ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ & ΥΠΗΡΕΣΙΕΣ
ΚΑΤΕΥΘΥΝΣΗ:ΠΡΟΗΓΜΕΝΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Διπλωματική εργασία

ΣΤΡΑΤΗΓΙΚΕΣ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΓΙΑ ΤΗΝ ΔΙΑΣΦΑΛΙΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Ελπινίκη Μαρούλη (ΑΜ: ΜΕ1745)

Πειραιάς 2020

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Διπλωματικής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Διπλωματικής μου Εργασίας και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Διπλωματική Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

. . . . . Ελπινίκη Μαρούλη

Περίληψη

Ένας από τους βασικούς κανόνες χρήσης δεδομένων για επιχειρηματικούς σκοπούς είναι τόσο απλός: η ποιότητα των αποφάσεών σας εξαρτάται σε μεγάλο βαθμό από την ποιότητα των δεδομένων σας. Ωστόσο, απλά γνωρίζοντας ότι δεν είναι εξαιρετικά χρήσιμο. Για να έχετε απτά αποτελέσματα, θα πρέπει να μετρήσετε την ποιότητα των δεδομένων σας και να δράσετε σε αυτές τις μετρήσεις για να το βελτιώσετε. Εδώ, ρίχνουμε λίγο φως στα περίπλοκα ζητήματα ποιότητας δεδομένων και μοιραζόμαστε συμβουλές για το πώς να υπερέχουν στην επίλυσή τους.

Abstract

One of the crucial rules of using data for business purposes is as simple as this: the quality of your decisions strongly depends on the quality of your data. However, simply knowing it isn't extremely helpful. To get tangible results, you should measure the quality of your data and act on these measurements to improve it. Here, we throw some light on complicated data quality issues and share tips on how to excel in resolving them.

Περιεχόμενα

Περιεχόμενα Εικόνων

Περιεχόμενα Πινάκων

Εισαγωγή

Βάζουμε ολοένα και περισσότερη εμπιστοσύνη στις εφαρμογές που χρησιμοποιούμε και για την διευκόλυνση μας κυρίως σε εφαρμογές κινητών συσκευών.Τις χρησιμοποιούμε για το ηλεκτρονικό εμπόριο και τις τράπεζες, είτε μέσω ενός πρόγραμμα περιήγησης ή με εξειδικευμένες εφαρμογές. Τέτοιες εφαρμογές διατηρούν διαπιστευτήρια υψηλής αξίας και επεξεργάζονται ευαίσθητα δεδομένα που πρέπει να προστατεύονται.

Παρόλα αυτά, οι κινητές συσκευές είναι αναξιόπιστες. Ενώ καταρχήν προσπαθούν να είναι πιο ασφαλή από τα επιτραπέζια μηχανήματα(π.χ. παρεμποδίζοντας τα τροποποιημένα OS από την εκκίνηση, χρησιμοποιώντας ασφαλέστερες γλώσσες ή με μηχανισμούς sandboxing), στην πράξη εξακολουθούν να είναι γεμάτες με τρωτά σημεία.

Τα λειτουργικά συστήματα για κινητές συσκευές είναι τόσο περίπλοκα όσο τα παραδοσιακά λειτουργικά συστήματα. Το isolation και το sandboxing που παρέχετε από το λειτουργικό σύστημα είναι συνήθως σπασμένο (π.χ Apple iOS jail-breaking).Οι εταιρίες που δημιουργούν OS για κινητές συσκευές συχνά μοιράζονται κώδικα με λειτουργικά συστήματα όπως το GNU / Linux, αλλά συχνά καθυστερούν στην εφαρμογή των διορθώσεων ασφαλείας, πράγμα που σημαίνει ότι οι επιτιθέμενοι πρέπει να κοιτάξουν μόνο στα πρόσφατα patches για να εντοπίσουν τρωτά σημεία στον κώδικα. Ως εκ τούτου, υπάρχει ανάγκη για απομόνωση και πρότυπα ασφαλείας που εκτίθενται στους προγραμματιστές με τέτοιο τρόπο ώστε να μην χρειάζεται να εμπιστεύονται το host OS.Η ζήτηση για κινητές εφαρμογές με ισχυρότερες απαιτήσεις ασφάλειας έχει οδηγήσει σε add-on hardware με ισχυρότερη ασφάλεια.

Το σημερινό οικοσύστημα υλικού και λογισμικού κινητών συσκευών αποτελείται από πολλαπλούς stake-holders, οι οποίοι περιλαμβάνουν κυρίως τον κατασκευαστή, τον πάροχο τηλεπικοινωνιών τους προγραμματιστές εφαρμογών και τον κάτοχο της συσκευής (τον χρήστη). Οι κατασκευαστές τυπικά εξυπηρετούν επίσης το ρόλο του platform integrator, προσαρμόζοντας τη συσκευή με πρόσθετα χαρακτηριστικά και branding (συνήθως μέσω firmware ή custom εφαρμογές). Μέχρι σήμερα, οι

ιδιότητες ασφαλείας που είναι επιθυμητές απο τους προγραμματιστές είναι δευτερεύουσες ανησυχίες για τους κατασκευαστές. Οι συμπράξεις μεταξύ των κατασκευαστών έχουν οδηγήσει σε ένα μονολιθικό μοντέλο εμπιστοσύνης στα βασικά πρωτόκολλα ασφάλειας υλικού. Τα πάντα "μέσα" είναι φαινομενικά αξιόπιστα.

Οι περισσότεροι χρήστες εμπιστεύονται σε ένα βαθμό τα καταστήματα εφαρμογών όπως το Google Play,Apple Store.Είναι όμως σχεδόν απίθανο για έναν χρήστη να αισθάνεται σίγουρος για την ποιότητα των εφαρμογών που εγκαθιστά στις συσκευές του όσων αφορά την ασφάλεια και την προστασία των προσωπικών του δεδομένων.Ενδεικτικά αναφέρουμε ότι πολλές φορές για να ενεργοποιηθούν πολλές εφαρμογές ζητούν πρόσβαση στην τρέχουσα τοποθεσία μας είτε συλλέγουν πληροφορίες τις οποίες και πωλούν σε εταιρείες μάρκετινγκ.Σύμφωνα με έρευνες ακόμα και δημοφιλείς εφαρμογές εκμεταλεύονται την πρόσβαση τους σε πόρους και υποκλέπτουν προσωπικές πληροφορίες.Με βάση τα παραπάνω η μελέτη της αξιοπιστίας των εφαρμογών και η βαθμονόμηση μπορεί να βοηθήσει τους χρήστες στην διασφάλιση του απορρήτου των δεδομένων τους.

Το πρόβλημα

Τα smartphones έχουν γίνει οι πιο χρησιμοποιούμενες ηλεκτρονικές συσκευές. Κάνουν τις περισσότερες λειτουργίες των επιτραπέζιων υπολογιστών, επιτρέποντας διάφορες χρήσιμες εφαρμογές που ταιριάζουν στις ανάγκες των χρηστών. Επομένως, αντί του χειριστή, ο χρήστης έχει γίνει ο νούμερο ένα ελεγκτής της συσκευής και των εφαρμογών της και έτσι η αξιοπιστία της γίνεται μια αναδυόμενη ανάγκη.

Όντας χρήστες έξυπνων κινητών συσκευών συχνά έχουμε παρατηρήσει ότι απλές εφαρμογές μας ζητάνε πρόσβαση σε προσωπικά μας δεδομένα τα οποία δεν θεωρούμε ότι είναι απαραίτητα για την εύρυθμη λειτουργία της εκάστωτε συσκευής.

Η αξιολόγηση της αξιοπιστίας δεν είναι ασήμαντη λόγω πολλών παραγόντων, όπως η σύνθετη και δυναμική φύση των εφαρμογών, ο μεγάλος αριθμός δεδομένων που εμπλέκονται στην αξιοπιστία και την υποκειμενική έννοια της εμπιστοσύνης.Το ζήτημα εμπιστοσύνης στα περιβάλλοντα εφαρμογών είναι πολύ πιο πέρα από τις ιδιότητες που σχετίζονται με μια παραδοσιακή σχέση εμπιστοσύνης μεταξύ των ανθρώπων. Έτσι, η δημιουργία εμπιστοσύνης και η δημιουργία αξιόπιστων υπηρεσιών αποτελεί πρόκληση. Η εμπιστοσύνη είναι μια έννοια πολύ δύσκολο να προσδιοριστεί και να εκτιμηθεί με ακρίβεια, κυρίως επειδή είναι υποκειμενική, δυναμική, εξαρτώμενη από το περιβάλλον, μη συμμετρική και μερικώς μεταβατική. Αν και ορίζεται διαφορετικά σε διαφορετικούς τομείς, ένας από τους κοινούς κύριους στόχους σε όλους τους ορισμούς είναι η ακριβής αξιολόγηση του επιπέδου εμπιστοσύνης ως ισχυρής βάσης για λήψη απόφασης(π.χ. προσαρμογή συστήματος), που αποδεικνύεται πολύ περίπλοκο πρόβλημα. Το πρώτο και το πιο σημαντικό βήμα για την οικοδόμηση της εμπιστοσύνης είναι να βρούμε έναν τρόπο για να αξιολογήσουμε με ακρίβεια την αξιοπιστία.

Σκοπός και αντικειμενικοί στόχοι

Η αξιοπιστία είναι το πιο σημαντικό ζητούμενο χαρακτηριστικό κάθε λογισμικού.Άτυπα, είναι το μέτρο του πόσο καλά νομίζουν οι χρήστες του συστήματος ότι τους παρέχει τις υπηρεσίες που απαιτούν. Συνήθως ορίζεται ως η πιθανότητα για ελεύθερη από αποτυχίες λειτουργία για καθορισμένο χρόνο σε ένα καθορισμένο πλαίσιο για ένα δεδομένο σκοπό.

Σκοπός της παρούσας εργασίας είναι να αναδείξει τα τρωτά σημεία και να επιδήξει την ανάγκη ανάπτυξης ασφαλών και αξιόπιστων εφαρμογών,με βάση την αξιολόγηση των σχετικών ιδιοτήτων, που να παρέχουν προστασία δεδομένων ιδιωτικού απορρήτου, ασφάλεια, δικαιοσύνη και διαφάνεια.

Μία σημαντική πρόκληση όσον αφορά τη διαχείριση δεδομένων αξιοπιστίας υπό το πρίσμα των πολλαπλών ιδιοτήτων που εξετάζονται στην παρούσα εργασία είναι η ικανοποίηση των λειτουργικών απαιτήσεων και των παραδοσιακών ιδιοτήτων αξιοπιστίας και συνέπειας, ενώ παράλληλα να τηρούνται οι κανονισμοί και ειδικότερα ο γενικός κανονισμός της ΕΕ για την προστασία των δεδομένων GDPR).

Το GDPR στοχεύει στην προστασία των δικαιωμάτων των υποκειμένων των δεδομένων σύμφωνα με τις ιδιότητες όπως η προστασία της ιδιωτικής ζωής, η ασφάλεια, η δικαιοσύνη και η διαφάνεια.Η σχέση μεταξύ ορισμένων από αυτές τις ιδιότητες οδηγεί σε αντικρουόμενους στόχους των μέσων για την επίτευξη καθεμίας από αυτές: π.χ. οι πληροφορίες που πρέπει να διατηρηθούν για τη διαφάνεια έρχονται σε σύγκρουση με το δικαίωμα των υποκειμένων να ξεχαστούν.

Δομή Εργασίας

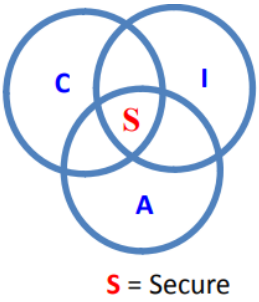
Σήμερα τα trending smart phones και άλλες φορητές συσκευές αυξάνονται ραγδαία. Τα έξυπνα τηλέφωνα δεν χρησιμοποιούνται μόνο ως υπολογιστές και μέσω επικοινωνίας αλλά και σαν έξυπνες για την ανίχνευση των δεδομένων.Όντας χρήστες έξυπνων κινητών συσκευών συχνά έχουμε παρατηρήσει ότι απλές εφαρμογές μας ζητάνε πρόσβαση σε προσωπικό μας δεδομένα τα οποία δεν θεωρούμε ότι είναι απαραίτητα για την εύρυθμη λειτουργία της εκάστωτε συσκευής.

Στην παρούσα εργασία έχοντας ως στόχο να αξιολογήσουμε τις στρατηγικές σχεδιασμού των εφαρμογών κινητών συσκευών για να διασφαλίσουμε το απόρρητο των δεδομένων θα αναφερθούμε στο πρώτο κεφάλιο αρχικά στα χαρακτηριστικά με βάση τα οποία θα στηριχτεί η αξιολόγηση (trustworthy properties) και έπειτα αφου κατηγοριοποιήσουμε σύνηθες εφαρμογές που οι περισσότεροι έχουμε εγκαταστήσει στις συσκεύες μας θα ορίσουμε την αναγκαιότητα των trustworthy properties ανα κατηγορία εφαρμογών σε έναν πίνακα.

Στο τρίτο κεφάλαιο θα ελένξουμε τους μηχανισμούς που χρησιμοποιούνται για την διασφάλιση του παραπάνω πίνακα.Στην συνέχεια στο τέταρτο κεφάλαιο θα αναφερθούμε στην ανάγκη της προστασίας των προσωπικών δεδομένων απο τον σχεδιασμό τψν εφαρμογών.Στο πέμπτο κεφάλαιο θα αναφερθούμε στα συμπεράσματα μας καθώς και τις προτάσεις μας για την βελτίωση της ιδιωτικότητας και της χρηστικότητας.

1.Κεφάλαιο 1 Μετρικές

Πολλές ιδιότητες μπορούν να ληφθούν υπόψη κατά την ανάλυση της αξιοπιστίας ενός συστήματος, συμπεριλαμβανομένης της ασφάλειας, της ιδιωτικότητας, της συνοχής, της απομόνωσης, της σταθερότητας, της αμεροληψίας, της διαφάνειας, της αξιοπιστίας, της ποιότητας των δεδομένων, του κόστους, της συμμόρφωσης, της χρηστικότητας, της ορθότητας, της πολυπλοκότητας, μεταξύ άλλων. Όλες αυτές έχουν και άλλα υπο-στοιχεία που διευρύνουν πολύ τις δυνατότητες που πρέπει να αντιμετωπιστούν.Μεταξύ όλων των πιθανών ιδιοτήτων που βρέθηκαν στη βιβλιογραφία, προσπαθήσαμε να προσδιορίσουμε τις πιο ενδιαφέρουσες από γενική άποψη και να είμαστε όσο το δυνατόν πιο περιεκτικοί λαμβάνοντας προφανώς υπόψη τις ιδιαιτερότητες της εργασίας.Για τον σκοπό αυτό σε αυτήν την ενότητα αναλύουμε τις ιδιότητες αξιοπιστίας που αναφέρθηκαν στο έργο ATMOSPHERE(Adaptive,Trustworthy, Manageable,Orchestrated, Secure, Privacy-assuring, Hybrid Ecosystem for REsilient Cloud Computing.)



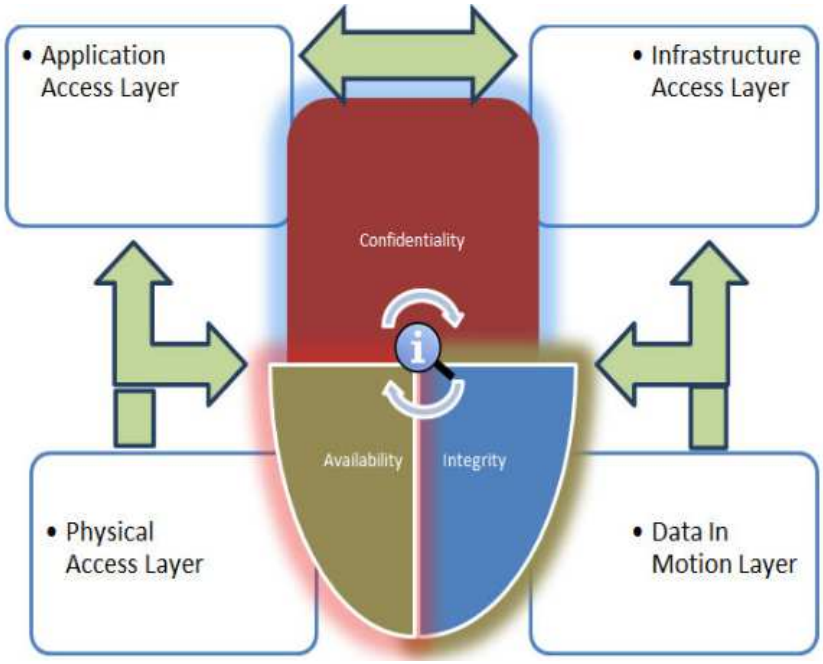
Εικόνα 1 Τριάδα C.I.A

1.1 Ασφάλεια

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, γνωστή και ως τριάδα της CIA, είναι ένα μοντέλο που έχει σχεδιαστεί για να καθοδηγεί πολιτικές για την ασφάλεια των πληροφοριών σε έναν οργανισμό. Το μοντέλο αναφέρεται επίσης μερικές φορές ως τριάδα AIC (διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα), προκειμένου να αποφευχθεί σύγχυση με την Κεντρική Υπηρεσία Πληροφοριών. Τα στοιχεία της τριάδας θεωρούνται τα τρία πιο κρίσιμα συστατικά της ασφάλειας.

Σε αυτό το πλαίσιο, η εμπιστευτικότητα είναι ένα σύνολο κανόνων που περιορίζει την πρόσβαση στις πληροφορίες, η ακεραιότητα είναι η διαβεβαίωση ότι οι

πληροφορίες είναι αξιόπιστες και ακριβείς και η διαθεσιμότητα αποτελεί εγγύηση για αξιόπιστη πρόσβαση των εξουσιοδοτημένων ατόμων στις πληροφορίες.
Ακολουθεί μια απεικόνιση της τριάδας της CIA μαζί με τα τέσσερα επίπεδα της ασφάλειας των πληροφοριών. Αυτά τα τέσσερα στρώματα αντιπροσωπεύουν τον τρόπο επικοινωνίας των συστημάτων και τον τρόπο ροής πληροφοριών μεταξύ των συστημάτων. Η έννοια των στρωμάτων υποδεικνύει ότι οι επικοινωνίες δεδομένων και τα πρωτόκολλα δικτύου υπολογιστών ορίζονται για να λειτουργούν με πολυεπίπεδη τρόπο, μεταφέροντας τα δεδομένα από το ένα στρώμα στο επόμενο.



Εικόνα 2 Επίπεδο ασφαλείας

16/07/2019 https://resources.infosecinstitute.com/guiding-principles-in-information-security/#gref

- Το Application Access Layer περιγράφει την άποψη ότι η πρόσβαση στις εφαρμογές των τελικών χρηστών πρέπει να περιορίζεται.
- Το επίπεδο πρόσβασης υποδομής (Infrastructure Access Layer) περιγράφει την ιδέα ότι η πρόσβαση στα εξαρτήματα υποδομής πρέπει να περιορίζεται.
- Το Layer Physical Access περιγράφει την ιδέα ότι η φυσική πρόσβαση σε οποιοδήποτε σύστημα, διακομιστή, υπολογιστή, κέντρο δεδομένων ή άλλο

φυσικό αντικείμενο που αποθηκεύει εμπιστευτικές πληροφορίες πρέπει να περιορίζεται.

- Το Data In Motion Layer περιγράφει την ιδέα ότι τα δεδομένα πρέπει να είναι ασφαλή ενώ «κινούνται».
- Αυτή η μικρή εικόνα στο κέντρο της εικόνας δείχνει το κέντρο της ασφάλειας των πληροφοριών και τον λόγο για την εμφάνιση των αρχών της CIA. το εικονίδιο αντιπροσωπεύει πληροφορίες καθώς και την ανάγκη προστασίας ευαίσθητων πληροφοριών.

1.1.1 Εμπιστευτικότητα

Η εμπιστευτικότητα (Confidentiality) είναι σχεδόν ισοδύναμη με το απόρρητο. Τα μέτρα που έχουν ληφθεί για την εξασφάλιση της εμπιστευτικότητας έχουν σχεδιαστεί για να αποτρέπουν την είσοδο ευαίσθητων πληροφοριών σε λάθος άτομα, ενώ παράλληλα διασφαλίζουν ότι τα σωστά άτομα μπορούν πράγματι να τα αποκτήσουν.Η πρόσβαση πρέπει να περιορίζεται σε όσους έχουν εξουσιοδότηση για την προβολή των εν λόγω δεδομένων. Είναι επίσης σύνηθες να ταξινομούνται τα δεδομένα ανάλογα με το μέγεθος και τον τύπο της ζημίας που θα μπορούσαν να γίνουν αν πέσουν σε λάθος χέρια. Εν συνεχεία, μπορούν να εφαρμοστούν περισσότερο ή λιγότερο αυστηρά μέτρα σύμφωνα με αυτές τις κατηγορίες.

Μερικές φορές, η διαφύλαξη του απορρήτου των δεδομένων μπορεί να συνεπάγεται ειδική εκπαίδευση για όσους ενδιαφέρονται για τέτοια έγγραφα. Τέτοιου είδους εκπαίδευση θα περιλαμβάνει συνήθως κινδύνους ασφαλείας που θα μπορούσαν να απειλήσουν αυτές τις πληροφορίες. Η εκπαίδευση μπορεί να βοηθήσει στην εξοικείωση των εξουσιοδοτημένων ατόμων με παράγοντες κινδύνου και τον τρόπο προστασίας τους. Περαιτέρω πτυχές της κατάρτισης μπορούν να περιλαμβάνουν ισχυρούς κωδικούς πρόσβασης και βέλτιστες πρακτικές που σχετίζονται με τον κωδικό πρόσβασης και πληροφορίες σχετικά με μεθόδους κοινωνικής μηχανικής, ώστε να αποφευχθεί η εξάπλωση των κανόνων χειρισμού δεδομένων με καλές προθέσεις και δυνητικά καταστροφικά αποτελέσματα.

Ένα καλό παράδειγμα μεθόδων που χρησιμοποιούνται για την εξασφάλιση της εμπιστευτικότητας είναι ο αριθμός λογαριασμού ή ο αριθμός δρομολόγησης κατά την ηλεκτρονική τραπεζική. Η κρυπτογράφηση δεδομένων είναι μια κοινή μέθοδος διασφάλισης της εμπιστευτικότητας. Τα αναγνωριστικά χρήστη και οι κωδικοί πρόσβασης αποτελούν μια τυπική διαδικασία.Ο έλεγχος ταυτότητας δύο παραγόντων γίνεται ο κανόνας. Άλλες επιλογές περιλαμβάνουν βιομετρικά στοιχεία επαλήθευσης και security tokens, κλειδιά ή soft tokens. Επιπλέον, οι χρήστες μπορούν να λάβουν προφυλάξεις για να ελαχιστοποιήσουν τον αριθμό των θέσεων

όπου εμφανίζονται οι πληροφορίες και τον αριθμό των φορών που πραγματικά μεταδίδονται για να ολοκληρώσουν μια απαιτούμενη συναλλαγή. Μπορούν να ληφθούν επιπλέον μέτρα στην περίπτωση εξαιρετικά ευαίσθητων εγγράφων.

1.1.2 Ακεραιότητα

Η ακεραιότητα συνεπάγεται τη διατήρηση της συνέπειας, της ακρίβειας και της αξιοπιστίας των δεδομένων καθ 'όλη τη διάρκεια του κύκλου ζωής τους. Τα δεδομένα δεν πρέπει να μεταβάλλονται κατά τη διαμετακόμιση και πρέπει να λαμβάνονται μέτρα ώστε να μην μπορούν να τροποποιηθούν από μη εξουσιοδοτημένους ανθρώπους (για παράδειγμα, παραβιάζοντας την εμπιστευτικότητα).Αυτά τα μέτρα περιλαμβάνουν τα δικαιώματα αρχείων και τα στοιχεία ελέγχου πρόσβασης των χρηστών. Ο έλεγχος έκδοσης μπορεί να χρησιμοποιηθεί για την αποτροπή λανθασμένων αλλαγών ή τυχαίας διαγραφής από εξουσιοδοτημένους χρήστες. Επιπλέον, πρέπει να υπάρχουν ορισμένα μέσα για την ανίχνευση οποιωνδήποτε αλλαγών στα δεδομένα που ενδέχεται να προκύψουν ως αποτέλεσμα συμβάντων που δεν προκαλούνται από τον άνθρωπο, όπως ηλεκτρομαγνητικό παλμό (EMP) ή crash διακομιστή. Ορισμένα δεδομένα ενδέχεται να περιλαμβάνουν checksums, ακόμη και κρυπτογραφικά αρχεία ελέγχου, για επαλήθευση της ακεραιότητας. Πρέπει να είναι διαθέσιμα αντίγραφα ασφαλείας ή redundancies για την επαναφορά των επηρεαζόμενων δεδομένων στη σωστή τους κατάσταση.

1.1.3 Διαθεσιμότητα

Η διαθεσιμότητα εξασφαλίζεται καλύτερα με την αυστηρή διατήρηση όλου του υλικού, την εκτέλεση επισκευών υλικού αμέσως όταν χρειάζεται και τη διατήρηση ενός λειτουργικού περιβάλλοντος λειτουργικού συστήματος που λειτουργεί σωστά, χωρίς συγκρούσεις λογισμικού (software conflicts). Είναι επίσης σημαντικό να διατηρήσετε την τρέχουσα κατάσταση με όλες τις απαραίτητες αναβαθμίσεις του συστήματος. Η παροχή επαρκούς εύρους ζώνης επικοινωνίας και η πρόληψη της εμφάνισης σημείων συμφόρησης είναι εξίσου σημαντικές. Ο πλεονασμός, η αποτυχία, τα αρχεία RAID ακόμη και υψηλής διαθεσιμότητας μπορούν να μετριάσουν σοβαρές συνέπειες όταν προκύψουν ζητήματα υλικού. Η ταχεία και προσαρμοστική αποκατάσταση των καταστροφών είναι απαραίτητη για τα χειρότερα σενάρια.Η ικανότητα αυτή εξαρτάται από την ύπαρξη ενός ολοκληρωμένου σχεδίου

αποκατάστασης καταστροφών (DRP). Οι διασφαλίσεις κατά της απώλειας δεδομένων ή των διακοπών στις συνδέσεις πρέπει να περιλαμβάνουν απρόβλεπτα γεγονότα, όπως φυσικές καταστροφές και πυρκαγιές. Για να αποφευχθεί η απώλεια δεδομένων από τέτοια περιστατικά, ένα αντίγραφο ασφαλείας μπορεί να αποθηκευτεί σε μια γεωγραφικά απομονωμένη τοποθεσία, ίσως ακόμη και σε ένα χρηματοκιβώτιο. Επιπλέον εξοπλισμό ή λογισμικό ασφαλείας, όπως τείχη προστασίας και διακομιστές μεσολάβησης, μπορούν να προστατεύσουν από το χρόνο καθυστέρησης και τα μη προσβάσιμα δεδομένα λόγω κακόβουλων ενεργειών όπως οι επιθέσεις DoS (Doom) και οι εισβολές δικτύου.

1.2 Ιδιωτικότητα

Οι κίνδυνοι ιδιωτικής χρήσης και προστασίας δεδομένων των εφαρμογών για κινητά προέρχονται κυρίως από δύο διαστάσεις: α) τη φύση τους, ως λογισμικό που εκτελείται σε ιδιωτικές συσκευές κινητών χρηστών (φορητές συσκευές) και β) τις ιδιαιτερότητες του περιβάλλοντος κινητής ανάπτυξης και διανομής. Παρακάτω παρέχουμε μια λεπτομερέστερη ανάλυση των σχετικών κινδύνων και παραγόντων κινδύνου.

1. Ποικιλία δεδομένων & πολλαπλοί αισθητήρες

Οι κινητές συσκευές μπορούν τυπικά να έχουν πρόσβαση σε διάφορους τύπους προσωπικών / ευαίσθητων δεδομένων (όπως ευημερία, υγεία, ιατρικά δεδομένα) που παρέχονται από χρήστες μέσω διαφόρων εφαρμογών για κινητά. Επιπλέον, οι τυπικές συσκευές χειρός ενσωματώνουν πολλούς και διάφορους αισθητήρες (μικρόφωνο, κάμερα, επιταχυνσιόμετρο, GPS, Wifi κ.λπ.) που παράγουν πολύ προσωπικά και διάφορα δεδομένα και μεταδεδομένα (τοποθεσία, ώρα, θερμοκρασία) που μπορεί να έχουν απροσδόκητες επιπτώσεις στο ιδιωτικό απόρρητο. Παραδείγματος χάριν, έχει αποδειχθεί ότι οι χρήστες μπορούν εύκολα να ταυτοποιηθούν και να πιστοποιούνται από σήματα κίνησης που έχουν αποκτηθεί από smartphone, όπως σήματα απο επιταχυνσιόμετρο και γυροσκόπιο (αδρανειακά) που παρέχονται από τα περισσότερα εμπορικά smartphones. Ομοίως, έχει αποδειχθεί ότι

οι κινητές συσκευές μπορούν μερικές φορές να παρακολουθούνται από την χωρητικότητα της μπαταρίας τους.

2. Προσωπική συσκευή, πάντα 'on'

Οι χρήστες συχνά βλέπουν ένα smartphone ή ένα tablet ως επέκταση του εαυτού τους και τείνουν να το θεωρούν αξιόπιστη,πολύ προσωπική συσκευή, την οποία δεν θα μοιράζονται με κανέναν. Επιπλέον, αυτές οι συσκευές σχεδόν πάντα ενεργοποιούνται, μεταφέρονται από τον χρήστη τους σχεδόν παντού και συνδέονται με ένα δίκτυο. Συνήθως αποθηκεύουν πολλά προσωπικά δεδομένα για μεγάλο χρονικό διάστημα. Αυτό τους καθιστά τέλειους στόχους για τους μεσίτες δεδομένων, τους διαφημιστές ή ιχνηλάτες εν γένει και μπορεί να οδηγήσει σε διαδεδομένη και συνεχή παρακολούθηση των χρηστών.

Αυτή είναι η έννοια του liquid surveillance’ , όπου εντοπίζονται οι μικρότερες λεπτομέρειες της καθημερινής μας ζωής. Επίσης, οι χρήστες συνηθίζουν όλο και περισσότερο χρησιμοποιούν τη δυνατότητα φωνητικού ελέγχου, υποστηριζόμενου από παράγοντες φωνητικής ανάλυσης όπως το Siri, το Google Now ή το Cortana. Ωστόσο, οι χρήστες έχουν λιγότερη επίγνωση του γεγονότος ότι η λειτουργία φωνητικού ελέγχου πραγματοποιείται από μια συσκευή που ακούει πάντα - τουλάχιστον ώστε αντιδράσει στους ορισμένους όρους ελέγχου όπως "Hey Siri", "Εντάξει Google "ή" Hey Cortana "- και ως εκ τούτου έχει πρόσβαση σε όλες τις ομιλούμενες επικοινωνίες.

3. Διαφορετικοί τύποι αναγνωριστικών

Οι κινητές συσκευές περιέχουν πολλούς διαφορετικούς τύπους αναγνωριστικών (αναγνωριστικό υλικού συσκευής, αποθηκευμένα αρχεία και μεταδεδομένα) ή δακτυλικά αποτυπώματα τα οποία μπορούν να χρησιμοποιηθούν από κινητές εφαρμογές για την παρακολούθησή τους.

Για παράδειγμα, ο Yves-Alexandre de Montjoye έδειξε ότι τέσσερα χωροχρονικά σημεία, που ενδεχομένως προέρχονται από ένα smartphone, αρκούν για να αποτυπώσουν τα δακτυλικά αποτυπώματα, δηλ. να αναγνωρίσουν με μοναδικό τρόπο το 95% των ατόμων.

4.Κινητό και σύνδεση

Οι κινητές συσκευές μπορούν να εντοπιστούν γεωγραφικά και να παρακολουθηθούν φυσικά. Αυτό το χαρακτηριστικό μπορεί να έχει ως αποτέλεσμα σημαντική ζημιά στην ιδιωτική ζωή. Στην πραγματικότητα, πολλές πιθανώς ευαίσθητες προσωπικές πληροφορίες (όπως η θρησκεία, η ασθένεια) μπορούν να συναχθούν για ένα άτομο από το ίχνος του κινητού του. Επιπλέον, επειδή είναι κινητά, συνδέονται με διαφορετικά, δυνητικά κακόβουλα δίκτυα, τα οποία εισάγουν νέους κινδύνους ασφάλειας και ιδιωτικότητας.

5. Δυνατότητα παρακολούθησης

Οι φορητές συσκευές μπορούν να παρακολουθούνται φυσικά μέσω των ασύρματων διεπαφών τους από τρίτους για τη δημιουργία φυσικών "προφίλ".Μπορούν επίσης να παρακολουθούνται από τρίτους στο Διαδίκτυο όταν είναι Online. Πολλά τρίτα μέρη πραγματοποιούν παρακολούθηση μεταξύ τομέων, δηλαδή συνδυάζουν τα φυσικά και τα διαδικτυακά προφίλ των χρηστών κινητών συσκευών. Αυτή η παρακολούθηση μπορεί να προσφέρει μια πιο πλήρη εικόνα της συμπεριφοράς του χρήστη και εισάγει νέους κινδύνους απορρήτου και ασφάλειας.

6. Περιορισμένη φυσική ασφάλεια

Συσκευές χειρός είναι συχνά μικρές φυσικές συσκευές, οι οποίες είναι δύσκολο να ασφαλιστούν. Μπορούν εύκολα να κλαπούν ή να σπάσουν, γεγονός που μπορεί να έχει αντίκτυπο στην εμπιστευτικότητα, αλλά και στη διαθεσιμότητα των δεδομένων. Επιπλέον, πολλές πηγές κινδύνου (σύντροφοι, σύζυγοι, συγγενείς) μπορούν να έχουν φυσική πρόσβαση σε αυτές, στους αισθητήρες τους ή σε συναφείς υπηρεσίες.

7. Περιορισμένες διεπαφές χρηστών

Οι συσκευές χειρός έχουν συνήθως περιορισμένες διεπαφές χρήστη (UI). Αυτό, φυσικά, επηρεάζει την ιδιωτικότητα, τη διαφάνεια, την ασφάλεια. Για παράδειγμα, ο Melicher et al. έδειξε ότι οι κωδικοί πρόσβασης που δημιουργούνται σε κινητές συσκευές είναι πιο αδύναμοι.Οι πολιτικές απορρήτου και οι ειδοποιήσεις είναι πιο δύσκολο να διαβαστούν σε ένα smartphone και απαιτούν ιδιαίτερη προσοχή. Ως αποτέλεσμα, οι πολιτικές απορρήτου θα πρέπει να οικοδομηθούν χρησιμοποιώντας μια προσέγγιση "στρωματοποιημένη" όπου συνοψίζονται τα πιο σημαντικά σημεία,

με περισσότερες λεπτομέρειες εύκολα διαθέσιμα εάν ο χρήστης θέλει να τα δει. Επιπλέον, καλό γραφικό σχέδιο, συμπεριλαμβανομένης της χρήσης χρωμάτων και συμβόλων, μπορεί να βοηθήσει τους χρήστες να καταλάβουν καλύτερα.

8. Περιορισμοί των προγραμματιστών εφαρμογών

Οι εφαρμογές για κινητά αναπτύσσονται συχνά από ένα άτομο ή μια μικρή ομάδα ατόμων, με περιορισμένους πόρους και τεχνογνωσία για την ασφάλεια / προστασία της ιδιωτικής ζωής. Είναι επομένως δύσκολο για τους προγραμματιστές να υιοθετήσουν τις τελευταίες τεχνικές λύσεις και μέτρα προστασίας της ιδιωτικής ζωής.

9. Χρήση λογισμικού τρίτου κατασκευαστή

Οι περισσότερες εφαρμογές για κινητά γράφονται συνδυάζοντας διάφορες λειτουργίες που αναπτύσσονται από άλλες εταιρείες (και όχι από τον προγραμματιστή εφαρμογών). Αυτές οι βιβλιοθήκες τρίτων βοηθούν τους προγραμματιστές, για παράδειγμα, παρακολουθούν την αφοσίωση των χρηστών (analytics), συνδέονται με κοινωνικά δίκτυα και παράγουν έσοδα προβάλλοντας διαφημίσεις. Ωστόσο, εκτός από την παρεχόμενη υπηρεσία, οι βιβλιοθήκες μπορούν επίσης να συλλέγουν προσωπικά δεδομένα για δική τους χρήση. Οι ιδιοκτήτες των βιβλιοθηκών μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για τη δημιουργία λεπτομερών ψηφιακών προφίλ χρηστών συνδυάζοντας τα δεδομένα που συλλέγουν από διαφορετικές εφαρμογές για κινητά. Για παράδειγμα, ένας χρήστης μπορεί να δώσει σε μία εφαρμογή την άδεια να συλλέξει την τοποθεσία του και μια άλλη εφαρμογή να έχει πρόσβαση στις επαφές του / της. Εάν και οι δύο εφαρμογές χρησιμοποιούν την ίδια βιβλιοθήκη τρίτου μέρους, ο προγραμματιστής της βιβλιοθήκης θα μπορούσε να συνδέσει τα δύο αυτά στοιχεία μαζί. Επιπλέον, αυτές οι βιβλιοθήκες είναι συχνά ιδιοκτησιακές και κλειστές πηγές,και δεν μπορούν εύκολα να αναλυθούν. Ως αποτέλεσμα, είναι κοινό ότι ένας προγραμματιστής εφαρμογών για κινητά δεν κατανοεί πλήρως ποια δεδομένα συλλέγουν αυτές οι υπηρεσίες. Αν και δεν αποτελεί κίνδυνο ως τέτοιο, ο συνδυασμός πηγών δεδομένων μπορεί να αποτελέσει το έδαφος για μια επίθεση.

10. App market

Οι εφαρμογές διανέμονται συχνά μέσω συγκεκριμένων app market, τα οποία ενδέχεται να διαδραματίσουν σημαντικό ρόλο στην ασφάλεια και την προστασία της ιδιωτικής ζωής των εφαρμογών. Ένα κατάστημα εφαρμογών συνήθως δεν παρέχει μόνο πρόσβαση σε εφαρμογές, αλλά παρέχει πληροφορίες για εφαρμογές και συλλέγει και εμφανίζει αξιολογήσεις χρηστών. Επίσης, ένα κατάστημα εφαρμογών μπορεί να πραγματοποιεί ελέγχους ασφαλείας σε κάθε εφαρμογή, για να αποτρέψετε τη διανομή κακόβουλων ή ψεύτικων εφαρμογών. Λόγω του σημαντικού ρόλου που διαδραματίζει η διανομή εφαρμογών, οι πάροχοι υπηρεσιών καταστημάτων εφαρμογών θα μπορούσαν να φιλτράρουν εφαρμογές με εμφανείς κινδύνους ασφαλείας.

Όσο τα καταστήματα εφαρμογών παραμένουν ανεξέλεγκτα, η πρόσβαση στις δυνατότητες διανομής τους από προμηθευτές εφαρμογών και προγραμματιστές εφαρμογών θα παραμείνει ασαφής.

Η διαθεσιμότητα εφαρμογών σε καταστήματα εφαρμογών καθώς και ο τρόπος παρουσίασής τους μπορεί να επηρεάσει τη διανομή των εφαρμογών.

Επιπλέον, από την άποψη της ιδιωτικής ζωής, πρέπει να σημειωθεί ότι το επίπεδο γνώσεων της επιλογής ενός χρήστη από μια εφαρμογή θα μπορούσε να συνιστά προσωπικά δεδομένα ή ακόμα και ευαίσθητα προσωπικά δεδομένα, μερικές φορές (π.χ. εάν έχει εγκατασταθεί μια εφαρμογή ηλεκτρονικής υγείας, αποκαλύπτοντας έτσι προσωπική προτίμηση υγείας ή δεδομένα). Επί του παρόντος, οι χρήστες ενδέχεται να μην είναι επαρκώς ενημερωμένοι ανά πάσα στιγμή για τη συλλογή πιθανών προσωπικών δεδομένων από τους παρόχους υπηρεσιών προστιθέμενης αξίας που χρησιμοποιούν, εκθέτοντας έτσι τους κινδύνους για την ασφάλεια στον κυβερνοχώρο.

11. Αποθήκευση στο σύννεφο

Οι εφαρμογές για κινητά αποθηκεύουν συχνά προσωπικές πληροφορίες στο σύννεφο. Η υπηρεσία αυτή πρέπει να είναι ασφαλής και να προστατεύει από τη

διαρροή δεδομένων. Στην πραγματικότητα, έχει αποδειχθεί ότι οι περισσότερες ποσοτικοποιημένες εφαρμογές αποκλειστικά αποθηκεύουν τα δεδομένα των χρηστών στο σύννεφο. Αυτό εισάγει μια νέα πηγή κινδύνου και απαιτεί από τον χρήστη να εμπιστεύεται τον πάροχο υπηρεσιών χωρίς να λαμβάνει υπόψη αντικειμενικά κριτήρια βάσει των οποίων μπορεί να βασιστεί μια απόφαση εμπιστοσύνης.

12. Διαδικτυακά κοινωνικά δίκτυα

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

1.3 Συνοχή

Εγγυάται ότι τα αποτελέσματα και η συμπεριφορά των υπηρεσιών είναι συνεπή από οποιοδήποτε σημείο. Η συνοχή της μνήμης είναι μια επιθυμητή κατάσταση στην οποία οι αντίστοιχες θέσεις μνήμης για κάθε στοιχείο επεξεργασίας σε έναν επεξεργαστή πολλαπλών πυρήνων περιέχουν πάντα τα ίδια αποθηκευμένα δεδομένα. Χωρίς συνοχή μνήμης, τα προγράμματα μπορούν να επηρεαστούν αρνητικά. Στους επεξεργαστές πολλών πυρήνων, δύο ή περισσότερα στοιχεία επεξεργασίας λειτουργούν ταυτόχρονα. Από καιρό σε μια στιγμή θα έχουν πρόσβαση στην ίδια θέση μνήμης. Εφόσον κανένα στοιχείο επεξεργασίας δεν μεταβάλλει τα δεδομένα στην επηρεαζόμενη τοποθεσία, όλα αυτά τα στοιχεία μπορούν να μοιράζονται και να αποθηκεύουν προσωρινά τα δεδομένα χωρίς κανένα πρόβλημα. Αλλά εάν ένα από τα στοιχεία επεξεργασίας αλλάξει τα δεδομένα στην κοινόχρηστη τοποθεσία και δεν ενημερώσει τους άλλους για την αλλαγή, τα άλλα στοιχεία ενδέχεται να χρησιμοποιούν την παλιά έκδοση των δεδομένων που παραμένουν στην τοπική τους προσωρινή μνήμη.

Σε ένα σύστημα επεξεργασίας πολλαπλών πυρήνων, το λεγόμενο πρωτόκολλο συνοχής μνήμης ειδοποιεί όλα τα στοιχεία επεξεργασίας των αλλαγών στις κοινές τιμές, διασφαλίζοντας έτσι ότι όλα τα αντίγραφα των δεδομένων παραμένουν συνεπή.

1.4 Απομόνωση

Η απομονωμένη εκτέλεση δίνει την δυνατότητα στον προγραμματιστή της εφαρμογής να εκτελέσει μια ενότητα λογισμικού σε πλήρη απομόνωση από τον άλλο κώδικα. Παρέχει την μυστικότητα και την ακεραιότητα του κώδικα και των δεδομένων της εν λόγω μονάδας κατά το χρόνο εκτέλεσης. Τα σημερινά κινητά λειτουργικά συστήματα παρέχουν απομόνωση με βάση τις διαδικασίες για την προστασία των χώρων διευθύνσεων των εφαρμογών και άλλων πόρων του συστήματος. Ωστόσο, αυτοί οι μηχανισμοί μπορούν να καταστραφούν όταν το ίδιο το λειτουργικό σύστημα είναι κατεστραμμένο. Για την παροχή απομονωμένης εκτέλεσης που δεν εξαρτάται από το λειτουργικό σύστημα, απαιτείται κάποιο εναλλακτικό περιβάλλον εκτέλεσης που δεν ελέγχεται από το λειτουργικό σύστημα. Ένα τέτοιο περιβάλλον θα μπορούσε να παρέχεται από ένα στρώμα που τρέχει κάτω από το λειτουργικό σύστημα στο ίδιο υλικό (δηλ. Ένας hypervisor), ή σε ένα παράλληλο περιβάλλον (coprocessor).

1.5 Σταθερότητα

Χαρακτηρίζει την ευαισθησία στην αλλαγή ενός δεδομένου συστήματος που είναι η αρνητική επίδραση που μπορεί να προκληθεί από τις αλλαγές του συστήματος.
Η δοκιμή σταθερότητας γίνεται για να ελέγξει την απόδοση ενός εξελιγμένου προϊόντος πέρα από την κανονική λειτουργική του ικανότητα, συχνά σε σημείο διακοπής. Η μεγαλύτερη σημασία έχει ο χειρισμός σφαλμάτων, η αξιοπιστία του λογισμικού, η ευρωστία και η δυνατότητα κλιμάκωσης ενός προϊόντος υπό υψηλό φορτίο, παρά ο έλεγχος της συμπεριφοράς του συστήματος υπό κανονικές συνθήκες.
Οι δοκιμές σταθερότητας αξιολογούν τα προβλήματα σταθερότητας. Αυτός ο έλεγχος αποσκοπεί κατά κύριο λόγο να ελέγξει αν η εφαρμογή θα διακοπεί σε οποιαδήποτε χρονική στιγμή.

Εικόνα 3 Δοκιμές Σταθερότητας

Στην Τεχνολογία Λογισμικού, η Δοκιμή Σταθερότητας περιλαμβάνει συνήθως την άσκηση του συστήματος με βαρείς χρήστες (εικονικά) και τη μέτρηση των παραμέτρων απόδοσης για να εξακριβωθεί αν το σύστημα μπορεί να υποστηρίξει το αναμενόμενο φορτίο.

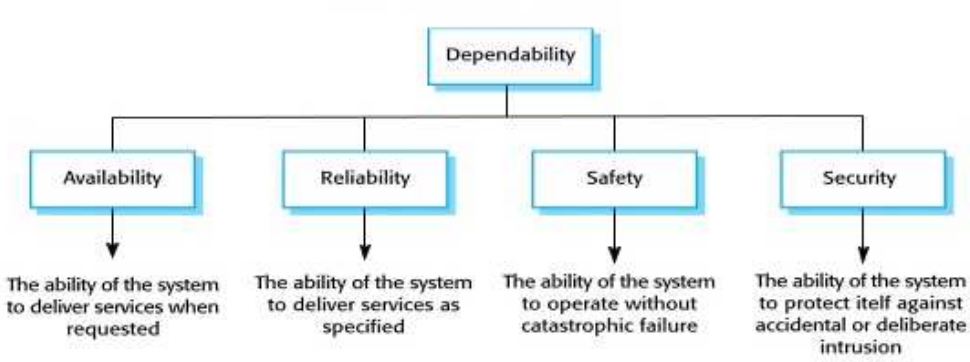
1.6 Διαφάνεια

Η διαφάνεια σημαίνει σαφήνεια, συνοπτικότητα.Η διαφάνεια είναι μια νέα μη λειτουργική απαίτηση για συστήματα λογισμικού. Είναι αναγνωρισμένη για τη βελτίωση της ποιότητας των υπηρεσιών, δεδομένου ότι παρέχει στους χρήστες

πρόσβαση σε πληροφορίες σχετικά με τις διαδικασίες του συστήματος, διευκρινίζοντας ποιος είναι υπεύθυνος εάν κάτι πάει στραβά. Επομένως, θεωρείται ότι υποστηρίζει το δικαίωμα των πολιτών σε ασφαλή και ιδιωτική επεξεργασία των προσωπικών τους δεδομένων. Αυτό αποκτά ιδιαίτερη σημασία στους χρήστες κινητών που εκτιμούν το υψηλό επίπεδο λεπτομέρειας για τον τρόπο με τον οποίο συμπεριφέρονται οι υπηρεσίες τους.

1.7 Αξιοπιστία

Η αξιοπιστία είναι το μέτρο της κατάστασης ενός συστήματος κατά τη διάρκεια μιας αποστολής, υπό την προϋπόθεση ότι είναι λειτουργικό και διαθέσιμο στην αρχή της αποστολής. Η αξιοπιστία μπορεί επίσης να περιγραφεί ως η πιθανότητα ένα σύστημα ή ένος προϊόντος να ολοκληρώσει την αποστολή του, και υπό την προϋπόθεση ότι ήταν διαθέσιμο για λειτουργία στην αρχή της αποστολής. Η αξιοπιστία του συστήματος επηρεάζει σημαντικά την αξιοπιστία ενός μη επανδρωμένου συστήματος / είδους.



Εικόνα 4 Αξιοπιστία

22/7/2019 https://www.slideshare.net/sommerville-videos/availability-and-reliability

2.Κεφάλαιο 2 Κατηγοριοποίηση Εφαρμογών

Το Mobile Sensing Crowd (MCS) είναι μια εξελισσόμενη τεχνολογία που βασίζεται στην ανίχνευση των δυνατοτήτων δικτύωσης φορητών συσκευών. Δύο σημαντικά ζητήματα που αντιμετωπίζει η MCS είναι η προστασία της ιδιωτικής ζωής και της αξιοπιστίας των χρηστών, τα οποία εξασφαλίζονται με τη λύση ασφάλειας ασύρματου αισθητήρα δικτύου. Το MCS βασίζεται σε μεμονωμένους συμμετέχοντες για τη συλλογή δεδομένων από τα περιβάλλοντά τους από τα έξυπνα τηλέφωνα και στη συνέχεια κάνει Upload τα δεδομένα στον application server μέσω της εγκατάστασης δικτύου. Ο διακομιστής εφαρμογών θα επεξεργάζεται όλα τα δεδομένα που αναφέρουν οι συμμετέχοντες, θα εξάγει τις πληροφορίες που ενδιαφέρουν τους ερωτηθέντες και θα διαβιβάζει τέτοιες πληροφορίες στους τελικούς χρήστες. Η εφαρμογή MCS μπορεί να χρησιμοποιηθεί σε διάφορες κατηγορίες όπως η υγειονομική περίθαλψη, η επιχείρηση, το περιβάλλον, δικτύωση. Η εφαρμογή MCS συλλέγει δεδομένα σε ευρείες γεωγραφικές περιοχές, χωροχρονικές πληροφορίες όπου υπάρχουν πιθανές απειλές για τους συμμετέχοντες που έκαναν Upload τα δεδομένα τους, όπως τα δεδομένα που συλλέχθηκαν, ενδέχεται να αποκαλύψουν τις θέσεις και τις τροχιές τους. Εδώ το κύριο ζήτημα ασφαλείας του MCS είναι η αξιοπιστία των μεταφορτωμένων δεδομένων που αναφέρουν οι συμμετέχοντες, τα οποία ενδεχομένως να είναι πλαστά. Ως εκ τούτου, αυτό εγείρει το ζήτημα της αξιοπιστίας των δεδομένων

Η εμπιστοσύνη είναι η αποδεκτή εξάρτηση ενός χρήστη σε ένα σύνολο ιδιοτήτων (λειτουργικών ή / και μη λειτουργικών) που παρέχονται / εφαρμόζονται από άλλο στοιχείο, υποσύστημα ή σύστημα.Μπορεί να οριστεί ως το μέτρο στο οποίο ένα συστατικό, ένα υποσύστημα ή ένα σύστημα ικανοποιεί ένα σύνολο αυτών των ιδιοτήτων. Ένας προγραμματιστής εφαρμογών θέλει να γνωρίζει (και τελικά να ενισχύει) την αξιοπιστία των υπηρεσιών που αναπτύσσει.Εκ των προτέρων, τα

στατικά μέτρα μπορούν να αξιολογηθούν με τον καθορισμό δοκιμών που εκτελούνται αυτόματα. Αυτές οι δοκιμές μπορούν να περιλαμβάνουν αξιολόγηση απόδοσης, κλιμάκωση, χρήση ασφαλών πρωτοκόλλων, διόρθωση σε σχέση με ένα συγκεκριμένο σετ δοκιμών, ευρωστία έναντι γνωστών τρωτών σημείων κλπ.
Για την επίτευξη της αξιολόγησης συλλέξαμε πληθώρα απο εφαρμογές που έχουμε εγκατεστημένες οι περισσότεροι στα κινητά μας και τις χωρίσουμε σε κατηγορίες με σκοπό να έχουμε συγκεντρωτικά αποτελέσματα.Η κατηγοριοποίηση που δώθηκε είναι εύκολα αντιληπτή απο οποιοδήποτε.

Applications Category
Κοινωνικά Δίκτυα
Ηλ.Ταχυδρομείο
Ενημέρωση
Χάρτες
Παιχνίδια
Υγεία
Παραγωγικότητα
Καιρός
Τράπεζα
Ταξί

Πίνακας 1 Κατηγορίες Εφαρμογών

Στην συνέχεια με δεδομένα όσα αναφέρθηκαν στο πρώτο κεφάλαιο προσθέσαμε και τις μετρικές με βάση των οποίων θα γίνει η αξιολόγηση. Οι ιδιότητες των αξιόπιστων υπηρεσιών που εξετάζονται είναι οι παρακάτω:

1) Ασφάλεια (Security (Integrity,Availability,Confidentiality)
2) Ιδιωτικότητα (Privacy)
3) Συνοχή (Coherence)
4) Απομόνωση (Isolation)
5) Σταθερότητα (Stability)
6) Διαφάνεια (Transparency)

7) Αξιοπιστία (Dependability)

Με δεδομένο ότι έχουν αναλυθεί οι μετρικές και γνωρίζουμε και όλες τις κατηγορίες των εφαρμογών ήταν εφικτή η ανάλυση της αναγκαιότητας κάθε μιας μετρικής με βάση των κατηγορία των εφαρμογών. Εστιάζουμε στην αυξημένη ασφάλεια και προστασία της ιδιωτικής ζωής, στην ανιχνευσιμότητα και στην τήρηση των κανονισμών.

Εφαρμογή	Security (Integrity,Availability ,Confidentiality)	Privacy	Coherence	Isolation	Stability	Transparency	Dependability
Κοινωνικά Δίκτυα	V	V	V	V	V	V	V
Ηλ.Ταχυδρομείο	V	V	V	V	V	V	V
Ενημέρωση	V	-	V	V	-	V	V
Χάρτες	V	V	-	V	-	V	V
Παιχνίδια	-	-	V	V	-	-	-
Υγεία	V	V	V	V	-	-	V
Παραγωγικότητα	V	V	V	V	V	-	V
Καιρος	-	-	V	V	V	-	V
Τράπεζα	V	V	V	V	V	V	V
Ταξί	V	V	-	V	-	-	-

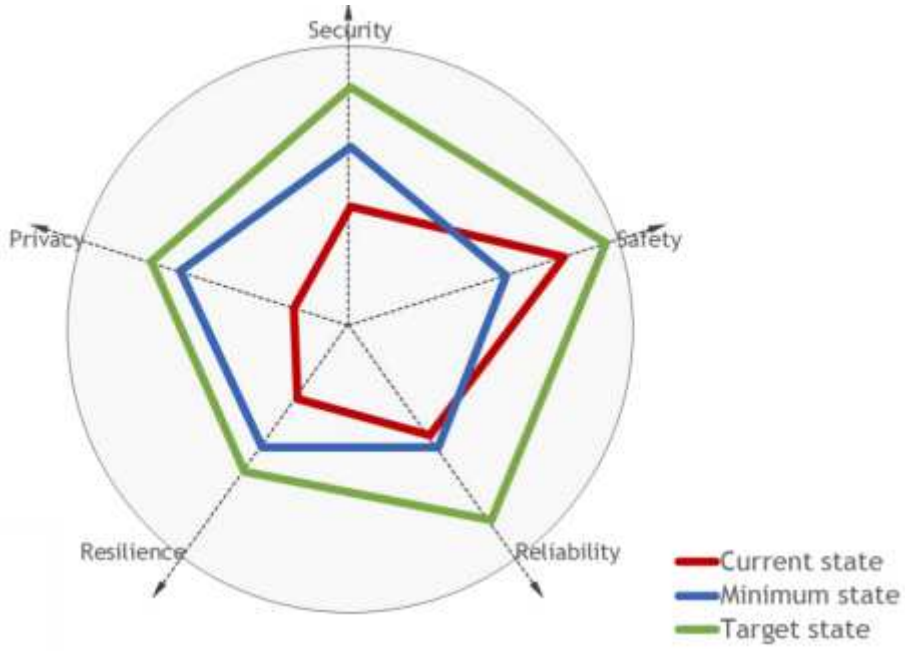
Πίνακας 2 Ανάλυση κατηγοριών με βάση τις μετρικές

Όπου με V απεικνίζονται οι μετρικές που απαιτούνται και με – (παύλα) όσες δεν χρειάζονται για τις εφαρμογές αυτές.Παρατηρώντας τον πίνακα διαπιστώσαμε ότι για να παίξουμε ένα παιχνίδι,να ενημερωθούμε για τα νέα, είτε να ενημερωθούμε για τον καιρό δεν απαιτείται διασφάλιση του απορρήτου διότι δεν θα πρέπει να δίνονται σε αυτές τις κατηγορίες εφαρμογών πληροφορίες απόρρητες. Είναι σημαντικό να σημειωθεί ότι η σημασία των ιδιοτήτων μπορεί να ποικίλει ανάλογα με την υπηρεσία, δηλ. Σε ορισμένες περιπτώσεις η ιδιωτικότητα μπορεί να είναι πιο σχετική από την απόδοση και σε άλλες περιπτώσεις μπορεί να συμβεί και το αντίστροφο.Η μεταφορά και η απομακρυσμένη επεξεργασία της ιατρικής απεικόνισης και τα συναφή δεδομένα για την υγεία είναι ένα τέλειο παράδειγμα εφαρμογών που απαιτούν

υψηλό βαθμό αξιοπιστίας. Οι διαστάσεις εμπιστοσύνης όπως η απόδοση,η διαθεσιμότητα, η προστασία της ιδιωτικής ζωής, η ασφάλεια είναι πολύ σημαντικό να διασφαλιστούν.

Ο σχεδιασμός και η υλοποίηση ενός στρώματος αξιοπιστίας επεξεργασίας δεδομένων εγείρει αρκετές σημαντικές προκλήσεις.Μπορούμε να χωρίσουμε τις προκλήσεις σε δυο κύριες ομάδες. Η πρώτη ομάδα περιλαμβάνει προκλήσεις που προκύπτουν κατά την εκτέλεση των εφαρμογών και πώς αλληλεπιδρούν και χρησιμοποιούν τη βασική υποδομή. Μέχρι στιγμής, οι μηχανές επεξεργασίας δεδομένων υποθέτουν ότι μπορεί κανείς να εμπιστευτεί το υποκείμενο σύστημα. Πρόσφατες έρευνες έχουν δείξει ότι δεν μπορούμε να εμπιστευτούμε κανένα λογισμικό και πρέπει να διασφαλίσουμε τις εγγυήσεις προστασίας προσωπικών δεδομένων παρά τους πιθανούς συμβιβασμούς του υποκείμενου λογισμικού συστήματος. Συγκεκριμένα, πρέπει να προστατεύσουμε την αξιοπιστία της επεξεργασίας δεδομένων παρά την πιθανή πρόσβαση στο υλικό, την πρόσβαση σε ρίζες και τον πλήρη έλεγχο του λογισμικού συστήματος από τους αντιπάλους. Η δεύτερη ομάδα ασχολείται με τις εγγενείς ιδιότητες των υπηρεσιών και τους αλγορίθμους που εφαρμόζουν, όπως η δικαιοσύνη και η διαφάνεια. Είναι σημαντικό να τονιστεί ότι όχι μόνο η ικανοποίηση καθεμιάς από τις προαναφερθείσες απαιτήσεις αποτελεί πρόκληση αλλά και η ισορροπημένη ένταξή τους, δεδομένου ότι υπάρχουν πολλά συμπεράσματα που πρέπει να αντιμετωπιστούν, όπως η διαφάνεια, η ιδιωτικότητα και η ασφάλεια, τα οποία παρέχουν αντιφατικές οδηγίες σχετικά με τη δημοσίευση δεδομένων δυνητικά κρίσιμα.

Η σχέση μεταξύ έννοιων εμπιστοσύνης και αξιοπιστίας πρέπει να εξετάζει τους κινδύνους και τις πιθανές συνέπειες, όταν οι υπερβολικά συντηρητικοί χρήστες χάνουν τα πιθανά οφέλη του συστήματος ή όταν υπερβολικά αισιόδοξοι χρήστες παίρνουν υπερβολικό κίνδυνο χρησιμοποιώντας το σύστημα, οδηγώντας σε κυβερνοχώρο - εγκλήματα, ηλεκτρονικές απάτες, κυβερνο-τρομοκρατία και δολιοφθορά.



Εικόνα 5 Μοντέλο Εμπιστοσύνης spider

https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI_Trustworthiness-Model-Representation-Corlina.pdf

Κεφάλιο 3

Η ανάπτυξη εφαρμογών έχει χαμηλό όριο εισόδου, που σημαίνει ότι σχεδόν οποιοσδήποτε με ορισμένες δεξιότητες κωδικοποίησης μπορεί να αναπτύξει μια εφαρμογή. Οι εφαρμογές αναπτύσσονται επίσης από μεγαλύτερες ομάδες που απασχολούνται από πολυεθνικές εταιρείες με τη στήριξη των διοικητικών και νομικών ομάδων. Εκτός από το εσωτερικό τμήμα πληροφορικής, οι μεγαλύτερες εταιρείες μπορούν να αναθέτουν την ανάπτυξη νέων εφαρμογών σε τρίτους, για μερικές από τις οποίες η ανάπτυξη εφαρμογών αποτελεί μέρος της "ανύψωσης και μετατόπισης" ενός παλαιού συστήματος επιχείρησης στο σύννεφο. Οι εφαρμογές αναπτύσσονται επίσης από start-ups. Μια πρόσφατη μελέτη στις ΗΠΑ δείχνει ότι το 82% των εφαρμογών αναπτύσσονται από μικρές εταιρείες (έσοδα λιγότερο από 38 εκατομμύρια δολάρια και / ή λιγότερα από 250 εργαζόμενους).

Οι προγραμματιστές από οποιοδήποτε από αυτά τα (μη) οργανωτικά υπόβαθρα μπορούν να αναπτύξουν εφαρμογές, μερικές φορές με υψηλές απαιτήσεις ασφάλειας και προστασίας προσωπικών δεδομένων, και να χρησιμοποιούνται από εκατομμύρια, αν όχι από δισεκατομμύρια χρήστες (π.χ. Signal και Whatsapp προέρχονται από δύο πολύ διαφορετικές οργανώσεις, μοιράζονται μερικώς μια βάση κώδικα και έχουν αλληλεπικαλυπτόμενες απαιτήσεις ιδιωτικότητας και ασφάλειας). Σύμφωνα με εκτιμήσεις της βιομηχανίας, παγκοσμίως υπάρχουν 8,7 εκατομμύρια προγραμματιστές εφαρμογών για κινητά στον κόσμο. Γεωγραφικά, οι προγραμματιστές εφαρμογών διανέμονται σε ολόκληρο τον κόσμο, με περίπου το ένα τρίτο να βρίσκεται στην Ευρώπη.

Η συμμόρφωση για την προστασία δεδομένων για κάποιον που υλοποιεί τις εφαρμογές στην κουζίνα του μπορεί να διαφέρει από εκείνη ενός μεγαλύτερου οργανισμού με πιθανή υποστήριξη από μια νομική ή τεχνική ομάδα με εμπειρία στην προστασία δεδομένων. Ένας μεμονωμένος προγραμματιστής δεν μπορεί ούτε έχει το χρόνο, τα χρήματα ούτε την τεχνογνωσία από πολύπλοκες νομικές έννοιες, ωστόσο μπορεί να είναι ο πρωταρχικός στόχος για συστάσεις προστασίας δεδομένων.

Σε αυτό το κεφάλαιο κάνουμε μια βαθιά κατάδυση στην ανάλυση των δικαιωμάτων, μια βασική πρόκληση για την προστασία των δεδομένων σε εφαρμογές για κινητά.

3.1 Μοντέλα αδειών και επιπτώσεις στην ιδιωτική ζωή

Τα μοντέλα δικαιωμάτων διαφέρουν ανάλογα με το λειτουργικό σύστημα και τη συσκευή. Η αρχιτεκτονική Android διακρίνει μεταξύ κανονικών και επικίνδυνων δικαιωμάτων. Οι "επικίνδυνες άδειες" είναι εκείνες που η Google έχει αποφασίσει ότι μπορεί να θέσει σε κίνδυνο την ιδιωτικότητα του χρήστη ή τις λειτουργίες της συσκευής (π.χ. τηλέφωνο, τοποθεσία, αισθητήρες), σε σύγκριση με τις "συνήθεις άδειες" (π.χ. πρόσβαση στο Internet, δόνηση,). Σε αντίθεση με τα κανονικά δικαιώματα, οι επικίνδυνες άδειες απαιτούν έγκριση από τον χρήστη πριν από την εγκατάσταση ή την πρώτη χρήση και ενδέχεται να ανακληθούν ανά πάσα στιγμή αργότερα.
Το Android προσφέρει μια κεντρική διασύνδεση για τις ρυθμίσεις απορρήτου, καθώς και τη δυνατότητα αλλαγής των δικαιωμάτων για μια συγκεκριμένη εφαρμογή. Επιπλέον, το λειτουργικό σύστημα επιτρέπει στους χρήστες να αποφασίζουν για εφαρμογές προεπιλογής (π.χ. για την αποστολή SMS) για τις οποίες οι χρήστες μπορούν να προσαρμόσουν τα δικαιώματα για να καλύψουν τις ανάγκες τους. Ο διάλογος εξήγησης εξουσιοδότησης επιτρέπει στους προγραμματιστές να παρέχουν στους χρήστες περισσότερες πληροφορίες σχετικά με μια άδεια. Ωστόσο, μελέτες δείχνουν ότι η χρησιμότητα αυτών των εξηγήσεων μπορεί να βελτιωθεί ακόμη .
Από την άλλη πλευρά, το IOS χρησιμοποιεί “entitlements” και “permissions”. Τα “entitlements” δημιουργούνται στη διαμόρφωση μιας εφαρμογής και καθορίζουν τις δυνατότητες που δεν είναι διαθέσιμες από προεπιλογή και είναι απαραίτητες για την λειτουργία της εφαρμογής (π.χ. πρόσβαση iCloud). Τα “entitlements” υποβάλλονται στην Apple στη δέσμη εφαρμογών και δεν μπορούν να τροποποιηθούν μετά την υποβολή της αίτησης στο App Store. Τα Permissions στο iOS εγκρίνονται μόνο κατά το χρόνο εκτέλεσης και χρησιμοποιούνται για την προτροπή του χρήστη για χρήση περιορισμένων πόρων, όπου η πρόσβαση παρέχεται μόνο εφόσον συμφωνεί ο χρήστης. Η συμφωνία σε μια άδεια σημαίνει ότι η πρόσβαση στον ίδιο πόρο εγκρίνεται στη συνέχεια. Ωστόσο, οι χρήστες μπορούν να ανακαλέσουν δικαιώματα ανά πάσα στιγμή χρησιμοποιώντας τις ρυθμίσεις απορρήτου και ασφάλειας της iOS .
Αντί να εγκαταστήσετε δικαιώματα χρόνου, το iOS του iPhone έχει μια επιλογή ρύθμισης μιας στάσης για όλες τις εφαρμογές συν δικαιώματα εκτέλεσης. Η ρύθμιση "one stop" επιτρέπει στους χρήστες να βλέπουν όλες τις εφαρμογές που ζητούν μια συγκεκριμένη άδεια, π.χ. τοποθεσία ή όλα τα δικαιώματα που ζητά κάθε εφαρμογή. Εάν οι χρήστες επιθυμούν να κατανοήσουν γιατί απαιτείται άδεια, προωθούνται στην πολιτική απορρήτου. Με τις συγκεντρωτικές ρυθμίσεις, το iOS έρχεται σε αντίθεση με την αρχή της χρηστικότητας της ιδιωτικής ζωής, η οποία καθιστά τις άδειες

συμφραζόμενες, χάριν μιας άλλης αρχής χρηστικότητας, της απλότητας. Το αν οι κεντρικοί έλεγχοι είναι χρησιμοποιήσιμοι όταν ένας χρήστης έχει δεκάδες εφαρμογές είναι μια ενδιαφέρουσα ερώτηση που αξίζει να διερευνηθεί περαιτέρω.
Υπάρχουν και άλλοι τύποι δικαιωμάτων που μπορούν να οριστούν από προγραμματιστές εφαρμογών. Αν απομακρυνθεί από τις ιδιαιτερότητες της πλατφόρμας, αυτές μπορούν να οριστούν ως εξής:

Στατικά δικαιώματα: αυτά είναι δικαιώματα που έχουν οριστεί από προγραμματιστές εφαρμογών και διαχειρίζονται από τους χρήστες κατά την εγκατάσταση της εφαρμογής (π.χ.: η εφαρμογή έχει τη δυνατότητα να στείλει ειδοποιήσεις κ.λπ.).

Δυναμικά δικαιώματα: αυτά είναι δικαιώματα που έχουν οριστεί από προγραμματιστές και τους ζητείται κατά τη διάρκεια της εκτέλεσης της εφαρμογής (π.χ.: όταν κατά τη χρήση μιας εφαρμογή χρειάζεται πρόσβαση στην κάμερα)

Προσαρμοσμένα δικαιώματα: αυτά τα διαχειρίζονται οι προγραμματιστές ή διαφορετικές ομάδες σε έναν οργανισμό ο οποίος μπορεί να είναι υπεύθυνος για την ανάπτυξη πολλαπλών εφαρμογών. Αφορούν δικαιώματα που μπορούν να οριστούν μεταξύ διαφορετικών εφαρμογών που ανήκουν στον ίδιο οργανισμό. Δεδομένου ότι οι εφαρμογές των ίδιων προγραμματιστών / οργανισμών ενδέχεται να αλληλεπιδρούν και να ανταλλάσσουν πληροφορίες μεταξύ τους, τα δικαιώματα αυτά ορίζονται κατά τη διάρκεια της φάσης ανάπτυξης και επιτρέπουν σε εφαρμογές του ίδιου κατασκευαστή να ανταλλάσσουν δεδομένα ή υπηρεσίες μεταξύ τους.

Δικαιώματα βιβλιοθήκης τρίτων: αυτά τα διαχειρίζονται οι βιβλιοθήκες εφαρμογών που χρησιμοποιούν οι προγραμματιστές. Οι βιβλιοθήκες τρίτων (π.χ., βιβλιοθήκες διαφημίσεων) μπορούν να ορίσουν τα δικά τους δικαιώματα. Στο Android, δεν υπάρχει απομόνωση μεταξύ των στοιχείων, και αυτά τα δικαιώματα μεταδίδονται στις εφαρμογές που βασίζονται σε αυτές τις βιβλιοθήκες. Αυτό μπορεί να έχει ως αποτέλεσμα ότι οι εφαρμογές ζητούν δικαιώματα που δεν είναι απαραίτητα για την κύρια λειτουργία τους. Το πώς λειτουργεί για το iOS είναι πιο περίπλοκο και δεν μπορέσαμε να βρούμε ερευνητικά έγγραφα που αναλύουν το πλαίσιο iOS για δικαιώματα βιβλιοθήκης τρίτων.

Κάθε τύπος άδειας έχει διαφορετικό αντίκτυπο στην προστασία της ιδιωτικής ζωής και της ασφάλειας. Ανάλογα με την πλατφόρμα, ο χρήστης διαχειρίζεται ορισμένα στατικά και δυναμικά δικαιώματα. Είτε κατά την εγκατάσταση είτε κατά τη διάρκεια εκτέλεσης, η εφαρμογή απαιτεί από τον χρήστη να συγκατατεθεί στη συλλογή δεδομένων ή σε κάποια λειτουργικότητα της συσκευής. Από την άλλη πλευρά, τα δικαιώματα διαφήμισης και διαφημίσεων δεν απαιτούν ρητά τη συγκατάθεση του

χρήστη. Οι προγραμματιστές θέτουν προσαρμοσμένες άδειες στη φάση ανάπτυξης - μπορούν να αναφερθούν στις πολιτικές απορρήτου, αλλά αυτό δεν συμβαίνει πάντα.

Στις περισσότερες περιπτώσεις, οι προγραμματιστές εφαρμογών ή οι πάροχοι εφαρμογών δεν είναι διαφανείς σχετικά με τα δεδομένα χρήστη ή τις υπηρεσίες που απαιτούνται από την εφαρμογή. Τα δικαιώματα διαφήμισης είναι ακόμη πιο κρίσιμα, καθώς οι προγραμματιστές ίσως να μην γνωρίζουν καν ότι απαιτούνται αυτά τα δικαιώματα ή να προβλέψουν τις πιθανές επιπτώσεις που μπορεί να έχουν αυτά για το απόρρητο των χρηστών.

3.2 Πολυπλοκότητα και προβλήματα διαχείρισης αδειών

Το μοντέλο άδειας είναι το επίκεντρο της ενημέρωσης των χρηστών και της απόκτησης συναίνεσης, αλλά είναι πολύπλοκο.

Ορισμένα γνωστά ζητήματα διαχείρισης δικαιωμάτων είναι τα εξής:

· Οι προεγκατεστημένες εφαρμογές ή οι εφαρμογές OEM στο Android θα λάβουν αυτόματα όλα τα απαιτούμενα δικαιώματα.

· Τις περισσότερες φορές ο τελικός χρήστης, για να μπορέσει να χρησιμοποιήσει μια συγκεκριμένη εφαρμογή, αναγκάζεται να δώσει όλα τα απαραίτητα δικαιώματα, διαφορετικά δεν εγγυάται ότι η εφαρμογή μπορεί να λειτουργήσει σωστά.

· Οι εξουσιοδοτήσεις δεν είναι χαρτογράφηση ένα προς ένα με τις συγκεκριμένες μεθόδους που εκτίθενται από το API για τη διαχείριση των δικαιωμάτων (π.χ. πρόσβαση στην κάμερα, μπορεί επίσης να επιτρέψει την πρόσβαση στις φωτογραφίες αυτόματα).

· Η ανάκληση άδειας χρήσης δεν παρέχει εγγυήσεις στο χρήστη ότι η εφαρμογή εξακολουθεί να λειτουργεί όπως προβλέπεται (π.χ. η εφαρμογή μπορεί να αποτύχει μετά την κατάργηση των δικαιωμάτων).

· Ορισμένες εφαρμογές ενδέχεται να χρειάζονται περισσότερα δικαιώματα από αυτά που χρειάζονται για να λειτουργούν σωστά.

· Ορισμένα API ενδέχεται να εισάγουν αδυναμίες ασφαλείας, επειδή δεν παρέχουν πλήρη έλεγχο των πόρων της κινητής συσκευής, εκθέτοντας έτσι ορισμένες προσωπικές πληροφορίες που είναι αποθηκευμένες στην κινητή συσκευή σε όλες τις εφαρμογές.

Αυτές οι αδυναμίες σχεδιασμού και οι εξαιρέσεις έχουν οδηγήσει σε υπερβολική συλλογή δεδομένων, όπως στην περίπτωση του CarrierIQ, μιας προεγκατεστημένης εφαρμογής αναλυτικών στοιχείων, στην οποία χορηγήθηκε αυτόματα άδεια πρόσβασης στα ημερολόγια τηλεφώνου που περιελάμβαναν τα διαπιστευτήρια σύνδεσης , μια εφαρμογή προσευχής που αποκάλυψε την τοποθεσία του χρήστη σε όλες τις άλλες εφαρμογές και σε εφαρμογές που ζητούν πρακτικά όλα τα πιθανά δικαιώματα, όπως στην περίπτωση του Goluk, μια εφαρμογή dashcam.

Τα παραπάνω ζητήματα παραβιάζουν σαφώς ορισμένους κανόνες προστασίας δεδομένων, ιδίως την αρχή της ελαχιστοποίησης των δεδομένων, του περιορισμού του σκοπού, της ενημέρωσης και του ελέγχου, καθώς και την ασφάλεια των προσωπικών δεδομένων.

Από την άποψη του απορρήτου, υπάρχει επίσης μια θεμελιώδης πρόκληση με το πεδίο των επικίνδυνων δικαιωμάτων, όπως ορίζεται από την Google. Η διαίρεση μεταξύ των δύο δεν αντικατοπτρίζει τις πιθανές διαρροές απορρήτου από τις κανονικές άδειες. Σε ένα πείραμα που διεξήχθη στο MIT, οι ερευνητές έγραψαν ένα scraper script που εξέτασε τις δημόσιες αναφορές API του Android για τον εντοπισμό κλήσεων API που δεν απαιτούν δικαιώματα. Βρήκαν 36.000 μοναδικές κλήσεις API και, μετά από χειροκίνητη ανάλυση, επιβεβαίωσαν ότι μερικές από αυτές μπορούν να χρησιμοποιηθούν για "δακτυλικά αποτυπώματα του τηλεφώνου, αναγνώριση ευάλωτων εφαρμογών και αναγνώριση της θέσης των ιδιωτικών δεδομένων για εκμετάλλευση". Πρόκειται για ένα ζήτημα που πρέπει να επιλυθεί σε επίπεδο OS και έχει συνέπειες σε ολόκληρο το οικοσύστημα εφαρμογών για κινητά.

Στο οικοσύστημα Android, μερικά από τα κύρια προβλήματα που σχετίζονται με τα μοντέλα άδειας μπορούν να συνοψιστούν ως εξής:

Πρόβλημα 1: Κατανόηση και προσοχή από τους χρήστες

Οι χρήστες έχουν περιορισμένη κατανόηση των συναφών κινδύνων ενεργοποίησης δικαιωμάτων (ή πρόσβασης σε) σε ορισμένες εφαρμογές. Οι προγραμματιστές εφαρμογών ενδέχεται να χρησιμοποιήσουν τις εξηγήσεις Android για να εκφράσουν γιατί απαιτείται άδεια, ωστόσο οι μελέτες δείχνουν ότι οι εξηγήσεις συχνά δεν είναι ενημερωτικές. Επιπλέον, η ερώτηση των χρηστών για άδειες μπορεί να οδηγήσει σε συνηθισμένη συμπεριφορά, αποτρέποντας κάθε αποτελεσματικό έλεγχο ή συναίνεση που παρέχεται από το χρήστη που συμμετέχει στο μοντέλο άδειας.

Πρόβλημα 2: Η κατανόηση και η προσοχή από τους προγραμματιστές εφαρμογών

Μελέτες έχουν δείξει ότι οι προγραμματιστές έχουν δυσκολίες στην κατανόηση και την κατάλληλη διαχείριση των δικαιωμάτων. Σε ορισμένες περιπτώσεις, οι

προγραμματιστές ενισχύουν τις κακές αποφάσεις ασφαλείας σε επίπεδο πλατφόρμας, π.χ. επιτρέποντας σε διαφορετικά προνομιακές εφαρμογές να επικοινωνούν μεταξύ τους. Σε άλλες περιπτώσεις, ενδέχεται να απαιτούν περισσότερα δικαιώματα από όσα χρειάζονται ή / και τα δικαιώματα επιτρέπουν τη συμπλήρωση άλλων ιδιωτικών πληροφοριών, π.χ. αποτύπωσης συσκευών για παρακολούθηση.

Οι προγραμματιστές εφαρμογών έχουν ελειπή ενημέρωση σχετικά με τον τρόπο χρήσης των API για τη σωστή διαχείριση των δικαιωμάτων. Τα API είναι συχνά ανεπαρκώς τεκμηριωμένα.Η ακατάλληλη εφαρμογή ενός μοντέλου άδειας έχει ως αποτέλεσμα την απενεργοποίηση εφαρμογών κατά τη διάρκεια του χρόνου εκτέλεσης.

Πρόβλημα 3: Η κατανόηση και η προσοχή από τους προγραμματιστές του IDE και του OS

Το Android κάνει διάκριση μεταξύ κανονικών και επικίνδυνων δικαιωμάτων. Ωστόσο, όπως αναφέρθηκε προηγουμένως, οι κανονικές άδειες μπορούν να συνδυαστούν με δακτυλικά αποτυπώματα και να παρακολουθούν τους χρήστες ενάντια στη θέλησή τους. Αυτές οι διαφορετικές προνομιακές εφαρμογές, οι οποίες μπορούν να επικοινωνούν μεταξύ τους, ανοίγουν την πλατφόρμα για να προνοήσουν επιθέσεις κλιμάκωσης. Τα δικαιώματα ομάδας Android είναι τέτοια ώστε η πρόσβαση σε ένα μόνο δικαίωμα στην ομάδα να δίνει πρόσβαση σε όλα τα δικαιώματα στην ίδια ομάδα.

3.3 Δημιουργία συστάσεων σχετικά με τις άδειες

Τα προαναφερθέντα προβλήματα με τα δικαιώματα δείχνουν ότι οι προγραμματιστές εφαρμογών είναι συχνά υπεύθυνοι για προβλήματα απορρήτου αλλά όχι πάντα. Για παράδειγμα, οι προγραμματιστές Android δρουν εντός ενός οικοσυστήματος εφαρμογών που έχει κενά και εξαιρέσεις για διάφορους φορείς όταν πρόκειται να ζητήσουν άδεια.Αυτό δίνει στις βιβλιοθήκες τρίτων ένα ανώτερο χέρι στις αιτήσεις άδειας οδήγησης. και παρέχει ανεπαρκή ή παραπλανητική τεκμηρίωση API και μοντέλων δικαιωμάτων. Προκειμένου να δοθεί η δυνατότητα στους προγραμματιστές εφαρμογών να εφαρμόσουν την προστασία της ιδιωτικής ζωής και των δεδομένων κατά το σχεδιασμό, οι συνθήκες αυτές πρέπει να αλλάξουν. Μέχρι να υπάρξει μια τέτοια αλλαγή, είναι σημαντικό να δοθούν συστάσεις στους προγραμματιστές σχετικά με τον τρόπο αντιμετώπισης της ιδιωτικής ζωής σε ένα τέτοιο οικοσύστημα , τονίζοντας τις κακές πρακτικές και ενθαρρύνοντας τις καλές. Κυρίως, οι συστάσεις πρέπει να διακρίνουν πού και γιατί προκύπτουν προβλήματα ιδιωτικής ζωής, ποιος είναι ικανός και ποιος είναι υπεύθυνος για να κάνει τις

απαραίτητες αλλαγές, υπογραμμίζοντας τις ευθύνες του υπεύθυνου επεξεργασίας δεδομένων.

Μελέτες δείχνουν επίσης ότι για τους προγραμματιστές εφαρμογών η διαφορά μεταξύ ασφάλειας και ιδιωτικότητας δεν είναι ξεκάθαρη. Οι προγραμματιστές συχνά πιστεύουν ότι η προστασία της ιδιωτικής ζωής είναι ισοδύναμη με τη διασφάλιση των δεδομένων χρηστών σε κατάσταση ηρεμίας ή διαμετακόμισης, χωρίς να υπάρχει βαθιά κατανόηση των απαιτήσεων προστασίας δεδομένων. Συνεπώς, είναι σημαντικό οι συστάσεις να περιλαμβάνουν μια εισαγωγή για τον τρόπο με τον οποίο η προστασία της ιδιωτικής ζωής και των δεδομένων διαφέρει και επικαλύπτεται με την ασφάλεια.

Τέλος, σε έναν ιδανικό κόσμο, οι συστάσεις προς τους προγραμματιστές εφαρμογών θα περιλαμβάνουν επίσης βέλτιστες πρακτικές ασφάλειας, προστασίας προσωπικών δεδομένων, μεθοδολογίες ή δραστηριότητες που μπορούν να προσαρμοστούν στην ανάπτυξη εφαρμογών σε ένα ευκίνητο περιβάλλον και εργαλεία αξιολόγησης των δικών τους εφαρμογών, βιβλιοθήκες τρίτων, συμμόρφωση της προστασίας δεδομένων. Η διαρκής ενημέρωση των εν λόγω πόρων μπορεί να αποτελέσει τρομακτικό καθήκον, το οποίο μπορεί να επωφεληθεί από τη θεσμική υποστήριξη και τη συνεχή εργασία σε ένα μελλοντικό Παρατηρητήριο Προστασίας Δεδομένων και Λογισμικού.

Κεφάλιο 4. Προστασία απορρήτου και δεδομένων από το σχεδιασμό σε εφαρμογές για κινητά

Η προστασία της ιδιωτικής ζωής από τη σχεδίαση είναι μια φιλοσοφία μηχανικής συστημάτων - αρχικά διατυπωμένη από την Ann Cavoukian [3] - η οποία τονίζει το γεγονός ότι πρέπει να λαμβάνονται υπόψη οι προβληματισμοί σχετικά με την προστασία της ιδιωτικής ζωής σε ολόκληρο τον κύκλο ανάπτυξης του συστήματος, από την αρχή ενός συστήματος μέσω του σχεδιασμού, και να χρησιμοποιηθούν όλοι οι τρόποι για τον παροπλισμό του συστήματος.Σε πιο τεχνικούς όρους ανάπτυξης λογισμικού η προστασία της ιδιωτικής ζωής είναι χαρακτηριστικό ποιότητας του συστήματος [4]. Η προστασία δεδομένων από το σχεδιασμό έχει καταστεί υποχρεωτική με την έναρξη ισχύος του GDPR, αλλά πολλοί οργανισμοί εξακολουθούν να αγωνίζονται με την έννοια, τόσο από την άποψη του τι σημαίνει ακριβώς, όσο και από τον τρόπο εφαρμογής του εντός του οργανισμού.

Το κεφάλαιο αυτό στοχεύει να καταστήσει σαφέστερη την έννοια της προστασίας της ιδιωτικής ζωής, ειδικά για τους προγραμματιστές εφαρμογών για κινητά. Θα αναφερθούμε σε προσεγγίσεις σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων από το σχεδιασμό από προεπιλογή, ώστε να μεταφέρουμε τις νομικές απαιτήσεις σε πιο απτά τεχνικά θέματα που οι προγραμματιστές είναι πιο άνετοι. Συγκεκριμένα, θα εξηγήσουμε την έννοια των στόχων προστασίας δεδομένων και θα το καταστήσουμε πιο συγκεκριμένο χρησιμοποιώντας στρατηγικές σχεδιασμού απορρήτου. Και οι δύο προσεγγίσεις είναι ιδιαίτερα κατάλληλες για να κατευθύνουν την προστασία της ιδιωτικής ζωής και της προστασίας δεδομένων κατά τον σχεδιασμό στις αρχές του κύκλου ανάπτυξης του συστήματος, δηλαδή στις πρώιμες φάσεις ανάπτυξης και ανάλυσης ιδεών, όπου τυπικά ορίζεται η αρχική αρχιτεκτονική πληροφοριών. Θα περιγράψουμε τις δύο προσεγγίσεις με γενικούς όρους, αλλά θα τις εξηγήσουμε και θα τις καταστήσουμε πιο συγκεκριμένες χρησιμοποιώντας παραδείγματα από την προοπτική ανάπτυξης εφαρμογών για κινητά.

Παρατηρούμε ότι οι προσεγγίσεις που περιγράφονται σε αυτό το κεφάλαιο είναι (αναγκαιότητα) αρκετά αφηρημένες και υψηλού επιπέδου στη φύση, λόγω της μεγάλης ποικιλίας σεναρίων εφαρμογών, ακόμα και σε περιορισμένο περιβάλλον όπως η ανάπτυξη εφαρμογών για κινητά. Για το λόγο αυτό, οι προσεγγίσεις δεν αντιμετωπίζουν ειδικά τις πολυπλοκότητες του οικοσυστήματος εφαρμογών για κινητά.Στην πραγματικότητα, οι προσεγγίσεις που περιγράφονται στο παρόν κεφάλαιο μπορούν να εφαρμοστούν σε διαφορετικά επίπεδα στη διαδικασία

ανάπτυξης λογισμικού (δίνοντας πιο συγκεκριμένες συστάσεις καθώς η προσέγγιση εφαρμόζεται περαιτέρω στη διαδικασία) και μπορεί να σχετίζεται με διαφορετικά στοιχεία του οικοσυστήματος ανάπτυξης εφαρμογών. Κάθε ενδιαφερόμενος σε αυτό το οικοσύστημα μπορεί μόνο να αντιμετωπίσει τη φιλικότητα προς το ιδιωτικό απόρρητο των συστημάτων που είναι υπεύθυνα για τον εαυτό τους και εξαρτάται (μερικές φορές ζωτικής σημασίας) από τις ευκαιρίες και τους περιορισμούς του φιλικού προς το ιδιωτικό σχεδιασμό σχεδιασμού που επιβάλλουν τα άλλα συστατικά στοιχεία. Συγκεκριμένα, οι προγραμματιστές εφαρμογών περιορίζονται απο π.χ. τις ιδιότητες του τηλεπικοινωνιακού δικτύου, το σύστημα αδειών και την απουσία / παρουσία των εγκαταστάσεων εντοπισμού που προσφέρει το κινητό λειτουργικό σύστημα, καθώς και τον τρόπο λειτουργίας του καταστήματος εφαρμογών.

4.1 Στόχοι προστασίας δεδομένων

Για την ασφάλεια, η κλασική τριάδα των στόχων προστασίας, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα είναι γνωστά και αποδεκτά. Οι προγραμματιστές χρησιμοποιούνται για το πρότυπο των στόχων προστασίας της ασφάλειας και έχουν τουλάχιστον κάποια κατανόηση του γιατί έχει νόημα να θεωρούν αυτούς τους στόχους στην αναπτυξιακή διαδικασία και ότι, ανάλογα με το σκοπό ή το σενάριο μιας εφαρμογής, η σημασία κάθε στόχου προστασίας μπορεί να ποικίλει . Διάφορες κοινότητες απέκτησαν περαιτέρω στόχους προστασίας. Αυτοί ομως οι τρεις βασικοί στόχοι προστασίας αποτελούν μια σταθερή βάση για την αξιολόγηση των ιδιοτήτων ασφαλείας, τον εντοπισμό των κινδύνων και την επιλογή κατάλληλων μέτρων για την αντιμετώπιση αυτών των κινδύνων.

Από το 2009, έχουν προταθεί τρεις στόχοι προστασίας που επικεντρώνονται στην προστασία δεδομένων, προκειμένου να συμπληρωθούν οι τρεις στόχοι προστασίας της ασφάλειας: αδιαλλαξία, διαφάνεια και παρεμβατικότητα [5]. Επεκτείνουν τη γνωστή τριάδα στόχων προστασίας της ασφάλειας, αλλά μετατοπίζουν την προοπτική στο άτομο του οποίου η ιδιωτική ζωή μπορεί να διακυβεύεται και τα προσωπικά του δεδομένα να υποβάλλονται σε επεξεργασία. Αυτοί οι στόχοι προστασίας δεν επελέγησαν κατά λάθος, αλλά απορρέουν από τη νομοθεσία περί προστασίας των δεδομένων: καθένας από τους στόχους προστασίας καλύπτει τις αρχές προστασίας δεδομένων όπως αυτές ορίζονται στο GDPR, ιδίως στο άρθρο 5 του GDPR. Ακολουθεί μια πιο λεπτομερής περιγραφή, η οποία αναφέρεται στη μελέτη του ENISA σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων κατά το σχεδιασμό [6].

Η εργασία με τους στόχους προστασίας σημαίνει την εξισορρόπηση των απαιτήσεων που απορρέουν από τους στόχους προστασίας όσον αφορά δεδομένα, τεχνικές και οργανωτικές διαδικασίες. Οι εκτιμήσεις σχετικά με τη νομιμότητα, τη δικαιοσύνη και τη λογοδοσία παρέχουν καθοδήγηση για την εξισορρόπηση των απαιτήσεων και για

τη λήψη αποφάσεων σχετικά με τις επιλογές σχεδιασμού και τις κατάλληλες διασφαλίσεις.

Για όλους τους ρόλους και τους συντελεστές ενός συστήματος, μπορούν να χρησιμοποιηθούν οι στόχοι προστασίας. Αυτό είναι επίσης απαραίτητο για τον εντοπισμό δυνητικών συγκρούσεων. Για παράδειγμα, εάν η ακεραιότητα ενός αρχείου ηλεκτρονικού ταχυδρομείου επιτυγχάνεται χρησιμοποιώντας τιμές κατακερματισμού που υπολογίζονται με βάση το προηγούμενο μήνυμα ηλεκτρονικού ταχυδρομείου, κανένα ηλεκτρονικό μήνυμα δεν μπορεί να διαγραφεί χωρίς να διακυβεύεται η ακεραιότητα. Ωστόσο, σε περίπτωση που ένα υποκείμενο των δεδομένων μπορεί νόμιμα να ζητήσει τη διαγραφή ενός συγκεκριμένου ηλεκτρονικού ταχυδρομείου, το δικαίωμά του να διαγράψει δεν πρέπει να αγνοηθεί λόγω της επιλογής του μηχανισμού ακεραιότητας. Αντ 'αυτού, η επιλογή των μηχανισμών πρέπει να λαμβάνει υπόψη όλους τους στόχους προστασίας στον αναγκαίο βαθμό. Αυτό το φαινόμενο είναι επίσης γνωστό και στο πλαίσιο της ασφάλειας των πληροφοριών, π.χ. όταν πρέπει να υπολογίσουμε υπό ποιες συνθήκες θα πρέπει να διαγραφούν τα δεδομένα (για να αποφευχθεί η παραβίαση της εμπιστευτικότητας) ή να διατηρηθούν (για να επιτευχθεί διαθεσιμότητα).

Οι ορισμοί των στόχων προστασίας και η περιγραφή του τυποποιημένου προτύπου προστασίας δεδομένων έχουν προταθεί από τη γερμανική διάσκεψη αρχών προστασίας δεδομένων ως μέσο για ελέγχους προστασίας δεδομένων [7]. Το πρότυπο προστασίας δεδομένων δεν μπορεί να χρησιμοποιηθεί μόνο για την αξιολόγηση των υφιστάμενων συστημάτων επεξεργασίας δεδομένων, αλλά είναι χρήσιμο στη διαδικασία σχεδιασμού τόσο για προγραμματιστές όσο και για ελεγκτές ή επεξεργαστές. Τα τεχνολογικά και οργανωτικά μέτρα αφορούν το σύνολο της ροής εργασίας και τον πλήρη κύκλο ζωής των προσωπικών δεδομένων.

4.1.2 Αντιμετώπιση στόχων προστασίας δεδομένων σε εφαρμογές για κινητά

Παρακάτω εστιάζουμε την προσοχή μας στην προστασία δεδομένων εφαρμογών για κινητά. Για παράδειγμα, ο στόχος προστασίας της αδυναμίας σύνδεσης μπορεί να είναι λιγότερο απαιτητικός σε μια κατάσταση όπου η σύνδεση μεταξύ εφαρμογών είναι απαραίτητη για το σκοπό ή είναι τουλάχιστον επιτρεπτή, π.χ. όταν ένας χρήστης επιλέγει να μοιραστεί δεδομένα από μια εφαρμογή με τις επαφές του.

Ορισμένα παραδείγματα στην παρακάτω λίστα ενδέχεται να απαιτούνται από το νόμο στο πλαίσιο του GDPR (π.χ. πολλά από τα ζητήματα διαφάνειας), ενώ για άλλα η εφαρμογή θα συνιστούσε τουλάχιστον ως βέλτιστη πρακτική:

Ασυμβατότητα:

- Για κάθε εφαρμογή ο σκοπός (οι) θα πρέπει να καθοριστεί και να δηλωθεί εκ των προτέρων. Πρέπει να υποβάλλονται σε επεξεργασία μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για τον (τους) σκοπό (ους).
- Η εφαρμογή πρέπει να απομονωθεί από την πλατφόρμα όσο το δυνατόν περισσότερο.Τα δεδομένα χρήσης που αφορούν την εφαρμογή δεν θα πρέπει να κοινοποιούνται στον πάροχο της πλατφόρμας.
- Οι διαφορετικές εφαρμογές, δηλαδή η επεξεργασία προσωπικών δεδομένων για διαφορετικούς σκοπούς, θα πρέπει να απομονωθούν από προεπιλογή. Η ανταλλαγή δεδομένων πρέπει να αποτρέπεται εκτός εάν έχει καθοριστεί ρητά ή άλλως επιλεγεί από τον χρήστη.
- Τα μοναδικά αναγνωριστικά δεν πρέπει να χρησιμοποιούνται για διαφορετικούς σκοπούς προκειμένου να αποφευχθεί η ανεπιθύμητη σύνδεση μεταξύ αναγνωριστικών.
- Τα προσωπικά δεδομένα θα πρέπει να διαγράφονται το συντομότερο δυνατό.
- Εάν τα προσωπικά δεδομένα δεν μπορούν να διαγραφούν, θα πρέπει να είναι ανώνυμα ή, εάν αυτό δεν είναι δυνατόν, να περιέχουν ψευδώνυμα το συντομότερο δυνατόν.
- Σε περίπτωση που η εφαρμογή προσφέρει διαφορετικούς τρόπους διαμόρφωσης, η προεπιλεγμένη διαμόρφωση θα πρέπει να εξασφαλίζει την επεξεργασία μόνο δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητα για το σκοπό αυτό, δηλαδή ελάχιστη συλλογή προσωπικών δεδομένων, ελάχιστη έκταση επεξεργασίας, ελάχιστη περίοδος αποθήκευσης, ελάχιστη προσβασιμότητα.
- Οι λειτουργίες που ενδέχεται να παραβιάζουν την ιδιωτικότητα και την ασφάλεια των χρηστών δεν θα πρέπει να ενεργοποιούνται προτού ο χρήστης εκουσίως και με γνώση των σχετικών κινδύνων δώσει τη συγκατάθεσή του. Αυτό περιλαμβάνει τη λειτουργία μεταφοράς δεδομένων ήχου ή βίντεο από την πλευρά του χρήστη (π.χ. ένα ενεργοποιημένο μικρόφωνο ή μια ενεργοποιημένη λειτουργία βίντεο), δεδομένα θέσης ή δεδομένα από τις επαφές του χρήστη.
- Οι χρήστες θα πρέπει να μπορούν να χρησιμοποιούν μια εφαρμογή χωρίς σύνδεση δικτύου και πιθανή ροή δεδομένων σε άλλα μέρη (π.χ. χρησιμοποιώντας έναν χάρτη εκτός σύνδεσης), εφόσον το επιτρέπει η εφαρμογή.
- Η εφαρμογή θα πρέπει να συνεργάζεται με εργαλεία προστασίας των προσωπικών δεδομένων.

Διαφάνεια:

- Οι χρήστες θα πρέπει να ενημερώνονται για τις πληροφορίες σχετικά με την προστασία της ιδιωτικής ζωής που συλλέγονται και αναλύονται. Αυτό περιλαμβάνει τόσο την εφαρμογή όσο και τον σχετικό κώδικα που παρέχεται από άλλα μέρη.
- Οι χρήστες θα πρέπει να ενημερώνονται για οποιαδήποτε ροή δεδομένων όσον αφορά την προστασία της ιδιωτικής ζωής και των δεδομένων.
- Οι χρήστες θα πρέπει να είναι σε θέση να κατανοήσουν από πού θα λάβουν βοήθεια για ερωτήσεις ή υποστήριξη (help desk). Ακόμη και σε περίπλοκα συστήματα, ο τρόπος για να λάβετε βοήθεια θα πρέπει να είναι σαφής. Σε περίπτωση διαφορετικών οργανώσεων που προσφέρουν βοήθεια, πρέπει να διευκρινιστούν οι αντίστοιχες αρμοδιότητες.
- Οι απαραίτητες πληροφορίες θα πρέπει να κοινοποιούνται στους χρήστες με τρόπο που να γίνεται εύκολα κατανοητός. Αυτό θα μπορούσε να περιλαμβάνει πολιτικές πολλαπλών επιπέδων με τις πιο σημαντικές πληροφορίες για το πρώτο στρώμα, υποστήριξη από οπτικά εικονίδια, πληροφορίες ήχου και μηχανικά αναγνώσιμες προσεγγίσεις.
- Θα πρέπει να υπάρχει λεπτομερής τεκμηρίωση του ανεπτυγμένου συστήματος. Η τεκμηρίωση θα πρέπει να περιέχει ειδικά ποια δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία και ποια ροή δεδομένων ενδέχεται ή θα συμβεί.
- Πρέπει να τεκμηριώνονται οι διεπαφές της εφαρμογής και οι δυνατότητες συνδυασμού της χρήσης της εφαρμογής με τα εργαλεία προστασίας δεδομένων.
- Οι δραστηριότητες των διαχειριστών και / ή οι αλλαγές του συστήματος πληροφορικής θα πρέπει να καταγράφονται στον απαραίτητο βαθμό, π.χ. για την υποστήριξη της ακεραιότητας του συστήματος και για την απόδειξη της σωστής επεξεργασίας των δεδομένων.
- Πρέπει να τεκμηριώνεται η διαχείριση κινδύνου, καθώς και η συμμόρφωση με τις απαιτήσεις του GDPR, π.χ. σε μια εκτίμηση αντικτύπου προστασίας δεδομένων.
- Πρέπει να κοινοποιηθούν λύσεις βέλτιστης πρακτικής και συγκεκριμένα επιτεύγματα για την προστασία της ιδιωτικής ζωής, ώστε να μπορούν άλλοι να αντλήσουν διδάγματα από αυτά τα επιτεύγματα και εμπειρίες.

Παρεμβατικότητα:

- Οι χρήστες θα πρέπει να έχουν τη δυνατότητα να ασκούν τα δικαιώματα των υποκειμένων των δεδομένων: πρόσβαση, διόρθωση, διαγραφή, παράδοση και ανάκληση συγκατάθεσης, φορητότητα.
- Οι χρήστες θα πρέπει να διαθέτουν κεντρικό σημείο επικοινωνίας για πιθανές καταγγελίες.
- Οι χρήστες θα πρέπει να μπορούν να αλλάζουν την προκαθορισμένη ρύθμιση ανάλογα με τις ανάγκες τους.
- Κατά την αλλαγή μιας προκαθορισμένης ρύθμισης "προστασίας δεδομένων από προεπιλογή", θα πρέπει να γίνει με την κατάλληλη λεπτομέρεια, εμποδίζοντας έτσι την πλήρη απώλεια της προστασίας των χρηστών.
- Η συμμετοχή όλων των χρηστών πρέπει να λαμβάνει υπόψη τις απαιτήσεις χρηστικότητας.
- Θα πρέπει να είναι δυνατή η παροχή των απαραίτητων ενημερώσεων.
- Θα πρέπει να είναι δυνατή η άμεση διακοπή οποιασδήποτε ροής δεδομένων.
- Θα πρέπει να είναι δυνατή η ανταλλαγή στοιχείων (όπως βιβλιοθήκες τρίτων ή σύννεφο).
- Πρέπει να εξασφαλίζονται οι σωστές αντιδράσεις σε αλλαγές ή συμβάντα που επηρεάζουν τη λειτουργικότητα προστασίας του συστήματος. Μεταξύ άλλων, πρέπει να εγκατασταθούν επιδιορθώσεις ενάντια σε τρωτά σημεία.

4.2 Στρατηγικές σχεδιασμού

Όπως περιγράφεται από τους Colesky, Hoepman και Hillen [8], μια στρατηγική σχεδίασης απορρήτου προσδιορίζει έναν ξεχωριστό αρχιτεκτονικό στόχο στην προστασία της ιδιωτικής ζωής για να επιτευχθεί ένα ορισμένο επίπεδο προστασίας της ιδιωτικής ζωής. Σημειώνεται ότι αυτό είναι διαφορετικό από αυτό που εννοείται ως αρχιτεκτονική στρατηγική στον τομέα της τεχνολογίας λογισμικού. Αντ 'αυτού, οι στρατηγικές μας μπορούν να θεωρηθούν ως οι στόχοι της προστασίας της ιδιωτικής ζωής. Εδω περιγράφουμε συνοπτικά τις οκτώ στρατηγικές σχεδιασμού της ιδιωτικής ζωής [9] και δίνουμε παραδείγματα για το πώς θα μπορούσαν να εφαρμοστούν κατά την ανάπτυξη μιας εφαρμογής για κινητά.

4.2.1 Περιορισμός

Ορισμός: Περιορίστε όσο το δυνατόν περισσότερο την επεξεργασία των προσωπικών δεδομένων.

Σχετικές τακτικές:

- Αποφεύγετε την επεξεργασία των προσωπικών δεδομένων του υποκειμένου των δεδομένων, εν μέρει ή εξ ολοκλήρου.
- Επιλέξτε να αποφασίζετε κατά περίπτωση για την πλήρη ή μερική χρήση προσωπικών δεδομένων.
- Αφαίρεση περιττών πεδίων προσωπικών δεδομένων του κάθε χρήστη από το σύστημα.
- Καταστρέψτε εντελώς τα προσωπικά δεδομένα του υποκειμένου δεδομένων.

Παράδειγμα: Οι εφαρμογές πρέπει να περιορίζουν στο ελάχιστο την πρόσβασή τους σε αισθητήρες (θέση, κίνηση, κάμερα, μικρόφωνο) και τοπικά αποθηκευμένα δεδομένα (εικόνες, επαφές). Η εφαρμογή φακός που ζητά άδεια πρόσβασης σε όλα αυτά είναι το τέλειο αντί-παράδειγμα αυτής της περίπτωσης. Μια εφαρμογή για καιρικές συνθήκες που ζητά την τοποθεσία, για να δώσει τοπικές πληροφορίες καιρού, μπορεί να είναι αποδεκτή. Σημειώστε, ωστόσο, ότι για μια εφαρμογή καιρού για την πρόγνωση καιρού δεν χρειάζεται να γνωρίζει την ακριβή τοποθεσία. Αντίθετα, το όνομα της πόλης είναι αρκετό.

4.2.2 Διαχωρισμός

Ορισμός: Αποτρέψτε τη συσχέτιση των προσωπικών δεδομένων διαχωρίζοντας την επεξεργασία λογικά ή φυσικά.

Σχετικές τακτικές:

- Διαμοιρασμός προσωπικών δεδομένων έτσι ώστε να απαιτείται περισσότερη πρόσβαση για την επεξεργασία τους.
- Επεξεργασία προσωπικών δεδομένων ανεξάρτητα, χωρίς πρόσβαση ή συσχετισμό με συναφή μέρη.

Παράδειγμα: Οι κινητές συσκευές είναι εξαιρετικά ισχυρές από την άποψη της επεξεργασίας, του εύρους ζώνης και της αποθήκευσης και μπορούν επομένως να εκτελούν πολλές τοπικές εργασίες που ήταν αδιανόητες πριν από αρκετά χρόνια. Για παράδειγμα, η αναγνώριση εικόνων μπορεί να γίνει στο έξυπνο τηλέφωνο, έτσι ώστε η μεταφόρτωση εικόνων σε κεντρικό διακομιστή να μην είναι πλέον απαραίτητη. Επίσης, οι αυξημένες δυνατότητες δικτύωσης κάνουν τις εφαρμογές peer-to-peer, όπου οι χρήστες μοιράζονται απευθείας ή επικοινωνούν χωρίς τη βοήθεια κεντρικού εξυπηρετητή πιθανές. Συγκεκριμένα, τα κοινωνικά δίκτυα "peer-to-peer" είναι, από τεχνική άποψη, μια πιθανότητα.

4.2.3 Αφηρημένος

Ορισμός:Περιορίστε όσο το δυνατόν περισσότερο τη λεπτομέρεια των επεξεργασμένων προσωπικών δεδομένων.

Σχετικές τακτικές:

- Εξάγοντας τα κοινά στοιχεία των προσωπικών δεδομένων εντοπίζοντας και επεξεργάζοντας συσχετισμούς αντί των ίδιων των δεδομένων.
- Λιγότερες λεπτομέρειες από τα δεδομένα προσωπικού χαρακτήρα πριν από την επεξεργασία, με την κατανομή σε κοινές κατηγορίες.
- Να προσθέσετε θόρυβο ή να προσεγγίσετε την πραγματική τιμή ενός στοιχείου δεδομένων

Παράδειγμα: Οι υπηρεσίες που βασίζονται σε τοποθεσίες τυπικά χρειάζονται μόνο μια κατά προσέγγιση ένδειξη της θέσης του τρέχοντος χρήστη, για να προσφέρουν μια επισκόπηση των υπηρεσιών κοντά σε αυτήν την τοποθεσία. Επομένως, αντί να χρησιμοποιήσετε τις ακριβείς συντεταγμένες GPS που προσφέρει το έξυπνο τηλέφωνο, μια εφαρμογή βασισμένη σε τοποθεσία θα μπορούσε να υπολογίσει μια πιο γενική θέση πριν ζητήσει από τις κεντρικές υπηρεσίες τις σχετικές υπηρεσίες. Στην πραγματικότητα, οι κινητές συσκευές θα μπορούσαν να διαθέτουν διάφορα επίπεδα χωρητικότητας της θέσης ως κλήσεις API OS και ακόμη και να επιτρέπουν στους χρήστες να χορηγούν ή να αποκλείουν την πρόσβαση σε ακριβέστερα δεδομένα τοποθεσίας ανά εφαρμογή.

Μια πιο γενική προσέγγιση της επαλήθευσης του ιδιωτικού απορρήτου είναι όταν επιτρέπεται στους χρήστες να έχουν πρόσβαση σε δεδομένα βάσει γενικότερων χαρακτηριστικών (π.χ. εάν ο χρήστης έχει συνδρομή), αντί να χρησιμοποιεί την ταυτότητα του ατόμου για να πάρει την απόφαση πρόσβασης. Τα λεγόμενα διαπιστευτήρια βασισμένα στα χαρακτηριστικά (ABCs) υποστηρίζουν ότι αυτό είναι φιλικό προς το ιδιωτικό απόρρητο.

4.2.4 Απόκρυψη

Ορισμός: να προστατεύονται τα προσωπικά δεδομένα ή να γίνονται ανεξάρτητα ή μη παρατηρήσιμα. Αποτρέψτε τη δημοσιοποίηση των προσωπικών δεδομένων. Αποτρέψτε την έκθεση προσωπικών δεδομένων περιορίζοντας την πρόσβαση ή κρύβοντας την ίδια την ύπαρξή τους.

Σχετικές τακτικές:

- Αποτροπή μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα.
- Επεξεργασία προσωπικών δεδομένων τυχαία μέσα σε μια αρκετά μεγάλη ομάδα για να μειωθεί ο συσχετισμός.
- Κρυπτογράφηση δεδομένων (σε διαμετακόμιση ή σε ηρεμία).
- Αποτρέψτε την αλλοίωση των προσωπικών δεδομένων σε εκείνους που δεν έχουν τη δυνατότητα να τις αποκρυπτογραφήσουν.
- Απομάκρυνση της συσχέτισης μεταξύ διαφορετικών προσωπικών δεδομένων.

Παράδειγμα: Σε ελάχιστες εφαρμογές θα πρέπει να κρυπτογραφούνται όλες οι επικοινωνίες τους και να χρησιμοποιούνται αποτυπώματα πιστοποιητικών (ή προεγκατεστημένα κλειδιά) για να αποτρέπονται οι επιθέσεις μεσαίων ατόμων όταν οι αντίπαλοι είναι σε θέση να θέσουν σε κίνδυνο την υποδομή πιστοποιητικών TLS. Οι πιο προηγμένες εφαρμογές θα προσπαθήσουν να αποκρύψουν τα μεταδεδομένα χρησιμοποιώντας τεχνικές ανάμειξης ή να αναπτύξουν ένα δίκτυο δρομολόγησης (π.χ. Tor).

4.2.5 Πληροφόρηση

Ορισμός: να παρέχονται στα πρόσωπα στα οποία αναφέρονται τα δεδομένα επαρκείς πληροφορίες σχετικά με τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται, τον τρόπο με τον οποίο υποβάλλονται σε επεξεργασία και για ποιο σκοπό.

Σχετικές τακτικές:

- Παροχή εκτεταμένων πόρων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων πολιτικών, διαδικασιών και δυνητικών κινδύνων.
- Ειδοποίηση των υποκειμένων των δεδομένων για τυχόν νέες πληροφορίες σχετικά με την επεξεργασία των προσωπικών τους δεδομένων εγκαίρως.
- Λεπτομερή στοιχεία σχετικά με την επεξεργασία των προσωπικών δεδομένων σε μια συνοπτική και κατανοητή μορφή.

Παράδειγμα 1: Μια πιθανή μέθοδος για να μεταβιβάσει διαισθητικά τον τρόπο με τον οποίο μια εφαρμογή χειρίζεται τα προσωπικά δεδομένα, ειδικά δεδομένης της μικρής οθόνης ενός έξυπνου τηλεφώνου, είναι να χρησιμοποιεί εικονίδια απορρήτου.

Παράδειγμα 2: Επίσης, η πρόσβαση σε αισθητήρες ή τοπικά αποθηκευμένα δεδομένα μπορεί να υποδηλώνεται στον χρήστη με λιγότερο ενοχλητικούς τρόπους

από ένα "ok-ή-cancel", δηλ. Για παράδειγμα, με τη χρήση ειδικών εικονιδίων που όταν πατηθουν,δίνουν στο χρήστη την επιλογή να αλλάξει τις ρυθμίσεις για να αντιμετωπίσει οποιεσδήποτε ανησυχίες σχετίζονται με την πρόσβαση. Ως συγκεκριμένο παράδειγμα, μπορούμε να εξετάσουμε τη χρήση ενός μικρού βέλους στη γραμμή κατάστασης στην κορυφή της οθόνης των συσκευών iOS για να σηματοδοτήσουμε την (πρόσφατη) χρήση των υπηρεσιών εντοπισμού θέσης.

4.2.6 Έλεγχος

Ορισμός: να παρέχονται στους φορείς δεδομένων οι μηχανισμοί ελέγχου της επεξεργασίας των προσωπικών δεδομένων τους.

Σχετικές τακτικές

- Επεξεργασία μόνο των προσωπικών δεδομένων για τα οποία έχει ληφθεί ρητή, ελεύθερη και ενημερωμένη συγκατάθεση.
- Επιτρέποντας την επιλογή ή τον αποκλεισμό προσωπικών δεδομένων, εν μέρει ή εξ ολοκλήρου, από οποιαδήποτε επεξεργασία.
- Να παρέχονται στα πρόσωπα στα οποία αναφέρονται τα δεδομένα τα μέσα για να διατηρούν τα προσωπικά τους δεδομένα ακριβή και ενημερωμένα.
- Να τηρηθεί το δικαίωμα του υποκειμένου των δεδομένων στην πλήρη κατάργηση οποιωνδήποτε προσωπικών δεδομένων εγκαίρως.

Παράδειγμα: Όταν ζητάτε δικαιώματα πρόσβασης σε αισθητήρες (τοποθεσία, κίνηση, κάμερα, μικρόφωνο) και τοπικά αποθηκευμένα δεδομένα (εικόνες, επαφές), οι εφαρμογές για κινητά πρέπει να εξακολουθούν να λειτουργούν (ίσως να προσφέρουν περιορισμένη λειτουργικότητα).

4.2.7 Επιβολή

Ορισμός: δεσμεύστε έναν τρόπο φιλικό προς το ιδιωτικό απόρρητο για την επεξεργασία προσωπικών δεδομένων και την επιβολή τους.

Σχετικές τακτικές:

- Αναγνώριση της αξίας της ιδιωτικής ζωής και λήψη αποφάσεων σχετικά με πολιτικές που της επιτρέπουν και διαδικασίες που σέβονται τα προσωπικά δεδομένα.
- Εξέταση της ιδιωτικότητας κατά το σχεδιασμό ή την τροποποίηση χαρακτηριστικών και ενημέρωση πολιτικών και διαδικασιών για καλύτερη προστασία των προσωπικών δεδομένων.
- Εξασφάλιση ότι τηρούνται οι πολιτικές.

Παράδειγμα: Πρώτα απ 'όλα, αυτή η στρατηγική απαιτεί από τον προγραμματιστή εφαρμογών να καθορίσει και να εφαρμόσει μια πολιτική απορρήτου. Μια άλλη προσέγγιση είναι να δημιουργηθεί ένα σύστημα διαχείρισης απορρήτου παρόμοιο με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που ορίζεται στο ISO 27001.

4.2.8 Επίδειξη

Ορισμός: προσκομίστε αποδεικτικά στοιχεία ότι επεξεργάζεστε τα προσωπικά σας δεδομένα με τρόπο φιλικό προς την ιδιωτικότητα.

Σχετικές τακτικές:

- Παρακολούθηση της επεξεργασίας δεδομένων, χωρίς αποκάλυψη προσωπικών δεδομένων, εξασφάλιση και επανεξέταση των πληροφοριών που συλλέγονται για τυχόν κινδύνους.
- Εξέταση όλων των καθημερινών δραστηριοτήτων για τυχόν κινδύνους για τα προσωπικά δεδομένα και αντιμετώπιση σοβαρών αποκλίσεων.
- Να αναλύονται περιοδικά οι πληροφορίες που συλλέγονται σχετικά με τις δοκιμές, τους ελέγχους και τα αρχεία καταγραφής για να εξεταστούν οι βελτιώσεις στην προστασία των προσωπικών δεδομένων.

Παράδειγμα: Εκτός από τις αυτοσυντηρητικές τακτικές που αναφέρθηκαν παραπάνω, όπου η καταγραφή μπορεί να γίνει τόσο κεντρικά όσο και στο έξυπνο τηλέφωνο (και ως εκ τούτου ο έλεγχος μπορεί να γίνει τόσο σε κεντρικό επίπεδο όσο και στη συσκευή του χρήστη, ίσως από ένα ανεξάρτητα ανεπτυγμένο και παρεχόμενο εργαλείο), η στρατηγική "επίδειξης" επιβαρύνει επίσης τον προγραμματιστή της εφαρμογής για να επιλέξει προσεκτικά τις βιβλιοθήκες που παρέχουν τρίτα μέρη και περιλαμβάνει την εφαρμογή ορισμένων λειτουργιών. Συγκεκριμένα, πρέπει να ελεγχθεί (επαληθεύσιμα τεκμηριωμένα) ότι η βιβλιοθήκη δεν παραβιάζει την πολιτική απορρήτου.

Επίσης, η εκπόνηση κατάλληλης αξιολόγησης αντικτύπου προστασίας δεδομένων και η τεκμηρίωση του αποτελέσματός της είναι βασικός συντελεστής αυτής της στρατηγικής.

4.3 Σχετικά με τις στρατηγικές σχεδιασμού απορρήτου και τους στόχους προστασίας δεδομένων

Οι στρατηγικές σχεδίασης για την προστασία της ιδιωτικής ζωής στοχεύουν στην τελειοποίηση των στόχων προστασίας δεδομένων, ιδίως μέσω του ορισμού των σχετικών τακτικών, και σε ορισμένες περιπτώσεις διευρύνουν το πεδίο εφαρμογής πέραν εκείνου του χρήστη (γνωστού και ως υποκείμενο δεδομένων) περιλαμβάνει την προοπτική του υπεύθυνου επεξεργασίας δεδομένων. Ας κάνουμε λίγο πιο ξεκάθαρη τη σχέση μεταξύ των στόχων προστασίας δεδομένων και των στρατηγικών σχεδιασμού απορρήτου. Ο στόχος προστασίας «μη δεσμευτικότητας» ενσωματώνει τόσο τη στρατηγική «Απόκρυψη» όσο και τη στρατηγική του «Διαχωρισμού» στρατηγική.

Ο στόχος προστασίας «Διαφάνεια» αντιστοιχεί ένας προς έναν με τη στρατηγική «Πληροφόρηση». Η στρατηγική αυτή εξαρτάται φυσικά από τη στρατηγική «Εφαρμογή» για τον ορισμό της πολιτικής απορρήτου. Επισημαίνουμε, ωστόσο, ότι η στρατηγική «Επιβάλω» υπερβαίνει κατά πολύ το στόχο της «διαφάνειας», καθόσον απαιτεί από έναν υπεύθυνο επεξεργασίας δεδομένων να διατηρεί αυτή την πολιτική απορρήτου εντός του οργανισμού ελέγχου δεδομένων. Αυτό συνεπάγεται, μεταξύ άλλων, τη δημιουργία ενός συστήματος διαχείρισης της ιδιωτικής ζωής (συγκρίσιμο με ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών [10]) και την ανάθεση ευθυνών και πόρων στον οργανισμό.

Ο στόχος προστασίας «παρεμβολής» αντιστοιχεί, επίσης, στη στρατηγική «έλεγχος». Και πάλι η στρατηγική «Επιδεικνύω» δεν αποτελεί πλήρως μέρος αυτού του στόχου προστασίας, καθώς στοχεύει κυρίως στην προοπτική του υπεύθυνου επεξεργασίας δεδομένων και στις σχέσεις του με την αρχή προστασίας δεδομένων. Είναι μάλλον μέρος του στόχου προστασίας «Διαφάνεια».

Βλέπουμε ότι η στρατηγική «Επιβάλλω» και, σε μικρότερο βαθμό, «Επιδεικνύω» δεν αποτελούν μέρος των στόχων προστασίας δεδομένων που περιγράφονται παραπάνω. Αυτό μπορεί να εξηγηθεί από το γεγονός ότι οι στρατηγικές σχεδιασμού της ιδιωτικότητας αποσκοπούν στη βελτίωση και επέκταση των στόχων προστασίας της ιδιωτικής ζωής στον τομέα της διαχείρισης της προστασίας δεδομένων.

4.4 Προς μια μεθοδολογία απορρήτου από το σχεδιασμό για εφαρμογές

Η τεχνολογία απορρήτου είναι ένα θέμα ενεργητικής και συνεχιζόμενης έρευνας, αλλά, λείπει αυτή τη στιγμή μια συγκεκριμένη και απλή μέθοδος για την εφαρμογή της προστασίας της ιδιωτικής ζωής από το σχεδιασμό των προγραμματιστών

εφαρμογών.Πιστεύουμε ότι μια ελαφριά μεθοδολογία που βασίζεται, για παράδειγμα, στις στρατηγικές σχεδιασμού της ιδιωτικής ζωής σε συνδυασμό με τους στόχους προστασίας δεδομένων είναι εφικτή, αρκεί να λαμβάνει υπόψη τις τρέχουσες πρακτικές και πολυπλοκότητες ανάπτυξης εφαρμογών. Το κύριο πλεονέκτημα αυτής της προσέγγισης είναι ότι διαχωρίζει σαφώς τις νομικές απαιτήσεις από τους πιο συγκεκριμένους τεχνικούς στόχους. Αυτό καταργεί την τρέχουσα αδικαιολόγητη προσδοκία ότι οι μηχανικοί πρέπει να σκέφτονται σαν δικηγόροι ή κοινωνικοί επιστήμονες. Παρόλο που η προσέγγιση αυτή δεν αποκλείει την ανάγκη ελέγχου της συμμόρφωσης με τις λεπτομερείς νομικές απαιτήσεις που μπορούν να θεσπιστούν, εξακολουθεί να αποτελεί τεράστιο βήμα προς την κατεύθυνση της οικοδόμησης αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων. Με αυτόν τον τρόπο, η προσέγγιση αυτή μπορεί να προσφέρει πολύ καλύτερες λύσεις από την τρέχουσα κατάσταση όπου σπάνια ενσωματώνονται οι εγγυήσεις προστασίας της ιδιωτικής ζωής και των δεδομένων. Επιπλέον, τόσο οι στόχοι προστασίας δεδομένων όσο και οι στρατηγικές σχεδίασης απορρήτου παρέχουν ένα μέσο έκφρασης απαιτήσεων και επιλογών σε γλώσσα που μπορεί να κατανοηθεί σε όλους τους κλάδους.

Ένα πρώτο βήμα προς μια τέτοια μεθοδολογία αποτελεί η επισκόπηση των βέλτιστων πρακτικών,σχεδιαστικά μοτίβα καθώς και τα λάθη απο τα οποία πρέπει να μάθουμε. Από αυτά τα παραδείγματα μπορεί να καταστεί σαφές ότι ακόμη και φαινομενικά μικρές αρχιτεκτονικές αποφάσεις μπορεί να έχουν τεράστια επίδραση στην προστασία της ιδιωτικής ζωής και των δεδομένων:

- Μια άλλη απόφαση που πρέπει να ληφθεί είναι η τοποθεσία αποθήκευσης και επεξεργασίας δεδομένων. Αυτό επηρεάζει το ποιος μπορεί να έχει πρόσβαση στα προσωπικά δεδομένα (π.χ. εάν τα δεδομένα αποθηκεύονται σε απομακρυσμένο σύννεφο, ενδεχομένως κάτω από μια δικαιοδοσία που επιτρέπει την κυβερνητική πρόσβαση) και πόσο καλά μπορούν να εξασφαλιστούν (π.χ. κατά της πειρατείας ή σε περίπτωση που ο χρήστης χάσει το τηλέφωνο).
- Η απόφαση σχετικά με τη λειτουργικότητα που είναι ενσύρματη (π.χ. πάντα κρυπτογραφημένη επικοινωνία) και τι μπορεί να ρυθμίσει ο χρήστης επηρεάζει τον βαθμό προστασίας προσωπικών δεδομένων.Ο προγραμματιστής πρέπει να αποφασίσει εάν υπάρχει μια προκαθορισμένη ρύθμιση ή εάν ο χρήστης ερωτηθεί κατά την ώρα εγκατάστασης.

5. Συμπεράσματα και Προτάσεις

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, η προστασία της ιδιωτικής ζωής και των δεδομένων αντιμετωπίζει μερικές σοβαρές προκλήσεις στον τομέα των εφαρμογών για κινητά, ιδίως λόγω της πολυπλοκότητας των σημερινών οικοσυστημάτων εφαρμογής και των αναπτυξιακών πρακτικών. Ειδικά οι προγραμματιστές εφαρμογών, ακόμη και αν γνωρίζουν τις βασικές νομικές απαιτήσεις (από τον κανονισμό για την προστασία του ιδιωτικού απορρήτου), αγωνίζονται συχνά να τις ενσωματώσουν στα προϊόντα τους και να αντιμετωπίσουν αρκετούς περιορισμούς, εξαιτίας περιορισμών άλλων φορέων του οικοσυστήματος λογισμικό τρίτων, κλπ.).

Μετά την ανάλυση στο προηγούμενο κεφάλαιο, σε αυτό το κεφάλαιο εξάγουμε μερικά βασικά συμπεράσματα και κάνουμε σχετικές προτάσεις και συστάσεις για την ενσωμάτωση της προστασίας της ιδιωτικής ζωής και των δεδομένων από το σχεδιασμό στη διαδικασία ανάπτυξης εφαρμογών. Όπως και σε όλη την εργασία, η εστίασή μας βασίζεται κυρίως στους προγραμματιστές εφαρμογών, καθώς αυτές οι οντότητες ενδέχεται να διαδραματίσουν από το σχεδιασμό τους κεντρικό ρόλο στις ιδιότητες απορρήτου και ασφάλειας των εφαρμογών για κινητά.

5.1 Παροχή καθοδήγησης στους προγραμματιστές εφαρμογών

Όπως δείχνει η έρευνά μας, ένα σημαντικό ζήτημα στον τομέα των εφαρμογών για κινητά και της ιδιωτικής ζωής είναι το χάσμα ανάμεσα στις νομικές απαιτήσεις και τη μετάφραση αυτών των απαιτήσεων σε πρακτικές λύσεις που μπορούν να εφαρμόσουν οι προγραμματιστές εφαρμογών. Πράγματι, οι υπάρχουσες συστάσεις προς τους προγραμματιστές εφαρμογών παρέχουν συνήθως πληροφορίες μόνο για το τι πρέπει να κάνουν οι προγραμματιστές, χωρίς περαιτέρω καθοδήγηση σχετικά με τον τρόπο με τον οποίο θα μπορέσουν να εκπληρώσουν αυτές τις απαιτήσεις.

Για παράδειγμα, στον τομέα των αδειών, παρατηρούμε ότι η καθοδήγηση σχετικά με την προστασία δεδομένων επικεντρώνεται στον τρόπο με τον οποίο οι πάροχοι υπηρεσιών / προγραμματιστές θα πρέπει να οργανώνουν τη συγκατάθεσή τους όσον αφορά τις προσωπικές πληροφορίες που συλλέγουν και επεξεργάζονται. Κατά μία έννοια, απαντούν σε μια ερώτηση: "Τι πρέπει να κάνει ο πάροχος / προγραμματιστής της εφαρμογής; Πρέπει να ζητήσει συγκατάθεση ». Ωστόσο, οι συστάσεις περιέχουν λιγότερο ή καθόλου καθοδήγηση για το πώς θα ζητήσουν τη συναίνεση, η οποία είναι βασική για την προστασία της ιδιωτικής ζωής από το σχεδιασμό. Το "πώς, πότε, με ποιον τρόπο" είναι οι ερωτήσεις που οι προγραμματιστές εφαρμογών πρέπει να ρωτήσουν όταν πρόκειται να μεταφράσουν μερικά από αυτά στα μοντέλα άδειας που παρέχονται από το διαφορετικό λειτουργικό σύστημα. Ως εκ τούτου, ιδανικά, οι

συστάσεις που είναι εφαρμόσιμες για τους προγραμματιστές εφαρμογών θα πρέπει να περιλαμβάνουν απαντήσεις σε ορισμένες βασικές ερωτήσεις όπως:

- Πότε πρέπει οι προγραμματιστές να ζητούν την άδεια (π.χ. κατά την εγκατάσταση, κατά το χρόνο εκτέλεσης, όταν ενημερώνεται μια εφαρμογή);
- Πόσο συχνά πρέπει οι προγραμματιστές να προτρέπουν τους χρήστες για άδειες και πώς πρέπει να αντιμετωπίζουν τις συνήθειες των χρηστών;
- Υπάρχουν τρόποι να επανασχεδιάσετε τη λειτουργικότητα των εφαρμογών (ή την πλατφόρμα λειτουργικών συστημάτων) έτσι ώστε ο αριθμός των απαραίτητων δικαιωμάτων να μπορεί να ελαχιστοποιηθεί;
- Ποιο είναι το αποδεκτό περιθώριο επιλογής χρήστη όσον αφορά τα δικαιώματα και την ειδοποίηση;

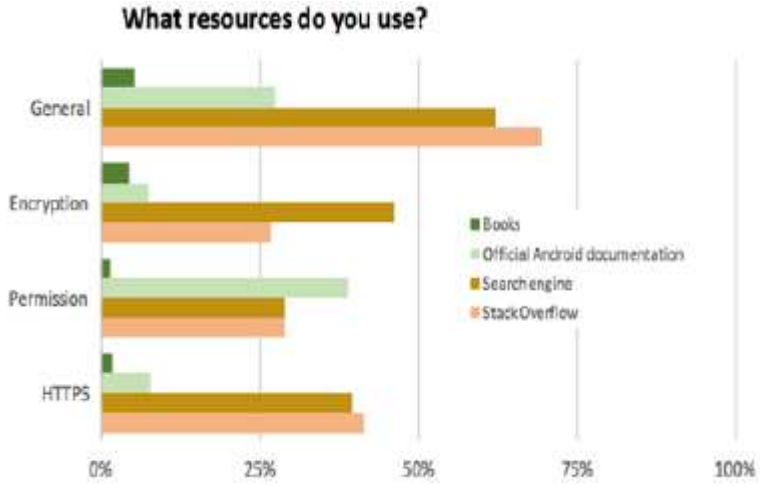
Το αν τα ερωτήματα αυτά είναι τα σωστά και πώς να τους απαντήσετε καλύτερα ώστε να είναι πραγματικά δυνατά για τους προγραμματιστές είναι σημαντικά θέματα που πρέπει να αποτελούν μέρος κάθε πρωτοβουλίας για την παροχή συστάσεων στους προγραμματιστές εφαρμογών. Μια βασική πρόκληση είναι να παρασχεθούν συστάσεις αρκετά γενικές ώστε να μην χάνουν τη συνάφεια τους με τις ενημερώσεις για τα λειτουργικά συστήματα και τη συναφή λειτουργικότητα απορρήτου και να είναι συνεπείς με τους τρέχοντες περιορισμούς στο οικοσύστημα.Επιπλέον, ορισμένα άλλα σημαντικά θέματα που πρέπει να αντιμετωπιστούν για να είναι χρήσιμες και αποτελεσματικές οι συστάσεις αυτές είναι τα εξής:

Ευαισθητοποίηση και εκπαίδευση. Σε πολλές περιπτώσεις, οι προγραμματιστές ενδέχεται να μην είναι αυτοί που ευθύνονται ή ενδέχεται να μην θεωρηθούν υπεύθυνοι για την προστασία των δεδομένων, ωστόσο, ενδέχεται να είναι σε θέση να κάνουν τη διαφορά. Οι συστάσεις πρέπει να συνδυαστούν με μια εκστρατεία ευαισθητοποίησης που επιτρέπει στον προγραμματιστή να εντοπίσει το ρόλο που μπορεί να διαδραματίσει στην αντιμετώπιση των απαιτήσεων προστασίας δεδομένων. Θα πρέπει επίσης να καταστήσουν σαφές ότι είναι επείγον ο υπεύθυνος για την ανάπτυξη να αντιμετωπίσει αυτά τα ζητήματα, δεδομένων των πολυάριθμων άλλων αρμοδιοτήτων που τους ανατίθενται. Η εκπαίδευση των προγραμματιστών σχετικά με την προστασία της ιδιωτικής ζωής και την ασφάλεια είναι ζωτικής σημασίας για το σκοπό αυτό.

Ειδικές για τις συνθήκες των προγραμματιστών εφαρμογών. Υπάρχουν λίγες επιστημονικές μελέτες που αξιολογούν τους προγραμματιστές και τις συνθήκες υπό τις οποίες αναπτύσσουν εφαρμογές για κινητά από άποψη προστασίας δεδομένων κατάς τον σχεδιασμό. Έχουν πρόσφατα δρομολογηθεί μερικά έργα για να εξεταστεί

ο καλύτερος τρόπος υποβολής συστάσεων προς μεμονωμένους προγραμματιστές. Πρόκειται για μια ενδιαφέρουσα πρόκληση και ένα θέμα που αξίζει να μελετηθεί περαιτέρω κατά πόσο είναι δυνατόν να παρέχονται γενικές συστάσεις για την προστασία των δεδομένων σε όλους τους προγραμματιστές εφαρμογών ή εάν πρέπει να προσαρμοστούν σε διάφορους περιορισμούς, όπως το μέγεθος ενός οργανισμού, η δομή της ομάδας, τη μεθοδολογία ανάπτυξης, τον τομέα της εφαρμογής και τον τύπο της εφαρμογής.

Διάδοση. Πρέπει να διερευνηθεί κατά πόσον ένα ενιαίο έγγραφο PDF, μία λίστα με τα 10 κορυφαία, μια πύλη ή άλλες επιλογές είναι ο καλύτερος τρόπος για να είναι διαθέσιμες οι συστάσεις, ενημερωμένες και χρησιμοποιήσιμες για τους προγραμματιστές. Η απάντηση μπορεί επίσης να εξαρτάται από τον τύπο των συστάσεων (π.χ. αποσπάσματα κώδικα μπορεί να εμφανίζονται καλύτερα στο StackOverflow, ενώ οι νομικές απαιτήσεις εξηγούνται καλύτερα σε ένα μεγαλύτερο PDF). Το Σχήμα δείχνει τα τελευταία στατιστικά στοιχεία για τους πόρους στους οποίους επιστρέφουν οι προγραμματιστές του Android όταν ζητούν τεχνική βοήθεια ή έχουν ερωτήσεις σχετικά με την ασφάλεια. Αυτά τα στατιστικά στοιχεία προέρχονται από μελέτες που δείχνουν ότι η πιο δημοφιλής πηγή ενδέχεται να μην είναι αυτή που επιστρέφει σωστά αποτελέσματα (δηλαδή, τα βιβλία ενδέχεται να προσφέρουν στους προγραμματιστές καλύτερα αποτελέσματα από μια τυχαία σελίδα στο StackOverflow [11]).



Εικόνα 6 Πόροι που χρησιμοποιούν οι προγραμματιστές για τεχνικές ερωτήσεις

Μιλώντας σε προγραμματιστές. Οι συστάσεις πρέπει να είναι εύκολο να κατανοηθούν και να μην αναμένουν οι προγραμματιστές να σκέφτονται σαν

δικηγόροι, ακαδημαϊκοί ή υπεύθυνοι χάραξης πολιτικής. Θα πρέπει να μιλούν ιδανικά για τις συνθήκες εργασίας τους και επίσης να σχετίζονται με το άγχος της διοίκησης όταν θέλουν να αντιμετωπίσουν θέματα όπως η προστασία δεδομένων και η ιδιωτικότητα.

Προσδιορίστε τα χαρακτηριστικά σημεία προστασίας δεδομένων: Είναι σημαντικό να εντοπίσετε και να καταγράψετε εκείνες τις στιγμές που οι προγραμματιστές παρατηρούν ότι έχουν ευθύνη για την προστασία δεδομένων. Εμπειρικές μελέτες θα μπορούσαν να εντοπίσουν τα τυπικά ερωτήματα που μπορούν να οδηγήσουν τους προγραμματιστές να αντιμετωπίσουν (ή να αποφύγουν) τις προκλήσεις προστασίας δεδομένων. Από το "Συλλέγω προσωπικά δεδομένα;" στο "Είμαι ασφαλής αν ανωνυμοποιήσω τα δεδομένα χρήστη" στο "Τι πρέπει να κάνω για να βεβαιωθώ ότι δεν πληρώνω το μεγάλο πρόστιμο προστασίας δεδομένων;" είναι πιθανά ερωτήματα που μπορεί οδηγούν τους προγραμματιστές σε συστάσεις για την προστασία δεδομένων.

Μαθαίνω απο λάθη. Είναι καλά τεκμηριωμένο ότι οι πολιτικές απορρήτου δεν είναι αποτελεσματικές στην ενημέρωση των τελικών χρηστών και η υπερβολική ζήτηση δικαιωμάτων μπορεί να οδηγήσει σε εξοικείωση. Είναι εύκολο να εφαρμοστούν μηχανισμοί για την προστασία των δεδομένων που χτυπούν το σκοπό της εκτέλεσης τους κατά κύριο λόγο. Οι συστάσεις δεν πρέπει να προτείνουν τυφλά την εφαρμογή του νόμου, αλλά θα πρέπει ιδανικά να αποτυπώνουν τα διδάγματα από την εφαρμογή της νομοθεσίας περί προστασίας δεδομένων και των τεχνολογιών προστασίας της ιδιωτικής ζωής τα τελευταία 20 χρόνια.

Στην ιδανική περίπτωση, οι συστάσεις θα πρέπει να αναπτύσσονται επαναληπτικά. Η συχνή αξιολόγηση της αποτελεσματικότητας και της ποιότητας των συστάσεων, καθώς και οι ενημερώσεις στο ταχέως μεταβαλλόμενο οικοσύστημα, μπορούν να χρησιμοποιηθούν για την παροχή συμβολής στην επόμενη επανάληψη των συστάσεων. Ακόμη και αν οι συστάσεις είναι ένα απλό έγγραφο, η αξιολόγηση της χρηστικότητας και της αποτελεσματικότητας θα πρέπει να ολοκληρωθεί και να δημοσιευθεί για χρήση σε μελλοντικές πρωτοβουλίες.

5.2 Ανάγκη για κλιμακούμενες μεθοδολογίες και βέλτιστες πρακτικές

Η στροφή προς τις ευέλικτες μεθόδους ανάπτυξης καθιστά δύσκολο για τους προγραμματιστές να εφαρμόζουν μεθόδους που αναπτύσσονται για μεγάλες σχεδιαστικές προσεγγίσεις. Ποιες είναι μερικές απλές τεχνικές ή βέλτιστες πρακτικές που μπορεί να αναλάβει ένας ευέλικτος προγραμματιστής εφαρμογών; Δεδομένης της μεγάλης προβολής των ευέλικτων μεθοδολογιών μεταξύ των προγραμματιστών εφαρμογών, υποστηρίζουμε ιδιαίτερα την έρευνα και την ανάπτυξη κλιμακωτών μεθοδολογιών για την προστασία δεδομένων από το σχεδιασμό. Αυτές οι μεθοδολογίες πρέπει να λαμβάνουν υπόψη τις διαφορετικές θέσεις που μπορούν να

λάβουν οι προγραμματιστές εφαρμογών στο οικοσύστημα της εφαρμογής (OS vs. Library versus app developers) και τις δυνατότητες και τους περιορισμούς που σχετίζονται με αυτές. Οι βέλτιστες πρακτικές, οι στρατηγικές και τα πρότυπα μπορούν επίσης να χρησιμοποιηθούν για την αύξηση των προτεινόμενων μεθοδολογιών.

Προκειμένου να αναπτυχθούν τέτοιες κλιμακούμενες μεθοδολογίες, είναι απαραίτητη μια αιτιολογημένη ανάλυση της κατάστασης. Μια τέτοια κατάσταση θα πρέπει να περιλαμβάνει:

Έρευνα σχετικά με τις μεθοδολογίες ανάπτυξης εφαρμογών που χρησιμοποιούνται στην πράξη. Οι προκλήσεις για προγραμματιστές που δεν χρησιμοποιούν δομημένες (ευκίνητες) προσεγγίσεις είναι πιθανό να είναι διαφορετικές και θα πρέπει να αναλύονται σε μια έρευνα σχετικά με τις τρέχουσες προσεγγίσεις ανάπτυξης. Τα αποτελέσματα αυτής της έρευνας είναι πολύτιμα για την κατανόηση του κατά πόσο χρησιμοποιούνται μέθοδοι SDL και αν είναι δυνατό να χρησιμοποιηθούν οι υπάρχουσες μεθοδολογίες (όπως η SDL) σε σχέση με θέματα προστασίας δεδομένων.

Αξιολόγηση του κατά πόσο είναι εύλογο, επιθυμητό και εφικτό να ενσωματωθούν τα ζητήματα προστασίας δεδομένων στο SDL. Η ιδιωτικότητα στο οικοσύστημα της εφαρμογής για κινητά θεωρείται συνήθως ως μέρος της έρευνας για την ασφάλεια. Ωστόσο, η άποψη της τεχνολογίας ασφαλείας σχετικά με την ιδιωτική ζωή συχνά δεν ανταποκρίνεται στην εφαρμογή των αρχών προστασίας δεδομένων σε εφαρμογές για κινητά που δεν είναι καλά ευθυγραμμισμένες με τις ανησυχίες σχετικά με την ασφάλεια. Θα αναμενόταν να βρεθούν μελέτες που επικεντρώνονται στο πώς δημιουργούνται προβλήματα προστασίας της ιδιωτικής ζωής και των δεδομένων κατά την ανάπτυξη εφαρμογών στο σημερινό οικοσύστημα, αλλά είναι σπάνιες. Τέτοιες μελέτες θα είναι πολύτιμες για τον εντοπισμό των σημείων συμμόρφωσης καθώς και για την εφαρμογή κανονιστικών, κοινωνικοτεχνικών, αγοραμικών ή τεχνικών λύσεων στο οικοσύστημα. Απαιτείται περαιτέρω έρευνα για να αξιολογηθεί κατά πόσον η SDL θα είναι ένας καλός χώρος για την αντιμετώπιση των ζητημάτων προστασίας δεδομένων. Μια άλλη πιθανή οδός έρευνας είναι να εξετάσει τον προσδιορισμό τρόπων μείωσης του φόρτου των προγραμματιστών, προσδιορίζοντας πιθανές ευθυγραμμίσεις μεταξύ προστασίας δεδομένων και άλλων απαιτήσεων ποιότητας που αναμένεται να υλοποιήσουν οι προγραμματιστές (π.χ., η ελαχιστοποίηση των δεδομένων μπορεί να ευθυγραμμιστεί με τις απαιτήσεις ασφαλείας, επιδόσεων και ανθεκτικότητας).

Εμπειρικές μελέτες για τον εντοπισμό και την εφαρμογή σημείων δράσης για την προστασία της ιδιωτικής ζωής. Μια προσέγγιση είναι να εντοπιστούν τα πιθανά

σημεία στον κύκλο ζωής της ανάπτυξης που μπορούν να χρησιμοποιηθούν για την εισαγωγή των δράσεων προστασίας προσωπικών δεδομένων. Εμπειρικές μελέτες μπορούν να χρησιμοποιηθούν για την ανεύρεση ενδεχόμενων σημείων δράσης για την προστασία της ιδιωτικής ζωής ή για την αξιολόγηση της χρήσης τους στην πράξη. Η οικοδόμηση μιας σουίτας "προστασίας δεδομένων" είναι μια άλλη ευκαιρία που αξίζει να συνεχιστεί σε αυτή τη γραμμή σκέψης.

Καλές πρακτικές, μοντέλα απορρήτου και αποσπάσματα κώδικα. Απαιτούνται περαιτέρω προσπάθειες για την κατανόηση των αποτελεσματικών και καλών απαντήσεων που θα μπορούσαν να χρησιμοποιηθούν για την ανταπόκριση στα ευάλωτα σημεία προστασίας της ιδιωτικής ζωής και των δεδομένων. Εκτός από τις μεθοδολογίες, οι προγραμματιστές εκτιμούν συγκεκριμένες συστάσεις, οι οποίες μπορεί να είναι μια λίστα με τις βέλτιστες πρακτικές, τα πρότυπα προστασίας προσωπικών δεδομένων, τα εργαλεία που μπορούν να ενσωματωθούν στο αναπτυξιακό περιβάλλον ή ακόμη και κατά καιρούς αποσπάσματα κώδικα. Οι συστάσεις για βέλτιστες πρακτικές μπορούν να εμπλουτιστούν με παραδείγματα τυπικών λαθών.

5.3 Ένα πλαίσιο DPIA για κινητές εφαρμογές

Ένας τόπος όπου το GDPR περιγράφει μια δραστηριότητα που ευθυγραμμίζεται καλά με την ανάπτυξη παρά με τις λειτουργίες δεδομένων είναι με εκτιμήσεις επιπτώσεων προστασίας δεδομένων (DPIAs).Απαιτούν ανάλυση των επιπτώσεων και των κινδύνων που μπορούν να χρησιμεύσουν ως αναφορά για τη μοντελοποίηση απειλών και μπορούν να καθοδηγήσουν μελλοντικές αναπτυξιακές δραστηριότητες. Ωστόσο, οι υπάρχουσες μέθοδοι για την εφαρμογή των DPIA τείνουν να υιοθετούν ένα μεγάλο πρότυπο που έρχεται σε σύγκρουση με τις ευέλικτες πρακτικές που κυριαρχούν στην ανάπτυξη εφαρμογών. Αυτό δείχνει ότι απαιτείται περαιτέρω έρευνα σχετικά με το εάν και πώς μπορούν να γίνουν αποτελεσματικά και αποτελεσματικά τα DPIA σε ένα ευκίνητο περιβάλλον.

Ορισμένα άλλα σημεία που χρήζουν προσοχής στο σημείο αυτό είναι τα εξής:

Ομογενοποίηση των DPIA. Διάφορες μεθοδολογίες DPIA έχουν προταθεί από διάφορους φορείς και από διαφορετικά DPA [12], [11], [13], [14], [15]. Αν και πολλοί από αυτούς μοιράζονται μια παρόμοια μεθοδολογία, είναι διαφορετικές. Οι περισσότεροι προγραμματιστές είναι συγκεχυμένοι και δεν ξέρουν πώς να επεξεργάζονται και ποια μεθοδολογία θα χρησιμοποιήσουν. Θα συνιστούσαμε να ομογενοποιηθούν αυτές οι προτάσεις για να καταλήξουμε σε μια ενιαία μεθοδολογία ή ένα πλαίσιο DPIA που θα ήταν αποδεκτό σε ολόκληρη την Ευρώπη. Επιπλέον, οι περισσότεροι προγραμματιστές δεν κατανοούν τη διαφορά μεταξύ μιας ανάλυσης

κινδύνου ασφαλείας και της αξιολόγησης του αντικτύπου της ιδιωτικής ζωής. Αυτό θα πρέπει επίσης να διευκρινιστεί.

Ειδικό DPIA για κινητές εφαρμογές. Πολλές εφαρμογές για κινητά συλλέγουν παρόμοια προσωπικά δεδομένα και πραγματοποιούν παρόμοια επεξεργασία. Θα ήταν ενδεδειγμένο να αναπτυχθεί μια συγκεκριμένη μεθοδολογία για τις εφαρμογές για κινητά, όπως έγινε για τις τεχνολογίες RFID [16]. Εναλλακτικά, μια μεθοδολογία για διαφορετικούς τύπους κινητών συσκευών.Θα μπορούσαν να ληφθούν υπόψη εφαρμογές (παιχνίδια,ειδήσεις, κοινωνικά δίκτυα κ.λπ.), βιβλιοθήκες ή SDK (Κιτ Ανάπτυξης Λογισμικού).

Εργαλεία υποστήριξης. Τα διαφορετικά μέρη που συνθέτουν ένα DPIA είναι καλά καθορισμένα. Συνεπώς, συνιστάται να αναπτυχθούν εργαλεία υποστήριξης για να βοηθηθεί ένας ελεγκτής δεδομένων να εκτελεί καθοδηγώντας τον ελεγκτή μέσω αυτών των διαφορετικών φάσεων. Ομοίως, τα εργαλεία ελέγχου θα ήταν επίσης πολύ χρήσιμα. Πολλοί προγραμματιστές χρησιμοποιούν τρίτους χωρίς να γνωρίζουν τι κάνουν πραγματικά και ποια προσωπικά δεδομένα συλλέγουν και επεξεργάζονται. Θα πρέπει να αναπτυχθούν και να προωθηθούν εργαλεία ανάλυσης και διαφάνειας, όπως ο Lumen [17], ο App-census [18] ή ο εξεταστής MobileApps [19]. Λάβετε υπόψη ότι αυτά τα εργαλεία θα μπορούσαν επίσης να χρησιμοποιηθούν από τους προγραμματιστές για να αναλύσουν τις δικές τους εφαρμογές για κινητά. Συνιστάται επίσης να προωθηθούν πρωτοβουλίες, όπως το Transparency Lab, το οποίο στοχεύει στην ανάπτυξη εργαλείων για τη βελτίωση της διαφάνειας.

5.4 Βελτίωση της ιδιωτικότητας και της χρηστικότητας στο οικοσύστημα των προγραμματιστών

Πρόσφατες έρευνες έχουν στραφεί στην βελτίωση της χρηστικότητας των εργαλείων ανάπτυξης. Αυτό μπορεί να περιλαμβάνει IDE, API και λειτουργικά συστήματα. Μεγάλο μέρος αυτής της έρευνας επικεντρώνεται στην ασφάλεια παρά στην προστασία της ιδιωτικής ζωής και των δεδομένων. Απαιτούνται περαιτέρω μελέτες για να κατανοήσουμε την κατάσταση της τεχνολογίας όσον αφορά τις ευκαιρίες ιδιωτικού απορρήτου και τα εμπόδια που ενυπάρχουν στους IDE, τα API και τα λειτουργικά συστήματα, καθώς επίσης και την παροχή των API για PETs και την σχετική λειτουργικότητα προστασίας δεδομένων. Επιπλέον, υπάρχει ανάγκη για εργαλεία για τη δοκιμή, την επαλήθευση και τον έλεγχο των υπαρχουσών βιβλιοθηκών, υπηρεσιών, API κλπ. Για την αντιμετώπιση αυτών των ζητημάτων συνιστάται η εκπόνηση μελετών:

Εμπειρική αξιολόγηση των περιβάλλοντων κατασκευής του IDE, του API. Μελετώντας τα API σχετικά με την προστασία της ιδιωτικής ζωής και των

δεδομένων. Προστασία απορρήτου και ασφάλειας σε API ειδικά για την προστασία των δεδομένων (π.χ. γεννήτριες πολιτικών απορρήτου), καθώς και την αξιολόγηση της χρηστικότητας των API σε σχέση με την προστασία της ιδιωτικής ζωής και των δεδομένων.

· Σε βάθος ανάλυση των βιβλιοθηκών διαφήμισης και των API τους. Οι προγραμματιστές χρειάζονται μεγαλύτερη διαφάνεια και έλεγχο των βιβλιοθηκών διαφήμισης, εάν θέλουν να εκπληρώσουν τις υποχρεώσεις τους για την προστασία των δεδομένων. Μας λείπει μια επισκόπηση των επιλογών που είναι ή πρέπει να είναι διαθέσιμες στους προγραμματιστές εφαρμογών (και υλοποιούνται από το λειτουργικό σύστημα ή από παρόχους βιβλιοθηκών τρίτου μέρους) έτσι ώστε να μπορούν να εκπληρώσουν τις απαιτήσεις προστασίας δεδομένων τους στις βιβλιοθήκες διαφημίσεων.

· Δημιουργία βιβλιοθηκών για τεχνολογίες ενίσχυσης της προστασίας της ιδιωτικής ζωής. Αν η ανάπτυξη είναι όλο και περισσότερο για την ενσωμάτωση διαφορετικών λειτουργιών από τις υπηρεσίες τρίτων, φαίνεται σαν μια μεγάλη ευκαιρία να ενθαρρυνθεί η ανάπτυξη της λειτουργικότητας PET με τη μορφή βιβλιοθηκών με χρήσιμα API. Είναι σημαντικό να προωθηθούν ορισμένες (απλές) πρακτικές τεχνικές διατήρησης της ιδιωτικής ζωής και λύσεις, ενδεχομένως με παραδείγματα και κώδικα. Είναι επίσης σημαντικό να τονωθεί η έρευνα και η ανάπτυξη σε αυτόν τον τομέα. Πολλά ζητήματα εξακολουθούν να απαιτούν κάποια ερευνητική εργασία (όπως η ανωνυμία δεδομένων). Θα ήταν, για παράδειγμα, πολύ χρήσιμο να αναπτυχθούν και να δημοσιευθούν βιβλιοθήκες που εκτελούν αναλύσεις διατήρησης της ιδιωτικής ζωής ή που υλοποιούν πίνακα ελέγχου απορρήτου. Οι προγραμματιστές θα μπορούσαν στη συνέχεια να τις χρησιμοποιήσουν χωρίς να χρειάζεται να τους κωδικοποιήσουν από το μηδέν ή να στραφούν σε εκθέσεις πειραματικών δεδομένων υπηρεσιών.

· Αξιολόγηση των εργαλείων απορρήτου που διατίθενται στους προγραμματιστές εφαρμογών. Υπάρχουν διάφορα ερευνητικά εργαλεία για την αξιολόγηση ροών πληροφοριών ευαίσθητων στην ιδιωτική ζωή των εφαρμογών. Οι προγραμματιστές μπορούν να τα χρησιμοποιήσουν για να δοκιμάσουν τις δικές τους εφαρμογές ή άλλες εφαρμογές και βιβλιοθήκες που θέλουν να ενσωματώσουν στη βάση τους κώδικα. Παρομοίως, οι DPA μπορούν να χρησιμοποιήσουν τέτοια εργαλεία ή να τα διαθέσουν σε μεγαλύτερο κοινό. Ωστόσο, επί του παρόντος δεν υπάρχουν μελέτες σχετικά με την υιοθέτηση τέτοιων εργαλείων και την αποτελεσματική χρήση τους για την προστασία των δεδομένων. Η αξιολόγηση των υφιστάμενων εργαλείων θα πρέπει επίσης να εξετάζει την πρόσβασή τους, τη χρηστικότητα και την αποτελεσματικότητά τους.

5.5 Αντιμετώπιση ολόκληρου του οικοσυστήματος εφαρμογών για κινητά

Ο σχεδιασμός και η λειτουργικότητα μιας εφαρμογής δεν εξαρτάται μόνο από τις μεθόδους ανάπτυξης εφαρμογών, αλλά από ολόκληρο το οικοσύστημα εφαρμογών για κινητά. Αυτό το οικοσύστημα βασίζεται στο υλικό, το λογισμικό, τα λειτουργικά συστήματα, τα πρωτόκολλα, τα API, τις υποδομές, τις συμβάσεις κλπ. Όπως φαίνεται από την ανάλυση, η επιρροή των προγραμματιστών εφαρμογών είναι συχνά περιορισμένη και σε μεγάλο βαθμό οι κανόνες του οικοσυστήματος που καθορίζονται από τους φορείς της βιομηχανίας, όπως οι πάροχοι πλατφόρμων. Για μια ολοκληρωμένη προσέγγιση στην προστασία της ιδιωτικής ζωής και της προστασίας των δεδομένων για χρήστες κινητών εφαρμογών, αυτά τα γενικά θέματα διακυβέρνησης δεν πρέπει να παραμεληθούν. Αυτό το μεγάλο ζήτημα θα πρέπει να αναλυθεί σε μελλοντικές εργασίες:

Υλοποίηση με βάση τις γνώσεις των προγραμματιστών εφαρμογών, των ελεγκτών δεδομένων, των ρυθμιστικών αρχών και των ερευνητών.

Καθορισμός και τυποποίηση κατάλληλων διεπαφών και πρωτοκόλλων. Οι οργανισμοί τυποποίησης καθώς και οι πρωτοβουλίες του κλάδου θα πρέπει να λαμβάνουν υπόψη τις απαιτήσεις ιδιωτικότητας και προστασίας δεδομένων που επηρεάζουν την ανάπτυξη της κινητής εφαρμογής, π.χ. για τον προσδιορισμό των διεπαφών ή των πρωτοκόλλων.

Διεπιστημονική προσέγγιση για τον επανασχεδιασμό του οικοσυστήματος εφαρμογών για κινητά. Η τρέχουσα κατάσταση του τρόπου λειτουργίας του οικοσυστήματος εφαρμογών για κινητά δεν πρέπει να θεωρείται δεδομένη. Για παράδειγμα, η σημερινή προσέγγιση της προσφοράς «δωρεάν» υπηρεσιών σε αντάλλαγμα της συλλογής προσωπικών δεδομένων μπορεί να αμφισβητηθεί: η αρχή της προστασίας δεδομένων από το σχεδιασμό και από προεπιλογή (άρθρο 25 του GDPR) μπορεί - εάν ληφθεί σοβαρά υπόψη - να περιορίσει την επεξεργασία δεδομένων σε αναγκαία έκταση και για ειδικούς σκοπούς. Τέτοιες πιθανές αλλαγές ενδέχεται να επηρεάσουν σημαντικά το οικοσύστημα της εφαρμογής για κινητά σε σχέση με τη διακυβέρνηση (καθώς και το Διαδίκτυο και η ψηφιοποίηση γενικά). Οι ερευνητές πολλαπλών κλάδων, οι επαγγελματίες, οι υπεύθυνοι για τη χάραξη πολιτικής και οι ρυθμιστικές αρχές πρέπει, συνεπώς, να ασχοληθούν με εναλλακτικές προσεγγίσεις που επιτρέπουν την προστασία της ιδιωτικής ζωής και των δεδομένων καθώς και την εφαρμογή άλλων θεμελιωδών δικαιωμάτων στο σχεδιασμό του συστήματος για τη μελλοντική κοινωνία. Η εργασία αυτή θα πρέπει να περιλαμβάνει τρόπους βελτίωσης του σημερινού ψηφιακού οικοσυστήματος, καθώς και να παρουσιάζει συμπληρωματικές προσεγγίσεις και θα πρέπει να προτείνει migration paths προς τις προβλεπόμενες επιλογές.

Βιβλιογραφία

[1] Trustworthiness Framework and Metrics Design DELIVERABLE D3.1
Stefan Ten Kate Trustworthiness within social networking sites

[2] Privacy and data protection in mobile applications

[3] A. Cavoukian, "Privacy by design – the 7 foundational principles (revised version)," 2011.

[4]M. Hansen, J.-H. Hoepman and M. Jensen, "Towards Measuring Maturity of Privacy-Enhancing Technologies," in Annual Privacy Forum (APF 2015), 2016.

[5] M. Hansen, M. Jensen and M. Rost, "Protection Goals for Privacy Engineering," in International Workshop on Privacy Engineering (IWPE), Security and Privacy Workshops (SPW), 2015.

[6] ENISA, "Privacy and data protection by design," 2014.

[7] German DPA, "Standard Data Protection Model," in German Conference of Data Protection Authorities, 2017.

[8] M. Colesky, J.-H. Hoepman and C. Hillen, "A Critical Analysis of Privacy Design Strategies," in International Workshop on Privacy Engineering – IWPE'16, San Jose, CA, USA, 2016.

[9] J. H. Hoepman., "Privacy Design Strategies," in IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014), 2014.

[10] ISO, "ISO/IEC 27001:2013 Information technology-Security techniques - Information security management systems -- Requirements," 2013.

[11] A. Yasemin, M. Backes, S. Fahl, D. Kim, M. L. Mazurek and C. Stransky, "You Get Where You're Looking For: The Impact Of Information Sources on Code Security," in Security and Privacy (SP), 2016 IEEE Symposium, 2016.

[12] CNIL, "Privacy Impact Assessment," 2015.

[13] ENISA, "Guidelines for SMEs on the Security of Personal Data Processing," 2016.

[14] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller and M. Rost, "A Process for Data Protection Impact Assessment under the European General Data Protection

Regulation. In: Privacy Technologies and Policy," in 4th Annual Privacy Forum (APF 2016), 2016.

[15] Australian Government, Office of the Australian Information Commissioner, "Guide to Understanding Privacy Impact Assessments," 2014.

[16] Article 29 Data Protection Working Party, "Opinion 9/2011 Privacy and Data Protection Impact Assessment Framework for RFID Applications," 2011.

[17] "The Lumen tool" 2019. Site: https://haystack.mobi. [Οκτώμβριος 2019].

[18] "The Appcensus tool" 2019. Site: https://www.appcensus.io/ [Οκτώμβριος 2019].

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