ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΡΑΔΙΟΣΥΧΝΙΚΗΣ ΑΝΑΓΝΩΡΙΣΗΣ (RFID)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τσαντεκίδης Ε. Μαρίνος

Επιβλέπων: Ηλιούδης Α. Χρήστος

Θεσσαλονίκη, Σεπτέμβριος 2010

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1

Κεφάλαιο 2

ΚΕΦΑΛΑΙΟ 1

ΓΕΝΙΚΑ

1. Ευρύτερη περιοχή μελέτης

Μέρος της αναγνώρισης μέσω ραδιοσυχνοτήτων (RFID – Radio Frequency IDentification) θεωρούνται, υπό την ευρεία έννοια και ραδιοεκπομπές που περιέχουν κάποιου είδους πληροφορίες αναγνώρισης. Για παράδειγμα, οδηγοί ταξί που χρησιμοποιούν τον αριθμό μονάδας τους μέσω του ασυρμάτου ή ο αριθμός κλήσης ενός ραδιοφωνικού σταθμού.

Το RFID αφορά συσκευές και τεχνολογία που χρησιμοποιούν ραδιοσήματα για να ανταλλάξουν δεδομένα αναγνώρισης. Υπό την συνήθη έννοια, αυτό προϋποθέτει μια μικρή *ετικέτα* ή *κάρτα* που προσδιορίζει ένα συγκεκριμένο αντικείμενο. Η ενέργεια λαμβάνει ένα ραδιοσήμα, το μεταφράζει και επιστρέφει τότε έναν αριθμό ή κάποιες άλλες αναγνωριστικές πληροφορίες (π.χ. “Τι είσαι” απάντησε “Είμαι το αντικείμενο με αριθμό αποθήκης 12345”). Εναλλακτικά, μπορεί να είναι τόσο πολύπλοκη όσο μια σειρά από κρυπτογραφημένες “ερωτήσεις” και “απαντήσεις”, οι οποίες εν συνεχεία μεταφράζονται μέσω μιας βάσης δεδομένων, αποστέλλονται σε ένα παγκόσμιο σύστημα δορυφορικών επικοινωνιών και τελικά επηρεάζουν ένα σύστημα κορμού (backend) για πληρωμές.

Μερικές από τις σύγχρονες χρήσεις της τεχνολογίας RFID περιλαμβάνουν:

- Σημεία πωλήσεων (Point of Sale – POS)
- Συστήματα αυτόματης αναγνώρισης οχημάτων (Automated Vehicle Identification – AVI)
- Περιορισμό πρόσβασης σε κτίρια ή χώρους μέσα σε κτήρια
- Αναγνώριση πανίδας
- Εντοπισμός εμπορευμάτων
- Αναγνώριση ιδιοκτησίας κατοικίδιων

- Διαχείριση αποθήκης και λογιστικά
- Εντοπισμός προϊόντων σε αλυσίδες προμηθειών
- Ασφάλεια προϊόντων
- Εντοπισμός πρώτων υλών / κινήσεις εξαρτημάτων εντός εργοστασίων
- Ενοικίαση / επιστροφή βιβλίων σε βιβλιοθήκες
- Εντοπισμός βαγονιών / τρένων
- Εντοπισμός αποσκευών σε αεροδρόμια κλπ.

Συχνά αποδεχόμαστε μια νέα τεχνολογία χωρίς να καταλαβαίνουμε τα ζητήματα ασφαλείας που την αφορούν. Έχουμε την τάση να είμαστε κυνικοί με τις υπερβολές των εμπόρων σχετικά με τις επιδόσεις, δεν είμαστε όμως κυνικοί, ενώ θα έπρεπε, σε θέματα που αφορούν απαιτήσεις ασφαλείας (ή στην απουσία τους) που περιβάλλουν νέες τεχνολογίες.

Η ασφάλεια θεωρείται δευτερεύουσα σε σχέση με άλλα ζητήματα συγκεκριμένων τεχνολογιών. Το RFID χρησιμοποιείται σε πολλαπλές εφαρμογές όπου τα θέματα ασφαλείας έχουν εξεταστεί ελάχιστα ή και καθόλου. Έτσι, ενώ η τεχνολογία αυτή είναι σχετικά καινούρια, η ασφάλεια κάποιων συστημάτων που την εφαρμόζουν, έχει ήδη τεθεί σε κίνδυνο. Παραδείγματος χάριν, τον Ιανουάριο του 2005, η κρυπτογράφηση του συστήματος SpeedPass[1] της εταιρίας ExxonMobil[2] και του RFID συστήματος πώλησής της, έσπασε από μια ομάδα φοιτητών (ως εργασία στο πανεπιστήμιο Johns Hopkins), επειδή δεν είχαν εφαρμοστεί κοινοί κανόνες αναφορικά με την ισχυρή κρυπτογράφηση.

Το να ασχοληθεί κανείς με την ασφάλεια και το RFID, σημαίνει να ασχοληθεί όχι μόνο με τις πτυχές ασφαλείας των RFID συστημάτων, αλλά επίσης με τις πτυχές ασφαλείας οτιδήποτε ή οποιουδήποτε επηρεάζεται από τα συστήματα αυτά. Η ευρεία διάδοση της τεχνολογίας αναγνώρισης και των συσκευών αποθήκευσης, έχει σίγουρα

[1]Το SpeedPass είναι ένα σύστημα αυτόματων ηλεκτρονικών πληρωμών που βρίσκει εφαρμογή σε πρατήρια βενζίνης στην Αμερική και αποτελείται από μια RFID συσκευή σε μορφή μπρελόκ. Στην αρχή, είχε εφαρμοστεί σε αλυσίδες ταχυφαγείων και supermarkets χωρίς, όμως, επιτυχία. Παράδειγμα η γνωστή αλυσίδα Mc'Donalds.

[2]Η εταιρία ExxonMobil είναι μια πετρελαιοπαραγωγός αμερικανική πολυεθνική που κατατάσσεται μεταξύ των 5 μεγαλύτερων αντίστοιχων εταιριών, τα τελευταία 5 χρόνια.

επιπτώσεις και μπορεί να οδηγήσει σε νέες απειλές σε άλλες περιοχές και εφαρμογές. Έτσι, η χρήση του RFID αποτελεί πρόκληση για τα υπάρχοντα συστήματα ασφαλείας τα οποία πρέπει να επανεξεταστούν.

Όπως με οποιαδήποτε άλλα μέτρα ασφαλείας, η ασφάλεια στο RFID πρέπει να είναι μια διαδικασία, παρά ένα μεμονωμένο γεγονός. Η διαδικασία αυτή θα πρέπει να στηριχθεί σε μια τεχνολογική βάση, παρέχοντας μηχανισμούς ασφαλείας για εφαρμογές που θα χτιστούν πάνω σε αυτή τη βάση. Η ασφάλεια των RFID συστημάτων δεν περιορίζεται μόνο στην τεχνολογία, αλλά πρέπει επίσης να δώσει απάντηση στην ερώτηση πόσο ασφαλές είναι να βασίζεται κανείς σε πληροφορίες που παρέχονται από τέτοια συστήματα.

2. Αντικείμενο της εργασίας

Σε αυτή τη διπλωματική εργασία παρέχονται σκέψεις για ζητήματα ασφαλείας που αφορούν τα συστήματα RFID και επισημαίνονται μερικές από τις περιοχές που πρέπει να ληφθούν υπόψη αναφορικά με το συγκεκριμένο θέμα.

Αντικείμενο αυτής της εργασίας είναι η διερεύνηση των ζητημάτων ασφάλειας και ιδιωτικότητας που προκύπτουν από τη χρήση της τεχνολογίας RFID, η εκτίμηση των δυνατοτήτων της μέχρι σήμερα διαθέσιμης τεχνολογίας να επιλύσει τα ζητήματα αυτά και η παροχή προτάσεων προς βοήθεια για την εκπλήρωση των απαιτήσεων ασφάλειας και ιδιωτικότητας.

Η εργασία αυτή παρέχει μια απαρίθμηση των απαιτήσεων ασφαλείας που απαιτούνται για την εφαρμογή της τεχνολογίας. Παρέχονται εκτιμήσεις για τους κινδύνους στην ασφάλεια και ιδιωτικότητα, μαζί με μια περιγραφή πιθανών αντιμέτρων για την αντιμετώπιση αυτών των κινδύνων.

Η γενική ανάλυση της τεχνολογίας RFID υποδεικνύει ότι αρκετές στρατηγικές είναι διαθέσιμες για τη μετρίαση των ανησυχιών αναφορικά με την ασφάλεια και την ιδιωτικότητα. Οι στρατηγικές αυτές περιλαμβάνουν τη χρήση κρυπτογράφησης, την εφαρμογή αλγορίθμων για την αποτροπή συγκρούσεων (anti-collision) ώστε να εξασφαλιστεί η διαθεσιμότητα των αναγνωστών και η ακεραιότητα των δεδομένων,

τη χρήση φίλτρων και ελέγχων για τον εντοπισμό πλαστών καρτών ή επιθέσεων επανάληψης και εκπαίδευση των ιδιοκτητών των καρτών για τη χρήση της φυσικής προστασίας που μπορεί να αποτρέψει την ανάγνωση των καρτών τους. Πρόσθετες στρατηγικές προστασίας της ιδιωτικότητας περιλαμβάνουν την ενημέρωση του κοινού και την επακόλουθη τοποθέτηση καρτών RFID σε ταξιδιωτικά έγγραφα και την εκχώρηση ενός νέου αριθμού ID όποτε εκδίδεται μια νέα κάρτα ή αντικαθίσταται μια.

Αυτές οι στρατηγικές θα πρέπει να αξιολογούνται περαιτέρω κατά τη φάση του σχεδιασμού και της ανάπτυξης των συστημάτων, με σκοπό να προσδιοριστεί η επίδρασή τους στις επιχειρησιακές δυνατότητες και να γίνει μια ανάλυση επιχειρηματικών κινδύνων πριν την εφαρμογή.

3. Στρατηγική σημασία του RFID

Ο Michael Porter περιγράφει τη στρατηγική ως "τη διεξαγωγή διαφορετικών δραστηριοτήτων σε σχέση με τους αντιπάλους" ή ως "τη διεξαγωγή παρόμοιων δραστηριοτήτων με διαφορετικούς τρόπους" και δίνει έμφαση στο γεγονός ότι, ενώ η επιχειρησιακή αποτελεσματικότητα είναι ζωτικής σημασίας για την κερδοφορία, δεν είναι στρατηγική [5].

Διάφορες μεγάλες εταιρίες συμβουλευτικής δίνουν μεγάλη έμφαση στην επίδραση του RFID στη στρατηγική. Σύμφωνα με την εταιρία Gartner Research, το RFID όχι μόνο έχει φέρει επανάσταση στον τρόπο με τον οποίο τα διάφορα αντικείμενα εντοπίζονται στην αλυσίδα διανομών, αλλά έχει και πολύ μεγάλες προοπτικές για να χρησιμοποιηθεί στον επανασχεδιασμό των επιχειρησιακών στρατηγικών [8].

Ο πρώτος τομέας που χρησιμοποίησε την τεχνολογία RFID ήταν ο αμερικανικός στρατός, αλλά σιγά σιγά το RFID βρήκε το δρόμο του προς άλλες επιχειρήσεις και ιδρύματα. Διάφορες επιχειρήσεις είναι αισιόδοξες για τις δυνατότητες της τεχνολογίας αυτής να βελτιστοποιήσει και να εκλογικεύσει τη διαχείριση της αλυσίδας προμηθειών [3]. Η εταιρία ερευνών ABI προβλέπει ότι κάποιες

συγκεκριμένες εταιρίες θα έχουν ενεργή συμμετοχή στο πεδίο του RFID, συμπεριλαμβανομένων εταιριών καταναλωτικών αγαθών, αυτοκινητοβιομηχανιών καθώς και κρατικών υπηρεσιών άμυνας και ασφάλειας [4].

Η διάδοση της θεωρίας καινοτομιών αναγνωρίζει πέντε χαρακτηριστικά καινοτομιών που επηρεάζουν την υιοθέτησή τους: σχετικό πλεονέκτημα, συμβατότητα, πολυπλοκότητα, "δοκιμαστικότητα" (trialability) και παρατηρησιμότητα [6]. Με την προϋπόθεση ότι η υιοθέτηση θα γίνει μόνο αν κάποιος δει μια συγκεκριμένη χρησιμότητα σε έναν νεωτερισμό, αυτοί οι παράγοντες θα μπορούσαν να επηρεάσουν την αντίληψη της στρατηγικής σημασίας μιας καινοτομίας, στη συγκεκριμένη περίπτωση του RFID.

Δοκιμαστικότητα είναι ο βαθμός στον οποίο μπορεί να βιωθεί μια καινοτομία. Όσο καλύτερα αντιλαμβάνεται κάποιος, υπό τους όρους του, ότι λειτουργεί μια καινοτομία, τόσο πιθανότερο είναι να την υιοθετήσει.

Παρατηρησιμότητα είναι ο βαθμός στον οποίο τα αποτελέσματα μιας καινοτομίας είναι ορατά στους άλλους. Πολλές εταιρίες έχουν ξεκινήσει δοκιμαστικά προγράμματα, δημιουργώντας, έτσι, μια συγκεκριμένη "δοκιμαστικότητα". Μαζί με τα προγράμματα επίδειξης των χονδρεμπόρων και άλλες διαθέσιμες πληροφορίες, αυτά τα πιλοτικά προγράμματα παρέχουν παρατηρησιμότητα σε άλλους.

Σχετικό πλεονέκτημα είναι ο βαθμός στον οποίο μια καινοτομία γίνεται αντιληπτή ως καλύτερη από την ιδέα που αντικαθιστά [6]. Μια παρόμοια προσέγγιση ακολουθείται από τον Davis στο Μοντέλο Τεχνολογικής Αποδοχής του (Technological Acceptance Model – TAM), όπου περιγράφει την αντιληπτή χρησιμότητα ως καθοριστικό παράγοντα για την υιοθέτηση μιας καινοτομίας [1]. Τα αντιληπτά οφέλη έχουν, επίσης, αποδειχθεί στην μελέτη των Ιακώβου και Benbasat [2] σχετικά με την καθιέρωση του EDI[3] και έχουν ακόμη ληφθεί σοβαρά υπόψιν σε έρευνα που είχε διεξαχθεί από τους Sharma και Citrus [7] πάνω στην καθιέρωση του RFID.

Σήμερα το RFID ενδιαφέρει ένα μεγαλύτερο κοινό και η συζήτηση μεταφέρεται

[3]EDI – Electronic Transmission Interchange: Οικογένεια προτύπων που αναφέρεται στη δομημένη μετάδοση δεδομένων μεταξύ οργανισμών, με ηλεκτρονικά μέσα.

σε επίπεδο επιχειρήσεων. Τα τελευταία χρόνια έχει παρατηρηθεί η κάμψη, από τη βιομηχανία, των φραγμών της καθιέρωσης του RFID (άνθρωποι, κόστος κλπ). Το κόστος μειώνεται χάρη στην ευρεία διάδοση της τεχνολογίας αυτής, οι τιμές του υλικού πέφτουν, η αξιοπιστία του λογισμικού αυξάνεται και η συνολική πολυπλοκότητα για τους πελάτες απλοποιείται.

Οι επιχειρήσεις σήμερα χρειάζονται διαφάνεια σε οποιαδήποτε έκφανση της επιχειρηματικής τους διαδικασίας, ανεξάρτητα από το μέγεθός τους ή τη βιομηχανία στην οποία δραστηριοποιούνται. Το RFID έχει μετατραπεί σε ένα βασικό παράγοντα για τη λήψη καλύτερων επιχειρηματικών αποφάσεων.

4. Σκοπός – διάρθρωση της πτυχιακής

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι η γενική παρουσίαση της τεχνολογίας RFID, η αναλυτική εξέταση των θεμάτων ασφάλειας και ιδιωτικότητας τα οποία εμφανίζονται στα συστήματα που ενσωματώνουν αυτή την τεχνολογία και η παρουσίαση μεθόδων και μέτρων προστασίας που μπορούν να χρησιμοποιηθούν για την καλύτερη δυνατή προστασία των συστημάτων αυτών. Συγκεκριμένα, γίνεται μία σύντομη εισαγωγή η οποία περιλαμβάνει τις βασικές έννοιες, τα ιδιαίτερα χαρακτηριστικά και τον τρόπο λειτουργίας των συστημάτων RFID καθώς και τις εφαρμογές που μπορεί να υλοποιήσει η τεχνολογία. Ακολούθως, περιγράφονται αναλυτικά τα θέματα ασφάλειας και ιδιωτικότητας των συστημάτων καθώς και τα προβλήματα που αντιμετωπίζονται σε αυτούς τους τομείς. Κατόπιν παρουσιάζονται εκτενώς μηχανισμοί ασφάλειας και κατευθυντήριες γραμμές για την προστασία των συστημάτων RFID. Έπειτα παρουσιάζεται μια μελέτη περίπτωσης χρήσης ενός θεωρούμενου ως ασφαλούς RFID πρωτοκόλλου πιστοποίησης, στην οποία γίνονται προσπάθειες επίθεσης σε συγκεκριμένες ιδιότητες ενός συστήματος. Τέλος παρατίθενται τα συμπεράσματα του γράφοντος για την παρούσα κατάσταση και τη μελλοντική εξέλιξη του RFID.

Τα θέματα στα οποία επικεντρώνεται η παρούσα διπλωματική εργασία είναι πολύ σημαντικά για την εξέλιξη και την ευρεία αποδοχή της τεχνολογίας RFID. Τα θέματα

αυτά αποτελούν ένα συνεχές πεδίο έρευνας και πρέπει να εξετάζονται εκτεταμένα έτσι ώστε το επίπεδο αξιοπιστίας να παραμένει ψηλά.

ΑΝΑΦΟΡΕΣ

[1] Davis, F. D. (1989) Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. MIS Quarterly, 319-339.

[2] Iacovou, C. and Benbasat, I. (1995) Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. MIS Quarterly, 19, 465-485.

[3] Lange, V. (2004) Perspektiven für die Nutzung der RFID-Technologie in Supply Chain Management und Logistik. IM, 19, 20-26.

[4] Maselli, J. (2003) ABI: RFID Market Poised for Growth RFID-Journal.

[5] Porter, M. E. (1996) What is Strategy? Harvard Business Review, 74, 61 - 78.

[6] Rogers, E. M. (1995) Diffusion of Innovations, New York, The Free Press.

[7] Sharma, A. and Citurs, A. (2005) Radio Frequency Identification (RFID) Adoption Drivers - A radical Innovation Adoption Perspective. Eleventh Americas Conference on Information Systems. Omaha, NE, USA.

[8] Woods, J., Peterson, K. and Hirst, C. (2003) Maturing Open RFID Applications Will Reshape SCM. Stanford, Gartner Research.

ΚΕΦΑΛΑΙΟ 2

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ RFID

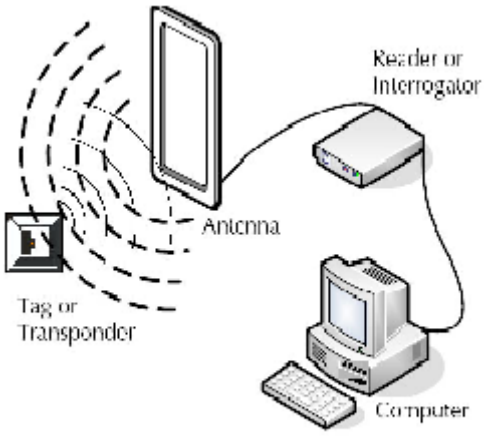
1. Εισαγωγή

1.1 Τι είναι η τεχνολογία RFID ;

Η τεχνολογία ταυτοποίησης μέσω ραδιοσυχνοτήτων (Radio Frequency Identification) επιτρέπει την ασύρματη και αυτόματη αναγνώριση οντοτήτων με τη χρησιμοποίηση συσκευών που ονομάζονται κάρτες (tags ή transponders) και αναγνώστες (readers ή interrogators).

Ένα τυπικό σύστημα RFID αποτελείται από μερικούς αναγνώστες οι οποίοι είναι σταθεροί ή κινητοί και πολλές κάρτες οι οποίες μπορούν να εφαρμοστούν ή να ενσωματωθούν σε αντικείμενα, προϊόντα, ζώα και ανθρώπους. Ο αναγνώστης, μέσω της χρήσης ραδιοσυχνοτήτων εντοπίζει, επικοινωνεί και αναγνωρίζει τις κάρτες που βρίσκονται εντός της ασύρματης εμβέλειάς του και συλλέγει πληροφορίες για τις οντότητες στις οποίες είναι προσαρτημένες οι κάρτες αυτές. Οι πληροφορίες που ανακτώνται από αυτές, μεταδίδονται από τον αναγνώστη σε υπάρχοντα δίκτυα υπολογιστών που τις επεξεργάζονται ανάλογα με την εφαρμογή που υλοποιείται.

Η τεχνολογία RFID καθιστά ικανή την εξ' αποστάσεως επικοινωνία μεταξύ αναγνώστη και κάρτας χωρίς να είναι απαραίτητο να βρίσκονται σε οπτική επαφή. Επίσης τα συστήματα RFID μπορούν να διακρίνουν πολλές διαφορετικές κάρτες που βρίσκονται στην ίδια περιοχή χωρίς ανθρώπινη βοήθεια. Αυτά, καθώς και άλλα πλεονεκτήματα, καθιστούν την τεχνολογία RFID ικανή να υλοποιήσει υπάρχουσες και καινούριες εφαρμογές με ιδιαίτερη επιτυχία.



Σχήμα 1. Σύστημα RFID

Τα συστήματα RFID είναι σε θέση να υλοποιήσουν εφαρμογές σε πολλούς τομείς της καθημερινής ζωής, απλοποιώντας διαδικασίες και λύνοντας προβλήματα που παρουσιάζονται συνεχώς. Η τεχνολογία παρουσιάζει αυξανόμενη χρήση σε τομείς όπως η παιδεία, η υγεία, το εμπόριο, οι μεταφορές, η ασφάλεια και άλλα. Μελλοντικά, υπάρχει η επιδίωξη για ακόμη μεγαλύτερη χρήση των RFID, ιδιαίτερα όταν κάποια τεχνικά και κατασκευαστικά εμπόδια που υπάρχουν, ξεπεραστούν, πάντα σε συνάρτηση με το κόστος τους, που για κάποιες εφαρμογές δεν είναι ακόμη ανταγωνιστικό.

1.2 Εξέλιξη των RFID

Η εκκίνηση της ιστορικής εξέλιξης των συστημάτων RFID στη σημερινή τους μορφή, μπορεί να ανιχνευθεί στις πρώτες δεκαετίες του εικοστού αιώνα με τη γένεση των συστημάτων ραντάρ, που βασίστηκαν στην ασύρματη εκπομπή και λήψη ανακλώμενης ενέργειας. Σε εκείνο το χρονικό διάστημα αναπτύχθηκαν πολλές εφαρμογές με χαρακτηριστικό παράδειγμα το Identify: Friend or Foe (IFF), ένα σύστημα που χρησιμοποιήθηκε στο Δεύτερο Παγκόσμιο πόλεμο από τους συμμάχους για την αναγνώριση των φιλικών αεροσκαφών και βασίστηκε σε παθητικούς ανακλαστήρες ραντάρ.

Ένα από τα πιο πρώιμα και σημαντικά συγγράμματα που σχετίζονται με τα RFID εκδόθηκε από τον Harry Stockman το 1948 και αφορούσε τη συνεχή χρονική

διαμόρφωση ανακλώμενων σημάτων. Ο Stockman σχεδίασε μια συσκευή που διαμόρφωνε ανθρώπινη φωνή πάνω σε ανακλώμενα σήματα.

Κατά τις δεκαετίες του 1960 και 1970 σημειώθηκε αυξημένο ενδιαφέρον για τα RFID από την επιστημονική ερευνητική κοινότητα. Διάφορες τεχνικές σύζευξης, μεταφοράς ενέργειας και επικοινωνίας αναπτύχθηκαν σε αυτό το διάστημα. Το 1975 οι Koelle, Depp και Freyman εισήγαγαν την διαμόρφωση επανασκέδασης (backscatter modulation) στις κάρτες RFID, τεχνική που χρησιμοποιείται στην πλειονότητα των σημερινών RFID καρτών.

Η πρώτη εμπορική εφαρμογή αναπτύχθηκε στα τέλη του 1960 όμως η εμπορευματοποίηση ενισχύθηκε τις δεκαετίες 1980 και 1990 με ποικίλο ενδιαφέρον σε όλο τον κόσμο. Η αύξηση της εμπορικής χρήσης οδήγησε στην ανάγκη δημιουργίας προτύπων και έτσι πολλές δραστηριότητες τυποποίησης έλαβαν χώρα τη δεκαετία του 1990. Ο Παγκόσμιος Οργανισμός Προτύπων (ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC) ανέπτυξαν πρότυπα για διάφορους τομείς. Η αποδοχή που συνέχισε να λαμβάνει η τεχνολογία RFID, κινητοποίησε περαιτέρω δραστηριότητες τυποποίησης από διάφορους οργανισμούς (ANA,EAN,UCC). Η δημιουργία ενός παγκόσμιου προτύπου για τον προσδιορισμό προϊόντων ανατέθηκε στο Auto-ID Center του πανεπιστημίου MIT και ονομάστηκε Electronic Product Code (EPC).

Η είσοδος στον εικοστό πρώτο αιώνα βρίσκει τις εφαρμογές των RFID μπροστά σε νέες προκλήσεις για ακόμη μεγαλύτερη αποδοχή, βοηθούμενη από την πρόοδο σε τεχνικό και κατασκευαστικό επίπεδο που μπορεί να παρέχει η τεχνολογία.

1.3 Κάρτες (Tags)

Η κάρτα RFID είναι μία συσκευή, μικρών διαστάσεων, που εφαρμόζεται ή ενσωματώνεται σε οντότητες όπως προϊόντα, ζώα αλλά και ανθρώπους με σκοπό την αναγνώριση-ταυτοποίησή τους μέσω της χρήσης ραδιοκυμάτων.

Μία κάρτα RFID αποτελείται από τουλάχιστον δύο κυρίως μέρη. Καταρχήν, ένα ολοκληρωμένο κύκλωμα υπεύθυνο για την αποθήκευση και επεξεργασία

πληροφορίας, τη διαμόρφωση και αποδιαμόρφωση σημάτων, καθώς και για άλλες ειδικές λειτουργίες. Το δεύτερο στοιχείο της κάρτας είναι μία κεραία, απαραίτητη για την εκπομπή και λήψη σημάτων. Συνήθως, τα δύο αυτά μέρη που συνιστούν την κάρτα RFID προστατεύονται με κάποιου είδους περίβλημα, το οποίο διατηρεί την ακεραιότητα της κάρτας. Το περίβλημα μπορεί να είναι ένα μικρό γυάλινο φιαλίδιο ή ένα υπόστρωμα πλαστικής μεμβράνης και προστατεύει το ολοκληρωμένο κύκλωμα και την κεραία από τις περιβαλλοντικές συνθήκες ή χημικές ουσίες που θα μπορούσαν να προκαλέσουν βλάβη σ'αυτά.

Η απλούστερη πληροφορία που μπορεί να ανακτηθεί από μια κάρτα είναι ένας μοναδικός σειριακός αριθμός ταυτότητας. Υπάρχει, όμως, η ευχέρεια για επιπρόσθετες πληροφορίες, όπως ο κατασκευαστής και το μοντέλο ενός προϊόντος ή ακόμη και η μέτρηση περιβαλλοντικών συνθηκών όπως η θερμοκρασία. Στο σχήμα 2 παρουσιάζονται κάποια είδη καρτών διαφόρων μεγεθών και σχημάτων που συναντώνται στην πράξη.

Σχήμα 2. Είδη καρτών

1.4 Αναγνώστες (Readers)

Ο αναγνώστης RFID είναι η συσκευή που επικοινωνεί με τις κάρτες που βρίσκονται εντός της εμβέλειάς του, τις αναγνωρίζει και συλλέγει πληροφορίες από αυτές. Επίσης είναι υπεύθυνος για την τροφοδόσίας τους στην περίπτωση παθητικών καρτών.

Υπάρχουν δύο κύριοι τύποι αναγνώστη RFID, ανάλογα με τη δυνατότητα επεξεργασίας της κάρτας. Στον πρώτο, ο αναγνώστης κάνει μόνο ανάγνωση των δεδομένων της κάρτας ενώ στον δεύτερο έχει και τη δυνατότητα εγγραφής σε αυτή εφόσον η μνήμη της κάρτας υποστηρίζει τέτοια λειτουργία.

Ο αναγνώστης μπορεί να είναι σταθερή ή κινητή συσκευή ανάλογα με την εφαρμογή που υλοποιείται. Σταθεροί αναγνώστες εφαρμόζονται σε πόρτες, πύλες διοδίων ή ακόμη σε ταβάνια και τοίχους όπου είναι κρυμμένοι. Κινητά μοντέλα αναγνώστη χρησιμοποιούνται για παράδειγμα σε υπεραγορές ή είναι ειδικά κατασκευασμένα για κινητές συσκευές όπως PDA και κινητά τηλέφωνα.

Η ραγδαία εξέλιξη των αναγνωστών επιτρέπει τη λειτουργία τους σαν πύλες προς κεντρικά δίκτυα συστημάτων επικοινωνιών αφού μπορούν να υποστηρίξουν διάφορα πρωτόκολλα επικοινωνιών και τεχνολογίες δικτύων.

Στο σχήμα 3 παρουσιάζονται μερικά είδη αναγνωστών που χρησιμοποιούνται στην πράξη.

Σχήμα 3. Είδη αναγνωστών

2. Βασικά χαρακτηριστικά συστημάτων RFID

2.1 Τύποι καρτών

Υπάρχουν πολλοί τύποι καρτών RFID, όμως στο υψηλότερο επίπεδο διαχωρίζονται σε τρεις κατηγορίες ανάλογα με την αρχή λειτουργίας τους : παθητικές, ημιπαθητικές και ενεργές.

2.1.1 Παθητικές κάρτες (Passive Tags)

Οι παθητικές κάρτες χρησιμοποιούν το ηλεκτρομαγνητικό πεδίο που εκπέμπει ο αναγνώστης για να φορτίσουν το εσωτερικό τους κύκλωμα, αφού δεν διαθέτουν εσωτερική πηγή ενέργειας. Για την μετάδοση πληροφορίας προς τον αναγνώστη, χρησιμοποιούν επανασκέδαση (backscattering), δηλαδή ανάκλαση κυμάτων πίσω προς τον αναγνώστη, εφόσον δεν διαθέτουν πομπό.

Με αυτές τις προδιαγραφές οι παθητικές κάρτες αποτελούν τη λιγότερο περίπλοκη και ως εκ τούτου τη φθηνότερη κατασκευή. Χωρίς να χρειάζονται εσωτερική τροφοδοσία (μπαταρία) ή συντήρηση έχουν ανεξάντλητη διάρκεια ζωής, γεγονός που τις καθιστά συμφέρουσα επιλογή για τις εφαρμογές όπου χρησιμοποιούνται. Έχουν επίσης το πλεονέκτημα ότι είναι αρκετά μικρές για να εφαρμοστούν σε πρακτικές αυτοκόλλητες ταινίες.

Το μειονέκτημα που προκύπτει για τις παθητικές κάρτες έγκειται στο γεγονός ότι για να λειτουργήσουν είναι απαραίτητη η παρουσία του αναγνώστη σε αρκετά κοντινή απόσταση, ούτως ώστε να είναι δυνατή η κατάλληλη φόρτισή τους . Επίσης, η ακτίνα επικοινωνίας κάρτας-αναγνώστη περιορίζεται από την μικρή ποσότητα ενέργειας που μπορεί να σταλεί από την κάρτα ώστε αυτή να ανταποκριθεί αξιόπιστα προς τον αναγνώστη.

2.1.2 Ημιπαθητικές κάρτες (Semi-Passive Tags)

Οι ημιπαθητικές κάρτες σε αντίθεση με τις παθητικές έχουν δική τους πηγή ενέργειας αλλά όχι πομπό και επίσης χρησιμοποιούν τεχνική backscattering. Έχοντας λοιπόν τη δική τους μπαταρία, είναι πιο αξιόπιστες και έχουν μεγαλύτερη εμβέλεια ανάγνωσης απ' ότι οι παθητικές κάρτες. Όμως, έχουν μικρότερη διάρκεια λειτουργίας λόγω της μπαταρίας, είναι πιο εύθραυστες και σε σημαντικό βαθμό πιο ακριβές.

2.1.3 Ενεργές κάρτες (Active Tags)

Οι ενεργές κάρτες διαθέτουν πομπό ραδιοσυχνοτήτων και χρειάζονται κάποια πηγή τροφοδοσίας για τη λειτουργία του ολοκληρωμένου κυκλώματος και την επικοινωνία με τον αναγνώστη. Έτσι είναι συνδεδεμένες με κάποια υποδομή που τις τροφοδοτεί ή διαθέτουν μια εσωτερικά ενσωματωμένη μπαταρία. Στην δεύτερη περίπτωση που είναι και η πιο συνηθισμένη, η διάρκεια ζωής της κάρτας είναι περιορισμένη από την αποθηκευμένη ενέργεια της μπαταρίας, εξαρτάται όμως και από τις λειτουργίες ανάγνωσης στις οποίες υποβάλλεται.

Στην περίπτωση ενεργών καρτών η εμβέλεια ανάγνωσης είναι αυξημένη, η αξιοπιστία τους βελτιώνεται σημαντικά ενώ οι αναγνώστες είναι ικανοί να διαβάσουν μεγάλο αριθμό ενεργών καρτών σε μικρό χρονικό διάστημα. Επίσης έχουν μεγαλύτερη μνήμη από τις παθητικές κάρτες και λόγω του ότι οι ικανότητες επεξεργασίας τους είναι υψηλότερες είναι και πιο ασφαλείς.

Παρόλα αυτά, οι μπαταρίες μεγαλώνουν το κόστος και το μέγεθος της κάρτας,

καθώς επίσης περιορίζουν τον κύκλο ζωής της, με αποτέλεσμα να μην είναι πρακτικές για χρήση στο λιανικό εμπόριο.

2.2 Τυπικές συχνότητες λειτουργίας

Η τεχνολογία RFID είναι βασισμένη στην ασύρματη επικοινωνία κάνοντας χρήση ραδιοκυμάτων, που αποτελούν μέρος του ηλεκτρομαγνητικού φάσματος, δηλαδή χρησιμοποιεί συχνότητες που κυμαίνονται περίπου μεταξύ 30 kHz εώς 3 GHz.

Πιο συγκεκριμένα, οι συχνότητες λειτουργίας των συστημάτων RFID χωρίζονται γενικά σε τέσσερις κύριες ζώνες συχνοτήτων. Τη ζώνη χαμηλών συχνοτήτων LF (Low Frequency band) μεταξύ 30-300kHz, υψηλών συχνοτήτων HF (High Frequency band) μεταξύ 3-30MHz, υπερυψηλών συχνοτήτων UHF (Ultra High Frequency) μεταξύ 300MHz-3GHz και συχνότητες μικροκυμάτων που κυμαίνονται μεταξύ 2-30GHz.

Αναλυτικά, χρησιμοποιούνται οι συχνότητες 119-135kHz (LF Band), 13.56MHz (HF Band), 860-960MHz (UHF Band) και 2.45GHz (Microwave Band). Ανάλογα με τη ζώνη συχνοτήτων στην οποία λειτουργεί ένα σύστημα RFID, υπάρχουν διαφορετικές δυνατότητες σε κάθε περίπτωση. Η εμβέλεια ανάγνωσης, ο ρυθμός μετάδοσης πληροφορίας καθώς και οι εφαρμογές που μπορούν να υλοποιηθούν διαφέρουν αναλόγως της συχνότητας λειτουργίας που χρησιμοποιείται.

2.3 Κεραίες

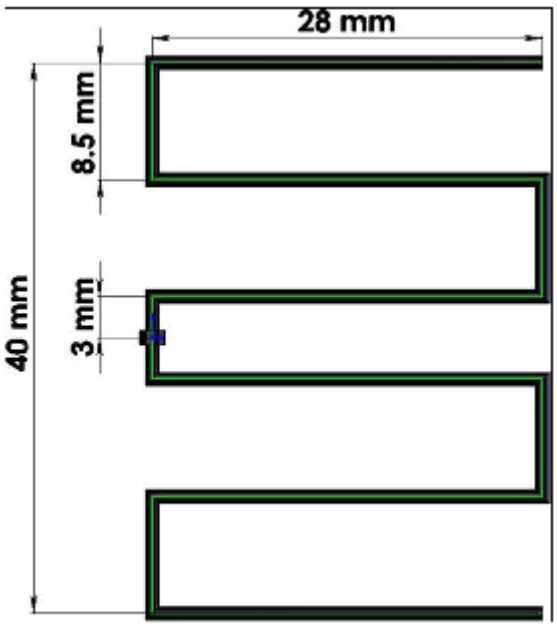
Ο τύπος κεραίας που χρησιμοποιείται για μια κάρτα RFID εξαρτάται και επηρεάζεται από τη συχνότητα λειτουργίας και την επιδιωκώμενη εφαρμογή στην οποία θα χρησιμοποιηθεί. Έτσι, αναλόγως της συχνότητας λειτουργίας, χρησιμοποιούνται οι κατάλληλοι τύποι κεραιών ούτως ώστε να επιτευχθεί η εύρυθμη λειτουργία της κάρτας. Η κεραία μιας RFID κάρτας είναι γενικά ένα αγώγιμο στοιχείο που επιτρέπει στην κάρτα να ανταλλάσει πληροφορίες με τον αναγνώστη. Στην περίπτωση παθητικών καρτών χρησιμοποιείται κάποιας μορφής σπειρωειδής κεραία, όπως ένα πηνίο, που είναι σε θέση να δημιουργήσει μαγνητικό πεδίο,

εκμεταλλευόμενη την ενέργεια που παρέχει το φέρον σήμα του αναγνώστη.

Οι παθητικές κάρτες χαμηλής συχνότητας (LF) απαιτούν πηνίο πολλών σπειρωμάτων, τα οποία είναι απαραίτητα ούτως ώστε να παραχθεί αρκετή ηλεκτρική τάση για τη λειτουργία του ολοκληρωμένου κυκλώματος. Κάποιες κάρτες που χρησιμοποιούνται για εξειδικευμένες εφαρμογές διαθέτουν πηνίο πολλών στρωμάτων με πολλά σπειρώματα.

Στην συχνότητα 13.56 MHz (HF) χρησιμοποιείται μία επίπεδη κεραία λίγων σπειρωμάτων, κατασκευαστικά φθηνότερη από ένα πηνίο LF, η οποία όμως χρειάζεται επιπλέον δύο μεταλλικά και ένα μονωτικό στρώμα για τη διασύνδεσή της με το ολοκληρωμένο κύκλωμα.

Οι παθητικές κάρτες UHF καθώς και οι μικροκυματικές, μπορούν να χρησιμοποιήσουν συνηθισμένες κεραίες μορφής διπόλου, οι οποίες όμως, λόγω του ότι είναι μεγάλες σε μέγεθος, σε πολλές εφαρμογές χρησιμοποιούνται σε κυρτή ή ελικοειδή μορφή. Το κόστος κατασκευής τους είναι μειωμένο, καθώς απαιτούν μόνο ένα μεταλλικό στρώμα.



Σχήμα 4. Ελικοειδές δίπολο

2.4 Μνήμη

Οι σύγχρονες κάρτες RFID μπορούν να περιέχουν πολύ περισσότερες πληροφορίες από έναν απλό αριθμό ταυτοποίησης (ID). Έχουν τη δυνατότητα να ενσωματώνουν επιπρόσθετη μνήμη, η οποία μπορεί να είναι μόνο αναγνώσιμη (read-only) ή για ανάγνωση και εγγραφή (read-write).

Η μνήμη μόνο-ανάγνωσης μπορεί να περιέχει συμπληρωματικές λεπτομέρειες για ένα προϊόν, που θα είναι διαθέσιμες όταν αυτές ζητηθούν και δεν θα χρειάζεται να προσπελαστούν κάθε φορά που η κάρτα ερωτάται από τον αναγνώστη. Για παράδειγμα, μπορεί να περιέχει ένα κωδικό ομάδας προϊόντος, ώστε εάν βρεθούν κάποια ελαττωματικά προϊόντα, ο κωδικός αυτός να βοηθήσει στην εύρεση και άλλων τεμαχίων με τις ίδιες ατέλειες.

Επίσης, η μνήμη κάρτας μπορεί να χρησιμοποιείται για να δίνει τη δυνατότητα στην κάρτα να αποθηκεύει πληροφορίες που θα την αυτοπεριγράφουν. Τέτοιου είδους πληροφορίες είναι ιδιαίτερα χρήσιμες όταν δεν υπάρχει η δυνατότητα άμεσης πρόσβασης σε κάποια βάση δεδομένων που να περιέχει όλες τις λεπτομέρειες της κάρτας. Αν, για παράδειγμα, μια συσκευασία μεταφερθεί σε λάθος προορισμό τότε οι σωστές πληροφορίες προορισμού θα μπορούσαν να ανακτηθούν άμεσα από τη μνήμη της κάρτας, βοηθώντας την μεταφορά της συσκευασίας στον ορθό προορισμό, χωρίς να χρειάζεται να προσπελαστούν τα αρχεία που αντιστοιχούν στην κάρτα.

Οι κάρτες με μνήμη ανάγνωσης-εγγραφής προσφέρουν περαιτέρω δυνατότητες επεξεργασίας στις εφαρμογές RFID που τις εκμεταλλεύονται. Παρόλο που το μέγεθος μιας τέτοιας μνήμης είναι επί του παρόντος μικρό, η δυνατότητα άμεσης εγγραφής σε αυτή από τον αναγνώστη, βρίσκει πολλούς τρόπους αξιοποίησης. Για παράδειγμα, κάρτες σε εμπορικά προϊόντα θα μπορούσαν να περιέχουν ένα ιστορικό ιδιοκτησίας ενός προϊόντος δεύτερης χρήσης. Ακόμη, σε μια εγγράψιμη μνήμη θα μπορούσε να αποθηκευτεί μαζί με ένα δεδομένο και η χρονική στιγμή στην οποία έχει εγγραφεί.

3. Εφαρμογές

3.1 Αλυσίδα Προμηθειών-Εφοδιασμού

Η αλυσίδα προμηθειών μπορεί να επωφεληθεί σε σημαντικό βαθμό από τη χρήση των συστημάτων RFID, τα οποία είναι σε θέση να επιταχύνουν χρονοβόρες διαδικασίες και να επιλύσουν διαφόρων ειδών προβλήματα. Στην αλυσίδα εφοδιασμού οποιουδήποτε οργανισμού, επιχείρησης ή εταιρείας υπάρχουν διάφορες βαθμίδες που συμμετέχουν σ'αυτή, ξεκινώντας από την παραγωγή μέχρι την κατανάλωση. Ένα εμπόρευμα, ξεκινώντας από το χώρο παραγωγής του περνά από διάφορα στάδια έως ότου φτάσει στον τελικό προορισμό του, όπως αποθήκες εμπορευμάτων και κέντρα διανομής. Έτσι, καθόλη τη διάρκεια και σε όλα τα στάδια διεκπεραίωσης μιας τόσο πολύπλοκης διαδικασίας, είναι χρήσιμη η βοήθεια που μπορούν να προσφέρουν τα συστήματα RFID, με τον κατάλληλο έλεγχο και τη διαρκή παρακολούθηση των αγαθών που διακινούνται.

Σχήμα 10. RFID στην αλυσίδα προμηθειών

Τα πλεονεκτήματα των εφαρμογών της τεχνολογίας RFID στις αλυσίδες προμηθειών είναι σημαντικά, αν και το υψηλό κόστος των καρτών περιορίζει την χρήση τους μόνο σε κιβώτια και παλέτες. Η χρήση των συστημάτων RFID επιτρέπει τον αυτοματισμό στην αποθήκευση και διανομή, όπως για παράδειγμα την έγκαιρη

αποστολή οδηγιών δρομολόγησης του εμπορεύματος. Επιτρέπει, επίσης, την καλύτερη παρακολούθηση των αγαθών, περιορίζοντας με αυτό τον τρόπο τις απώλειες αγαθών. Εμποδίζει, ακόμη, την εμφάνιση πλαστών ή παραποιημένων προϊόντων με τη χρήση ενσωματωμένων καρτών RFID για την αναγνώριση των γνήσιων προϊόντων. Τέλος, προσφέρει βελτιωμένη διαχείριση των αποθεμάτων, αφού είναι σε θέση να ενημερώνει για το απόθεμα αγαθών σε πραγματικό χρόνο.

3.2 Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης σε εγκαταστάσεις και άλλα μέρη όπου είναι απαραίτητη η εξουσιοδοτημένη άδεια εισόδου για λόγους ασφάλειας ή άλλους λόγους, είναι ένας ακόμη τομέας στον οποίο η τεχνολογία RFID χρησιμοποιείται ευρέως. Τα συστήματα RFID βρίσκουν εφαρμογή ως ηλεκτρονικά κλειδιά για τον έλεγχο πρόσβασης σε κτιριακές εγκαταστάσεις όπως γραφεία, αεροδρόμια, σχολεία και άλλους χώρους όπου για κάποιο λόγο, είναι αναγκαίος ο έλεγχος εισόδου μόνο σε εξουσιοδοτημένα πρόσωπα.

Στα συστήματα ελέγχου πρόσβασης χρησιμοποιούνται εκτενώς ειδικές κάρτες που περιέχουν μία επαγωγική παθητική κάρτα RFID. Ο αριθμός ταυτοποίησής της, που αντιστοιχεί βέβαια στον κάτοχό της, αναγνωρίζεται από τον αναγνώστη εντός μιας συγκεκριμένης απόστασης, επιτρέποντας την αυτόματη πιστοποίηση της αυθεντικότητας του κατόχου και την ελεύθερη πρόσβασή του. Οι κάρτες αυτές, που

Σχήμα 11. Ειδική κάρτα και αναγνώστης RFID για έλεγχο πρόσβασης

αντικαθιστούν τις παλαιότερου τύπου μαγνητικές κάρτες, καλύπτονται από το πρότυπο ISO/ICE 14443, ενώ οι διαχειριστές των συστημάτων πρόσβασης, συνήθως, προσθέτουν σε αυτές τα δικά τους ιδιωτικά στρώματα απόκρυψης, με στόχο την αύξηση της ασφάλειας.

3.3 Πληρωμή Μεταφορών

Τα συστήματα RFID για πληρωμή μεταφορών χρησιμοποιούνται για την αναγνώριση προσώπων ή οχημάτων καθώς και για την καταγραφή προπληρωμένων διελεύσεων. Οι εφαρμογές περιλαμβάνουν την ηλεκτρονική χρέωση διοδίων για οχήματα και τη συλλογή ναύλων διέλευσης.

Στην παρούσα φάση υπάρχουν πολλά και διαφορετικά συστήματα πληρωμής ανά την υφήλιο σε πολλές χώρες. Αυτά τα συστήματα χρησιμοποιούν τεχνολογία RFID για πληρωμές σε αυτοκινητόδρομους, σιδηροδρομικούς σταθμούς, λεωφορεία, μετρό και γενικά για μέσα μαζικής μεταφοράς. Ειδικότερα, η διέλευση από διόδια επιτυγχάνεται με τη χρήση ενεργών καρτών στα οχήματα, οι οποίες διαβάζονται από απόσταση καθώς το όχημα περνά από τις πύλες των διοδίων, ενώ οι πληροφορίες της κάρτας χρησιμοποιούνται για τη χρέωση ενός προπληρωμένου λογαριασμού. Η εφαρμογή του συστήματος βοηθά στην επιτάχυνση της κυκλοφοριακής κίνησης διά μέσου του σημείου πληρωμής διοδίων, καταγράφοντας τον ακριβή χρόνο και τη

χρέωση που αντιστοιχεί στην κάρτα RFID του οχήματος.

Σχήμα 12. Ενεργή ετικέτα για πληρωμή διοδίων

Σχήμα 13. Σημείο ηλεκτρονικής πληρωμής διοδίων

3.4 Ηλεκτρονικά Διαβατήρια

Οι κάρτες RFID βρίσκουν εφαρμογή σε διαβατήρια που εκδίδουν αρκετές χώρες. Τα πρώτα RFID διαβατήρια (“E-Passport”) εκδόθηκαν το 1998 από την Μαλαισία, ενώ στη συνέχεια ακολούθησαν και άλλες χώρες. Ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (ICAO) είναι υπεύθυνος για τον καθορισμό προτύπων για τα RFID διαβατήρια.

Το ολοκληρωμένο κύκλωμα της κάρτας του διαβατηρίου μπορεί να περιέχει εκτός των βασικών πληροφοριών που είναι καταγραμμένες στη σελίδα πληροφοριών του διαβατηρίου και άλλες χρηστικές πληροφορίες που είναι επιθυμητό να ενσωματωθούν. Αυτές οι πληροφορίες μπορεί να είναι για παράδειγμα, ένα ιστορικό ταξιδίων στο οποίο καταγράφονται ο χρόνος, η ημερομηνία και ο προορισμός εισόδων και εξόδων από τη χώρα ή ακόμη μία ψηφιακή φωτογραφία του κατόχου του διαβατηρίου.

Στην προσπάθεια για αύξηση της ασφάλειας των διαβατηρίων από μη εξουσιοδοτημένους αναγνώστες που επιδιώκουν την υποκλοπή πληροφοριών, λαμβάνονται διάφορα μέτρα προφύλαξης έτσι ώστε η κάρτα του διαβατηρίου να μη μπορεί να διαβαστεί από τον αναγνώστη RFID εάν πρώτα δεν εισαχθεί σε αυτόν ένας προσωπικός μυστικός αριθμός που αντιστοιχεί στο συγκεκριμένο διαβατήριο.

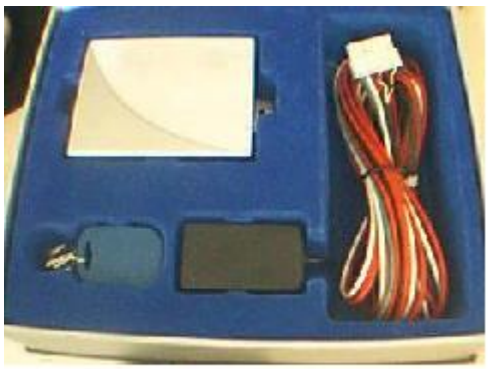
Σχήμα 14. Ασύρματος αναγνώστης RFID για ηλεκτρονικά διαβατήρια

Σχήμα 15. RFID chip ενσωματωμένο σε e - passport

3.5 Ασφάλεια Οχημάτων

Η χρήση συστημάτων RFID σε εφαρμογές ασφάλειας οχημάτων είναι πλέον πολύ συνηθισμένη. Σε πολλά καινούρια αυτοκίνητα χρησιμοποιούνται συστήματα RFID τα οποία επιτρέπουν μόνο σε ειδικά κλειδιά εφοδιασμένα με RFID να εκκινήσουν το όχημα. Οι εφαρμογές αυτές αποτελούν ένα ισχυρό αντικλεπτικό μέτρο.

Ένας αναγνώστης RFID ανιχνεύει την κρυπτογραφημένη κάρτα RFID, η οποία είναι ενσωματωμένη στο κλειδί του ιδιοκτήτη, όταν το κλειδί εισάγεται για εκκίνηση του οχήματος. Στη συνέχεια, στέλλει ένα κρυπτογραφημένο σήμα στην κάρτα απαιτώντας ένα σήμα ανταπόκρισης ίδιας κρυπτογράφησης. Αν η κάρτα απαντήσει σωστά τότε ο αναγνώστης επιτρέπει στο σύστημα έγχυσης καυσίμου του οχήματος να λειτουργήσει, αλλιώς το όχημα δεν ξεκινά.



Σχήμα 16. Ειδικός αναγνώστης RFID (immobilizer) για ασφάλεια οχημάτων

3.6 Ταυτοποίηση Ζώων

Η χρησιμοποίηση τεχνολογίας RFID για την αναγνώριση ζώων εξυπηρετεί σε σημαντικό βαθμό, κυρίως τη βιομηχανία ζωικών προϊόντων αλλά και ιδιώτες. Με τη χρήση της αναγνώρισης ζώων επιτυγχάνεται καλή διαχείριση σε φάρμες ζώων και έλεγχος των ασθενειών που εκδηλώνονται. Έτσι τα οφέλη που αποκομίζονται από αυτές τις εφαρμογές είναι εξίσου σημαντικά για το κοινωνικό σύνολο. Επίσης, καθίσταται δυνατή η εύρεση χαμένων ζώων.

Οι κάρτες RFID που χρησιμοποιούνται είναι παθητικές και μπορούν να εμφυτευτούν στα ζώα, όπου κοινώς έχουν την ονομασία chips και χρησιμοποιούνται ως πομποί όταν ενεργοποιηθούν.

Σχήμα 17. Ετικέτες RFID για εξωτερική εφαρμογή σε ζώα

3.7 Αυτοματοποιημένες Βιβλιοθήκες

Η χρησιμότητα των συστημάτων RFID είναι προφανής στην εφαρμογή τους σε βιβλιοθήκες. Ο εκσυγχρονισμός των βιβλιοθηκών επιτυγχάνεται λόγω των πλεονεκτημάτων της τεχνολογίας RFID έναντι παλιότερων παραδοσιακών τεχνολογιών για την αναγνώριση αντικειμένων βιβλιοθήκης (βιβλία, CD, DVD, κ.ά.). Η καθιερωμένη τεχνολογία γραμμωτού κώδικα (barcode) έχει ήδη αρχίσει να αντικαθιστάται με τεχνολογία RFID και στην παρούσα φάση υπολογίζεται ότι περίπου τριάντα εκατομμύρια αντικείμενα βιβλιοθήκης έχουν προσαρτημένες κάρτες RFID.

Οι κάρτες που είναι προσαρτημένες στα αντικείμενα μπορούν να διαβάζονται χωρίς να χρειάζεται να ανοιχτεί ένα βιβλίο ή μια θήκη DVD. Επίσης, η ανάγνωση των καρτών μπορεί να γίνει χωρίς επαφή, ακόμη κι όταν βρίσκονται σε κίνηση. Τα πλεονεκτήματα αυτά κάνουν ευκολότερο το δανεισμό και την επιστροφή βιβλίων, την απογραφή βιβλίων χωρίς τη μετακίνησή τους από τα ράφια καθώς και την καταγραφή τους σε πραγματικό χρόνο.

Δύο κύριοι τύποι συστημάτων χρησιμοποιούνται στις βιβλιοθήκες για την ανάκτηση των πληροφοριών ενός βιβλίου. Η κάρτα RFID, είτε περιέχει τα δεδομένα στο chip της και αυτά λαμβάνονται απευθείας, είτε περιέχει μια απλή βιβλιογραφική

Σχήμα 18. Κάρτες για βιβλιοθήκη: Τετράγωνη για βιβλίο, κυκλική για CD / DVD

αναφορά και τα δεδομένα λαμβάνονται από βάσεις δεδομένων της βιβλιοθήκης.

3.8 RFID στην υγεία

Η χρησιμοποίηση της τεχνολογίας RFID έχει αρχίσει και σε τομείς που αφορούν την υγεία. Τα οφέλη από τη χρήση της τεχνολογίας ήδη έχουν γίνει αντιληπτά και προβλέπεται ότι στο μέλλον θα αποκτήσουν ακόμη μεγαλύτερη βαρύτητα.

Κάποιες από τις εφαρμογές αφορούν εντοπισμό προσωπικού, εξοπλισμού και προμηθειών νοσοκομείων, ο οποίος σε πολλές περιπτώσεις πρέπει να γίνεται άμεσα. Επίσης, απαραίτητος είναι ο έλεγχος για παραποιημένα προϊόντα καθώς και η πρόληψη λαθών στην ιατρική φροντίδα. Οι εφαρμογές περιλαμβάνουν, ακόμη, την υποστήριξη της πρόσβασης σε ιατρικά αρχεία με ασφάλεια, καθώς και τον έλεγχο πρόσβασης προσωπικού σε αυτά.

Σχήμα 19. Βραχιόλι με ετικέτα RFID για ταυτοποίηση ασθενών

3.9 Μελλοντικές Χρήσεις

Οι δυνατότητες που προσφέρει η τεχνολογία RFID και έχουν ήδη χρησιμοποιηθεί σε υπάρχουσες εφαρμογές είναι ιδιαίτερα αξιόλογες, με αποτέλεσμα να διαφαίνεται ότι στο μέλλον θα υπάρξει περαιτέρω προσπάθεια αξιοποίησης της τεχνολογίας σε μεγαλύτερη κλίμακα απ'ότι σήμερα. Η εξάπλωση της τεχνολογίας στον εμπορικό, αλλά και σε άλλους τομείς, ήδη εξετάζεται σοβαρά, ενώ τα εμπόδια που παρουσιάζονται όπως είναι το κόστος κατασκευής και άλλα τεχνικά προβλήματα, βρίσκονται σε διαδικασία έρευνας με στόχο την οριστική υπερπήδησή τους.

Η αντικατάσταση της τεχνολογίας του γραμμωτού κώδικα (barcode) έχει επιτευχθεί μέχρι στιγμής μόνο στις περιπτώσεις χαρτοκιβωτίων και παλέτων, όμως ο αντικειμενικός σκοπός των συστημάτων RFID είναι η πλήρης εφαρμογή τους για όλα τα αγαθά που μπορεί να αγοράσει κάποιος σε ένα κατάστημα. Για παράδειγμα, το

διάβασμα των καρτών RFID από προϊόντα και η χρέωση αυτών, καθώς ένα καρότσι σε μια τυπική υπεραγορά θα σπρώχνεται σε ένα ανάλογα εφοδιασμένο διάδρομο που θα έχει ρόλο ταμείου, θα μείωνε σημαντικά τα λειτουργικά έξοδα και θα επιτάχυνε τη διαδικασία στα ταμεία. Ένα τέτοιο αυτόματο σύστημα δεν χρειάζεται σάρωση γραμμωτού κώδικα, όμως απαιτεί τεράστιο χώρο μνήμης για αποθήκευση δεδομένων σχετικά με τα εμπλεκόμενα αντικείμενα σε όλα τα επίπεδα. Παρέχει, όμως, σημαντικά πλεονεκτήματα σε σχέση με το γραμμωτό κώδικα, όπως είναι η δυνατότητα ύπαρξης ενός μοναδικού αριθμού ταυτοποίησης για κάθε ένα αντικείμενο σε αντίθεση με το γραμμωτό κώδικα που περιορίζεται σε ένα μόνο τύπο κωδικού για κάθε προϊόν. Αν τα προβλήματα που εμποδίζουν αυτές τις εφαρμογές δεν καταστεί δυνατό να ξεπεραστούν, ίσως τότε να υπάρξει συνδυασμός RFID και υπαρχουσών τεχνολογιών με στόχο πάντα τον εκσυγχρονισμό στη λειτουργία αυτού του τομέα.

Σε άλλες εφαρμογές υπάρχει η δυνατότητα χρησιμοποίησης ενεργών καρτών σαν χαμηλού κόστους απομακρυσμένους αισθητήρες οι οποίοι να μπορούν να εκπέμπουν δεδομένα τηλεμετρίας προς ένα σταθμό βάσης. Τα δεδομένα αυτά μπορούν να αφορούν τις συνθήκες σε δρόμους, τις καιρικές συνθήκες καθώς και τον έλεγχο των επιπέδων θορύβου.

Οι εμφυτεύσιμες κάρτες RFID σε ανθρώπους είναι επίσης μία εφαρμογή που ενδέχεται να τύχει μεγαλύτερης αποδοχής και χρήσης. Κάποιες επιτυχημένες προσθήκες chips RFID σε ανθρώπους που έγιναν μεμονωμένα για διάφορους σκοπούς, ίσως να ωθήσουν την ευρύτερη χρησιμοποίησή τους σε όποιους τομείς μπορεί να φανεί χρήσιμο. Υπάρχουν ήδη, για παράδειγμα, διαθέσιμα RFID chips τα οποία είναι σε θέση να ενσωματώσουν προσωπικά ιατρικά δεδομένα και έτσι να σώσουν ζωές και να περιορίσουν τραυματισμούς από λάθη στην ιατρική θεραπεία. Ακόμα, τα εμφυτεύσιμα chips μπορούν να χρησιμοποιηθούν για τον έλεγχο προσωπικού ή επισκεπτών σε όποιο μέρος αυτό κριθεί απαραίτητο.

Οι εφαρμογές που θα παρουσιαστούν στο μέλλον, ίσως να περάσουν και σε τομείς όπου δεν υπάρχει σκέψη για χρησιμοποίηση της τεχνολογίας RFID στην

παρούσα φάση. Ούτως ή άλλως οι εφαρμογές RFID περιορίζονται μονάχα από τη φαντασία μας.

4. Προβλήματα και Σκέψεις

Η προοπτική που δείχνει να έχει η τεχνολογία RFID για να αναδειχθεί σε σημαντικό παράγοντα σε πολλούς επιχειρηματικούς τομείς, ίσως να εκτροχιαστεί εάν τα προβλήματα που υπάρχουν δεν αντιμετωπιστούν στο μέλλον. Η επίδραση που θα μπορούσε να έχει η τεχνολογία σε ένα μεγάλο αριθμό δραστηριοτήτων της καθημερινής ζωής, εξαρτάται από τη δυνατότητα να ξεπεραστούν τα εμπόδια τα οποία περιορίζουν την υιοθέτηση της τεχνολογίας σε ευρεία κλίμακα. Ακολουθεί μία σύντομη περιγραφή των εμποδίων που παρουσιάζονται στην πορεία για την ευρεία αποδοχή των RFID, καθώς και κάποιες ανησυχίες που εγείρονται σε σχέση με την προστασία της ιδιωτικής ζωής των χρηστών σε μερικές εφαρμογές.

4.1 Κόστος

Το πρώτο και σπουδαιότερο εμπόδιο που υπάρχει, είναι το σχετικά υψηλό κόστος των καρτών RFID. Το ολοκληρωμένο κύκλωμα, η κεραία και η συναρμολόγηση της κάρτας, είναι οι τρεις κύριες πηγές που προκαλούν το κόστος αυτό. Η γρήγορη πτώση της τιμής των ολοκληρωμένων και η ανάπτυξη λιγότερο ακριβών μεθόδων συναρμολόγησης που έχουν επιτευχθεί προσφάτως, αποτελούν ενθαρρυντικές εξελίξεις. Ωστόσο ακόμα παραμένει σχετικά υψηλό το κόστος, ώστε να είναι σε θέση να αντικαταστήσει την τεχνολογία γραμμωτού κώδικα για μικρά και πολύ φθηνά προϊόντα.

4.2 Αξιοπιστία

Η απόδοση ενός συστήματος RFID εξαρτάται από διάφορους παράγοντες όπως είναι ο προσανατολισμός των κεραιών κάρτας και αναγνώστη, το υλικό από το οποίο είναι κατασκευασμένο το αντικείμενο στο οποίο εφαρμόζεται η κάρτα, καθώς και το περιβάλλον στο οποίο λειτουργεί το σύστημα. Η μειωμένη απόδοση του συστήματος

σε κάποιες περιπτώσεις, ίσως να είναι τόσο σοβαρή ώστε να παρουσιαστούν προβλήματα αξιοπιστίας. Διάφορα μέτρα είναι δυνατό να ληφθούν, όπως καλύτερα σχεδιασμένες κεραίες, συνδυασμός πολλαπλών κεραιών και χρήση πίσω επιμετάλλωσης για τη βελτίωση της ισχύος του σήματος. Τα μέτρα αυτά βελτιώνουν σε σημαντικό βαθμό την αξιοπιστία των συστημάτων RFID που αντιμετωπίζουν προβλήματα, όμως περαιτέρω μελέτη και έρευνα είναι απαραίτητο να διεξαχθεί με στόχο το καλύτερο δυνατό αποτέλεσμα.

4.3 Ασφάλεια και ιδιωτική ζωή

Οι ανησυχίες για την ασφάλεια και την προστασία της ιδιωτικής ζωής συνυπάρχουν σε όλα τα ασύρματα συστήματα, συμπεριλαμβανομένων των συστημάτων RFID. Οι ανησυχίες αυτές εντείνονται μάλιστα και υπερτονίζονται, μετά από επιδείξεις κατά τις οποίες τα προγράμματα για την ασφάλεια των συστημάτων RFID "σπάστηκαν" επιτυχώς. Αυτά τα κενά που παρουσιάστηκαν στην ασφάλεια, οφείλονται κατά κύριο λόγο στο γεγονός ότι κάποιες εφαρμογές RFID και κάποια πρότυπα συμβιβάστηκαν για χάρη του χαμηλού κόστους, με αποτέλεσμα να γίνουν ευάλωτα στην πλαστογραφία, τον παράνομο εντοπισμό και τη διαρροή πληροφοριών.

Η προσπάθεια για ενίσχυση της ασφάλειας των συστημάτων RFID περιλαμβάνει διάφορες τεχνικές . Μια τυπική προσέγγιση που μπορεί να χρησιμοποιηθεί, είναι η κωδικοποίηση του αριθμού ταυτοποίησης (ID) της κάρτας RFID που όμως παρουσιάζει δυσκολίες στην υλοποίηση, αφού δεν υπάρχει αρκετή ενέργεια για την τροφοδοσία κυκλωμάτων κωδικοποίησης. Μία άλλη προσέγγιση είναι η εξασφάλιση της επικοινωνίας μεταξύ κάρτας και αναγνώστη με τη χρησιμοποίηση σχημάτων ασύμμετρης διαμόρφωσης, τα οποία είναι στενή ζώνη για ενίσχυση της τροφοδότησης και πολύ πλατιά ζώνη για επικοινωνία.

4.4 Ενσωμάτωση Συστημάτων

Ένα μεγάλης κλίμακας σύστημα RFID, ειδικά όταν αφορά εφαρμογές όπως την

αλυσίδα προμηθειών και την παρακολούθηση αποσκευών, κάνει τη διαδικασία ενσωμάτωσης πιο περίπλοκη. Περιλαμβάνει ενσωμάτωση νέων δεδομένων στο σύστημα κατά τη λήψη τους και χρήση των πληροφοριών που συγκεντρώνονται, για μεγαλύτερη αποτελεσματικότητα. Η διαδικασία γίνεται ακόμη πιο πολύπλοκη, λόγω της έλλειψης ενός ευρέως αποδεκτού προτύπου τόσο για εξαρτήματα όσο και για λογισμικό. Η αναγκαιότητα εύρεσης προτύπων που να είναι καθολικής αποδοχής, θα εξυπηρετήσει τους υπάρχοντες αλλά και τους μελλοντικούς χρήστες των συστημάτων RFID, αφού με αυτό τον τρόπο θα καταστεί δυνατή η διασύνδεση των νέων συστημάτων στις υπάρχουσες υποδομές που τα υποστηρίζουν.

ΑΝΑΦΟΡΕΣ

Βιβλιογραφία

- R. Want, RFID Explained: A Primer on Radio Frequency Identification Technologies Synthesis Lectures on Mobile and Pervasive Computing, Morgan & Claypool Publishers, 15 Oct. 2006.
- Whitepaper on “RFID Technology and its Use in the Supply Chain” http://www.printronix.com/library/assets/public/case-studies/rfid-laranwhite-paper-english.pdf
- P. Peris-Lopez et al., “RFID Systems: A Survey on Security Threats and Proposed Solutions,” Proc. Int’l. Conf. Pers. Wireless Commun., Sept. 2006.
- K. Finkelzeller, The RFID Handbook, 2nd edition., John Wiley & Sons, 2003.

- J. D. Griffin, G. D. Durgin, A. Haldi, and B. Kippelen, “RF tag antenna performance of various materials using radio link budgets,” IEEE Trans. Antenna Wireless Propag. Lett., vol. 5, 2006.
- D. Henrici, “RFID Security and Privacy”, Springer-Verlag, 2008

Ιστοσελίδες

- http://en.wikipedia.org/wiki/RFID
- “RFID Journal ”, http://www.rfidjournal.com/
- http://www.rfidconsultation.eu/
- http://www.rsa.com/rsalabs
- http://www.rfidnews.org
- http://www.rfidgazette.org
- http://www.itsc.org.sg
- http://www.technovelgy.com
- http://www.autoidlabs.org

ΚΕΦΑΛΑΙΟ 3

ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ RFID

1. Γενικά

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, οι εφαρμογές του RFID είναι πάρα πολλές, γεγονός το οποίο μας θα μας βοηθά στο μέλλον στην καθημερινή μας – και όχι μόνο – ζωή, είτε το αντιλαμβανόμαστε είτε όχι. Η χρήση συσκευών RFID θα αυξηθεί δραματικά τα επόμενα χρόνια καθώς έμποροι και επιχειρήσεις χρησιμοποιούν αυτή τη συχνά διακριτική τεχνολογία επικοινωνιών.

Αλλά μήπως αυτά τα κυκλώματα και συστήματα, που εκπέμπουν bits πληροφοριών, ανοίγουν πόρτες σε πιθανές παραβιάσεις ασφαλείας; Μήπως η χρήση τους δημιουργεί ακόμη ένα σημείο πρόσβασης για ιούς και κακόβουλο κώδικα; Αυτές είναι ελάχιστες μόνο από τις ερωτήσεις με τις οποίες καταπιάνονται ειδικοί ασφάλειας και χρήστες RFID, καθώς αυτές οι συσκευές καλούνται να παραδώσουν πολλά περισσότερα από την απλή παρακολούθηση προϊόντων.

“Κάθε είδους ψηφιακή τεχνολογία που είναι δικτυωμένη, μπορεί να παραβιαστεί και να φθαρεί με κακή πρόθεση¨, είπε ο Srini Krishnamurthy, αντιπρόεδρος στρατηγικής και επιχειρησιακής ανάπτυξης της εταιρίας Airbee Wireless, ενός μεγάλου παροχέα ασύρματων τηλεπικοινωνιακών λύσεων. “Τα δεδομένα που διακινούνται μέσω RFID, μπορεί να είναι μόνο για ανάγνωση και σε μερικές περιπτώσεις ανάγνωση/εγγραφή, αλλά ζουν στο ίδιο περιβάλλον στο οποίο ζουν οι ιοί και τα “σκουλήκια” που κατακλύζουν το Διαδίκτυο.”

Έτσι, λοιπόν, εγείρεται το ζήτημα της ασφάλειας σε τέτοιες διατάξεις. Αυτό είναι πολύ σημαντικό, καθώς με την τεχνολογία RFID δημιουργούνται θέματα σχετικά με την τήρηση του απορρήτου, δεδομένου ότι χρησιμοποιείται για τη συλλογή και διάδοση πληροφοριών προσωπικού ή και διαφορετικού χαρακτήρα.

2. Ανησυχία στους αριθμούς

Αυτό που κάνει τους ειδικούς της ασφάλειας να ανησυχούν ιδιαίτερα, είναι ο μεγάλος αριθμός των εκατομμυρίων συσκευών RFID που υπάρχουν ήδη στην αγορά και χρησιμοποιούνται.

Σύμφωνα με έρευνες, οι παγκόσμιες δαπάνες για το RFID, ανέρχονταν στα 504 εκατομμύρια δολάρια το 2005, ενώ το 2010 θα ξεπεράσουν τα 3 δις!

Μεγάλοι πωλητές λιανικής έχουν δεχτεί την τεχνολογία αυτή σαν μέσο για καλύτερη κατανόηση της δυναμικής της προμηθευτικής αλυσίδας και του κόστους ελέγχου.

Και ενώ οι πωλητές και οι χρήστες RFID πάντα ανησυχούσαν για την ασφάλεια και την πιθανότητα κατάχρησης αυτών των συστημάτων, αναφορές για πιθανές ευπάθειες αυτών των συσκευών έχουν προκαλέσει περαιτέρω ανησυχία.

3. Παραβίαση συστημάτων

Οι περισσότερες εταιρίες ανησυχούν περισσότερο για τις ηθελημένες επιθέσεις και τη φθορά των δεδομένων που αποθηκεύονται προσωρινά στις συσκευές RFID και τα οποία αργότερα διακινούνται μέσω δικτύων και εταιρικών βάσεων δεδομένων. Ένας εισβολέας θα μπορούσε για παράδειγμα να κρύψει κακόβουλο κώδικα μέσα στα 90 με 100 bits δεδομένων που περιέχονται στις περισσότερες κάρτες RFID. Παρότι αμελητέα, αυτά τα δεδομένα θα μπορούσαν να χρησιμοποιηθούν για να παραβιάσουν με χρήση SQL μια βάση δεδομένων με σκοπό να δημιουργήσουν μια πίσω πόρτα ή να εκμεταλλευτούν κάποια αδυναμία σε μια ιστοσελίδα κατασκευασμένη με PHP.

Ο Krishnamurthy της εταιρίας Airbee[1], κατέδειξε πιθανά προβλήματα που υπάρχουν στους αναγνώστες και στο ενδιάμεσο λογισμικό (middleware) που αλληλεπιδρά με τις κάρτες. Αυτού του είδους το λογισμικό μπορεί να μην είναι σχεδιασμένο να συλλαμβάνει κάτι πέρα από απλά σφάλματα υπερχείλισης των buffers στις κάρτες, με αποτέλεσμα κακόβουλος κώδικας να παρερμηνευθεί σαν εντολές για βάση δεδομένων και να δημιουργηθεί, έτσι, μια αλυσιδωτή αντίδραση

[1]Airbee: Εταιρία ανάπτυξης λογισμικού διασύνδεσης για επικοινωνίες φωνής και δεδομένων στις ΗΠΑ

φθαρμένων δεδομένων που ρέει στην κεντρική πηγή πληροφοριών.

Ένα τέτοιο σενάριο θα ήταν οπωσδήποτε αληθοφανές αν και όχι πιθανό, καθώς ένα σχεδιαστικό ψεγάδι τέτοιου μεγέθους θα ήταν καταστροφικό.

Οι ανησυχίες που εγείρονται για την ασφάλεια των καρτών RFID, δεν παραβλέπονται εύκολα από αυτούς που βρίσκονται στην πλευρά της ανάπτυξης και σχεδίασης. Οι κατασκευαστές τέτοιων συσκευών κάνουν κάποια θετικά βήματα προς την κατεύθυνση της δημιουργίας μιας καινούριας γενιάς που θα είναι εγγενώς πιο ασφαλή από τα προηγούμενα συστήματα.

4. Ποιος ελέγχει τι;

Τα δεδομένα που βρίσκονται αποθηκευμένα σε μια κάρτα (tag) RFID είναι συνήθως προσβάσιμα από όλους, όπως για παράδειγμα αυτά που προσδιορίζουν την περιγραφή ενός προϊόντος. Τέτοια δεδομένα απαιτούν μικρού μόνο βαθμού προστασία, καθώς δεν μεταφέρουν προσωπικά στοιχεία (εκτός κι αν συνδυαστούν με άλλες πληροφορίες). Υπάρχουν, ωστόσο, εφαρμογές οι οποίες μπορεί να απαιτούν την αποθήκευση ιδιωτικών δεδομένων, τα οποία και πρέπει να προστατεύονται κατά τη μεταβίβασή τους από την κάρτα στη συσκευή ανάγνωσης και από εκεί στο δίκτυο.

Την απόφαση για το ποιος επιτρέπεται να συλλέγει δεδομένα από αντικείμενα που έχουν εφοδιαστεί με κάρτες RFID, την παίρνει το άτομο ή οργανισμός στον οποίο αυτά ανήκουν. Όμως, ουσιαστικά οποιοσδήποτε διαθέτει και μπορεί να χειριστεί έναν αναγνώστη RFID, με την προϋπόθεση ότι βρίσκεται εντός της εμβέλειας μιας κάρτας, μπορεί να λάβει και να διαχειριστεί με όποιο τρόπο θέλει τις πληροφορίες που εκπέμπονται από αυτή. Προς το παρόν, στην πλειονότητα των περιπτώσεων δεν υπάρχουν οι κατάλληλες διατάξεις που να επιτρέπουν τον προσδιορισμό του παραλήπτη των δεδομένων.

Στις σύγχρονες εφαρμογές του RFID, την απόφαση λαμβάνει αυτός που συλλέγει τα δεδομένα. Έτσι, μπορεί να τα κρατήσει κρυφά και προστατευμένα, ή να τα δημοσιεύσει. Υπάρχει περίπτωση κάποιες φορές ο αρχικός κάτοχος των δεδομένων να ενημερωθεί για την “υποκλοπή” αυτή, άλλοτε πάλι όχι. Ωστόσο, στην πλειοψηφία των περιπτώσεων δε θα μπορεί να κάνει κάτι γι' αυτό.

Οι περισσότερες κάρτες – ακόμη και αυτές που προστατεύουν τα δεδομένα με κάποιο κρυπτογραφικό αλγόριθμο – εκπέμπουν συγκεκριμένα ειδικά αναγνωριστικά. Κατά συνέπεια, κάποιος που φέρει μια τέτοια κάρτα, εκπέμπει ένα προκαθορισμένο σειριακό αριθμό που είναι εξαιρετικά επιρρεπής σε υποκλοπές.

Ακόμη μεγαλύτερη απειλή για την ιδιωτικότητα παρουσιάζεται, όταν ένας σειριακός αριθμός συνδυάζεται με προσωπικές πληροφορίες. Παραδείγματος χάριν, όταν ένας καταναλωτής κάνει μια αγορά μέσω πιστωτικής , ένα κατάστημα μπορεί να κάνει συσχετισμούς μεταξύ της ταυτότητάς του και των αριθμών των tags που διαθέτει, με αποτέλεσμα αναλυτές της αγοράς να μπορούν να αναγνωρίσουν και να επεξεργαστούν τις καταναλωτικές του συνήθειες χρησιμοποιώντας ένα δίκτυο από αναγνώστες RFID.

Επιπλέον, ορισμένες κάρτες, εκτός από το συγκεκριμένο σειριακό αριθμό, μεταφέρουν και πληροφορίες για το είδος του αντικειμένου στο οποίο είναι προσκολλημένες. Έτσι, κάποιος μπορεί να προσδιορίσει τι φάρμακα έχουμε αγοράσει (και κατ' επέκταση από ποιες ασθένειες πάσχουμε), τι είδους κάρτες αγορών έχουμε (και επομένως από που κάνουμε τις αγορές μας) κλπ. Το συγκεκριμένο είναι ένα σημαντικό πρόβλημα στον τομέα του RFID.

Προς το παρόν τα θέματα αυτά δεν είναι μείζονος σημασίας, καθώς η τεχνολογία αυτή δεν είναι ιδιαίτερα διαδεδομένη στην καθημερινή μας ζωή, ωστόσο μόλις αυτό συμβεί – κάτι το οποίο είναι σχεδόν αναπόφευκτο – τα προβλήματα αυτά θα λάβουν ακόμη μεγαλύτερες διαστάσεις.

Ορισμένες εφαρμογές του RFID είναι οι πομποδέκτες πληρωμής διοδίων, οι κάρτες των βιβλιοθηκών, τα διαβατήρια και όχι σε τόσο μεγάλο βαθμό η εμφύτευση σε ανθρώπους (για χρήση σε ιατρικό ιστορικό, για απαίτηση φυσικής παρουσίας για την είσοδο σε περιοχές περιορισμένης πρόσβασης κτλ.)

5. Νέες απειλές ασφαλείας

Οι απειλές ασφαλείας που προκύπτουν από τα διάφορα RFID συστήματα, μπορεί να μη σχετίζονται μόνο με τον τεχνικό εξοπλισμό ή τις επιχειρηματικές

δραστηριότητες για τις οποίες προορίζονται, άλλα να περιλαμβάνουν κι οποιαδήποτε άλλη κατάσταση σχετική με την ασφάλεια.

Επομένως, σε αντιδιαστολή με τα προβλήματα ασφαλείας που προκύπτουν από άλλες τεχνολογίες (π.χ. η χρήση των Η/Υ) τα οποία μπορούν να επιλυθούν με την διασφάλιση των συστημάτων που χρησιμοποιούνται, η χρήση του RFID μπορεί να οδηγήσει στην εξάπλωση τεχνολογίας που δε μπορεί να διαχειριστεί ή να διασφαλιστεί.

6. Η φύση της ασφάλειας

Η ασφάλεια των συστημάτων RFID δεν είναι, όμως, μόνο τεχνικό ζήτημα. Ενώ ουσιαστικά η διασφάλιση τους για την προστασία των συλλεχθέντων και αποθηκευμένων πληροφοριών είναι ένα θέμα, ένα δεύτερο θέμα είναι και η διασφάλιση της ποιότητας της αποθηκευμένης πληροφορίας.

Αυτό οδηγεί σε κάποια πρόσθετα ερωτήματα: Ποιος κατέχει και ελέγχει τα δεδομένα που αποθηκεύονται στην κάρτα ή συλλέγονται από διάφορα πληροφοριακά συστήματα; Σε ποιου τη δικαιοδοσία υπόκεινται αυτές οι πληροφορίες; Αυτά και άλλα παρόμοια ερωτήματα είναι επιτακτικό να απαντηθούν.

Είναι εμφανές λοιπόν, ότι είναι σημαντικό να επιβεβαιώνουμε ποιος παρέχει, τροποποιεί, ελέγχει ή είναι υπεύθυνος για ένα σύνολο δεδομένων. Οι πληροφορίες που υπάρχουν σε μια κάρτα RFID μπορούν να διαμοιραστούν σε όλη την υφήλιο . Η πρόκληση σε αυτό βρίσκεται στο διαχωρισμό των δεδομένων σε ακριβή και ανακριβή. Αυτό θα κάνει τη διαφορά στο αν θα είναι ασφαλές ή όχι να βασίζονται αποφάσεις σε πληροφορίες που παρέχονται από RFID συστήματα.

7. Προβλήματα με τα standards

Ένα σύστημα RFID μπορεί να χρησιμοποιήσει διάφορα πρότυπα. Το πρόβλημα μέχρι σήμερα είναι ότι δεν υπάρχει κάποιο παγκόσμια αποδεκτό standard, παρά το γεγονός ότι η έρευνα είναι διαρκής για την ανάπτυξη τέτοιων προτύπων. Η κοινή πεποίθηση είναι πως δεν υπάρχουν πρότυπα, αντιθέτως όμως το ζήτημα είναι ότι υπάρχουν πολλά (είτε καθιερωμένα είτε υπό ανάπτυξη). Τα ανταγωνιζόμενα

standards είναι ένα από τα πιο δύσκολα θέματα του RFID και, αποτέλεσμα αυτού είναι ότι οι περισσότερες τέτοιες εφαρμογές σήμερα είναι κλειστά συστήματα.

Το RFID έχει εφαρμοστεί με διαφορετικούς τρόπους από διαφορετικούς κατασκευαστές. Υπάρχουν υφιστάμενα και προταθέντα standards που ασχολούνται με το πρωτόκολλο επικοινωνίας μέσω αέρα (air interface protocol – ο τρόπος με τον οποίο επικοινωνούν οι κάρτες με τους αναγνώστες), με το περιεχόμενο δεδομένων (ο τρόπος με τον οποίο οργανώνονται ή διαμορφώνονται τα δεδομένα), με τη συμμόρφωση (τρόποι για να ελέγχεται αν τα προϊόντα συμμορφώνονται με ένα standard) και με τις εφαρμογές (πώς τα standards χρησιμοποιούνται, σε tags αποστολής δεμάτων για παράδειγμα).

Ο Διεθνής Οργανισμός Προτύπων (ISO) έχει δημιουργήσει πρότυπα για τον εντοπισμό κοπαδιών ζώων μέσω RFID, για τον καθορισμό της δομής των δεδομένων στις κάρτες RFID (ISO 11784) και για τον καθορισμό του πρωτοκόλλου διεπαφής αέρα (ISO 11785). Επίσης πρότυπα για τις κάρτες RFID που χρησιμοποιούνται σε συστήματα πληρωμών και έξυπνων καρτών (ISO 14443), πρότυπα για τον έλεγχο της συμμόρφωσης των καρτών και αναγνωστών RFID σε ένα πρότυπο (ISO 18047), καθώς επίσης και για τον έλεγχο της απόδοσής τους (ISO 18046).

Εν τούτοις, η κατάσταση με τα πρότυπα περιπλέχθηκε από το γεγονός ότι το Κέντρο Αυτόματων Ταυτοτήτων (Auto-ID Center – συνεργασία μεταξύ 100 παγκόσμιων επιχειρήσεων και έξι εκ των πρωτοπόρων στην έρευνα πανεπιστημίων του κόσμου) το οποίο ανέπτυξε την τεχνολογία του Ηλεκτρονικού Κωδικού Προϊόντος (Electronic Product Code – EPC), επέλεξε να δημιουργήσει το δικό της τρόπο επικοινωνίας καρτών-αναγνωστών για τον εντοπισμό προϊόντων στην παγκόσμια αλυσίδα προμηθειών.

Πρότυπα και προδιαγραφές μπορούν να τεθούν σε διεθνές, εθνικό, βιομηχανικό ή εμπορικής συνεργασίας επίπεδο και μεμονωμένοι οργανισμοί μπορούν να θέσουν τις δικές τους προδιαγραφές σαν standards. Πολλά πρότυπα του χώρου της βιομηχανίας που τίθενται από τέτοιους οργανισμούς, βασίζονται σε διεθνή πρότυπα για να κάνουν πιο εύκολη την εφαρμογή και την υποστήριξη και να παρέχουν ένα ευρύτερο πεδίο επιλογής προϊόντων. Όλο και περισσότεροι κατασκευαστές δημιουργούν δικά τους

πρότυπα με σκοπό να κερδίσουν την αγορά μέσω της δικής τους πνευματικής ιδιοκτησίας. Έτσι πολλές επιχειρήσεις οδηγούνται στο να υιοθετήσουν την συγκεκριμένη τεχνολογία χωρίς αυτή να έχει ωριμάσει, κάτι που σημαίνει ότι περιέχει μεταξύ άλλων και τα όποια άλυτα προβλήματα αναφορικά με την ασφάλεια.

Τα standards μπορούν να προσαρμοστούν για να περιλαμβάνουν τη διαμόρφωση (format) και το περιεχόμενο των κωδικών που τοποθετούνται στις κάρτες RFID, τα πρωτόκολλα και τις συχνότητες που θα χρησιμοποιηθούν από τις κάρτες και τους αναγνώστες για να εκπέμπουν και να λαμβάνουν τα δεδομένα καθώς και την ασφάλεια και την ανθεκτικότητα στις πλαστογραφήσεις.

8. Τεχνικά προβλήματα

- *Παρεμβολές στα συστήματα RFID*

Εφόσον τα συστήματα RFID κάνουν χρήση του ηλεκτρομαγνητικού φάσματος (όπως τα ασύρματα δίκτυα ή τα κινητά), είναι πολύ εύκολο να δημιουργηθούν παρεμβολές χρησιμοποιώντας ενέργεια στη σωστή συχνότητα. Παρά το ότι αυτό θα αποτελούσε μια απλή ενόχληση για τους καταναλωτές στα καταστήματα, θα μπορούσε να έχει καταστροφικές συνέπειες σε άλλα ευαίσθητα περιβάλλοντα όπου γίνεται αυξανόμενη χρήση των RFID όπως σε νοσοκομεία ή στο στρατό στο πεδίο της μάχης.

- *Συγκρούσεις συσκευών ανάγνωσης*

Τέτοιες συγκρούσεις συμβαίνουν όταν τα σήματα από δυο οι περισσότερους αναγνώστες επικαλύπτονται. Η κάρτα δεν είναι σε θέση να απαντήσει σε ταυτόχρονα ερωτήματα. Τα προβλήματα αυτά έχουν κάποιες ομοιότητες με τα προβλήματα ανάθεσης συχνοτήτων στα συστήματα κινητής τηλεφωνίας. Ωστόσο, οι προσεγγίσεις που έχουν αποτέλεσμα στην κινητή τηλεφωνία, δεν λειτουργούν στο RFID λόγω της περιορισμένης λειτουργικότητας των καρτών. Η ανικανότητα των καρτών να βοηθήσουν στην επικοινωνία, σημαίνει ότι δε μπορούν να ξεχωρίσουν μεταξύ δυο αναγνωστών που επικοινωνούν μαζί τους ταυτόχρονα. Ως αποτέλεσμα, δυο αναγνώστες που επικοινωνούν με την ίδια κάρτα, πρέπει να το κάνουν σε

διαφορετικούς χρόνους. Τα συστήματα πρέπει να εγκαθίστανται προσεκτικά, ώστε να αποφεύγονται τέτοιου είδους προβλήματα. Πολλά συστήματα χρησιμοποιούν κάποιο πρωτόκολλο αντί-σύγκρουσης. Τέτοια πρωτόκολλα επιτρέπουν στις κάρτες να στέλνουν δεδομένα με τη σειρά σε έναν αναγνώστη.

- *Συγκρούσεις καρτών*

Αυτές συμβαίνουν όταν υπάρχουν πολλές κάρτες σε μια μικρή περιοχή. Έτσι κατά τη διάρκεια της επικοινωνίας τους με έναν αναγνώστη, τα σήματά τους περιπλέκονται. Αυτές οι παρεμβολές οδηγούν συνήθως σε αποτυχία της μετάδοσης. Για να μην συμβαίνει αυτό, πρέπει να εφαρμοστεί κάποια μέθοδος αποτροπής συγκρούσεων. Επειδή, όμως ο χρόνος ανάγνωσης είναι πολύ μικρός, είναι πιο εύκολο για τους κατασκευαστές να αναπτύσσουν συστήματα που εξασφαλίζουν ότι οι κάρτες απαντούν μια κάθε φορά.

9. Προβλήματα ασφαλείας, ιδιωτικότητας και ηθικής

- *Τα περιεχόμενα μιας κάρτας RFID μπορούν να διαβαστούν ακόμη και αφού το αντικείμενο έχει φύγει από την καταναλωτική αλυσίδα*

Μια κάρτα δε μπορεί να καταλάβει τη διαφορά μεταξύ δυο διαφορετικών συσκευών ανάγνωσης. Τέτοιες συσκευές είναι εξαιρετικά φορητές και μπορούν να διαβάσουν τις κάρτες από απόσταση μερικών εκατοστών μέχρι μερικά μέτρα. Έτσι, ο οποιοσδήποτε έχει τη δυνατότητα να δει τα περιεχόμενα της τσάντας ή της τσέπης μας καθώς περπατάμε στο δρόμο. Γι' αυτό και ορισμένες κάρτες έχουν δυνατότητα απενεργοποίησης.

- *Οι κάρτες είναι δύσκολο να αφαιρεθούν*

Οι καταναλωτές δεν είναι εύκολο να αφαιρέσουν μια κάρτα RFID. Άλλες είναι πολύ μικρές, ενώ άλλες είναι ενσωματωμένες μέσα στο προϊόν όπου κάποιος δε μπορεί να τις δει. Νέες τεχνολογίες επιτρέπουν στις κάρτες να "εκτυπώνονται" κατευθείαν επάνω στο προϊόν και ίσως να μην είναι δυνατόν να αφαιρεθούν καθόλου.

- *Οι κάρτες μπορεί να αναγνωστούν χωρίς τη γνώση μας*

Εφόσον οι κάρτες μπορούν να αναγνωστούν χωρίς να κλαπούν ή να "σαρωθούν" εμφανώς (όπως συμβαίνει με π.χ. με τις μαγνητικές ταινίες), ο οποιοσδήποτε με έναν αναγνώστη RFID μπορεί να διαβάσει τις κάρτες που υπάρχουν στα ρούχα μας ή σε άλλα προϊόντα, εν αγνοία μας.

- *Οι κάρτες μπορούν να διαβαστούν από μεγάλες αποστάσεις με μια κεραία υψηλότερου κέρδους σήματος (high-gain antenna)*

Τα συστήματα RFID σχεδιάζονται ώστε η απόσταση ανάγνωσης μεταξύ κάρτας-αναγνώστη να διατηρείται στο ελάχιστο. Ωστόσο μια κεραία υψηλού κέρδους σήματος, μπορεί να χρησιμοποιηθεί για να διαβάσει μια κάρτα από πολύ μακρύτερα οδηγώντας σε προβλήματα ιδιωτικότητας.

- *Κάρτες με διακριτούς σειριακούς αριθμούς θα μπορούσαν να συνδεθούν σε ένα συγκεκριμένο αριθμό πιστωτικής .*

Γίνεται έρευνα πάνω σε ένα παγκόσμιο σύστημα ταυτοποίησης προϊόντων, που θα επιτρέπει σε κάθε ξεχωριστό αντικείμενο να έχει ένα συγκεκριμένο δικό του αριθμό. Όταν το αντικείμενο σαρώνεται προς πώληση και πληρώνεται, ο αριθμός της κάρτας RFID του συγκεκριμένου αντικειμένου, θα μπορούσε να συσχετιστεί με έναν αριθμό πιστωτικής .

10. Η διαμάχη για την ιδιωτικότητα

Η πιθανότητα μια επιχείρηση να χάσει τον έλεγχο της ιδιωτικότητας των πληροφοριών της, είναι ένας από τους μεγαλύτερους κινδύνους που σχετίζονται με το RFID. Όπως τα δίκτυα Ethernet, οι ασύρματες επικοινωνίες με κάρτες είναι επιρρεπείς σε υποκλοπές των δεδομένων. Με όλους τους τρόπους προστασίας, εκτός από τους πιο δυνατούς αλγόριθμους ασφάλειας δεδομένων, να είναι δυνατόν να καμφθούν από επιτυχείς επιθέσεις ωμής δύναμης (brute-force cracking), οι

δυνατότητες κρυπτογράφησης των καρτών είναι ένα από τα βασικά θέματα που πρέπει να λάβει υπόψιν μια επιχείρηση στην επιλογή της για ένα τέτοιο σύστημα.

Οι πληροφορίες σε ένα RFID tag είναι ευπαθείς σε μεταβολή, φθορά και διαγραφή. Το πρώτο ερώτημα που πρέπει να απαντηθεί είναι το κατά πόσο είναι τρωτά τα δεδομένα. Η ασφάλεια των καρτών μπορεί να εκφραστεί με όρους δύναμης της κρυπτογραφίας που χρησιμοποιείται, ταχύτητας επεξεργασίας της και του χρόνου που απαιτείται για να δημιουργηθεί δίαυλος επικοινωνίας με την κάρτα. Υποχωρήσεις στις τεχνικές ασφαλείας με σκοπό τη μείωση της πολυπλοκότητας και του κόστους των καρτών, αποφέρει tags των οποίων ο χρόνος που απαιτείται για να "σπάσουν" μετριέται μονάχα σε λεπτά.

Η ασφάλεια των πληροφοριών που ανταλλάσσονται μεταξύ καρτών και αναγνωστών, γίνεται προσπάθεια να ενδυναμωθεί για να ικανοποιήσει εμπορικές ανάγκες. Κάρτες που διαθέτουν ξεπεράσιμα εμπόδια για λόγους συμβιβασμού, αποτελούν ευκαιρίες υποκλοπής και τροποποίησης σημαντικών πληροφοριών. Σε ακραίες περιπτώσεις, τέτοιες τροποποιήσεις μπορεί να περιλαμβάνουν εσκεμμένο αναπρογραμματισμό των καρτών ώστε να εξυπηρετούν τους αντιπάλους της επιχείρησης. Τέτοιες εταιρίες που επιλέγουν ένα ασθενώς προστατευμένο σύστημα καρτών, δίνουν στους ανταγωνιστές τους μια χαμηλού κόστους ευκαιρία να μάθουν τα επαγγελματικά μυστικά τους.

11. Τύποι επιθέσεων

Είναι πολύ σημαντικό να προσδιοριστούν επακριβώς οι όροι "ασφάλεια" και "ιδιωτικότητα" στα πλαίσια του RFID. Σε αυτά τα πλαίσια, η ασφάλεια αναφέρεται σε ένα ή συνδυασμό των αντικειμενικών στόχων που θα αναπτυχθούν παρακάτω.

Είναι σημαντικό να σημειωθεί εδώ, ότι η ιδιωτικότητα είναι ένα πολυδιάστατο θέμα που περιλαμβάνει πολλούς τομείς, όπως οι πολιτικές ασφαλείας και οι υπηρεσίες επιβολής του νόμου. Ένα κριτήριο αξιολόγησης της ιδωτικότητας ενός συστήματος RFID, προϋποθέτει την παροχή

1. ανωνυμίας, και
2. μη συνδεσιμότητας

Ενώ η συγκεκριμένη τεχνολογία παρέχει πολυάριθμα οφέλη, τα διάφορα συστήματα που την εφαρμόζουν παράγουν νέους κινδύνους. Πρωταρχικά, η επικοινωνία μεταξύ των καρτών και των αναγνωστών είναι εκτεθειμένη σε υποκλοπή και ανάλυση κίνησης. Ως εκ τούτου, ένα τέτοιο σύστημα είναι υπό τη συνεχή απειλή επιθέσεων του διαμέσου (man in the middle), όπου ένα τρίτο μέρος μπορεί να ελέγχει τη "συνομιλία" ενός αναγνώστη με μια κάρτα για να αποκτήσει ευαίσθητες πληροφορίες. Τέτοιες παράνομα αποκτηθείσες πληροφορίες μπορεί να χρησιμοποιηθούν για να δημιουργηθούν πλαστές κάρτες, μη εξουσιοδοτημένοι αναγνώστες ή να ανακαλυφθούν μυστικά δεδομένα που βρίσκονται αποθηκευμένα στις κάρτες (όπως κάποιος κωδικός αυθεντικοποίησης). Προς το παρόν, δεν υπάρχει κανένας τρόπος για να αποδείξει την ταυτότητά της μια συσκευή ανάγνωσης σε μια κάρτα ή το αντίστροφο, με αποτέλεσμα κάρτες και αναγνώστες να βρίσκονται συνεχώς σε ένα αφερέγγυο περιβάλλον το οποίο υπολείπεται σε εμπιστευτικότητα, όπου η ακεραιότητα των μηνυμάτων είναι αμφίβολη και δεν υπάρχει κανένας τρόπος για να εγγυηθεί η ιδιότητα της μη-απάρνησης από οποιαδήποτε από τις δυο μεριές.

Επιπροσθέτως, οι ίδιες οι κάρτες είναι εκτεθειμένες σε φυσικές επιθέσεις. Πολύ απλά ένας αντίπαλος θα μπορούσε να κατασκευάσει με αντίστροφη διαδικασία μια πλαστή κάρτα για χρήση σε επιθέσεις εξαπάτησης (spoofing) ή πολλές κάρτες για επίθεση άρνησης υπηρεσίας (DoS – denial of service) πλήττοντας τη διαθεσιμότητα του συστήματος.

Οι κυριότερες επιθέσεις χωρίζονται σε τρεις κατηγορίες:

- Συλλογή (gather): Ξάφρισμα (skimming), υποκλοπή (eavesdropping), Παραποίηση δεδομένων (data tampering)
- Μίμηση (mimic): Εξαπάτηση (spoofing), Κλωνοποίηση (cloning), Κακόβουλος κώδικας (malicious code)
- Άρνηση υπηρεσίας (denial of service), Θανάτωση (killing), Παρεμβολή/ Απόκρυψη (jamming/shielding), Φραγή (Blocking)

- *Ξάφρισμα (skimming)* δεδομένων είναι η μη εξουσιοδοτημένη πρόσβαση για ανάγνωση των δεδομένων. Τα δεδομένα διαβάζονται απευθείας από την κάρτα χωρίς τη γνώση ή συγκατάθεση του ιδιοκτήτη της .

- *Υποκλοπή (eavesdropping)* ή "μύρισμα" (sniffing) – επίσης αποκαλείται και παθητικός ενδιάμεσος (passive man in the middle) αναγνώστης – είναι η μη εξουσιοδοτημένη ακοή/υποκλοπή, μέσω της χρήσης εξοπλισμού λήψης ραδιοσήματος, μιας εξουσιοδοτημένης μετάδοσης για τον έλεγχο ή την καταγραφή δεδομένων μεταξύ του αποστολέα και του παραλήπτη με σκοπό: τη συλλογή αυτούσιων μεταδόσεων για τον προσδιορισμό των πρωτοκόλλων επικοινωνίας ή/και της κρυπτογράφησης, τη συλλογή δεδομένων ή τον προσδιορισμό προτύπων κίνησης (traffic)

- Ως *κλωνοποίηση (cloning)* ορίζεται η πιστή αντιγραφή των δεδομένων μιας κάρτας σε μια άλλη. Δεδομένα που αποκτούνται από μια κάρτα, με οποιαδήποτε μέσα, γράφονται σε μια αντίστοιχη.

- *Παραποίηση δεδομένων (data tampering)* είναι η μη εξουσιοδοτημένη αλλαγή ή διαγραφή των δεδομένων για να καταστεί η κάρτα άχρηστη. Για παράδειγμα, η παραποίηση δεδομένων σε ένα κατάστημα θα μπορούσε να περιλαμβάνει την αλλαγή της τιμής ενός προϊόντος προς ζημία του ιδιοκτήτη.

- *Κακόβουλη εισαγωγή* εκτελέσιμου κώδικα/ιού (malicious code) για τη φθορά των συστημάτων μιας επιχείρησης, είναι υποθετικά πιθανή δεδομένης μιας κάρτας με επαρκή μνήμη και εμβέλεια.

- Η *θανάτωση* (killing) – φυσική ή μηχανική - μιας κάρτας είναι μια λειτουργική απειλή υπό την έννοια ότι η φυσική ή ηλεκτρονική καταστροφή της , στερεί τους χρήστες τις από τα δεδομένα της.

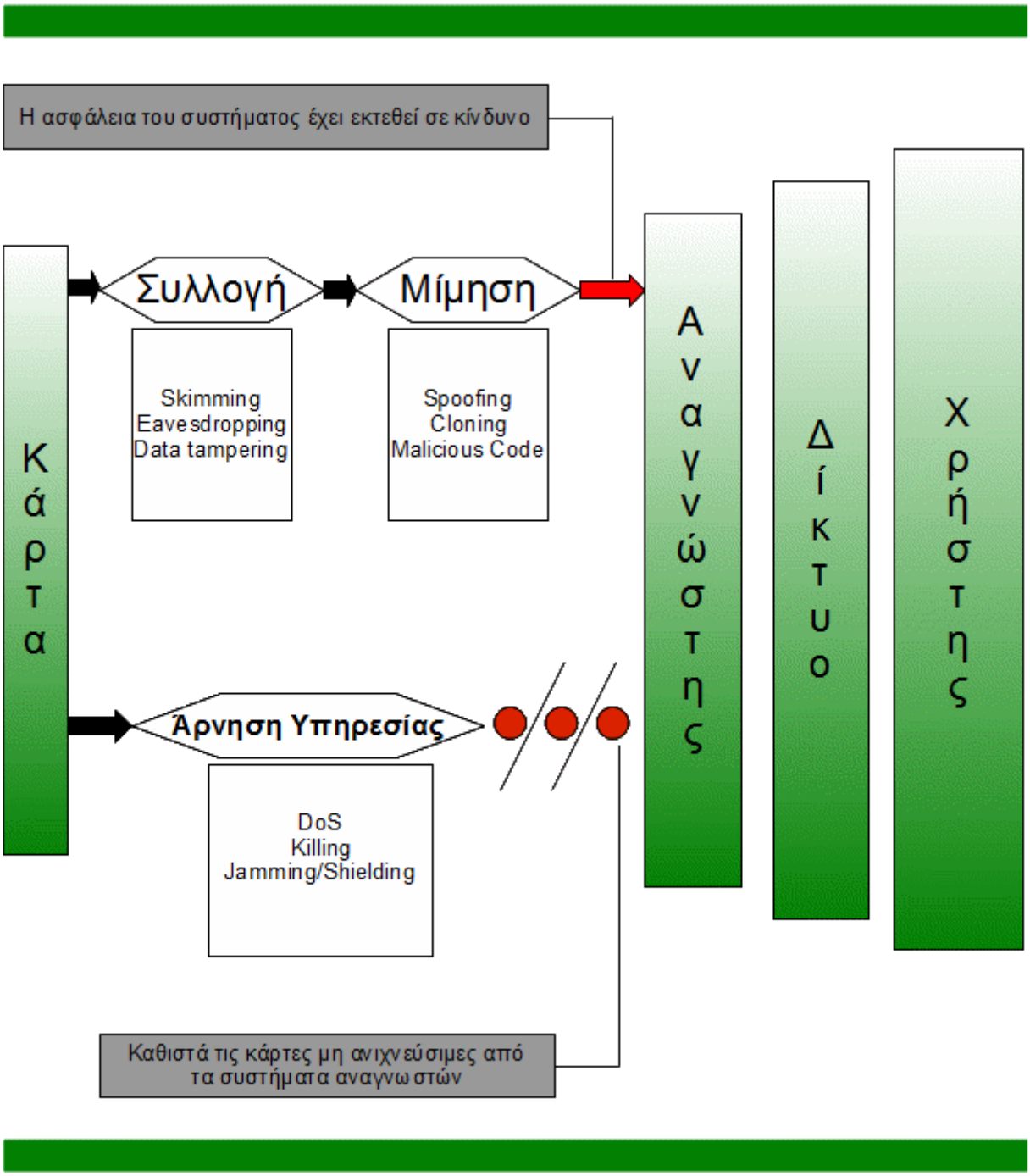
- *Παρεμβολή/Απόκρυψη (jamming/shielding)* είναι η χρήση μιας συσκευής για τη διακοπή της λειτουργίας του αναγνώστη. Απόκρυψη είναι η χρήση μηχανικών μέσων για την αποτροπή της ανάγνωσης μιας κάρτας.

- Ως *εξαπάτηση (spoofing)* ορίζεται η πιστή αντιγραφή των δεδομένων μιας κάρτας και η μετάδοσή τους σε έναν αναγνώστη. Δεδομένα που αποκτούνται από μια κάρτα, με οποιαδήποτε μέσα, μεταδίδονται σε έναν αναγνώστη για να μιμηθούν μια νόμιμη πηγή. Η συγκεκριμένη επίθεση αποτελεί σοβαρή απειλή για ένα σύστημα RFID και θα προσθέσει μια νέα διάσταση στην κλοπή. Ένας κλέφτης μπορεί να αντικαταστήσει ένα έγκυρο αντικείμενο με μια πλαστή κάρτα RFID ή την κάρτα ενός ακριβού αντικειμένου με μια πλαστή που περιέχει δεδομένα αποκτηθέντα από ένα πιο φθηνό αντικείμενο. Ως εκ τούτου, η έλλειψη κάποιου τρόπου αυθεντικοποίησης, επιτρέπει σε έναν αντίπαλο να ξεγελάσει ένα σύστημα ασφαλείας, ώστε αυτό να πιστεύει ότι ένα αντικείμενο είναι παρόν ή να ξεγελάσει αυτόματα συστήματα πληρωμών ώστε να χρεώνουν πιο φθηνά αντικείμενα. Πλαστές κάρτες μπορεί επίσης να χρησιμοποιηθούν για τη δημιουργία απομιμήσεων. Έτσι είναι σημαντικό να μπορούν να πιστοποιηθούν οι κάρτες για να αποδειχθεί η νομιμότητά τους.
- *Άρνηση υπηρεσίας (denial of service)* συμβαίνει όταν πολλαπλές ή ειδικά σχεδιασμένες κάρτες χρησιμοποιούνται για να κατακλύσουν την ικανότητα ενός αναγνώστη να ξεχωρίζει μεταξύ τους τις κάρτες, καθιστώντας έτσι το σύστημα μη λειτουργικό. Ένας αντίπαλος μπορεί να ξεκινήσει μια τέτοια επίθεση για να υπερπηδήσει ή να αποφύγει συστήματα ασφαλείας. Εκτελείται εύκολα τοποθετώντας ένα μεγάλο αριθμό καρτών για αναγνώριση από έναν αναγνώστη. Η εφαρμογή ενός συστήματος RFID μπορεί επίσης να διαταραχθεί με την καταστροφή μιας μεγάλης παρτίδας καρτών. Οι κάρτες είναι επίσης ευπαθείς σε επιθέσεις πρωτοκόλλου. Έτσι, μπορεί επανειλημμένα να τους ζητηθεί να εκτελέσουν μια εργασία, καθιστώντας τες μη διαθέσιμες σε έναν νόμιμο αναγνώστη. Οι κάρτες, είναι προφανές ότι, πρέπει να μπορούν αμυνθούν σε τέτοιες απλές επιθέσεις ωμής δύναμης καθώς εγείρονται ζητήματα διαθεσιμότητας των συστημάτων. Στο σχήμα 1 φαίνεται η κατηγοριοποίηση των κυριότερων τύπων επιθέσεων.

Υπάρχει επίσης μια ξεκάθαρη πιθανότητα, μη εξουσιοδοτημένοι “ανακριτές” να διαβάσουν μια απροστάτευτη RFID κάρτα εξαιτίας της έλλειψης κάποιου μηχανισμού πιστοποίησης. Τέτοιοι αναγνώστες μπορούν να χρησιμοποιηθούν για να παραβιάσουν την “ανωνυμία” ή την “απόκρυψη τοποθεσίας”, έχοντας πρόσβαση σε απροστάτευτες κάρτες.

Ζητήματα ιδιωτικότητας που προκύπτουν απ' το RFID, είναι επίσης εν μέρει ζητήματα πολιτικής, καθώς οι μηχανισμοί που χρησιμοποιούνται για να εξασφαλίσουν την ασφάλεια και την ιδιωτικότητα, είναι περισσότερο αποτελεσματικοί όταν συνδυάζονται με μια καλά σχηματισμένη πολιτική ασφαλείας.

Παρακάτω φαίνονται κάποια παραδείγματα μέσα από τα οποία παρουσιάζονται και κάποιοι άλλοι τύποι επιθέσεων.



Σχήμα 1. Κυριότεροι τύποι επιθέσεων

12. Μερικά τυπικά παραδείγματα επιθέσεων

Μία ολοκληρωμένη εικόνα για τη σημασία της ασφάλειας ενός συστήματος RFID μπορεί να δοθεί με την παρουσίαση διαφόρων παραδειγμάτων επίθεσης που είναι δυνατό να απειλήσουν ένα σύστημα. Ο επιτιθέμενος μπορεί να είναι οποιοσδήποτε θέλει να προσβάλει το σύστημα και να επωφεληθεί από αυτή του τη δράση. Μπορεί να είναι ανταγωνιστής, βιομηχανικός κατάσκοπος κ.ά., όπως επίσης υπάλληλος ή

πελάτης κάποιας επιχείρησης ή οργανισμού. Το κίνητρο που ωθεί σε αυτές τις επιθετικές ενέργειες διαφέρει κατά περίπτωση και δεν ενδιαφέρει την τεχνολογία RFID από πού προέρχεται.

(*Spying*) *:* Η κατασκοπία δεδομένων μπορεί να επιτευχθεί με τους πιο κάτω τρόπους δράσης *:*

- Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τον δικό του δέκτη για να υποκλέψει, δηλαδή να παρακολουθήσει μυστικά την ασύρματη επικοινωνία μεταξύ καρτών και αναγνωστών. Έτσι μπορεί να αποκτήσει πληροφορίες για τους τρόπους επικοινωνίας που χρησιμοποιούνται μεταξύ των συσκευών στο εκάστοτε περιβάλλον συστήματος.

- Ο επιτιθέμενος έχει τη δυνατότητα χρησιμοποιώντας τον δικό του αναγνώστη να διαβάσει δεδομένα από τις κάρτες. Η συσκευή αναγνώστη που χρησιμοποιείται μπορεί να εγκατασταθεί σε κάποιο κρυμμένο σημείο ή να δράσει ως κινητή μονάδα. Εάν ο αναγνώστης απαιτεί πιστοποίηση, τότε ο επιτιθέμενος πρέπει να έχει τη δυνατότητα να παραποιήσει την ταυτότητα (identity) του αναγνώστη ώστε να καταστεί επιτυχής η προσπάθεια.

(Deception) : Ο επιτιθέμενος τροφοδοτεί ψευδή δεδομένα έχοντας πρόθεση να παραπλανήσει. Αυτό γίνεται χρησιμοποιώντας τους πιο κάτω τρόπους δράσης *:*

- Μπορεί να αλλάξει τα περιεχόμενα μιας υπάρχουσας κάρτας αλλά όχι το σειριακό αριθμό ταυτοποίησης (ID). Αυτό μπορεί να καταστεί εφικτό μόνο όταν τα δεδομένα που συσχετίζονται με το ID είναι αποθηκευμένα στις κάρτες και όχι στο backend σύστημα (κορμού). Στις περισσότερες εφαρμογές, αυτού του τύπου η αποθήκευση δεν είναι απαραίτητη, με αποτέλεσμα η συγκεκριμένη μορφή επίθεσης να μη μπορεί να πραγματοποιηθεί.

- Αποσυνδέοντας την ετικέτα από το αντικείμενο στο οποίο είναι προσαρτημένη, έχει ως πρόθεση να αποκρύψει τις μετακινήσεις του αντικειμένου

από τον έλεγχο του αναγνώστη. Επίσης μπορεί να επιδιώκεται, με στόχο πάντα την εξαπάτηση, να παρουσιαστεί ένα άλλο αντικείμενο το οποίο να παριστάνει το αυθεντικό, στο οποίο και ήταν αρχικά προσαρτημένη η ετικέτα. Ωστόσο η χρησιμότητα της επίθεσης μειώνεται σημαντικά, αν λόγω των μηχανικών μέτρων προστασίας που εφαρμόζονται σε κάθε περίπτωση, η αποσύνδεση της κάρτας από το αντικείμενο οδηγεί σε καταστροφή του εν λόγω αντικειμένου.

(Cloning): Ο επιτιθέμενος εξομοιώνει ή κλωνοποιεί κάρτες για να εξαπατήσει τον αναγνώστη στο να αποδεχτεί την ταυτότητά τους

- Για να γίνει αυτό κατορθωτό, πρέπει να ανακαλύψει τουλάχιστον τους μοναδικούς σειριακούς αριθμούς ταυτοποίησης στους οποίους αντιστοιχούν οι κάρτες. Εάν τα πρωτόκολλα προστασίας το απαιτούν, πρέπει να βρει επίσης το ανάλογο κλειδί αποκρυπτογράφησης του κώδικα ή όποιο άλλου είδους συνθηματικό χρειάζεται ώστε η πλαστή ετικέτα να λειτουργεί όπως ακριβώς και οι αυθεντικές.

(*Denial of Service*) *:* Ο επιτιθέμενος επιδιώκει να προκαλέσει βλάβη στην ορθή λειτουργία του συστήματος *RFID* πράττοντας με τους πιο κάτω τρόπους *:*

- Οι κάρτες καταστρέφονται με χρησιμοποίηση μηχανικών ή χημικών μέσων. Μερικά τέτοια μέσα είναι το λύγισμα ή το στράβωμα της κάρτας, η άσκηση πίεσης, η ηλεκτρική φόρτιση, η χρήση οξέων. Αυτά καθώς και άλλα μέσα καταστρέφουν άμεσα τις κάρτες καθιστώντας τις ανίκανες να λειτουργήσουν.

- Οι κάρτες καταστρέφονται από την επίδραση ηλεκτρομαγνητικών πεδίων. Αυτό μπορεί καταρχήν να πραγματοποιηθεί από πομπούς που έχουν σχεδιαστεί ειδικά για αυτό το σκοπό, αλλά επίσης από τη δράση φούρνων μικροκυμάτων ή ισχυρών επαγωγικών ηλεκτρικών εκκενώσεων.
- Οι κάρτες τίθενται εκτός λειτουργίας με τη χρήση εντολών διαγραφής ή θανάτωσης (kill command) της κάρτας. Ο επιτιθέμενος εκμεταλλεύεται αυτές τις εντολές εκούσια για να προσβάλει το σύστημα. Απαραίτητη προϋπόθεση για μια

τέτοια ενέργεια είναι ο επιτιθέμενος να έχει την ικανότητα να προσποιηθεί την ταυτότητα μιας εξουσιοδοτημένης συσκευής ανάγνωσης ή εγγραφής. Μέσω αυτής της εξαπάτησης, είναι σε θέση να αχρηστεύσει τις κάρτες στις οποίες χρησιμοποιεί αυτές τις εντολές.

- Στην περίπτωση ενεργητικών καρτών μπορεί να αποφορτιστεί η μπαταρία με την οποία η κάθε ετικέτα είναι εφοδιασμένη. Αυτό μπορεί να επιτευχθεί με μια σειρά από ερωτήσεις προς την ετικέτα, αρκετά μεγάλη ούτως ώστε η συνεχής αναίτια χρησιμοποίηση της μπαταρίας εν τέλει να την αποφορτίσει. Η επίθεση αυτής της μορφής δεν είναι βέβαια αποτελεσματική στην περίπτωση παθητικών καρτών καθώς αυτές τροφοδοτούνται από το πεδίο που παρέχει ο αναγνώστης.

- Μία ετικέτα blocker προσομοιώνει την παρουσία ενός μεγάλου αριθμού καρτών που αντιλαμβάνεται ο αναγνώστης, με αποτέλεσμα να εμποδίζει τις πραγματικά προβλεπόμενες κάρτες από το να διαβαστούν από αυτόν. Αυτό το παράδειγμα επίθεσης αποτελεί άμεση εφαρμογή φραγής (Blocking), βασικού τύπου επίθεσης που χρησιμοποιείται για να προκαλέσει δυσλειτουργία στο σύστημα.

- Η επικοινωνία μεταξύ κάρτας και αναγνώστη μπορεί να εμποδιστεί με τη χρήση συσκευών που εκπέμπουν παράσιτα (Jamming devices). Για να είναι αποτελεσματική μια τέτοια παρεμβολή σε μεγάλες αποστάσεις, απαιτούνται συσκευές πολύ υψηλής έντασης. Η ανίχνευση τέτοιου είδους επίθεσης είναι πολύ εύκολο να γίνει.

- Η χρησιμοποίηση ανακλαστικών αντικειμένων είναι ικανή να εξουδετερώσει ένα ηλεκτρομαγνητικό πεδίο καθιστώντας έτσι αδύνατη την επικοινωνία και την ανταλλαγή δεδομένων στο σύστημα.

- Η χρησιμοποίηση κάποιων υλικών σε κοντινή απόσταση μπορεί να οδηγήσει

σε αποσυντονισμό της συχνότητας λειτουργίας του πεδίου. Αυτό το αποτέλεσμα προκύπτει με τη χρήση νερού, μετάλλου, σιδερίτη και άλλων υλικών.

- Η κάλυψη των καρτών από τα ηλεκτρομαγνητικά πεδία επιτυγχάνεται αν τοποθετηθούν πάνω στις κάρτες λεπτά μεταλλικά ελάσματα ή τσάντες που περιέχουν ραβδώσεις μετάλλου. Έτσι δεν είναι δυνατή η ασύρματη επικοινωνία με τους αναγνώστες, οδηγώντας σε δυσλειτουργία το σύστημα.

Η εκτέλεση στην πράξη των προαναφερθέντων παραδειγμάτων επίθεσης, δεν έχει αναλυθεί σε εκτεταμένο βαθμό καθώς η πείρα αντιμετώπισης τέτοιων καταστάσεων είναι πολύ μικρή. Ωστόσο, η θεωρητική έστω γνώση των προβλημάτων που μπορεί να παρουσιαστούν θέτει σε μεγαλύτερη ετοιμότητα την επιστημονική κοινότητα για να αντιμετωπίσει τις προκλήσεις στο μέλλον.

13. Αντικειμενικοί στόχοι του RFID

Τα συστήματα RFID πρέπει να χρησιμοποιούν μηχανισμούς για να επιτύχουν έναν ή και περισσότερους αντικειμενικούς στόχους ασφαλείας, όπως η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα, η αυθεντικοποίηση και ο έλεγχος πρόσβασης για να μετριάσουν τα διάφορα προβλήματα ασφαλείας.

- *Εμπιστευτικότητα*: Ο όρος "εμπιστευτικότητα" μπορεί να χρησιμοποιηθεί για να περιγράψει ένα μηχανισμό ο οποίος αποκρύπτει τις πληροφορίες από όλους εκτός από εκείνους που είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε αυτές. Οι πληροφορίες που ανταλλάσσονται μεταξύ μιας κάρτας και ενός αναγνώστη πρέπει να είναι εμπιστευτικές όταν ευαίσθητα δεδομένα, όπως μυστικά κλειδιά, μεταφέρονται ανάμεσα στις δυο συσκευές.

- *Ακεραιότητα:* Η παροχή της ακεραιότητας περιλαμβάνει μια μέθοδο με την οποία διαβεβαιώνεται ότι οι πληροφορίες δεν έχουν τροποποιηθεί με οποιαδήποτε μη εξουσιοδοτημένα ή άγνωστα μέσα. Η τροποποίηση στα πλαίσια του RFID μπορεί να

περιλαμβάνει την σύλληψη, αντικατάσταση, διαγραφή ή εισαγωγή πληροφοριών και την επανεκμπομή αυτών των τροποποιημένων πληροφοριών σε μια κάρτα ή ένα αναγνώστη. Η ακεραιότητα ενός RFID συστήματος έγκειται στην ακεραιότητα των συσκευών με την έννοια ότι αυτές δεν έχουν αλλαχθεί κακόβουλα. Ένας αναγνώστης που λαμβάνει δεδομένα από μια κάρτα, πρέπει να είναι σίγουρος ότι αυτά τα δεδομένα είναι σωστά, ενώ μια κάρτα πρέπει να είναι σε θέση να πιστεύει ότι τα δεδομένα που λαμβάνει από ένα κατά τα φαινόμενα αυθεντικό αναγνώστη, μπορεί να τα εμπιστευτεί. Η διασφάλιση της ακεραιότητας ενός συστήματος, είναι επίσης ένα σημαντικό βήμα για τη αποτροπή φυσικών επιθέσεων.

- *Διαθεσιμότητα:* Η διασφάλιση της διαθεσιμότητας στα RFID συστήματα είναι πολύ σημαντική εφόσον οι συσκευές ανάγνωσης πρέπει να είναι έτοιμες να εντοπίσουν κάρτες που μπορεί να εισέλθουν στην εμβέλειά τους σε συγκεκριμένα χρονικά διαστήματα. Στα πλαίσια του RFID, η διαθεσιμότητα στοχεύσει στην διαβεβαίωση ότι οι υπηρεσίες που παρέχονται από έναν αναγνώστη σε μια κάρτα και αντίστροφα είναι διαθέσιμες όταν αυτό απαιτείται. Συστήματα που εκπληρώνουν αυτό τον αντικειμενικό στόχο, θα μπορούν να εξασφαλίσουν ότι οι υπηρεσίες τους είναι σε θέση να αποτρέψουν μια επίθεση άρνησης υπηρεσίας.

- *Αυθεντικοποίηση*: Η αυθεντικοποίηση στα πλαίσια του RFID μπορεί να εκφραστεί ως η εξακρίβωση των συσκευών που συμμετέχουν στην επικοινωνία ή σε μια εφαρμογή όπου οι κάρτες τοποθετούνται σε προϊόντα, ως εξακρίβωση προϊόντων. Σε μερικές εφαρμογές, όπου η κάρτα πιθανώς θεωρείται ως αναπόσπαστο κομμάτι ενός αντικειμένου, η αυθεντικοποίηση της μπορεί να είναι επαρκής για να εγγυηθεί και η αυθεντικότητα του αντικειμένου με το οποίο αυτή συσχετίζεται. Όμως, σε άλλες εφαρμογές όπου η κάρτα τοποθετείται εξωτερικά σε κάποιο αντικείμενο μεγάλης αξίας, απλώς η εξακρίβωση της μπορεί να μην είναι επαρκής. Οι στόχοι της διαπίστευσης καρτών-αναγνωστών και προϊόντων αντίστοιχα είναι οι εξής:

- <u>Διαπίστευση καρτών-αναγνωστών:</u> Στα πλαίσια του RFID, η διαπίστευση αποδεικνύει τη διατεινόμενη ταυτότητα των συσκευών. Είναι ένα σημαντικό μέτρο

προστασίας για την αποτροπή της πλαστογραφίας. Επίσης, η εξακρίβωση μιας κάρτας είναι χρήσιμη για την αντιμετώπιση ευπαθειών που προκύπτουν ως αποτέλεσμα κλωνοποίησης.

- Διαπίστευση προϊόντων: Σε συγκεκριμένες περιπτώσεις η αυθεντικοποίηση της κάρτας δεν είναι επαρκής για να εγγυηθεί και την αυθεντικότητα του προϊόντος στο οποίο βρίσκεται προσκολλημένη. Αυτά τα προϊόντα είναι ευπαθή σε συγκεκριμένες επιθέσεις τύπου "αφαίρεσης και επανατοποθέτησης" (remove and reapply). Έτσι σε περιπτώσεις χρήσης καρτών σε προϊόντα, η διαπίστευση προϊόντων αναφέρεται στην εξακρίβωση της αυθεντικότητας τους, μέσω της ασφαλούς σύνδεσης της ταυτότητας της κάρτας και της νομιμότητάς των προϊόντων με ένα αδιάψευστο σύνδεσμο που μπορεί να επιβεβαιωθεί από κάποιον τρίτο.

- *Έλεγχος πρόσβασης:* Στην αλληλεπίδραση μεταξύ καρτών και αναγνωστών, η διαχείριση της πρόσβασης προϋποθέτει ένα μηχανισμό μέσω του οποίου οι συσκευές αποκτούν πρόσβαση ή αναιρούν το δικαίωμα πρόσβασης σε μερικά δεδομένα ή κάνουν κάποια λειτουργία. Γενικά οι κάρτες θα απαιτούν έλεγχο πρόσβασης, για να αποτρέπουν μη εξουσιοδοτημένη πρόσβαση στα δεδομένα τους.

Με τη χρήση συνδυασμών των ανωτέρω απειλών μπορούν να γίνουν πιο σοβαρές επιθέσεις συμπεριλαμβανομένου του ανεπιθύμητου εντοπισμού ατόμων ή αντικειμένων, τις κοινωνικές συναναστροφές κάποιου ή τις οικονομικές του συναλλαγές (με συσχετισμό των σαρώσεων μιας κάρτας από διάφορους αναγνώστες). Ακόμη και αν εφαρμοστεί κάποια τεχνική ασφαλείας στα δεδομένα της κάρτας, κάποιος μπορεί να εντοπιστεί μέσω ενός "αστερισμού" προβλεπόμενων απαντήσεων της κάρτας του. Πέρα από αυτές τις απειλές, οι κάρτες υποφέρουν από μια ποικιλία δεξιοτεχνικών επιθέσεων όπως επιθέσεις πλάγιου τρόπου, όπου κάποιος χρησιμοποιώντας χρονική, δυναμική και ηλεκτρομαγνητική ανάλυση μπορεί να εξάγει δεδομένα από την κάρτα.

14. Προκλήσεις στην ασφάλεια των συστημάτων RFID χαμηλού κόστους.

Υπάρχουν πολλές προκλήσεις στην παροχή ασφάλειας και προστασίας στα συστήματα RFID χαμηλού κόστους (πίνακας). Αυτές οι δυσκολίες είναι αποτέλεσμα της φύσης των ηλεκτρομαγνητικών κυμάτων και των περιορισμών που υφίστανται σε τέτοια συστήματα.

Πρόκληση	**Περιγραφή**
Κόστος	Περιορισμός αποθηκευτικού χώρου - Περιοχή πυριτίου.
Κανονισμοί	Εκπεμπόμενη ενέργεια, συχνότητα λειτουργίας, διαθέσιμο εύρος ζώνης
Κατανάλωση ενέργειας	Κατανάλωση ενέργειας του ολοκληρωμένου κυκλώματος της
Επιδόσεις	Στόχοι επιδόσεων και συστήματος
Διακοπές ενέργειας	Απότομη απώλεια ισχύος

Πίνακας 1. Γενική περιγραφή των προκλήσεων που αντιμετωπίζονται από RFID συστήματα χαμηλού κόστους

Η βασική πρόκληση έγκειται στους περιορισμένους πόρους ενός ολοκληρωμένου κυκλώματος RFID. Οι κάρτες χαμηλού κόστους δεν έχουν δική τους πηγή ενέργειας και αποτελούνται από μονάχα ένα κλάσμα των πυλών που είναι διαθέσιμες για τις έξυπνες κάρτες. Κρυπτογραφικά συστήματα και πρωτόκολλα πρέπει να χωρέσουν στο αποτύπωμα μιας κάρτας, χωρίς να αυξήσουν πολύ το κόστος της. Ο αριθμός των πυλών που είναι διαθέσιμος για ένα μηχανισμό ασφαλείας είναι στο εύρος 400 – 4000.

Οι μηχανισμοί και τα πρωτόκολλα ασφαλείας πρέπει να είναι προσεκτικά σχεδιασμένα ώστε να μην αφήνουν την κάρτα εκτεθειμένη κατά τη διάρκεια απότομης απώλειας ισχύος ή διακοπών στην επικοινωνία. Είναι επίσης σημαντικό για τους μηχανισμούς αυτούς να λάβουν υπόψιν το δυνατότερο σήμα κατά την επικοινωνία αναγνώστη-κάρτας, το οποίο μπορεί να ανιχνευθεί από εκατοντάδες μέτρα μακριά, σε σχέση με την ισχύ του σήματος στην αντίστροφη επικοινωνία, το οποίο μπορεί να εντοπισθεί από μια απόσταση όχι μεγαλύτερη από 20 μέτρα με τη χρήση ιδιαίτερα ευαίσθητων δεκτών.

15. Συχνότητες και κανονισμοί

Πολύ βασικό χαρακτηριστικό των συστημάτων RFID είναι η συχνότητα λειτουργίας τους. Όταν λέμε συχνότητα λειτουργίας, εννοούμε τη φέρουσα συχνότητα επικοινωνίας του αναγνώστη προς τον πομποδέκτη, η οποία μπορεί να συμπίπτει, αλλά όχι υποχρεωτικά, με τη συχνότητα της αντίστροφης επικοινωνίας. Οι ιδιότητες του ηλεκτρομαγνητικού πεδίου εξαρτώνται από τη φέρουσα συχνότητα και ως εκ τούτου και η απόδοση των συστημάτων RFID.

Η λειτουργία των συστημάτων RFID παγκοσμίως, συντονίζεται από τοπικά κυβερνητικά σώματα που ελέγχουν το ηλεκτρομαγνητικό φάσμα σε μια περιοχή. Η πλειοψηφία αυτών των συστημάτων λειτουργεί στις επονομαζόμενες Βιομηχανικές-Επιστημονικές-Ιατρικές (Industrial-Scientific-Medical ISM) ζώνες. Αυτές οι ζώνες είναι ελεύθερες για χρήση από συστήματα χαμηλής ισχύος και μικρής εμβέλειας και προσδιορίζονται από τη Διεθνή Ένωση Τηλεπικοινωνιών.

Επομένως, είναι σημαντικό να επιλεγεί η σωστή ζώνη συχνοτήτων για μια εφαρμογή. Μερικές σημαντικές παράμετροι που εξαρτώνται από τη συχνότητα είναι :

- *Ρυθμός μετάδοσης δεδομένων (data transmission rate)*

  Μια υψηλότερη φέρουσα συχνότητα μπορεί να επιτύχει έναν υψηλότερο ρυθμό μετάδοσης δεδομένων, χάρη στο μεγαλύτερο διαθέσιμο εύρος ζώνης. Έτσι, με έναν υψηλότερο ρυθμό μετάδοσης μπορεί να εφαρμοστεί και ένας πιο περίπλοκος αλγόριθμος επίλυσης συγκρούσεων κατά τη διάρκεια των προσπαθειών ανάγνωσης με αποτέλεσμα ο αναγνώστης να μπορεί να διαβάσει μεγαλύτερο αριθμό ετικετών.

- *Αντανάκλαση και παρεμβολή (reflections and interference)*

  Τα ανακλώμενα και μεταδιδόμενα ηλεκτρομαγνητικά κύματα δημιουργούν παρεμβολές, γεγονός που έχει μεγάλη επίπτωση για το RFID σύστημα απομακρυσμένου πεδίου που λειτουργεί στη UHF (300-3000 MHz) ή μικροκυματική (3-30 GHz) ζώνη. Η καταστρεπτική συμβολή των ανακλώμενων και μεταδιδόμενων κυμάτων οδηγεί σε σημεία με μηδενική ένταση του ηλεκτρομαγνητικού πεδίου, πράγμα το οποίο μπορεί να προκαλέσει σημαντικό

πρόβλημα αξιοπιστίας για το σύστημα RFID του απομακρυσμένου πεδίου. Η παρεμβολή αυτή δεν είναι τόσο προβληματική για την αξιόπιστη λειτουργία του RFID κοντινού πεδίου.

- *Απώλειες ρευμάτων στροβιλισμού (eddy current losses)*

Τέτοιες απώλειες στις αγώγιμες επιφάνειες είναι ανάλογες προς τη συχνότητα. Αυτό σημαίνει ότι η υποβάθμιση της απόδοσης ενός συστήματος RFID κοντά σε αντικείμενα από μέταλλο είναι σημαντικά μεγαλύτερη για τις συχνότητες UHF και μικροκυμάτων σε σύγκριση με τις συχνότητες LF και HF.

- *Απορρόφηση από κακούς αγωγούς (absorption by non-conductors)*

Οι κακοί αγωγοί με υψηλή διηλεκτρική σταθερά μπορούν να υποβαθμίσουν σημαντικά την απόδοση ενός συστήματος RFID που λειτουργεί στη UHF ή μικροκυματική ζώνη. Αντίθετα ασκούν μικρή επίδραση στη ζώνη χαμηλών συχνοτήτων. Επομένως οι LF ή HF ετικέτες προτιμώνται για εμφύτευση σε ανθρώπους ή ζώα.

Μία περίληψη των ζωνών RFID, χαρακτηριστικών συχνότητας, και των αντίστοιχων προτύπων είναι ταξινομημένα στον πίνακα 2.

Ζώνες συχνοτήτων	<135 KHz [LF]	13.56 MHz [HF]	860-960 MHz [UHF]	2.45 GHz [Μικροκύματα]
Αρμόδια Πρότυπα	-ISO 11784 & 11785 -ISO/IEC 18000-2 -ISO 14223-1	-ISO/IEC 18000-3 -EPC class-1 -ISO 15693 -ISO 14443 (A/B)	-ISO/IEC 18000-6 -EPC class-0,class-1	-ISO/IEC 18000-4
Τυπική εμβέλεια ανάγνωσης	< 0.5 m	~ 1 m	~ 4 – 5 m	~ 1 m
Τύπος ετικέτας	Παθητική επαγωγικής σύζευξης	Παθητική επαγωγικής σύζευξης	Παθητική ή ενεργητική	Παθητική ή ενεργητική
Τυπικές Εφαρμογές	Έλεγχος πρόσβασης, ετικέτες σε ζώα, ακινητοποιητής οχήματος (immobilizer)	Έξυπνες κάρτες, έλεγχος πρόσβασης, ταυτότητες πληρωμών, ετικέτες αντικειμένων, έλεγχος αποσκευών, βιομετρία, βιβλιοθήκες, μεταφορές, ενδυμασία	Παλέτες αλυσίδας προμηθειών και ετικέτες καβωτίων, χειρισμός αποσκευών, συλλογή ηλεκτρονικών διοδίων	Συλλογή ηλεκτρονικών διοδίων, διαχείριση αλυσίδας προμηθειών εξαρτώμενων από θερμοκρασία, παρακολούθηση περιβάλλοντος
Ρυθμός ανάγνωσης πολλαπλών ετικετών	Πιο αργός → Ταχύτερος			
Ικανότητα ανάγνωσης κοντά σε μεταλλικές ή υδάτινες επιφάνειες	Καλύτερα → Χειρότερα			
Μέγεθος παθητικής ετικέτας	Μεγαλύτερο → Μικρότερο			

Πίνακας 2. Ζώνες, χαρακτηριστικά συχνοτήτων, πρότυπα

Οι ετικέτες RFID και οι αναγνώστες εντάσσονται στις μικρής εμβέλειας συσκευές, οι οποίες κανονικά δεν χρειάζονται άδεια για τη λειτουργία τους. Εντούτοις, οι εκπομπές τους στις διάφορες συχνότητες διακατέχονται από κανονισμούς που ποικίλλουν από χώρα σε χώρα.

Οι κανονισμοί του ηλεκτρομαγνητικού πεδίου θέτουν περιορισμούς στην εκπεμπόμενη ενέργεια σε δεδομένες αποστάσεις. Αυτό υπονοεί ότι υπάρχει κάποιο ανώτατο όριο στη διαθέσιμη ενέργεια για μια συγκεκριμένη απόσταση κάρτας-αναγνώστη. Η διαθέσιμη σε μια κάρτα ενέργεια, είναι ένας παράγοντας που συμβάλλει στον προσδιορισμό του τύπου του σχεδίου ασφαλείας και του κρυπτογραφικού υλικού που χρησιμοποιείται σε αυτή. Τέτοιο υλικό, που καταναλώνει σεβαστά ποσά ενέργειας (στο εύρος δεκάδων μWatts), θα περιορίσει σημαντικά τις αποστάσεις ανάγνωσης της κάρτας και θα υποβαθμίσει την απόδοση ολόκληρου του συστήματος RFID.

Κάθε περιοχή έχει τη δική της ισχύ ακτινοβολίας και τους δικούς της κανονισμούς εύρους ζώνης. Οι κανονισμοί των UHF για τα άλματα μεταξύ συχνοτήτων καθορίζουν ένα μέγιστο χρονικό όριο για τη χρήση ενός καναλιού μιας συγκεκριμένης συχνότητας. Αυτός ο κανονισμός βάζει ένα σημαντικό περιορισμό στο χρόνο συναλλαγής μιας κάρτας, καθώς αυτή δε μπορεί να είναι σε συνεχόμενη λειτουργία κατά τη διάρκεια ενός άλματος μεταξύ συχνοτήτων.

Ο πίνακας του σχήματος 3 συνοψίζει ραδιο-κανονισμούς των αντιπροσωπευτικών χωρών και ηπείρων.

16. Συνοψίζοντας

Οι εφαρμογές του RFID είναι πολλές και προορίζονται για να βοηθήσουν τους ανθρώπους στην καθημερινή τους ζωή και όχι μόνο. Είναι εμφανές, όμως, ότι τα προβλήματα που αντιμετωπίζει αυτή η σχετικά νέα – για το ευρύ κοινό – τεχνολογία είναι πολλά και πολύπλοκα. Αυτό εξηγεί τη δυσκολία που αντιμετωπίζει στην αποδοχή της από το κοινό, το οποίο επιθυμεί τη λήψη και εφαρμογή μέτρων προστασίας των δικαιωμάτων του. Στο πεδίο αυτό πρέπει, επομένως, να ληφθούν υπόψη οι κοινωνικές, πολιτικές, δεοντολογικές και νομικές επιπτώσεις από τη διάδοση του RFID.

Για τον περιορισμό των επιβουλών εναντίον της ασφάλειας και της προστασίας της ιδιωτικής ζωής, απαιτείται διαρκής εγρήγορση αναφορικά με όλες τις επιπτώσεις του RFID. Ένας βασικός παράγοντας προς αυτή την κατεύθυνση είναι και η

ευαισθητοποίηση και πληροφόρηση του κοινού επί του θέματος.

1. Ζώνη χαμηλών συχνοτήτων LF (119 – 135) kHz			
Η.Π.Α/Καναδάς	**Ευρώπη**	**Ιαπωνία**	**Κίνα**
$2400/f\ (kHz)^{\mu V/m}$ @ 300m	119 – 127 kHz : 66 dBμA/m @ 10 m 127 – 135 kHz : 42 dBμA/m @ 10 m	30 V/m @ 3 m	$P_{peak} < 1W$
2. Ζώνη υψηλών συχνοτήτων HF (13.56 MHz)			
Η.Π.Α/Καναδάς	**Ευρώπη**	**Ιαπωνία**	**Κίνα**
13.553-13.567 MHz 42 dBμA/m @ 10 m	13.553-13.567 MHz 42 dBμA/m @ 10 m	13.553-13.567 MHz 42 dBμA/m @ 10 m	13.553-13.567 MHz 42 dBμA/m @ 10 m
3. Ζώνη πολύ υψηλών συχνοτήτων UHF (860 – 960) MHz			
Η.Π.Α/Καναδάς	**Ευρώπη***	**Ιαπωνία**	**Κίνα**
902 – 928 MHz $P_{e.i.r.p.}$** = 4 W	865.0 - 868.0 MHz $P_{e.r.p.} = +20dBm$ 865.6 – 868.0 MHz $P_{e.r.p.} = +27dBm$ 865.6 – 867.6 MHZ $P_{e.r.p.} = +33dBm$	952 – 955 MHz $P_{e.r.p.}$ = 1 W + κέρδος κεραίας 6dB = 4 W	840.5 – 844.5 MHz $P_{e.r.p.} = 2W$ 920.5 – 924.5 MHz $P_{e.r.p.} = 2W$
4. Ζώνη μικροκυμάτων (2.45 GHz)			
Η.Π.Α/Καναδάς	**Ευρώπη**	**Ιαπωνία**	**Κίνα**
2.400 – 2.483 GHz $P_{e.i.r.p.}$ = 4 W	2.446 – 2.454 GHz $P_{e.i.r.p.}$ = 500 mW ή 4W (εσωτερικός χώρος)	2.400–2.4835 GHz 3mW/MHz ($P_{e.i.r.p.}$ = 1 W)	2.400 – 2.425 GHz 250mW/m @ 3m ($P_{e.i.r.p.}$ =21mW)
*Listen before talk για κανάλια 200 kHz. **(e.i.r.p) = 1.64 × (e.r.p)			

Πίνακας 3. Κανονισμοί ραδιοσυχνοτήτων

ΑΝΑΦΟΡΕΣ

Βιβλιογραφία

- Whitepaper on “RFID Technology and its Use in the Supply Chain” http://www.printronix.com/library/assets/public/case-studies/rfid-laranwhite-paper-english.pdf
- P. Peris-Lopez et al., “RFID Systems: A Survey on Security Threats and Proposed Solutions,” Proc. Int’l. Conf. Pers. Wireless Commun., Sept. 2006.
- K. Finkelzeller, The RFID Handbook, 2nd edition., John Wiley & Sons, 2003.
- D. Henrici, “RFID Security and Privacy”, Springer-Verlag, 2008

Ιστοσελίδες

- http://en.wikipedia.org/wiki/RFID
- “RFID Journal ”, http://www.rfidjournal.com/
- http://www.rfidconsultation.eu/
- http://www.rsa.com/rsalabs
- http://www.rfidnews.org
- http://www.rfidgazette.org
- http://www.itsc.org.sg
- http://www.technovelgy.com
- http://www.autoidlabs.org

ΚΕΦΑΛΑΙΟ 4

ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ RFID

1. Εισαγωγή στα μέτρα προστασίας των συστημάτων RFID

Η συνεχής ανάπτυξη και η αυξανόμενη συμμετοχή της τεχνολογίας RFID σε όλο και περισσότερες δραστηριότητες που λαμβάνουν χώρα στο σημερινό κόσμο, αυξάνει παράλληλα τους κινδύνους τους οποίους η τεχνολογία καλείται να αντιμετωπίσει. Οι κίνδυνοι αυτοί, οι οποίοι έχουν ήδη παρουσιαστεί αναλυτικά, απειλούν σε διάφορα επίπεδα την ασφάλεια των συστημάτων RFID και τα προσωπικά δεδομένα ατόμων που χρησιμοποιούν εφαρμογές RFID ή εμπλέκονται με αυτές με κάποιο τρόπο. Για την αποτελεσματική αντιμετώπιση αυτών των κινδύνων απαιτείται κατάλληλος χειρισμός των διαθέσιμων μέτρων προστασίας, ούτως ώστε να μετριαστούν όσο το δυνατό περισσότερο οι συνέπειες που αυτοί προκαλούν ανά περίπτωση.

Κάθε συγκεκριμένος τύπος εφαρμογής που υλοποιείται με τη χρησιμοποίηση τεχνολογίας RFID έχει ιδιαίτερα χαρακτηριστικά, αφού χρησιμοποιεί ένα συνδυασμό διαφορετικών συνιστωσών και έχει να αντιμετωπίσει ένα διαφορετικό σύνολο κινδύνων. Για να καταστεί δυνατή η καταλληλότερη επιλογή μέτρων προστασίας που είναι απαραίτητα για τον κάθε τύπο εφαρμογής, πρέπει να ληφθούν υπόψη όλοι οι σχετικοί παράγοντες που τον επηρεάζουν στην εκάστοτε περίπτωση.
Οι παράγοντες που πρέπει να μελετηθούν είναι οι εξής [1] :

- *Ο γενικός αντικειμενικός σκοπός που εξυπηρετεί η λειτουργία του συστήματος RFID*. Ο σκοπός αυτός είναι, για παράδειγμα, το σύστημα να πρέπει να προσδιορίσει τη θέση ή την παρουσία ενός αντικειμένου, να πιστοποιήσει ένα άτομο, να διεκπεραιώσει μία οικονομική συναλλαγή ή να επιβεβαιώσει ότι ένα προκαθορισμένο σύνολο τεμαχίων δεν έχουν διασκορπιστεί.

- *Η φύση της πληροφορίας που το σύστημα παράγει ή επεξεργάζεται*. Μία εφαρμογή μπορεί μόνο να απαιτεί ένα μοναδικό στατικό αριθμό ταυτοποίησης σε κάθε κάρτα, ενώ μία άλλη εφαρμογή μπορεί να απαιτεί την αποθήκευση επιπρόσθετων πληροφοριών σε κάθε κάρτα μέσα στο χρόνο. Σημαντικό παράγοντα αποτελεί επίσης η ευαισθησία της πληροφορίας.

- *Τα φυσικά και τεχνητά χαρακτηριστικά του περιβάλλοντος* στο οποίο διεξάγονται οι λειτουργίες του συστήματος RFID κατά την διάρκεια που αυτές εκτελούνται. Μεταξύ άλλων περιλαμβάνονται η απόσταση ανάμεσα σε κάρτες και αναγνώστες, καθώς και το χρονικό περιθώριο στο οποίο κάθε λειτουργία πρέπει να εκτελεστεί.

- *Το φυσικό και τεχνητό περιβάλλον* που διαμορφώνεται πριν και μετά τη διεξαγωγή των λειτουργιών του συστήματος. Για παράδειγμα, η ακεραιότητα των καρτών κατά την αποθήκευση ή τη μεταφορά των αντίστοιχων αντικειμένων μπορεί να κινδυνεύσει από απειλές που προέρχονται από ανθρώπινο παράγοντα ή λόγω του περιβάλλοντος. Σε μερικές εφαρμογές που χρησιμοποιούν κάρτες ως αισθητήρες ανίχνευσης για την παρακολούθηση περιβαλλοντικών συνθηκών όπως θερμοκρασία και υγρασία, πρέπει να ληφθεί υπόψη η αντίστοιχη κατάσταση του περιβάλλοντος στο οποίο θα υλοποιηθεί μια τέτοιου είδους εφαρμογή.

2. Έλεγχοι για την προστασία συστημάτων RFID

Όπως γίνεται κατανοητό απ' τα προηγούμενα, οι υλοποιήσεις με RFID προσαρμόζονται ανάλογα με τις ανάγκες που παρουσιάζει ο κάθε τύπος εφαρμογής, με αποτέλεσμα οι διαθέσιμοι τρόποι προστασίας των συστημάτων να μην είναι εφαρμόσιμοι ή αποτελεσματικοί για όλες τις εφαρμογές RFID. Έτσι, σε κάθε ξεχωριστή περίπτωση απαιτείται η σωστή εκτίμηση των κινδύνων που ενδέχεται να παρουσιαστούν, ούτως ώστε να γίνει η καταλληλότερη επιλογή ενός συνδυασμού

μέτρων προστασίας. Σε αυτή την επιλογή, πέρα από τους παράγοντες που παρουσιάστηκαν προηγουμένως, πρέπει να ληφθούν υπόψη οι ρυθμίσεις που απαιτείται να γίνουν, το μέγεθος της κάθε απειλής για το σύστημα καθώς και οι επιπτώσεις στην αποδοτικότητα του συστήματος αλλά και το κόστος που θα έχει η εφαρμογή αυτών των μέτρων προστασίας.

Οι διαθέσιμοι τρόποι ελέγχου που χρησιμοποιούνται για την προστασία των συστημάτων RFID, χωρίζονται σε τρεις ομάδες [1]:

Διαχειριστικοί Έλεγχοι : Ένας διαχειριστικός έλεγχος συνδέεται με την γενική εποπτεία των διαφόρων μέτρων προστασίας του συστήματος RFID.

Λειτουργικοί Έλεγχοι : Ένας λειτουργικός έλεγχος εμπλέκει τις ενέργειες που εκτελούνται σε καθημερινή βάση από τους διαχειριστές και τους χρήστες του συστήματος.

Τεχνικοί Έλεγχοι : Ένας τεχνικός έλεγχος χρησιμοποιεί την τεχνολογία για να παρακολουθήσει, να ελέγξει ή να περιορίσει τις εχθρικές ενέργειες που μπορεί να παρουσιαστούν εντός του συστήματος.

Στα επόμενα παρουσιάζεται αναλυτικά η κάθε ομάδα ελέγχων ξεχωριστά. Για κάθε έλεγχο δίνεται μία αντίστοιχη περιγραφή και πώς αυτή λειτουργεί, οι τύποι των υλοποιήσεων ή εφαρμογών στους οποίους μπορεί να είναι χρήσιμη, τα πλεονεκτήματα που προσφέρει και τα μειονεκτήματα που παρουσιάζει.

2.1 Διαχειριστικοί Έλεγχοι

Οι διαχειριστικοί έλεγχοι συνδέονται τυπικά με την εκτίμηση κινδύνων, την απόκτηση και οργάνωση του κατάλληλου συστήματος, όπως επίσης με πιστοποιήσεις, επικυρώσεις και αποτιμήσεις ασφαλείας. Ακολουθεί μία λεπτομερής

παρουσίαση των ελέγχων αυτού του είδους που σχετίζονται με τα συστήματα RFID.

❿ Σύμβαση χρήσης για την ασφάλεια συστήματος RFID

Περιγραφή Ελέγχου : Μία τέτοια σύμβαση καθορίζει τις εξουσιοδοτημένες και μη εξουσιοδοτημένες χρήσεις της τεχνολογίας RFID μέσα σε ένα οργανισμό και τους ρόλους που ανατίθενται στο προσωπικό για την εκτέλεση ειδικών αποστολών που πρέπει να επιτελέσει το σύστημα RFID.

Η σύμβαση πρέπει να είναι σύμφωνη ή να ενσωματωθεί με τη σύμβαση διασφάλισης προσωπικών δεδομένων του οργανισμού, η οποία ασχολείται με τον τρόπο που αυτά τα δεδομένα αποθηκεύονται και διανέμονται. Επίσης πρέπει να διευθύνει παρόμοια θέματα προστασίας ιδιωτικής ζωής σχετιζόμενα με τον τρόπο ταυτοποίησης των καρτών και με την πιθανή αποκάλυψη πληροφοριών.

Εφαρμοσιμότητα Ελέγχου : Ο έλεγχος είναι κατάλληλος για όλους τους οργανισμούς που χρησιμοποιούν τεχνολογία RFID.

Πλεονεκτήματα : Η σύμβαση εγκαθιστά ένα πλαίσιο εργασίας για πολλούς άλλους ελέγχους που αφορούν την ασφάλεια των συστημάτων. Αποτελεί ένα μέσο που χρησιμοποιεί η διοίκηση για να εκπληρώσει τις προσδοκίες της σχετικά με την προστασία του συστήματος RFID. Μέσω αυτού, η διοίκηση έχει τη δυνατότητα να κινηθεί νομικά ή να εφαρμόσει πειθαρχικά μέτρα έναντι σε οποιονδήποτε δεν συμμορφώνεται με τη σύμβαση.

Μειονεκτήματα : Η ύπαρξη της σύμβασης δεν εξασφαλίζει τη συμμόρφωση με αυτή. Για να γίνει αποτελεσματική πρέπει να συνδυαστεί με την υλοποίηση και επιβολή κατάλληλων λειτουργικών και τεχνικών ελέγχων.

❿ Συμβάσεις προστασίας που αφορούν την τεχνολογία της πληροφορίας

Περιγραφή Ελέγχου : Οι συμβάσεις αυτές περιγράφουν την προσέγγιση που

απαιτείται για να επιτευχθούν σε υψηλό επίπεδο οι αντικειμενικοί στόχοι για την ασφάλεια, οι οποίοι επιδιώκονται από τη σύμβαση χρήσης. Οι σχετιζόμενες με την τεχνολογία RFID συμβάσεις αυτού του είδους πρέπει να καλύπτουν κάθε υποσύστημα RFID, δηλαδή όλα τα μέρη του backend, και να μην περιορίζονται μόνο στην προστασία των καρτών και αναγνωστών μέσα στο υποσύστημα της ραδιοεπικοινωνίας.

Οι συμβάσεις προστασίας IT που αφορούν συστήματα RFID πρέπει να κατευθύνουν :

- Τον έλεγχο πρόσβασης σε πληροφορίες, ιδιαίτερα σε αρχεία που περιέχονται σε οργανωμένες αναλυτικές βάσεις δεδομένων.
- Την περιμετρική προστασία των υποσυστημάτων με τον καθορισμό κατάλληλων περιορισμών στη χρήση θυρών και πρωτοκόλλων για την δικτυακή επικοινωνία μεταξύ τους. Η επικοινωνία αυτή μπορεί να είναι μεταξύ του υποσυστήματος ραδιοεπικοινωνίας και των άλλων υποσυστημάτων ή ανάμεσα σε ένα δημόσιο δίκτυο και το backend σύστημα.
- Την διαχείριση των κωδικών ασφαλείας, ιδιαιτέρως αυτών που αφορούν την παραγωγή, διανομή και αποθήκευση καρτών.
- Την διαχείριση του συστήματος προστασίας για αναγνώστες και middleware.
- Την εκπαίδευση σε θέματα προστασίας RFID των διαχειριστών και χειριστών των συστημάτων.
- Την διαχείριση συνεργαζόμενων συστημάτων κρυπτογράφησης στα οποία περιλαμβάνονται πιστοποιήσεις αυθεντικότητας και διαχείριση κλειδιών για κώδικες κρυπτογράφησης και αποκρυπτογράφησης.

Εφαρμοσιμότητα Ελέγχου : Όλες οι υλοποιήσεις RFID και ιδιαιτέρως αυτές που έχουν τα διάφορα υποσυστήματα backend.

Πλεονεκτήματα : Οι συμβάσεις ορίζουν τις απαιτήσεις και παρέχουν τις κατευθυντήριες γραμμές που πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό, την υλοποίηση, τη χρήση και τη συντήρηση ενός συστήματος RFID. Με τη βοήθεια των

συμβάσεων, οι εκάστοτε ιθύνοντες του κάθε τομέα είναι σε θέση να πάρουν τις κατάλληλες αποφάσεις, ώστε να διασφαλιστεί η εύρυθμη και ορθή λειτουργία του συστήματος και η σωστή αντιμετώπιση των κινδύνων που παραμονεύουν.

Μειονεκτήματα : Η ύπαρξη της σύμβασης δεν εξασφαλίζει τη συμμόρφωση με αυτή. Για να γίνει αποτελεσματική πρέπει να συνδυαστεί με την υλοποίηση και επιβολή κατάλληλων λειτουργικών και τεχνικών ελέγχων.

⑩ Συμφωνίες μεταξύ οργανισμών

Περιγραφή Ελέγχου : Όταν τα δεδομένα που αφορούν ένα σύστημα RFID πρέπει να μοιράζονται μεταξύ οργανισμών, τότε μπορούν να υπάρξουν μεθοδικές συμφωνίες ανάμεσα στα συμμετέχοντα μέρη, ούτως ώστε με αυτές να τυποποιηθούν οι ρόλοι και οι ευθύνες που θα έχει το καθένα από τα μέρη αυτά. Αυτές οι συμφωνίες είναι δυνατό να τεκμηριώνονται με επίσημα μνημόνια τα οποία θα υπαγορεύουν τις υποχρεώσεις των συμμετεχόντων που τα προσυπογράφουν και θα καθορίζουν με λεπτομέρεια τους μηχανισμούς προστασίας των δεδομένων σε όλα τα επίπεδα όπου απαιτείται. Ακόμα, τέτοιες συμφωνίες μπορούν να επεκταθούν και για τον έλεγχο όσων άλλων έχουν πρόσβαση στο σύστημα.

Εφαρμοσιμότητα Ελέγχου : Κάθε σύστημα RFID που εμπλέκει περισσότερους από ένα οργανισμούς. Η πιο κοινή εφαρμογή γίνεται στις αλυσίδες προμηθειών.

Πλεονεκτήματα : Οι συμφωνίες αυτές περιορίζουν σημαντικά το ενδεχόμενο διαδοχικών παρεξηγήσεων και παραβιάσεων των κανόνων ασφαλείας. Με αυτές, οι συνυπογράφοντες μπορούν να κοινοποιούν ο ένας στον άλλο τις αντίστοιχες απαιτήσεις ασφαλείας που χρειάζονται και να συνεργάζονται για την σωστή αξιοποίηση και χρήση του συστήματος RFID.

Μειονεκτήματα : Η εφαρμογή της συμφωνίας από ένα οργανισμό είναι δύσκολο να

ελεγχθεί εφόσον δεν υπάρχει η δυνατότητα για πλήρη πρόσβαση στα συστήματα και στο προσωπικό του, με αποτέλεσμα οι όποιες παραβιάσεις της συμφωνίας μπορεί να συμβούν, να μην γίνουν αντιληπτές. Το μειονέκτημα αυτό μπορεί να μετριαστεί αν οι συμμετέχοντες στη συμφωνία αναθέσουν σε κάποιους ανεξάρτητους φορείς να εξετάζουν και να ελέγχουν το κατά πόσο η συμφωνία εφαρμόζεται σωστά από όλους τους εμπλεκόμενους.

❿ Ελαχιστοποίηση ευαίσθητων δεδομένων στις κάρτες

Περιγραφή Ελέγχου : Για την προστασία των ευαίσθητων δεδομένων, αντί της αποθήκευσής τους στις κάρτες, αυτά μπορούν να αποθηκευτούν σε ένα ασφαλές υποσύστημα στο backend και να ανακτώνται από εκεί μέσω του μοναδικού αριθμού ταυτοποίησης (ID) των καρτών.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλη λύση για εφαρμογές που χρησιμοποιούν κάρτες εφοδιασμένες με δική τους μνήμη στην οποία μπορούν να αποθηκευτούν ευαίσθητα δεδομένα.

Πλεονεκτήματα : Αντιμετωπίζονται οι εχθρικές επιθέσεις για αποκόμιση πληροφοριών μέσω υποκλοπής (eavesdropping) και σάρωσης από μη εξουσιοδοτημένους αναγνώστες στην ασύρματη επικοινωνία. Επίσης, η κρυπτογράφηση δεδομένων και ο έλεγχος πρόσβασης γίνονται πιο οικονομικά στο backend σε σχέση με το υποσύστημα ραδιοεπικοινωνίας (RF).

Μειονεκτήματα : Οι επιτιθέμενοι μπορούν συχνά να αποκομίσουν πολύτιμες πληροφορίες από τη γνώση και μόνο του ID της κάρτας. Επίσης, η αποθήκευση δεδομένων στο backend τα κάνει πιθανώς διαθέσιμα προς όλο το δίκτυο, ενώ η ανάκτησή τους από το αυτό συνεπάγεται μία μικρή χρονική καθυστέρηση που σε μερικές εφαρμογές είναι ανεπιθύμητη.

2.2 Λειτουργικοί Έλεγχοι

Υπάρχουν διάφοροι τύποι λειτουργικών ελέγχων οι οποίοι χρησιμοποιούνται για την προστασία των συστημάτων RFID. Ακολουθεί μία σύντομη αναφορά σε αυτούς και στη συνέχεια μία αναλυτική παρουσίαση όλων των λειτουργικών ελέγχων που είναι διαθέσιμοι.

Στα είδη λειτουργικών ελέγχων περιλαμβάνονται :

- *Οι φυσικοί έλεγχοι πρόσβασης* που περιορίζουν την είσοδο στους χώρους όπου είναι εγκατεστημένα συστήματα RFID, μόνο σε εξουσιοδοτημένο προσωπικό.
- *Η κατάλληλη τοποθέτηση του εξοπλισμού ραδιοεπικοινωνίας* για την αποφυγή παρεμβολών και τη μείωση κινδύνων που δημιουργούνται λόγω της ηλεκτρομαγνητικής ακτινοβολίας.
- *Η καταστροφή καρτών* όταν δεν είναι πλέον χρήσιμες, ώστε να εμποδιστεί η πρόσβαση σε πληροφορίες από πιθανούς εχθρούς.
- *Η κατάλληλη εκπαίδευση του προσωπικού* που χρησιμοποιεί το σύστημα μπορεί να εξασφαλίσει την ορθή εφαρμογή των κατευθυντήριων γραμμών και συμβάσεων που έχουν τεθεί.
- *Οι πληροφοριακές επιγραφές και προειδοποιήσεις* μπορούν να ενημερώσουν τους χρήστες για τους προτεινόμενους στόχους που εξυπηρετεί το σύστημα RFID και για απλές μεθόδους προστασίας από ενδεχόμενους κινδύνους.

❿ Φυσικός έλεγχος πρόσβασης

Περιγραφή Ελέγχου : Για να αποφευχθεί η φυσική πρόσβαση σε χώρους όπου έχουν αναπτυχθεί συστήματα RFID από μη εξουσιοδοτημένα άτομα, χρησιμοποιούνται έλεγχοι όπως φράχτες, ειδικές πύλες, τοίχοι, κλειδωμένες πόρτες, περιστροφικές θύρες, κάμερες παρακολούθησης και φρουροί ασφαλείας. Επίσης, όταν ο στόχος είναι να περιοριστεί η ασύρματη επικοινωνία σε μικρές αποστάσεις τότε η χρησιμοποίηση κλειστών δωματίων ή χωρισμάτων μπλοκαρίσματος είναι ικανή να παρέχει επαρκή προστασία εάν δεν επηρεάζουν τις ραδιοσυχνότητες που χρησιμοποιούνται για τη ραδιοεπικοινωνία.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλο για όλες τις υλοποιήσεις RFID εκτός από αυτές στις οποίες οι κάρτες ή άλλα στοιχεία του συστήματος RFID βρίσκονται σε δημόσιο χώρο.

Πλεονεκτήματα : Οι φυσικοί έλεγχοι πρόσβασης περιορίζουν τη δυνατότητα σε κάποιο εχθρό να πλησιάσει αρκετά κοντά σε στοιχεία ενός συστήματος RFID. Με αυτό τον τρόπο ο εχθρός δεν μπορεί να εκθέσει την ασφάλεια του συστήματος με παραποίηση, καταστροφή και κλοπή στοιχείων και δεδομένων του συστήματος.
Μερικά απτά παραδείγματα κινδύνων που περιορίζονται με τη χρήση αυτών των μέτρων προστασίας είναι τα πιο κάτω :

- Μη εξουσιοδοτημένη ανάγνωση και εγγραφή σε δεδομένα καρτών.
- Παραποιημένες και κλώνοι κάρτες.
- Εξαπάτηση αναγνωστών.
- Δυσλειτουργίες (Denial of Service) που προέρχονται από παρεμβολές στη ραδιοεπικοινωνία και μη εξουσιοδοτημένες εντολές στο σύστημα.
- Φυσική καταστροφή εξοπλισμού RFID.
- Κίνδυνοι που οφείλονται στην ηλεκτρομαγνητική ακτινοβολία.

Μειονεκτήματα : Οι έλεγχοι παρουσιάζουν αδυναμίες αφού :

- Δεν μπορούν να αντιμετωπίσουν παρεμβολές στην ραδιοεπικοινωνία που προέρχονται από νόμιμες εκπομπές σήματος εντός της περιμέτρου, αφού αυτή έχει σχεδιαστεί για να αποφευχθούν οι παρεμβολές από τον έξω χώρο.
- Η ακτίνα δράσης των ραδιοσημάτων στοχευμένων επιθέσεων, ίσως να είναι πολύ μεγαλύτερη από αυτή που έχει υπολογιστεί αν χρησιμοποιηθούν κατευθυντικές κεραίες ή άλλες τεχνολογίες για αυτό το σκοπό.
- Δεν υπάρχει προστασία σε εσωτερικές επιθέσεις, όπως αυτές που μπορεί να υπάρξουν από άτομα στα οποία έχει παραχωρηθεί άδεια πρόσβασης στον

προστατευμένο χώρο.

- Μέσα στη φυσική περίμετρο εξακολουθούν να υπάρχουν κίνδυνοι που οφείλονται στην εκπομπή ηλεκτρομαγνητικής ακτινοβολίας.
- Ο περιορισμός ανεπιθύμητων ραδιοσημάτων μπορεί να αποτύχει λόγω διαφόρων μορφών ανοιγμάτων που θα επιτρέπουν στα ραδιοσήματα να διαφύγουν.

⑩ Κατάλληλη τοποθέτηση καρτών και αναγνωστών

Περιγραφή Ελέγχου : Ο εξοπλισμός του συστήματος RFID τοποθετείται με κατάλληλο τρόπο ώστε να ελαχιστοποιούνται οι συνέπειες που προκαλούνται από την ηλεκτρομαγνητική ακτινοβολία.

Οι κάρτες και αναγνώστες πρέπει να κρατηθούν μακριά από :

- Καύσιμα, πολεμικά εφόδια και άλλα υλικά τα οποία μπορεί να αναφλεγούν, προκαλώντας ατυχήματα αν εκτεθούν σε ηλεκτρομαγνητική ακτινοβολία.
- Ανθρώπους και ευαίσθητα προϊόντα (φάρμακα κ.ά.) που μπορεί να υποστούν βλάβες υπό παρατεταμένη έκθεση σε ακτινοβολία, που οφείλεται στην ασύρματη επικοινωνία του συστήματος RFID.
- Μεταλλικά και ανακλαστικά αντικείμενα τα οποία μεταβάλλουν ή ενισχύουν τα μεταδιδόμενα σήματα με ανεπιθύμητο ή πιθανώς βλαβερό τρόπο.
- Άλλες νόμιμες ραδιοεκπομπές οι οποίες παρεμβάλλονται με τις RFID επικοινωνίες.

Εφαρμοσιμότητα Ελέγχου : Σε όλα τα περιβάλλοντα στα οποία υπάρχει η δυνατότητα καθορισμού της θέσης εγκατάστασης του εξοπλισμού. Από αυτά αποκλείονται πολλές εφαρμογές κατανάλωσης και αλυσίδας προμηθειών.

Πλεονεκτήματα : Η σωστή τοποθέτηση του εξοπλισμού ελαττώνει :

- Τον κίνδυνο παρεμβολών από νόμιμη εκπομπή σήματος.
- Τον κίνδυνο υποκλοπής (eavesdropping) και μη εξουσιοδοτημένης πρόσβασης μέσω της ασύρματης επικοινωνίας του συστήματος.

- Τις πηγές κινδύνου που οφείλονται στην ηλεκτρομαγνητική ακτινοβολία.

Μειονεκτήματα : Αδυναμίες παρατηρούνται στις πιο κάτω περιπτώσεις :

- Η θέση των καρτών δεν μπορεί να ελέγχεται πάντα, όπως όταν οι κάρτες αφορούν κινητά αντικείμενα ή αντικείμενα που είναι υπό συχνή μεταφορά.
- Η τοποθέτηση σε νέο σημείο, καρτών ή αναγνωστών για την αποφυγή παρεμβολών δεν εξασφαλίζει απαραιτήτως ότι αυτό θα επιτευχθεί αφού και στο καινούριο σημείο πιθανόν να υφίστανται άλλες ραδιοεπικοινωνίες.

⑩ Ασφαλής εξουδετέρωση καρτών

Περιγραφή Ελέγχου : Η ασφαλής εξουδετέρωση των καρτών συνεπάγεται την καταστροφή τους με φυσικά ή ηλεκτρονικά μέσα και όχι απλά την απόρριψή τους. Αυτό συμβαίνει όταν οι κάρτες δεν χρειάζεται πλέον να εκτελούν τις λειτουργίες για τις οποίες προορίζονταν. Η φυσική καταστροφή μπορεί να γίνει με χειροκίνητο σκίσιμο ή κόψιμο της κάρτας με κάποιο εργαλείο κοπής. Η ηλεκτρονική εξουδετέρωση μπορεί να επιτευχθεί χρησιμοποιώντας τη χαρακτηριστική εντολή "θανάτωσης" (kill command) της κάρτας ή ένα ισχυρό ηλεκτρομαγνητικό πεδίο που καθιστά μόνιμα το κύκλωμα της κάρτας άχρηστο. Όταν η κάρτα προς εξουδετέρωση διαθέτει ένα ηλεκτρονικό μηχανισμό μόνιμης απενεργοποίησης, τότε αυτός προτιμάται καθώς κάνει ευκολότερη τη διαδικασία και μειώνει την προσπάθεια που απαιτείται.

Εφαρμοσιμότητα Ελέγχου : Είναι κατάλληλη μέθοδος για εφαρμογές RFID στις οποίες δεν είναι επιθυμητή η δυνατότητα χρησιμοποίησης της κάρτας αφού έχει ολοκληρώσει τη λειτουργία για την οποία προοριζόταν. Η παρουσία μιας ικανής να λειτουργήσει κάρτας χωρίς αυτό να είναι αναγκαίο εμπεριέχει κινδύνους, αφού μπορεί να χρησιμοποιηθεί για κακόβουλους σκοπούς.

Πλεονεκτήματα : Η καταστροφή ή η μόνιμη απενεργοποίηση καρτών εξαλείφει την

πιθανότητα χρησιμοποίησης τους για ιχνηλασία (tracking) ή στοχοποίηση. Επίσης εμποδίζει την πρόσβαση σε ευαίσθητα δεδομένα που υπάρχουν αποθηκευμένα στις κάρτες.

Μειονεκτήματα : Έστω και ελάχιστα, αυξάνεται το κόστος του κύκλου ζωής της κάρτας από την προσπάθεια που καταβάλλεται για την εξουδετέρωσή της. Επίσης, αποκλείεται η δυνατότητα μελλοντικής χρήσης της κάρτας σε επιπρόσθετες εφαρμογές.

❿ Εκπαίδευση για χειρισμό και διαχείριση

Περιγραφή Ελέγχου : Η εκπαίδευση σε θέματα χειρισμού και διαχείρισης παρέχει στο προσωπικό τις ικανότητες και τις γνώσεις που είναι απαραίτητες ώστε αυτό να μπορεί να εξοικειωθεί με τη χρήση RFID και να συμμορφωθεί με τις συμβάσεις και συμφωνίες που έχουν υπογραφεί. Στις περισσότερες υλοποιήσεις RFID το προσωπικό καλείται να εκτελέσει ποικίλους ρόλους, κάτι το οποίο χρειάζεται εξειδικευμένη εκπαίδευση και διαφορετικές γνώσεις ώστε να μπορεί να ανταποκριθεί σε κάθε ξεχωριστό ρόλο.

Μία κατάλληλη εκπαίδευση επικεντρώνει στην αναγνώριση και εντοπισμό των μη εξουσιοδοτημένων χρήσεων του συστήματος όταν αυτές συμβαίνουν, καθώς επίσης στην αναφορά παραβιάσεων προς τον αρμόδιο γι' αυτά τα θέματα.

Στις περιπτώσεις που υπάρχουν κίνδυνοι λόγω ηλεκτρομαγνητικής ακτινοβολίας, τότε η εκπαίδευση παρέχει διάφορες τεχνικές προστασίας όπως το χειρισμό του εκάστοτε συστήματος από ασφαλή απόσταση.

Ακόμη, για την καταστροφή ή ανακύκλωση καρτών, είναι αναγκαία η κατάλληλη εκπαίδευση ώστε να εκτελεστούν σωστά αυτές οι λειτουργίες. Για παράδειγμα, οι χειριστές πρέπει να μάθουν πώς να καθαρίζουν τη μνήμη των καρτών ώστε αυτές να είναι έτοιμες για επαναχρησιμοποίηση.

Εφαρμοσιμότητα Ελέγχου : Όλες οι υλοποιήσεις RFID.

Πλεονεκτήματα : Η εκπαίδευση βοηθάει στην εξασφάλιση σωστής χρήσης και συντήρησης του συστήματος. Επίσης βοηθάει τους χειριστές να αναγνωρίζουν τις παραβιάσεις ασφαλείας και να φροντίζουν για την έγκαιρη αντιμετώπισή τους όταν αυτές επαναληφθούν.

Μειονεκτήματα : Η ύπαρξη εκπαίδευσης δεν είναι ικανή από μόνη της να εξασφαλίσει ότι θα γίνεται σωστός χειρισμός του συστήματος και ότι θα υπάρχει συμμόρφωση με τις όποιες συμβάσεις και συμφωνίες έχουν γίνει.

❿ Πληροφοριακές επιγραφές και προειδοποιήσεις

Περιγραφή Ελέγχου : Ένα γραπτό μήνυμα το οποίο επισυνάπτεται ή διανέμεται μαζί με κάθε κάρτα ή αναρτάται κοντά στους αναγνώστες. Σκοπό έχει να πληροφορήσει τους χρήστες για τους στόχους του συστήματος RFID ή να συμβουλεύσει τους χρήστες με ποιο τρόπο μπορούν να ελαχιστοποιήσουν ενδεχόμενους κινδύνους (για παράδειγμα χρήση λεπτού μεταλλικού ελάσματος ή ειδικής θήκης για προστασία προσωπικών δεδομένων ή προστασία από ακτινοβολία).

Εφαρμοσιμότητα Ελέγχου : Όλες οι εφαρμογές στις οποίες η χρήση απλών ενημερωτικών μηνυμάτων μπορεί να μετριάσει τους ενδεχόμενους κινδύνους που υπάρχουν. Ειδικότερα, ο συγκεκριμένος έλεγχος είναι κατάλληλος σε εφαρμογές όπου εμπλέκονται καταναλωτές και υπάρχουν ανησυχίες για την ασφάλεια προσωπικών δεδομένων.

Πλεονεκτήματα : Τα μηνύματα δίνουν βασικές πληροφορίες στους χρήστες για κινδύνους που υπό άλλες συνθήκες δεν θα μπορούσαν να γνωρίζουν και τους οποίους μπορούν να αντιμετωπίσουν με απλές τεχνικές προστασίας.

Μειονεκτήματα : Η διανομή μιας προειδοποίησης δεν εγγυάται ότι αυτή θα

διαβαστεί ή θα γίνει κατανοητή. Δεν αποτελεί επίσης το κατάλληλο μέτρο όταν αφορά περίπλοκες έννοιες ή οδηγίες που για να εμπεδωθούν σωστά χρειάζεται συστηματική εκπαίδευση και πείρα.

⑩ Διαχωρισμός καθηκόντων

Περιγραφή Ελέγχου : Τα καθήκοντα σε ένα σύστημα RFID διανέμονται σε διαφορετικούς ρόλους στο προσωπικό με σκοπό την ελαχιστοποίηση της ζημιάς που μπορεί να υπάρξει από ακούσια ή κακόβουλη δραστηριότητα ενός ατόμου. Η κύρια αρχή του ελέγχου είναι πως μία κακόβουλη συνωμοσία ανάμεσα σε δύο ή περισσότερους εξουσιοδοτημένους χρήστες του συστήματος είναι λιγότερο πιθανό να συμβεί σε σχέση με ένα μόνο πρόσωπο που εμπλέκεται σε τέτοιου είδους παράνομες δραστηριότητες.

Ένα παράδειγμα διαχωρισμού καθηκόντων είναι η ανάθεση σε ξεχωριστά άτομα του προσωπικού (α) να αναρτούν κάρτες σε αντικείμενα και (β) να εκτελούν ανάγνωση των καρτών. Αν ένα μόνο άτομο εκτελούσε και τις δύο λειτουργίες, θα μπορούσε σκόπιμα να βάλει λάθος κάρτα σε αντικείμενο ώστε να εξαπατήσει το σύστημα και να κερδίσει κάτι από αυτή την ενέργεια. Μια τέτοια προσπάθεια θα μπορούσε να γίνει με τοποθέτηση καρτών που αντιστοιχούν σε φτηνά προϊόντα πάνω σε αντικείμενα υψηλής αξίας με σκοπό το οικονομικό όφελος.

Εφαρμοσιμότητα Ελέγχου : Εφαρμογές RFID στις οποίες κάποιο πρόσωπο εκ των έσω, ίσως να έχει το κίνητρο να εκτελέσει παράνομες συναλλαγές. Αυτό μπορεί να συμβεί όταν οι κάρτες εξυπηρετούν εμπορικές συναλλαγές, ειδικά όταν αυτές αφορούν αντικείμενα υψηλής αξίας.

Πλεονεκτήματα : Ο διαχωρισμός καθηκόντων βοηθά στη μείωση κακόβουλων ζημιών ή προσπαθειών εξαπάτησης αφού όποιος θέλει να προχωρήσει σε τέτοιες ενέργειες θα αναγκαστεί να συνεργαστεί με τουλάχιστον ακόμα ένα χρήστη. Μειώνει επίσης τα λάθη εφόσον ένας χρήστης μπορεί να αντιληφθεί ενδεχόμενα σφάλματα

που έγιναν προηγουμένως από κάποιον άλλο.

Μειονεκτήματα : Η περίπτωση πολλαπλής συνεργασίας υπαλλήλων με στόχο την απάτη ή τη ζημιά συνεχίζει να υφίσταται. Ακόμη, σε περιπτώσεις περιορισμένου αριθμού προσωπικού, ένας πλήρης διαχωρισμός καθηκόντων ίσως να μην είναι εφικτός.

❿ Τύποι αναγνώρισης για απόκρυψη πληροφοριών

Περιγραφή Ελέγχου : Η εκχώρηση κωδικών αναγνώρισης στις κάρτες RFID γίνεται με τη χρήση τύπων αναγνώρισης μέσω των οποίων οι κάρτες προσδιορίζονται με τέτοιο τρόπο ώστε να μην αποκαλύπτονται ούτε πληροφορίες που αφορούν τα αντίστοιχα αντικείμενα, ούτε και ο διαχειριστής του συστήματος RFID που έχει εκχωρήσει τους αντίστοιχους κωδικούς. Οι τύποι αναγνώρισης για απόκρυψη μπορεί να επιλεχθεί να εκχωρηθούν σειριακά ή τυχαία, ανάλογα το ποιος τρόπος εξυπηρετεί καλύτερα.

Σε αντιπαραβολή, αν ένας εχθρός διαβάσει σωστά ένα τύπο αναγνώρισης που κωδικοποιεί σύμφωνα με κάποιο πρότυπο, όπως είναι για παράδειγμα το EPC (Electronic Product Code), τότε ίσως να είναι σε θέση να διακρίνει τον κατασκευαστή ή διανομέα του αντικειμένου, όπως επίσης και το είδος του αντικειμένου. Με την τυποποιημένη μορφή αναγνώρισης EPC που αφορά ένα συγκεκριμένο είδος προϊόντος, καθορίζονται ένα ίδιο ID που χαρακτηρίζει το διαχειριστή EPC και ίδια bits που χαρακτηρίζουν σε ποια κατηγορία ανήκει το αντικείμενο. Το παρακάτω σχήμα που ακολουθεί δείχνει ένα παράδειγμα 96-bit EPC το οποίο αποτελείται από τέσσερα πεδία.

Σχήμα 1. Παράδειγμα 96-bit EPC

Οι κάρτες πρέπει να διαθέτουν τύπους αναγνώρισης που να μπορούν να προγραμματισθούν ώστε να είναι δυνατή η να υποστήριξη του ελέγχου. Ακόμα και σε κάρτες που έχουν σχεδιαστεί να υποστηρίζουν πρότυπες μορφές αναγνώρισης, μπορεί να ανατεθούν μη πρότυπες μορφές αναγνώρισης στα πεδία που αυτό κρίνεται σκόπιμο. Ωστόσο, υπάρχουν κάποιες κάρτες που έχουν αρχικές εργοστασιακές μορφές αναγνώρισης οι οποίες δεν μπορούν να τροποποιηθούν μετά την κατασκευή τους.

Εφαρμοσιμότητα Ελέγχου : Σε όποιες εφαρμογές κρίνεται αναγκαία η απόκρυψη των τύπων αναγνώρισης ώστε να αποφευχθεί ο κίνδυνος διαρροής χρήσιμων πληροφοριών.

Πλεονεκτήματα : Οι εχθροί δεν μπορούν να αποκομίσουν πληροφορίες μόνο από τους κωδικούς αναγνώρισης.

Μειονεκτήματα :

- Με τη χρήση τύπων αναγνώρισης για απόκρυψη, χάνονται τα οφέλη από τη χρήση καθιερωμένων πρότυπων τύπων αναγνώρισης στην περίπτωση των οποίων ο σχεδιασμός και η συντήρηση κατανεμημένων βάσεων δεδομένων στο backend γίνονται πολύ ευκολότερα.
- Αν επιλεχθεί τυχαία εκχώρηση κωδικών αναγνώρισης, υπάρχει μικρή πιθανότητα να δοθεί ο ίδιος κωδικός δύο φορές και έτσι να επακολουθήσουν λάθη στην παραγωγική και επιχειρηματική διαδικασία.
- Εάν υπάρχει συγκεκριμένη λογική με την οποία εκχωρούνται κωδικοί αναγνώρισης, τότε ενδεχόμενη αποκάλυψη της μεθόδου που χρησιμοποιείται, από ένα εχθρό, θα ανατρέψει την ισχύ του ελέγχου.

⑩ Εφεδρικό σύστημα ταυτοποίησης

Περιγραφή Ελέγχου : Ένα εφεδρικό σύστημα ταυτοποίησης παρέχει εναλλακτικά

μέσα για ταυτοποίηση, πιστοποίηση ή επιβεβαίωση ενός αντικειμένου όταν το σύστημα RFID δεν είναι διαθέσιμο ή όταν μία κάρτα είναι χαλασμένη. Οι επιλογές που υπάρχουν για ένα τέτοιο σύστημα περιλαμβάνουν αυτοκόλλητο με περιγραφικό κείμενο και τεχνολογία AIDC όπως είναι οι γραμμωτοί κώδικες (bar codes). Το σύστημα μπορεί να αποτελείται από ένα απλό αναγνωριστικό αλλά μπορεί να περιλαμβάνει και επιπρόσθετα δεδομένα για το χαρακτηρισμό του αντικειμένου που περιγράφεται. Συνοδεύεται επίσης από καθιερωμένες διαδικασίες χειρισμού και την ανάλογη εκπαίδευση προσωπικού, ώστε αυτό να γνωρίζει πότε και με ποιο τρόπο να το χρησιμοποιήσει.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλο για όλες τις εφαρμογές RFID.

Πλεονεκτήματα : Η ύπαρξη των αναγνωριστικών ταυτοποίησης και των δεδομένων της κάρτας με ένα εφεδρικό τρόπο, αποτελεί ένα μέσο φύλαξης σε περίπτωση κακόβουλης ή τυχαίας ζημιάς στην κάρτα, δυσλειτουργίας ενός αναγνώστη ή βλάβης σε κάποιο υποσύστημα του backend.

Μειονεκτήματα : Ο έλεγχος παρουσιάζει αρκετές πιθανές αδυναμίες όπως :

- Μία ζημιά σε κάρτα μπορεί να καταστήσει αμφότερα τα αποθηκευμένα και τα τυπωμένα δεδομένα μη χρησιμοποιήσιμα. Επίσης αν συμβούν πολλές βλάβες στο backend τότε είναι πιθανό ούτε το εφεδρικό σύστημα να μπορεί να δουλέψει.
- Τα δεδομένα που αναγράφονται στο αυτοκόλλητο μέρος είναι ορατά και έτσι ευκολότερα προσβάσιμα από μη εξουσιοδοτημένα άτομα.
- Το περιγραφικό κείμενο ή το barcode μπορεί να μην παρέχουν την ίδια χωρητικότητα με τη μνήμη RFID.
- Οι εναλλακτικές μέθοδοι που έχουν περιγραφεί είναι στατικής μορφής και έτσι δεν μπορούν να παρέχουν μία πλήρη εφεδρική λύση για εφαρμογές στις οποίες τα δεδομένα κάρτας μεταβάλλονται κατά τη διάρκεια του χρόνου. Ωστόσο, στις περισσότερες εφαρμογές είναι καλύτερο να υπάρχουν έστω κάποιες πληροφορίες

ταυτοποίησης, παρά να μην υπάρχουν καθόλου.

2.3 Τεχνικοί Έλεγχοι

Επί του παρόντος, υπάρχουν αρκετοί διαθέσιμοι τεχνικοί έλεγχοι για τα συστήματα RFID, ενώ πολλοί άλλοι βρίσκονται υπό ανάπτυξη σε βιομηχανικά και ακαδημαϊκά ερευνητικά εργαστήρια. Εδώ παρουσιάζονται οι εμπορικά διαθέσιμοι έλεγχοι που υπάρχουν μέχρι στιγμής. Οι περισσότεροι από αυτούς είναι λεπτομερώς καθορισμένοι σε πρότυπα ενώ κάποιοι άλλοι είναι διαθέσιμοι μόνο σε ιδιόκτητα συστήματα.

Σε πολλούς τεχνικούς ελέγχους απαιτείται από τις κάρτες να έχουν τη δυνατότητα εκτέλεσης πρόσθετων υπολογισμών ή να έχουν πρόσθετη ευμετάβλητη μνήμη, γεγονός που προϋποθέτει την ύπαρξη ενός πολυπλοκότερου ολοκληρωμένου κυκλώματος από τα συνήθη, έτσι ώστε να είναι ικανές οι κάρτες να εκτελέσουν τις προηγμένες λειτουργίες που απαιτούνται. Επίσης, όταν πρόκειται για παθητικές κάρτες, τότε ίσως να πρέπει να βρίσκονται σε πιο κοντινή απόσταση στους αναγνώστες ούτως ώστε να αποκτήσουν την αναγκαία ισχύ που χρειάζεται για να εκτελέσουν τους προαναφερθέντες υπολογισμούς. Εναλλακτικά, η επιπλέον ισχύς που απαιτείται μπορεί να δοθεί από τους αναγνώστες αν αυτοί εκπέμπουν σε υψηλότερα επίπεδα ισχύος, αν και αυτό ίσως να μην είναι δυνατό ή να ξεπερνά τα επιτρεπτά όρια. Αυτά τα ενυπάρχοντα χαρακτηριστικά των παθητικών καρτών περιορίζουν τη χρήση κάποιων τεχνικών ελέγχων σε μερικά περιβάλλοντα.

Υπάρχουν τεχνικοί έλεγχοι για όλες τις συνιστώσες ενός συστήματος RFID όμως μόνο το υποσύστημα ασύρματης επικοινωνίας (RF subsystem) εμπίπτει αποκλειστικά στις αρμοδιότητες της τεχνολογίας RFID και η παρουσίαση των ελέγχων επικεντρώνεται σε αυτό. Τα υπόλοιπα υποσυστήματα, τυπικά, απευθύνονται σε άλλες τεχνολογίες οι οποίες αναπτύσσουν αντίστοιχους ελέγχους για αυτά.

Οι γενικοί τύποι των τεχνικών ελέγχων του υποσυστήματος RF περιλαμβάνουν :

- Την παροχή υπηρεσιών πιστοποίησης και ακεραιότητας στα στοιχεία και στις συναλλαγές που αφορούν την τεχνολογία RFID.

- Την προστασία της ασύρματης επικοινωνίας μεταξύ αναγνώστη και κάρτας.
- Την προστασία των δεδομένων που βρίσκονται αποθηκευμένα στις κάρτες.

Οι έλεγχοι που αντιστοιχούν στις πιο πάνω κατηγορίες παρουσιάζονται με λεπτομέρεια και αναλυτικά παραδείγματα στη συνέχεια.

- **Πιστοποίηση και ακεραιότητα δεδομένων**

Οι συνηθέστερες τεχνικές πιστοποίησης που χρησιμοποιούνται για το υποσύστημα RF των συστημάτων RFID είναι οι συνθηματικοί κωδικοί ασφαλείας (passwords), οι κωδικοί πιστοποίησης HMAC (keyed-hash message authentication codes) και οι ψηφιακές υπογραφές (digital signatures). Σε κάποιες περιπτώσεις, ο πρωταρχικός αντικειμενικός σκοπός των μεθόδων πιστοποίησης είναι να εμποδίσουν τη μη εξουσιοδοτημένη εγγραφή ή ανάγνωση στις κάρτες, ενώ σε άλλες περιπτώσεις ο σκοπός είναι η ανίχνευση καρτών κλώνων.

Οι τεχνικές πιστοποίησης που βασίζονται στη κρυπτογραφία παρέχουν συχνά υπηρεσίες ακεραιότητας για τα δεδομένα που περιλαμβάνονται στη διεξαγωγή των πιστοποιήσεων, δηλαδή, όταν ένας εχθρός παραποιήσει αυτά τα δεδομένα τότε η αλλαγή αυτή θα εντοπιστεί άμεσα από τον αναγνώστη ή την κάρτα.

⑩ Πιστοποίηση συνθηματικών κωδικών ασφαλείας

Περιγραφή Ελέγχου : Η κάρτα δεν επιτρέπει την εκτέλεση εντολών που προστατεύονται από συνθηματικό κωδικό ασφαλείας, εάν δεν συνοδεύονται από το σωστό συνθηματικό κωδικό. Τέτοιου είδους προστατευμένες εντολές μπορεί να είναι εντολές που υποστηρίζουν εγγραφή και ανάγνωση δεδομένων κάρτας, έλεγχο πρόσβασης στη μνήμη και την εντολή kill.

Για την ορθή υλοποίηση του ελέγχου, πρέπει να αναπτυχθεί ένα σύστημα διαχείρισης συνθηματικών κωδικών το οποίο να διευθύνει την δημιουργία, μεταφορά, αποθήκευση και όποια άλλη μορφή διαχείρισης των συνθηματικών κωδικών. Όταν είναι εφικτό, η εκχώρηση των κωδικών στις κάρτες πρέπει να γίνεται

σε ένα φυσικά προστατευμένο περιβάλλον για να ελαχιστοποιηθεί η πιθανότητα υποκλοπών.

Επίσης, οι κάρτες δεν πρέπει να μοιράζονται κωδικούς όπου αυτό μπορεί να εφαρμοστεί, ενώ η περιοδική αλλαγή κωδικών, αν είναι εφικτή, προσδίδει μεγαλύτερη ασφάλεια.

Εφαρμοσιμότητα Ελέγχου : Σε όποια εφαρμογή στην οποία η εξουσιοδοτημένη εκτέλεση μιας συγκεκριμένης εντολής αντιπροσωπεύει κάποια επιχειρηματική διαδικασία ή πληροφορία, αφορά προσωπικά δεδομένα ή εκφράζει ένα εξωτερικό κίνδυνο.

Πλεονεκτήματα : Ελαττώνεται σημαντικά η πιθανότητα χρήσης των καρτών για μη εξουσιοδοτημένους σκοπούς.

Μειονεκτήματα : Παρουσιάζονται τα πιο κάτω μειονεκτήματα :

- Η διαχείριση των συνθηματικών κωδικών για συστήματα RFID είναι πολύπλοκη, ιδιαίτερα αν η εφαρμογή αφορά μεγάλο αριθμό καρτών ή όταν οι κωδικοί πρέπει να διανέμονται πέραν των ορίων του οργανισμού που τους αναπτύσσει, όπως συμβαίνει στις αλυσίδες προμηθειών.
- Η ασύρματη μετάδοση μη κρυπτογραφημένων κωδικών, που συμβαίνει συχνά, δίνει τη δυνατότητα σε εχθρούς να επέμβουν στη μετάδοση και να αποκτήσουν τους κωδικούς ώστε να τους χρησιμοποιήσουν αργότερα για μη εξουσιοδοτημένες συναλλαγές.
- Αν το περιβάλλον της εφαρμογής αποκλείει την άμεση πρόσβαση σε βάση δεδομένων για κωδικούς καρτών, όπως συμβαίνει με κινητούς αναγνώστες που βρίσκονται σε απομακρυσμένες τοποθεσίες, τότε ίσως είναι αναγκαστική η εκχώρηση του ίδιου κωδικού σε πολλαπλές κάρτες. Σε τέτοιες περιπτώσεις η έκθεση ενός και μόνο κωδικού θα θέσει σε κίνδυνο την ακεραιότητα ολόκληρου του συστήματος.

- Οι συνθηματικοί κωδικοί μπορεί να αποκτηθούν με κάποια εξαναγκαστική μέθοδο, όπως είναι η δοκιμή όλων των δυνατών συνδυασμών κωδικών που υπάρχουν. Αυτή η μέθοδος είναι αποτελεσματική όταν το μήκος λέξης των κωδικών είναι μικρό, κάτι που συνεπάγεται μικρό αριθμό δυνατών συνδυασμών.
- Οι κωδικοί μπορούν να αποκαλυφθούν με τη χρησιμοποίηση επιθέσεων ανάλυσης ισχύος σε κάποιους τύπους παθητικών καρτών. Οι κάρτες που επιδέχονται αυτού του είδους την επίθεση, εκπέμπουν σε διαφορετικά επίπεδα ισχύος ανάλογα σε ποιο βαθμό είναι ορθό το συνθηματικό που έχουν πάρει. Το γεγονός αυτό το εκμεταλλεύονται οι επιτιθέμενοι για να αναλύσουν τα επίπεδα ισχύος της κάρτας και να βρουν το σωστό συνθηματικό κωδικό ασφαλείας.

⑩ Κωδικοί πιστοποίησης HMAC

Περιγραφή Ελέγχου : Στους κωδικούς πιστοποίησης HMAC (keyed-hash message authentication codes), τόσο ο αναγνώστης όσο και η κάρτα μοιράζονται ένα δημόσιο μυστικό κλειδί το οποίο μπορεί να χρησιμοποιηθεί σε συνδυασμό με ένα αλγόριθμο hash ο οποίος ανακατεύει και μπερδεύει τα κλειδιά, για να παρέχουν μίας κατεύθυνσης ή αμοιβαία πιστοποίηση μεταξύ κάρτας και αναγνώστη. Όταν οι κωδικοί πιστοποίησης HMAC χρησιμοποιούνται σε μηνύματα, τότε επίσης εξασφαλίζουν την ακεραιότητα των δεδομένων που περιέχονται στα μηνύματα αυτά. Οι HMAC υποστηρίζουν όλους τους κρυπτογραφικούς αλγόριθμους hash και δεν καθορίζονται σε κάποιο πρότυπο RFID αλλά είναι διαθέσιμοι σε ιδιόκτητες διατάξεις.

Εφαρμοσιμότητα Ελέγχου : Εφαρμογές στις οποίες η χρήση συνθηματικών κωδικών ασφαλείας θεωρείται ανεπαρκής μηχανισμός πιστοποίησης, διότι υπάρχει πιθανώς υψηλός κίνδυνος “κρυφακοής”. Επίσης, εφαρμογές στις οποίες χρειάζεται απόδειξη αυθεντικότητας της κάρτας.

Πλεονεκτήματα : Τα πλεονεκτήματα του HMAC σε σχέση με τις πιστοποιήσεις

συνθηματικών κωδικών ασφαλείας είναι ότι το HMAC :

- Παρέχει απόδειξη αυθεντικότητας της κάρτας.
- Παρέχει προστασία στην ακεραιότητα των δεδομένων, αφού οποιαδήποτε αλλαγή στα δεδομένα έχει ως επακόλουθο μία διαφορετική τιμή του HMAC η οποία θα εντοπιστεί από τον παραλήπτη.
- Δεν μεταδίδει στο ασύρματο κανάλι απόρρητους γραπτούς κωδικούς, εξουδετερώνοντας έτσι τον κίνδυνο υποκλοπής (eavesdropping).

Μειονεκτήματα : Οι αδυναμίες που παρουσιάζουν οι πιστοποιήσεις HMAC είναι :

- Η διαχείριση των κλειδιών HMAC παρουσιάζει τις ίδιες δυσκολίες και προκλήσεις με τη διαχείριση των συνθηματικών κωδικών και ως επακόλουθο μπορεί να μην είναι πρακτική λύση, όταν οι κινητοί αναγνώστες δεν έχουν αξιόπιστη πρόσβαση σε ένα σύστημα διαχείρισης κλειδιών HMAC.
- Οι αξιώσεις αυθεντικότητας που σχετίζονται με την πιστοποίηση HMAC αντέχουν μόνο όταν τα κλειδιά HMAC παραμένουν μυστικά. Αν ένας πεπειραμένος εχθρός που διαθέτει τις απαραίτητες γνώσεις έχει φυσική πρόσβαση σε μια κάρτα και αποκομίσει το κλειδί HMAC που της αντιστοιχεί, τότε μπορεί να δημιουργήσει κλώνο της κάρτας.
- Η διανομή κλειδιών HMAC ανάμεσα σε διάφορους οργανισμούς δεν εξασφαλίζει τις απαιτήσεις αυθεντικότητας αφού βασίζεται στη μεταξύ των οργανισμών εμπιστοσύνη, η οποία μπορεί να μην υπάρχει σε πρακτικό επίπεδο.
- Οι μέθοδοι πιστοποίησης HMAC απαιτούν μεγαλύτερη υπολογιστική ισχύ σε σύγκριση με τους συνθηματικούς κωδικούς και για αυτό το λόγο απαιτείται σχεδιασμός πολυπλοκότερων καρτών για να υποστηριχτούν.

⑩ Ψηφιακές υπογραφές

Περιγραφή Ελέγχου : Οι αναγνώστες, χρησιμοποιώντας ψηφιακό τρόπο για να υπογράψουν τους τύπους αναγνώρισης (IDs) των καρτών, αφήνουν χρονικές σφραγίδες και άλλα σχετικά δεδομένα που αφορούν γεγονότα των συναλλαγών στις

κάρτες. Οι υπογραφές που προκύπτουν αποθηκεύονται στις κάρτες και χρησιμοποιούνται για διαδοχικές επαληθεύσεις, αν και η καταγραφή των υπογραφών σε εσωτερικές βάσεις δεδομένων παρέχει επιπρόσθετη εγγύηση για την αλυσίδα συναλλαγών της κάρτας.

Οι ψηφιακές υπογραφές βασίζονται στην ασύμμετρη κρυπτογραφία που κοινώς ονομάζεται κρυπτογραφία δημόσιου κλειδιού. Η χρήση της τεχνολογίας ψηφιακής υπογραφής στο περιβάλλον των συστημάτων RFID, αναφέρεται ως αυθεντικά πιστοποιημένο RFID. Η τυπική λειτουργία της μεθόδου είναι η εξής :

1. Η κάρτα έχει ένα μόνιμο μοναδικό ID για την αναγνώρισή της που δεν μπορεί να μεταβληθεί μετά την κατασκευή της.
2. Ο αναγνώστης δημιουργεί ένα δημόσιο/ιδιωτικό ζευγάρι κλειδιών και εξασφαλίζει ένα αντίστοιχο πιστοποιητικό δημόσιου κλειδιού.
3. Ο αναγνώστης χρησιμοποιεί ένα καθορισμένο αλγόριθμο hash για να υπολογίσει ένα συνοπτικό μήνυμα για το ID της κάρτας και για άλλα πιθανά δεδομένα που συνδέονται με τη συναλλαγή, κρυπτογραφεί το συνοπτικό μήνυμα με το ιδιωτικό του κλειδί για να δημιουργήσει τη ψηφιακή υπογραφή της συναλλαγής και αποθηκεύει την υπογραφή που προκύπτει στην κάρτα.
4. Οι άλλοι αναγνώστες που διαβάζουν την υπογραφή, την αποκρυπτογραφούν μέσω του δημόσιου κλειδιού του πρώτου αναγνώστη και υπολογίζουν το πανομοιότυπο συνοπτικό μήνυμα για να αποφασίσουν αν ταιριάζουν. Εφόσον τα συνοπτικά μηνύματα ταιριάζουν τότε η διαδικασία επαλήθευσης εγγυάται την αυθεντικότητα της προηγούμενης συναλλαγής. Εάν δεν ταιριάζουν τότε είτε τα δεδομένα της συναλλαγής έχουν μεταβληθεί, είτε μία μη εξουσιοδοτημένη συσκευή δημιούργησε τη ψηφιακή υπογραφή.
5. Οι υπόλοιποι αναγνώστες μπορούν να αποθηκεύσουν τα δικά τους γεγονότα συναλλαγής στην κάρτα ή να τα καταγράψουν στις κατάλληλες βάσεις δεδομένων για μεταγενέστερη άντληση πληροφοριών αναφορικά με την αλυσίδα των συναλλαγών της κάρτας.

Εφαρμοσιμότητα Ελέγχου : Εφαρμογές που απαιτούν πιο δυνατή απόδειξη αυθεντικότητας από αυτή που προσφέρει η τεχνολογία HMAC, καθώς επίσης πιστοποίηση αυθεντικότητας της αλυσίδας γεγονότων πολλαπλών συναλλαγών. Ακόμη, είναι κατάλληλη μέθοδος για εφαρμογές που απαιτούν πιστοποίηση αυθεντικότητας χωρίς να έχουν σύνδεση με το δίκτυο.

Πλεονεκτήματα : Οι ψηφιακές υπογραφές έχουν να επιδείξουν πολλά πλεονεκτήματα σε σχέση με τις πιστοποιήσεις συνθηματικών κωδικών και HMAC :

- Τα συστήματα ψηφιακής υπογραφής δεν προϋποθέτουν την αποθήκευση κρυπτογραφικών μυστικών στις κάρτες. Αντ' αυτού, οι αναγνώστες διατηρούν ιδιωτικά κλειδιά. Έτσι, στα συστήματα αυτά δεν μοιράζονται μυστικά σε αντίθεση με τις πιστοποιήσεις συνθηματικών και HMAC στις οποίες, αναγνώστης και κάρτα πρέπει να μοιράζονται ένα μυστικό για να λειτουργήσει το σύστημα. Οι κάρτες είναι πολύ πιο ευάλωτες σε επιθέσεις σε σχέση με τους αναγνώστες και έτσι όταν εξαλειφθεί η ανάγκη αποθήκευσης μυστικών στις κάρτες, αυξάνεται σημαντικά η ασφάλεια του ευρύτερου συστήματος.

- Σε πολλές περιπτώσεις οι ψηφιακές υπογραφές δεν χρειάζονται σύνδεση με το δίκτυο για να εκτελέσουν επιτυχώς τη λειτουργία πιστοποίησης. Στις πιστοποιήσεις συνθηματικών και HMAC, ένας αναγνώστης είναι δύσκολο να έχει την απαιτούμενη μνήμη να για αποθηκεύσει τους κωδικούς ή τα κλειδιά για μεγάλο αριθμό καρτών. Σε αντίθεση, με τις ψηφιακές υπογραφές ο αναγνώστης μπορεί απλά να πρέπει να αποθηκεύσει την πιστοποίηση δημόσιου κλειδιού της οντότητας που έδωσε αρχικές τιμές στις κάρτες. Επίσης, ο κάθε οργανισμός που συμμετέχει σε ενδοεπιχειρησιακά συστήματα, πρέπει μόνο να διαμοιράσει τα δημόσια κλειδιά των αναγνωστών του και όχι να παρέχει πρόσβαση σε βάσεις δεδομένων που αφορούν συνθηματικούς κωδικούς ή κλειδιά.

- Οι ψηφιακές υπογραφές είναι συμβατές με τα υπάρχοντα πρότυπα καρτών RFID. Η τεχνολογία HMAC απαιτεί οι κάρτες να υποστηρίζουν αλγόριθμους hash και να υλοποιούν ένα πρωτόκολλο διεκπεραίωσης της πιστοποίησης, απαιτήσεις οι οποίες αμφότερες δεν περιλαμβάνονται στα υπάρχοντα πρότυπα RFID. Αντίθετα, στα αυθεντικά πιστοποιημένα συστήματα RFID, οι κάρτες μπορούν να λαμβάνουν, να αποθηκεύουν και να μεταδίδουν ψηφιακές υπογραφές με τις υπάρχουσες εντολές ανάγνωσης και εγγραφής, αφού η πολυπλοκότητα ανήκει στους αναγνώστες ή το λογισμικό διασύνδεσης (middleware).

Μειονεκτήματα :

- Ένα σύστημα ψηφιακών υπογραφών απαιτεί μία υποδομή δημόσιων κλειδιών, η οποία περιλαμβάνει κατάλληλες αρχές εγγραφής και πιστοποίησης, λειτουργίες ανάκλησης και ανάλογες συμβάσεις και πρακτικές αναφορές. Μία τέτοια υποδομή για να υλοποιηθεί και να λειτουργήσει με επιτυχία, προϋποθέτει προσεκτικό σχεδιασμό και αξιοσημείωτη βοήθεια από ειδικούς. Επιπλέον, οι αναγνώστες ή το middleware πρέπει να μπορούν να υποστηρίξουν τις ψηφιακές υπογραφές και την απαραίτητη υποδομή, λειτουργίες με τις οποίες δεν είναι εξοπλισμένη σε καλό βαθμό η τεχνολογία RFID επί του παρόντος.

- Τα συστήματα ψηφιακών υπογραφών χρειάζονται περισσότερη από τη συνηθισμένη μνήμη των περισσοτέρων καρτών που κυκλοφορούν. Η επιπρόσθετη μνήμη απαιτείται για την αποθήκευση πληροφοριών αναγνώρισης που σχετίζονται με την κάθε συναλλαγή.

- Οι ψηφιακές υπογραφές που δεν παράγονται από την κάρτα είναι αίτιο για επανάληψη επιθέσεων. Ένας εχθρός μπορεί να αντλήσει την απόδειξη αυθεντικότητας της κάρτας, για παράδειγμα τη ψηφιακή υπογραφή που δημιούργησε ένας προηγούμενος αναγνώστης, έτσι ώστε να την αντιγράψει πιστά σε μία κάρτα κλώνο.

- Η χρήση ψηφιακών υπογραφών για την υποστήριξη πιστοποίησης αναγνωστών στις κάρτες απαιτεί την υποστήριξη σχετικά πολύπλοκων κρυπτογραφικών λειτουργιών από τις αυτές, που είναι πέρα από τις ικανότητες των περισσοτέρων κοινών μοντέλων καρτών. Επομένως, στο προσεχές μέλλον, οι κατάλληλες πιθανές λύσεις που θα υποστηρίζουν τον έλεγχο πρόσβασης στις κάρτες, θα είναι μάλλον τα συστήματα πιστοποίησης που βασίζονται στους συνθηματικούς κωδικούς και τα συμμετρικά κλειδιά.

- **Προστασία συστήματος ασύρματης διασύνδεσης**

Υπάρχουν διάφοροι τύποι τεχνικών ελέγχων που εστιάζουν στην προστασία της ασύρματης διασύνδεσης προς τις κάρτες και αναφέρονται παρακάτω :

- Η καλυπτόμενη κωδικοποίηση μπορεί να χρησιμοποιηθεί για να κρύψει το περιεχόμενο των μηνυμάτων από τους αναγνώστες στις κάρτες.
- Τα δεδομένα μπορεί να αποκρύπτονται πριν από τη μετάδοσή τους.
- Μπορεί να γίνει προφύλαξη με χρήση προστατευτικού καλύμματος ώστε να περιοριστεί η υποκλοπή και η σάρωση από μη εξουσιοδοτημένους αναγνώστες.
- Η επιλογή μιας συχνότητας λειτουργίας μπορεί να χρησιμοποιηθεί για την αποφυγή παρεμβολών από άλλες πηγές ή για την επίτευξη συγκεκριμένων χαρακτηριστικών λειτουργίας όπως την ικανότητα διάδοσης δια μέσου μετάλλων, υγρών και άλλων υλικών που είναι αδιαφανή σε πολλές συχνότητες.
- Τα χαρακτηριστικά μετάδοσης του αναγνώστη και της ενεργητικής κάρτας μπορούν να ρυθμιστούν έτσι ώστε να ελαττωθεί η πιθανότητα υποκλοπής και να μετριαστούν οι παρεμβολές και οι κίνδυνοι λόγω ηλεκτρομαγνητικής ακτινοβολίας.
- Η ασύρματη διασύνδεση προς τις κάρτες μπορεί να διακοπεί προσωρινά ώστε να εμποδιστεί μη εξουσιοδοτημένη πρόσβαση σε αυτές όταν υπάρχει πιθανότητα να μη χρησιμοποιηθούν για εξουσιοδοτημένους σκοπούς.
- Η ασύρματη επικοινωνία μπορεί να διακοπεί προκαθορισμένα μέχρι κάποιος χρήστης να την ενεργοποιήσει.
- Οι αναγνώστες μπορούν να εξετάζουν περιοδικά τις κάρτες για να καθορίσουν

τη συνολική παρουσία τους, να αποτιμήσουν την κατάσταση του συστήματος και να αποκτήσουν δεδομένα από το περιβάλλον.

Στα επόμενα, που υπάγονται στην προστασία της ασύρματης διασύνδεσης, ακολουθεί αναλυτική παρουσίαση των προαναφερθέντων ελέγχων.

❿ Καλυπτόμενη κωδικοποίηση (cover-coding)

Περιγραφή Ελέγχου : Το cover-coding είναι μία μέθοδος που χρησιμοποιείται για την απόκρυψη πληροφοριών στο κανάλι αποστολής προς τις κάρτες από ενδεχόμενους υποκλοπείς.

Ένα χαρακτηριστικό παράδειγμα λειτουργίας της μεθόδου φαίνεται μέσω του προτύπου EPC global Class-1 Generation-2 στο οποίο το cover coding χρησιμοποιείται για να κρύψει συνθηματικούς κωδικούς και πληροφορίες που εγγράφονται σε μια κάρτα με τη χρήση της εντολής write.

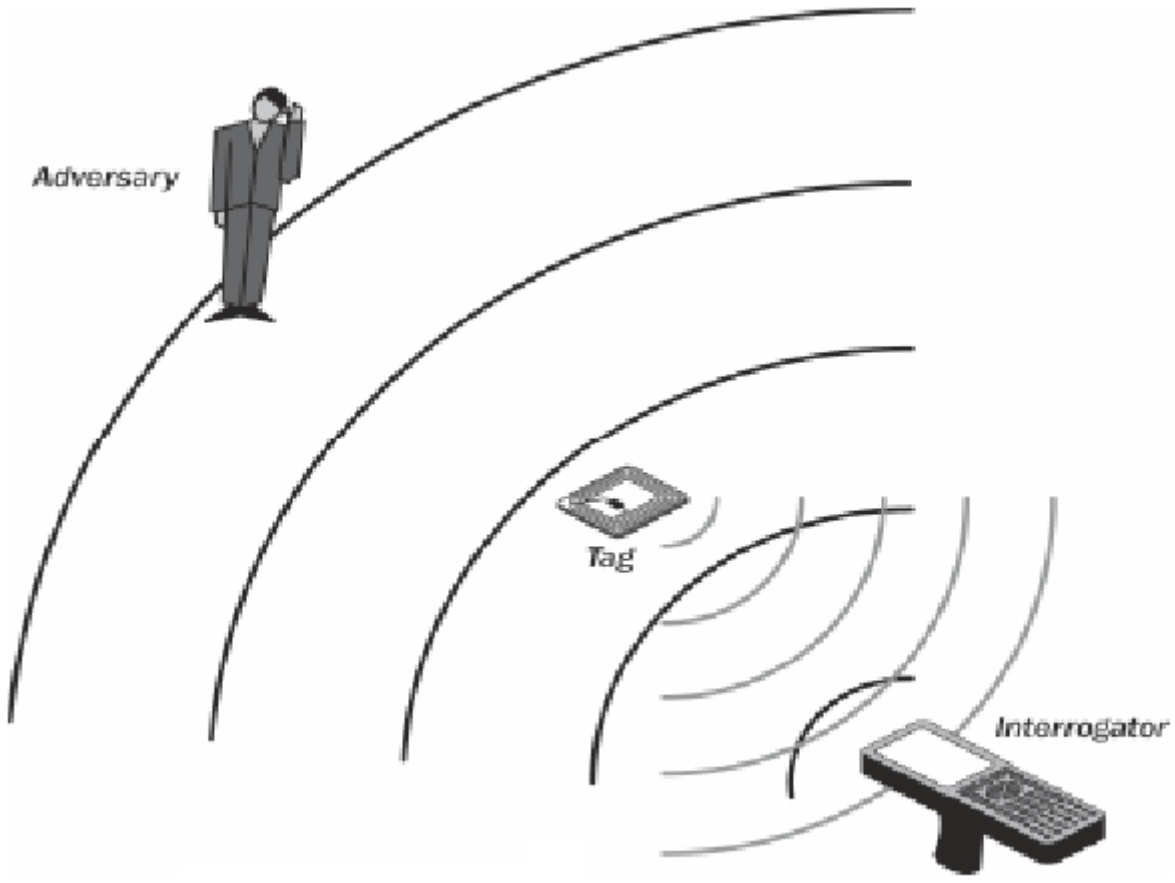
Το πρωτόκολλο EPC global Class-1 Generation-2 cover-coding δουλεύει ως εξής :

1. Ο αναγνώστης αποστέλλει στην κάρτα ένα μήνυμα ζητώντας ένα κλειδί.
2. Η κάρτα δημιουργεί ένα 16-bit αριθμό (το κλειδί) και τον επιστρέφει στον αναγνώστη.
3. Ο αναγνώστης εφαρμόζει αποκλειστικό OR (XOR) στο κλειδί και στο μη κωδικοποιημένο μήνυμα που θέλει να στείλει, και παράγει με αυτή τη διαδικασία ένα κρυπτογραφημένο κείμενο το οποίο ένας υποκλοπέας δεν μπορεί να κατανοήσει εφόσον δεν γνωρίζει το κλειδί.
4. Ο αναγνώστης στέλνει το κρυπτογραφημένο κείμενο στην κάρτα.
5. Η κάρτα εφαρμόζει τη λειτουργία XOR χρησιμοποιώντας το κρυπτογραφημένο κείμενο και το κλειδί για να ανακτήσει το μη κωδικοποιημένο μήνυμα του αναγνώστη.

Το cover coding είναι ένα παράδειγμα “μινιμαλιστικής κρυπτογραφίας” επειδή λειτουργεί εντός των περιορισμών ισχύος και μνήμης που μπορούν να έχουν οι

παθητικές κάρτες. Επίσης, ενώ η λειτουργία XOR από μόνη της θεωρείται ασήμαντος αλγόριθμος απόκρυψης στην παραδοσιακή κρυπτογραφία, παρόλα αυτά ελαττώνει σε ικανοποιητικό βαθμό τον κίνδυνο στα περισσότερα περιβάλλοντα RFID.

Στο επόμενο σχήμα φαίνεται η λειτουργία του cover coding. Το σήμα στο πίσω κανάλι της κάρτας είναι πιο αδύναμο από το σήμα του αναγνώστη στο μπροστινό κανάλι, κάτι που συμβαίνει πάντα για μια παθητική κάρτα η οποία χρησιμοποιεί το σήμα από τον αναγνώστη για να αποκτήσει την ισχύ που χρειάζεται για τις δικές της λειτουργίες. Εφόσον ο εχθρός κρυφακούει το μπροστινό κανάλι, αλλά όχι και το πίσω, δεν μπορεί να μάθει το κλειδί που αποστέλλει η κάρτα και επακόλουθα δεν έχει τη δυνατότητα να αποκωδικοποιήσει το καλυπτόμενο μήνυμα.



Σχήμα 2. Cover Coding

Εφαρμοσιμότητα Ελέγχου : Το cover coding είναι χρήσιμο όταν ο κίνδυνος υποκλοπής (eavesdropping) πρέπει να μειωθεί, όμως οι επιτιθέμενοι αναμένεται να

βρίσκονται πιο μακριά από τις κάρτες σε σχέση με τους αναγνώστες. Στις περισσότερες εφαρμογές η λήψη των σημάτων παθητικής κάρτας στο πίσω κανάλι, απαιτεί εγγύτητα λιγότερη των τεσσάρων μέτρων. Εντός μιας τέτοιας απόστασης η συσκευή λήψης του επιτιθέμενου θα γίνει εύκολα αντιληπτή. Σε αντίθεση, τα σήματα του αναγνώστη μπορεί να εντοπιστούν σε αποστάσεις που ξεπερνούν το ένα χιλιόμετρο. Δεδομένων των προαναφερθέντων στοιχείων, το cover coding είναι κατάλληλο για υποσυστήματα ασύρματης ραδιοεπικοινωνίας στα οποία τα σήματα μπροστινού καναλιού είναι ισχυρότερα από αυτά στο πίσω κανάλι. Συμπερασματικά, αυτό περιορίζει τη μέθοδο στις παθητικές κάρτες. Όπως έχει ήδη αναφερθεί, οι τεχνολογίες EPC global Class-1 Generation-2 υποστηρίζουν cover coding, ενώ υπάρχουν και ιδιόκτητα συστήματα με παρόμοια χαρακτηριστικά.

Πλεονεκτήματα : Η χρήση cover coding βοηθά να εμποδιστεί η εκτέλεση μη εξουσιοδοτημένων εντολών οι οποίες μπορούν να καταστήσουν μη λειτουργική μια κάρτα ή να μεταβάλουν τα δεδομένα της. Ως επακόλουθο, το cover coding μετριάζει τον κίνδυνο που απειλεί προσωπικά δεδομένα και επιχειρηματικές διαδικασίες και πληροφορίες.

Μειονεκτήματα : Ο έλεγχος παρουσιάζει τα εξής μειονεκτήματα :

- Αν ένας εχθρός αποκομίσει ένα κλειδί μέσω του πίσω καναλιού τότε μπορεί να αποκωδικοποιήσει οποιοδήποτε κρυπτογραφημένο κείμενο το οποίο έχει δημιουργηθεί με αυτό το κλειδί.
- Η αποτελεσματικότητα του cover coding εξαρτάται από την απόδοση του γεννήτορα τυχαίων κλειδιών της κάρτας. Αν το τυχαίο κλειδί μπορεί να προβλεφθεί λόγω ελαττωματικής σχεδίασης της κάρτας ή με χρήση κρυπτογραφικής ανάλυσης, τότε ένας εχθρός μπορεί να μάθει το κλειδί και να αποκρυπτογραφήσει διαδοχικά μηνύματα επικοινωνίας.

❿ Απόκρυψη δεδομένων σε μεταφορά

Περιγραφή Ελέγχου : Τα δεδομένα που συλλέγει ή επεξεργάζεται η κάρτα αποκρύπτονται πριν τη μετάδοσή τους στο ασύρματο κανάλι (στον αέρα).

Εφαρμοσιμότητα Ελέγχου : Κατάλληλη μέθοδος για εφαρμογές που χρειάζονται ένα αποτελεσματικό αντίμετρο για απειλές υποκλοπής και για τις οποίες το cover coding προσφέρει ανεπαρκή προστασία. Τυπικά, οι κάρτες χρειάζονται μόνο τις δυνατότητες απόκρυψης που παρέχει το κυκλώμά τους για να προστατέψουν την εμπιστευτικότητα των δεδομένων προς μεταφορά, εφόσον τα δεδομένα που συλλέγουν ή επεξεργάζονται προέρχονται από αισθητήρες ανίχνευσης ή άλλες άμεσα συνδεδεμένες πηγές. Σε αυτές τις περιπτώσεις δεν υπάρχει άλλη εναλλακτική μέθοδος απόκρυψης του περιεχομένου των δεδομένων διότι αυτά ξεκινούν από τις κάρτες. Αντίθετα, στις περιπτώσεις εφαρμογών όπου η μόνη πηγή δεδομένων είναι ο αναγνώστης δεν χρειάζεται κρυπτογράφηση από τα κυκλώματα των καρτών.

Οι μέθοδοι απόκρυψης δεδομένων σε μεταφορά υποστηρίζονται από ιδιόκτητες υλοποιήσεις όχι όμως από τα επίσημα πρότυπα EPC global και ISO/IEC.

Πλεονεκτήματα : Η απόκρυψη δεδομένων σε μεταφορά εμποδίζει την υποκλοπή των εναέριων συναλλαγών RFID.

Μειονεκτήματα :

- Η απόκρυψη δεδομένων απαιτεί ένα σύστημα διαχείρισης κλειδιών το οποίο μπορεί να είναι πολύπλοκο στη διαχείριση και το χειρισμό του.

- Οι λειτουργίες κρυπτογράφησης μπορεί να παρουσιάσουν σημαντική καθυστέρηση, η οποία είναι ανεπιθύμητη σε συστήματα RFID τα οποία απαιτούν γρήγορες συναλλαγές εγγραφής και ανάγνωσης.

- Οι λειτουργίες κρυπτογράφησης απαιτούν επιπρόσθετη ισχύ για την ολοκλήρωσή τους, επηρεάζοντας έτσι εφαρμογές που χρησιμοποιούν παθητικές

κάρτες.

- Οι κάρτες που υποστηρίζουν επί της πλακέτας απόκρυψη, έχουν μεγαλύτερο κόστος από αυτές που δεν έχουν τέτοιες δυνατότητες.

⑩ Κάλυψη ηλεκτρομαγνητικής ακτινοβολίας

Περιγραφή Ελέγχου : Με τη χρησιμοποίηση ενός αγώγιμου υλικού περιβάλλεται η προφυλασσόμενη περιοχή και με τη μέθοδο αυτή περιορίζεται η διάδοση ηλεκτρομαγνητικών σημάτων έξω από την περιοχή που έχει καλυφθεί.

Παραδείγματα εφαρμογής της συγκεκριμένης μεθόδου είναι η προστασία ταξιδιωτικών εγγράφων με τη χρήση ειδικού μεταλλικού υλικού το οποίο εμποδίζει τις προσπάθειες από εχθρούς να διαβάσουν την ενσωματωμένη κάρτα όταν το κάλυμμα του διαβατηρίου είναι κλειστό. Επίσης, μερικές φορές η μέθοδος χρησιμοποιείται για κάλυψη κοντέινερ που μεταφέρονται σε πλοία για να εμποδιστεί η ανάγνωση των καρτών τους. Ακόμη, μπορεί να χρησιμοποιηθεί σε τοίχους και χωρίσματα για να κρατήσει τις εκπομπές σημάτων εντός ορίων μιας συγκεκριμένης περιοχής. Η μέθοδος μπορεί να εφαρμοστεί ακόμη και με τη χρήση ενός φύλλου αλουμινίου με το οποίο τυλίγεται η κάρτα.

Εφαρμοσιμότητα Ελέγχου : Η μέθοδος είναι κατάλληλη σε περιβάλλοντα που αντιμετωπίζουν προβλήματα λόγω υποκλοπής ή ηλεκτρομαγνητικής ακτινοβολίας, ενώ παράλληλα η χρήση προσωρινής κάλυψης δεν θα σταματήσει τις έγκυρες συναλλαγές.

Πλεονεκτήματα : Η μέθοδος μπορεί να περιορίσει την δυνατότητα μη εξουσιοδοτημένων αναγνωστών να συλλέξουν δεδομένα από ένα σύστημα RFID.

Μειονεκτήματα : Η μέθοδος μπορεί να εμποδίσει ή να καθυστερήσει νόμιμες συναλλαγές αναιρώντας έτσι το σημαντικό προτέρημα της γρήγορης εξ αποστάσεως

ανάγνωσης καρτών χωρίς επιπρόσθετους χειρισμούς. Επίσης, μπορεί να είναι ακόμη εφικτό για ένα εχθρό να εκπέμπει για κακόβουλο σκοπό εντός της περιβαλλόμενης περιοχής αν τοποθετήσει κατάλληλη συσκευή εντός αυτής.

⑩ Επιλογή ραδιοσυχνότητας

Περιγραφή Ελέγχου : Η τεχνολογία RFID μπορεί να επικοινωνήσει σε διάφορες ραδιοσυχνότητες συμπεριλαμβανομένων αυτών που ανήκουν στις LF, HF, UHF και μικροκυματικές ζώνες συχνοτήτων. Εκχωρώντας σε μια εφαρμογή RFID συγκεκριμένες σταθερές συχνότητες, μπορούν να αποφευχθούν ή να μειωθούν οι επιδράσεις λόγω παρεμβολών. Εξάλλου, κάποιες τεχνολογίες καρτών έχουν τη δυνατότητα να αλλάζουν συχνότητες μέσα σε ένα περιορισμένο εύρος συχνοτήτων, αν και αυτή η τεχνική χρησιμοποιείται κυρίως για άλλους σκοπούς.

Για να επιτευχθούν καλύτερα αποτελέσματα, πριν την εγκατάσταση ενός συστήματος RFID θα πρέπει να γίνει μια επισκόπηση των ήδη χρησιμοποιούμενων συχνοτήτων στην περιοχή και να αποφασιστεί η κατάλληλη επιλογή τους ώστε να αποφευχθούν ενδεχόμενες παρεμβολές. Σε μερικές περιπτώσεις απαιτείται ειδική άδεια για τη χρησιμοποίηση μιας συγκεκριμένης επιθυμητής συχνότητας.

Εφαρμοσιμότητα Ελέγχου : Όλες οι υλοποιήσεις των οποίων η ραδιοσυχνότητα δεν καθορίζεται από άλλες απαιτήσεις της αντίστοιχης εφαρμογής. Σε μια υλοποίηση κλειστού συστήματος RFID υπάρχει μεγαλύτερη ελευθερία επιλογής συχνότητας λειτουργίας, όμως, αν οι κάρτες βασίζονται σε κάποιο συγκεκριμένο πρότυπο, τότε ίσως να περιορίζονται οι επιλογές στο εύρος συχνοτήτων που ορίζεται από το πρότυπο.

Πλεονεκτήματα : Η επιλογή ραδιοσυχνότητας επιτρέπει την αποφυγή παρεμβολών με άλλα συστήματα που εκπέμπουν. Έτσι, η επιθυμητή επιλογή συγκεκριμένης συχνότητας μπορεί να γίνει επειδή παρατηρείται παρεμβολή σε άλλες ζώνες συχνοτήτων. Επίσης, η επιλογή κάποιων συχνοτήτων μπορεί να γίνει λόγω

επιθυμητών χαρακτηριστικών διάδοσης, όπως είναι η ικανότητα να διαπερνούν κάποια ιδιαίτερα υλικά.

Μειονεκτήματα :

- Υπάρχει δυσκολία στην αναγνώριση των πηγών παρεμβολής. Παράσιτα μπορούν να προκαλέσουν ανεπαρκώς γειωμένοι κινητήρες, θορυβώδεις σταθμοί αναμετάδοσης, παλιές αντιστάσεις ρύθμισης ρεύματος φθοριζόντων λαμπτήρων και άλλες συσκευές που δημιουργούν ανεπιθύμητο θόρυβο στο κοντινό τους περιβάλλον. Γι' αυτό το λόγο, κάθε υλοποίηση RFID πρέπει να δοκιμαστεί στο προοριζόμενο περιβάλλον της πριν να μπει σε παραγωγική χρήση, ώστε να αναγνωριστούν όλες οι πιθανές πηγές παρασίτων.

- Μπορεί να υπάρξουν νέες πηγές παρεμβολής στην θέση του συστήματος RFID μετά την εγκατάστασή του.
- Κατά την υλοποίηση ενός ενδοεπιχειρησιακού συστήματος RFID, οι οργανισμοί που έχουν ανάμειξη με αυτό πρέπει να συμφωνήσουν σε έναν τύπο κάρτας που να υποστηρίζει όλες τις συχνότητες που προτίθενται να χρησιμοποιήσουν οι συμμετέχοντες οργανισμοί.

⑩ Ρύθμιση χαρακτηριστικών μετάδοσης εκτός συχνότητας

Περιγραφή Ελέγχου : Οι χειριστές ρυθμίζουν το επίπεδο της ηλεκτρομαγνητικής ενέργειας που εκπέμπει ένας αναγνώστης ή μία ενεργητική κάρτα. Επίσης, με τη χρήση ειδικών τύπων κεραίας και κατάλληλες διαμορφώσεις, μπορεί να καθοριστεί η κατεύθυνση της ενέργειας. Ακόμη, το duty cycle[1] του αναγνώστη μπορεί να ελεγχθεί.

Εφαρμοσιμότητα Ελέγχου : Όλες οι εφαρμογές για τις οποίες η υποκλοπή, οι ασύρματες παρεμβολές και οι πηγές κινδύνου από την ηλεκτρομαγνητική ακτινοβολία αποτελούν πρόβλημα.

[1]duty cycle : κλάσμα του χρόνου στο οποίο ένα σύστημα βρίσκεται σε “ενεργή” κατάσταση

Πλεονεκτήματα : Η μείωση της ισχύος εκπομπής :

- Μειώνει την πιθανότητα να εμποδίσει κάποιος εχθρός την επικοινωνία.
- Περιορίζει τις παρεμβολές από άλλες νόμιμες εκπομπές.
- Ελαττώνει τις πηγές κινδύνου λόγω ηλεκτρομαγνητικής ακτινοβολίας.

Μειονεκτήματα : Το μειονέκτημα που προκύπτει από τη μείωση της ισχύος εκπομπής ή του duty cycle, είναι η υποβάθμιση της απόδοσης του συστήματος, ειδικά όσον αφορά το πίσω κανάλι επικοινωνίας από μία παθητική κάρτα, αφού για παράδειγμα οι αναγνώστες μπορεί να αποτύχουν να εντοπίσουν την παρουσία έγκυρων καρτών. Επίσης, οι αλλαγές στο φυσικό περιβάλλον του συστήματος ή η εισαγωγή καινούριου εξοπλισμού ασύρματης εκπομπής και λήψης, μπορούν να επηρεάσουν τα επίπεδα ισχύος που απαιτούνται για συνεχείς επιτυχημένες συναλλαγές. Συνεπώς, τα οφέλη που αποκομίζονται από την τοπογράφηση της θέσης του συστήματος, αναιρούνται από τις αλλαγές στο περιβάλλον αυτό.

⑩ Προσωρινή απενεργοποίηση καρτών

Περιγραφή Ελέγχου : Η ασύρματη διασύνδεση σε κάποιες ιδιόκτητες κάρτες μπορεί να κλείσει προσωρινά. Οι κατασκευαστές καρτών διαθέτουν διαφορετικές μεθόδους για την ενεργοποίηση και απενεργοποίησή τους. Για παράδειγμα, μερικές κάρτες σχεδιάζονται με τέτοιο τρόπο, ώστε να βρίσκονται σε λειτουργία ή όχι ανάλογα με ποια άκρη της κάρτας εισάγεται σε μια βάση σύνδεσης. Άλλες κάρτες έχουν επανατοποθετήσιμες μπαταρίες, οι οποίες μπορούν να αφαιρεθούν για να απενεργοποιηθεί η κάρτα.

Όταν ο έλεγχος τεθεί σε εφαρμογή, οι κάρτες θα μπαίνουν σε λειτουργία μέσα σε μια καθορισμένη περιοχή στην οποία λειτουργεί το σύστημα, ενώ όταν απομακρύνονται από αυτή την περιοχή θα απενεργοποιούνται. Για παράδειγμα, σε μια εφαρμογή αλυσίδας προμηθειών, οι κάρτες μπορεί να απενεργοποιούνται κατά την διάρκεια της μεταφοράς εμπορεύματος ώστε να εμποδίζονται μη

εξουσιοδοτημένες συναλλαγές κατά το διάστημα της μεταφοράς και να τίθενται ξανά σε λειτουργία όταν φτάσουν στον προορισμό τους. Αντιστρόφως, οι κάρτες που χρησιμεύουν κατά τη μεταφορά ενεργοποιούνται σε αυτό το διάστημα, ενώ απενεργοποιούνται όταν φτάσει το φορτίο στον προορισμό του.

Εφαρμοσιμότητα Ελέγχου : Ο έλεγχος είναι πολύ χρήσιμος όταν η επικοινωνία αναγνωστών και κάρτας είναι σπάνια και προβλέψιμη. Για παράδειγμα, μία αποθήκη εμπορευμάτων μπορεί να αποθηκεύει αντικείμενα για ένα ετήσιο γεγονός. Σε αυτές τις περιπτώσεις, παρόλο που η χρήση RFID περιορίζεται σε ένα μικρό χρονικό διάστημα κάθε χρόνο, αν παραμείνει σε λειτουργία όλο το χρόνο θα είναι ευάλωτη σε παράνομες συναλλαγές και για αυτό το λόγο είναι ασφαλέστερο να ενεργοποιηθεί μόνο στο διάστημα που χρειάζεται.

Πλεονεκτήματα : Η προσωρινή απενεργοποίηση καρτών εμποδίζει τις μη εξουσιοδοτημένες συναλλαγές με κάρτες κατά τις περιόδους αδράνειας και παρατείνει τη διάρκεια ζωής των μπαταριών των ενεργητικών καρτών.

Μειονεκτήματα : Τα μειονεκτήματα του ελέγχου είναι τα εξής :

- Αν οι χειριστές ή το λογισμικό του συστήματος αποτύχουν να ενεργοποιήσουν ξανά την κάρτα όταν πρέπει, τότε οι χαμένες συναλλαγές θα έχουν αντίκτυπο στην επιχειρηματική διαδικασία.
- Εάν η ενεργοποίηση ή απενεργοποίηση μιας κάρτας απαιτεί ανθρώπινη μεσολάβηση, τότε ο έλεγχος θα έχει ως αποτέλεσμα πρόσθετη εργατική δαπάνη, η οποία μπορεί να είναι σημαντική ιδιαίτερα για συστήματα τα οποία επεξεργάζονται μεγάλο αριθμό καρτών. Σε μια τέτοια περίπτωση, η χρήση RFID θα έχει σημαντικό μειονέκτημα έναντι άλλων τεχνολογιών.

- Ακόμα κι αν η διαδικασία ενεργοποίησης και απενεργοποίησης της κάρτας γίνεται αυτόματα, θα παρουσιάζει μία χρονική καθυστέρηση που ίσως να μην είναι

αποδεκτή σε ευαίσθητες ως προς το χρόνο εφαρμογές.

❿ Διακόπτης ενεργοποίησης κάρτας

Περιγραφή Ελέγχου : Η κάρτα παραμένει συνεχώς απενεργοποιημένη εκτός αν κάποιος χρήστης ή χειριστής πιέσει ένα διακόπτη στην κάρτα για να την ενεργοποιήσει. Όταν ο διακόπτης παραμένει πιεσμένος η κάρτα έχει τη δυνατότητα επικοινωνίας, ενώ όταν ο διακόπτης απελευθερωθεί, η κάρτα επιστρέφει στην προκαθορισμένη κατάσταση απενεργοποίησης, ούτως ώστε να μην μπορούν να διεξαχθούν συναλλαγές.

Εφαρμοσιμότητα Ελέγχου : Είναι κατάλληλη λύση κυρίως για έλεγχο πρόσβασης ή αυτόματες εφαρμογές πληρωμής, στις οποίες ο κάτοχος της κάρτας επιθυμεί ή χρειάζεται τον έλεγχο κατά τη διάρκεια των συναλλαγών της κάρτας και μόνο.

Πλεονεκτήματα : Ο συγκεκριμένος τύπος διακόπτη παρέχει στο χρήστη τη δυνατότητα φυσικού ελέγχου όποτε και όπου μπορεί η κάρτα να ανταποκριθεί στον αναγνώστη. Συνεπώς, αυτός ο έλεγχος αποτελεί μέτρο προστασίας έναντι της υποκλοπής και της μη εξουσιοδοτημένης εκτέλεσης εντολών στην κάρτα και μετριάζει τους αντίστοιχους κινδύνους που προκύπτουν από τέτοιες εχθρικές ενέργειες. Έτσι, οι ενδεχόμενες προσπάθειες υποκλοπής περιορίζονται στην άμεση περιοχή γύρω από τους εξουσιοδοτημένους αναγνώστες, ενώ οι προσπάθειες ιχνηλασίας πέραν αυτής της περιοχής δεν είναι δυνατές.

Ο έλεγχος προσφέρει επίσης τη σιγουριά ότι ένα πρόσωπο κατέχει εις γνώση του την κάρτα και δεν την έχει αποχωριστεί σκόπιμα ή αθέλητα. Για παράδειγμα, ο έλεγχος μπορεί να είναι χρήσιμος σε εφαρμογές πληρωμών ή ελέγχου πρόσβασης, στις οποίες ο αντικειμενικός σκοπός είναι η ακριβής μέτρηση των ατόμων που έχουν παρουσία εκεί και να εμποδίσει επιπλέον κάρτες που δεν χρησιμοποιούνται, να επηρεάσουν την ακρίβεια της μέτρησης.

Μειονεκτήματα : Ο έλεγχος εμφανίζει τα ακόλουθα μειονεκτήματα :

- Η ανάγκη ενεργοποίησης της κάρτας από το χρήστη απαιτεί μία ελάχιστη, έστω, γνώση κατευθυντήριων οδηγιών που μπορεί να προσθέτει κάποιο κόστος ή καθυστέρηση στην επιχειρηματική διαδικασία. Ο χρήστης, για παράδειγμα, πρέπει να γνωρίζει πότε και για πόσο χρονικό διάστημα θα πρέπει να ενεργοποιήσει την κάρτα.

- Μερικοί χρήστες μπορεί να θεωρήσουν την ενεργοποίηση του διακόπτη ενοχλητική διαδικασία, κάτι το οποίο μπορεί να καθυστερήσει την αποδοχή της τεχνολογίας από αυτούς.
- Ένας διακόπτης αυτού του είδους θα μπορούσε να αποσπάσει την προσοχή του χρήστη από άλλες λειτουργίες που εκτελεί. Για παράδειγμα, δεν είναι κατάλληλος έλεγχος για ένα σύστημα αυτόματης πληρωμής διοδίων, διότι ο χρήστης πρέπει να έχει και τα δύο χέρια διαθέσιμα για την οδήγηση του οχήματος.

⑩ Σφυγμομέτρηση καρτών

Περιγραφή Ελέγχου : Ο αναγνώστης εξετάζει περιοδικά την κάρτα για να προσδιορίσει την κατάσταση λειτουργίας της.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλος έλεγχος για εφαρμογές που αφορούν έλεγχο διαδικασίας και διαχείριση αγαθών, στις οποίες η αντικειμενική επιδίωξη είναι η περιοδική ή η σχεδόν συνεχής παρακολούθηση και έλεγχος της κατάστασης. Στα παραδείγματα περιλαμβάνονται ιατρικές εγκαταστάσεις που απαιτούν απογραφή ειδικών ιατρικών εφοδίων σε πραγματικό χρόνο και συστήματα συλλογής δεδομένων από ανιχνευτές. Η μέθοδος είναι επίσης κατάλληλη για επιχειρηματικές διαδικασίες υψηλής αξίας που χρειάζονται πρώιμες ενδείξεις όταν υπάρχουν αποτυχίες του συστήματος ή προβλήματα απόδοσης. Ο έλεγχος είναι πολύ αποτελεσματικός σε εφαρμογές στις οποίες πρόσβαση στις κάρτες έχουν άτομα εμπιστοσύνης ή όπου η αφαίρεση της κάρτας δεν είναι εφικτή.

Πλεονεκτήματα : Οι χειριστές αποκτούν εγκαίρως πληροφορίες για αποτυχίες του

συστήματος, κλοπές αντικειμένων και ασυνήθιστες περιβαλλοντολογικές συνθήκες, έχοντας έτσι τη δυνατότητα να δράσουν νωρίς και να επιλύσουν τα όποια προβλήματα παρουσιαστούν.

Μειονεκτήματα : Η σφυγμομέτρηση καρτών :

- Μειώνει τη διάρκεια ζωής των μπαταριών ενεργητικών και ημι-ενεργητικών καρτών.
- Μπορεί να μην ανιχνεύσει κρίσιμα γεγονότα εάν η συχνότητα της όλης διαδικασίας είναι πολύ χαμηλή.
- Μπορεί να προκαλέσει κίνδυνο διαρροής επιχειρηματικών πληροφοριών εάν δώσει τη δυνατότητα σε ένα εχθρό να εκτελέσει ανάλυση επικοινωνίας, να ανιχνεύσει ή να στοχοποιήσει κάρτες, ενέργειες που δεν θα ήταν εφικτές αν οι κάρτες παρέμεναν σιωπηλές.
- Σε μερικές περιπτώσεις μπορεί να εξαπατηθεί, αν κάποιος αφαιρέσει την κάρτα από το αντικείμενο, πάρει το αντικείμενο και αφήσει την κάρτα σε σημείο όπου θα συνεχίζει να εκπέμπει σήματα της παρουσίας της.

⑩ Προστασία δεδομένων κάρτας

Οι επί του παρόντος διαθέσιμοι τεχνικοί έλεγχοι για την προστασία των δεδομένων μιας κάρτας είναι οι ακόλουθοι :

- Ο έλεγχος πρόσβασης στη μνήμη της κάρτας, ο οποίος μπορεί να περιορίσει τη χρήση εντολών στην κάρτα και να προστατεύσει τα δεδομένα που είναι αποθηκευμένα στη μνήμη της.
- Η απόκρυψη των δεδομένων της κάρτας.
- Η εντολή kill, που μπορεί να εμποδίσει τη διαδοχική μη εξουσιοδοτημένη χρήση της κάρτας.
- Η φυσική προστασία της κάρτας σε σχέση με το αντικείμενο με το οποίο είναι συνδεδεμένη.

Οι προαναφερθέντες έλεγχοι περιγράφονται με μεγαλύτερη λεπτομέρεια στη συνέχεια.

⑩ Έλεγχος πρόσβασης στη μνήμη της κάρτας

Περιγραφή Ελέγχου : Πολλές κάρτες υποστηρίζουν μία χαρακτηριστική λειτουργία κλειδώματος lock που προστατεύεται με κωδικό, η οποία παρέχει προστασία ανάγνωσης ή εγγραφής στη μνήμη. Σε κάποιες τεχνολογίες RFID η λειτουργία κλειδώματος είναι μόνιμη ενώ σε άλλες είναι αναστρέψιμη. Για παράδειγμα, στην EPC global Class-1 Generation-2 υπάρχουν πέντε περιοχές μνήμης που κάθε μία μπορεί να προστατευθεί με χρήση της εντολής lock. Η προστασία της μνήμης μπορεί να είναι είτε για ανάγνωση και εγγραφή είτε μόνο για εγγραφή ανάλογα με τις παραμέτρους που δίνονται μαζί με την εντολή. Το πρότυπο EPC global Class-1 Generation-2 UHF διαθέτει επίσης τη λειτουργία permalock, η οποία αν χρησιμοποιηθεί θα κάνει τη κατάσταση lock (κλειδωμένη ή ξεκλείδωτη) μόνιμη σε ολόκληρη ή σε ένα μέρος της μνήμης της κάρτας.

Επίσης, υπάρχει το πρότυπο ISO/IEC 18000-3 Mode 2 που υποστηρίζει προστασία ανάγνωσης και εγγραφής σε όλες τις περιοχές της μνήμης με ένα 48-bit κωδικό πρόσβασης. Ακόμα, το πρότυπο αυτό περιγράφει ένα “δείκτη κλειδώματος” (lock pointer) που είναι μία διεύθυνση μνήμης. Όλες οι περιοχές της μνήμης με χαμηλότερη διεύθυνση από το lock pointer έχουν προστασία εγγραφής ενώ οι περιοχές μνήμης που είναι πάνω από αυτόν δεν έχουν προστασία.

Η αποτελεσματικότητα των ελέγχων αυτού του είδους εξαρτάται από τη σωστή διαχείριση των κωδικών.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλο για όλες τις εφαρμογές που αποθηκεύουν δεδομένα στις κάρτες.

Πλεονεκτήματα : Μία εντολή προστασίας εγγραφής lock θα εμποδίσει την μεταβολή των περιεχομένων της μνήμης της κάρτας. Μία εντολή προστασίας

ανάγνωσης lock θα εμποδίσει τους μη εξουσιοδοτημένους χρήστες να διαβάσουν ή να αποκτήσουν πρόσβαση στα δεδομένα των καρτών.

Μειονεκτήματα : Υπάρχουν οι εξής αδυναμίες :

- Το μήκος λέξης των κωδικών που χρησιμοποιούν οι περισσότερες κάρτες είναι πολύ μικρό για να προσφέρει σημαντική προστασία πρόσβασης στη μνήμη. Ακόμα κι όταν η τεχνολογία υποστηρίζει μεγαλύτερο μήκος λέξης κωδικών, η διαχείριση των κωδικών είναι πολύπλοκη για διάφορους λόγους που έχουν ήδη εξηγηθεί σε προηγούμενο εδάφιο.

- Το κλείδωμα της μνήμης της κάρτας δεν εμποδίζει την απώλεια δεδομένων λόγω ηλεκτρομαγνητικής παρεμβολής ή φυσικής καταστροφής της κάρτας.

⑩ Απόκρυψη δεδομένων προ εγγραφής

Περιγραφή Ελέγχου : Η απόκρυψη των δεδομένων που αποθηκεύονται στην κάρτα γίνεται πριν αυτά εγγραφούν στην κάρτα. Έτσι ο έλεγχος δεν απαιτεί διαδικασίες απόκρυψης ή αποκωδικοποίησης των δεδομένων από αυτήν. Η απόκρυψη εκτελείται από τον αναγνώστη, το middleware ή κάποια άλλη συνιστώσα.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλος έλεγχος για όλες τις εφαρμογές που αποθηκεύουν πρόσθετα δεδομένα στην κάρτα πέραν του αριθμού ταυτοποίησης και πρέπει να διατηρηθούν εμπιστευτικά σε αυτήν. Αν οι λειτουργίες απόκρυψης και αποκωδικοποίησης των δεδομένων εκτελούνται στο backend, τότε απαιτείται πρόσβαση στο δίκτυο για να αναγνωσθεί το περιεχόμενο των δεδομένων που είναι αποθηκευμένα στην κάρτα. Η τελευταία απαίτηση καθιστά τον έλεγχο ακατάλληλο για κινητούς αναγνώστες οι οποίοι δεν έχουν πάντα πρόσβαση στο δίκτυο σε πραγματικό χρόνο.

Πλεονεκτήματα : Η απόκρυψη δεδομένων προστατεύει την πρόσβαση σε ευαίσθητα δεδομένα στην κάρτα από μη εξουσιοδοτημένα άτομα.

Μειονεκτήματα : Υπάρχουν τα πιο κάτω μειονεκτήματα :

- Η απόκρυψη δεδομένων χρειάζεται ένα σύστημα διαχείρισης κλειδιών το οποίο μπορεί να είναι πολύπλοκο στη διαχείριση και το χειρισμό του.
- Η αποστολή δεδομένων από την κάρτα σε στοιχεία του δικτύου για την κρυπτογράφηση ή αποκρυπτογράφησή τους, συνιστά μία λανθάνουσα κατάσταση η οποία σε συνδυασμό με το χρόνο που χρειάζεται για την ολοκλήρωση των κρυπτογραφικών λειτουργιών, μπορεί να παρουσιάσει μία μη αποδεκτή καθυστέρηση σε συστήματα RFID που απαιτούν πολύ γρήγορες συναλλαγές ανάγνωσης και εγγραφής.

⑩ Χαρακτηριστικό kill

Περιγραφή Ελέγχου : Η χρήση του χαρακτηριστικού kill με τη χρησιμοποίηση μιας εξ αποστάσεως εντολής καθιστά μόνιμα ανίκανη την κάρτα να λειτουργήσει. Η πιο κοινή υλοποίηση του χαρακτηριστικού αυτού είναι η εντολή EPC global "kill". Όταν χρησιμοποιηθεί μια τέτοια εντολή, η κάρτα απενεργοποιείται και δεν ανταποκρίνεται πλέον σε σήματα αναγνώστη. Οι εντολές kill συνοδεύονται από αντίστοιχους συνθηματικούς κωδικούς για να επιτραπεί η εκτέλεσή τους. Για παράδειγμα, υπάρχει η εντολή EPC global Class-1 Generation-2 kill που χρησιμοποιεί κωδικό 32-bit.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλος έλεγχος για εφαρμογές RFID που αντιμετωπίζουν κινδύνους διαρροής επιχειρηματικών πληροφοριών ή προσωπικών δεδομένων, όταν πλέον οι κάρτες έχουν εξυπηρετήσει τους λειτουργικούς σκοπούς για τους οποίους προορίζονταν. Για παράδειγμα, όταν οι κάρτες έχουν φύγει από την αλυσίδα προμηθειών όπου χρησιμοποιούνταν για απογραφές και άλλους ελέγχους δεν εξυπηρετούν πλέον άλλους σκοπούς λειτουργίας.

Πλεονεκτήματα : Η χρήση της εντολής kill εμποδίζει την ακατάλληλη ή μη εξουσιοδοτημένη επαναχρησιμοποίηση της κάρτας. Αρχικά, ο σχεδιασμός και η υλοποίηση του kill στις κάρτες EPC global, που είναι οι μόνες κάρτες βασισμένες σε

πρότυπο που υποστηρίζει εντολή kill, έγινε κυρίως για την προστασία των προσωπικών δεδομένων των καταναλωτών. Παρέχει όμως και προστασία από ακατάλληλη πρόσβαση στα δεδομένα καρτών που χρησιμοποιούνται στις επιχειρηματικές διαδικασίες. Για παράδειγμα, απορριφθείσες κάρτες από προϊόντα που ένας οργανισμός ή άτομο έχει αγοράσει ή χρησιμοποιεί, μπορεί να διαβαστούν από εχθρούς για την απόκτηση πρόσβασης σε δεδομένα.

Μειονεκτήματα : Υπάρχουν τα εξής μειονεκτήματα :

- Η ύπαρξη δυνατότητας εντολής kill αποτελεί σημαντική απειλή για ένα σύστημα RFID που χρησιμοποιείται για κάποια επιχειρηματική διαδικασία. Αν ένας εχθρός μάθει τον κωδικό για την εντολή kill, μπορεί να απενεργοποιήσει κάρτες που θα έπρεπε να βρίσκονται σε λειτουργία, με αποτέλεσμα η υποστηριζόμενη εφαρμογή να μην λειτουργεί κανονικά, εφόσον οι συναλλαγές με τις απενεργοποιημένες κάρτες δεν είναι δυνατό να γίνουν. Αυτός ο κίνδυνος γίνεται ιδιαίτερα αξιοπρόσεκτος αν έχει δοθεί ο ίδιος κωδικός σε πολλαπλές κάρτες, δίνοντας έτσι τη δυνατότητα σε κάποιο εχθρό που έχει μάθει ένα και μόνο κωδικό να απενεργοποιήσει μεγάλο αριθμό καρτών.

- Αφού έχει γίνει χρήση του kill, δεν μπορεί να χρησιμοποιηθεί η κάρτα σε περαιτέρω εφαρμογές που εμπλέκουν το αντίστοιχο αντικείμενο.

- Αν εκχωρηθεί ένας αδύναμος κωδικός, δηλαδή μικρού μήκους ή προβλέψιμος, για την εντολή kill, τότε μη εξουσιοδοτημένες πλευρές μπορούν να απενεργοποιήσουν την κάρτα αν το θελήσουν. Εκτός αυτού, όσο περισσότερο διάστημα διατηρείται ο ίδιος κωδικός, τόσο πιο πιθανή θα γίνεται η έκθεσή του.

- Τα αποθηκευμένα δεδομένα στην κάρτα παραμένουν στη μνήμη της και μετά τη χρήση του kill, αν και δεν μπορούν να προσπελαστούν ασύρματα. Επομένως κάποιος που έχει φυσική πρόσβαση στην κάρτα και διαθέτει τις κατάλληλες γνώσεις

και τον ειδικό εξοπλισμό που απαιτείται, μπορεί να προσπελάσει αυτά τα δεδομένα.

⓿ Παρόλο που η εντολή kill προστέθηκε στις κάρτες ως πιθανή λύση για κινδύνους που αφορούν προσωπικά δεδομένα, οι καταναλωτές δεν μπορούν εύκολα να εξακριβώσουν κατά πόσο η κάρτα έχει απενεργοποιηθεί. Επιπλέον, οι τυπικοί καταναλωτές δεν μπορούν εύκολα να χρησιμοποιήσουν την εντολή kill αφού η όλη διαδικασία απαιτεί τη χρήση ενός αναγνώστη και τη γνώση του κωδικού της εντολής kill.

⓾ Αντίσταση σε παραποιήσεις στην κάρτα

Περιγραφή Ελέγχου : Συγκεκριμένου τύπου κάρτες RFID διαθέτουν τρόπους αντίστασης σε παραποιήσεις στην κάρτα, που βοηθούν ως προληπτικό μέτρο για εχθρικές προσπάθειες μεταβολής των καρτών ή αφαίρεσής τους από τα αντικείμενα στα οποία είναι προσαρτημένες. Ένας απλός τύπος αντίστασης είναι η χρήση μίας εύθραυστης κεραίας. Αν μια κάρτα αυτού του τύπου αφαιρεθεί, σπάζει η κεραία και ως εκ τούτου η ηλεκτρική σύνδεση με την κεραία γίνεται δύσκολη με αποτέλεσμα η κάρτα να μην μπορεί να λειτουργήσει. Επίσης, με τη χρήση παρόμοιων μεθόδων ένα πολύπλοκο σύστημα RFID μπορεί να παρακολουθήσει και να ελέγξει τα αντικείμενα που σχετίζονται με τις κάρτες, εξασφαλίζοντας ότι τα αντικείμενα δεν έχουν παραποιηθεί, μεταβληθεί ή υποβληθεί σε ακραίες συνθήκες.

Εφαρμοσιμότητα Ελέγχου : Κατάλληλη μέθοδος για εφαρμογές στις οποίες οι κάρτες βρίσκονται συχνά εκτός του άμεσου ελέγχου του οργανισμού που υλοποιεί την εφαρμογή και συνεπώς είναι ευάλωτες σε παραποιήσεις. Οι μέθοδοι αυτού του τύπου είναι διαθέσιμες μόνο σε ειδικές κάρτες RFID που έχουν σχεδιαστεί για την υποστήριξη συγκεκριμένων αγοραστικών απαιτήσεων.

Πλεονεκτήματα : Ο έλεγχος βοηθά στην παρεμπόδιση εχθρικών προσπαθειών αποσύνδεσης της κάρτας από το αντίστοιχο αντικείμενο. Η χρήση πιο πολύπλοκων

καρτών αυτού του είδους παρέχει καλύτερη ικανότητα παρακολούθησης της κατάστασης των σχετικών αντικειμένων ώστε να εξασφαλιστεί ότι αυτά δεν έχουν ανοιχτεί, παραποιηθεί, καταστραφεί ή υποβληθεί σε ακραία θερμοκρασία, υγρασία ή κάποιο δυνατό χτύπημα.

Μειονεκτήματα : Κάποιοι έμπειροι εχθροί ίσως να έχουν την ικανότητα να ανατρέψουν τους μηχανισμούς αντίστασης της κάρτας επιδιορθώνοντας, για παράδειγμα, την εύθραυστη κεραία της. Επίσης, οι μέθοδοι αυτές δεν αποτρέπουν την κλοπή ή καταστροφή της κάρτας ή των αντίστοιχων αντικειμένων.

ΑΝΑΦΟΡΕΣ

Βιβλιογραφία

[1] “Συστήματα RFID: Θέματα ασφάλειας και ιδιωτικότητας”, Πτυχιακή, Κλεάνθης Κουλλάπης, Δεκέμβριος 2009

[2] Center for Democracy and Technology, "CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology," Interim Draft, May 1, 2006, http://www.cdt.org/privacy/20060501rfid-best-practices.php

[3] EPCglobal, "Guidelines on EPC for Consumer Products," September 2005, http://www.epcglobalinc.org/public/ppsc_guide/

[4] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Radio Frequency Identification (RFID) Policy," July 2004, http://www.acq.osd.mil/log/rfid/Policy/RFID%20Policy%2007-30-2004.pdf

[5] Privacy Rights Clearinghouse, "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations," November 20, 2003, http://www.privacyrights.org/ar/RFIDposition.htm

[6] Guidelines for Securing Radio Frequency Identification (RFID) Systems, http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

[7] K. Finkenzeller, RFID Handbook: Fundamentals and applications in contactless smart cards and identification, 2nd edition.: John Wiley & Sons Ltd., 2003.

[8] S. Garfinkel, Ed., and B. Rosenberg, Ed., RFID Applications, Security, and Privacy. Upper Saddle River, New Jersey: Pearson Education, Inc., 2006.

[9] S. Lahiri, RFID Sourcebook. Pearson Education, 2005.

Ιστοσελίδες

[10] “ RFID Journal ”, http://www.rfidjournal.com/

[11] “ EPCglobal ” , http://www.epcglobalinc.org/

[12] “Auto-ID Labs ”, http://www.autoidlabs.org/

ΚΕΦΑΛΑΙΟ 5

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΧΡΗΣΗΣ

1. Γενικά

Στα πλαίσια του στυλ ανάλυσης Dolev-Yao για πρωτόκολλα ασφαλείας, θα διερευνηθούν εδώ οι αξιώσεις ασφαλείας ενός προτεινόμενου ως ισχυρού RFID πρωτοκόλλου αυθεντικοποίησης. Επιδεικνύεται ένα σφάλμα που έχει περάσει απαρατήρητο και παρουσιάζονται οι επακόλουθες επιθέσεις στην αυθεντικοποίηση, τη μη ιχνηλασιμότητα και την αντίσταση στους αποσυγχρονισμούς. Επίσης, αναλύονται και συζητούνται οι αποδείξεις ασφαλείας των συγγραφέων και γίνονται αναφορές σε άλλα ευάλωτα πρωτόκολλα. Τέλος, παρουσιάζεται ένα πρωτόκολλο χαμηλού κόστους και ισχυρής ασφάλειας που διορθώνει το σφάλμα αυτό.

2. Εισαγωγή

Οι υπολογιστικοί περιορισμοί των καρτών RFID επιβάλουν σημαντικούς περιορισμούς στον αριθμό και το είδος των κρυπτογραφικών αρχών που μπορούν να εφαρμοστούν σε αυτές. Επομένως, είναι ένα λεπτό ζήτημα η επίτευξη ισχυρής αυθεντικοποίησης και ιδιοτήτων μη ιχνηλασιμότητας με απλές αρχές κρυπτογράφησης. Σε μια επικοινωνία με έναν αναγνώστη RFID, τα μηνύματα μιας κάρτας θα πρέπει να μεταδίδουν επαρκείς πληροφορίες ώστε ο αναγνώστης να είναι σε θέση να πιστοποιήσει την αυθεντικότητα της κάρτας, χωρίς να αποκαλύπτουν τίποτα που θα επέτρεπε σε έναν επιτιθέμενο να αναγνωρίσει την κάρτα. Επιπροσθέτως, για να επιτευχθεί μεγάλης κλίμακας ανάπτυξη, ο αναγνώστης θα πρέπει να μπορεί να αυθεντικοποιήσει αποτελεσματικά την κάρτα χρησιμοποιώντας τις παρεχόμενες πληροφορίες. Έτσι, οι κάρτες και επομένως τα πρωτόκολλα που αυτές τρέχουν, πρέπει να ικανοποιούν διάφορες αντιφατικές απαιτήσεις.

Κατά συνέπεια, υπάρχει μια μεγάλη ποικιλία προτάσεων που αποσκοπούν στην επίτευξη ασφαλών, μη ανιχνεύσιμων και αποτελεσματικών πρωτοκόλλων με χρήση των περιορισμένων πηγών που είναι διαθέσιμες σήμερα για τις κάρτες RFID, π.χ. [7, 8, 21, 34, 36]. Ο σημαντικός αριθμός των δημοσιεύσεων που αναφέρονται σε τέτοια πρωτόκολλα, για παράδειγμα [3, 4, 6, 13, 32], δείχνει ότι ο σχεδιασμός πρωτοκόλλων RFID με περιορισμένους πόρους δεν είναι ακόμα καλά κατανοητός.

Αυτό το κεφάλαιο αναφέρεται στο πρωτόκολλο αυθεντικοποίησης RFID που προτείνεται στο [12], το οποίο και θα αποκαλείται HNMB από τα επώνυμα των συγγραφέων. Το πρωτόκολλο αυτό είναι ενδιαφέρον για διάφορους λόγους. Ενώ υπάρχει μια τάση στα προσφάτως προταθέντα πρωτόκολλα να χρησιμοποιούν μη συνηθισμένες κατασκευές, όπως τελεστές με αλγεβρικές ιδιότητες [4, 22, 34], τροποποιημένες μεθόδους hash [7], ακόμα και περιορισμένη σε πόρους κρυπτογραφία δημόσιου κλειδιού [23] για να εκπληρώσουν τις αυστηρές απαιτήσεις των πρωτοκόλλων RFID, το πρωτόκολλο HNMB χρησιμοποιεί μόνο συνηθισμένες τεχνικές. Παρ' όλα αυτά, ένα απλό σφάλμα εκθέτει σε κίνδυνο τους τρεις σχεδιαστικούς στόχους, αυθεντικοποίηση, μη ιχνηλασιμότητα και αντίσταση στους αποσυγχρονισμούς. Επιπλέον, όπως αναφέρεται και στα συμπεράσματα του κεφαλαίου, οι επακόλουθες επιθέσεις σε αυτό το πρωτόκολλο είναι διαφορετικές από επιθέσεις σε άλλα πρωτόκολλα RFID.

3. Περιγραφή πρωτοκόλλου

Αρχικά, επεξηγείται η ορολογία και το μοντέλο επίθεσης και στη συνέχεια περιγράφεται το πρωτόκολλο HNMB.

Στα επόμενα, ως αναγνώστης αναφέρεται ένας πραγματικός αναγνώστης RFID καθώς επίσης και η βάση δεδομένων που επικοινωνεί με αυτόν, εφόσον η επικοινωνία λαμβάνει χώρα σε ασφαλές κανάλι. Σαν *πράκτορας* αναφέρεται είτε μια κάρτα είτε ένας αναγνώστης, ενώ ένας *ρόλος* αναφέρεται στα βήματα που πρέπει να εκτελέσει ένας πράκτορας. Μια *εκτέλεση* είναι η εκτέλεση ενός ρόλου από έναν πράκτορα.

Υιοθετείται ένα τυπικό μοντέλο εισβολής Dolev-Yao στο οποίο ο επιτιθέμενος ελέγχει το δίκτυο. Ενώ μπορεί να υπάρχουν επιθέσεις σε αυτό το μοντέλο που δεν είναι εφικτές σε ένα σύστημα RFID πραγματικού κόσμου, αυτό είναι το πιο ώριμο μοντέλο επίθεσης. Επιπλέον, η εφικτότητα μιας επίθεσης δεν εξαρτάται μόνο απ' το μοντέλο επίθεσης, αλλά και από τις συνθήκες κάτω από τις οποίες χρησιμοποιείται ένα σύστημα. Επομένως, για κάθε μια από τις επιθέσεις που παρουσιάζονται στα επόμενα, επεξηγείται και ένα σενάριο στο οποίο μπορεί να πραγματοποιηθεί. Στην επεξήγηση ενός συγκεκριμένου σεναρίου επίθεσης γίνεται λόγος για έναν ή περισσότερους επιτιθέμενους που εκτελούν την επίθεση. Έτσι, ένας θεωρητικός επιτιθέμενος ενσωματώνει έναν ή περισσότερους πραγματικούς.

Απόκριση κάρτας	Ενημέρωση
h(ID), nt	ID′ := ID; ID := h(ID, nr); HID := h(ID)
h(ID, nt, nr), nt	ID′ := ID; ID := h(ID, nr); HID := h(ID)
h(ID′, nt, nr), nt	ID := h(ID′, nr); HID := h(ID)
άλλη	απόρριψη κάρτας

Πίνακας 1. Διαδικασία επαλήθευσης και ανανέωσης αναγνώστη στο πρωτόκολλο HNMB

Το πρωτόκολλο HNMB στοχεύει στην αμοιβαία αυθεντικοποίηση κάρτας και αναγνώστη, στη διατήρηση της κάρτας ως μη ανιχνεύσιμης και στην αντίσταση σε ένα συγκεκριμένο είδος επιθέσεων άρνησης υπηρεσίας (denial-of-service), γνωστές ως επιθέσεις αποσυγχρονισμού. Επιπλέον, έχει σχεδιαστεί με περιορισμένες υπολογιστικές απαιτήσεις στις κάρτες, χρησιμοποιώντας μια συνάρτηση κατακερματισμού σαν τη μόνη μέθοδο κρυπτογράφησης. Η αποτελεσματικότητα του αναγνώστη εξετάζεται όπως περιγράφεται στα ακόλουθα.

Το πρωτόκολλο υποθέτει ότι ο αναγνώστης R και η κάρτα T μοιράζονται ένα μυστικό κωδικό ID, ο οποίος ανανεώνεται στο τέλος μιας επιτυχημένης εκτέλεσης του πρωτοκόλλου. Για λόγους αποδοτικότητας, ο αναγνώστης αποθηκεύει το hash του ID στη μεταβλητή HID και την τιμή του ID πριν την τελευταία ενημέρωση στο ID'. Επιπροσθέτως, η κάρτα παρακολουθεί αν η τελευταία εκτέλεση τελείωσε επιτυχώς ή όχι. Γι' αυτό το σκοπό χρησιμοποιείται η μεταβλητή S.

Το πρωτόκολλο ξεκινά με τον αναγνώστη να αποστέλλει στην κάρτα ένα nonce[1] nr. Η κάρτα τότε παράγει ένα nonce nt. Η απάντηση της κάρτας εξαρτάται από την τιμή του S. Σε περίπτωση που η προηγούμενη εκτέλεση ολοκληρώθηκε με επιτυχία, η τιμή του S είναι 0 και η κάρτα απαντά με το (h(ID), nt) επιτρέποντας έτσι στον αναγνώστη να αναζητά την κάρτα συνεχώς. Στην περίπτωση που δεν ολοκληρώθηκε επιτυχώς, η τιμή του S είναι 1 και η κάρτα απαντά με το (h(ID, nt, nr), nt). Αυτή η περίπτωση όμως θα πρέπει να συμβαίνει σπάνια. Σε οποιαδήποτε από τις δυο περιπτώσεις η κάρτα θέτει το S σε 1. Ο αναγνώστης αποδέχεται την κάρτα αν η απάντηση, εκτός από το nonce nt, ισούται με HID, (h(ID), nt) ή (h(ID, nt, nr), nt) για όποια αποθηκευμένη τιμή του HID, ID ή ID'. Ο αναγνώστης ενημερώνει, τότε, τις πληροφορίες για την κάρτα σύμφωνα με τον πίνακα 1 και στέλνει το h(ID', nt) στην κάρτα. Τέλος, αν το ληφθέν μήνυμα ταιριάζει με το h(ID, nt), η κάρτα αντικαθιστά το ID της με το h(ID, nr) και θέτει το S ίσο με 0. Το πρωτόκολλο απεικονίζεται σαν διάγραμμα αλληλουχίας μηνυμάτων στο σχήμα 1.

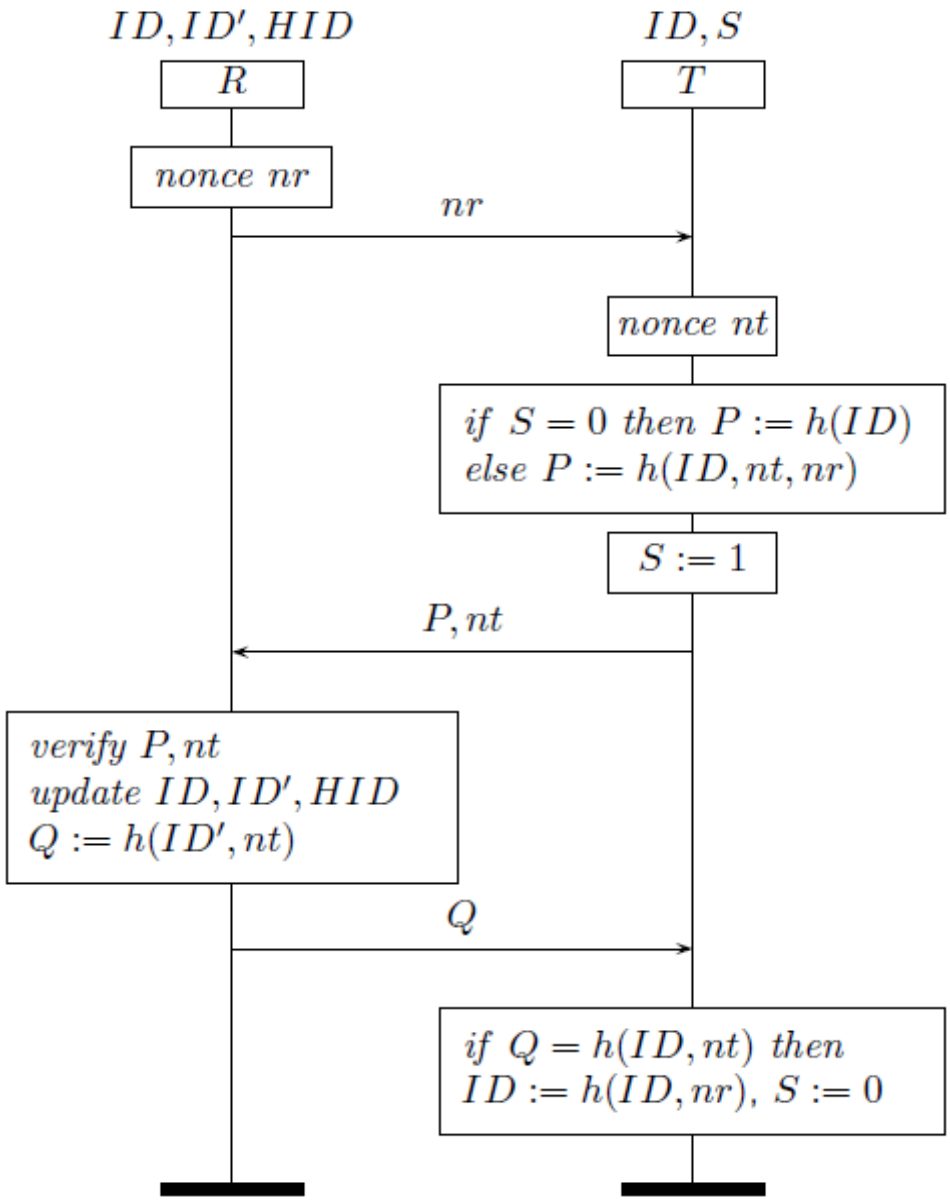
Το διάγραμμα αυτό δείχνει τα ονόματα των ρόλων, σε πλαίσια, στην κορυφή του. Πάνω από τα ονόματα φαίνονται οι μυστικοί όροι των ρόλων. Ενέργειες όπως παραγωγή nonce, υπολογισμός, επαλήθευση όρων και εκχωρήσεις τιμών παρουσιάζονται σε ορθογώνια. Μηνύματα που αποστέλλονται και αναμένεται να ληφθούν, προσδιορίζονται πάνω από τα βέλη που συνδέουν τους ρόλους. Ισχύει η υπόθεση ότι ένας πράκτορας συνεχίζει την εκτέλεσή του, μόνο αν λαμβάνει κάποιο μήνυμα που να συμμορφώνεται με τις προδιαγραφές.

4. Πιστοποίηση

Όταν κάποιος ασχολείται με τις ιδιότητες της αυθεντικοποίησης, πρέπει να καταστήσει σαφές ποια συγκεκριμένη μορφή πιστοποίησης υιοθετείται. Υπό την έννοα της ιεραρχίας αυθεντικοποίησης του Lowe [29], θεωρείται ότι η *πρόσφατη ζωτικότητα* (recent aliveness) είναι η πιο κατάλληλη απαίτηση πιστοποίησης για

[1]Στη μηχανική ασφαλείας, nonce είναι συντόμευση για τη φράση number once used (αριθμός μιας χρήσης). Συνήθως είναι ένας τυχαίος ή ψευδο-τυχαίος αριθμός που εκδίδεται από ένα πρωτόκολλο πιστοποίησης, για να εξασφαλίσει ότι παλιές επικοινωνίες δε μπορούν να χρησιμοποιηθούν σε επιθέσεις επανάληψης.

πρωτόκολλα RFID. Η απαίτηση αυτή συλλαμβάνει το γεγονός ότι μια κάρτα πρέπει να δημιουργήσει ένα μήνυμα ως συνέπεια της ερώτησης ενός αναγνώστη. Πιο επίσημα, ένα πρωτόκολλο εγγυάται σε έναν πράκτορα a που έχει ένα ρόλο A, ότι οποιοσδήποτε αντίστοιχος πράκτορας b ήταν πρόσφατα "ζωντανός", αν και μόνο αν οποτεδήποτε ο a ολοκληρώνει μια εκτέλεση, έχει υπάρξει ένα γεγονός του b κατά τη διάρκεια αυτής της εκτέλεσης.



Σχήμα 1. Το πρωτόκολλο HNMB

Πρέπει να σημειωθεί εδώ πως κάποια ασθενέστερη ιδιότητα αυθεντικοποίησης από την πρόσφατη ζωτικότητα, θα έπρεπε να έχει και ασθενέστερη απαίτηση του

πρόσφατου. Έτσι κάποιος έπαιρνε μια ιδέα της ζωντάνιας που απλώς θα εγγυώταν ότι μια κάρτα δεν έχει υπάρξει ποτέ ζωντανή. Σε αυτή την περίπτωση, μια επίθεση επανάληψης δε θα ακύρωνε την αξίωση της ασφάλειας. Εφόσον, για το πρωτόκολλο υπό μελέτη έχει δηλωθεί σαφώς ότι οι επιθέσεις επανάληψης δεν είναι επιθυμητές, βγαίνει το συμπέρασμα ότι οι συγγραφείς είχαν ως πρόθεση μια ιδέα πιστοποίησης η οποία είναι τουλάχιστον τόσο δυνατή όσο και η "πρόσφατη ζωτικότητα".

4.1 Η επίθεση

Είναι ευρέως γνωστό ότι για να υπάρξει "πρόσφατη ζωτικότητα" σε ένα πρωτόκολλο ερώτησης – απόκρισης, η ερώτηση και η απόκριση πρέπει να σχετίζονται [1, 11, 18, 19]. Ωστόσο, πρέπει να παρατηρηθεί εδώ ότι, αν κανένα μήνυμα δεν μπλοκαριστεί ή χαθεί στο πρωτόκολλο HNMB, η κάρτα απαντά πάντα σε ερώτηση ενός αναγνώστη με το h(ID), το οποίο δεν εξαρτάται από την ερώτηση. Ενώ αυτή η κατασκευή επιτρέπει την αποτελεσματική αναζήτηση από τον αναγνώστη, αν μια κάρτα είναι στην κατάσταση S = 0, το πρωτόκολλο δεν παρέχει αυθεντικοποίηση της κάρτας. Ένας επιτιθέμενος μπορεί να υποδυθεί οποιαδήποτε κάρτα βρίσκεται στην κατάσταση S = 0 στέλνοντας μια ερώτηση σε αυτή και επαναλαμβάνοντας την απάντησή της σε κάποιον αναγνώστη, πριν η κάρτα προλάβει να ερωτηθεί από κάποιον εξουσιοδοτημένο αναγνώστη. Σε κάποιο σενάριο όπου οι κάρτες χρησιμοποιούνται για έλεγχο πρόσβασης, ένας επιτιθέμενος θα μπορούσε να χρησιμοποιήσει έναν παράνομο αναγνώστη για να "ρωτήσει" διάφορες κάρτες. Από ένα ικανοποιητικά μεγάλο αριθμό καρτών, είναι πιθανό ότι θα υπάρχουν αρκετές κάρτες που θα βρίσκονται στην κατάσταση S = 0. Στην πραγματικότητα, το πρωτόκολλο είναι σχεδιασμένο με την υπόθεση ότι οι περισσότερες κάρτες βρίσκονται σε αυτή την κατάσταση. Εάν ο επιτιθέμενος χρονομετρήσει σωστά την επίθεση, για παράδειγμα ερωτώντας κάρτες όταν κάποιος φεύγει από μια απαγορευμένη περιοχή ή επιστρέφει αντικείμενα υπό έλεγχο πρόσβασης, είναι πιθανό ότι θα μπορεί επαναλάβει τα συλληφθέντα μηνύματα στον πιστοποιημένο αναγνώστη, πριν η κάρτα του θύματος επιστρέψει στην εμβέλειά του.

Για να εκτελέσει αυτή την επίθεση, ο επιτιθέμενος μπορεί να εγκαταστήσει μια συσκευή ανάγνωσης σε σημείο όπου αναμένει ότι θα είναι σε θέση να "ρωτήσει" κάποια κάρτα που θέλει να προσωποποιηθεί. Η συσκευή αυτή δεν είναι υποχρεωμένη να υπακούει στους επίσημους κανονισμούς που περιορίζουν την εμβέλεια της επικοινωνίας των συστημάτων RFID. Από τη στιγμή που δεν είναι απαραίτητη η φυσική επαφή ή ακόμη και καθαρό οπτικό πεδίο μεταξύ αναγνώστη – κάρτας, η επικοινωνία είναι πολύ πιθανό να περάσει απαρατήρητη από τον κάτοχο της κάρτας. Αφού λάβει την απάντηση της κάρτας, ο επιτιθέμενος μπορεί να κατασκευάσει μια κάρτα που να στέλνει το συλληφθέν μήνυμα όταν ερωτάται από μια νόμιμη συσκευή ανάγνωσης.

Το ίδιο είδος σφάλματος υπάρχει και σε άλλα πρωτόκολλα. Τα πρωτόκολλα στα [10, 26, 27, 28] είναι βασισμένα σε ερωτήσεις – αποκρίσεις, στα οποία η απάντηση δεν εξαρτάται από την ερώτηση. Έτσι, τα πρωτόκολλα αυτά περιέχουν ένα παρόμοιο σφάλμα πιστοποίησης το οποίο μέχρι σήμερα έχει περάσει απαρατήρητο.

4.2 Το σφάλμα στην ανάλυση ασφαλείας

Στη βασική ανάλυση ασφαλείας του HNMB, αρχικά διαπιστώνεται ότι ο επιτιθέμενος δε μπορεί να υπολογίσει το ID της κάρτας από παρατηρούμενα μηνύματα. Έπειτα, δηλώνεται ότι το h(ID) δε μπορεί να υπολογιστεί χωρίς τη γνώση του ID. Οι συγγραφείς, τότε, χρησιμοποιούν το γεγονός ότι το ID ενημερώνεται στο τέλος του πρωτοκόλλου για να ισχυριστούν ότι η γνώση του h(ID) που μπορεί να έχει ο επιτιθέμενος, είναι άχρηστη για τη μίμηση μιας κάρτας. Η ιδέα πίσω από αυτή τη λογική είναι ότι ο επιτιθέμενος μπορεί να παρατηρήσει το h(ID) κατά τη διάρκεια μιας επικοινωνίας μεταξύ κάρτας – αναγνώστη, αλλά δε θα μπορεί να το χρησιμοποιήσει για να υποδυθεί την κάρτα, αφού αυτή και ο αναγνώστης θα έχουν ανανεώσει την τιμή του ID στο τέλος της επικοινωνίας τους.

Η λογική αυτή ισχύει μόνο εφόσον το h(ID) δε μπορεί να παρατηρηθεί από τον αντίπαλο ελλείψει αξιόπιστου αναγνώστη. Όπως δείχνει και η επίθεση στην προηγούμενη υποενότητα, ο επιτιθέμενος μπορεί απλά να υποβάλει ένα ερώτημα σε

μια κάρτα για να αποκτήσει το h(ID). Αν δεν υπάρχει κάποιος αξιόπιστος αναγνώστης, τότε δεν υπάρχει επικοινωνία μεταξύ κάρτας – αναγνώστη και επομένως ο αναγνώστης δε μπορεί να ενημερώσει το ID. Έτσι ο αντίπαλος μπορεί να χρησιμοποιήσει το h(ID) για να μιμηθεί την κάρτα.

5. Μη ανιχνευσιμότητα

Η συνεχής παρουσία και η δυνατότητα ασύρματης επικοινωνίας των καρτών RFID, διευκολύνουν και ενθαρρύνουν την ανίχνευσή τους μέσω του χώρου και του χρόνου. Από την άποψη της ιδιωτικότητας, αυτό είναι εξαιρετικά ανεπιθύμητο. Ένα πρωτόκολλο προσφέρει μη ιχνηλασιμότητα, αν ένας αντίπαλος δεν είναι σε θέση να αναγνωρίσει μια κάρτα που έχει προηγουμένως παρατηρήσει. Για πρωτόκολλα που βασίζονται στην κατάσταση, όπως το HNMB, εξυπακούεται ότι ο αντίπαλος δε θα έπρεπε να μπορεί να παρατηρήσει σε ποια κατάσταση είναι μια συγκεκριμένη κάρτα.

Επίσημοι ορισμοί της έννοιας την μη ιχνηλασιμότητας έχουν προταθεί στα [3, 6, 17]. Το HNMB, υπάρχει η αξίωση ότι είναι μη ανιχνεύσιμο με βάση τον ορισμό στο [17], όπου η μη ανιχνευσιμότητα ορίζεται υπό την έννοια πειραμάτων μυστικότητας. Ένα τέτοιο RFID πείραμα ιδιωτικότητας αποτελείται από δυο φάσεις. Στη φάση εκμάθησης, ο αντίπαλος A μπορεί να ξεκινήσει μια επικοινωνία με τον αναγνώστη R (ReaderInit) ή τις κάρτες T (TagInit), μετά την οποία μπορεί να αλληλεπιδράσει μαζί τους. Ο αναγνώστης και οι κάρτες απαντούν ανάλογα με τις προδιαγραφές του πρωτοκόλλου. Στη φάση ερωτήσεων, ο αντίπαλος επιλέγει δυο υποψήφιες κάρτες Ti και Tj. Τότε μια απ' τις δυο αυτές κάρτες επιλέγεται τυχαία (αναφέρεται ως T*) και ο A αποκτά πρόσβαση στην κάρτα. Ο αντίπαλος μπορεί και πάλι να αλληλεπιδράσει με τον αναγνώστη και τις κάρτες και πρέπει τότε να αποφασίσει αν η επιλεγμένη κάρτα είναι Ti ή Tj. Αν ο επιτιθέμενος έχει κάποιο μη αμελητέο πλεονέκτημα στην επιτυχή εικασία της επιλεγμένης κάρτας, τότε το πρωτόκολλο δεν είναι μη ανιχνεύσιμο.

Οι συγγραφείς του HNMB ισχυρίζονται ότι το πρωτόκολλο παρέχει μη ιχνηλασιμότητα, επειδή η κάρτα δε στέλνει ποτέ την ίδια απάντηση δυο φορές. Παρέχουν μια επίσημη απόδειξη της ιδιότητας αυτής τον ορισμό της ισχυρής

ιδιωτικότητας του [17] που επεξηγήθηκε παραπάνω. Στα επόμενα γίνεται επίδειξη ενός αλγορίθμου που αποδεικνύει ότι το πρωτόκολλο δεν είναι μη ανιχνεύσιμο και ο οποίος δίνει στον επιτιθέμενο ένα ισχυρό πλεονέκτημα στο να μαντέψει την επιλεγμένη κάρτα. Έπειτα αναλύεται το σφάλμα της ανάλυσης ασφαλείας στο HNMB.

5.1 Η επίθεση

Στο πρωτόκολλο HNMB, η απάντηση της κάρτας στην ερώτηση ενός αναγνώστη, εξαρτάται από την κατάστασή της στην αρχή του πρωτοκόλλου. Υπενθύμιση εδώ ότι η κατάσταση της κάρτας παριστάνεται απ' το S. Αν το S = 0, η κάρτα απαντά με το h(ID), nt, αλλιώς απαντά με το h(ID, nt, nr), nt. Αφού ο αντίπαλος δε γνωρίζει το ID, δε μπορεί να συμπεράνει απ' την απάντηση της κάρτας σε ποια κατάσταση αυτή ήταν. Ωστόσο, ο επιτιθέμενος μπορεί να εκμεταλλευτεί την δυνατότητα του αναγνώστη να διακρίνει τις δυο καταστάσεις μεταξύ τους. Αν η κάρτα βρισκόταν στην κατάσταση S = 0 στην αρχή του πρωτοκόλλου, η συσκευή ανάγνωσης δε μπορεί να επαληθεύσει αν η τιμή του nonce nt άλλαξε κατά τη διάρκεια της μετάδοσης. Έτσι, μια κατά λάθος ή κακόβουλη τροποποίηση του nt δεν οδηγεί σε απόρριψη της απάντησης της κάρτας από τον αναγνώστη, ο οποίος ολοκληρώνει την εκτέλεσή του στέλνοντας το τρίτο μήνυμα του πρωτοκόλλου. Αν η κάρτα ήταν στην κατάσταση S = 1, ο αναγνώστης χρησιμοποιεί το nr το δικό του nonce nt και το ID για να υπολογίσει μια τιμή hash και να τη συγκρίνει με αυτή που έλαβε. Σε αυτή την περίπτωση, η τροποποίηση του nt μπορεί να ανιχνευθεί και οδηγεί στην απόρριψη της απάντησης της κάρτας και την πρόωρη ολοκλήρωση της εκτέλεσης από τον αναγνώστη.

Υπό την έννοια των πειραμάτων ιδιωτικότητας, η στρατηγική του αντιπάλου είναι ως ακολούθως: Στη φάση εκμάθησης, επιλέγονται δυο κάρτες Ti και Tj και η Ti τίθεται στην κατάσταση S = 1. Ο επιτιθέμενος μπορεί να το κάνει αυτό κάνοντας μια ερώτηση στην Ti και τερματίζοντας το πρωτόκολλο πριν την αποστολή του τρίτου μηνύματος. Η φάση αυτή επιδεικνύεται στον Αλγόριθμο 1.

Αλγόριθμος 1 *Φάση 1: Φάση εκμάθησης*
Ο Α επιλέγει ένα ζευγάρι διακριτών καρτών Ti και Tj στην τύχη.
Ο Α εκκινεί την επικοινωνία με τον R χρησιμοποιώντας τη ReaderInit και αποκτά το nr της ερώτησης.
Ο Α εκκινεί την επικοινωνία με την Ti χρησιμοποιώντας τη TagInit
Ο Α στέλνει το nr στην Ti.

Στη φάση ερωτήσεων ο αντίπαλος εκτελεί μια επίθεση ενδιάμεσου (man-in-the-middle). Αποκτά μια ερώτηση από τον αναγνώστη και τη στέλνει στην κάρτα για να αποκτήσει μια απάντηση. Αντικαθιστά, τότε, το nonce που έλαβε απ' την κάρτα με μια διαφορετική τιμή και υποβάλει την απάντηση στον αναγνώστη. Αν αυτός κάνει αποδεκτή την απάντηση, αυτό σημαίνει ότι η κάρτα ήταν στην κατάσταση S = 0 και ως εκ τούτου η επιλεγμένη κάρτα είναι η Tj. Αν η συσκευή ανάγνωσης απορρίψει την απάντηση, η κάρτα βρισκόταν στην κατάσταση S = 1 και η επιλεγμένη κάρτα είναι η Ti. Η φάση αυτή επιδεικνύεται στον Αλγόριθμο 2.

Αλγόριθμος 2 *Φάση 2: Φάση ερωτήσεων*
Ο Α υποβάλει τις Ti και Tj ως τις υποψήφιές του για ερωτήσεις.
Ο Α εκκινεί την επικοινωνία με τον R χρησιμοποιώντας τη ReaderInit και αποκτά ένα nr ερώτησης.
Ο Α μεταβιβάζει το nr αυτό του R στην επιλεγμένη κάρτα T.*
Ο Α τροποποιεί την απάντηση της T από (P, nt) σε (P, nr) και τη στέλνει στον R.*
Αν ο R δεχτεί την απάντηση, ο Α υποθέτει ότι T = Tj, αλλιώς υποθέτει T* = Ti.*

Επειδή αυτή είναι μια επίθεση ενδιάμεσου, είναι εφικτή σε ένα σενάριο όπου μπορούμε να υποθέσουμε ότι ο αντίπαλος έχει ταυτόχρονη πρόσβαση σε έναν νόμιμο αναγνώστη και σε μια κάρτα που δεν είναι εντός της εμβέλειάς του. Δουλεύει καλύτερα, αν όλες ή οι περισσότερες κάρτες βρίσκονται στην κατάσταση S = 0, εκτός αν έχουν τροποποιηθεί από κάποιον επιτιθέμενο. Αυτό σημαίνει ότι είτε

υπάρχει ένας επιτιθέμενος που αλλάζει τις καταστάσεις των καρτών ή ότι όλοι οι επιτιθέμενοι συνωμοτούν. Ο επιτιθέμενος θα έθετε τις κάρτες προς εντοπισμό στην κατάσταση S = 1 "ρωτώντας" κάθε μια από αυτές, χωρίς όμως να στείλει το τρίτο μήνυμα του πρωτοκόλλου. Κατά τη διάρκεια του σταδίου αναγνώρισης, όταν η κάρτα βρίσκεται κοντά στον αντίπαλο, η επίθεση ενδιάμεσου εκτελείται προωθώντας μηνύματα μεταξύ κάρτας κι αναγνώστη. Αν η τροποποίηση του nt στο δεύτερο μήνυμα οδηγήσει σε απόρριψη απ' τον αναγνώστη, ο αντίπαλος αναγνωρίζει την κάρτα.

5.2 Το σφάλμα στην ανάλυση ασφαλείας

Για να επιβεβαιωθεί ότι το πρωτόκολλο ικανοποιεί τον ορισμό της ιδιωτικότητας που δηλώνεται στο [17], όλες οι πιθανές αλληλεπιδράσεις με τις λειτουργίες κάρτας και αναγνώστη πρέπει να ληφθούν υπόψιν.

Οι συγγραφείς παρέχουν αποδείξεις ασφαλείας ότι ο αντίπαλος δε μπορεί να προσδιορίσει το ID από το πρώτο και το δεύτερο μήνυμα με μεγάλο πλεονέκτημα, χρησιμοποιώντας τις λειτουργίες τις κάρτας. Ωστόσο, οι αποδείξεις αυτές δε λαμβάνουν υπόψη τις λειτουργίες του αναγνώστη.

Όπως δείχνεται και παραπάνω, χρησιμοποιώντας τη λειτουργία του αναγνώστη που ξεκινά με τη ReaderInit, ο αντίπαλος έχει ένα σημαντικό πλεονέκτημα να μαντέψει την επιλεγμένη κάρτα. Στην πραγματικότητα, η πιθανότητα σωστής εικασίας της κάρτας είναι 1.

Ένα σχετικό σφάλμα είχε βρεθεί από τον Avoine [4] στο πρωτόκολλο στο [14]. Ο Avoine σπάζει τη μη ανιχνευσιμότητα μιας κάρτας, αυξάνοντας τον εσωτερικό της μετρητή σε μεγάλο επίπεδο, ώστε να την αναγνωρίσει αργότερα.

6. Αποσυγχρονισμός

Η εισαγωγή διαφόρων εννοιών ασφαλείας όπως *μη ιχνηλασιμότητα* και *προς τα εμπρός μη ιχνηλασιμότητα,* έχουν οδηγήσει σε πολλά νέα "καταστασιακά"[2]

[2]Που γνωρίζουν, θυμούνται και συσχετίζουν την κατάσταση ενός στοιχείου του hardware, με άλλα στοιχεία

πρωτόκολλα π.χ. [21, 24, 30, 31, 34]. Πρωτόκολλα που στοχεύουν να ικανοποιήσουν αυτές τις απαιτήσεις, συχνά ενημερώνουν τα μυστικά τους μετά από μια επιτυχή εκτέλεσή τους. Προφανώς, αμφότεροι αναγνώστης και κάρτα πρέπει να διεκπεραιώσουν την ανανέωση του κλειδιού, για να διασφαλιστεί ότι ο αναγνώστης είναι σε θέση να πιστοποιήσει την κάρτα σε μελλοντικές εκτελέσεις του πρωτοκόλλου.

Σε μια *επίθεση αποσυγχρονισμού,* ο αντίπαλος στοχεύει στο να διακόψει την ενημέρωση του κλειδιού που φεύγει από τον αναγνώστη και την κάρτα σε μια αποσυγχρονισμένη κατάσταση, και να καταστήσει την οποιαδήποτε μελλοντική προσπάθεια αυθεντικοποίησης αδύνατη.

Οι συγγραφείς του HNMB παρατηρούν ότι αν το τελευταίο μήνυμα του αναγνώστη δε ληφθεί απ' την κάρτα, ο αναγνώστης διεκπεραιώνει μια ανανέωση του κλειδιού ενώ η κάρτα όχι. Για την αποτροπή του αποσυγχρονισμού, οι συγγραφείς προτείνουν ο αναγνώστης να παρακολουθεί τα προηγούμενα ID κάθε κάρτας. Έτσι, κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου HNMB, μετά τη λήψη της απάντησης μιας κάρτας και με σκοπό να την πιστοποιήσει, ο αναγνώστης ψάχνει στις τρέχουσες τιμές του ID όλων των καρτών, καθώς επίσης και στις προηγούμενες τιμές. Αυτό, όμως, είναι ανεπαρκές για την αποτροπή του αποσυγχρονισμού, όπως φαίνεται και παρακάτω.

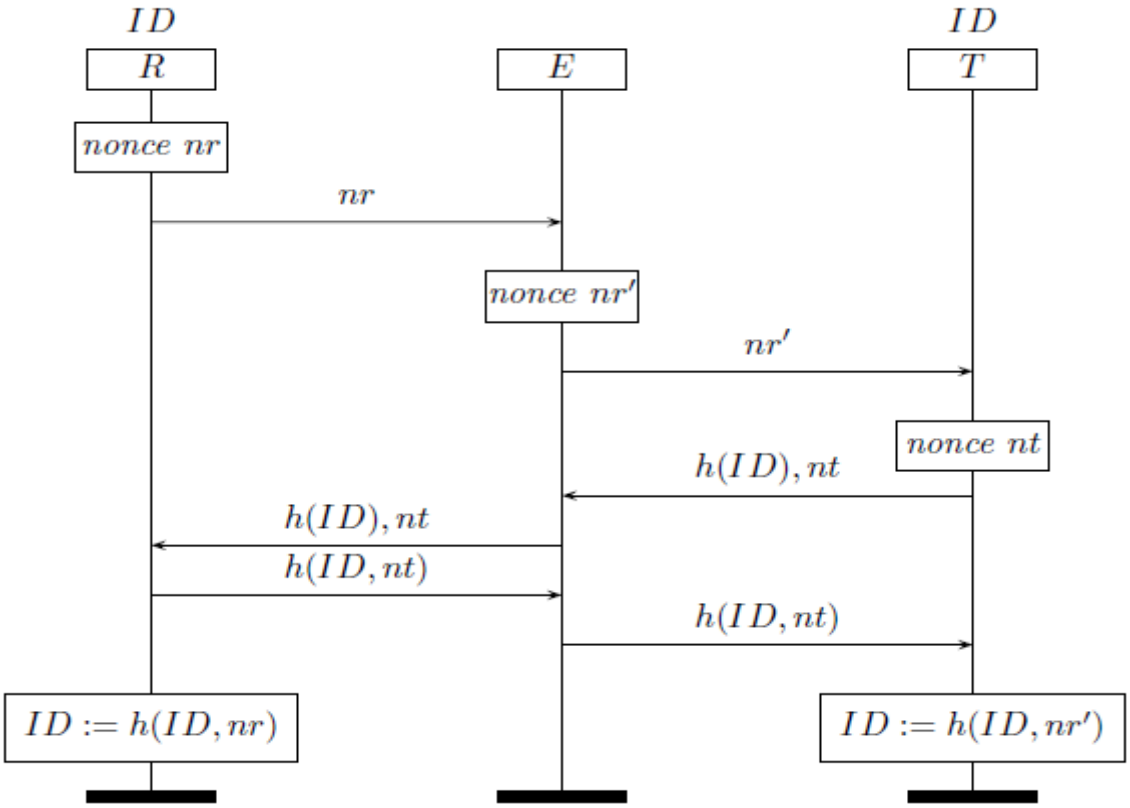
6.1 Η επίθεση

Οποιαδήποτε κάρτα βρίσκεται στην κατάσταση S = 0 μπορεί να αποσυγχροινιστεί από τον αναγνώστη με μια επίθεση ενδιάμεσου. Σε μια επικοινωνία μεταξύ κάρτας – αναγνώστη, ο αντίπαλος υποκλέπτει και τροποποιεί την ερώτηση nr της συσκευής ανάγνωσης, σε οποιαδήποτε τιμή nr' != nr. Ο αντίπαλος στέλνει τότε την αλλαγμένη τιμή στην κάρτα και προωθεί όλα τα άλλα μηνύματα μεταξύ κάρτας και αναγνώστη χωρίς τροποποίηση. Εφόσον στην περίπτωση S = 0 ο αναγνώστης δεν επικυρώνει ότι η κάρτα έλαβε το nr με τη σωστή τιμή, η αλλαγή από τον επιτιθέμενο περνά

του.

απαρατήρητη. Έτσι, στο τέλος της εκτέλεσης, κάρτα και αναγνώστης ενημερώνουν το ID με διαφορετικές τιμές. Η πρώτη αποθηκεύει h(ID, nr'), ενώ ο δεύτερος h(ID,nr). Επομένως και οι δυο βρίσκονται σε αποσυγχρονισμένη κατάσταση και οποιαδήποτε μελλοντική πιστοποίηση είναι αδύνατη. Η επίθεση απεικονίζεται στο σχήμα 2. Πρέπει να σημειωθεί εδώ ότι τα μέτρα του HNMB για την αντιμετώπιση της επίθεσης αυτής, δεν επιτρέπουν τον επανασυγχρονισμό σε αυτή την περίπτωση, επειδή η κάρτα δεν αποθηκεύει την προηγούμενη τιμή του ID και ο αναγνώστης δεν ξέρει την τιμή nr' από την οποία υπολογίζεται το νέο ID της κάρτας.

Η επίθεση που περιγράφεται εδώ είναι ρεαλιστική, αν δεχτούμε ότι ο αντίπαλος έχει ταυτόχρονη πρόσβαση σε έναν αναγνώστη και σε μια κάρτα εκτός εμβέλειάς του. Εναλλακτικά, είναι αρκετό το γεγονός ότι ο αναγνώστης είναι σε θέση να φθείρει το πρώτο μήνυμα του πρωτοκόλλου, εκπέμποντας για παράδειγμα θόρυβο κοντά στη συσκευή ανάγνωσης. Ο επιτιθέμενος θα μπορούσε να το επιτύχει αυτό φέροντας μια συσκευή που παρεμβάλει ραδιοσήματα [16].



Σχήμα 2. Επίθεση αποσυγχρονισμού στο πρωτόκολλο HNMB

Ο αποσυγχρονισμός μιας κάρτας από έναν αναγνώστη εκθέτει επίσης τη μη ανιχνευσιμότητα της κάρτας. Ο αντίπαλος μπορεί να αποκτήσει μια ερώτηση από τον αναγνώστη και να τη χρησιμοποιήσει για να αποκτήσει μια απάντηση από την κάρτα. Μπορεί, τότε, να ελέγξει την απάντηση μέσω του αναγνώστη, ο οποίος θα την απορρίψει αν και μόνο αν προέρχεται από αποσυγχρονισμένη κάρτα. Επομένως, ο αντίπαλος θα μπορεί πάντα να αναγνωρίζει μια τέτοια κάρτα.

6.2 Το σφάλμα στην ανάλυση ασφαλείας

Η ανάλυση του πρωτοκόλλου από τους συγγραφείς, όσον αφορά τον αποσυγχρονισμό, λαμβάνει υπόψιν μόνο επιθέσεις στις οποίες ο αντίπαλος εμποδίζει συγκεκριμένα μηνύματα. Η ανάλυση αυτή χωρίζεται σε δυο περιπτώσεις: στην περίπτωση όπου ο αντίπαλος εμποδίζει το δεύτερο μήνυμα του πρωτοκόλλου και σε αυτήν όπου εμποδίζει το τρίτο μήνυμα. Ενώ οι επιθέσεις αποσυγχρονισμού παραδοσιακά γίνονται με μπλοκάρισμα μηνυμάτων, υπάρχουν και άλλοι τρόποι με τους οποίους μπορούν να εκτελεστούν. Γενικά, η επιτυχής μίμηση ενός αναγνώστη σε μια κάρτα από έναν αντίπαλο μπορεί να οδηγήσει σε αποσυγχρονισμό, για παράδειγμα επειδή η κάρτα ενημερώνει τα κλειδιά της, το ID ή άλλες πληροφορίες, με τιμές που η συσκευή ανάγνωσης δε μπορεί να υπολογίσει. Μια άλλη πιθανότητα είναι η επιλεκτική ή τυχαία τροποποίηση μεταδιδόμενων μηνυμάτων όπως φαίνεται στο προηγούμενο σχήμα.

Έτσι το σφάλμα στην ανάλυση ασφαλείας των συγγραφέων, προκύπτει απ' το γεγονός ότι έχουν λάβει υπόψη μόνο μια συγκεκριμένη επίθεση στην ιδιότητα του αποσυγχρονισμού, παρά να δώσουν κάποια απόδειξη ορθότητας της ιδιότητας.

7. Χαμηλού κόστους και ισχυρής ασφάλειας πρωτόκολλο αυθεντικοποίησης

Σε αυτή την υποενότητα[3] παρουσιάζεται ως λύση για το σφάλμα που περιγράφηκε αναλυτικά στα προηγούμενα, ένα πρωτόκολλο RFID χαμηλού κόστους και ισχυρής ασφάλειας με σκοπό τη μείωση του υπολογιστικού φόρτου σε αμφότερες τις κάρτες

[3]Αυτή η έρευνα διενεργήθηκε από τους Jea Cheol Ha, Sang Jae Moon, Juan Manuel Gonzalez Nieto, and Colin Boyd

και τη βάση δεδομένων σε ένα σύστημα RFID. Όταν συμβαίνει αποσυγχρονισμός ως αποτέλεσμα κάποιας βλάβης στην επικοινωνία ή κακόβουλης επίθεσης, το προτεινόμενο πρωτόκολλο μπορεί να επαναφέρει το συγχρονισμό μεταξύ βάσης δεδομένων και καρτών. Επιπλέον ικανοποιεί τις περισσότερες απαιτήσεις ασφαλείας συμπεριλαμβανομένης και της ιδιότητας της ισχυρής ασφάλειας όπως ορίζεται από τους Juels και Weis [17],ενώ παραμένει ασφαλές εναντίον επιθέσεων εξαπάτησης (spoofing), και επανάληψης.

Ένας τρόπος προστασίας των καρτών από τις απειλές που έχουν περιγραφεί, είναι η ασφαλής πιστοποίηση μεταξύ κάρτας και αναγνώστη. Ωστόσο, εξαιτίας της υπολογιστικής δύναμης και του αποθηκευτικού χώρου της κάρτας, απαιτείται ένα πρωτόκολλο πιστοποίησης χαμηλού κόστους που λαμβάνει υπόψιν τη χωρητικότητα του server και τους περιορισμούς της κάρτας.

7.1 Ανάλυση πρωτοκόλλου

Συνήθως θεωρείται δεδομένο πως το κανάλι επικοινωνίας μεταξύ του αναγνώστη (R) και της βάσης δεδομένων (DB) είναι ασφαλές και το αντίστοιχο κανάλι μεταξύ αναγνώστη και κάρτας (T) είναι μη ασφαλές καθώς βασίζεται σε επικοινωνία μέσω αέρα. Στον πίνακα 2 φαίνονται οι χρησιμοποιούμενες έννοιες και η ερμηνεία τους.

Η βάση δεδομένων DB διαχειρίζεται το ID και τις τιμές hash HID και PID για κάθε T στο πεδίο της. Σύμφωνα με την κατάσταση της προηγούμενης εκτέλεσης της κάρτας, η DB βρίσκει το ID για την τρέχουσα εκτέλεση ή το PID που χρησιμοποιήθηκε στην προηγούμενη, συγκρίνοντας το ληφθέν P με το HID και το PID. Αφού πιστοποιηθεί η T, η DB ενημερώνει το ID της κάρτας και εκπέμπει ένα μήνυμα αυθεντικοποίησης.

Μια κάρτα εκπέμπει ένα $P = H(ID)$ ή $P = H(ID||r_T||rR)$ ανάλογα με την κατάσταση του SYNC ως απάντηση σε μια ερώτηση από τον R. Αν η T δε λάβει το τελευταίο μήνυμα από τον R λόγω βλάβης στην επικοινωνία ή αποτυχίας στη διαδικασία επαλήθευσης, το SYNC τίθεται ίσο με 1 και η T απαντά στον R με $P = H(ID||r_T||rR)$ στην επόμενη εκτέλεση. Στην περίπτωση που το πρωτόκολλο τελειώσει κανονικά, το

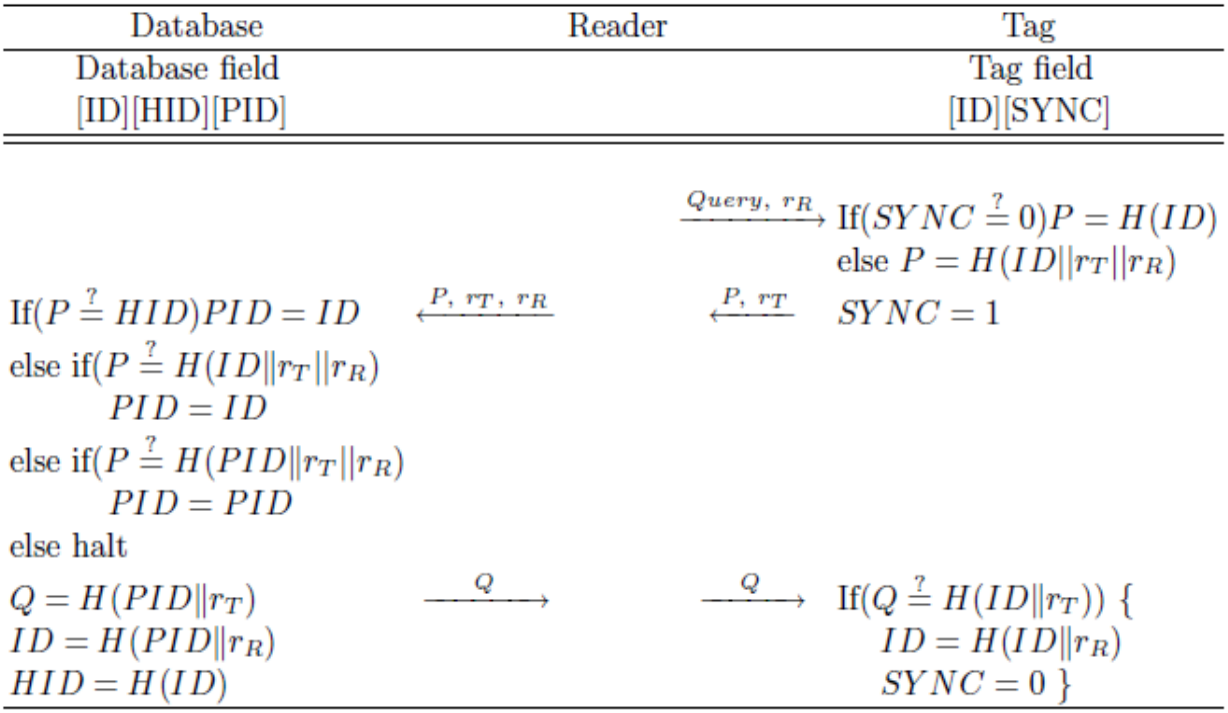
SYNC γίνεται 0 και η T εκπέμπει το P = H(ID) στην επόμενη εκτέλεση.

Έννοια	Ερμηνεία
T	Κάρτα RFID
R	Αναγνώστης RFID
DB	Βάση δεδομένων ή server κόρμού
ID	Ταυτότητα της κάρτας, k bits
HID	Hash τιμή του ID, k bits
PID	Τιμή του ID που χρησιμοποιήθηκε σε προηγούμενη εκτέλεση, k bits
rR	Τυχαίος αριθμός του R
rT	Τυχαίος αριθμός της T
Ερώτηση	Αίτημα προερχόμενο από τον R
SYNC	Παράμετρος που ελέγχει αν η T και η DB ανανέωσαν ταυτόχρονα το ID με επιτυχία ή όχι, 1bit
H()	Μέθοδος hash μιας κατεύθυνσης
||	Συνένωση δυο εισόδων
?=	Σύγκριση δυο εισόδων

Πίνακας 2. Έννοιες και ερμηνείες της προτεινόμενης λύσης

Ο R κάνει μια ερώτηση στην T με ένα τυχαίο αριθμό rR και λαμβάνει από αυτή πληροφορίες σχετικές με την πιστοποίηση, όπως τιμές hash και ένα τυχαίο αριθμό rT. Το μήνυμα που λαμβάνεται από την T προωθείται τότε στη DB και αφού αυτή αυθεντικοποιήσει την T, ο R εκπέμπει το μήνυμα που έλαβε από τη DB στην T. Το σχήμα 3 δείχνει τη διαδικασία της προτεινόμενης λύσης και ακολουθεί λεπτομερής περιγραφή του κάθε βήματος:

1. Ο R παράγει ένα rR και το εκπέμπει σε μια T χρησιμοποιώντας μια *ερώτηση*.
2. Η T επιλέγει ένα rT και υπολογίζει διαφορετικά το P ανάλογα με την κατάσταση του SYNC. Αυτό σημαίνει ότι, αν το SYNC είναι 0, η T υπολογίζει το P = H(ID) αλλίως το P = H(ID||rT||rR) χρησιμοποιώντας τα rT και rR και θέτει SYNC = 1. Η T τότε εκπέμπει το P και το rT στον R, ο οποίος προωθεί αυτά τα μηνύματα στη DB μαζί με το rR που παρήγαγε ο ίδιος στο βήμα 1.



Σχήμα 3. Το προτεινόμενο ισχυρό πρωτόκολλο χαμηλού κόστους

3. Η DB ψάχνει για τη συγκεκριμένη κάρτα μέσω του P που έλαβε. Αρχικά η DB συγκρίνει το ληφθέν P = H(ID) με τις τιμές HID που είναι αποθηκευμένες στη βάση. Αν οι τιμές ταιριάζουν, παράγει το ID ως την ταυτότητα της T που ζητά πιστοποίηση. Αυτή η γενική περίπτωση ισχύει όταν η προηγούμενη εκ΄τελεση ολοκληρώθηκε ομαλά. Εάν η DB δε μπορεί να βρει το HID στην πρώτη αναζήτηση, υπολογίζει την τιμή H(ID||rT||rR) και τη συγκρίνει με το P. Έτσι, αν τα μηνύματα-απαντήσεις της κάρτας μπλοκαρίστηκαν στην προηγούμενη εκτέλεση – κάτι που σημαίνει ότι το SYNC θα είναι 1 και τα ID στη βάση δε θα έχουν ενημερωθεί – τότε η DB θα ταιριάξει το ID στη δεύτερη αναζήτηση. Αν, ωστόσο, σε καμία απ' τις δυο προηγούμενες περιπτώσεις η βάση δεν καταφέρει να βρει το ID της κάρτας, υπολογίζει μια τιμή H(PID||rT||rR) για όλα τα PID και τη συγκρίνει με το P. Έτσι, η DB θα ταιριάξει το PID της T αν τα τελευταία μηνύματα του αναγνώστη μπλοκαρίστηκαν στην προηγούμενη εκτέλεση (δηλαδή αν το SYNC ήταν 1 και η DB είχε ανανεώσει το ID, ενώ το ID της κάρτας δεν είχε ενημερωθεί. Αν η DB εξακολουθεί να μη μπορεί να βρει το ID της κάρτας χρησιμοποιώντας τις τρεις

προηγούμενες περιπτώσεις, αναβάλει την αναζήτηση του ID και δίνει εντολή στον R να ερωτήσει ξανά. Αν η DB δε βρει το ID ή το PID με μια απ' τις τρεις μεθόδους αναζήτησης, πιστοποιεί την κάρτα ελέγχοντας την ύπαρξη ενός ID. Υπολογίζει το Q = H(PID||rT)[4] και το αποστέλλει στον R, έπειτα υπολογίζει το ID = H(PID||rR) και ενημερώνει το HID = H(ID) για την επόμενη εκτέλεση. Ο R προωθεί, τότε, το μήνυμα Q στην T.

4. Για να επαληθεύσει την ορθότητα του Q που έλαβε από τη DB, η T ελέγχει την ακόλουθη εξίσωση:

Q ?= H(ID||rT)

Αν αυτή η εξίσωση είναι σωστή, η T ενημερώνει το ID της με την τιμή H(ID||rT) και θέτει SYNC = 0.

7.2 Ασφάλεια και αποδοτικότητα

Για να αποκτήσει μυστικές πληροφορίες από μια κάρτα, ένας επιτιθέμενος θα πρέπει να μπορεί να υπολογίσει το ID της. Ωστόσο, δε μπορεί ένας οποιοσδήποτε επιτιθέμενος να εξάγει την τιμή του ID από τα H(ID), H(ID||rT)ή H(ID||rT||rR) εξαιτίας της ιδιότητας της μονής κατεύθυνσης της μεθόδου hash.

Ένας αντίπαλος συλλέγει τα μηνύματα μιας κάρτας και στη συνέχεια επιχειρεί μια επίθεση εξαπάτησης (spoofing) η οποία βασίζεται στη μίμηση μιας νόμιμης κάρτας. Όμως ο επιτιθέμενος δε μπορεί να υπολογίσει το εκπεμπόμενο μήνυμα P χωρίς να ξέρει το ID της κάρτας. Από την άλλη μεριά, για να υποδυθεί κάποιος μια κάρτα, θα πρέπει να στείλει το σωστό μήνυμα Q, πράγμα επίσης αδύνατο καθώς δε μπορεί να το υπολογίσει χωρίς να ξέρει το ID. Μια επίθεση επανάληψης επίσης δε μπορεί να θέσει σε κίνδυνο το προτεινόμενο πρωτόκολλο, καθώς το H(ID) ή το H(ID||rT||rR) ανανεώνονται με την ενημέρωση του ID ή τη συμπερίληψη των τυχαίων αριθμών rT και rR σε κάθε εκτέλεση.

Σε περίπτωση μιας επίθεσης αποσυγχρονισμού, όπου παρουσιάζεται απώλεια μηνύματος εξαιτίας κάποιου επιτιθέμενου, η προτεινόμενη λύση επιτρέπει σε κάρτα

[4]Εφόσον το ID ανανεώνεται σε PID μετά την εύρεση του ID από το HID, το Q = H(PID||rT) υπολογίζεται ανεξάρτητα από το ID ή το PID.

και αναγνώστη να επανακτήσουν το συγχρονισμό. Στην πρώτη περίπτωση, αν ένας επιτιθέμενος εμποδίσει τα μηνύματα-απαντήσεις που εκπέμπονται από την κάρτα, π.χ. στο βήμα 2 του σχήματος 2, καθώς επίσης κι αν η κάρτα δε λάβει κανένα σωστό μήνυμα από τον αναγνώστη, η κατάσταση SYNC τίθεται ίση με 1, ούτως ώστε η κάρτα να εκπέμψει το H(ID||rT||rR) στην επόμενη εκτέλεση. Παρ' όλα αυτά, οι δυο οντότητες μπορούν να επαναφέρουν το συγχρονισμό τους αναζητώντας το ID στη βάση, καθώς η DB αποθηκεύει τα τις τιμές των ID. Στη δεύτερη περίπτωση, αν ο αντίπαλος εμποδίσει το μήνυμα Q που εκπέμπεται από τον αναγνώστη, η DB έχει ήδη ενημερώσει το ID, ωστόσο το SYNC γίνεται 1. Έτσι, όταν η κάρτα εκπέμψει το H(ID||rT||rR) σαν απάντηση στην επόμενη εκτέλεση, η T και η DB μπορούν ακόμη να επαναφέρουν το συγχρονισμό βασιζόμενες στην εύρεση του PID στη βάση δεδομένων. Επομένως, η προτεινόμενη λύση μπορεί να προστατεύσει από μια επίθεση αποσυγχρονισμού.

Για τον εντοπισμό της τοποθεσίας μιας κάρτας, το πρωτόκολλο εγγυάται τη μυστικότητα της τοποθεσίας, βασισμένο στην ανανέωση του ID σε κάθε εκτέλεση. Αφού η πιστοποίηση έχει κλείσει ολοκληρωτικά στην προηγούμενη εκτέλεση, η κάρτα στέλνει το H(ID) σαν απάντηση σε ερώτηση στην τρέχουσα εκτέλεση. Έτσι, ικανοποιείται η ιδιότητα της μη διακριτότητας (που περιέχεται στον ορισμό της ισχυρής ιδιωτικότητας που δίνεται από τους Juels και Weis [17]), καθώς το ID στην προηγούμενη εκτέλεση έχει ανανεωθεί με χρήση μιας μεθόδου κατακερματισμού μονής κατεύθυνσης. Αντιθέτως, αν η προηγούμενη εκτέλεση τελειώσει μη ομαλά, η τιμή P που εκπέμπεται από την κάρτα είναι η H(ID||rT||rR) κι έτσι δεν εκπέμπεται η ίδια απάντηση από την κάρτα σε ακόλουθη εκτέλεση.

Στην περίπτωση της προς τα εμπρός ασφάλειας, θεωρείται ότι ένας επιτιθέμενος έχει, σε κάποια στιγμή, αποκτήσει το σωστό ID της κάρτας. Ωστόσο, οποιδήποτε προηγούμενο ID δε μπορεί να εξαχθεί, χάρη στην ιδιότητα της ασφάλειας της μεθόδου κατακερματισμού μονής κατεύθυνσης που χρησιμοποιείται για την ανανέωση του ID. Ως αποτέλεσμα, είναι αδύνατο να εντοπίσει κάποιος επιτιθέμενος την τοποθεσία της κάρτας ανάποδα. Όμως, είναι πιο δύσκολο να ικανοποιηθεί η προς

τα πίσω ασφάλεια κατά τη διάρκεια μιας κατάστασης επιτυχούς αποσυγχρονισμού κατά την οποία ένας αντίπαλος συλλέγει όλα τα μηνύματα της επικοινωνίας μέχρι να αποκτήσει το μυστικό ID που επιθυμεί. Σε αυτή την περίπτωση μπορεί να εντοπίσει την πρόσφατη ιστορία της T, καθώς το ID της κάρτας δεν έχει αλλαχθεί. Παρ' όλα αυτά, το προτεινόμενο πρωτόκολλο μπορεί να εγγυηθεί την προς τα εμπρός ασφάλεια από τη στιγμή της έναρξης μέχρι το πιο πρόσφατο σημείο επιτυχούς ανανέωσης του ID.

8. Συνοψίζοντας

Οι επιθέσεις που περιγράφονται σε αυτό το κεφάλαιο είναι διαφορετικές από άλλες επιθέσεις που περιγράφονται στη σχετική βιβλιογραφία. Για τις ευπάθειες αυθεντικοποίησης, οι επιθέσεις, τυπικά, επικεντρώνονται στον καθορισμό του μυστικού μιας κάρτας ή ενός αναγνώστη ή στην επανάληψη μηνυμάτων που έχουν παρατηρηθεί από προηγούμενες επικοινωνίες μεταξύ αυτών των συσκευών. Στην παρούσα περίπτωση, έγινε προφανές ότι ο αντίπαλος είναι αρκετό απλά να "ρωτήσει" μια κάρτα για να την προσωποποιηθεί και έτσι να ξεπεράσει την πιστοποίηση. Η ευπάθεια της μη ιχνηλασιμότητας δεν είναι τυπική, καθώς χρησιμοποιούνται πληροφορίες κατάστασης μιας κάρτας που διέρρευσαν από την ίδια την κάρτα, ενώ παραδοσιακά ο επιτιθέμενος προσπαθεί να ξεγελάσει την κάρτα ώστε να αναπαράξει ένα μήνυμα που έχει προηγουμένως παρατηρήσει. Τέλος, ενώ όπως αναφέρθηκε, οι επιθέσεις αυτού του τύπου επιτυγχάνονται συνήθως με το μπλοκάρισμα μηνυμάτων, εδώ ήταν εφικτό να αποσυγχρονιστούν κάρτα και αναγνώστης μέσω επίθεσης man-in-the-middle και εξαναγκασμού των συσκευών αυτών να κάνουν διαφορετικές ανανεώσεις.

Φυσικά, να σημειωθεί εδώ ότι το σφάλμα πιστοποίησης θα μπορούσε να βρεθεί και με τη χρήση αυτοματοποιημένων εργαλείων επαλήθευσης [2, 5]. Τα σφάλματα στην απόδειξη της μη ανιχνευσιμότητας του πρωτοκόλλου HNMB, δείχνουν ότι υπάρχει ανάγκη για αυτοματοποιημένη επαλήθευση αυτής της ιδιότητας, παρά το ότι είναι ακόμη ένα ανοιχτό πρόβλημα. Επιπρόσθετα, η εισαγωγή "καταστασιακών"

πρωτοκόλλων, οδηγεί στην ανάγκη για επιβεβαίωση της αντίστασης στους αποσυγχρονισμούς. Σαν ένα πρώτο βήμα, η ιδιότητα αυτή θα μπορούσε να οριστεί επίσημα.

Το χαμηλού κόστους και ασφαλές πρωτόκολλο που προτείνεται, εγγυάται την αυθεντικοποίηση, την στιβαρότητα απέναντι σε επιθέσεις εξαπάτησης και επανάληψης και τη μη ιχνηλασιμότητα. Επιπλέον, παρά το γεγονός ότι μπορεί να επέλθει μια κατάσταση αποσυγχρονισμού εξαιτίας ενός κακόβουλου επιτιθέμενου (στην οποία η βάση και η κάρτα έχουν διαφορετικά ID), ο συγχρονισμός μπορεί να επανέλθει στην επόμενη εκτέλεση. Τελικά, το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί σε συστήματα RFID χαμηλού κόστους που απαιτούν χαμηλό υπολογιστικό φόρτο και για τη βάση δεδομένων και για τις κάρτες.

ΑΝΑΦΟΡΕΣ

[1] Abadi, M. and R. Needham, Prudent engineering practice for cryptographic protocols, IEEE Trans. Softw. Eng. 22 (1996), pp. 6–15.

[2] Armando, A., D. A. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cu´ellar, P. H. Drielsma, P.-C. H´eam, O. Kouchnarenko, J. Mantovani, S. M¨odersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan`o and L.Vigneron, The avispa tool for the automated validation of internet security protocols and applications, in: CAV, 2005, pp. 281–285.

[3] Avoine, G., Adversary model for radio frequency identification, Technical Report LASEC-REPORT- 2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland (2005).

[4] Chien, H.-Y. and C.-W. Huang, A lightweight RFID protocol using substring, in: EUC, 2007, pp. 422 – 431.

[5] Cremers, C., “Scyther - Semantics and Verification of Security Protocols,” Ph.D. Dissertation, Eindhoven University of Technology (2006).

[6] Deursen, T. v., S. Mauw and S. Radomirovi´c, Untraceability of RFID protocols, in: Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks, Lecture Notes in Computer Science 5019 (2008), pp. 1–15.

[7] Di Pietro, R. and R. Molva, Information confinement, privacy, and security in RFID systems, in: ESORICS, 2007, pp. 187–202.

[8] Dimitriou, T., A secure and efficient RFID protocol that could make big brother (partially) obsolete,in: PerCom, 2006, pp. 269–275.

[9] Dolev, D. and A. Yao, On the security of public key protocols, IEEE Transactions on Information Theory IT-29 (1983), pp. 198–208.

[10] Duc, D. N., J. Park, H. Lee and K. Kim, Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning, in: Proc. of SCIS 2006, 2006.

[11] Gong, L., A variation on the themes of message freshness and replay or, the

difficulty in devising formal methods to analyze cryptographic protocols, in: CSFW, 1993, pp. 131–136.

[12] Ha J., S.-J. Moon, J. M. G. Nieto and C. Boyd, Low-cost and strong-security RFID authentication protocol, in: EUC Workshops, 2007, pp. 795–807.

[13] Ha, J., S.-J. Moon, J. M. G. Nieto and C. Boyd, Security analysis and enhancement of one-way hash based low-cost authentication protocol (OHLCAP), in: PAKDD Workshops, 2007, pp. 574–583.

[14] Henrici, D. and P.M¨uller, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, in: PerCom Workshops, 2004, pp. 149–153.

[15] Hoepman, J.-H., E. Hubbers, B. Jacobs, M. Oostdijk and R. Wichers Schreur, Crossing borders: Security and privacy issues of the european e-passport, in: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama and S.-i. Kawamura, editors, Advances in Information and Computer Security, First International Workshop on Security – IWSEC, Lecture Notes in Computer Science 4266 (2006), pp. 152–167.

[16] Juels, A., R. L. Rivest and M. Szydlo, The blocker tag: selective blocking of RFID tags for consumer privacy, in: ACM Conference on Computer and Communications Security, 2003, pp. 103–111.

[17] Juels, A. and S. A. Weis, Defining strong privacy for RFID, in: PerCom Workshops, 2007, pp. 342–347. 10 van Deursen and Radomirovi´c

[18] Kao, I.-L. and R. Chow, An efficient and secure authentication protocol using uncertified keys, Operating Systems Review 29 (1995), pp. 14–21.

[19] Keung, S. and K.-Y. Siu, Efficient protocols secure against guessing and replay attacks, in: ICCCN, 1995, p. 105.

[20] Kulyukin, V., A. Kutiyanawala, E. LoPresti, J. Matthews and R. Simpson, iWalker: Toward a rollator-mounted wayfinding system for the elderly, in: Proceedings of the 2008 IEEE International Conference on RFID, 2008, pp. 303–311.

[21] Le, T. v., M. Burmester and B. d. Medeiros, Forward-secure RFID authentication and key exchange, Cryptology ePrint Archive, Report 2007/051 (2007).

[22] Lee, S., T. Asano and K. Kim, RFID mutual authentication scheme based on synchronized secret information, in: Symposium on Cryptography and Information Security, Hiroshima, Japan, 2006.

[23] Lee, Y. K., L. Batina and I. Verbauwhede, EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol, in: Proceedings of the 2008 IEEE International Conference on RFID, 2008, pp. 97–104.

[24] Li, Y. and X. Ding, Protecting RFID communications in supply chains, in: ASIACCS, 2007, pp. 234–241.

[25] Li, Z., C.-H. Chu and W. Yao, SIP-RLTS: An RFID location tracking system based on SIP, in: Proceedings of the 2008 IEEE International Conference on RFID, 2008, pp. 173–182.

[26] Lo, N.W. and K.-H. Yeh, An efficient mutual authentication scheme for EPCglobal class-1 generation-2 RFID system, in: EUC Workshops, 2007, pp. 43–56.

[27] Lo, N. W. and K.-H. Yeh, Hash-based mutual authentication protocol for mobile RFID systems with robust reader-side privacy protection, to appear, 2007.

[28] Lo, N. W. and K.-H. Yeh, Novel RFID authentication schemes for security enhancement and system efficiency, in: Secure Data Management, 2007, pp. 203–212.

[29] Lowe, G., A hierarchy of authentication specifications, in: CSFW, 1997, pp. 31-44.

[30] Osaka, K., T. Takagi, K. Yamazaki and O. Takahashi, An efficient and secure RFID security method with ownership transfer, in: CIS, 2006, pp. 778–787.

[31] Peris-Lopez, P., J. C. H. Castro, J. M. Est´evez-Tapiador and A. Ribagorda, An efficient authentication protocol for RFID systems resistant to active attacks, in: EUC Workshops, 2007, pp. 781–794.

[32] Peris-Lopez, P., J. C. Hernandez-Castro, J. Estevez-Tapiador and A. Ribagorda, Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. (2007).

[33] Sarma, S. E., D. Brock and D. W. Engels, Radio frequency identification and the electronic product code, IEEE Micro 21 (2001), pp. 50–54.

[34] Song, B. and C. J. Mitchell, RFID authentication protocol for low-cost tags, in: WISEC, 2008, pp. 140–147.

[35] Transport for London, Oyster card, http://www.oystercard.co.uk (last accessed: May 19, 2008).

[36] Tsudik, G., A family of dunces: Trivial RFID identification and authentication protocols, in: Privacy Enhancing Technologies, 2007, pp. 45–61.

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΕΠΕΚΤΑΣΕΙΣ

Η πλήρης μυστικότητα είναι μόνο μια μαθηματική έννοια. Στην πραγματικότητα, πάντα θα υπάρχει ένα ανθρώπινο στοιχείο που είναι δύσκολο να ποσοτικοποιηθεί σε οποιαδήποτε μαθηματική διατύπωση. Ως εκ τούτου, είναι απίθανο να υπάρχει η απόλυτη ασφάλεια σε ένα σύστημα. Από τη στιγμή που θα γίνει αυτό κατανοητό, τότε είναι δυνατόν να γίνουν κινήσεις προς την αντιμετώπιση των διαφόρων ζητημάτων προστασίας και ασφάλειας που επισκιάζουν την τεχνολογία RFID.

Είναι εκπληκτικό πως μια τόσο "σεμνή" συσκευή, όπως μια κάρτα RFID, ουσιαστικά μια ασύρματη πινακίδα κυκλοφορίας, μπορεί να οδηγήσει στον πολύπλοκο συνδυασμό των προβλημάτων ασφάλειας και ιδιωτικότητας που συναντήσαμε εδώ.

Η εργασία αυτή έχει αναγνωρίσει πολλούς κινδύνους αναφορικά με την ασφάλεια και την ιδιωτικότητα για τα RFID συστήματα και έχει πραγματευθεί πολλές απ' τις μεθόδους που χρησιμοποιούνται για την επίτευξή τους. Οι περισσότερες απ' αυτές, όμως, έχουν πολύ υψηλές απαιτήσεις σε χώρο ή ενέργεια για να προσαρμοστούν στους περιορισμούς των συστημάτων RFID και πολύ από το διαθέσιμο υλικό (hardware) κρυπτογράφησης είναι μόνο για "έξυπνες" κάρτες. Αν και οι λύσεις μπορούν να εφαρμοστούν κατευθείαν στο RFID, το κύριο εμπόδιο είναι ότι οι επεξεργαστές των "έξυπνων" καρτών είναι πολύ πιο δυνατοί από μια απλή ετικέτα RFID που αποτελείται από 200 – 4000 πύλες μόνο[1]. Έτσι οι λύσεις δε μπορούν να μεταφερθούν σε μια πλατφόρμα RFID, αν περιμένουμε να διατηρηθεί σε χαμηλά επίπεδα το κόστος των ασφαλών καρτών.

Είναι προφανές ότι η ασφάλεια και η ιδιωτικότητα του RFID αποτελούν μια περιοχή έρευνας με μεγάλη πρόκληση. Υπάρχει ένας αριθμός από συγκεκριμένες περιοχές έρευνας από τον οποίο θα επωφεληθούν πολύ οι στόχοι αυτοί του RFID και

το αποτέλεσμα αυτής της έρευνας θα είναι η ευρεία υιοθέτηση της τεχνολογίας αυτής.

1. Οικονομικώς αποδοτικές και αποτελεσματικές εφαρμογές hardware συμμετρικών και ασυμμετρικών κρυπτοσυστημάτων. Αυτό μπορεί να περιλαμβάνει την εύρεση τρόπων βελτιστοποίησης και βελτίωσης των υπαρχόντων κρυπτογραφικών συστημάτων για οικονομικώς αποδοτικές και αποτελεσματικές εφαρμογές hardware, λαμβάνοντας υπόψη την ειδική φύση των καρτών RFID χαμηλού κόστους.

2. Ανάπτυξη νέων αποδοτικών κρυπτοσυστημάτων κατάλληλων για συστήματα RFID χαμηλού κόστους. Αυτό μπορεί να περιλαμβάνει την ανάπτυξη αποδοτικών και αποτελεσματικών μεθόδων κατακερματισμού (hash), συμμετρική και ασυμμετρική κρυπτογράφηση και τυχαίες και ψευδοτυχαίες γεννήτριες αριθμών.

3. Η ανάγκη για την ανάπτυξη πρωτοκόλλων με την ευελιξία να ενσωματώνουν διαφορετικές αρχές κρυπτογράφησης και μέτρα ασφαλείας ώστε να αποτρέπουν τις κάρτες απ' το να καταστούν ευάλωτες κατά τη διάρκεια μιας απότομης διακοπής στην επικοινωνία.

4. Βελτίωση και βελτιστοποίηση της σύνδεσης μεταξύ καρτών και αναγνωστών. Αυτό μπορεί να περιλαμβάνει την ανάπτυξη νέων εννοιών για τη δημιουργία συνδέσεων μεταξύ κεραιών, νέα σχέδια κεραιών και ανάλυση, ούτως ώστε να μεγιστοποιηθεί η διαθέσιμη πηγή ενέργειας των κυκλωμάτων.

Είναι σημαντικό να αναγνωριστεί ότι ο περιορισμός των πόρων των καρτών χαμηλού κόστους, υποδεικνύει ότι η απλότητα των μικρών συσκευών μιας χρήσης που εμπεριέχουν ένα ή περισσότερα μικρά διαμοιραζόμενα μυστικά μεταξύ κάρτας

και αναγνώστη, καθώς και οι εφαρμογές σχετικά απλών chip θα πρέπει επίσης να ληφθούν υπόψιν. Μερικές από τις ανησυχίες που προκύπτουν από την ασφάλεια και την ιδιωτικότητα μπορούν να αρθούν με τη χρήση θωρακισμένων ηλεκτρομαγνητικών επικοινωνιών μεταξύ μιας κάρτας και ενός αναγνώστη.

Είναι επίσης σημαντικό να σημειωθεί ότι το επίπεδο της ασφάλειας και ιδιωτικότητας θα εξαρτηθεί από την εκάστοτε εφαρμογή. Είναι προφανές ότι δεν υπάρχει μια γενική λύση, αλλά μια συλλογή από λύσεις που ταιριάζουν σε διαφορετικές εφαρμογές.

Μια άλλη σημαντική πτυχή της ασφάλειας στο RFID, είναι αυτή της αντίληψης του χρήστη για την ασφάλεια και την ιδιωτικότητα σε τέτοια συστήματα. Καθώς οι χρήστες δε μπορούν να δουν τις ραδιο-εκπομπές, σχηματίζουν τις εντυπώσεις τους βασισμένοι σε φυσικά, απτά στοιχεία και στις επεξηγήσεις της βιομηχανίας.

Πρέπει να γίνει κατανοητό ότι η ασφάλεια θα έρθει σε πολλές μορφές και επίπεδα δύναμης, αλλά το χαμηλό κόστος θα συνεπάγεται ότι θα βρίσκουμε μηχανισμούς που είναι “αρκετά καλοί” και όχι μηχανισμούς που είναι δύσκολο να σπάσουν.

Η πλειοψηφία των άρθρων που παρουσιάζονται σε αυτή την έρευνα, αντιμετωπίζουν τη ασφάλεια και την ιδιωτικότητα σαν ένα θέμα μεταξύ καρτών και αναγνωστών. Φυσικά, αυτές οι συσκευές βρίσκονται στη βάση ενός ολοκληρωμένου συστήματος RFID, στην καρδιά του οποίου θα υπάρχει μια τεράστια υποδομή από servers και λογισμικό. Πολλά απ' τα επακόλουθα προβλήματα ασφάλειας δεδομένων – όπως αυτό της αυθεντικοποίησης αναγνωστών στους servers – συμπεριλαμβάνουν ήδη γνωστά πρωτόκολλα ασφάλειας δεδομένων. Αλλά, η τεράστια έκταση της ροής των δεδομένων που σχετίζονται με το RFID και των διαμοιραζόμενων δια-επιχειρησιακών πληροφοριών, θα εισάγουν και νέα προβλήματα σχετικά με την ασφάλεια δεδομένων. Έχει αναφερθεί η διαχείριση κλειδιών σαν ένα πιθανό τέτοιο πρόβλημα, ενώ και άλλες προκλήσεις θα εμφανιστούν ως αποτέλεσμα της ρευστότητας των αλλαγών στην ιδιοκτησία των καρτών. Σήμερα, για παράδειγμα, τα domain names δεν αλλάζουν χέρια τόσο συχνά. Έτσι το DNS μπορεί να

περιλαμβάνει διαχείριση από ανθρώπους. Το ONS[1], απ' την άλλη – αν όντως πραγματοποιηθεί – θα χρειαστεί να περιλάβει πολύ περισσότερα αντικείμενα που αλλάζουν χέρια με μεγάλη συχνότητα.

Οι αισθητήρες είναι μικρές συσκευές παρόμοιες με τις κάρτες RFID. Ενώ οι κάρτες RFID εκπέμπουν αναγνωριστικά, οι αισθητήρες εκπέμπουν πληροφορίες για το περιβάλλον τους, όπως θερμοκρασία ή υγρασία. Οι αισθητήρες, τυπικά, περιέχουν μπαταρίες και ως εκ τούτου είναι πιο μεγάλοι και ακριβοί σε σχέση με τις παθητικές κάρτες RFID. Μεταξύ ενεργών καρτών και αισθητήρων, όμως, υπάρχουν μικρές διαφορές. Για παράδειγμα, μερικές εμπορικά διαθέσιμες ενεργές συσκευές RFID είναι σχεδιασμένες για να ασφαλίζουν containers στα λιμάνια. Εκπέμπουν αναγνωριστικά, ενώ παράλληλα "αισθάνονται" αν ένα container έχει ανοιχτεί ή όχι. Δεδομένων τέτοιων παραδειγμάτων, υπάρχει απρόσμενα μικρή επικάλυψη ανάμεσα στη βιβλιογραφία για την ασφάλεια αισθητήρων και σε αυτή για την ασφάλεια RFID. Τα όρια μεταξύ των διαφόρων ειδών ασύρματων συσκευών αναπόφευκτα θα "θολώσουν" κάποια στιγμή, όπως άλλωστε φαίνεται και από τη διττό ρόλο κάρτας-αναγνώστη που έχουν οι συσκευές NFC[2].

Το RFID, εν τέλει, θα ασφαλίσει ακόμα περισσότερες διαφοροποιούμενες μορφές φυσικής και λογικής πρόσβασης. Για να κατασκευαστούν χρησιμοποιήσιμα συστήματα RFID και να επιτραπεί η ενημερωμένη λήψη αποφάσεων σε θέματα πολιτικής απ' τα ανώτερα στελέχη των διαφόρων οργανισμών, είναι σημαντικό να κατανοηθεί πώς το RFID και οι άνθρωποι μπορούν να εμπλακούν [2, 3, 4].

[1]Ο οργανισμός EPCglobal έχει αναπτύξει ένα δημόσιο σύστημά αναζήτησης για κάρτες EPC, ονόματι Object Name Service (ONS), ανάλογο σε όνομα και λειτουργία με το DNS (Domain Name System). Ο σκοπός του ONS είναι να καθοδηγεί γενικά ερωτήματα καρτών στις βάσεις δεδομένων των ιδιοκτητών και διαχειριστών των καρτών αυτών.

[2]Το NFC (Near Field Consortium) είναι ένα standard (NFCIP-1/ECMA340, ISO 18092), συμβατό με τα ISO 14443 και ISO 15693. Μια συσκευή που υποστηρίζει αυτό το standard, μπορεί να λειτουργήσει είτε ως αναγνώστης είτε ως κάρτα και έτσι να μπορεί είτε να εκπέμψει είτε να λάβει σήμα.

Βιβλιογραφία

[1] Hall, D., Senior Design Engineer, TagSys, Australia. Personal Conversation, July 2004.

[2] P. de Jager. Experimenting on humans using Alien technology. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 439–448. Addison-Wesley, 2005.

[3] T. Kindberg, A. Sellen, and E. Geelhoed. Security and trust in mobile interactions: A study of users' perceptions and reasoning. In N. Davies, E. D. Mynatt, and I. Siio, editors, *Ubiquitous Computing: 6th International Conference (Ubicomp)*, volume 3205 of *Lecture Notes in Computer Science*, pages 196–213. Springer-Verlag, 2004.

[4] S. Spiekermann. Perceived control: Scales for privacy in ubiquitous computing environments. In L. Ardissono and T. Mitrovic, editors, *Conference on User Modeling – UM'05*, 2005. To appear.