Ειδικά Θέματα Τεχνολογίας Λογισμικού

Αναφορά Εργασίας Υλοποίησης

Έργο: TextSecure

Παπαδάς Κωνσταντίνος

Πεπονής Παναγιώτης

Περιεχόμενα

1. Εισαγωγή

Η ενασχόληση με το TextSecure ήταν η πρώτη μας επαφή με το λειτουργικό σύστημα Android σε επίπεδο ανάπτυξης, καθώς και με το git σαν σύστημα διαχείρισης εκδόσεων. Για να ξεκινήσουμε να δουλεύουμε πάνω στο έργο χρειάστηκε πρώτα να κατανοήσουμε τις βασικές λειτουργίες του git καθώς και τα δομικά στοιχεία μιας android εφαρμογής, και τέλος τον τρόπο ανάπτυξης, μεταγλώτισσης και εκτέλεσης. Επίσης ήταν η πρώτη μας επαφή με ολοκληρωμένα συστήματα μεταγλώττισης, όπως το gradle. Η επιλογή του συγκεκριμένου έργου έγινε επειδή ανήκει στο (ευρύ) πεδίο της ασφάλειας και των νέων σχετικά τεχνολογιών(Android) όπως και τα ενδιαφεροντά μας.

2. Κατανόηση και τεκμηρίωση του έργου

Η τεκμηρίωση του έργου, απο την πλευρά μας, κρίνεται ελλιπής. Δεν υπάρχει οργανωμένο documentation που να εξηγεί τον τρόπο λειτουργίας του σε μορφή Javadoc, αλλά υπάρχει αρκετή τεκμηρίωση όσο αφορά το πρωτόκολλο ασφάλειας που έχουν σχεδιάσει και χρησιμοποιούν [1] και το μοντέλο κινδύνων(threat model) [2] που θα καλείται να αντιμετωπίσει το εν λόγω πρωτόκολλο. Στα πλαίσια της κατανόησης του πρωτοκόλλου, πριν ακόμα αποφασίσουμε ποια θα είναι η συνεισφορά μας, αντλήσαμε στοιχεία και απο μια επιστημονική δημοσίευση [3] η οποία αποδεικνύει οτι η εφαρμογή ειναι ευάλωτη σε επίθεση UKS(Uknown Key-Share attack), αλλά πρωτού καταλήξει σε αυτό κάνει μια εμπεριστατωμένη ανάλυση του πρωτοκόλλου και των κρυπτογραφικών αλγορίθμων που χρησιμοποιούνται. Υπήρχαν επίσης οδηγίες για την μεταγλώττιση της εφαρμογής μεσα απο eclipse ή AndroidStudio, τις οποίες αξιοποιήσαμε.Παρά την ελλείψη τεκμηρίωσης ο κώδικας αυτοτεκμηριώνεται μέσα απο τον τρόπο συγγραφής του(ονόματα μεταβλητων και κλάσεων, οργάνωση σε πακέτα κλπ). Τελικά κατανοήσαμε ένα μεγάλο κομμάτι του έργου, κυρίως σε επίπεδο διαδικασιών και συγκεκριμένα την διαδικασία λήψης μηνύματος, αποκρυπτογράφησης, αποθήκευσης στην βάση, ανάκτησης ενός μηνύματος απο την βάση και προβολής του στην οθόνη.

3. Πλάτος των αλλαγών

Παρατηρώντας το αποθετήριο της OpenWhisperSystems παρατηρήσαμε οτι δεν δέχονται εύκολα pull request και οτι ο χρόνος ελέγχου είναι αρκετά μεγάλος, κάτι αναμενόμενο βάσει της φύσης του έργου. Γι’ αυτό το λόγο προσπαθήσαμε η αλλαγή μας να περιοριστεί οσο το δυνατόν περισσότερο σε πλάτος, ψάχνοντας ταυτόχρονα για την πιο αποδοτική υλοποίηση. Αυτή εκφράζεται με την αλλαγή ενός αρχείου κώδικα στο οποίο προστέθηκε μια επιπλέον κλάση και 3 μέθοδοι. Η κλάση αναπαριστά ένα

τηλεφωνικό αριθμό με το όνομα της συσχετιζόμενης με αυτό επαφής, καθώς και την θέση του μέσα στο αρχικό κείμενο. Οι μέθοδοι αφορούν:

- Την αναζήτηση ενός τηλεφωνικού αριθμού, βάσει ενός regular expression
- Την αναζήτηση στον λίστα επαφών της συσκευής για το όνομα που πιθανόν να σχετίζεται με έναν αριθμό
- Την επεξεργασία ενός String ώστε να προστεθεί δίπλα απο το νούμερο, μέσα σε παρένθεση, το όνομα της επαφής

4. Ποιότητα υλοποίησης

Θεωρούμε οτι ο κώδικας που γράψαμε είναι σύμφωνα με τις αρχές ποιότητας λογισμικού. Έχουν χρησιμοποιήθει έννοιες οπως η αφαίρεση και η ενθυλάκωσηέχουμε φροντίσει να μην δημιουργήσουμε νέες εξαρτήσεις μεταξύ πακέτων(κυρίως περιορίζοντας τις αλλαγές μας σε μια μόνο κλάση) και έχουμε εξασφαλίσει την πληρότητα(πχ δεν ψάχνουμε μόνο για ένα αριθμό ανα μήνυμα). Εξετάσαμε τον κωδικα που γράψαμε και απο την πλευρά της απλότητας και αναγνωσιμότητας, φροντίζοντας για τα κατάλληλα ονόματα κλάσεων, μεθόδων και μεταβλητών. Μένοντας πιστοί σε μια απο τις βασικές αρχές της ασφάλειας πληροφοριών, την ακεραιότητα(Integrity) και κατ' επέκταση και του TextSecure, φροντίσαμε η αλλαγή μας να μην την καταπατά, αφήνοντας το αρχικό μήνυμα ανεπηρέαστο και κρυπτογραφημένο στην βάση δεδομένων, ενώ τροποποιούμε αυτό που βλέπει ο χρήστης στην οθόνη.

5. Ολοκλήρωση

Ολοκληρώσαμε την αλλαγή μας, επανασχεδιάζοντας κάποια κομμάτια(σε σχέση με τον σχεδιασμό που παρουσιάσαμε στην πρώτη παρουσίαση), με γνώμονα την ποιότητα λογισμικού και είχαμε τελικά τα αναμενόμενα αποτελέσματα. Σε αυτήν την ενότητα είχαμε και την επιπλέον επιτυχία, οτι επιλέξαμε την συνεισφορά μας βάσει του διαθέσιμου χρόνου εκτιμώντας με ακρίβεια τον αναμενόμενο χρόνο υλοποίησης.

6. Έλεγχος

Ελέγξαμε την νέα λειτουργικότητα με σενάρια ελέγχου σε emulator αλλά και σε φυσικές συσκευές, κάτι το οποίο οδήγησε στην διόρθωση κάποιων σφαλμάτων και στην προσθήκη ελέγχων για ακραίες τιμές(πχ άδεια λίστα με γνωστούς τηλεφωνικούς αριθμούς). Unit testing πραγματοποιήθηκε για προσωπική χρήση στην μέθοδο που ψάχνει τηλεφωνικούς αριθμούς για να εξασφαλιστει η σωστή λειτουργία του regex, ενώ είναι στα σχεδιά μας, αν το pull request γίνει δεκτό, να συνεισφέρουμε και το unit test.

Στα υπόλοιπα κομμάτια της συνεισφοράς μας λόγω της φύσης τους δεν ήταν εύκολο να γίνει unit testing(πχ αναζήτηση ενός αριθμού στις επαφές).

7. Συνεργασία με την ομάδα ανάπτυξης

Η συνεργασία μας με την ομάδα ανάπτυξης ήταν ελάχιστη. Δεν λάβαμε απάντηση στην δήλωση ενδιαφέροντός μας για την λειτουργικότητα που επιλέξαμε, την οποία εκδηλώσαμε στα σχόλια του αντίστοιχου issue στο github. Λόγω της έλλειψης συνεργασίας αυτοσχεδιάσαμε σε κάποια κομμάτια, όπως στο αν θα αντικαθιστούμε το νούμερο με το όνομα της επαφής ή θα το προσθέτουμε δίπλα. Σε κάθε περίπτωση σχεδιάσαμε έτσι την υλοποίηση ώστε να είναι δυνατό και το αντιστροφο με μικρές αλλαγές.

8. Ποιότητα παραδοτέων

Φροντίσαμε τα παραδοτέα μας να ακολουθουν τα ενδεδειγμένα πρότυπα. Σε επίπεδο κώδικα φροντίσαμε να ακολουθούνται συμβάσεις συγγραφής όπως η σειρά με την οποία δηλώνονται τα import, το αν θα χρησιμοποιείται space ή tab για τα κενά, το μέγεθος της εσοχής, το μέγιστο μήκος γραμμής κλπ. Επίσης ακολουθήσαμε το LowerCamelCase πρότυπο για την ονοματοδοσία μεταβλητών και μεθόδων όπως προτείνει η ομάδα ανάπτυξης. Σχόλια εκτός Javadoc, φροντίσαμε να μην βάλουμε ακολουθώντας τις υποδείξεις της ομάδας ανάπτυξης, η οποία προτρέπει για την συγγραφή self-documenting κώδικα. Σε επίπεδο καταχώρησης αλλαγών στο αποθετήριο, φροντίσαμε τα commit messages να είναι σαφή, πλήρη και συνοπτικά.

9. Οργάνωση στο GitHub (wiki, issues, commits, branching)

Αξιοποιήσαμε πλήρως το github και τις ευκολίες που μας προσέφερε. Δηλώσαμε ενδιαφέρον για ένα ανοιχτό issue αφήνοντας σχόλιο. Δημιουργήσαμε έναν οργανισμό στον οποίο κάναμε fork το αποθετήριο της WhisperSystems. Σε αυτό δημιουργήσαμε ένα branch με το όνομα contactNames οπου δουλεύαμε και πραγματοποιούσαμε τις αλλαγές. Λόγω ενός προβλήματος που προέκυψε με μια third-party, ανοιχτού κώδικα πάλι, βιβλιοθήκη, αναγκαστήκαμε να προσθέσουμε ένα δεύτερο remote, στα τοπικά μας αποθετήρια, ώστε να μπορούμε να παίρνουμε τυχόν αλλαγές απο το επίσημο αποθετήριο της WhisperSystems. Χρησιμοποιήσαμε και την λειτουργία merge για την επίλυση του ιδιου προβλήματος(merge απο το πλεον συγχρονισμένο master, με αυτο της WhisperSystems, στο contactNames).

10. Επίλογος

Όλες οι συνεισφορές μας φαίνονται απο τους προσωπικούς μας λογαριασμούς . Το pull request βρίσκεται σε αυτόν τον σύνδεσμο: https://github.com/WhisperSystems/TextSecure/pull/3352.

Το branch στο οποίο δουλέψαμε βρίσκεται εδώ: https://github.com/codeBusters-cs/TextSecure/tree/contactNames

11.Παραπομπές

1. Πρωτόκολλο Ασφάλειας https://github.com/WhisperSystems/TextSecure/wiki/ProtocolV2
2. Threat Model https://github.com/WhisperSystems/TextSecure/issues/782
3. How secure is TextSecure? https://eprint.iacr.org/2014/904.pdf