Ιονιο Πανεπιστημιο
Σχολη Επιστημης της Πληροφοριας και Πληροφορικης
Τμημα Πληροφορικης

Ανέπαφες Τραπεζικές Συναλλαγές μέσω Κινητών Συσκευών

10 Ιουνίου 2019

Συγγραφέας: Γιάννης Κωβαίος

Επιβλέπων: Εμμανουήλ Β. Μάγκος

Περιεχόμενα

Περίληψη

Τα τελευταία χρόνια στην παγκόσμια οικονομική κοινότητα έχουν αρχίσει και εμφανίζονται συστήματα ανέπαφων συναλλαγών, τα οποία εκμεταλλεύονται τις δυνατότητες και την χρηστικότητα των κινητών συσκευών. Η κινητή συσκευή αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας του χρήστη οπότε η ικανότητα διεκπεραίωσης ανέπαφων πληρωμών μέσω της κινητής συσκευής αποτελεί την φυσική εξέλιξη του τραπεζικού συστήματος. Οι κινητές συσκευές όπως και οι ανέπαφες κάρτες κάνουν χρήση της τεχνολογίας Near Field Communication (NFC) για την εδραίωση και την εκτέλεση συναλλαγών μέσω του τραπεζικού δικτύου με ενδιάμεσο συστατικό στοιχείο το τερματικό πληρωμής.

Όσο η μετάβαση από τις πλαστικές κάρτες προς τις κινητές συσκευές γίνεται όλο και περισσότερο αποδεκτή από τους χρήστες γεννιούνται ερωτηματικά για το ποσοστό ασφάλειας που διακατέχουν αυτά τα συστήματα και το ποσοστό ασφάλειας που παρέχεται στον τελικό χρήστη και στα δεδομένα του.

Στην παρούσα πτυχιακή εργασία αναλύεται και εξηγείται η αρχιτεκτονική του συστήματος πληρωμής, τα επιμέρους στοιχεία και οι μέθοδοι που χρησιμοποιούνται για την ενίσχυση του επίπεδου ασφάλειας. Επιπρόσθετα, επεξηγούνται και αναλύονται οι πιθανές επιθέσεις προς την κινητή συσκευή καθώς και πιθανά αντίμετρα απέναντι σε αυτές. Τέλος, γίνονται τρεις (3) μελέτες περίπτωσης στις διασημότερες εφαρμογές διεκπεραίωσης ανέπαφων συναλλαγών καθώς και πιθανές ευπάθειες τους.

Λέξεις κλειδιά: Μικροτσίπ, ανέπαφες συναλλαγές, κινητή συσκευή, NFC, EMV, Tokenization, ηλεκτρονικά πορτοφόλια.

1 Εισαγωγή

Τα τελευταία χρόνια, τόσο στην ελληνική όσο και στην παγκόσμια πραγματικότητα, έχουν αρχίσει να εμφανίζονται και να εδραιώνονται συστήματα, τα οποία εκμεταλλεύονται τεχνολογίες ανέπαφης διάδρασης. Τα συστήματα αυτά κατά κόρον είναι βασισμένα στην τεχνολογία που διέπουν τα μικροτσίπ RFID. Τέτοιου είδους συστήματα διακατέχονται από την μοναδική ικανότητα αφαίρεσης της φυσικής σύνδεσης μεταξύ των συσκευών που θέλουν να επικοινωνήσουν (Michael, 2012).

Με την γέννηση της τεχνολογίας ανέπαφης σύνδεσης, δημιουργήθηκε η ανάγκη ένταξης των συστημάτων αυτών στον τραπεζικό τομέα, τόσο για την αποδοτικότερη όσο και για την ταχύτερη διεκπεραίωση τραπεζικών συναλλαγών, με κυριότερο σκοπό την εξάλειψη του φυσικού χρήματος. Καθώς, τα συστήματα αυτά ωρίμαζαν στα τραπεζικά οικοσυστήματα της Ευρώπης και της Αμερικής, οι ανέπαφες συναλλαγές έκαναν το επόμενο βήμα στην εξέλιξη τους και μεταπήδησαν από τις πλαστικές κάρτες, σε μια συσκευή που χρησιμοποιείται καθημερινά από ένα μεγάλο ποσοστό του παγκόσμιου πληθυσμού, το κινητό τηλέφωνο (Bocek et al, 2016).

Οι κινητές συσκευές με ικανότητες διασύνδεσης μέσω NFC πρωτοκόλλου, και χάρη στην διαφοροποίηση που διεξάχθηκε στο πρωτόκολλο του EMV, έχουν πλέον την ικανότητα διεκπεραίωσης ανέπαφων συναλλαγών με την ίδια ευκολία και αποδοτικότητα με αυτή των πλαστικών καρτών. Σε αντιστοιχία με την ευρεία αποδοχή των τεχνολογιών αυτών από τον παγκόσμιο πληθυσμό, άρχισαν να δημιουργούνται ερωτήματα για το ποσοστό ασφάλειας που διακατέχουν οι τεχνολογίες αυτές (Akinyokun and Teague, 2017).

Τα ερωτήματα που απασχολούν όχι μόνο τους ερευνητές και επιστήμονες της ασφάλειας των πληροφοριών αλλά και τους τελικούς χρήστες των συστημάτων αυτών είναι στοχευμένα και ουσιαστικά. Τα κυριότερα ερωτήματα που χρειάζεται να απαντηθούν για τα εν λόγω συστήματα ανέπαφων τραπεζικών συναλλαγών έτσι ώστε να μπορούμε να θεωρήσουμε τα συστήματα αυτά ασφαλή· είναι τα παρακάτω:

1. Πόσο ανθεκτικά είναι πραγματικά τα συστήματα αυτά, που καθημερινώς επεξεργάζονται τραπεζικά στοιχεία και ευαίσθητες πληροφορίες χρηστών, απέναντι σε κάποιον δυνητικό εχθρό;
2. Πώς αντιμετωπίζει η κινητή συσκευή, που πλέον αποτελεί το μέσο διεκπεραίωσης των συναλλαγών, μια επίθεση και τι μηχανισμοί και άμυνες έχουν ενσωματωθεί για να προστατέψουν τον τελικό χρήστη;
3. Τι αντίμετρα έχουν ενσωματωθεί στο ήδη υπάρχον τραπεζικό οικοσύστημα για την αποφυγή και αντιμετώπιση επιθέσεων;
4. Πως διασφαλίζει και σε τι ποσοστό το μηχάνημα POS και η κινητή συσκευή την ασφάλεια του καναλιού επικοινωνίας που εδραιώνεται αναμεταξύ τους σε περιπτώσεις επιθέσεων πλαστοπροσωπίας, επιθέσεις Man-in-The-Middle και άλλες παρεμφερή επιθέσεις;

Λόγω της ευαισθησίας του θέματος, έχουν γίνει ποικίλες προσπάθειες απάντησης του ερωτήματος αν τα συστήματα πληρούν επαρκώς τις προϋποθέσεις για ασφαλείς συναλλαγές. Έχουν διεξαχθεί έρευνες και πειράματα στους κρυπτογραφικούς μηχανισμούς που διέπουν τα συστήματα αυτά, στα μηχανήματα ανάγνωσης (POS) και στην μεταξύ τους επικοινωνία χωρίς να έχει απαντηθεί ξεκάθαρα το ερώτημα ασφάλειας.

Πρώτος κύριος στόχος της έρευνας που πραγματοποιήθηκε αποτελεί η εκτενής ανάλυση της αρχιτεκτονικής των συστημάτων ανέπαφων συναλλαγών τόσο ως προς την κινητή συσκευή όσο και προς το τραπεζικό οικοσύστημα και την πορεία των δεδομένων μέσα σε αυτό. Ως δεύτερος στόχος ορίστηκε η παρακολούθηση της συμπεριφοράς των συστατικών στοιχείων μιας ανέπαφης συναλλαγής (κινητή συσκευή, κανάλι επικοινωνίας, μηχάνημα ανάγνωσης) απέναντι σε ένα δυνητικό εχθρό σε συνδυασμό με τα παρεχόμενα αντίμετρα και τους παρεχόμενους μηχανισμούς ασφάλειας ανάλογα το συστατικό στοιχείο της επικοινωνίας.

Τα συμπεράσματα τα οποία εξάχθηκαν κατά την διάρκεια της μελέτης, της συγγραφής και της ολοκλήρωσης της παρούσας πτυχιακής εργασίας όσον αφορά την παρεχόμενη ασφάλεια των συστημάτων

ανέπαφης συναλλαγής μέσω κινητών συσκευών είναι θετικά αν αναλογιστούμε την ανωριμότητα των συστημάτων αυτών. Το τραπεζικό οικοσύστημα έχει προβεί στις κατάλληλες ενέργειες ώστε να αποκρύπτεται αποτελεσματικά η ταυτότητα και τα δεδομένα του χρήστη έχοντας ενσωματώσει μηχανισμούς όπως το Tokenization και το κεντρικοποιημένο σύστημα αποθήκευσης των κλειδιών πληρωμής. Σε περιπτώσεις όπου η κινητή συσκευή δεν πληροί της προδιαγραφές ασφάλειας το τραπεζικό οικοσύστημα με σκοπό να προστατέψει τον χρήστη δημιούργησε ένα ασφαλές περιβάλλον νεφοϋπολογιστικής, όπου αποθηκεύονται τα ευαίσθητα δεδομένα του χρήστη εκτός συσκευής ενισχύοντας την παρεχόμενη ασφάλεια και την ακεραιότητα των δεδομένων.

Όσον αφορά τις κινητές συσκευές έχουν ενσωματωθεί ειδικά μικροτσίπ και εργαλεία ασφάλειας με σκοπό την προστασία του χρήστη από δυνητικούς εχθρούς και από μη εξουσιοδοτημένη χρήση των εφαρμογών που εκτελούν τις ανέπαφες συναλλαγές. Επιπρόσθετα, έχουν ενσωματωθεί μηχανισμοί ασφάλειας απέναντι στις πιο διαδομένες μορφές επιθέσεις αναχαίτισης του παραγόμενου καναλιού επικοινωνίας και παραποίησης δεδομένων καθώς και μηχανισμούς προστασίας απέναντι σε επιθέσεις πλαστοπροσωπίας και μη εξουσιοδοτημένης χρήσης των τραπεζικών δεδομένων του χρήστη. Όλες οι παραπάνω μορφές άμυνας προσφέρουν στην κινητή συσκευή ένα αποδεκτό επίπεδο παρεχόμενης ασφάλειας.

Η σημαντικότερη ανησυχία ασφάλειας όμως δεν προκύπτει από τα παραπάνω στοιχεία των συστημάτων ανέπαφης συναλλαγής μέσω κινητών συσκευών αλλά από την άγνοια περί πραγματικής ασφάλειας των χρηστών τους. Η μη σωστή παραμετροποίηση των συστημάτων του εμπόρου ή η χρήση του ίδιου δικτύου για το μηχάνημα POS και τους πελάτες, η μη σωστή χρήση της κινητής συσκευής από τον ίδιο τον χρήστη και η χρήση αδύναμων διαπιστευτηρίων για την προστασία των δεδομένων πληρωμής αποτελούν τις πραγματικές ευπάθειες των συστημάτων αυτών.

1.1 Παρόμοιες Εργασίες

Στα πλαίσια της πτυχιακής εργασίας αναλύθηκαν τρεις διαφορετικοί τομείς των συστημάτων ανέπαφης συναλλαγής μέσω κινητών συσκευών. Στον πρώτο τομέα συζητήθηκε η αρχιτεκτονική, τα πρωτόκολλα επικοινωνίας καθώς και η λειτουργικότητα τόσο του τραπεζικού οικοσυστήματος όσο και της ίδιας της συσκευής που εκτελεί την συναλλαγή με γνώμονα την παρεχόμενη ασφάλεια προς τον τελικό χρήστη. Ο δεύτερος τομέας αποτελεί τις πιθανές ευπάθειες και επιθέσεις που είναι σε θέση ένας δυνητικός εχθρός να υλοποιήσει με σκοπό είτε την έκθεση είτε την παραποίηση είτε την μη εξουσιοδοτημένη χρήση των δεδομένων του χρήστη καθώς και προτεινόμενες λύσεις και αντίμετρα με στόχο την ενδυνάμωση της παρεχόμενης ασφάλειας. Ο τρίτος και τελευταίος τομέας που συζητήθηκε στα πλαίσια της έρευνας αποτέλεσε ο τρόπος λειτουργίας καθώς και γνωστές ευπάθειες απέναντι στις πιο διαδεδομένες εφαρμογές εκτέλεσης ανέπαφων τραπεζικών συναλλαγών, οι οποίες κάνουν χρήση του πρωτοκόλλου επικοινωνίας NFC.

Ο τομέας των ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών αποτελεί ένα ιδιαίτερα καινούργιο και σχετικά ανώριμο τομέα έρευνας. Οι διαθέσιμες δημοσιοποιημένες έρευνες στοχεύουν στα επιμέρους στοιχεία των συστημάτων αυτών και λιγότερο σε μια γενικευμένη και συνδυαστική έρευνα αναγκάζοντας τον αναγνώστη να διαβάσει παραπάνω από μια έρευνα με σκοπό να κατανοήσει την λειτουργικότητα και την παρεχόμενη ασφάλεια των συστημάτων. Η συγκεκριμένη αντιμετώπιση προκύπτει από το γεγονός ότι η διεκπεραίωση ανέπαφων συναλλαγών μέσω κινητών συσκευών αποτελεί μια τεχνολογία με λιγότερο από πέντε χρόνια ύπαρξης με αποτέλεσμα την απουσία ενός γενικευμένου οδηγού ασφάλειας.

Σύμφωνα με τις υπάρχουσες έρευνες, τα συστήματα αυτά αποτελούν την εξέλιξη των τραπεζικών συναλλαγών οπότε είναι επιτακτική η ανάγκη λεπτομερούς εξέτασης των επιμέρους συστατικών στοιχειών με σκοπό την απάντηση του ερωτήματος περί πραγματικής ασφάλειας. Δηλαδή, αν το παρεχόμενο επίπεδο ασφάλειας είναι επαρκές για την καθολική προστασία του τελικού χρήστη. Όμως μελετώντας τις διαθέσιμες στο ευρύ κοινό εργασίες, όπως του Abd Allah, M [2], του Badra, M [5], Roland, Michael [30] για τις δυνατότητες και τις αδυναμίες του πρωτοκόλλου επικοινωνίας NFC ή τις έρευνες του Reveilhac, M et al [29] και του Rosenberg, D[31] για τους μηχανισμούς ασφάλειας της κινητής συσκευής ή τέλος για τους μηχανισμούς ασφάλειας που παρέχονται από το ίδιο το τραπεζικό οικοσύστημα [27, 32, 33] ο αναγνώστης δεν είναι σε θέση να έχει μια ολοκληρωμένη άποψη περί του θέματος. Εξετάζοντας περισσότερες διαθέσιμες έρευνες στοχοποιημένες στις αδυναμίες και

στις πιθανές επιθέσεις ενάντια σε ολόκληρο το σύστημα διεκπεραίωσης ανέπαφων συναλλαγών και τα πιθανά αντίμετρα τους όπως είτε του Simon, L [35] είτε του Bocek, T et al [7] είτε του Beniamini, G [6] δεν είναι δυνατή η εξαγωγή ενός συμπεράσματος για τον μοναδικό λόγο ότι όλες οι παραπάνω έρευνες είναι στοχοποιημένες σε ένα συστατικό στοιχείο των συστημάτων αυτών χωρίς να επιτρέπουν την δημιουργίας μιας γενικής εικόνας.

Εξετάζοντας με περισσότερη προσοχή τις διαθέσιμες έρευνες αναδύθηκε η ανάγκη ύπαρξης μιας γενικής προσέγγισης, η οποία να συνδυάζει όλα τα επιμέρους στοιχεία καθώς και τις σημαντικότερες ευπάθειες των συστημάτων αυτών σε μια βιβλιογραφική έρευνα με σκοπό την δημιουργία μιας σφαιρικής προσέγγισης απέναντι στα συστήματα διεκπεραίωσης ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών συνδυάζοντας προγενέστερες έρευνες καθώς και συμπεράσματα και αποτελέσματα, τα οποία απορρέουν από την προσεκτική μελέτη των διαθέσιμων δημοσιευμένων ερευνών.

1.2 Συνεισφορά Πτυχιακής Εργασίας

Η συνεισφορά της παρούσας πτυχιακής εργασίας προς την επιστημονική κοινότητα αποτελεί η συγκέντρωση πολλαπλών επιστημονικών ερευνών και μεθοδολογιών καθώς και η ενσωμάτωση συμπερασμάτων που απορρέουν από την προσεκτική μελέτη τους. Οι έρευνες που μελετήθηκαν καθώς και τα συμπεράσματα που εξάχθηκαν έχουν ως στόχο την βαθύτερη κατανόηση της παρεχόμενης ασφάλειας τόσο ως προς τα μεμονωμένα συστατικά στοιχεία των συστημάτων διεκπεραίωσης ανέπαφων συναλλαγών όσο και ως προς την παρεχόμενη συνδυαστική ασφάλεια τους.

Συγκεντρώθηκαν και συνενώθηκαν οι σημαντικότερες λειτουργίες και μηχανισμοί ασφάλειας που προσφέρονται τόσο από την κινητή συσκευή ως μέσο διεκπεραίωσης όσο και οι μηχανισμοί που παρέχονται από το ίδιο το τραπεζικό οικοσύστημα. Επιπρόσθετα, κατηγοριοποιήθηκαν υπό την μορφή πίνακα οι διάφορες τροποποιήσεις στο ήδη υπάρχον τραπεζικό οικοσύστημα καθώς και στις κινητές συσκευές που επιτρέπουν την ασφαλή λειτουργία των συστημάτων προτείνοντας επίσης και διαφορετικές υλοποιήσεις για την ενίσχυση της ασφάλειας των δεδομένων.

Επιπρόσθετα, συγκεντρώθηκαν και αναλύθηκαν οι επιθέσεις που στοχεύουν την κινητή συσκευή και διακατέχονται από το μεγαλύτερο ποσοστό επιτυχίας καθώς και λύσεις και αντίμετρα με γνώμονα την αποδοτικότερη αντιμετώπιση μιας πιθανής διαρροής των πληροφοριών και των δεδομένων του χρήστη. Οι παραπάνω απειλές και λύσεις κατηγοριοποιήθηκαν ανάλογα τον στόχο και την επικινδυνότητα τους και συνδυάστηκαν με τα αποδοτικότερα αντίμετρα σε μορφή πίνακα. Στα τελευταία κεφάλαια, αναλύονται οι διασημότερες εφαρμογές διεκπεραίωσης ανέπαφων συναλλαγών τόσο ως προς τα βήματα που απαιτείται από τον χρήστη να εκτελέσει έτσι ώστε να μπορεί να τις χρησιμοποιήσει όσο και τις πιθανές ευπάθειες που προκύπτουν εκτελώντας το κάθε βήμα.

Συνδυάζοντας όλα τα παραπάνω, η ουσιαστική συνεισφορά στην επιστημονική κοινότητα της εν λόγω πτυχιακής εργασίας είναι η μεθοδική και στοχευμένη συγκέντρωση και ανάλυση των επιμέρους στοιχείων των συστημάτων, των ευπαθειών τους και των πιθανών επιθέσεων που μπορεί να εκτελέσει ένας δυνητικός εχθρός με σκοπό την δημιουργία μιας σφαιρικής αντίληψης και ενός οδηγού ασφάλειας ως προς τα συστήματα ανέπαφης συναλλαγής που κάνουν χρήση του πρωτοκόλλου NFC.

1.3 Μεθοδολογία και Δομή Εργασίας

1.3.1 Μεθοδολογία

Οι μέθοδοι που ακολουθήθηκαν στα πλαίσια της πτυχιακής εργασίας χωρίζονται σε δυο κύρια τμήματα. Στο πρώτο σκέλος πραγματοποιήθηκε βιβλιογραφική έρευνα στα κύρια συστατικά στοιχεία των συστημάτων ανέπαφης συναλλαγής σύμφωνα με προϋπάρχουσες έρευνες. Πραγματοποιήθηκε εκτενής αναφορά και ανάλυση της αρχιτεκτονικής των συστημάτων ανέπαφης συναλλαγής τόσο από την σκοπιά του τραπεζικού οικοσυστήματος όσο και από την σκοπιά της κινητής συσκευής. Αναλύθηκαν οι παρεχόμενοι μηχανισμοί ασφάλειας εντός της κινητής συσκευής όπως το Secure Element (SE), το Trusted Execution Environment (TEE) καθώς και το υποστηριζόμενο από το τραπεζικό οικοσύστημα Host Card Emulation (HCE).

Επιπρόσθετα, αναλύθηκαν οι μηχανισμοί ενίσχυσης της ασφάλειας που ενσωματώθηκαν στο ήδη υπάρχον τραπεζικό οικοσύστημα, για την υποστήριξη των ανέπαφων συναλλαγών μέσω κινητών συ-

σκευών, όπως το Tokenization, το κλειδί πληρωμής (Payment Token) καθώς και η οντότητα που είναι υπεύθυνη για την ομαλή λειτουργία των παραπάνω, ο πάροχος υπηρεσιών κλειδιού (Token Service Provider - TSP).

Στο δεύτερο σκέλος της πτυχιακής εργασίας πραγματοποιήθηκε έρευνα και ανάλυση των απαιτήσεων ασφάλειας των διαθέσιμων στην αγορά εφαρμογών ανέπαφης συναλλαγής καθώς και πιθανές επιθέσεις και ευπάθειες ενάντια τόσο στο πρωτόκολλο επικοινωνίας Near Field Communication (NFC) όσο και στην κινητή συσκευή που εκτελεί την ανέπαφη συναλλαγή. Επιπρόσθετα, αναφέρονται και επεξηγούνται τα διαθέσιμα αντίμετρα για την αποφυγή και την αποδοτική αντιμετώπιση όλων των επιθέσεων που αναλύθηκαν και αναφέρθηκαν παραπάνω.

Τέλος, πραγματοποιήθηκαν τρεις (3) μελέτες περιπτώσεις πάνω στις πιο διαδεδομένες εφαρμογές ανέπαφων πληρωμών καθώς και τα πλεονεκτήματα και τα μειονεκτήματα της κάθε μιας. Σε κάθε αναφερόμενη εφαρμογή πραγματοποιήθηκε εκτενής αναφορά και ανάλυση των προϋποθέσεων και των απαιτήσεων ασφάλειας καθώς και οι βασικότερες μορφές επιθέσεων που μπορούν να υλοποιηθούν πάνω σε αυτές. Επίσης, προτάθηκαν βασικά αντίμετρα και μεθοδολογίες αντιμετώπισης των αναφερόμενων επιθέσεων με γνώμονα την αποδοτικότητα των συστημάτων και τις υψηλές απαιτήσεις ασφάλειας.

1.3.2 Ενδεικτική Μορφή Εργασίας

Η παρούσα πτυχιακή αποτελείται από επτά κύρια κεφάλαια. Το πρώτο κεφάλαιο αποτελείται από την εισαγωγή και τα ερευνητικά ερωτήματα που τέθηκαν κατά την διάρκεια της εκπόνησης της πτυχιακής εργασίας. Γίνεται αναφορά στις παρόμοιες εργασίες καθώς και την συνεισφορά την πτυχιακής εργασίας στην επιστημονική κοινότητα.Τέλος, γίνεται αναφορά στην μεθοδολογία που ακολουθήθηκε στην συγγραφή της πτυχιακής καθώς και η ενδεικτική μορφή της.

Το δεύτερο κεφάλαιο αναφέρει εισαγωγικά τον τρόπο με τον οποίο εκτελούνται οι ανέπαφες τραπεζικές συναλλαγές μέσω πλαστικών καρτών καθώς και την μετάβαση από τις πλαστικές κάρτες στις κινητές συσκευές ικανές να διεκπεραιώσουν ανέπαφες τραπεζικές συναλλαγές. Επιπρόσθετα, εκτελείται αναφορά στις τεχνολογίες επικοινωνιών που επιτρέπουν την επικοινωνία της κινητής συσκευής με το τερματικό πληρωμής και τέλος το σύνολο των κανόνων που χαρακτηρίζουν τις ανέπαφες τραπεζικές συναλλαγές μέσω κινητών συσκευών όπως έχουν οριστεί από τους τραπεζικούς κολοσσούς Visa, MasterCard και EuroPay.

Το τρίτο κεφάλαιο αποτελείται από την εκτενή ανάλυση της αρχιτεκτονικής των συστημάτων διεκπεραίωσης ανέπαφων συναλλαγών. Αναφέρεται και αναλύεται το παρεχόμενο υλικό και οι απαραίτητες λειτουργίες εντός των κινητών συσκευών, τα οποία επιτρέπουν την διεκπεραίωση των συναλλαγών. Στη συνέχεια, αναλύονται οι διεργασίες και οι μηχανισμοί του τραπεζικού οικοσυστήματος, οι οποίοι είναι υπεύθυνοι για την ομαλή λειτουργία των συστημάτων σε συνδυασμό με την σύγκριση με τα συστήματα ανέπαφων τραπεζικών συναλλαγών μέσω πλαστικών καρτών. Τέλος, γίνεται μια αναφορά σε έναν ακόμα βασικό πυλώνα των συστημάτων αυτών και αφορά την δημιουργία και την χρήση ειδικά διαμορφωμένων κλειδιών πληρωμής, τα οποία επιτρέπουν την ασφαλή εκτέλεσης της ανέπαφης συναλλαγής. Επίσης, γίνεται λεπτομερής επεξήγηση της έννοιας του παρόχου υπηρεσιών πληρωμής Token Service Provider (TSP) καθώς και τον ρόλο που διακατέχει εντός του τραπεζικού οικοσυστήματος.

Στο τέταρτο κεφάλαιο, επεξηγούνται και αναλύονται τα πιθανότερα σενάρια επιθέσεων απέναντι στην κινητή συσκευή καθώς και στο παραγόμενο κανάλι επικοινωνίας που εδραιώνεται μεταξύ της συσκευής και του τερματικού πληρωμών Point-Of-Sale (POS) κατά την διάρκεια μιας ανέπαφης συναλλαγής. Ως αποτέλεσμα της παραπάνω ανάλυσης ευπαθειών και απειλών αναφέρονται οι απαιτήσεις ασφάλειας των συστημάτων πληρωμής στοχευμένα ως προς την ασφάλεια των εξουσιοδοτημένων εφαρμογών ανέπαφης συναλλαγής καθώς και της ίδιας της κινητής συσκευής.

Το πέμπτο κεφάλαιο αποτελείται από τις λύσεις και τις προτάσεις ενάντια στις απειλές και τις ευπάθειες της κινητής συσκευής και του λειτουργικού συστήματος της. Επιπρόσθετα, προτείνονται λύσεις και προτάσεις ενάντια στις πιθανές επιθέσεις που μπορεί να εκτελέσει ένας δυνητικός εχθρός προς το εδραιωμένο κανάλι επικοινωνίας μεταξύ της κινητής συσκευής και του τερματικού πληρωμής καθώς τα πιθανά αντίμετρα στις υπάρχουσες απειλές ενάντια του πρωτοκόλλου επικοινωνίας NFC με σκοπό την μείωση της επικινδυνότητας έκθεσης των ευαίσθητων δεδομένων του τελικού χρήστη.

Στο έκτο κεφάλαιο, πραγματοποιήθηκαν τρεις μελέτες περίπτωσης των πιο διαδεδομένων εφαρμογών εκτέλεσης ανέπαφων συναλλαγών καθώς και πιθανά σενάρια επίθεσης απέναντι σε αυτές. Αναφέρονται επίσης και γνωστές ευπάθειες των εφαρμογών και το αντίκτυπο τους στην παρεχόμενη ασφάλεια του τελικού χρήστη καθώς και οι προϋποθέσεις ασφάλειας των εφαρμογών με τελικό σκοπό την καλή πρακτική και την διασφάλιση της ασφάλειας των προσωπικών και τραπεζικών δεδομένων του χρήστη.

2 Εισαγωγή στα συστήματα ηλεκτρονικών πορτοφολιών και στις τεχνολογίες επικοινωνιών ανέπαφων συναλλαγών.

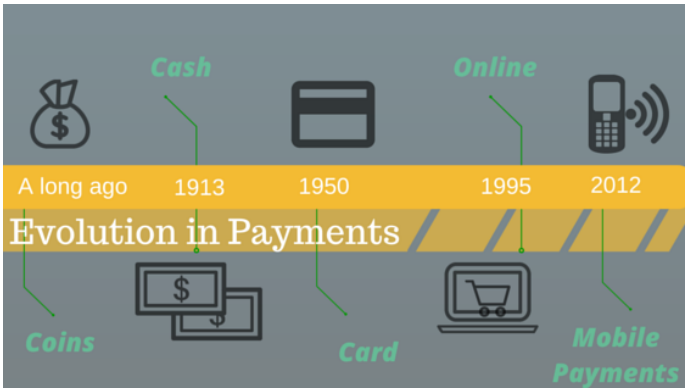
Στο παρακάτω κεφάλαιο εκτελείται μια εισαγωγή στις ανέπαφες τραπεζικές συναλλαγές μέσω κινητών συσκευών. Αναλύεται και επεξηγείται η μετάβαση από τις πλαστικές κάρτες, ανέπαφες και μη, καθώς και η λειτουργικότητα των ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών. Επεξηγείται η ποικιλομορφία της λειτουργικότητας του πρωτοκόλλου επικοινωνίας NFC εξειδικεύοντας στην προσφερόμενη λειτουργικότητα που προσφέρει το εν λόγω πρωτόκολλο επικοινωνίας στο τραπεζικό οικοσύστημα. Εξειδικεύοντας την λειτουργικότητα του πρωτοκόλλου προς τον τομέα των τραπεζικών συναλλαγών επεξηγούνται επιπλέον οι δυνατές υλοποιήσεις και λειτουργίες του πρωτοκόλλου εντός των κινητών συσκευών με σκοπό την διεκπεραίωση τραπεζικών συναλλαγών. Επιπρόσθετα, επεξηγείται το παγκόσμιο πρωτόκολλο που έχει δημιουργηθεί από την EMVCo που διέπει τόσο τις πλαστικές ανέπαφες τραπεζικές κάρτες όσο και τις συναλλαγές που εκτελούνται μέσω των κινητών συσκευών.

Καθ΄ όλη την διάρκεια της ανθρώπινης ιστορίας, ο άνθρωπος δημιουργεί και βασίζεται σε συστήματα πληρωμών με σκοπό να αγοράσει ή να πουλήσει τα αγαθά του. Ξεκινώντας από το ανταλλακτικό εμπόριο και μεταπηδώντας στην δημιουργία και στην χρήση νομισμάτων και στο χάρτινο χρήμα, η ανάγκη για μεγαλύτερη ευκολία στις συναλλαγές επιφέρει την πρώτη πλαστική κάρτα στις αρχές της δεκαετίας του 1960. Στις αρχές του 2000 αρχίζουν και ενσωματώνονται στην αγορά κινητές συσκευές ικανές να εκτελέσουν μια διαδικτυακή τραπεζική συναλλαγή με πρωτοπόρο την εταιρεία PayPal, η οποία αρχίζει να μπαίνει δυναμικά στις αγορές, καθώς και εταιρείες που προσφέρουν υπηρεσίες και εφαρμογές κινητών πορτοφολιών (Nearfieldcommunication.org, 2015).

Μετά από σχεδόν μια δεκαετία και αφού έχουν εμφανιστεί οι πρώτες πλαστικές κάρτες, με κύριο γνώμονα την αποδοτικότητα, την ταχύτητα και την ευκολία χρήσης, εμφανίζονται οι πρώτες συσκευές υπό την μορφή καρτών ικανές να εκτελέσουν ανέπαφες τραπεζικές συναλλαγές κάνοντας χρήση του πρωτοκόλλου επικοινωνίας Radio Frequency Identification (RFID). Μετά από σύντομο χρονικό διάστημα εμφανίστηκαν οι πρώτες ανέπαφες τραπεζικές κάρτες, οι οποίες κάνουν χρήση μαγνητικών δυνάμεων για να εδραιώσουν ένα κανάλι επικοινωνίας και να ανταλλάξουν δεδομένα πληρωμής που δεν απαιτούν την φυσική σύνδεση της κάρτας με το τερματικό πληρωμής (Rampton, 2016).

Παράλληλα από το 1997 εμφανίζεται το πρώτο κινητό πορτοφόλι από την Merita Bank. Στην συγκεκριμένη εφαρμογή ο χρήστης μπορεί να εκτελέσει τραπεζικές συναλλαγές υπό την μορφή γραπτών μηνυμάτων με σκοπό την εξουσιοδότηση της πληρωμής. Η πρώτη εμπορική χρήση της συγκεκριμένης λειτουργίας υλοποιήθηκε από την Coca Cola όπου παρείχε την δυνατότητα πληρωμής μέσω κινητού πορτοφολιού. Από τις αρχές της δεκαετίας του 2010 γίνεται ο συνδυασμός των ανέπαφων τραπεζικών συναλλαγών με την ιδέα των κινητών πορτοφολιών δημιουργώντας τις πρώτες συσκευές ικανές να εκτελέσουν ανέπαφες τραπεζικές συναλλαγές και τα πρώτα ηλεκτρονικά πορτοφόλια. Οι εν λόγω συσκευές χρησιμοποιούσαν το πρωτόκολλο επικοινωνίας Near Field Communication (NFC), το οποίο είναι η μετεξέλιξη του RFID, για να επικοινωνήσουν με το εκάστοτε τερματικό πληρωμής (Nearfieldcommunication.org, 2015).

Ουσιαστικά, η διεκπεραίωση ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών δεν αποτελεί ένα υποσύστημα του τραπεζικού συστήματος αλλά την φυσική εξέλιξη του αξιοποιώντας την συνένωση και την ενσωμάτωση όλων των προηγούμενων τεχνολογιών σε μια και μόνο συσκευή. Στο σχήμα 1, γίνεται με γραφικό τρόπο η αναπαράσταση της εξέλιξης των τρόπων πληρωμής από τις αρχές του χρόνου μέχρι και την σημερινή εποχή.



Σχήμα 1: Ιστορική Εξέλιξη των Συστημάτων Πληρωμής (Source: Global Platform)

Για λόγους κατανόησης παρακάτω γίνεται ο κύριος διαχωρισμός μεταξύ των ηλεκτρονικών πορτοφολιών και των κινητών πορτοφολιών. Τα κινητά πορτοφόλια (Mobile Wallets) είναι εφαρμογές κινητών συσκευών, οι οποίες έχουν την ικανότητα να αποθηκεύουν πολύτιμες πληροφορίες σε ηλεκτρονική μορφή. Οι συγκεκριμένες εφαρμογές επιτρέπουν την εκτέλεση ηλεκτρονικών αγορών ή την αποστολή χρηματικών ποσών σε άλλους αντίστοιχους χρηστές. Ανάλογα το είδος του ηλεκτρονικού πορτοφολιού, οι αποθηκευμένες πληροφορίες κυμαίνονται από δεδομένα χρεωστικών ή πιστωτικών καρτών μέχρι και προσωπικές πληροφορίες που αφορούν τον δικαιούχο της κάρτας.

Αντίθετα, τα ηλεκτρονικά πορτοφόλια (Digital Wallets) είναι εφαρμογές που αποτελούνται από ένα συνδυασμό τεχνολογιών λογισμικού και υλικού εντός των κινητών συσκευών με ικανότητες διεκπεραίωσης ανέπαφων τραπεζικών συναλλαγών με απώτερο σκοπό την αντικατάσταση των παραδοσιακών πλαστικών καρτών και του φυσικού χρήματος (Thienes,2016).

2.1 Μετάβαση από τις Πλαστικές Κάρτες στις Κινητές Συσκευές

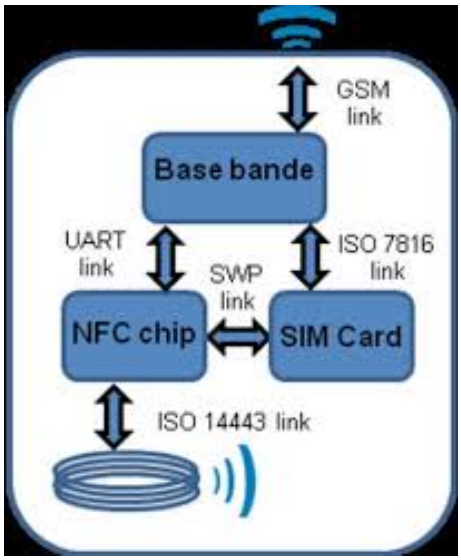
Οι ανέπαφες συναλλαγές και ειδικότερα οι ανέπαφες πλαστικές κάρτες αποτελούν μια μορφή υλοποίησης της τεχνολογίας των ανέπαφων έξυπνων μικροτσίπ, οι οποίες κάνουν χρήση τεχνολογιών μαγνητικής σύζευξης. Μια ανέπαφη τραπεζική συναλλαγή αποτελείται από μια ανταλλαγή δεδομένων, η όποια δεν απαιτεί την φυσική σύνδεση μεταξύ της πλαστικής κάρτας και του τερματικού πληρωμών. Αναπτύχθηκαν με αρχικό σκοπό την ενσωμάτωση τους στο τραπεζικό οικοσύστημα των χρεωστικών και πιστωτικών καρτών με πρωτοπόρο σύστημα, το επονομαζόμενο πρόγραμμα Pay Pass.

Για να διεκπεραιωθεί μια ανέπαφη συναλλαγή μέσω του συστήματος καρτών, τυπικά ο κάτοχος της χρεωστικής ή πιστωτικής κάρτας ξεκινάει την συναλλαγή με την αναμετάδοση δεδομένων επιβεβαίωσης πληρωμής καθώς και τον αριθμό λογαριασμού (PAN) προς τον έμπορο. Η διαδικασία μπορεί να εκτελεστεί είτε με το πέρασμα της κάρτας πάνω από το μηχάνημα POS είτε με την εισαγωγή και την ανάγνωση του EMV μικροτσίπ. Το τερματικό με την σειρά του, προωθεί την απαραίτητη πληροφορία στην τράπεζα του εμπόρου και εκείνη μεταφέρει το αίτημα συναλλαγής στην τράπεζα-εκδότη της κάρτας για επιβεβαίωση. Η τράπεζα-εκδότης της εν λόγω κάρτας εξουσιοδοτεί ή απορρίπτει την συναλλαγή και μέσω του δικτύου πληρωμής επιστρέφεται στην οθόνη του τερματικού πληρωμής η εξουσιοδότηση ή η απόρριψη της συναλλαγής.

Καθώς, οι ανέπαφες συναλλαγές μέσω πλαστικών καρτών είναι αρκετά περιορισμένες διότι οι κάρτες που εκτελούν τις συναλλαγές δεν κατέχουν εσωτερική πηγή ενέργειας, οθόνη ή πληκτρολόγιο ή κάποιο μηχανισμό αποτροπής της μη εξουσιοδοτημένης χρήσης τους αποτελεί ενδιαφέρουσα οπτική η χρήση ενός μηχανήματος, το οποίο χρησιμοποιείται κατά κόρων από τον παγκόσμιο πληθυσμό, το κινητό τηλέφωνο. Κύριος σκοπός της μεταπήδησης από τις πλαστικές κάρτες στις κινητές συσκευές αποτελεί η αύξηση της αποδοτικότητας και της ταχύτητας των συναλλαγών καθώς και ο καλύτερος έλεγχος τους (Pasquet et al,2018).

Οι ικανότητες που προσφέρονται για την διεκπεραίωση ανέπαφων συναλλαγών μέσω της κινητής συσκευής μπορούν να εκτελεστούν με δυο κυρίους τρόπους σύμφωνα με το σχήμα 2 (Nearfieldcommunication.org, 2015):

- Με την χρήση διπλού τσιπ, όπου η κάρτα SIM χρησιμοποιείται αποκλειστικά για την χρήση του κυψελικού δικτυού κινητής τηλεφωνίας, με κύριες λειτουργίες την αποστολή και την παραλαβή μηνυμάτων καθώς και την αποδοχή τηλεφωνικών κλήσεων, και ένα δεύτερο μικροτσίπ, το όποιο εκτελεί τις διεργασίες του πρωτόκολλου NFC. Τα δυο μικροτσίπ είναι εντελώς διαχωρισμένα το ένα από το άλλο.
- Με την χρήση μονού μικροτσίπ, όπου ενσωματώνεται η λειτουργία των ανέπαφων συστημάτων εντός του περιβάλλοντος της κάρτας SIM.



Σχήμα 2: Διαφορετικές υλοποιήσεις σύνδεσης εντός της κινητής συσκευής (Nearfieldcommunication.org, 2015).

Ο τελικός χρήστης μιας συσκευής με ικανότητες διασύνδεσης μέσω NFC μπορεί να χρησιμοποιήσει την κινητή συσκευή είτε για την απλή καθημερινή χρήση της αποστολής/ παραλαβής μηνυμάτων και κλήσεων είτε για την εκτέλεση ανέπαφων τραπεζικών συναλλαγών (Reveilhac & Pasquet, 2009).
Οι διαθέσιμες εκδοχές συστημάτων ανέπαφης διάδρασης μέσω της κινητής συσκευής του χρήστη χωρίζονται σε τέσσερις κύριες κατηγορίες, όπως φαίνεται και στο σχήμα 3:

Σχήμα 3: Διαφορετικές υλοποιήσεις των συστημάτων ανέπαφης διάδρασης (Nearfieldcommunication.org, 2015).

- Touch and Go: Συστήματα ικανά να διεκπεραιώσουν ανέπαφες συναλλαγές χωρίς την ανάγκη

πληκτρολόγησης κωδικού. Τέτοιου είδους συστήματα ενεργοποιούνται με το απλό πέρασμα της πλαστικής κάρτας σε κοντινή απόσταση από το τερματικό πληρωμής.

- Touch and Confirm: Πληρωμές βασισμένες στο σύστημα πληρωμών μέσω του κινητού δικτύου όπου ο χρήστης είναι αναγκασμένος να πληκτρολογήσει τον κωδικό πρόσβασης με σκοπό να εκτελέσει την εν λόγω συναλλαγή.
- Touch and Connect: Εγκαθίδρυση απευθείας σύνδεσης μεταξύ δυο συσκευών με σκοπό την μεταφορά χρημάτων ή δεδομένων .
- Touch and Explore: Μορφή σύνδεσης όπου ο χρήστης έχει την ικανότητα να εξερευνήσει τις δυνατότητες της συσκευής στην όποια θέλει να συνδεθεί και να διαλέξει την καταλληλότερη.

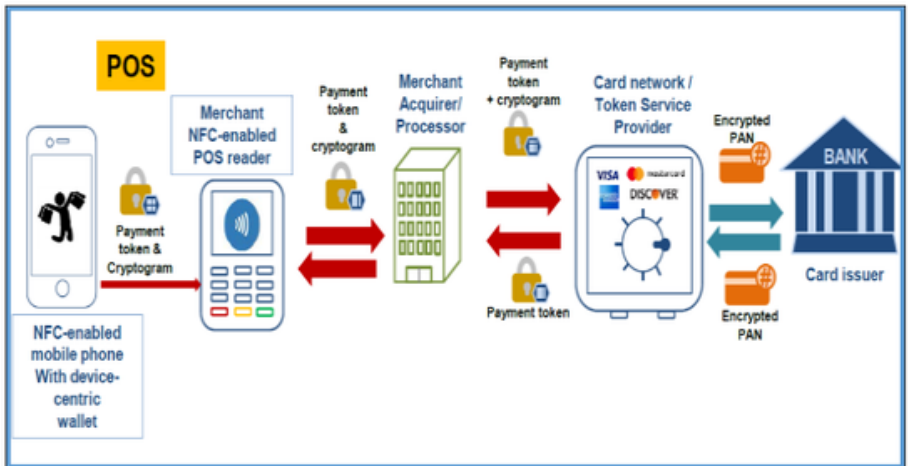
2.2 Ανέπαφες συναλλαγές μέσω κινητών συσκευών

Πληρωμές, οι οποίες είναι βασισμένες σε εφαρμογές κινητών συσκευών, χρησιμοποιούν πρωτόκολλα μαγνητικής σύζευξης (NFC, RFID) και επεξεργάζονται και εκτελούνται μέσω του ιδίου δικτύου πληρωμών που χρησιμοποιείται από τις παραδοσιακές κάρτες ανέπαφων συναλλαγών.

Η ιδία ακριβώς διαδικασία με στις ανέπαφες πλαστικές κάρτες ακολουθείται στο σενάριο λειτουργίας όπου η συναλλαγή εκτελείται μέσω μιας κινητής συσκευής με την μοναδική διάφορα την αντικατάσταση του αριθμού της κάρτας και του αριθμού επιβεβαίωσης (CVC-Card Verification Code) με ειδικές αναπαραγόμενες τιμές, επονομαζόμενες Tokens. Ο λόγος που γίνεται η εν λόγω αντικατάσταση στοχεύει στην αποτροπή αποστολής πραγματικών τιμών αντιστοίχησης της κάρτας μέσω του δικτύου πληρωμών με σκοπό την αποφυγή αποθήκευσης τους σε ενδιάμεσους διακομιστές (Vanderhoof et al,2018).

Οι συγκεκριμένες τιμές αυτές δημιουργούνται από τους εκδότες της κάρτας (MasterCard, Visa), οι όποιοι είναι οι πάροχοι των υπηρεσιών κλειδιού (Token Service Providers –TSP). Οι πάροχοι, οι οποίοι αποτελούν μια καινούργια οντότητα στο τραπεζικό οικοσύστημα με κύριο σκοπό την ενσωμάτωση της δυνατότητας εκτέλεσης ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών, διατηρούν αρχεία αντιστοίχησης των διαθέσιμων κλειδιών στους αντίστοιχους αριθμούς λογαριασμών σε ειδικά σχεδιασμένους πίνακες.

Οι πίνακες είναι αποθηκευμένοι σε ασφαλής βάσεις δεδομένων, γνωστές και ως θησαυροφυλάκια κλειδιών (Token Vault). Κατά την διάρκεια της εκτέλεσης μιας ανέπαφης συναλλαγής, το αντίστοιχο κλειδί παρουσιάζεται στον πάροχο κλειδιών. Ο πάροχος του δικτύου πληρωμών ανατρέχει στον πινάκα τιμών με τα διαθέσιμα κλειδιά και ανασύρει τον πραγματικό αριθμό λογαριασμού (Security of Mobile Payments and Digital Wallets, 2017).



Σχήμα 4: Ροή δεδομένων κατά την διάρκεια εκτέλεσης ανέπαφης συναλλαγής μέσω κινητής συσκευής

Στο σχήμα 4 αναλύεται εξ ολοκλήρου η διαδικασία εκτέλεσης της ανέπαφης συναλλαγής καθώς και τις ενδιάμεσες οντότητες που είναι αρμόδιες για την μεταφορά των δεδομένων με σκοπό την εξουσιοδότηση της συναλλαγής του χρήστη.

2.3 Υφιστάμενες Κατηγορίες Τρόπων Διεκπεραίωσης Συναλλαγών

Μεταπηδώντας από τις ανέπαφες πλαστικές κάρτες στις κινητές συσκευές δεν παρατηρούνται ριζικές αλλαγές όσον αφορά τον τρόπο με τον οποίο το κανάλι επικοινωνίας εδραιώνεται μεταξύ της συσκευής και του τερματικού πληρωμής. Για λόγους σύγκρισης παρακάτω αναφέρονται όλες οι πιθανές υλοποιήσεις συναλλαγών που μπορούν να διεκπεραιωθούν είτε με την φυσική σύνδεση της κάρτας με το τερματικό πληρωμής είτε μέσω ανέπαφης σύνδεσης της πλαστικής κάρτας ή της κινητής συσκευής του χρήστη.

Διεκπεραίωση συναλλαγών μέσω Chip and Pin καρτών
Οι πλαστικές κάρτες που κάνουν χρήση της τεχνολογίας Chip and Pin αποτελούν μια σημαντική τεχνολογική αναβάθμιση από τις παραδοσιακές κάρτες που έκαναν χρήση της αρχικής τεχνολογίας της μαγνητικής ταινίας. Τα τραπεζικά δεδομένα και τα δεδομένα του κατόχου της κάρτας δεν αποθηκεύονται πλέον εντός της μαγνητικής ταινίας αλλά εντός ενός μικροσκοπικού τσιπ εντός της κάρτας. Η εν λόγω τεχνολογία του Chip and Pin προϋπάρχει από το 1984 όμως το 1996 οι κολοσσοί των τραπεζικών συναλλαγών EuroPay, Mastercard και Visa ενώθηκαν για την δημιουργία ενός ασφαλέστερου πρωτοκόλλου λειτουργίας των εν λόγω καρτών, το οποίο μετονομάστηκε EMV από τον συνδυασμό των ακρωνυμίων του κάθε οργανισμού.

Το ενσωματωμένο μικροτσίπ εντός των πλαστικών καρτών κατέχει δυνατότητες αποθήκευσης και επεξεργασίας δεδομένων. Επιπρόσθετα, κατά την διάρκεια της επικοινωνίας με το τερματικό πληρωμών η εν λόγω κάρτα χρησιμοποιεί μεθόδους κρυπτογράφησης με σκοπό να προστατεύσει τα ευαίσθητα τραπεζικά δεδομένα της κάρτας κατά την διάρκεια επικοινωνίας με το τερματικό πληρωμής. Το εν λόγω μικροτσίπ δεν διακατέχεται από κάποια εσωτερική μορφή ενέργειας αλλά ενεργοποιείται από την στιγμή που έρθει σε επαφή με κάποιου είδους τερματικό πληρωμής (Π.χ. POS, ATM).

Η εν λόγω τραπεζική κάρτα χρησιμοποιείται με την είσοδο της κάρτας εντός κάποιου τερματικού πληρωμής. Ανάλογα το είδος του τερματικού, για να μπορεί να χρησιμοποιηθεί η κάρτα, ο χρήστης είτε θα πρέπει να πληκτρολογήσει το τετραψήφιο κωδικό που του έχει παραχωρηθεί από την τράπεζα εκδότη της κάρτας είτε θα πρέπει να υπογράψει ένα σχετικό παραστατικό, το οποίο ουσιαστικά τον αυθεντικοποιεί ως τον υπεύθυνο για την εν λόγω συναλλαγή.

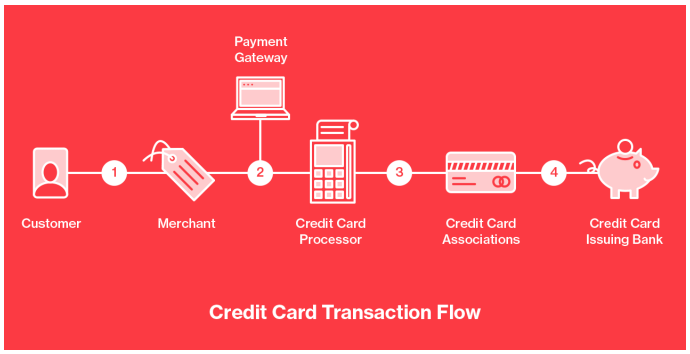
Τα κύρια πλεονεκτήματα της υλοποίησης των καρτών που κάνουν χρήση της τεχνολογίας Chip and Pin αποτελούν η ικανότητα της κάρτας να αποθηκεύει, να επεξεργάζεται και να κρυπτογραφεί τα τραπεζικά δεδομένα και τα δεδομένα του χρήστη με μεγαλύτερο ποσοστό επιτυχίας σε σχέση με τις μαγνητικές κάρτες καθώς και την ικανότητα εκτέλεσης τραπεζικών συναλλαγών ακόμα και χωρίς την ύπαρξη σύνδεσης στο διαδίκτυο, όπου η συναλλαγή αποθηκεύεται στο τερματικό πληρωμής και αποστέλλεται μαζικά στο τέλος της ημέρας με το κλείσιμο του καταστήματος και της ημέρας (Roos, 2017).

Διεκπεραίωση Συναλλαγών μέσω Ανέπαφων Πλαστικών Καρτών
Οι ανέπαφες πλαστικές κάρτες αποτελούν μια μεταγενέστερη λειτουργικότητα των πλαστικών καρτών, η οποία πρωτοεμφανίστηκε το 1996 στην Νότια Κορέα. Η συγκεκριμένη λειτουργικότητα επιτρέπει την διεκπεραίωση τραπεζικών συναλλαγών χωρίς την φυσική σύνδεση μεταξύ της κάρτας και του τερματικού πληρωμής, λειτουργικότητα η οποία προσφέρει ταχύτητα και αποδοτικότητα στις συναλλαγές του χρήστη. Στις ανέπαφες τραπεζικές συναλλαγές το ενσωματωμένο μικροτσίπ της κάρτας εδραιώνει ασύρματη επικοινωνία με το τερματικό πληρωμής μέσω του πρωτοκόλλου του NFC με ταχύτητες της κλίμακας των 106-424 kbit/s. Οι εν λόγω κάρτες απαιτούν μόνο την ύπαρξη μιας κεραίας εγγύτητας για την εδραίωσης της επικοινωνίας. Το πρότυπο που τις διέπει είναι το ISO/IEC 14443 και η αποδεκτή απόσταση μεταξύ της πλαστικής κάρτας και του τερματικού πληρωμής έχει οριστεί στα 10 εκατοστά.

Η χρήση της ανέπαφης τραπεζικής κάρτας δεν απαιτεί την φυσική σύνδεση της κάρτας με το τερματικό πληρωμής παρά μόνο το πέρασμα της εντός της ακτίνας των 10 εκατοστών από την κεραία του τερματικού. Επιπρόσθετα, για συναλλαγές κάτω των 25 Ευρώ, ο χρήστης για λόγους ταχύτητας δεν απαιτείται να πληκτρολογήσει τον τετραψήφιο κωδικό της κάρτας. Τέλος, η εν λόγω κάρτα χρησιμοποιεί το ίδιο τραπεζικό δίκτυο με τις κάρτες Chip and Pin και επιπρόσθετα διέπονται από τις ίδιες αρχές και πρότυπα λειτουργίας και ασφάλειας που έχουν οριστεί από την EMVCo.

Όμως, μια ανέπαφη κάρτα ταυτόχρονα αποτελεί και μια κάρτα Chip and Pin ταυτόχρονα και υπό

περιπτώσεις όπου η ανέπαφη λειτουργικότητα δεν μπορεί να χρησιμοποιηθεί. Για παράδειγμα, αν το ποσό συναλλαγής υπερβαίνει το όριο των 25 Ευρώ. Στην ουσία μια τραπεζική κάρτα με δυνατότητες διεκπεραίωσης ανέπαφων τραπεζικών συναλλαγών αποτελείται από δυο διεπαφές και λειτουργεί ως μια EMV κάρτα όταν δεν χρησιμοποιείται η ανέπαφη λειτουργικότητα. Αυτό που προσφέρει η ανέπαφη διεπαφή της κάρτας εκτός από ταχύτητα και αποδοτικότητα είναι ένα σύνολο από περαιτέρω λειτουργικότητες που τις επιτρέπουν την διεκπεραίωση ανέπαφων συναλλαγών (En.wikipedia.org, 2017).



Σχήμα 5: Υλοποιήσεις ανέπαφων και μη πλαστικών καρτών (source Visa.com, 2015).

Στο σχήμα 5 αναπαριστάται το γεγονός ότι οι πλαστικές κάρτες, ανέπαφες και μη, κάνουν χρήση του ίδιου συστήματος πληρωμής. Η μοναδική διαφορά, όσον αφορά τον τρόπο εδραίωσης της επικοινωνίας, βρίσκεται στο γεγονός ότι στις ανέπαφες πλαστικές κάρτες το πέρασμα των δεδομένων πληρωμής εκτελείται μέσω του πρωτοκόλλου του NFC σε αντίθεση με τις κάρτες που κάνουν χρήση της μεθόδου Chip and Pin όπου τα δεδομένα πληρωμής μεταβιβάζονται προς το τερματικό πληρωμής μέσω του ενσωματωμένου στην κάρτα μικροτσίπ. Η συνέχεια της συναλλαγής είναι πανομοιότυπη και η συναλλαγή ολοκληρώνεται από την στιγμή που τα δεδομένα πληρωμής έχουν μεταβιβαστεί και επεξεργαστεί από της τράπεζα εκδότη της κάρτας του χρήστη προς την τράπεζα του εμπόρου με σκοπό την εξουσιοδότηση και την ολοκλήρωση της συναλλαγής.

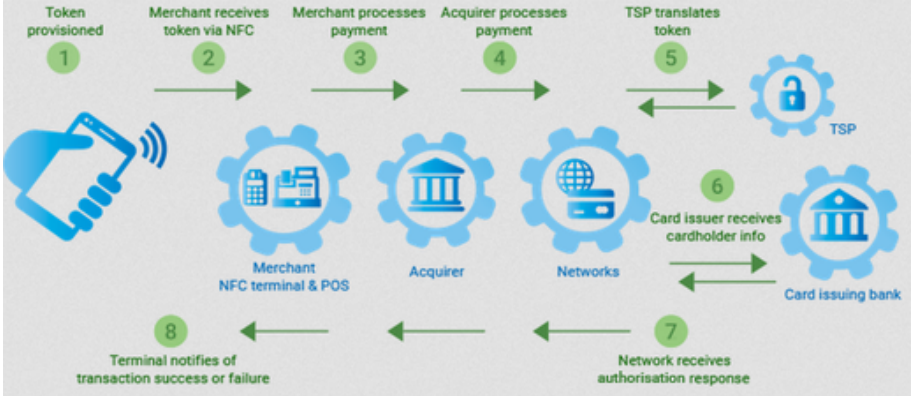
Διεκπεραίωση Ανέπαφων Συναλλαγών μέσω Κινητών Συσκευών

Ως μετεξέλιξη των ανέπαφων τραπεζικών καρτών άρχισαν να εμφανίζονται κινητές συσκευές ικανές να εκτελέσουν ανέπαφες τραπεζικές συναλλαγές. Η λειτουργικότητα των συστημάτων αυτών είναι παρόμοια με αυτή των ανέπαφων πλαστικών καρτών με την βασική διαφορά ότι οι συναλλαγές εκτελούνται μέσω της κινητής συσκευής του χρήστη. Για να είναι σε θέση ο εκάστοτε χρήστης να πραγματοποιήσει συναλλαγές μέσω της κινητής συσκευής του θα πρέπει να είναι βρίσκεται στην ορισμένη απόσταση από το πρωτόκολλο του NFC απόσταση από το τερματικό πληρωμής όπως και σε μια ανέπαφη συναλλαγή μέσω μιας πλαστικής κάρτας. Επιπρόσθετα, τα δεδομένα πληρωμής μετακινούνται και επεξεργάζονται στο ίδιο τραπεζικό δίκτυο με τις πλαστικές κάρτες.Εξακολουθείται να γίνεται κατά κόρων η χρήση του πρωτοκόλλου επικοινωνίας NFC για λόγους συμβατότητας με τα προϋπάρχοντα συστήματα που κάνουν χρήση των πλαστικών καρτών.

Όμως, οι εφαρμογές που βρίσκονται εγκατεστημένες εντός των κινητών συσκευών και είναι ικανές να εκτελέσουν ανέπαφες συναλλαγές έχουν την ικανότητα να χρησιμοποιούν και παραπάνω από μια τεχνολογίες εδραίωσης επικοινωνίας, όχι ταυτόχρονα, για την αναμετάδοση δεδομένων πληρωμής από/προς την κινητή συσκευή από/προς το τερματικό POS του εμπόρου.Οι διαθέσιμες μορφές επικοινωνίας μεταξύ της κινητής συσκευής και του τερματικού POS αποτελούνται από επικοινωνίες βασισμένες σε τεχνολογίες μαγνητικής ταινίας (Magnetic Secure Transmission-MST), NFC, QR Code, Bluetooth, SMS καθώς και μέσω του διαδικτύου (Hillali Wadii et al,2017).

Όμως, με σκοπό την πλήρη λειτουργικότητα της εν λόγω εξέλιξης το τραπεζικό δίκτυο αναβαθμίστηκε με καινούργιες λειτουργίες με σκοπό την ενίσχυση της παρεχόμενης ασφάλειας των συστημάτων της καθώς οι κινητές συσκευές είναι πιο δεκτικές σε επιθέσεις παραβίασης από ότι οι τραπεζικές πλαστικές κάρτες λόγω των πολλαπλών λειτουργιών που μπορούν να εκτελέσουν. Όσον αφορά τις παραλλαγές του συστήματος συναλλαγών ενσωματώθηκε ο μηχανισμός του Tokenization, όπου ο αριθμός του λογαριασμού της αναπαριστώμενης κάρτας του χρήστη μεταφράζεται σε μια τυχαία, μη

χρησιμοποιήσιμη εκτός του καναλιού ορισμού της, ακολουθία αριθμών καθώς και η οντότητα του Token Service Provider, όπου είναι υπεύθυνη για την συσχέτιση του κλειδιού πληρωμής (Token) με τον πραγματικό αριθμό λογαριασμού και την ασφαλή αποθήκευση του πραγματικού αριθμού λογαριασμού του εκάστοτε χρήστη (Sorensen, 2018).



Σχήμα 6: Ροή δεδομένων μιας Ανέπαφης Συναλλαγής μέσω μιας Κινητής Συσκευής (source Android.com, 2016).

Σε αντίθεση με τις πλαστικές κάρτες η ροή της εκτέλεσης μιας τραπεζικής συναλλαγής μέσω κινητών συσκευών διαφέρει. Έχει ενσωματωθεί στο ήδη υπάρχον τραπεζικό οικοσύστημα μια ακόμη οντότητα, ο Πάροχος Υπηρεσιών Κλειδιού (TSP, ο οποίος είναι υπεύθυνος για την αντικατάσταση και την χαρτογράφηση του πραγματικού αριθμού λογαριασμού του χρήστη με μια τυχαία παραγόμενη ακολουθία αριθμών.

Σύμφωνα με το σχήμα 6, η ροή των δεδομένων πληρωμής και το παραγόμενο κλειδί πληρωμής από την εκτελούμενη τραπεζική συναλλαγή μεταβιβάζονται στην τράπεζα του εμπόρου όπου εκείνη με την σειρά της αναγνωρίζει το κλειδί πληρωμής και αποστέλλει την εντολή πληρωμής προς τον Πάροχο Κλειδιού. Ο πάροχος μεταφράζει το απεσταλμένο κλειδί πληρωμής και το ταυτίζει με τον πραγματικό αριθμό λογαριασμού του χρήστη και έπειτα αποστέλλει τις εν λόγω πληροφορίες στην τράπεζα του εκδότη της κάρτας του χρήστη με σκοπό την εξουσιοδότηση ή την απόρριψη του αιτήματος πληρωμής. Η εξουσιοδότηση ή η απόρριψη της συναλλαγής αποστέλλεται μέσω του δικτύου πληρωμών στην οθόνη του τερματικού πληρωμής του εμπόρου.

2.3.1 Λειτουργικότητα πρωτοκόλλου NFC

Όπως προαναφέρθηκε το πρωτόκολλο επικοινωνίας των συστημάτων διεκπεραίωσης ανέπαφων συναλλαγών τόσο των πλαστικών καρτών όσο και των κινητών συσκευών αποτελεί το Near Field Communication. Το συγκεκριμένο πρωτόκολλο έχει την ικανότητα να εδραιώνει το κανάλι επικοινωνίας μέσω μαγνητικής σύζευξης, το οποίο αφαιρεί την αναγκαιότητα φυσικής σύνδεσης μεταξύ των συστατικών στοιχειών της επικοινωνίας.

Το πρωτόκολλο επικοινωνίας NFC αποτελεί ένα σχετικά καινούργιο και ολοένα και δημοφιλέστερο πρωτόκολλο επικοινωνίας, το οποίο βρίσκεται καταχωρημένο υπό το στάνταρ ISO/IEC 21481. Το εν λόγω πρωτόκολλο χρησιμοποιείται σε κινητές συσκευές ή παρόμοιες συσκευές και έχει σχεδιαστεί ως μέσο επικοινωνίας κοντινής απόστασης. Λειτουργεί σε συχνότητες που αγγίζουν τα 13,56 Megahertz με ταχύτητες που κυμαίνονται από 106-424 kilobits/s.

Το NFC λειτουργεί κάνοντας χρήση της κωδικοποίησης Manchester για όλα τα δεδομένα που αποστέλλονται με ταχύτητες πάνω από 106 kbits/s ενώ για τα δεδομένα που αποστέλλονται με ακριβώς 106 kbits/s χρησιμοποιείται κωδικοποίηση Miller. Τα δεδομένα αποστέλλονται σε προκαθορισμένες στιγμές και ταχύτητες σύμφωνα με το παραγόμενο πεδίο. Δηλαδή, τις στιγμές που το παραγόμενο πεδίο βρίσκεται σε μετάβαση low-to-high αναμεταδίδεται 0 ενώ αντίθετα αποστέλλεται 1 τις στιγμές που το πεδίο βρίσκεται σε κατάσταση high-to-low (Nelson et al , 2013).

Οι συσκευές ικανές να χρησιμοποιήσουν το συγκεκριμένο πρωτόκολλο επικοινωνίας χωρίζονται σε δυο κύριες κατηγορίες:

- Οι συσκευές που λειτουργούν σε ενεργητική κατάσταση, διακατέχονται από δικές τους πηγές ενέργειας και ανιχνεύουν συνεχώς για παθητικές συσκευές, οι οποίες βρίσκονται στο εύρος της ακτίνας του πρωτοκόλλου. Επιπρόσθετα, έχουν την ικανότητα να παράγουν το δικό τους μαγνητικό πεδίο σε αντίθεση με τις παθητικές συσκευές.
- Οι συσκευές που λειτουργούν σε παθητική κατάσταση γνωστές και ως NFC Tags, δεν διακατέχονται από τις δικές τους πηγές ενέργειας και δεν μπορούν να παράξουν το μαγνητικό πεδίο που είναι απαραίτητο για την επικοινωνία με την ενεργητική συσκευή αλλά τροφοδοτούνται από το πεδίο που δημιουργεί η ενεργητική συσκευή.

Το χαρακτηριστικό του NFC που το κάνει μοναδικό είναι η ικανότητα που παρέχει στις συσκευές να μεταπηδούν από ενεργητική σε παθητική κατάσταση και το αντίστροφο. Δηλαδή μια συσκευή με δυνατότητες διασύνδεσης μέσω NFC μπορεί να χρησιμοποιηθεί και ως παθητικό tag με σκοπό να ολοκληρώσει μια ανέπαφη πληρωμή αλλά και ως ενεργητική συσκευή έχοντας την ικανότητα σκαναρίσματος ενός παθητικού tag (Securetechalliance.org. 2015).

Το πρωτόκολλο NFC λειτουργεί σε τρεις κυρίες λειτουργικές εκφάνσεις (Vanderhoof et al., 2018):

1. Peer-to-peer: Ειδικά σχεδιασμένη λειτουργία έτσι ώστε δυο συσκευές να μπορούν να εγκαθιδρύσουν απευθείας κανάλι επικοινωνίας αναμεταξύ τους.
2. Reader/Writer mode: Λειτουργία στην οποία οι συσκευές μπορούν να αλληλεπιδράσουν με ανέπαφες κάρτες, αναμεταδότες RFID και NFC tags. Είναι μια λειτουργία που καθιστά δυνατή την ανταλλαγή ανέπαφων δειγμάτων πληροφορίας (Token).
3. Card emulation mode: Λειτουργία με δυνατότητες αναπαράστασης και αναπαραγωγής μιας ανέπαφης κάρτας, η οποία καθιστά δυνατή την επικοινωνία με RFID αναμεταδότες.

Η τεχνολογία NFC αποτελεί μια τεχνολογία προερχόμενη από το RFID πρωτόκολλο επικοινωνίας. Θεωρείται πρωτόκολλο που υλοποιεί μετάδοση δεδομένων με αμφίδρομη εναλλασσόμενη επικοινωνία. Αυτό σημαίνει ότι και τα δυο συστατικά στοιχειά του συστήματος μπορούν να αναμεταδώσουν και να λάβουν δεδομένα αλλά όχι ταυτόχρονα. Επιπρόσθετα, το εν λόγω πρωτόκολλο δεν περιορίζεται στην σύζευξη μεταξύ δυο και μόνο συσκευών. Αντιθέτως σε περιπτώσεις όπου η συσκευή ανιχνεύσει παραπάνω από μια συσκευή στο παραγόμενο πεδίο αποστέλλει τις πληροφορίες και τα δεδομένα σε όλες τις συσκευές. Όμως, μόνο η συσκευή που έχει επιλεχθεί από την ενεργητική συσκευή αποθηκεύει τα δεδομένα. Οι υπόλοιπες συσκευές που βρίσκονται στο παραγόμενο πεδίο δέχονται τα δεδομένα και τις πληροφορίες και αυτόματα τις αγνοούν (Nelson et al, 2013).

Τέλος, εκτός από το επιλεγμένο πρωτόκολλο επικοινωνίας για να είναι ολοκληρωμένο ένα σύστημα ανέπαφων συναλλαγών μέσω κινητής συσκευής θα πρέπει να υπάρχει μια κοινά αποδεκτή ομάδα προϋποθέσεων για την εξασφάλιση της ομαλής λειτουργίας του συστήματος. Το εν λόγω εγχείρημα ολοκληρώθηκε από την EMVCo, η οποία ήταν ήδη αρμόδια για την δημιουργία και ενσωμάτωση παγκόσμιων προϋποθέσεων λειτουργίας για τις ανέπαφες συναλλαγές μέσω πλαστικών καρτών. Οι δυο τεχνολογίες είναι αλληλένδετες καθώς το πρωτόκολλο NFC αποτελεί τον τρόπο με τον οποίο οι συσκευές επικοινωνούν μεταξύ τους για να διεκπεραιώσουν την συναλλαγή ενώ το πρότυπο του EMV χρησιμοποιείται στην ίδια την συναλλαγή έτσι ώστε να εκτελεστεί διακατέχοντας ένα αποδεκτό επίπεδο λειτουργικότητας και ασφάλειας (Merkus, 2018, EMVCo, 2015).

2.3.2 Πρωτόκολλο EMVCo

Η EMVCo, η οποία αποτελεί ορόσημο στα πρωτόκολλα τραπεζικών συναλλαγών, σχεδίασε ένα ιδιωτικό σετ προϋποθέσεων το οποίο σχεδιάστηκε και αναπτύχθηκε από τους οργανισμούς τραπεζικών καρτών Europay, Mastercard και Visa. Οι τραπεζικοί κολοσσοί έγραψαν από κοινού τους κανόνες και τις προδιαγραφές που διέπουν τις έξυπνες πλαστικές κάρτες μέσω των συσκευών (EFT-POS, ATM), οι οποίοι χρησιμοποιούνται κατά την διάρκεια εκτέλεσης ανέπαφων τραπεζικών συναλλαγών.

Οι στόχοι του EMV είναι η μείωση της αυξανόμενης συχνότητας τραπεζικών απατών καθώς και η αποτελεσματικότερη διαχείριση του παγκοσμίως αυξανόμενου όγκου συναλλαγών. Επιπρόσθετα,

είναι υπεύθυνο για την διασφάλιση της σωστής συνεργασίας μεταξύ των διαφορετικών εφαρμογών που εκμεταλλεύονται τις λειτουργίες και τις ικανότητες των χρεωστικών/πιστωτικών καρτών.

Για να μπορεί η κινητή συσκευή να εκτελέσει ανέπαφες τραπεζικές συναλλαγές θα πρέπει να είναι σύμφωνη με τις προϋποθέσεις που έχουν τεθεί από την EMVCO. Οι προϋποθέσεις που έχουν τεθεί είναι οι εξής (EMVCo, 2015):

- Μια κινητή συσκευή έχει την δυνατότητα να υποστηρίξει παραπάνω από μια εφαρμογές ικανές να εκτελέσουν ανέπαφες συναλλαγές ανεξαρτήτως οικονομικού ινστιτούτου έκδοσης της πλαστικής κάρτας που αναπαράγεται από την εφαρμογή.
- Ο χρήστης της συσκευής μπορεί να καθορίσει το εργαλείο πληρωμής για την κάθε συναλλαγή.
- Η EMVCO δεν απαιτεί την ύπαρξη συγκεκριμένου ασφαλούς περιβάλλοντος (Secure Element - SE) ή πολιτική ασφάλειας με σκοπό την ύπαρξη ελαστικότητας ανάλογα την εν λόγω αγορά. Ουσιαστικά υποστηρίζει ελαστικότητα στην τοποθεσία του SE είτε αυτό βρίσκεται εντός της συσκευής είτε σε κάποιο εξουσιοδοτημένο περιβάλλον νεφοϋπολογιστικής.
- Όπου είναι δυνατόν, η EMVCO χρησιμοποιεί τις ήδη υπάρχουσες υποδομές αντί να δημιουργεί καινούργιες.
- Οι εφαρμογές με ικανότητες ανέπαφης διεκπεραίωσης συναλλαγών θα πρέπει να είναι συμβατές με τις ήδη υπάρχουσες υποδομές των τερματικών πληρωμής.

Επιπρόσθετα, το μικροτσίπ που βρίσκεται εντός της κινητής συσκευής και είναι υπεύθυνο για την επεξεργασία και την διαχείριση των δεδομένων πληρωμής, συνηθέστερα το μικροτσίπ του SE, θα πρέπει να είναι σε θέση να (Merkus, 2018):

1. Αποθηκεύει με ασφάλεια τα δεδομένα και τις πληροφορίες πληρωμής.
2. Να μπορεί να εκτελέσει επεξεργασία δεδομένων πληρωμής.
3. Να είναι ικανό να εκτελέσει κρυπτογραφικές μεθόδους.

Για να είναι σε θέση μια κινητή συσκευή να εκτελέσει ανέπαφες συναλλαγές σύμφωνα με το πρότυπο του EMV θα πρέπει να εκτελεστούν οι παρακάτω ενέργειες.

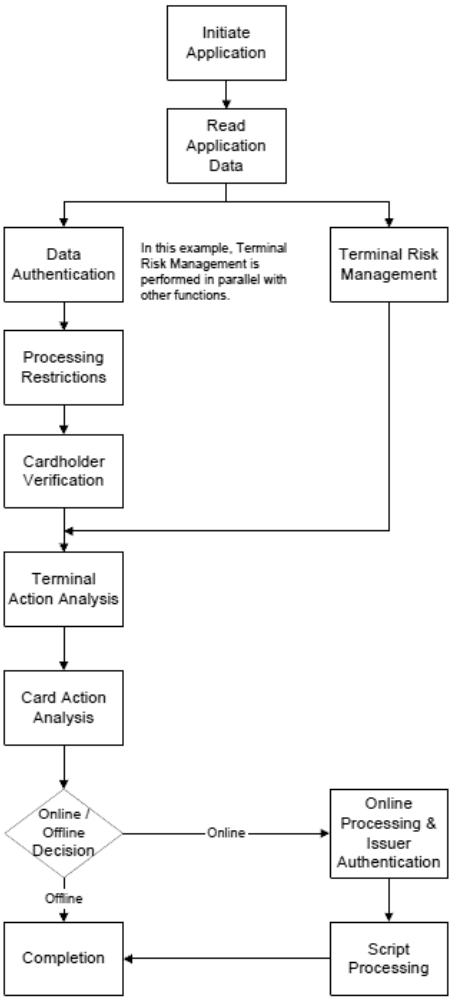
1. Θα πρέπει να εκτελείται αυθεντικοποιήση της συσκευής με σκοπό την προστασία του χρήστη από μη εξουσιοδοτημένες συναλλαγές.
2. Διαρκής διαχείριση ρίσκου κατά την διάρκεια χρήσης της εφαρμογής διεκπεραίωσης ανέπαφων συναλλαγών της συσκευής.
3. Ηλεκτρονική υπογραφή των δεδομένων πληρωμής με σκοπό την διατήρηση της ακεραιότητας των δεδομένων.
4. Αυθεντικοποιήση χρηστών με Robust τεχνικές για την περαιτέρω προστασία του χρήστη σε περιπτώσεις απώλειας ή κλοπής της συσκευής.

Η διαδικασία εξουσιοδότησης και επαλήθευσης που ακολουθείται έτσι ώστε ο τελικός χρήστης να έχει την ικανότητα χρήσης της ανέπαφης κάρτας ή της κινητής του συσκευής για την διεκπεραίωση συναλλαγών είναι παρόμοια με εκείνη που απαιτείται για τις κάρτες με ενσωματωμένο μικροτσίπ (Securetechalliance.org, 2015).

Τέλος, σύμφωνα με τις προϋποθέσεις που έχουν τεθεί από την EMVCo το διάγραμμα ροής μιας ανέπαφης συναλλαγής μέσω κινητής συσκευής απεικονίζεται στο σχήμα 5. Αρχικά, εκκινείτε η εφαρμογή, η οποία έχει επιλεχθεί από τον χρήστη για να εκτελέσει την συναλλαγή, και διαβάζονται τα δεδομένα της εφαρμογής (τρόπος λειτουργίας κ.α.). Στο επόμενο βήμα εκτελείται η διαχείριση ρίσκου της εφαρμογής παράλληλα με την αυθεντικοποιήση των δεδομένων πληρωμής, την επεξεργασία των περιορισμών που έχουν τεθεί από την εκάστοτε τράπεζα εκδότη και την αυθεντικοποιήση του κατόχου της πλαστικής κάρτας που αναπαριστάται από την εφαρμογή.

Με την ολοκλήρωση των παραπάνω εκτελείται μια ανάλυση στις πιθανές ενέργειες που θα εκτελέσει το τερματικό πληρωμής καθώς και τις αντίστοιχες της συσκευής. Σε περιπτώσεις όπου η

συσκευή δεν είναι συνδεδεμένη στο διαδίκτυο η συναλλαγή ολοκληρώνεται απευθείας με τον κωδικό του χρήστη που βρίσκεται αποθηκευμένος στη συσκευή. Σε περιπτώσεις όμως όπου η συσκευή είναι συνδεδεμένη στο διαδίκτυο εκτελείται μια on-line επεξεργασία και αυθεντικοποιήση του χρήστη προς την τράπεζα-εκδότη με την παροχή υπό την μορφή εισαγωγής κωδικού και έπειτα ολοκληρώνεται η ανέπαφη συναλλαγή.



Σχήμα 7: Διάγραμμα ροής εκτέλεσης μιας ανέπαφης συναλλαγής σύμφωνα με την EMVCo (EMVCo, 2015)

3 Αρχιτεκτονική Συστημάτων Πληρωμής

Σε συνέχεια του κεφαλαίου 2, το συγκεκριμένο κεφάλαιο επεξηγεί ολοκληρωμένα την αρχιτεκτονική που διέπει τα συστήματα διεκπεραίωσης ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών. Επεξηγείται το παρεχόμενο υλικό εντός των κινητών συσκευών που επιτρέπει την ασφαλή μεταφορά, αποθήκευση και επεξεργασία των ευαίσθητων τραπεζικών δεδομένων του χρήστη. Εν συνεχεία, επεξηγείται η βασική διαφοροποίηση και υλοποίηση που έχει υποστεί το τραπεζικό οικοσύστημα των ενχρήματων συναλλαγών με σκοπό την ενσωμάτωση των ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών με σκοπό την διατήρηση και την ενίσχυση της παρεχόμενης ασφάλειας. Επεξηγούνται όροι όπως το Tokenization, De-Tokenization, Key Vault και Payment Token καθώς και ο όρος της οντότητας του Token Service Provider σε συνδυασμό με τις παρεχόμενες υπηρεσίες του.

Οι ανέπαφες συναλλαγές μέσω κινητών συσκευών, οι οποίες ανήκουν στην κατηγορία των πληρωμών εγγύτητας καθώς βρίσκονται σε κοντινή απόσταση από το τερματικό πληρωμής, εκμεταλλεύονται την ήδη υπάρχουσα τραπεζική υποδομή για την εκτέλεση μιας συναλλαγής. Μια κινητή συσκευή με ικανότητες διασύνδεσης μέσω του NFC πρωτοκόλλου κάνει χρήση μιας εφαρμογής, συνήθως προερχόμενη από την τράπεζα εκδότη της πλαστικής κάρτας του χρήστη με σκοπό να επικοινωνήσει με το τερματικό πληρωμής και να εκτελέσει την συναλλαγή. Η εν λόγω εφαρμογή καθώς και τα δεδομένα του τραπεζικού λογαριασμού του χρήστη μεταφορτώνονται και αποθηκεύονται εντός μιας ασφαλούς περιοχής εντός της συσκευής, επονομαζόμενη Ασφαλές Περιβάλλον (Secure Element - SE). Η κινητή συσκευή με σκοπό να είναι σε θέση να επικοινωνήσει με το τερματικό πληρωμής του εμπόρου κάνει χρήση της εργοστασιακά ενσωματωμένης τεχνολογίας του πρωτοκόλλου NFC. Οι εσωτερικές διαδικασίες που εκτελούνται εντός και εκτός από την συσκευή με σκοπό την ολοκλήρωση της συναλλαγής είναι ακριβώς ίδιες με αυτές που ακολουθούνται με την εκτέλεση μιας ανέπαφης τραπεζικής συναλλαγής μέσω ανέπαφων πλαστικών καρτών (Massoth and Bingel, 2011).

Η αρχιτεκτονική των συστημάτων ανέπαφης συναλλαγής μέσω κινητών συσκευών βασίζεται στα παρακάτω συστατικά στοιχεία, τα οποία αναλύονται βαθύτερα στις παρακάτω ενότητες:

- Καταναλωτές.
- Έμποροι.
- Τράπεζα του εμπόρου.
- Πάροχος πληρωμών.
- Τράπεζα-εκδότης του χρήστη.

.

Καταναλωτές
Αποτελούν την ομάδα χρηστών που χρησιμοποιούν την κινητή συσκευή τους με σκοπό την εκτέλεση των ανέπαφων τραπεζικών συναλλαγών. Με το πέρασμα της κινητής συσκευής εντός του πεδίου που έχει δημιουργήσει το τερματικό πληρωμής πραγματοποιείται ανάγνωση των δεδομένων πληρωμής, των πληροφοριών του κατόχου της κάρτας, το ποσό πληρωμής καθώς και το παραγόμενο κλειδί πληρωμής που έχει δημιουργηθεί από την εφαρμογή πληρωμών που χρησιμοποιεί ο χρήστης, το οποίο αποκρύπτει το πραγματικό αριθμό λογαριασμό του χρήστη (Gomzin, 2014).

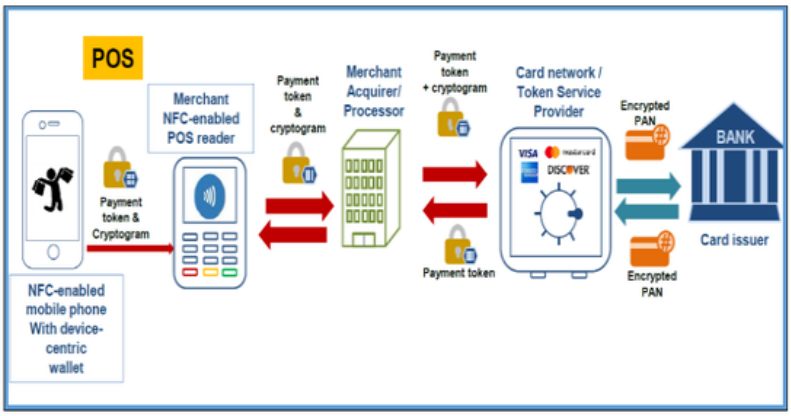
Έμποροι
Οι έμποροι αποτελούν κύρια οντότητα εντός της αρχιτεκτονικής των συστημάτων πληρωμής. Είναι υπεύθυνοι για την επιλογή του τύπου πληρωμής που αποδέχονται (επιλογή ανάμεσα σε χρεωστικές ή πιστωτικές συναλλαγές), τα χαρακτηριστικά των τερματικών πληρωμής που χρησιμοποιούν εντός της επιχείρησης τους κατευθυνόμενα είτε προς το λογισμικό των τερματικών πληρωμής είτε προς το υλικό των τερματικών καθώς και τον τρόπο με τον οποίο θα προστατεύσουν τα δεδομένα των χρηστών τους. Τα τερματικά πληρωμής που βρίσκονται υπό την κατοχή των εμπόρων είναι υπεύθυνα για την ανάγνωση και την επεξεργασία των δεδομένων πληρωμής που παραλαμβάνονται από την κινητή συσκευή, την αποστολή των δεδομένων στην τράπεζα στην οποία είναι καταχωρημένο το τερματικό πληρωμής και μέσω διαφόρων εσωτερικών διαδικασιών να παραλάβει ο έμπορος το χρηματικό ποσό

που αναλογεί στην αγορά των αγαθών (Massoth and Bingel, 2011).

Τράπεζα του εμπόρου
Η τράπεζα του εμπόρου είναι υπεύθυνη για τη εξουσιοδότηση των συναλλαγών πληρωμής και την ολοκλήρωση τους. Είναι υπεύθυνη για την δρομολόγηση των δεδομένων πληρωμής ανάλογα το ποσό πληρωμής και τον τύπο της αναπαριστώμενης κάρτας από την συσκευή του καταναλωτή προς την τράπεζα του μέσω του παρόχου υπηρεσιών κλειδιού λαμβάνοντας ταυτόχρονα το ποσό προμήθειας που έχει οριστεί (Massoth and Bingel, 2011).

Πάροχος υπηρεσιών κλειδιού
Αποτελεί μια ανεξάρτητη οντότητα εντός του τραπεζικού οικοσυστήματος με κύριο σκοπό ύπαρξης την αντικατάσταση του πραγματικού αριθμού λογαριασμού του χρήστη με μια ακολουθία αριθμών, το επονομαζόμενο κλειδί πληρωμής, με αποτέλεσμα την αποφυγή έκθεσης του αριθμού λογαριασμού του χρήστη στον έμπορο και την αποφυγή αποθήκευσης του σε ενδιάμεσους διακομιστές στο δίκτυο πληρωμών. Επιπρόσθετα είναι υπεύθυνος για την ασφαλή αποθήκευση της αντιστοίχισης του κλειδιού πληρωμής με τον αριθμό λογαριασμού καθώς και για την συνεχόμενη έκδοση και διατήρηση της λειτουργικότητας των κλειδιών πληρωμής (Gomzin, 2014).

Τράπεζα εκδότης
Αποτελούν τις οντότητες εκείνες που διατηρούν αρχεία για τους λογαριασμούς των χρηστών καθώς και την δημιουργία και την ενσωμάτωση των πλαστικών καρτών εντός των εξουσιοδοτημένων εφαρμογών των κινητών συσκευών. Επιπρόσθετα, εξουσιοδοτούν και χρεώνουν τους τραπεζικούς λογαριασμούς των χρηστών ανάλογα την αγορά και αποστέλλουν την εξουσιοδότηση ή την απόρριψη της συναλλαγής στο τερματικό πληρωμής του εμπόρου μέσω του ίδιου τραπεζικού δικτύου που εκτελέστηκε η ανέπαφη συναλλαγή (Massoth and Bingel, 2011).



Σχήμα 8: Αρχιτεκτονική Συστημάτων Διεκπεραίωσης Ανέπαφων Τραπεζικών Συναλλαγών μέσω Κινητών Συσκευών (Uspaymentsforum.org, 2018)

Σύμφωνα με το σχήμα 6, με σκοπό ο χρήστης να εκτελέσει την συναλλαγή μέσω της συσκευής θα πρέπει να προσεγγίσει το τερματικό πληρωμής εντός της ακτίνας λειτουργίας που επιτρέπει το πρωτόκολλο επικοινωνίας του NFC, δηλαδή περίπου 9 εκατοστά από το τερματικό πληρωμής. Ανάλογα το ποσό της συναλλαγής, δηλαδή αν η συναλλαγή είναι της κατηγορίας μίκρο (ποσά πληρωμής κάτω των 25 ευρώ) ή μάκρο (ποσά πληρωμής άνω των 25 ευρώ), ο χρήστης καλείται να πληκτρολογήσει στο τερματικό πληρωμής των κωδικό που έχει ορίσει κατά την διάρκεια ενεργοποίησης και σύζευξης του τραπεζικού λογαριασμού του στην εφαρμογή πληρωμών που έχει επιλέξει.

Στην συνέχεια, μέσω της εφαρμογής παράγεται το απαραίτητο κλειδί πληρωμής και ένα συνοδευόμενο κρυπτογράφημα τα οποία αποστέλλονται στο τερματικό πληρωμής του εμπόρου, το οποίο με την σειρά του προωθεί τα δεδομένα στην τράπεζα του. Έπειτα, η τράπεζα του εμπόρου αποστέλλει τα δεδομένα στην ενδιάμεση οντότητα μεταξύ της τράπεζας του εμπόρου και του χρήστη, τον λεγόμενο Πάροχο Πληρωμών (Token Service Provider - TSP), με σκοπό την αντιστοίχηση του παραγόμενου

από την εφαρμογή κλειδιού πληρωμής με τον πραγματικό αριθμό λογαριασμού του χρήστη και την αποστολή του στην τράπεζα του χρήστη. Η τράπεζα του χρήστη λαμβάνοντας την αίτηση για την συναλλαγή εξουσιοδοτεί ή απορρίπτει το αίτημα και αποστέλλει την απόφαση της μέσω του ίδιου δικτύου πληρωμής στην οθόνη του τερματικού πληρωμής του εμπόρου με σκοπό την εκτέλεση ή την απόρριψη της εν λόγω συναλλαγής (Uspaymentsforum.org, 2018).

Για να είναι ευρέως αποδεκτά τα συστήματα ανέπαφων συναλλαγών μέσω κινητών συσκευών από το ευρύ κοινό θα πρέπει να χαρακτηρίζονται από αποδοτικότητα, ταχύτητα και ένα αποδεκτό επίπεδο ασφάλειας των δεδομένων του χρήστη. Με σκοπό την ενίσχυση της ασφάλειας των εν λόγω συστημάτων δημιουργήθηκαν και ενσωματώθηκαν μηχανισμοί ασφάλειας τόσο στο τραπεζικό οικοσύστημα όσο και στην ίδια την συσκευή του χρήστη. Η ασφάλεια της αρχιτεκτονικής των συστημάτων πληρωμής μέσω κινητών συσκευών χωρίζεται σε δυο βασικούς πυλώνες:

- Η πρώτη κατηγορία στοχεύει στο διαθέσιμο υλικό των συσκευών, το οποίο καθιστά μια ανέπαφη συναλλαγή υλοποιήσιμη, σε συνδυασμό με ένα αποδοτικό επίπεδο ασφάλειας. Οι μηχανισμοί ασφάλειας τοποθετούνται από τον κατασκευαστή της κινητής συσκευής και διακατέχονται από την ικανότητα ασφαλούς εκτέλεσης ευαίσθητων διεργασιών καθώς και αποθήκευσης πληροφοριών. Οι μηχανισμοί είναι απομονωμένοι από το κύριο λειτουργικό σύστημα της συσκευής για την αποφυγή διαρροής δεδομένων σε μη ασφαλή επιμέρους συστατικά στοιχεία της συσκευής.
- Η δεύτερη κατηγορία αποτελείται από τους μηχανισμούς ασφάλειας που έχει δημιουργήσει και ενσωματώσει το ίδιο το τραπεζικό οικοσύστημα εντός των εφαρμογών πληρωμής καθώς και από την παραγόμενη ροή πληροφοριών που απορρέει από και προς τους μηχανισμούς αυτούς. Οι μηχανισμοί που έχουν οριστεί από το τραπεζικό οικοσύστημα έχουν ως σκοπό την απόκρυψη των δεδομένων της εισαγόμενης χρεωστικής ή πιστωτικής κάρτας καθ΄ όλη την διάρκεια των εκτελούμενων συναλλαγών.

Στα πλαίσια της παρούσας πτυχιακής δόθηκε περισσότερο βάρος στους μηχανισμούς που δημιουργήθηκαν και ενσωματώθηκαν στις κινητές συσκευές καθώς όπως προαναφέρθηκε οι αλλαγές που πραγματοποιήθηκαν στο ήδη υπάρχον τραπεζικό οικοσύστημα είναι ελάχιστες.

3.1 Παρεχόμενο Υλικό Εντός της Κινητής Συσκευής

Για να είναι σε θέση η κινητή συσκευή να εκτελέσει ανέπαφες συναλλαγές θα πρέπει να είναι εξοπλισμένη με ενσωματωμένους μηχανισμούς ασφάλειας, οι οποίοι να της ενισχύουν την ήδη παρεχόμενη ασφάλεια των δεδομένων πληρωμής. Για να θεωρηθεί η κινητή συσκευή κατάλληλη να εκτελέσει διεργασίες αποθήκευσης και εκτέλεσης ευαίσθητων δεδομένων θα πρέπει να διακατέχεται από έναν ή περισσότερους μηχανισμούς ενίσχυσης της ασφάλειας.

Οι πιο διαδεδομένοι μηχανισμοί είναι το ασφαλές περιβάλλον (Secure Element), το ασφαλές περιβάλλον εκτέλεσης εντολών (Trusted Execution Environment), η προσομοίωση του ασφαλούς περιβάλλοντος μέσω του κύριου επεξεργαστή της συσκευής (Software Card Emulation) και τέλος το Host Card Emulation, το οποίο κάνει χρήση ενός περιβάλλοντος νεφοϋπολογιστικής για την ασφαλή αποθήκευση των δεδομένων του χρήστη.

3.1.1 Secure Element

Ο συνδετικός κρίκος των συστημάτων αυτών αποτελεί το λεγόμενο Secure Element, ο ρόλος του οποίου αποτελεί την εκτέλεση του συνόλου των εντολών των εφαρμογών εκείνων που κάνουν χρήση του πρωτοκόλλου NFC.

Το Secure Element (SE) αποτελεί ένα ανθεκτικό στην παραβίαση μικροτσίπ, σύμφωνο με το ISO 7816 πρότυπο, το οποίο βρίσκεται ενσωματωμένο εντός της κινητής συσκευής και χρησιμοποιείται για την αποθήκευση και την φύλαξη ευαίσθητων δεδομένων. Μερικά από τα δεδομένα που είναι σε θέση να αποθηκεύσει το μικροτσίπ αποτελούνται από πληροφορίες χρεωστικών καρτών, διαπιστευτήρια εισόδου σε εγκαταστάσεις καθώς και ηλεκτρονικά εισιτήρια μέσων μαζικής μεταφοράς. Επίσης, είναι υπεύθυνο για την αποθήκευση και διαχείριση των κλειδιών πληρωμής σε περιπτώσεις προσομοίωσης πλαστικών καρτών. Το τσιπ αυτό διακατέχει τα ίδια υψηλά πρότυπα ασφάλειας με αυτά των ανέπαφων τραπεζικών καρτών. Δηλαδή, τα υψηλά κριτήρια ασφάλειας που τηρούνται στο Secure Element

τηρούνται και στα τσιπ των έξυπνων καρτών και των λειτουργικών τους συστημάτων.

Ίσως η πιο σημαντική λειτουργία που μπορεί να εκτελέσει το SE είναι μέσω του ελεγκτή του NFC της συσκευής. Το ασφαλές περιβάλλον μπορεί να συμπεριφερθεί και να προσομοιάσει πλήρως μια ανέπαφη κάρτα. Ο τομέας των πληρωμών (το σκέλος της τεχνολογίας NFC που προσφέρει την μεγαλύτερη ροή εσόδων) κάνει χρήση του ασφαλούς περιβάλλοντος της συσκευής για την εκτέλεση συναλλαγών. Ως αποτέλεσμα, όλο και περισσότερες εταιρίες θέλουν να αποκτήσουν πρόσβαση σε αυτό το περιβάλλον για μια θέση στην αγορά των ανέπαφων συναλλαγών.

Το συγκεκριμένο μικροτσίπ κρατείται κάτω από στενό έλεγχο από τους διαχειριστές των δικτύων πληρωμών καθώς και τους κατασκευαστές των συσκευών για ευνόητους λόγους. Ωστόσο, η προσομοίωση καρτών μέσω κινητών συσκευών είναι απαραίτητη για την αλληλεπίδραση με την πλειονότητα των συστημάτων RFID, τα οποία χρησιμοποιούνται για έλεγχους εισόδου, έκδοση εισιτήριων και διενέργεια πληρωμών. Τα συγκεκριμένα μικροτσίπ εκτός από μνήμη διακατέχουν την ικανότητα εκτέλεσης κρυπτογραφικών διεργασιών λόγω του ενσωματωμένου μικροεπεξεργαστή. Επιπλέον, έχουν την ικανότητα εκτέλεσης εντολών και διεργασιών καθώς και το απαραίτητο συνοδευόμενο υλικό, το οποίο είναι ειδικά κατασκευασμένο για την εκτέλεση κρυπτογραφικών διεργασιών (Vanderhoof et al., 2018) .

Διακατέχεται από τέσσερις (4) αρχιτεκτονικές λειτουργίας με διαφορετικό επίκεντρο η καθεμία. Κάθε διαφορετική αρχιτεκτονική βασίζεται και σε διαφορετικά συστατικά στοιχεία της κινητής συσκευής.

- **Πρώτη υλοποίηση**: Έχει ως επίκεντρο ένα ειδικά διαμορφωμένο μικροτσίπ εντός της κινητής συσκευής, το οποίο αποτελεί μια απομονωμένη ασφαλής ζώνη με ικανότητες αποθήκευσης ευαίσθητων πληροφοριών και δεδομένων. Επιπρόσθετα, το ασφαλές στοιχείο (Secure Element) εγγυάται την πρόσβαση στα αποθηκευμένα δεδομένα μόνο σε εξουσιοδοτημένους χρήστες και εφαρμογές. Η αρχιτεκτονική του μικροτσίπ δεν είναι σταθερή καθώς εντοπίζονται διαφοροποιήσεις από κατασκευαστή σε κατασκευαστή.

- **Δεύτερη υλοποίηση**: Βασίζεται στην κάρτα SIM που βρίσκεται εντός της συσκευής. Η συγκεκριμένη υλοποίηση αποτελεί έναν ασφαλή και αξιόπιστο τρόπο επαλήθευσης της ταυτότητας του χρήστη. Η κάρτα SIM μπορεί να συγκριθεί με το αντίστοιχο τραπεζικό μικροτσίπ, το οποίο βρίσκεται ενσωματωμένο στις πλαστικές κάρτες αναλήψεως, όσον αφορά την παρεχόμενη ασφάλεια και λειτουργικότητα.

  Χάρη στα παραπάνω χαρακτηριστικά, οικονομικά και τεχνολογικά ινστιτούτα εκμεταλλεύονται τις ήδη υπάρχουσες υποδομές των συστημάτων τηλεπικοινωνίας με κύριο σκοπό την ασφαλή αποθήκευση των δεδομένων των πλαστικών καρτών. Το μόνο μειονέκτημα της συγκεκριμένης υλοποίησης αποτελεί το γεγονός ότι δεν παρέχεται σε προγραμματιστές η πρόσβαση στις λειτουργίες της κάρτας SIM (Hillali Wadii et al, 2017).

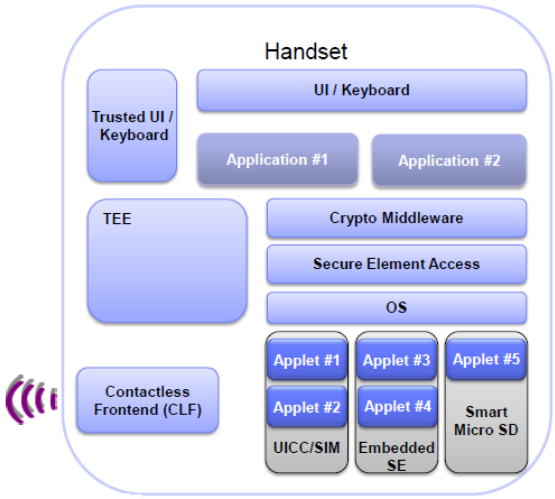
- **Τρίτη υλοποίηση:** Διαφοροποιείται στην δρομολόγηση των δεδομένων πληρωμής μεταξύ της κινητής συσκευής και του τερματικού πληρωμής. Στην συγκεκριμένη υλοποίηση τα δεδομένα πληρωμής δεν βρίσκονται αποθηκευμένα στην κινητή συσκευή αλλά έχουν δρομολογηθεί μέσω του μικροελεγκτή που ορίζει το πρωτόκολλο του NFC σε έναν εξωτερικό εξυπηρετητή, ο οποίος είναι υπεύθυνος για την αποθήκευση των στοιχείων της κάρτας του χρήστη. Αφού ληφθούν, οι απαραίτητες πληροφορίες από τον εξυπηρετητή τότε η κινητή συσκευή εκτελεί την ανέπαφη συναλλαγή (Smartcardalliance.org, 2014).

- **Τέταρτη υλοποίηση:** Είναι βασισμένη σε εξωτερικές μονάδες αποθήκευσης και προσφέρεται στους τελικούς χρήστες από συγκεκριμένους και εγκεκριμένους πάροχους. Η συγκεκριμένη υλοποίηση είναι περιορισμένη σε συγκεκριμένες βιομηχανικές εφαρμογές (Hillali Wadii, Boutahar and EL Ghazi, 2017).

3.1.2 Εναλλακτικές υλοποιήσεις του μικροτσίπ του SE

Με την εξέλιξη της τεχνολογίας τόσο στο επίπεδο του λογισμικού όσο και στο παρεχόμενο υλικό εντός των κινητών συσκευών, υπήρξαν προτάσεις για εναλλακτικές υλοποιήσεις του ασφαλούς περιβάλλοντος SE.
Όπως φαίνεται και στο σχήμα 9, τα επιμέρους στοιχεία που μπορούν να προσομοιάζουν σε ένα βαθμό

την ασφάλεια που παρέχει το SE είναι ο βασικός επεξεργαστής της συσκευής (Baseband Processor), ειδικά διαμορφωμένο και ενσωματωμένο υλικό (Embedded Hardware), μια αποσπώμενη κάρτα αποθήκευσης και τέλος μια αποσπώμενη έξυπνη κάρτα με τα ίδια χαρακτηριστικά ασφάλειας και λειτουργικότητας με την κάρτα SIM (Universal Integrated Circuit Card).



Σχήμα 9: Ανατομία κινητής συσκευής (Source: Global Platform)

.

Βασικός Επεξεργαστής - Baseband Processor

Ο βασικός επεξεργαστής, το σημαντικότερο κομμάτι της κινητής συσκευής, διαχειρίζεται την συνδεσιμότητα του κινητού καθώς και την λειτουργία των διαφόρων εφαρμογών. Παρέχοντας ένα υψηλό επίπεδο ασφάλειας έχει την ικανότητα υλοποίησης του SE εντός της μνήμης του επεξεργαστή.

Με αυτόν το τρόπο η αρχιτεκτονική του συστήματος της κινητής συσκευής δεν χρειάζεται περαιτέρω διαφοροποιήσεις για την υλοποίηση ασφαλών διεργασιών . Επιπλέον, με αυτή την υλοποίηση ο χρήστης δεν είναι αναγκασμένος να εισάγει κάποιου είδους εξωτερική συσκευή στο κινητό του για να κάνει χρήση των λειτουργιών που προσφέρει το SE. Όμως, σε περίπτωση απώλειας της κινητής συσκευής , το περιβάλλον του SE θα πρέπει να μην μπορεί να χρησιμοποιηθεί σε κάποια άλλη συσκευή (Reveilhac&Pasquet, 2009).

Ενσωματωμένο υλικό (Embedded Hardware)

Στις περιπτώσεις που το SE βρίσκεται ενσωματωμένο στο υλικό της κινητής συσκευής το επίπεδο ασφάλειας που προσφέρεται είναι του ιδίου επίπεδου με το επίπεδο ασφάλειας μιας πιστωτικής ή χρεωστικής κάρτας. Ανεξαρτήτως αυτού, η προσωποποίηση του μικροτσίπ που επιτρέπει τις ασφαλές λειτουργίες του SE γίνεται εκτός γραμμής παράγωγης και ενώ βρίσκεται στα χεριά του τελικού χρηστή. Καθώς, το μικροτσίπ βρίσκεται ενσωματωμένο στη συσκευή απαιτείται εκ νέου προσωποποίηση του τσιπ κάθε φορά που ο χρήστης αλλάζει συσκευή (Enisa,2018).

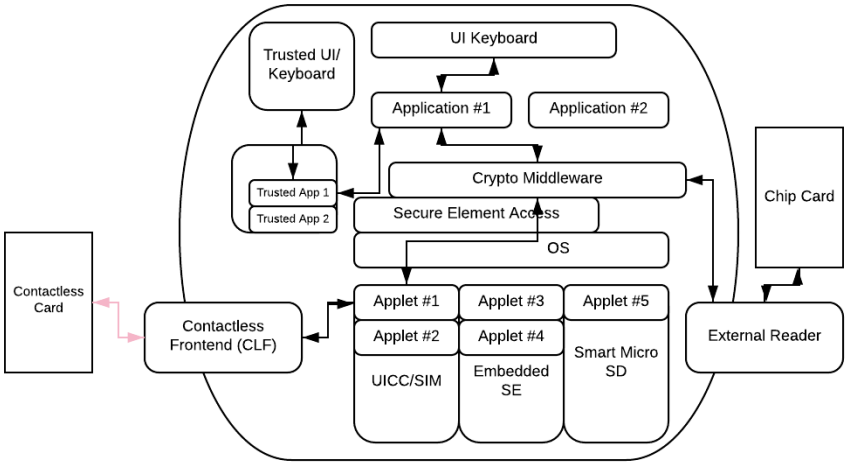
Ασφαλής κάρτα αποθήκευσης (Secure Memory Card-SMC)

Μια αποσπώμενη κάρτα αποθήκευσης αποτελεί τον συνδυασμό μιας ή περισσότερων μονάδων μνήμης καθώς και ένα μικρό ελεγκτή παρόμοιο με αυτό μιας έξυπνης κάρτας. Με αλλά λογία αποτελεί τον συνδυασμό μιας κάρτας μνήμης και μιας έξυπνης κάρτας.

Το συγκεκριμένο είδος αποσπώμενης κάρτας μνήμης διακατέχεται από το ίδιο υψηλό επίπεδο ασφάλειας των χρεωστικών ή πιστωτικών καρτών και είναι συμμορφούμενο με τις κύριες διεπαφές, περιβάλλοντα και πρότυπα με αυτά των έξυπνων καρτών (π.χ. EMV, Global Platform, ISO 7816, Java card). Λόγω της ικανότητας απόσπασης από την κινητή συσκευή και της μεγάλης περιεκτικότητας σε μνήμη, το SMC μπορεί να φιλοξενήσει ένα μεγάλο αριθμό εφαρμογών. Επίσης, εξαλείφεται η ανάγκη επανέκδοσης της κάρτας κάθε φορά που ο τελικός χρήστης αλλάζει συσκευή για διαφόρους λόγους. Έχει την ικανότητα εισαγωγής σε οποιαδήποτε συσκευή με ικανότητες NFC και δεν περιορίζεται από την κινητή συσκευή ή το λειτουργικό της (Reveilhac&Pasquet, 2009).

Universal Integrated Circuit Card-UICC
Αποτελεί μια αποσπώμενη έξυπνη κάρτα που εισέρχεται εντός της κινητής συσκευής. Αρχικά , ο κύριος σκοπός της ήταν η αντικατάσταση της κάρτας SIM καθώς κατέχει ικανότητες σύνδεσης τόσο στο κυψελιδικό δίκτυο τηλεφωνίας όσο και με τους πάροχους του.

Ως έξυπνη κάρτα είναι συμμορφούμενη με όλα τα πρότυπα που διέπουν τις έξυπνες κάρτες, διακατέχεται από το ίδιο επίπεδο ασφάλειας και μπορεί να φιλοξενήσει πολλαπλές εφαρμογές την ιδία στιγμή. Αυτό που την διαφοροποιεί από μια απλή κάρτα SIM είναι η ικανότητα φιλοξενίας εφαρμογών που διεκπεραιώνουν τραπεζικές συναλλαγές, έκδοση εισιτήριων και λειτουργούν ως διαδικτυακά διαβατήρια. Δημιουργήθηκε με σκοπό την αντικατάσταση του SE αλλά δεν υλοποιήθηκε επαρκώς λόγω μη συμβατών τεχνολογιών (Reveilhac&Pasquet, 2009).



Σχήμα 10: Διαφορετικές Υλοποιήσεις του SE (Reveilhac M. et al, 2009)

Στο σχήμα 10, αναλύεται με περισσότερη λεπτομέρεια η ανατομία της κινητής συσκευής και οι κινήσεις των δεδομένων ανάλογα την υλοποίηση του SE που ακολουθεί η συσκευή. Από την στιγμή που ενεργοποιείται ο μικροελεγκτής του NFC της συσκευής τα δεδομένα "ταξιδεύουν" μέσω κάποιας υλοποίησης του SE ή μέσω του ίδιου του SE. Έπειτα, τα δεδομένα έχοντας παραλλαχθεί ανάλογα τις απαιτήσεις και τις ενέργειες που απαιτεί η εφαρμογή που χρησιμοποιεί ο χρήστης την συγκεκριμένη χρονική περίοδο εμφανίζονται στην οθόνη της συσκευής.

Σε περιπτώσεις όπου γίνεται συνδυαστική χρήση του ασφαλούς περιβάλλοντος εκτέλεσης (TEE), τα δεδομένα εισέρχονται στο συγκεκριμένο περιβάλλον ασφαλίζονται ή δέχονται παραμετροποίηση περαιτέρω πριν εμφανιστούν στην οθόνη του χρήστη. Η παραπάνω διαδικασία είναι αμφίδρομη. Δηλαδή είτε ο χρήστης εκκινώντας μια εφαρμογή θέλει να χρησιμοποιήσει τον μικροελεγκτή του NFC είτε μέσω του μικροελεγκτή για την εμφάνιση αποτελεσμάτων και πιθανών ενεργειών του χρήστη.

3.1.3 Αναπαράσταση Ανέπαφης Κάρτας μέσω του Κυρίους Επεξεργαστή της Συσκευής - Software Card Emulation

Η τάση της μετάβασης από το ασφαλές περιβάλλον εκτέλεσης (SE) στον επεξεργαστή της κινητής συσκευής για την λειτουργία της αναπαράσταση έξυπνων καρτών δίνει την δυνατότητα σε μια εφαρμογή να μιμηθεί ένα NFC tag τύπου 4 (το πιο διαδεδομένο στην αγορά μικροτσίπ) και να ορίσει ένα NFC Data Exchange Format (NDEF) μήνυμα το οποίο αποθηκεύεται σε ένα εικονικό Tag.

Η ετικέτα τύπου 4 χειρίζεται αυτόματα από το λειτουργικό σύστημα της συσκευής. Το συγκεκριμένο είδος λειτουργίας μπορεί να χρησιμοποιηθεί για την ανταλλαγή δεδομένων με μια δεύτερη συσκευή , η οποία βρίσκεται σε κατάσταση λειτουργίας Read/Write. Επιπλέον, η εφαρμογή έχει την ικανότητα να μπορεί να αναπαραστήσει ένα ολοκληρωμένο ISO/IEC 14443-4 πρωτόκολλο επικοινω-

νίας. Η αναπαράσταση είναι εφικτή και για τους δυο τύπου καρτών, τύπου Α και τύπου Β αντίστοιχα (Roland, Michael 2012).

Επιπρόσθετα, είναι δυνατός ο προσδιορισμός των στατικών ιδιοτήτων της αναπαραχθείσας κάρτας όπως το μοναδικό αναγνωριστικό της (UID- Unique Identifier) και το ιστορικό συναλλαγών της. Έχει την πρόσθετη δυνατότητα της ανταλλαγής δεδομένων πρωτοκόλλου εντός του μπλοκ αναμετάδοσης έτσι όπως ορίζεται από το ISO/IEC 14443-4. Όταν μια εντολή καταφθάνει στην εφαρμογή που απαιτείται να έρθει σε επαφή με έναν εξωτερικό RFID/NFC αναμεταδότη εκτελείται μια μέθοδος επονομαζόμενη μέθοδος CallBack. Η εισερχόμενη εντολή καταχωρείται στην μέθοδο ως παράμετρος και γίνεται αντικείμενο επεξεργασίας με σκοπό να προμηθεύσει μια τιμή επιστροφής στον αναμεταδότη (Enisa, 2018).

Μειονεκτήματα και ανησυχίες ασφάλειας του Soft-SE

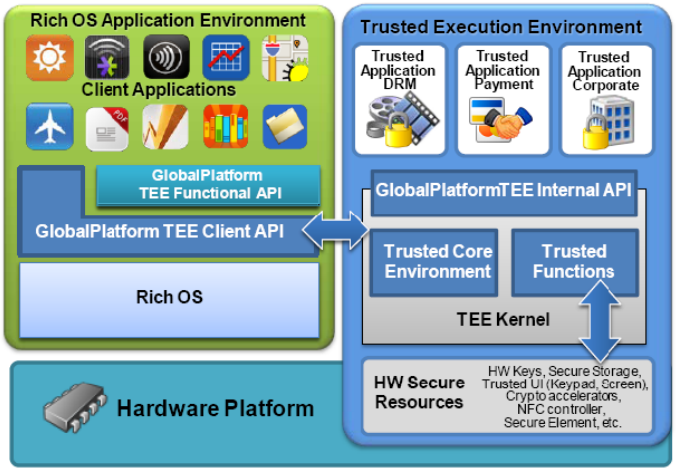
Τα πλεονεκτήματα που προσφέρει η αναπαράσταση καρτών με την μέθοδο soft-SE είναι εμφανή, δυστυχώς όμως δημιουργήθηκαν και τα ανάλογα μειονεκτήματα. Εξαιρώντας μικρές τεχνικές αδυναμίες, το κυριότερο μειονέκτημα αποτελεί η απώλεια ικανοποιητικού επίπεδου ασφάλειας. Εφαρμογές που εκτελούνται στον επεξεργαστή της κινητής συσκευής δεν επωφελούνται από την ύπαρξη της ασφαλούς αποθήκευσης και του ασφαλούς περιβάλλοντος εκτέλεσης εντολών. Χωρίς την ύπαρξη ασφαλούς αποθήκευσης δημιουργείται δυσκολία στην αποθήκευση ευαίσθητων πληροφοριών (διαπιστευτήρια εισόδου σε συστήματα, ιδιωτικά κλειδιά υπογραφής για συστήματα πληρωμών κ.α.). Επιπρόσθετα, η έλλειψη ασφαλούς περιβάλλοντος εκτέλεσης εντολών δημιουργεί ένα κενό ασφάλειας και επιτρέπει σε δεύτερες εφαρμογές να εμπλακούν.

Ακόμα ένα σοβαρό μειονέκτημα της χρήσης της επεξεργαστικής μονάδας της κινητής συσκευής είναι η ίδια η συσκευή που θα μπορούσε να λειτουργήσει ως πλατφόρμα επίθεσης. Έρευνες έχουν αποδείξει ότι δυο ή περισσότερες συσκευές με ικανότητες επικοινωνίας μέσω του πρωτοκόλλου NFC μπορούν να αναπαράγουν την μεταξύ τους επικοινωνία σε μεγαλύτερες αποστάσεις από αυτή των 10 εκατοστών που ορίζει το ίδιο το πρωτόκολλο. Συγκεκριμενοποιώντας, οι κινητές συσκευές διακατέχουν τις κατάλληλες δυνατότητες έτσι ώστε να μπορούν να προωθήσουν τα δεδομένα που ανταλλάσσονται μεταξύ τους μέσω των υπολοίπων πρωτοκόλλων επικοινωνίας (π.χ. Bluetooth, Wifi, GSMS κ.α.) (Enisa, 2018).

3.1.4 Ασφαλές περιβάλλον εκτέλεσης-Trusted Execution Environment

Το ασφαλές περιβάλλον εκτέλεσης εντολών (Trusted Execution Environment) αποτελεί μια ασφαλή περιοχή εντός είτε του κύριου επεξεργαστή είτε κάποιου βοηθητικού, με ιδιαίτερο γνώρισμα την ασφαλή αποθήκευση και επεξεργασία δεδομένων. Το TEE αποτελεί μια μίξη λογισμικού και υλικού προσφέροντας προστασία εναντία σε επιθέσεις που απορρέουν από το λειτουργικό σύστημα της κινητής συσκευής (Rich OS). Αποτελεί επίσης, ένα τμηματοποιημένο ασφαλές περιβάλλον εκτέλεσης εντολών, το όποιο παρέχει μεγαλύτερη χρηστικότητα από το SE. Μια ολόκληρη εφαρμογή μπορεί να εκτελεστεί εντός του TEE και να κάνει χρήση του περιβάλλοντος SE καθώς και άλλες λειτουργίες της κινητής συσκευής με υψηλό βαθμό ακεραιότητας και εμπιστευτικότητας.

Τα χαρακτηριστικά που διακατέχει το TEE είναι η ασφαλής εκτέλεση των ευαίσθητων εντολών και κλάσεων μιας εφαρμογής. Παραδείγματος χάρη, η αποθήκευση δεδομένων και οι τεχνικές αυθεντικοποίησης και ταυτοποίησης δεδομένων του χρηστή είναι δυο από τις λειτουργίες που εκτελούνται εντός του TEE(Security of Mobile Payments and Digital Wallets, 2018).
Επιπλέον γνώρισμα αποτελεί το γεγονός ότι το TEE λειτουργεί με βάση το δικό του λειτουργικό σύστημα με αποτέλεσμα να μην επηρεάζεται από τυχόν αλλαγές στο λειτουργικό σύστημα της συσκευής. Επίσης, το TEE μπορεί να λειτουργήσει παράλληλα με το SE για την παροχή ασφάλειας (Smartcardalliance.org, 2014).

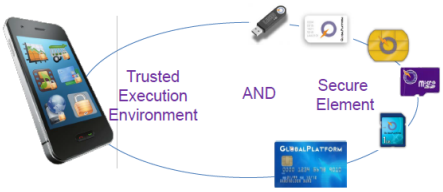


Σχήμα 11: Ανατομία Περιβάλλοντος Εκτέλεσης TEE (Source: Global Platform)

Όπως φαίνεται και στην εικόνα 9, το TEE διακατέχεται από διαφορετικό λειτουργικό σύστημα από αυτό της συσκευής. Μπορεί να εκτελέσει με υψηλό επίπεδο ασφάλειας εφαρμογές που χειρίζονται πνευματικά δικαιώματα του χρήστη, συναλλαγές ανέπαφες και μη καθώς και εταιρικές πληροφορίες.

Επιπρόσθετα, το TEE εκτός την δυνατότητα ασφαλούς αποθήκευσης δεδομένων μπορεί να εκτελέσει και κρυπτογραφικές και άλλες διαδικασίες χάρη στον πυρήνα του λειτουργικού και στο παρεχόμενο υλικό. Όσον αφορά το λειτουργικό σύστημα του περιβάλλοντος περιλαμβάνει το ασφαλές περιβάλλον πυρήνα καθώς και το σύνολο των έμπιστων διαδικασιών και λειτουργιών.

Το υλικό που απαιτεί η κάθε διαδικασία και λειτουργία που τρέχει εντός του TEE "κλειδώνεται" και δεν μπορεί να χρησιμοποιηθεί από το κυρίως λειτουργικό. Παραδείγματος χάρη, αν κάποια εφαρμογή που τρέχει εντός του περιβάλλοντος απαιτήσει από τον χρήστη να αυθεντικοποιηθεί μέσω βιομετρικών μεθόδων τότε μόνο το περιβάλλον ασφαλούς εκτέλεσης μπορεί να χρησιμοποιήσει τον βιομετρικό μηχανισμό.



Σχήμα 12: Κύκλος Πιθανών Υλοποιήσεων (Source: Global Platform)

Το σχήμα 12 υποδηλώνει τους πιθανούς συνδυασμούς του TEE με μεθόδους και τεχνικές ασφαλούς αποθήκευσης δεδομένων. Μερικοί από τους συνδυασμούς είναι η χρήση του TEE είτε με το SE είτε με την κάρτα SIM είτε με κάποια εξωτερική μονάδα αποθήκευσης. Όλοι οι διαφορετικοί συνδυασμοί στοχεύουν στην περαιτέρω ενίσχυση του επιπέδου ασφάλειας.

Πλεονεκτήματα του Ασφαλούς Περιβάλλοντος Εκτέλεσης

1. Κάνει χρήση της μνήμης της συσκευής, η όποια ασφαλίζεται μέσω ενός κρυπτογραφικού επεξεργαστή.
2. Είναι αποδεκτό από το λειτουργικό σύστημα των Android συσκευών και από ποικίλα πρωτοκολλά (π.χ. FIDO).
3. Η αποθήκευση των κλειδιών μπορεί να γίνει εντός του SE ή κάποιου παρεμφερές υλικού στοιχείου του συστήματος, το όποιο προσφέρει αποδεκτό επίπεδο ασφάλειας.
4. Υπάρχουν καλά ορισμένες προδιαγραφές για την ασφαλή διεπαφή χρηστή και για την ασφαλή αποθήκευση δεδομένων.

5. Οι μηχανισμοί ασφάλειας του είναι εγκεκριμένοι από τον οργανισμό Global Platform.

6. Προσφέρει απομόνωση μνήμης.

7. Προσφέρει κρυπτογραφική επιβεβαίωση και απομόνωση του συνόλου του εκτελούντος κώδικα εντός του περιβάλλοντος εκτέλεσης.

8. Αποτελεί ένα μικρό TCB , το οποίο είναι ευκολότερα διαχειρίσιμο από το Rich Os της συσκευής.

Μειονεκτήματα του Ασφαλούς Περιβάλλοντος Εκτέλεσης

1. Αποτελεί ένα περιορισμένο περιβάλλον εκτέλεσης, στο όποιο η είσοδος σε αυτό απαιτεί τις ενέργειες του κατασκευαστή.

2. Η διαχείριση του κύκλου ζωής απαιτεί έμπιστα και ασφαλή συστήματα.

(Smartcardalliance.org, 2017, Beniamini, 2017)

3.1.5 Προσομοίωση Πλαστικών Καρτών - Host Card Emulation (HCE)

Όσο γίνεται χρήση της λειτουργίας του HCE από κάποια εφαρμογή ηλεκτρονικών πληρωμών, η επικοινωνία μεταξύ της κινητής συσκευής και του τερματικού πληρωμής δεν δρομολογείται πλέον στο μικροτσίπ εντός της κινητής συσκευής αλλά μέσω του μικρό ελεγκτή που ορίζει το πρωτοκόλλου NFC. Έπειτα, ο μικροελεγκτής αποστέλλει τις πληροφορίες στην επεξεργαστική μονάδα του εξυπηρετητή που βρίσκεται εκτός της συσκευής.

Ο παρών μηχανισμός δεν αποτελεί κάποιο μηχανισμό ασφάλειας αλλά απεναντίας επιτρέπει την δρομολόγηση των εντολών και των δεδομένων, που απορρέουν από το πρωτόκολλο του NFC, από κάποια εφαρμογή που λειτουργεί εντός του λειτουργικού συστήματος προς έναν εξωτερικό εξυπηρετητή αντί να δρομολογούνται απευθείας μέσω του SE. Η συγκεκριμένη ανταλλαγή πληροφοριών είναι αμφίδρομη.

Η χρήση του HCE δεν ορίζει που αποθηκεύονται τα διαπιστευτήρια και τα ευαίσθητα δεδομένα ούτε τον τρόπο με τον όποιο επεξεργάζονται. Επίσης, δεν ορίζει τεχνικές ασφάλειας όποτε το οποιοδήποτε μετρό ασφάλειας πρέπει να οριστεί και να υλοποιηθεί πάνω στην υλοποίηση του HCE (Securetechalliance.org, 2015).

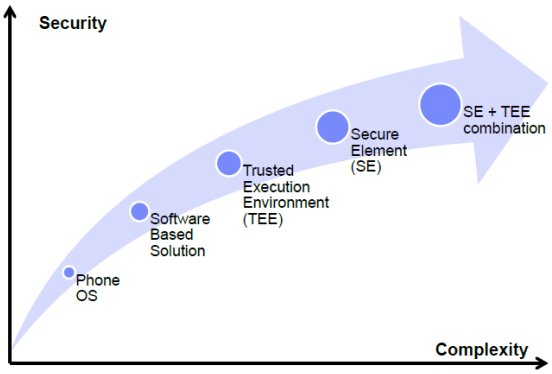
Η συγκεκριμένη υλοποίηση όμως είναι πιθανόν να εμπεριέχει κινδύνους όσον αφορά την ασφάλεια των δεδομένων καθώς η επικοινωνία μεταξύ της συσκευής και του περιβάλλοντος νεφοϋπολογιστικής που την υποστηρίζει μπορεί να μολυνθεί από κακόβουλες εφαρμογές. Οι εν λόγω εφαρμογές μπορούν να επιτεθούν στο λειτουργικό σύστημα της συσκευής ειδικότερα αν η συσκευή έχει υποστεί JailBreak ή βρίσκεται σε κατάσταση Rooted λειτουργίας. Επιπρόσθετα, είναι πιθανό η ίδια η κακόβουλη εφαρμογή να φέρει την κινητή συσκευή στις παραπάνω καταστάσεις.
Παραδείγματος χάρη,τα σενάρια επιθέσεων άρνησης εξυπηρέτησης μπορούν να εκτελεστούν αν μια κακόβουλη εφαρμογή αποκτήσει τον έλεγχο της συσκευής.

Προτείνεται η χρήση του HCE να ακολουθείται και από άλλες τεχνικές ασφάλειας όπως η κρυπτογράφηση, η διαδικασία του Tokenization, η συσκότιση κώδικα ή κρυπτογραφία τύπου White Box. Επίσης, το ρίσκο έκθεσης των δεδομένων μπορεί να μειωθεί κάνοντας χρήση των αντιμέτρων που έχουν οριστεί σε επίπεδο συστήματος (Securetechalliance.org, 2015).
Επιθυμητός είναι ο συνδυασμός του HCE με το SE ή το TEE για την ενδυνάμωση της παρεχομένης ασφάλειας (Vanderhoof et al., 2018).

Τα μέτρα που μπορούν να χρησιμοποιηθούν για να διασφαλίσουν περαιτέρω την ασφάλεια των συναλλαγών που διεκπεραιώνονται μέσω κινητών συσκευών που δεν κάνουν χρήση του ασφαλούς περιβάλλοντος (SE) είναι:

- Κρυπτογραφία τύπου white Box
- Απαραβίαστο λογισμικό
- Βιομετρική επαλήθευση χρήστη
- Μεθόδους επαλήθευσης της κινητής συσκευής

- Ασφαλή περιβάλλοντα εκτέλεσης εντολών/ Frameworks ενίσχυσης ασφάλειας
- Κρυπτογράφηση δεδομένων
- Tokenization
- Επιπρόσθετα χαρακτηριστικά ασφάλειας παρεχόμενα από το μικροτσίπ του SE



Σχήμα 13: Ταξινόμηση Μεθόδων Ασφάλειας (Enisa, 2018)

Όπως φαίνεται και στο σχήμα 13 με το πέρασμα του χρόνου και την αύξηση των απαιτήσεων ασφάλειας των εφαρμογών, η πολυπλοκότητα των μεθόδων ασφάλειας έχει αυξηθεί αναλογικά με την παρεχόμενη ασφάλεια.

Οι εφαρμογές που δεν απαιτούν υψηλό ποσοστό ασφάλειας κάνουν χρήση μόνο του λειτουργικού συστήματος της συσκευής ενώ αντίθετα εφαρμογές που απαιτούν υψηλό επίπεδο ασφάλειας κάνουν χρήση εξειδικευμένων εργαλείων και ξεχωριστού περιβάλλοντος εκτέλεσης. Η αύξηση της πολυπλοκότητας στις εκτελούμενες διεργασίες έχει αντίκτυπο στα υπόλοιπα συστατικά στοιχεία της συσκευής (π.χ. υψηλές απαιτήσεις ενέργειας).

Αναλυτικότερα, τα μέτρα που μπορούν να χρησιμοποιηθούν για την ενδυνάμωση των συναλλαγών που διεκπεραιώνονται μέσω κινητών συσκευών μέσω της διαδικασίας του HCE και δεν κάνουν χρήση του SE είναι τα παρακάτω:

- **Κρυπτογραφία White Box**
  Οι κρυπτογραφικές μέθοδοι τέτοιου τύπου είναι μια μορφή συσκότισης που αφορά ντετερμινιστικούς αλγορίθμους. Χρησιμοποιούνται για την μείωση της έκθεσης κρυφών δεδομένων στο κύριο σώμα του κώδικα της εφαρμογής ή στην μνήμη της συσκευής.
  Γενικότερα, οι μέθοδοι αυτοί κρύβουν τα δεδομένα εντός του κώδικα με τέτοιο τρόπο ώστε να μην μπορούν να ανακτηθούν από αυτόν κάνοντας την ανάκτηση πληροφοριών αρκετά πιο δύσκολη και χρονοβόρα.

- **Απαραβίαστο λογισμικό**
  Λογισμικό ανθεκτικό έναντι παραβιάσεων είναι μια προσθήκη ασφάλειας λογισμικού με σκοπό την αύξηση της δυσκολίας παραβίασης ή τροποποίησης του λογισμικού είτε στατικά είτε δυναμικά απέναντι σε μια πιθανή επίθεση.

  Με κύριο σκοπό της ασφάλεια του λειτουργικού συστήματος χρησιμοποιούνται επιπρόσθετοι μέθοδοι ασφάλειας όπως η συσκότιση κώδικα, η άμυνα με χρήση Breakpoints καθώς και Anti-Bug εργαλεία. Από την στιγμή που το σύστημα ανακαλύψει μια επίθεση αναγκάζει τον ίδιο του τον εαυτό να υπολειτουργήσει και να διαγράψει τα δεδομένα του με αποτέλεσμα την αδυναμία σωστής εκτέλεσης της επίθεσης εναντία στο σύστημα (Smartcardalliance.org, 2014).

- **Βιομετρική επαλήθευση χρήστη**
  Οι μέθοδοι βιομετρικής επαλήθευσης μπορούν να χρησιμοποιηθούν για την ενδυνάμωση της

διαδικασίας επαλήθευσης της ταυτότητας του χρηστή για εφαρμογές HCE σε συνδυασμό με άλλους τρόπους ενδυνάμωσης.

Το κύριο πλεονέκτημα της χρήσης βιομετρικών μηχανισμών επαλήθευσης είναι η οικειότητα που προσφέρει στον τελικό χρηστή σε αντίθεση με την εισαγωγή πολλαπλών κωδικών. Οι επικρατέστερες εκδοχές βιομετρικής επαλήθευσης, οι οποίες χρησιμοποιούνται ευρέως από τους χρήστες, αποτελούνται από το δαχτυλικό αποτύπωμα του χρήστη, την αναγνώριση του προσώπου του καθώς και την αναγνώριση της φωνητικής συχνότητας της ομιλίας του.

- **Μέθοδοι επαλήθευσης της κινητής συσκευής**
Μέθοδοι επαλήθευσης συσκευής έχουν την ικανότητα να επαληθεύουν την ταυτότητα της συσκευής μέσω διαδικτυακών διεργασιών. Ένα πλήθος λύσεων είναι διαθέσιμο στην υποστήριξη της επαλήθευσης της κινητής συσκευής και μπορούν να προσδώσουν ένα επιπλέον επίπεδο ασφάλειας σε εφαρμογές βασισμένες στο μοντέλο του HCE (Securetechalliance.org, 2015).

Τέτοιο παράδειγμα αποτελεί το λεγόμενο Fast Identity Online (FIDO). Η συγκεκριμένη υλοποίηση ασφάλειας κάνει χρήση κρυπτογραφικών μεθόδων δημόσιου κλειδιού για την επαλήθευση της ταυτότητας του χρηστή σε πραγματικό χρόνο. Από την στιγμή που ο χρήστης εκκινεί την εφαρμογή που χρησιμοποιεί την μέθοδο FIDO δημιουργείται ένα καινούργιο ζευγάρι κλειδιών, κρατώντας το μυστικό κλειδί εντός της συσκευής και καταχωρώντας το δημόσιο κλειδί στην διαδικτυακή υπηρεσία.

Η κινητή συσκευή επαληθεύει τον εαυτό της κατά την έξοδο από την εφαρμογή όπου χρησιμοποιείται το ιδιωτικό κλειδί που με απαραίτητη προϋπόθεση την εισαγωγή του κωδικού της συσκευής ή την βιομετρική επαλήθευση του χρήστη (Smartcardalliance.org, 2014, Securetechalliance.org, 2017).

- **Ασφαλή περιβάλλοντα εκτέλεσης εντολών/ Frameworks ενίσχυσης ασφάλειας**
Το ασφαλές περιβάλλον εκτέλεσης εντολών (Trusted Execution Environment) αποτελεί μια ασφαλή περιοχή εντός είτε του κύριου επεξεργαστή είτε κάποιου βοηθητικού , με ιδιαίτερο γνώρισμα την ασφαλή αποθήκευση και επεξεργασία δεδομένων.

Το TEE αποτελεί μια μίξη λογισμικού και υλικού προσφέροντας προστασία εναντία σε επιθέσεις που απορρέουν από το λειτουργικό σύστημα της κινητής συσκευής (Rich OS). Μπορεί να λειτουργήσει παράλληλα με το SE για την παροχή ασφάλειας. Επιπλέον γνώρισμα αποτελεί το γεγονός ότι το TEE λειτουργεί με βάση το δικό του λειτουργικό σύστημα με αποτέλεσμα να μην επηρεάζεται από τυχόν αλλαγές στο λειτουργικό σύστημα της ιδίας της συσκευής.

Συνδυαστικά, εφαρμογές που λειτουργούν με βάση το HCE προσφέρουν επιπλέον επίπεδα ασφάλειας υπό την μορφή των παρακάτω.

1. **Εισαγωγή κωδικού πρόσβασης/PIN:** Επιτρέπεται η ασφαλής εισαγωγή του κωδικού πρόσβασης καθώς το TEE έχει την ικανότητα εισαγωγής κωδικού σε εντελώς ξεχωριστό κομμάτι λόγω του διαφορετικού λειτουργικού, η όποια εισαγωγή δεν μπορεί να ανακτηθεί από κάποιο κακόβουλο πρόγραμμα το όποιο μπορεί να έχει προσβάλει το λειτουργικό σύστημα της συσκευής.
2. **Ασφαλής αποθήκευση διαπιστευτηρίων:** Καθιστά δυνατή την ασφαλή αποθήκευση κλειδιών καθώς οι κρυπτογραφικές μέθοδοι που χρησιμοποιούνται στα δεδομένα εκτελείται εντός του ασφαλούς περιβάλλοντος εκτέλεσης αποκλείοντας την έκθεση τους από κάποια ευπάθεια στο λειτουργικό σύστημα της συσκευής.
3. **Ασφαλές πρωτόκολλο μεταφοράς από άκρο σε άκρο:** Καθώς είναι επιτρεπτή η φόρτωση εμπίστων εφαρμογών (Trusted Applications) και δεδομένων κρυπτογράφησης στο ασφαλές περιβάλλον εκτέλεσης καθίσταται δυνατή η εγκαθίδρυση ενός ασφαλούς καναλιού επικοινωνίας από άκρο σε άκρο μεταξύ του τερματικό πληρωμής και το ίδιο το TEE. Αυτό σημαίνει ότι οι εντολές που μεταφέρονται από το τερματικό πληρωμής μέσω της ανέπαφης διεπαφής μπορούν να μεταφερθούν εντός του TEE προστατεύοντας έτσι την ακεραιότητα και την ιδιωτικότητα των δεδομένων πληρωμής.

Επίσης είναι δυνατή και η απευθείας επικοινωνία του TEE με τους διακομιστές που βρίσκονται σε περιβάλλοντα νεφοϋπολογιστικής χωρίς την έκθεση των κλειδιών πληρωμής στο λειτουργικό της κινητής συσκευής. Το μόνο μειονέκτημα του TEE αποτελεί το γεγονός ότι δεν διακατέχεται από το ίδιο επίπεδο ανθεκτικότητας εναντία σε πιθανές επιθέσεις όπως είναι το SE .

3.2 Μηχανισμοί Τραπεζικού Οικοσυστήματος

Στο παρών κεφάλαιο αναφέρονται οι μηχανισμοί ασφαλείας που έχουν δημιουργηθεί και ενσωματωθεί τόσο στο τραπεζικό οικοσύστημα όσο και στις ίδιες τις κινητές συσκευές για την εκτέλεση ανέπαφων τραπεζικών συναλλαγών.

Οι μηχανισμοί αυτοί έχουν ως σκοπό την ενίσχυση της ασφάλειας των δεδομένων του χρήστη από την στιγμή που τα δεδομένα "άπελευθερωθούν" εντός του τραπεζικού δικτύου. Αναφέρεται και εξηγείται η μέθοδος του Tokenization και De-Tokenization καθώς και η χρησιμότητα της. Επιπρόσθετα, αναλύεται και εξηγείται περαιτέρω το κλειδί πληρωμής καθώς και ο ρόλος του εντός του τραπεζικού οικοσυστήματος. Τέλος αναλύεται εκτενώς ο ρόλος και οι αρμοδιότητες του πάροχου υπηρεσιών κλειδιού Token Service Provider (TSP).

3.2.1 Μέθοδος Tokenization

Tokenization ονομάζεται η διαδικασία αντικατάστασης του Personal Account Number (PAN), το οποίο διαθέτουν όλες οι πλαστικές τραπεζικές κάρτες (χρεωστικές και πιστωτικές), με μια παρεμφερή ακολουθία αριθμών που αναπαριστά τον λογαριασμό τραπέζης του χρήστη.

Η συγκεκριμένη ακολουθία αριθμών ονομάζεται Payment Token και διατηρεί όλες τις απαραίτητες πληροφορίες για την διεκπεραίωση μιας συναλλαγής αυξάνοντας όμως την ασφάλεια τόσο των συναλλαγών όσο και του τελικού χρήστη καθώς η ακολουθία αυτή μπορεί να χρησιμοποιηθεί μόνο εντός του συστήματος για το οποίο δημιουργήθηκε. Τα δεδομένα αυτά δεν διακατέχουν σημασία άξια εκμετάλλευσης εκτός του περιβάλλοντος στο οποίο ορίστηκαν (Security of Mobile Payments and Digital Wallets, 2018).
Οι τιμές των Token ποικίλουν στην μορφή και έχουν την ικανότητα να δημιουργούνται από κρυπτογραφικές ή μη γεννήτριες τιμών ανάλογα τον τύπο και την χρήση τους. Τα Tokens αποθηκεύονται και χαρτογραφούνται εντός ενός ασφαλούς κεντρικοποιημένου συστήματος που ονομάζεται Token Vault.

Οι βασικές λειτουργίες του Tokenization είναι τρεις:

1. Έκδοση και παροχή αριθμού Token
2. Επεξεργασία συναλλαγών
3. Διασυνδέσεις με άλλα συστήματα - Application Programming Interfaces (APIs)

Όπως γίνεται κατανοητό για την υλοποίηση των παραπάνω διαδικασιών καθίσταται αναγκαία η ύπαρξη ενός νέου πάροχου, ο οποίος θα είναι επιφορτισμένος με την εκτέλεση αυτών των υπηρεσιών και ονομάζεται Token Service Provider (TSP).

Ο TSP μπορεί να λειτουργεί είτε μέσω των έκδοτων των καρτών (τράπεζες), είτε μέσω των οργανισμών των καρτών (Visa, MasterCard, AmEx κ.α.) ή ακόμα και μέσω ενός τρίτου φορέα, ο οποίος μπορεί να είναι τελείως ανεξάρτητος (Παπαδόπουλος, 2015).

3.2.2 Tokenization VS Encryption

Από την σκοπιά της ασφάλειας, η διαδικασία του Tokenization ενισχύει την ασφάλεια των δεδομένων του χρήστη με εντελώς διαφορετικό τρόπο από αυτόν της κρυπτογράφησης. Η κρυπτογράφηση περιπλέκει τα δεδομένα χρησιμοποιώντας ένας αλγόριθμο κρυπτογράφησης σε συνδυασμό με κρυπτογραφικά κλειδιά για την προστασία των δεδομένων. Η διαδικασία της κρυπτογράφησης αποτελεί την καλύτερη λύση για την διασφάλιση της εμπιστευτικότητας των δεδομένων και προστατεύει τα δεδομένα μόνο όταν αυτά είναι κρυπτογραφημένα.

Κατά την διάρκεια της επεξεργασίας των δεδομένων πληρωμής, για να είναι δυνατή η χρήση των κρυπτογραφημένων δεδομένων θα πρέπει πρώτα να αποκρυπτογραφηθούν, να επεξεργαστούν και μετέπειτα να κρυπτογραφηθούν ξανά.
Όπως είναι λογικό κατά την διάρκεια της αποκρυπτογράφησης τα δεδομένα βρίσκονται εντελώς εκτεθειμένα και ευαίσθητα εναντία σε επιθέσεις.

Σε αντίθεση, η διαδικασία του Tokenization αντικαθιστά τα ευαίσθητα δεδομένα με εναλλακτικά μη ευαίσθητα, τα όποια δεν μπορούν να χρησιμοποιηθούν έξω από το περιβάλλον από το όποιο ορίστηκαν. Μόνο η σύνδεση μεταξύ των Token και των αρχικών δεδομένων είναι ευαίσθητη σε επιθέσεις. Όμως η σύνδεση αυτή είναι αποθηκευμένη εντός του ασφαλούς κεντρικοποιημένου συστήματος που ονομάζεται Token Vault (Enisa,2018).

Πλεονεκτήματα της μεθόδου Tokenization

Τα πλεονεκτήματα της μεθόδου αυτής βασίζονται σε δυο κυρίους πυλώνες:

1. **ID&V**: Προσφέρει μεθόδους εμπιστευτικής σύνδεσης και επαλήθευσης μεταξύ του Token πληρωμής και του αριθμού λογαριασμού προσφέροντας ένα εύρος χρήσης ανάλογα τις απαιτήσεις του χρηστή.
2. **Token Domain Controls:**
    - Απαγορεύει την χρήση του Token για μη ορισμένους τομείς.
    - Ο τομέας μπορεί να είναι βασισμένος στο κανάλι επικοινωνίας ή στον έμπορο και απαιτεί δυναμικά ορισμένα δεδομένα σε συνδυασμό με το Token για να διεκπεραιωθεί η συναλλαγή.
    - Δεν είναι απαραίτητη η ύπαρξη όλων των περιορισμών για να μπορέσει να λειτουργήσει το σύστημα πληρωμών.

Π.χ. Ένα Token μπορεί να επιτρέπει την διεκπεραίωση συναλλαγών Tap-and-Go ενώ ένα άλλο σύστημα να επιτρέπει συναλλαγές μέσω του ενσωματωμένου μικροτσίπ της κάρτας σε συνδυασμό με την ύπαρξη ενός κρυπτογραφήματος. (Παπαδόπουλος, 2015)

Επιπλέον προνομία ασφάλειας της μεθόδου Tokenization

1. **Περιορισμός στον πολλαπλασιασμό των αριθμών λογαριασμού**
    - Καθώς αυξάνονται σε αριθμό οι συσκευές που χρησιμοποιούνται για αγορές, η αποθήκευση των αριθμών λογαριασμού σε όλες τις συσκευές αποτελεί πιθανό κίνδυνο έκθεσης του λογαριασμού.
    - Η διαδικασία του Tokenization επιλύει το συγκεκριμένο πρόβλημα με την έκδοση συγκεκριμένων Token για συγκεκριμένες συσκευές και σκοπούς εξαλείφοντας έτσι την έκθεση του λογαριασμού στον έμπορο.
2. **Διαχείριση Token σε πραγματικό χρόνο.**
    - Η ικανότητα διαγραφής και παύσης ενός Token από μια συσκευή επιτρέπει την περαιτέρω προστασία του λογαριασμού του χρηστή σε περίπτωση κλοπής της συσκευής του. Καθώς διαφορετικά Token μπορούν να τοποθετηθούν σε διαφορετικές συσκευές όταν μια συσκευή εκτεθεί μόνο αυτή η συσκευή χρειάζεται να απενεργοποιηθεί. Έτσι, οι υπόλοιπες καταχωρημένες συσκευές δεν επηρεάζονται (European Payments Council, 2017).

Στον πίνακα 1, αναφέρονται οι κυριότερες διαφορές στις παρεχόμενες υπηρεσίες μεταξύ κρυπτογράφησης και Tokenization σε περιπτώσεις ανέπαφων συναλλαγών.

3.2.3 Μέθοδος De-Tokenization

Αποτελεί την αντίστροφη διαδικασία και επιτρέπει την επιστροφή του Token στην αρχική του μορφή και σημασία. Ο TSP αποτελεί την οντότητα εκείνη που είναι επιφορτισμένη με τις παραπάνω υπηρεσίες.

Τα χαρακτηριστικά που διακατέχουν την διαδικασία αυτή είναι (Securetechalliance.org, 2015):

Tokenization	Encryption
Χρήση του Token για την προστασία των δεδομένων	Χρήση μυστικών κλειδιών για την προστασία των δεδομένων
Τα Token αποτελούν μια αναφορά των πραγματικών δεδομένων	Χρήση αλγορίθμων για την μετατροπή των δεδομένων σε μη ευανάγνωστο κείμενο
Χρήση του Token Vault για την αποθήκευση των δεδομένων και του Token	Απαίτηση ύπαρξης του κλειδιού αποκρυπτογράφησης για την μετατροπή σε ευανάγνωστο κείμενο
Καμία χρησιμότητα του Token εκτός του ορισμένου περιβάλλοντος	Σε περίπτωση αναχαίτισης του κλειδιού αποκρυπτογράφησης όλα τα δεδομένα είναι ευάλωτα.
Ευκολία χρήσης	Ικανότητα κρυπτογράφησης αδόμητων δεδομένων

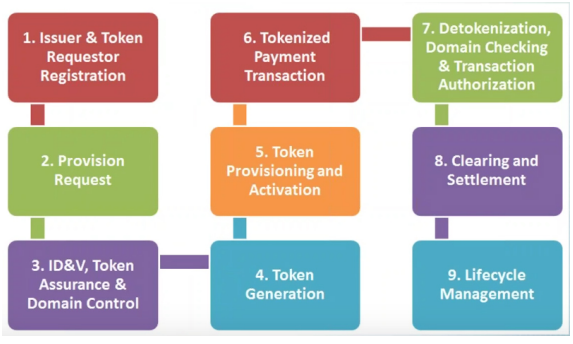
Πίνακας 1: Διαφορές μεθόδων Encryption και Tokenization

- Ένας αριθμός λογαριασμού μπορεί να χαρτογραφηθεί και να αποθηκευτεί εντός του θησαυροφυλακίου χρησιμοποιώντας παραπάνω από ένα Token την φόρα ανάλογα την χρήση που απαιτείται.
- Τα Tokens χρησιμοποιούνται είτε στα συστήματα του έμπορου είτε στο κανάλι επικοινωνίας που εδραιώνεται είτε εντός μιας συγκεκριμένης συσκευής και μπορούν να χρησιμοποιηθούν για μια ή και παραπάνω λειτουργικές περιπτώσεις.
- Σε περίπτωση κλοπής της συσκευής δεν παρέχονται πληροφορίες για τον λογαριασμό του χρηστή σε κάποιο δυνητικό επιτιθέμενο καθώς τα κλειδιά έχουν σημασία μονό εντός της συσκευής ή του καναλιού επικοινωνίας για τα όποια έχουν οριστεί. Επίσης,είναι εύκολη η δημιουργία τους ή η διαγραφή τους μετά από αίτηση του χρήστη.

3.2.4 Κλειδί πληρωμής-Payment Token

Το Payment Token αποτελεί τον αριθμό εκείνο που αντικαθιστά το PAN μιας τραπεζικής κάρτας και χρησιμοποιείται κυρίως σε ηλεκτρονικές πληρωμές μέσω κινητών συσκευών, με ικανότητες NFC σύνδεσης, με κύριο σκοπό την προστασία του φυσικού αριθμού της κάρτας.

Το Payment Token μπορεί να έχει οποιαδήποτε μορφή αλλά για λόγους συμβατότητας και διαλειτουργικότητας των συστημάτων, ακολουθείται η ίδια μορφή που χρησιμοποιείται και από το Personal Account Number (PAN) των τραπεζικών καρτών.



Σχήμα 14: Γέννηση και χρήση Payment Token (Source: Global Plaform)

Όπως φαίνεται και στο σχήμα 14, η δημιουργία και η χρήση ενός Payment Token ξεκινάει με

την αίτηση και την καταχώρηση του εκδότη της κάρτας σε συνδυασμό με την αίτηση της τραπεζικής εφαρμογής.Έπειτα από αρκετά στάδια εξουσιοδοτήσεων και ελέγχων, το Payment Token είναι ικανό να αντικαταστήσει τον τραπεζικό λογαριασμό του χρήστη (PAN) σε μελλοντικές αγορές.

Το Payment Token αφού εξουσιοδοτηθεί βρίσκεται σε μια συνεχόμενη διαδικασία αλλαγών και τροποποιήσεων ανάλογα τις απαιτήσεις του χρήστη και της τραπεζικής εφαρμογής, η οποία επονομάζεται διαχείριση κύκλου ζωής. PAN ονομάζεται ο αριθμός εκείνος που αντιπροσωπεύει τον αριθμό λογαριασμού του χρήστη και βρίσκεται καταγεγραμμένος σε όλες τις πιστωτικές ή χρεωστικές κάρτες σύμφωνα με το πρότυπο ISO/IEC 7812 και αποτελείται από μια ακολουθία 13-19 αριθμητικών ψηφίων.

Η καθιερωμένη δομή του PAN είναι η ακόλουθη (Παπαδόπουλος, 2015):

- **6 ψηφία:** Αναπαριστά των μοναδικό αριθμό BIN, ο οποίος αναπαριστά την εκδότρια της πλαστικής κάρτας. Η εκδότρια τράπεζα έχει την δυνατότητα να αντιπροσωπεύεται και από παραπάνω από έναν αριθμό BIN .
- **6-12 ψηφία:** Το εύρος των πιθανών αριθμών καρτών που συγκαταλέγεται σε κάποιο συγκεκριμένο BIN.
- **Τελευταίο ψηφίο:** Αποτελεί το ψηφίο επαλήθευσης της πλαστικής κάρτας και υπολογίζεται από την χρήση του αλγόριθμου του Luhn.

Τα Payment Tokens διαθέτουν ένα εύρος από χαρακτηριστικά, μερικά από τα οποία είναι υποχρεωτικά, ορισμένα είναι υπό συνθήκη υποχρεωτικά, ενώ κάποια άλλα είναι προαιρετικά. Τα συνηθέστερα χαρακτηριστικά στοιχεία των Tokens αποτελούνται από τα παρακάτω (Securetechalliance.org, 2015):

1. Token Expiry Date
2. Τα τελευταία 4 ψηφία του PAN
3. PAN Product ID
4. POS Entry Mode
5. Token Requestor ID
6. Token Assurance Level
7. Token Assurance Data
8. Token Cryptogram
9. Token Request Indicator

.
Token Expiry Date: Αποτελεί την ημερομηνία λήξης του Payment Token, η οποία όμως είναι διαφορετική από την ημερομηνία λήξης της φυσικής κάρτας. Η ημερομηνία λήξης ποικίλει σε διάρκεια, από μια ημέρα για τα δυναμικά Token μέχρι και την ημερομηνία λήξης της φυσικής κάρτας για τα στατικά.

Τα τελευταία 4 ψηφία του PAN: Περιλαμβάνει τα 4 τελευταία ψηφία της φυσικής κάρτας και χρησιμοποιείται είτε ως ένα επιπλέον μέτρο συσχέτισης του Payment Token με τον πραγματικό αριθμός της κάρτας είτε για την εκτύπωση της σχετικής απόδειξης της συναλλαγής

PAN Product ID: Αποτελεί ένα προαιρετικό στοιχείο, το οποίο περιέχει τον τύπο της φυσικής κάρτας. Διαφοροποιείται ανάλογα τις παρεχόμενες υλοποιήσεις που εφαρμόζονται σε διαφορετικές πολιτικές χρέωσης ή προνόμια ανάλογα τον τύπο της πλαστικής κάρτας.

POS Entry Mode: Υποδεικνύει τον τρόπο χρήσης του Payment Token. Επομένως, ένα Payment Token μπορεί να χρησιμοποιηθεί μόνο από συγκεκριμένα κανάλια, τα οποία σχετίζονται με την διαδικασία αίτησης έκδοσης του.

Token Request Indicator: Προαιρετικό πεδίο το οποίο αποστέλλεται ως δείκτης κατά τη διάρκεια μιας αίτησης έκδοσης του Payment Token.

Token Requestor ID: Είναι ένα ID, το οποίο αποτελείται από ένα μοναδικό αριθμό, ο οποίος χαρακτηρίζει τον TSP

- Θέσεις 1-3: Ο μοναδικός κωδικός του Token Service Provider
- Θέσεις 4-11: Αποδίδετε από τον Token Service Provider σε κάθε οντότητα που αιτείται ένα Token για ένα συγκεκριμένο πεδίο εφαρμογής.

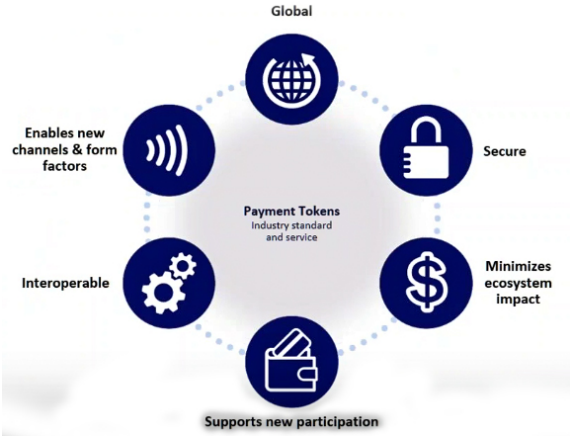
.
Token Assurance Level: Είναι η τιμή του επίπεδου διασφάλισης που παρέχει ο Token Service Provider με σκοπό να αναδείξει το επίπεδο εμπιστοσύνης του Payment Token σε σχέση με τον αριθμό του τραπεζικού λογαριασμού. Προσδιορίζεται ως το αποτέλεσμα του υλοποιημένου ID&V σε συνδυασμό με το επίπεδο ασφάλειας της συσκευής που την εκτέλεσε.

Token Assurance Data: Επίσης ένα προαιρετικό στοιχείο το οποίο περιλαμβάνει επιπλέον πληροφορίες σχετικά με το δεδομένα που συμμετείχαν στην απόδοση του Assurance Level.

Token Cryptogram: Αποτελεί ένα κρυπτογράφημα, το οποίο παράγεται μοναδικά κατά την διενέργεια μιας συναλλαγής και αποστέλλεται μαζί με το Payment Token για την επικύρωση της χρήσης του. Το κλειδί κρυπτογράφησης και αποκρυπτογράφησης παράγεται μαζί με την γέννηση του Payment Token.
Το Token Cryptogram μπορεί να χαρακτηριστεί και ως δυναμικό CVV κατά τα πρότυπα του EMV. Για τον υπολογισμό του λαμβάνονται υπόψη διάφορα δεδομένα που χαρακτηρίζουν μια συναλλαγή (Securetechalliance.org, 2015).

3.2.5 EMV Payment Tokens

Διακατέχουν ακριβώς την ιδία μορφή με έναν αριθμό λογαριασμού (PAN) με την μοναδική διαφοροποίηση την μορφή επεξεργασίας που υφίστανται εντός των συστημάτων πληρωμής.
Επίσης, διακατέχονται από περιορισμούς ανά τομέα υλοποίησης (Domain Restrictions) ανάλογα την χρήση για την οποία δημιουργήθηκαν (Παπαδόπουλος, 2015).



Σχήμα 15: Χαρακτηριστικά EMV Payment Token (Vanderhoof,R et al, 2018)

Όπως φαίνεται και στο σχήμα 15 το κλειδί πληρωμής EMV διακατέχεται από τα παρακάτω τα χαρακτηριστικά Securetechalliance.org, 2015):

1. Δεν δημιουργείται σύγκρουση (conflict) με τον πραγματικό αριθμό λογαριασμού του χρηστή.
2. Διακατέχονται από τους ίδιους βασικούς κανόνες επαλήθευσης ταυτότητας με αποτέλεσμα την ενίσχυση της διαλειτουργικότητας.
3. Έχουν την ικανότητα να συνδυάζονται και να χαρτογραφούνται με τον πραγματικό αριθμό λογαριασμού με την οντότητα εκείνη που δημιουργεί και εκδίδει τον λογαριασμό του χρηστή.

4. Επεξεργάζονται και δρομολογούνται από οντότητες εντός του οικοσυστήματος πληρωμών.

5. Αποτελούνται από μια ακολουθία από 13-19 αριθμών με αποτέλεσμα να είναι φαινομενικά ίδια με τον αριθμό λογαριασμού.

3.3 Πάροχος υπηρεσιών κλειδιών-Token Service Provider (TSP)

Ένας Token Service Provider αποτελεί μια ανεξάρτητη οντότητα εντός του οικοσυστήματος συναλλαγών, ο οποίος είναι υπεύθυνος τόσο για την αδιάλειπτη έκδοση και παροχή των Payment Tokens στους αιτούντες όσο και στην παροχή όλων των υπηρεσιών που σχετίζονται με αυτά.

Ρόλος Token Service Provider

1. **Δημιουργία και έκδοση Κλειδιών Πληρωμής**: Ο πάροχος των υπηρεσιών πληρωμής είναι υπεύθυνος για την οριοθέτηση των Token- PAN έτσι ώστε κατά την διάρκεια δημιουργίας ενός καινούργιου Token να μην συμπίπτει με ένα ήδη υπάρχον PAN καθώς και να είναι σύμφωνο με τα κριτήρια που έχουν οριστεί από την EMVCo.

2. **Θησαυροφυλάκιο Κλειδιών**: Τα παραγόμενα Token και οι αρχικοί αριθμοί λογαριασμών αποθηκεύονται με ασφάλεια στο θησαυροφυλάκιο. Η χαρτογράφηση μεταξύ των δυο τιμών χρησιμοποιείται για την αντίστροφη διαδικασία του Tokenazition.

3. **Περιορισμοί Τομέα**: Η ενσωμάτωση ενός Token σε συγκεκριμένες επαληθευμένες συσκευές ή σε κανάλια επικοινωνίας ή σε εμπόρους ή γεωγραφικές περιοχές με κύριο σκοπό την αποφυγή συναλλαγών έκτος του ορισμένου τομέα.

4. **Διαχείριση Κύκλου Ζωής των Κλειδιών Πληρωμής**: Η διαδικασία στην όποια η διαχείριση των Token εκτελείται συνεχόμενα και ανεξαρτήτως αλλαγών, διαγραφών ή αναβαθμίσεων του λογισμικού της συσκευής.

5. **Μέθοδοι Επαλήθευσης και Διαβεβαίωσης Κλειδιού Πληρωμής**: Ο πάροχος χρησιμοποιεί διαδικασίες επαλήθευσης του χρηστή με σκοπό την δημιουργία ενός προφίλ επικινδυνότητας.
Έτσι το Token μπορεί να έχει τιμές επικινδυνότητας από 0-99 ανάλογα το προφίλ επικινδυνότητας και την αξιοπιστία των μεθόδων επαλήθευσης που χρησιμοποιήθηκαν.

Σχήμα 16: Κύκλος Ζωής Token μέσω TSP (Securetechalliance.org, 2015)

Σύμφωνα με το σχήμα 16, ο κύκλος ζωής ενός κλειδιού πληρωμής αποτελεί μια αρμοδιότητα του TSP. Ο TSP είναι υπεύθυνος για την αναστολή, την συνέχιση, την διαγραφή και την ανανέωση, την ενεργοποίηση, την λήξη καθώς και την επανέκδοση του κλειδιού πληρωμής.

Συμπερασματικά, ο TSP αποτελεί τον καταλληλότερο στόχο επίθεσης καθώς είναι αρμόδιος για όλες τις διακυμάνσεις λειτουργίας του κλειδιού πληρωμής εντός του τραπεζικού οικοσυστήματος. Από την στιγμή που μολυνθεί ο TSP, ο επιτιθέμενος έχει πρόσβαση σε όλους τους τραπεζικούς λογαριασμούς που έχουν καταχωρηθεί στον εν λόγω πάροχο καθώς εκτός από τον κύκλο ζωής του κλειδιού πληρωμής είναι υπεύθυνος και για την αντιστοιχία του κλειδιού πληρωμής με τον PAN του χρήστη.

Το σύστημα των υπηρεσιών που παρέχονται από έναν TSP αποτελούνται από τα παρακάτω δύο βασικά υποσυστήματα:

- Πλατφόρμα εξουσιοδότησης
- Πλατφόρμα συναλλαγών

(Securetechalliance.org, 2015, Παπαδόπουλος, 2015)

3.3.1 Πλατφόρμα εξουσιοδότησης

Για την δημιουργία ενός Payment Token μέσω του PAN θα πρέπει ο κάτοχος της κάρτας (Cardholder) μέσω μιας εξουσιοδοτημένης οντότητας (Token Requestor, Merchant) να αποστείλει σχετικό αίτημα στον TSP, παρέχοντας του ταυτόχρονα τα απαραίτητα διαπιστευτήρια με κύριο σκοπό την επαλήθευση της ταυτότητας του κατόχου της κάρτας. Από την στιγμή που ο TSP λάβει κάποιο αίτημα δημιουργίας ενός Payment Token, εκτελεί ενέργειες ταυτοποίησης και επαλήθευσης (ID&V) προωθώντας μέρος ή το σύνολο των διαπιστευτηρίων που έχει λάβει προς τον εκδότη της κάρτας.

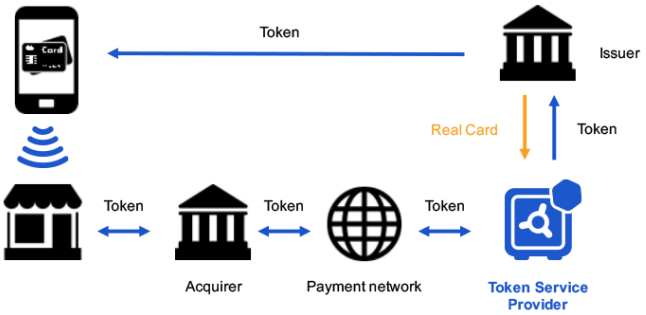
Ο εκδότης της κάρτας με την σειρά του εκτελεί αντίστοιχες διεργασίες ID&V σύμφωνα τις πολιτικές που απορρέουν από την τράπεζα και επιστρέφει το κατάλληλο αποτέλεσμα στον TSP. Εφόσον τα στοιχεία της ταυτοποίησης και επαλήθευσης της ταυτότητας του χρήστη είναι επαρκή και έχει ληφθεί θετική απόκριση από τον εκδότη της κάρτας, ο TSP εκτελεί την μέθοδο του Tokenization, η οποία αποτελείται από τις παρακάτω ενέργειες (Securetechalliance.org, 2015):

- Δημιουργία ενός Payment Token διατηρώντας την μορφή που έχει το αρχικό PAN (BIN, μήκος).
- Εκτελείται καθορισμός των χαρακτηριστικών στοιχείων του Payment Token.

3.3.2 Πλατφόρμα συναλλαγών

Κατά την διενέργεια μιας ηλεκτρονικής συναλλαγής, η πλατφόρμα συναλλαγών αναλαμβάνει την διαδικασία μετατροπής του Payment Token στο πραγματικό PAN εκτελώντας μια λειτουργία De-Tokenization, η οποία αποτελείται από τις παρακάτω ενέργειες (Παπαδόπουλος, 2015):

- Διενέργεια ελέγχων σχετικά με την εγκυρότητα του Payment Token (Expiry Date, PoS Entry Mode, Cryptogram κ.α.).
- Εάν το Payment Token δεν είναι έγκυρο για την συγκεκριμένη συναλλαγή τότε απορρίπτεται η συναλλαγή. Διαφορετικά ανακτάτε από την βάση δεδομένων, γνωστή και ως θησαυροφυλάκιο Token, το PAN και το PAN Expiry Date.
- Πραγματοποιείται η προώθηση της συναλλαγής στον εκδότη της κάρτας εκτελώντας την αντικατάσταση του Payment Token με το πραγματικό αριθμό λογαριασμού καθώς και την σχετική ημερομηνία λήξης.



Σχήμα 17: Οικοσύστημα TSP. (Source: Rambus)

Σύμφωνα με το σχήμα 17, γίνεται μια παρουσίαση της ανατομίας του οικοσυστήματος του TSP. Αρχικά, ο χρήστης επικοινωνεί με την τράπεζα του για την αίτηση χρήσης εξουσιοδοτημένης εφαρμογής για την διεκπεραίωση ανέπαφων συναλλαγών. Έπειτα, η τράπεζα επικοινωνεί με τον πάροχο για την αντικατάσταση του τραπεζικού λογαριασμού του χρήστη με το κλειδί πληρωμής και το αποστέλλει στην εφαρμογή του χρήστη.

Ο χρήστης στην επόμενη αγορά του μέσω της κινητής συσκευής κάνει χρήση του κλειδιού πληρωμής, το οποίο αποστέλλεται στον τράπεζα του εμπόρου και μέσω του δικτύου πληρωμών στον εκάστοτε TSP. Ο πάροχος αποστέλλει το αίτημα πληρωμής μαζί με το κλειδί πληρωμής στην τράπεζα του χρήστη για επιβεβαίωση και έγκριση της συναλλαγής. Τέλος, με την ολοκλήρωση της συναλλαγής, εκδίδεται καινούργιο κλειδί πληρωμής και αποστέλλεται στην εφαρμογή του χρήστη για την επόμενη αγορά.

4 Απειλές και Ευπάθειες των Συστημάτων Ανέπαφων Συναλλαγών μέσω Κινητών Συσκευών

Έχοντας επεξηγήσει στα παραπάνω κεφάλαια την λειτουργικότητα και την αρχιτεκτονική των συστημάτων ανέπαφης διεκπεραίωσης τραπεζικών συναλλαγών μέσω κινητών συσκευών στο παρακάτω κεφάλαιο αναλύεται σε σύνδεση με τα προηγούμενα κεφάλαια οι πιθανές επιθέσεις που μπορούν να πραγματοποιηθούν στα εν λόγω συστήματα.

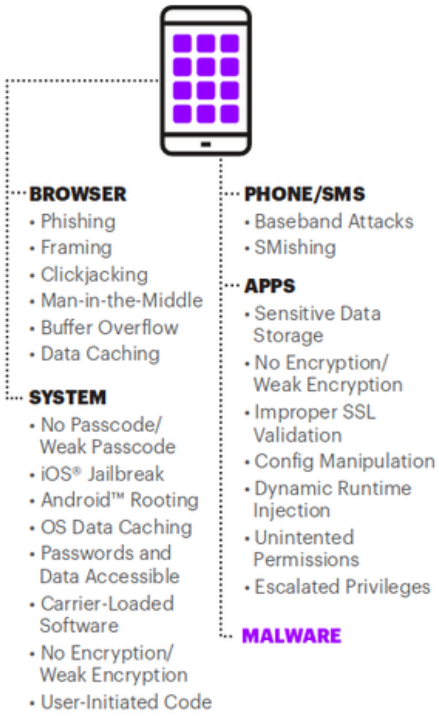
Οι πιθανές επιθέσεις κατηγοριοποιούνται σε επιθέσεις ενάντια στην ίδια την κινητή συσκευή, που αποτελεί το μέσο πραγματοποίησης και υλοποίησης των ανέπαφων συναλλαγών, στο παραγόμενο κανάλι επικοινωνίας, το οποίο κάνει χρήση του πρωτοκόλλου επικοινωνίας του NFC και τέλος στις πιθανές επιθέσεις που μπορεί να πραγματοποιήσει ένας δυνητικός εχθρός έναντι στο τραπεζικό δίκτυο πληρωμών. Στο τέλος του κεφαλαίου και έχοντας πραγματοποιήσει και ολοκληρώσει την ανάλυση των πιθανών ευπαθειών σε όλο το φάσμα των συστημάτων αναφέρονται οι απαιτήσεις ασφαλείας που πρέπει να χαρακτηρίζουν τα εν λόγω συστήματα.

Με την ολοένα αυξανόμενη λειτουργικότητα των συστημάτων εκτέλεσης ανέπαφων συναλλαγών μέσω κινητών συσκευών και με την ευρεία χρήση τους από το ευρύ κοινό ξεκίνησαν να γεννιούνται ερωτηματικά όσον αφορά την πραγματική ασφάλεια των συστημάτων αυτών. Ο συγκεκριμένος τομέας έρευνας έχει κεντρίσει το ενδιαφέρον πολλαπλών χρηματοοικονομικών ινστιτούτων και ερευνητών ασφάλειας με σκοπό την απάντηση του ερωτήματος περί πραγματικής ασφάλειας.

Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί ανά τα χρόνια λειτουργίας των συστημάτων αυτών καθορίστηκε το βασικό εύρος των πιθανών επιλογών ενός δυνητικού εχθρού με σκοπό την απόκτηση των δεδομένων πληρωμής και των ευαίσθητων δεδομένων των χρηστών. Ο δυνητικός εχθρός έχει την πολυτέλεια να διαλέξει ανάμεσα σε επιθέσεις ενάντια στην κινητή συσκευή και την εκάστοτε εφαρμογή πληρωμών, ενάντια στο εδραιωμένο κανάλι επικοινωνίας και το πρωτόκολλο επικοινωνίας NFC και τέλος ενάντια στο δίκτυο πληρωμών και των μεταφερόμενων δεδομένων με σκοπό να εκπληρώσει το στόχο του (Accenture Consulting, 2016).

4.1 Πιθανές Επιθέσεις Ενάντια στο Λειτουργικό Σύστημα της Συσκευής

Ο πρώτος και βασικότερος στόχος επίθεσης ενός δυνητικού εχθρού αποτελεί η ίδια η κινητή συσκευή του χρήστη, η οποία έχει χαρακτηριστεί ως η καταλληλότερη πλατφόρμα επίθεσης λόγω των πολλαπλών ικανοτήτων και διεργασιών που μπορεί να εκτελέσει. Ο δεύτερος στόχος αποτελεί το ίδιο το δίκτυο πληρωμών που χρησιμοποιεί το τραπεζικό οικοσύστημα και η επιλεγμένη από τον χρήστη εφαρμογή για την εξουσιοδότηση και την εκτέλεση της συναλλαγής και τέλος οι ενδιάμεσοι διακομιστές και βάσεις δεδομένων του δικτύου πληρωμής.



Σχήμα 18: Η κινητή συσκευή ως πλατφόρμα επίθεσης (Source: Accenture Consulting)

Ξεκινώντας την αναφορά των πιθανών ευπαθειών είναι λογικό να αναφερθούμε στην ίδια την κινητή συσκευή. Ο εχθρός στοχεύοντας την κινητή συσκευή, σύμφωνα με το σχήμα 18, μπορεί να αποκτήσει τα δεδομένα που στοχεύει είτε μέσω του περιηγητή της συσκευής είτε μέσω του λειτουργικού συστήματος είτε με την εκμετάλλευση της ικανότητας της συσκευής να δέχεται και να αποστέλλει γραπτά μηνύματα είτε τέλος στοχεύοντας τις ίδιες τις εφαρμογές που βρίσκονται εντός της συσκευής.

Μέσω του περιηγητή της συσκευής ο εχθρός μπορεί να εκτελέσει επιθέσεις ψαρέματος (Phishing Attacks) μέσω ψευδών ιστοσελίδων και επιθέσεις ψευδών κλικ (Clickjacking) εκμεταλλευόμενος το γεγονός ότι στους κινητούς περιηγητές δεν εμφανίζεται ολόκληρο το URL της ιστοσελίδας για λόγους εξοικονόμησης χώρου στην οθόνη της συσκευής. Επιπρόσθετα, μπορεί να εκτελέσει επιθέσεις του τύπου Man-In-The-Middle σε συνδυασμό με επιθέσεις υπερχείλισης του buffer του περιηγητή της συσκευής με σκοπό να αποκτήσει πρόσβαση στα δεδομένα της συσκευής (Enisa, 2018).

Εκτός από τον περιηγητή της συσκευής, ο εχθρός έχει την ικανότητα να εκμεταλλευτεί αδυναμίες που απορρέουν από το ίδιο το λειτουργικό σύστημα της συσκευής. Παραδείγματος χάρη, εκμετάλλευση του αδύναμου ή ανύπαρκτου κωδικού κλειδώματος της συσκευής του χρήστη ή την εκμετάλλευση των κενών ασφαλείας που έχουν δημιουργηθεί σε περιπτώσεις όπου η συσκευή βρίσκεται σε κατάσταση Rooted λειτουργίας. Επιπρόσθετα, λόγω μη σωστού διαχωρισμού της μνήμης της συσκευής ο εχθρός μπορεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα ή δεδομένα πληρωμής ή λειτουργίες που υπό κανονικές συνθήκες θα βρισκόντουσαν υπό ασφαλή διαχωρισμό από τα δεδομένα και τις λειτουργίες του υπόλοιπου λειτουργικού συστήματος της. Η πιθανότητα εκμετάλλευσης της παραπάνω αδυναμίας της συσκευής μεγιστοποιείται αν οι κρίσιμες διεργασίες της συσκευής δεν προστατεύονται από κάποιο

κρυπτογραφικό αλγόριθμο ή αν ο ίδιος ο χρήστης έχει ενσωματώσει στο λειτουργικό της συσκευής δικό του εκτελέσιμο κώδικα. Επίσης, η συσκευή μπορεί να καταστεί ευάλωτη ενάντια στην ανάκτηση των ευαίσθητων δεδομένων της ακόμα και σε περιπτώσεις όπου υπάρχει σωστός διαχωρισμός αποθήκευσης των ευαίσθητων δεδομένων και των απλών δεδομένων με στοχευμένες επιθέσεις ενάντια στο Ασφαλές Περιβάλλον Εκτέλεσης (TEE) της συσκευής μέσω μεθόδων αντίστροφης μηχανικής λόγω των ελάχιστων διαθέσιμων εκδοχών του περιβάλλοντος (Enisa, 2018).

Τέλος, η συσκευή μπορεί να είναι ευάλωτη απέναντι σε κάποιο κακόβουλο λογισμικό ή παραποιημένη εφαρμογή που έχει δημιουργήσει ο εχθρός ή από εφαρμογές που δεν τηρούν τους βασικούς κανόνες ασφάλειας με αποτέλεσμα την έκθεση ευαίσθητων δεδομένων του χρήστη, την αποτροπή χρήσης κρυπτογραφικών μεθόδων, την μη σωστή επαλήθευση τοποθεσίας (SSL Pinning) και την εξύψωση των δικαιωμάτων του εχθρού προς το λειτουργικό σύστημα της συσκευής. Επιπρόσθετα, με την παραπάνω ευπάθεια ο εχθρός μπορεί να αποκτήσει μη εξουσιοδοτημένα δικαιώματα ή να παραποιήσει το αρχείο διαμόρφωσης (Config File) είτε της ίδιας της εφαρμογής πληρωμών είτε ολόκληρου του λειτουργικού συστήματος της συσκευής (Accenture Consulting, 2016).

Συγκεκριμενοποιώντας, οι κύριες μέθοδοι επίθεσης που στοχεύουν σε εφαρμογές και ειδικότερα σε εφαρμογές ηλεκτρονικών πορτοφολιών βασίζονται στις παρακάτω κατηγορίες:

- Κοινωνική Μηχανική
- Χαμένη ή κλεμμένη συσκευή
- Εργαλεία και εφαρμογές τρίτων
- Περιβάλλον εκτέλεσης ευαίσθητων διεργασιών

Ο εχθρός είναι πιθανόν να στοχεύσει σε παρεχόμενα εργαλεία τρίτων για την εκτέλεση μιας επίθεσης ή να εκτελέσει επιθέσεις βασισμένες σε μεθόδους κοινωνικής μηχανικής εκμεταλλευόμενος την καθημερινή βιασύνη του χρήστη της κινητής συσκευής. Σε περίπτωση που αναφερόμαστε καθαρά σε εφαρμογές ηλεκτρονικών πορτοφολιών, ο εχθρός στοχεύει κυρίως στην εισαγωγή και στην καταχώρηση της κάρτας στην εφαρμογή καθώς και στις μεθόδους αυθεντικοποίησης της ταυτότητας του χρήστη. Αυτό επιτυγχάνεται είτε στοχεύοντας τους μηχανισμούς αυθεντικοποίησης που κατέχει η συσκευή είτε με την απόκτηση ή αποστολή ψευδών μηνυμάτων επαλήθευσης και αποδοχής με κύριο σκοπό την ενσωμάτωση ενός καινούργιου εξουσιοδοτημένου δικαιούχου πληρωμής εντός της εφαρμογής (Loïc Falletta,2017).

Επιπρόσθετα, οι χρήστες των κινητών συσκευών είναι ευάλωτοι απέναντι σε επιθέσεις βασισμένες στην ανταλλαγή και στην κλωνοποίηση καρτών SIM καθώς και σε επιθέσεις ψαρέματος μέσω γραπτών μηνυμάτων (SMishing). Συνηθέστερη μορφή επίθεσης ψαρέματος μέσω γραπτών μηνυμάτων είναι η προσωποποίηση του πάροχου υπηρεσιών μέσω διαφόρων μεθόδων όπως πλαστογραφημένα γραπτά μηνύματα ή με την δημιουργία κακόβουλης τραπεζικής εφαρμογής με ειδικά διαμορφωμένο λογισμικό έτσι ώστε να αποθηκεύονται στην κινητή συσκευή σε Cleartext προσωπικές και τραπεζικές πληροφορίες του εκάστοτε χρήστη (European Payments Council 2017).

4.2 Επιθέσεις Ενάντια στο Υλικό της Συσκευής

Ένας δυνητικός εχθρός εκτός από την πιθανότητα και την ικανότητα επίθεσης στο πρωτόκολλο επικοινωνίας και στην σύνδεση που εδραιώνεται μεταξύ της κινητής συσκευής και του τερματικού πληρωμής κατά την διάρκεια μιας ανέπαφης συναλλαγής έχει και την επιλογή να επιτεθεί και στο υλικό της συσκευής με σκοπό να αποκτήσει τα ευαίσθητα τραπεζικά στοιχεία του χρήστη.

Για να είναι δυνατή η εξαγωγή των δεδομένων από την κινητή συσκευή ο επιτιθέμενος θα πρέπει με κάποιο τρόπο να κατέχει την φυσική συσκευή του χρήστη. Από την στιγμή που η συσκευή έρθει στην κατοχή του εχθρού υπάρχουν δυο κύριες επιλογές επίθεσης. Ο εχθρός έχει την ικανότητα να επιλέξει είτε μια επίθεση στο Ασφαλές Περιβάλλον Εκτέλεσης (TEE) είτε στο τρόπο με τον οποίο οι συσκευές αποθηκεύουν και κρυπτογραφούν τα ευαίσθητα δεδομένα χωρίζοντας τα σε δεδομένα Ασφαλούς και Μη-Ασφαλούς Κόσμου (Secure and Non-Secure World).

4.2.1 Επίθεση Ενάντια στο TEE

Όπως προαναφέρθηκε, το περιβάλλον ασφαλούς εκτέλεσης εντολών αποτελεί έναν από τους βασικούς πυλώνες ασφάλειας που διακατέχουν οι συσκευές με ικανότητες διεκπεραίωσης τραπεζικών συναλλαγών. Αποτελεί ένα ξεχωριστό λειτουργικό σύστημα εντός της συσκευής και είναι ειδικά σχεδιασμένο για την ασφαλή εκτέλεση και αποθήκευση δεδομένων και κλάσεων.

Αποτελεί μια τεχνολογία κεκλεισμένων θυρών και δεν υπάρχει πληθώρα δημόσιων ερευνών καθώς ούτε και μεγάλος αριθμός πληροφοριών για την συγκεκριμένη δικλείδα ασφάλειας. Ο μοναδικός τρόπος να αποκτηθεί κάποια γνώση για το λειτουργικό σύστημα είναι μέσω τεχνικών αντίστροφης μηχανικής. Για έναν δυνητικό εχθρό, η διενέργεια αντίστροφης μηχανικής αποτελεί ιδιαίτερα επίπονη και χρονοβόρα διαδικασία. Το γεγονός ότι γίνεται χρήση μόνο δυο διαφορετικών εκδοχών του TEE, καθιστά τις πιθανότητες επιτυχούς επίθεσης ενάντια στο ασφαλές περιβάλλον εκτέλεσης σχετικά περισσότερες.

Οι δυο εκδοχές παρέχονται από τις εταιρείες QSEE και MobiCore (Trustonic) αντίστοιχα.
Οι παρεχόμενοι μηχανισμοί που προσφέρονται από την QSEE ως προς το ασφαλές περιβάλλον εκτέλεσης αποτελούνται από:

- Προστασία μνήμης του λειτουργικού συστήματος του TEE
- Παρεχόμενοι Περιορισμοί Αλλοίωσης Μνήμης
- Απομόνωση παρεχόμενων Trustlets εντός του QSEOS

.
Προστασία μνήμης του λειτουργικού συστήματος του TEE της QSEE
Όσον αφορά το TEE της QSEE, όλα τα Trustlets φορτώνονται σε μια ασφαλής περιοχή μνήμης επονομαζόμενη "secapp-region", όπως παρουσιάζεται ενδεικτικά στο σχήμα 19. Η συγκεκριμένη περιοχή μνήμης δεν μπορεί να προσπελαστεί από καμία εφαρμογή εκτός του Secure-World. Ο φορτωτής φορτώνει τα εξουσιοδοτημένα Trustlet με τυχαία σειρά εντός της ασφαλής περιοχής μνήμης. Ένας ασφαλές περιβάλλον εκτέλεσης με στόχο την ασφάλεια θα όριζε δυναμικές διευθύνσεις μνήμης για τα παρεχόμενα Trustlet όμως ο πίνακας των θέσεων μνήμης στην συγκεκριμένη υλοποιήση είναι επίπεδος.

Αυτό ουσιαστικά σημαίνει ότι το κάθε Trustlet είναι ικανό να αναγνωρίσει και να εκμεταλλευτεί μόνο την περιοχή της φυσικής μνήμης της συσκευής με αποτέλεσμα η εικονική μνήμη να είναι ιδιαίτερα περιορισμένη και να κατέχει μόνο 9 Bit εντροπίας (Beniamini, 2017).

```
qcom,qseecom@fe806000 {
        compatible = "qcom,qseecom";
        reg = <0x7f00000 0x500000>;
        reg-names = "secapp-region";
        qcom,disk-encrypt-pipe-pair = <2>;
        qcom,file-encrypt-pipe-pair = <0>;
        qcom,hlos-ce-hw-instance = <1>;
        qcom,qsee-ce-hw-instance = <0>;
        qcom,support-fde;
        qcom,support-pfe;
        qcom,msm_bus,name = "qseecom-noc";
        qcom,msm_bus,num_cases = <4>;
        qcom,msm_bus,active_only = <0>;
        qcom,msm_bus,num_paths = <1>;
        qcom,no-clock-support;
        qcom,msm_bus,vectors =
                <55 512 0 0>,
                <55 512 3936000000 393600000>,
                <55 512 3936000000 393600000>,
                <55 512 3936000000 393600000>;
};
```

Σχήμα 19: Περιοχή Μνήμης του TEE της QSEE (Source: Beniamini, G. 2017)

.

Παρεχόμενοι Περιορισμοί Αλλοίωσης Μνήμης του QSEOS
Όλα τα Trustlets χρησιμοποιούν το λεγόμενο "Stack Cookie" με σκοπό την αποφυγή εκμετάλλευσης ευπαθειών που απορρέουν από την υπερχείλιση της στοίβας εκτέλεσης. Το Cookie παράγεται από τα εργαλεία (RNGtools) του πυρήνα που είναι αρμόδια για την παραγωγή και την τροφοδότηση τυχαίων αριθμών για την μεγιστοποίηση της εντροπίας του συστήματος και αναπαράγεται κάθε φορά που καλείται το TEE.

Όμως, πολλές εφαρμογές που βρίσκονται εντός του περιβάλλοντος κάνουν χρήση Buffers του τύπου BSS για την αποθήκευση των προσωρινών αρχείων, οι οποίοι δεν είναι προστατευμένοι από τα τυχαία παραγόμενα Cookies. Επιπρόσθετα, η στοίβα των trustlets βρίσκεται ακριβώς δίπλα από τους BSS-buffers, χωρίς καμία προστασία μετάβασης.
Ουσιαστικά, αυτό σημαίνει ότι οποιαδήποτε υπερχείλιση μνήμης του BSS αποδίδει απευθείας πρόσβαση στην στοίβα και άρα πλήρη δικαιώματα εκτέλεσης εξουσιοδοτημένου και μη κώδικα (Rosenberg, 2017).

Απομόνωση παρεχόμενων Trustlets εντός του QSEOS
Το λειτουργικό σύστημα που δημιουργήθηκε από την QSEE παρέχει ένα μεγάλο αριθμό κλήσεων συστήματος προς τα QSEE Trustlets, όπως κλήση συστήματος για την διαχείριση μνήμης , δημιουργία κρυπτογραφικών κλειδιών κ.α.. Καθώς, μερικές κλήσεις συστήματος λαμβάνουν δείκτες απευθείας από το QSEE (π.χ. την τοποθεσία μνήμης κρυπτογραφικών μεθόδων) απαιτείται κάποια μορφή επιβεβαίωσης που να διαβεβαιώνει ότι οι συγκεκριμένες διευθύνσεις μνήμης ανήκουν στο λειτουργικό σύστημα του QSEE.

Στην συγκεκριμένη υλοποίηση ασφαλούς περιβάλλοντος εκτέλεσης δεν επιβεβαιώνονται με κανένα τρόπο οι διευθύνσεις μνήμης των κλήσεων συστήματος, κάτι που μπορεί να οδηγήσει στην καταστροφή της μνήμης του πυρήνα και στην πιθανή αλλαγή δικαιωμάτων εκτέλεσης προς όφελος του εχθρού (Beniamini, 2017).

Υλοποίηση του Ασφαλούς Περιβάλλοντος Εκτέλεσης της MobiCore
Στην αντίθετη περίπτωση, οι παρεχόμενοι μηχανισμοί που προσφέρονται από την MobiCore για το ασφαλές περιβάλλον εκτέλεσης αποτελούνται από:

- Προστασία μνήμης του λειτουργικού συστήματος του TEE.
- Παρεχόμενοι Περιορισμοί Αλλοίωσης Μνήμης.

.

Προστασία Μνήμης του TEE της MobiCore
Όσον αφορά την υλοποίηση της MobiCore, η εταιρεία κάνει χρήση ολόκληρης της εικονικής μνήμης της συσκευής όμως χωρίς να έχει ενσωματώσει καμία μορφή ASLR (Adress Space Layout Randomization).

Η έλλειψη τέτοιων τεχνικών σημαίνει ότι όλα τα Trustlets και οι απαραίτητες βιβλιοθήκες φορτώνονται σε προκαθορισμένες διευθύνσεις μνήμης. Από την οπτική του εχθρού αυτό σημαίνει ότι τοπικά με μεθόδους Brute-Force έχει την ικανότητα να ανακαλύψει τις συγκεκριμένες διευθύνσεις μνήμης καθώς και να εκμεταλλευτεί ευπάθειες της συσκευής απομακρυσμένα (Beniamini, 2017).

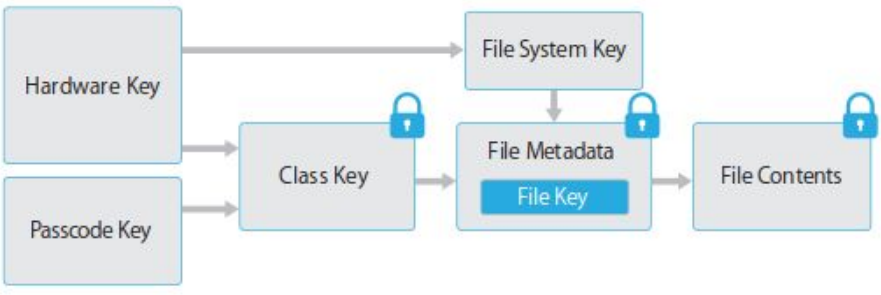
Παρεχόμενοι Περιορισμοί Αλλοίωσης Μνήμης του OS της MobiCore:
Δεν υπάρχει παραγόμενο Stack Cookie από τον πυρήνα του λειτουργικού, οπότε κάθε υπερχείλιση στοίβας είναι εκμεταλλεύσιμη. Σε συνδυασμό με την έλλειψη ASLR, καθιστά το περιβάλλον εκτέλεσης εκμεταλλεύσιμο από απόσταση και αναιρεί την ανάγκη του εχθρού για αναζήτηση διαρροής πληροφοριών. Επιπρόσθετα, η διεύθυνση φόρτωσης είναι προκαθορισμένη και επιτρέπει την εκτέλεση επιθέσεων με την χρήση ROP εργαλείων.(Simon, 2017, Beniamini, 2017)

4.2.2 Κρυπτογράφηση Πλήρους Δίσκου

Όσον αφορά τις συσκευές Android, οι οποίες διακατέχουν μεγάλο ποσοστό της αγοράς των κινητών συσκευών, υποστηρίζονται μηχανισμοί κρυπτογράφησης με σκοπό την προστασία των προσωπικών δεδομένων του χρήστη. Το λειτουργικό σύστημα των συσκευών παρέχει μηχανισμούς κρυπτογράφησης πλήρους δίσκου (FDE-Full Disk Encryption) καθώς και αρχείων (FBE-File Based Encryption) από Default από την έκδοση 6.0 και έπειτα (Beniamini, 2017).

Ο λόγος που θα αναφερθεί μόνο το λειτουργικό σύστημα της Android παρέχεται από ένα και μοναδικό χαρακτηριστικό παράδειγμα από τον πραγματικό κόσμο. Το δεύτερο μεγαλύτερο κομμάτι της αγοράς, το κατέχουν οι συσκευές με λειτουργικό σύστημα iOS. Το 2015 κατά την διάρκεια της τρομοκρατικής επίθεσης στο San Bernardino, οι αρχές είχαν κατασχέσει την κινητή συσκευή ενός από τους δράστες. Η κινητή συσκευή είχε ενεργοποιημένη την λειτουργία πλήρους κρυπτογράφησης δίσκου και από κατασκευής οι επιθέσεις ενάντια στην συσκευή με μεθόδους Brute-Force ήταν και είναι αδύνατες.

Ο λόγος που δεν κατάφεραν οι αρχές να "σπάσουν" τον κωδικό της συσκευής είναι διότι η Apple προστατεύει τις συσκευές της από τέτοιες επιθέσεις με την δημιουργιά του κλειδιού αποκρυπτογράφησης, το οποίο αποτελείται από τον συνδυασμό του κωδικού πρόσβασης του χρήστη και ενός μοναδικού αριθμού ενσωματωμένου στο υλικό της συσκευής, ο οποίος παράγεται τυχαία στο εργοστάσιο παραγωγής. Ο συγκεκριμένος αριθμός αποτελεί ένα 256 Bit κλειδί, το οποίο δεν είναι προσβάσιμο από κανένα λογισμικό ή Firmware της συσκευής παρά μόνο από την κρυπτογραφική γεννήτρια AES.



Σχήμα 20: Κρυπτογράφηση Πλήρους Δίσκου του λειτουργικού συστήματος iOS (Beniamini, G. 2017)

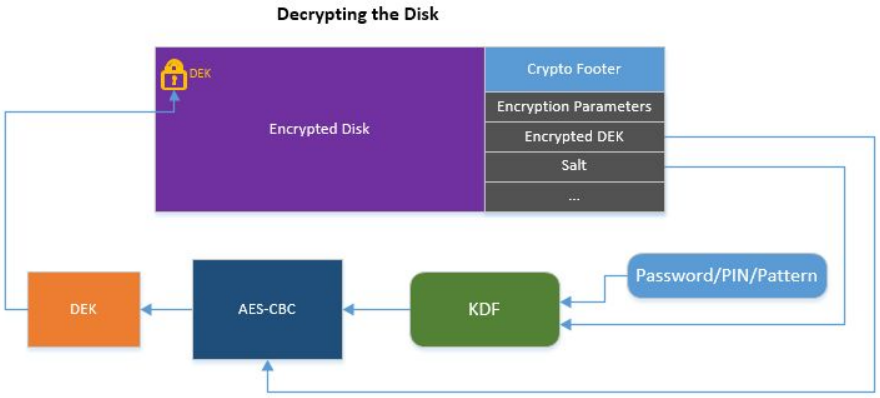
Στο παραπάνω σχήμα αναφέρεται η ανατομία της κρυπτογράφησης πλήρους δίσκου που προσφέρει η Apple στις συσκευές της. Κάθε φορά που ένα καινούργιο αρχείο δημιουργείται, το σύστημα παράγει ένα 256-Bit κλειδί, το οποίο παρέχεται στην μηχανή κρυπτογράφησης AES του υλικού της συσκευής για να κρυπτογραφήσει το εν λόγω αρχείο. Έπειτα, το κρυπτογραφικό κλειδί ενσωματώνεται σε μια ή παραπάνω κλάσεις κλειδιού (Class Keys) ανάλογα τις απαιτήσεις ασφάλειας.

Όταν ένα αρχείο ανοιχθεί, τα μεταδεδομένα του αποκρυπτογραφούνται από το κλειδί του λειτουργικού (File System Key) αποκαλύπτοντας το ενσωματωμένο κλειδί καθώς και ποια κλάση το προστατεύει. Τέλος, το κλειδί προμηθεύεται στην μηχανή AES για την αποκρυπτογράφηση του αρχείου και την ανάκτηση του από την ταχεία μνήμη για να καλύψει τις ανάγκες του χρήστη (Apple.com, 2018).

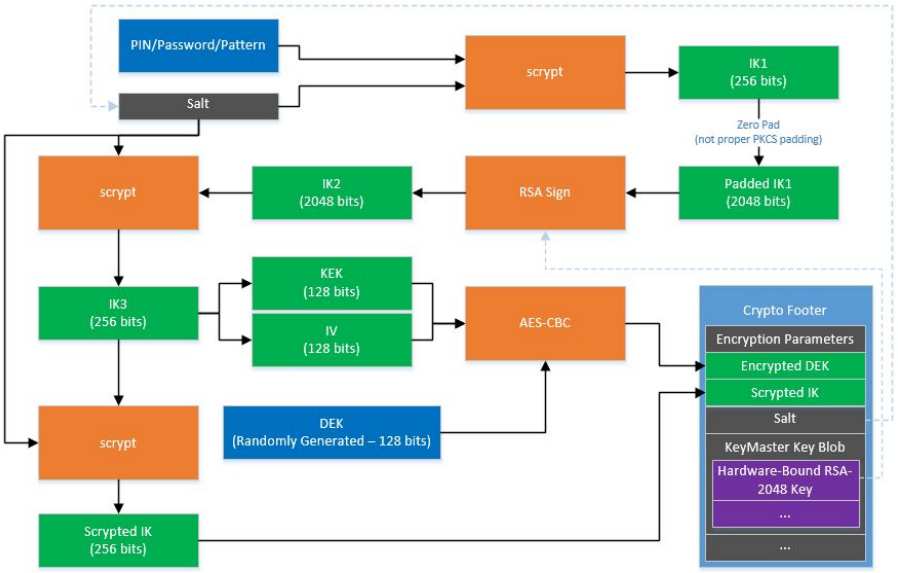
Οι συσκευές Android από την άλλη βασίζονται στην κρυπτογραφική μέθοδο dm-crypt, η οποία είναι βασισμένη στο υποσύστημα του πυρήνα των Linux. Όμως, η μέθοδος αυτή δεν καλύπτει την FDE KDF (Key Derivation Function) του συστήματος. Η εταιρεία βασίζεται σε ένα Trustlet, το οποίο ονομάζεται KeyMaster, με σκοπό να συγχωνεύσει την συνάρτηση κλειδιού με το κλειδί που βρίσκεται χαραγμένο στο υλικό της συσκευής. Ο μηχανισμός αυτός παράγει το κλειδί κρυπτογράφησης των δεδομένων και τα υπογράφει μέσω της μεθόδου υπογραφής, η οποία είναι βασισμένη στον κρυπτοαλγόριθμο RSA, με το παραγόμενο κλειδί.

Ο μηχανισμός λειτουργεί εντός του ασφαλούς περιβάλλοντος εκτέλεσης (TEE) και σύμφωνα με τα προαναφερθέντα, ο εχθρός έχει την ικανότητα να το παραβιάσει. Από την στιγμή που παραβιαστεί το περιβάλλον, και σε συνδυασμό με το γεγονός ότι το χαραγμένο κλειδί δεν μπορεί να παραμετροποιηθεί εκτός εργοστασίου, ο εχθρός φορτώνει το κλειδί στο Non-Secure World και η συσκευή είναι ευάλωτη.

Από την στιγμή που το κλειδί περάσει στον Μη ασφαλή Κόσμο, ο εχθρός έχει την δυνατότητα να αποκρυπτογραφήσει το KeyMaster, να υπολογίσει το κλειδί που βρίσκεται ενσωματωμένο στο υλικό και τέλος να αποκρυπτογραφήσει όλα τα δεδομένα του χρήστη (Simon, 2017, Beniamini, 2017).



Σχήμα 21: Κρυπτογράφηση Πλήρους Δίσκου του λειτουργικού συστήματος Android (Beniamini, G. 2017)



Σχήμα 22: Αρχιτεκτονική Συστήματος Κρυπτογράφησης Πλήρους Δίσκου του λειτουργικού συστήματος Android (Beniamini, G. 2017)

Όπως φαίνεται και στα σχήματα 21-22 η κρυπτογραφία πλήρους δίσκου της Android ακολουθεί την παρακάτω ροή για την κρυπτογράφηση του δίσκου της συσκευής. Αρχικά, ο κωδικός ή το μοτίβο ασφαλείας του χρήστη σε συνδυασμό με τυχαία δεδομένα (Salt) χρησιμοποιούνται ως είσοδο σε μια κρυπτογραφική συνάρτηση παραγωγής κλειδιών (Scrypt) για να παράξουν ένα ενδιάμεσο κλειδί 256-Bit (IK1).

Έπειτα, με την μέθοδο του Padding συμπληρώνονται στον IK1 μηδενικά bytes μέχρι να εξισωθεί με το μέγεθος του μυστικού κλειδιού που βρίσκεται χαραγμένο στο υλικό της συσκευής (Hardware Bound Private Key – HBK). Το παραλλαγμένο κλειδί IK1 υπογράφεται με το HBK για την παραγωγή του IK2 μεγέθους 2048-Bit. Εφαρμόζοντας ξανά την μέθοδο scrypt με τα τυχαία δεδομένα που χρησιμοποιήθηκαν στο πρώτο βήμα παράγεται ο IK3.

Τα πρώτα 128 Bit αποτελούν το KEK (Key Encryption Key) ενώ τα τελευταία 128 Bit αποτελούν το διάνυσμα αρχικοποίησης IV. Ο συνδυασμός του κλειδιού κρυπτογράφησης δίσκου (Disk Encryption Key – DEK) με το διάνυσμα αρχικοποίησης IV και το KEK τροφοδοτούνται στην κρυπτογραφική μέθοδο AES-CBC, η οποία κρυπτογραφεί ολόκληρο το δίσκο της συσκευής (Android Open Source Project, 2014).

4.3 Πιθανές Επιθέσεις Ενάντια στο Πρωτόκολλο Επικοινωνίας NFC

4.3.1 Επιθέσεις Προώθησης-Relay Attacks

Την εποχή όπου οι πλαστικές κάρτες αποτελούσαν το προσκήνιο των ανέπαφων τραπεζικών συναλλαγών εμφανίζεται μια καινούργια τάση υποκλοπής και παραποίησης δεδομένων, γνωστή και ως μέθοδος Relay Attack. Μεταπηδώντας στα συστήματα διεκπεραίωσης ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών η εν λόγω μορφή επίθεσης συνεχίζει να υφίσταται και να αποτελεί μια από τις διαδεδομένες μορφές επιθέσεις ενάντια στην κινητή συσκευή. Είναι οι επιθέσεις εκείνες όπου η επικοινωνία προς και από την κινητή συσκευή προωθείται μέσω μεγαλυτέρων αποστάσεων μέσω ενός εναλλακτικού φορέα ή με την χρήση πολλαπλών συσκευών, οι οποίες λειτουργούν ως Proxy. Ο επιτιθέμενος έχει την δυνατότητα να καταχραστεί την καταχωρημένη κάρτα του θύματος απομακρυσμένα χωρίς την επίγνωση του.

Η βιωσιμότητα αυτού του σεναρίου επιβεβαιώθηκε από τον Hanke, ο όποιος κατάφερε να προωθήσει το σήμα επικοινωνία μεταξύ της συσκευής και του RFID αναμεταδότη μέσω του πρωτοκόλλου Bluetooth της συσκευής (Reveilhac & Pasquet, 2009).
Οι Roland & Michael απέδειξαν ότι το ασφαλές περιβάλλον είναι ευαίσθητο σε επιθέσεις που προέρχονται από την ανέπαφη διεπαφή άλλα και σε σενάρια επιθέσεων της κατηγορίας Relay Attack. Οι

επιθέσεις μπορούν να υλοποιηθούν και να εκτελεστούν μέσω της επεξεργαστικής μονάδας της κινητής συσκευής. Οι κινητές συσκευές με ικανότητες διασύνδεσης μέσω NFC έχουν αναδειχθεί ως η καταλληλότερη πλατφόρμα για την εκτέλεση επιθέσεων σε ανέπαφες κάρτες (Roland, Michael. 2012).

Επιπρόσθετα, κατά την διάρκεια μετάβασης από τις πλαστικές κάρτες στις κινητές συσκευές, σε συνδυασμό με την περαιτέρω γνωριμία με την λειτουργικότητα που παρέχει το HCE, η επίθεση έγινε λιγότερο πολύπλοκη για τον επιτιθέμενο καθώς πλέον δεν χρησιμοποιούνται πολλαπλές συσκευές για την διεκπεραίωση της επίθεσης παρά μόνο η συσκευή του χρήστη και η αντίστοιχη του επιτιθέμενου λόγω της ικανότητας της κινητής συσκευής να αλλάζει λειτουργικότητα (π.χ. μετάβαση από Reader/Writer Mode σε Peer-to-Peer Mode).

Έχει αποδειχθεί με την μορφή πειραμάτων ότι η επικοινωνία που εδραιώνεται μεταξύ δυο συσκευών μπορεί με το κατάλληλο σετ εντολών να προωθηθεί κάνοντας χρήση των εναπομεινάντων πρωτοκόλλων επικοινωνίας της συσκευής (π.χ. Bluetooth, Wifi), παρακάμπτοντας με αυτό τον τρόπο την δικλείδα ασφάλειας της απόστασης. Να αναφερθεί εδώ ότι η μεταξύ επικοινωνία δυο NFC συσκευών μπορεί να εδραιωθεί σε απόσταση το πολύ 10 εκατοστών. (Hillali Wadii, Boutahar & EL Ghazi, 2017).

Η βασική ροή ενεργειών που παρέχει το πρωτόκολλο του NFC ξεκινάει με την κατάσταση στην οποία βρίσκεται η κινητή συσκευή την συγκεκριμένη χρονική στιγμή (Ενεργή ή όχι). Από την στιγμή που η κινητή συσκευή βρίσκεται ενεργοποιημένη, ο κάτοχος της συσκευής καλείται να παραχωρήσει τον τηλεφωνικό του αριθμό, το όνομα χρήστη και άλλες παρεμφερή πληροφορίες στην εφαρμογή ηλεκτρονικών πληρωμών που έχει επιλέξει. Από την στιγμή που καταχωρείται ο χρήστης, ενεργοποιείται ο λογαριασμός του και αποστέλλονται στοιχεία επαλήθευσης στις εξουσιοδοτημένες συσκευές του.
Με την ολοκλήρωση της διαδικασίας επαλήθευσης της ταυτότητας του χρήστη, οι κεντρικοί διακομιστές της εφαρμογής αποστέλλουν στην κινητή συσκευή κλειδιά πρόσβασης μέσω διαδικτυακών υποδομών σε μορφή JSON που επιτρέπουν στην συσκευή να επικοινωνήσει με το μηχάνημα POS.

Η επίθεση ξεκινάει την στιγμή που ο χρήστης επιθυμεί να εκτελέσει μια συναλλαγή μέσω της συσκευής του. Όπως φαίνεται και στο σχήμα 23, ο επιτιθέμενος, ο οποίος βρίσκεται σε κοντινή απόσταση από τον χρήστη, έχει την δυνατότητα να επέμβει στην μεταξύ τους επικοινωνία και να αποκτήσει το διαμοιραζόμενο κλειδί, βρισκόμενος σε κατάσταση Reader/Writer προσομοιώνοντας το μηχάνημα POS.

Σχήμα 23: Relay Channel (Gurulian.I et al, 2017)

Σε παραλλαγμένη μορφή της επίθεσης, αν ο χρήστης δεν είναι σε θέση να εξακριβώσει αν το μηχάνημα αποτελεί μηχάνημα συναλλαγής, ο επιτιθέμενος με ιδιαίτερη ευκολία μπορεί να αποκτήσει το διαμοιραζόμενο κλειδί βρισκόμενος σε κατάσταση λειτουργίας Peer-to-Peer.
Για να μπορεί να θεωρηθεί η επίθεση επιτυχής, η συσκευή του επιτιθέμενου θα πρέπει να αποστείλει αίτηση πρόσβασης στο μηχάνημα POS κάνοντας χρήση του κλειδιού που αποκτήθηκε από την συσκευή του θύματος. Για να επιτευχθεί αυτό το στάδιο της επίθεσης, συσκευή μεταβαίνει σε λειτουργία HCE, με σκοπό να αναπαραστήσει μια ανέπαφη κάρτα και να αποστείλει αιτήματα πληρωμής.

Η βιωσιμότητα του συγκεκριμένου σεναρίου επίθεσης βασίζεται στην πιθανότητα ανίχνευσης του επιτιθέμενου κατά την διάρκεια αυθεντικοποίησης του χρήστη. Αν δεν ανιχνευθεί, η επίθεση είναι βιώσιμη και εκτελέσιμη (Matthew A. Crossman, Hong Liu,2016).

4.3.2 Eavesdropping-Κρυφάκουσμα

Η κλοπή δεδομένων μέσω της μεθόδου Eavesdropping αποτελεί την νούμερο ένα απειλή που αντιμετωπίζουν τα συστήματα ανέπαφων πληρωμών που κάνουν χρήση της τεχνολογίας NFC. Ουσιαστικά αποτελεί το μη εξουσιοδοτημένο «άκουσμα» των δεδομένων από έναν δυνητικό εχθρό. Κατά την διάρκεια μιας συναλλαγής, πραγματοποιείται ανταλλαγή δεδομένων μεταξύ της κινητής συσκευής και του τερματικού πληρωμής. Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν με σκοπό να προσκομιστούν πληροφορίες για τον κάτοχο της κάρτας είτε με την μορφή πληροφοριών του τραπεζικού λογαριασμού του χρηστή είτε με την προσκόμιση προσωπικών δεδομένων του που αργότερα μπορούν να χρησιμοποιηθούν για την πλαστοπροσωπογραφία του θύματος (Paganini P, n.d.).

Γενικεύοντας, υπάρχουν τρεις κύριοι στόχοι για τον επιτιθέμενο. Ο πρώτος αποτελεί τα σήματα που αποστέλλονται μεταξύ των δυο συσκευών υπό την μορφή συχνοτήτων μέσω του αέρα για να εδραιωθεί η απαραίτητη επικοινωνία, η αποκωδικοποίηση του καναλιού επικοινωνίας και τέλος η ανάλυση των δεδομένων που προσκομίστηκαν αντίστοιχα. Το σκέλος της συναλλαγής που εκμεταλλεύεται το κρυφάκουσμα των δεδομένων αποτελούν τα σήματα που αποστέλλονται μεταξύ των δυο συσκευών υπό την μορφή συχνοτήτων(Dang et al., 2017).

Μερικές από τις παραμέτρους που απαρτίζουν μια τέτοια επικοινωνία είναι οι παρακάτω:

- Τα χαρακτηριστικά του πεδίου των ραδιοκυμάτων που δημιουργείται λόγω της επικοινωνίας των δυο συσκευών (π.χ. η θέση της κεραίας, ο τύπος της κεραίας, τα χαρακτηριστικά ασφάλειας που διέπουν τα μεταφερόμενα κύματα, το περιβάλλον στο όποιο εκτελείται η επικοινωνία κ.α.).
- Τα χαρακτηριστικά της κεραίας του επιτιθέμενου
- Η ποιότητα του δέκτη του επιτιθέμενου
- Η ποιότητα του αποκωδικοποιητή του χρηστή
- Η χωροταξική τοποθέτηση του χρηστή σε σχέση με τις συσκευές που βρίσκονται σε επικοινωνία
- Η ισχύς του σήματος που δημιουργούν οι συσκευές.

Λόγω των παραπάνω μεταβλητών είναι δύσκολη η απάντηση του παραπάνω ερωτήματος καθώς και η δημιουργία βασικών οδηγιών ασφάλειας.

Επίσης, είναι μείζονος σημασίας ο τρόπος λειτουργίας της συσκευής-αποστολέα των δεδομένων. Δηλαδή, αν βρίσκεται σε ενεργητική ή σε παθητική κατάσταση. Οι δυο αυτές καταστάσεις διαφοροποιούνται στο τρόπο με τον όποιο αποστέλλουν τα δεδομένα (Badra et al,2016).
Να αναφερθεί ότι η ανάκτηση δεδομένων από μια συσκευή που εκπέμπει ενώ βρίσκεται σε παθητική κατάσταση είναι δυσκολότερη.

Καθώς η τεχνολογία NFC χρησιμοποιεί μαγνητική σύζευξη για να μεταφέρει ενέργεια στους παθητικούς αποδεκτές είναι περιορισμένη η ακτίνα λειτουργίας του πρωτοκόλλου. Έχει αποδειχθεί όμως ότι αυτός ο περιορισμός μπορεί να παρακαμφθεί χρησιμοποιώντας τα υπόλοιπα πρωτοκολλά επικοινωνίας της συσκευής με αποτέλεσμα να μπορούν να αποσταλθούν δεδομένα σε κάποιον επιτιθέμενο από μεγαλύτερη απόσταση από αυτή των 10 εκατοστών που ορίζει το πρωτόκολλο του NFC (Siitonen et al,2012).

Ένας πιθανός τρόπος υλοποίησης της επίθεσης θα μπορούσε να είναι η δημιουργία ενός Relay Channel μεταξύ της συσκευής του χρήστη και του τερματικού πληρωμής μέσω ενδιάμεσων συσκευών που θα λειτουργούν ως Proxy. Στην περίπτωση που η επίθεση αποδειχθεί επιτυχής, ο εχθρός έχοντας συλλέξει τις απαραίτητες πληροφορίες (π.χ. όνομα κατόχου, μοντέλο κινητής συσκευής, το παραγόμενο Payment Token κ.α.) είναι σε θέση να αναπαράξει μια ανέπαφη συναλλαγή εις βάρος του θύματος.

4.3.3 Interception Attacks-Επιθέσεις Αναχαίτισης

Τα συστήματα ανέπαφων συναλλαγών είναι επίσης ευάλωτα εναντία σε επιθέσεις αναχαίτισης. Λειτουργούν με παρόμοιο τρόπο με τις επιθέσεις Man-in –The-Middle λαμβάνοντας πληροφορίες από την μια συσκευή, εκτελώντας παραμετροποίηση των δεδομένων και έπειτα αποστέλλοντας τα στην

συσκευή που θα τα λάμβανε εξαρχής (Raina, 2017).

Αυτό το σενάριο επίθεσης μπορεί να εκτελεστεί μονό όταν και οι δυο συσκευές βρίσκονται σε ενεργή κατάσταση καθώς μονό τότε μπορούν και οι δυο συσκευές να λαμβάνουν και να αποστέλλουν πληροφορίες ταυτόχρονα. Αποτελεί ένα ιδιαίτερα δύσκολο σενάριο καθώς οι συσκευές μπορούν ανά πασά στιγμή να διακόψουν την αναμετάδοση δεδομένων αν αντιληφθούν κάποιο λάθος πρωτοκόλλου (Price, 2017).

Η εγκαθίδρυση ενός ασφαλούς καναλιού μεταξύ δυο συσκευών αποτελεί την καλύτερη προσέγγιση προστασίας εναντία σε επιθέσεις Eavesdropping ή κάποιου αλλού είδους αλλοίωσης δεδομένων σε συστήματα πληρωμών που υποστηρίζουν αγορές μέσω NFC. Λόγω της έμφυτης προστασίας που προσφέρει το πρωτόκολλο εναντία σε επιθέσεις MiTM αποτελεί ξεκάθαρη λύση η εδραίωση ενός ασφαλούς καναλιού επικοινωνίας.

Ένα πρωτόκολλο συμφωνίας κλειδιού όπως το πρωτόκολλο Diffie-Hellmann το όποιο είναι βασισμένο στον RSA ή στην μέθοδο Elliptic Curves μπορεί να χρησιμοποιηθεί για την εδραίωση ενός διαμοιρασμένου μυστικού κλειδιού μεταξύ των δυο συσκευών. Το συγκεκριμένο εγχείρημα δεν αποτελεί διόλου εύκολο αν αναλογιστούν οι περιορισμένες ικανότητες τόσο των συσκευών όσο και των περιβαλλόντων επεξεργασίας που βασίζονται στο πρωτόκολλο NFC. Κρυπτογραφικές μέθοδοι βασισμένες στην μέθοδο των Elliptic Curves παρέχουν την πιο αποδοτική αξιοποίηση της μνήμης σε περιβάλλοντα επικοινωνίας που κάνουν χρήση του NFC από τα αντίστοιχα σύστηματα, τα όποια είναι βασισμένα σε υλοποίησεις βασισμένες στον αλγόριθμο RSA.

Ένα από τα κυρία πλεονεκτήματα της συγκεκριμένης υλοποίησης είναι η οικονομία στην μνήμη καθώς μπορεί να πράξει κρυπτογραφικές μεθόδους ισάξιας δύναμης με την χρήση μικρότερων σε μέγεθος κλειδιών σε αντίθεση με άλλες κρυπτογραφικές μεθόδους. Καθώς, η εγκαθίδρυση ενός διαμοιρασμένου μυστικού κλειδιού αποτελεί ένα δύσκολο εγχείρημα για ένα περιβάλλον επικοινωνίας που βασίζεται στο NFC, χρησιμοποιείται το λεγόμενο «Paired Secret».

Το «Paired Secret» κάνει χρήση μιας διεργασίας διγραμμικής σύζευξης σε συνδυασμό με την μέθοδο της ECC (Elliptic Curves) για την επίτευξη ενός αποδεκτού επίπεδου ασφάλειας και αποδοτικότητας (Chen, X., Choi, K. and Chae, K., 2017).

4.3.4 Data Corruption-Διαφθορά Δεδομένων

Διαφορετικό σενάριο επίθεσης αποτελλεί η παραλλαγή των μεταφερόμενων δεδομένων, κατά την διάρκεια μιας επικοινωνίας, με σκοπό την αλλοίωση κομβικών σημείων και δεδομένων της εγκαθιδρυμένης επικοινωνίας .

Στην πιο απλή της μορφή, η επίθεση αυτή έχει την ικανότητα να παραλλάξει τα δεδομένα με τέτοιο τρόπο ώστε η συσκευή που θα τα παραλάβει να μην μπορεί να διακρίνει τις ενέργειες που πρέπει να εκτελέσει. Ουσιαστικά, αποτελεί μια επίθεση άρνησης εξυπηρέτησης (Denial of Service-DoS) (Rajaram, 2014).

Η αλλοίωση των δεδομένων μπορεί να επιτευχτεί με την αποστολή δεδομένων στο ίδιο εύρος συχνοτήτων του φάσματος που χρησιμοποιείται από τις δυο συσκευές που επικοινωνούν την σωστή στιγμή. Ο σωστός χρόνος αποστολής μπορεί να υπολογιστεί με την σωστή κρίση του επιτιθέμενου πάνω στην κωδικοποίηση και τρόπο λειτουργίας του συστήματος. Η συγκεκριμένη επίθεση λόγω της μη ιδιαίτερης πολυπλοκότητας που την ορίζει δεν μπορεί να εκτελέσει πραγματική αλλοίωση των δεδομένων (Raina, 2017).

4.3.5 Data Modification-Παραποίηση Δεδομένων

Στο εν λόγω είδος σεναρίου επίθεσης, ο επιτιθέμενος επιθυμεί η συσκευή που λειτουργεί ως δέκτης των δεδομένων να παραλάβει τα αποσταλθέντα δεδομένα, με την μονή διαφοροποίηση ότι αυτά έχουν παραλλαχθεί συμφώνα με τις βλέψεις του επιτιθέμενου. Η εφαρμοσιμότητα της συγκεκριμένης επίθεσης βασίζεται κυρίως στην ισχύ και στην ποιότητα των τεχνικών που κατέχει ο επιτιθέμενος για να πραγματοποιήσει την επίθεση. Επίσης, μεγάλη σημασία έχει η διαμόρφωση του πλάτους στην όποια

εκτελείται η επικοινωνία.

Σε περιπτώσεις όπου η επικοινωνία καλύπτει το 100% του πλάτους διαμόρφωσης ο αποκωδικοποιητής στην ουσία ελέγχει τα δυο μισά Bit πληροφορία των ραδιοκυμάτων. Δηλαδή αν υπάρχει παύση σήματος ή όχι. Για να είναι σε θέση ο αποκωδικοποιητής να καταλάβει την μη-παύση ως παύση ο επιτιθέμενος θα πρέπει να εκτελέσει δυο βασικά βήματα. Αρχικά, μια παύση στην διαμόρφωση πλάτους πρέπει να εισαχθεί στο εύρος της συχνότητας. Έπειτα, θα πρέπει να παραχθεί μια παύση του ραδιοκύματος, η όποια θα αποσταλθεί στον αρχικό δέκτη. Αυτό, ουσιαστικά σημαίνει ότι ο επιτιθέμενος θα πρέπει να παράξει και να αποστείλει ραδιοκύματα, τα όποια θα επικαλύψουν τα αρχικά με αποτέλεσμα να παράξουν μηδενικό σήμα στην κεραία του δέκτη (Rajaram, 2014).

Το συγκεκριμένο εγχείρημα είναι πρακτικά αδύνατο όμως με την χρήση του παραλλαγμένου αλγορίθμου του Miller είναι δυνατή η μετατροπή ενός μη μηδενικού σήματος σε μηδενικό με την προϋπόθεση ότι το προηγούμενο κύμα είναι και αυτό μη μηδενικό. Το συγκεκριμένο σενάριο επίθεσης έχει πιθανότητα επιτυχίας 50% και εξαρτάται καθαρά από την σειρά των ραδιοκυμάτων που εκπέμπονται.

Στην αντίθετη περίπτωση, όπου η επικοινωνία καλύπτει το 10% του πλάτους διαμόρφωσης, ο αποκωδικοποιητής προσμετράει και τα δυο επίπεδα σήματος (82% και πλήρες) και εκτελεί μια σύγκριση μεταξύ τους. Σε περίπτωση που τα σήματα βρίσκονται στο σωστό εύρος εκπομπής το σήμα θεωρείται γνήσιο και αποκωδικοποιείται. Ένας επιτιθέμενος θα μπορούσε να προσθέσει μια ποσότητα σήματος, στο σήμα που εκπέμπεται στο 82%, έτσι ώστε να φαίνεται ως πλήρες σήμα. Ταυτόχρονα, το σήμα που έπιανε ολόκληρο το εύρος αυτόματα μεταφράζεται ως σήμα της τάξης του 82%. Με την μετατροπή αυτή , ο αποκωδικοποιητής αποκωδικοποιεί ένα γνήσιο σήμα αντίθετης όμως άξιας και σημασίας.

Η επιτυχία της επίθεσης εξαρτάται από το εύρος του δυναμικού εύρους εισαγωγής σήματος του δέκτη. Είναι πολύ πιθανή η υπέρβαση του ορίου του σήματος του παραλλαγμένου σήματος και να απορριφτεί από την συσκευή-δέκτη (Chattha, 2014).

Ουσιαστικά, η διάφορα των δυο επιθέσεων ορίζεται από το ποσοστό του πλάτους διαμόρφωσης στο όποιο εκτελείται η επικοινωνία των δυο συσκευών. Στο 100% του πλάτους διαμόρφωσης έχει σημασία η σειρά με την όποια εμφανίζονται τα σήματα ενώ σε πλάτος της τάξης του 10% η επίθεση μπορεί να εκτελεστεί σε όλα τα Bit πληροφορίας ανεξαρτήτως σειράς εμφάνισης.

4.3.6 Data Insertion-Εισαγωγή Δεδομένων

Ο επιτιθέμενος εκτελεί μια εισαγωγή μηνυμάτων στην ροή των μεταφερόμενων δεδομένων. Το συγκεκριμένο σενάριο επίθεσης είναι εφικτό μόνο όταν η συσκευή δέκτης χρειάζεται αρκετό χρόνο για να αποστείλει την απαραίτητη απάντηση. Ο επιτιθέμενος μόνο σε αυτό το χρονικό περιθώριο έχει την ικανότητα να αποστείλει τη μολυσμένη ροη μηνυμάτων και να θεωρηθεί επιτυχημένη η επίθεση.

Σε περίπτωση αλληλοεπικάλυψης των μηνυμάτων του επιτιθέμενου και της εξουσιοδοτημένης συσκευής, η ροη των δεδομένων της απάντησης θα παραληφτεί κατεστραμμένη και μη χρησιμοποιήσιμη (Goje, Gornale and Yannawar, 2007).

4.3.7 Επιθέσεις του Τύπου Man in the Middle

Στην κλασσική υλοποίηση της επίθεσης MiTM, δυο οντότητες που επιθυμούν να επικοινωνήσουν αναμεταξύ τους ξεγελιούνται από την είσοδο μιας τρίτης εχθρικής οντότητας στην αναμεταξύ τους επικοινωνία. Οι δυο οντότητες δεν πρέπει να αντιληφθούν ότι δεν επικοινωνούν αναμεταξύ τους έμμεσα για να είναι επιτυχής η επίθεση. Στην πραγματικότητα, ο επιτιθέμενος ορίζει ένα κλειδί με την κάθε οντότητα στην αρχή της εδραίωσης της επικοινωνίας. Αργότερα, κατά την διάρκεια της επικοινωνίας τους ο επιτιθέμενος είναι ικανός να κρυφακούσει την συνομιλία καθώς και να αλλοιώσει με κάθε τρόπο τα δεδομένα που ανταλλάσσονται ανάμεσα στις δυο οντότητες (Gurulian et al., 2016).

Στην περίπτωση της επικοινωνίας μέσω του πρωτοκόλλου NFC δυο είναι οι πιθανές υλοποιήσεις της συγκεκριμένης επίθεσης. Αρχικά, η μια οντότητα βρίσκετε σε ενεργητική κατάσταση και η δεύτερη σε παθητική. Η ενεργητική οντότητα παράγει το πεδίο ραδιοκυμάτων και αποστέλλει δεδομένα στην δεύτερη συσκευή. Σε περίπτωση που ο δυνητικός εχθρός βρίσκεται σε κοντινή απόσταση από τις δυο συσκευές μπορεί να κρυφακούσει τα δεδομένα που αποστέλλονται. Επίσης, θα πρέπει να

διαταράξει με τέτοιο τρόπο το παραγόμενο πεδίο έτσι ώστε η δεύτερη οντότητα να μην παραλάβει τα δεδομένα που αποστάλθηκαν. Ιδιαίτερα επίφοβο για την επιτυχία της επίθεσης καθώς η οντότητα που βρίσκεται σε ενεργητική κατάσταση και αποστέλλει τα δεδομένα είναι σε θέση να ανιχνεύσει αν τα δεδομένα φτάνουν στην δεύτερη οντότητα. Σε περίπτωση που ανιχνεύσει κάποια ανωμαλία τερματίζει το πρωτόκολλο συμφωνίας κλειδιού που έχει εδραιωθεί (Key Agreement Protocol).

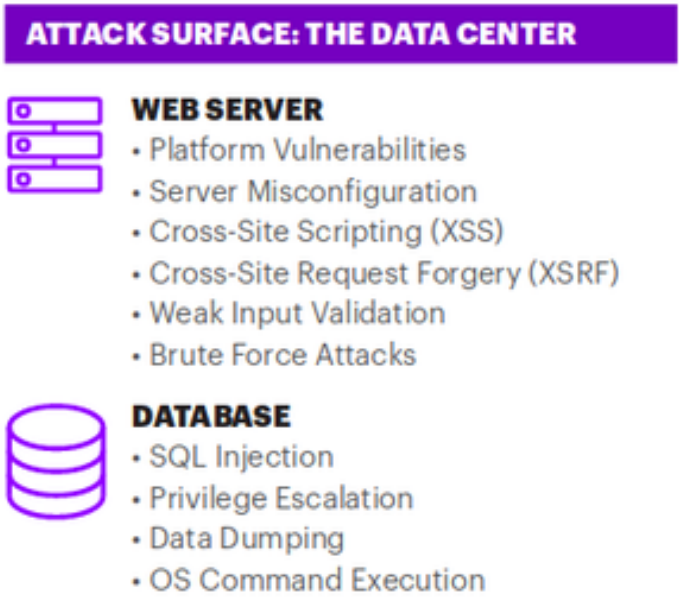
Αν η ενεργητική συσκευή δεν ανιχνεύσει κάποια ανωμαλία το πρωτόκολλο συνεχίζεται. Μόνο τότε ο επιτιθέμενος έχει την ικανότητα να αποστείλει δεδομένα στην παθητική συσκευή. Καθώς υπάρχει το ήδη παραγόμενο πεδίο ραδιοκυμάτων από την ενεργητική συσκευή ο επιτιθέμενος θα πρέπει να δημιουργήσει ένα δικό του καινούργιο πεδίο. Όμως, είναι σχεδόν αδύνατον να διατηρηθούν και να ευθυγραμμιστούν τα δυο παραγόμενα πεδία με αποτέλεσμα τα δεδομένα που αποστέλλονται στην παθητική συσκευή να μην κατέχουν πληροφορία άξια χρήσης. Δεδομένου της ικανότητας της ενεργητικής συσκευής να ανιχνεύει τυχόν ανωμαλίες στο πεδίο ραδιοκυμάτων καθώς και την δυσκολία διατήρησης των δυο πεδίων καθιστά την συγκεκριμένη επίθεση πρακτικά αδύνατη.

Στην δεύτερη υλοποίηση, οι δυο συσκευές-οντότητες βρίσκονται σε ενεργητική κατάσταση. Σε αυτή την περίπτωση η συσκευή Α αποστέλλει δεδομένα στην συσκευή Β. Ο επιτιθέμενος θα πρέπει να διακόψει την επικοινωνία της συσκευής Α προς την Β έτσι ώστε η Β να μην παραλάβει τα δεδομένα που αποστάλθηκαν από την συσκευή Α. Όπως και στην προηγούμενη περίπτωση η συσκευή που αποστέλλει τα δεδομένα έχει την ικανότητα να ανιχνεύσει τον επιτιθέμενο και να διακόψει την επικοινωνία. Στην περίπτωση που δεν ανιχνεύθει κάποια ανωμαλία η συσκευή Α συνεχίζει κανονικά την αποστολή των δεδομένων. Ως επόμενο βήμα ο επιτιθέμενος θα πρέπει να αποστείλει δεδομένα στην συσκευή Β. Καθώς και οι δυο συσκευές βρίσκονται σε ενεργητική κατάσταση, η συσκευή Α αφού αποστείλει τα δεδομένα παύει το παραγόμενο πεδίο ραδιοκυμάτων. Ο επιτιθέμενος ενεργοποιεί το δικό του πεδίο ραδιοκυμάτων για να αποστείλει τα αλλοιωμένα δεδομένα στην συσκευή Β. Όμως εκείνη την χρονική στιγμή και οι δυο συσκευές βρίσκονται σε κατάσταση παραλαβής δεδομένων με αποτέλεσμα και η συσκεύη Α να παραλάβει τα αλλοιωμένα δεδομένα. Ως αποτέλεσμα η συσκευή Α ανιχνεύει την μη εξουσιοδοτημένη αποστολή δεδομένων και διακόπτει την επικοινωνία.
Λόγω των παραπάνω λόγων είναι πρακτικά αδύνατη η επιτυχής υλοποίηση της επίθεσης MiTM σε πραγματικές συνθήκες (Mehrnezhad M. et al,2014).

4.4 Πιθανές Επιθέσεις Ενάντια στο Δίκτυο Πληρωμών

Ο τελευταίος και πολυπλοκότερος στόχος επίθεσης ενός δυνητικού εχθρού, σύμφωνα με το σχήμα 24, αποτελεί το ίδιο το τραπεζικό δίκτυο. Με σκοπό να αποκτήσει τα δεδομένα που ¨ταξιδεύουν' εντός του τραπεζικού δικτύου ο επιτιθέμενος στοχεύει είτε τους διαδικτυακούς διακομιστές εκμεταλλευόμενος τυχόν λάθη στην διαμόρφωση του διακομιστή ή στις τυχόν αδυναμίες της ίδιας της πλατφόρμας ή εκτελώντας επιθέσεις ωμής βίας (Brute Force Attack). Επίσης, κατά την διάρκεια επικοινωνίας της εφαρμογής πληρωμών με τους διακομιστές του δικτύου πληρωμών είναι πιθανή η εκμετάλλευση πιθανών αδυναμιών επιβεβαίωσης των εισαγόμενων δεδομένων του χρήστη καθώς και εκτέλεση επιθέσεων Cross Site Scripting και Cross Site Request Forgery.

Ο δεύτερος πιθανός στόχος εντός του τραπεζικού δικτύου αποτελούν οι ενδιάμεσες βάσεις δεδομένων. Ένας δυνητικός εχθρός μπορεί να επιτεθεί στις εν λόγω ενδιάμεσες βάσεις δεδομένων εκτελώντας επιθέσεις βάση των μεθόδων SQL Injection ή με την ανύψωση δικαιωμάτων εντός της βάσης δεδομένων ή με την εκτέλεση εντολών λειτουργικού (OS Command Execution) ή εκτελώντας μεθόδους Data Dumping με σκοπό την απόκτηση ενός μη εξουσιοδοτημένου αντίγραφου της βάσης δεδομένων, η οποία επί το πλείστων κατέχει δεδομένα πληρωμής και ευαίσθητα προσωπικά δεδομένων των χρηστών.



Σχήμα 24: Ευπάθειες των βάσεων δεδομένων και των ενδιάμεσων διακομιστών του τραπεζικού δικτύου (Source: Accenture Consulting)

Στα πλαίσια της εν λόγω πτυχιακής εργασίας δίνεται περισσότερο έμφαση στις επιθέσεις που στοχεύουν το πρωτόκολλο επικοινωνίας αναμεταξύ της συσκευής και του τερματικού πληρωμής με σκοπό την εξουσιοδότηση και την εκτέλεση της συναλλαγής και στις επιθέσεις ενάντια στους κρυπτογραφικούς μηχανισμούς και το Ασφαλές Περιβάλλον Εκτέλεσης της συσκευής TEE.

4.5 Απαιτήσεις Ασφάλειας Εφαρμογών Ανέπαφων Συναλλαγών

Τα επίπεδα ασφάλειας που διακατέχουν οι περισσότερες εφαρμογές υλοποιούν βασικές διεργασίες με σκοπό την διασφάλιση της ασφάλειας του χρήστη. Μερικές από αυτές είναι η διασφάλιση των ορισμένων εξουσιοδοτήσεων, μεθόδους συμμετρικής κρυπτογράφησης, βασική ανίχνευση της κατάστασης της συσκευής (π.χ. αν η κινητή συσκευή βρίσκεται σε κατάσταση υπερχρήστη κ.α.) και τέλος υλοποιήσεις μεθόδων SSL Pinning.

Καθώς όμως τα συστήματα ανέπαφων συναλλαγών μέσω κινητών συσκευών επεξεργάζονται και αποθηκεύουν δεδομένα και πληροφορίες αυξημένης πληροφοριακής αξίας που αφορούν είτε τον ίδιο τον χρήστη είτε πληροφορίες για τον τραπεζικό του λογαριασμό είναι λογικό να αποτελούν στόχους υψηλής σημασίας για τους δυνητικούς εχθρούς. Όπως είναι λογικό τα συστήματα αυτά θα πρέπει να διακατέχονται από ένα συγκριτικά υψηλότερο επίπεδο ασφάλειας από ότι τα υπόλοιπα συστήματα καθώς επεξεργάζονται πληροφορίες που έχουν απευθείας αντίκτυπο στους τραπεζικούς λογαριασμούς των χρηστών και στο γενικότερο τραπεζικό σύστημα.

Όπως είναι λογικό, απαιτούνται δικλείδες ασφαλείας, οι οποίες ενισχύουν την πολυπλοκότητα και καθιστούν δυσκολότερη την εκτέλεση μιας επίθεσης. Παραδείγματος χάρη, αποδοτικότερη ανίχνευση της κατάστασης της συσκευής, SSL Pinning σε συνδυασμό με SSL Stack Checks, πολυπλοκότερη κρυπτογράφηση καθώς και την παρακολούθηση της σύνδεσης μεταξύ συσκευής και διασυνδεδεμένου διακομιστή (Dubey, 2016).

Η κινητή συσκευή και οι τραπεζικές εφαρμογές, που αποτελούν το μέσο για την διεκπεραίωση των ανέπαφων συναλλαγών, θα πρέπει να χαρακτηρίζονται από ένα υψηλό επίπεδο ασφάλειας. Για να είναι εφικτό το παραπάνω εγχείρημα θα πρέπει να διασφαλιστούν τα τρία παρακάτω κομβικά σημεία (Pcisecuritystandards.org, 2017):

- Η ασφάλεια των εισαγόμενων δεδομένων λογαριασμού εντός της συσκευής

- Η ασφάλεια των αποθηκευμένων δεδομένων λογαριασμού που βρίσκονται εντός της συσκευής
- Η ασφάλεια των εξαγόμενων δεδομένων λογαριασμού

Αρχικά, θα πρέπει να διασφαλιστεί η ασφάλεια των δεδομένων λογαριασμού από αναχαιτίσεις κατά την διάρκεια εισαγωγής των πληροφοριών εντός της συσκευής. Η εν λόγω αποτροπή μπορεί να εκπληρωθεί με την χρήση του Ασφαλούς Περιβάλλοντος Εκτέλεσης της συσκευής, το οποίο παραλαμβάνει τα εισαγόμενα δεδομένα μέσω ενός ασφαλούς δίαυλου επικοινωνίας και τα αποθηκεύει εντός του περιβάλλοντος. Το Ασφαλές Περιβάλλον Εκτέλεσης διακατέχεται από δικό του λειτουργικό σύστημα και μονάδες αποθήκευσης, οι οποίες είναι διαχωρισμένες από το λειτουργικό σύστημα της συσκευής. Επιπρόσθετα, η εφαρμογή διεκπεραίωσης των συναλλαγών θα πρέπει να διακατέχεται από μηχανισμούς αποτροπής και άμυνας απέναντι σε επιθέσεις υπερχείλισης της μνήμης της, την εισαγωγή κακόβουλου κώδικα ή οποιαδήποτε άλλη μορφή μη εξουσιοδοτημένης εισαγωγής δεδομένων εντός της εφαρμογής καθώς και μηχανισμούς προστασίας ενάντια σε κακόβουλες εφαρμογές ή διεργασίες που έχουν μολύνει την συσκευή του χρήστη. Τέλος, οι εφαρμογές θα πρέπει να διακατέχονται από ισχυρούς μηχανισμούς επαλήθευσης της ταυτότητας του χρήστη είτε με την εισαγωγή πολύπλοκου κωδικού πρόσβασης κατά την έναρξη της εφαρμογής πληρωμών είτε με την χρήση βιομετρικών μηχανισμών επαλήθευσης (δαχτυλικό αποτύπωμα χρήστη, φωνητική αναγνώριση κ.α.) (Pcisecuritystandards.org, 2017).

Η δεύτερη απαίτηση και προϋπόθεση ασφάλειας των συσκευών ικανών εκτέλεσης ανέπαφων συναλλαγών αποτελεί η αποτροπή μη εξουσιοδοτημένης πρόσβασης στα δεδομένα πληρωμής και τις πληροφορίες του λογαριασμού του χρήστη όταν αυτά βρίσκονται αποθηκευμένα εντός της συσκευής ή βρίσκονται υπό κάποιου είδους επεξεργασία από τις διεργασίες της εφαρμογής. Η συγκεκριμένη προϋπόθεση ασφάλειας εκπληρώνεται με την διασφάλιση της χρήσης είτε του ενσωματωμένου μικροτσίπ του SE είτε με την χρήση του Ασφαλούς Περιβάλλοντος Εκτέλεσης. Ανεξαρτήτως επιλογής αναμεταξύ των δυο παραπάνω μηχανισμών θα πρέπει να διασφαλίζεται η αποτροπή διαρροής δεδομένων πληρωμής ή δεδομένων λογαριασμού εκτός του εξουσιοδοτημένου περιβάλλοντος καθώς και η εξασφάλιση της ασφαλούς διανομής των δεδομένων μεταξύ των εκτελούμενων διεργασιών της εφαρμογής και η ασφαλής αποθήκευση και πρόσβαση στα παρεχόμενα δεδομένα λογαριασμού (Dubey, 2016).

Επιπρόσθετα, η εφαρμογή θα πρέπει να διακατέχεται από μηχανισμούς αποτροπής ενεργειών που μπορεί να επιφέρουν διαρροή πληροφοριών. Παραδείγματος χάρη, κατά την διάρκεια χρήσης της εφαρμογής να μην δίνεται η επιλογή φωτογράφησης της οθόνης (Screenshot) ή η επιλογή της αντιγραφής/επικόλλησης των αναγραφόμενων δεδομένων. Τέλος, όσο τα ευαίσθητα δεδομένα του χρήστη βρίσκονται εντός της συσκευής θα πρέπει να αποκλείεται οποιαδήποτε μορφή διαρροής δεδομένων από μη εξουσιοδοτημένους χρήστες. Επιπρόσθετα, αν τα δεδομένα βρίσκονται αποθηκευμένα για οποιοδήποτε λόγο σε κάποια προσωρινή μνήμη πριν την επεξεργασία ή την εξουσιοδότηση της πληρωμής, η προσωρινή μνήμη θα πρέπει να βρίσκεται εντός κάποιου ασφαλούς περιβάλλοντος.

Ως τελευταία απαίτηση ασφάλειας ορίζεται η αποτροπή αναχαίτισης των δεδομένων λογαριασμού και πληρωμής κατά την διάρκεια της επικοινωνίας με το τερματικό πληρωμής κάνοντας χρήση της μεθόδου Tokenization σε συνδυασμό με μεθόδους συμμετρικής ή ασύμμετρης κρυπτογράφησης (π.χ. αλγόριθμος κρυπτογράφησης RSA) από την χρονική στιγμή που τα δεδομένα εξάγονται από το επιλεχθέν ασφαλές περιβάλλον εκτέλεσης και ¨ταξιδεύουν' προς το τερματικό πληρωμής μέσω του εδραιωμένου καναλιού επικοινωνίας των δυο συσκευών (Loïc Falletta,2017).

Ως συμπληρωματικές δικλείδες ασφάλειας καθώς οι απαιτήσεις ασφάλειας είναι υψηλές, οι συγκεκριμένες εφαρμογές θα πρέπει να διακατέχονται από μεθόδους SSL Pinning με ελέγχους χαμηλού επιπέδου και γραμμένους σε ειδικά σχεδιασμένο κώδικα (Native Code) με σκοπό την δυσκολότερη κατανόηση της λειτουργίας της εφαρμογής από τον εχθρό και τέλος αποδοτικότερη σύνδεση και καταγραφή της ενεργής συνεδρίας της εφαρμογής με τους εξωτερικούς διακομιστές. Επιπρόσθετα, είναι αναγκαία η ανίχνευση και η καταγραφή της συμπεριφοράς της κινητής συσκευής ανάλογα το μοντέλο της καθώς και η δημιουργία ενός ασφαλούς κλοιού εκτέλεσης διεργασιών εντός της συσκευής.

Τέλος, ιδιαίτερα σημαντική είναι η ύπαρξη μεθόδων συσκότισης κώδικα, σε κομβικά σημεία του πηγαίου κώδικα της εφαρμογής, με σκοπό την απόκρυψη πληροφοριών. Επιθυμητή είναι και η ύπαρξη μεθόδων Anti-Tampering για την περαιτέρω προστασία των δεδομένων που υπάρχουν εντός της εφαρμογής ή που δημιουργούνται κατά την εκτέλεση ορισμένων διεργασιών της (Loïc Falletta,2017).

5 Συστήματα και Μεθοδολογίες Ασφαλών Ανέπαφων Συναλλαγών

Στο παρακάτω κεφάλαιο επεξηγούνται και αναλύονται τα πιθανά αντίμετρα στις ευπάθειες που αναφέρθηκαν στο κεφάλαιο 4. Αναφέρονται οι πιθανές λύσεις απέναντι στις πιθανές επιθέσεις που απορρέουν από την ίδια την κινητή συσκευή και τις αδυναμίες του εκάστοτε λειτουργικού συστήματος της συσκευής καθώς και λύσεις και καλές πρακτικές λειτουργίας των εφαρμογών που είναι υπεύθυνες για την πραγμάτωση των ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών καθώς και προσδοκώμενες συμπεριφορές του εκάστοτε χρήστη. Επιπρόσθετα, προτείνονται λύσεις απέναντι στις πιθανές επιθέσεις που μπορεί να πραγματοποιήσει ένας δυνητικός εχθρός ενάντια στο παραγόμενο κανάλι επικοινωνίας καθώς και στο ίδιο το πρωτόκολλο επικοινωνίας μεταξύ της κινητής συσκευής και του τερματικού πληρωμής του εμπόρου.

5.1 Λύσεις και Προτάσεις έναντι σε Πιθανές Ευπάθειες των Εφαρμογών Διεκπεραίωσης Ανέπαφων Συναλλαγών και των Κινητών Συσκευών

Με σκοπό την ενίσχυση της ασφάλειας των εφαρμογών εκτέλεσης ανέπαφων τραπεζικών συναλλαγών καθώς και της ίδιας της συσκευής απαιτείται η εφαρμογή ορισμένων στοχευμένων ενεργειών. Τα κομβικά σημεία που θα αναφέρονται με σκοπό την ενίσχυση της παρεχόμενης ασφάλειας είναι τα παρακάτω:

- Αποτροπή μη εξουσιοδοτημένης λογικής πρόσβασης της συσκευής.
- Δημιουργία ελέγχων από την σκοπιά των διακομιστών καθώς και αναφορά μη εξουσιοδοτημένων προσβάσεων.
- Αποτροπή εξύψωσης δικαιωμάτων.
- Ανίχνευση κλοπής ή απώλειας της συσκευής.
- Ενίσχυση ασφάλειας των παρεχόμενων λειτουργικών συστημάτων της συσκευής και της εφαρμογής πληρωμών.
- Προστασία της συσκευής από γνωστές ευπάθειες, μη εξουσιοδοτημένες εφαρμογές και κακόβουλο λογισμικό.

5.1.1 Αποτροπή μη εξουσιοδοτημένης λογικής πρόσβασης της συσκευής

Η κινητή συσκευή θα πρέπει να προστατεύεται από οποιαδήποτε μορφή μη εξουσιοδοτημένης λογικής πρόσβασης στα δεδομένα και τις λειτουργίες της. Αρχικά, η συσκευή θα πρέπει να κάνει χρήση βιομετρικών μηχανισμών ή πολυπλοκότερων μηχανισμών ξεκλειδώματος όπως περίπλοκοι κωδικοί ξεκλειδώματος ή περίπλοκα μοτίβα ξεκλειδώματος με στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στα δεδομένα της συσκευής. Επιπρόσθετα, η εφαρμογή εκτέλεσης των τραπεζικών συναλλαγών θα πρέπει να απαιτεί από τον χρήστη την επαλήθευση της ταυτότητας του κατά την είσοδο καθώς και κατά την διάρκεια της χρήσης της εφαρμογής πριν την εκτέλεση της συναλλαγής.

Επίσης, θα πρέπει να υπάρχουν μηχανισμοί ανίχνευσής της λειτουργίας USB-Debugging καθώς και μηχανισμοί αποτροπής χρήσης μη αξιόπιστων εφαρμογών με στόχο την προστασία των ευαίσθητων δεδομένων του χρήστη. Οι εφαρμογές διεκπεραίωσης τραπεζικών συναλλαγών θα πρέπει επίσης να διακατέχονται από συγκεκριμένες τεχνικές ενδυνάμωσης που καθιστούν δυσκολότερη την εκτέλεση μεθόδων αντίστροφης μηχανικής σε συνδυασμό με την ύπαρξη εγγενή κώδικα (Native Code) μειώνοντας την επιφάνεια επίθεσης του δυνητικού εχθρού.

Τέλος, οι εν λόγω εφαρμογές θα πρέπει να διακατέχονται από μηχανισμούς ανίχνευσης της ύπαρξης της πλήρους κρυπτογράφησης δίσκου και να μην επιτρέπουν την διεκπεραίωση συναλλαγών αν δεν βρίσκονται σε ισχύ όλοι οι παραπάνω μηχανισμοί (Porcu, G. 2018).

5.1.2 Δημιουργία ελέγχων πρόσβασης και αναφορά μη εξουσιοδοτημένων προσβάσεων

Δημιουργία και ενσωμάτωση ελέγχων, οι οποίοι να είναι ικανοί να αποτρέπουν και να αναφέρουν προσπάθειες μη εξουσιοδοτημένης πρόσβασης στην εφαρμογή πληρωμών καθώς και αναγνώριση και αναφορά μη συνηθισμένων ενεργειών τόσο του χρήστη όσο και της κινητής συσκευής αποτελούν αναγκαία προϋπόθεση ασφάλειας των τραπεζικών συστημάτων. Σε περιπτώσεις όπου παρατηρηθούν μη συνηθισμένες συμπεριφορές είναι δυνατή η παύση της λειτουργίας της εφαρμογής απομακρυσμένα χωρίς την ανάμιξη του τελικού χρήστη. Οι βασικότεροι έλεγχοι είναι η καταγραφή και η υποστήριξη των εξουσιοδοτημένων προσβάσεων στην εφαρμογή, η ικανότητα καταγραφής των συναλλαγών και ικανότητα διαχωρισμού συνηθισμένης από ασυνήθιστης συμπεριφοράς. Τέλος, είναι απαραίτητη η ικανότητα καταγραφής και ενημέρωσης τόσο των χρηστών όσο και των διαχειριστών σε περιπτώσεις όπου παρατηρηθεί ανύψωση δικαιωμάτων, τυχόν αλλαγές στα κλειδιά πληρωμής και τους κρυπτογραφικούς μηχανισμούς, την ενημέρωση περί πολλαπλών λανθασμένων προσπαθειών εισόδου στην εφαρμογή και τέλος για ενημέρωση και καταγραφή τυχόν αναβαθμίσεων της εφαρμογής και του λειτουργικού συστήματος της κινητής συσκευής (Dexter, A. 2016).

5.1.3 Αποτροπή εξύψωσης δικαιωμάτων

Με σκοπό την αποτροπή διαρροής ευαίσθητων δεδομένων και δεδομένων πληρωμής είτε από την ίδια την εφαρμογή είτε από την συσκευή είναι επιθυμητή η ύπαρξη μηχανισμών αποτροπής εξύψωσης δικαιωμάτων εντός της συσκευής. Με την ύπαρξη τέτοιων μηχανισμών είναι εφικτή η αντιμετώπιση παρακάμψεων στις υπάρχουσες εξουσιοδοτήσεις μειώνοντας το εύρος των πιθανών επιθέσεων ενάντια στην συσκευή και στην εφαρμογή εκτέλεσης τραπεζικών συναλλαγών. Επιπρόσθετα, η συσκευή θα πρέπει να διακατέχετε από μηχανισμούς ανίχνευσης της κατάστασης της συσκευής (π.χ. αν η συσκευή έχει υποστεί το λεγόμενο Rooting) καθώς και να παράγει την κατάλληλη ειδοποίηση τόσο στον χρήστη όσο και στους διαχειριστές της εφαρμογής πληρωμών.

Σε περίπτωση που ανιχνευθεί ότι η συσκευή έχει υποστεί ανύψωση δικαιωμάτων ή βρίσκεται σε κατάσταση Rooted λειτουργίας η συσκευή τίθεται σε καραντίνα και η εφαρμογή διεκπεραίωσης συναλλαγών παύει να λειτουργεί με αποτέλεσμα την μείωση της πιθανότητας της έκθεσης των δεδομένων σε κάποιο δυνητικό εχθρό. Τέλος, η εφαρμογή θα πρέπει να διακατέχεται από την ικανότητα αναγνώρισης των απαραίτητων και μόνο διαδικασιών που είναι απαραίτητες για την λειτουργία της και να εξουσιοδοτεί μόνο αυτές (Pcisecuritystandards.org, 2017).

5.1.4 Ανίχνευση κλοπής ή απώλειας της συσκευής

Με γνώμονα την ενίσχυση της παρεχόμενης ασφάλειας των δεδομένων πληρωμής του χρήστη η συσκευή θα πρέπει να διακατέχεται από διεργασίες ανίχνευσης και αναφοράς σε περιπτώσεις απώλειας ή κλοπής της συσκευής του χρήστη. Παραδείγματος χάρη, η χρήση και η σύγκριση της γεωγραφικής θέσης του χρήστη σύμφωνα με την καταγεγραμμένη συμπεριφορά και τοποθεσία της συσκευής καθώς και την εφαρμογή περιορισμών λειτουργίας της εφαρμογής ανάλογα την γεωγραφική της θέση. Η αυθεντικοποίηση της συσκευής και του χρήστη θα πρέπει να γίνεται ανά τακτά χρονικά διαστήματα σε συνδυασμό με μηχανισμούς ανίχνευσης των χρονικών στιγμών όπου η συσκευή είναι ενεργοποιημένη (Dexter, 2016).

5.1.5 Ενίσχυση ασφάλειας του λειτουργικού συστήματος της συσκευής και της εφαρμογής πληρωμών

Τόσο η συσκευή όσο και η εφαρμογή που διαχειρίζεται τις τραπεζικές συναλλαγές θα πρέπει να διακατέχουν λειτουργίες και μηχανισμούς ασφάλειας όπως κρυπτογράφηση των δεδομένων, την ασφαλή αποθήκευση και επεξεργασία των δεδομένων πληρωμής εντός κάποιου ασφαλούς και διαχωρισμένου περιβάλλοντος (προτείνεται η χρήση είτε του SE είτε του TEE) καθώς και διαχωρισμός της παρεχόμενης μνήμης από την μνήμη του κυρίους λειτουργικού συστήματος.

Επιπρόσθετα, η συσκευή και η εφαρμογή διεκπεραίωσης ανέπαφων τραπεζικών συναλλαγών θα πρέπει να διακατέχονται από αμυντικούς μηχανισμούς αποτροπής ενσωμάτωσης κακόβουλου κώδικα εντός του σώματος κώδικα της εφαρμογής καθώς και μηχανισμούς αποτροπής και αναφοράς εκτέλεσης μεθόδων αντιστροφής μηχανικής της εν λόγω εφαρμογής. Όλοι οι παραπάνω μηχανισμοί ασφάλειας

έχουν ως κύριο σκοπό την αποτροπή έκθεσης και διαρροής των δεδομένων πληρωμής και της συναλλαγής και την αποτροπή μη εξουσιοδοτημένης λογικής πρόσβασης στα δεδομένα της συσκευής και της εφαρμογής πληρωμών (Dexter, 2016)(Pcisecuritystandards.org, 2017).

5.1.6 Προστασία της συσκευής από γνωστές ευπάθειες, μη εξουσιοδοτημένες εφαρμογές και κακόβουλο λογισμικό

Με σκοπό την συνεχή προστασία της συσκευής θα πρέπει η συσκευή και η εφαρμογή πληρωμών να βρίσκονται συνεχώς ενημερωμένες από μεριάς λογισμικού μέσω έμπιστων πηγών με σκοπό την αποφυγή εκμετάλλευσης γνωστών ευπαθειών της συσκευής και της εφαρμογής από κάποιο δυνητικό εχθρό Με την συνεχόμενη ανά τακτά διαστήματα ενημέρωση λογισμικού τόσο της συσκευής όσο και της εφαρμογής μεγιστοποιείται η πιθανότητα αποφυγής επιθέσεων μνήμης, ενσωμάτωσης κακόβουλου κώδικα, αντίστροφης μηχανικής καθώς και μόλυνσης της συσκευής από κακόβουλο λογισμικό καθώς η συσκευή και η εφαρμογή ενημερώνονται τακτικά. Οι ενημερώσεις θα πρέπει να λαμβάνονται από έμπιστες πηγές και να γίνεται μια αρχική εκτίμηση της ασφάλειας τους από τον τελικό χρήστη.

Επίσης, οι συσκευές θα πρέπει να είναι εξοπλισμένες με εφαρμογές άμυνας ενάντια σε ιούς κινητών συσκευών, κακόβουλο λογισμικό και εφαρμογές Antispyware καθώς και λογισμικά ενίσχυσης της ιδιωτικότητας σε συνδυασμό με αξιόπιστες λύσεις αυθεντικοποίησης των χρηστών με σκοπό την ολοκληρωτική προστασία από τις συνεχόμενα εξελισσόμενες απειλές λογισμικού (Pcisecuritystandards.org, 2017)(Porcu, G. 2018)(Dexter, 2016).

Συμπερασματικά, για να θεωρηθεί μια κινητή συσκευή και μια εφαρμογή υπεύθυνη για την διεκπεραίωση ανέπαφων τραπεζικών συναλλαγών ασφαλή θα πρέπει να χαρακτηρίζεται από τα παρακάτω στοιχεία:

1. Σωστή χρήση της κινητής πλατφόρμας και των λειτουργιών της.
2. Ασφαλής αποθήκευση των ευαίσθητων δεδομένων πληρωμής του χρήστη.
3. Ασφαλής μηχανισμοί αυθεντικοποιήσης της ταυτότητας του τελικού χρήστη.
4. Έμπιστους και λειτουργικούς κρυπτογραφικούς μηχανισμούς.
5. Στοχευμένη εξουσιοδότηση χρηστών.
6. Ποιότητα του κώδικα πυρήνα της εφαρμογής.
7. Ανθεκτικότητα και ενημέρωση του χρήστη απέναντι σε προσπάθειες εκτέλεσης αντίστροφης μηχανικής στην χρησιμοποιούμενη εφαρμογή.
8. Οχύρωση του κώδικα της εφαρμογής και της συσκευής απέναντι σε πιθανές επιθέσεις.

5.2 Λύσεις και Προτάσεις έναντι σε Πιθανές Επιθέσεις στο Πρωτόκολλο NFC

5.2.1 Επιθέσεις Προώθησης-Relay Attacks

Οι προτάσεις ασφάλειας και τα αντίμετρα που προτείνονται για την αποφυγή και την αντιμετώπιση επιθέσεων του τύπου Relay Attack βασίζονται σε τρείς κύριες κατηγορίες.

Η πρώτη κατηγορία αποτελείται από την επιπρόσθετη αυθεντικοποίηση του χρήστη είτε με την μορφή κωδικού είτε με την μορφή μεθόδων βιομετρικής επαλήθευσης. Η συγκεκριμένη μέθοδος απαιτεί περαιτέρω διάδραση του χρήστη με την εφαρμογή, η οποία σε μερικές περιπτώσεις αναιρεί την ευκολία και την ταχύτητα των ανέπαφων συναλλαγών.

Η δεύτερη προσέγγιση αποτελεί την μέτρηση και την παρακολούθηση της χρονικής διάρκειας της αποστολής και παραλαβής δεδομένων στην εγκαθιδρυμένη επικοινωνία. Όπως είναι λογικό, η εναλλαγή μηνυμάτων ανάμεσα σε τρεις συσκευές (συσκευή χρήστη, συσκευή επιτιθέμενου, τερματικό συναλλαγής) απαιτεί παραπάνω χρόνο από ότι η εναλλαγή μηνυμάτων ανάμεσα σε δύο συσκευές. Ως αμυντικός μηχανισμός μπορεί να θεωρηθεί ο ορισμός ενός ανώτατου κατωφλίου χρονικής απόκρισης

έτσι ώστε η επικοινωνία να διακόπτεται σε περίπτωση που ανιχνευθεί περαιτέρω καθυστέρηση.

Η τρίτη και τελευταία πρόταση ασφάλειας αποτελεί η δέσμευση της απόστασης μεταξύ των συσκευών που επικοινωνούν. Η μεταξύ τους απόσταση υπολογίζεται μέσω κρυπτογραφικών διεργασιών, οι οποίοι βρίσκονται στο επίπεδο της φυσικής σύνδεσης. Οι διεργασίες αυτές παράγουν κρυπτογραφημένα Bit πληροφορίας και αποστέλλουν τα δεδομένα αναμεταξύ τους σε υψηλές ταχύτητες με σκοπό να υπολογίσουν την απόλυτη απόσταση.

Θεωρητικά αποτελεί το αποδοτικότερο αντίμετρο σε τέτοιου είδους επιθέσεις, πρακτικά όμως λόγω των διεργασιών που εκτελούνται στα ανώτερα επίπεδα, η απόλυτη απόσταση που υπολογίζεται δεν είναι πάντα σωστή (Bocek et al., 2016, Matthew A. Crossman, Hong Liu,2016).

5.2.2 Eavesdropping–Κρυφάκουσμα Δεδομένων

Όπως αναφέρθηκε και παραπάνω το πρωτόκολλο επικοινωνίας του NFC δεν κατέχει ενσωματωμένους μηχανισμούς αντιμετώπισης επιθέσεων Eavesdropping. Αξίζει να αναφερθεί ότι τα δεδομένα που αναμεταδίδονται σε παθητική λειτουργία είναι τάξης δυσκολότερη η αναχαίτιση τους. Όμως η χρήση μόνο της παθητικής λειτουργίας δεν εξυπηρετεί ολόκληρο το εύρος των απαραιτήτων εφαρμογών που αναμεταδίδουν ευαίσθητα δεδομένα.

Η μονή πραγματική αντιμετώπιση του σεναρίου επίθεσης είναι η εδραίωση ενός ασφαλούς καναλιού επικοινωνίας. Λόγω της προστασίας που προσφέρει το συγκεκριμένο πρωτόκολλο εναντία σε επιθέσεις MiTM η διαδικασία εδραίωσης ενός ασφαλούς καναλιού επικοινωνίας κατέχει μικρή πολυπλοκότητα. Μπορούν να χρησιμοποιηθούν πρωτοκολλά όπως το πρωτόκολλο Diffie-Hellmann βασισμένο στον αλγόριθμο κρυπτογράφησης RSA ή στην μεθοδολογία των Elliptic Curves για την παράγωγη και τον διαμοιρασμό ενός μυστικού κλειδιού μεταξύ των δυο συσκευών.

Επειδή, όπως προαναφέρθηκε δεν μπορεί να πραγματοποιηθεί σε πραγματικά σενάρια η επίθεση MiTM, η μορφή του Diffie-Hellmann, η οποία δεν απαιτεί αυθεντικοποίηση, αποτελεί την καλύτερη λύση. Με το διαμοιρασμένο κλειδί μπορεί να δημιουργηθεί ένα συμμετρικό κλειδί όπως το 3DES ή το AES το όποιο μετέπειτα χρησιμοποιείται για να ασφαλίσει το κανάλι επικοινωνίας προσφέροντας ένα αποδοτικό επίπεδο εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των αποσταλθέντων δεδομένων (Badra et al,2016).

5.2.3 Data Corruption-Διαφθορά Δεδομένων

Συσκευές με ικανότητες NFC έχουν την ικανότητα να αντιμετωπίσουν την αλλοίωση των δεδομένων λόγω της ικανότητας τους να ελέγχουν το παραγόμενο πεδίο ραδιοκυμάτων ενώ αποστέλλουν δεδομένα.

Η ικανότητα τους να ανιχνεύουν τέτοιου είδους επιθέσεις απορρέει από το γεγονός ότι για να μπορέσει ο επιτιθέμενος να παραλλάξει τα δεδομένα που αποστέλλονται χρειάζεται μεγάλη ποσότητα ενεργείας κάτι που γίνεται αντιληπτό από τις συσκευές που επικοινωνούν. Ως αποτέλεσμα κάθε τέτοιου είδους επίθεση μπορεί να ανιχνεύει σχετικά εύκολα (Raina, 2017).

5.2.4 Data Modification-Παραποίηση Δεδομένων

Όπως στα παραδοσιακά συστήματα έτσι και στα συστήματα που έχουν ως κύριο μέσο την κινητή συσκευή, η παραποίηση δεδομένων αποτελεί μια ενεργητική επίθεση με στόχο την διαμόρφωση και την παραλλαγή είτε των αποσταλθέντων δεδομένων είτε τον τελικό προορισμό τους. Ουσιαστικά, ο επιτιθέμενος αποσκοπεί είτε η εξουσιοδοτημένη συσκευή-δέκτης να παραλάβει τα παραποιημένα δεδομένα είτε τα δεδομένα αυτά να αποσταλθούν σε άλλη συσκευή, παραποιώντας τον header προορισμού των δεδομένων.

Προστασία εναντία στην παραλλαγή των δεδομένων μπορεί να επιτευθεί με ποικίλους τρόπους. Αρχικά, χρησιμοποιώντας ταχύτητες την τάξης των 106k Baud σε ενεργητική λειτουργία καθιστά σχεδόν αδύνατο από τον επιτιθέμενο να αλλάξει όλα τα δεδομένα που αποστέλλονται μέσω του πεδίου ραδιοκυμάτων που δημιουργείται από την συσκευή.

Η προστασία των δεδομένων του χρήστη από επιθέσεις παραποίησης δεδομένων προϋποθέτει ότι και οι δυο συσκευές που επικοινωνούν θα πρέπει να βρίσκονται σε ενεργητική κατάσταση για να είναι προστατευμένες πλήρως. Όμως το κύριο μειονέκτημα είναι το γεγονός ότι οι συσκευές που βρίσκονται σε ενεργητική κατάσταση είναι πιο ευάλωτες σε επιθέσεις Eavesdropping. Επιπρόσθετα, η προστασία που προσφέρεται δεν είναι ολοκληρωμένη καθώς είναι πιθανή η παραλλαγή μερικών δεδομένων κατά την διάρκεια της συνομιλίας.

Ο δεύτερος τρόπος αντιμετώπισης της επίθεσης είναι η ικανότητα των συσκευών να ελέγχουν το παραγόμενο πεδίο ραδιοκυμάτων ενώ αποστέλλουν δεδομένα. Αυτό σημαίνει ότι η συσκευή που εκείνη την στιγμή αποστέλλει δεδομένα ταυτόχρονα ελέγχει και το πεδίο για τυχόν ανωμαλίες. Σε περίπτωση ανίχνευσης ανωμαλίας μια από τις δυο συσκευές έχει την ικανότητα διακοπής της επικοινωνίας ανά πάσα στιγμή.

Ως τρίτος τρόπος αντιμετώπισης ορίζεται η δημιουργία ενός ασφαλούς καναλιού επικοινωνίας όπως προαναφέρθηκε και στην περίπτωση του Eavesdropping (Chattha, 2014).

5.2.5 Data Insertion-Εισχώρηση Δεδομένων

Η συγκεκριμένη επίθεση βασίζεται σε εφαρμογές ή λειτουργίες της κινητής συσκευής, οι οποίες είναι ευπαθείς στο λεγόμενο "Data Injection". Ο επιτιθέμενος με κατάλληλες μεθόδους και εργαλεία είναι σε θέση να ενσωματώσει στον ήδη υπάρχον κώδικα, εντολές που είναι ικανές να του παραχωρήσουν ευαίσθητα δεδομένα του χρήστη. Σε μια τραπεζική εφαρμογή ή στο πρωτόκολλο του NFC η συγκεκριμένη επίθεση έχει ως στόχο είτε το ενεργό κλειδί πληρωμής ή τα προσωπικά στοιχεία του εκάστοτε χρήστη.

Σε αυτό το σενάριο προτείνονται τρεις πιθανές αντιμετωπίσεις. Ως πρώτη ορίζεται η ικανότητα της συσκευής-δέκτη των πληροφοριών να απαντάει απευθείας χωρίς καθυστέρηση ώστε να αποκλείσει τον επιτιθέμενο από το να απαντήσει γρηγορότερα. Ακόμα και στην περίπτωση που ο επιτιθέμενος καταφέρει να φτάσει την ταχύτητα της εξουσιοδοτημένης συσκευής καμία από τις δυο ροές δεδομένων δεν θα φτάσει σωστά στην άλλη συσκευή.

Ως δεύτερο αντίμετρο μπορεί να θεωρηθεί το άκουσμα του καναλιού επικοινωνίας από την συσκευή-δέκτη καθόλη την διάρκεια της επικοινωνίας. Έτσι είναι πιθανότερη η ανίχνευση του επιτιθέμενου την στιγμή που προσπαθεί να εισάγει δεδομένα στο κανάλι.
Ως τρίτο αντίμετρο προτείνεται η εδραίωση ενός ασφαλούς καναλιού επικοινωνίας (Goje, Gornale and Yannawar, 2007).

5.2.6 Εδραίωση διαμοιραζόμενου κλειδιού εντός της παραγόμενης επικοινωνίας μέσω του πρωτοκόλλου NFC - NFC Specific Key Agreement

Έκτος από το μηχανισμό εδραίωσης κλειδιού είναι πιθανή η ενσωμάτωση ενός ειδικού μηχανισμού εδραίωσης κλειδιού πάνω στο πρωτόκολλο του NFC. Ο μηχανισμός αυτός δεν απαιτεί κάποιου είδους ασύμμετρης κρυπτογραφίας και έτσι μειώνεται σημαντικά η απαιτουμένη υπολογιστική δύναμη. Θεωρητικά επίσης προσφέρει και απολυτή ασφάλεια.

Η τεχνολογία ειδικού μηχανισμού εδραίωσης κλειδιού "Specific Key Agreement" λειτουργεί σε περιπτώσεις χρήσης του 100% του εύρους και δεν αποτελεί μέρος του προτύπου που έχει οριστεί από την ISO. Η ιδέα είναι ότι και οι δυο συσκευές που λαμβάνουν μέρος στην επικοινωνία αποστέλλουν τυχαία δεδομένα την ιδία στιγμή. Στην φάση του στησίματος της επικοινωνίας, οι δυο συσκευές συγχρονίζονται όσον αφόρα το εύρος και τις φάσεις του πεδίου ραδιοκυμάτων. Αυτό είναι εφικτό καθώς οι συσκευές έχουν την ικανότητα να αποστέλλουν και να λαμβάνουν δεδομένα ταυτόχρονα (Abd Allah, M. 2011).

Μετά το συγχρονισμό, οι συσκευές μπορούν να αποστείλουν δεδομένα την ιδία χρονική στιγμή στο ίδιο εύρος και φάσεις του πεδίου. Καθώς αποστέλλονται τυχαία Bit 0 και 1 κάθε συσκευή ακούει το πεδίο των ραδιοκυμάτων. Την στιγμή που και οι δυο συσκευές αποστέλλουν 0 το άθροισμα του σήματος ισούται με 0. Αυτό έχει ως αποτέλεσμα ο δυνητικός εχθρός να μην μπορεί να χρησιμοποιείσαι τα αποσταλθέντα δεδομένα. Το ίδιο ισχύει και στις περιπτώσεις που οι δυο συσκευές αποστέλλουν

Bit αξίας 1.

Αρχίζει και αποκτά ενδιαφέρον την στιγμή που η μια συσκευή αποστέλλει 1 και η δεύτερη 0. Σε αυτή την περίπτωση οι δυο συσκευές έχουν επίγνωση τι δεδομένα αποστέλλονται λόγω του συγχρονισμού τους. Ο δυνητικός εχθρός μπορεί να διακρίνει μόνο το άθροισμα που προκύπτει από τα ραδιοκύματα και δεν είναι σε θέση να διακρίνει τι δεδομένα έστειλε η κάθε συσκευή.

Η ασφάλεια της συγκεκριμένης υπόθεσης και υλοποίησης εξαρτάται από την ποιότητα του συγχρονισμού ανάμεσα στις δυο συσκευές. Προφανώς, στην περίπτωση που ο επιτιθέμενος είναι σε θέση να διακρίνει τι δεδομένα στέλνει η μια από τις δυο συσκευές τότε το πρωτόκολλο παραβιάζεται. Τα δεδομένα που αποστέλλονται πρέπει να βρίσκονται σε συμφωνία φάσης και εύρους. Από την στιγμή που οι διαφορές ανάμεσα στις δυο συσκευές πέσουν κάτω από το επίπεδο του θορύβου τότε το πρωτόκολλο θεωρείται ασφαλές.

Επιπρόσθετα, η ασφάλεια του πρωτόκολλου ορίζεται και από την ποιότητα του δέκτη. Ο συγχρονισμός των δυο συσκευών μπορεί να πραγματοποιηθεί στην περίπτωση που τουλάχιστον μια από τις δυο συσκευές είναι σε ενεργητική κατάσταση την ώρα του συγχρονισμού.(Haselsteiner, Ernst & Semiconductors, Philips, 2006)

Επιθέσεις	Στόχος Επίθεσης	Αντίμετρο
Eavesdropping-Κρυφάκουσμα	Κανάλι Επικοινωνίας	Ασφαλές Κανάλι Επικοινωνίας
Interception Attacks-Επιθέσεις Αναχαίτισης	Κανάλι Επικοινωνίας	Ασφαλές Κανάλι Επικοινωνίας
Data Corruption-Διαφθορά Δεδομένων	Δεδομένα	Ανίχνευση Καναλίου Επικοινωνίας για Μεταβολές στα Επίπεδα Ενέργειας
Data Modification-Παραποίηση Δεδομένων	Δεδομένα	Χρήση Ρυθμού Μετάδοσης της Τάξης των 106k Baud
Data Insertion-Εισχώρηση Δεδομένων	Δεδομένα	Ελάχιστη Καθυστέρηση, Άκουσμα του Καναλίου Επικοινωνίας
Επιθέσεις του Τύπου Man in the Middle	Δεδομένα, Κανάλι Επικοινωνίας	Ενεργητική-Παθητική Επικοινωνία, Άκουσμα του Καναλίου Επικοινωνίας

Πίνακας 2: Επιθέσεις Ενάντια στο πρωτόκολλο επικοινωνίας, οι Στόχοι τους και πιθανά Αντίμετρα

Ο παραπάνω πίνακας δείχνει συγκεντρωτικά τις πιθανές επιθέσεις που μπορούν να πραγματοποιηθούν ενάντια στο πρωτόκολλο NFC, το στόχο της εκάστοτε επίθεσης καθώς και τα πιθανά αντίμετρα. Οι πιθανοί στόχοι ενός δυνητικού εχθρού αποτελούν τα παρακάτω:

- Το κανάλι επικοινωνίας
- Τα μεταφερόμενα δεδομένα εντός και εκτός της συσκευής
- Συνδυασμός των παραπάνω

Σύμφωνα με τον παραπάνω πίνακα και με συμπεράσματα που συλλέχθηκαν κατά την διάρκεια της έρευνας που πραγματοποιήθηκε οι πιθανές επιθέσεις που μπορεί να πραγματοποιηθεί ένας δυνητικός εχθρός στο κανάλι επικοινωνίας που δημιουργείται κατά την εκτέλεσης της συναλλαγής με το τερματικό πληρωμής του εμπόρου είναι το κρυφάκουσμα των δεδομένων που ταξιδεύουν στο κανάλι καθώς και οι επιθέσεις αναχαίτισης των μεταφερόμενων δεδομένων.
Σύμφωνα με τις πληροφορίες που συλλέχθηκαν οι παραπάνω επιθέσεις αντιμετωπίζονται με την δημιουργία και την υλοποίηση ενός ασφαλούς καναλιού επικοινωνίας μεταξύ της συσκευής και του τερματικού πληρωμής.

Συνεχίζοντας την συγκεντροποίηση των συμπερασμάτων που δημιουργήθηκαν από το παραπάνω κεφάλαιο, οι επιθέσεις που στοχεύουν είτε στην παραποίηση είτε στην διαφθορά είτε στην εισχώρηση δεδομένων στα δεδομένα της συναλλαγής μπορούν να αντιμετωπιστούν με την χρήση μεγαλύτερης

ταχύτητας εκπομπής των δεδομένων, με την ανίχνευση ανωμαλιών στο παραγόμενο κανάλι επικοινωνίας και τέλος με το άκουσμα του καναλιού επικοινωνίας και την ελαχιστοποίηση της καθυστέρησης απόκρισης μεταξύ των συσκευών αντίστοιχα.

Τέλος, η επίθεση που στοχεύει και στα παραγόμενα δεδομένα και στο κανάλι επικοινωνίας είναι οι επιθέσεις MiTM όμως η εν λόγω επίθεση είναι αντιμετώπιση εγγενώς από το σύστημα λόγω των χαρακτηριστικών που διέπουν τις ενεργητικές και τις παθητικές συσκευές που λαμβάνουν και αποστέλλουν δεδομένα κατά την διάρκεια της συναλλαγής.

6 Μελέτες Περίπτωσης Ηλεκτρονικών Πορτοφολιών

Ολοκληρώνοντας την ανάλυση της αρχιτεκτονικής, της λειτουργικότητας, των ευπαθειών και των απαιτήσεων ασφάλειας καθώς και τις προτεινόμενες λύσεις ενάντια σε αυτές όσον αφορά τα συστήματα ανέπαφης διεκπεραίωσης τραπεζικών συναλλαγών μέσω κινητών συσκευών αναφέρονται και επεξηγούνται οι διασημότερες εφαρμογές που υποστηρίζουν τα εν λόγω συστήματα και δεν αποτελούν λύσεις που έχει προσφέρει το δίκτυο τραπεζών.

Επεξηγείται η διαδικασία εγγραφής, αυθεντικοποιήσης καθώς και τα μέτρα προστασίας που διέπουν τόσο τις εφαρμογές όσο και το λειτουργικό σύστημα της εκάστοτε συσκευής για την ύπαρξη μιας ολοκληρωμένης οπτικής γωνίας. Ανάλογα την εφαρμογή και το λειτουργικό σύστημα της εφαρμογής αναφέρονται και πιθανές επιθέσεις στις εν λόγω συσκευές έχοντας γνώμονα τις πληροφορίες και τα δεδομένα που συλλέχθηκαν κατά την διάρκεια της έρευνας και της εκπόνησης της παρούσας πτυχιακής εργασίας.

6.1 Apple Pay

Η εφαρμογή Apple Pay είναι η λύση που προσφέρει η Apple για την διεκπεραίωση συναλλαγών μέσω κινητής συσκευής. Είναι σχεδιασμένη να προστατεύει τις ευαίσθητες πληροφορίες του χρηστή καθώς και να επιτρέπει την διεκπεραίωση ηλεκτρονικών αγορών.
Η εν λόγω εφαρμογή συνδυάζει ένα πλήθος από ήδη υπάρχουσες τεχνολογίες και μεθόδους ασφάλειας, τα όποια επιτρέπουν στον χρηστή την ασφαλή εκτέλεση τραπεζικών συναλλαγών.

6.1.1 Καταχώρηση κάρτας-Card Enrolment

Το πρώτο βήμα στην χρήση της εφαρμογής απαιτεί την καταχώρηση των στοιχείων μιας χρεωστικής ή πιστωτικής κάρτας εντός της εφαρμογής.

Βήματα καταχώρησης:

1. Ο χρήστης εισάγει τις πληροφορίες της κάρτας είτε με την πληκτρολόγηση των στοιχείων της είτε με το τράβηγμα μιας φωτογραφίας, στην όποια φαίνονται καθαρά τα στοιχειά της κάρτας.

2. Η συσκευή λαμβάνει τις πληροφορίες που εισήχθηκαν και της αποστέλλει μέσω ενός ασφαλούς καναλιού στους διακομιστείς της Apple μαζί με δεδομένα που αφορούν τον χρήστη και την συσκευή την όποια χρησιμοποιεί.

3. Η τράπεζα λαμβάνει τις πληροφορίες και καλείται να εξακριβώσει αν η εν λόγω κάρτα είναι γνήσια ή όχι. Η συγκεκριμένη διαδικασία συνήθως εκτελείται σε συνεργασία με τον πάροχο του δίκτυο πληρωμών. Οι πληροφορίες που λήφθηκαν θα περάσουν από έναν έλεγχο επικινδυνότητας για την εξακρίβωση της γνησιότητας του αιτήματος καθώς και αν η χρεωστική ή πιστωτική κάρτα ανήκει στον χρηστή από τον όποιον κατατέθηκε το αίτημα. Αυτή η διαδικασία ελαχιστοποιεί τις πιθανότητες άπατης καθώς η ιδία κάρτα έχει την δυνατότητα να καταχωρηθεί σε πάνω από μια συσκευές.

4. Αφού εξακριβωθεί η γνησιότητα του αιτήματος καταχώρησης, η τράπεζα επικοινωνεί με τον πάροχο του δικτύου πληρωμής για την δημιουργία ενός μοναδικού κλειδιού που θα αντιπροσωπεύει την εν λόγω κάρτα.

5. Δημιουργείται ένας μοναδικός αριθμός λογαριασμού (DAN-Device Account Number) για την συγκεκριμένη κάρτα και συσκευή. Έπειτα αποστέλλονται τα παραχθέντα δεδομένα πίσω στους διακομιστές της εταιρείας σε συνδυασμό με ένα κρυπτογράφημα, το όποιο θα χρησιμοποιηθεί για την δημιουργία ασφαλών κωδικών κατά την διάρκεια μιας συναλλαγής.

Τα δεδομένα αποθηκεύονται στην μνήμη της συσκευής για μελλοντική χρήση.

6.1.2 Διαδικασία πληρωμής (Payment Process)

Για την έναρξη της διαδικασίας πληρωμής, απαιτείται από τον χρήστη η τοποθέτηση της συσκευής σε κοντινή απόσταση από το τερματικό πληρωμής, το όποιο κατέχει δυνατότητες NFC. Η Apple βασίζεται στο λεγόμενο Touch ID για την επιβεβαίωση της ταυτότητας του χρηστή.

Βήμα 1: Αφού επιλεχθεί η κάρτα που θα χρησιμοποιηθεί για την συναλλαγή φορτώνεται ο αριθμός DAN στο ασφαλές περιβάλλον εκτέλεσης SE. Η Apple υποστηρίζει δυνατότητες αναπαραγωγής EMV μικροτσίπ και δημιουργεί ένα δυναμικό κρυπτογράφημα.

Βήμα 2: Ο έμπορος αποστέλλει την πληροφορία προς την τράπεζα που είναι υπεύθυνη για την διεκπεραίωση της συναλλαγή.

Βήμα 3: Η τράπεζα λαμβάνει τον αριθμό DAN χωρίς να μπορεί να ξεχωρίσει εάν επρόκειτο για τον αριθμό λογαριασμού ή αν είναι κάποιο κλειδί. Αφού λάβει αυτές τις πληροφορίες, επιβεβαιώνει τον τραπεζικό αναγνωριστικό αριθμό και αποστέλλει ένα πακέτο πληροφοριών προς την τράπεζα έκδοτη της κάρτας μέσω του δικτύου πληρωμών.Το δίκτυο αυτό αποτελεί τον μεσάζοντα μεταξύ της τράπεζας που θα εκτελέσει την συναλλαγή και την τράπεζα έκδοτη της κάρτας.

Βήμα 4: Το δίκτυο πληρωμής είναι ικανό να ξεχωρίσει τον αριθμό DAN από τον πραγματικό αριθμό λογαριασμού. Από την στιγμή που θα αναγνωρίσει την φύση του αριθμού που έλαβε θα προωθήσει στον πάροχο των υπηρεσιών κλειδιού το αίτημα για την αποστολή του πραγματικού αριθμού λογαριασμού πίσω στην τράπεζα έκδοτη.

Βήμα 5: Η τράπεζα εκδότης θα επιβεβαιώσει ή θα απορρίψει την συναλλαγή και θα αποστείλει την κατάλληλη ειδοποίηση πίσω στον έμπορο με την μορφή μηνύματος στην οθόνη του τερματικού του POS.

6.1.3 Αυθεντικοποίηση χρήστη (User Identification)

Η αυθεντικοποίηση του χρηστή στην συσκευή είναι απαραίτητη για να εκτελεστεί μια τραπεζική συναλλαγή. Η αυθεντικοποίηση γίνεται είτε μέσω της εισαγωγής του δακτυλικού αποτυπώματος του χρηστή πάνω στον βιομετρικό αισθητήρα της συσκευής είτε με την εισαγωγή του κωδικού πρόσβασης της συσκευής.

Ο σκοπός αυτού του έλεγχου είναι η μείωση των δυνατοτήτων της συσκευής σε περίπτωση κλοπής. Η είσοδος τέτοιων δικλείδων ασφάλειας αποτελεί ένα βήμα παραπέρα από την ασφάλεια που διακατέχουν τα παραδοσιακά συστήματα ανέπαφων συναλλαγών όπου σε περίπτωση κλοπής της κάρτας υπάρχει δυνατότητα χρήσης της χωρίς την ύπαρξη αυθεντικοποίησης.

6.1.4 Αυθεντικοποίηση συσκευής (Device Authentication)

Κάθε συναλλαγή που εκτελείται μέσω του Apple Pay αντιστοιχίζεται σε μια μοναδική τιμή, η όποια εξασφαλίζει ότι η συναλλαγή προέρχεται από αξιόπιστη και εξουσιοδοτημένη συσκευή. Η μοναδική αυτή τιμή σε συνδυασμό με το παραγόμενο κρυπτογράφημα διασφαλίζουν ότι η εν λόγω κάρτα δεν μπορεί να χρησιμοποιηθεί από άλλη συσκευή παρά μόνο από αυτή που είναι καταχωρημένη.

Επιπλέον, τα κλειδιά λαμβάνουν τιμές ανάλογα το χρηματικό ποσό της αγοράς που εκτελείται. Με αυτή την λεπτομέρεια το ίδιο κλειδί (Token) δεν μπορεί να χρησιμοποιηθεί από ένα επιτιθέμενο για διαφορετική συναλλαγή.

6.1.5 Προστασία δεδομένων (Data Protection)

Η εφαρμογή προσφέρει προστασία των δεδομένων της με τους ακολούθους τρόπους:

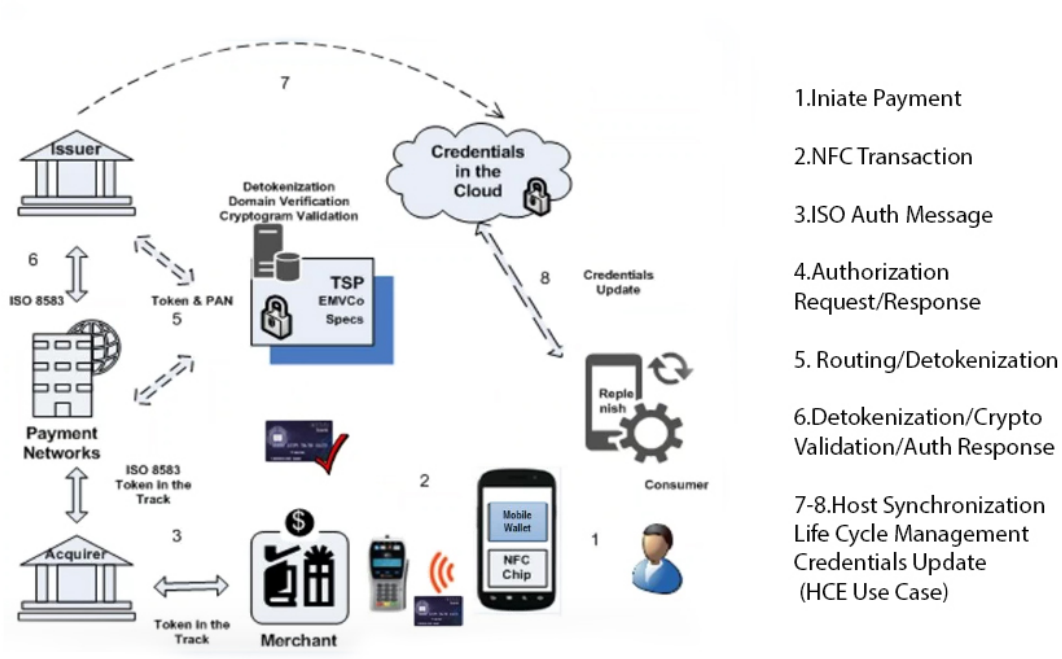
- **Tokenization:** Κατά την διάρκεια της διαδικασίας καταχώρησης της κάρτας στην συσκευή, δημιουργείται ένα μοναδικός αριθμός αναγνώρισης ή κλειδί (Token), ο όποιος αποθηκεύεται στη μνήμη της συσκευής και χρησιμοποιείται κατά την εκτέλεση μιας συναλλαγής.
  Όσο εκτελείται η συναλλαγή, ο πραγματικός αριθμός λογαριασμού της κάρτας καθώς και ο κωδικός αναγνώρισης της κάρτας δεν χρησιμοποιούνται ποτέ. Αυτή η δικλείδα ασφάλειας εξασφαλίζει την μείωση του κίνδυνου απόκτησης ευαίσθητων πληροφοριών της κάρτας και του χρήστη και επιτρέπει της γρήγορη ακύρωση της συσκευής σε περίπτωσης απώλειας της.
  Επίσης προστατεύει τον χρήστη από αναξιόπιστους έμπορους, οι όποιοι λόγω της προαναφερθείσας δικλείδας ασφάλειας δεν έρχονται ποτέ σε επαφή με τον αριθμό λογαριασμού της κάρτας ή με το CVC.

- **Αξιοποίηση του Secure Element:** Το Secure Element είναι τοποθετημένο στις συσκευές της Apple και αποτελεί ένα ασφαλές απαραβίαστο μικροτσίπ. Σε περίπτωση ανίχνευσης προσπάθειας εισβολής στα δεδομένα του μηδενίζει την μνήμη του και εξαλείφει την πιθανότητα συγκομιδής δεδομένων.
- **Κρυπτογράφηση επικοινωνίας:** Τα δεδομένα της χρεωστικής ή πιστωτικής κάρτας αποστέλλονται από το δίκτυο πληρωμών ή τον έκδοτη της κάρτας κρυπτογραφημένα χρησιμοποιώντας εφαρμογές που βρίσκονται εντός του SE.
- **Υλικό:** Κατά την διάρκεια της συναλλαγής , το τερματικό επικοινωνεί απευθείας με το SE, μέσω του πεδίου που δημιουργείται από το NFC, με την χρήση ενός αποκλειστικού δίαυλου επικοινωνίας που προέρχεται από τις δυνατότητες που προσφέρει το υλικό στις συσκευές της εταιρείας.

Στο σχήμα 25 περιγράφεται η αλληλουχία ενεργειών που εκτελούνται με την εκτέλεση μιας ανέπαφης συναλλαγής μέσω μιας εξουσιοδοτημένης εφαρμογής είναι η ακόλουθη.
Αρχικά, ο χρήστης εκκινεί την πληρωμή κάνοντας χρήση του μικροελεγκτή NFC που βρίσκεται εντός της συσκευής εγκαθιδρύοντας μια σύνδεση με το μηχάνημα POS του εμπόρου. Το τερματικό πληρωμής αποστέλλει τις απαραίτητες πληροφορίες στην τράπεζα του εμπόρου για επιβεβαίωση.

Η τράπεζα του εμπόρου μέσω του δικτύου πληρωμών στέλνει το αίτημα πληρωμής στον TSP πάροχο με σκοπό να επικοινωνήσει με την τράπεζα του εκδότη της κάρτας του χρήστη. Αφού εγκριθεί η συναλλαγή, ο TSP επιστρέφει, μέσω της διαδικασίας του De-Tokenization, το πραγματικό αριθμό λογαριασμού του χρήστη στην τράπεζα και μέσω του ίδιου καναλιού επικοινωνίας αποστέλλει στο τερματικό πληρωμής του εμπόρου αν η συναλλαγή εγκρίθηκε ή απορρίφθηκε.

Σε περιπτώσεις χρήσης του HCE, η συσκευή πρέπει να επικοινωνήσει στην αρχή και στο τέλος της συναλλαγή με το περιβάλλον νεφοϋπολογιστικής, το οποίο διατηρεί τα δεδομένα πληρωμής, για τον συγχρονισμό και την ανανέωση των κλειδιών πληρωμής.



Σχήμα 25: Χρήση εφαρμογής για την διεκπαιρέωση ανέπαφης συναλλαγής (Source:Global Platform)

6.1.6 Παρεχόμενη Ασφάλεια του Λειτουργικού Συστήματος και της Εφαρμογής Πληρωμών

Όσον αφορά τα χαρακτηριστικά ασφάλειας του λειτουργικού συστήματος που προσφέρει η Apple οι προϋποθέσεις και οι απαιτήσεις ασφάλειας που έχει θέσει η εταιρεία καθιστούν το εν λόγω λειτουρ-

γικό σύστημα ως ένα από τα ασφαλέστερα της αγοράς. Το μοντέλο ασφάλειας που χρησιμοποιείται στις κινητές συσκευές της εταιρείας είναι βασισμένες στη δομή του TrustedBSD και κάνει χρήση του υποχρεωτικού ελέγχου πρόσβασης (Mandatory Access Control - MAC) με σκοπό την μείωση των ικανοτήτων των εφαρμογών και των δυνατοτήτων του τελικού χρήστη. Επιπρόσθετα, το λειτουργικό σύστημα υλοποιεί την μέθοδο του Sandboxing για τις παρεχόμενες εφαρμογές πληρωμών. Η συγκεκριμένη μέθοδος λειτουργεί παρέχοντας σε κάθε εφαρμογή συγκεκριμένες προσβάσεις σε αρχεία, πόρους δικτύου και υλικού. Κάθε εφαρμογή εγκαθίσταται σε διαφορετικό αποθετήριο εντός του λειτουργικού συστήματος, το οποίο λειτουργεί ως το κεντρικό αποθετήριο της εφαρμογής και των παραγόμενων δεδομένων της.

Όσον αφορά τους παρεχόμενους ελέγχους πρόσβασης και τις παρεχόμενες προσβάσεις η εφαρμογή διεκπεραίωσης τραπεζικών συναλλαγών έχει πρόσβαση σε συγκεκριμένους πόρους συστήματος εντός του δικού της αποθετηρίου με αποτέλεσμα τον ασφαλή αποκλεισμό από τις υπόλοιπες εφαρμογές. Επιπρόσθετα, κάθε προσπάθεια ανύψωσης δικαιωμάτων παρακολουθείται και σε περιπτώσεις ανίχνευσης ανύψωσης δικαιωμάτων εμφανίζει μήνυμα αποδοχής ή απόρριψης στην οθόνη του χρήστη (Porcu, 2018). Η αποθήκευση των βασικών δεδομένων της εφαρμογής γίνεται σε εσωτερικές βάσεις δεδομένων ενώ τα ευαίσθητα δεδομένα της συσκευής αποθηκεύονται εντός του ασφαλούς περιβάλλοντος με σκοπό την αποτροπή διαρροής δεδομένων. Η αυθεντικοποιήση του χρήστη της εφαρμογής γίνεται μέσω βιομετρικών μεθόδων κατά την έναρξη της εφαρμογής καθώς και σε με διεκπεραίωση συναλλαγής με αποτέλεσμα την επιβεβαίωση της ταυτότητας του τελικού χρήστη. Σε περιπτώσεις όπου η αυθεντικοποιήση του χρήστη δεν είναι διαθέσιμη η εφαρμογή απορρίπτει την συναλλαγή.

Τέλος, εκτελείται αυθεντικοποίηση της συσκευής του χρήστη με ποικίλες μεθόδους, όπως την εξακρίβωση της γεωγραφικής τοποθεσίας και της συμπεριφοράς της συσκευής, και κρυπτογραφείται το παραγόμενο κανάλι επικοινωνίας μεταξύ της συσκευής και του τερματικού πληρωμής σε συνδυασμό με την μέθοδο του Tokenization με σκοπό την οχύρωση των μεταφερόμενων δεδομένων πληρωμής (Dexter, 2016).

6.1.7 Πιθανά Σενάρια Επίθεσης

Σύμφωνα με αναλυτές, έχουν βρεθεί δυο πιθανά σενάρια επίθεσης ενάντια στην εφαρμογή πληρωμών που προσφέρει η Apple, αναφέροντας πιθανές αδυναμίες στην μέθοδο πληρωμής.

Η πρώτη επίθεση στοχεύει μια κινητή συσκευή που έχει υποστεί Jailbreak και την μολύνει με κακόβουλο λογισμικό. Έχοντας εγκαταστήσει το κακόβουλο λογισμικό είναι δυνατή η αναχαίτιση των δεδομένων κίνησης προς κάποιον διακομιστή της εταιρείας, τα οποία εμπεριέχουν πληροφορίες χρήστη και δεδομένα πληρωμής. Η επίθεση θεωρείται επιτυχής από την στιγμή που ο εχθρός καταφέρει να μολύνει την κινητή συσκευή με κακόβουλο λογισμικό με δικαιώματα υπερχρήστη.

Η δεύτερη μορφή επίθεσης, δεν απαιτεί από τη συσκευή να βρίσκεται σε κατάσταση Jailbreak, καθώς μπορεί να εκτελεστεί σε όλες τις συσκευές. Ο δυνητικός εχθρός στοχεύει στην αναχαίτιση ή στην τροποποιήση των δεδομένων πληρωμής, τα οποία βρίσκονται σε κίνηση. Αρχικά, ο εχθρός θα πρέπει να αναχαιτίσει το κλειδί πληρωμής από την συσκευή του χρήστη.

Για να επιτευχθεί η αναχαίτιση του κλειδιού ο εχθρός δελεάζει τον χρήστη να εισέλθει σε κάποιο δημόσιο δίκτυο ή σε κάποιο πλαστό και να εκτελέσει μια ανέπαφη αγορά. Έχοντας εισέλθει στο δίκτυο, ο εχθρός είναι σε θέση να ανακτήσει το κρυπτόγραμμα του ApplePay. Έπειτα, ο εχθρός έχει την ικανότητα να παραλλάξει είτε τα στοιχεία πληρωμής είτε να εκτελέσει περαιτέρω αγορές κάνοντας χρήση των στοιχείων του χρήστη (Leyden, 2017).

Αν και τα δυο σενάρια επίθεσης δεν είναι ευπάθειες που απορρέουν από την εφαρμογή καθεαυτή αλλά από το σύνολο της διαδικασίας πληρωμής δεν έχουν ληφθεί από την εταιρεία μέτρα προστασίας. Οι ευπάθειες που αναφέρθηκαν προέρχονται από την άγνοια του χρήστη και του εμπόρου σε βασικές έννοιες και μεθόδους διασφάλισης των δεδομένων. Όμως, οι επιθέσεις είναι υλοποιήσιμες και επικίνδυνες για τον τελικό χρήστη.

6.2 Google Wallet/Android Pay

Στα πρώιμα σταδία της κυκλοφορίας της εφαρμογής, η αποθήκευση των ευαίσθητων πληροφοριών του χρηστή γινόταν εντός του ασφαλούς περιβάλλοντος της συσκευής. Το 2015 η εταιρεία αλλάζει κατεύθυνση όσον αφορά την αποθήκευση των δεδομένων και μεταφέρει την διαδικασία της αποθήκευσης σε περιβάλλοντα νεφοϋπολογιστικής. Επιπρόσθετα υλοποιεί ριζικές αλλαγές και στο τρόπο με τον όποιο ο χρήστης αυθεντικοποιείται . Οι παραπάνω αλλαγές επέφεραν τεράστιες αλλαγές όσον αφορά την αρχιτεκτονική των συστημάτων πληρωμών της εταιρείας.

6.2.1 Καταχώρηση κάρτας (Card Enrolment)

Η ταυτοποίηση του χρηστή προτού εκτελεστεί η καταχώρηση της τραπεζικής κάρτας είναι απαραίτητη για την χρήση της εφαρμογής. Η ταυτοποίηση του χρηστή γίνεται από την τράπεζα, η όποια και αποφασίζει αν η εν λόγω κάρτα ανήκει στον χρηστή που καταχώρησε το αίτημα.

Οι παρακάτω τρόποι προσφέρονται για την ταυτοποίηση του χρηστή:

1. Ταυτοποίηση μέσω μηνύματος ηλεκτρονικού ταχυδρομείου ή γραπτού μηνύματος.
2. Ταυτοποίηση μέσω τηλεφωνικής συνομιλίας με την τράπεζα-εκδότη.
3. Ταυτοποίηση μέσω της εφαρμογής της τράπεζας.

Ο χρήστης θα πρέπει να είναι ενήμερος ότι κατά την διάρκεια της καταχώρησης της κάρτας, ο αριθμός της κάρτας αποστέλλεται και αποθηκεύεται στους διακομιστείς της Google.

6.2.2 Διαδικασία πληρωμής (Payment Process)

Στις πρώτες εκδόσεις της, η εφαρμογή έκανε χρήση ενός μοντέλου βασισμένου κατά κόρον στο ασφαλές περιβάλλον της συσκευής για την αποθήκευση κρυπτογραφημένων ευαίσθητων πληροφοριών, όπως τα στοιχειά του κατόχου της κάρτας και κωδικούς επιβεβαίωσης με τη μορφή Token εντός της συσκευής.

Μετά την απόφαση για ριζική αλλαγή των συστημάτων της, η εταιρεία αποφάσισε ότι οι κινητές συσκευές δεν πληρούν τα απαραίτητα κριτήρια ασφάλειας και για αυτό το λόγο μεταφέρθηκαν οι απαραίτητες, για την διεκπεραίωση τραπεζικών συναλλαγών, λειτουργίες σε περιβάλλον νεφοϋπολογιστικής.

Βήματα διαδικασίας πληρωμής:
Προτού ξεκινήσει η διαδικασία πληρωμής, η συσκευή συνδέεται με τους διακομιστείς της εταιρείας με σκοπό να της παραχωρηθούν ένα πλήθος από κλειδιά (Token) πληρωμής.

Βήμα 1: Όταν ο χρήστης θα πλησιάσει το τερματικό POS, η υπηρεσία HCE ενεργοποιεί τον NFC αναμεταδότη της συσκευής. Ο συγκεκριμένος αναμεταδότης θα αναλάβει την επικοινωνία μεταξύ της συσκευής και του τερματικού.Τέλος ένα δυναμικό Token και ένα κρυπτογράφημα αποστέλλονται προς το τερματικό.

Βήμα 2: Ο έμπορος αποστέλλει τις πληροφορίες που έλαβε μέσω του τερματικού στην τράπεζα που έχει αναλάβει την συναλλαγή.

Βήμα 3: Η τράπεζα λαμβάνει το κρυπτογράφημα και το κλειδί πληρωμής και τα αποστέλλει στην τράπεζα έκδοτη της κάρτας μέσω του δικτύου πληρωμών.

Βήμα 4: Το δίκτυο πληρωμών θα απαιτήσει τον πραγματικό αριθμό λογαριασμού της συσκευής (PAN) από την υπηρεσία TSP και θα τα αποστείλει στην τράπεζα έκδοτη για επιβεβαίωση.

Βήμα 5: Η τράπεζα-εκδότης θα απορρίψει ή θα επιβεβαιώσει την συναλλαγή και θα αποστείλει το κατάλληλο μήνυμα στην οθόνη του τερματικού του εμπόρου.

6.2.3 Αυθεντικοποίηση χρηστή (User Authentication)

Η εφαρμογή προσφέρει ποικίλους τρόπους αυθεντικοποίησης του χρηστή πριν προβεί σε κάποια συναλλαγή. Μερικές από αυτές περιλαμβάνουν το δακτυλικό αποτύπωμα του χρηστή ή την εισαγωγή του κωδικού πρόσβασης της συσκευής ή του μοτίβου ξεκλειδώματος της συσκευής.

6.2.4 Αυθεντικοποίηση συσκευής (Device Authentication)

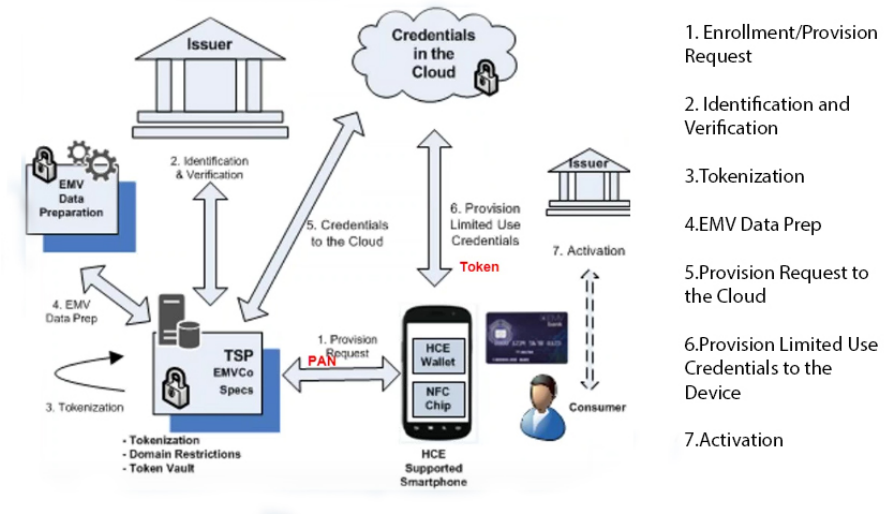
Τα κλειδιά πληρωμής φορτώνονται στη συσκευή εκ των πρότερων πριν την συναλλαγή. Η διαδικασία αυτή επαναλαμβάνεται περιοδικά όταν υπάρχει δυνατότητα διασύνδεσης στο διαδίκτυο. Σαν επιπλέον μετρό, η εφαρμογή είναι σχεδιασμένη να μην λειτουργεί σε συσκευές που βρίσκονται σε λειτουργία υπέρ-χρήστη.

6.2.5 Προστασία δεδομένων (Data Protection)

Καθώς το HCE υποθέτει ότι οποιοδήποτε δεδομένο βρίσκεται αποθηκευμένο στην συσκευή είναι ευάλωτο, αποθηκεύει τις πληροφορίες της κάρτας σε βάσεις δεδομένων σε ασφαλή περιβάλλοντα νεφοϋπολογιστικής.

Για την αποτροπή μη εξουσιοδοτημένων εισόδων στο HCE έχουν οριστεί τέσσερις βασικοί πυλώνες ασφάλειας:

- **Περιορισμενη χρήση κλειδιών ασφάλειας:** Λήγουν σε μικρό χρονικό διάστημα για την αποτροπή μη εξουσιοδοτημένες χρήσης.
- **Tokenization:** Μειώνει το ρίσκο έκθεσης του αριθμού λογαριασμού με την αντικατάσταση του με δεδομένα που ταξιδεύουν στο δίκτυο πληρωμών ανεμπόδιστα.
- **Χρηση δακτυλικού αποτυπώματος:** Για την επιβεβαίωση χρηστή και συσκευής.
- **Αναλυση ρίσκου σε πραγματικό χρόνο:** Για την ανίχνευση ασυνήθιστων ενεργειών από μέρους της συσκευής.



Σχήμα 26: Εξουσιοδότηση εφαρμογής μέσω HCE (Smartcardalliance.org. 2014)

Στο σχήμα 26 αναλύεται η διαδικασία ενσωμάτωσης μιας ανέπαφης κάρτας εντός μιας εφαρμογής ανέπαφων τραπεζικών συναλλαγών που κάνει χρήση του HCE.
Αρχικά, ο χρήστης αποστέλλει ένα αίτημα στην τράπεζα εκδότη της κάρτας του, η οποία αποδέχεται ή απορρίπτει το αίτημα του. Σε περίπτωση αποδοχής αποστέλλει στον πάροχο πληρωμής το λογαριασμό του χρήστη με σκοπό την αντικατάσταση του με το κλειδί πληρωμής μέσω της μεθόδου του Tokenization.

Έπειτα, το κλειδί πληρωμής συμμορφώνεται με τα πρότυπα του EMV και αποστέλλεται για αποδοχή στο περιβάλλον νεφοϋπολογιστικής που υποστηρίζει η εφαρμογή. Το περιβάλλον νεφοϋπολογιστικής αποστέλλει πίσω στην εφαρμογή μια αλληλουχία χρονικά περιορισμένων διαπιστευτηρίων μαζί με ένα προφίλ επικινδυνότητας, Τέλος, μέσω της εφαρμογής αποστέλλονται οι παραπάνω πληροφορίες για την τελική ενεργοποίηση του λογαριασμού του χρήστη.

6.2.6 Παρεχόμενη Ασφάλεια του Λειτουργικού Συστήματος και της Εφαρμογής Πληρωμών

Όσον αφορά την παρεχόμενη ασφάλεια του λειτουργικού συστήματος της Adroid, το λειτουργικό της σύστημα είναι βασισμένο στο λειτουργικό σύστημα των Linux, σε κάθε διεργασία αντιστοιχεί ένα μοναδικό UserId το οποίο προϋποθέτει την δέσμευση του εκάστοτε πόρου του συστήματος στην διαδικασία που εκτελείτε εκείνη την ώρα παρέχοντας ένα επιπλέον χαρακτηριστικό ασφάλειας και τέλος κάθε εφαρμογή τρέχει στο δικό της εικονικό περιβάλλον εντός του συστήματος και ενισχύοντας την παρεχόμενη ασφάλεια.

Όσον αφορά τις προσβάσεις και του ελέγχους πρόσβασης η εκάστοτε εφαρμογή πληρωμών δεν αλληλεπιδρά με το κυρίως λειτουργικό εκτός αν έχει καταγραφεί στο Manifest αρχείο της εφαρμογής. Κάθε εφαρμογή είτε συγκαταλέγεται στην κατηγορία εφαρμογών πληρωμής είτε όχι υπογράφεται από τον προγραμματιστή με σκοπό την μείωση των παραποιημένων εφαρμογών και την μείωση της πιθανότητας μόλυνσης της συσκευής από κακόβουλο λογισμικό. Επιπρόσθετα, η αποθήκευση των δεδομένων της εφαρμογής αποθηκεύονται σε ξεχωριστό αποθετήριο εντός του λειτουργικού και τα δεδομένα πληρωμής καθώς και τα ευαίσθητα δεδομένα του χρήστη αποθηκεύονται εντός του ασφαλούς περιβάλλοντος με αποτέλεσμα την μείωση της έκθεσης των δεδομένων σε πιθανούς εχθρούς (Porcu, 2018).

Η εφαρμογή Google Pay κάνοντας χρήση των παραπάνω μηχανισμών ασφαλείας και με σκοπό την περαιτέρω ενίσχυση της ασφάλειας των τραπεζικών συναλλαγών και δεδομένων του χρήστη έχει ενσωματώσει περαιτέρω μηχανισμούς ασφάλειας εντός της εφαρμογής. Δεν επιτρέπει την λήψη Screenshot σε περιπτώσεις όπου ο χρήστης βρίσκεται εντός της εφαρμογής και χρησιμοποιείται το λεγόμενο Transport Layer Security (TLS) και μεθόδους κρυπτογράφησης με σκοπό την ασφαλή αναμετάδοση των δεδομένων του χρήστη, όχι προς το τερματικό πληρωμής αλλά προς κάποιον Backend διακομιστή, και την μείωση της πιθανότητας παρέμβασης στην επικοινωνία.

Τέλος, η παρεχόμενη εφαρμογή πληρωμών αντιμετωπίζει της επιθέσεις εξύψωσης δικαιωμάτων υλοποιώντας την παρεχόμενη λειτουργία του λειτουργικού συστήματος να διαχωρίζει την κάθε εφαρμογή εντός του δικού της εικονικού περιβάλλοντος και με το να αναγκάζει την κάθε εφαρμογή να αιτείται τους απαιτούμενους πόρους του συστήματος. Οποιαδήποτε μη συμμόρφωση με τα παραπάνω αποτελεί κρίσιμη ευπάθεια του συστήματος και της εφαρμογής πληρωμών (Dexter, 2016).

6.3 Samsung Pay

Η συγκεκριμένη έκδοση ηλεκτρονικού πορτοφολιού εκμεταλλεύεται την τεχνολογία MST(Magnetic Secure Transition) για την διεκπεραίωση αγορών. Η τεχνολογία αυτή έχει την ικανότητα να αναπαριστά μια χρεωστική ή πιστωτική κάρτα που κάνει χρήση της μαγνητικής ταινίας για την διεκπεραίωση συναλλαγών.

Τα κλειδιά πληρωμής αποστέλλονται στο τερματικό POS αφού έχει προηγηθεί η αυθεντικοποίηση του χρήστη στην εφαρμογή. Η χρήση της συγκεκριμένης τεχνολογίας επιτρέπει στις συσκευές να διεκπεραιώνουν αγορές όχι μόνο με την μέθοδο «Tap-and-Pay» αλλά και με το να υιοθετούν τις ιδιότητες μιας μαγνητικής κάρτας.

Αυτόματα η υιοθέτηση αυτής της τεχνικής δίνει την δυνατότητα στη εφαρμογή να επεκτείνει το εύρος λειτουργίας της . Η εφαρμογή Samsung Pay υποστηρίζεται από την πλατφόρμα KNOX της ίδιας εταιρείας για την ασφαλή και κρυπτογραφημένη αποθήκευση των κλειδιών πληρωμής.

6.3.1 Καταχώρηση κάρτας (Card Enrolment)

Κατά την διάρκεια της διαδικασίας καταχώρησης, ο χρήστης θα πρέπει να καταχωρήσει την κάρτα στην εφαρμογή καθώς και να εκτελέσει μια ταυτοποίηση των στοιχείων του.

Ο χρήστης μπορεί να εκτελέσει την ταυτοποίηση είτε με SMS είτε με μήνυμα ηλεκτρονικού ταχυδρομείου είτε με μια κλήση στην τράπεζα του για να του αποσταλθεί ένας κωδικός μια χρήσης (OTP-One Time Password).

Αφού εκτελεστεί η διαδικασία ενσωμάτωσης, απαιτείται μια διαδικασία επαλήθευσης της γνησιότητας της κάρτας μέσω του δικτυού πληρωμών και την τράπεζα έκδοτη της κάρτας. Οι ακόλουθες πληροφορίες μοιράζονται με τον έκδοτη της κάρτας:

- Πληροφοριες λογαριασμού Samsung του χρήστη καθώς και το πλήθος των καρτών που είναι ήδη καταχωρημένες εντός της εφαρμογής.
- Πληροφοριες σχετικές με την συσκευή, όπως το λειτουργικό σύστημα και τον αριθμό του μοντέλου.
- Πληροφοριες τοποθεσίας.
- Πληροφοριες κάρτας και διεύθυνση χρήστη που αποστέλλεται στον εκδότη μέσω των διακομιστών της Samsung.

Ο χρήστης δεν μπορεί να εκτελέσει καμία συναλλαγή μέχρι να ολοκληρωθούν οι παραπάνω ενέργειες.

6.3.2 Διαδικασία πληρωμής (Payment Process)

Η διαδικασία πληρωμής μέσω της εφαρμογής ακολουθεί τα παρακάτω βήματα:

Βήμα 1: Ο χρήστης ξεκινάει την διαδικασία πληρωμής με την τοποθέτηση του ακουστικού της συσκευής σε κοντινή απόσταση από το τερματικό POS. Αυτόματα, η εφαρμογή θα ξεκινήσει την συναλλαγή χρησιμοποιώντας είτε το πρωτόκολλο NFC είτε το πρωτόκολλο MST.

Αφού επιλεχθεί η κάρτα, από την οποία θα εκτελεστεί η συναλλαγή, η συσκευή δημιουργεί τρία κομμάτια πληροφοριών.

- Ένα ηλεκτρονικό κλειδί πληρωμής σχετικό με την εν λόγω κάρτα. Ο σκοπός της δημιουργίας του κλειδιού είναι η απόκρυψη του αριθμού λογαριασμού του χρήστη καθώς και η σωστή δρομολόγηση του αιτήματος μέσω του δικτύου πληρωμών προς τον έκδοτη της κάρτας.
- Ένα μετρητή συναλλαγών, ο όποιος καταχωρείται σε κάθε συναλλαγή και επιτρέπει την αναγνώριση της σειράς των συναλλαγών στον έκδοτη της κάρτας.
- Τέλος, δημιουργείται ένα κρυπτογράφημα αποτελούμενο από το μυστικό κλειδί, το κλειδί πληρωμής και τον μετρητή συναλλαγών.

Βήμα 2: Οι παραπάνω πληροφορίες αποστέλλονται στο τερματικό POS, το όποιο προωθεί τις πληροφορίες στην τράπεζα που θα εκτελέσει την συναλλαγή.

Βήμα 3: Η εν λόγω τράπεζα θα αναγνωρίσει το κατάλληλο δίκτυο πληρωμών και θα προωθήσει τις πληροφορίες της συναλλαγής.

Βήμα 4: Το δίκτυο πληρωμών θα αναγνωρίσει το κλειδί πληρωμής και μέσω του TSP θα ανασύρει τον αντίστοιχο αριθμό λογαριασμού. Έπειτα οι πληροφορίες θα προωθηθούν στην τράπεζα-εκδότη με σκοπό την διεκπεραίωση της συναλλαγής.

Βήμα 5: Ο εκδότης της κάρτας θα επιβεβαιώσει ή θα απορρίψει την συναλλαγή και θα προωθήσει την απόφαση της στην οθόνη του τερματικού.

6.3.3 Αυθεντικοποίηση χρήστη και συσκευής (User & Device Authentication)

Υπάρχουν δυο τρόποι αυθεντικοποίησης του χρήστη στις συσκευές Samsung. Ο ένας τρόπος ορίζει το δακτυλικό αποτύπωμα του χρήστη ως τρόπο αυθεντικοποίησης ενώ ο δεύτερος την εισαγωγή του κωδικού πρόσβασης της συσκευής.

Η εταιρεία προσφέρει ένα πλήθος από μηχανισμούς επαλήθευσης ταυτότητας για την διασφάλιση της ακεραιότητας του κλειδιού πληρωμής κατά την διάρκεια της δημιουργίας του. Τα κλειδιά πληρωμής προσφέρονται στην συσκευή εκ των προτέρων αν υπάρχει διασύνδεση στο διαδίκτυο. Επίσης, η εφαρμογή δεν λειτουργεί σε συσκευές που βρίσκονται σε λειτουργία υπερχρήστη.

6.3.4 Προστασία δεδομένων (Data Protection)

Η προστασία των δεδομένων στις συσκευές βασίζεται στο Firmware KNOX και στο TEE. Το KNOX διαχωρίζει το υλικό της συσκευής σε δυο μέρη:

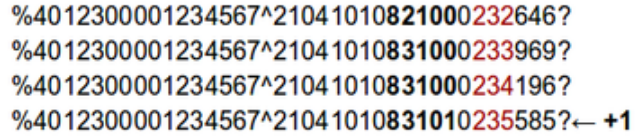
- Κανονική λειτουργία-Normal world
- Ασφαλής λειτουργία-Secure world

Οι αριθμοί λογαριασμών δεν βρίσκονται αποθηκευμένοι στην συσκευή και γίνονται διαθέσιμοι μονάχα κατά την διάρκεια εκτέλεσης μιας συναλλαγής και μόνο προς τον έκδοτη της κάρτας.
Η πιθανότητα διαρροής του αριθμού λογαριασμού είναι ελάχιστη.

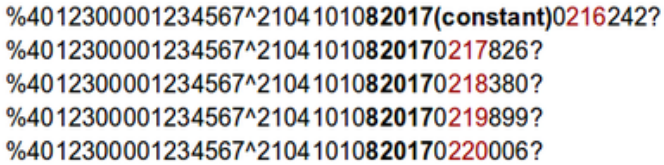
6.3.5 Πιθανά Σενάρια Επίθεσης

Σύμφωνα με πειράματα και μελέτες που διεξάχθηκαν στην εφαρμογή πληρωμών της Samsung ανακαλύφθηκαν δυο πιθανές επιθέσεις ενάντια της εφαρμογής. Η πρώτη επίθεση στοχεύει στο παραγόμενο Token πληρωμής. Καθώς η εφαρμογή μπορεί να εκτελέσει ανέπαφες συναλλαγές ακόμα και σε περιπτώσεις έλλειψης διαδικτυακής σύνδεσης δημιουργήθηκε το ερώτημα της ασφάλειας του παραγόμενου Token και πως εκτελείται η συναλλαγή χωρίς την σύγκριση του Token με τους διακομιστές της εφαρμογής. Η εφαρμογή παράγει το κλειδί πληρωμής κάνοντας χρήση ενός συνδυασμού από πίνακες και τυχαίους αριθμούς για την διασφάλιση διαφορετικών ids για κάθε παραγόμενο κλειδί χωρίς την ύπαρξη κάποιου μοτίβου.

Οι κύριες διαφορές των κλειδιών παρατηρήθηκαν στα τελευταία 4-6 ψηφία καθώς και στις τιμές που βρίσκονται στην μέση. Όταν εκτελούνται συναλλαγές εκτός δικτύου, οι τιμές που βρίσκονται στη μέση δεν αλλάζουν σε αντίθεση με τις συναλλαγές εντός δικτύου, όπου οι τιμές αυξάνονται κατά 1 (βλ. σχήμα 27-28).



Σχήμα 27: Παραγόμενα Token με την ύπαρξη σύνδεσης (Mendoza, 2016)



Σχήμα 28: Παραγόμενα Token χωρίς την ύπαρξη σύνδεσης (Mendoza, 2016)

Καθώς, τα κλειδιά πληρωμής δεν μπορούν να ξαναχρησιμοποιηθούν, ο επιτιθέμενος αναλύοντας πολλά κλειδιά πληρωμής μπορεί να μαντέψει τα επόμενα Token εκτελώντας επιθέσεις Brute-Force , επιθέσεις λεξικού ή κάποια μέθοδο πρόβλεψης.

Ένα δεύτερο σενάριο επίθεσης προβλέπει την χρήση της εφαρμογής για κάποια αγορά και για κάποιο λόγο δεν μπορεί να εκτελεστεί. Το κλειδί πληρωμής που δημιουργήθηκε είναι ακόμα ενεργό και μπορεί να χρησιμοποιηθεί. Ένας δυνητικός εχθρός μπορεί να χρησιμοποιήσει την συγκεκριμένη λειτουργία και να παρεμποδίσει την διαδικασία πληρωμής αναγκάζοντας την εφαρμογή να αποτύχει και να δημιουργήσει το επόμενο Token. Ως αποτέλεσμα, ο επιτιθέμενος μπορεί να χρησιμοποιήσει το προηγούμενο κλειδί πληρωμής για την διενέργεια αγορών χωρίς κανένα περιορισμό (Mendoza, 2016).

7 Συμπεράσματα

Η διεκπεραίωση ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών αποτελεί την εξέλιξη των ανέπαφων τραπεζικών συναλλαγών μέσω πιστωτικής/χρεωστικής κάρτας. Όπως κάθε καινούργια τεχνολογία τραπεζικού ενδιαφέροντος έτσι και η εν λόγω εξέλιξη θα πρέπει να διακατέχεται από ένα αποδεκτό επίπεδο παρεχόμενης ασφάλειας ως προς τον τελικό χρήστη και ταυτόχρονα να παρέχει αποδοτικότητα και ταχύτητα. Καθώς τα συστήματα αυτά γίνονται αποδεκτά από ολοένα και περισσότερους χρήστες είναι επιτακτική η απάντηση στην ερώτηση « Πόσο ασφαλή είναι τελικά τα συστήματα ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών·».

Αναλυτές και επιστήμονες της ασφάλειας πληροφοριών έχοντας διεξάγει μια σειρά πειραμάτων και πιθανών επιθέσεων ενάντια στα συστήματα αυτά, δεν είναι σε θέση να απαντήσουν με απόλυτη σιγουριά την παραπάνω ερώτηση. Εξετάζοντας κάθε συστατικό στοιχείο των συστημάτων αυτών, όπως τους μηχανισμούς άμυνας της κινητής συσκευής ή τους μηχανισμούς και λειτουργίες του τραπεζικού οικοσυστήματος ή τις απαραίτητες ενέργειες του χρήστη για να είναι σε θέση να χρησιμοποιήσει την κινητή συσκευή του για την διεκπεραίωση συναλλαγών, αφήνουν ερωτηματικά ασφάλειας ως προς την ασφάλεια των δεδομένων του χρήστη.

Στην παρούσα πτυχιακή εργασία μελετήθηκαν εκτενώς οι μηχανισμοί άμυνας των κινητών συσκευών ως προς την παρεχόμενη ασφάλεια, τις πιθανές και γνωστές αδυναμίες τους καθώς και διαφορετικές υλοποιήσεις των μηχανισμών αυτών για την ενίσχυση της παρεχόμενης ασφάλειας. Επιπρόσθετα, μελετήθηκαν εκτενώς οι μηχανισμοί και η λογική του τραπεζικού συστήματος ως προς την ασφάλεια που παρέχουν στον τελικό χρήστη. Τέλος, μελετήθηκαν οι διασημότερες εφαρμογές διεκπεραίωσης ανέπαφων συναλλαγών καθώς και γνώστες ευπάθειες και αδυναμίες τους.

Μελετώντας τα συστατικά στοιχεία των συστημάτων ανέπαφης συναλλαγής απορρέουν βασικές ανησυχίες ως προς την παρεχομένη ασφάλεια. Από την μια μεριά υπάρχει μια συσκευή, η οποία έχει χαρακτηριστεί από πολλούς ειδικούς ασφάλειας ως η καταλληλότερη πλατφόρμα επίθεσης και αναχαίτισης των μεταφερόμενων δεδομένων λόγω των πολλαπλών πρωτοκόλλων επικοινωνίας, και από την άλλη ένα τραπεζικό σύστημα που έχει εναποθέσει όλες τις κρίσιμες λειτουργίες ασφάλειας, όπως την διαδικασία του Tokenization και De-Tokenization, την χαρτογράφηση του πραγματικού αριθμού λογαριασμού με το κλειδί πληρωμής καθώς και την διαχείριση του κλειδιού πληρωμής, σε μια και μοναδική οντότητα εντός του τραπεζικού οικοσυστήματος, τον πάροχο υπηρεσιών κλειδιού (TSP).

Ακόμα και αν σε ένα υποθετικό σενάριο αναιρεθούν οι πιθανότητες μιας πετυχημένης επίθεσης ενάντια στα παραπάνω συστατικά στοιχεία, υπάρχει και ο απρόβλεπτος παράγοντας είτε του εμπόρου που δεν έχει υλοποιήσει σε αποδεκτό επίπεδο τις προβλεπόμενες προδιαγραφές ασφάλειας (π.χ. χρήση ίδιου δικτύου για το τερματικό πληρωμής και για το παρεχόμενου δικτύου για τους πελάτες) είτε του ίδιου του χρήστη, ο οποίος επί το πλείστων δεν είναι ενήμερος για σωστές πρακτικές ασφάλειας και διατήρησης της ακεραιότητας των δεδομένων του.

Όσο τα εν λόγω συστήματα ωριμάζουν, όλο και περισσότεροι μηχανισμοί ασφάλειας έχουν ενσωματωθεί τόσο στις κινητές συσκευές όσο και στο ίδιο το τραπεζικό οικοσύστημα για την αποτροπή διαρροής και μη εξουσιοδοτημένης χρήσης των τραπεζικών δεδομένων του χρήστη τέτοιων συστημάτων και εφαρμογών. Ο μόνος αστάθμητος παράγοντας σε όλα τα συστήματα ανεξαιρέτως χρήσης και λειτουργίας αποτελούν οι χρήστες του. Με την κατάλληλη ενημέρωση των ανθρώπινων συστατικών στοιχειών των συστημάτων είναι εφικτή η ύπαρξη ενός υψηλού και ίσως απόρθητου τραπεζικού συστήματος.

Ως μελλοντική συνεισφορά της παρούσας πτυχιακής εργασίας στην επιστημονική και τραπεζική κοινότητα θα μπορούσε να είναι η διεξαγωγή πειραμάτων στις τρέχουσες εφαρμογές εκτέλεσης τραπεζικών συναλλαγών για να εξακριβωθεί κατά πόσο έχουν ακολουθηθεί σωστές πρακτικές ασφάλειας στις εν λόγω εφαρμογές καθώς και αν υπάρχουν ευπάθειες σε κρίσιμα σημεία των εφαρμογών που παρέχονται από τις ελληνικές τράπεζες προς το ευρύ κοινό.

Όπως προκύπτει από την παραπάνω έρευνα, μέχρι να ωριμάσουν εντελώς τα συγκεκριμένα συστήματα τόσο από τεχνολογική άποψη όσο και από την γνώση του τελικού χρήστη για ζητήματα ασφάλειας, η διεκπεραίωση ανέπαφων τραπεζικών συναλλαγών μέσω κινητών συσκευών δεν μπορεί να

θεωρηθεί απόλυτα ασφαλής.

8 Αναφορές

1. Παπαδόπουλος, Μ. (2015). APPLE PAY - Αξιολόγηση Υπηρεσίας και Αποτίμηση Ασφάλειας. pp.3-5.
2. Abd Allah, M. (2011). Strengths and Weaknesses of Near Field Communication (NFC) Technology. Global Journal Of Computer Science And Technology, . Retrieved from https://computerresearch.org/ind
3. Accenture Consulting (2016). Mobile Banking Applications - Security Challenges for Banks. [online] Accenture.com. Available at: https://www.accenture.com/t20180223T145013Z__w__/us-en/_acnmedia/PDF-49/Accenture-Mobile-Banking-Apps-Security-Challenges-Banks.pdf
4. Android Open Source Project. (2014). Full-Disk Encryption Android Open Source Project.[online] Available at: https://source.android.com/security/encryption/full-disk [Accessed 30 Sep. 2018].
5. Apple.com. (2018). iOS Security. [online] Available at: https://www.apple.com/business/site/docs/iOS-Security-Guide.pdf [Accessed 30 Sep. 2018]
6. Badra, M., Badra, R.B. A Lightweight Security Protocol for NFC-based Mobile Payments.Procedia Comput. Sci. 2016, 83, 705–711
7. Beniamini, G. (2017). Trust Issues: Exploiting TrustZone TEEs. [online] Googleprojectzero.blogspot.gr. Available at: https://googleprojectzero.blogspot.gr/2017/07/trust-issues-exploiting-trustzone-tees.html [Accessed 4 May 2018].
8. Bocek, T., Killer, C., Tsiaras, C. and Stiller, B. (2016). An NFC Relay Attack with Off-the-shelf Hardware and Software. Management and Security in the Age of Hyperconnectivity, pp.71-83.
9. Chattha, N. (2014). NFC : Vulnerabilities and defenses. 2014 Conference on Information Assurance and Cyber Security (CIACS).
10. Chen, X., Choi, K. & Chae, K. (2017). A Secure and Efficient Key Authentication using Bilinear Pairing for NFC Mobile Payment Service. Wireless Personal Communications, 97(1), pp.1-17.
11. Dang, F., Zhou, P., Li, Z., Zhai, E., Mohaisen, A., Wen, Q. and Li, M. (2017). Large-scale invisible attack on AFC systems with NFC-equipped smartphones. IEEE INFOCOM 2017 - IEEE Conference on Computer Communications.
12. Dexter, A. (2016). Mobile Security and Payments Infrastructure. cigital.org.
13. Dubey, A. (2016). 19 Security controls in Mobile Banking | TCS Cyber Security Community. [online] Securitycommunity.tcs.com. Available at: https://securitycommunity.tcs.com/infosecsoapbox/articles/20 security-controls-mobile-banking [Accessed 13 Mar. 2018].
14. EMVCo. (2017). 3-D Secure Press Kit - EMVCo. [online] Available at:https://www.emvco.com/media-centre/emv-3ds-press-kit/ [Accessed 21 May 2018].
15. EMVCo. 2015, White Paper on Contactless Mobile Payment
16. Enisa (2018) Security of Mobile Payments and Digital Wallets. [online] pp.10-17. Available at: https://www.enisa.europa.eu/publications/mobile-payments-security [Accessed 11 Jan.2018].
17. En.wikipedia.org. (2017). Contactless smart card. [online] Available at: https://en.wikipedia.org/wiki/Contactle
18. European Payments Council 2017 PAYMENT THREATS AND FRAUD TRENDS REPORT
19. Goje, A., Gornale, S. and Yannawar, P. (2007). Proceedings of the 2nd National Conference on Emerging Trends in Information Technology (eIT-2007). Dist. Pune: Institute of Information Technology.

20. Gomzin, S. (2014). Hacking point of sale. Indianapolis, IN: Wiley.

21. Gurulian, I., Shepherd, C., Markantonakis, K., Akram, R. and Mayes, K. (2016). When Theory and Reality Collide: Demystifying the Effectiveness of Ambient Sensing for NFC-based Proximity Detection by Applying Relay Attack Data.

22. Haselsteiner, Ernst & Semiconductors, Philips. (2006). Security in Near Field Communication (NFC). Workshop on RFID Security.

23. Hillali Wadii, E., Boutahar, J. and EL Ghazi, S. (2017). NFC Technology for Contactless Payment Echosystems. International Journal of Advanced Computer Science and Applications, 8(5).

24. Leyden, J. (2017). Wallet-snatch hack, ApplePay vulnerable to attack Available at: https://www.theregister.co.uv [Accessed 27 Aug. 2017]

25. Loïc Falletta,Practical Attacks against Digital Wallets,April 2017

26. Massoth, M. and Bingel, T. (2011). Performance of different mobile payme nt service concepts compared with a NFC-based solution. [online] Academia.edu. [Accessed 6 Jan. 2019].

27. Matthew A. Crossman, Hong Liu, "Two-factor authentication through near field communication", Technologies for Homeland Security (HST) 2016 IEEE Symposium on, pp. 1-5, 2016.

28. Mehrnezhad, M., Hao, F., & Shahandashti, S. F. Tap-Tap and Pay (TTP): Preventing Man-In-The-Middle Attacks in NFC Payment Using Mobile Sensors. In 2nd International Conference on Research in Security Standardisation (SSR'15) (October 2014)

29. Merkus, J. (2018). Security evaluation of the NFC contactless payment protocol using Model Based testing. [online] Dspace.ou.nl. Available at: https://dspace.ou.nl/bitstream/1820/9768/1/Merkus%20J%2 [Accessed 23 Dec. 2018].

30. Mendoza, S. (2016). Samsung Pay: Tokenized Numbers, Flaws and Issues. [online] Blackhat.com. Available at: https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues.pdf [Accessed 27 Sep. 2018].

31. Nelson, Dakota Qiao, Mengyu & Carpenter, Andrew. (2013). Security of the near field communication protocol: an overview. Journal of Computing Sciences in Colleges. 29. 94-104.

32. Paganini, P. (n.d.). Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema. [online] InfoSec Resources. Available at: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/ [Accessed 17 Feb. 2018].

33. Pasquet, Marc & Reynaud, Joan & Rosenberger, Christophe. (2016). "Payment with mobile NFC phones" How to analyze the security problems.

34. Pcisecuritystandards.org. (2017). PCI Mobi le Payment Acceptance Security Guidelines for Developers.

35. Price, D. (2017). 5 NFC Security Issues to Consider Before Your Next Contactless Payment.[online] MakeUseOf. Available at:https://www.makeuseof.com/tag/nfc-security-contactless-payment-issues/ [Accessed 7 Nov. 2017].

36. Porcu, G. (2018). How to test your mobile applications against security vulnerabilities. [online] Owasp.org. Available at: https://www.owasp.org/images/9/99/GiuseppePorcu-OWASPItalyDay19-10-2018.pdf [Accessed 24 Jan. 2019].

37. Rampton, J. 2016. The evolution of the mobile payment. [online] TechCrunch. Available at: https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment/?guccounter=1 [Accessed 13 Dec. 2018].

38. Raina, V. (2017). NFC Payment Systems and the New Era of Transaction Processing.Hershey: IGI Global.

39. Rajaram, S. (2014). Vulnerability Analysis And Security System For NFC - Enabled Mobile Phones. INTERNATIONAL JOURNA L OF SCIENTIFIC & TE CHNOLOGY RESEARCH, VOLUME 3(ISSUE 6).

40. Reveilhac, M. & Pasquet, M. (2009). Promising Secure Element Alternatives for NFC Technology. 2009 First International Workshop on Near Field Communication.

41. Roland, Michael. (2012). Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?

42. Roos, D. (2017). How Chip and PIN Credit Cards Work. [online] HowStuffWorks. Available at: https://money.howstuffworks.com/personal-finance/debt-management/chip-and-pin-credit-cards1.html [Accessed 10 Mar. 2019].

43. Rosenberg, D. (2017). Reflections on Trusting TrustZone. [online] Blackhat.com. Available at: https://www.blackhat.com/docs/us-14/materials/us-14-Rosenberg-Reflections-on-Trusting-TrustZone.pdf [Accessed 20 Feb. 2018].

44. Securetechalliance.org. (2015). Available at: https://www.securetechalliance.org/wp-content/uploads/EMV-and-NFC-WP-Final-Nov-2015.pdf [Accessed 11 Jan. 2018].

45. Securetechalliance.org. (2017). Mobile Identity Authentication. [online] Available at: https://www.securetechalli Identity-Authentication-WP-FINAL-March-2017.pdf [Accessed 11 Jan. 2018].

46. Siitonen Kortvedt, Henning & Mjølsnes, Stig. (2012). Eavesdropping Near Field Communication.

47. Simon, L. (2017). Exploring new attack vectors for the exploitation of smartphones. Cambridge, England: University of Cambridge.

48. Smartcardalliance.org. (2014). Host Card Emulation (HCE) 101. [online] Available at:http://www.smartcardallia content/uploads/HCE-101-WP-FINAL-081114-clean.pdf [Accessed 11 Jan. 2018].

49. Sorensen, E. (2018). What Are Mobile Payments? And How to Use Them. [online] Square. Available at: https://squareup.com/guides/mobile-payments [Accessed 10 Mar. 2019].

50. Techopedia.com. (2016). What is Two-Factor Authentication? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/13699/twofactor-authentication [Accessed 21 May 2018].

51. Thienes, C. (2016). What's the Difference between Mobile and Digital Wallets? - TMG Financial Services. [online] Tmgfinancialservices.com. Available at: http://www.tmgfinancialservices.com/the-future-of-credit/future-of-credit-blog/whats-the-difference-between-mobile-and-digital-wallets [Accessed 15 Apr. 2018].

52. Uspaymentsforum.org. (2018). U.S. Payments Forum ©201 8 Page 1 Mobile and Digital Wallets : U . S . Landscape and Strategic Considerations for Merchants and Financial Instit ut ions. [online] Available at: http://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf [Accessed 6 Jan. 2019].

53. Vanderhoof, R., Manahan, O., Correa, J., Friedman, A. and Quinn, M. (2018). Smart Card Alliance Webinar to Explore Benefits of Contactless Card and Mobile EMV Payments for US Merchants » Secure Technology Alliance. [online] Securetechalliance.org. Available at: https://www.securetechalliance.org/smart-card-alliance-webinar-to-explore-benefits-of-contactless-card-and-mobile-emv-payments-for-us-merchants/ [Accessed 11 Jan. 2018].

9 Ορισμοί

1. **Token Service Provider (TSP):** Οντότητα η όποια παρέχει υπηρεσίες Token. Έχει δυνατότητες δημιουργίας, χαρτογράφησης και επαλήθευσης των Token από τους αριθμούς λογαριασμών.

2. **Token Cryptogram:** Κρυπτογράφημα με μοναδική τιμή, το όποιο δημιουργείται μέσω του Token πληρωμής, των κλειδιών και επιπρόσθετων δεδομένων με σκοπό την δημιουργία μιας μοναδικής τιμής.

3. **Host Card Emulation (HCE):** Επιτρέπει την διεκπεραίωση ανέπαφων συναλλαγών με το να προσομοιώνει υπηρεσίες ανέπαφων καρτών και να αποθηκεύει τα δεδομένα είτε στην εφαρμογή που χρησιμοποιείται είτε σε κάποια άλλη ασφαλή τοποθεσία όπως το ασφαλές περιβάλλον εκτέλεσης (Trusted Execution Environment) ή σε περιβάλλοντα νεφοϋπολογιστικής.

4. **Trusted Service Manager (TSM):** Μια οντότητα η όποια επιβλέπει την ασφαλή τοποθέτηση των διαπιστευτηρίων συναλλαγής εντός του ασφαλούς περιβάλλοντος (Secure Element) σε κινητές συσκευές.

5. **ID&V:** Μια μέθοδος μέσω της όποιας μια οντότητα μπορεί επιτυχώς να επαλήθευση τον κάτοχο της κάρτας και τον λογαριασμό του με σκοπό την εγκαθίδρυση ενός επίπεδου εμπιστευτικότητας για την σύνδεση του Token και του αριθμού λογαριασμού.

6. **Token Vault:** Ένα αποθετήριο ενσωματωμένο στη διαδικασία του Tokenization το όποιο κατέχει τις πληροφορίες που απαιτούνται για την χαρτογράφηση μεταξύ του Token και του αριθμού λογαριασμού.

7. **Token Requestor:** Μια οντότητα (π.χ. ένα ηλεκτρονικό πορτοφόλι) το όποιο αναζητά να υλοποιήσει την διαδικασία του Tokenization και να ξεκινήσει αιτήματα μετατροπής του αριθμού λογαριασμού μέσω του Tokenization με την τοποθέτηση αιτημάτων στον TSP.

8. **Token Assurance Level:** Τιμή η όποια επιτρέπει στον παροχή υπηρεσιών να αναγνωρίσει το επίπεδο εμπιστευτικότητας της μετάβασης ενός Token σε ένα αριθμό λογαριασμού με κριτήρια όπως την τοποθεσία του τοκεν και του χρηστή.

9. **TCB:** Αποτελεί μια ασφαλή υπολογιστική βάση ενός υπολογιστικού συστήματος, στην οποία βρίσκονται συγκεντρωμένα όλο το υλικό, λογισμικό και σετ εντολών (firmware) που είναι υπεύθυνα για την ασφάλεια του συστήματος. Οποιαδήποτε ανωμαλία ή ευπάθεια εμφανιστεί εντός του TCB μπορεί να καταστήσει ολόκληρο το σύστημα ευάλωτο.

10. **Address space layout randomization (ASLR):** Αποτελεί μια τεχνική ασφαλείας, η οποία διακατέχει τον ρόλο της αποφυγής εκμετάλλευσης ευπαθειών μνήμης από κάποιο επιτιθέμενο. Με σκοπό την αποφυγή μεταπήδησης από ένα κομμάτι μνήμης του συστήματος σε κάποιο άλλο, η συγκεκριμένη τεχνική ασφάλειας αποθηκεύει με τυχαίο τρόπο τις διευθύνσεις μνήμης των σημείων κλειδιών μιας διεργασίας για να μην είναι δυνατή η μεταπήδηση σε κάποια άλλη από τον επιτιθέμενο. Παραδείγματος χάρη, γίνεται τυχαία αποθήκευση του εκτελέσιμου και τις στοίβας εκτέλεσης καθώς και των απαραίτητων βιβλιοθηκών μιας διεργασίας.

11. **Return-oriented programming (ROP):** Αποτελεί μια τεχνική επίθεσης, η οποία επιτρέπει στον επιτιθέμενο την εκτέλεση κακόβουλου κώδικα υπό την παρουσία αμυντικών μηχανισμών (π.χ. υπογραφή κώδικα, προστασία εκτελέσιμου χώρου μνήμης).
    Σε αυτή την τεχνική, ο επιτιθέμενος παίρνει τον έλεγχο της στοίβας εκτέλεσης με σκοπό να σφετεριστεί τον έλεγχο ροής και να εκτελέσει συγκεκριμένες εντολές εκτέλεσης, οι οποίες είναι ήδη παρών στην μνήμη του συστήματος. Οι εντολές εκτέλεσης που επιλέγει ο επιτιθέμενος ονομάζονται "gadgets". Κάθε "gadget" εμπεριέχει συνήθως μια εντολή επιστροφής και βρίσκεται εντός μιας υπορουτίνας στο ήδη υπάρχον πρόγραμμα.
    Η σύνδεση πολλαπλών "gadgets" επιτρέπει στον επιτιθέμενο την εκτέλεση αυθαίρετων ενεργειών στο μηχάνημα-θύμα, ακόμα και αν αυτό είναι εξοπλισμένο με αμυντικούς μηχανισμούς.

12. **BSS Buffer:** Αποτελεί το σημείο της μνήμης εκείνο, το οποίο αποθηκεύει μη αρχικοποιημένες στατικές/παγκόσμιες μεταβλητές. Το συγκεκριμένο κομμάτι της μνήμης γεμίζει με μηδενικές τιμές από το λειτουργικό σύστημα με αποτέλεσμα όλες οι μη αρχικοποιημένες μεταβλητές να ξεκινούν με 0.

13. **Trustedbsd Mac:** Το εν λόγω Framework αποτελεί την επέκταση της πολιτικής ελέγχου πρόσβασης του λειτουργικού συστήματος επιτρέποντας στους διαχειριστές του λειτουργικού συστήματος και των εφαρμογών που κάνουν χρήση του συγκεκριμένου Framework την επιβολή περαιτέρω περιορισμούς στον τελικό χρήστη και στην συμπεριφορά της εφαρμογής. Αποτελεί μια διεπαφή πυρήνα (Kernel Programming Interface) που επιτρέπει σε φορτώσιμες υπομονάδες (Loadable Modules) την ενίσχυση της πολιτικής ασφάλειας του συστήματος με σκοπό την ευέλικτη υλοποίηση υποχρεωτικών ελέγχων πρόσβασης εντός του συστήματος.