ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Πρόγραμμα Προπτυχιακών Σπουδών

Σύστημα Ηλεκτρονική Ψηφοφορίας Βασισμένο Στην Τεχνολογία NFC

Βασιλάκης Γεώργιος

Επιτροπή

Επιβλέπων : Γεώργιος Καμπουράκης - Επ. Καθηγητής

Μέλη : Μαραγκουδάκης Εμμανουήλ - Επ. Καθηγητής ,
Καλλίγερος Εμμανουήλ - Επ. Καθηγητής

Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη διπλωματική εργασία.

Καρλόβασι, 27/09/2013
Βασιλάκης Γεώργιος

Περίληψη

Οι κινητές συσκευές που χρησιμοποιούμε σήμερα, όπως είναι τα κινητά τηλέφωνα και τα tablets υποστηρίζουν πλήθος προηγμένων τεχνολογιών. Το NFC είναι μια τεχνολογία που τον τελευταίο καιρό έχει κεντρίσει το ενδιαφέρον τόσο των κατασκευαστών όσο και των χρηστών. Στην παρούσα διπλωματική εργασία κάνουμε χρήση της τεχνολογίας του NFC για τη δημιουργία ενός συστήματος ηλεκτρονικής ψηφοφορίας. Χρησιμοποιούμε την ασύμμετρη κρυπτογράφηση, τα πρωτόκολλα SSL, IPSEC και TOR για να διασφαλιστεί η ιδιωτικότητα και η ασφάλεια των συναλλαγών. Το σύστημα που δημιουργήσαμε επιτρέπει στο χρήστη να ψηφίσει από οπουδήποτε χρησιμοποιώντας μία κινητή συσκευή όπως είναι ένα κινητό τηλέφωνο και είναι ιδιαίτερα απλό στη χρήση. Για την υλοποίηση του συστήματος έχουμε χρησιμοποιήσει δύο διακομιστές, τον Catalog Server και τον Ballot Server. Η κινητή συσκευή συνδέεται αρχικά στον Catalog Server για να αυθεντικοποιηθεί με το σύστημα και κατόπιν στον Ballot Server για να καταχωρήσει την ψήφο που επιθυμεί. Επιπλέον, για να ελέγξουμε τη λειτουργία του συστήματος μας και να εντοπίσουμε πιθανά προβλήματα δημιουργήσαμε ένα πρωτότυπο που υλοποιεί το πρωτόκολλο μας.

Abstract

The mobile devices we use today, such as mobile phones and tablets support a variety of advanced technologies. NFC is a technology that has, lately, intrigued manufacturers and users alike. In this thesis we are using the NFC technology in order to create an electronic voting system. We are using asymmetric cryptography,SSL, IPSEC and TOR protocols to ensure the privacy and security of transactions. Our system is very simple to use and allows the user to vote from any location using a mobile device. Two servers, Catalog and Ballot Server, are responsible for the implementation of the system. The mobile device first connects to the Catalog Server for authentication and then to the Ballot Server for vote submission. In addition, we created a working prototype of our system for troubleshooting and functionality tests.

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του προγράμματος προπτυχιακών σπουδών του τμήματος Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, υπό την επίβλεψη του Επίκουρου Καθηγητή Καμπουράκη Γεώργιου.

Κατ’ αρχάς θα ήθελα να δώσω τις θερμές μου ευχαριστίες στον Επίκουρο Καθηγητή Καμπουράκη Γεώργιο, η βοήθεια και η υποστήριξη του σε όλα τα στάδια της εκπόνησης της διπλωματικής αυτής εργασίας υπήρξε καθοριστική.

Επίσης, οφείλω να ευχαριστήσω τους Επίκουρους Καθηγητές Μαραγκουδάκη Εμμανουήλ και Καλλίγερο Εμμανουήλ που μου έκαναν την τιμή να είναι μέλη της τριμελούς εξεταστικής επιτροπής της παρούσας διπλωματικής εργασίας.

Ακόμα, θα ήθελα να ευχαριστήσω ιδιαίτερα το διδάκτορα του τμήματος Δαμόπουλο Δημήτριο. Ήταν πάντα διαθέσιμος και γεμάτος όρεξη να μου προσφέρει τις γνώσεις του και τις πολύτιμες συμβουλές του.

Τέλος, ιδιαίτερες ευχαριστές θα ήθελα να δώσω στην οικογένεια μου για την ηθική και οικονομική υποστήριξη που μου παρείχαν σε όλα τα χρόνια των σπουδών μου.

Καρλόβασι, 27/09/2013
Βασιλάκης Γεώργιος

Περιεχόμενα

Κατάλογος σχημάτων

Κατάλογος πινάκων

Κεφάλαιο 1

Εισαγωγή

Η πρόοδος της τεχνολογίας τα τελευταία χρόνια έχει δώσει τη δυνατότητα για την ανάπτυξη νέων εφαρμογών που καλύπτουν όλο και περισσότερες ανάγκες των χρηστών. Οι κινητές συσκευές, όπως είναι τα κινητά τηλέφωνα, εμφανίζουν τεράστια ανάπτυξη και ευρεία διάδοση σε όλο τον κόσμο. Οι χρήστες των συσκευών αυτών μπορούν πλέον να τις χρησιμοποιήσουν για να εκτελέσουν εφαρμογές που απαιτούν ασφαλείς συναλλαγές. Οι ηλεκτρονικές πληρωμές αλλά και η ηλεκτρονική ψηφοφορία με τη χρήση κινητών συσκευών έχουν αρχίσει να γίνονται πραγματικότητα. Στην παρούσα διπλωματική εργασία θα δούμε ένα σύστημα ηλεκτρονικής ψηφοφορίας που σχεδιάσαμε με χρήση της τεχνολογίας του NFC. Στο Κεφάλαιο 2 κάνουμε μια εισαγωγή στην τεχνολογία του NFC, αναφέρουμε τα βασικά της χαρακτηριστικά που είναι απαραίτητα για την κατανόησή του συστήματος που δημιουργήσαμε. Στο Κεφάλαιο 3 κάνουμε εισαγωγή στην ηλεκτρονική ψηφοφορία που περιέχει και μια μικρή ιστορική αναδρομή. Στο Κεφάλαιο 4 περιγράφουμε συνοπτικά μερικές από τις εργασίες που διαβάσαμε και επηρέασαν τη διπλωματική αυτή εργασία. Τέλος στο κεφάλαιο 5 αναλύουμε το δικό μας σύστημα ηλεκτρονικής ψηφοφορίας και βλέπουμε τα αποτελέσματα του πρωτοτύπου που δημιουργήσαμε με βάση αυτό το σύστημα.

1.1 Σκοπός και στόχος της διπλωματικής

Σκοπός της παρούσας διπλωματικής εργασίας είναι να αποδείξουμε ότι είναι δυνατή η δημιουργία ενός πρωτοκόλλου ηλεκτρονικής ψηφοφορίας με τη χρήση των κινητών συσκευών που κυκλοφορούν σήμερα και της τεχνολογίας του NFC. Ακόμα, σκοπός μας είναι η ανάδειξη των πλεονεκτημάτων της χρήσης κινητών συσκευών σε απαιτητικά περιβάλλοντα, όσο αφορά την ασφάλεια και την ιδιωτικότητα των συναλλαγών, όπως είναι ένα περιβάλλον ηλεκτρονικής ψηφοφορίας.

Στόχος της διπλωματικής εργασίας αυτής είναι η δημιουργία ενός συστήματος ηλεκτρονικής ψηφοφορίας που είναι ιδιαίτερα απλό στη χρήση αφού το κοινό στο οποίο απευθύνεται δεν θα είναι απαραίτητα εξοικειωμένο με τις νέες τεχνολογίες. Επιπλέον, ένας σημαντικός παράγοντας που λάβαμε υπόψη μας, είναι η αφαίρεση των γεωγραφικών περιορισμών που υπάρχουν στα σημερινά συστήματα ψηφοφορίας.

Κεφάλαιο 2

Εισαγωγή στο NFC

Το NFC (Near Field Communication) είναι μία τεχνολογία ασύρματης επικοινωνίας που δημιουργήθηκε από τις εταιρίες Philips,Sony και Nokia το 2004. Έχει βασιστεί κατά πολύ στην τεχνολογία RFID (Radio-frequency identification) και τα πρότυπα της παρέχονται από το NFC Forum. Το NFC forum είναι ένας μη κερδοσκοπικός οργανισμός που έχει πάνω από 170 μέλη παγκοσμίως, τα πρότυπα του είναι απαραίτητα για να υπάρχει δια λειτουργικότητα μεταξύ των NFC συσκευών διαφορετικών κατασκευαστών. Το NFC περιγράφεται από τα ISO 18092/ECMA 340 και ISO 21481/ECMA 352 και είναι συμβατό με τα ISO14443, ISO 15693 και FELICA, κάτι που το κάνει ικανό να χρησιμοποιηθεί με παλαιότερες υποδομές (RFID).

Η ραδιοσυχνότητα που χρησιμοποιεί το NFC είναι 13.56 Mhz και μπορεί να λειτουργήσει σε απόσταση όχι μεγαλύτερη από 10 εκατοστά. Η απόσταση αυτή το διαφοροποιεί από το RFID που είναι ικανό να λειτουργήσει σε μεγαλύτερες αποστάσεις. Οι ταχύτητες μεταφοράς δεδομένων που μπορούν να επιτευχθούν με το NFC δεν μπορούν να χαρακτηριστούν γρήγορες. Υπάρχουν τέσσερις ταχύτητες που υποστηρίζονται, αυτές είναι οι : 106, 212, 424 και 848 kbps[4, 8, 9]. Όπως φαίνεται από τους ρυθμούς μετάδοσης,το NFC δεν είναι κατάλληλο για τη μεταφορά μεγάλου όγκου δεδομένων καθώς υπάρχουν ασύρματες τεχνολογίες όπως για παράδειγμα το Wifi που παρέχουν πολύ μεγαλύτερες ταχύτητες.

Ένα από τα μεγαλύτερα πλεονεκτήματα του NFC είναι ο τρόπος λειτουργίας του. Για να ξεκινήσει η επικοινωνία δεν απαιτείται καμία διαδικασία εγκαθίδρυσης σύνδεσης όπως συμβαίνει στις περισσότερες ασύρματες τεχνολογίες που γνωρίζουμε μέχρι τώρα. Δεν χρειάζεται ο χρήστης να εισάγει για παράδειγμα ένα κωδικό ή να επιλέξει τη συσκευή που θέλει να επικοινωνήσει. Μόλις οι δύο συσκευές έρθουν σε απόσταση αρκετά μικρή, μπορούν αμέσως να επικοινωνήσουν χωρίς καμία άλλη διαδικασία, κάτι που το κάνει ιδιαίτερα εύχρηστο αλλά και γρήγορο για τους χρήστες.

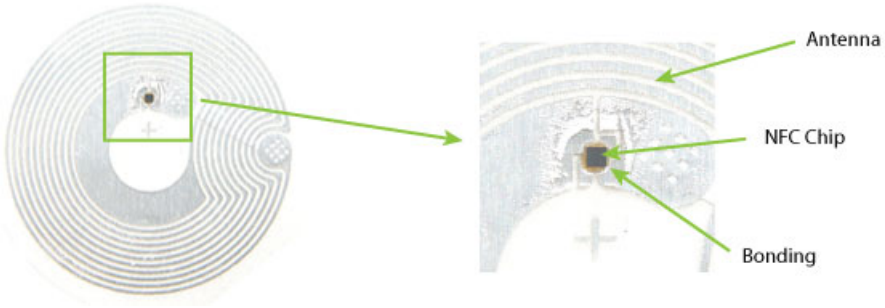
2.1 Κατηγορίες συσκευών

Οι συσκευές που χρησιμοποιούν το NFC χωρίζονται σε δύο κύριες κατηγορίες, τις **ενεργές** και τις **παθητικές**. Οι ενεργές συσκευές είναι εκείνες που μπορούν να παράγουν ηλεκτρομαγνητικό πεδίο. Οι παθητικές είναι ο συσκευές που δεν έχουν τη δυνατότητα να παράγουν οι ίδιες ηλεκτρομαγνητικό πεδίο και έτσι βασίζονται στη συσκευή που επικοινωνούν για να λειτουργήσουν και οι ίδιες.

2.1.1 Παθητικές συσκευές

Το κυριότερο παράδειγμα μιας παθητικής συσκευής είναι τα **NFC tags**. Τα NFC tags είναι συσκευές που επιτρέπουν την αποθήκευση δεδομένων. Ανάλογα με τον τύπο τους ενδέχεται να υποστηρίζουν και κάποιες επιπλέον λειτουργίες όπως είναι για παράδειγμα η κρυπτογράφηση. Είναι συνήθως μικρά και λεπτά σε μέγεθος και εμφανίζονται στο εμπόριο σε διαφορετικές μορφές, όπως είναι τα αυτοκόλλητα και οι κονκάρδες.

Τα μέρη που αποτελούν ένα NFC tag φαίνονται στο σχήμα 2.1.



Σχήμα 2.1: NFC Tag Parts

Όπως βλέπουμε από το σχήμα το μεγαλύτερο μέρος της επιφάνειας ενός NFC tag καλύπτεται από την κεραία του. Η κεραία αυτή είναι ένα πηνίο κατασκευασμένο με τέτοιο τρόπο ώστε να μπορεί να μετατρέπει το μαγνητικό πεδίο σε ενέργειά . Το υλικά κατασκευής της είναι το αλουμίνιο ή ο χαλκός, λόγο κόστους όμως το αλουμίνιο είναι πιο διαδεδομένο στην αγορά. Το πάχος της κεραίας δεν είναι ανάλογο της αποδοτικότητας της, για το λόγο αυτό βλέπουμε ότι οι κεραίες είναι τόσο λεπτές που μπορούν να χωρέσουν σε ένα αυτοκόλλητο για παράδειγμα. Αντίθετα με το πάχος, η διάμετρος της κεραίας έχει σημασία στην αποδοτικότητα της. Η καλύτερη απόδοση σε ένα NFC tag του δίνει δυνατότητα να λειτουργεί σε μεγαλύτερη απόσταση, χωρις βέβαια ποτέ αυτή να ξεπερνά τα 10 εκατοστά. Για παράδειγμα ένα NFC tag με κεραία διαμέτρου 25mm μπορεί να λειτουργήσει σε μία απόσταση μέχρι και 7 εκατοστών,

ενώ ένα που έχει κεραία διαμέτρου 38mm μπορεί να λειτουργήσει σε απόσταση 9 εκατοστών. Όσο μεγαλύτερη είναι η κεραία τόσο πιο ισχυρό είναι και το μαγνητικό πεδίο που απαιτεί για να μπορέσει να λειτουργήσει το NFC tag, για αυτό δεν συναντάμε ιδιαίτερα μεγάλες κεραίες αφού οι συσκευές που διαβάζουν/γράφουν τα NFC tags, που είναι κυρίως κινητά τηλέφωνα, δεν μπορούν να παρέχουν ισχυρό μαγνητικό πεδίο.

Εκτός της κεραίας ένα βασικό μέρος του NFC tag είναι το NFC chip. Το NFC chip είναι ένα πολύ μικρό σε μέγεθος ολοκληρωμένο κύκλωμα που είναι υπεύθυνο για όλες τις λειτουργίες του NFC tag. Τα NFC chips διαφέρουν σε τομείς όπως είναι ο διαθέσιμος αποθηκευτικός χώρος, η δυνατότητα προγραμματισμού ώστε να είναι μόνο για ανάγνωση, η υποστήριξη κρυπτογραφημένης επικοινωνίας, τα υποστηριζόμενα ISO, και άλλα.

Το NFC forum έχει κατηγοριοποιήσει τα NFC tags σε τέσσερις τύπους. Στον πίνακα 2.1 μπορούμε να δούμε τα βασικά χαρακτηριστικά του κάθε τύπου και μερικά προϊόντα που ανήκουν στην κάθε κατηγορία[2].

2.1.2 Ενεργές συσκευές

Οι ενεργές συσκευές μπορούν να παράγουν το ηλεκτρομαγνητικό πεδίο που απαιτείται για να υπάρξει NFC επικοινωνία. Υπάρχουν στο εμπόριο συσκευές που συνδέονται και ελέγχονται με τον υπολογιστή, ονομάζονται **NFC Readers/Writers** και μπορούν να διαβάσουν/γράψουν κάποια είδη από NFC tags ανάλογα βέβαια με το κάθε μοντέλο. Οι συσκευές αυτές σε αντίθεση με τα **κινητά τηλέφωνα**, δεν είναι φορητές. Τον τελευταίο καιρό αρχίζει το NFC να γίνεται μία τεχνολογία που υιοθετούν όλο και περισσότεροι κατασκευαστές κινητών τηλεφώνων. Ήδη μερικές μόνο από τις εταιρίες που παράγουν συσκευές με υποστήριξη NFC είναι οι : Nokia, Sony,Samsung, LG, RIM και ZTE. Τα κινητά τηλέφωνα έχουν ένα NFC chip όπως είναι τα NXP N65 και Broadcom BCM20793 και έχουν την κεραία του NFC είτε πάνω στη μπαταρία είτε στο στο πίσω καπάκι της συσκευής.

Τύπος NFC Tag	**Σύντομη περιγραφή**	**Παραδείγματα προϊόντων**
NFC Forum Type 1	Βασίζονται στο ISO/IEC 14443A. Μπορούν να διαβαστούν και να γραφούν/ επανεγραφούν. Μπορούν να προγραμματιστούν και ώστε να είναι μόνο για ανάγνωση. Η διαθέσιμη χωρητικότητα είναι από 96 bytes μέχρι και 2 KB.	Broadcom Topaz
NFC Forum Type 2	Βασίζονται στο ISO/IEC 14443A. Μπορούν να διαβαστούν και να γραφούν/ επανεγραφούν. Μπορούν να προγραμματιστούν και ώστε να είναι μόνο για ανάγνωση. Η διαθέσιμη χωρητικότητα είναι από 48 bytes μέχρι και 2 KB.	NXP NTAG203, NXP Mifare Ultralight
NFC Forum Type 3	Βασίζονται στο Japanese Industrial Standard (JIS) X 6319-4 που είναι γνωστό και ως FeliCa. Είναι ρυθμισμένα από τον κατασκευαστή να είναι είτε με δυνατότητα επανεγγραφής είτε μόνο για ανάγνωση. Η διαθέσιμη μνήμη διαφέρει με το θεωρητικό όριο να αγγίζει το 1 MB ανά υπηρεσία.	Sony FeliCa
NFC Forum Type 4	Είναι πλήρως συμβατά με το ISO/IEC 14443, το περιβάλλον επικοινωνίας μπορεί να είναι τύπου A ή του τύπου B. Είναι ρυθμισμένα από τον κατασκευαστή να είναι είτε με δυνατότητα επανεγγραφής είτε μόνο για ανάγνωση. Η διαθέσιμη μνήμη διαφέρει και φτάνει τα 32 KB ανά υπηρεσία.	NXP DesFire, NXP SmartFX with JCOP

Πίνακας 2.1: NFC Forum Tag Types

2.2 Περιπτωσεις χρήσης του NFC

Τώρα που έχουμε κατανοήσει τις κατηγορίες των συσκευών που χρησιμοποιούνται στο NFC μπορούμε να ορίσουμε τις περιπτώσεις χρήσης της τεχνολογίας. Έχουμε τρεις περιπτώσεις χρήσης οι οποίες είναι οι εξής:

- **Reader/Writer Mode**
- **Peer to peer Mode**
- **Card Emulation Mode**

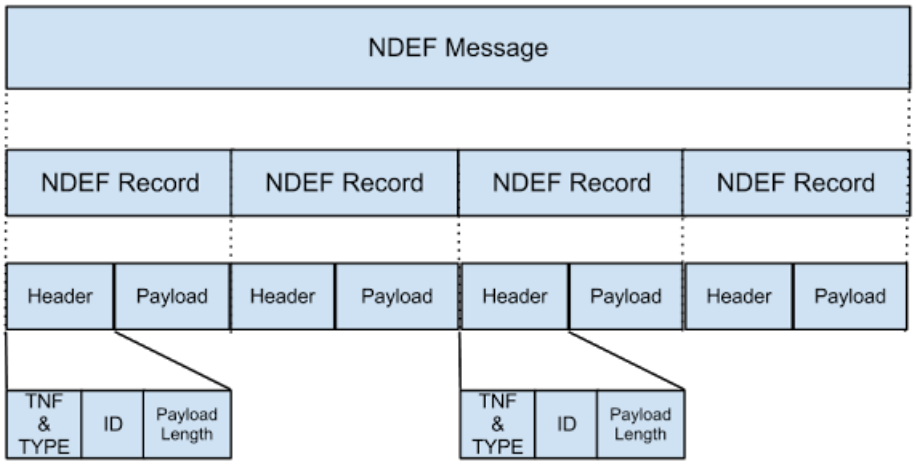
Reader/Write Mode: Σε αυτήν την περίπτωση χρήσης έχουμε επικοινωνία ανάμεσα σε μία ενεργή και σε μία παθητική συσκευή. Έχουμε λοιπόν για παράδειγμα ένα κινητό τηλέφωνο το οποίο διαβάζει ή γράφει ένα NFC tag. Όταν έρθουν σε κοντινή απόσταση το κινητό τηλέφωνο δημιουργεί το ηλεκτρομαγνητικό πεδίο που βάζει σε λειτουργία το NFC tag και ξεκινάει η ανταλλαγή των δεδομένων. Τα δεδομένα που ανταλλάσσονται έχουν συνήθως μια συγκεκριμένη δομή που έχει ορίσει το NFC forum και ονομάζεται NFC Data Exchange Format (NDEF). Θα περιγράψουμε το NDEF αργότερα σε αυτό το κεφάλαιο.

Peer to peer Mode: Με αυτήν την περίπτωση χρήσης έχουμε επικοινωνία ανάμεσα σε δύο ενεργές συσκευές. Δύο κινητά τηλέφωνα παραδείγματος χάριν ανταλλάσσουν πληροφορίες το ένα με το άλλο. Δεν υποστηρίζεται η ταυτόχρονη επικοινωνία, όταν η μία συσκευή στέλνει δεδομένα, η άλλη μπορεί μόνο να διαβάζει. Το πρωτόκολλο που χρησιμοποιείται λέγεται Logical Link Control Protocol (LLCP) και έχει δημιουργηθεί από το NFC forum. Οι συσκευές ανταλλάσσουν δεδομένα οποιουδήποτε τύπου, όπως είναι εικόνες, ηλεκτρονικές διευθύνσεις ή κείμενο αρκεί αυτά να έχουν τη δομή NDEF.

Card Emulation Mode: Σε αυτήν περίπτωση επικοινωνίας έχουμε δύο ενεργές συσκευές που αλληλεπιδρούν μεταξύ τους. Η μία από τις συσκευές προσομοιώνει ένα NFC tag ενώ η άλλη διαβάζει η γράφει σε αυτό το “εικονικό” NFC tag. Αυτού του τύπου η επικοινωνία χρησιμοποιείται κυρίως για ηλεκτρονικές πληρωμές, ηλεκτρονικά εισιτήρια ή έλεγχο πρόσβασης. Όταν μία συσκευή προσομοιώνει ένα NFC tag τα κυριότερα ζητήματα που προκύπτουν αφορούν την ασφάλεια των δεδομένων που υπάρχουν σε αυτό το tag. Για να προστεθεί ένα επιπλέον επίπεδο ασφαλείας στα δεδομένα που αποθηκεύονται στο NFC tag, οι κατασκευαστές επέλεξαν να ασφαλίσουν αυτά τα δεδομένα με τη χρήση εξειδικευμένων για αυτόν το σκοπό συσκευών. Οι συσκευές αυτές ονομάζονται Secure Elements και θα τις αναφέρουμε αναλυτικότερα στο τέλος του κεφαλαίου.

2.3 NDEF

Το NDEF είναι μία δυαδική δομή δεδομένων που μπορεί να χρησιμοποιηθεί για την ανταλλαγή πληροφοριών μεταξύ NFC συσκευών που υποστηρίζουν τα πρότυπα του NFC forum. Οι πληροφορίες ενθυλακώνονται και μεταφέρονται στα επονομαζόμενα NDEF μηνύματα. Πληροφορίες οποιουδήποτε είδους η μεγέθους μπορούν να ενθυλακωθούν σε ένα η περισσότερα NDEF μηνύματα. Κάθε NDEF μήνυμα αποτελείται από μία η περισσότερες εγγραφές που ονομάζονται NDEF records. Στο σχήμα 2.2 φαίνεται η δομή του NDEF μηνύματος καθώς και της NDEF εγγραφής.



Σχήμα 2.2: NDEF Format Overview

Κάθε NDEF εγγραφή μπορεί να έχει θεωρητικά μέγεθος μέχρι και περίπου 4 GB, δεν υπάρχει βέβαια κανένα NFC tag που να υποστηρίζει τέτοια χωρητικότητα. Όπως φαίνεται και στο σχήμα 2.2 η κεφαλίδα του NDEF record αποτελείται από τρία μέρη, το ID που είναι ένα μοναδικό αναγνωριστικό, το Payload Length που είναι το μέγεθος του φορτίου, και το TNF & Type που υποδεικνύει τον τύπο των δεδομένων της NDEF εγγραφής. Υπάρχουν αρκετοί υποστηριζόμενοι τύποι δεδομένων όπως είναι οι ηλεκτρονικές διευθύνσεις για παράδειγμα, πέραν αυτών όμως μια NDEF εγγραφή μπορεί να περιέχει δεδομένα που δεν ανήκουν στους υποστηριζόμενους τύπους αρκεί να βάλει την αντίστοιχη τιμή στο πεδίο TNF & Type.

2.4 Secure elements

Τα secure elements είναι συνήθως συσκευές που εξασφαλίζουν την ασφάλεια στις συναλλαγές με το NFC. Με τις συσκευές αυτές παρέχεται ένα επιπλέον επίπεδο ασφαλείας με τη χρήση κρυπτογράφησης στο υλικό και όχι στο λογισμικό το οποίο και παραβιάζεται συγκριτικά πιο εύκολα. Εξασφαλίζουν ένα ασφαλές περιβάλλον για την αποθήκευση δεδομένων, την εκτέλεση και τη διαχείριση εφαρμογών. Υπάρχουν τα εξής ήδη από secure elements:

- **Hardware Modules**
- **Subscriber Identity Application (SIM)**
- **Secure Multimedia Card (Secure MMC)**
- **Soft-SE**

Hardware Modules: Είναι chip (συνήθως έξυπνη κάρτα) που έχει τοποθετήσει εντός του κινητού τηλεφώνου ο κατασκευαστής του. Δεν είναι εμφανές στο χρήστη παρά μόνο εάν αποσυναρμολογήσει το κινητό τηλέφωνο. Μερικά παραδείγματα από τέτοια chips είναι το Broadcom BCM20793 που χρησιμοποιεί το LG Nexus 4 καθώς και το NXP FN544 που χρησιμοποιεί το HTC ONE X[3].

Subscriber Identity Application (SIM): Η κάρτα SIM μπορεί να χρησιμοποιηθεί και ως secure element αφού παρέχει δυνατότητες κρυπτογράφησης. Η επιλογή αυτή έχει κάποια οφέλη αφού δεν προστίθεται καθόλου επιπλέον κόστος. Οι πάροχοι κινητής τηλεφωνίας προωθούν τη χρήση της κάρτας SIM ως secure element αφού αυτοί έχουν τον έλεγχο για τις κάρτες αυτές.

Secure Multimedia Card (Secure MMC): Κάρτες μνήμης μπορούν να χρησιμοποιηθούν ως secure elements εάν και η εκδοχή αυτή δεν είναι ιδιαίτερα δημοφιλής. Ένα παράδειγμα μίας τέτοιας κάρτας είναι η Salinon SD της UBIVELOX.

Soft-SE: Αυτό είναι το μόνο είδος που δεν αποτελεί υλικό και είναι μία καινούργια τεχνολογία που ξεκίνησε η εταιρία RIM[16]. Η υλοποίηση στο λογισμικό του secure element όμως έχει κάποιο αντίκτυπο στην ασφάλεια αφού όλες οι λειτουργίες ασφαλής εκτέλεσης πλέον εξαρτώνται από τις δυνατότητες της ίδιας της CPU.

Κεφάλαιο 3

Εισαγωγή στο e-voting

Η εκλογές αποτελούν μία διαδικασία που είναι απαραίτητη σε όλες τις δημοκρατικές κοινωνίες. Η διαδικασία της ψηφοφορίας στις περισσότερες ακόμα χώρες γίνεται με τη χρήση εκλογικών κέντρων. Κάθε εκλογικό κέντρο δέχεται ένα μερίδιο των ψηφοφόρων, πιστοποιεί την ταυτότητα τους και το δικαίωμα τους για ψήφο με τα κατάλληλα έγραφα και έπειτα τους επιτρέπετε να ψηφίσουν. Αφού επιλέξει ο κάθε ψηφοφόρος την ψήφο του, που είναι σε χάρτινη μορφή, τη βάζει σε ένα φάκελο και την τοποθετεί στην κάλπη. Αφότου περάσει το χρονικό διάστημα που έχει προκαθοριστεί, οι ψήφοι καταμετρούνται για να βγουν τα τελικά αποτελέσματα. Από την παραπάνω περιγραφή είναι εμφανές ότι η διαδικασία της ψηφοφορίας είναι δύσχρηστη για τον ψηφοφόρο και πολυέξοδη για το διεξαγωγέα. Για να λυθούν τα όποια προβλήματα της εκλογικής διαδικασίας αλλά και για την εξέλιξη της, έχουν σχεδιαστεί συστήματα ηλεκτρονικής ψηφοφορίας. Με τα συστήματα αυτά είναι δυνατόν να γίνει η καταχώρηση και η καταμέτρηση των ψήφων με ηλεκτρονικές συσκευές. Η σημερινή τεχνολογία μας επιτρέπει να χρησιμοποιούμε ηλεκτρονικά μέσα για την ψηφοφορία χωρίς να καταπατούμε τις απαιτήσεις της διαδικασίας. Σε αυτό το κεφάλαιο θα δούμε τις απαιτήσεις της ηλεκτρονικής ψηφοφορίας όπως αυτές εμφανίζονται στη βιβλιογραφία και θα κάνουμε μία μικρή ιστορική αναδρομή.

3.1 Απαιτήσεις σύστηματος ηλεκτρονικής ψηφοφορίας

Παρακάτω αναφέρουμε τις βασικές απαιτήσεις της ηλεκτρονικής ψηφοφορίας, όπως αυτές υπάρχουν στη βιβλιογραφία[20].

Ακρίβεια: Ακρίβεια ή αλλιώς ορθότητα, είναι η απαίτηση τα αποτελέσματα των εκλογών να είναι χωρίς σφάλματα. Όλες δηλαδή οι έγκυρες ψήφοι πρέπει να καταμετρηθούν κανονικά και όλες η άκυρες πρέπει να μην συμπεριλαμβάνονται στην καταμέτρηση.

Δημοκρατία: Η δημοκρατία είναι η απαίτηση να ψηφίζουν μόνο όσοι έχουν το νόμιμο δικαίωμα, μία μοναδική φορά.

Ιδιωτικότητα: Με βάση αυτήν την απαίτηση δεν πρέπει να είναι δυνατόν κάποιος να μπορεί να συνδέσει ένα ψηφοφόρο με την ψήφο του.

Ανθεκτικότητα: Η απαίτηση αυτή εγγυάται ότι δεν μπορεί να λάβει χώρα μια προσωρινή συνεργασία, είτε ψηφοφόρων είτε αρχών, η οποία θα μπορούσε να διακόψει τη διαδικασία της ψηφοφορίας.

Επαληθευσιμότητα: Η επαληθευσιμότητα εγγυάται ότι υπάρχουν οι απαραίτητοι μηχανισμοί ελέγχου της σωστής διεξαγωγής των εκλογών.

Προστασία απο εξαναγκασμό: Αυτή η απαίτηση αφορά την αδυναμία ενός ψηφοφόρου να αποδείξει με οποιονδήποτε τρόπο την επιλογή της ψήφου του.

Δικαιοσύνη: Με την απαίτηση αυτή δεν πρέπει να είναι δυνατόν κάποιος να μάθει τα αποτελέσματα της ψηφοφορίας πριν την επίσημη καταμέτρηση τους.

Επαληθεύσιμη συμμετοχή: Με την απαίτηση αυτή θα πρέπει να υπάρχει δυνατότητα να ελεγχθεί εάν κάποιος πήρε μέρος στην ψηφοφορία.

3.2 Η εξέλιξη της ηλεκτρονικής ψηφοφορίας

Για να φτάσουμε σήμερα να έχουμε ολοκληρωμένα συστήματα ηλεκτρονικής ψηφοφορίας που χρησιμοποιούνται για τις εθνικές εκλογές η μετάβαση δεν ήταν ακαριαία. Στο παρελθόν έχουν προταθεί μορφές ψηφοφορίας, που η εξέλιξη τους μας έδωσε τα σημερινά συστήματα ηλεκτρονικής ψηφορορίας[18, 19].

Lever Machines

Το 1892 παρουσιάστηκαν για πρώτη φορά στη Νέα Υόρκη οι Lever Machines. Αποτελούν μηχανικές συσκευές που βασίζονται στη χρήση μοχλών για την επιλογή των ψήφων. Το κάθε ψηφοδέλτιο ήταν δίπλα από ένα μοχλό, μόλις ο ψηφοφόρος τραβούσε κάποιο μοχλό δεν ήταν δυνατόν να τραβήξει άλλον. Αυτές η μηχανές αντικατέστησαν την κάλπη που υπάρχει στο εκλογικό κέντρο και τα ίδια τα ψηφοδέλτια, ακόμα άλλαξαν και τον τρόπο καταμέτρησης των ψήφων. Από το 1930 πολλές πόλεις των ΗΠΑ χρησιμοποιούσαν αυτές τις μηχανές για τη διεξαγωγή των εκλογών τους, ενώ με τα χρόνια η χρήση τους μειώθηκε, ακόμα και μετά το 2000 είχαν ένα σημαντικό ποσοστό χρήσης στις ΗΠΑ.

Punched-Card

Στα τέλη της δεκαετίας του 1880 παρουσιάστηκε από τον Herman Hollerith το σύστημα ψηψοφορίας με χρήση των Punched cards. Το σύστημα αυτό χρησιμοποιούσε κάρτες που είχαν εκτυπωμένες πάνω τους τις επιλογές των ψήφων. Ο ψηφοφόρος έπρεπε να τρυπήσει στα σημεία που υποδείκνυε η κάρτα ότι βρίσκονται οι επιλογές του. Τέλος η κάρτα τοποθετούνταν σε μία συσκευή που έκανε ανάγνωση των επιλογών της. Το 2000 χρησιμοποιούνταν στο 37% των πόλεων στις ΗΠΑ.

Direct Recording Electronic Systems

Τη δεκαετία του 1970 παρουσιάστηκαν για πρώτη φορά τα συστήματα Direct Recording Electronic System. Τα DRE συστήματα χρησιμοποιούν συσκευές που βασίζονται σε μια οθόνη αφής για την επιλογή της ψήφου. Έχουν χρησιμοποιηθεί για τις εθνικές εκλογές στις ΗΠΑ αλλά και σε άλλες χώρες. Μετά την επιλογή της ψήφου από την οθόνη αφής η ψήφος αποθηκεύεται στο μηχάνημα για να σταλεί αργότερα στην τοποθεσία καταμέτρησης, μπορεί όμως και να εκτυπώνεται σε χαρτί ώστε ο ψηφοφόρος να μπορεί να την ελέγξει πριν ολοκληρωθεί η διαδικασία . Η καταμέτρηση των ψήφων γίνεται με τη χρήση ειδικών μηχανημάτων και είναι πολύ ταχύτερη από την καταμέτρηση από τους ανθρώπους όπως γίνεται σήμερα. Το 2004 το 31% των πόλεων στις ΗΠΑ χρησιμοποιούσαν τα συστήματα DRE για τη διεξαγωγή των εκλογών τους.

Αρκετές χώρες εντός και εκτός της Ευρωπαϊκής ένωσης έχουν ξεκινήσει να υιοθετούν την ηλεκτρονική ψηφοφορία για τη διεξαγωγή είτε των εθνικών είτε άλλου είδους εκλογών. Σε κάποιες πόλεις του Καναδά χρησιμοποιείται ηλεκτρονική ψηφοφορία για τις εθνικές εκλογές με το σύστημα VOTEX . Ακόμα σε ένα μέρος της Ελβετίας χρησιμοποιείται ηλεκτρονική ψηφοφορία για τη διεξαγωγή τοπικών εκλογών. Έπειτα στην Ινδία, σε τοπικό επίπεδο, και στη Νορβηγία, σε εθνικό επίπεδο, εφαρμόζονται πιλοτικά κάποια συστήματα ηλεκτρονικής ψηφοφορίας. Τέλος το 2005 η Εσθονία έγινε η πρώτη χώρα στον κόσμο που υιοθέτησε πλήρως σύστημα ηλεκτρονικής ψηφοφορίας, και συγκεκριμένα το σύστημα i-Voting, για τη διεξαγωγή των εθνικών εκλογών της[14].

Κεφάλαιο 4

Σχετικές εργασίες

Στο κεφάλαιο αυτό θα αναφέρουμε κάποιες σχετικές εργασίες που διαβάσαμε κατά τη διάρκεια της εκπόνισης της διπλωματικής αυτής εργασίας. Έχουμε επιλέξει να εμφανίσουμε τις σχετικές εργασίες με χρονολογική σειρά.

Sensus: A security-conscious electronic polling system for the Internet

Το 1997 οι Lorrie Faith Cranor και Ron K. Cytron παρουσίασαν το Sensus [10], ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας που βασίζεται στις τυφλές υπογραφές. Ο ψηφοφόρος αρχικά προετοιμάζει την ψήφο του κρυπτογραφόντας τη με ένα μυστικό κλειδί και έπειτα εφαρμόζοντας τη διαδικασία της τύφλωσης. Στη συνέχεια υπογράφει την ψήφο αυτή και τη στέλνει σε μία οντότητα που ονομάζεται Validator. Ο Validator ελέγχει την υπογραφή και πιστοποιεί ότι ο χρήστης έχει δικαίωμα ψήφου. Εάν ο έλεγχος είναι επιτυχής ο Validator υπογράφει την ψήφο και τη στέλνει πίσω στο χρήστη. Αυτός τότε αφαιρεί την τύφλωση και έτσι έχει μία κρυπτογραφημένη ψήφο που είναι υπογεγραμμένη από τον Validator. Έπειτα ο ψηφοφόρος στέλνει την ψήφο αυτή σε μία οντότητα που ονομάζεται Tallier. Αφού κάνει τον έλεγχο της υπογραφής ο Tailler τοποθετεί την ψήφο σε μια λίστα έγκυρων ψήφων και στη συνέχεια υπογράφει την ψήφο και τη στέλνει στον ψηφοφόρο σαν αποδεικτικό. Τέλος, αφού πάρει το αποδεικτικό, ο ψηφοφόρος στέλνει στον Tallier το μυστικό κλειδί που χρησιμοποίησε για να μπορέσει να διαβάσει το περιεχόμενο της ψήφου.

Security in Near Field Communication (NFC) Strengths and Weaknesses

Το 2006 οι Ernst Haselsteiner και Klemens Breitfuß έκαναν μία έρευνα για τους κινδύνους ασφαλείας αλλά και τις πιθανές λύσεις στην επικοινωνία με το NFC [5]. Η επίθεση eavesdropping είναι αρκετά δύσκολη επειδή επηρεάζεται από ένα μεγάλο πλήθος παραγόντων όπως είναι η γεωμετρία της κεραίας του θύματος αλλά και του επιτιθέμενου. Ένας επιτιθέμενος μπορεί να κάνει με σχετικά εύκολο τρόπο μία επίθεση άρνησης υπηρεσιών στέλνοντας το κατάλληλο ηλεκτρομαγνητικό πεδίο στο θύμα. Ακόμα η επίθεση της παραποίησης των δεδομένων που λαμβάνει το θύμα εί-

ναι δυνατή μόνο σε συγκεκριμένες κωδικοποιήσεις. Ένα αντίμετρο για τις δύο προηγούμενες επιθέσεις είναι ένας έλεγχος από τη συσκευή που στέλνει τα δεδομένα για την ύπαρξη άλλου ηλεκτρομαγνητικού πεδίου στο χώρο. Τέλος αναφέρεται η επίθεση man-in-the-middle χωρίς όμως μεγάλη επικινδυνότητα καθώς θεωρείται αδύνατη σε πραγματικά σενάρια. Η κύρια πρόταση τους για την αντιμετώπιση των απειλών είναι η δημιουργία ενός ασφαλούς καναλιού με τη χρήση του γνωστού αλγορίθμου Diffie-Hellman, προτείνουν μάλιστα έναν τρόπο υλοποίησης της αρχικής συμφωνίας του πρωτοκόλλου που κάνει ακόμα και το eavesdropping αδύνατο.

Mobile implementation and formal verification of an e-voting system

Το 2008 οι Stefano Campanelli, Alessandro Falleni, Fabio Martinelli, Marinella Petrocchi και Anna Vaccarelli πρότειναν ένα σύστημα ηλεκτρονικής ψηφοφορίας που βασίζεται στο Sensus πρωτόκολλο με όνομα “M-Seas”[7]. Το “M-Seas” προσθέτει μία φάση εγγραφής που στόχο έχει να αφαιρέσει μία ευπάθεια που είχε αναγνωριστεί στο Sensus πρωτόκολλο και έδινε τη δυνατότητα σε μία από τις οντότητες που συμμετέχουν στη διαδικασία να μπορεί να καταχωρήσει ψήφους από ψηφοφόρους που απείχαν των εκλογών. Στη φάση της εγγραφής ο ψηφοφόρος πρέπει να κάνει εγγραφή σε μια οντότητα που λέγεται Tallier με το δημόσιο κλειδί του και κάποιων επιπλέον ανανγνωριστικών. Για να γίνει η εγγραφή ο ψηφοφόρος στέλνει την υπογραφή των στοιχείων αυτών αφού πρώτα εφαρμόσει τη διαδικασία της τύφλωσης. Αφού ο Tallier πιστοποιήσει ότι ο χρήστης έχει δικαίωμα ψήφου υπογράφει με τη σειρά του τα δεδομένα του ψηφοφόρου και του τα στέλνει. Στη συνέχεια ο ψηφοφόρος αφαιρεί την τύφλωση και έτσι έχει τα δεδομένα του υπογεγραμμένα από τον Tallier. Τέλος για να ολοκληρωθεί η διαδικασία της εγγραφής ο ψηφοφόρος στέλνει στον Tallier τα δεδομένα του σε μη κρυπτογραφημένη μορφή προσθέτοντας όμως και την υπογραφή που έλαβε πριν απο τον Tallier. Στη συνέχεια ο ψηφοφόρος κρυπτογράφει την ψήφο του με ένα μυστικό κλειδί, παράγει την σύνοψη της, της εφαρμόζει τη διαδικασία της τύφλωσης και αφού την κρυπτογραφίσει και πάλι με το δημόσιο κλειδί του, τη στέλνει σε μια οντότητα που λέγεται Validator. Ο Validator ελέγχει την ταυτότητα του ψηφοφόρου και το δικαίωμα του για ψήφο, εάν οι έλεγχοι είναι επιτυχείς, ο Validator υπογράφει τη σύνοψη και τη στέλνει πίσω στον ψηφοφόρο. Ο ψηφοφόρος στη συνέχεια στέλνει την ψήφο του αλλά και τη σύνοψη της, που είναι υπογεγραμμένη και από αυτόν αλλά και από τον Validator, στην οντότητα Tallier. Ο Tallier ελέγχει την ταυτότητα του ψηφοφόρου και εάν όλοι οι έλεγχοι είναι επιτυχείς, τοποθετεί την ψήφο του στη λίστα με τις έγκυρες ψήφους. Έπειτα ο Tallier υπογράφει την ψήφο που έλαβε και τη στέλνει στον ψηφοφόρο. Τέλος ο ψηφοφόρος στέλνει στον Tallier το κλειδί για να αποκρυπτογραφήσει την ψήφο του.

Secure Communication between Web Browsers and NFC Targets by the Example of an e-Ticketing System

Το 2008 οι Gerald Madlmayr, Peter Kleebauer, Josef Langer και Josef Scharinger παρουσιάσαν ένα σύστημα ηλεκτρονικών εισιτηρίων που χρησιμοποιεί ένα ασφαλές κανάλι με NFC για τη μεταφορά των εισιτηρίων στις συσκευές[15]. Τα εισιτήρια αποθηκεύονται στο secure element του κινητού ή σε μία έξυπνη κάρτα. Η συναλλαγή γίνεται ως εξής , ο πελάτης πηγαίνει στην ιστοσελίδα του παρόχου των εισιτηρίων, κάνει την αγορά και επιλέγει την παράδοση με NFC. Ένα plugin στον browser του πελάτη συνδέεται αρχικά με το διακομιστή του παρόχου και στη συνέχεια με μία συσκευή ανάγνωσης/εγγραφής NFC συσκευών που θα πρέπει να έχει ο πελάτης. Ο πελάτης τότε τοποθετεί της συσκευή στην οποία θέλει να αποθηκευτούν τα εισιτήρια κοντά στη συσκευή ανάγνωσης/εγγραφής NFC για να γίνει η μεταφορά των εισιτηρίων . Η επικοινωνία από το διακομιστή του παρόχου μέχρι και τη συσκευή του χρήστη είναι κρυπτογραφημένη. Η αρχιτεκτονική PKI χρησιμοποιείται για την αυθεντικοποίηση και την κρυπτογράφηση των δεδομένων. Εκτός από τις οντότητες πελάτης και εκδότης έχει προστεθεί και μία τρίτη οντότητα η οποία θεωρείται έμπιστη και είναι απαραίτητη για την ασφαλή επικοινωνία.

A secure NFC application for credit transfer among mobile phones

Το 2012 οι David M. Monteiro,Joel J. P. C. Rodrigues,και Jaime Lloret υλοποίησαν μία εφαρμογή που επιτρέπει στο χρήστη να μεταφέρει χρήματα απο το λογαριασμό του κινητού του, σε κάποιον άλλο χρήστη[17]. Ο χρήστης πρέπει να εισάγει την ποσότητα των χρημάτων που θέλει να στείλει και έπειτα πρέπει να φέρει το κινητό του αρκετά κοντά με το κινητό του δέκτη για να ξεκινήσει η NFC επικοινωνία. Αυτή με τη σειρά της, θα ξεκινήσει μία σύνδεση μέσω bluetooth με το δέκτη ώστε να μη χρειάζεται να βρίσκονται τα κινητά σε κοντινή απόσταση για μεγάλο χρονικό διάστημα. Τη μεταφορά των χρημάτων την αναλαμβάνει βέβαια ο πάροχος των υπηρεσιών, η εφαρμογή αυτή κάνει μόνο μία αίτηση προς το πάροχο για τη μεταφορά των χρημάτων. Αναφέρεται ότι είναι ασφαλής η επικοινωνία αλλά δεν προτείνει κάποιο συγκεκριμένο πρωτόκολλο που χρησιμοποιεί το σύστημα.

Potential Misuse of NFC Enabled Mobile Phones with Embedded Security Elements as Contactless Attack Platforms

Το 2009 οι Lishoy Francis, Gerhard Hancke, Keith Mayes και Konstantinos Markantonakis χρησιμοποίησαν το κινητό Nokia 6131 για να υλοποιήσουν κάποιες επιθέσεις με τη χρήση του NFC[12]. Έχουν “ξεκλειδώσει” το secure element του κινητού για να γίνει δυνατό να βάλουν εφαρμογές σε αυτό. Έτσι το κινητό μπορεί να προσομοιώσει έξυπνες κάρτες και NFC tags μόνο με τον προγραμματισμό της κατάλληλης εφαρμογής (Cloning attack). Ακόμα υλοποίησαν μία επίθεση με την οποία έγινε ικανό να υποκλέψουν τα δεδομένα που ανταλλάχθηκαν σε μία νόμιμη συναλλαγή με NFC (Skimming attack). Στη συνέχεια προτείνουν μέτρα για να μην γίνονται ικανές

τέτοιες επιθέσεις. Η υποχρεωτική υπογραφή όλων των εφαρμογών που χρησιμοποιούν NFC και η προσθήκη επιπλέον ρυθμίσεων ελέγχου του secure element από τον κατασκευαστή αποτελούν ένα μέρος των προτάσεων τους.

Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones

Το 2011 οι Lishow Francis, Gerhard Hancke, Keith Mayes και Konstantinos Markantonakis παρουσίασαν μία επίθεση αναμετάδοσης που υλοποίησαν με τη χρήση δύο κινητών τηλεφώνων[13]. Στην επίθεση αυτή το κινητό Nokia 6131 ρυθμίστηκε ώστε να λειτουργεί ως πληρεξούσιος αναγνώστης και το κινητό Blackberry 9900 ως πληρεξούσια έξυπνη κάρτα. Βάζοντας τον πληρεξούσιο αναγνώστη (Nokia 6131) σε κοντινή επαφή με την πραγματική έξυπνη κάρτα και την πληρεξούσια έξυπνη κάρτα (Blackberry 9900) κοντά στον πραγματικό αναγνώστη καρτών κατάφεραν να ολοκληρώσουν συναλλαγές που θα απαιτούσαν ο αναγνώστης και η κάρτα να έρθουν σε πολύ κοντινή απόσταση. Στη συγκεκριμένη υλοποίηση τα δύο κινητά επικοινωνούν με bluetooth για την ανταλλαγή των δεδομένων τους αλλά αντ'αυτού θα μπορούσε να χρησιμοποιηθεί οποιαδήποτε ασύρματη τεχνολογία. Η αναμετάδοση παρατηρήθηκε ότι πρόσθεσε κάποια καθυστέρηση στην επικοινωνία, ο έλεγχος της καθυστέρησης θα μπορούσε να αποτελέσει ένα μέτρο καταπολέμησης της επίθεσης αυτής. Τέλος η χρήση του GPS για τον έλεγχο της τοποθεσίας των συσκευών που επικοινωνούν θα ήταν ικανή να λύσει και αυτή το πρόβλημα των επιθέσεων τέτοιου είδους.

Anonymous Ticketing for NFC-Enabled Mobile Phones

Το 2012 οι David Derler, Klaus Potzmader, Johannes Winter και Kurt Dietrich πρότειναν έναν πρωτόκολλο ηλεκτρονικών εισιτηρίων με τη χρήση του NFC που παρέχει ανωνυμία στο χρήστη[11]. Θεώρησαν ότι εάν δεν υπάρχει ανωνυμία στα εισιτήρια κάποιος θα μπορούσε να βρει από ποια σημεία πέρασε ο κάθε πελάτης, κάτι που θα παραβίαζε ιδιαίτερα την ιδιωτικότητα του. Χρησιμοποίησαν ένα πρωτόκολλο τύπου selective disclosure που επιτρέπει με τη χρήση ψηφιακών υπογραφών την επιλεκτική τύφλωση ενός μέρους των στοιχείων του χρήστη. Στην υλοποίηση τους τα εισιτήρια αποθηκεύονται στο secure element ενός κινητού τηλεφώνου Nokia 6131. Για την έκδοση των εισιτηρίων ο πελάτης θα πρέπει να μεταβεί στα σημεία έκδοσης εισιτηρίων ώστε να φέρει σε επαφή το κινητό του με τις συσκευές έκδοσης εισιτηρίων. Αντίστοιχα όταν ο χρήστης θέλει να χρησιμοποιήσει το εισιτήριο του θα πρέπει να φέρει το κινητό του σε κοντινή απόσταση με τις συσκευές επικύρωσης εισιτηρίων.

Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme

Το 2013 οι Jurlind Budurushi, Stephan Neumann, Maina Olembo και Melanie Volkamer παρουσίασαν ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας που χρησιμοποιεί τη μέθοδο του code voting[6]. Τονίζουν ιδιαίτερα τη δυνατότητα να κατανοήσει ο ψηφοφόρος τη λειτουργία του πρωτοκόλλου τους, καθώς αυτός είναι ο μόνος τρόπος να το εμπιστευθεί. Πριν ξεκινήσει η διαδικασία της ψηφοφορίας ο κάθε ψηφοφόρος λαμβάνει ένα φάκελο με τα απαραίτητα για την ψηφοφορία στοιχεία. Όλες οι επιλογές των ψήφων βρίσκονται σε αυτόν το φάκελο και η κάθε ψήφος συνδέεται με έναν κωδικό. Ο χρήστης καταχωρεί τον κωδικό αυτόν κατά τη διάρκεια της ψηφοφορίας. Οι κωδικοί που λαμβάνει ο ψηφοφόρος είναι μοναδικοί για αυτόν. Η ψηφοφορία γίνεται μέσω μιας ιστοσελίδας την οποία επισκέπτονται οι χρήστες για να καταχωρήσουν τις ψήφους τους. Η επικοινωνία με τους διακομιστές γίνεται με τη χρήση του πρωτοκόλλου SSL.

Κεφάλαιο 5

NFC Voting

5.1 Εισαγωγή

Σχεδιάζοντας ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να λάβουμε υπόψιν μας όλους τους παράγοντες που διασφαλίζουν την ασφάλεια αλλά και την εγκυρότητα των συναλλαγών που διεξάγονται. Εκτός αυτών όμως, ένα σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να είναι εύχρηστο καθώς απευθύνεται σε μεγάλο κοινό. Παρακάτω θα παρουσιάσουμε το δικό μας πρωτόκολλο για τη διεξαγωγή ηλεκτρονικής ψηφοφορίας χρησιμοποιώντας την τεχνολογία του NFC. Προσπαθήσαμε να φτιάξουμε ένα εύκολο στην υλοποίηση σύστημα που παρέχει όμως τους απαραίτητους μηχανισμούς για την εξασφάλιση της ασφάλειας και της ιδιωτικότητας της διαδικασίας. Στο πρωτόκολλο μας ο ψηφοφόρος μπορεί να ψηφίσει από οπουδήποτε και εάν βρίσκεται, το μόνο που χρειάζεται είναι μία κινητή συσκευή με υποστήριξη NFC που έχει εγκατεστημένη την εφαρμογή της ηλεκτρονικής ψηφοφορίας, ένα NFC tag που θα του παρέχει η αρχή διεξαγωγής και μία σύνδεση στο διαδίκτυο.

5.1.1 Στάδια ψηφοφορίας

Στάδιο εγγραφής χρήστη

Στο στάδιο αυτό ο χρήστης εγγράφεται στο σύστημα της ηλεκτρονικής ψηφοφορίας ώστε να αναγνωρίζεται από αυτό ως νόμιμος ψηφοφόρος. Για την εγγραφή του απαιτείται η φυσική παρουσία του ψηφοφόρου σε κάποιο χώρο της αρχής διεξαγωγής των εκλογών. Στόχος της επίσκεψης αυτής είναι η απόκτηση ενός NFC tag ειδικά διαμορφωμένου για τον ψηφοφόρο που θα χρησιμοποιηθεί στα επόμενα στάδια της ψηφοφορίας. Το NFC tag περιέχει δεδομένα που έχει στην κατοχή της μόνο η αρχή διεξαγωγής των εκλογών. Κατά την παραλαβή του NFC tag θα ζητάται από τον ψηφοφόρο να ορίσει για αυτό έναν προσωπικό κωδικό. Τον κωδικό αυτό θα πρέπει να τον γνωρίζει μόνο ο ψηφοφόρος και είναι απαραίτητος για την πρόσβαση στα δεδομένα του NFC tag. Ένα tag θα μπορούσε να χρησιμοποιηθεί σε περισσότερες από μία εκλογικές διαδικασίες, δεν είναι δηλαδή απαραίτητο ο ψηφοφόρος να λαμβάνει ένα καινούργιο NFC tag πριν από κάθε ψηφοφορία.

Στάδιο αυθεντικοποίησης ψηφοφόρου

Στο στάδιο αυτό ο ψηφοφόρος αυθεντικοποιείται με το σύστημα της ηλεκτρονικής ψηφοφορίας χρησιμοποιώντας το NFC tag που πήρε στο στάδιο της εγγραφής αλλά και την κινητή του συσκευή. Για να συμβεί αυτό ο ψηφοφόρος φέρνει σε αρκετά μικρή απόσταση την κινητή συσκευή με το NFC tag ώστε να είναι δυνατή η επικοινωνία. Ένα μήνυμα θα εμφανιστεί στην οθόνη της συσκευής με μία λίστα από εφαρμογές που μπορούν να διαχειριστούν το NFC tag. Ο ψηφοφόρος τότε θα πρέπει να επιλέξει την εφαρμογή της ηλεκτρονικής ψηφοφορίας και μόλις γίνει αυτό η εφαρμογή θα του ζητήσει τον κωδικό για να έχει πρόσβαση στο NFC tag. Εάν ο κωδικός είναι σωστός θα ξεκινήσει η διαδικασία της αυθεντικοποίησης, ο χρήστης δεν χρειάζεται να κάνει κάποια ενέργεια σε αυτήν τη διαδικασία.

Στάδιο επιλογής ψήφου

Στο στάδιο της επιλογής ψήφου η εφαρμογή της ηλεκτρονικής ψηφοφορίας θα εμφανίσει όλα τα ψηφοδέλτια στην οθόνη της κινητής συσκευής. Ο ψηφοφόρος στη συνέχεια θα πρέπει να επιλέξει την ψήφο που επιθυμεί να καταχωρήσει. Έπειτα, η εφαρμογή εμφανίζει ένα μήνυμα επιβεβαίωσης όπου ο χρήστης μπορεί να ελέγξει την επιλογή του πριν την καταχωρήσει οριστικά. Επιπλέον της ψήφου, στην οθόνη επιβεβαίωσης εμφανίζονται κάποια προσωπικά στοιχεία του ψηφοφόρου και ένα Captcha. Εάν όλα τα στοιχεία είναι σωστά , ο ψηφοφόρος λύνει το Captcha και επιλέγει την ολοκλήρωση της διαδικασίας από την εφαρμογή. Αφού η ψηφοφορία ολοκληρωθεί, εμφανίζεται στην οθόνη της εφαρμογής μήνυμα επιβεβαίωσης. Σε όλη τη διάρκεια

της ψηφοφορίας θα πρέπει να το NFC tag να βρίσκεται σε επικοινωνία με την κινητή συσκευή.

5.2 Ανάλυση του πρωτοκόλλου NFC Voting

Στο πρωτόκολλο που προτείνουμε η κινητή συσκευή επικοινωνεί με δύο διακομιστές κατά τη διαδικασία της ψηφοφορίας. Ο ένας ονομάζεται Catalog Server και χρησιμοποιείται κυρίως για την αυθεντικοποίηση του ψηφοφόρου. Ο δεύτερος ονομάζεται Ballot Server και είναι υπεύθυνος για τη συλλογή των ψήφων. Το πρωτόκολλο μας χρησιμοποιεί δημόσια και ιδιωτικά κλειδιά για την κρυπτογράφιση των δεδομένων αλλά και για την αυθεντικοποίηση του χρήστη. Για την ασφάλεια των επικοινωνιών χρησιμοποιούνται τα πρωτόκολλα SSL,IPSEC και TOR όπως θα δούμε αναλυτικότερα παρακάτω.

5.2.1 Βασικά Στοιχεία

NFC tag: Το NFC tag που χρησιμοποιούμε στο NFC voting έχει τα δεδομένα του χωρισμένα στα ακόλουθα πεδία.

- ***User ID*** Το πεδίο User ID περιέχει γενικές πληροφορίες για τον ψηφοφόρο όπως είναι το όνομα και η ημερομηνία γέννησης του.
- ***Upu*** Το δημόσιο κλειδί του ψηφοφόρου.
- ***Upr*** Το ιδιωτικό κλειδί του ψηφοφόρου.
- ***CSpu*** Το δημόσιο κλειδί του Catalog Server.
- ***VFCS*** Το πεδίο αυτό έχει μία μεταβλητή με όνομα Vote Flag CS η οποία αλλάζει ανάλογα με το στάδιο της ψηφοφορίας στο οποίο βρίσκεται ο ψηφοφόρος. Οι τιμές που παίρνει η μεταβλητή αυτή είναι 0, 1, 2. Η τιμή 0, που ειναι και η αρχική τιμή, υποδεικνύει ότι ο ψηφοφόρος δεν έχει αυθεντικοποιηθεί ακόμα. Η τιμή 1 δείχνει ότι ο ψηφοφόρος έχει αυθεντικοποιηθεί επιτυχώς αλλά δεν έχει στείλει ακόμα τις επιλογές των ψήφων του. Τέλος η τιμή 2 υποδεικνύει ότι ο ψηφοφόρος έχει ολοκληρώσει τη διαδικασία της ψηφοφορίας. Το πεδίο αυτό περιέχει τη μεταβλητή Vote Flag CS κρυπτογραφημένη και υπογεγραμμένη από τον Catalog Server.
- ***VFBS*** Το πεδίο αυτό περιέχει τη μεταβλητή Unique Random ID που έχει τυχαίο περιεχόμενο όπως δείχνει και το όνομα της. Το πεδίο VFBS περιέχει τη μεταβλητή Unique Random ID κρυπτογραφημένη και υπογεγραμμένη από τον Ballot Server.

Τα πεδία User Info, Upu, Upr και CSpu αρχικοποιούνται κατά την παραλαβή του NFC tag από την αρχή διεξαγωγής των εκλογών και έκτοτε δεν είναι δυνατή η τροποποίηση τους. Επιπλέον, ο κωδικός που έχει ορίσει ο ψηφοφόρος κατά την παραλαβή του tag ονομάζεται User Password και είναι απαραίτητος για την πρόσβαση στο πεδίο Upr.

Η πρόσβαση στο πεδίο VFCS απαιτεί την εισαγωγή ενός κωδικού με όνομα VFCS password. Τον κωδικό αυτόν έχει στην κατοχή του ο Catalog Server και όχι ο ψηφοφόρος όπως θα δούμε παρακάτω.

Catalog Server: Ο Catalog Server έχει ένα δημόσιο και ένα ιδιωτικό κλειδί που χρησιμοποιεί για την κρυπτογράφιση/υπογραφή δεδομένων όπου απαιτείται. Ακόμα έχει στην κατοχή του όλα τα δημόσια κλειδιά των έγκυρων ψηφοφόρων και το δημόσιο κλειδί του Ballot Server.

Ballot Server: Ο Ballot Server έχει και αυτός, όπως και οι άλλες δύο οντότητες, ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού για να κρυπτογραφεί και να υπογράφει τα απαραίτητα δεδομένα. Έπειτα έχει το δημόσιο κλειδί του Catalog Server ώστε να μπορεί να ελέγχει για την εγκυρότητα της υπογραφής του.

5.3 Ανάλυση διαδικασίας ψηφοφορίας

Ο χρήστης φέρνει σε κοντινή επαφή την κινητή συσκευή με το NFC tag και επιλέγει την εφαρμογή της ηλεκτρονικής ψηφοφορίας. Η εφαρμογή ξεκινάει και ζητάει απο τον ψηφοφόρο να εισάγει τον κωδικό για την πρόσβαση στο NFC tag (User password). Η εφαρμογή διαβάζει τα πεδία User ID, Upu, Cspu και χρησιμοποιεί τον κωδικό User Password για να διαβάσει το πεδίο Upr. Σε αυτό το σημείο η εφαρμογή έχει πλέον το ζεύγος κλειδιών του ψηφοφόρου αλλά και το δημόσιο κλειδί του Catalog Server και έτσι είναι δυνατό να ξεκινήσει η επικοινωνία μεταξύ τους. Για τη σύνδεση χρησιμοποιείται το πρωτόκολλο SSL με αμοιβαία αυθεντικοποίηση των οντοτήτων για να διασφαλιστεί η ασφάλεια και η ακεραιότητα της επικοινωνίας .

Όταν ολοκληρωθεί η εγκαθίδρυση της σύνδεσης, ο Catalog Server στέλνει στην εφαρμογή τον κωδικό VFCS password. Η εφαρμογή χρησιμοποιεί τον κωδικό αυτό για να έχει πρόσβαση στο πεδίο VFCS, διαβάζει τα περιεχόμενα του πεδίου και τα στέλνει στον Catalog Server. Ο Catalog Server λαμβάνει τα δεδομένα, τα αποκρυπτογραφεί και ελέγχει την ακεραιότητα τους κάνοντας χρήση του δημόσιου/ιδιωτικού κλειδιού του αντίστοιχα. Τα αποκρυπτογραφημένα δεδομένα είναι η τιμή της μεταβλητής Vote Flag CS που θα πρέπει να είναι 0 σε αυτό το στάδιο. Ο Catalog Server ελέγχει την τιμή της μεταβλητής και εάν είναι έγκυρη στέλνει στον ψηφοφόρο όλες τις ψήφους σε κρυπτογραφημένη και μη κρυπτογραφημενη μορφή. Η κρυπτογράφηση των ψήφων

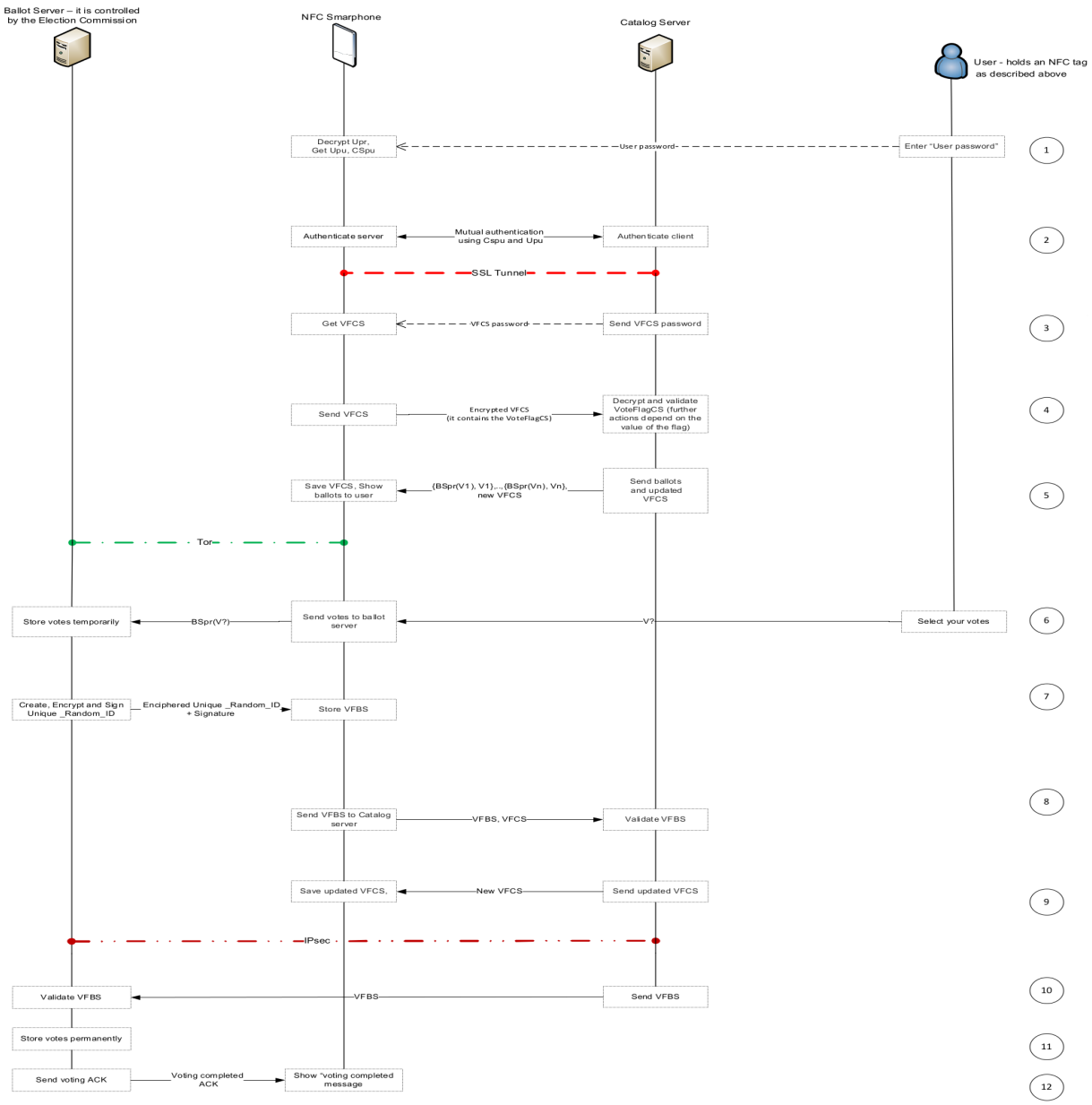
έχει γίνει με χρήση του ιδιωτικού κλειδιού του Ballot Server. Ακόμα ο Catalog Server στέλνει στην εφαρμογή τη νέα τιμή για το πεδίο VFCS, όπου δηλαδή η τιμή της μεταβλητής Vote Flag CS είναι ίση με 1. Η εφαρμογή εμφανίζει τη μη κρυπτογραφημένη μορφή των ψήφων στην οθόνη της κινητής συσκευής και αποθηκεύει στο NFC tag τη νέα τιμή του πεδίου VFCS. Όταν ο χρήστης επιλέξει την ψήφο που επιθυμεί, η εφαρμογή συνδέεται με τον Ballot Server μέσω του δικτύου TOR για να εξασφαλιστεί η ανωνυμία της επικοινωνίας. Ο Ballot Server στέλνει στην εφαρμογή ένα Captcha το οποίο και απαιτείται να λύσει ο ψηφοφόρος. Τότε εμφανίζεται η οθόνη επιβεβαίωσης της εφαρμογής που περιέχει κάποιες γενικές πληροφορίες για τον ψηφοφόρο, την επιλογή της ψήφου του, αλλά και το Captcha που καλείται να λύσει. Αφού ελέγξει την εγκυρότητα των στοιχείων και λύσει το σύστημα Captcha, ο ψηφοφόρος επιλέγει την ολοκλήρωση της διαδικασίας. Η εφαρμογή τότε στέλνει τη λύση του Captcha και εάν αυτή γίνει δεκτή, ο Ballot Server απαντά με ένα κατάλληλο μήνυμα επιβεβαίωσης.

Στη συνέχεια η εφαρμογή στέλνει στον Ballot Server την κρυπτογραφημένη μορφή της ψήφου που επέλεξε ο χρήστης. Ακολούθως ο Ballot Server δημιουργεί μία τυχαία και μοναδική τιμή για τη μεταβλητή Unique Random ID, την κρυπτογραφεί με το δημόσιο κλειδί του, την υπογράφει με το ιδιωτικό κλειδί του και στέλνει και τις δύο μορφές στην εφαρμογή. Αυτές οι δύο μορφές της μεταβλητής είναι το πεδίο VFBS που αναφέραμε παραπάνω. Την τιμή της μεταβλητής Unique Random ID ο Ballot Server την έχει “συνδέσει” με τις κρυπτογραφημένες ψήφους που έλαβε από την εφαρμογή. Κατόπιν, η εφαρμογή αποθηκεύει το πεδίο VFBS στο NFC tag και στέλνει την τιμή του στον Catalog Server. Ο Catalog Server ελέγχει την εγκυρότητα του πεδίου VFBS και εάν ο έλεγχος είναι επιτυχής στέλνει στην εφαρμογή τη νέα τιμή για το πεδίο VFCS, ορίζοντας την τιμή της μεταβλητής Vote Flag CS ίση με 2. Η εφαρμογή αποθηκεύει τότε στο NFC tag τη νέα τιμή του πεδίου VFCS. Ο Catalog Server συνδέεται με τον Ballot Server με τη χρήση του πρωτοκόλλου IPSEC για να εξασφαλιστεί η κρυπτογράφηση και η ακεραιτότητα των δεδομένων που ανταλλάσσονται και στέλνει σε αυτόν την τιμή του πεδίου VFBS. Ο Ballot Server ελέγχει την τιμή του πεδίου και εάν είναι έγκυρη αποθηκεύει μόνιμα τους κρυπτογραφημένους ψήφους που συνδέονται με την τιμή αυτή. Κατόπιν στέλνει στην εφαρμογή κατάλληλο μήνυμα επιβεβαίωσης. Τέλος η εφαρμογή εμφανίζει το μήνυμα επιβεβαίωσης στην οθόνη της κινητής συσκευής και ολοκληρώνεται η διαδικασία της ψηφοφορίας.

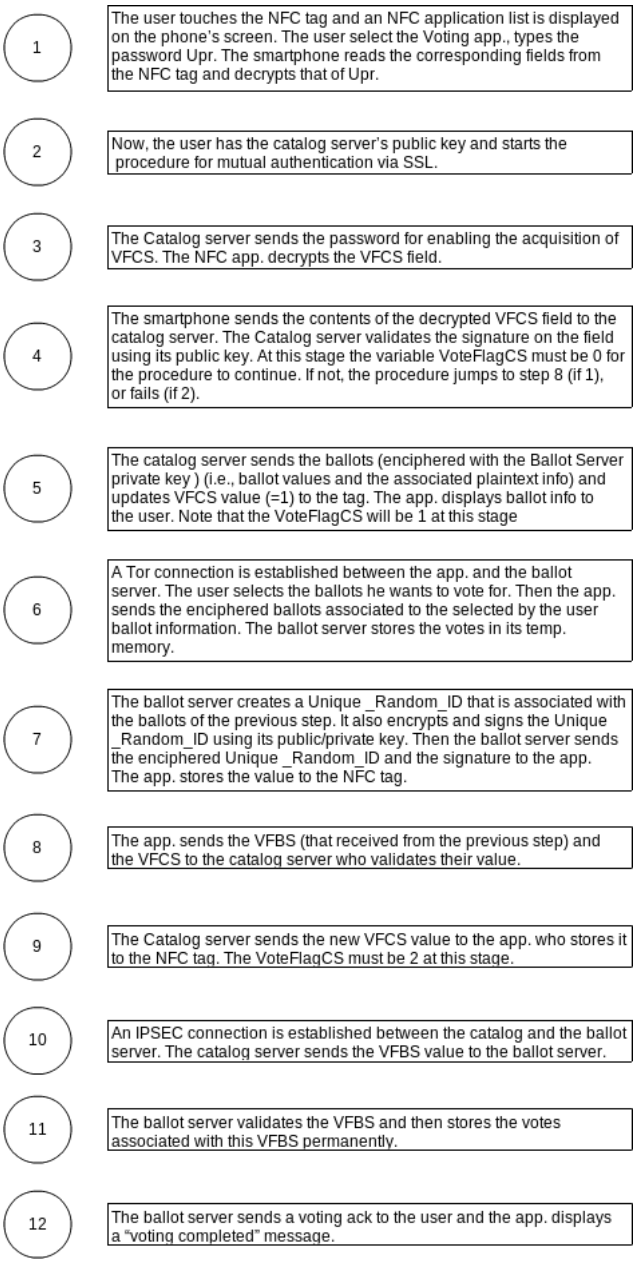
Ασφάλεια NFC Voting

Για να παρέχει τον NFC Voting την απαραίτητη ασφάλεια θεωρούμε ότι όλα τα πρωτόκολλα που χρησιμοποιήσαμε δεν είναι δυνατόν να παραβιασθούν. Ακόμα και να παραβιαστεί όμως κάποιο πρωτόκολλο δεν είναι βέβαιο ότι η ανωνυμία της ψηφοφορίας θα παραβιαστεί. Εάν για παράδειγμα παραβιαστεί η SSL σύνδεση μεταξύ της εφαρμογής και του Catalog Server, ένας επιτιθέμενος τα μοναδικά δεδομένα που θα μπορέσει να λάβει σε μη κρυπτογραφημένη μορφή είναι το VFCS password και η μη κρυπτογραφημένη μορφή των ψήφων. Η κατοχή των δεδομένων αυτών δεν παραβιάζει την ιδιωτικότητα της διαδικασίας. Εάν κάποιος παραβιάσει τη σύνδεση της εφαρμογής με τον Catalog Server και τη σύνδεση του Catalog Server με τον Ballot Server είναι πιθανόν να μπορεί να παραβιάσει την ανωνυμία της ψηφοφορίας καθώς θα μπορεί να συνδυάσει την κρυπτογραφημένη μορφή της ψήφου με τις πληροφορίες όλων των ψήφων που έστειλε ο Catalog Server στην εφαρμογή. Ακόμα θεωρούμε ότι το κινητό τηλέφωνο είναι ασφαλές καθώς πιθανή παρεμβολή στη λειτουργία της εφαρμογής θα μπορούσε να παραβιάσει τόσο την ιδιωτικότητα όσο και την ασφάλεια της διαδικασίας.

Στο σχήμα 5.1 μπορούμε να δούμε σε μορφή διαγράμματος τη διαδικασία της ψηφοφορία και στο σχήμα 5.2 εμφανίζονται τα βήματα με αναλυτική περιγραφή.



Σχήμα 5.1: Σχήμα NFC Voting



Σχήμα 5.2: Βήματα NFC Voting

5.4 Πρωτότυπο NFC Voting

Για να δοκιμάσουμε τη λειτουργία του NFC Voting στην πράξη υλοποιήσαμε το πρωτόκολλο αυτό χρησιμοποιώντας ένα σύνολο από διαθέσιμες τεχνολογίες. Παρακάτω θα δούμε αναλυτικά το περιβάλλον στο οποίο έγινε η υλοποίηση αλλά και τα αποτελέσματα της δοκιμής αυτής.

5.4.1 Περιβάλλον υλοποίησης

NFC Tag

Το NFC tag που επιλέξαμε να χρησιμοποιήσουμε για την υλοποίηση μας είναι το Mifare DesFire EV1 της NXP. Τα tags αυτού του είδους παρέχουν τη δυνατότητα δημιουργίας πολλών εφαρμογών. Αυτό μας δίνει τη δυνατότητα να έχουμε έλεγχο πρόσβασης στα αρχεία της κάθε εφαρμογής ξεχωριστά. Ακόμα, η σειρά Mifare DesFire υποστηρίζει την κρυπτογραφημένη επικοινωνία και την εξασφάλιση της ακεραιότητας των δεδομένων που ανταλλάσσονται με το NFC. Τέλος τα NFC tags του είδους αυτού παρέχουν ιδιαίτερα μεγάλες χωρητικότητες αποθήκευσης δεδομένων που φτάνουν τα 8 KB. Το NFC της δοκιμής μας είχε χωρητικότητα 4 KB.

Catalog Server

Ο Catalog Server υλοποιήθηκε με χρήση της γλώσσας προγραμματισμού Java. Για την SSL επικοινωνία με την εφαρμογή χρησιμοποιήθηκε η κλάση SSLSocket τροποποιημένη έτσι ώστε να απαιτεί την αμοιβαία αυθεντικοποίηση. Η επικοινωνία IPSEC με τον Ballot Server ρυθμίστηκε από το λειτουργικό σύστημα στο οποίο εκτελέστηκε ο Catalog Server. Το λειτουργικό σύστημα της δοκιμής μας είναι τα Windows Server 2012.

Ballot Server

Ο Ballot Server υλοποιήθηκε και αυτός με χρήση της γλώσσας προγραμματισμού Java. Η επικοινωνία με την εφαρμογή έγινε με την κλάση Socket και η IPSEC επικοινωνία με τον Catalog Server έγινε με τις κατάλληλες ρυθμίσεις στο λειτουργικό σύστημα. Το λειτουργικό σύστημα για τη δοκιμή μας είναι και πάλι τα Windows Server 2012.

Δημόσια και ιδιωτικά κλειδιά

Όλα τα δημόσια και ιδιωτικά κλειδιά που χρησιμοποιήσαμε είναι τύπου X509 και δημιουργήθηκαν με το εργαλείο Openssl. Για τη δοκιμή μας έχουμε δημιουργήσει κλειδιά μεγέθους 1024 bytes λόγο της χωρητικότητας των 4 Kb του NFC tag που χρησιμοποιήσαμε. Εάν χρησιμοποιούσαμε μεγαλύτερο σε χωρητικότητα NFC tag θα μπορούσαμε να αποθηκεύσουμε σε αυτό κλειδιά με μεγαλύτερο μέγεθος.

Εφαρμογή NFC Voting

Η εφαρμογή για την ηλεκτρονική ψηφοφορία υλοποιήθηκε στην πλατφόρμα Android και στοχεύει λειτουργικά έκδοσης 4.0.4 ή νεότερα. Για την επικοινωνία με το NFC tag δεν χρησιμοποιήθηκε η πλέον διαδεδομένη μορφή δεδομένων NDEF. Αντ'αυτού, τα δεδομένα στο NFC tag αποθηκεύονται σε αρχεία που περιέχουν bytes. Για τη διαχείριση της επικοινωνίας με το NFC tag χρησιμοποιήθηκε η κλάση IsoDep που παρέχει το Android API. Η SSL επικοινωνία με τον Catalog Server έγινε με τη χρήση του SSLSocket τροποποιημένη κατάλληλα για να αυθεντικοποιείται και η εφαρμογή. Για την TOR επικοινωνία με τον Ballot Server χρησιμοποιήθηκε ο επίσημος proxy του δικτύου TOR για το Android που ονομάζεται `https://guardianproject.info/apps/orbot/`Orbot. Η εφαρμογή ελέγχει εάν ο proxy αυτός είναι εγκατεστημένος πριν την εκκίνηση της και εάν δεν είναι εμφανίζει κατάλληλο μήνυμα λάθους στο χρήστη.

Εφαρμογή Init Tag

Στο NFC Voting η αρχή διεξαγωγής των εκλογών πρέπει να αρχικοποιήσει το NFC tag του κάθε ψηφοφόρου. Την αρχικοποίηση αυτήν εμείς την υλοποιήσαμε με μία ακόμα εφαρμογή για την πλατφόρμα Android που στοχεύει λειτουργικά έκδοσης 4.0.4 ή νεότερα. Στο πρωτότυπο μας η εφαρμογή αυτή δεν έχει κάποια είσοδο από το χρήστη και εμφανίζει μόνο δεδομένα χρήσιμα για τη διόρθωση σφαλμάτων. Για να αλλάξει η λειτουργία της εφαρμογής θα πρέπει να τροποποιηθεί ο πηγαίος κώδικας της και να εκτελεστεί εκ νέου.

Κινητή Συσκευή

Η κινητή συσκευή της δοκιμής μας ήταν το κινητό τηλέφωνο Vega LTE M της εταιρίας SKY.

5.4.2 Δείγματα κώδικα

Στην ενότητα αυτή θα δούμε μερικά δείγματα κώδικα, περιγράφοντας συνοπτικά τη λειτουργία τους.

```
01.  public static void initConnection() throws Exception {
02.      Socks5Proxy proxy = new Socks5Proxy(socksServerIP, socksServerPort);
03.      SocksSocket sock = new SocksSocket(proxy, ballotServerIP, ballotServerPort);
04.      sock.connect(new InetSocketAddress(ballotServerIP, ballotServerPort));
05.      ObjectOutputStream out = new ObjectOutputStream(sock.getOutputStream());
06.      ObjectInputStream in = new ObjectInputStream(sock.getInputStream());
07.
08.  }
```

Σχήμα 5.3: Κώδικας - Σύνδεση με TOR proxy

Για τη σύνδεση με το TOR χρησιμοποιούμε τις κλάσεις Socks5Proxy και SocksSocket που υπάρχουν στην βιβλιοθήκη Java SOCKS Proxy όπως φαίνεται στο σχήμα 5.3. Η μεταβλητή socksServerIP περιέχει τη διεύθυνση IP ενώ η μεταβλητή socksServerPort περιέχει την πόρτα στις οποίες δέχεται συνδέσεις ο διακομιστής proxy που χρησιμοποιούμε για τη σύνδεση με το δίκτυο TOR.

```
01.          OrbotHelper orbotH = new OrbotHelper(this);
02.          if (!orbotH.isOrbotInstalled()) {
03.              Toast.makeText(getApplicationContext(), "You must install Orbot to"
04.                              + "use this app!Exiting...",Toast.LENGTH_LONG).show();
05.              finish();
06.          } else if (!orbotH.isOrbotRunning()) {
07.              Toast.makeText(getApplicationContext(), "You must run Orbot before"
08.                              + "using this app!Exiting...",Toast.LENGTH_LONG).show();
09.              finish();
10.          }
```

Σχήμα 5.4: Κώδικας - Έλεγχος για TOR proxy

Το αντικείμενο orbotH που ανήκει στην κλάση OrbotHelper και έχουμε εισάγει από την βιβλιοθήκη OnionKit, μας βοηθάει να ελέγξουμε εάν ο Orbot proxy είναι εγκατεστημένος στη συσκευή αλλά και εάν βρίσκεται σε λειτουργία. Στο σχήμα 5.4, στη γραμμή 2 γίνεται ο έλεγχος για την ύπαρξη του Orbot proxy και στη γραμμή 6 ελέγχεται εάν αυτός εκτελείται.

```java
public static byte[] wrapMessage(byte command, byte[] parameters)
throws Exception {
    ByteArrayOutputStream stream = new ByteArrayOutputStream();

    stream.write((byte) 0x90);
    stream.write(command);
    stream.write((byte) 0x00);
    stream.write((byte) 0x00);
    if (parameters != null) {
        stream.write((byte) parameters.length);
        stream.write(parameters);
    }

    stream.write((byte) 0x00);
    return stream.toByteArray();
}
```

Σχήμα 5.5: Κώδικας - Ενθυλάκωση εντολής για αποστολή στο DesFire NFC tag

Οι εντολές που στέλνουμε στο DesFire NFC tag ενθυλακώνονται με βάση το ISO7816-4 [1] για να δημιουργηθούν έτσι τα κατάλληλα APDUs. Η διαδικασία της ενθυλάκωσης γίνεται με τη συνάρτηση wrapMessage που περιγράφεται στο σχήμα 5.5.

```java
public byte[] createStdDataFile(byte fileNo, byte comSet,
    byte[] accessRights, byte[] fileSize) throws Exception {

    byte[] command;
    byte[] result;
    command = ArraysManipulation.concatArrays(new byte[] {(byte) fileNo},
                                              new byte[] {(byte) comSet});
    command = ArraysManipulation.concatArrays(command, accessRights);
    command = ArraysManipulation.concatArrays(command, fileSize);

    command = wrapMessage((byte) 0xCD, command);
    result = desFire.transceive(command);
    return result;
}
```

Σχήμα 5.6: Κώδικας - Εγγραφή αρχείου στο DesFire NFC tag

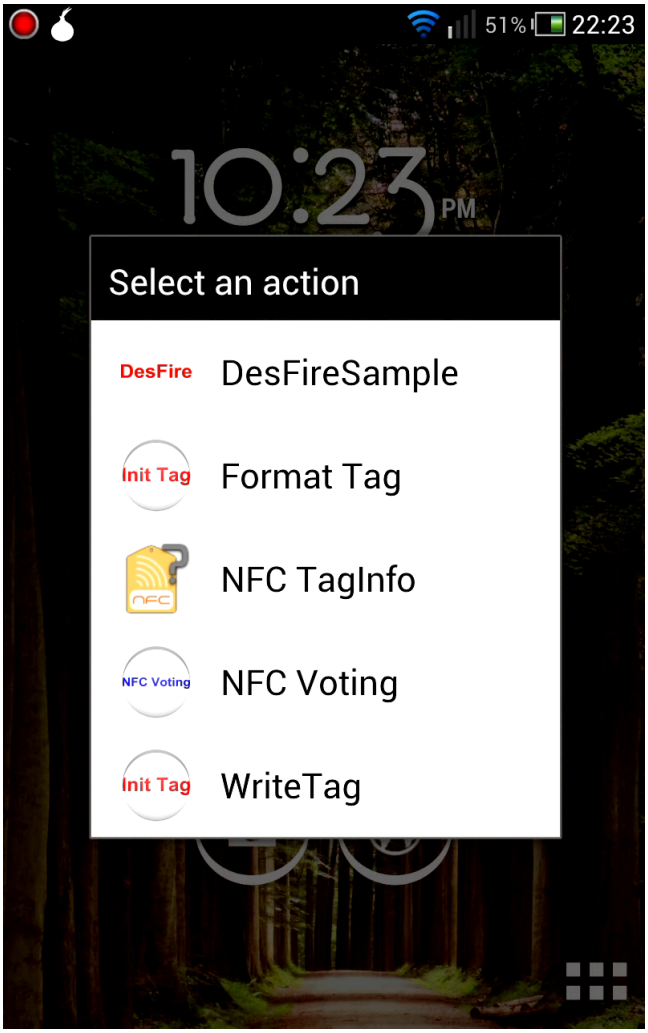
Η συνάρτηση createStdDataFile που εμφανίζεται στο σχήμα 5.6 είναι υπεύθυνη για τη δημιουργία ενός αρχείου στο DesFire NFC tag. Η συνάρτηση concatArrays της κλάσης ArraysManipulation ενώνει τους δύο πίνακες από bytes που δέχεται ως είσοδο. Για την επικοινωνία με το DesFire NFC tag χρησιμοποιούμε το αντικείμενο desFire της κλάσης IsoDep του Android API. Αφού ενθυλακωθεί στα κατάλληλα APDUs με τη

συνάρτηση wrapMessage, η κάθε εντολή στέλνεται στο DesFire NFC tag με τη συνάρτηση transceive της κλάσης IsoDep.

5.4.3 Δοκιμές πρωτοτύπου

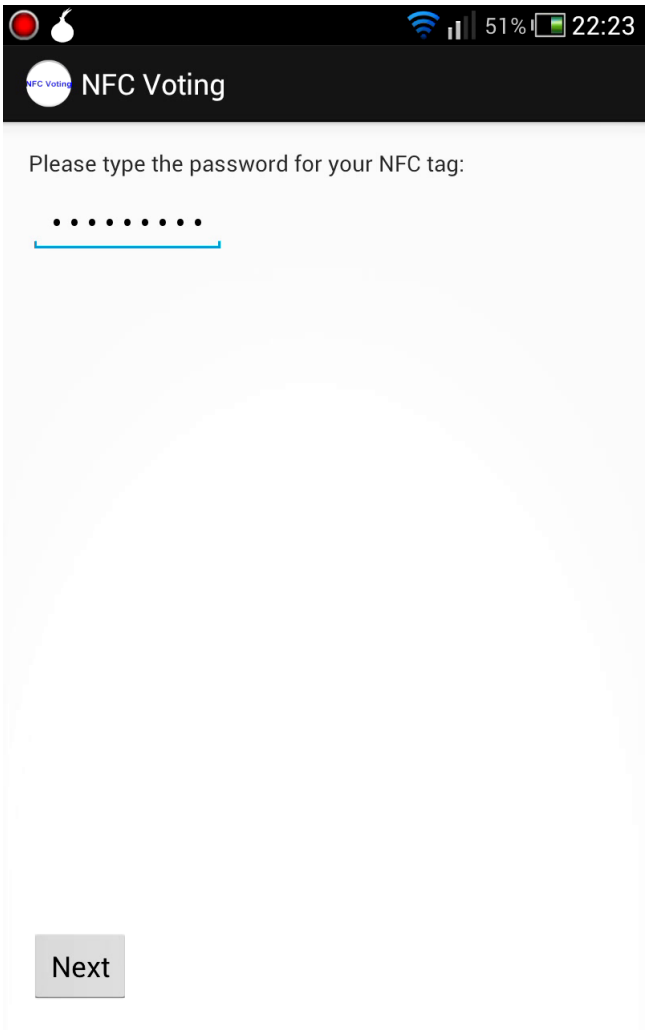
Παρακάτω θα δούμε την εκτέλεση του πρωτοτύπου που δημιουργήσαμε. Έχουμε προσθέσει τα στιγμιότυπα από την εφαρμογή της ηλεκτρονικής ψηφοφορίας, από τους διακομιστές, αλλά και από το πρόγραμμα Wireshark για την ανάλυση της εκάστοτε επικοινωνίας .

Αρχικά φέρνουμε σε κοντινή επαφή το κινητό τηλέφωνο με το NFC tag και το Android εμφανίζει τη λίστα με τις εφαρμογές που μπορούν να διαχειριστούν το tag αυτό, όπως φαίνεται στο σχήμα 5.7.



Σχήμα 5.7: Οθόνη επιλογής εφαρμογής

Στη συνέχεια εμφανίζεται στο σχήμα 5.8 η πρώτη οθόνη της εφαρμογής όπου ο χρήστης εισάγει τον κωδικό User Password.



Σχήμα 5.8: Οθόνη εισαγωγής User Password

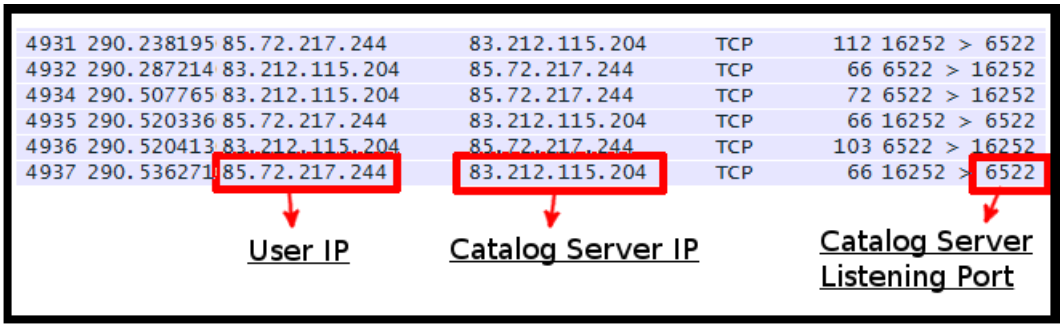
Όταν επιλέξει συνέχεια, η εφαρμογή συνδέεται με τον Catalog Server και κάνει όλες τις εργασίες που απαιτείται από το πρωτόκολλο. Τα μηνύματα που εμφανίζει ο Catalog Server σε αυτό το στάδιο παρουσιάζονται στο σχήμα 5.9.

```
----Catalog server started----
TLS connection Started with:
CN=Client, O=University of Aegean, ST=North Aegean, C=GR

VFCS password sent!
VFCS field recieved!
VFCS Decrypted!
VFCS verified!
VFCS value correct! (Phase 0)
Ballots sent to user!
VFCS sent to user!
```

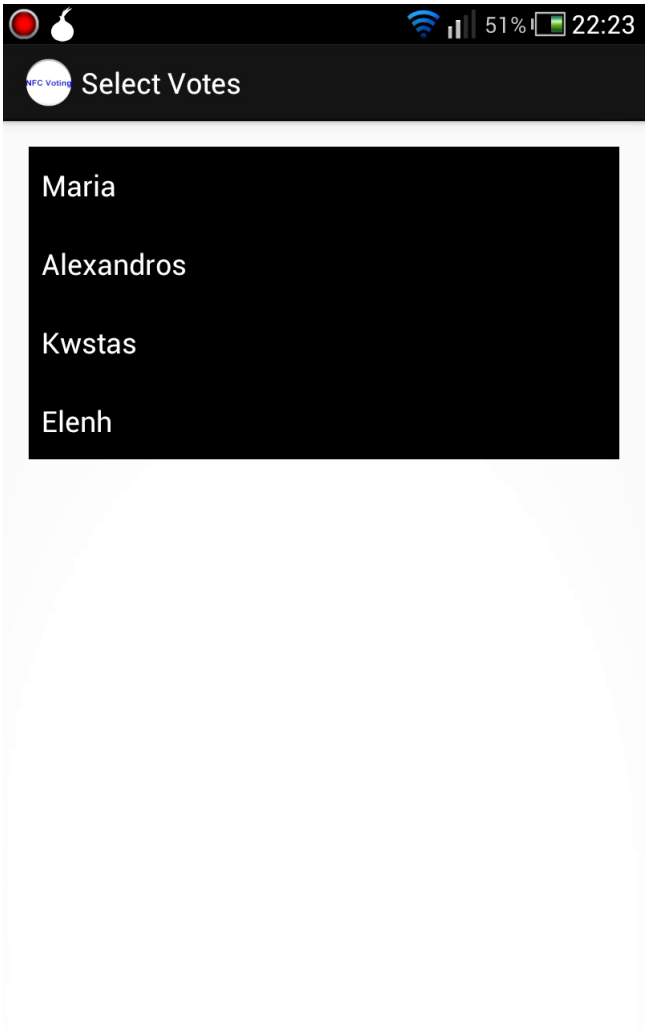
Σχήμα 5.9: Μηνύματα Catalog Server 1/2

Με τη χρήση του προγράμματος Wirehshark βλέπουμε στο σχήμα 5.10 τα στοιχεία της σύνδεσης του Catalog Server με την εφαρμογή της ηλεκτρονικής ψηφοφορίας.



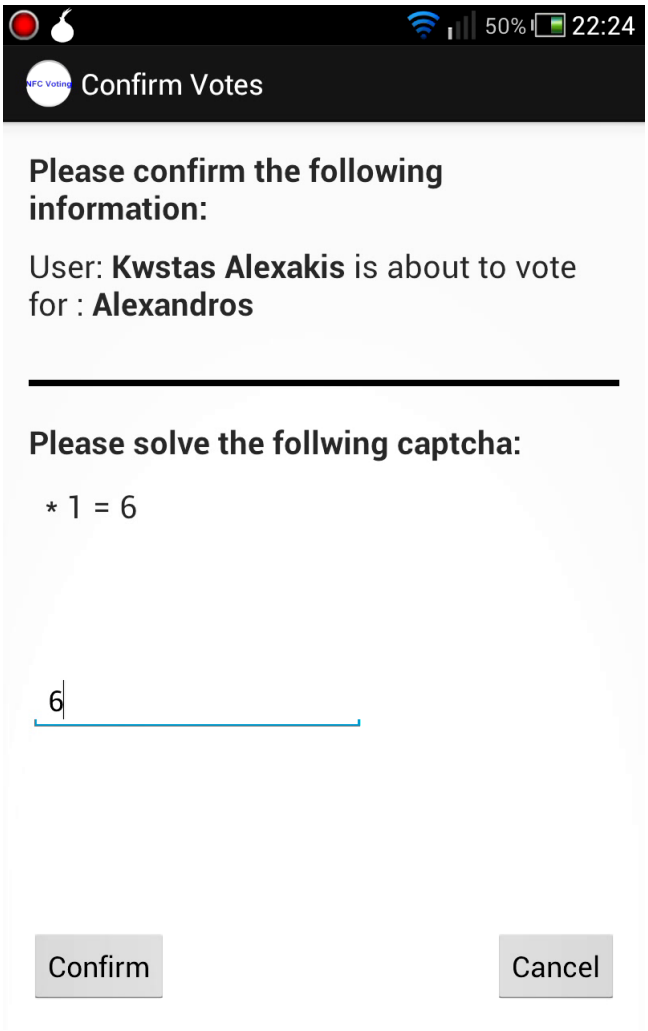
Σχήμα 5.10: Κίνηση Catalog Server - Εφαρμογής

Στη συνέχεια ο Catalog Server στέλνει στην εφαρμογή τις διαθέσιμες ψήφους. Η εφαρμογή τότε εμφανίζει μία λίστα που περιέχει τις επιλογές των ψήφων όπως φαίνεται στο σχήμα 5.11.



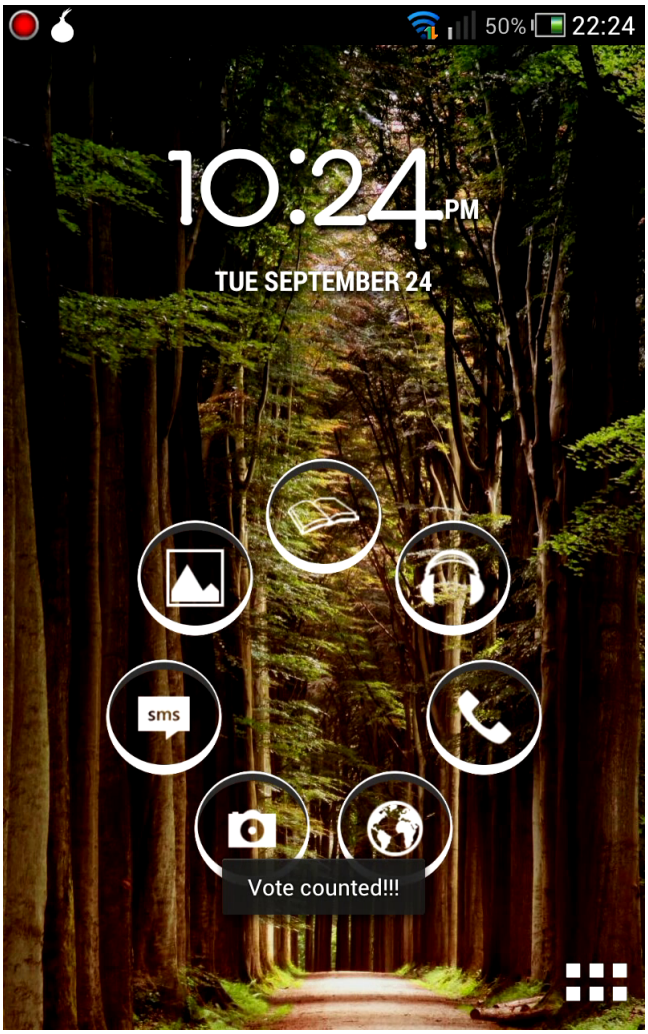
Σχήμα 5.11: Οθόνη επιλογής ψήφων

Όταν ο χρήστης επιλέξει την ψήφο που επιθυμεί η οθόνη επιβεβαίωσης εμφανίζεται στην εφαρμογή όπως φαίνεται στο σχήμα 5.12.



Σχήμα 5.12: Οθόνη επιβεβαίωσης ψήφων

Αφού λύσει το Captcha ο χρήστης μπορεί να επιλέξει την επιβεβαίωση των επιλογών του και εάν δεν υπάρχει κάποιο σφάλμα, η εφαρμογή της ηλεκτρονικής ψηφοφορίας θα εμφανίσει κατάλληλο μήνυμα όπως βλέπουμε στο σχήμα 5.13 και θα τερματίσει τη λειτουργία της.



Σχήμα 5.13: Οθόνη ολοκλήρωσης ψηφοφορίας

Τα μηνύματα που εμφανίζονται στον Catalog Server μετά την επιβεβαίωση των επιλογών αναλύονται στο σχήμα 5.14.

```
VFCS field recieved!
Got VFBS from user!
VFCS Decrypted!
VFCS verified!
VFCS value correct! (Phase 1)
VFBS verified!
VFCS sent to user!
User connection closed!
VFBS sent to ballot!
Voting procedure ended!
```

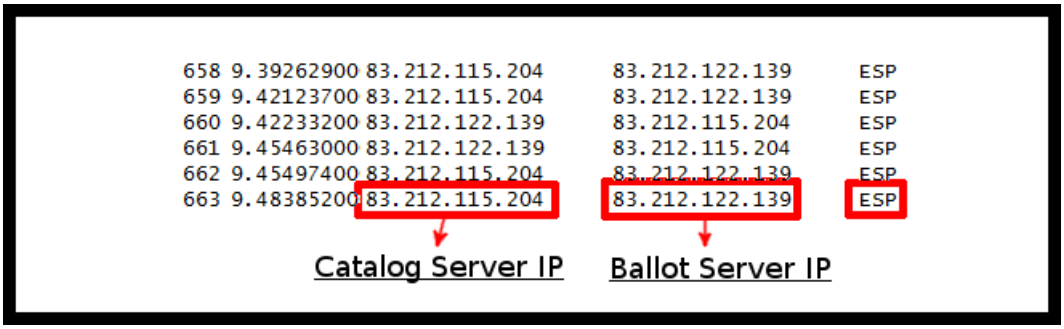
Σχήμα 5.14: Μηνύματα Catalog Server 2/2

Τέλος τα μηνύματα που εμφανίζονται στον Ballot Server κατά τη διάρκεια του σταδίου της επιβεβαίωσης και μέχρι την ολοκλήρωση της διαδικασίας παρουσιάζονται στο σχήμα 5.15.

```
----Ballot server started----
Waiting User...
Waiting Catalog Server...
User connected!
Captsa solved!
Ballots recieved!
VFBS sent to user!
Catalog connected!
VFBS from catalog server recieved!
VFBS verified!
Ballot stored!
```

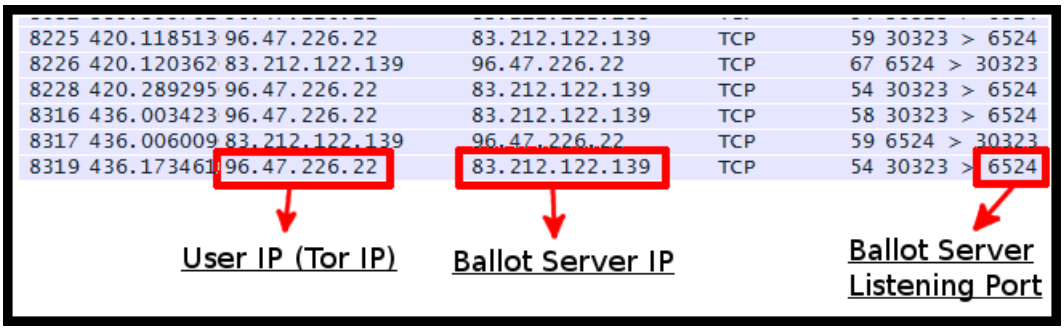
Σχήμα 5.15: Μηνύματα Ballot Server

Η επικοινωνία μεταξύ του Ballot Server και του Catalog Server γίνεται με το πρωτόκολλο IPSEC, για το λόγο αυτό υπάρχει η κεφαλίδα ESP στην ανάλυση της κίνησης τους απο το πρόγραμμα Wireshark όπως φαίνεται στο σχήμα 5.16.



Σχήμα 5.16: Κίνηση Ballot Server - Catalog Server

Στο σχήμα 5.17 παρουσιάζουμε την κίνηση του Ballot Server με την εφαρμογή του NFC Voting . Αξίζει να σημειωθεί ότι η διεύθυνση IP του χρήστη είναι **96.47.226.22** , είναι δηλαδή διαφορετική από τη διεύθυνση IP που είχε όταν συνδέθηκε στον Catalog Server, την οποία είδαμε στο σχήμα 5.10 και ήταν **85.72.217.244**. Ελέγξαμε τη διεύθυνση 96.47.226.22 και επιβεβαιώσαμε ότι αυτή ανήκει σε ένα TOR Node κάτι που μας επιβεβαίωσε την επιτυχή χρήση του πρωτοκόλλου TOR απο την εφαρμογή.



Σχήμα 5.17: Κίνηση Ballot Server - Εφαρμογής

Κεφάλαιο 6

Επίλογος - Μελλοντική εργασία

Έχουν προταθεί πολλά συστήματα ηλεκτρονικής ψηφοφορίας που χρησιμοποιούν πληθώρα τεχνολογιών για την υλοποίηση τους. Εμείς επιλέξαμε να δημιουργήσουμε ένα σύστημα ηλεκτρονικής ψηφοφορίας χρησιμοποιώντας την τεχνολογία του NFC. Σχεδιάσαμε ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας υιοθετώντας τεχνολογίες ιδιαίτερα διαδεδομένες όπως είναι η κρυπτογράφιση με κλειδιά τύπου X509. Φροντίσαμε ακόμα το σύστημα μας να είναι απλό στη χρήση για τον ψήφοφόρο αλλά και εύκολο στην υλοποίηση για το διοργανωτή των εκλογών. Επιπλέον, δημιουργήσαμε ένα πρωτότυπο για το σύστημα μας για να δοκιμάσουμε τη λειτουργία του. Σε επόμενα στάδια της εργασίας αυτής θέλουμε να βελτιώσουμε το πρωτότυπο που δημιουργήσαμε για να υποστηρίζει μεγαλύτερο αριθμό χρηστών. Επίσης, θα θέλαμε να οργανώσουμε δοκιμαστικές εκλογικές διαδικασίες για να ελέγξουμε και να διορθώσουμε όποια προβλήματα μπορεί να προκύψουν κατά την εκτέλεση του συστήματος. Τέλος έχουμε στόχο να κάνουμε μια επιπλέον μελέτη για την ασφάλεια του συστήματος κατά τη διάρκεια των δοκιμαστικών εκλογών.

Βιβλιογραφία

[1] ISO/IEC 7816-4:2013, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54550.

[2] NFC Forum Technical Specifications. http://www.nfc-forum.org/specs/spec_list/.

[3] NFC Research Lab Hagenberg: Devices. http://www.nfc-research.at/index.php?id=45.

[4] Ø yvind Berget. Investigation of security features in Near-field communication. https://www.duo.uio.no/handle/10852/9990, 2008.

[5] VA Bhole, RR More, and NC Khadke. Security In Near Field Communication(NFC) Strengths And Weaknesses. 2007.

[6] Jurlind Budurushi, Stephan Neumann, Maina M Olembo, and Melanie Volkamer. Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme. In *ARES Conference : The Eight International Conference on Availability, Reliability and Security*, 2013.

[7] Stefano Campanelli, Alessandro Falleni, Fabio Martinelli, Marinella Petrocchi, and Anna Vaccarelli. Mobile Implementation and Formal Verification of an e-Voting System. In *2008 Third International Conference on Internet and Web Applications and Services*, pages 476–481. IEEE, 2008.

[8] Ann Cavoukian. Mobile Near Field Communications (NFC) " Tap 'n Go " Keep it Secure & Private. http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1136, 2011.

[9] Benninger Corey and Max Sobell. Shmoocon 2012: Intro to Near Field Communication (NFC) Mobile Security. http://www.shmoocon.org/2012/videos/BenningerSobell-IntroToNearFieldComm.m4v.

[10] L.F. Cranor and R.K. Cytron. Sensus: a security-conscious electronic polling system for the Internet. In *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, volume 3, pages 561–570. IEEE Comput. Soc. Press, 1997.

[11] David Derler, Klaus Potzmader, Johannes Winter, and Kurt Dietrich. Anonymous Ticketing for NFC-Enabled Mobile Phones. In *Third International Conference, INTRUST 2011*, 2011.

[12] Lishoy Francis, Gerhard Hancke, Keith Mayes, Konstantinos Markantonakis, Egham Hill, United Kingdom, Email L Francis, and K Markantonakis. Potential Misuse of NFC Enabled Mobile Phones with Embedded Security Elements as Contactless Attack Platforms. In *ICITST'09*, pages 1–8. 2009.

[13] Lishoy Francis, Gerhard Hancke, Keith Mayes, Konstantinos Markantonakis, Egham Hill, United Kingdom, and K Markantonakis. Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones. 2011.

[14] John Turner Jordi Barrat i Esteve, Ben Goldsmith. International Experience with E-Voting - Norwegian E-Vote Project. http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf, 2012.

[15] Gerald Madlmayr, Peter Kleebauer, Josef Langer, and Josef Scharinger. Secure Communication between Web Browsers and NFC Targets by the Example of an e-Ticketing System. http://link.springer.com/chapter/10.1007%2F978-3-540-85717-4_1, 2008.

[16] Roland Michael. Software Card Emulation in NFC-enabled Mobile Phones : Great Advantage or Security Nightmare ?, 2012.

[17] David M. Monteiro, Joel J. P. C. Rodrigues, and Jaime Lloret. A secure NFC application for credit transfer among mobile phones. In *2012 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pages 1–5. IEEE, 2012.

[18] Elenh Mpourliou and Myrto Tafyli. Arts & Crafts Voting Machine - Fax Machine. http://extev.syros.aegean.gr/bsc/1250s1.pdf.

[19] Michael I. Shamos. Electronic Voting. http://triton.towson.edu/~swartout/cosc321/electronic_voting.pdf, 2004.

[20] M. Furnell Steven, Sokratis Katsikas, Javier Lopez, and Ahmed Patel. Securing Information and Communications Systems: Principles, Technologies and Applications. chapter 15, page 362. 2008.

Ακρωνύμια

NFC Near Field Communication

RFID Radio-frequency identification

NDEF NFC Data Exchange Format

LLCP Logical Link Control Protocol

DRE Direct Recording Electronic System

PKI Public Key Infrastructure

GPS Global Positioning System

SSL Secure Sockets Layer

IPSEC Internet Protocol Security

TOR The Onion Router

SIM Subscriber Identity Module

MMC MultiMediaCard

SD Secure Digital

CPU Central Processing Unit

API Application Programming Interface

APDU Application Protocol Data Unit

Captcha Completely Automated Public Turing test to tell Computers and Humans Apart

Γλωσσάρι

Έξυπνη κάρτα Ένα είδος κάρτας που περιέχει μικροεπεξεργαστή και επιτρέπει την εκτέλεση εφαρμογών.

Τυφλές υπογραφές Με τις τυφλές υπογραφές επιτρέπεται σε μια οντότητα να υπογράψει δεδομένα χωρίς να μάθει το περιεχόμενο τους.

Eavesdropping Η παράνομη παρακολούθηση των δεδομένων που ανταλλάσσονται απο μία νόμιμη συναλλαγή.

Man-in-the-middle Ένα είδος επίθεσης όπου ο επιτιθέμενος παρεμβένει σε μία νόμιμη επικοινωνία δύο οντοτήτων στέλνοντας ο ίδιος μυνήματα σε κάποια οντότητα, παραποιώντας τα έτσι ώστε να φαίνεται ότι προέρχονται απο μία νόμιμη οντότητα.

Selective disclosure Μία μέθοδος που επιτρέπει την υπογραφή δεδομένων από μια οντότητα γνωρίζοντας μόνο μέρος του περιεχομένου τους.

Code voting Μία μέθοδος ψηφοφορίας όπου η κάθε ψήφος συνδέεται με έναν κωδικό, αυτόν τον κωδικό καταχωρεί ο ψηφοφόρος κατά τη διάρκεια της ψηφοφορίας.

Βασιλάκης Γεώργιος

Βιογραφικό Σημείωμα

Προσωπικές πληροφορίες

Ημερομηνία γέννησης	31/01/1990
Πόλη γέννησης	Ηράκλειο Κρήτης
Mail	icsd07009@icsd.aegean.gr

Μόρφωση

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων 2007-2013

Πανεπιστήμιο Αιγαίου, Σχολή θετικών επιστημών

Επαγγελματική Εμπειρία

Web Developer 2011

Cj-Web,Πρακτική άσκηση

Δημιουργία και διαχείριση ιστοσελίδων με χρήση αυτοματοποιημένων εργαλείων. Διαδικτυακός προγραμματισμός για την εξατομίκευση λειτουργιών.

Συνέδρια και Επιμορφωτικά Σεμινάρια

Ηλεκτρονικό επιχειρείν και ηλεκτρονική διακυβέρνηση:Πεδία επιχειρηματικότητας για νέους επιστήμονες πληροφορικής, 3ο Επιστημονικό Συμπόσιο

(Μάιος 2011, Αίθουσα εκδηλώσεων Νέου Καρλοβάσου, Σάμος)

OWASP AppSec Research 2012

(Ιούλιος 2012, Τμήμα Πληροφορικής και Τηλεπικοινωνιών , Αθήνα)

OWASP AppSec University Challenge 2012

(Ιούλιος 2012, Τμήμα Πληροφορικής και Τηλεπικοινωνιών , Αθήνα)

Ατομικές δεξιότητες

Γλώσσες προγραμματισμού:	Java, Php, Html, Css, Javascript, C++, C, Prolog, SQL, Bash
Πακέτα Λογισμικού:	Word, Excel, PowerPoint, Netbeans, Eclipse, Nmap, VirtualBox
Λειτουργικά Συστήματα:	Windows, Linux
Γλώσσες:	Ελληνική (Μητρική) Αγγλική (Καλά)