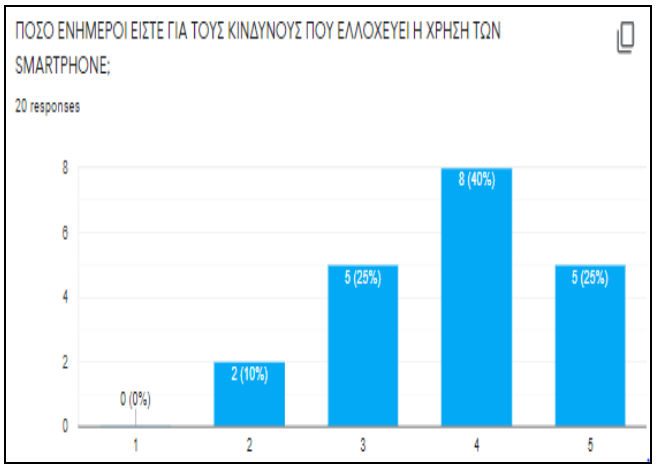
Το 70% των χρηστών ασχολούνται με το κινητό τους τηλέφωνο συνολικό 2-3 ώρες καθημερινά, ενώ το 25% τουλάχιστον πέντε ώρες και η κύρια ενασχόληση τους είναι τα μέσα κοινωνικής δικτύωσης.

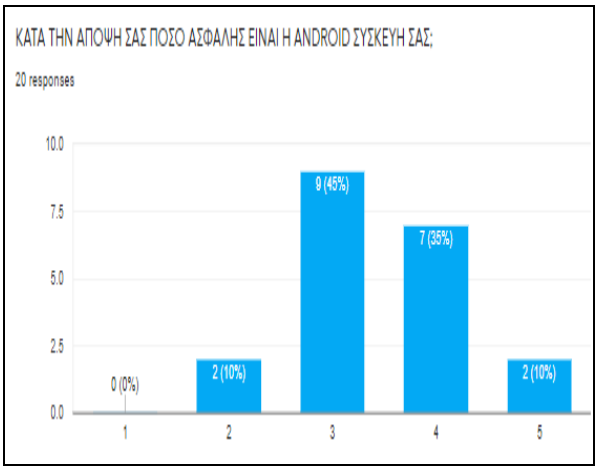


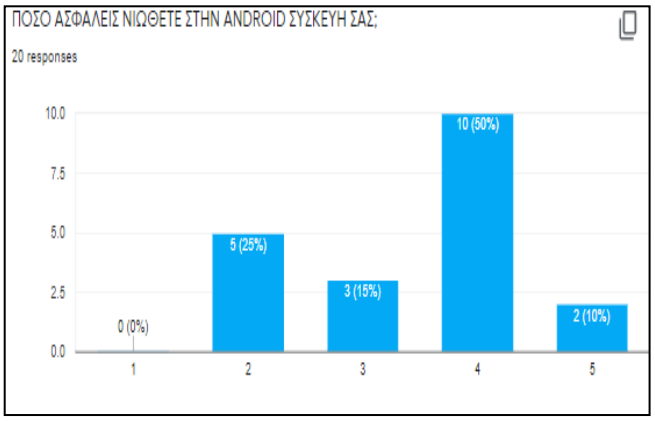


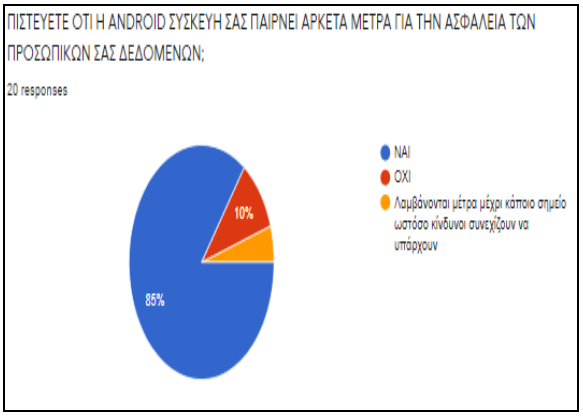
Γραφικές Παραστέσεις 7.2 Ερωτήσεις για χρήση smartphone

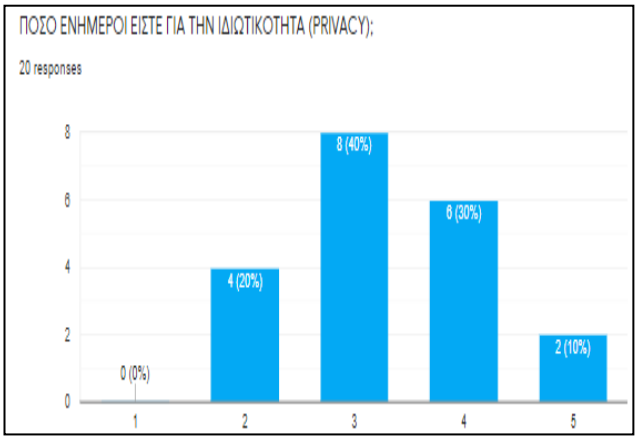
Στη συνέχεια παραθέτω δεδομένα όσον αφορά τις απόψεις καθώς επίσης και την επίγνωση τους σε θέματα ασφάλειας και ιδιωτικότητας στο Android. Παρατηρούμε ότι ένα πολύ μικρό ποσοστό των συμμετεχόντων είναι λίγο έως καθόλου ενήμεροι όσον αφορά τους κινδύνους που ελλοχεύουν από τη χρήση των Android εφαρμογών κάτι το οποίο ισχύει και γενικότερα για τα θέματα ιδιωτικότητας. Το 90% θεωρούν την Android συσκευή μέτρια ως αρκετά ασφαλή, ενώ ελαφρώς χαμηλότερο είναι το ποσοστό αυτών που νιώθουν ασφαλείς με τη συσκευή τους καθώς πιστεύουν ότι η Android συσκευή τους παίρνει αρκετά μέτρα για την ασφάλειά τους. Τέλος, παρόλο που όλοι θεωρούν την Android μέτρια έως αρκετά επικίνδυνη για παραβίαση της ιδιωτικότητας τους, εντούτοις ένα ποσοστό 40% καταβάλλει μια μέτρια προσπάθεια και το 30% σχεδόν καθόλου για την προστασία της ιδιωτικότητας τους.

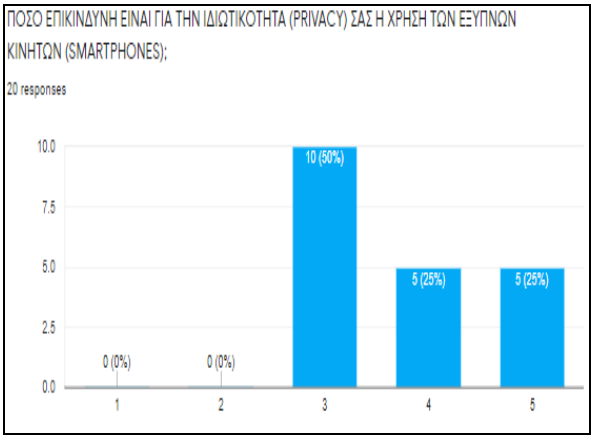

ΠΟΣΟ ΕΝΗΜΕΡΟΙ ΕΙΣΤΕ ΓΙΑ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΠΟΥ ΕΛΛΟΧΕΥΕΙ Η ΧΡΗΣΗ ΤΩΝ SMARTPHONE;
20 responses
0 (0%)
2 (10%)
5 (25%)
8 (40%)
5 (25%)


ΚΑΤΑ ΤΗΝ ΑΠΟΨΗ ΣΑΣ ΠΟΣΟ ΑΣΦΑΛΗΣ ΕΙΝΑΙ Η ANDROID ΣΥΣΚΕΥΗ ΣΑΣ;
20 responses
0 (0%)
2 (10%)
9 (45%)
7 (35%)
2 (10%)


ΠΟΣΟ ΑΣΦΑΛΕΙΣ ΝΙΩΘΕΤΕ ΣΤΗΝ ANDROID ΣΥΣΚΕΥΗ ΣΑΣ;
20 responses
0 (0%)
5 (25%)
3 (15%)
10 (50%)
2 (10%)

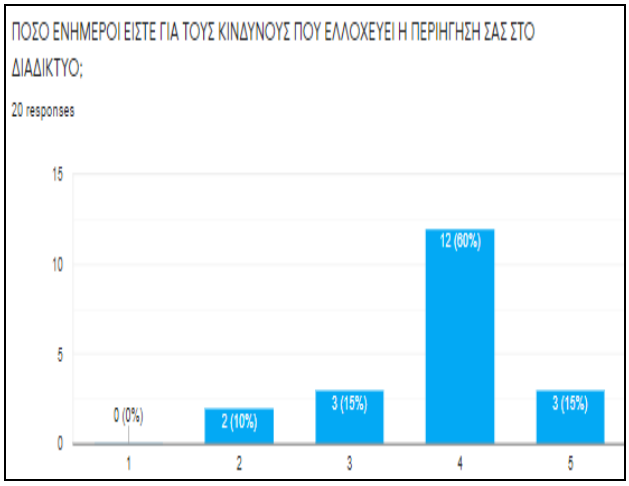

ΠΙΣΤΕΥΕΤΕ ΟΤΙ Η ANDROID ΣΥΣΚΕΥΗ ΣΑΣ ΠΑΙΡΝΕΙ ΑΡΚΕΤΑ ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΣΑΣ ΔΕΔΟΜΕΝΩΝ;
20 responses
10%
85%
ΝΑΙ
ΟΧΙ
Λαμβάνονται μέτρα μέχρι κάποιο σημείο ωστόσο κίνδυνοι συνεχίζουν να υπάρχουν

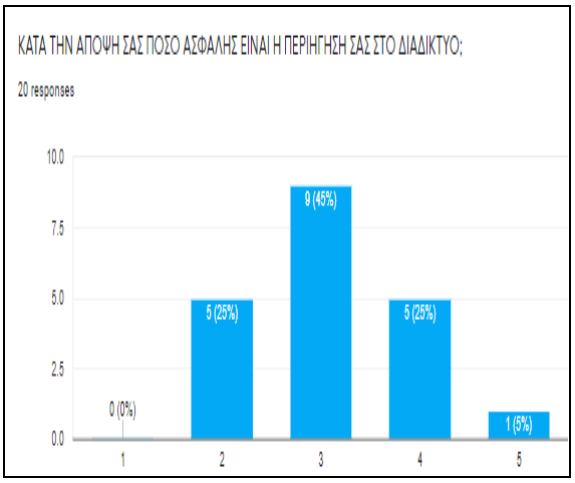

ΠΟΣΟ ΕΝΗΜΕΡΟΙ ΕΙΣΤΕ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ (PRIVACY);
20 responses
0 (0%)
4 (20%)
8 (40%)
6 (30%)
2 (10%)

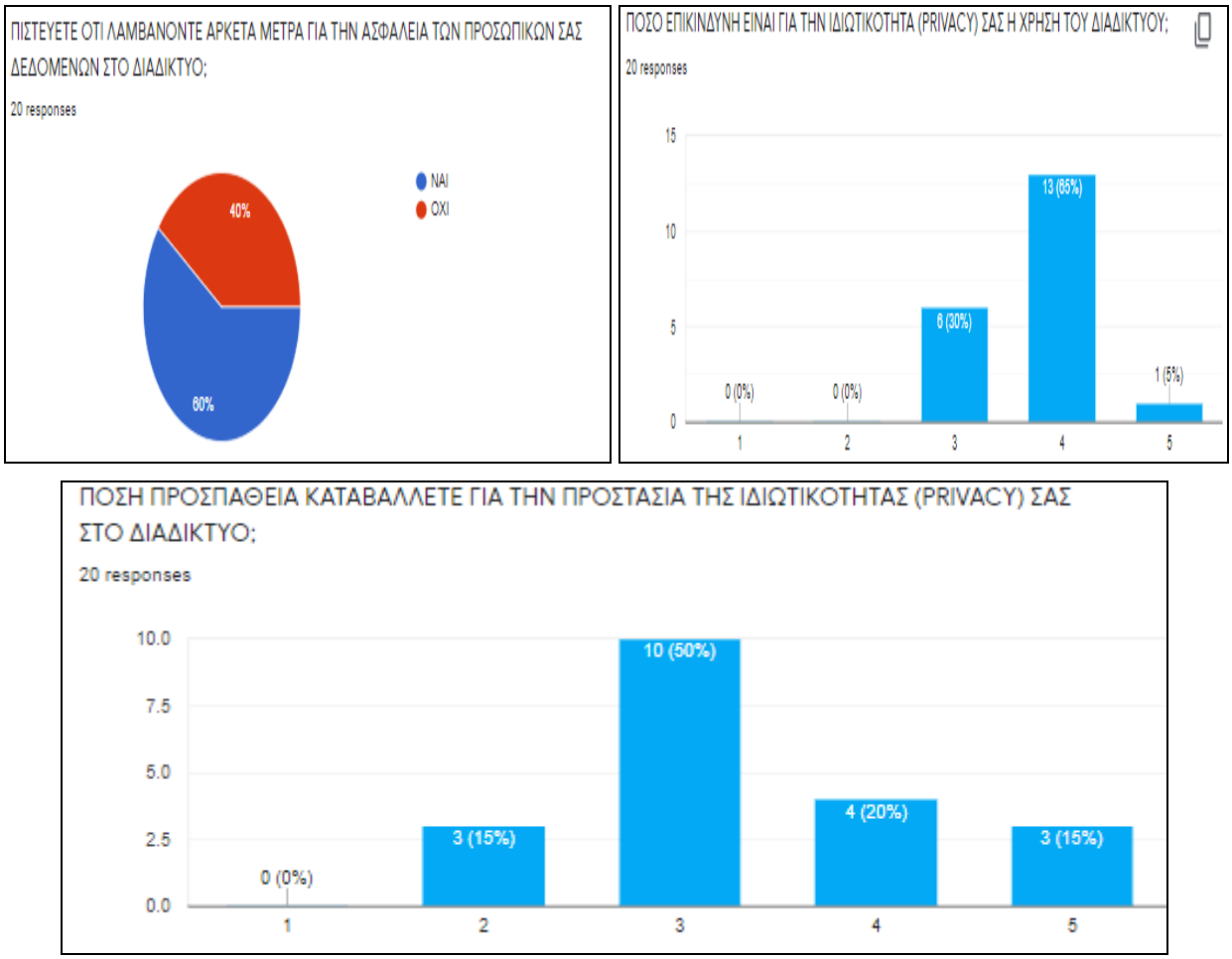

ΠΟΣΟ ΕΠΙΚΙΝΔΥΝΗ ΕΙΝΑΙ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ (PRIVACY) ΣΑΣ Η ΧΡΗΣΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΙΝΗΤΩΝ (SMARTPHONES);
20 responses
0 (0%)
0 (0%)
10 (50%)
5 (25%)
5 (25%)

Γραφικές Παραστέσεις 7.3 Ερωτήσεις για Ασφάλεια και Ιδιωτικότητα στο Android

Παρόμοιο είναι το ποσοστό των συμμετεχόντων που είναι ενήμεροι όσον αφορά τους κινδύνους που ελλοχεύουν από τη χρήση των Web εφαρμογή (90%). Σε σύγκριση με τις Android συσκευές, μικρότερο κατά 15% είναι το ποσοστό των συμμετεχόντων που δηλώνουν πως θεωρούν ασφαλή την περιήγηση στο διαδίκτυο (75%), ενώ αισθητά λιγότεροι (60%) ήταν αυτοί που πιστεύουν ότι το διαδίκτυο προσφέρει ιδιωτικότητα και προστασία των προσωπικών τους δεδομένων. Τέλος, πολλοί είναι αυτοί που θεωρούν ότι η χρήση του διαδικτύου παραβιάζει την ιδιωτικότητα τους (95%), ωστόσο πολύ μικρό ποσοστό θεωρεί ότι αυτό συμβαίνει σε πολύ μεγάλο βαθμό (5%). Οι μισοί από του συμμετέχοντες καταβάλλουν μέτρια προσπάθεια για την διασφάλιση της ιδιωτικότητας τους, ενώ γενικότερα σε αυτή τη κατηγορία παρατηρείται αύξηση του αριθμού των ατόμων που επιδιώκουν προστασία της ιδιωτικότητας τους σε σχέση με τις Android συσκευές.



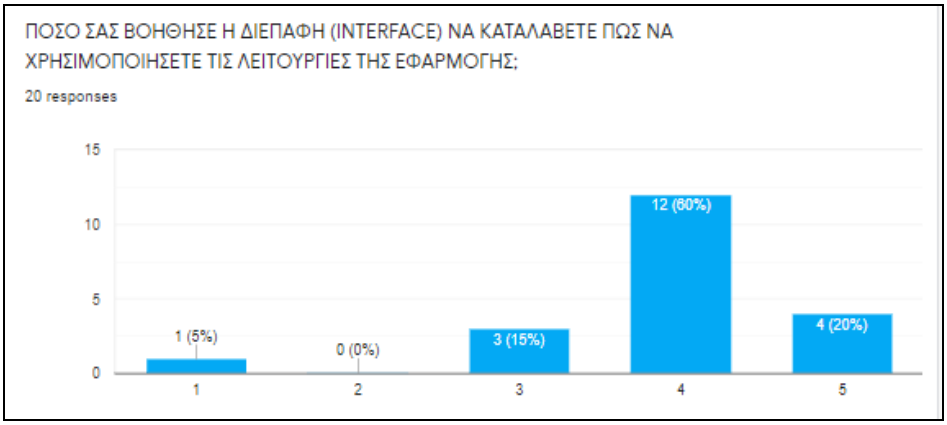


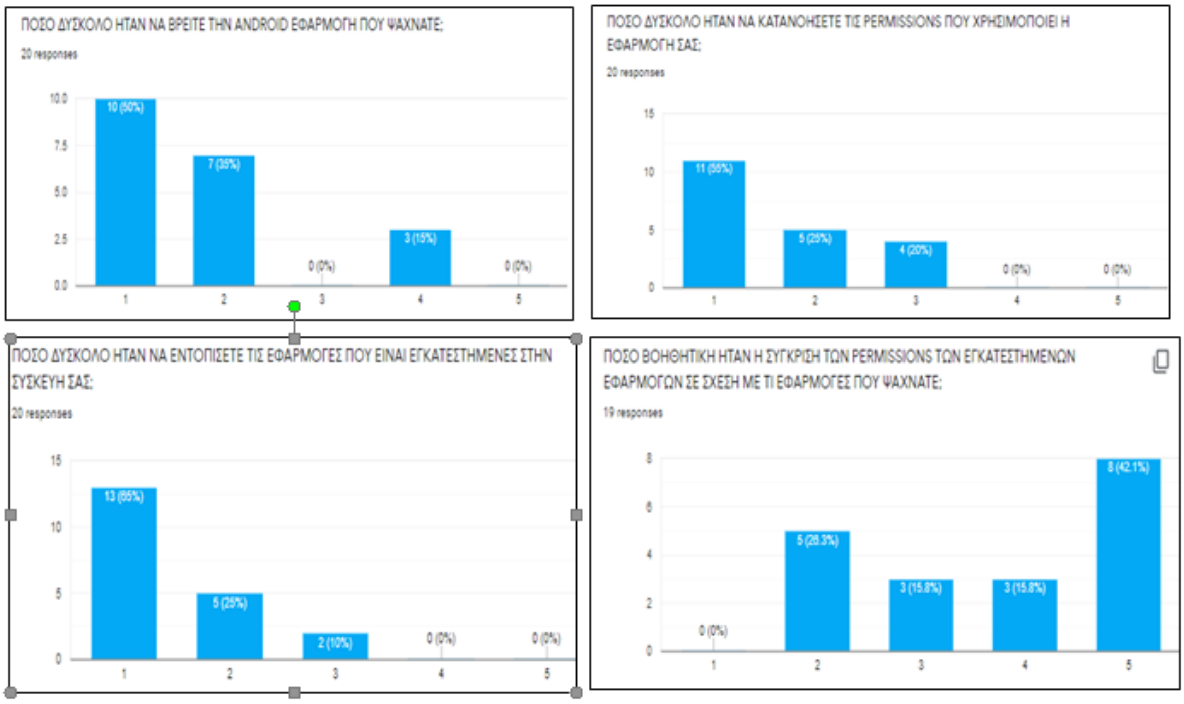


Γραφικές Παραστέσεις 7.4 Ερωτήσεις για Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο

Στην τελευταία κατηγορία του ερωτηματολογίου που αφορά την εφαρμογής AppPrivacyAnalyzer που υλοποιήθηκε στα πλαίσια της παρούσας διπλωματικής εργασίας παρατηρήθηκε ότι είχε θετικό αντίκτυπο στους χρήστες και στη προσπάθεια τους να διασφαλίσουν τη ιδιωτικότητα και τα προσωπικά τους δεδομένα. Συγκεκριμένα, σχεδόν όλοι θεωρούν ότι το interface της εφαρμογής βοήθησε στη ευκολότερη χρήση της. Επιπλέον , το 80-85% τους φάνηκε εύκολη τόσο η εύρεση της εφαρμογής που έψαχναν για να αναλύσουν, όσο και η κατανόηση των permissions που εμφανίζονται μετά την αναζήτηση και ανάλυση κάποιας εφαρμογής. Τα πιο πάνω αποτελέσματα αντικατοπτρίζουν την αποτελεσματικότητα και την αμεσότητα της συγκεκριμένης λειτουργίας. Κατά αναλογία, το ίδιο εύκολο θεώρησαν οι χρήστες την εύρεση

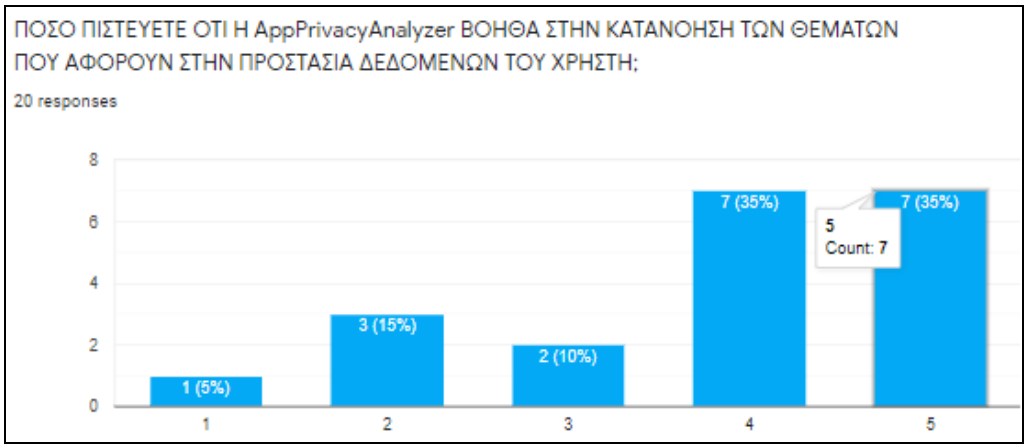
εφαρμογών που είναι ήδη εγκατεστημένες στη συσκευή τους. Επίσης, ποικίλουν οι απόψεις κατά πόσο η σύγκριση των permissions των διάφορων εφαρμογών μεταξύ τους είναι βοηθητική για τους χρήστες, χωρίς ωστόσο να υπάρχουν αρνητικές απόψεις για την συγκεκριμένη λειτουργία.

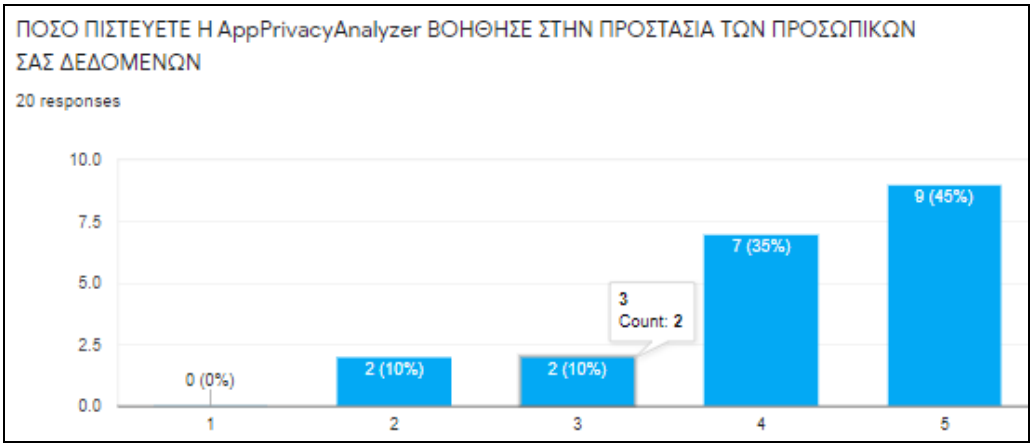




Γραφικές Παραστέσεις 7.5 Ερωτήσεις για την εφαρμογή AppPrivacyAnalyzer

Εν κατακλείδι, οι περισσότεροι συμμετέχοντες (70-80%) στην έρευνα βρίσκουν την εφαρμογή AppPrivacyAnalyzer λειτουργική και θεωρούν ότι ήταν βοηθητική όχι μόνο για την κατανόηση ζητημάτων ιδιωτικότητας αλλά και αποτελεσματική για τη προστασία των προσωπικών δεδομένων.





Γραφικές Παραστέσεις 7.6 Αξιολόγηση εφαρμογής AppPrivacyAnalyzer

7.3 Γενικά Συμπεράσματα

Η μελέτη που χρειάστηκε να γίνει για την εκπόνηση της διπλωματικής εργασίας με βοήθησε να καταλάβω τη σημαντικότητα του θέματος της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων. Έγινε μια ευρεία ανασκόπηση για το θέμα με ανάγνωση άρθρων και άλλων ερευνών δίνοντας έμφαση στις Android εφαρμογές και Web εφαρμογές που βασίζονται στο HTML5.

Η απεριόριστη χρήση των έξυπνων τηλεφώνων αλλά και η φύση του Android, στο οποίο μπορεί ο καθένας να κατεβάσει μια εφαρμογή, φέρει καθημερινά τους χρήστες σε κίνδυνο. Οι περισσότεροι χρήστες έχουν άγνοια για το πως μπορεί μια εφαρμογή να έχει πρόσβαση στα προσωπικά τους στοιχεία. Έτσι έχοντας ως σκοπό τη χρήση της εφαρμογής αποδέχονται τα permissions χωρίς να δίνουν σημασία σε αυτά.

Το ίδιο συμβαίνει και με τις Web εφαρμογές για τις οποίες οι πλείστοι χρήστες δεν είναι ενημερωμένοι για τους κινδύνους που μπορεί να διατρέχουν στο διαδίκτυο και αγνοούν τις πιθανές ειδοποιήσεις τους εμφανίζει ο εκάστοτε browser.

Λόγω των πιο πάνω δημιουργήθηκε η εφαρμογή AppPrivacyAnalyzer. Μέσω αυτής οι χρήστες θα μπορούν να ενημερώνονται για τα προσωπικά στοιχεία που τους ζητά μια εφαρμογή για να προχωρήσει στις λειτουργίες της. Το AppPrivacyAnalyzer προσφέρει στους χρήστες τη δυνατότητα να δουν πια permission έχουν ήδη αποθηκευτεί για να μπορεί να τα μπορεί να προστατευτεί στη συνέχεια αν επιθυμεί.

7.4 Μελλοντική εργασία

Σαν μελλοντική εργασία θα μπορούσε να υπάρχει μια βελτιωμένη έκδοση της εφαρμογής AppPrivacyAnalyzer, στην οποία θα διορθωθούν κάποια προβλήματα όπως είναι αυτό με την αναζήτηση των εφαρμογών από το Google Play, και να προστεθεί στη θέση του ένα searchbar που θα δίνει τη δυνατότητα να βγαίνουν επιλογές από εφαρμογές που υπάρχουν στο Google Play. Κάτι άλλο που θα μπορούσε να προστεθεί είναι η ανάλυση apk αρχείων ούτως ώστε να μπορούν να βρεθούν και τα permissions που δεν είναι δηλωμένα στο manifest αλλά υπάρχουν μέσα στον κώδικα και είναι επικίνδυνα για την ιδιωτικότητα των χρηστών.

Η εφαρμογή AppPrivacyAnalyzer δίνει έμφαση στις Android συσκευές, η μόνη λειτουργία που γίνετε για web εφαρμογές είναι απλά μέσω ενός URL. Στο μέλλον θα μπορούσαν να αναπτυχθούν και άλλα στοιχεία όσον αφορά την ιδιωτικότητα στις web εφαρμογές. Όπως για παράδειγμα η ανάλυση των δικαιωμάτων αυτών που ζητούνται.

Βιβλιογραφία

[1] How the digital age is impacting our personal privacy, Charls Okwe ,05 May2017
https://medium.com/@cre8tivemediaservices/how-the-digital-age-is-impacting-our-personal-privacy-695326dd1455

[2] Κίνδυνοι: Παραβίαση ιδιωτικής ζωής, Ασφάλεια στο διαδίκτυο
https://internetsafety.pi.ac.cy/teenagers-privacy-violation

[3] Τι είναι ιδιωτικότητα ; , Ξεχασμένος και ατίθασος
https://antiauthor.wordpress.com/2011/08/06/%CF%84%CE%AF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7-%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1/

[4] Duhaime's law dictionary , Wayback Machine (Internet archive)
https://web.archive.org/web/20190923113639/http://www.duhaime.org/LegalDictionary/P/Privacy.aspx

[5] Privacy and human rights, Global Internet Liberty Campaign
http://gilc.org/privacy/survey/intro.html

[6] Set up for Android development, Source
https://source.android.com/setup

[7] Android – statistics and facts, Statista by Shanhong Liu, 02 June 2020
https://www.statista.com/topics/876/android/

[8] Android – Architecture, Tutorials point
https://www.tutorialspoint.com/android/android_architecture.htm

[9] An introduction to android interprocess communication and common pitfalls, Vardaan Shamra, 29 March 2019

https://medium.com/@vardaansh1/an-introduction-to-android-interprocess-communication-and-common-pitfalls-ac4dfeddf89b

[10] Application signings, Source
https://source.android.com/security/apksigning

[11] Permissions on Android, Developers
https://developer.android.com/guide/topics/permissions/overview

[12] Android permissions can be dangerous: full guide to managing them, Heimdal security, Elena Georgescu
https://heimdalsecurity.com/blog/android-permissions-full-guide/#:~:text=Dangerous%20permissions,RECEIVE_SMS%2C%20READ_SMS%20and%20so%20on.

[13] Understanding app permissions, Codepath
https://guides.codepath.com/android/Understanding-App-Permissions

[14] HTML5 Basics for everyone tired of reading about deprecated code, htlm.com
https://html.com/html5/

[15] How to ensure privacy in the age of HTML5, CIO, Chriss Minnick and Ed TIttel, 25 June 2013
https://www.cio.com/article/2384651/how-to-ensure-privacy-in-the-age-of-html5.html?fbclid=IwAR3m0Nkxvzeio7MmgVFN76oIRasRQR-dRHcmKrO4Sg23UNvbh0WXvKw1jXo

[16] What is the JVM? Introducing the java virtual machine, Infoworld, Matthew Tyson 17 January 2020
https://www.infoworld.com/article/3272244/what-is-the-jvm-introducing-the-java-virtual-machine.html

[17] What is python? Executive summary, Python
https://www.python.org/doc/essays/blurb/

[18] Google play scraper, GitHub
https://github.com/facundoolano/google-play-scraper

[19] History of php and related projects, Php
https://www.php.net/history

[20] Learn the model view controller pattern, Openclassrooms
https://openclassrooms.com/en/courses/4661936-develop-your-first-android-application/4679186-learn-the-model-view-controller-pattern#:~:text=Most%20Android%20developers%20use%20a,apply%20to%20our%20TopQuiz%20application.

[21] Client-Server Model, GeeksforGeeks
https://www.geeksforgeeks.org/client-server-model/

[22] Elinux, Android Architecture
https://elinux.org/Android_Architecture

[23] Παρακολούθηση των προσωπικών ευαίσθητων δεδομένων στις Android Εφαρμογές, Χριστιάνα Γιαπιτζάκη

Παράρτημα Α

Ερωτηματολόγιο

https://docs.google.com/forms/d/e/1FAIpQLSc1bTbE61Y0DBf2sb73an-qqu9cny1PABy0eFXtBfcY83r3ww/viewform?usp=sf_link

Απαντήσεις Ερωτηματολογίου

https://docs.google.com/spreadsheets/d/11Oj-q5rxpNZjIRDamhF5KGPBjBFyzCH67UUus-zOH4k/edit#gid=1211806462