ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΟ ΣΠΟΥΔΩΝ -
ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΔΙΟΙΚΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ενίσχυση Ενημερότητας Ιδιωτικότητας Χρηστών Κινητών Εφαρμογών μέσω Τεχνικών Οπτικοποίησης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΣΠΑΤΗ ΙΩΑΝΝΗ

Επιβλέπων : Σπύρος Κοκολάκης, Αναπληρωτής Καθηγητής Πανεπιστημίου Αιγαίου
Συνεπιβλέπουσα: Αγγελική Τσώχου, Επίκουρος Καθηγήτρια Ιόνιου Πανεπιστημίου

Μέλη εξεταστικής επιτροπής: **ΑΓΓΕΛΙΚΗ ΤΣΩΧΟΥ**
ΣΠΥΡΟΣ ΚΟΚΟΛΑΚΗΣ
ΜΑΡΙΑ ΚΑΡΥΔΑ

Σάμος, Φεβρουάριος 2017

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η εκπόνηση της παρούσας διπλωματικής εργασίας ήταν το αποτέλεσμα ενός κοπιαστικού και συνάμα ευχάριστου ταξιδιού στο χώρο της ασφάλειας υπολογιστικών συστημάτων. Ένα ταξίδι που φρόντισε το κοινωνικό και εκπαιδευτικό μου περιβάλλον να γεμίσει με όμορφες αναμνήσεις.

Αρχικά θα ήθελα να ευχαριστήσω τη συνεπιβλέπουσα κα. Αγγελική Τσώχου Επίκουρο Καθηγήτρια του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου και τον επιβλέπων καθηγητή κ. Σπύρο Κοκολάκη Επίκουρο Καθηγητή του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων για τη βοήθειά τους και τη καθοδήγηση που μου προσέφεραν καθ' όλη τη διάρκεια της εκπόνησης αυτής της διατριβής.

Θα ήθελα επίσης να ευχαριστήσω το κ. Δημήτρη Φωτάκη Επίκουρο Καθηγητή της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου καθώς και το κ. Νίκο Δημητρίου Συνεργαζόμενο Ερευνητή του Εθνικού Κέντρου Έρευνας Φυσικών Επιστημών «Δημόκριτος» για την αμέριστη συμπαράστασής τους και τα κίνητρα που μου έδωσαν για να συνεχίσω σε επίπεδο Μεταπτυχιακών Σπουδών.

Τέλος θα ήθελα να ευχαριστήσω τη σύζυγό μου Παναγιώτα Γουέμπερ χωρίς τη συμπαράσταση της οποίας το έργο μου θα ήταν πολύ δύσκολο καθώς και τη πολύτεκνη οικογένεια από την οποία προέρχομαι για τη σύσσωμη υποστήριξή τους.

Πίνακας περιεχομένων

Περίληψη

Οι ραγδαίες εξελίξεις στο χώρο της τεχνολογίας και δη στο χώρο των φορητών συσκευών, ώθησε τους καταναλωτές στην αγορά συσκευών όπως έξυπνα κινητά τηλέφωνα και ταμπλέτες. Οι εταιρείες από τη πλευρά τους καθώς και ανεξάρτητοι δημιουργοί εκμεταλλεύτηκαν αυτό το γεγονός δημιουργώντας αναρίθμητες εφαρμογές για φορητές συσκευές.

Οι νέες δυνατότητες τόσο των φορητών συσκευών όσο και της αύξησης της επεξεργαστικής ισχύος των εξυπηρετητών και των χώρων ηλεκτρονικής αποθήκευσης ώθησε διάφορες εταιρείες και ιδιώτες να εκμεταλλευτούν το χαμηλό επίπεδο ενημερότητας των χρηστών περί των προσωπικών τους δεδομένων. Συγκεκριμένα, εξακολούθησαν τη κοινή πρακτική συλλογής και επεξεργασίας των δεδομένων αυτών που ήδη εφάρμοζαν σε ιστοσελίδες και σε χώρους κοινωνικής δικτύωσης κατά το παρελθόν.

Οι χρήστες που ήδη παρουσίαζαν ανησυχητικές τάσεις για τα δεδομένα τους και παρατηρώντας ότι δεν υπάρχει δυνατότητα οποιασδήποτε ηλεκτρονικής συναλλαγής χωρίς τη δημοσιοποίηση των προσωπικών τους δεδομένων κατέφυγαν σε διαδικασίες έως και ακραίου αυτοπεριορισμού χρήσης των διαδικτυακών μέσων. Από την άλλη πλευρά, οι μη ενημερωμένοι χρήστες συνεχίζουν την εθελοντική ή μη, αποκάλυψη προσωπικών δεδομένων χωρίς να λαμβάνουν υπόψη τους δυνητικούς κινδύνους από την υπερβολική έκθεση των δεδομένων τους. Σχεδόν απορρίπτουν την ανάγνωση των αναρτημένων πολιτικών ασφάλειας θεωρώντας τες δύσκολες στην ανάγνωση λόγω των νομικών όρων που χρησιμοποιούν ή χρονικά και οικονομικά ασύμφορες καθώς απαιτούν αρκετές εκατοντάδες ώρες για την ανάγνωσή τους ετησίως.

Μέσω της μεθοδολογίας που παρουσιάζουμε σε αυτή τη διπλωματική αναδείξαμε πως με τη χρήση κοινών εφαρμογών και δημόσια αναρτημένων δεδομένων είναι δυνατή η ταυτοποίηση και η παρακολούθηση μεγάλου αριθμού χρηστών και μέσω δειγματοληπτικής τους παρακολούθησης και επεξεργασίας ερωτηματολογίων που συντάξαμε να ανακαλύψουμε το ύψος της ενημερότητάς τους και τους λόγους που δεν μπήκαν στη διαδικασία ανάγνωσης των πολιτικών ασφάλειας του κοινωνικού δικτύου που χρησιμοποιούν.

Η διπλωματική αυτή κλείνει με τη δημιουργία της εφαρμογής appWare που έχει ως σκοπό την εκλαΐκευση των πολιτικών ασφάλειας που ακολουθούν οι εφαρμογές για φορητές συσκευές. Έγινε προσπάθεια οπτικοποίησης του δυνητικού κινδύνου της αποδοχής των δικαιωμάτων που αποκτά η εκάστοτε εφαρμογή με τη χρήση αντιπροσωπευτικών εικόνων καθώς και τη περιγραφή του εν λόγω δικαιώματος με χρήση απλής και κατανοητής γλώσσας με έμφαση στη μέγιστη δυνατή ζημιά που μπορεί να προκληθεί συνδυαστικά ή ατομικά.

Abstract

The excessive progress in technology development and innovation, especially in portable cellular devices has lead consumers in the acquisition of cellular technology such as smart phones and tablets. Production companies and independent developers saw into this business reality a major investment opportunity by creating innumerous applications for these portable devices.

The combination of the advanced capacities and capabilities of these portable devices and use of faster data processors by the internet providers, plus the expansion of remote data storage space, has managed to allow the production companies, along with the independent developers to exploit social media users' low level of knowledge of the use of their private and personal information, using a practice that has already been used in the past, the data collection, which already has been applied to social media applications, search engines and wed sites.

Concerned about their privacy social media users, after comprehending that all electronical and internet activities are traceable and collected by the parties involved and after realizing that there is not a legal way to avert this so called "common practice", have decided to cut down on their social media and online transactions, sometimes choosing a full shut down of their internet and online exposure.

The non informed users on the other hand, continue the unintended or even voluntary exposure of their privacy and personal data, without taking under consideration the immense danger of the over exposure of their personal information. It is a common thing the fact that most of them, disregard the briefing on the privacy policy of each website, search engine or application they use, due the difficult legal terminology used or due to the time consuming process that is required in order to read all of the them, on a annual base.

In this Thesis and the methodology presented in it, we managed to prove that by using sharing technology between online applications and the collection of personal data with the freedom to be used as any developer sees fit, it is possible to track down and basically "stalk" a great number of internet and social media users as critical personal information such as addresses, telephone numbers, etc are free to be exploited by anyone interested. By conducting a sample inquiry and a survey amongst them, we figured out the level of their awareness, when it comes to internet and online exposure of their personal information and the reasons why they did not read the privacy policy of the online social services they use.

The creation of the appWare application which concludes this Thesis, has the sole purpose of making the privacy policies used by the parties involved, more accessible and easier to be understood by the users. By using graphic images and simple, every day language terminology, we tried to visualize the danger involved when ones accepts the privacy policy of the portable devices' applications and to make emphatically clear the problems that can be caused on a personal and a social level.

1

Εισαγωγή

1.1 Οι νέες τάσης στο χώρο των Τ.Π.Ε. και η αμφιβολίες για την αποτελεσματικότητα των πολιτικών ασφάλειας και ιδιωτικότητας

Στην εποχή του 21 αιώνα οι ραγδαίες εξελίξεις στο τομέα της πληροφορικής και της τεχνολογίας είχαν ως αποτέλεσμα τη δημιουργία νέων τάσεων στο χώρο της επικοινωνίας καθώς και νέους τρόπους κοινωνικοποίησης των ατόμων. Στο τομέα των νέων τεχνολογιών αυξητικές τάσεις παρατηρούνται στην απόκτηση έξυπνων συσκευών όπως κινητά τηλέφωνα και ταμπλέτες ενώ στο χώρο της επικοινωνίας μεγάλο ποσοστό του πληθυσμού γίνεται μέλος ενός ή παραπάνω κοινωνικών δικτύων. Με τη δημιουργία των νέων αυτών πλαισίων στο χώρο των τεχνολογιών πολλοί ερευνητές έχουν διατυπώσει αμφιβολίες για την αποτελεσματικότητα των πολιτικών ιδιωτικότητας όπως αυτές παρουσιάζονται στους χρήστες στα παραπάνω τεχνολογικά πλαίσια. Καθώς οι γλώσσες αναγραφής πολιτικών ασφάλειας όπως η XACML [1] και η EPAL[2] περιλαμβάνουν σύνθετη ή ιδιαίτερη νομική ορολογία Kambiz et al [3] στις περισσότερες περιπτώσεις οι χρήστες δεν θα διαβάσουν καθόλου τη πολιτική ιδιωτικότητας πριν την αποδεχθούν καθώς δεν μπορούν να κατανοήσουν τα προβλήματα που μπορούν να προκύψουν από την μεταβίβαση των δεδομένων σε τρίτους όπως πάροχους ή δημιουργούς εφαρμογών. Εναλλακτικά παρατηρείται δυσκολία ή αδυναμία κατανόησης των συνδέσεων που μπορούν να προκύψουν με τη χρήση των δεδομένων αυτών, τα συμπεράσματα που μπορούν να εξαχθούν από το συνδυασμό αυτών των πληροφοριών καθώς και τους κινδύνους που διατρέχουν οι χρήστες σε σχέση με την ιδιωτικότητά τους (Andreas Buchenscheit et al).[4] . Με βάση τα παραπάνω κρίνουμε απαραίτητο να περιγράψουμε τους κινδύνους καθώς και ένα νέο τεχνολογικό πλαίσιο παρουσίασης και εφαρμογής πολιτικών ασφάλειας για εφαρμογές κινητών συσκευών.

1.2 Αντικείμενο διπλωματικής

Η διπλωματική αυτή θα επικεντρωθεί στις πολιτικές ασφάλειας των εφαρμογών των κινητών τηλεφώνων και ταμπλετών. Ο βασικός στόχος είναι να αναδείξει τα προβλήματα που παρατηρούνται κατά την ανάγνωση των πολιτικών ασφάλειας. Θα παρουσιάσει μέσω βιβλιογραφικής ανασκόπησης την άποψη που έχουν οι χρήστες γι' αυτές ενώ θα αναδείξει τους λόγους μη ανάγνωσης και τυφλής αποδοχής αυτών. Θα δείξει το προβληματικό μοντέλο παρουσίασης που χρησιμοποιείται για την παρουσίαση των πολιτικών ασφάλειας στο χρήστη και θα αποδείξει ότι ο τρόπος βαθμολόγησης και αξιολόγησης των εφαρμογών σύμφωνα με τις αγορές μεταφόρτωσης εφαρμογών για κινητές συσκευές (market places) δεν μπορεί να κριθεί αντικειμενικός. Θα μελετήσει σε βάθος μία δημοφιλής εφαρμογή ανταλλαγής μηνυμάτων και επικοινωνίας. Συγκεκριμένα θα αναδείξει το πρόβλημα της ενημερότητας των χρηστών με τη προβολή των κινδύνων που εγκυμονεί η μη ανάγνωση και βαθιά κατανόηση της πολιτικής ασφάλειας αυτής και θα παρουσιαστεί αναλυτικά ο κίνδυνος που δυνητικά μπορεί να προκύψει από τη διασύνδεση των προσωπικών δεδομένων που διαρρέουν μέσω αυτής της εφαρμογής. Σε επόμενο επίπεδο θα αναδείξει εναλλακτικούς τους τρόπους αναγραφής πολιτικών ασφάλειας όπως έχουν παρουσιαστεί από διάφορούς μελετητές[1][5]. Θα αναδείξει πως μία διαφορετική προσέγγιση οπτικοποίησης μιας πολιτικής ασφάλειας μπορεί να γίνει πιο κατανοητή στο χρήστη, θα δημιουργηθεί το μοντέλο οπτικοποίησης και θα δημιουργηθεί αντίστοιχη εφαρμογή η οποία θα παρουσιάζει ανά εφαρμογή τη τρέχουσα πολιτική ασφάλειας όπως παρουσιάζεται στο χρήστη, θα αναδεικνύει τα προβλήματα που δημιουργεί, θα οπτικοποιεί με εναλλακτικό τρόπο τους σύνθετους κινδύνους που υπάρχουν με τη πιθανή διασύνδεση αυτών των δεδομένων.

1.3 Η Στατιστική ανάλυση στο χώρο των έξυπνων κινητών συσκευών

Τα στατιστικά στο χώρο των έξυπνων κινητών τηλεφώνων μας δείχνουν τις μεγάλες αυξητικές τάσεις που επικρατούν στην αγοράς. Στις Η.Π.Α. ο ρυθμός των έξυπνων κινητών τηλεφώνων από 62,6 εκατομμύρια το 2010 υπερτριπλασιάστηκε φτάνοντας τα 190,5 εκατ. το 2015 με πρόβλεψη να φτάσουν τα 236,8 εκατ. έως το 2019 [6]. Σε παγκόσμια κλίμακα οι πωλήσεις των έξυπνων κινητών τηλεφώνων από 36,5 εκατ. το πρώτο τρίμηνο του 2009 ανήλθαν στα 349,3 εκατ. το πρώτο τρίμηνο του 2016 παρουσιάζοντας μία αύξηση περίπου 957% [7]. Οι δε εφαρμογές για κινητά τηλέφωνα και ταμπλέτες ακολουθούν μία ακόμη μεγαλύτερη αυξητική τάση. Ενώ το Δεκέμβριο του 2009 υπήρχαν μόλις 2.000 περίπου εφαρμογές μέσα σε δύο μόλις έτη είχαν παρουσιαστεί 400.000 εφαρμογές καταγράφηκε δηλαδή αύξηση κατά 20.000% ενώ το Φεβρουάριο του 2016 οι εφαρμογές είχαν φτάσει τα δύο εκατομμύρια [8]. Επίσης η πλειονότητα των χρηστών έξυπνων συσκευών εγκαθιστούν 1-10 εφαρμογές το 30%, 11-20 εφαρμογές το 32%, 21-30 εφαρμογές το 16%, 31-40 το 10%, 41-50 το 5% και 50 ή παραπάνω το 7% σύμφωνα με έρευνα που διενεργήθηκε μεταξύ 27-1-2015 και 16-2-2015 από το Pew Research Center Surveys [9].

1.4 Το εύρος και τα όρια της εργασίας

Η Διπλωματική επικεντρώνεται στην αγορά μεταφόρτωσης εφαρμογών για κινητές συσκευές android Google Play (https://play.google.com) . Επικεντρωνόμαστε σε αυτή τη συγκεκριμένη αγορά καθώς αποτελεί αφενός τον επίσημο ιστότοπο μεταφόρτωσης εφαρμογών για κινητές συσκευές android, και αφετέρου είναι ο δημοφιλέστερος ιστότοπος γενικότερα σε σύνολο εφαρμογών και μεταφορτώσεων εφαρμογών ενώ η ύπαρξη της υποχρέωσης για την αναγραφή των πολιτικών ασφάλειας όπως αυτή πηγάζει από τη κείμενη νομοθεσία τον καθιστά ένα εξαιρετικό παράδειγμα για έρευνα. Τέλος να επισημάνουμε ότι η ύπαρξη αναρίθμητων ανεπίσημων αγορών μεταφόρτωσης εφαρμογών για κινητές συσκευές θα καθιστούσε δύσκολη την εκπόνηση μίας συνολικής έρευνας. Σε ότι αφορά τις πολιτικές ασφάλειας μελετήθηκε η σχετική βιβλιογραφία από το 2002 και έπειτα όπου εμφανίζονται τα πρώτα σχήματα για τη δημιουργία αυτών των πολιτικών ενώ κάνουν την εμφάνισή τους και οι πρώτοι προβληματισμοί σε σχέση με αυτές. Σε ότι αφορά την αγορά google play (πρώην android market) μελετήθηκε η σχετική βιβλιογραφία από το 2008, έτος δημιουργίας του ιστότοπου android market που μετονομάστηκε αργότερα σε google play.

1.5 Η αντιμετώπιση των αναχρονιστικών πολιτικών ασφάλειας

Μέσω της ανασκόπησης της σχετικής βιβλιογραφίας θα αναδειχθούν σε πρώτη φάση οι προβληματισμοί που υπάρχουν σε σχέση με το τρέχον τρόπο αναγραφής των πολιτικών ασφάλειας στο google play. Σε δεύτερο επίπεδο για να αναδειχτεί το πρόβλημα διαρροής προσωπικών δεδομένων θα δοθεί ένα εκτενές παράδειγμα κάνοντας χρήση της δημοφιλούς εφαρμογής ανταλλαγής μηνυμάτων και επικοινωνίας viber. Ο τελικός σκοπός της εργασίας αυτής είναι η ανάδειξη της απώλειας της ιδιωτικότητας μέσω συνδυαζόμενων δεδομένων καθώς και η δημιουργία μιας εφαρμογής με προσωρινό όνομα appWare που θα αποσκοπεί στην βέλτιστη οπτικοποίηση της πολιτικής ασφάλειας που εφαρμόζει μία εφαρμογή από το google play ώστε να ενισχύεται ενημερότητα του χρήστη σχετικά με τους κίνδυνους που εγκυμονεί αυτή. Συγκεκριμένα, μετά τη συγκέντρωση του συνόλου των πολιτικών και δικαιωμάτων ασφαλείας (data set) που μπορεί να χρησιμοποιήσει ένας προγραμματιστής εφαρμογών για android κινητές συσκευές, μέσω της προτεινόμενης εφαρμογής θα γίνει προσπάθεια βελτιστοποίησης τους τρόπου αναγραφής της κάθε πολιτικής ασφαλείας ώστε να είναι περισσότερο κατανοητή στον χρήστη. Επίσης μέσω της εφαρμογής θα δημιουργείται μία συνολική και εύκολα κατανοητή αναφορά για το χρήστη η οποία με σαφήνεια θα οπτικοποιεί τους δυνητικούς κινδύνους αυτής της εφαρμογής. Ως απαραίτητη προϋπόθεση για την ανάδειξη της τρέχουσας ενημερότητας των χρηστών περί πολιτικών ασφάλειας και αναγνώρισης κινδύνου κρίνεται αναγκαία η δημιουργία ενός ερωτηματολογίου που θα μας απαντήσει στα ερωτήματα αυτά.

1.6 Η δομή της εργασίας

Στη συνέχεια της διπλωματικής αυτής και συγκεκριμένα στο κεφάλαιο 2 θα γίνει μία ανασκόπηση της υπάρχουσας βιβλιογραφίας, της αρθρογραφίας και έρευνας. Όπως αναφέρθηκε και παραπάνω η βιβλιογραφική ανασκόπηση χωρίζεται διακριτά σε δύο χρονικές περιόδους από το 2002 έως και σήμερα σε ότι αφορά τις τρέχουσες μεθόδους οπτικοποίησης των μοντέλων πολιτικών ασφάλειας και από το 2008 έως και σήμερα σε σχέση με τις εφαρμογές κινητών συσκευών android. Σκόπιμα δεν μελετάται εκτενώς το χρονικό διάστημα πριν από το 2008 μολονότι υπήρχαν διαφόρου τύπου εφαρμογές για κινητά με εναλλακτικά λογισμικά όπως για παράδειγμα το symbian διότι αφενός η ανάπτυξη των εφαρμογών αυτών έχουν εκλείψει αρκετά χρόνια και αφετέρου δεν υπήρχε σαφή και καθορισμένη υποχρέωση αποδοχής πολιτικών ασφάλειας. Πιο συγκεκριμένα θα γίνει σε βάθος ανασκόπηση των πολιτικών ιδιωτικότητας τόσο στο διαδίκτυο όσο και στις φορητές συσκευές, θα μελετηθεί ο διαδικτυακός αναλφαβητισμός και η κοινωνική ενημερότητα των χρηστών και θα μελετηθεί το χρηματικό και χρονικό κόστος ανάγνωσης των πολιτικών ενημερότητας. Η διαχείριση της ασφάλειας στις συσκευές android θα μελετηθούν στο κεφάλαιο 3 και πιο συγκεκριμένα θα μελετηθεί η πλήρη διαχείριση από πλευράς ασφάλειας του λειτουργικού συστήματος και θα αναδειχθούν τα μοντέλα απειλών που αντιμετωπίζει. Επίσης θα γίνει μία εισαγωγή στους όρους συνδυαζόμενα δεδομένα ως ένα μοντέλο απειλής και θα αναδειχθούν εκτός από τις παραδοσιακές απειλές που αντιμετωπίζουν οι χρήστες από τα συνδυαζόμενα δεδομένα και νέες απειλές που προέκυψαν από τη χρήση των νέων τεχνολογιών και την αξιοποίηση των δημόσιων δεδομένων. Στο κεφάλαιο 4 θα γίνει μία προσομοίωση απειλής μέσω της εφαρμογής Viber, θα αναδειχθεί η μεθοδολογία που εφαρμόσαμε για την άντληση των δεδομένων καθώς και του τρόπου επεξεργασίας αυτών ενώ θα παρουσιαστεί η εκτίμηση της ενημερότητας των χρηστών μέσω της στατιστικής ανάλυσης των δεδομένων που προέκυψαν από την εφαρμογή της μεθόδου μας. Στο κεφάλαιο 5 θα παρουσιαστεί μία μέθοδος ενίσχυσης της ενημερότητας του χρήστη με τη χρήση τεχνικών οπτικοποίησης μιας πολιτικής ασφάλειας μέσω της εφαρμογής appWare που θα αναπτύξουμε ενώ στο κεφάλαιο 6 θα παρουσιαστούν τα συμπεράσματα που θα προκύψουν από το σύνολο της διπλωματικής.

2

Ανασκόπηση Βιβλιογραφίας

2.1 Γενική ανασκόπηση των πολιτικών ιδιωτικότητας

Η εισβολή και προσβολή της ιδιωτικότητας και προσωπικότητας περιλαμβάνει τη μη εξουσιοδοτημένη συλλογή προσωπικών δεδομένων, τη δημοσίευση και ανάρτηση αυτών καθώς και οποιαδήποτε άλλη χρήση χωρίς την πρότερη συναίνεση των υποκειμένων των οποίων τα προσωπικά δεδομένα τυγχάνουν επεξεργασίας (Wang, Lee, and Wang, 1998)[10]. Η συλλογή και η πώληση ή ανταλλαγή προσωπικών πληροφοριών μεταξύ εταιρειών ή ιδιωτών έχει γίνει πλέον κοινή πρακτική (Gillmor, 1998)[11], καθώς έχει γίνει ιδιαίτερα εύκολη η συλλογή και η αποθήκευση σε βάσεις δεδομένων μεγάλου όγκου προσωπικών - ιδιωτικών πληροφοριών μέσω διαδικτύου (Caruso, 1998)[12].

Παρ΄ ό,τι σύμφωνα με έρευνα του 2002 (Rust, Kannan, and Peng, 2002)[13] έχει γίνει αδύνατο ένας καταναλωτής να πραγματοποιήσει οποιαδήποτε συναλλαγή χωρίς να αναγκαστεί να αποκαλύψει προσωπικές πληροφορίες, από την πλευρά των χρηστών παρατηρείται ανάλογη άνοδος της ανησυχίας τους σχετικά με την αποκάλυψη των προσωπικών τους πληροφοριών στο διαδίκτυο· ποιες εταιρείες δραστηριοποιούνται στη συλλογή των προσωπικών δεδομένων καθώς και τη χρήση αυτών (Fletcher, 2003)[14]. Διάφοροι ερευνητές από το 2000 έως και το 2006 κατέληξαν να ορίσουν αρχικά δείκτες σχετικά με τις ανησυχίες των καταναλωτών σε σχέση με τις προσωπικές τους πληροφορίες. Κάποιοι από τους δείκτες αυτούς είναι η ενημερότητα περί συλλογής δεδομένων, η ευπάθεια κατάχρησης των συλλεγόμενων πληροφοριών, η εμπειρία σε σχέση με τη χρήση του διαδικτύου, το κοινωνικό προφίλ και η μόρφωση των καταναλωτών και λοιποί άλλοι δείκτες (Sheehan and Hoy, 2000; Dinev and Hart, 2004; Bellman et al., 2004)[15][16][17].

Ως προς τον πρώτο δείκτη οι Raab και Bennett το 1998 (Raab & Bennett, 1998)[18] περιέγραψαν ότι η ευπάθεια κατάχρησης των ευαίσθητων συλλεγόμενων πληροφοριών ορίζεται ως το δυνητικό ρίσκο μίας ευαίσθητης πληροφορίας να αποκαλυφθεί. Η ευπάθεια αυτή μπορεί να πραγματοποιηθεί κάτω από αρκετές συνθήκες, όπως τυχαία αποκάλυψη, μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, παράνομη εισβολή σε δίκτυα κ.ο.κ. (Rindfleish, 1997)[19]. Οι δε επιπτώσεις για τους καταναλωτές περιλαμβάνουν την κλοπή ταυτότητας (Saunders and Zucker, 1999)[20], την επιθυμητή καταγραφή προσωπικών συνηθειών (Budnitz, 1998), καθώς και τη

στοχευμένη αποστολή διαφημιστικών μηνυμάτων με ποικίλους τρόπους, όπως διαφημιστικά e-mail. Οι παραπάνω παράγοντες συνεισφέρουν στην αυξανόμενη ανησυχία των χρηστών περί διαδικτυακά συλλεγόμενων ευαίσθητων προσωπικών δεδομένων καθώς και της κατάχρησης αυτών (Dinev and Hart, 2004)[16].

Σύμφωνα με τους Culnan και Armstrong (1999)[21] οι καταναλωτές εκδηλώνουν μικρότερη ανησυχία περί αποκάλυψης των προσωπικών τους δεδομένων όταν πιστεύουν ότι μπορούν να ελέγξουν ποια προσωπικά δεδομένα τους αποκαλύπτονται και πώς αυτά μπορούν να χρησιμοποιηθούν στο μέλλον. Η Ομοσπονδιακή Επιτροπή Εμπορίου των Η.Π.Α. (Federal Trade Commission, συντ. FTC) από τη πλευρά της θέσπισε πέντε βασικές αρχές οι οποίες θα πρέπει να χρησιμοποιούνται για τη κατάρτιση μίας πολιτικής προστασίας στο διαδίκτυο περί προσωπικών δεδομένων (Sheehan and Hoy, 2000)[22]. Οι πέντε βασικές αρχές είναι :

1. Ενημέρωση: Οι καταναλωτές θα πρέπει να είναι ενήμεροι σχετικά με το είδος των πληροφοριών που συλλέγει μία ιστοσελίδα καθώς και το είδος των πρακτικών που χρησιμοποιούνται για να συλλεχθούν.
2. Επιλογή: Ο καταναλωτής θα πρέπει να έχει το δικαίωμα να επιλέξει εάν θα επιτρέψει ή απαγορεύσει τη συλλογή προσωπικών δεδομένων.
3. Πρόσβαση: Ο καταναλωτής πρέπει να έχει πρόσβαση στα συλλεγόμενα προσωπικά δεδομένα, ενώ επίσης θα πρέπει να έχει τη δυνατότητα να διορθώσει τις όποιες λανθασμένες πληροφορίες.
4. Ασφάλεια: Η πολιτική ασφάλειας θα πρέπει να διασφαλίζει την ακεραιότητα των δεδομένων καθώς και την ύπαρξη δικλείδων ασφάλειας περί μη κατάχρησης αυτών των δεδομένων.
5. Συμμόρφωση με τις βασικές αρχές (Redress): Δημιουργία αυτορρυθμιστικών ή κυβερνητικών μηχανισμών που να διασφαλίζουν τη συμμόρφωση με τις παραπάνω αρχές.

Η εφαρμογή των παραπάνω αρχών από μία ιστοσελίδα παρέχει τη δυνατότητα στους διαδικτυακούς καταναλωτές να ελέγξουν τη χρήση και τη συλλογή των προσωπικών τους δεδομένων με αποτέλεσμα οι καταναλωτές να εμπιστεύονται τον συγκεκριμένο ιστότοπο (Bandyopadhyay, 2009)[23]. Ένα άλλο στοιχείο που θα μπορούσε να ενισχύσει την εμπιστοσύνη του καταναλωτή σε σχέση με έναν διαδικτυακό τόπο είναι η χρήση τρίτων έμπιστων αρχών (third parties),όπως η Verisign και TRUSTe, οι οποίες θα πιστοποιούσαν τη χρήση των κανόνων ασφάλειας περί χρήσης και ελέγχου των προσωπικών πληροφοριών όπως αναφέρθηκαν (Miyazaki and Krishnamurthy, 2002)[24].

Συμπερασματικά μπορούμε να καταλήξουμε στο γεγονός ότι οι καταναλωτές ήδη από το 1999 εκδηλώνουν τις ανησυχίες τους περί αποκάλυψης των συλλεγμένων προσωπικών τους δεδομένων αλλά εάν εφαρμοστούν μέθοδοι που να αποδεικνύουν ότι έστω εν μέρει έχουν κάποιο έλεγχο πάνω σε αυτά η ανησυχίες θα μπορούσαν να απομειωθούν ιδιαίτερα δε εάν εφαρμοστούν οι πέντε αρχές που θέσπισε ο FTC.

2.2 Η μελέτη του διαδικτυακού αναλφαβητισμού και κοινωνικής ενημερότητας

2.2.1 Ο διαδικτυακός αναλφαβητισμός

Ο ρόλος του διαδικτυακού αναλφαβητισμού ή αλλιώς διαδικτυακής καλλιέργειας μελετήθηκε και ορίστηκε από τους Dinev και Hart το 2006 (Dinev and Hart 2006)[25]. Ως διαδικτυακή καλλιέργεια ορίστηκε το επίπεδο ικανότητας και γνώσης των καταναλωτών όταν χρησιμοποιούν το διαδίκτυο, συμπεριλαμβανομένης της προσπάθειας επίτευξης μίας σύνδεσης στο διαδίκτυο, της πλοήγησης σε αυτό, του διαδικτυακού εμπορίου, της προστασίας του προσωπικού τους υπολογιστή από ιομορφικό και κακόβουλο λογισμικό, της ρύθμισης των επιλογών ασφάλειας και ιδιωτικότητας του φυλλομετρητή τους, καθώς και της εφαρμογής κατάλληλων μέτρων για προστασία της ιδιωτικότητας τους πριν την αποκάλυψη πληροφοριών στο διαδίκτυο (Dinev and Hart, 2006a; Spiekermann, Grossklags, and Berendt, 2001)[25][26].

2.2.2 Η μελέτη της κοινωνικής ενημερότητας

Σε ό,τι αφορά στην κοινωνική ενημερότητα, αυτή ορίζεται ως το σύνολο των γνώσεων που έχει ένας καταναλωτής για τη χρήση των κοινωνικών δικτύων, των όρων όπως η εμπιστοσύνη, ιδιωτικότητα, ασφάλεια, λογοκρισία, και τον τρόπο επιλογής των περιορισμών ασφάλειας (Burn and Loch, 2001; Papazafeiropoulou and Pouloudi, 2001)[27][28]. Παράλληλα, κατά τους Bickford και Reynolds (Bickford & Reynolds, 2002)[29], κλειδί για την ανάπτυξη της κοινωνικής συνείδησης και κουλτούρας τους θεωρείται η επαύξηση του ενδιαφέροντος των καταναλωτών περί των υπαρχόντων κοινωνικών απειλών. Οι καταναλωτές οι οποίοι έχουν ένα υψηλό επίπεδο κοινωνικής ενημερότητας παρακολουθούν στενότερα τις πιθανές διαδικτυακές απειλές καθώς και την ανάπτυξη των πολιτικών ασφάλειας και κανονισμών (Dinev and Hart, 2006a)[25]. Η ανάπτυξη της διαδικτυακής κουλτούρας και διαδικτυακής κοινωνικής ενημερότητας βοηθούν τον καταναλωτή να αναγνωρίσει το σύνολο των τρόπων παρακολούθησης της διαδικτυακής του ζωής και να αναγνωρίσει τις απειλές που μπορεί να δεχτεί η ιδιωτικότητά του, με αποτέλεσμα να αναπτύξει μεγαλύτερη ανησυχία για την προστασία των προσωπικών του δεδομένων.

2.2.3 Συμπέρασμα μελέτης του διαδικτυακού αναλφαβητισμού και κοινωνικής ενημερότητας

Σε συνδυασμό με τα συμπεράσματα όπως αυτά διαπιστώθηκαν στην ενότητα 2.1 και μετά τον ορισμό της διαδικτυακής κουλτούρας καθώς και της κοινωνικής ενημερότητας μπορούμε να οδηγηθούμε στο ότι θα πρέπει να βρεθούν τρόποι ανάπτυξης των δύο παραπάνω ορισμών καθώς μέσω αυτών ο καταναλωτής θα είναι σε θέση τόσο στο να παρακολουθεί πιο στενά τις πιθανές απειλές που ενδεχομένως να βρεθεί αντιμέτωπος όσο και στο να αναπτύξει μία τεκμηριωμένη άποψη περί των ανησυχιών που ενδεχομένως έχει καθώς και στο να βρει τρόπους αντιμετώπισης και απομείωσης αυτών των ανησυχιών.

2.3 Χρονικό και χρηματικό κόστος ανάγνωσης των πολιτικών ασφαλείας

2.3.1 Αιτίες και υπολογισμός οικονομικού κόστους ανάγνωσης των πολιτικών ασφάλειας

Τις αιτίες πίσω από τις οποίες κρύβεται η μη ανάγνωση των πολιτικών ιδιωτικότητας, καθώς και το χρονικό και οικονομικό κόστος προσπάθησαν να διερευνήσουν οι McDonald και Cranor (2008)[30]. Ένα από τα πρώτα συμπεράσματά τους ερευνώντας τους 75 πιο δημοφιλείς ιστότοπους ήταν ότι με έναν μέσο ρυθμό ανάγνωσης μίας πολιτικής ασφάλειας 250 λέξεων το λεπτό, προκύπτει ένας μέσος ρυθμός ανάγνωσης μίας πολιτικής ασφάλειας στα 10 λεπτά. Η δε Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission, συντ. FTC) σε έρευνα που διεξήχθη το 1998 διαπίστωσε ότι ενώ το 92% των ιστοσελίδων συνέλεγε δεδομένα χρηστών, μόλις το 14% αυτών παρείχε κάποιου τύπου ενημέρωση για το ποιες πρακτικές ακολουθούν για τη συλλογή των δεδομένων [31], ενώ διαπίστωσε επίσης ότι οι καταναλωτές δεν γνώριζαν για τη διαχείριση των δεδομένων που συλλέχθηκαν [31]. Στα πρώιμα αυτά στάδια της ανάπτυξης του διαδικτύου οι πολιτικές ιδιωτικότητας ήταν σε εθελοντικό επίπεδο και χωρίς συγκεκριμένες προδιαγραφές σε ό,τι αφορά στον τρόπο παρουσίασης, το μέγεθος ή την ευκολία ανάγνωσης, ενώ αντίθετα εάν ένας ιστότοπος είχε γνωστοποιήσει την πολιτική ιδιωτικότητάς του, τότε ήταν υποχρεωμένος να την ακολουθεί (McDonald και Cranor (2009)[30].

Εξετάζοντας το κόστος από την πλευρά των εταιρειών διαχείρισης πληροφοριών προσωπικών δεδομένων και το πιθανό όφελος από την πλευρά του καταναλωτή, ο Laudon (1999)[32] πρότεινε τη δημιουργία ενός μηχανισμού διαχείρισης προσωπικών πληροφοριών (National Information Market, NIM), στον οποίο οι ιδιώτες θα μπορούσαν να αποκομίσουν μικροοικονομικά οφέλη δίδοντας εθελοντικά πληροφορίες για τους εαυτούς τους σχετικά με προσωπικά δεδομένα και ευαίσθητα προσωπικά δεδομένα (οικονομικά στοιχεία, υγεία, δημογραφικά στατιστικά κ.τ.λ.) και για χρήση για συγκεκριμένο χρονικό διάστημα. Ο Garfinkel (2001) [33] από τη πλευρά του διαπιστώνει ότι το κόστος πώλησης προσωπικών δεδομένων από εταιρεία σε εταιρεία είναι ήδη χαμηλό, και ότι η αξία αγοράς τους από έναν ιδιώτη θα κυμαινόταν κοντά στη 0,01 λίρα Αγγλίας, ποσό δηλαδή που δεν θα ήταν εύκολα αποδεκτό για εθελοντική αποκάλυψη, τη στιγμή που η αξία αγοράς κλεμμένων πληροφοριών προσωπικών δεδομένων είναι ήδη στο 1/10 της παραπάνω αξίας (Mark Trevelyan, 2008)[34]. Οι McDonald και Cranor (2009)[30] στην προσπάθειά τους να καθορίσουν το οικονομικό κόστος ανάγνωσης μίας πολιτικής ιδιωτικότητας όρισαν τρεις κατηγορίες πολιτικών ιδιωτικότητας με βάση το μέγεθός τους, η οποία ορίζεται ως τα λεπτά που προκύπτουν από το σύνολο των λέξεων προς τον ρυθμό ανάγνωσης (time to read one policy in minutes = words/read ingrate). Οι κατηγορίες έχουν ως εξής:

1) μικρή σε μέγεθος πολιτική 2071 λέξεις / 250 λέξεων το λεπτό = 8 λεπτά χρόνος ανάγνωσης

2) μέτρια σε μέγεθος πολιτική 2514 λέξεις / 250 λέξεων το λεπτό = 10 λεπτά χρόνος ανάγνωσης

3) μεγάλη σε μέγεθος πολιτική 3112 λέξεις / 250 λέξεων το λεπτό = 12 λεπτά χρόνος ανάγνωσης

Τα μεγέθη σε άθροισμα λέξεων των πολιτικών ιδιωτικότητας βασίστηκαν στην ανάλυση των 75 πιο γνωστών ιστοσελίδων που διενεργήθηκε από την A.O.L. το 2005[35]. Από τα παραπάνω συνάγεται το συμπέρασμα ότι ο χρόνος ανάγνωσης μίας πολιτικής ιδιωτικότητας κυμαίνεται μεταξύ των 8 και 12 λεπτών.

Ένας άλλος παράγοντας που ερευνήθηκε ήταν το άθροισμα των μοναδικών ιστοσελίδων που επισκέπτεται και θα έπρεπε να αναγνώσει ένας πολίτης των Η.Π.Α. ανά έτος (McDonald και Cranor, 2009)[30]. Η εν λόγω έρευνα καταλήγει στο κατώτερο όριο των 1354 μοναδικών πολιτικών ασφάλειας, εκ των οποίων οι 412 θα έπρεπε να αναγνωστούν στον χώρο εργασίας, και οι 942 εκτός αυτού, εντός ανωτάτου ορίου 1518 μοναδικών πολιτικών ιδιωτικότητας εκ των οποίων οι 586 στο χώρο εργασίας και οι 932 εκτός αυτού.

Μελετήθηκε επίσης η δυνατότητα γρήγορης – επιπόλαιης ανάγνωσης μίας πολιτικής ασφάλειας όπου οι χρήστες θα μπορούσαν να απαντήσουν σε ερωτήσεις σχετικά με το περιεχόμενο της εν λόγω πολιτικής. Σύμφωνα με τα συμπεράσματα μία μικρή σε μέγεθος πολιτική ιδιωτικότητας θα απαιτούσε 66% λιγότερο χρόνο, ενώ μία μεγάλη σε μέγεθος πολιτική ιδιωτικότητας θα απαιτούσε περίπου 4% λιγότερο χρόνο.

Στην προσπάθεια προσδιορισμού του κόστους ορίστηκε η αξία ανάγνωσης μιας πολιτικής ιδιωτικότητας στο χώρο εργασίας σε 35,86 δολάρια την ώρα και 4,48 δολάρια την ώρα εκτός αυτού.

Με βάση τα παραπάνω στοιχεία συνάγεται το συμπέρασμα ότι το ελάχιστο χρονικό κόστος ανάγνωσης του συνόλου των πολιτικών ασφάλειας ανά έτος για τους πολίτες των Η.Π.Α. θα ήταν 39,9 δις ώρες ανά έτος για πλήρη ανάγνωση και 17,9 δις ώρες ανά έτος για γρήγορη – επιπόλαια ανάγνωση. Το δε ανώτατο όριο είναι 67,1 δις ώρες ανά έτος για πλήρη ανάγνωση και 64,8 δις ώρες ανά έτος για γρήγορη – επιπόλαια ανάγνωση. Αυτό σημαίνει αφενός ότι κάθε πολίτης των Η.Π.Α. θα έπρεπε να δαπανά 40 λεπτά ημερησίως στην ανάγνωση πολιτικών ιδιωτικότητας όταν ο μέσος όρος πλοήγησης στο διαδίκτυο την ημέρα είναι περίπου 72 λεπτά (McDonald και Cranor, 2009)[30]. Αφετέρου σε κάθε Αμερικανό χρήστη του διαδικτύου το οικονομικό κόστος ανάγνωσης των πολιτικών ιδιωτικότητας θα ήταν περίπου 3,534 δολάρια το έτος, ενώ σε εθνικό επίπεδο το οικονομικό κόστος θα έφτανε περίπου τα 781 δις δολάρια, τη στιγμή που η αξία διαφήμισης για το 2007 για τις Η.Π.Α. ήταν κοντά στα 21 δις δολάρια.

2.3.2 Συμπέρασμα οικονομικών επιπτώσεων ανάγνωσης πολιτικών ασφάλειας

Με βάση όσα ειπώθηκαν στη παραπάνω ενότητα καταλήγουμε στο συμπέρασμα ότι είναι πρακτικά δύσκολο ένας καταναλωτής να δαπανήσει ακόμη και τον ελάχιστο το χρόνο που απαιτείται ώστε να είναι σε πλήρη ενημέρωση η επίγνωση της ιδιωτικότητάς του. Η δε περίπτωση οικονομικής ανταπόδοσης κρίνεται ως οικονομικά αδύνατη καθώς από τη πλευρά των καταναλωτών το ποσό ανταπόδοσης κρίνεται μικρό σε σχέση με αυτά που εθελοντικά αποκαλύπτουν ενώ από τη πλευρά των εταιρειών διαχείρισης αυτών των δεδομένων αποδεικνύεται ότι με εναλλακτικούς τρόπους μπορεί να ανακαλύψει αυτά τα ήδη σε υποπολλαπλάσιο ποσοστό. Με βάση τα παραπάνω κρίνεται απαραίτητο να βρεθεί εναλλακτικός τρόπος αποτύπωσης των πολιτικών ασφάλειας ο οποίος θα είναι ταχύτερος στην ανάγνωση, οπτικά ελκυστικός και τεκμηριωμένα αποσαφηνίζει τις δύσκολα κατανοητά έννοιες περί ασφάλειας και ιδιωτικότητας των προσωπικών δεδομένων.

2.4 Ενημερότητα χρηστών - Τι απασχολεί τους χρήστες

2.4.1 Ενημερότητα Χρηστών

Σύμφωνα με την έρευνα των Govani και Pashley (Govani & Pashley, 2005)[36] η οποία επικεντρώθηκε στην ενημερότητα των φοιτητών τοπικού πανεπιστημίου σε σχέση με το κοινωνικό δίκτυο η πλειοψηφία των φοιτητών γνώριζε τις πιθανές επιπτώσεις σχετικά με τη διαρροή προσωπικών δεδομένων καθώς και τον επικείμενο κίνδυνο για την αντιγραφή ταυτότητας ή της παρακολούθησης τους. Παρόλα αυτά και ενώ γνώριζαν τη δυνατότητα περιορισμού της διαρροής προσωπικών δεδομένων, δεν πήραν κάποιο μέτρο (Govani & Pashley, 2005)[36]. Σε μία άλλη έρευνα που διεξήχθη το 2008 (Towet al, 2008)[37] βγήκε το συμπέρασμα ότι οι χρήστες ή δεν είναι πλήρως ενήμεροι σχετικά με τα περιστατικά ιδιωτικότητας ή ένιωθαν ότι η πιθανότητα παραβίασης ιδιωτικότητας ήταν πάρα πολύ μικρή, εφόσον κατά την πεποίθησή τους ότι οι διαδικτυακές κοινότητες είναι ασφαλείς.

Έρευνα της Γερμανικής Ομοσπονδίας προστασίας Δεδομένων (German Federal And State Data Protection Commissioners, 1997)[38] δείχνει ότι οι χρήστες δεν κατανοούν ότι τα ηλεκτρονικά ίχνη που αφήνουν δίνουν τη δυνατότητα σε τρίτους να δημιουργήσουν μία εικόνα σχετικά με τη συμπεριφορά των ιδίων. Επίσης παραδέχεται ότι η πολυπλοκότητα της χρήσης των νέων τεχνολογιών καθώς και των πληροφοριών και των επικοινωνιακών συστημάτων είναι τόσο μεγάλη και συχνά δύσκολη στην κατανόηση, ώστε οι περισσότεροι χρήστες στις ανεπτυγμένες κοινωνίες δεν γνωρίζουν τι δεδομένα αποθηκεύονται γι' αυτούς, ούτε πού διακρατούνται ή για πόσο χρονικό διάστημα, ούτε και πως θα χρησιμοποιηθούν.

Το 2005 οι Gross και Acquisti [37] έδειξαν ότι το ρίσκο έκθεσης ή κλοπής ταυτότητας και λοιπών άλλων αρνητικών επιπτώσεων είναι ανάλογο με τη ποσότητα των πληροφοριών που ένας χρήστης εκθέτει μόνος του στο διαδίκτυο (Gross και Acquisti, 2005)[39]. Ενημερώνουν επίσης χαρακτηριστικά ότι, ακόμη και όταν υπάρχει μία πολιτική ασφάλειας πολλοί χρήστες δεν κάνουν χρήση της. Ενδεικτικά αναφέρουν ότι σε έρευνά τους σχετικά με το κοινωνικό δίκτυο Facebook, μόνο ένα πολύ μικρό ποσοστό χρηστών άλλαζε τις προεπιλεγμένες επιλογές ασφάλειας που ήταν ρυθμισμένες έτσι ώστε να υπάρχουν αναρτημένα όσο το δυνατόν περισσότερα δεδομένα για δημόσια χρήση, με απώτερο σκοπό την αυξημένη ευκολία να ανακαλυφθούν αυτά τα άτομα από άλλους χρήστες. Οι Cranor et al. (2006)[40] σημειώνουν ότι παρά τις προσπάθειες που έχουν γίνει ώστε μία πλατφόρμα να έχει μία εύκολα κατανοητή διεπαφή προς το χρήστη, οι περισσότεροι δεν αλλάζουν τις προεπιλεγμένες ρυθμίσεις, είτε για να μη σπαταλήσουν χρόνο, είτε επειδή μπερδεύονται, είτε υπό το φόβο ότι θα χαλάσουν τις συγκριμένες ρυθμίσεις.

Επίσης ενημερώνουν ότι η πρόσβαση σε προσωπικές πληροφορίες ενέχουν το ρίσκο όχι μόνο οικονομικών επιπτώσεων αλλά μπορεί να προκληθεί ζημιά στο επίπεδο των κοινωνικών σχέσεων μεταξύ φίλων. Πράγμα το οποίο ορισμένες φορές θεωρείται περισσότερο επιζήμιο από το να χάσει κάποιος τον αριθμό του της πιστωτικής του κάρτας. Οι Acquisti και οι συνεργάτες του (2005)[39] προειδοποιούν ότι λόγω της νομικής αυτονομίας κάθε χώρας ή ενότητας (Ευρωπαϊκή Ένωση ή Η.Π.Α.), υπάρχει περίπτωση διαφορετικής νομικής προστασίας καθώς και μεταχείρισης των προσωπικών δεδομένων.

Ιδιαίτερη εντύπωση μας κάνουν οι αναφορές πλήθους ερευνητών ήδη από το 1997 (German Federal And State Data Protection Commissioners, 1997, Cranol et al. 2006, Goettke & Chrisiana, 2007)[38][40][41] που δείχνουν ότι οι χρήστες έχουν μειωμένη γνώση σχετικά με τους κινδύνους που υπάρχουν περί ταυτοποίησης των ίδιων χρηστών μέσω προσωπικών δεδομένων που οι ίδιοι διαρρέουν στο διαδίκτυο.

Με βάση τα παραπάνω, οι Cross και Acquisti (Gross & Acquisti 2005)[39] συμπεραίνουν ότι οι χρήστες έχουν μειωμένο ενδιαφέρον σε σχέση με την ιδιωτικότητα των προσωπικών τους δεδομένων, και μία μυωπική εκτίμηση και αντίληψη των κινδύνων που μπορεί αυτά να τους δημιουργήσουν. Οι έρευνες των Cross και Acquisti το 2005 και 2006 καθώς και των Jones και Soltren το 2005[44] καταδεικνύουν ότι οι χρήστες δεν κάνουν προσπάθεια να διαβάσουν τις διαδικτυακά αναρτημένες πολιτικές ιδιωτικότητας μήτε τους όρους χρήσης. Ακόμη περισσότερο οι Cranor et al. το 2006[40] έδειξαν ότι η ανάγνωση των αναρτημένων στο διαδίκτυο πολιτικών ιδιωτικότητας καθώς και το τι είναι ιδιωτικότητα βρέθηκε να είναι μια διαδικασία δύσκολη και χρονοβόρα. Παρ΄ ότι κάποιοι ελάχιστοι χρήστες βρέθηκαν να είναι ενήμεροι σχετικά με τις δυνατότητες προστασίας των ιδιωτικών τους δεδομένων, εντούτοις δεν προσπάθησαν να τα προστατέψουν (Acquisti & Gross, 2006, Debatin et al. 2009, Dwyer, 2007, Govani & Pashley, 2007)[43][44][42][39]. Σύμφωνα με ένα σύνολο ερευνών (Donath 2007[45], Govani & Pashley, 2007, Acquisti & Gross, 2006, Debatin et al. 2009,Dwyer 2007) βρέθηκε ότι οι χρήστες που είναι φοιτητές νιώθουν ότι έχουν την ανάγκη να δείχνουν τη παρουσία τους και να κάνουν καλή εντύπωση στα άτομα που βρίσκονται στον κοινωνικό εικονικό τους κύκλο αναρτώντας ένα μεγάλο σύνολο προσωπικών δεδομένων και αναγνωριστικών δεδομένων δημοσίως (αληθινό όνομα, φωτογραφίες, ημερομηνία γέννησης, τόπο διαμονής κ.α.), καθώς περιμένουν ότι τα πλεονεκτήματα της δημόσιας ανάρτησης προσωπικών δεδομένων ξεπερνούν το αναμενόμενο κόστος αυτών (Gross & Acquisti, 2005, p.80)[39]. Ενδεικτικά, σε έρευνα που δημοσιεύτηκε το 2012 (Pitkanen, Kristiina Tuunainen, 2012)[46] σχετικά με το κοινωνικό δίκτυο Facebook και τη δημόσια ανάρτηση προσωπικών δεδομένων βρέθηκε ότι από τους 210 ενήμερους για την έρευνα φοιτητές μόλις 2 δεν χρησιμοποίησαν το πραγματικό τους όνομα (1%), ενώ 4 φοιτητές δεν χρησιμοποίησαν πραγματική φωτογραφία διαδικτυακού προφίλ (2%). Τα αποτελέσματα της έρευνας συνοψίζονται στο παρακάτω πίνακα όπως αυτά παρουσιάστηκαν (Pitkanen, Kristiina Tuunainen, 2012, p. 15):

Πίνακας Προσωπικών Δεδομένων των 210 φοιτητών (n=210)

Αντικείμενο έρευνας	Πλήθος (n=210)	Ποσοστό (%)
Πραγματικό όνομα	208	99
Φωτογραφία προφίλ	206	98
Ημερομηνία γενεθλίων	186	89
Πόλη Διαμονής	186	89
Διεύθυνση e-mail	174	83
Επίπεδο Εκπαίδευσης	169	80
Προσωπικές φωτογραφίες	158	75
Φωτογραφίες φίλων	130	62
Προσωπική σχέση	124	59

Κατάσταση Σχέσης	124	59
Σεξουαλικός Προσανατολισμός	103	49
Αγαπημένη μουσική, ταινίες	70	33
Τηλέφωνο επικοινωνίας	69	33
Δραστηριότητες/Ενδιαφέροντα	67	32
Όνομα συντρόφου	55	26
Διεύθυνση	38	18
Ιστοσελίδα	25	12
Πολιτικές πεποιθήσεις	20	10

(Πίνακας 1, Pitkanen, Tuunainen, 2012, Journal of Information Privacy & Security, p. 15)

Σε συνέχεια των παραπάνω, η έρευνα των Pitkanen, Tuunainen (2012)[46] δείχνει ότι μολονότι η πλειοψηφία των υποκειμένων δημοσίευσαν ένα μεγάλο σύνολο προσωπικών δεδομένων καθιστώντας τα δεδομένα τους δημόσια, τα εν λόγω υποκείμενα έχουν ανησυχίες σχετικά με την ασφάλειά τους. Συγκεκριμένα σε ανάλυση εφταβάθμιας κλίμακας όπου 1 = «δεν συμφωνώ καθόλου» έως 7 = συμφωνώ απόλυτα, οι χρήστες απάντησαν κατά μέσο όρο 4,5 ότι ανησυχούν για την ιδιωτικότητά τους όσο πλοηγούνται στο διαδίκτυο, καθώς και ότι η κλοπή της προσωπικής τους ταυτότητας είναι ένας κίνδυνος που θα μπορούσε να γίνει πραγματική απειλή. Με χαμηλότερο ποσοστό ρίσκου, και συγκεκριμένα με μ.ο. 3,7, απάντησαν ότι ανησυχούν για τη πιθανότητα ψευδών στοιχείων από τα άτομα με τα οποία συνομιλούν διαδικτυακά, ενώ λίγο χαμηλότερα με μ.ο. 3,2 απάντησαν ότι ανησυχούν για το γεγονός της πλοήγησης στο διαδίκτυο μέσω κινητού τηλεφώνου μήπως κάποιος μπορεί να έχει πρόσβαση στα προσωπικά δεδομένα τους σε περίπτωση που αυτό κλαπεί. Το μεγαλύτερο μ.ο. 4,8 συγκέντρωσε η κατηγορία «είμαι γνώστης της προστασίας δεδομένων και της ασφάλειας αυτών κατά τη γενική χρήση πλοήγησης τους διαδικτύου (Pitkanen, Tuunainen, 2012, Journal of Information Privacy & Security, p. 16, πίνακας 2).

Τα παραπάνω έρχονται σε πλήρη αντίθεση με το πίνακα 1 που κατέδειξε ότι τα υποκείμενα δημοσίευσαν ένα μεγάλο σύνολο προσωπικών δεδομένων μολονότι θεωρούν ότι έχουν γνώση της κυβερνοασφάλειας, αλλά και ανησυχίες ρίσκου και γνώσεις σχετικά με την ασφάλεια αυτών των δεδομένων. Τα ανωτέρω μας δείχνουν την ασυμβατότητα και τη μη ενημερότητα των εν λόγω χρηστών σχετικά με την αναλογία της ποσότητας προσωπικών δεδομένων που δημοσιεύονται ως προς το ρίσκο και την ασφάλεια αυτών. Υπενθυμίζουμε ότι σύμφωνα με τους Gross και Acquisti (2005)[39] η πιθανότητα ρίσκου έκθεσης των προσωπικών δεδομένων είναι ανάλογη της ποσότητας των δεδομένων που δημοσιεύονται κάτι που οι χρήστες δεν δείχνουν να το αντιλαμβάνονται, παρόλο τον μεγάλο βαθμό ανησυχίας τους.

Στη συνέχεια της ίδιας έρευνας των Pitkanen, Tuunainen (2012)[46] επιβεβαιώνονται οι ανησυχίες των χρηστών σε σχέση με τα προσωπικά τους, καθώς με την ίδια εφταβάθμια κλίμακα απάντησαν με μ.ο. 4,0 σε σχέση με το κοινωνικό δίκτυο Facebook ότι ανησυχούν για την ιδιωτικότητα και την ασφάλειά τους όταν χρησιμοποιούν το Facebook, αλλά παρόλα αυτά απάντησαν με μ.ο. 5,2 ότι νιώθουν άνετα να γράφουν δημόσια μηνύματα στο ιστολόγιο ενός φίλου στο facebook. Επίσης με 4,3 απάντησαν ότι εμπιστεύονται στο facebook ότι δεν θα χρησιμοποιήσει τα προσωπικά τους δεδομένα για άλλη χρήση, και με 3,9 ότι νιώθουν η ιδιωτικότητα των

προσωπικών τους πληροφοριών να προστατεύεται από το Facebook. Ακριβώς στη μέση της κλίμακας (μ.ο. 3,5) απάντησαν ότι θα ανησυχούσαν οι χρήστες εάν μία λάθος πληροφορία δημοσιευόταν για τους ίδιους στο κοινωνικό αυτό δίκτυο (Pitkanen, Tuunainen, 2012, Journal of Information Privacy & Security, p. 16, πίνακας 3). Παρ΄ όλη την ανησυχία που διαπιστώνεται εκ μέρους των υποκειμένων της έρευνας και ενώ το 94% αυτών δηλώνουν ότι γνωρίζουν (197 από τα 210 άτομα) πως μπορούν να αλλάξουν τις ρυθμίσεις ασφάλειας, δεν προχώρησαν σε παραμετροποίηση του προφίλ τους 84% εξ αυτών (164 άτομα από τους 210). Τέλος από την ίδια έρευνα των Pitkanen, Tuunainen (2012) προέκυψε ότι το 24% των υποκειμένων δεν ήταν ενήμερο ότι σε περίπτωση που δεν αλλαχθούν από τους ίδιους ρυθμίσεις ιδιωτικότητας τότε τα μέλη που συμμετέχουν σε μία ίδια ομάδα εργασίας αποκτούν πρόσβαση σε πληροφορίες του προφίλ τους, ενώ το 21% ανέφερε ότι γενικότερα δεν γνωρίζει πως κάποια άτομα έχουν τη δυνατότητα να δουν πληροφορίες που έχουν οι ίδιοι αναρτήσει.

2.4.2 Οι αρνητικές επιπτώσεις λόγω της ανησυχίας της ιδιωτικότητας

Η αυξημένη ανησυχία που παρατηρείται από τους καταναλωτές λόγω πιθανής απώλειας της ιδιωτικότητας τους κατά τη διάρκεια της περιήγησής τους στο διαδίκτυο είναι πιθανό να έχει αρνητικές επιπτώσεις σε όλες τις δραστηριότητες που αυτοί εκτελούν (Nam et al., 2006). Συγκεκριμένα, ανάλογα με το επίπεδο ανησυχίας παρατηρούνται τα εξής τρία ενδεχόμενα:

Πρώτον είναι πιθανό οι καταναλωτές να αρνηθούν να αποκαλύψουν τις προσωπικές τους πληροφορίες στο διαδίκτυο με αποτέλεσμα είτε να περιηγούνται σε ιστοσελίδες όπου δεν ζητούνται προσωπικές πληροφορίες ή να δίδουν αναληθείς πληροφορίες όταν αυτές τους ζητούνται (Nam et al., 2006, Rice, McCreadie, and Chang, 2001, Dinev and Hart, 2006b)[47][48][49].

Δεύτερον είναι πιθανό να αρνηθούν να εκτελέσουν ηλεκτρονικές συναλλαγές εάν παράλληλα τους ζητηθεί να αποκαλύψουν προσωπικές πληροφορίες, καθώς στη συντριπτική τους πλειοψηφία οι ιστοσελίδες που προσφέρουν ηλεκτρονικές διαδικτυακές συναλλαγές απαιτούν την αποκάλυψη ευαίσθητων προσωπικών δεδομένων όπως αριθμούς πιστωτικών καρτών, αριθμό τηλεφώνου, διεύθυνση ηλεκτρονικού ταχυδρομείου, ταχυδρομική διεύθυνση κ.τ.λ. (Dinev and Hart, 2006a)[25]. Με έρευνα των Graeff και Harmon (2002)[50] αποκαλύφθηκε ότι σχεδόν τα τρία τέταρτα των υποκειμένων απάντησαν ότι νιώθουν άβολα στη χρήση των πιστωτικών καρτών για διαδικτυακές συναλλαγές.

Τρίτον είναι πιθανό να αρνηθούν πλήρως τη χρήση του διαδικτύου εξ αιτίας του φόβου τους για πιθανή εισβολή στην ιδιωτική τους ζωή (Nam et al., 2006)[47]. Η κατηγορία αυτή των χρηστών περιλαμβάνει άτομα τα οποία ανησυχούν για ακούσια αποκάλυψη προσωπικών τους δεδομένων από τη χρήση ιστοσελίδων ακόμη και εάν οι ίδιοι δεν επιθυμούν να τα εκθέσουν εθελοντικά, όπως τη διεύθυνση IP που τους έχει προσδώσει ο πάροχος αποκαλύπτοντας εν μέρει τη τοποθεσία του χρήστη. Αυτό συνέβη στην περίπτωση της AOL όπου ο πάροχος διαδικτύου αποκάλυψε ότι οι χρήστες μπορούν να ταυτοποιηθούν με τη χρήση μόνο του ιστορικού της περιήγησής τους (Barbaro and Zeller, 2006)[51]. Μία ακόμη ανησυχία είναι ο φόβος της εγκατάστασης κακόβουλων

προγραμμάτων συλλογής δεδομένων, τα λεγόμενα spywares τα οποία παρακολουθούν τη δραστηριότητα περιήγησης του χρήστη και αποστέλλουν πληροφορίες σε συγκεκριμένους εξυπηρετητές (Staples, 2004)[52]. Ο φόβος δεν περιορίζεται μόνο στην εγκατάσταση κακόβουλου λογισμικού αλλά και στην πρακτική της εγκατάστασης προσωρινών αρχείων που χρησιμοποιούνται ως μεταβλητές, τα λεγόμενα cookies. Η εγκατάσταση των cookies θεωρείται νόμιμη εάν αναφέρονται στη πολιτική χρήσης της ιστοσελίδας, και εκτελούνται χωρίς ο χρήστης να τα αποδεχτεί με άμεσο τρόπο εφόσον ο ίδιος δεν παραμετροποιήσει μόνος του τις προεπιλεγμένες επιλογές ασφάλειας του φυλλομετρητή του (Strauss, El-Ansary & Frost, 2006)[53]. Τα cookies αυτά έχουν λειτουργία προσωρινής αποθήκευσης δεδομένων και μεταβλητών για την καλύτερη λειτουργία της ιστοσελίδας και την αλληλεπίδραση με τον χρήστη. Παρ΄ όλα αυτά η χρήση των cookies μπορεί να αποδειχθεί απειλή καθώς κακόβουλες ιστοσελίδες μπορούν να αναζητήσουν τα δεδομένα που περιέχονται σε αυτά με σκοπό να συλλέξουν προσωπικά δεδομένα (αριθμούς πιστωτικών καρτών, καταναλωτικές συνήθειες κτλ.). Οι παραπάνω ανησυχίες είναι ικανές να περιορίσουν στο μέγιστο βαθμό τη χρήση του διαδικτύου από έναν εξαιρετικά ανήσυχο για τα προσωπικά του δεδομένα χρήστη.

2.4.3 Συμπέρασμα ενημερότητας χρηστών και των αρνητικών επιπτώσεων

Με βάση όσα αναλύθηκαν παραπάνω προκύπτει τόσο η μειωμένη ενημερότητα των χρηστών όσο και η μειωμένη επίγνωση των αρνητικών επιπτώσεων αυτών. Μολονότι οι χρήστες πιστεύουν ότι έχουν ανεπτυγμένη ενημερότητα καθώς περιγράφουν τους πιθανούς κινδύνους, από την ανάλυση δεν προκύπτει αυτό το συμπέρασμα. Οι χρήστες ενώ διαφαίνεται να έχουν τη δυνατότητα να αλλάξουν τις επιλογές ασφάλειας στα κοινωνικά τους δίκτυα δεν προβαίνουν στις ανάλογες ενέργειες καθώς θεωρούν ότι το επίπεδο κινδύνου έκθεσης είναι μικρό. Ταυτοχρόνως αναφέρουν τη δυσκολία ανάγνωσης μίας πολιτικής ασφάλειας εξαιτίας του τρόπου γραφής και του χρόνου που απαιτεί. Το φαινόμενο δε της δημοσιοποίησης μεγάλου όγκου προσωπικών πληροφοριών στο διαδίκτυο είναι άλλος ένας παράγοντας που καταδεικνύει τη μειωμένη αντίληψη περί ενημερότητας καθώς και των αρνητικών επιπτώσεων από τους δυνητικούς κινδύνους. Αμφίδρομα οι χρήστες που έχουν τάσεις ανησυχίας δείχνουν να επιλέγουν ως προστατευτικά μέσα τα οποία περιέχουν από απόρριψη της επιλογής χρήσης συγκεκριμένων ιστότοπων έως και το ακραίο μέσω πλήρης αποχής από τη χρήση του διαδικτύου. Από τα παραπάνω γίνεται σαφές ότι πρέπει να βρεθεί ένας τρόπος ενίσχυσης της ενημερότητας των χρηστών με σκοπό οι χρήστες από τη μία πλευρά να την ενισχύσουν, να παίρνουν τα ενδεδειγμένα μέσα προφύλαξης καθώς και να καταλάβουν πλήρως τους κινδύνους που υπάρχουν ενώ αντίστοιχα να δειχθεί ότι υπάρχουν ενδεδειγμένες μορφές προστασίας της ιδιωτικής τους ζωής ώστε να μη προβαίνουν σε ακραία μέτρα προστασίας όπως τη πλήρη διαδικτυακή χρήση.

2.5 Αναπαράσταση Πολιτικών Ασφάλειας σε φορητές συσκευές

2.5.1 Παραδοσιακή αναπαράσταση

Για να καθησυχαστούν οι χρήστες σχετικά με τις περιπτώσεις διαρροής προσωπικών δεδομένων καθώς και των ενδεχόμενων απειλών σε πολλές ιστοσελίδες, η εκάστοτε πολιτική

ασφάλειας αναφέρει συγκεκριμένα πού διοχετεύονται αυτά τα προσωπικά δεδομένα, ενώ πρέπει να αναφέρονται τα νομικά όρια διανομής και πρόσβασης σε πληροφορίες που επιτρέπουν την αποκάλυψη ταυτότητας (Robert A. Robertson, 2012)[54]. Επίσης η πολιτική ασφάλειας μπορεί να περιέχει το είδος του περιεχομένου στο οποίο ο χρήστης έχει δώσει συγκατάθεση για επεξεργασία, και εάν ο ίδιος έχει τροφοδοτήσει την εν λόγω ιστοσελίδα με προσωπικά δεδομένα. Συνεπώς και η νομική σχέση και συσχέτιση μεταξύ της προστασίας των δεδομένων και των πολιτικών ασφάλειας είναι σημαντική.

Ο Acquisti στο άρθρο του (2005)[39] μας αναφέρει ότι μία πολιτική ασφάλειας αναπαρίσταται σε μία ιστοσελίδα δίδοντας πληροφορίες σχετικά με τη χρήση των προσωπικών δεδομένων που συλλέγονται, με το είδος τους, σε ποιον θα μπορούσαν να αποκαλυφθούν, καθώς και με τα μέτρα που έχουν ληφθεί για την προστασία τους. Επίσης παρέχονται πληροφορίες σχετικά με το είδος των τεχνολογιών που χρησιμοποιεί η ιστοσελίδα ώστε να συλλέξει αυτά τα δεδομένα, όπως τα cookies, ή προγραμματιστικά σφάλματα με τα οποία θα μπορούσαν συνδυαστικά και μη να αποκαλύψουν τις συνήθειες περιήγησης του χρήστη.

Ο τρόπος αναγραφής των πολιτικών ασφάλειας όπως αναφέρθηκε και στο κεφάλαιο 1 στηρίζεται κατά κύριο λόγο σε γλώσσες αναγραφής πολιτικών ασφάλειας όπως η XACML [1] και η EPAL[2]. Πρόκειται όμως για σύνθετη αναπαράσταση της εκάστοτε πολιτικής, λόγω της χρήσης νομικής ορολογίας η οποία θα μπορούσε να χαρακτηριστεί δυσνόητη για μεγάλο ποσοστό των χρηστών (Kambiz et al.) [3], ενώ μεταγενέστερα προτάθηκαν και άλλα μοντέλα αναπαράστασης όπως το Privacy Policy Visualization Method –PPVM (Kambiz et al., 2009)[1], το οποίο έκανε διαγραμματική οπτικοποίηση της πολιτικής ασφάλειας μέσω διαγραμμάτων σχέσεων – οντοτήτων (Entity–Relationship model diagramming, ERD). Σε αυτό το πρωτόκολλο η οπτικοποίηση της πολιτικής ασφάλειας γινόταν σε διακριτά επίπεδα όπου διαγραμματικά απεικονίζεται ο συλλέκτης των δεδομένων ως μία οντότητα με έναν ή πολλούς ρόλους και ο κάθε ρόλος αναλυόταν σε επιμέρους γνωρίσματα. Μεταξύ των οντοτήτων και των γνωρισμάτων παρεμβάλλονται πέντε συσχετίσεις όπου καθορίζουν τις απαιτήσεις ασφάλειας. Οι συσχετίσεις αυτές είναι επιγραμματικά:

Α) Σκοπός (Purpose): Όπου περιγράφεται συγκεκριμένα ο λόγος διακράτησης των δεδομένων.

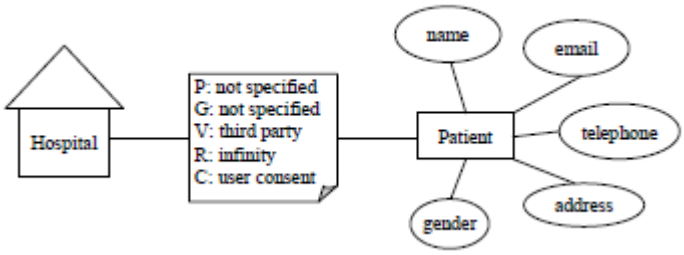
Β) Ορατότητα (Visibility): όπου περιγράφεται ποιος έχει πρόσβαση στα δεδομένα που συλλέχθηκαν.

Γ) Διακριτικότητα (Granularity): όπου καθορίζεται πως τα αποθηκευμένα δεδομένα ανακτώνται και με τι τρόπο προβάλλονται σε περίπτωση ζήτησης όπως για παράδειγμα ο βαθμός ανωνυμοποίησης και κανονικοποίησης.

Δ) Διακράτηση (Retention): όπου καθορίζεται για πόσο χρόνο θα είναι διαθέσιμα τα συλλεγμένα δεδομένα ή/και για πόσες φορές θα είναι αυτά προσβάσιμα ακόμη και για τους νόμιμους κατόχους.

Ε) Περιορισμός (Constraint): όπου περιγράφονται οι υπόλοιποι περιορισμοί που μπορούν να χαρακτηρίσουν τα δεδομένα.

Παρακάτω απεικονίζονται οι συσχετίσεις που περιεγράφηκαν έχοντας ως παράδειγμα οντότητας και συσχετίσεων ένα ασθενή νοσοκομείου μαζί με τα γνωρίσματα του ασθενή (γράφημα 1).



(Γράφημα 1 : Παράδειγμα οπτικοποίησης πολιτικής ασφάλειας με τη μέθοδο P.P.V.M. Ανάκτηση από Kambiz e tal, (2009)[1] σελ.3.)

Ένας εναλλακτικός τρόπος αναπαράστασης πολιτικών ασφάλειας με περισσότερο κατανοητή αναπαράσταση και που πλησιάζει τους τρόπους αναπαράστασης πολιτικών ασφάλειας για φορητές συσκευές που θα δούμε στην επόμενη ενότητα είναι η προσπάθεια που γίνεται τον Ιούνιο του 2012 με την έναρξη της δημιουργίας της ιστοσελίδας Terms of Service Didn't Read (συντ. TOS;DR) [99] στη διαδικτυακή διεύθυνση http://tosdr.org. Ο συγκεκριμένος ιστότοπος εμφανίζει επιγραμματικά σε τι είδους δεδομένα έχει πρόσβαση μία ιστοσελίδα μέσω της αποδοχής της Πολιτικής Ασφάλειάς της. Επίσης παρουσιάζει έναν αξιολογικό δείκτη με οπτική αναπαράσταση εικόνας που καταδεικνύει εάν αυτό το δικαίωμα που αποκτάται θεωρείται κατά την αξιολογική κρίση των διαχειριστών του TOS;DR καθώς και των χρηστών της ιστοσελίδας ως θετικό, αρνητικό ή επικίνδυνο. Επίσης οι χρήστες έχουν τη δυνατότητα να προσθέσουν νέες εφαρμογές για αξιολόγηση της Πολιτικής Ασφάλειας καθώς και να αξιολογήσουν την εν λόγω πολιτική. Οι χρήστες έχουν επίσης τη δυνατότητα να δουν σε αριθμητικά μεγέθη κατά πόσοι έχουν αξιολογήσει ότι το εκάστοτε δικαίωμα θεωρείται για παράδειγμα θετικό. Η ιστοσελίδα φαίνεται προς το παρόν να αξιολογεί μόνο εφαρμογές για σταθερούς υπολογιστές καθώς και διάσημες ιστοσελίδες. Παρόμοιο τρόπο οπτικοποίησης θα χρησιμοποιηθεί κι από εμάς για τη δημιουργία της εφαρμογής appWare που θα παρουσιαστεί στο κεφάλαιο 5 και θα αναφέρεται στη πλατφόρμα των εφαρμογών για φορητές συσκευές με λειτουργικό σύστημα Android.

2.5.2 Αναπαράσταση πολιτικών ασφάλειας σε συσκευές Android.

Με την έλευση των έξυπνων φορητών συσκευών, την επικράτηση μόνο τριών λειτουργικών συστημάτων (Android, Apple IoS, Windows Mobile) και τη δημιουργία αντίστοιχων εφαρμογών (mobile apps) έγινε επιτακτική η δημιουργία τρόπου οπτικοποίησης και απεικόνισης των πολιτικών ασφάλειας και ιδιωτικότητας. Ταυτόχρονα με τη δημιουργία αυτών των τριών λειτουργικών συστημάτων έγινε και η δημιουργία των αντίστοιχων διαδικτυακών καταστημάτων προμήθειας εφαρμογών (App Markets). Η μεθοδολογία που ακολουθήθηκε από τα App Markets διέφερε από τον παραδοσιακό τρόπο αναγραφής που αναφέρθηκε παραπάνω, και αυτή θα αναλυθεί εκτενέστερα στο κεφάλαιο 3.

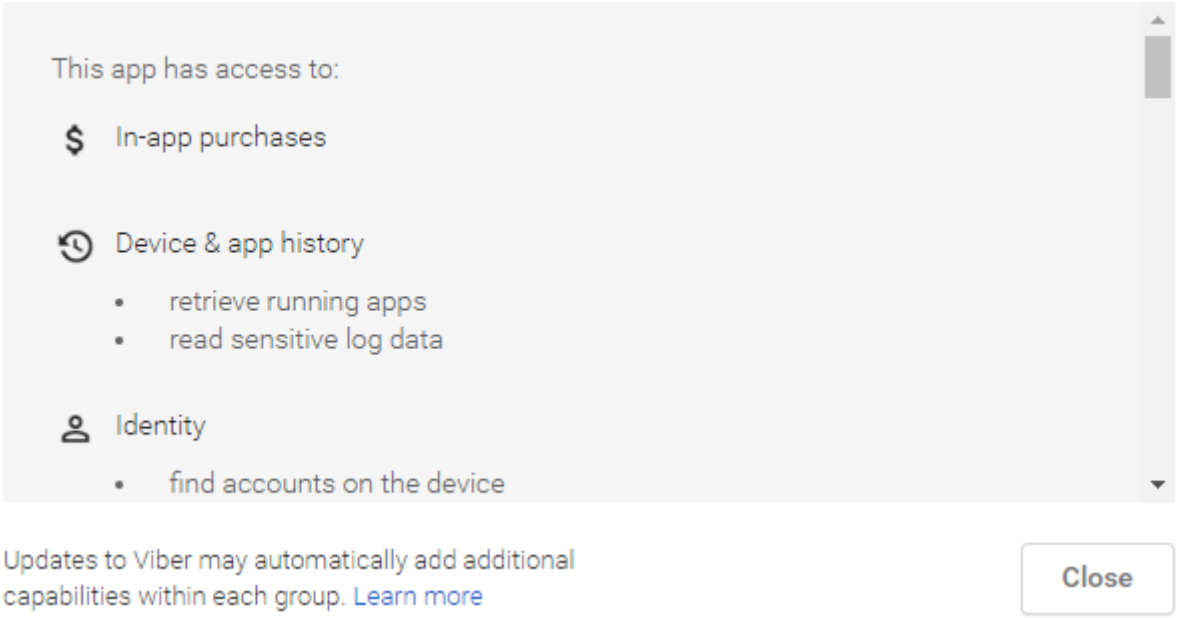
Για παράδειγμα στο google play store που είναι η επίσημη ιστοσελίδα προμήθειας εφαρμογών για φορητές συσκευές με λειτουργικό σύστημα android και η οποία βρίσκεται στη

πρώτη θέση σε επισκεψιμότητα και μεταφορτώσεις εφαρμογών (Applications–συντ. Apps) εφαρμόστηκε ένα μοντέλο απλής αναφοράς επιτρεπόμενων ενεργειών/δικαιωμάτων χρήσης, οι οποίες δεν είναι άμεσα ορατές στον καταναλωτή, δεν απαιτούν την έγκρισή του πριν ή κατά τη διάρκεια της εγκατάστασης για το ποια δικαιώματα απαιτεί για χρήση η εφαρμογή, ούτε εμφανίζονται κατά την έναρξη της αλλά ούτε και κατά τη πρώτη εκτέλεσή της. Ο μοναδικός τρόπος για να δει κάποιος χρήστης τα δικαιώματα μέχρι σήμερα είναι να μεταβεί στην αντίστοιχη ιστοσελίδα της εφαρμογής του Google Play store κι έπειτα στην επιλογή permissions. Κατά τη μετάβαση στον συγκεκριμένο χώρο ο χρήστης μπορεί να δει επιγραμματικά ποια από τα 233 δυνατά δικαιώματα απαιτεί η εφαρμογή (figure X) χωρίς περαιτέρω ανάλυση και χωρίς η αναγραφή τους να έχει ακολουθήσει κάποια από τα πρότυπα που προαναφέραμε. Ο καταναλωτής μπορούσε να αποκτήσει επίσης γνώση των ίδιων δικαιωμάτων μέσω του μενού της φορητής συσκευής, ενώ αξίζει να αναφέρουμε ότι μέχρι την έκδοση android Marshmallow ήταν αδύνατο να απαγορευτεί χειροκίνητα η πρόσβαση σε κάποιο μη αποδεκτό από το χρήστη δικαίωμα. Η μόνη περίπτωση άμεσης ενημέρωσης του χρήστη σχετικά με τα δικαιώματα πρόσβασης που απαιτεί η εφαρμογή είναι μόνο όταν η εφαρμογή αυτή λάμβανε κάποια μία νέα έκδοση και υπό την προϋπόθεση ότι προστίθεντο κάποιο νέο δικαίωμα. Επίσης η αναφορά γίνεται μόνο για τα νέα δικαιώματα που προστέθηκαν και δεν γίνεται καμία αναφορά για τα δικαιώματα που δόθηκαν μη εθελοντικά κατά τη πρώτη εγκατάσταση.

Αξίζει να αναφέρουμε ότι ο FTC ορίζει ρητά ότι οι προγραμματιστές εφαρμογών για φορητές συσκευές εφόσον συλλέγουν προσωπικά δεδομένα μέσω των εφαρμογών τους θα πρέπει να υπάρχει σχετικός σύνδεσμος εύκολα διαθέσιμος στο κοινό ο οποίος να οδηγεί στην ιστοσελίδα του κατασκευαστή που αναγράφεται η πολιτική ιδιωτικότητας [94]. Το Google Play από τη πλευρά του ενημερώνει τους δημιουργούς ότι εφόσον συλλέγονται προσωπικά δεδομένα αυτά όπως αναφέρει και ο FTC να υπάρχει ο αντίστοιχος σύνδεσμος στη σελίδα μεταφόρτωσης [95]. Παρόλα αυτά τόσο κατά την επιλογή της μεταφόρτωσης της εφαρμογής όσο και κατά την εκκίνηση της στη φορητή συσκευή δεν απαιτείται η ανάγνωση και η αποδοχή των όρων της πολιτικής ασφάλειας. Επίσης πρέπει να αναφέρουμε ότι ο τρόπος αναγραφής των πολιτικών ασφάλειας δεν διαφέρει από όσα αναφέρθηκαν στο παρόν κεφάλαιο μήτε εξαναγκάζεται με κάποιο τρόπο η υποχρεωτικότητά τους. Κατά συνέπεια ο χρήστης είναι σε θέση να μεταφορτώσει οποιαδήποτε εφαρμογή χωρίς να είναι υποχρεωμένος να αποδεχτεί φανερά και τη πολιτική ασφάλειας της εκάστοτε εταιρείας ενώ εάν δεν είναι ιδιαίτερα εξειδικευμένος στις νέες τεχνολογίες ο τρόπος προβολής των δικαιωμάτων που αποκτά η εκάστοτε εφαρμογή δεν είναι πάντα άμεσα κατανοητή στη χρήστη πόσο δε μάλλον των δυνητικών επιπτώσεων που μπορεί να έχει η τυφλή αποδοχή των δικαιωμάτων αυτών.

Με βάση τα παραπάνω αλλά και όσα θα αναφερθούν στο επόμενο κεφάλαιο κρίνεται επιτακτικό να βρεθεί ένας εναλλακτικός και άμεσος τρόπος οπτικοποίησης των πολιτικών ασφάλειας ο οποίος θα βοηθά το χρήστη να κατανοήσει εύκολα και προσιτά μία οπτικοποιημένη πολιτική ασφάλειας καθώς και των δικαιωμάτων που εκχωρεί η κάθε πιθανώς μεταφορτωμένη εφαρμογή.

Τα μοντέλα απειλής καθώς και η ανάλυση των παραπάνω δικαιωμάτων θα εξεταστούν και θα αναλυθούν εκτενέστερα στο επόμενο κεφάλαιο.



(γράφημα 2: Προβολή δικαιωμάτων της εφαρμογής Viber στο Google Play Store στο υπό μενού permissions)

2.6 Συμπεράσματα – Σύνοψη

Με βάση όσα υπόθηκαν στο παρόν κεφάλαιο εύκολα συνεπάγεται ότι η συλλογή και πώληση των προσωπικών δεδομένων και κατ' επέκταση η προσβολή της ιδιωτικότητας χωρίς πρότερη συναίνεση των υποκειμένων επεξεργασίας είναι μία κοινή πρακτική η οποία ακολουθείται τουλάχιστον από το 1998 (Wang, Lee, and Wang, 1998)[10] και δεν δύναται να ανακοπεί καθώς πλέον έχει καταστεί ιδιαίτερα εύκολη η αποθήκευσή τους. Από τη σκοπιά των χρηστών του διαδικτύου που ήδη κρίνονται ως ανήσυχοι για τα προσωπικά τους δεδομένα είναι πλέον αδύνατο να πραγματοποιηθεί οποιαδήποτε συναλλαγή χωρίς να αποκαλυφθούν προσωπικές πληροφορίες (Rust, Kannan, and Peng, 2002)[13]. Ένας από τους τρόπους απομείωσης της ανησυχίας αυτής είναι εάν οι εταιρείες που συλλέγουν αυτά τα δεδομένα αναγκαστούν να ακολουθήσουν πρακτικές καλής χρήσης όπως αυτές που προτάθηκαν από την Ομοσπονδιακή Επιτροπή Εμπορίου των Η.Π.Α. (F.T.C.). Για τους χρήστες θα πρέπει να βρεθεί ένας τρόπος επαύξησης της ενημερότητάς τους καθώς και του επιπέδου αντίληψης τους αποτρέποντας τον κοινωνικό αναλφαβητισμό τους και ενισχύοντας τη διαδικτυακή τους κουλτούρα και την ενημερότητά τους σε επίπεδα που θα τους επιτρέψουν να αναγνωρίζουν ευκολότερα τους κινδύνους που δύναται να βρεθούν αντιμέτωποι δημοσιεύοντας οι ίδιοι τα προσωπικά τους δεδομένα όπως για παράδειγμα σε ιστότοπους κοινωνικής δικτύωσης. Η τρέχουσα διαδικασία ενημέρωσης μέσω της δημοσίευσης των πολιτικών ασφάλειας που ακολουθεί ο εκάστοτε ιστότοπος δεν φαίνεται να είναι αποδοτικός καθώς το χρονικό

και οικονομικό κόστος κρίνεται απαγορευτικό για το μέσο χρήστη των Η.Π.Α. απαιτώντας μεσοσταθμικά 72 λεπτά ημερησίως ανάγνωσης πολιτικών ασφάλειας για ένα χρήστη που θα ήθελε να είναι ενήμερος, το οποίο μεταφράζεται σε 3.500 δολάρια ετησίως. Οπότε είναι επιτακτικό να βρεθεί εναλλακτικός τρόπος αποτύπωσης των πολιτικών ασφάλειας ο οποίος θα είναι ταχύτερος στην ανάγνωση, οπτικά ελκυστικός και τεκμηριωμένα αποσαφηνίζει τις δύσκολα κατανοητά έννοιες περί ασφάλειας και ιδιωτικότητας των προσωπικών δεδομένων.

3

3. Απειλές Ασφάλειας και Διαχείριση Ασφάλειας σε Φορητές Συσκευές

3.1 Διαχείριση Ασφάλειας φορητών συσκευών android

Το λειτουργικό σύστημα android χρησιμοποιεί ένα πολυμεθοδικό σύστημα ασφάλειας για να προστατέψει τόσο τους χρήστες όσο και τη συσκευή από απειλές διαφορετικών τύπων. Οι μέθοδοι χωρίστηκαν σε εφτά διακριτές κατηγορίες από τους Boksasp et al [56]:

1) Διαχείριση επιτρεπόμενων ενεργειών/δικαιωμάτων,
2) Εκτέλεση εφαρμογών σε ασφαλές περιβάλλον (sandboxing)
3) Μοναδικής υπογραφής εφαρμογών μέσω πιστοποιητικών ασφάλειας (Certification signing)
4) Απομακρυσμένης αποτροπής εκτέλεσης εφαρμογών και διαγραφής αυτών (remote kill switch)
5) Αρχειακό σύστημα ασφάλειας (File system protection)
6) Google Bouncer
7) Αντι- ϊϊκό λογισμικό (Antivirus)

3.1.1 Διαχείριση επιτρεπόμενων ενεργειών/δικαιωμάτων

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο η πρώτη μέθοδος που ακολουθήθηκε ήταν η χρήση επιτρεπόμενων ενεργειών/δικαιωμάτων (Google, 2017) [55] από ένα σύνολο 233 επιτρεπόμενων δικαιωμάτων (Παράρτημα), τα οποία καθορίζουν την απαγόρευση ή όχι της χρήσης ενός πόρου ή ενός υποσυστήματος της συσκευής. Αν μία εφαρμογή για παράδειγμα έχει πρόσβαση στο δικαίωμα WRITE_SMS τότε της δίνεται η δυνατότητα πρόσβασης στα σύντομα μηνύματα του χρήστη της συσκευής καθώς και η εγγραφή νέου μηνύματος (χρήση πόρου) ενώ με το δικαίωμα CAMERA δίνεται η δυνατότητα χρήσης της κάμερας της συσκευής (χρήση υποσυστήματος). Το σύνολο των δικαιωμάτων της συσκευής αποθηκεύεται σε ένα αρχείο τύπου xlm (Extensible Markup Language) το οποίο ονομάζεται manifest.xlm και το οποίο συνοδεύει υποχρεωτικά το πακέτο

εγκατάστασης της εφαρμογής (Application Package, APK) και δεν μπορεί να μεταβληθεί μετά την εγκατάστασή της εφαρμογής παρά μόνο εάν η εφαρμογή ενημερωθεί σε κάποια νέα έκδοση. Στη περίπτωση που απαιτείται κάποιο νέο δικαίωμα, ο χρήστης ενημερώνεται γι' αυτό. Σημειώνεται ότι δεν είναι δυνατόν ο χρήστης κατά τη διάρκεια της εγκατάστασης να απαγορέψει τη πρόσβαση σε κάποιο δικαίωμα το οποίο δεν επιθυμεί και το οποίο θεωρεί ότι παραβιάζει την ιδιωτικότητά του. Από τη πλευρά των προγραμματιστών η προαναφερθείσα δυνατότητα στοχεύει στη μείωση της πιθανότητας να καταστεί η εφαρμογή μη λειτουργική από κάποια δυσλειτουργίας της εφαρμογής λόγω έλλειψης κάποιου σημαντικού για τη λειτουργία δικαίωμα. Αν για παράδειγμα αν σε μία εφαρμογή πλοήγησης αυτοκινήτου (gps navigator) απαγορευτεί η χρήση των δικαιωμάτων ACCESS_GPS ή ACCESS_LOCATION η εφαρμογή δεν θα μπορέσει να επιτελέσει το βασικό σκοπό για τον οποίο έχει μεταφορτωθεί. Πέρα των 233 δικαιωμάτων ένας προγραμματιστής μπορεί να δημιουργήσει και δικά του σύνολα δικαιωμάτων προς χρήση της εφαρμογής ώστε να είναι δυνατή η μεταβίβαση δεδομένων από μία εφαρμογή σε μία άλλη. Λόγω του sandboxing που θα μιλήσουμε παρακάτω θα ήταν αδύνατη η διαβίβαση δεδομένων με χρήση μόνο των προεπιλεγμένων δικαιωμάτων.

3.1.2 Εκτέλεση σε προστατευμένο περιβάλλον (sandboxing)

Μία από τις καινοτομίες που εισαγάγει το περιβάλλον android είναι η εκτέλεση σε προστατευμένο περιβάλλον (sandbox) (Google, 2017) [55]. Κάθε είδους εφαρμογή ακόμη και της ίδιας της Google εκτελείται σε ένα εικονικό ατομικό περιβάλλον όπως περίπου εκτελούνται οι πολλαπλοί εικονική εξυπηρετητές (virtual machine servers, συντ. VMS) ή τα εικονικά μηχανήματα (Virtual Machines, συντ. VM) σε ένα μόνο μηχάνημα ή οι εφαρμογές που εκτελούνται σε εξυπηρετητές νέφους (Cloud Servers). Το android αποδίδει ένα μοναδικό αναγνωριστικό χρήστη (User Identification, συντ. UID) σε κάθε ξεχωριστή εφαρμογή για να επιτύχει την απομόνωση των δεδομένων μεταξύ των εφαρμογών. Εάν ο προγραμματιστής επιθυμεί τη δυνατότητα ανταλλαγής πληροφοριών μεταξύ δύο εφαρμογών του, τότε μπορεί να δημιουργήσει ένα νέο δικαίωμα το οποίο Θα αναθέτει σε αυτές τις δύο εφαρμογές ένα κοινό UID. Με αυτό τον τρόπο επιτυγχάνεται η χρήση του συνόλου των δικαιωμάτων και στις δύο εφαρμογές. Εάν, για παράδειγμα ο προγραμματιστής ορίσει κοινό UID για δύο του εφαρμογές την Α και τη Β, η Α έχει το δικαίωμα ACCESS_GPS και η δεύτερη το ACCESS_LOCATION τότε και οι δύο μπορούν έμμεσα να κάνουν χρήση αυτού του δικαιώματος καθώς η μία εφαρμογή είναι δυνατόν να ανταλλάσσει δεδομένα με την δεύτερη.

3.1.3 Μοναδικής υπογραφής των εφαρμογών μέσω πιστοποιητικών ασφάλειας (Certification signing)

Για τη δημιουργία του τρίτου αναχώματος ασφάλειας ορίστηκε η υποχρεωτική διαδικασία υπογραφής μέσω πιστοποιητικού (Signing by Certification)[57]. Με τη διαδικασία της υπογραφής της εφαρμογής μέσω του ατομικού πιστοποιητικού του προγραμματιστή αποφεύγεται η δυνατότητα κλοπής ταυτότητας δεύτερου προγραμματιστή ενώ παράλληλα αποδεικνύεται η πατρότητα της

δημιουργίας της εφαρμογής. Επίσης εάν η εφαρμογή αποδειχθεί ότι συμπεριφέρεται κακόβουλα τότε είναι δυνατό να βρεθούν οι υπόλοιπες εφαρμογές που έχει δημιουργήσει ο ίδιος προγραμματιστής.

3.1.4 Απομακρυσμένης αποτροπής εκτέλεσης εφαρμογών και διαγραφής αυτών (remote kill switch)

Για να μεταφορτωθεί μία εφαρμογή στον επίσημο ιστότοπο της Google το Google Play ο προγραμματιστής θα πρέπει να αποδεχτεί πρώτα τόσο τη Πολιτική Ανάπτυξης Προγραμμάτων της (Developer Program Policies, συντ. DPP)[58] καθώς και τη Συμφωνία Πολιτικής περί Διανομής Εφαρμογών (Developer Distribution Agreement, συντ. DPA) [59]. Στη περίπτωση που μία εφαρμογή αποδειχθεί ότι συμπεριφέρεται κακόβουλα ή ο δημιουργός της αποδειχθεί ότι έχει φτιάξει άλλες κακόβουλες εφαρμογές ή υποπέσει σε παράπτωμα έναντι των DPP ή DPA τότε το Google Play έχει τη δυνατότητα να διαγράψει τις εφαρμογές που έχουν μεταφορτωθεί σε αυτό, καθώς και από το σύνολο των φορητών συσκευών που έχει αυτή η εφαρμογή εγκατασταθεί, χωρίς τη συγκατάθεση του κάτοχου της φορητής συσκευής [60].

3.1.5 Αρχειακό σύστημα ασφάλειας (File system protection)

Το λειτουργικό σύστημα μιας φορητής συσκευής με λειτουργικό σύστημα android OS είναι αποθηκευμένο σε ένα τμήμα της αποθηκευτικής μνήμης που έχει οριστεί σε κατάσταση «μόνο για ανάγνωση» (read only) [61]. Μόνο το Google Play μέσω αναβάθμισης μπορεί να τροποποιήσει τα αρχεία συστήματος εκτός της περίπτωσης που κάποιος εξειδικευμένος χρήστης ξεκλειδώσει το συγκεκριμένο τμήμα της υποθηκευμένης μνήμης (rooting) και μόνο με τη χρήση εξειδικευμένου λογισμικού και για το οποίο απαιτείται η φορητή συσκευή να συνδεθεί εξωτερικά με ηλεκτρονικό υπολογιστή. Σε περίπτωση δε ξεκλειδώματος της προστατευμένης μνήμης λήγει η εγγύηση της συσκευής. Μέχρι τη συγγραφή της διατριβής δεν έχει βρεθεί εφαρμογή που να αποκτήσει απευθείας πρόσβαση στο προστατευμένο τμήμα της αποθηκευτικής αυτής μνήμης.

3.1.6 Google Bouncer

Το 2012 η Google ενσωμάτωσε στο Google Play το Google Bouncer (Lockheimer 2012)[62] το οποίο συμπεριφέρεται ως ένα ενσωματωμένο πρόγραμμα αντιικής προστασίας καθώς και ως προσομοιωτής. Κάθε εφαρμογή η οποία μεταφορτώνεται στο Google Play ελέγχεται για τυχόν κακόβουλο γνωστό κώδικα όπως θα έκανε ένα αντιικό πρόγραμμα αλλά η πρωτοτυπία του έγκειται στο γεγονός ότι προσομοιώνει την εκτέλεση της εφαρμογής για τη τυχόν ανίχνευση περίεργης συμπεριφοράς όπως αποστολή δεδομένων ή προσπάθεια προσπέλασης σε μη εξουσιοδοτημένα

δεδομένα. Σε περίπτωση που γίνει ανίχνευση περίεργης συμπεριφοράς τότε η εφαρμογή διαγράφεται ενώ υπάρχει η περίπτωση αποκλεισμού του δημιουργού της εφαρμογής από το google play καθώς και αφαίρεσης και άλλον προγραμμάτων που έχει δημιουργήσει (Rash 2012)[63].

3.1.7 Αντι- ιϊκό λογισμικό (Antivirus)

Αν και το Google Bouncer φαίνεται να προσφέρει μία κάποιου τύπου προστασία αφού συμπεριφέρεται ως αντι-ιικό λογισμικό οι συνήθεις εταιρείες προγραμμάτων ασφάλειας αντι-ιικών προγραμμάτων όπως η McAfee (McAfee Mobile Security) [64] και η Bitdefender (Mobile security for android)[65], έχουν δημιουργήσει τις αντίστοιχες εκδόσεις για φορητές συσκευές android. Ο σκοπός των προγραμμάτων αυτών είναι αφενός η μείωση της πιθανότητας μόλυνσης της συσκευής από πολύ πρόσφατο κακόβουλο λογισμικό (zero day threats) οι οποίες περιορίζονται όπως εξηγήσαμε λόγω του sandboxing και από άλλους λόγους που θα επεξηγήσουμε περισσότερο στα μοντέλα απειλών στην υποενότητα 3.2. Επίσης αφορούν το λογισμικό που μεταφορτώνεται στις συσκευές από τρίτες ανεπίσημες αγορές μεταφόρτωσης εφαρμογών για φορητές συσκευές (third party app markets) οι οποίες δεν διαθέτουν τις δυνατότητες που προσδίδει το Google Bouncer. Επίσης προστατεύουν από τη πρόσφατη απειλή αθέμιτης κρυπτογράφησης δεδομένων - ransomware) (Shannon McCarty-Caplan 2016)[66] όπου για να αποκρυπτογραφηθούν τα δεδομένα του χρήστη απαιτείται να πληρωθούν λύτρα στο κατασκευαστή του λογισμικού συνήθως μέσω του ηλεκτρονικού κρυπτονομίσματος bitcoin (JP Buntix, 2017)[67].

3.2 Μοντέλα Απειλών φορητών συσκευών android

3.2.1 Δούρειοι Ίπποι (Trojan Horses)

Οι επιθέσεις μέσω δούρειων ίππων σε φορητές συσκευές είναι ανάλογες με εκείνες στους κλασικούς ηλεκτρονικούς υπολογιστές όπου ένα πρόγραμμα κακόβουλου λογισμικού εγκαθίσταται στο σύστημα με σκοπό τη μεταγενέστερη επίθεση σε άλλα υπολογιστικά συστήματα, τη διαγραφή, τροποποίηση και υποκλοπή συστημάτων (Kaspersky Labs) [81]. Αφετέρου στοχεύει στη δημιουργία μεγάλης και περιττής κίνησης δεδομένων στο διαδίκτυο με σκοπό να δημιουργήσει το φαινόμενο άρνησης εξυπηρέτησης υπηρεσιών (Cara McGoogan 2016)[83] ή αλλιώς Distributed Denial Of Services (συντ. DDOS) σε ιστοσελίδες και δίκτυα. Οι δούρειοι ίπποι ενσωματώνονται συνήθως σε νόμιμες εφαρμογές που αναδιανέμονται μέσω τρίτων ιστοσελίδων μεταφόρτωσης εφαρμογών για φορητές συσκευές και σπανιότερα από τον επίσημο ιστότοπο Google Play (Stone-Gross 2013)[82]. Αξίζει να διευκρινιστεί ότι λόγω του Sandboxing (κεφ. 3.1.2) οι κακόβουλες εφαρμογές όπως ιοί και σκουλήκια δεν θα είχαν σοβαρές επιπτώσεις στη φορητή συσκευή καθώς δεν μπορούν να επιμολύνουν τις υπόλοιπες εφαρμογές που βρίσκονται εγκατεστημένες στη φορητή συσκευή εκτός των εφαρμογών με κοινά UIDs που θα ήταν εφαρμογές του ίδιου δημιουργού.

3.2.2 Λογισμικό Κατασκοπίας – Spyware

Οι εφαρμογές κατασκοπίας Margaret Rouse (2016) [84] όπως και οι δούρειοι ίπποι μολύνουν μία φορητή συσκευή μέσω της ενσωμάτωσής τους σε νόμιμες εφαρμογές ακολουθώντας την ίδια τακτική κάνοντας δηλαδή χρήση τρίτων ιστοσελίδων μεταφόρτωσης εφαρμογών. Οι εφαρμογές αυτές έχουν ως σκοπό τη κατασκοπία του χρήση, τη καταγραφή συνηθειών του καθώς και την υποκλοπή προσωπικών του δεδομένων όπως αριθμούς πιστωτικών καρτών και αρχείων του και μεταβίβαση σε τρίτους (Brook 2013)[85].

3.2.3 Εκμετάλλευση Δικαιωμάτων Υπερχρήστη (Root Exploit)

Όπως αναφέρθηκε και στην εισαγωγή οι φορητές συσκευές έρχονται στην αγορά με κλειδωμένες τις δυνατότητες υπερχρήστη. Οι χρήστες από τη πλευρά τους με σκοπό να εκμεταλλευτούν όσο το δυνατόν περισσότερα χαρακτηριστικά της συσκευής τους όπως την απεγκατάσταση προγραμμάτων και παιχνιδιών που είναι προεγκατεστημένα στη συσκευή και καταναλώνουν πολύτιμο χώρο και υπολογιστικούς πόρους προσπαθούν να ξεκλειδώσουν τη συσκευή τους με τη χρήση λογισμικών τρίτων κατασκευαστών. Κακόβουλοι προγραμματιστές κάνουν χρήση αυτού του ξεκλειδώματος και δυνητικά μπορούν να αποκτήσουν το πλήρη έλεγχο της συσκευής και να εγκαταστήσουν ακόμη και χωρίς την γνώση του κατόχου της συσκευής διάφορα προγράμματα που περιέχουν Trojans και spywares ή να τα μετατρέψουν σε υπολογιστές ζόμπι ή αλλιώς botnets (κεφ. 3.2.4).

3.2.4 Botnets

Ως botnets χαρακτηρίζονται οι συσκευές στις οποίες έχει εγκατασταθεί κακόβουλο λογισμικό το οποίο βρίσκεται σε αδράνεια μέχρι να δεχθεί τις εντολές του προγραμματιστή τους BullGuard[86]. Συνήθως τα botnets χρησιμοποιούνται ταυτόχρονα σε μεγάλο αριθμό για να πραγματοποιήσουν επιθέσεις τύπου άρνησης εξυπηρέτησης υπηρεσιών με τα αποτελέσματα να είναι αυτά που αναφέρθηκαν στο κεφάλαιο 3.2.1. ή για αποστολή αυτόκλητων μηνυμάτων sms από εταιρείες υψηλής χρέωσης (premium SMS).

3.2.5 Αποστολή μηνυμάτων SMS υψηλής χρέωσης.

Μολονότι η αποστολή μηνυμάτων υψηλής χρέωσης συνήθως δεν κάνει χρήση συγκεκριμένης ευπάθειας αλλά συνήθως εκμεταλλεύεται τη μη επαρκή ενημέρωση των χρηστών, αναφέρεται ως ένα από τα μοντέλα απειλών για φορητές συσκευές εξαιτίας της πολύ υψηλής συχνότητας και στόχων που παρουσιάζει. Στην έκθεση κυβερνοαπειλών της Kaspersky Labs (2014) [87] παρουσιάστηκε ότι η προσπάθεια χρέωσης χρηστών φορητών συσκευών μέσω μηνυμάτων υψηλής

χρέωσης καταλάμβανε το 48,15 % επί των συνολικών λοιπών απειλών ενώ κατά τα έτη 2010 έως το 2012 τα ποσοστά κυμαίνονταν στο 40%(ESET, 2012) [89]. Για την εφαρμογή αυτής απειλής ο χρήστης συνήθως πείθεται από μία ιστοσελίδα ή εφαρμογή να γράψει και να αποστείλει τον τηλεφωνικό του αριθμό και έπειτα λαμβάνει ένα κωδικό επιβεβαίωσης που τον επανεγγράφει στην εν λόγω ιστοσελίδα χωρίς να διαβάσει τους όρους χρήσης (Cybersecurity, 2015) [88]. Στη συνέχεια το κινητό του είτε αποστέλλει είτε δέχεται πλέον μηνύματα υψηλής χρέωσης χρεώνοντας τον αποστολέα. Η αποστολή μηνυμάτων υψηλής χρέωσης μπορεί να θεωρηθεί ως ευπάθεια όταν αυτή λαμβάνει χώρα έπειτα από την εγκατάσταση κακόβουλου λογισμικού όπως Botnets και Trojans.

3.3 Συνδυαζόμενα Δεδομένα ως μοντέλο απειλής ενάντια στην Ιδιωτικότητα χρηστών

3.3.1 Παραδοσιακές συνδυαστικές μέθοδοι αποκάλυψης ανωνυμοποιημένων δεδομένων.

Με τον όρο «συνδυαζόμενα δεδομένα ως μοντέλο απειλής» νοούνται τα δεδομένα που από μόνα τους δεν μπορούν ταυτιστούν με πραγματικές οντότητες, σε συνδυασμό με άλλα δεδομένα επέρχεται η πλήρη ταυτοποίηση τους. Το 1997, για παράδειγμα, η ερευνήτρια Barth-Jones (2015)[90] κάνοντας χρήση μίας λίστας στην οποία υπήρχαν ως δημόσια δεδομένα η ημερομηνία γέννησης, το φύλο και ο ταχυδρομικός κώδικας και μία ανωνυμοποιημένη βάση δεδομένων που περιείχε ιατρικά δεδομένα υπαλλήλων της πολιτείας της Μασαχουσέτης ταυτοποίησε και ανέκτησε ιατρικά δεδομένα για τον κυβερνήτη της Bill Weld. Άλλο χαρακτηριστικό παράδειγμα αποτελούν όταν το 2007 ερευνητές από το Texas (Narayanan, 2008)[91] οι οποίοι αξιοποίησαν δεδομένα που βρήκαν διαθέσιμα στο διαδίκτυο και εφαρμόζοντας ανάλογες συνδυαστικές μεθοδολογίες κατάφεραν να αποανωνυμοποιήσουν μία ανωνυμοποιημένη βάση δεδομένων που περιείχε 500.000 πελάτες του διαδικτυακού καναλιού Netflix. Με ανάλογο τρόπο μαθητές σχολείου του Σικάγο (Emam & Dankar, 2008)[92] κατάφεραν να ταυτοποιήσουν τη Βάση Δεδομένων αυτοχείρων του Σικάγο διασυνδέοντας δημόσια δεδομένα όπως ευρετήρια θανάτων και δημοσιευμάτων.

3.3.2 Συνδυαστικές μέθοδοι μη εθελοντικής παρακολούθησης χρηστών με χρήση νέων τεχνολογιών και αξιοποίηση δημόσιων δεδομένων.

Λόγω της επέκτασης της τεχνολογίας, της ανόδου της χρήσης κοινωνικών δικτύων και της δημοσιοποίησης μεγάλου μεγέθους δεδομένων στο διαδίκτυο χωρίς πλήρη ενημερότητα των χρηστών έκαναν την εμφάνισή τους νέες μέθοδοι παρακολούθησης μέσω συνδυαστικών δεδομένων. Όπως αναφέρθηκε και στο κεφάλαιο 2 πάρα πολλοί χρήστες δημοσιοποιούν στα κοινωνικά δίκτυα προσωπικά δεδομένα, όπως δεδομένα θέσης που θεωρούνται επικίνδυνα εξ ορισμού αλλά και δεδομένα όπως το επάγγελμα ή τον χώρο εργασίας. Παρόλο που εκ πρώτης

όψεως δεν φαίνεται επικίνδυνο με κατάλληλους συνδυασμούς είναι δυνατό να προκύψει έμμεσα ή άμεσα η τοποθέτηση του εν λόγω ατόμου σε συγκεκριμένο χώρο σε συγκεκριμένο εύρος ώρας. Χαρακτηριστικό παράδειγμα είναι οι εφαρμογές για κινητά οι οποίες έχουν πρόσβαση στο δικαίωμα Approximate location οπότε παρέχεται στον προγραμματιστή της εφαρμογής πρόσβαση στα MNC, MCC, ECI και TAC. Η εφαρμογή Viber, για παράδειγμα, που θα αναλύσουμε στην επόμενη ενότητα παρέχει αυτά τα δικαιώματα. Πλέον με τη χρήση ιστοσελίδων όπως η cellidfinder.com μπορεί να βρεθεί η κεραία κινητής τηλεφωνίας στην οποία είναι συνδεδεμένος ο χρήστης της εφαρμογής, αλλά και το εύρος κάλυψης αυτής της κεραίας. Άρα γνωρίζει ότι το άτομο δεν βρίσκεται κοντά στο χώρο του σπιτιού του αλλά κοντά στον χώρο εργασίας του οπότε είναι επιρρεπές σε διαφόρου τύπου επιθέσεις όπως ληστεία ή ανεπιθύμητη παρακολούθηση. Επίσης με συχνή παρακολούθηση αυτού του δικαιώματος καθώς και την ανάρτηση δεδομένων σε κοινωνικά δίκτυα είναι δυνατή η δημιουργία προφίλ των συνηθειών του χρήστη όπως δημοσιοποίησε η εφημερίδα The Guardian το 2013 (Gallagher, 2013)[93]. Πιο συγκεκριμένα, περιγράφει τη χρήση της εφαρμογής RIOT (Rapid Information Overlay Technology) που ανέπτυξε η πέμπτη μεγαλύτερη ανάδοχος εταιρεία αμυντικών συμβολαίων για το στρατό των ΗΠΑ Raytheon. Η εφαρμογή RIOT συλλέγει τακτικά αυτοματοποιημένα πληροφορίες από τα πιθανά κοινωνικά δίκτυα χρηστών όπως το Facebook, το Twitter και το Foursquare, αναλύει τα τρισεκατομμύρια δεδομένων που προκύπτουν και έτσι δημιουργεί το ψηφιακό χάρτη τους με απώτερο σκοπό να βοηθήσει τις ΗΠΑ στην ανάπτυξη της εθνικής της ασφάλειας. Με τη χρήση του Riot είναι δυνατό με μερικά μόλις κλικ να παρθεί ένα στιγμιότυπο της οντότητας που παρακολουθείται και να περιέχει ένα μεγάλο υποσύνολο των δεδομένων του όπως ποιοι είναι οι φίλοι της, τα μέρη που έχει επισκεφτεί και λοιπές άλλες δημόσια αναρτημένες συνήθειες. Προσπάθειες για τη δημιουργία ανάλογων προγραμμάτων έχει κάνει και το FBI (infosecurity 2012)[94] όταν ζήτησε να εξεταστεί η δυνατότητα της δημιουργίας ενός προγράμματος ανοικτού κώδικα που να αντλεί και να αναλύει δεδομένα από τους κοινωνικούς ιστότοπους, να αναγνωρίζει κρίσιμα γεγονότα και να προειδοποιεί άμεσα για πιθανή περίπτωση κρίσης ή απειλής.

3.4 Σύνοψη και Συμπεράσματα

Η διαχείριση της ασφάλειας στις φορητές συσκευές android πραγματοποιείται με ένα πολυμεθοδικό σύστημα 7 κατηγοριών (Boksasp et al [56]). Μέσω επιτρεπόμενων ενεργειών/δικαιωμάτων όπου η εφαρμογή αποκτά πρόσβαση στο υλικό, στο λογισμικό του χρήστη καθώς και δεδομένα του και τα οποία προσδιορίζονται επιγραμματικά στο manifest.xlm. Μέσω της εκτέλεσης της εφαρμογής σε απομονωμένο και ασφαλές περιβάλλον (sandboxing) όπου η κάθε εφαρμογή εκτελείται απομονωμένα χωρίς να έχει δυνατότητα επικοινωνίας με τις υπόλοιπες εφαρμογές που εκτελούνται στη φορητή συσκευή πλην τις λοιπές εφαρμογές που έχει υλοποιήσει ο ίδιος προγραμματιστής ή η ίδια εταιρεία κατασκευής. Η μοναδική υπογραφή των εφαρμογών του δημιουργού μέσω ατομικού πιστοποιητικού ασφάλειας (Certification Signing) διασφαλίζει το χρήστη της συσκευής ότι δεν εκτελεί κάποια εφαρμογή που είναι πλαστή αναπαραγωγή αυθεντικού προϊόντος ενώ μέσω της απομακρυσμένης αποτροπής εκτέλεσης εφαρμογών και διαγραφής (remote kill switch) σε περίπτωση αναγνώρισης μιας κακόβουλα δημιουργημένης εφαρμογής δύναται η απομακρυσμένη απεγκατάστασή της καθώς και αφαίρεσης έως και όλων των εφαρμογών του ίδιου

δημιουργού τόσο από τον επίσημο ιστότοπο όσο και από το σύνολο των φορητών συσκευών που έχει εγκατασταθεί. Επίσης ο βασικός κώδικας του λογισμικού δηλαδή το αρχειακό σύστημα ασφάλειας (file system protection) είναι σε κατάσταση «ανάγνωση μόνο» και δεν δύναται να τροποποιηθεί από καμία εφαρμογή ή χρήστη πλην των έμπειρων χρηστών που μπορούν να προσπαθήσουν να ξεκλειδώσουν το λειτουργικό σύστημα μέσω εκρίζωσης (rooting) του λειτουργικού συστήματος της συσκευής. Επίσης, μέσω του Bouncer μόλις μία εφαρμογή μεταφορτωθεί στον επίσημο ιστότοπο Google Play εκτελείται σε εικονικό περιβάλλον προσομοίωσης με σκοπό να ανακαλυφθεί τυχών περίεργη συμπεριφορά ακόμη και πριν την εγκαταστήσουν χρήστες ενώ σε περίπτωση πραγματοποίησης αυτής της απειλής εκτελούνται τα μέτρα που περιεγράφηκαν παραπάνω όπως το remote kill switch αφαιρώντας την εφαρμογή από τον ιστότοπο και τα πιθανά του θύματα ενώ δύναται να αφαιρεθούν και οι υπόλοιπες εφαρμογές του ίδιου δημιουργού. Τέλος μέσω της χρήσης αντι-ϊϊκών λογισμικών (antiviruses) τρίτων κατασκευαστών γίνεται η προσπάθεια αντιμετώπισης απειλών ημέρας (zero day threat) ενώ με αυτό τον τρόπο επιτυγχάνεται η προσπάθεια αντιμετώπισης των κακόβουλα γραμμένων εφαρμογών που έχουν μεταφορτωθεί από ανεπίσημους ιστότοπους.

Σε ότι αφορά τις απειλές που βρίσκονται αντιμέτωποι οι χρήστες εδώ βρίσκουμε τόσο της κλασικές περιπτώσεις που υπάρχουν στους ηλεκτρονικούς υπολογιστές όπως τους «Δούρειους Ίππους» και τα λογισμικά κατασκοπίας (spywares) μέσω των οποίων ο χρήστης μπορεί να γίνει θύμα υποκλοπής των προσωπικών του δεδομένων ή στόχος διαφημίσεων, ενώ επίσης μπορεί να βρεθεί αντιμέτωπος να γίνει η συσκευή του προϊόν δημιουργίας περιττής κίνησης δεδομένων στο διαδίκτυο (DDoS ή DoS Attacks) καθώς και να γίνει αποστολέας ή παραλήπτης μηνυμάτων SMS υψηλής χρέωσης. Τα παραπάνω γίνονται περισσότερο εφικτά όταν ο χρήστης προσπαθήσει και καταφέρει να αποκτήσει δικαιώματα υπερχρήστη στο κινητό καθώς πλέον πολλές από τις μεθόδους αντιμετώπισης απειλών που προσφέρει το android λειτουργικό είναι πλέον αναποτελεσματικές.

Στην ενότητα «Συνδυαζόμενα δεδομένα ως μοντέλο απειλής» παρουσιάστηκαν οι συνδυαστικές μέθοδοι επεξεργασίας δεδομένων που μπορούν να εφαρμοστούν με σκοπό την αποανωνυμοποίηση Βάσεων Δεδομένων ενώ εκτενέστερα παρουσιάστηκε πως με τη χρήση νέων τεχνολογιών και την αξιοποίηση δημόσιων δεδομένων είναι δυνατή η μη εθελοντική παρακολούθηση των χρηστών σε τεχνολογικό και φυσικό επίπεδο. Ειδικότερα ανεδείχθη πως με τη δημιουργία λογισμικού συνδυαζόμενων δεδομένων όπως το R.I.O.T. είναι δυνατή η μαζική παρακολούθηση των χρηστών εκμεταλλευόμενο την έλλειψη ενημερότητάς τους και την εθελοντική αποκάλυψη από τους ίδιους δημόσιων πλέον δεδομένων σε ιστότοπους κοινωνικής δικτύωσης.

4

Προσομοίωση απειλής

4.1 Παράδειγμα απειλής συνδυαζόμενων δεδομένων ευπάθειας με χρήση της εφαρμογής Viber.

4.1.1 Η περίπτωση Viber

Το Viber είναι μία δημοφιλής εφαρμογή αποστολής άμεσων μηνυμάτων καθώς και παροχής τηλεφωνίας μέσω διαδικτύου (Voice Over I.P. συντ. v.o.i.p.) για android και iOS συσκευές ενώ πλέον υπάρχει και αντίστοιχη εφαρμογή για Η/Υ. Η εφαρμογή αυτή έως σήμερα έχει εγκατασταθεί σε πάνω από 500.000.000 android συσκευές σύμφωνα με το google play ενώ έχει αξιολογηθεί με 4,3 με ανώτερο το 5 από πάνω από 9 εκ. Χρήστες. Οι εγκαταστάσεις αυτές δεν αφορούν διακριτά άτομα αλλά άθροισμα εγκαταστάσεων σε πολλαπλές συσκευές. Κατά τη διάρκεια της έρευνας αυτής ανακαλύφθηκαν πολλαπλές δυνατότητες διαρροής προσωπικών δεδομένων. Συγκεκριμένα ένας μέτριος γνώστης χρήσης Η/Υ έχει τη δυνατότητα να ανακτήσει πλήθος προσωπικών δεδομένων όπως τη φωτογραφία προφίλ του συνόλου των χρηστών του Viber ή την ώρα που τελευταία φορά συνδέθηκαν στην εφαρμογή. Επίσης είναι και πιθανή η διασύνδεση της φωτογραφίας προφίλ με φυσικό πρόσωπο ή με βάση τον αριθμό τηλεφώνου του (ενότητα 4.2.1), οπότε γίνεται πιθανή και η διαρροή του πραγματικού ονόματος του χρήστη. Επιπροσθέτως αξίζει να σημειωθούν τρία πράγματα για την εν λόγω εφαρμογή. Πρώτον ότι κατά την εγκατάστασή της αποστέλλεται ο αριθμός του κινητού τηλεφώνου στους εξυπηρετητές του Viber από προεπιλογή. Κατά συνέπεια οι λοιποί χρήστες της εφαρμογής ενημερώνονται ότι ο νέος χρήστης έχει εγκαταστήσει πλέον το Viber ενώ φαίνεται και η πρώτη σύνδεσή του. Κατά δεύτερον υπάρχει πρακτική αδυναμία στο να κλείσει ο χρήστης το Viber. Ακόμη και εάν επιλέξει έξοδο από την εφαρμογή αυτή εξακολουθεί να τρέχει στο παρασκήνιο με το σύνολο των δυνατοτήτων του. Κατά τρίτον και σοβαρότερο είναι ότι δεν ζητάει επιβεβαίωση ώστε κάποιος να σε προσθέσει ως επαφή στο Viber και γι’ αυτό το λόγο είναι δυνατές οι τεχνικές που θα εφαρμόσουμε.

4.1.2 Ο σκοπός της Προσομοίωσης

Ο σκοπός του παραδείγματος μας είναι να δημιουργηθούν κατάλληλα στατιστικά δεδομένα που να μπορούν να αποδείξουν τη διαρροή δεδομένων που μπορούν να προκύψουν από απλές συνδυαστικές διαδικασίες οι οποίες μπορούν να γίνουν από το μέσο επίπεδο χρηστών καθώς δεν απαιτούνται εξειδικευμένες προγραμματιστικές γνώσεις. Επίσης έχει ως σκοπό να καταδείξει σε επόμενο επίπεδο τη μη ενημερότητα των χρηστών περί ανάκλησης των πραγματικών τους δεδομένων μέσω συνδυαστικών τεχνικών.

4.1.3 Μεθοδολογία και προετοιμασία για την άντληση δεδομένων (data mining).

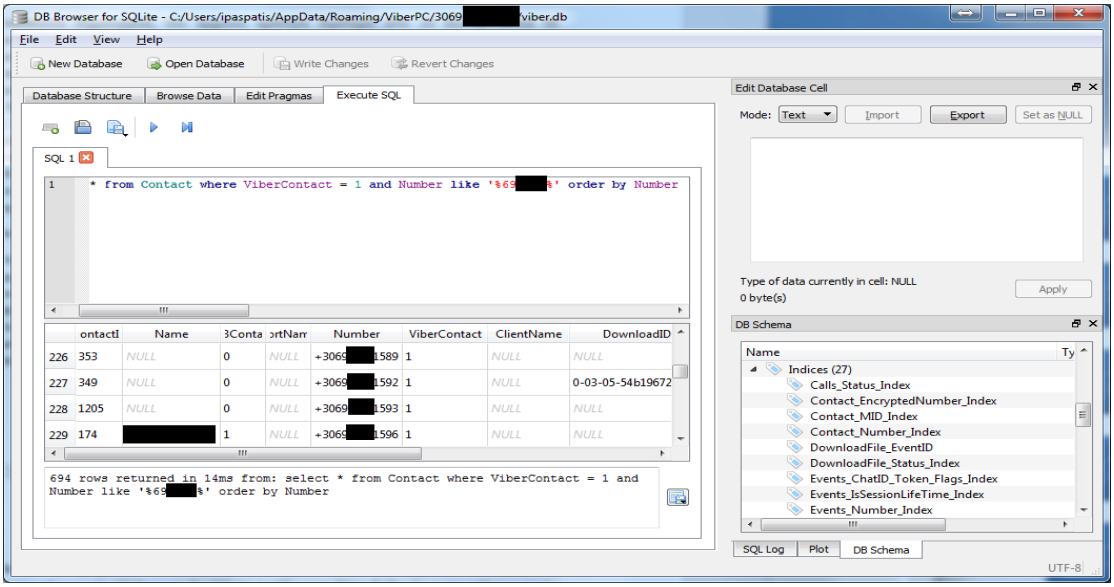
Το μοντέλο της άντλησης δεδομένων έχει ως εξής. Ο ερευνητής δημιουργεί ένα αρχείο χωρισμένο με κόμματα π.χ. csv το οποίο να είναι συμβατό είτε με τη γραμμογράφηση του google contacts account είτε με android account. Με ένα μικρό python script λιγότερο των 10 γραμμών [Παράρτημα] δημιουργήσαμε ένα αρχείο csv στο οποίο περιέχονται εικονικά δεδομένα επαφών και πραγματικοί σειριακοί αριθμοί κινητών τηλεφώνων. Στο δικό μας αρχείο περιέχονται 2.000 σειριακές εγγραφές που γνωρίζαμε ότι κατά πάσα πιθανότητα ανήκαν σε εταιρικά κινητά τηλέφωνα εταιρείας που έχει κλείσει. Οι εγγραφές μέσα στο αρχείο τύπου csv είναι καταγεγραμμένες ως εξής:

1. Οι τίτλοι NAME, FAMILY NAME, PHONE
2. Ένα εικονικό όνομα επαφής με ονομασία dummy[σειριακός αριθμός]
3. Ένα εικονικό επώνυμο επαφής με ονομασία dummySurname[σειριακός αριθμός]
4. Ένας αριθμός κινητού τηλεφώνου με τη προσθήκη του κωδικού χώρας (+30 για Ελλάδα)

Η διαδικασία δημιουργίας του αρχείου κράτησε λιγότερο από 10 δευτερόλεπτα σε προσωπικό υπολογιστή (Intel i7 6700, 16GB RAM, 250 GB SSD SATA 3). Στη συνέχεια δημιουργήθηκε ένα google account με όνομα dummyViberVulnerability και έγινε η εισαγωγή του αρχείου στο google.com/contacts. Έπειτα αγοράστηκε κάρτα sim και εγκαταστάθηκε στο εργαστηριακό κινητό (Samsung Galaxy2) στο οποίο προστέθηκε ο λογαριασμός google που δημιουργήσαμε ώστε να πραγματοποιηθεί η εγκατάσταση του Viber [68] από το google play. Για τη διαχείριση των δεδομένων και για να επιτευχθεί η πλήρης απομόνωση τους δημιουργήθηκε μία εικονική μηχανή (Virtual Machine) με VMware Workstation Player 12 [69] και εγκαταστάθηκε λειτουργικό σύστημα Windows 10. Έπειτα εγκαταστάθηκε έκδοση Viber για Η/Υ (Viber for Windows) [70] και εγκαταστάθηκε ο αριθμός τηλεφώνου της sim καθώς και το λογισμικό DB Browser for SQLite [71] που θα χρησιμοποιηθεί για την άντληση των δεδομένων.

4.1.4 Άντληση των δεδομένων και επεξεργασία (Data mining).

Με την εγκατάσταση της εφαρμογής και την ταυτοποίηση του αριθμού τηλεφώνου sim η εφαρμογή ξεκινά τον συγχρονισμό της με το google account. Επίσης το σύνολο των εικόνων προφίλ αποθηκεύονται αυτόματα σε φάκελο στη συσκευή android. Εάν η επαφή βρίσκεται σε κάποια κοινή ομάδα εργασίας όπως φιλικές ή ομαδικές ομάδες χρηστών τότε θα επιστραφεί και το πραγματικό του όνομα. Πλέον είμαστε σε θέση να διαπιστώσουμε σε πρώτη φάση οπτικά ποιοι από τους εικονικούς αριθμούς που έχουμε εισαγάγει έχουν εγκατεστημένο το Viber. Όλα τα άτομα τα οποία έχουμε εισάγει φαίνονται με το εικονικό τους όνομα πλην των ατόμων που έχουν καταχωρήσει οι ίδιοι το ονοματεπώνυμό τους στην εφαρμογή. Επίσης φαίνεται η φωτογραφία προφίλ που έχουν εισάγει η οποία είναι διαθέσιμη για προβολή ενώ αναγράφεται επάνω της η τελευταία σύνδεση στην εφαρμογή του επιλεγόμενου ατόμου. Στην επόμενη φάση του πειράματος μέσω της εφαρμογής DB Browser for SQLite ανοίξαμε τη βάση δεδομένων του Viber η οποία βρίσκεται αποθηκευμένη στο σύστημά μας με όνομα viber.db. Στην εφαρμογή αυτή εκτελέσαμε ένα SQL script : "select * from Contact where ViberContact = 1 and order by Number" το οποίο μας επέτρεψε να ανακτήσουμε όλες τις επαφές οι οποίες έχουν εγκατεστημένο Viber (ViberContact = 1) καθώς και όσες επαφές έχουν αναρτήσει φωτογραφία προφίλ (DownloadID not null) (εικόνα 3).



(γράφημα 3, ανάκτηση δεδομένων μέσω του DB Browser for SQLite)

4.1.5 Ταυτοποίηση επαφών Viber με πραγματικές οντότητες

4.1.5.1 Ταυτοποίηση επαφών με χρήση διαδικτυακών βάσεων δεδομένων.

Για τη ταυτοποίηση των επαφών Viber με πραγματικές οντότητες υπάρχουν δύο δυνατές λύσεις. Η πρώτη λύση είναι να γίνει χρήση βάσεων δεδομένων που είναι αναρτημένες ήδη στο διαδίκτυο έτοιμες προς χρήση. Οι βάσεις αυτές προσφέρουν τη δυνατότητα ταυτοποίησης ατόμου με χρήση του τηλεφωνικού αριθμού. Συνήθως όμως προσφέρουν ελάχιστες επιτρεπόμενες φορές χρήσης σε ημερήσια βάση κι έπειτα κλειδώνουν. Στη παρούσα διπλωματική εργασία έγινε χρήση

των μηχανών αναζήτησης Sync.me [72], TrueCaller [73] και GreekPhones [80] με τη πρώτη να ζητάει οπτική ταυτοποίηση (Captcha) για να αποτρέπει προσπάθειες αυτοματοποιημένης αναζήτησης ενώ επιτρέπει 10 εκτελέσεις αναζήτησης σε ημερήσια βάση και έπειτα δεν επιτρέπει περαιτέρω αναζήτηση. Το TrueCaller επιτρέπει 5 αναζητήσεις και μετά απαιτεί επιβεβαίωση αναζήτησης μέσω οπτικής ταυτοποίησης (re-Capcha) επίσης για να αποτρέψει της αυτοματοποιημένες αναζητήσεις. Για να ξεπεραστεί το εμπόδιο του κλειδώματος έπειτα από 10 και 5 αναζητήσεις αντίστοιχα χρησιμοποιήθηκε ο φυλλομετρητής ανωνυμοποίησης Tor [74] του οποίου κάναμε χρήση της δυνατότητας δημιουργίας νέου κυκλώματος ανωνυμοποίησης (New Tor Circuit for this site) ξεπερνώντας το ημερήσιο όριο αναζητήσεων και επιβαρύνοντας το χρόνο αναζήτησης. Επίσης αν και δημιουργήθηκε το πρόγραμμα για αυτοματοποιημένη αναζήτηση (Html Parser) δεν μπόρεσε να ξεπεραστεί το εμπόδιο της οπτικής επιβεβαίωσης οπότε οι αναζητήσεις έγιναν με ημιαυτόματο τρόπο. Το GreekPhone από τη πλευρά του δεν διαθέτει μηχανισμό ασφαλείας από αυτοματοποιημένη αναζήτηση. Αντιθέτως προσφέρει το σύνολο της βάσης δεδομένων του έναντι αμοιβής από την οποία τα δεδομένα του εξάγονται σε μορφή excel οπότε υπάρχει η δυνατότητα συγκεντρωτικής αναζήτησης και η οποία περιέχει εκτός των κινητών τηλεφώνων, τη διεύθυνση καθώς και το επάγγελμα της επαφής. Αξίζει να αναφέρουμε ότι η μηχανή αναζήτησης sync.me συλλέγει τα δεδομένα τους μέσω της αντίστοιχης εφαρμογής της για φορητές συσκευές και η οποία μολονότι διαφημίζεται ως εφαρμογή αναγνώρισης κλήσεων και εμπλοκής ανεπιθύμητων κλήσεων μετά την εγκατάστασή της μεταφορτώνει το τηλεφωνικό κατάλογο της συσκευής στους εξυπηρετητές της εταιρείας (Heather Clancy, 2013) [75]. Επίσης αντλεί επίσης δεδομένα από τα κοινωνικά δίκτυα με τα οποία συνεργάζεται (Loie Favre, 2014)[76]. Το Truecaller από τη πλευρά του δηλώνει ότι αντλεί δεδομένα μόνο από τους εγγεγραμμένους του χρήστες και δεν κάνει χρήση του τηλεφωνικού καταλόγου της συσκευής που έχει εγκατασταθεί[77]. Για την ολοκλήρωση της έρευνάς του δείγματός μας μέσω των ανωτέρω μηχανών αναζήτησης χωρίς τη στατιστική ανάλυση απαιτήθηκαν 14 εργατοώρες.

4.1.5.2 Ταυτοποίηση επαφών με χρήση φωτογραφίας προφίλ.

Όπως αναφέρθηκε και στην εισαγωγή αυτού του κεφαλαίου οι φωτογραφίες χρηστών των επαφών μας είναι πλέον διαθέσιμες προς επεξεργασία καθώς είναι αποθηκευμένες τόσο στον υπολογιστή που χρησιμοποιήσαμε για την άντληση των δεδομένων όσο και στο εργαστηριακό κινητό που πραγματοποιούμε τις δοκιμές μας.

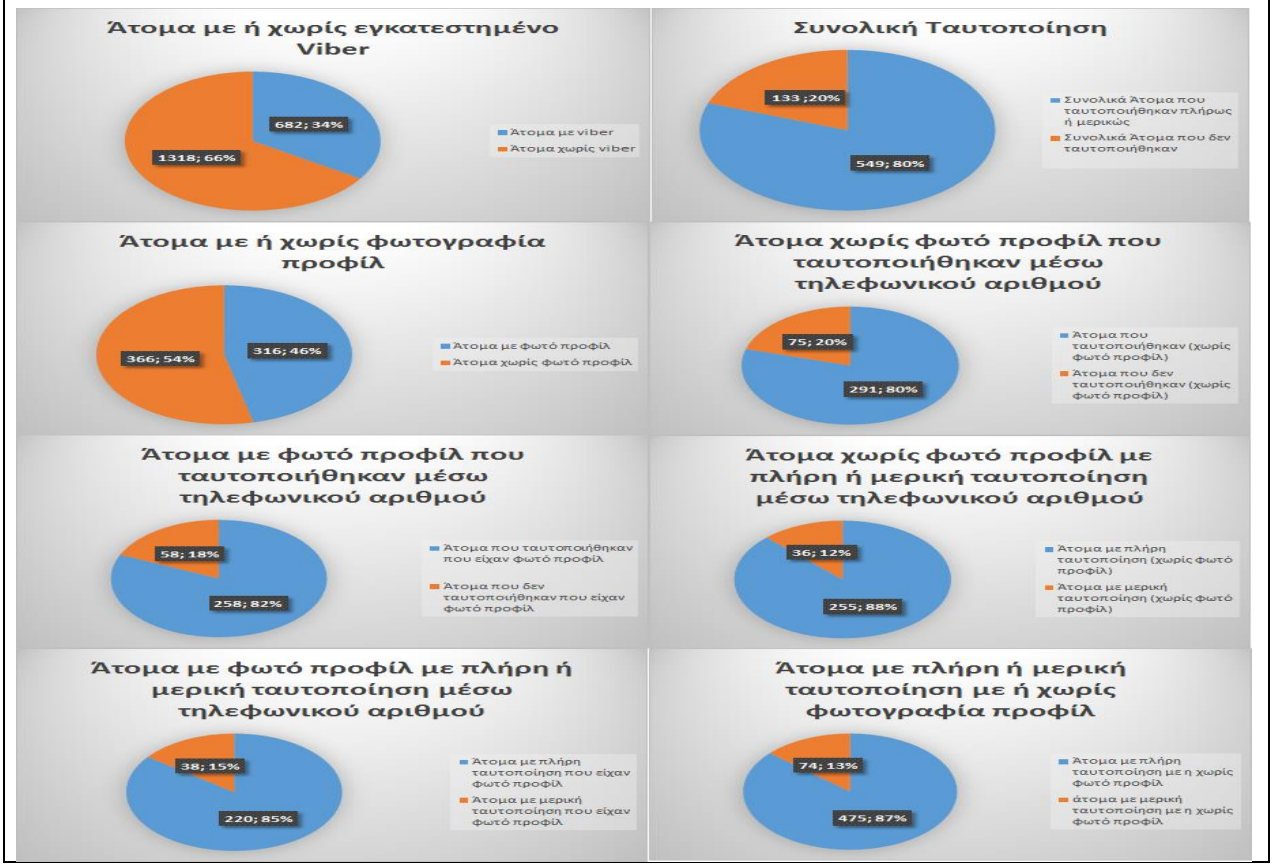
Σε επόμενο επίπεδο κάνοντας χρήση των φωτογραφιών αυτών είναι δυνατό να αναζητηθεί χειροκίνητα ή αυτοματοποιημένα μέσω της μηχανής αναζήτησης εικόνας του google (www.google.com/searchbyimage/upload ή πηγαίνοντας στο google.com εικόνες, ανέβασμα μίας εικόνας) μία από της εικόνες προφίλ. Η μηχανή αναζήτησης θα αναζητήσει παρόμοιες φωτογραφίες και θα επιστρέψει τα αποτελέσματα. Η δε αναγνώριση προσώπου της google χαρακτηρίζεται ικανοποιητική, καθώς επέστρεψε πλήθος αποτελεσμάτων. Αν δε κάποιος χρήστης του Viber χρησιμοποιεί την ίδια φωτογραφία προφίλ σε κοινωνικά δίκτυα ή ιστοσελίδες τότε η μηχανή αναζήτησης θα μας επιστρέψει με ποσοστό επιτυχίας που πλησιάζει το 100% τη σελίδα προφίλ του κοινωνικού δικτύου της επαφής μας καθώς και πλήθος άλλων πληροφοριών.

Για τη πραγματοποίηση της ταυτοποίησης με τη χρήση φωτογραφίας προφίλ κρίθηκε σημαντικό να δημιουργηθεί μία μικρή εφαρμογή σε java το οποίο μας διευκόλυνε στη διαχείριση των αναζητήσεων. Συγκεκριμένα δημιουργήθηκε ένας τοπικός ftp server και μεταφορτώθηκαν οι φωτογραφίες προφίλ σε αυτόν. Έπειτα η βάση SQLite που αναφέραμε προηγουμένως εισήχθη σε τοπική Βάση Δεδομένων (MySQL). Μέσω της java εφαρμογής μας δημιουργήσαμε τη δυνατότητα ατομικής ή πολλαπλής αναζήτησης στο google images. Η πιθανή ταυτοποίηση του προσώπου έγινε με οπτικό και χειροκίνητο τρόπο καθώς η Google το 2011 σταμάτησε την επίσημη υποστήριξη της αυτοματοποιημένης αναζήτησης ενώ από το 2016 δεν επιτρέπει να μεταφορτωθούν αποτελέσματα (Google, 2011) [78]. Αξίζει να διευκρινιστεί ότι η Google δημιούργησε νέα προγραμματιστική βιβλιοθήκη για τη δημιουργία προγραμμάτων αυτοματοποιημένης αναζήτησης, η οποία ονομάζεται Google Custom Search αλλά περιορίζει τις αναζητήσεις σε 100 την ημέρα μέσω μοναδικού αναγνωριστικού και έπειτα χρεώνει την κάθε αναζήτηση με βάση το πλήθος των αναζητήσεων [79].

4.1.6 Στατιστική Ανάλυση των Δεδομένων

Έπειτα από τη συσσώρευση των δεδομένων που ανακτήθηκαν προέκυψαν τα κατάλληλα και επαρκή στατιστικά δεδομένα προς επεξεργασία. Συγκεκριμένα από το σύνολο των 2000 επαφών προέκυψε ότι 682 επαφές (34%) έχουν εγκατεστημένη την εφαρμογή Viber εκ των οποίων οι 316 επαφές (46,3%) είχαν μεταφορτώσει φωτογραφία προφίλ. Από τις επαφές που είχαν φωτογραφία προφίλ ταυτοποιήθηκαν πλήρως ή μερικώς οι 258 επαφές (82%) ενώ από τις επαφές που δεν είχαν φωτογραφία προφίλ ταυτοποιήθηκαν πλήρως ή μερικώς 291 επαφές (80%). Συνολικά δηλαδή ταυτοποιήθηκαν πλήρως ή μερικώς 549 επαφές (80%). Συμπερασματικά ταυτοποιήθηκαν πλήρως και στις δύο κατηγορίες 475 άτομα δηλαδή το 70% των συνολικών ατόμων που βρέθηκαν να έχουν εγκατεστημένο το viber. Ως πλήρη ταυτοποίηση θεωρείται όταν η πλήρης ανάκτηση του ονοματεπώνυμου της επαφής ενώ ως μη πλήρη ταυτοποίηση η μερική ανάκτηση αυτού. Στο παρακάτω πίνακα οπτικοποιούνται τα γραφήματα σε μεγαλύτερη ανάλυση (γράφημα 4):

γράφημα 4 :



4.1.7 Εκτίμηση ενημερότητας

Μετά τη στατιστική ανάλυση το επόμενο βήμα είναι η εκτίμηση της ενημερότητας των ανωτέρω χρηστών Viber. Για την εκτίμηση αυτή επιλέξαμε 20 χρήστες οι οποίοι ήταν γνωστοί σε εμάς και οι αριθμοί τηλεφώνων τους ήταν αποθηκευμένοι στο κινητό του εργαστηρίου. Οι λόγοι που επιλέχθηκαν γνωστοί χρήστες ήταν πρώτον ώστε να έχουμε τη συγκατάθεσή τους για να κάνουμε χρήση των δεδομένων αυτών, δεύτερον για να μπορέσουμε να επαληθεύσουμε τα στοιχεία αυτά και τρίτον για λόγους χρονικής πρακτικότητας και παρακολούθησης. Ο σκοπός του πειράματος αυτού ήταν να συλλεχθούν όσο το δυνατόν περισσότερα δεδομένα για τα υποκείμενα του πειράματος καθώς και να καταγραφούν οι καθημερινές τους συνήθειες . Η παρακολούθησή τους κράτησε για 30 συνεχείς ημέρες. Κάθε μέρα και σε τρεις χρονικές περιόδους 08:00, 16:00, 22:00 αναζητούνταν δεδομένα σύνδεσης και πιθανή αλλαγή εικόνας προφίλ. Ενδεικτικά συμπληρωνόταν ο κάτωθι πίνακας ενώ στο τέλος κλήθηκαν να απαντήσουν σε ένα ερωτηματολόγιο 11 σύντομων ερωτήσεων με σκοπό να προκύψει η ενημερότητα των χρηστών σε σχέση με τη γνώση της πολιτικής ασφάλειας του Viber καθώς και τη γενικότερη επίγνωση χρήσης των προσωπικών τους δεδομένων. Οι ερωτήσεις που κλήθηκαν να απαντήσουν (παρατίθενται σε ελληνική μετάφραση) πλην των δημογραφικών ερωτήσεων ήταν οι εξής:

- Διαβάσατε τη πολιτική ασφάλειας της εφαρμογής Viber πριν την εγκαταστήσετε;
- Αν διαβάσατε τη πολιτική ασφάλειας θεωρείτε ότι τη κατανοήσατε;
- Γνωρίζετε ότι με την εγκατάσταση τα δεδομένα που έχετε δημοσιοποιήσει στη viber πλέον θεωρούνται δημόσια δεδομένα;

- Γνωρίζετε ότι με βάση τη πολιτική ασφάλειας, το Viber έχει το δικαίωμα να δημοσιοποιήσει τα δεδομένα σας σε τρίτους όπως το Facebook και το Twitter;
- Γνωρίζετε ότι το Viber μπορεί να συλλέξει δεδομένα μέσω της συνεργασίας της με άλλα κοινωνικά δίκτυα όπως το Facebook και το Twitter;
- Γνωρίζετε ότι μπορεί κάποιος άγνωστος σε εσάς να ανακαλύψει τη φωτογραφία προφίλ σας καθώς και άλλα προσωπικά δεδομένα όπως ονοματεπώνυμο και επάγγελμα;
- Γνωρίζετε ότι μπορούν άγνωστοι, εργοδότες ή γνωστοί να παρακολουθηθούν οι συνήθειές σας μέσω της εφαρμογής Viber όπως τι ώρα ανοίξατε τη φορητή σας συσκευή καθώς και εάν βρίσκεστε σε σύνδεση;
- Γνωρίζετε ότι είναι δυνατόν μέσω του Viber να γίνετε στόχος ανεπιθύμητων διαφημιστικών μηνυμάτων;
- Γνωρίζετε ότι είναι δυνατόν μέσω του Viber να γίνετε στόχος ηλεκτρονικού ψαρέματος;
- Γνωρίζετε ότι με χρήση διασυνδεδεμένων δεδομένων από πολλαπλά κοινωνικά δίκτυα όπως Viber, Twitter, Facebook δύναται να γίνετε στόχος ηλεκτρονικής και φυσικής παρακολούθησης;
- Μετά τα παραπάνω θα συστήνατε το Viber σε κάποιο φίλο/γνωστό;
- Θα συνεχίσετε να χρησιμοποιείτε την εφαρμογή Viber;

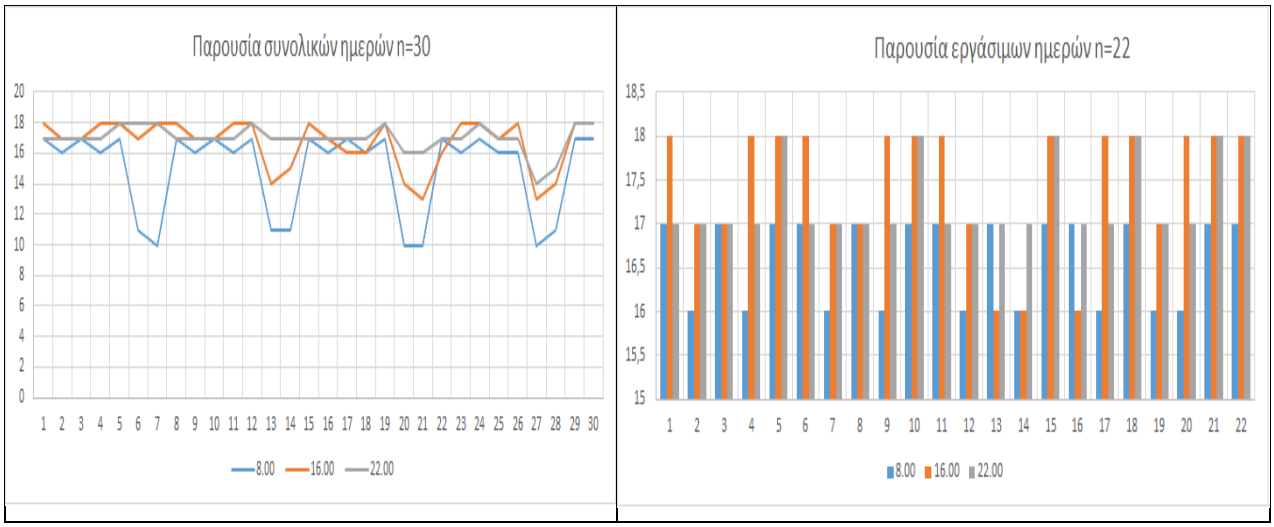
Οι ερωτήσεις δημογραφικού χαρακτήρα επιλέχτηκαν από το υπόδειγμα της ιστοσελίδας κατασκευής ερωτηματολογίων SurveyMonkey (surveymonkey.com). Για την εκτίμηση της ενημερότητας των χρηστών οι ερωτήσεις δημιουργήθηκαν με τη χρήση τριών μεθόδων. Με βάση την ανασκόπηση των Buchenscheit et al [4] όπου μελέτησαν παρόμοια εφαρμογή με το Viber και συγκεκριμένα την εφαρμογή Whats App. Με βάση την έρευνα Boksasp et al [56] που μελετήθηκε σε βάθος η ασφάλεια των φορητών συσκευών και των δικαιωμάτων ασφάλειας και τέλος από την μελέτη της πολιτικής ασφάλειας του Viber.

Υποκείμενο 1								
Μέρα 1			Μέρα 2			Μέρα 3		
	Ώρα σύνδεσης	Εικόνα προφίλ		Ώρα σύνδεσης	Εικόνα προφίλ		Ώρα σύνδεσης	Εικόνα προφίλ
8:00	Πριν 23’	ιδιωτικό	8:00	Πριν 11’	Ίδια	8:00	Πριν 14’	Ίδια
16:00	Σε σύνδεση	Ίδια	16:00	Σε σύνδεση	Ίδια	16:00	Σε σύνδεση	Ίδια
22:00	Σε σύνδεση	ίδια	22:00	Σε σύνδεση	ίδια	22:00	Σε σύνδεση	ίδια

4.1.7.1 Γενική εκτίμηση αποτελεσμάτων.

Από την ανάλυση του πίνακα παρακολούθησης προέκυψαν τα εξής στοιχεία. Όλα τα υποκείμενα πλην ενός δεν τροποποίησαν τη φωτογραφία προφίλ τους (95%). Αυτό θεωρείται θετικό αντίκτυπο από την άποψη της ασφάλειας καθώς άπαξ και δεν μπορούσε να ταυτοποιηθεί με ανάστροφη αναζήτηση εικόνας, οι υπόλοιπες αναζητήσεις θα έχουν το ίδιο αποτέλεσμα. Ως προς την ώρα σύνδεσης 8.00 14,97 (74,9%) άτομα είχαν σύνδεση ή ήταν σε σύνδεση έως και πριν 2 ώρες στο σύνολο των 30 ημερών και 16,59 (82,9%) κατά τις εργάσιμες ημέρες . Από αυτό το δεδομένο

μπορούμε να κρίνουμε ότι τουλάχιστον το 79,4% των υποκειμένων έχουν ήδη συνδεθεί στο διαδίκτυο είτε από τον οικείο χώρο είτε από τον εργασιακό. Λόγω όμως της αύξησης κατά 10,8% τις εργάσιμες ημέρες συμπεραίνουμε ότι περισσότεροι προτιμούν να συνδέονται από τον εργασιακό τους χώρο. Ό,τι αφορά στη χρονική περίοδο 16.00 παρατηρήθηκε μία αύξηση των συνδεδεμένων ατόμων ύψους 17,45 άτομα τις εργάσιμες ημέρες και στο 16,73 στο σύνολο των ημερών ενώ ανάλογα ποσοστά 17,27 κατά τις εργάσιμες ημέρες και 17,03 στο σύνολο των ημερών εμφάνισε και ο χρονικός ορίζοντας 22.00. Από αυτό μπορούμε να συμπεράνουμε ότι ο αριθμός συνδεδεμένων ατόμων κανονικοποιείται κατά το χρονικό διάστημα 16.00 και 22.00 στα 17,12 άτομα σε σύνδεση και δεν μπορεί να δειχθεί με σαφήνεια εάν τα άτομα βρίσκονται στον εργασιακό τους χώρο ή στον οικείο χώρο ενώ προκύπτει ότι τα άτομα διαθέτουν ευρυζωνική σύνδεση και στον οικείο τους χώρο λόγω της στατιστικά ασήμαντης διαφοράς 1.5 τις εργάσιμες ημέρες κατά το χρονικό διάστημα 22.00. Από τη πλευρά της ασφάλειας φαίνεται ότι το άτομο είναι περισσότερο ευάλωτο σε επιθέσεις ανεπιθύμητων διαφημιστικών μηνυμάτων (spam messages) καθώς και ανεπιθύμητων τηλεφωνικών διαφημιστικών κλήσεων από τις 16.00 και μετά με ελαφρά υψηλότερη πιθανότητα τις εργάσιμες ημέρες κατά τις μεσημεριανές βραδινές ώρες. Οι παρουσίες βρίσκονται σε μεγαλύτερη ανάλυση στα κάτωθι γραφήματα (γράφημα 5) :



(γράφημα 5)

Από την ανάλυση των ερωτηματολογίων προέκυψε ότι το σύνολο των υποκειμένων έχουν τουλάχιστον μεταλυκειακή εκπαίδευση με το 80% να έχει τουλάχιστον πτυχίο τριτοβάθμιας εκπαίδευσης ενώ το 90% διαθέτει λογαριασμό σε κάποιο κοινωνικό δίκτυο με τη μεγαλύτερη πλειοψηφία να διαθέτει άνω των 100 επαφών σε αυτά και από τους οποίους το 30% των υποκειμένων γνώριζαν λιγότερο από τις μισές επαφές. Το 75% δήλωσε ότι σπάνια ή πολύ σπάνια αλλάζουν φωτογραφία προφίλ ενώ το 50% δήλωσε ότι αντιμετωπίζει από μέτρια δυσκολία έως μεγάλη δυσκολία στο να αλλάξει τις ρυθμίσεις απορρήτου. Μόλις το 5% απάντησε ότι θα προτιμούσε ως κοινωνικό δίκτυο το Viber ως μοναδικό κοινωνικό δίκτυο ενώ το 50% θα προτιμούσε το Facebook. Το 40% απάντησε ότι δαπανά περίπου το μισό του χρόνο στο να παρακολουθεί τι δημοσιεύουν οι επαφές του ενώ δήλωσε ότι το 65% του χρόνου τον δαπανά για να δημοσιεύσει δικές του πληροφορίες. Σε ό,τι αφορά το Viber δήλωσε ότι το 70% δεν διάβασε τη πολιτική ασφάλειας του viber πριν το εγκαταστήσει ενώ το 20% απάντησε ότι δεν θυμάται εάν τη διάβασε και μόλις το 10% ότι τη διάβασε. Το 85% των υποκειμένων δήλωσαν ότι δεν είναι σίγουροι εάν θα κατανοούσαν τη πολιτική ασφάλειας. Το 90% δήλωσε ότι δεν γνώριζε ότι τα δεδομένα που

δημοσιεύει στο Viber θεωρούνται ως δημόσια δεδομένα ενώ το ίδιο ποσοστό δεν γνώριζε ή δεν ήταν σίγουρο ότι σύμφωνα με τη πολιτική ιδιωτικότητας του viber αποκτάται από αυτή το δικαίωμα να μοιραστεί πληροφορίες με άλλα κοινωνικά δίκτυα όπως το Facebook ή το Twitter. Το 85% επίσης δεν γνώριζε ότι το Viber σύμφωνα με τη πολιτική του ασφάλειας ότι μπορεί να συλλέγει πληροφορίες γι' αυτούς από άλλα κοινωνικά δίκτυα. Σε επίπεδο παρακολούθησης το 65% δεν γνώριζε ή δεν ήξερε ότι μέσω της φωτογραφίας προφίλ είναι δυνατόν να ταυτοποιηθεί το πλήρες όνομά του ή/και το επάγγελμά του. Το 75% δήλωσε ότι δεν γνώριζε ή δεν ήταν σίγουρο ότι δύναται να παρακολουθούνται οι συνήθειές του μέσω του Viber όπως εάν το άτομο βρίσκεται σε σύνδεση ή εάν έχει ανοίξει το κινητό του τηλέφωνο. Το 60% δήλωσε ότι δεν γνώριζε ότι μέσω του Viber είναι δυνατό να γίνει στόχος ανεπιθύμητων μηνυμάτων (spam) ή υποψήφιο θύμα ηλεκτρονικού ψαρέματος. Το 60% δεν ανέμενε ότι με τη χρήση διασύνδεσης δεδομένων από πολλαπλά κοινωνικά δίκτυα είναι δυνατό να γίνει στόχος φυσικής και ηλεκτρονικής παρακολούθησης. Παρόλα τα παραπάνω το 35% θα σύστηνε για εγκατάσταση το Viber σε κάποιο φίλο ενώ το 60% δήλωσε ότι θα συνεχίσει να χρησιμοποιεί το Viber.

4.1.7.2 Συμπεράσματα στατιστικών αποτελεσμάτων.

Από την ανάλυση των στατιστικών αποτελεσμάτων γίνεται εμφανές ότι μολονότι τα υποκείμενα είχαν υψηλό μορφωτικό επίπεδο δεν μπήκαν κατά τη πλειοψηφία τους στη διαδικασία ανάγνωσης της πολιτικής ασφάλειας του Viber ενώ η συντριπτική πλειοψηφία δήλωσε ότι δεν είναι σίγουροι ότι θα τη καταλάβαιναν ακόμη και εάν τη διάβαζαν. Από αυτό μπορούμε να κρίνουμε ότι το υψηλό μορφωτικό επίπεδο δεν παίζει σαφή ρόλο στη κατανόηση μίας πολιτικής ασφάλειας στη τρέχουσα μορφή της και ταυτοχρόνως μη κατανόησης των δυνητικών κινδύνων που υπάρχουν από τη τυφλή αποδοχή της. Επίσης με το γεγονός ότι σχεδόν το σύνολο των υποκειμένων δεν γνώριζε ότι τα δεδομένα τους θεωρούνται δημόσια μας δείχνει βασική έλλειψη ενημερότητας και σε συνδυασμό με τη σχετικά μέτρια έως μεγάλη δυσκολία που έχουν στο να αλλάξουν τις ρυθμίσεις ασφάλειας και ενώ το σύνολο των υποκειμένων διαθέτει τουλάχιστον ένα λογαριασμό σε κάποιο κοινωνικό δίκτυο μας δείχνει ότι δύσκολα θα μπορούσαν να προφυλάξουν τα προσωπικά τους δεδομένα ακόμη και εάν το ήθελαν. Ένα άλλο σημείο το οποίο καταδεικνύει το επίπεδο ενημερότητάς τους καθώς και των κινδύνων που εγκυμονεί η έλλειψη αυτής είναι το γεγονός ότι ενώ τα ¾ των συμμετεχόντων δεν γνώριζαν ότι είναι δυνατή η παρακολούθησή τους μέσω του κοινωνικών δικτύων όπως το Viber και είναι υποψήφιοι στόχοι τόσο για ανεπιθύμητα μηνύματα ή κλήσεις όσο και ως στόχος φυσικής παρακολούθησης δήλωσαν ότι κατά πάσα πιθανότητα θα συνεχίσουν να χρησιμοποιούν το Viber.

Από τα παραπάνω γίνεται σαφές ότι πρέπει να υπάρξει ένας εναλλακτικός τρόπος αποτύπωσης και παρουσίασης της πολιτικής ασφάλειας και ενίσχυσης της ενημερότητάς του ο οποίος συγκεντρωτικά θα αποτυπώνει με αποδοτικό τρόπο σε τι δεδομένα δίνει ο χρήστης το δικαίωμα χρήσης τους καθώς τους πιθανούς κινδύνους με τους οποίους πιθανώς να έρθει αντιμέτωπος. Τα παραπάνω πιστεύουμε ότι γίνεται να υλοποιηθούν με τη δημιουργία της εφαρμογής appWare όπως αυτή παρουσιάζεται στο 5 κεφάλαιο.

4.1.8 Παρακολούθηση σε ευρεία κλίμακα.

Εύλογα μετά τα παραπάνω μας δημιουργήθηκε η απορία εάν θα μπορούσαν τα χαρακτηριστικά που προσφέρουν εφαρμογές σαν το Viber να χρησιμοποιηθούν για τη παρακολούθηση χρηστών σε μεγάλη κλίμακα. Για να επιβεβαιώσουμε εργαστηριακά το ανωτέρω σενάριο δημιουργήσαμε ένα αρχείο χωρισμένο με κόμματα που περιλαμβάνει τους αριθμούς κινητών τηλεφώνων όλων των δυνητικά χρηστών στην Ελλάδα από 6900000000 έως 6999999999. Για να δημιουργηθεί αυτό το data set απαιτήθηκαν 7 ώρες συνεχούς χρήσης προσωπικού υπολογιστή (Intel i7 6700, 16GB RAM, 250 GB SSD SATA 3) δημιουργώντας ένα αρχείο μεγέθους 1 GB. Τα δεδομένα σε συμπιεσμένη μορφή καταλαμβάνουν λίγο περισσότερο από 10 MB. Για τη διαχείριση τέτοιας ποσότητας δεδομένων θα απαιτείτο μία βάση δεδομένων όπως η MySQL ή η SQLite που χρησιμοποιεί το Viber η οποία αν και παρέχεται δωρεάν δέχεται ως μέγιστο σύνολο 64 GB δεδομένων. Η διαδικασία μέσω της χρήσης του google account δεν χαρακτηρίζεται ως εφικτή λύση καθώς θέτει ως όριο τις 25.000 εγγραφές. Αυτό θα είχε ως αποτέλεσμα να χρειαστούμε 4.000 λογαριασμούς google για τις 100.000.000 εγγραφές. Αντιθέτως θα μπορούσε να γίνει η εισαγωγή των δεδομένων απευθείας στη βάση του Viber for Pc μέσω ενός sql script που μπορούμε να δημιουργήσουμε μέσω του ίδιου python script που χρησιμοποιήσαμε στην ενότητα 3.4.2. Για να τεκμηριώσουμε στατιστικά τα δεδομένα μας με ένα εφικτό υποσύνολο αυτών δημιουργήσαμε ένα αρχείο έτοιμο για εισαγωγή στη βάση με 100.000 εγγραφές. Για τη δημιουργία του αρχείου απαιτήθηκαν λιγότερο από 20 λεπτά αποκλειστικής χρήσης του ανωτέρω προσωπικού ηλεκτρονικού υπολογιστή δημιουργώντας ένα ασυμπίεστο αρχείο μεγέθους 8 MB. Οι εγγραφές εισήχθησαν στη βάση δεδομένων του Viber χωρίς προβλήματα και μπορούσαν να τεθούν άμεσα σε επεξεργασία. Για τη δε αυτοματοποίηση της ταυτοποίησης απαιτείται η αγορά κάποια από τις παραπάνω βάσεις. Για να υπολογίσουμε το χρονικό ορίζοντα της επεξεργασίας χρησιμοποιήσαμε το ταυτοποιημένο υποσύνολο που προέκυψε στην ενότητα 3.4.4 και το πολλαπλασιάσαμε μέχρι να πλησιάσουν τις 100.000 εγγραφές. Η αυτοματοποιημένη ολοκλήρωση της επεξεργασίας σε περίπου 400 λεπτά αποκλειστικής χρήσης του Η/Υ. Συνεπώς με βάση τα παραπάνω κρίνουμε ότι θα ήταν εφικτή η δυνατότητα αυτοματοποιημένης συλλογής δεδομένων και παρακολούθησης σε ευρεία κλίμακα.

4.2 Σύνοψη – Συμπεράσματα

Με σκοπό την απόδειξη της απειλής των συνδυαζόμενων δεδομένων καθώς και το ύψος της ενημερότητας των χρηστών, στο παρόν κεφάλαιο δόθηκε ένα εκτενές παράδειγμα χρησιμοποιώντας τη δημοφιλή εφαρμογή κοινωνικής δικτύωσης Viber. Με τη προσομοίωσή του όπως εκτενώς παρουσιάστηκε συλλέχτηκε πλήθος δεδομένων από ένα δείγμα 682 ατόμων με σκοπό τη στατιστική τους ανάλυση. Μέσω της μεθοδολογίας μας και της επεξεργασίας αυτών των δεδομένων έγινε δυνατή η πλήρη ταυτοποίηση 475 ατόμων (δηλαδή το 70%) διασυνδέοντας το τηλεφωνικό αριθμό με πραγματική οντότητα ανακαλύπτοντας σε πολλές περιπτώσεις, εκτός του ονοματεπωνύμου της οντότητας, τη διεύθυνση κατοικίας της και το επάγγελμά της. Πλέον τα άτομα αυτά ήταν επιρρεπή σε παρακολούθηση των συνηθειών τους μέσω ελέγχου της κατάστασης σύνδεσής τους στο Viber ενώ είναι επίσης εν δυνάμει στόχος ανεπιθύμητων κλήσεων, ηλεκτρονικών μηνυμάτων ή στόχος ηλεκτρονικού ψαρέματος.

Η εκτίμηση της ενημερότητας 20 εκ των εν λόγω χρηστών πραγματοποιήθηκε με τη συμπλήρωση ερωτηματολογίου όπου διαφάνηκε ότι το υψηλό επίπεδο μόρφωσης που είχαν όλα τα υποκείμενα δεν τους προέτρεψε να διαβάσουν τη πολιτική ασφάλειας του Viber ενώ η συντριπτική πλειοψηφία δήλωσε ότι δεν είναι σε θέση να εκτιμήσει εάν θα τη καταλάβαινε. Λόγω της μη ανάγνωσης της πολιτικής ασφάλειας τα υποκείμενα δεν ήταν σε θέση να γνωρίζουν ότι όχι μόνο τα προσωπικά τους δεδομένα ήταν αντικείμενο συλλογής και επεξεργασίας αλλά και διανομής προς τρίτους. Παρόλη την ανησυχία για τα δεδομένα τους και τα οποία δεν γνώριζαν ότι πλέον θεωρούνται δημόσια δεδομένα, η πλειοψηφία των υποκειμένων δήλωσε ότι θα εξακολουθεί να χρησιμοποιεί το Viber μολονότι τους έγινε γνωστό ότι είναι υποψήφιοι στόχοι ανεπιθύμητων κλήσεων και ηλεκτρονικών μηνυμάτων ή/και ηλεκτρονικού ψαρέματος. Από τα παραπάνω συμπεράναμε ότι θα πρέπει να δημιουργηθεί ένας εναλλακτικός τρόπος αποτύπωσης και παρουσίασης της πολιτικής ασφάλειας και ενίσχυσης της ενημερότητάς των χρηστών ο οποίος συγκεντρωτικά θα αποτυπώνει με αποδοτικό τρόπο σε τι δεδομένα δίνει ο χρήστης το δικαίωμα χρήσης τους καθώς τους πιθανούς κινδύνους με τους οποίους πιθανώς να έρθει αντιμέτωπος.

Επίσης εξετάστηκε κατά πόσο θα ήταν δυνατό η μεθοδολογία μας θα μπορούσε να χρησιμοποιηθεί σε μία ευρεία κλίμακα. Τα αποτελέσματα των εργαστηριακών μας πειραμάτων έδειξαν ότι για τη δημιουργία των κατάλληλων δεδομένων προς επεξεργασία για 100.000.000 εγγραφές θα απαιτούνταν μόλις 7 ώρες χρήσης ισχυρού οικιακής χρήσης Η/Υ. Για τη δε αυτοματοποιημένη ταυτοποίηση του 1% του παραπάνω δείγματος θα απαιτούνταν 400 λεπτά αποκλειστικής χρήσης του Η/Υ. Αυτό συνεπάγεται ότι με μία μέτρια σε μέγεθος βιομηχανική υποδομή η παρακολούθηση συνηθειών σε ευρεία κλίμακα θα ήταν ένα άκρως εφικτό σενάριο.

5

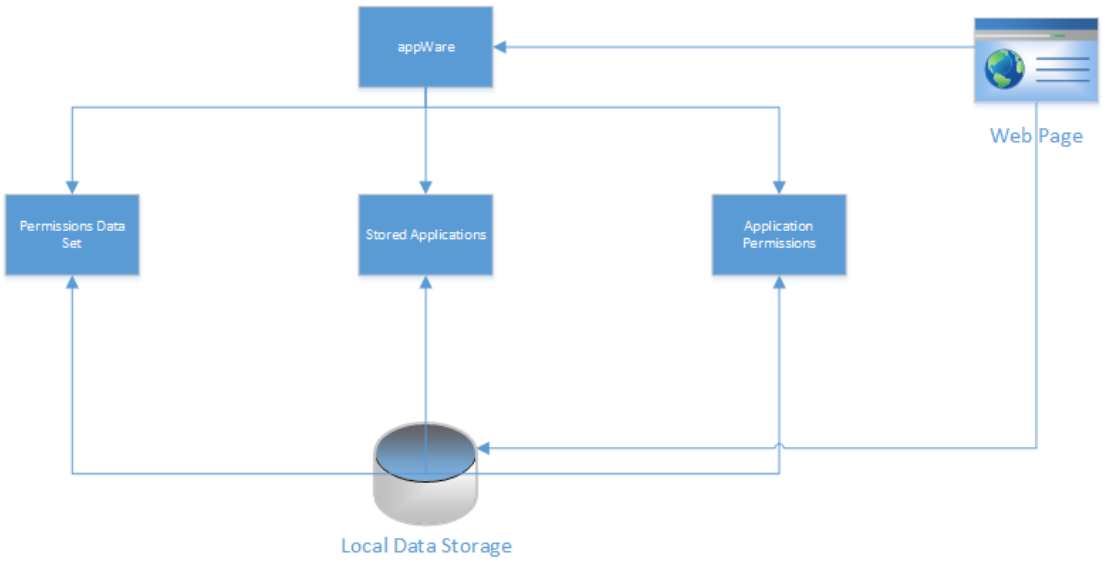
appWare

5.1 Εισαγωγή στο appWare

Στο πλαίσιο της εκπόνησης της διπλωματικής και για τη βελτίωση της ενημερότητας του απλού αλλά και προχωρημένου χρήστη εφαρμογών για κινητά τηλέφωνα και συσκευές όπως ταμπλέτες έγινε αντιληπτό ότι σκόπιμη είναι η ανάπτυξη της εφαρμογής με προσωρινό όνομα appWare. Ο σκοπός της εφαρμογής αυτής είναι όχι μόνο να ενημερώσει το χρήστη κατάλληλα και να του οπτικοποιήσει την πολιτική ασφάλειας της εκάστοτε εφαρμογής αλλά και να του γνωστοποιήσει το κίνδυνο που ενδεχομένως να διατρέξει από τη διασύνδεση των πληροφοριών που αποκτά η εφαρμογή. Η εφαρμογή αυτή έχει ως σκοπό να αναδείξει με αποσυγκεντρωτικό τρόπο το σύνολο των κινδύνων που εγκυμονεί αυτή τόσο μεμονωμένα όσο και συγκεντρωτικά. Για την αρχική της έκδοση (Version 1.0) έγινε χρήση του δημοφιλέστερου ιστότοπου μεταφόρτωσης εφαρμογών για κινητές συσκευές Google Play (play.google.com) . Η αρχική αυτή έκδοση γράφτηκε στη γλώσσα προγραμματισμού Java 8 με jdk 1.8 ενώ για την αποθήκευση και την ανάκτηση δεδομένων χρησιμοποιήθηκε η γλώσσα Βάσεων Δεδομένων MySql. Τα παραπάνω εργαλεία επιλέχθηκαν λόγω του γεγονότος ότι είναι ανοικτού κώδικα και ελεύθερης χρήσης. Όπως γίνεται αντιληπτό σε αυτή τη πρώιμη φάση, η εφαρμογή διατίθεται σε έκδοση πελάτη-εξυπηρετητή (client server) με πλήρεις τις δυνατότητες λειτουργίας εκτός δικτύου, και με προοπτική να ενσωματωθεί αυτούσια σε διαδραστική ιστοσελίδα. Στην αρχική έκδοση του appWare έχουν καταχωρηθεί και αντιστοιχιστεί με δικαιώματα οι 18 δημοφιλέστερες εφαρμογές για το 2015 σύμφωνα με το Pew Research Center (2015)[96]. Σε αυτό το σημείο, αξίζει να μνημονεύσουμε ότι 3 από τις 18 αυτές εφαρμογές βρίσκονται προεγκατεστημένες σε κάθε κινητό android καθώς είναι εφαρμογές του πάροχου του λογισμικού. Επίσης ο πάροχος δεν επιτρέπει για κανένα λόγο την απεγκατάστασή τους. Ακόμη και ένας προηγμένος χρήστης δεν έχει τη δυνατότητα να αφαίρεσης αυτών των εφαρμογών. Ο μόνος τρόπος είναι η εκρίζωση του λειτουργικού συστήματος android (rooting) και εγκατάστασης μίας τροποποιημένης έκδοσης του ίδιου λειτουργικού από τρίτους. Η παραπάνω ενέργεια εκτός από δύσκολη για το μέσο χρήστη δημιουργεί και πιθανό πρόβλημα στη χρήση εγγύησης της συσκευής. Με βάση τα παραπάνω ο χρήστης με την αγορά μίας πρόσφατης κινητής

συσκευής με λογισμικό android βρίσκεται αμελλητί εκτεθειμένος στις απειλές διαρροής πληροφοριών όπως αυτές περιγράφονται από το λογισμικό μας.

Για τη δημιουργία της εφαρμογής χρειάστηκε να δημιουργηθεί ένα σύνολο δεδομένων (data set) το οποίο περιλαμβάνει όλες τις πολιτικές ασφάλειας που μπορεί να ενσωματώσει μία εφαρμογή δηλαδή σε ό,τι δυνητικά θα μπορούσε να έχει πρόσβαση σε σχέση με τη συσκευή και το λογισμικό αυτής όπως τηλεφωνικός κατάλογος, χρήση δεδομένων, τηλεφωνικό δίκτυο κ.α. Η αφαιρετική σχεδίαση της εφαρμογής φαίνεται στο παρακάτω σχήμα (γράφημα 6) :



(γράφημα 6)

Για τη μεταφόρτωση της εφαρμογής πελάτη-εξυπηρετητή ο χρήστης εισέρχεται στην ιστοσελίδα όπου μπορεί να κατεβάσει τη τελευταία έκδοση της εφαρμογής, την τελευταία ενημέρωση των δεδομένων καθώς και τις οδηγίες εγκατάστασης. Για τη χρήση της εφαρμογής είναι απαιτητό να υπάρχουν ήδη εγκατεστημένα έκδοση java 8 ή νεότερη και MySQL έκδοση 5 ή νεότερη. Η διάθεση των παραπάνω εργαλείων είναι δωρεάν από τις επίσημες ιστοσελίδες τους.

5.2 Η δομή του appWare

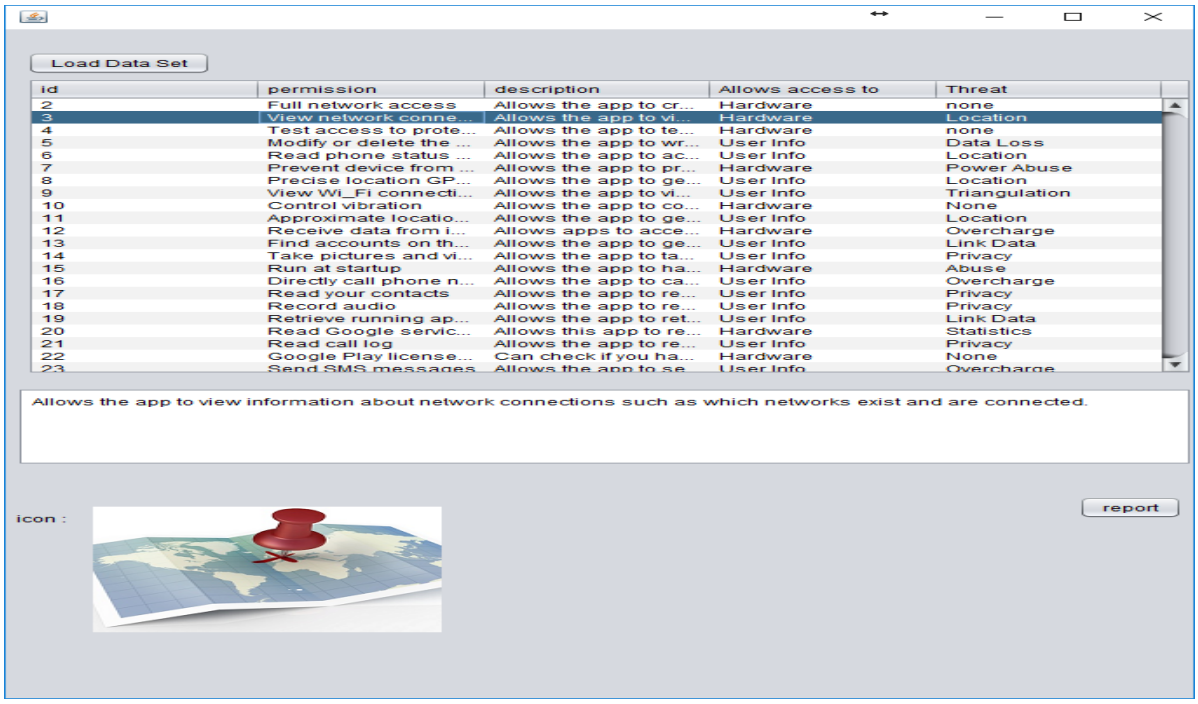
Η εφαρμογή μπορεί να χωριστεί με προγραμματιστικούς όρους σε τέσσερις διακριτές κλάσεις ή τέσσερις διακριτές καρτέλες με απλούστερους όρους. Οι τέσσερις αυτές κλάσεις ενσωματώνονται σε μία μητρική κλάση που θα θεωρείται το μενού της εφαρμογής και θα επιτρέπει τη πλήρη διαχείριση. Στο μοντέλο που θα αναδειχτεί παρακάτω, θα περιγράψει τόσο από τη πλευρά του απλού χρήστη όσο και από τη πλευρά της ομάδας διαχείρισης του appWare. Στην αρχική έκδοση του appWare έχουν καταχωρηθεί και αντιστοιχιστεί με δικαιώματα οι 18 δημοφιλέστερες εφαρμογές για το 2015 σύμφωνα με το Pew Research Center (2015)[96].

5.2.1 Η κλάση Dataset

Στη κλάση αυτή μπορούμε να περιηγηθούμε στο σύνολο των επιτρεπτών δικαιωμάτων όπως τα αναφέρει το Google Play καθώς και μία απλοποιημένη περιγραφή του κάθε δικαιώματος και την ενδεχόμενη δυνητική απειλή εάν υπάρχει όπως την περιγράφηκε από το Pew Research Center (2015)[96] καθώς και τη συγκεντρωτική απειλή του εν λόγω δικαιώματος. Συγκεκριμένα περιλαμβάνει τέσσερις λειτουργικές κολόνες οι οποίες είναι οι εξής: Δικαίωμα (permission), περιγραφή (description), πρόσβαση σε (Allows access to) και απειλή οι οποίες αναλύονται ως εξής:

1) Δικαίωμα (permission) : Το επίσημο όνομα του δικαιώματος σύμφωνα με το Google Play όπως αυτό αναφέρεται στον επίσημο ιστότοπο της εκάστοτε εφαρμογής στην καρτέλα δικαιώματα.
2) Περιγραφή (description) : Περιγράφει σε απλή και κατανοητή γλώσσα το εν λόγω δικαίωμα όπως το περιγράφηκε Pew Research Center (2015)[96] καθώς και την δυνητική απειλή εάν αυτή υπάρχει.
3) Πρόσβαση σε (Allows access to) : Περιγράφεται ο πόρος στον οποίο δίνει πρόσβαση το εκάστοτε δικαίωμα όπως το υλικό (hardware), λογισμικό (software) ή της πληροφορίες χρήστη (user info).
4) Απειλή (Threat) : Περιγράφεται συγκεντρωτικά η απειλή που ενδεχομένως να αντιμετωπίσει ο χρήστης δίνοντας πρόσβαση σε αυτό το δικαίωμα. Κάποιες από τις απειλές είναι οι εύρεση θέσης του χρήστη (Location), η αποκάλυψη προσωπικών δεομένων (Privacy), η ενόχληση (Abuse), η διασύνδεση δεδομένων (Link Data) και η υπερχρέωση (Overcharge).

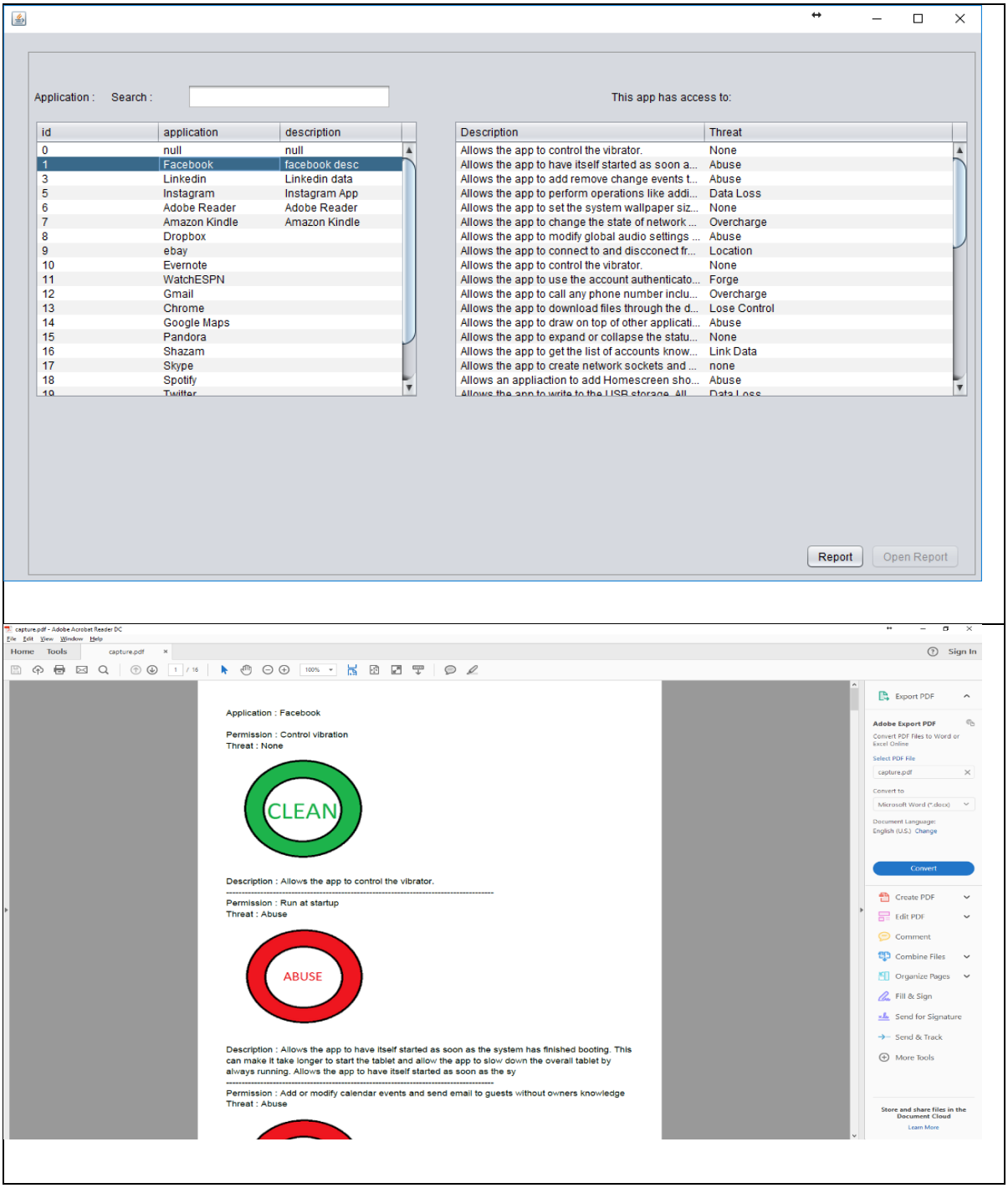
Ο χρήστης επιλέγοντας ένα από αυτά τα δικαιώματα μπορεί να δει περισσότερο αναλυτικά σε μεγαλύτερο πλαίσιο κειμένου τη περιγραφή του εν λόγω δικαιώματος. Επίσης του οπτικοποιείται η απειλή εμφανίζοντας μία εικόνα αναλόγως της απειλής. Επίσης με την επιλογή «αναφορά» (report) έχει τη δυνατότητα να δημιουργήσει και να ανακτήσει μία αναφορά σε ηλεκτρονικό αρχείο τύπου pdf η οποία περιγράφει όλα τα παραπάνω. Μία επισκόπηση των παραπάνω φαίνεται στη εικόνα 7 :



(γράφημα 7 : απόσπασμα εικόνας από την εφαρμογή appWare version 1.0)

5.2.2 Η κλάση appData

Η κλάση αυτή χαρακτηρίζεται ως η κεντρικότερη του appWare. Από αυτή τη κλάση ο χρήστης έχει τη δυνατότητα να αναζητήσει τις εφαρμογές που έχουν αντιστοιχιστεί με δικαιώματα και υπάρχουν στη βάση δεδομένων μας. Ο χρήστης πληκτρολογώντας κάποια από τα γράμματα της εφαρμογής που θέλει να αναζητήσει τα δικαιώματα της, της ανακτά με δυναμικό τρόπο στον παρακείμενο πίνακα. Επιλέγοντας την εφαρμογή που επιθυμεί ανακτάται το σύνολο των δικαιωμάτων που έχουν καταχωρηθεί γι' αυτή την εφαρμογή. Επιλέγοντας «αναφορά» (report) και «άνοιγμα αναφοράς» (Open Report) δημιουργείται όπως και στη κλάση Dataset ηλεκτρονικό αρχείο τύπου pdf μόνο που αυτή τη φορά μεταφορτώνει στο αρχείο την πολιτική ασφάλειας όπως αυτή μεταφράζεται από τα δικαιώματα που αποκτά η εφαρμογή. Συγκεκριμένα μεταφορτώνει το τίτλο της εφαρμογής, το σύνολο των συγκεντρωτικών απειλών ανά δικαίωμα με απλό και κατανοητό τρόπο, το σύνολο των περιγραφών των δικαιωμάτων ανά δικαίωμα καθώς και την αντιπροσωπευτική εικόνα του δικαιώματος. Παρακάτω παρατίθεται αποσπάσματα από την κλάση appData καθώς και την αναφορά:

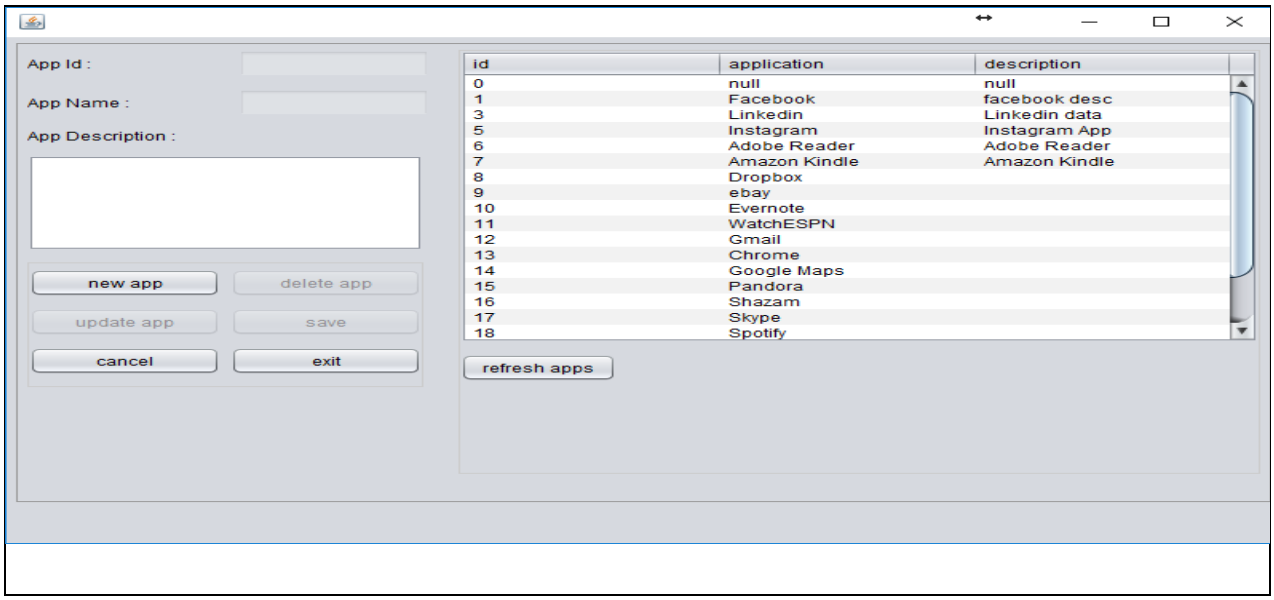


(γράφημα 8, 9: αποσπάσματα από τη κλάση appData της εφαρμογής appWare Version 1.0)

5.2.3 Η κλάση appHandling

Από τη κλάση αυτή υπάρχει η δυνατότητα καταγραφής μίας εφαρμογής η οποία δεν υπάρχει στη βάση δεδομένων μας καθώς και προβολής όλων των εφαρμογών που είναι καταχωρημένα σε αυτή ενώ δίνεται και η δυνατότητα τροποποίησης ή διαγραφής μίας εφαρμογής. Η τελευταία δυνατότητα θα είναι δυνατή μόνο στην ομάδα διαχείρισης του appWare. Όπως αναφέραμε και στην εισαγωγή αρχικά υπάρχουν οι 18 δημοφιλέστερες εφαρμογές για το 2015. Η ομάδα διαχείρισης από

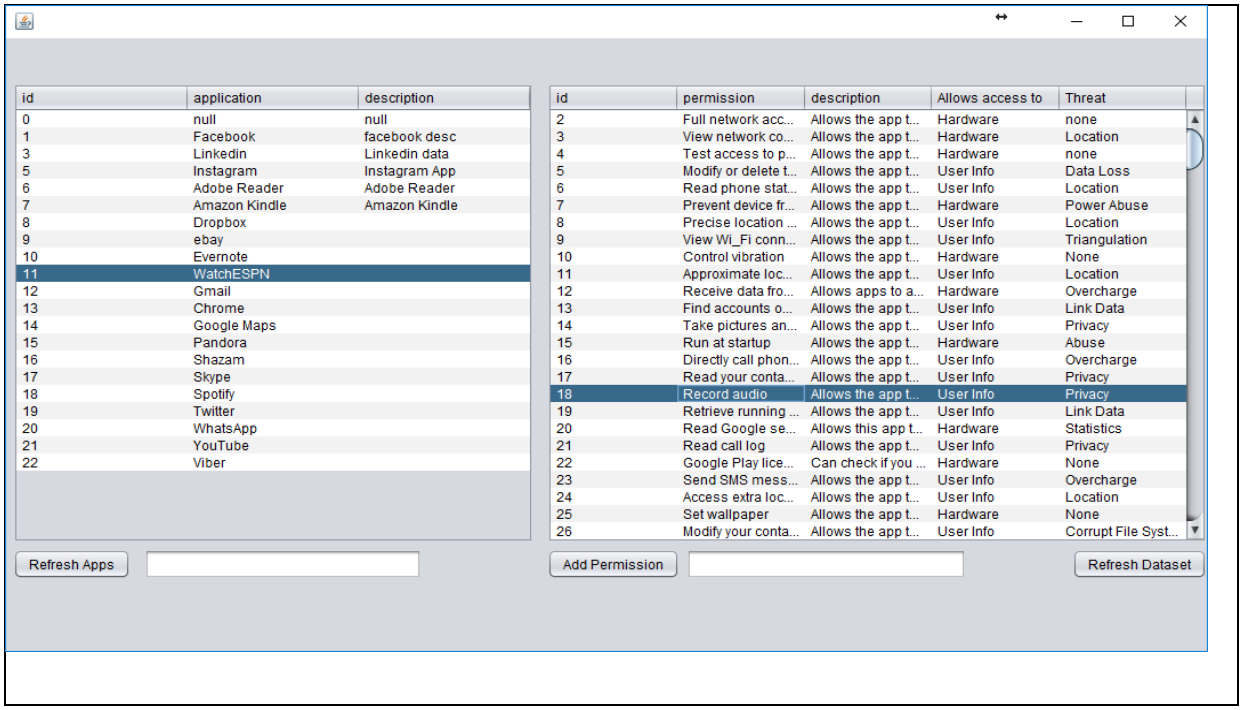
αυτή τη καρτέλα μπορεί να καταγράφει νέες εφαρμογές απευθείας στη βάση αναγράφοντας το όνομα της εφαρμογής και τη περιγραφή της. Από τη πλευρά του χρήστη, μπορεί και ο ίδιος να εισάγει νέες εφαρμογές. Για να του δοθεί η δυνατότητα να εγγράψει νέα εφαρμογή θα πρέπει να έχει μεταφορτώσει τη τελευταία έκδοση της εφαρμογής από τα εργαλεία (tools) της εφαρμογής appWare. Μόλις εγγράψει τη νέα εφαρμογή, αυτή καταγράφεται τοπικά σε προσωρινό πίνακα της βάσης δεδομένων και μόλις αντιστοιχιστεί με τα σχετικά δικαιώματα αποστέλλεται για τεκμηρίωση στην ομάδα διαχείρισης του appWare. Στην εικόνα x παρατείθεται ένα απόσπασμα της εν λόγω κλάσης:



(γράφημα 10: Απόσπασμα της κλάσης appHandling της εφαρμογής appWare Version 1.0)

5.2.4 Η κλάση appPerms

Από αυτή τη κλάση δύναται η δυνατότητα αντιστοίχισης μίας εφαρμογής με τα αντίστοιχα δικαιώματα. Με το που εισέρχεται ο χρήστης ή άτομο από την ομάδα διαχείρισης στη καρτέλα συναντά δύο πίνακες. Ένα πίνακα με τις εφαρμογές που είναι καταχωρημένες στη Βάση Δεδομένων μας και ένα δεύτερο πίνακα που έχει το σύνολο των δικαιωμάτων που μπορεί να έχει μία εφαρμογή android. Ο χρήστης πληκτρολογώντας είτε στο πεδίο αναζήτησης των εφαρμογών είτε στο πεδίο αναζήτησης των δικαιωμάτων, ανακτά με δυναμικό τρόπο την εφαρμογή ή το δικαίωμα που επιθυμεί και τα οποία παρατίθενται στους παρακείμενους πίνακες της εφαρμογής. Όπως και στη περίπτωση της καρτέλας appHandling η ομάδα διαχείρισης εγγράφει την εφαρμογή απ' ευθείας στη βάση. Αντιθέτως, ο χρήστης πρώτα θα πρέπει να ενημερώσει την εφαρμογή appWare στη τελευταία του έκδοση, να εγγράψει στη καρτέλα appHandling μία νέα εφαρμογή και μετά από τη καρτέλα appPerms να κάνει τις ανάλογες αντιστοιχίσεις. Στη συνέχεια, εγγράφονται τα δεδομένα σε προσωρινό πίνακα και ο χρήστης όποτε επιθυμεί μπορεί να τα αποστείλει για τεκμηρίωση στην ομάδα διαχείρισης του appWare. Στην εικόνα x παρατίθεται ένα απόσπασμα της εν λόγω κλάσης:



(γράφημα 11: Απόσπασμα της κλάσης appPerms της εφαρμογής appWare Version 1.0)

5.2.5 *Λοιπές δυνατότητες της εφαρμογής*

Με τα λοιπά εργαλεία της εφαρμογής όπως μνημονεύτηκε στις παραπάνω ενότητες μπορούμε να ενημερωθούμε κατά πόσο υπάρχει μία νεότερη έκδοση της εφαρμογής, να ενημερώσουμε μέσω εισαγωγής αρχείου την εφαρμογή αλλά και να ενημερώσουμε ως χρήστες πλέον τη κεντρική Βάση Δεδομένων για μία νέα εφαρμογή που εισήχθη από το χρήστη μαζί με τα ανάλογα δικαιώματα. Η εφαρμογή θα εξεταστεί από την ομάδα εργασίας του προγράμματος και θα αποφασίσει για το εάν χρήζει εισαγωγής στη βάση δεδομένων ή πρόκειται για κάτι αναληθές. Επίσης δεν είναι δυνατή η πρόσθεση της ίδιας εφαρμογής με τα ίδια δικαιώματα από πολλαπλούς χρήστες καθώς για να είναι δυνατόν ο χρήστης να αποστείλει αίτημα για εισαγωγή στη κεντρική Βάση Δεδομένων πρέπει πρώτα να ενημερώσει μέσω της προηγούμενης διαδικασίας τη τοπική βάση δεδομένων. Το τελευταίο χαρακτηριστικό κρίνεται ως πάρα πολύ βασικό καθώς πολλοί χρήστες μπορούν να φροντίζουν τόσο για τη χρονική ενημερότητα της εφαρμογής όπως και για τη πληρότητά της εφόσον τα εκατομμύρια εφαρμογών που ήδη υπάρχουν καθιστούν αδύνατη τη χειροκίνητη εισαγωγή από τους συγγραφείς και διαχειριστές της εφαρμογής. Επίσης ο χρήστης μελλοντικά δύναται να μην έχει εγκατεστημένη καθόλου βάση δεδομένων στο τοπικό του υπολογιστή αλλά να χρησιμοποιεί την εφαρμογή ενημερωτικά, χρησιμοποιώντας μόνο τη διαδικτυακή βάση δεδομένων. Σε αυτή τη περίπτωση δεν θα είναι δυνατή η προσθήκη νέας εφαρμογής και αντιστοίχισης δικαιωμάτων. Παρόλα αυτά μπορεί να δημιουργήσει εξωτερικό αρχείο με μία νέα εφαρμογή που θα ήθελε να προσθέσει, με εργαλείο που θα ενσωματωθεί μελλοντικά στην εφαρμογή και με το οποίο θα είναι δυνατή η αποστολή του αρχείου απευθείας στους διαχειριστές της εφαρμογής.

5.2.6 Σύγκριση του appWare με το TOS;DR

Όπως αναφέρθηκε και στην βιβλιογραφική ανασκόπηση τον Ιούνιο του 2012 ξεκίνησε το project TOS;DR το οποίο οπτικοποιεί Πολιτικές Ασφάλειας με εναλλακτικό τρόπο σε σχέση με το παραδοσιακό τρόπο αναγραφής με σκοπό την αφύπνιση του χρήστη και παρουσιάζει αρκετά κοινά με τον τρόπο λειτουργίας του appWare.

Σε ότι αφορά τα κοινά και τα δύο συστήματα έχουν ως σκοπό με την απεικόνιση του κινδύνου μέσω στατικής εικόνας, να αναδείξει το ενδεχόμενο πρόβλημα και μέσω της περιγραφής να το κάνει περισσότερο κατανοητό από την ιδιαίτερα δύσκολη στη κατανόηση νομική γλώσσα. Επίσης προσπαθεί να αντιμετωπίσει το πρόβλημα του μεγάλου όγκου των εφαρμογών μέσω της συνεργασίας των χρηστών.

Παρόλα αυτά μπορούμε να διακρίνουμε ουσιαστικές διαφορές. Το TOS;DR εξετάζει εξατομικευμένα τη Πολιτική Ασφάλειας μιας εφαρμογής, επιλέγει τα δομικά της κομμάτια τα οποία την απαρτίζουν, τα μετατρέπει σε κατανοητή μορφή κι έπειτα οι χρήστες καλούνται να τα βαθμονομήσουν ως θετικά, αρνητικά ή επικίνδυνα. Ο δε δείκτης επικινδυνότητας καλείται να φανεί από το ποια κατηγορία από τις τρεις έχει τις περισσότερες αξιολογήσεις. Αντιθέτως το appWare προσεγγίζει τη Πολιτική Ασφάλειας από τα 233 δικαιώματα που αποκτά η εφαρμογή μέσω του manifest.xml. Σε αυτά τα δικαιώματα τους αποδόθηκε μία περισσότερο κατανοητή και εκλαϊκευμένη περιγραφή, ο δυνητικός κίνδυνος δίδεται περιγραφικά ή και μονολεκτικά ενώ η φωτογραφία οπτικοποίησης είναι αντικειμενική του κινδύνου και δεν αποδίδεται περιγραφικά ως θετική, αρνητική ή επικίνδυνη. Ιδιαίτερα δε από την έκδοση android 7 ο χρήστης μπορεί να απαγορέψει απευθείας το συγκεκριμένο δικαίωμα εάν το θεωρήσει επικίνδυνο. Αυτό έχει ως αποτέλεσμα να εκμηδενίζει τις επιπτώσεις του εν λόγω δικαιώματος. Κάτι ιδιαίτερα σημαντικό είναι ότι δεν χρειάζεται η ατομική ανασκόπηση της Πολιτικής Ασφάλειας της εκάστοτε εφαρμογής αφού ο δυνητικός κίνδυνος εκμαιεύεται από τα δικαιώματα χρήσης που αποκτούνται και τα οποία είναι συγκεκριμένα σε πλήθος με προσδιορισμένη περιγραφή και κατ' επέκταση προσδιορισμένο δυνητικό κίνδυνο. Αυτό έχει ως θετικό ότι απαιτείται σημαντικά λιγότερος χρόνος για το προσδιορισμό των επικίνδυνων χαρακτηριστικών μίας εφαρμογής αλλά έχει ως επίπτωση το μη εξατομικευμένο προσδιορισμό του κινδύνου.

Το TOS;DR έως και την συγγραφή αυτής της διατριβής περιγράφει τα χαρακτηριστικά των Πολιτικών Ασφάλειας Ιστοσελίδων χωρίς να προσδιορίζει εάν θα επεκταθεί σε εφαρμογές για φορητές συσκευές. Το appWare από τη πλευρά του έχει ως κεντρικό στόχο την οπτικοποίηση της Πολιτικής Ασφάλειας όπως αυτή πηγάζει από τα δικαιώματα χρήσης για εφαρμογές φορητών συσκευών και όχι ιστοσελίδων. Στο παρακάτω πίνακα περιγράφονται συνοπτικά οι δυνατότητες των δύο εφαρμογών:

Περιγραφή	TOS;DR	appWare
Πολιτική Ασφάλειας	Εξατομικευμένη ανασκόπηση της Πολιτικής Ασφάλειας	Ο δυνητικός κίνδυνος πηγάζει από τα δικαιώματα χρήσης που αποκτά μία εφαρμογή
Πλατφόρμα	Εφαρμογή Ιστοσελίδας	Java, Client-Server, εφαρμογή ιστοσελίδας μέσω webstart

Αντικείμενο	Ιστοσελίδες παγκόσμιου ιστού	Εφαρμογές φορητών συσκευών
Δυνατότητες επέκτασης σε άλλες πλατφόρμες	Ναι	Ναι
Δυνατότητα επέκτασης σε άλλα αντικείμενα	Ναι (π.χ. εφαρμογές για φορητές συσκευές)	Ναι μέσω προσδιορισμού τους
Ταχύτητα ανασκόπησης Π.Α.	Εξαρτάται από το μέγεθος της Π.Α.	Αυξημένη ταχύτητα λόγω των αυστηρά 233 καθορισμένων δικαιωμάτων
Επέκταση της Βάσης Δεδομένων	Ναι, μέσω των χρηστών της ιστοσελίδας	Ναι, μέσω των χρηστών της εφαρμογής
Περιγραφή κινδύνου	Μέσω εκλαΐκευσης των στοιχείων της Π.Α.	Μέσω εκλαΐκευσης των δικαιωμάτων χρήσης
Οπτικοποίηση του κινδύνου	Μέσω των τριών γραφημάτων {θετικό, αρνητικό, επικίνδυνο}	Μέσω αντικειμενικού γραφήματος αναλόγως του κινδύνου
Δυνητικός Κίνδυνος	Πηγάζει από τη περιγραφή	Εκτός της περιγραφής προσδιορίζεται με το πολύ δύο λέξεις

Από τα παραπάνω, εύκολα βγαίνει το συμπέρασμα λόγω των αρκετών σημείων παρόμοιας συμπεριφοράς θα ήταν εφικτή η συνεργασία των δύο εφαρμογών με σκοπό τη γεφύρωση των διαφορών τους και την επέκτασή τους σε όσο το δυνατών περισσότερες πλατφόρμες ενώ θα γινόταν ταυτοχρόνως χρήση της συνεισφοράς και των δύο ομάδων των χρηστών της εφαρμογής.

5.2.7 Μελλοντικές ενέργειες

5.2.7.1 Επίλυση του προβλήματος του όγκου των δεδομένων

Αν και ο χρόνος καταχώρισης μίας νέας εφαρμογής και αντιστοίχισής τους με δικαιώματα απαιτεί από την ομάδα διαχείρισης μόλις 5 λεπτά, γίνεται αντιληπτό ότι η καταχώριση και η αντιστοίχιση με δικαιώματα για το σύνολο των 2.6 εκ. εφαρμογών που υπήρχαν μεταφορτωμένες στο Google Play το Δεκέμβρη του 2016 (Statista 2017) [97] από μία ομάδα διαχείρισης θα απαιτούσε πάνω από 210.000 εργατοώρες καταχώρισης όταν δε μόνο μέσα σε ένα έτος υπήρξε αύξηση κατά 600.000 νέες εφαρμογές. Οι παραπάνω αριθμοί κάνουν απαγορευτική την οποιαδήποτε σκέψη για κλειστή διαχείριση της εφαρμογής από μόνο μία ομάδα διαχείρισης. Μία διέξοδος λοιπόν είναι το άνοιγμα της εφαρμογής στο κοινό και η δυνατότητα καταχώρισης απευθείας στη βάση. Για να αποφευχθούν οι περιπτώσεις ψευδών καταχωρίσεων θα μπορούσε να δημιουργηθεί σύστημα αξιολόγησης χρηστών σε πρώτη φάση με κριτήριο τις αναρτήσεις τους και βαθμολόγησης από την ομάδα διαχείρισης. Έπειτα είναι δυνατό να σχηματιστούν βαθμολογικά επίπεδα πυραμίδας στα οποία θα υπάρχει και η ανάλογη δυνατότητα καταχώρισης και επεξεργασίας δεδομένων. Πριν φτάσουμε στην ανωτέρω λύση προτείνεται να καταχωρείται ικανοποιητικός

αριθμός από τις δημοφιλέστερες νέες εφαρμογές της εβδομάδας όπως τις ανακοινώνει το Google Play καθώς και από τις εφαρμογές που έχουν αντιστοιχιστεί από τους χρήστες των οποίων ο αριθμός είναι αδύνατο να υπολογιστεί αυτή τη στιγμή. Η λύση της αυτοματοποιημένης καταχώρισης του συνόλου των δεδομένων δεν είναι δυνατή κατά τη στιγμή συγγραφής αυτής της διπλωματικής καθώς το Google Play αποτρέπει τις μαζικές αυτοματοποιημένες αναζητήσεις. Συγκεκριμένα, αν και ανεπίσημα έχει δημιουργήσει τη σχετική βιβλιοθήκη την οποία τη διανέμει ελεύθερα και η οποία παρέχει μερική πρόσβαση στα δεδομένα του Google Play (android-market-api)[98] σε περίπτωση μαζικής αναζήτησης αποκλείει τη πρόσβαση σε αυτό το λογαριασμό google. Παρόλα αυτά θα μπορούσε πιθανώς να χρησιμοποιηθεί για να καταχωρίζονται αυτοματοποιημένα οι δημοφιλέστερες εφαρμογές της εβδομάδας ή/και του μήνα.

5.2.7.2 Μελλοντικές υλοποιήσεις της εφαρμογής σε άλλες πλατφόρμες

Στο άμεσο μέλλον η εφαρμογή appWare εκτός από εφαρμογή με το σύστημα εξυπηρετητή-πελάτη (Client-Server) θα μεταφερθεί αυτούσια σε μορφή ιστοσελίδας. Αν και ήδη δύναται ο χρήστης να χρησιμοποιήσει την εφαρμογή μέσω διαδικτύου με τη χρήση του webstart που ήδη έχει ενσωματωθεί στην εφαρμογή, κρίνεται απαραίτητο να μεταφερθεί αυτούσιο και σε μία προγραμματιστική γλώσσα διαδικτύου όπως η php ή η Html5. Επίσης στα άμεσα σχέδιά μας είναι η μεταφορά της εφαρμογής σε έκδοση για φορητές συσκευές android. Ο ανωτέρω σχεδιασμός βρίσκεται ήδη στη φάση της ανάπτυξης. Για όλες τις πλατφόρμες θα υπάρχει κοινή βάση δεδομένων για άμεσο συγχρονισμό μεταξύ τους.

5.3 Σύνοψη και συμπεράσματα

Μετά την ανάλυση της ενημερότητας των χρηστών όπως αυτή προέκυψε από τα προηγούμενα κεφάλαια έγινε επιτακτική δημιουργία μίας εφαρμογής η οποία θα βοηθά στην ανάπτυξη της ενημερότητας του χρήστη αλλά και στην οπτικοποίηση της πολιτικών ασφάλειας και των δικαιωμάτων χρήσης που αποκτά μία εφαρμογή όταν εγκαθίσταται σε φορητές συσκευές. Η εφαρμογή που υλοποιήσαμε ονομάστηκε προσωρινά appWare όπου περιέχει το σύνολο των δικαιωμάτων που μπορεί να αποκτήσει μία εφαρμογή για φορητές συσκευές, μία εκλαϊκευμένη περιγραφή του εν λόγω δικαιώματος σε κατανοητή γλώσσα που περιγράφει τους κινδύνους που δύναται να αντιμετωπίσει ο χρήστης καθώς και μία συνοπτική περιγραφή του κινδύνου. Μέσα στην εφαρμογή είναι αποθηκευμένες ήδη οι δημοφιλέστερες εφαρμογές του Google Play για το 2015 και στο άμεσο μέλλον και σε τακτά χρονικά διαστήματα θα προστίθενται περισσότερες. Το appWare δημιουργεί μία αναφορά σε ηλεκτρονικό αρχείο pdf άμεσα διαθέσιμη στο χρήστη η οποία εκτός του συνόλου των δικαιωμάτων που απαιτεί μία εφαρμογή και τις περιγραφές που αναφέρθηκαν παραπάνω προσθέτει επίσης μία εικόνα αντιπροσωπευτική του εν λόγω δικαιώματος με σκοπό την εγρήγορση του χρήστη της εφαρμογής.

Η εφαρμογή χωρίζεται σε 4 διακριτές καρτέλες. Η πρώτη καρτέλα Dataset περιλαμβάνει το σύνολο των δικαιωμάτων που μπορούν να λάβουν οι εφαρμογές. Η δεύτερη καρτέλα με ονομασία appData είναι η κεντρικότερη καρτέλα της εφαρμογής, καθώς σε αυτήν χρήστης μπορεί να λάβει γνώση για το σύνολο των δικαιωμάτων που έχουν οι αποθηκευμένες εφαρμογές. Από τις δύο αυτές καρτέλες ο χρήστης μπορεί να λάβει αναφορά σε ηλεκτρονικό αρχείο τύπου pdf όπου στη μεν

πρώτη εκτυπώνεται το δικαίωμα που επιλέχτηκε μαζί με την αναλυτική περιγραφή του δικαιώματος και του δυνητικού κινδύνου εάν υπάρχει, τη συνοπτική περιγραφή της απειλής καθώς και την αντιπροσωπευτική εικόνα που χαρακτηρίζει την απειλή. Από τη δεύτερη καρτέλα ο χρήστης λαμβάνει αναφορά για το σύνολο πλέον το δικαιωμάτων σε επίπεδο περιγραφής, συνοπτικής απειλής και αντιπροσωπευτικής εικόνας. Οι δύο επόμενες καρτέλες appHandling και addPerms έχουν διαχειριστικό ρόλο. Εξαιτίας του μεγάλου αριθμού των εφαρμογών κρίθηκε επιτακτική ανάγκη οι χρήστες να συνδράμουν στην ενημέρωση της βάσης δεδομένων των εφαρμογών και των αντίστοιχων δικαιωμάτων καθώς το Google Play μέσω διαφόρων δικλείδων ασφάλειας δεν επιτρέπει την αυτοματοποιημένη αναζήτηση εφαρμογών και δικαιωμάτων χρήσης ούτε τη μεταφόρτωσή τους. Έτσι με τις δύο αυτές καρτέλες οι χρήστες και η ομάδα διαχείρισης του appWare έχουν τη δυνατότητα να εγγράψουν νέες εφαρμογές στο appWare καθώς και να τις αντιστοιχίσουν με τα ανάλογα δικαιώματα.

Για να αποσοβηθεί η πιθανότητα διπλοεγγραφών ο χρήστης πριν εγγράψει μία νέα εφαρμογή και της αντιστοιχίσει δικαιώματα πρόσβασης πρέπει πρώτα να ενημερώσει το appWare στη τελευταία του έκδοση. Τέλος στα άμεσα σχέδιά μας είναι η εφαρμογή να επεκταθεί επίσης σε νέες τεχνολογικές πλατφόρμες. Θα θέλαμε άμεσα εκτός από πρόγραμμα της μορφής πελάτης-εξυπηρετητής να μεταφερθεί αυτούσιο τόσο σε μορφή ιστοσελίδας ή/και ως πρόσθετο (add-on) για φυλλομετρητές, όσο και σε εφαρμογή για φορητές συσκευές

6

Συμπεράσματα

Η ταχύτητα εξέλιξης της τεχνολογίας στο τομέα των έξυπνων φορητών συσκευών όπως κινητά τηλέφωνα και ταμπλέτες ώθησε μεγάλο ποσοστό του πληθυσμού να προβεί στην αγορά και τη χρήση τους. Οι κατασκευαστές φορητών συσκευών καθώς και μεγάλες πολυεθνικές εταιρείες εκμεταλλεύτηκαν επίσης τις νέες αυτές τεχνολογίες προχωρώντας στη δημιουργία διαδικτυακών ηλεκτρονικών καταστημάτων μεταφόρτωσης εφαρμογών για φορητές συσκευές (App Stores) από τα οποία το ευρύ κοινό δωρεάν ή με πληρωμή είχε τη δυνατότητα να μεταφορτώσει εφαρμογές απευθείας στη φορητή του συσκευή. Σε ό,τι αφορά τις πολιτικές ασφαλείας, τα κανονιστικά πλάισια που καθόριζαν τη συλλογή και διαχείριση των προσωπικών δεδομένων, ίσχυαν στο παρελθόν και αφορούσαν στα παραδοσιακά ηλεκτρονικά καταστήματα ή τις κοινές ιστοσελίδες, εξακολουθούν να ισχύουν με μικρές μόνο διορθώσεις και προσαρμογές ακολουθώντας κυρίως τα πρότυπα XACML[1] και EPAL[2]. Οι δε χρήστες από τη πλευρά τους παρουσίασαν αδυναμία κατανόησης των πολιτικών κατανόησης κυρίως εξαιτίας της σύνθετης ή ιδιαίτερης νομικής ορολογίας που αυτές υιοθετούσαν (Kambiz et al)[3] με αποτέλεσμα τη τυφλή τους αποδοχή και την αγνόηση των κινδύνων που διατρέχει η ιδιωτικότητά τους (Buchenscheit et al).[4]. Οι εταιρείες από τη πλευρά τους εκμεταλλεύτηκαν την έλλειψη ενημερότητας των χρηστών κάνοντας κοινή πρακτική την αγορά και πώληση προσωπικών δεδομένων χωρίς πρότερη συναίνεση των χρηστών.

Οι χρήστες που εμφάνιζαν ανησυχία για τα προσωπικά τους δεδομένα ήταν αδύνατο να πραγματοποιήσουν οποιαδήποτε ηλεκτρονική συναλλαγή χωρίς να αποκαλυφθούν προσωπικές πληροφορίες (Rust, Kannan, and Peng, 2002)[13]. Κατ' επέκταση ξεκίνησαν να παίρνουν υπέρμετρα μέτρα ασφάλειας τα οποία κυμαίνονταν από το περιορισμό της χρήσης του διαδικτύου έως τη πλήρη αποχή από την ηλεκτρονική εποχή.

Από τα παραπάνω έγινε σαφής η ανάγκη ανεύρεσης ενός τρόπου βελτίωσης της ενημερότητάς τους καθώς και του επιπέδου αντίληψης τους προκειμένου να αποτραπεί ο κοινωνικός αναλφαβητισμός και να ενισχυθεί η ενημερότητα και η διαδικτυακή κουλτούρα, σε επίπεδα επιτρέπουν τον εντοπισμό των δυνατών κινδύνων από την τυφλή αποδοχή των πολιτικών ασφαλείας.

Η τρέχουσα διαδικασία ενημέρωσης μέσω της δημοσίευσης των πολιτικών ασφάλειας που ακολουθείται έως και σήμερα δεν φαίνεται να είναι αποδοτική καθώς το χρονικό κόστος κρίνεται απαγορευτικό για το μέσο χρήστη απαιτώντας τουλάχιστον 72 λεπτά ημερησίως ανάγνωσης

πολιτικών ασφάλειας για ένα χρήστη που θα ήθελε να είναι πλήρως ενήμερος. Το δε οικονομικό κόστος υπολογίστηκε ότι ξεπερνάει τα 3.500 δολάρια ετησίως για μία αγορά όπως η Η.Π.Α. . Τα παραπάνω έκαναν επιτακτική την ανάγκη ανεύρεσης νέων τρόπων απεικόνισης των πολιτικών ασφαλείας, οι οποίες θα ήταν περισσότερο κατανοητές και ελκυστικές για το μέσο χρήστη και ταχύτερα στην ανάγνωση.

Σε ό,τι αφορά τις φορητές συσκευές με λειτουργικό σύστημα android, το πολυμεθοδικό σύστημα ασφάλειας που ακολουθούν δεν φάνηκε να βοηθά το μέσο χρήστη στην εις βάθος κατανόηση των κινδύνων που ενδεχομένως να αντιμετωπίσει παρά μόνο στράφηκε στη προστασία της συσκευής και του δημιουργού του λειτουργικού συστήματος. Τουναντίον, εισήγαγε ένα τρόπο απλής αναφοράς δικαιωμάτων που μπορούσε να λάβει μία εφαρμογή για λειτουργικό σύστημα android τα οποία ο χρήστης μέχρι την έκδοση 7 του λειτουργικού δεν είχε καμία δυνατότητα να ανακόψει. Ο τρόπος ενημέρωσης του χρήστη παρέμεινε η ανάγνωση της πολιτικής ασφάλειας της εταιρείας δημιουργίας της εκάστοτε εφαρμογής η οποία δεν βρίσκεται απευθείας στο ηλεκτρονικό κατάστημα που μεταφορτώνεται η εφαρμογή αλλά πιθανώς στον επίσημο δικτυακό ιστότοπο. Ο δε χρήστης είχε τη δυνατότητα να μεταφορτώσει την εφαρμογή της αρεσκείας του χωρίς να αποδεχτεί υποχρεωτικά τη πολιτική ασφάλειας του δημιουργού της εφαρμογής ή να ενημερωθεί άμεσα σε τι είδους δεδομένα είχε πρόσβαση η εφαρμογή. Όπως προαναφέραμε η πολιτική ασφάλειας δεν βρισκόταν στον ιστότοπο μεταφόρτωσης της εφαρμογής με αποτέλεσμα να μπορεί να αναγνωστεί μόνο εάν ο δημιουργός είχε τοποθετήσει σχετικό ηλεκτρονικό σύνδεσμο που να ανακατευθύνει σε αυτή. Όσο δε για τα δικαιώματα που αποκτούσε η εφαρμογή αυτά βρίσκονταν σε υπομενού του ηλεκτρονικού καταστήματος, όχι άμεσα ορατά στο χρήστη και χωρίς να αναφέρουν του δυνητικούς κινδύνους που ενδεχομένως να αντιμετωπίσει ο χρήστης. Τα παραπάνω μας κατεύθυναν στο να αναζητήσουμε νέους τρόπους αναγραφής αυτών των δικαιωμάτων που θα συνοψίζουν τους δυνητικούς κινδύνους που ενδεχομένως να αντιμετωπίσει ο χρήστης οπτικοποιώντας όσο το δυνατόν καλύτερα τον δυνητικό κίνδυνο μέσω εικόνων.

Στη διπλωματική αυτή έγινε χρήση των λειτουργιών που προσφέρει η δωρεάν εφαρμογή επικοινωνίας και άμεσων μηνυμάτων Viber. Ο λόγος της επιλογής αυτής ήταν η δημοφιλία της καθώς και η ευκολία με την οποία θα μπορούσαμε να εξάγουμε δεδομένα για στατιστική μελέτη. Μέσω των τεχνικών που εφαρμόσαμε, εντοπίσαμε μέσα σε ένα ανωνυμοποιημένο δείγμα 2000 αριθμών κινητής τηλεφωνίας ότι 682 άτομα είχαν εγκατεστημένη την εν λόγω εφαρμογή. Από τα 682 άτομα ταυτοποιήθηκαν πλήρως ως προς το ονοματεπώνυμο τα 475, δηλαδή το 70% των χρηστών ενώ για αρκετά άτομα ανακτήθηκαν πρόσθετες πληροφορίες όπως τόπος κατοικίας και επάγγελμα. Τα παραπάνω ανακτήθηκαν κάνοντας χρήση μόλις τριών μηχανών αναζήτησης κάτι που μας κάνει να πιστεύουμε ότι είναι δυνατή περαιτέρω βελτίωση ταυτοποίησης. Από το δείγμα που ταυτοποιήθηκε επιλέχτηκαν με τη θέλησή τους 20 άτομα τα οποία έγιναν αντικείμενο μελέτης μας για περαιτέρω ανάλυση της τρέχουσας ενημερότητάς τους μέσω συμπλήρωσης ηλεκτρονικών ερωτηματολογίων και παρακολούθησης της δραστηριότητάς τους μέσω του Viber. Από την ανάλυση προέκυψε ότι η συντριπτική πλειοψηφία δεν διάβασε τη πολιτική ασφάλειας ενώ εάν τη διάβασε δήλωσε διστακτική στο εάν θα τη κατανοούσε. Παρατηρήθηκε δε, ότι η μεγάλη πλειοψηφία των υποκειμένων δεν γνώριζε για τη διαβίβαση των προσωπικών τους δεδομένων προς τρίτους ούτε γνώριζε τους δυνητικούς κινδύνους με τους οποίους θα μπορούσε να βρεθεί αντιμέτωπη. Επίσης, εξετάστηκε το ενδεχόμενο της δυνατότητας παρακολούθησης πληθυσμού σε ευρεία κλίμακα. Όπως παρατηρήθηκε το σενάριο αυτό λόγω της εξέλιξης της τεχνολογίας δεν

κρίνεται πλέον απαγορευτικό και είναι δυνατό να πραγματοποιηθεί με μέτριους σε μέγεθος ανθρώπινους και υλικούς πόρους.

Τα αποτελέσματα που προέκυψαν από τη βιβλιογραφική ανασκόπηση του δεύτερου κεφαλαίου καθώς και από την ανάλυση και εκτίμηση της ενημερότητας των υποκειμένων που αναλύσαμε στο τέταρτο κεφάλαιο έδειξαν ότι οι χρήστες δεν επιθυμούν να διαβάσουν τις πολιτικές ασφάλειας είτε λόγω τους χρονικού και οικονομικού κόστους που απαιτούν, είτε λόγω του φόβου μη κατανόησής τους είτε λόγω χαμηλής αντίληψης των κινδύνων που ενδεχομένως αντιμετωπίσουν. Από τα παραπάνω έγινε σαφές ότι πρέπει να δημιουργηθεί ένας νέος τρόπος αποτύπωσης και οπτικοποίησης των πολιτικών ασφάλειας και των δικαιωμάτων που αποκτούν οι εφαρμογές για φορητές συσκευές. Προσπαθήσαμε να αντιμετωπίσουμε το πρόβλημα δημιουργώντας της εφαρμογή appWare η οποία θα είναι δωρεάν στο κοινό και η οποία είναι δυνατό να περιλάβει πλήθος εφαρμογών για φορητές συσκευές. Στις εφαρμογές που βρίσκονται στη βάση δεδομένων του appWare έχουν αντιστοιχιστεί όλα τα δικαιώματα που αυτή η εφαρμογή αποκτά με την εγκατάστασή της. Στα δικαιώματα αυτά έχει ενσωματωθεί μία απλή και κατανοητή περιγραφή καθώς και μία συνοπτική και πολλές φορές μονολεκτική περιγραφή δυνητικού κινδύνου. Μέσω αναφοράς σε ηλεκτρονικό αρχείο τύπου pdf που εκτυπώνει το appWare αναγράφεται η κατανοητή περιγραφή και ο δυνητικός κίνδυνος ανά δικαίωμα ενώ για την βέλτιστη οπτικοποίηση του δικαιώματος έχει ενσωματωθεί μία αντιπροσωπευτική εικόνα του δυνητικού κινδύνου. Για την ενημέρωση της Βάσης δεδομένων του appWare εκτός της ομάδας διαχείρισής του υπάρχει η δυνατότητα ενημέρωσης και από τους χρήστες τους. Μελλοντικά το appWare εκτός από εφαρμογή τύπου πελάτη-εξυπηρετητή θα θέλαμε να επεκταθεί και σε νέα περιβάλλοντα όπως σε διαδραστικές ιστοσελίδες καθώς και σε αυτόνομη εφαρμογή για φορητές συσκευές.

Τα αποτελέσματα του appWare θα μπορούσαν να δημιουργήσουν θετικές προοπτικές στη στην αποτύπωση των δικαιωμάτων που αποκτά μία εφαρμογή για φορητές συσκευές. Εάν οι χρήστες λόγω της επαύξησης της ενημερότητάς τους αποκτήσουν αμυντική στάση έναντι των μεταφορτώσεων από τα app markets πιστεύουμε ότι αυτά θα προβούν στην εκτέλεση θετικών αντιμέτρων. Συγκεκριμένα, οι επίσημοι ιστότοποι όπως το Google Play που ήταν το αντικείμενο μελέτης μας θα μπορούσαν να μεταφέρουν στη κεντρική ιστοσελίδα της εφαρμογής τα δικαιώματα χρήσης και όχι να αποκρύπτονται σε υπομενού. Επίσης, η υποχρεωτικότητα του συνδέσμου της Πολιτικής Ασφάλειας της εκάστοτε εφαρμογής να εφαρμόζεται αν μία εφαρμογή αποκτά κάποιο από τα δικαιώματα από τα οποία δύναται να αποκτηθούν δεδομένα προσωπικού χαρακτήρα όπως τα δεδομένα χρήστη ή η τοποθεσία χρήστη. Οι δε προγραμματιστές από τη πλευρά τους θα μπορούσαν να υποχρεωθούν είτε από τα app markets είτε από την αμυντική στάση των πιθανών χρηστών τους να κάνουν υποχρεωτική την αποδοχή της Πολιτικής Ασφάλειας πριν την εγκατάσταση της εφαρμογής ή/και κατά την εκτέλεση της πρώτης χρήσης της εφαρμογής καθώς και επανάληψη της αποδοχής εάν προστεθεί νέο δικαίωμα σε περίπτωση νέας έκδοσης αυτής. Τέλος, οι προγραμματιστές πιθανώς να προβούν στην ενσωμάτωση στο manifest.xml μόνο των απαραίτητων δικαιωμάτων χρήσης για την εύρυθμη λειτουργία της εφαρμογής και να μειωθεί το φαινόμενο της υπεραπόκτησης δικαιωμάτων (overpermission) που δεν δικαιολογούνται από τη χρήση της αυτής (Richard and Chow, 2012)[100].

.

7

Αναφορές

[1] Kambiz Ghazinour, Maryam Majedi, Ken Barker, A Model for Privacy Policy Visualization in 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2009.

[2] EXtensible Access Control Markup Language (XACML) Version 2.0. (2005). 2nd ed. [ebook] Tim Moses, Entrust Inc. Available at: https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf [Accessed 20 Jan. 2017].

[3] W3C. Enterprise Privacy Authorization Language. http://www.w3.org/Submission/2003/SUBM-EPAL-20031110 , 2003.

[4] Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M. and Kargl, F. (2014). Privacy implications of presence sharing in mobile messaging applications. *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia - MUM '14*.

[5] Ghazinour, K. and Albalawi, T. (2016). A Usability Study on the Privacy Policy Visualization Model. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).

[6] Statista. (2017). Number of smartphone users in the United States from 2010 to 2021. [online] Available at: http://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/ [Accessed 20 Oct. 2016].

[7] Statista. (2017)a. Number of smartphone users in the United States from 2010 to 2021. [online] Available at: http://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us. [Accessed 20 Oct. 2016].

[8] Statista. (2017)b. Google Play Store: number of apps 2009-2016 | Statistic. [online] Available at: http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store [Accessed 20 Jan. 2017].

[9] OLMSTEAD, K. and ATKINSON, M. (2015). APPS PERMISSIONS IN THE GOOGLE PLAY. [online] Pew Research Center. Available at: http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/ [Accessed 20 Jan. 2017].

[10] Wang, H., Lee, M.K.O., & Wang, C. (1998). Consumer Privacy Concerns About Internet Marketing. Communications of the ACM, 41, 63-70.

[11] Gillmor, D. (1998). Violating Privacy is Bad Business. Computerworld, 32 (12), 38-39.
[12] Caruso, D. (1998). The Law and the Internet Beware. Columbia Journalism Review, 37 (1), 57-61.
[13] Rust, R.T., Kannan, P.K., & Peng, N. (2002). The Customer Economics of Internet Privacy. Journal of the Academy of Marketing Science, 30, 455-464.
[14] Fletcher, K. (2003). Consumer Power and Privacy: The Changing Nature of CRM. International Journal of Advertising, 22, 249-272.
[15] Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy and Marketing, 19 (1), 62-73.
[16] Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model. Behavior and Information Technology, 23 (6), 413-422.
[17] Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. The Information Society, 20, 313-324.
[18] Raab, C.D. & Bennet, C.J. (1998). The Distribution of Privacy Risks: Who Needs Protection? The Information Society, 14 (4), 253-262.
[19] Rindfleish, T.C. (1997). Privacy, Information Technology, and Healthcare. Communications of the ACM, 40, 92-100.
[20] Saunders, K. & Zucker, B. (1999). Contracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. International Review of Law, Computers, and Technology, 13 (2), 183-192.
[21] Culnan, M. & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, 10 (1), 104-115.
[22] Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy and Marketing, 19 (1), 62-73.
[23] Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. Journal of Business & Economics Research (JBER), [online] 7(3). Available at: https://www.researchgate.net/publication/239920578_Antecedents_And_Consequences_Of_Consumers_Online_Privacy_Concerns [Accessed 20 Jan. 2017].
[24] Miyazaki, A.D. & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. The Journal of Consumer Affairs, 36, 28-49.
[25] Dinev, T. & Hart, P. (2006a). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. International Journal of Electronic Commerce, 10 (2), 7-29.
[26] Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-Privacy in 2nd Generation E-Commerce. Privacy Preferences versus Actual Behavior. In Proceedings of EC‟01: Third ACM Conference on Electronic Commerce. New York: Association for Computing Machinery, 38-47.
[27] Burn, J. & Loch, K. (2001). The Societal Impact of the World Wide Web—Key Challenges for the 21st Century. Information Resources Management Journal, 14 (4), 4-14.
[28] Papazafeiropoulou, A. & Pouloudi, A. (2001). Social Issues in Electronic Commerce: Implications for Policy Makers. Information Resources Management Journal, 14 (4), 24-32.
[29] Bickford, D.M. & Reynolds, M. (2002). Activism and Service-Learning: Reframing Volunteerism as an Act of Dissent. Critical Approaches to Teaching, Literature, Language, Composition, and Culture, 8 (2), 229-252.

[30] McDonald A., Cranor L.F., 2008. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008. Privacy Year in Review issue. [online] Available at: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[31] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," 4. [online] Available at : http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[32] Kenneth C. Laudon, "Markets and Privacy," Communications of the ACM 39, no. 9 (1996): 96.

[33] Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century (Sebastopol, CA: O'Reilly & Associates, 2001), 183.

[34] Mark Trevelyan, "Stolen account prices fall as market flooded," news.com.au, July 15, 2008, [online] Avalaible at : http://www.news.com.au/technology/story/0,25642,24023758-5014111,00.html.

[35] Serge Egelman, Lorrie Faith Cranor, and Abdur Chowdhury, "An Analysis of P3P-Enabled Web Sites among Top-20 Search Results." (Proceedings of the Eighth International Conference on Electronic Commerce, Fredericton, New Brunswick, Canada, August 14-16).

[36] Govani T., Pashley H. (2007). Student Awareness of the Privacy Implications while Using Facebook. Unpublished manuscript, 2007. [online] Available at : http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

[37] Tow, W., Dell, P. and Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. Journal of Information Technology, [online] 25(2), pp.126-136. Available at: http://link.springer.com/article/10.1057/jit.2010.18 [Accessed 21 Jan. 2017].

[38] German Federal and State Data Protection Commissioners. "Privacy-enhancing technologies" by the Working Group on "privacy enhancing technologies" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners (October 1997), published on http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

[39] Gross, R., Acquisti, A. and Heinz, H. (2005). Information revelation and privacy in online social networks. Proceedings of the 2005 ACM workshop on Privacy in the electronic society - WPES '05, [online] pp.71-80. Available at: https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf [Accessed 21 Jan. 2017].

[40] Cranor, L., Guduru, P. and Arjula, M. (2006). User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction, [online] 13(2), pp.135-178. Available at: http://lorrie.cranor.org/pubs/privacy-bird-20050714.pdf [Accessed 21 Jan. 2017].

[41] Goettke R. and Christiana J., "Privacy and Online Social Networking Websites", [online] available at : http://www.eecs.harvard.edu/cs1999r/fp/RichJoe.pdf, 2005

[42] Dwyer, C. (2007). Digital Relationships in the "MySpace" Generation: Results From a Qualitative Study. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. [online] Available at: http://csis.pace.edu/dwyer/research/DwyerHICSS2007.pdf [Accessed 21 Jan. 2017].

[43] Acquisti, A. and Gross, R. (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. 1st ed. [ebook] Cambridge: Privacy Enhancing Technologies Workshop (PET). Available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf [Accessed 21 Jan. 2017].

[44] Debatin, B., Lovejoy, J., Horn, A. and Hughes, B. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, [online] 15(1), pp.83-108. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2009.01494.x/full [Accessed 21 Jan. 2017].

[45] Donath, J. (2007). Signals in Social Supernets. *Journal of Computer-Mediated Communication*, [online] 13(1), pp.231-251. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00394.x/full [Accessed 21 Jan. 2017].

[46] Pitkänen, O. and Tuunainen, V. (2012). Disclosing Personal Data Socially — An Empirical Study on Facebook Users' Privacy Awareness. *Journal of Information Privacy and Security*, 8(1), pp.3-29.

[47] Changi Nam, Chanhoo Song, Euehun Lee,Chan Ik Park, and Euehun Lee,Chan Ik Park (2006) ,"Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online", in NA - Advances in Consumer Research Volume 33, eds. Connie Pechmann and Linda Price, Duluth, MN : Association for Consumer Research, Pages: 212-217.[online]. Available at: http://www.acrwebsite.org/volumes/v33/naacr_v33_98.pdf. [Accessed 21 Jan. 2017].

[48] McCreadie, M., Rice, R. and Chang, S. (2002). Accessing and Browsing Information and Communication, ISBN 0-262-18214-9. *The Information Society*, [online] 18(5), pp.417-418. Available at: https://pdfs.semanticscholar.org/a2a4/20dd0364a18dce3ace04c1c69ebaf357cd37.pdf [Accessed 22 Jan. 2017].

[49] Dinev, T. and Hart, P. (2006)b. Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. *e-Service Journal*, 4(3), pp.25-60.

[50] Graeff, T. and Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, 19(4), pp.302-318.

[51] Barbaro, M. & Zeller, T. (2006). A Face is exposed for AOL Searcher No. 4417749. New York Times, August 9. [online] available at: http://www.nytimes.com/2006/08/09/technology/09aol.html . [Accessed 21 Jan. 2017].

[52] Staples, B. (2004). The Battle Against Junk Mail and Spyware on the Web. New York Times, January 3. [online] Available at: http://www.nytimes.com/2004/01/03/opinion/editorial-observer-the-battle-against-junk-mail-and-spyware-on-the-web.html?_r=0 . [Accessed 21 Jan. 2017].

[53] Strauss, J., El-Ansary, A., & Frost, R. (2006). E-Marketing. Upper Saddle River, NJ: Pearson Prentice Hall.

[54] Robertson, R. (2012). Security Auditing: The Need for Policies and Practices. *Journal of Information Privacy and Security*, 8(1), pp.30-37.

[55] Google. Android security overview. [online] Available: http://source.android.com/tech/security/index.html. [Accessed 21 Jan. 2017].

[56] Boksasp, Trond, and Eivind Utnes. "Android apps and permissions: Security and privacy risks." (2012).

[57] Google. Signing your applications.[Online] Available at: http://developer.android.com/guide/publishing/app-signing.html. [Accessed 4 Feb. 2017].

[58] Google. Android market developer program policies. [online] Available at: https://play.google.com/intl/el/about/developer-content-policy. [Accessed 4 Feb. 2017].
[59] Google. Developer distribution agreement. [online] Available at: https://play.google.com/about/developer-distribution-agreement.html. [Accessed 4 Feb. 2017].
[60] Rich Cannings. Exercising our remote application removal feature. [online] Available: http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html. [Accessed 4 Feb. 2017].
[61] Android Central. How Does Smartphone Memory Work [online] Available at: http://forums.androidcentral.com/general-help-how/83835-how-does-smartphone-memory-work.html . [Accessed 4 Feb. 2017].
[62] Hiroshi Lockheimer (2012). Android and security. [online] Available at: http://googlemobile.blogspot.com/2012/02/android-and-security.html. [Accessed 4 Feb. 2017].
[63] Rash Wayne (2012). Google Bouncer Gives Android Market Some Security Muscle. [online]. Available at: http://www.eweek.com/c/a/Security/Google-Bouncer-Gives-Android-Market-Some-Security-Muscle-884540. [Accessed 4 Feb. 2017].
[64] McAfee Mobile Security. [online]. Available at: https://play.google.com/store/apps/details?id=com.wsandroid.suite. [Accessed 5 Feb. 2017].
[65] Bitdefender Mobile Security for android. [online]. Available at: https://play.google.com/store/apps/details?id=com.bitdefender.security . [Accessed 5 Feb. 2017].
[66] Shannon McCarty-Caplan 2016. Trend Micro. Mobile Ransomware: The Fast Growing Yet Unknown Threat. [online]. Available at: http://blog.trendmicro.com/mobile-ransomware-fast-growing-yet-unknown-threat. [Accessed 5 Feb. 2017].
[67] JP Buntix, 2017. Android Users Face a new Ransomware Threat. [online]. Available at: https://themerkle.com/android-users-face-a-new-ransomware-threat . [Accessed 5 Feb. 2017].
[68] Viber. [online]. Available at: https://play.google.com/store/apps/details?id=com.viber.voip. [Accessed 8 Feb. 2017].
[69] Vmware Workstation Player 12. [online]. Available at: https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0. [Accessed 8 Feb. 2017].
[70] Viber for Windows. [online]. Available at: https://www.viber.com/en/products/windows. [Accessed 8 Feb. 2017].
[71] DB Browser for SQLite. [online]. Available at: http://sqlitebrowser.org. [Accessed 8 Feb. 2017].
[72] Sync.me. Caller ID and Phone Number Search. [Online]. Available at: https://sync.me. [Accessed 8 Feb. 2017].
[73] Truecaller. Phone Number Search | Truecaller. [Online]. Available at: https://www.truecaller.com. [Accessed 8 Feb. 2017].
[74] Tor. Tor – Anonymity Online. [online]. Available at: https://www.torproject.org. [Accessed 8 Feb. 2017].

[75] Heather Clancy (2013). Yearning for a unified contact list? Sync.Me wants your number. [online]. Available at: http://www.zdnet.com/article/yearning-for-a-unified-contact-list-sync-me-wants-your-number. [Accessed 8 Feb. 2017].

[76] Loie Favre (2014). HOW TO SYNC CONTACT PHOTOS FROM FACEBOOK. [online]. Available at: https://www.androidpit.com/how-to-sync-contact-photos-from-facebook. [Accessed 8 Feb. 2017].

[77] Truecaller: Caller ID & Dialer. [online] Available at: https://play.google.com/store/apps/details?id=com.truecaller. [Accessed 8 Feb. 2017].

[78] Google 2011. Google Image Search API (Deprecated). [online]. Available at: https://developers.google.com/image-search/v1/jsondevguide. [Accessed 9 Feb. 2017].

[79] Google 2016. What is Google Custom Search. [online]. Available at: https://developers.google.com/custom-search/json-api/v1/overview. [Accessed 9 Feb. 2017].

[80] GreekPhone. Lexicon Software GreekPhones. [online]. Available at: http://www.greekphones.gr. [Accessed 9 Feb. 2017].

[81] Kaspersky Labs. What is a Trojan Virus? [online]. Available at: https://usa.kaspersky.com/internet-security-center/threats/trojans#.WKFy8lOLRaQ. [Accessed 13 Feb. 2017].

[82] Stone-Gross (2013), Stels Android Trojan Malware Analysis [online]. Available at : https://www.secureworks.com/research/stels-android-trojan-malware-analysis. [Accessed 13 Feb. 2017].

[83] Cara McGoogan (2016), The Telegraph, What is a DDoS attack? And could my computer be a weapon? [online]. Available at: http://www.telegraph.co.uk/technology/0/what-is-a-ddos-attack-and-could-my-computer-be-a-weapon. [Accessed 13 Feb. 2017].

[84] Margaret Rouse (2016). Spyware. [online]. Available at: http://searchsecurity.techtarget.com/definition/spyware. [Accessed 13 Feb. 2017].

[85] Brook Chris (2016). ASACUB TRANSITIONS FROM SPYWARE TO BANKING MALWARE. [online]. Available at: https://threatpost.com/asacub-transitions-from-spyware-to-banking-malware/115961. [Accessed 13 Feb. 2017].

[86] BullGuard. Mobile botnets taking over smartphones. [online]. Available at: http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-botnets.aspx. [Accessed 13 Feb. 2017].

[87] Kaspersky Lab Report: Financial cyberthreats in 2014. (2015). 1st ed. [ebook] Kaspersky Lab, pp.21-31. Available at: https://securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf [Accessed 13 Feb. 2017].

[88] Cybersecurity (2015). SMS υψηλής χρέωσης από την Πολωνία. [online]. Available at: http://www.cybersecurity.gr/poland-sms-high-cost-facebook. [Accessed 13 Feb. 2017].

[89] ESET (2012). Threat Trends for 2013: Growth of Mobile Malware; Botnets; Cloud and Leaks. [online]. Available at: https://www.eset.com/int/about/newsroom/announcements/eset-threat-trends-for-2013-growth-of-mobile-malware-botnets-cloud-and-leaks. [Accessed 13 Feb. 2017].

[90] Barth-Jones, D. C. (2015). The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy

Protections, Then and Now. [online] Available at: http://papers.ssrn.com/abstract=2076397. [Accessed 13 Feb. 2017].

[91] Narayanan, A. a. S., V. (2008). Robust De-anonymization of Large Sparse Datasets Paper presented at the IEEE Symposium on Security and Privacy, 2008, Oakland, CA. [online]. Available at: http://arxiv.org/pdf/cs/0610105.pdf. [Accessed 13 Feb. 2017].

[92] El Emam, K., & Dankar, F. K. (2008). Protecting Privacy Using k-Anonymity (Vol. 15).

[93] Gallagher R. (2013). The Guardian. Software that tracks people on social media created by defence firm. [online]. Available at: https://www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence. [Accessed 14 Feb. 2017].

[94] TermsFeed. Privacy Policy for mobile apps. [online] Available at: https://termsfeed.com/blog/privacy-policy-mobile-apps. [Accessed 16 Feb. 2017].

[95] Google Play (c). Privacy and Security. [online] Available at: https://play.google.com/about/privacy-security. [Accessed 16 Feb. 2017].

[96] Pew Research Center (2015). Google Play Store Apps Permissions. [online] Available at: http://www.pewinternet.org/interactives/apps-permissions. [Accessed 16 Feb. 2017].

[97] Statista 2017. Number of available applications in the Google Play Store from December 2009 to December 2016. [online]. Available at: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store. [Accessed 16 Feb. 2017].

[98] Android-market-api. An open-source API for the Android Market. [online]. Available at: https://code.google.com/archive/p/android-market-api. [Accessed 16 Feb. 2017].

[99] TOS;DR (2012). Terms Of Service Didn't Read. [online]. Available at: https://tosdr.org. [Accessed 3 Mar. 2017].

[100] Richard, W. and Chow, M. (2012). Android Permissions. 1st ed. [ebook] Medford: Tufts University, p.9. Available at: http://www.cs.tufts.edu/comp/116/archive/wrichard.pdf [Accessed 22 Mar. 2017].

8

ΠΑΡΑΡΤΗΜΑ

8.1 Android Manifest Data Set

Permission
ACCESS ALL DOWNLOADS
ACCESS BLUETOOTH SHARE
ACCESS CHECKIN PROPERTIES
ACCESS COARSE LOCATION
ACCESS DOWNLOAD MANAGER
ACCESS DRM
ACCESS FINE LOCATION
ACCESS LOCATION EXTRA COMMANDS
ACCESS MOCK LOCATION
ACCESS NETWORK STATE
ACCESS PROVIDER
ACCESS SURFACE FLINGER
ACCESS WIFI STATE
ACCOUNT MANAGER
ADD VOICEMAIL
AUTHENTICATE ACCOUNTS
BATTERY STATS
BIND APPWIDGET
BIND DEVICE ADMIN
BIND INPUT METHOD
BIND REMOTEVIEWS
BIND TEXT SERVICE
BIND VPN SERVICE
BIND WALLPAPER
BLUETOOTH ADMIN
BLUETOOTH
BRICK

BROADCAST PACKAGE REMOVED
BROADCAST SMS
BROADCAST STICKY
BROADCAST WAP PUSH
CALL PHONE
CALL PRIVILEGED
CAMERA
CHANGE COMPONENT ENABLED STATE
CHANGE CONFIGURATION
CHANGE NETWORK STATE
CHANGE WIFI MULTICAST STATE
CHANGE WIFI STATE
CLEAR APP CACHE
CLEAR APP USER DATA
CONTROL LOCATION UPDATES
DELETE CACHE FILES
DELETE PACKAGES
DEVICE POWER
DIAGNOSTIC
DISABLE KEYGUARD
DUMP
EXPAND STATUS BAR
FACTORY TEST
FLASHLIGHT
FORCE BACK
FORCE STOP PACKAGES
GET ACCOUNTS
GET PACKAGE SIZE
GET TASKS
GLOBAL SEARCH CONTROL
GLOBAL SEARCH
HARDWARE TEST
INJECT EVENTS
INSTALL DRM
INSTALL LOCATION PROVIDER
INSTALL PACKAGES
INTERNAL SYSTEM WINDOW
INTERNET
KILL BACKGROUND PROCESSES
MANAGE ACCOUNTS
MANAGE APP TOKENS
MASTER CLEAR
MODIFY AUDIO SETTINGS
MODIFY PHONE STATE
MOUNT FORMAT FILESYSTEMS

MOUNT UNMOUNT FILESYSTEMS
NFC
PACKAGE USAGE STATS
PERSISTENT ACTIVITY
PROCESS OUTGOING CALLS
READ CALENDAR
READ CONTACTS
READ FRAME BUFFER
READ HISTORY BOOKMARKS
READ INPUT STATE
READ LOGS
READ PHONE STATE
READ PROFILE
READ SMS
READ SOCIAL STREAM
READ SYNC SETTINGS
READ SYNC STATS
REBOOT
RECEIVE BOOT COMPLETED
RECEIVE MMS
RECEIVE SMS
RECEIVE WAP PUSH
RECORD AUDIO
REORDER TASKS
RESTART PACKAGES
SEND DOWNLOAD COMPLETED INTENTS
SEND SMS
SET ACTIVITY WATCHER
SET ALARM
SET ALWAYS FINISH
SET ANIMATION SCALE
SET DEBUG APP
SET ORIENTATION
SET POINTER SPEED
SET PREFERRED APPLICATIONS
SET PROCESS LIMIT
SET TIME ZONE
SET TIME
SET WALLPAPER HINTS
SET WALLPAPER
SIGNAL PERSISTENT PROCESSES
STATUS BAR SERVICE
STATUS BAR
STOP APP SWITCHES
SUBSCRIBED FEEDS READ

SUBSCRIBED FEEDS WRITE
SYSTEM ALERT WINDOW
UPDATE DEVICE STATS
USE CREDENTIALS
USE SIP
VIBRATE
WAKE LOCK
WRITE APN SETTINGS
WRITE CALENDAR
WRITE CONTACTS
WRITE EXTERNAL STORAGE
WRITE GSERVICES
WRITE HISTORY BOOKMARKS
WRITE PROFILE
WRITE SECURE SETTINGS
WRITE SETTINGS
WRITE SMS
WRITE SOCIAL STREAM
WRITE SYNC SETTINGS
WRITE USER DICTIONARY

8.2 Google Play Permissions Data Set

S/N	Permission	Description	Allows access to:	# of Apps using it*	% of Apps using it*
1	Full network access	Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet so this permission is not required to send data to the internet.	Hardware	859684	82.56%
2	View network connections	Allows the app to view information about network connections such as which networks exist and are connected.	Hardware	717054	68.86%
3	Test access to protected storage	Allows the app to test a permission for USB storage that will be available on future devices. Allows the app	Hardware	565705	54.32%

		to test a permission for the SD card that will be available on future devices			
4	Modify or delete the contents of your USB storage	Allows the app to write to the USB storage. Allows the app to write to the SD card.	User Info	563181	54.08%
5	Read phone status and identity	Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs whether a call is active and the remote number connected by a call.	User Info	364009	34.96%
6	Prevent device from sleeping	Allows the app to prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.	Hardware	280802	26.97%
7	Precise location GPS and network_based	Allows the app to get your precise location using the Global Positioning System GPS or network location sources such as cell towers and Wi_Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are and may consume additional battery power.	User Info	247420	23.76%
8	View Wi_Fi connections	Allows the app to view information about Wi_Fi networking such as whether Wi_Fi is enabled and name of connected Wi_Fi devices.	User Info	235411	22.61%

9	Control vibration	Allows the app to control the vibrator.	Hardware	221196	21.24%
10	Approximate location network_based	Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi_Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.	User Info	217304	20.87%
11	Receive data from internet	Allows apps to accept cloud to device messages sent by the apps service. Using this service will incur data usage. Malicious apps could cause excess data usage.	Hardware	166497	15.99%
12	Find accounts on the device	Allows the app to get the list of accounts known by the device. This may include any accounts created by applications you have installed. Allows the app to get the list of accounts known by the phone. This may include any accounts created by applications you have installed.	User Info	163183	15.67%
13	Take pictures and videos	Allows the app to take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation	User Info	125126	12.02%
14	Run at startup	Allows the app to have itself started as soon as the system has finished booting. This can make	Hardware	95700	9.19%

		it take longer to start the tablet and allow the app to slow down the overall tablet by always running. Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the phone and allow the app to slow down the overall phone by always running.			
15	Directly call phone numbers	Allows the app to call any phone number including emergency numbers without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services	User Info	84493	8.11%
16	Read your contacts	Allows the app to read data about your contacts stored on your tablet including the frequency with which youve called emailed or communicated in other ways with specific individuals. This permission allows apps to save your contact data and malicious apps may share contact data without your knowledge. Allows the app to read data about your contacts stored on your phone including the frequency with which youve called emailed or communicated in other ways with specific individuals. This permission allows apps to save your contact data and malicious apps may share contact data	User Info	64700	6.21%

		without your knowledge.			
17	Record audio	Allows the app to record audio with the microphone. This permission allows the app to record audio at any time without your confirmation	User Info	63618	6.11%
18	Retrieve running apps	Allows the app to retrieve information about currently and recently running tasks. This may allow the app to discover information about which applications are used on the device.	User Info	61569	5.91%
19	Read Google service configuration	Allows this app to read Google service configuration data.	Hardware	47408	4.55%
20	Read call log	Allows the app to read your tablets call log including data about incoming and outgoing calls. This permission allows apps to save your call log data and malicious apps may share call log data without your knowledge. Allows the app to read your phones call log including data about incoming and outgoing calls. This permission allows apps to save your call log data and malicious apps may share call log data without your knowledge.	User Info	43106	4.14%
21	Google Play license check	Can check if you have a license for this app from Google Play	Hardware	42449	4.14%
22	Send SMS messages	Allows the app to send SMS messages. This may result in	User Info	38567	3.70%

		unexpected charges. Malicious apps may cost you money by sending messages without your confirmation.			
23	Access extra location provider commands	Allows the app to access extra location provider commands. This may allow the app to to interfere with the operation of the GPS or other location sources.	User Info	38135	3.66%
24	Set wallpaper	Allows the app to set the system wallpaper.	Hardware	36862	3.54%
25	Modify your contacts	Allows the app to modify the data about your contacts stored on your phone including the frequency with wich youve called emailed or communicated in other ways with specific contacts. This permission allows apps to delete contact data.	User Info	34976	3.36%
26	Modify system settings	Allows the app to modify the system settings data. Malicious apps may corrupt your systems configuration.	Hardware	34138	3.28%
27	Change your audio settings	Allows the app to modify global audio settings such as volume and which speaker is used for output.	Hardware	30943	2.97%
28	Draw over other apps	Allows the app to draw on top of other applications or parts of the user interface. They may interfere with your use of the interface in any application or change what you think you are seeing in other applications.	Hardware	30099	2.89%
29	Connect and disconnect from Wi_Fi	Allows the app to connect to and	Hardware	29227	2.81%

		discconect from Wi_Fi access points and to make changes to device configuration for Wi_Fi networks.			
30	Install shortcuts	Allows an appliaction to add Homescreen shortcuts without user intervention.	Hardware	29178	2.80%
31	Pair with Bluetooth devices	Allows the app to view the configuration of the Bluetooth on the phone and to make and accept connections with paired devices.	Hardware	28345	2.72%
32	Send sticky broadcast	Allows the app to send sticky broadcasts which remain after the broadcast ends. Excessive use may make the tablet slow or unstable by causing it to use too much memory. Allows the app to send sticky broadcasts which remain after the broadcast ends. Excessive use may make the phone slow or unstable by causing it to use too much memory.	Hardware	25436	2.44%
33	Receive text messages SMS	Allows the app to receive and process SMS messages. This means the app could monitor or delete messages sent to your device without showing them to you.	User Info	24971	2.40%
34	Write call log	Allows the app to modify your phones call log including data about incoming and outgoing calls. Malicious apps may use this to erase or modify your call log.	User Info	25044	2.40%

35	Access Bluetooth settings	Allows the app to configure the local Bluetooth phone and to discover and pair with remote devices	Hardware	21733	2.09%
36	Control flashlight	Allows the app to control the flashlight.	Hardware	21291	2.04%
37	Disable your screen lock	Allows the app to disable the keylock and any associated password security. For example the phone disables the keylock when receiving and incoming phone call then re_enables the keylock when the call is finished.	Hardware	20510	1.97%
38	Use accounts on the device	Allows the app to request authentication tokens.	User Info	19531	1.88%
39	Mock location sources for testing	Create mock location sources for testing or install a new location provider. This allows the app to override the location and/or status returned by other location sources such as GPS or location providers.	User Info	19524	1.87%
40	Read sensitive log data	Allows the app to read from the systems various log files. This allows it to discover general information about what you are doing with the device potentially including personal or private information. Allows the app to read from the systems various log files. This allows it to discover general information about what you are doing with the phone potentially	User Info	19014	1.83%

		including personal or private information.			
41	Close other apps	Allows the app to end background processes of other apps. This may cause other apps to stop running.	Hardware	16126	1.55%
42	Read calendar events plus confidential information	Allows the app to read all calendar events stored on your device including those of friends or co_workers. This may allow the app to share or save your calendar data regardless of confidentiality or sensitivity. Allows the app to read all calendar events stored on your phone including those of friends or co_workers. This may allow the app to share or save your calendar data regardless of confidentiality or sensitivity.	User Info	18567	1.78%
43	Read your web bookmarks and history	Allows the app to read the history of all URLs that the Browser has visited and all of the Browsers booksmarks. Note: this permission may not be enforeced by third_party browsers or other applications with web browsing capabilities.	User Info	17787	1.71%
44	Add or modify calendar events and send email to guests without owners knowledge	Allows the app to add remove change events that you can modify on your tablet includbookmarksing those of friends or co_workers. This may allow the app to send messages that appear to come from calendar owners or modify	User Info	17279	1.66%

		events without the owners knowledge. Allows the app to add remove change events that you can modify on your phone including those of friends or co_workers. This may allow the app to send messages that appear to come from calendar owners or modify events without the owners knowledge.			
45	Change system display settings	Allows the app to change the current configuration such as the locale or overall font size.	Hardware	14772	1.42%
46	Access USB storage filesystem	Allows the app to mount and unmount filesystems for removable storage.	Hardware	13579	1.30%
47	Control near field communication	Allows the app to communicate with near field communication NFC tags cards and readers.	User Info	13000	1.25%
48	Change network connectivity	Allows the app to change the state of network connectivity.	Hardware	12296	1.18%
49	Read your text messages SMS Or MMS	Allows the app to read SMS messages stored on your tablet or SIM card. This allows the app to read all SMS messages regardless of content or confidentiality. Allows the app to read SMS messages stored on your phone or SIM card. This allows the app to read all SMS messages regardless of content or confidentiality.	User Info	11554	1.11%

50	Write web bookmarks and history	Allows the app to modify the Browsers history or bookmarks stored on your tablet. This may allow the app to erase or modify Browser data. Note: this permission may note be enforced by third_party browsers or other applications with web browsing capabilities. Allows the app to modify the Browsers history or bookmarks stored on your phone. This may allow the app to erase or modify Browser data. Note: this permission may note be enforced by third_party browsers or other applications with web browsing capabilities	User Info	10199	0.98%
51	Add or remove accounts	Allows the app to perform operations like adding and removing accounts and deleting their password.	User Info	8126	0.78%
52	Reroute outgoing calls	Allows the app to process outgoing calls and change the number to be dialed. This permission allows the app to monitor redirect or prevent outgoing calls.	User Info	7607	0.73%
53	Adjust your wallpaper size	Allows the app to set the system wallpaper size hints.	Hardware	7417	0.70%
54	Edit your text messages SMS Or MMS	Allows the app to write to SMS messages stored on your tablet or SIM card. Malicious apps may delete your messages. Allows the app to write to SMS messages stored on	User Info	7004	0.67%

		your phone or SIM card. Malicious apps may delete your messages.			
55	Uninstall shortcuts	Allows the application to remove Homescreen shortcuts without user intervention.	Hardware	5864	0.56%
56	Create accounts and set passwords	Allows the app to use the account authenticator capabilities of the AccountManager including creating accounts and getting and setting their passwords.	User Info	4784	0.46%
57	Toggle sync on and off	Allows the app to modify the sync settings for an account.	Hardware	4200	0.40%
58	Read sync settings	Allows the app to read the sync settings for an account. For example this can determine whether the People app is synced with an account.	Hardware	3988	0.38%
59	Read home settings and shortcuts	Allows the app to read settings and shortcuts in Home.	Hardware	3755	0.36%
60	Allow Wi_Fi multicast reception	Allows the app to receive packets sent to all devices on a Wi_Fi network using multicast addresses not just your phone. It uses more power than the non_multicast mode.	Hardware	3746	0.36%
61	Enable or disable app components	Allows the app to change whether a component of another app is enabled or not. Malicious apps may use this to disable important tablet capabilities. Care must be used with this permission as it is possible to get app	Hardware	3047	0.29%

		components into an unusable inconsistent or unstable state. Allows the app to change whether a component of another app is enabled or not. Malicious apps may use this to disable important phone capabilities. Care must be used with this permission as it is possible to get app components into an unusable inconsistent or unstable state.			
62	Directly install apps	Allows the app to install new or updated Android packages. Malicious apps may use this to add new apps with arbitrarily powerful permissions.	Hardware	2998	0.29%
63	Delete all app cache data	Allows the app to free tablet storage by deleting files in the cache directories of other applications. This may cause other applications to start up more slowly as they need to re_retrieve their data. Allows the app to free phone storage by deleting files in the cache directories of other applications. This may cause other applications to start up more slowly as they need to re_retrieve their data.	Hardware	2922	0.28%
64	Read battery statistics	Allows an application to read the current low_level battery use data. May allow the application to find out detailed information	Hardware	2868	0.28%

		about which apps you use.			
65	Read your own contact card	Allows the app to read personal profile information stored on your device such as your name and contact information. This means the app can identify you and may send your profile information to others.	User Info	2771	0.27%
66	Modify phone state	Allows the app to control the phone features of the device. An app with this permission can switch networks turn the phone radio on and off and the like without ever notifying you.	Hardware	2667	0.26%
67	Power device on or off	Allows the app to turn the tablet on or off. Allows the app to turn the phone on or off.	Hardware	2349	0.23%
68	Expand/Collapse status bar	Allows the app to expand or collapse the status bar.	Hardware	2295	0.22%
69	Set an alarm	Allows the app to set an alarm in an installed alarm clock app. Some alarm clcok apps may not implement this feature.	Hardware	2175	0.21%
70	Directly call any phone numbers	Allows the app to call any phone number including emergency numbers without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services.	Hardware	2044	0.20%
71	Modify secure system settings	Allows the app to modify the systems secure settings data. Not for use by normal apps.	Hardware	2011	0.19%

72	Download files without notification	Allows the app to download files through the download manager without any notification being shown to the user	Hardware	1955	0.19%
73	Change screen orientation	Allows the app to change the rotation of the screen at any time. Should never be needed for normal apps.	Hardware	1891	0.18%
74	Delete apps	Allows the app to delete Android packages. Malicious apps may use this to delete important apps.	Hardware	1851	0.18%
75	Read sync statistics	Allows an app to read the sync stats for an account including the history of sync events and how much data is synced.	Hardware	1795	0.17%
76	Act as the Accountmanagerservice	Allows the app to make calls to AccountAuthenticators.	Hardware	1706	0.16%
77	Receive text messages MMS	Allows the app to receive and process MMS messages. This means the app could monitor or delete messages sent to your device without showing them to you.	User Info	1612	0.15%
78	Change/Intercept network settings and traffic	Allows the app to change network settings and to intercept and inspect all network traffic for example to change the proxy and port of any APN. Malicious apps may monitor redirect or modify network packets without your knowledge.	Hardware	1340	0.13%
79	Reorder running apps	Allows the app to move tasks to the foreground and background. The	Hardware	1363	0.13%

		app may do this without your input.			
80	Full license to interact across users	Allows all possible interactions across users.	User Info	1292	0.12%
81	Modify battery statistics	Allows the app to modify collected battery statistics. Not for use by normal apps	Hardware	1262	0.12%
82	Enable app debugging	Allows the app to turn on debugging for another app. Malicious apps may use this to kill other apps.	Hardware	1192	0.11%
83	Measure app storage space	Allows the app to retrieve its code data and cache sizes.	Hardware	1140	0.11%
84	Control location update notifications	Allows the app to enable/disable location update notifications from the radio. Not for use by normal apps.	Hardware	1083	0.10%
85	Access download manager	Allows the app to access the download manager and to use it to download files. Malicious apps can use this to disrupt downloads and access private information.	Hardware	1050	0.10%
86	Make/Receive internet calls	Allows the app to use the SIP service to make/receive Internet calls.	Hardware	1019	0.10%
87	Write home settings and shortcuts	Allows the app to change the settings and shortcuts in Home.	Hardware	955	0.09%
88	Make app always run	Allows the app to make parts of itself persistent in memory. This can limit memory available to other apps slowing down the tablet. Allows the app to make parts of itself persistent in memory. This can limit memory available to	Hardware	955	0.09%

		other apps slowing down the phone.			
89	Disable or modify status bar	Allows the app to disable the status bar or add and remove system icons.	Hardware	814	0.08%
90	Choose widgets	Allows the app to tell the system which widgets can be used by which app. An app with this permission can give access to personal data to other apps. Not for use by normal apps.	Hardware	818	0.08%
91	Test hardware	Allows the app to control various peripherals for the purpose of hardware testing.	Hardware	717	0.07%
92	Delete other apps caches	Allows an application to delete cache files.	Hardware	702	0.07%
93	Add words to user_defined dictionary	Allows the app to write new words into the user dictionary.	Hardware	683	0.07%
94	Read terms you added to the dictionary	Allows the app to read all words names and phrases that the user may have stored in the user dictionary.	User Info	677	0.07%
95	Force device reboot	Allows the app to force the device to reboot.	Hardware	590	0.06%
96	Access SurfaceFlinger	Allows application to use SurfaceFlinger low_level features.	Hardware	542	0.05%
97	Access email provider data	Allows this application to access your email database including received messages sent messages usernames and passwords.	User Info	529	0.05%
98	Receive text messages WAP	Allows the app to receive and process WAP messages. This permission includes the ability to monitor or delete messages sent to	User Info	524	0.05%

		you without showing them to you.			
99	Read frame buffer	Allows application to read the content of the frame buffer.	Hardware	521	0.05%
100	Read email attachments	Allows the app to read your email attachments.	User Info	509	0.05%
101	Broadcast data messages to apps	Can broadcast data messages received from the Internet to apps registered to listen for them.	Hardware	507	0.05%
102	View configured accounts	Allows apps to see the usernames email addresses of the Google accounts you have configured.	User Info	465	0.04%
103	Set preferred apps	Allows the app to modify your preferred apps. Malicious apps may silently change the apps that are run spoofing your existing apps to collect private data from you.	User Info	449	0.04%
104		Erase USB storage	Hardware	427	0.04%
105	Bind to a notification listener service	Allows the holder to bind to the top_level interface of a notification listener service. Should never be needed for normal apps.	Hardware	368	0.04%
106	Delete other apps data	Allows an application to clear user data.	Hardware	367	0.04%
107	Bind to a wallpaper	Allows the holder to bind to the top_level interface of a wallpaper. Should never be needed for normal applications.	Hardware	363	0.03%
108	Press keys and control buttons	Allows an application to modify the Google services map. Not for use by normal applications.	Hardware	342	0.03%

109	Access checkin properties	Allows the app read/write access to properties uploaded by the checkin service. Not for use by normal apps.	Hardware	326	0.03%
110	Access all system downloads	Allows the app to view and modify all downloads initiated by any app on the system.	Hardware	321	0.03%
111	Read Gmail	Allows the app to read your Gmail.	User Info	315	0.03%
112	Modify/Delete internal media storage contents	Allows the app to modify the contents of the internal media storage.	Hardware	314	0.03%
113	Send SMS_Received broadcast	Allows the app to broadcast a notification that an SMS message has been received. Malicious apps may use this to forge incoming SMS messages.	Hardware	312	0.03%
114	Set time zone	Allows the app to change the tablets time zone. Allows the app to change the phones time zone.	Hardware	300	0.03%
115	Permission to install a location provider	Create mock location sources for testing. Malicious applications can use this to override the location and/or status returned by the real location and/or status returned by real location sources such as GPS or Network providers or monitor and report your location to an external source.	User Info	266	0.03%
116	Modify the Google services map	Allows the app to modify the Google services map. Not for use by normal apps.	Hardware	253	0.02%
117	Set time	Allows an application to change the phone's clock time.	Hardware	236	0.02%

118	Display unauthorized windows	Allows the app to create windows that are intended to be used by the internal system user interface. Not for use by normal apps.	Hardware	229	0.02%
119	Retrieve system internal state	Allows the app to retrieve internal state of the system. Malicious apps may retrieve a wide variety of private and secure information that they should never normally need.	User Info	224	0.02%
120	Force stop other apps	Allows the app to forcibly stop other apps.	Hardware	213	0.02%
121		Access mail information	Hardware	205	0.02%
122	Modify your own contact card	Allows the app to change or add to personal profile information stored on your device such as your name and contact information. This means the app can identify you and may send your profile information to others.	User Info	200	0.02%
123	Bind to an accessibility service	Allows the holder to bind to the top_level interface of an accessibility service. Should never be needed for normal apps.	Hardware	190	0.02%
124	Force background apps to close	Allows the app to control whether activities are always finished as soon as they go to the background. Never needed for normal apps.	Hardware	175	0.02%
125	Record what you type and actions you take	Allows applications to watch the keys you press even when interacting with another application such as	User Info	173	0.02%

		entering a password. Should never be needed for normal applications.			
126	YouTube	Allows apps to sign in to YouTube using the accounts stored on this Android device.	Hardware	152	0.01%
127	Bind to an input method	Allows the holder to bind to the top_level interface of an input method. Should never be needed for normal apps.	Hardware	151	0.01%
128	Send package removed broadcast	Allows the app to broadcast a notification that an app package has been removed. Malicious apps may use this to kill any other running app.	Hardware	147	0.01%
129	Send download notifications	Allows the app to send notifications about completed downloads. Malicious apps can use this to confuse other apps that download files.	Hardware	145	0.01%
130	Interact with a device admin	Allows the holder to send intents to a device administrator. Should never be needed for normal applications.	Hardware	143	0.01%
131	Monitor and control all app launching	Allows an application to monitor and control how the system launches activities. Malicious applications may completely compromise the system. This permission is only needed for development never for normal use.	Hardware	141	0.01%
132	Read subscribed feeds	Allows the app to get details about the currently synced feeds.	Hardware	141	0.01%

133	Connect and disconnect from WiMAX	Allows the app to determine whether WiMAX is enabled and information about any WiMAX networks that are connected.	Hardware	135	0.01%
134	Modify global animation speed	Allows the app to change the global animation speed faster or slower animations at any time.	Hardware	129	0.01%
135	Write subscribed feeds	Allows the app to modify your currently synced feeds. Malicious apps may change your synced feeds.	Hardware	128	0.01%
136	Interact across users	Allows the app to perform actions across different users on the device. Malicious apps may use this to violate the protection between users.	Hardware	125	0.01%
137	Send Linux signals to apps	Allows the app to request that the supplied signal be sent to all persistent processes.	Hardware	122	0.01%
138	Install DRM content	Allows app to install DRM_protected content.	Hardware	119	0.01%
139	Reset system to factory defaults	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.	Hardware	115	0.01%
140	Read your social stream	Allows the app to access and sync social updates from you and your friends. Be careful when sharing information this allows the app to read communications between you and your friends on social networks regardless of	User Info	112	0.01%

		confidentiality. Note: this permission may not be enforced on all social networks.			
141	Force app to close	Allows an application to force any activity that is in the foreground to close and go back. Should never be needed for normal apps.	Hardware	112	0.01%
142	Read/Write to resources owned by diag	Allows the app to read and write to any resource owned by the diag group; for example files in /dev. This could potentially affect system stability and security. This should be ONLY be used for hardware_specific diagnostics by the manufacturer or operator.	Hardware	106	0.01%
143	Limit number Of running processes	Allows the app to control the maximum number of processes that will run. Never needed for normal apps.	Hardware	103	0.01%
144	Write to your social stream	Allows the app to display social updates from your friends. Be careful when sharing information this allows the app to produce messages that may appear to come from a friend. Note: this permission may not be enforced on all social networks.	User Info	100	0.01%
145	Send WAP_Push_Received broadcast	Allows the app to broadcast a notification that a WAP PUSH message has been received. Malicious apps may use this to forge MMS message receipt or to silently replace the content of	Hardware	100	0.01%

		any webpage with malicious variants			
146	Manage app tokens	Allows applications to create and manage their own tokens bypassing their normal Z_ordering. Should never be needed for normal apps.	Hardware	95	0.01%
147	Modify Gmail	Allows the app to modify your Gmail including sending and deleting mail.	User Info	94	0.01%
148	Change WiMAX State	Allows the app to connect the tablet to and disconnect the tablet from WiMAX networks. Allows the app to connect the phone to and disconnect the phone from WiMAX networks.	Hardware	93	0.01%
149	Access the cache filesystem	Allows an application to read and write the cache filesystem.	Hardware	70	0.01%
150	Google Mail	Allows apps to sign in to Google Mail services using the accounts stored on this Android device.	User Info	66	0.01%
151	Control system backup and restore	Allows the application to control the system's back and restore mechanism. Not for use by normal applications.	Hardware	66	0.01%
152	Bind to a widget service	Allows the holder to bind to the top_level interface of a widget service. Should never be needed for normal appliactions.	Hardware	62	0.01%
153	Change background data usage setting	Allows the app to change the background data usage setting.	Hardware	61	0.01%
154	Advanced download manager functions	Allows the app to access the download manager's advanced functions. Malicious	Hardware	60	0.01%

		apps can use this to disrupt downloads and access private information.			
155		Modify google service configuration	Hardware	53	0.01%
156	Google Docs	Allows apps to sign in to Google Docs using the accounts stored on this Android device.	User Info	49	0.00%
157	Google Spreadsheets	Allows apps to sign in to Google Spreadsheets using the accounts stored on this Android device.	User Info	48	0.00%
158	Get current app info	Allows the holder to retrieve private information about the current application in the foreground of the screen.	Hardware	48	0.00%
159	Modify app ops statistics	Allows the app to modify collected application operation statistics. Not for use by normal apps.	Hardware	44	0.00%
160	Run in factory test mode	Run as low_level manufacturer test allowing complete access to the phone hardware. Only available when phone is running in manufacturer test mode.	Hardware	42	0.00%
161	Add voicemail	Allows the app to add messages to your voicemail inbox.	Hardware	40	0.00%
162	Prevent app switches	Prevents the user from switching to another app.	Hardware	40	0.00%
163	Google Maps	Allows apps to sign in to Google Maps using the accounts stored on this Android device.	User Info	37	0.00%

164	Access DRM content	Allows application to access DRM_protected content.	Hardware	34	0.00%
165	Read instant messages	Allows apps to read data from the Google Talk content provider.	User Info	33	0.00%
166	Update component usage statistics	Allows the app to modify collected component usage statistics. Not for use by normal apps.	Hardware	32	0.00%
167	Manage users	Allows apps to manage users on the device including query creation and deletion.	Hardware	31	0.00%
168	Partial shutdown	Puts the activity manager into a shutdown state. Does not perform a complete shutdown.	Hardware	31	0.00%
169	Permanently disable device	Allows the application to disable the entire phone permanently. This is very dangerous.	Hardware	31	0.00%
170	Send respond_via_message events	Allows the app to send requests to other messaging apps to handle respond_via_message events for incoming calls.	Hardware	28	0.00%
171	Status bar	Allows the application to be the status bar.	Hardware	23	0.00%
172	Send Gmail	Allows the app to send Gmail messages without opening the Gmail app	User Info	20	0.00%
173	Manage preferences and permissions for USB devices	Allows the app to manage preferences and permissions for USB devices.	Hardware	19	0.00%
174	Contacts data in Google accounts	Allows apps to access the contacts and profile information of accounts stored on this Android device.	User Info	19	0.00%

175	Bind to a text service	Allows the holder to bind to the top_level interface of a text servicee.g. SpellCheckerService.	Hardware	18	0.00%
176	Change pointer speed	Allows an application to change the mouse or trackpad pointer speed at any time. Should never be needed for normal applications.	Hardware	15	0.00%
177	Access other Google services	Allows apps to sign in to unspecified Google services using the accounts stored on this Android device.	User Info	15	0.00%
178	Bind to a VPN service	Allows the holder to bind to the top_level interface of a VPN service. Should never be needed for normal applications.	Hardware	13	0.00%
179	Access all voicemails	Allows the app to store and retrieve all voicemails that this device can access.	User Info	11	0.00%
180	Move app resources	Allows an application to move application resources from internal to external media and vice versa.	Hardware	11	0.00%
181		Configure Wi_Fi displays	Hardware	11	0.00%
182	Stop running apps	Allows the app to remove tasks and kill their apps. Malicious apps may disrupt the behavior of other apps.	Hardware	10	0.00%
183	Google Calendar	Allows apps to sign in to Google Calendar using the accounts stored on this Android device.	User Info	9	0.00%
184	Manage network policy	Allows an application to manage network policies and define application specific rules.	Hardware	9	0.00%

185	Read cell broadcast messages	Allows the app to read cell broadcast messages received by your device. Cell broadcast alerts are delivered in some locations to warn you of emergency situations. Malicious apps may interfere with the performance or operation of your device when an emergency cell broadcast is received.	Hardware	6	0.00%
186	Directly start CDMA device setup	Allows the application to start CDMA provisioning. Malicious appliactions may unnecessarily start CDMA provisioning.	Hardware	6	0.00%
187	Change keyboard layout	Allows the app to change the keyboard layout. Should never be needed for normal apps.	Hardware	6	0.00%
188	Access all Google services	Allows apps to sign in to ALL Google services using the accounts stored on this Android device.	User Info	5	0.00%
189	Access Google Photos data	Allows the app to read photo data from Google Photos including account name file names photo IDs locations where photo were taken etc.	User Info	5	0.00%
190	Create internal storage	Allows the app to create internal storage.	Hardware	5	0.00%
191	Google App Engine	Allows apps to sign in to Google App Engine using the accounts stored on this Android device.	User Info	5	0.00%
192	Access external storage of all users	Allows the app to access external storage for all users.	User Info	5	0.00%

193	Get information on internal storage	Allows the app to get information on internal storage.	Hardware	5	0.00%
194	Retrieve details of running apps	Allows the app to retrieve detailed information about currently and recently running tasks. Malicious apps may discover private information about other apps.	Hardware	5	0.00%
195	Modify network usage accounting	Allows modification of how network usage is accounted against applications. Not for use by normal applications.	Hardware	5	0.00%
196		Access serial ports	Hardware	5	0.00%
197	Grant or revoke permissions	Allows an application to grant or revoke specific permissions for it or other appliactions. Malicious applications may use this to access features you have not granted them.	Hardware	5	0.00%
198		Read Google settings	Hardware	4	0.00%
199	Google Finance	Allows apps to sign in to Google Finance using the accounts stored on this Android device.	User Info	4	0.00%
200	Receive emergency broadcasts	Allows the app to receive and process emergency broadcast messages. This permission is only available to system apps.	Hardware	4	0.00%
201	Retrieve app ops statistics	Allows the app to retrieve collected application operation statistics. Not for use by normal apps.	Hardware	4	0.00%
202	Use any media decoder for playback	Allows an application to use any installed	Hardware	4	0.00%

		media decoder to decode for playback.			
203	Access content providers externally	Allows the holder to access content providers from the shell. Should never be needed for normal apps.	Hardware	4	0.00%
204	Access notifications	Allows the app to retrieve examine and clear notifications including those posted by other apps.	Hardware	4	0.00%
205	Start any activity	Allows the app to start any activity regardless of permission protection or exported state.	Hardware	4	0.00%
206		Copy content	Hardware	4	0.00%
207	Discourage automatic device updates	Allows the holder to offer information to the system about when would be a good time for a noninteractive reboot to upgrade the device.	Hardware	4	0.00%
208	FM Radio	Allows the app to access FM radio to listen to programs.	Hardware	3	0.00%
209	Implement MTP protocol	Allows access to the kernel MTP driver to implement the MTP USB protocol.	Hardware	3	0.00%
210	YouTube usernames	Allows apps to see the YouTube usernames associated with the Google accounts stored on this device	User Info	3	0.00%
211	Freeze screen	Allows the application to temporarily freeze the screen for a full_screen transition.	Hardware	3	0.00%
212	Read historical network usage	Allows an application to read historical network usage for specific networks and applications.	Hardware	3	0.00%

213	Control Wi_Fi displays	Allows the app to control low_level features of Wi_Fi displays.	Hardware	3	0.00%
214	Temporary enable accessibility	Allows and application to temporarily enable accessibility on the device. Malicious apps may enable accessibility without user consent.	Hardware	3	0.00%
215	Write instant messages	Allows apps to write data to the Google Talk content provider.	User Info	3	0.00%
216	Destroy internal storage	Allows the app to destroy internal storage.	Hardware	3	0.00%
217		Retrieve window info	Hardware	3	0.00%
218	Retrieve screen content	Allows the app to retrieve the content of the active window. Malicious apps may retrieve the entire window content and examine all its text except passwords.	User Info	3	0.00%
219	Mount/Unmount internal storage	Allows the app to mount/unmount internal storage.	Hardware	3	0.00%
220	Filter events	Allows an application to register an input filter which filters the stream of all user events before they are dispatched. Malicious app may control the system UI without user intervention.	Hardware	3	0.00%
221		Magnify display	Hardware	3	0.00%
222	Exchanges messages and receives sync notifications from Google servers.	Used for server cloud to device messages and for sync notifications. Google Talk uses this service to exchange messages and to synchronize presence status. Malicious apps	Hardware	2	0.00%

		could use this service to transmit excess data.			
223	Picasa Web Albums	Allows apps to sign in to Picasa Web Albums using the accounts stored on this Android device.	User Info	2	0.00%
224	Verify packages	Allows the app to verify a package is installable.	Hardware	2	0.00%
225	Set screen compatibility	Allows the app to control the screen compatibility mode of other applications. Malicious applications may break the behavior of other applications.	Hardware	2	0.00%
226	Rename internal storage	Allows the app to rename internal storage.	Hardware	2	0.00%
227		Modify Google settings	Hardware	2	0.00%
228		Preload results	Hardware	1	0.00%
229	Blogger	Allows apps to sign in to Blogger using the accounts stored on this Android device.	User Info	1	0.00%
230	Google Voice	Allows apps to sign in to Google Voice using the accounts stored on this Android device.	User Info	1	0.00%
231	Google Voice	Permission to write sound search matches	Hardware	1	0.00%
232	Google Voice	Access to passwords for Google accounts	User Info	1	0.00%
233	Google Voice	Bind to a package verifier	Hardware	undefined	1

Ο ανωτέρω πίνακας έχει μεταφορτωθεί από την ιστοσελίδα Pew Research Center (2015)[96]

8.3 Β. Κώδικας

8.3.1 Κώδικας δημιουργίας Dummy Set

```
steps=0
dummyValue=1
for x in range(697xxxx000,697xxxx000):
    with open("phoneNumbersDataSet2.txt", "a") as myfile:
        myfile.write('dummy%s,dummySurname%s,%d \n' % (dummyValue, dummyValue,
x))
        dummyValue += 1
    steps = x%1000
```

```
    if steps == 0:
        print("number : %d"%x)
```

8.3.2 Κώδικας δημιουργίας SQLite Insert

```
steps=0
for x in range(697xxxx001,6979999999):
    with open("phoneFakeDataSet100iik.txt", "a") as myfile:
        myfile.write("insert into Contact (Number,ClientName) Values
('%d','dummy%d');\n"%(x,x))
    steps = x%100000
    if steps == 0:
        print("insert into Contact (Number,ClientName) Values
('%d','dummy%d');"%(x,x))
```