Πανεπιστήμιο Πειραιώς

Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα

στις Ψηφιακές Επικοινωνίες και Δίκτυα

Διπλωματική Εργασία στο:

RFID SECURITY

Αριστέλα Καλυβιώτη

Αθήνα 2008

Αφιερώνεται στην οικογένειά μου.

Περίληψη

Αντικείμενο αυτής της διπλωματικής εργασίας είναι το RFID Security. Στο κεφάλαιο 1 παρουσιάζεται η ιστορική αναδρομή και οι εφαρμογές του RFID. Στο κεφάλαιο 2 αναλύεται περισσότερο η αρχιτεκτονική του RFID και κάποια χαρακτηριστικά του γνωρίσματα καθώς και τα πρότυπα που το περιβάλλουν. Στο κεφάλαιο 3 περιγράφονται οι στόχοι και οι ιδιότητες της ασφάλειας. Στο κεφάλαιο 4 παρουσιάζονται οι βασικοί τύποι επίθεσης , οι τύποι σύμφωνα με τον αντικειμενικό σκοπό τους και αναλύονται περισσότερο οι απειλες στο active και στο passive party. Στο κεφάλαιο 5 αναφέρονται και αναλύονται περισσότερο οι μηχανισμοί ασφάλειας ενώ στο κεφάλαιο 6 δίνεται η εκτίμηση των απειλών και τα μέτρα εναντίων αυτών των απειλών αλλά και η εκτίμηση των απειλών κατά της ιδιωτικότητας και παρουσιάζονται τα μέτρα εναντίων αυτών των απειλών. Τέλος, στο κεφάλαιο 7 αναφέρονται κάποια συμπεράσματα.

Ευχαριστίες

Θερμές ευχαριστίες εκφράζω στον λέκτορα κο Χ. Ξενάκη για την καθοδήγηση, τις συμβουλές και την άριστη συνεργασία για την ολοκλήρωση της διπλωματικής μου.

Τέλος, εκφράζω την ευγνωμοσύνη μου στους γονείς μου και τον αδελφό μου για την υποστήριξη και βοήθειά τους σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Συντομογραφίες

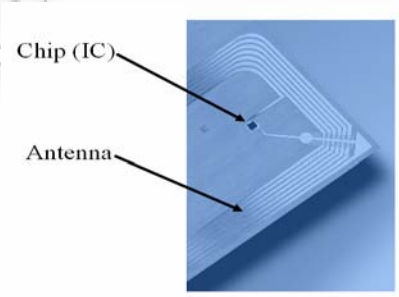
CIA	Confidentiality, Integrity και Availability
DoS	Denial of Service
EAS	Electronic Article Surveillance
EPC	Electronic Product Code
FIB	Focused Ion Beam
FIP	Fair Information Practices
HF	High Frequency
IFF	Identification Friend or Foe
LF	Low Frequency
POS	Point-Of-Sales
RFID	Radio Frequency Identification
UCC	Uniform Code Council
UHF	Ultra High Frequency

ΚΕΦΑΛΑΙΟ 1

1.1. Εισαγωγή

Το RFID (Radio Frequency Identification) είναι μια σύγχρονη τεχνολογία ηλεκτρονικής ταυτοποίησης η οποία στηρίζεται στην χρήση ραδιοκυμάτων και επιτρέπει στην αυτόματη αναγνώριση ανθρώπων, αντικειμένων και ζώων τα οποία φέρουν RFID tags (ετικέτες που ενσωματώνουν μικροεπεξεργαστή και κεραία) και μπορούν να ανιχνευτούν αυτόματα από σταθερούς ή φορητούς αναγνώστες RFID readers, χωρίς να είναι απαραίτητη η σάρωση του κάθε μεμονωμένου αντικειμένου.

Η κεραία επιτρέπει στον μικροεπεξεργαστή να μεταφέρει τις πληροφορίες αναγνώρισης στον αναγνώστη, ο οποίος με την σειρά του μετατρέπει τα ραδιοκύματα που «αντανακλώνται» από την ετικέτα RFID σε ψηφιακές πληροφορίες. Οι πληροφορίες αυτές μπορούν στην συνέχεια να «περάσουν» σε υπολογιστές για περαιτέρω χρήση. Στο Σχήμα 1.1 απεικονίζεται ένα RFID tag.



Σχήμα 1.1. RFID tag

Ο λόγος για τον οποίο η συγκεκριμένη τεχνολογία δεν εξαπλώθηκε όλα αυτά τα χρόνια έχει κυρίως να κάνει με το υψηλό κόστος κατασκευής των μικροεπεξεργαστών και των αναγνωστών. Ένας άλλος λόγος αφορά στην έλλειψη κοινών προτύπων που θα επέτρεπαν σε κάθε αναγνώστη RFID να αναγνωρίζει κάθε μικροεπεξεργαστή.

Έτσι, οι κατασκευαστές βλέπουν μία νέα τεχνολογία σαφώς πιο αποτελεσματική αλλά και πιο ανθεκτική από τα barcodes (γραμμωτός κώδικας), τα οποία παρουσιάζουν αρκετές δυσκολίες στην ανάγνωση μπροστά από το scanner , ή αν είναι ξεθωριασμένο ή σχισμένο). Ένα RFID tag μπορεί να μεταφέρει πληροφορίες αρκετά χρήσιμες από αυτές των barcodes, όπως για παράδειγμα την ημερομηνία λήξεως, στοιχείο ιδιαίτερα χρήσιμο για πολλά ευπαθή προϊόντα όπως για π.χ. το γάλα. Τα barcode χρησιμοποιούνταν από το 1970 στα λιανικά καταστήματα. Ένα παράδειγμα τυπικού UPC barcode παρουσιάζεται στο Σχήμα 1.2. Κάθε UPC barcode περιέχει βασικές πληροφορίες για το σύστημα bar coding, τον κατασκευαστή, το τεμάχιο, και ένα ψηφίο ελέγχου. Το UPC δεν επιτρέπει σειριακούς αριθμούς να κωδικοποιηθούν μέσα στο barcode.

Σχήμα 1.2. Τυπικό UPC barcode

Υπάρχουν πολλά πλεονεκτήματα των RFID έναντι των barcodes. Παρόλα ταύτα, και για το άμεσο τουλάχιστον μέλλον δεν προβλέπεται αντικατάσταση των barcodes, τα οποία είναι σαφώς φθηνότερα από το RFID tag, αλλά πιο αποτελεσματικά σε συγκεκριμένους τομείς. Έτσι, το πιο πιθανό είναι τα barcodes και το RFID να συνυπάρχουν για αρκετά χρόνια.

1.2. Ιστορική Αναδρομή του RFID

Το RFID δεν είναι μία νέα τεχνολογία. Ο στρατός των Ηνωμένων Πολιτειών χρησιμοποιούσε RFID ή τις προγενέστερες τεχνολογίες από το 1940, προκειμένου να επισημάνουν τον χώρο των προμηθειών όπως τα καύσιμα ή τις εκρηκτικές ύλες ή για να υποστηρίξουν την αναγνώριση των φίλων/εχθρών (Identification Friend or Foe) στα συμμαχικά αεροπλάνα. Τα "φιλικά" αεροπλάνα αποκρίνονταν με το σωστό αναγνωριστικό, ενώ εκείνα που δεν αποκρίνονταν θεωρούνταν "εχθροί". Σε γενικές γραμμές, το IFF λειτουργεί με τον ίδιο περίπου τρόπο με το RFID. Το IFF έχει αναπτυχθεί από το Δεύτερο Παγκόσμιο πόλεμο, και τώρα περιλαμβάνει διαφορετικούς τρόπους αναγνωριστικού τόσο για τα ιδιωτικά αεροπλάνα όσο και για τα στρατιωτικά. Ακόμα και εάν ο σύγχρονος ρόλος τώρα περιλαμβάνει τα ιδιωτικά αεροπλάνα το σύστημα είναι ακόμα γνωστό ως IFF.

Ένα από τα πιο πρόσφατα έγγραφα που εξερευνά το RFID είναι ένα άρθρο γραμμένο από τον Harry Stockman και το οποίο ονομάζεται «Communication by Means of Reflected Power», το οποίο είχε δημοσιευτεί το 1948. Αυτό ήρθε την στιγμή της

έρευνας η οποία είχε ανατεθεί για το radar και το radio κατά τη διάρκεια του δεύτερου παγκόσμιου πολέμου.

Στη δεκαετία του ‘50 υπήρξε μια θεωρητική εξερεύνηση των τεχνικών του RFID με έναν ικανοποιητικό αριθμό από επιστημονικά άρθρα τα οποία δημοσιεύθηκαν.

Στην δεκαετία του ’60 αρκετοί ερευνητές ανέπτυξαν πρωτότυπα συστήματα. Μερικά εμπορικά συστήματα προωθήθηκαν εκείνη την εποχή.

Στην δεκαετία του ‘70 υπήρξε πολύ μεγάλο ενδιαφέρον για το RFID από τους ερευνητές και από τα ακαδημαϊκά ιδρύματα συμπεριλαμβανομένου και των οργανισμών όπως το Los Alamos Scientific Laboratory και το Swedish Microwave Institute Foundation. Από το 1977 συγκεκριμένα τα RFID συστήματα κυκλοφόρησαν για εφαρμογές για τους πολίτες .Υπήρξε μεγάλη ανάπτυξη αυτή την περίοδο και εφαρμογές όπως οι ετικέτες για τα ζώα (animal tagging) έγιναν εμπορικά εφικτές.

Στην δεκαετία του ’80 η εφαρμογές του RFID επεκτάθηκαν σε πολλές άλλες περιοχές. Στην Ευρώπη τα συστήματα παρακολούθησης των ζώων διαδόθηκαν και δρόμοι με διόδια στην Ιταλία, τη Γαλλία, την Ισπανία, την Πορτογαλία και τη Νορβηγία εξοπλίστηκαν με RFID.

Η δεκαετία του ’90 ήταν σημαντική με την διαδεδομένη υιοθέτηση της ηλεκτρονικής συλλογής των διοδίων στις Ηνωμένες Πολιτείες. Το 1991 ένα ηλεκτρονικό σύστημα

διοδίων άνοιξε στην Οκλαχόμα όπου τα οχήματα μπορούσαν να περάσουν τα σημεία συλλογής διοδίων με τις ταχύτητες εθνικών οδών (χωρίς κανένα θάλαμο διοδίων).

Επίσης, στην Ευρώπη υπήρχε ιδιαίτερο ενδιαφέρον για τις εφαρμογές RFID συμπεριλαμβανομένου της συλλογής των διοδίων, εφαρμογές για τους σιδηρόδρομους και τον έλεγχο πρόσβασης.

Οι εφαρμογές των διοδίων και των σιδηρόδρομων εμφανίστηκαν σε πολλές χώρες συμπεριλαμβανομένης της Αργεντινής, της Αυστραλίας, της Βραζιλίας, του Καναδά, της Κίνας, του Χονγκ Κονγκ, της Ιαπωνίας, της Μαλαισίας, του Μεξικού, της Νέας Ζηλανδίας, της Νότιας Κορέας, της Νότιας Αφρικής, Σιγκαπούρης και της Ταϊλάνδης.

Οι εξελίξεις συνεχίστηκαν στην δεκαετία του ’90 με την ανάπτυξη ολοκληρωμένων κυκλωμάτων και την μείωση του μεγέθους μέχρι που οι μικροκυματικές RFID ετικέτες μειώθηκαν σε ένα ενιαίο ολοκληρωμένο κύκλωμα.

Αυτή την περίοδο υπάρχει μία σημαντική εργασία η οποία έχει ανατεθεί για την αιτιολόγηση της κατανομής φάσματος συχνότητας μεταξύ των χωρών, την ανάπτυξη προτύπων και την εισαγωγή πολλών εμπορικών εφαρμογών.

1.3. Εφαρμογές του RFID

Τα RFID tag αποθηκεύουν πληροφορίες σχετικές με τους ανθρώπους ή τα αντικείμενα που τα φέρουν. Έτσι στην πράξη, μπορούν να βρουν εφαρμογή σε

πληθώρα τομέων όπου η αναγνώριση ανθρώπων ή αντικειμένων είναι απαραίτητη. Για παράδειγμα μπορούν να χρησιμοποιηθούν στην συσκευασία των προϊόντων, σε βιβλιοθήκες, σε πιστωτικές κάρτες ή ακόμα και σε ένα σήμα ή έγγραφο ταυτοποίησης όπως η ταυτότητα, το διαβατήριο, ή το δίπλωμα οδήγησης. Ένας από τους πιο συνηθισμένους χώρους εφαρμογής των RFID είναι ο χώρος της εφοδιαστικής αλυσίδας, όπου μπορούν να αναγνωρίζουν προϊόντα είτε κατά την διάρκεια μεταφοράς τους είτε εντός βιομηχανικών μονάδων είτε αυτά βρίσκονται σε παλέτες, αποθήκες ή στα ράφια των καταστημάτων. Στο εξωτερικό ή χρήση τους έχει ήδη επεκταθεί σε πάρα πολλούς τομείς .Για παράδειγμα ενσωματώνονται σε κατοικίδια ζώα ή σε ζώα σε κτηνοτροφικές μονάδες, καθώς και σε βραχιόλια που φορούν ασθενείς που πάσχουν από την νόσο του Αλτζχάιμερ, τρόφιμοι σωφρονιστικών ή άλλων ιδρυμάτων, ακόμη και σε παιδιά που νοσηλεύονται για την αποφυγή των απαγωγών. Η λίστα με τους τομείς που χρησιμοποιούν RFID είναι μακριά αλλά αξίζει τον κόπο να την αναφέρουμε:

1. Σε ζώα. Τα tags τοποθετούνται κάτω από την επιφάνεια του δέρματος για τον προσδιορισμό της ιδιοκτησίας του κατοικίδιου. (Σχήμα 1.4.)
2. Αγροτικά Ζώα
3. Τοξική και ιατρική διαχείριση των αποβλήτων
4. Ταχυδρομικός εντοπισμός
5. Διαχείριση αεροπορικών αποσκευών
6. Αντι - πλαστογράφηση των χαρτονομισμάτων
7. Αντι - πλαστογράφηση στην βιομηχανία των φαρμάκων
8. Συστήματα ακινητοποίησης οχημάτων και συναγερμούς

9. Στην είσπραξη των διοδίων των δρόμων
10. EAS
11. Έλεγχος πρόσβασης
12. Χρόνος και παρουσία
13. Διαδικασίες κατασκευής με τη ρομποτική
14. Έλεγχος των παραβατών
15. Στα διαβατήρια και στον συνοριακό έλεγχο
16. Αλυσίδες ανεφοδιασμού, συμπεριλαμβανομένου του χονδρικού και λιανικού καταλόγου πώλησης και της διαχείρισης υλικών
17. Στα λιανικά ράφια τα εμπορεύματα ενσωματώνονται με tag
18. Έξυπνες κάρτες
19. POS
20. Logistics
21. Παρακολούθηση των περιουσιακών στοιχείων
22. Στα αθλήματα για να παρακολουθούν στους μαραθώνιους τους αθλητές και τους άλλους συμμετέχοντες αθλητές
23. Τοποθέτηση ετικετών
24. Τοποθέτηση των tags σε ανθρώπους. Κυρίως χρησιμοποιούνται για ιατρικούς λόγους και για λόγους ασφάλειας, όπως για παράδειγμα προστατεύοντας τα βρέφη από την απαγωγή στα νοσοκομεία.
25. Βιβλιοθήκες
26. Διαχείριση αρχείων
27. Σε ανθρώπους (Σχήμα 1.5.)
28. Στα νοσοκομεία (Σχήμα 1.3.)

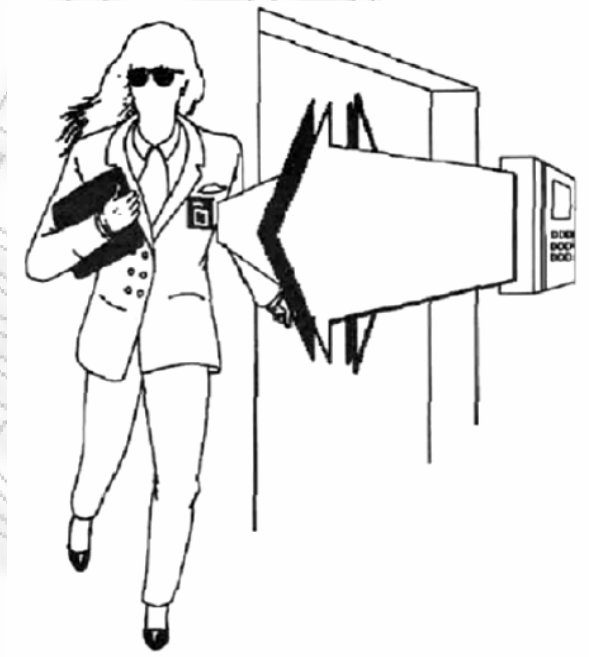
Σχήμα 1.3. Νοσοκομειακό βραχιόλι

Σχήμα 1.4. Ενσωμάτωση του tag σε ψάρι κάτω για παρακολούθηση της κίνησής του

Σχήμα 1.5. Ενσωμάτωση του tag σε άνθρωπο

Οι επιχειρήσεις έχουν πολλά πλεονεκτήματα που μπορούν να αποκομίσουν από την χρήση των RFID. Μερικά από αυτά είναι:

- Μείωση κόστους
- Αύξηση της παραγωγικότητας
- Μείωση σε λάθη, κλοπές και πλαστογραφίες
- Ενημέρωση του προσωπικού σε πραγματικό χόνο
- Αύξηση της αποδοτικότητας και ποιότητας υπηρεσιών
- Ακρίβεια και αποδοτικότητα στις παραλλαγές
- Διαφάνεια στην διαχείριση
- Μείωση αποθεμάτων
- Αποδοτικότητα και ακρίβεια στην αποστολή
- Βοήθεια στην ανάκληση προϊόντων
- Μείωση προϊόντων που δεν διακινούνται
- Μείωση των περιπτώσεων έλλειψης αποθέματος (out-of-stock)
- Παρακολούθηση των υπαλλήλων που εισέρχονται στην εταιρία (Σχήμα 1.6.)



Σχήμα 1.6. Παρακολούθηση των υπαλλήλων

ΚΕΦΑΛΑΙΟ 2

2.1. Αρχιτεκτονική του RFID

Η αρχιτεκτονική συστημάτων RFID αποτελείται από έναν αναγνώστη (reader) και μια ετικέτα (tag). Ο reader ρωτά το tag, παίρνει πληροφορίες, και έπειτα λαμβάνει δράση βασιζόμενος σε εκείνες τις πληροφορίες. Αυτή η πράξη μπορεί να εμφανίσει έναν αριθμό σε μία μηχανή χειρός, ή μπορεί να περάσει πληροφορίες σε ένα POS (Point-Of-Sales) σύστημα μία βάση δεδομένων λεπτομερούς καταλόγου, ή να το αναμεταδώσει σε ένα σύστημα πληρωμών χιλιάδες μίλια μακριά. Γενικά , το POS σύστημα συλλέγει τα στοιχεία από κάθε στοιχείο που αγοράζεται, όπως είναι το εμπορικό σήμα στοιχείων, την κατηγορία, το μέγεθος, το χρόνο και την ημερομηνία της αγοράς και σε ποια τιμή το στοιχείο αγοράστηκε. Παράδειγμα ενός POS συστήματος είναι μία ταμειακή μηχανή. Ένα τυπικό σύστημα RFID απεικονίζεται στο Σχήμα 2.1.

Σχήμα 2.1. Ένα τυπικό RFID σύστημα

Όπως παρατηρούμε από το Σχήμα 2.1 ένα RFID σύστημα αποτελείται από τα εξής στοιχεία:

- Μία συσκευή RFID (*tag*)
- Τον *tag reader* με μία κεραία και έναν πομποδέκτη
- Ένα σύστημα φιλοξενίας ή σύνδεσης σε ένα επιχειρηματικό σύστημα(Enterprise System)

2.1.1. Οι ετικέτες tags ή labels

Οι μονάδες RFID είναι μία κατηγορία από radio συσκευές γνωστές και ως transponders (αναμεταδότες). Ο transponder ενεργεί σαν πραγματικός φορέας δεδομένων. Ακόμη, ο transponder εφαρμόζεται σε ένα αντικείμενο (παραδείγματος χάριν, σε ένα αγαθό ή μια συσκευασία) ή ενσωματώνεται σε ένα αντικείμενο (παραδείγματος χάριν, σε μια έξυπνη κάρτα) και μπορεί να διαβαστεί χωρίς να γίνει κάποια επαφή, και μπορεί να ξαναγραφεί εξαρτώμενο από την τεχνολογία η οποία χρησιμοποιείται. Ένας αριθμός αναγνώρισης αποθηκεύεται μαζί με άλλα δεδομένα στον transponder και στο αντικείμενο με το οποίο συνδέεται.

Ένας transponder είναι ένας συνδυασμός πομπού και δέκτη, το οποίο είναι σχεδιασμένο για να λαμβάνει ένα συγκεκριμένο ραδιοσήμα και αυτόματα να μεταδώσει μία απάντηση. Στην απλούστερη εφαρμογή του, ο transponder αφουγκράζεται ένα ραδιόφαρο (radio beacon), και στέλνει ένα δικό του ραδιόφαρο ως απάντηση. Τα πιο περίπλοκα συστήματα μπορούν να μεταδώσουν ένα μοναδικό

γράμμα ή ψηφίο πίσω στην πηγή ή να στείλουν πολλαπλά strings από γράμματα και αριθμούς. Τέλος, τα προηγμένα συστήματα μπορούν να κάνουν μια διαδικασία υπολογισμού ή επαλήθευσης και να περιλάβουν κρυπτογραφημένες ραδιομεταδόσεις για να αποτρέψουν τους eavesdroppers (ωτακουστές) από τη λήψη των πληροφοριών που μεταδίδονται. Οι trasnpoders που χρησιμοποιούνται σε RFID καλούνται συνήθως *tags*, *chips*, or *labels,* τα οποία είναι αρκετά ανταλλάξιμα, παρόλο που το «chip» υποδηλώνει μία μικρότερη μονάδα, και το «tag» χρησιμοποιείται για μεγαλύτερες συσκευές. Ένα RFID tag περιέχει τα ακόλουθα επιμέρους στοιχεία:

- Διάταξη κυκλώματος κωδικοποίησης / αποκωδικοποίησης
- Μνήμη
- Κεραία
- Παροχή Ηλεκτρικού ρεύματος
- Έλεγχος των επικοινωνιών

Η ποσότητα της πληροφορίας που μπορεί να αποθηκεύσει ένα RFID tag εξαρτάται από τον προμηθευτή και την εφαρμογή, αλλά τυπικά δεν υπερβαίνει τα 2 KB δεδομένων αρκετά για να αποθηκεύσουν βασικές πληροφορίες για το αντικείμενο που την φέρει. Στην παρούσα φάση οι εταιρίες εξετάζουν την χρήση ενός tag αντίστοιχου με μία «πινακίδα άδειας κυκλοφορίας», το οποίο περιλαμβάνει μόνο ένα σειριακό αριθμό 96-bit, έχει χαμηλότερο κόστος κατασκευής και είναι πιο χρήσιμο στις εφαρμογές όπου το tag θα παταχθεί με την συσκευασία. Τα tag μπορούν να φέρουν από απλές πληροφορίες, όπως τα στοιχεία του κατόχου ενός κατοικίδιου ή τις

οδηγίες καθαρισμού ενός ρούχου, έως και πιο σύνθετες, όπως οδηγίες συναρμολόγησης ενός αυτοκινήτου. Μερικοί κατασκευαστές αυτοκινήτων χρησιμοποιούν συστήματα RFID στην γραμμή παραγωγής, όπου σε κάθε στάδιο το tag "πληροφορεί" τους υπολογιστές για το επόμενο στάδιο συναρμολόγησης.

2.1.2. Reader

Το δεύτερο βασικό στοιχείο του RFID συστήματος είναι ο *reader* ή ο *interrogator*. Ο όρος reader είναι μία ακυρολογία . Τεχνικά, οι μονάδες reader είναι transceivers (πομποδέκτες) (δηλαδή, ένας συνδυασμός από πομπό και δέκτη). Αλλά επειδή ο ρόλος του είναι να ρωτήσει ένα tag και να λάβει δεδομένα από αυτό, θεωρούνται σαν να "διαβάζουν το tag", ως εκ τούτου και ο όρος "reader". Οι readers μπορούν να έχουν μία ενσωματωμένη κεραία ή η κεραία μπορεί να είναι χωριστά. Η κεραία μπορεί να είναι αναπόσπαστο τμήμα του reader, ή μπορεί να είναι μια ξεχωριστή συσκευή. Το Σχήμα 2.2 απεικονίζει κάποια ενδεικτικά δείγματα από RFID readers.

Σχήμα 2.2. RFID αναγνώστες (readers)

Άλλα μέρη τα οποία τυπικά ένας reader περιέχει είναι:

- Μία διεπαφή συστημάτων όπως μία σειριακή θύρα RS-232 ή ένα Ethernet jack
- Διάταξη κυκλώματος κωδικοποιήσης/αποκωδικοποιήσης
- Μία παροχή ηλεκτρικού ρεύματος ή μια μπαταρία
- Κυκλώματα ελέγχου των επικοινωνιών

Ο reader ανακτά τις πληροφορίες από το RFID tag. Οι readers επίσης ελέγχουν την ποιότητα της μετάδοσης των δεδομένων. Ο reader μπορεί να είναι ανεξάρτητος και να καταγράφει τις πληροφορίες εσωτερικά. Εντούτοις, μπορεί να είναι μέρος ενός συστήματος εντοπισμού όπως ένας καταχωρητής χρημάτων POS, μία μεγάλη περιοχή τοπικού δικτύου (LAN), ή μία ευρεία περιοχή δικτύου (WAN).

Οι readers οι οποίοι στέλνουν δεδομένα σε ένα LAN ή σε κάποιο άλλο σύστημα το κάνουν αυτό χρησιμοποιώντας μία διεπαφή δεδομένων όπως το Ethernet ή το σειριακό RS-232. Οι readers και ειδικότερα οι διατάξεις των κεραιών τους, μπορούν να έχουν διαφορετικό μέγεθος, από το μέγεθος ενός ταχυδρομικού γραμματόσημου σε πιο μεγάλες συσκευές με πίνακες, τα οποία είναι αρκετά πλατιά και ψηλά.

2.1.3. Enterprise System

Αποτελείται από έναν ή περισσότερους υπολογιστές συμπεριλαμβανομένου ενός συστήματος βάσεων δεδομένων που συνδέεται με μια ή περισσότερες reader συσκευές. Ο reader περνά την τιμή του tag στην μονάδα επεξεργασίας από την οποία ανακτά περισσότερες πληροφορίες για το tag από την βάση δεδομένων των πληροφοριών tag.

2.2. Read/only και Read/write tag

Τα tag στο RFID μπορεί να είναι “read/write”, “read/only”, ή “write once”, “read many” (WORM).

Στα “read/write” tag μπορούμε να προσθέσουμε πληροφορίες στο tag ή να γράψουμε πάνω σε υπάρχουσες πληροφορίες όταν το tag βρίσκεται πάνω στην ακτίνα του reader . Συνήθως τα tag αυτά έχουν ένα σειριακό αριθμό που δεν μπορούμε να διαγράψουμε, ενώ μπορούμε να κλειδώσουμε και κάποια δεδομένα, έτσι ώστε να μην

παραγραφούν. Τα read/write tag είναι ακριβότερα να κατασκευάσουν λόγω του χαρακτηριστικού γνωρίσματος της μνήμης τους.

Τα "read/only" tag ενσωματώνουν πληροφορίες που έχουν αποθηκευτεί σε αυτά κατά την διάρκεια της κατασκευής τους και οι οποίες δεν μπορούν να τροποποιηθούν. Στα tag WORM μπορούμε να γράψουμε ένα σειριακό αριθμό μία φορά, και η συγκεκριμένη πληροφορία δεν μπορεί στην συνέχεια να διαγραφεί. Τα read/write tag είναι πιο φθηνά στην παραγωγή τους.

2.3. Active, Passive, Semi-Passive και Semi-active tags

Τα tags εμπίπτουν σε δυο κατηγορίες: σε εκείνα με παροχή ηλεκτρικού ρεύματος (μπαταρία) και σε αυτά χωρίς .Έτσι λοιπόν έχουμε τα *active* και τα *passive tags*. Εκτός από τις δυο κύριες κατηγορίες υπάρχει και άλλες δυο οι οποίες ονομάζονται *semi-passive tags* και *semi-active tags*.

Τα *passive tags* δεν έχουν μπαταρία ή κάποια άλλη συσκευή και τροφοδοτούνται από τον αναγνώστη, ο οποίος εκπέμπει ηλεκτρομαγνητικά κύματα που δημιουργούν πεδίο στην κεραία της ετικέτας. Το tag περιέχει ένα ηχηρό κύκλωμα ικανό να απορροφήσει την ισχύ από την κεραία του reader. Η λήψη της ισχύος από τη συσκευή του γίνεται χρησιμοποιώντας ένα ηλεκτρομαγνητικό στοιχείο γνωστό ως *Near Field*. Όπως, το όνομα υποδηλώνει, η συσκευή πρέπει να είναι σχετικά κοντά με τον reader προκειμένου να δουλέψει. Ο *Near Field* εν συντομία παρέχει αρκετή ισχύς στο tag

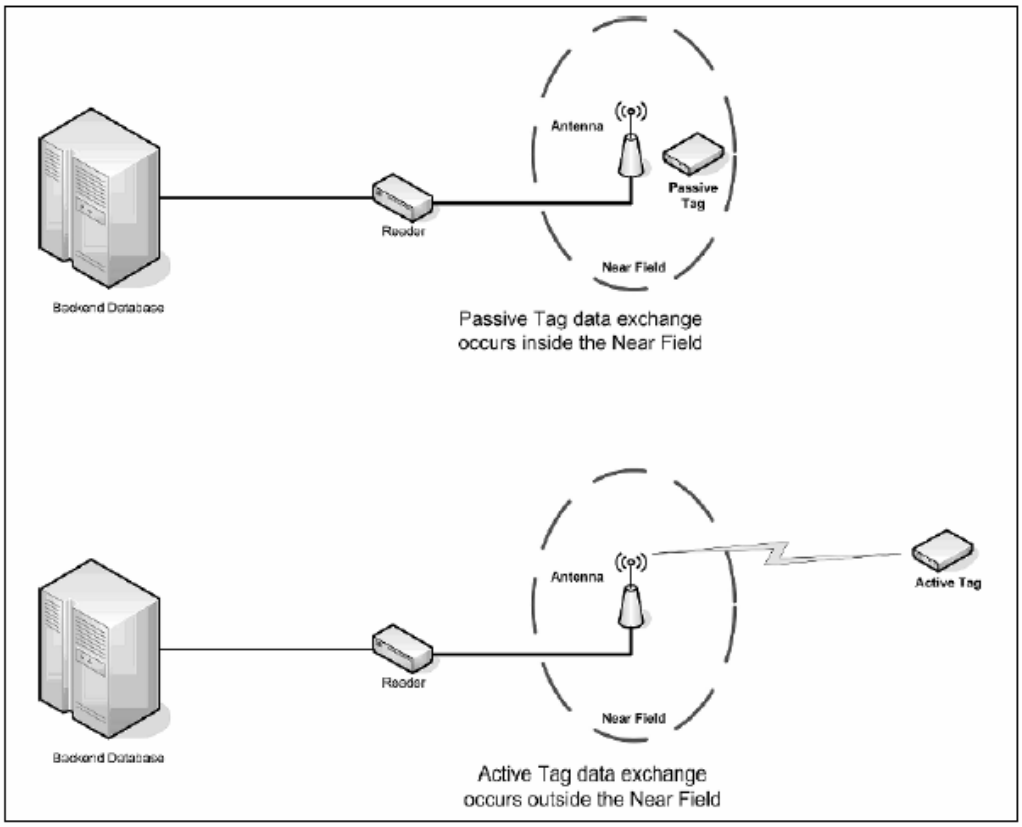
έτσι ώστε να μπορεί να στείλει απάντηση. Ακόμη, τα passive tag είναι γενικά read only.

Τα *active tags* διαθέτουν ένα πομπό και την δική τους πηγή ενέργειας (συνήθως μια μπαταρία) που χρησιμοποιείται για την λειτουργία του κυκλώματος του μικροεπεξεργαστή και την μετάδοση του σήματος στον αναγνώστη. Από την στιγμή που διαθέτουν δικής τους πηγή ενέργειας, δεν χρειάζεται να τους παρέχει ισχύ ο *Near Field* της κεραίας του reader. Επειδή δεν είναι απαραίτητο να στηριχθούν στην τροφοδότηση από τον reader, δεν περιορίζονται να λειτουργήσουν μέσα στο Near Field. Μπορούν να ρωτηθούν και να αποκριθούν σε μακρινές αποστάσεις μακριά από τον reader , πράγμα που σημαίνει ότι τα active tags (τουλάχιστον) μπορούν να μεταδώσουν και να λάβουν πέρα από μεγάλες αποστάσεις. Επίσης, τα active tags είναι read/write συσκευές. Τα active tag είναι γενικά πιο ακριβά αλλά έχουν τα καλύτερα ραδιοχαραχτηριστικά και μπορούν και μπορούν να ενσωματώνουν άλλα λειτουργικά συστατικά, π.χ. αισθητήρες (sensors).
Στο Σχήμα 2.3 απεικονίζονται οι παραπάνω διαδικασίες των active και passive tag.

Υπάρχουν, επίσης, και τα *semi-passive tags* που χρησιμοποιούν μπαταρία για το μικροεπεξεργαστή, αλλά επικοινωνούν απορροφώντας ενέργεια από τον αναγνώστη. Τα semi-passive tags βασίζονται στο *Near Field* να τροφοδοτήσουν τα ραδιοκυκλώματα κατά την διάρκεια της λήψης και της αποστολής των δεδομένων. Τυπικά είναι πιο μικρά και φθηνά από τα active tags, αλλά έχουν μεγαλύτερη λειτουργία από ότι τα passive tags επειδή περισσότερη ισχύς είναι διαθέσιμη για άλλους λόγους. Κάποιες βιβλιογραφίες χρησιμοποιούν τους όρους “semi-passive” και “semi-active” κατ΄ εναλλαγή.

Τα active και τα semi-passive tag χρησιμοποιούνται κυρίως για την ανίχνευση αγαθών υψηλής αξίας που πρέπει να παρακολουθούνται σε μεγάλες κλίμακες (π.χ. αυτοκίνητα που μεταφέρονται από φορτηγό) και είναι πιο ακριβά από τα passive, και τα οποία είναι και τα πιο συνηθέστερα και χρησιμοποιούνται συχνότερα σε προϊόντα χαμηλής αξίας.

Ένα *semi-active tag* είναι ένα active tag το οποίο παραμένει κοιμισμένο έως ότου λάβει ένα σήμα από τον reader για να ξυπνήσει. Ένα tag μπορεί έπειτα να χρησιμοποιήσει την μπαταρία του για να επικοινωνήσει με το reader. Όπως τα active tags, έτσι και τα semi-active tags μπορούν να επικοινωνήσουν πέρα από μία μεγαλύτερη απόσταση από τα passive tags. Το κύριο πλεονέκτημά τους σε σχέση με τα active tags είναι ότι έχουν μία μπαταρία που έχει πιο μεγάλη διάρκεια. Η διαδικασία του ξυπνήματος, εντούτοις, μερικές φορές προκαλεί μία απαράδεκτη χρονική καθυστέρηση όταν τα tags περνούν τους readers πολύ γρήγορα ή όταν πολλά tags χρειάζεται να διαβαστούν σε μικρό χρονικό διάστημα. Στο Σχήμα 2.4 απεικονίζονται κάποιοι τύποι tags.



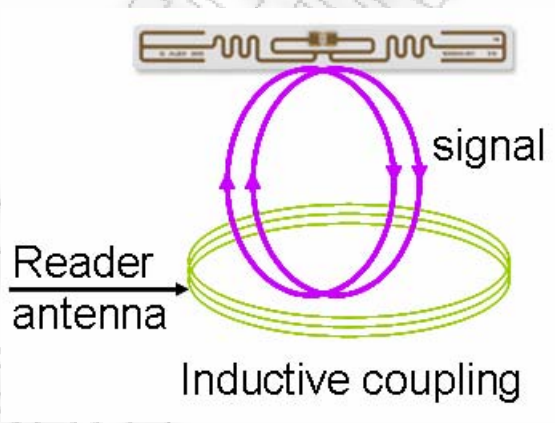
Σχήμα 2.3. Passive και Active Tag Διαδικασίες

Σχήμα 2.4. Τύποι κάποιων από τους τύπους των tags

2.4. Τύποι σύζευξης tag-reader

Υπάρχουν δύο τύποι συζεύξεων tag-reader η επαγωγική σύζευξη (inductive) και η οπισθοδιασπορά (backscatter) :

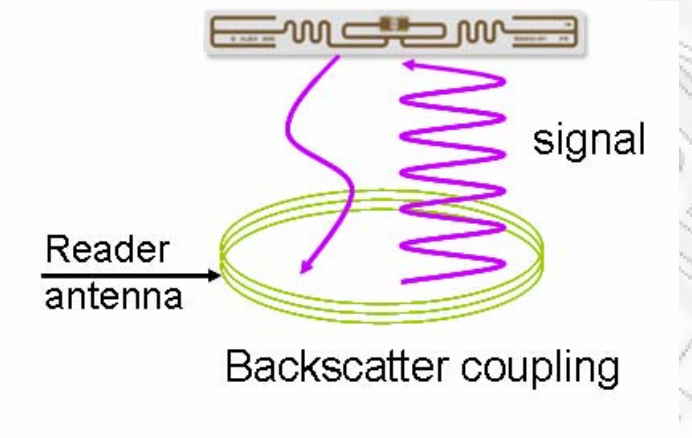
Η επαγωγική σύζευξη (Σχήμα 2.5) χρησιμοποιεί συχνότητες κάτω από 30 MHz. Η σπείρα κεραιών του reader παράγει ένα εναλλασσόμενο μαγνητικό πεδίο και προκαλεί μια τάση στη σπείρα του tag. Η μεταφορά δεδομένων από τον reader στον tag είναι συνήθως βασισμένη στη διαμόρφωση μετατόπισης εύρους (ASK) και το tag υιοθετεί τη διαμόρφωση φορτίων για να μεταφέρει τα δεδομένα πίσω στον reader.



Σχήμα 2.5. Επαγωγική σύζευξη

Η σύζευξη οπισθοδιασποράς (Σχήμα 2.6) χρησιμοποιείται για τις συχνότητες πάνω από 100 MHz. Εδώ η κεραία του tag λαμβάνει τα σήματα και την ενέργεια (passive tags μόνο) από το ηλεκτρομαγνητικό πεδίο που εκπέμπεται από τον reader. Προκειμένου να μεταφερθούν τα δεδομένα στον reader, η απεικονισμένη δύναμη

διαμορφώνεται από τον transponder (modulated backscatter: διαμορφωμένη οπισθοδιασπορά).



Σχήμα 2.6. Σύζευξη οπισθοδιασποράς

2.5. Λειτουργία των tag

Τα passive tags τραβούν την ισχύ τους από την μετάδοση του reader μέσω της επαγωγικής σύζευξης (inductive coupling). Τα passive tags τότε θα αποκριθούν στην ερώτηση. Το inductive coupling συνήθως απαιτεί στενή εγγύτητα.

Τα active tags επικοινωνούν συνήθως μέσω της σύζευξης διάδοσης (propagation coupling) και αποκρίνονται στη μετάδοση του reader βασιζόμενα στην εσωτερική ισχύ της μετάδοσης.

2.6. Φάσματα συχνότητας (Frequency ranges)

Στην περίπτωση του RFID θα πρέπει τα tags και τα readers να ρυθμιστούν στην ίδια συχνότητα για να επικοινωνήσουν μεταξύ τους. Οι κατανομές συχνότητας γενικά ελέγχονται μέσω της νομοθεσίας και του κανονισμού από τις κάθε μεμονωμένες κυβερνήσεις .

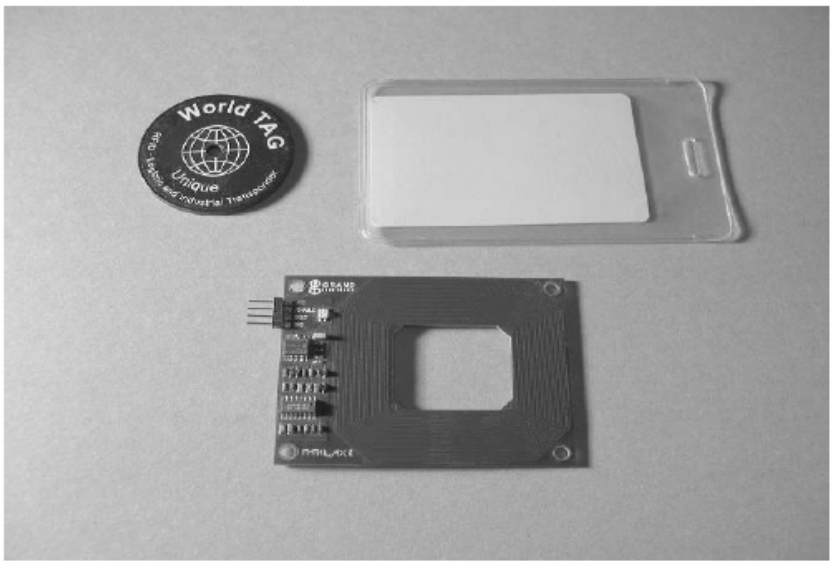
Διεθνώς, υπάρχουν διαφορές στις συχνότητες που προορίζονται για τις RFID εφαρμογές παρόλο που η τυποποίηση μέσω του ISO και των παρόμοιων οργανώσεων βοηθά στη συμβατότητα. Για παράδειγμα, η Ευρώπη χρησιμοποιεί 860 MHz για UHF (υπερύψηλες) ενώ οι Ηνωμένες πολιτείες χρησιμοποιούν 915 MHz. Αυτήν την περίοδο, πολύ λίγες συχνότητες είναι διαθέσιμες σε παγκόσμια βάση για τις εφαρμογές RFID.

Τα συστήματα RFID χρησιμοποιούν πολλές διαφορετικές συχνότητες, αλλά γενικά οι πλέον συνηθισμένες είναι τρεις και είναι αυτές που φαίνονται στον Πίνακα 2.1. Σε μερικές εφαρμογές χρησιμοποιείται και η μικροκυματική συχνότητα (2.45 GHz).

Ζώνες Συχνοτήτων (Frequency Bands)	
Χαμηλή συχνότητα (LF: Low Frequency)	125 KHz - 134 KHz
Υψηλή συχνότητα (HF: High Frequency)	13.56 MHz
Υπερύψηλη (UHF: Ultra High Frequency)	860 MHz - 930 MHz

Πίνακας 2.1. Φάσματα Συχνότητας

Οι ιδιότητες της ζώνης επηρεάζουν επίσης το φυσικό μέγεθος των κεραιών και ποια επίπεδα μετάδοσης ισχύος μπορούν να χρησιμοποιηθούν. Αντίθετα, οι φυσικοί περιορισμοί μπορούν να επηρεάσουν ποιες συχνότητες και RF ζώνες θα χρησιμοποιηθούν για μια δεδομένη εφαρμογή. Το Σχήμα 2.7 παρουσιάζει δυο διαφορετικά RFID tag και έναν reader. Τα αντικείμενα από επάνω είναι RFID tags και το αντικείμενο από κάτω είναι ο reader.



Σχήμα 2.7. Δυο διαφορετικά RFID tags και ένας reader μία ενσωματωμένη κεραία

Η διαφορά στην συχνότητα παίζει ρόλο και στην εφαρμογή. Έτσι για παράδειγμα τα tags χαμηλής συχνότητας θεωρούνται ιδανικά για αναγνώριση αντικειμένων με υψηλή περιεκτικότητα σε νερό, όπως τα φρούτα, και έχουν ακτίνα ανάγνωσης περίπου 0.3 μέτρα, ενώ τα tag υψηλής συχνότητας λειτουργούν καλύτερα σε μεταλλικά αντικείμενα, με ακτίνα ανάγνωσης ενός μέτρου. Τα tag υπερύψηλης συχνότητας χρησιμοποιούνται κυρίως για αναγνώριση πελατών σε αποθήκες με

ακτίνα ανάγνωσης από 3,3 μέτρα έως 6,6 μέτρα. Στις υπερύψηλες συχνότητες, η ακτίνα ανάγνωσης ,μπορεί με κάποιους περιορισμούς να ξεπεράσει και τα 30 μέτρα.

2.7. Κατηγορίες χρήσης του RFID

Οι συσκευές RFID μπορούν να ταξινομηθούν σε τέσσερις κατηγορίες χρήσης:

- EAS (Electronic Article Surveillance)
- Φορητή συλλογή δεδομένων (Portable data capture)
- Δικτυωμένα συστήματα (Networked systems)
- Συστήματα τοποθεσίας (Positioning systems)

2.7.1. EAS (Electronic Article Surveillance)

Αυτά είναι χαρακτηριστικά 1-bit συστήματα που χρησιμοποιούνται για να γίνει αντιληπτή η παρουσία ή απουσία ενός αντικειμένου. Η πιο κοινή χρήση είναι στα λιανικά καταστήματα ως αντικλεπτική συσκευή. Τα tags συνδέονται στα ρούχα ή στα άλλα εμπορεύματα και προκαλούν ένα συναγερμό εάν τα αγαθά "αφήνουν" το κατάστημα προτού να απενεργοποιηθεί το tag.

Αυτά ήταν σε διαδεδομένη χρήση για μερικά έτη και βρίσκονται σε ποικίλα λιανικά καταστήματα συμπεριλαμβανομένου του ρουχισμού, των μικρών συσκευών, των ηλεκτρικών αγαθών και των βιβλιοπωλείων.

2.7.2. Portable data capture

Χρησιμοποιείται με φορητές συσκευές, όπου τα απαιτούμενα δεδομένα από το αντικείμενο που έχει tag μπορεί να ποικίλουν. Μερικές συσκευές ενσωματώνουν αισθητήρες για να καταγράψουν παραδείγματος χάριν, τη θερμοκρασία, τη μετακίνηση (σεισμική) και την ακτινοβολία. Τα δεδομένα μπορούν να είναι αποθηκευμένα στην φορητή συσκευή για επεξεργασία (processing) και καταφόρτωση (download).

2.7.3. Networked systems

Αυτά τα συστήματα χαρακτηρίζονται από τους σταθερούς στην θέση readers και χρησιμοποιούνται για να αποτυπώσουν τη μετακίνηση των αντικειμένων που έχουν tag. Συνήθως είναι άμεσα συνδεδεμένα με ένα επιχειρηματικό σύστημα, αυτό είναι μια χαρακτηριστική εφαρμογή καταλόγων της τεχνολογίας.

2.7.4. Positioning systems

Αυτά τα συστήματα χρησιμοποιούνται όπου τα αντικείμενα (όπως τα οχήματα, τα ζώα ή ακόμα και άνθρωποι) έχουν tag και παρέχεται αυτόματη θέση και υποστήριξη πλοήγησης.

2.8. RFID πρότυπα (RFID standards)

Η έλλειψη προτυποποίησης και η έλλειψη της εναρμόνισης της κατανομής συχνότητας παρακωλύει την αύξηση αυτής της βιομηχανίας. Παρόλα ταύτα η διαδικασία της προτυποποίησης βρίσκεται σε εξέλιξη. Ήδη, υπάρχουν διεθνή πρότυπα για μερικές εξιδικευμένες εφαρμογές, όπως η ανίχνευση ζώων και οι "έξυπνες κάρτες" που απαιτούν κρυπτογράφηση για την ασφάλεια των δεδομένων.

Επίσης σε εξέλιξη βρίσκονται πολλές πρωτοβουλίες για την δημιουργία προτύπων. Ο πιο γνωστός διεθνής οργανισμός προτυποποίησης (ISO και ANSI) δουλεύουν πάνω σε πρότυπα για την παρακολούθηση προϊόντων καθ' όλη την διαδικασία της εφοδιαστικής αλυσίδας χρησιμοποιώντας ετικέτες υψηλής (18000-3) και υπερύψηλης συχνότητας (ISO 18000-6) . Επίσης, εργάζονται για να αναπτύξουν πρότυπα RFID και μερικά έχουν υιοθετηθεί για εφαρμογές όπως τη ζωική παρακολούθηση (ISO 11784 και 11785) .

Το EPC σύστημα καθορίζει τα τεχνικά πρωτόκολλα και δημιουργεί μία δομή δεδομένων για τις αποθηκευμένες πληροφορίες. Το σύστημα EPC ερευνήθηκε και αναπτύχθηκε στο Auto-ID Center στο ίδρυμα της τεχνολογίας της Μασαχουσέτης (MIT) και τον Νοέμβριο του 2003 η ευθύνη για την εμπορευματοποίηση και τη διαχείριση του συστήματος EPC μεταβιβάστηκε στην EPCglobal Inc.

Η EPCglobal, είναι μία μη κερδοσκοπική κοινοπραξία που ιδρύθηκε από το Uniform Code Council(UCC) με στόχο λοιπόν της εμπορευματοποίησης των τεχνολογιών των ηλεκτρονικών προιόντων κωδικών (Electronic Product Code-EPC),διαθέτει την δική του διαδικασία προτυποποίησης που χρησιμοποιήθηκε και στα πρότυπα των barcodes. Σκοπός της EPCglobal είναι να υποβάλλει τα πρωτόκολλα EPC και στον ISO, έτσι ώστε να αποτελέσουν διεθνή πρότυπα.

Αυτή η οργάνωση είναι θυγατρική του Uniform Code Council (UCC) και της διεθνούς EAN (EAN). Το EAN και το UCC δημιούργησαν και διατήρησαν το EAN.UCC σύστημα, το οποίο καλύπτει τα παγκόσμια πρότυπα επικοινωνιών του e-business, τα σχέδια αρίθμησης, την διαχείριση μοναδικότητας, τα πρότυπα συμβολισμού των barcode, συμπεριλαμβανομένων του UPC και των EAN barcode συμβόλων που χρησιμοποιούνται στα καταναλωτικά αγαθά σε όλο τον κόσμο. Ενώ υπάρχουν μερικές διαφορές με τα πρότυπα του ISO, αυτές οι οργανώσεις εργάζονται τώρα μαζί για να οργανώσουν ορθολογικά τα πρότυπα. Οι προδιαγραφές του EPC έχουν καθορίσει πέντε κατηγορίες κλάσεων των tag βασιζόμενες στην λειτουργία. Οι κλάσεις ενός tag δίνονται στο Πίνακα 2.2.

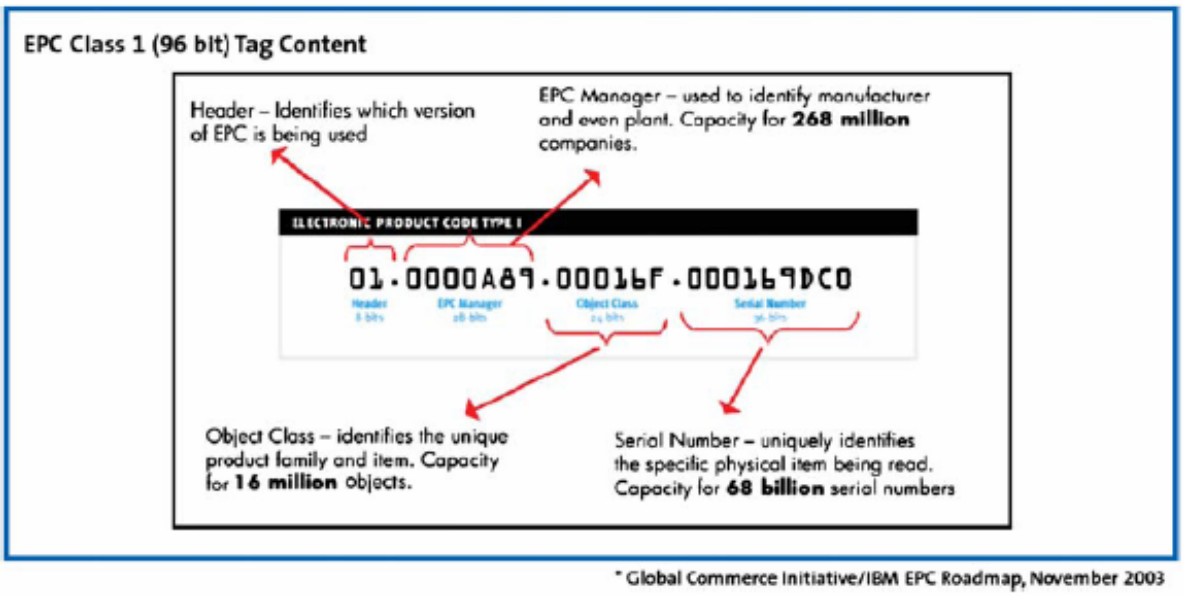
Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

Πίνακας 2.2. Οι πέντε κατηγορίες κλάσεων

Η τρέχουσα έκδοση του Electronic Product Code (EPC) Tag Data Standard διευκρινίζει την διάταξη για την κωδικοποίηση και την ανάγνωση των δεδομένων από 64 και 96 bit RFID tags. Ο Πίνακας 2.3 δίνει την δομή του tag. Ενώ το Σχήμα 2.8 δείχνει το περιεχόμενο του tag.

ECP TYPE	HEADER SIZE	FIRST BITS	DOMAIN MANAGER	OBJECT CLASS	SERIAL NUMBER	TOTAL
64 bit type I	2	01	21	17	24	64
64 bit type II	2	10	15	13	34	64
64 bit type III	2	11	26	13	23	64
64 bit and more	8	00	28	24	36	96

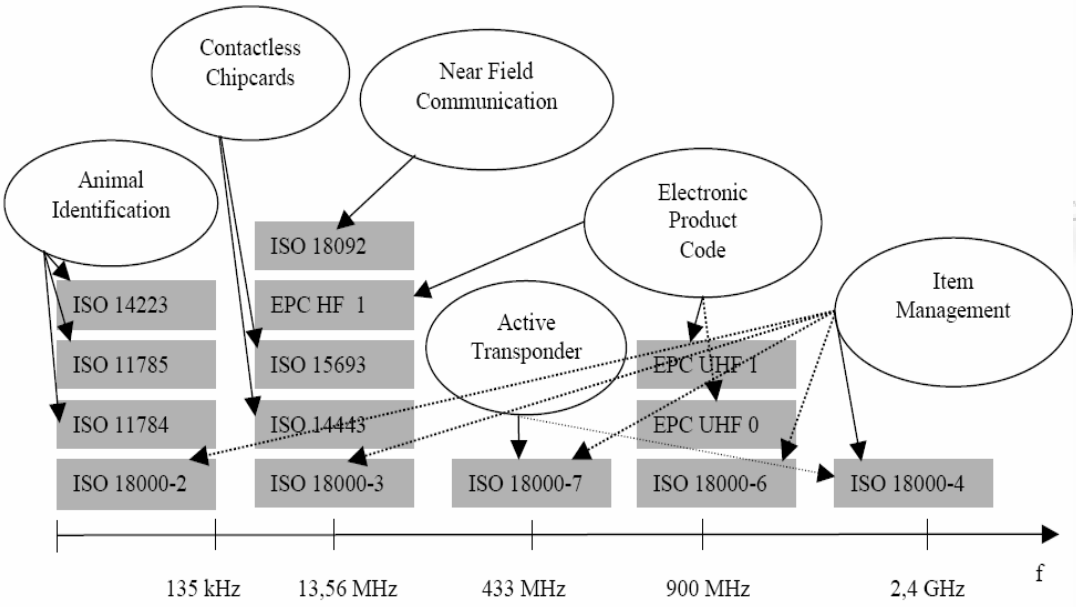
Πίνακας 2.3. Δομή του tag



Σχήμα 2.8. Περιεχόμενο του tag

Όπως είπαμε και πιο πριν το RFID είναι μία ετερογενής ραδιοτεχνολογία με έναν σημαντικό αριθμό συσχετισμένων προτύπων. Το Σχήμα 2.9 περιέχει τα πιο συσχετισμένα τεχνολογικά πρότυπα, δηλαδή εκείνα τα οποία περιγράφουν το physical και το data link στρώμα (διεπιφάνεια αέρα, εναντίον της σύγκρουσης, πρωτόκολλα επικοινωνίας, και λειτουργίες ασφάλειας).

Τα περαιτέρω πρότυπα RFID περιγράφουν τα πρότυπα μεθόδων δοκιμής και στοιχείων εφαρμογής (διαμόρφωση του μοναδικού προσδιοριστικού, του πρωτοκόλλου δεδομένων και των διεπαφών των εφαρμογών προγραμματισμού).



Σχήμα 2.9. Πρότυπα της Τεχνολογίας RFID και τις ζώνες συχνοτήτων

ΚΕΦΑΛΑΙΟ 3

3.1. Στόχοι ασφάλειας

Οι ραδιοεπικοινωνίες μεταξύ των RFID transponder και των reader εγείρουν, όπως βασικά όλες οι ασύρματες τεχνολογίες, έναν αριθμό από θέματα ασφάλειας. Οι θεμελιώδεις στόχοι ασφάλειας πληροφοριών συχνά δεν είναι εφικτοί εκτός και εάν ειδικοί μηχανισμοί ασφάλειας ενσωματώνονται μέσα στο σύστημα. Οι θεμελιώδεις στόχοι ασφάλειας πληροφοριών είναι:

- η εμπιστευτικότητα (confidentiality)
- η ακεραιότητα (integrity)
- η διαθεσιμότητα (availability)
- η επικύρωση (authentication)
- η εξουσιοδότηση (authorization)
- η αποδοχή (non-repudiation)
- η ανωνυμία (anonymity)

Η πλευρά της μυστικότητας (privacy) έχει κερδίσει την ιδιαίτερη προσοχή για τα συστήματα RFID. Οι καταναλωτές μπορούν να φέρουν αντικείμενα με αθόρυβους transponders επικοινωνίας χωρίς ακόμη να αντιλαμβάνονται την ύπαρξη των tag. Τα passive tags στέλνουν συνήθως το αναγνωριστικό τους χωρίς περαιτέρω επαλήθευση

ασφάλειας όταν τροφοδοτούνται με ηλεκτρομαγνητικά κύματα από τον αναγνώστη. Οι πληροφορίες ID μπορούν να συνδεθούν με άλλα στοιχεία ταυτότητας και με τις πληροφορίες θέσης. Οι καταναλωτές μπορούν να απασχολούν ένα προσωπικό reader για να προσδιορίσουν τα tags στο περιβάλλον τους αλλά ο μεγάλος αριθμός από διαφορετικά πρότυπα μπορεί να καταστήσει αυτό δύσκολο. Οι επιχειρήσεις αντιμετωπίζουν τους φόβους των πελατών και τα ζητήματα μυστικότητας μπορεί να αποτελέσουν σημαντικό εμπόδιο στον περαιτέρω διάδοση του RFID.

3.2. Ιδιότητες ασφάλειας

3.2.1. Εμπιστευτικότητα (confidentiality)

Η επικοινωνία μεταξύ του reader και του tag είναι απροστάτευτη στις περισσότερες περιπτώσεις. Το εμπρόσθιο κανάλι (forward channel: Το κανάλι στο οποίο ένας reader μεταδίδει τα σήματά του) από το reader στο tag έχει μία μεγάλη σειρά και είναι πιο πολύ σε ρίσκο από το οπισθοδρομικό κανάλι (backward channel: Το κανάλι στο οποίο ένα tag μεταδίδει τα σήματά του). Επιπλέον, η μνήμη του tag μπορεί να διαβαστεί εάν ο έλεγχος πρόσβασης δεν εφαρμόζεται.

3.2.2. Ακεραιότητα (integrity)

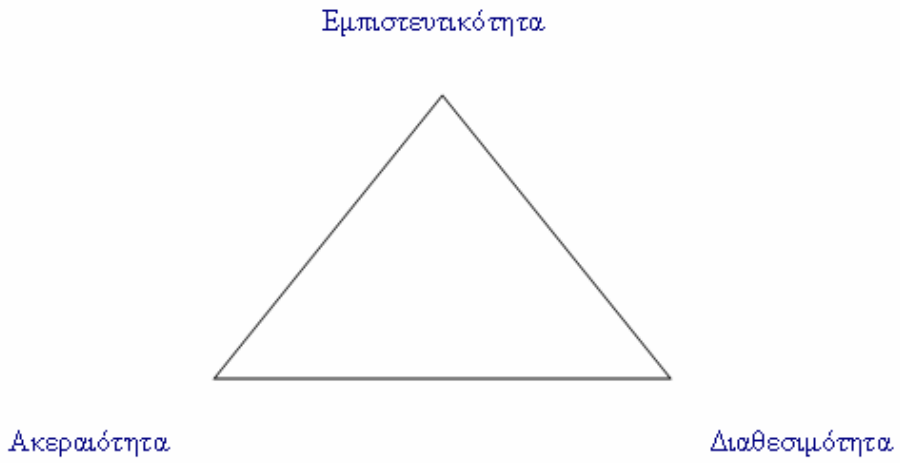
Με εξαίρεση των high-end ISO 14443 συστημάτων που χρησιμοποιούν τους κώδικες επικύρωσης μηνυμάτων (MACs), η ακεραιότητα των μεταδιδόμενων πληροφοριών

δεν μπορεί να διαβεβαιωθεί. Τα Checksums (CRCs) συχνά επιδίδονται στην διεπιφάνεια επικοινωνίας αλλά προστατεύουν μόνο εναντίον των τυχαίων βλαβών. Επιπλέον, η εγγράψιμη μνήμη μπορεί να ελεγχθεί επιδέξια εάν ο έλεγχος πρόσβασης δεν εφαρμόζεται.

3.2.3. Διαθεσιμότητα (availability)

Οποιοδήποτε σύστημα RFID μπορεί εύκολα να ενοχληθεί από το frequency jamming. Αλλά, οι denial-of-service επιθέσεις είναι επίσης εφικτές στα υψηλότερα στρώματα επικοινωνίας. Το αποκαλούμενο "blocker RFID" εκμεταλλεύεται τους ιδιότυπους (anti-collision) μηχανισμούς των tag για να διακόψει την επικοινωνία του reader με όλα ή με συγκεκριμένα tags.

Τα τρία παραπάνω δόγματα ασφάλειας των πληροφοριών Confidentiality, Integrity και Availability (CIA) αναφέρονται συνήθως ως "The Big Tree" και απεικονίζονται συνήθως με το Σχήμα 3.1.



Σχήμα 3.1. Το CIA δέντρο

3.2.4. Επικύρωση (authentication)

Η αυθεντικότητα ενός tag διατρέχει κίνδυνο από την στιγμή που το μοναδικό προσδιοριστικό (UID) ενός tag μπορεί να ξεγελαστεί ή να ελεγχθεί επιδέξια. Τα tags είναι γενικά μη ανθεκτικά στην πλαστογράφηση.

3.2.5. Έξουσιοδότηση (authorization)

Η εξουσιοδότηση αναφέρεται στην προστασία των πόρων των υπολογιστών με το να επιτρέπει οι πόροι να χρησιμοποιούνται από εκείνους που τους έχει εκχωρηθεί το δικαίωμα.

3.2.6. Αποδοχή (non-repudiation)

Η αποδοχή βοηθά στο να εξασφαλιστεί ότι οι οντότητες σε μία επικοινωνία δεν μπορούν να αρνηθούν ότι συμμετείχαν σε όλη την επικοινωνία ή σε ένα μέρος της επικοινωνίας. Συγκεκριμένα η οντότητα η οποία στέλνει το μήνυμα δεν μπορεί να αρνηθεί ότι έχει στείλει το μήνυμα και η οντότητα η οποία το δέχεται δεν μπορεί να αρνηθεί ότι το έχει δεχτεί. Η αποδοχή μπορεί να παρέχεται μέσα από την χρήση των τεχνικών κρυπτογράφησης ενός δημόσιου κλειδιού (public key) χρησιμοποιώντας ψηφιακές υπογραφές.

3.2.7. Ανωνυμία (anonymity)

Το μοναδικό προσδιοριστικό μπορεί να χρησιμοποιηθεί για να ακολουθήσει τα ίχνη ενός προσώπου ή ενός αντικειμένου που φέρει ένα tag στο χρόνο και στο χώρο. Αυτό μπορεί και να μην παρατηρηθεί από το άτομο του οποίου τα ίχνη ακολουθούνται. Οι πληροφορίες οι οποίες συλλέγονται μπορούν να συγχωνευτούν και να συνδεθούν προκειμένου να παραχθεί το προφίλ ενός ατόμου. Ένα παρόμοιο πρόβλημα εμφανίζεται στις εφαρμογές των ανεφοδιαστικών αλυσίδων, όπου οι ανεπιθύμητες ανιχνεύσεις προϊόντων είναι δυνατές. Η αυτοματοποιημένη ανάγνωση των tag επιτρέπει το μέτρημα των αντικειμένων (π.χ. τραπεζογραμμάτια με επισυναπτόμενα tags) το οποίο μπορεί να είναι ανεπιθύμητο.

ΚΕΦΑΛΑΙΟ 4

4.1. Βασικοί τύποι επίθεσης

Ο σκοπός των RFID συστημάτων είναι να επιτύχουν καλύτερη συμφωνία μεταξύ του εικονικού κόσμου των δεδομένων και του κόσμου των πραγματικών αντικειμένων. Είναι επομένως ύψιστης σημασίας για την ακεραιότητα των RFID συστημάτων ότι τρεις σχέσεις να εξασφαλίζονται:

- Η σχέση μεταξύ των δεδομένων που αποθηκεύονται στον transponder και με το transpoder κάθε αυτό. Αυτή πρέπει να είναι μία μοναδική σχέση, επειδή το transponder προσδιορίζεται αποκλειστικά από τα δεδομένα. Το σημαντικότερο μέρος των δεδομένων είναι ένας μοναδικός αριθμός ταυτότητας ID (serial number). Η ταυτότητα μπορεί επιπρόσθετα να προστατευτεί με την αποθήκευση των κλειδιών ή άλλων πληροφοριών ασφάλειας στον transponder. Είναι επιτακτικό να αποφευχθεί η ύπαρξη δυο tag που φέρουν την ίδια ταυτότητα.

- Η σχέση μεταξύ του transponder και του στοιχείου το οποίο προορίζεται να ταυτοποιηθεί. Αυτή η σχέση, επίσης, πρέπει να είναι μοναδική υπό την έννοια ότι ένας transponder δεν πρέπει ποτέ να οριστεί σε διαφορετικά στοιχεία ενώ είναι σε χρήση.

- Η σχέση μεταξύ του transponder και του reader. Αυτή η σχέση πρέπει να καθιερωθεί κατά τέτοιο τρόπο ώστε οι εξουσιοδοτημένοι readers να μπορούν να ανιχνεύσουν την παρουσία του transponder και να μπορούν να έχουν πρόσβαση στα δεδομένα με ορθό τρόπο, ενώ η πρόσβαση από τους μη εξουσιοδοτημένους readers φράζεται.

Από τις σχέσεις αυτές προκύπτουν οι βασικοί τύποι επίθεσης οι οποίοι είναι η εξής:

1. Παραποίηση του περιεχομένου (Falsification of contents)
2. Παραποίηση της ταυτότητας (transpoder) (Falsification of identity (transponder))
3. Απενεργοποίηση (Deactivation)
4. Αποσύνδεση του tag (Detaching the tag)
5. Να κρυφακούσει (Eavesdropping)
6. Φράξιμο (Blocking)
7. Μπλοκάρισμα (Jamming)
8. Παραποίηση της ταυτότητας (reader) (Falsifying identity (reader))

Ας δούμε ένα-ένα αναλυτικά τους βασικούς τύπους επίθεσης:

Παραποίηση του περιεχομένου (Falsification of content)

Τα στοιχεία μπορούν να παραποιηθούν από μη εξουσιοδοτημένη πρόσβαση γραφής στο tag. Αυτός ο τύπος επίθεσης είναι κατάλληλος για στοχευόμενη εξαπάτηση μόνο εάν, όταν πραγματοποιείται η επίθεση, η ταυτότητα ID (serial number) και

οποιεσδήποτε άλλες πληροφορίες ασφάλειας που μπορεί να υπάρχουν (π.χ. κλειδιά) παραμένουν αμετάβλητα. Με αυτόν τον τρόπο ο reader συνεχίζει ορθά να αναγνωρίζει την ταυτότητα των transponder. Αυτό το είδος επίθεσης είναι δυνατό μόνο στην περίπτωση των RFID συστημάτων που, εκτός από το ID και τις πληροφορίες ασφαλείας , αποθηκεύουν άλλες πληροφορίες στο tag.

Παραποίηση της ταυτότητας (transpoder) (Falsification of identity (transponder))

Ο επιτιθέμενος αποκτά το ID και οποιεσδήποτε πληροφορίες ασφάλειας του tag και τα χρησιμοποιεί για να εξαπατήσει τον reader στο να δεχτεί την ταυτότητα αυτού του ιδιαίτερου tag.Αυτή η μέθοδος επίθεσης μπορεί να πραγματοποιηθεί χρησιμοποιώντας μια συσκευή που είναι σε θέση να συναγωνιστεί οποιοδήποτε είδος tag ή με την παραγωγή ενός νέου tag ως αντίγραφο του παλαιού (cloning: κλωνοποίηση). Αυτό το είδος επίθεσης οδηγεί σε διάφορους transponders με την ίδια ταυτότητα που βρίσκονται σε κυκλοφορία.

Απενεργοποίηση (Deactivation)

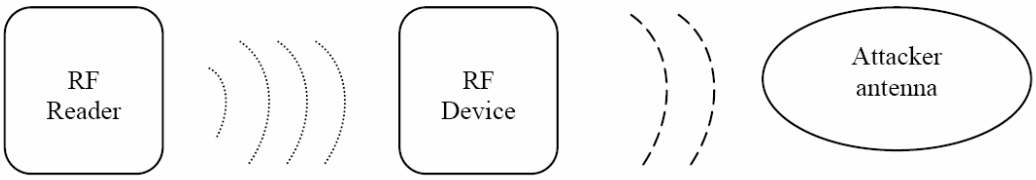
Αυτός ο τύπος επίθεσης καθιστά τον transponder άχρηστο μέσω της μη εξουσιοδοτημένης εφαρμογής των εντολών διαγραφής ή των εντολών θανάτωσης, ή μέσω της φυσικής καταστροφής. Ανάλογα με τον τύπο απενεργοποίησης, ο reader δεν μπορεί είτε πλέον να ανιχνεύσει την ταυτότητα του tag, είτε δεν μπορεί ακόμη και να ανιχνεύσει την παρουσία του tag στην εμβέλεια ανάγνωσης.

Αποσύνδεση του tag (Detaching the tag)

Ένα transponder είναι διαχωρισμένο φυσικά από το κολλημένο στοιχείο και μπορεί στη συνέχεια να συσχετιστεί με διαφορετικό στοιχείο, με τον ίδιο τρόπο με το οποίο που τα tags τιμών "εναλλάσσονται". Δεδομένου ότι τα συστήματα RFID εξαρτώνται απολύτως από το σαφή προσδιορισμό των κολλημένων στοιχείων από τους transponders, αυτός ο τύπος επίθεσης δημιουργεί ένα θεμελιώδες πρόβλημα ασφάλειας, ακόμα κι αν εμφανίζεται ασήμαντο εκ πρώτης όψεως.

Να κρυφακούσει (Eavesdropping ή Skimming)

Η επικοινωνία μεταξύ του reader και του transponder μέσω της διεπαφής αέρα ελέγχεται από υποκλοπή και την αποκωδικοποίηση των ράδιο σημάτων. Αυτή είναι μία από τις πιο συγκεκριμένες απειλές στα RFID συστήματα. Στο Σχήμα 4.1. απεικονίζεται το κρυφάκουσμα.



Σχήμα 4.1. Κρυφάκουσμα (eavesdropping/skimming)

Φράξιμο (Blocking)

Τα blocker tags υποδύονται εις τον reader την παρουσία οποιουδήποτε αριθμού από τους transponders, εμποδίζοντας κατά αυτόν τον τρόπο τον reader. Ένα blocker tag

πρέπει να διαμορφωθεί για το αντίστοιχο κατά της σύγκρουσης πρωτόκολλο το οποίο χρησιμοποιείται.

Μπλοκάρισμα (Jamming)

Τα στοιχεία τα οποία ανταλλάσσονται μέσω της διεπιφάνειας αέρα μπορούν να αναστατωθούν από τα παθητικά μέσα όπως η θωράκιση ή από τα ενεργά μέσα (πομποί μπλοκαρίσματος). Δεδομένου ότι η διεπαφή αέρα δεν είναι πολύ γερή, ακόμη και τα απλά παθητικά μέτρα μπορούν να είναι πολύ αποτελεσματικά.

Παραποίηση της ταυτότητας (reader) (Falsifying identity (reader))

Σε ένα ασφαλές σύστημα RFID ο reader πρέπει να αποδείξει την εξουσιοδότησή του στο tag. Εάν ένας επιτιθέμενος θέλει να διαβάσει τα δεδομένα με τον reader του, αυτό πρέπει να προσποιηθεί την ταυτότητα ενός εξουσιοδοτημένου reader. Ανάλογα με τα μέτρα ασφάλειας σε ισχύ, μια τέτοια επίθεση μπορεί να είναι "πολύ εύκολη" μέχρι "πρακτικά αδύνατο" να πραγματοποιηθεί. Ο reader μπορεί να χρειαστεί πρόσβαση στο backend με σκοπό, παραδείγματος χάριν, να ανακτήσει τα κλειδιά που αποθηκεύονται εκεί.

4.2. Τύποι επιθέσεων σύμφωνα με τον αντικειμενικό στόχο τους

Προτού να μπορέσουμε *να* αναλύσουμε τις πιθανές επιθέσεις, πρέπει *να* προσδιορίσουμε τους πιθανούς στόχους. Ένας στόχος μπορεί να είναι ένα ολόκληρο

σύστημα (εάν η πρόθεση είναι να διαταράξει εντελώς μια επιχείρηση), ή μπορεί να είναι οποιοδήποτε τμήμα του γενικού συστήματος (από μια λιανική βάση δεδομένων καταλόγων σε ένα πραγματικό λιανικό στοιχείο). Εκείνοι οι οποίοι ασχολούνται στην τεχνολογική ασφάλεια πληροφοριών τείνουν να επικεντρώνονται απλώς "στην προστασία των δεδομένων." Όταν κάνουμε εκτίμηση και εφαρμόζουμε ασφάλεια γύρω από RFID, είναι σημαντικό να θυμόμαστε ότι μερικά περιουσιακά στοιχεία είναι σημαντικότερα από τα πραγματικά δεδομένα. Τα δεδομένα ίσως να μην επηρεαστούν ποτέ, ακόμα κι αν ο οργανισμός θα μπορούσε ακόμα να υποστεί τεράστια απώλεια.

Για παράδειγμα σε ένα λιανικό κατάστημα όταν ένα RFID tag μεταχειριστεί επιδέξια ώστε η τιμή στο POS να μειωθεί από μια μεγαλύτερη τιμή σε μία πιο χαμηλή το κατάστημα πάλι θα έχανε, αλλά χωρίς ζημιά στο σύστημα βάσεων δεδομένων καταλόγων. Η βάση δεν δέχτηκε επίθεση απευθείας και τα δεδομένα στην βάση δεν μεταχειρίσθηκαν επιδέξια ή διαγράφηκαν, και ακόμα, μία απάτη διαπράχθηκε επειδή μέρος του συστήματος RFID μεταχειρίστηκαν επιδέξια.

Κάποιος που επιτίθεται σε ένα σύστημα RFID μπορεί να το χρησιμοποιήσει για να κλέψει ένα μοναδικό αντικείμενο, ενώ μια άλλη επίθεση μπορεί να χρησιμοποιείται για να εμποδίσει όλες τις πωλήσεις σε ένα μοναδικό κατάστημα ή σε μια αλυσίδα καταστημάτων.

Ένα πρόσωπο που επιτίθεται σε ένα σύστημα RFID μπορεί να ακολουθήσει διάφορους στόχους, οι οποίοι μπορούν να ταξινομηθούν ως εξής:

Κατασκόπευση (Spying)

Ο επιτιθέμενος κερδίζει μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες.

Εξαπάτηση (Deception)

Ο επιτιθέμενος εξαπατά το χειριστή ή το χρήστη ενός συστήματος RFID με την τροφοδότηση λανθασμένων πληροφοριών.

Denial of Service (DoS)

Η διαθεσιμότητα των λειτουργιών του συστήματος RFID συμβιβάζεται.

Προστασία της ιδιωτικότητας (Protection of privacy)

Επειδή ο επιτιθέμενος θεωρεί ότι η ιδιωτικότητα του απειλείται από το σύστημα RFID, προστατεύεται με να επιτεθεί στο σύστημα.

Ο Πίνακας 4.1 παρακάτω δείχνει ότι τους βασικούς τύπους επίθεσης που αναλύσαμε παραπάνω ανάλογα με τον σκοπό τους.

	Κατασκόπευση	Εξαπάτηση	Denial of Service (Dos)	Προστασία της ιδιωτικότητας
Παραποίηση του περιεχομένου				
Παραποίηση της ταυτότητας (transpoder)				
Απενεργοποίηση				
Αποσύνδεση του tag				
Να κρυφακούσει				
Φράξιμο				
Μπλοκάρισμα				
Παραποίηση της ταυτότητας (reader)				

Πίνακας 4.1. Οι βασικοί τύποι επίθεσης ανάλογα με τον σκοπό τους.

Πρέπει να σημειωθεί ότι σε ένα χαρακτηριστικό πλαίσιο στο οποίο τα συστήματα RFID χρησιμοποιούνται, υπάρχουν δύο συμβαλλόμενα μέρη με διάφορα ενδιαφέροντα. Υπάρχει και ένα άλλο μέρος το οποίο λέγεται third party.

Active party

Είναι ο χειριστής του συστήματος RFID, εφεξής καλούμενος το ενεργό συμβαλλόμενο μέρος. Το ενεργό συμβαλλόμενο μέρος ασκεί τον έλεγχο επάνω στα δεδομένα του συστήματος RFID και πάνω στη χρήση για το ποια δεδομένα τοποθετούνται. Είναι αυτό το μέρος το οποίο εκδίδει τα tags και διαχειρίζεται τα δεδομένα που συνδέονται με αυτά.

Passive party

Είναι ο πραγματικός μεταφορέας ενός tag ή ενός στοιχείου ενσωματωμένου με tag. Αυτό το μέρος είναι συνήθως ένας πελάτης ή ένας υπάλληλος του χειριστή. Το παθητικό συμβαλλόμενο μέρος κατέχει τα tags, αλλά κανονικά δεν έχει καμία επιρροή στον τρόπο με τον οποίο χρησιμοποιούνται.

Third party

Ένας τρίτος επιτίθεται σε ένα σύστημα RFID προκειμένου να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα.

4.3. Απειλές στο Active και στο Passive Party

Οι επιθέσεις μπορούν είτε να στοχεύσουν στο ενεργό συμβαλλόμενο μέρος (active party), είτε στο παθητικό συμβαλλόμενο μέρος.

4.3.1. Απειλές στο Active Party

Ένας επιτιθέμενος μπορεί να είναι το passive party όπως είναι οι υπάλληλοι και οι πελάτες ή ένα τρίτο συμβαλλόμενο μέρος (third party) το οποίο μπορεί να είναι τρομοκράτες, βιομηχανικοί κατάσκοποι και οι ανταγωνιστικές εταιρίες. Οι απειλές στο active party είναι:

- Κατασκόπευση δεδομένων (Spying out data)
- Τροφοδότηση με λανθασμένα δεδομένα (Εξαπάτηση) (Feeding in false data (deception))
- Denial of Service (DoS)

Κατασκόπευση δεδομένων (Spying out data)

Ένας επιτιθέμενος μπορεί να κατασκοπεύσει τα δεδομένα με τον ακόλουθο τρόπο:

- Μπορεί να χρησιμοποιήσει το δικό του δέκτη για να ακούσει την επικοινωνία μεταξύ των tags και των readers.

- Μπορεί να χρησιμοποιήσει τον δικό του reader για να διαβάσει τα δεδομένα από τα tags. Η συσκευή μπορεί να εγκατασταθεί σε μια κρυμμένη θέση, ή μπορεί να χρησιμοποιηθεί κατά τρόπο κινητό. Εάν ο reader απαιτεί επικύρωση, ο επιτιθέμενος πρέπει να είναι σε θέση να πλαστογραφήσει την ταυτότητα του reader.

Τροφοδότηση με λανθασμένα δεδομένα (Εξαπάτηση) (Feeding in false data (deception))

Ένας επιτιθέμενος μπορεί να πραγματοποιήσει τις ακόλουθες επιθέσεις με σκοπό την εξαπάτηση:

- Μπορεί να αλλάξει το περιεχόμενο αλλά όχι την ταυτότητα ID ενός υπάρχοντος tag. Αυτό είναι δυνατό μόνο εάν τα δεδομένα που συνδέονται με την ταυτότητα ID αποθηκεύονται στα tags από μόνα τους, το οποίο για τις περισσότερες εφαρμογές δεν είναι απαραίτητο.

- Μπορεί να μιμηθεί ή να αναπαραγάγει tags (κλωνοποίηση) προκειμένου να εξαπατήσει τον reader στο να δεχτεί την ταυτότητα αυτών. Για να το επιτύχει αυτό, πρέπει πρώτα να ανακαλύψει τουλάχιστον τις ταυτότητες IDs και , εξαρτώμενος από τις διαδικασίες ασφάλειας, επίσης οποιουσδήποτε κωδικούς πρόσβασης ή κλειδιά.

- Μπορεί να αποσυνδέσει το tag από το στοιχείο που είναι ενσωματωμένο με tag προκειμένου να αποκρύψει τις κινήσεις του στοιχείου από τον reader, ή να διεξάγει άλλο στοιχείο ως το αρχικό στοιχείο ενσωματωμένο με tag. Ανάλογα με τα μηχανικά μέτρα ασφάλειας που βρίσκονται σε ισχύ, θα πρέπει να βλάψει στοιχείο το οποίο είναι ενσωματωμένο με tag για να επιτύχει τον στόχο του, ο οποίος σε πολλές περιπτώσεις σε μεγάλο βαθμό μικραίνει τη χρησιμότητα της επίθεσης.

Denial of Service (DoS)

Ένας επιτιθέμενος έχει πολλούς τρόπους να εξασθενίσει τη σωστή λειτουργία ενός συστήματος RFID και έτσι να υπονομεύσει τη συμφωνία μεταξύ του πραγματικού και εικονικού κόσμου που αυτά τα συστήματα επιδιώκουν να επιτύχουν:

- Τα tags καταστρέφονται από μηχανικά ή χημικά μέσα (μέσω της κάμψης, με την εφαρμογή των φορτίων πίεσης ή έντασης, μέσω της δράσης του οξέος, κ.λ.π.).

- Τα tags καταστρέφονται μέσω της επίδρασης των ηλεκτρομαγνητικών πεδίων, παρόμοια με την κανονική διαδικασία για την απενεργοποίηση των 1-bit transponder. Σε γενικές γραμμές, αυτή η επίδραση μπορεί να επιτευχθεί από τους πομπούς οι οποίοι σχεδιάζονται συγκεκριμένα για αυτόν το λόγο, αλλά και από τους φούρνους μικροκυμάτων ή τους ισχυρούς επαγωγικούς σπινθήρες.

- Τα tags τίθενται εκτός δράσης μέσα από την κακή χρήση των εντολών διαγραφής ή θανάτωσης. Τέτοια κακή χρήση προϋποθέτει τη δυνατότητα του επιτιθεμένου να προσποιηθεί την ταυτότητα μιας εξουσιοδοτημένης συσκευής ανάγνωσης ή γραψίματος.

- Η μπαταρία ενός active tag εκφορτίζεται από μία σειρά ερωτημάτων. Αυτή η μέθοδος δεν λειτουργεί στην περίπτωση των passive tag, επειδή αντλούν την ενέργειά τους αποκλειστικά από τον τομέα ανεφοδιασμού που παρέχεται από τον reader.

- Ένα blocker tag εξομοιώνει την παρουσία οποιουδήποτε αριθμού από tags στον reader προκειμένου να αποτρέψει τα πραγματικά tags να διαβαστούν.

- Οι jamming πομποί αποτρέπουν την επικοινωνία μεταξύ του reader και του tag. Προκειμένου να είναι αποτελεσματικά για μεγάλες αποστάσεις, θα απαιτούνταν πολύ ισχυροί πομποί. Μια τέτοια επίθεση θα ήταν εύκολο να ανιχνευθεί.

- Τα ανακλώμενα αντικείμενα είναι ικανά για την ακύρωση ενός ηλεκτρομαγνητικού πεδίου.

- Η εγγύτητα, για παράδειγμα του νερού, μετάλλου ή του φερρίτη οδηγεί στον αποσυντονισμό του πεδίου συχνότητας.

- Τα φύλλα μετάλλου ή οι τσάντες με μεταλλικές λωρίδες προστατεύουν τα tags από τα ηλεκτρομαγνητικά πεδία.

4.3.2. Απειλές στο Passive Party

Το passive party χρησιμοποιεί tags ή στοιχεία τα οποία έχουν ταυτοποιηθεί από τα tags, αλλά το passive party δεν έχει καθόλου έλεγχο στα δεδομένα τα οποία έχουν αποθηκευτεί στα tags. Η μυστικότητα μπορεί να απειληθεί από το active party ή από το third party.

Είναι προφανές ότι στην πρώτη περίπτωση καμία επίθεση στο σύστημα RFID δεν απαιτείται, επειδή το σύστημα είναι υπό πλήρη έλεγχο του active party. Το active party ίσως, για παράδειγμα, να παραβιάσει την τρέχουσα προστασία δεδομένων

(μυστικότητα) με το να δώσει τα δεδομένα χωρίς την γνώση των ανθρώπων που εμπλέκονται.

Στη δεύτερη περίπτωση, ένας τρίτος επιτίθεται σε ένα σύστημα RFID προκειμένου να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα. Οι συνέπειες για το passive party είναι παρόμοιες με αυτές της πρώτης περίπτωσης, αφού τα ευαίσθητα δεδομένα περνούν σε λανθασμένα χέρια χωρίς την γνώση και την σύμφωνη γνώμη των ανθρώπων που τους αφορά.

- Απειλή στην μυστικότητα των δεδομένων (Threat to data privacy)
- Απειλή στην τοποθεσία της μυστικότητας (Threat to location privacy)

Απειλή στην μυστικότητα των δεδομένων (Threat to data privacy)

Αποθηκεύοντας δεδομένα ενός συγκεκριμένου ατόμου σε ένα RFID σύστημα μπορούν να απειλήσουν τη μυστικότητα του passive party. Θα ασχοληθούμε εδώ μόνο με τις συγκεκριμένες πτυχές RFID της κατάστασης απειλής:

- Με το να κρυφακούσει στη διεπαφή αέρα ή από την μη εξουσιοδοτημένη ανάγνωση των tag, ένας πιθανός επιτιθέμενος έχει νέες μεθόδους στη διάθεσή του για να κερδίσει μη εξουσιοδοτημένη πρόσβαση στα δεδομένα.

- Ξέχωρα από τα δεδομένα ενός συγκεκριμένου ατόμου, ακόμη και τα πιθανά δεδομένα του συγκεκριμένου ατόμου θα μπορούσαν όλο και περισσότερο να γίνουν ο στόχος μιας επίθεσης. Παρόλο που αυτά τα δεδομένα είναι ανώνυμα

ή, με ψευδώνυμο, η πιθανότητα είναι υψηλή ότι μπορούν να γίνουν επώνυμα αργότερα και επομένως επιτρέπουν εύλογα συμπεράσματα να συναχθούν για τα άτομα. Με το RFID, η χρονική και χωρική πυκνότητα των ιχνών των δεδομένων που αφήνονται από τα άτομα αυξάνεται, έτσι σύμφωνα με τους στατιστικούς όρους βελτιώνονται οι πιθανότητες της μη ανωνυμίας.

- Ο προκύπτων υψηλός βαθμός συμφωνίας μεταξύ του εικονικού και του πραγματικού κόσμου, που είναι ένας δηλωμένος στόχος για χρησιμοποιούμενα συστήματα RFID, μπορεί να προκαλέσει την ώθηση εκ μέρους των active parties όπως και των third parties (π.χ. επίσης οι κρατικοί ρυθμιστικοί οργανισμοί) για να εκτελέσουν νέες αξιολογήσεις που μπορεί να μην είναι απαραίτητα στο ενδιαφέρον των passive parties. Δεδομένου ότι τα δεδομένα γίνονται ευπρόσιτα, οι κίνδυνοι αυξάνονται ότι οι βάσεις δεδομένων νωρίτερα ή αργότερα θα αξιολογηθούν για λόγους εκτός από εκείνους που προορίζονταν αρχικά, χωρίς τη γνώση των ανθρώπων που επηρεάζονται.

Απειλή στην τοποθεσία της μυστικότητας (Threat to location privacy)

Υποθέτοντας ότι τα tags θα παραμείνουν στην κατοχή του ίδιου προσώπου κατά μεγάλη χρονική περίοδο, η επαναλαμβανόμενη ανάγνωση των ταυτοτήτων IDs επιτρέπει να παραχθούν σχεδιαγράμματα μετακίνησης (tracking:καταδίωξη). Αυτή η δυνατότητα γίνεται μια απειλή για την μυστικότητα, εάν και όταν τα συστήματα RFID γίνονται ένα πανταχού παρόν μέρος της καθημερινής ζωής. Ακόμα κι αν τίποτα εκτός από τα IDs διαβιβάζονται κατά τη διάρκεια ανάγνωσης των RFID tags, ενώ όλα

τα άλλα στοιχεία μετατοπίζονται στο backend, μία απειλή στην μυστικότητα μπορεί να προκύψει. Όσο περισσότερα tags είναι στην κυκλοφορία, τόσο καλύτερες είναι οι πιθανότητες η παρακολούθηση των ιχνών (tracking) να πραγματοποιηθεί. Παρακολουθώντας τα ίχνη περισσότερων από έναν ανθρώπων επίσης επιτρέπει στα σχεδιαγράμματα επαφών να καθιερωθούν.

Πάλι, ένα συγκεκριμένο χαρακτηριστικό του RFID είναι η πιθανότητα να κρυφακούσει κάποιος στη διεπιφάνεια του αέρα. Από την άλλη πλευρά, η πιθανότητα δεν μπορεί να αποκλειστεί ότι οι επιθέσεις στην περιοχή του backend θέτει μία μεγαλύτερη απειλή στην μυστικότητα από τις επιθέσεις στην διεπιφάνεια του αέρα. Σε σύγκριση με την χρήση των κινητών τηλεφώνων, η χρήση των RFID tags παράγει ακριβέστερα ίχνη δεδομένων, επειδή όχι μόνο η γεωγραφική θέση, αλλά και η συγκεκριμένη αλληλεπίδραση με τις υπάρχουσες εταιρίες και τις υποδομές μπορούν να καθοριστούν.

ΚΕΦΑΛΑΙΟ 5

5.1. Μέτρα για την προφύλαξη της ασφάλειας

Οι αποτελεσματικοί μηχανισμοί ασφάλειας μπορούν να παρέχουν προστασία ενάντια στις περιγεγραμμένες απειλές. Αλλά πρέπει να ληφθεί υπόψη ότι ο αρχικός σκοπός της τεχνολογίας RFID είναι η πραγματοποίηση της φτηνής και αυτοματοποιημένης ταυτοποίησης. Παρακάτω, περιγράφουμε τους εφαρμοσμένους και προτεινόμενους μηχανισμούς ασφάλειας RFID:

1. Επικύρωση
    - Ελέγχοντας την ταυτότητα του tag
    - Ελέγχοντας την ταυτότητα του reader
    - Δυνατή αμοιβαία επικύρωση
2. Κρυπτογράφηση
3. Πρωτόκολλα αντι-σύγκρουσης τα οποία είναι ασφαλή από το κρυφάκουσμα
    - Silent Tree-Walking
    - Aloha διαδικασία με προσωρινά IDs
4. Ψευδωνυμία
    - Τυχαία hash-lock
    - Chained Hashes
    - Διαδικασία από τον Henrici και τον Muller

5. Παρεμπόδιση της ανάγνωσης
    - Χρήση των Blocker tags

6. Οριστική απενεργοποίηση
    - Διαταγή θανάτωσης
    - Τομέας τεχνικής απενεργοποίησης
7. Μετασχηματίζοντας πρακτικές δίκαιων πληροφοριών σε RFID πρωτόκολλα

5.2. Επικύρωση

Όταν η επικύρωση πραγματοποιείται, η ταυτότητα ενός ανθρώπου ή ενός προγράμματος ελέγχεται. Κατόπιν, σε εκείνη την βάση, η εξουσιοδότηση πραγματοποιείται, δηλ. δικαιώματα, όπως το δικαίωμα της πρόσβασης στα δεδομένα, χορηγείται. Στην περίπτωση των συστημάτων RFID, είναι ιδιαίτερα σημαντικό για τα tags να επικυρωθούν από τον reader και αντίστροφα. Επιπλέον, οι readers πρέπει επίσης να επικυρώσουν τον εαυτό τους στο backend, αλλά σε αυτήν την περίπτωση δεν υπάρχουν συγκεκριμένα RFID προβλήματα ασφάλειας.

5.2.1. Ελέγχοντας την ταυτότητα του tag

Όταν το σύστημα RFID ανιχνεύει ένα tag, πρέπει να ελέγξει την ταυτότητά του προκειμένου να εξακριβωθεί εάν το tag έχει το δικαίωμα για να είναι μέρος του συστήματος . Ένας παγκόσμιος και σαφής κανονισμός για την έκδοση των αριθμών ταυτότητας ID, όπως προτείνεται, παραδείγματος χάριν, υπό μορφή ηλεκτρονικού

κώδικα προϊόντων (EPC), προσφέρει, μία αναμφίβολη ποσότητα προστασίας από πλαστογραφημένα tags. Στο ελάχιστο, η εμφάνιση των αριθμών που δεν εκδόθηκαν ποτέ ή των αντιγράφων (κλωνοποίηση) μπορούν να αναγνωριστούν σε ορισμένες εφαρμογές.

Επιπλέον, η επικύρωση μπορεί να πραγματοποιηθεί μέσω του συστήματος πρόκληση-απάντησης (challenge-response system), στο οποίο ο reader στέλνει έναν τυχαίο αριθμό ή ένα χρονικό γραμματόσημο στο tag (πρόκληση) το οποίο το tag το επιστρέφει με κρυπτογραφημένη μορφή στον reader (απάντηση).Το κλειδί χρησιμοποιούμενο σε αυτήν την περίπτωση είναι ένα από κοινού γνωστό μυστικό με τη βοήθεια του οποίου το tag αποδεικνύει την ταυτότητά του. Το αποφασιστικό στοιχείο σε αυτήν την διαδικασία είναι το γεγονός ότι το ίδιο το κλειδί δεν διαβιβάζεται ποτέ και ότι ένας διαφορετικός τυχαίος αριθμός χρησιμοποιείται για κάθε πρόκληση. Κατά συνέπεια, ο reader δεν μπορεί να εξαπατηθεί από την επικοινωνία που καταγράφεται και που επαναλαμβάνεται (replay attack:επίθεση επανάληψης). Αυτή η μονομερής διαδικασία επικύρωσης ορίζεται στα πρότυπα του ISO9798 ως "symmetric-key two-pass unilateral authentication protocol ".

Ένας επιτιθέμενος θα πρέπει να εξασφαλίσει το κλειδί που αποθηκεύεται και στο tag και στο backend του RFID συστήματος. Προκειμένου να το κάνει αυτό, θα ήταν απαραίτητο να αποκωδικοποιηθούν τα στοιχεία απάντησης που μεταδόθηκαν σε κρυπτογραφημένη φόρμα, το οποίο είναι ένας πολύ σύνθετος εάν όχι σχεδόν αδύνατος στόχος, ανάλογα με το μήκος του κλειδιού. Σε γενικές γραμμές, το κλειδί θα μπορούσε επίσης να διαβαστεί με τα φυσικά μέσα από τα κελιά αποθήκευσης του

τσιπ, αλλά αυτό θα απαιτούσε περίπλοκες μεθόδους του εργαστηρίου, όπως την τεχνική "Focused Ion Beam" (FIB: Focused Ion Beam). Σε αυτήν την διαδικασία, μια ιονική ακτίνα αφαιρεί τα πολύ λεπτά στρώματα (μερικά στρώματα από ατόμα) σε χωριστά βήματα έτσι ώστε το περιεχόμενο μπορεί να αναλυθεί μικροσκοπικά. Μια μέθοδος πρόκλησης-απάντησης μπορεί επίσης να χρησιμοποιηθεί για την αμοιβαία επικύρωση του reader και του tag. Σε αυτήν την περίπτωση, το tag πρέπει επίσης να είναι ικανό να παράγει τυχαίους αριθμούς.

5.2.2. Ελέγχοντας την ταυτότητα του reader

Η πιο απλή μέθοδος επικύρωσης του reader σε σχέση με το tag είναι να χρησιμοποιείται κωδικός πρόσβασης, δηλ. ο reader προσδιορίζεται στο tag με τη μετάδοση του κωδικού πρόσβασης. Το transponder συγκρίνει αυτόν τον κωδικό πρόσβασης με τον κωδικό πρόσβασης που αποθηκεύεται στη μνήμη. Εάν και οι δύο είναι ίδιοι, το tag χορηγεί πλήρη πρόσβαση στα αποθηκευμένα δεδομένα. Μερικά προϊόντα χορηγούν την προστασία κωδικού πρόσβασης για επιλεγμένους τομείς της μνήμης.

Στα απλά συστήματα, όλα τα tags περιέχουν τον ίδιο κωδικό πρόσβασης σε έναν προστατευμένο τομέα των μνημών τους. Στα περιπλοκότερα read-only συστήματα σε κάθε transponder ορίζεται ένας μεμονωμένος κωδικός πρόσβασης από τον κατασκευαστή, ο οποίος αποθηκεύεται έπειτα στη μνήμη του με τη βοήθεια ενός λέιζερ. Οι μεταβλητοί κωδικοί είναι σε θέση να παρέχουν την καλύτερη προστασία,

αλλά λειτουργούν μόνο με τους read-write transponders. Το μήκος ενός χαρακτηριστικού κωδικού πρόσβασης θα ήταν 8, 24 ή 32 bits.

Τα συστήματα κωδικού πρόσβασης χωρίς κρυπτογράφηση θεωρούνται ως αδύνατη μέθοδος προσδιορισμού, επειδή επιτρέπουν το κρυφάκουσμα στη μετάδοση κωδικού πρόσβασης μέσω της επισφαλούς διεπαφής αέρα. Επιπλέον, οι σύντομοι κωδικοί πρόσβασης μπορούν να σπάσουν απλά από την συστηματική εμπειροτεχνική μέθοδο (trial-and-error).

Τα συστήματα κωδικού πρόσβασης χωρίς κρυπτογράφηση μπορεί να είναι επαρκής σε περιπτώσεις όπου το tag εξετάζεται ακριβώς μόλις μία φορά ή όπου ο κίνδυνος ανακάλυψης του κωδικού πρόσβασης με την κατασκόπευση είναι ήδη χαμηλός. Εάν η πρόσβαση απαιτείται μόνο για έναν περιορισμένο αριθμό χρόνων, ένας κατάλογος μίας και μοναδικής φοράς κωδικών πρόσβασης που αποθηκεύονται στον transponder και στο backend μπορεί επίσης να χρησιμοποιηθεί αντί ενός μοναδικού κωδικού πρόσβασης.

Σε αντίθεση με τις κρυπτογραφικές διαδικασίες, τέτοια συστήματα κωδικού πρόσβασης προβάλλουν λίγες απαιτήσεις στα tags και μπορούν να εφαρμοστούν με τα απλά read-only tags.

Βελτιωμένη ασφάλεια ενάντια στις μη εξουσιοδοτημένες αναγνώσεις επιτυγχάνεται από τη διαδικασία hash-lock. Σε αυτή την περίπτωση, πριν το tag γραφτεί για πρώτη φορά, μία αποκαλούμενη μετα-ταυτότητα ID παράγεται από ένα κλειδί ως

ψευδώνυμο για το tag. Αυτό γίνεται με την βοήθεια μιας hash λειτουργίας, ο υπολογισμός της οποίας είναι σχεδόν αμετάκλητος, και η μετα ταυτότητα ID αποθηκεύεται στο tag. Από εκείνη την στιγμή το tag κλειδώνεται, δηλαδή, αυτό αντιδρά στα σήματα του reader απλώς με την μετάδοση της μετα ταυτότητας ID.Για να ξεκλειδώσει το tag, ο reader πρέπει να ανακτήσει από μια βάση δεδομένων backend το κλειδί που ανήκει στη μετα-ταυτότητα ID και το διαβιβάσει έπειτα στο tag. Το tag εφαρμόζει τη hash λειτουργία στο κλειδί που έχει λάβει και ελέγχει εάν το αποτέλεσμα είναι ίδιο με την μετα ταυτότητά του. Εάν αυτό συμβαίνει, ο reader επικυρώνεται και το tag επιτρέπει την πρόσβαση στα δεδομένα του.

Θα ήταν σχεδόν αδύνατο για έναν επιτιθέμενο να υπολογίσει το αρχικό κλειδί. Επομένως σε πολλές πρακτικές περιοχές επέκτασης μια μετα ταυτότητα είναι μία αρκετή προστασία ενάντια στην μη εξουσιοδοτημένη ανάγνωση. Εντούτοις, κατά τη διάρκεια της μετάδοσης μέσω της διεπαφής του αέρα το μυστικό κλειδί το οποίο ανήκει σε μια μετα ταυτότητα μπορεί να κατασκοπευτεί από έναν επιτιθέμενο που μπορεί αργότερα να εξαπατήσει το tag με το να αναγνώρισει έναν reader ως εξουσιοδοτημένο (replay attack). Η hash διαδικασία μπορεί να εφαρμοστεί για τους transponders ακόμη και χωρίς την χρησιμοποίηση των περίπλοκων cryptoprocessors έτσι ώστε αυτή η διαδικασία να μπορεί να χρησιμοποιηθεί ακόμη και για ανέξοδους transponders.

Η μέγιστη προστασία ενάντια στην μη εξουσιοδοτημένη πρόσβαση στα tags παρέχεται από τις διαδικασίες επικύρωσης με την κρυπτογράφηση σύμφωνα με την αρχή πρόκλησης-απάντησης (ισχυρές κρυπτογραφικές διαδικασίες). Εντούτοις, αυτές οι διαδικασίες προϋποθέτουν ότι το tag μπορεί όχι μόνο να εκτελέσει

κρυπτογραφικούς αλγόριθμους αλλά μπορεί επίσης να παράγει τους τυχαίους αριθμούς. Στην περίπτωση των tags που ικανοποιούν αυτές τις απαιτήσεις και μπορούν επομένως να ελέγξουν την εξουσιοδότηση του reader σε υψηλό επίπεδο ασφάλειας, δεν αξίζει να γίνουν οι συμβιβασμοί όταν εμφανίζεται το αντίστροφο πρόβλημα (επικύρωση του tag στον reader), επειδή η ικανότητα επεξεργασίας του reader ή του backend δεν αποτελεί μια δυσχέρεια. Συνεπώς, στην περίπτωση των υψηλής απόδοσης transponder οι ισχυρές αμοιβαίες διαδικασίες είναι κατάλληλες.

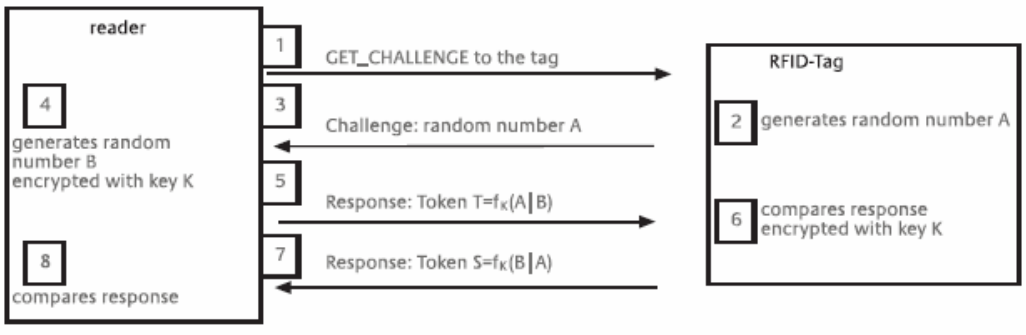
5.2.3. Δυνατή αμοιβαία επικύρωση

Το πρότυπο του ISO 9798 καθορίζει διάφορες διαδικασίες πρόκλησης-απάντησης για ισχυρή επικύρωση στην περίπτωση των έξυπνων καρτών επαφών και των συστημάτων RFID, συμπεριλαμβανομένης της αμοιβαίας επικύρωσης σύμφωνα με το "αμοιβαίο πρωτόκολλο επικύρωσης three-pass ".

Όταν ένα tag λαμβάνει μία εντολή "get challenge" από έναν reader, παράγει έναν τυχαίο αριθμό A και τον στέλνει στον reader. Ο reader παράγει στη συνέχεια έναν τυχαίο αριθμό B και με αυτό τον αριθμό και με τον τυχαίο αριθμό A ιεραρχεί ένα κρυπτογραφημένο data block (σύμβολο T) στην βάσει ενός αλγορίθμου κρυπτογράφησης και ενός μυστικού κλειδιού K. Δεδομένου ότι και οι δύο πλευρές χρησιμοποιούν τον ίδιο αλγόριθμο κρυπτογράφησης και δεδομένου ότι το κλειδί K αποθηκεύεται στο tag, το tag είναι σε θέση να φανερώσει αποκρυπτογραφήσει το σύμβολο T. Εάν ο αρχικός τυχαίος αριθμός A και ο τυχαίος αριθμός A’, που έχει αποκρυπτογραφηθεί τώρα, είναι ίδιοι, αυτό αποδεικνύει την αυθεντικότητα του

reader. Η διαδικασία επαναλαμβάνεται τώρα προκειμένου να επικυρωθεί το tag στον reader. Σε αυτήν την περίπτωση, ένα δεύτερο σύμβολο παράγεται στο tag και μεταδίδεται στον reader. Εάν οι αποκρυπτογραφημένοι τυχαίοι αριθμοί B και B' είναι ίδιοι, κατόπιν η αυθεντικότητα του tag έναντι του reader έχει επίσης αποδειχθεί.

Σε αυτή την διαδικασία κανένα μυστικό κλειδί δεν διαβιβάζεται πάντα μέσω της επισφαλούς διεπαφής του αέρα. Αντ' αυτού μόνο οι κρυπτογραφημένοι τυχαίοι αριθμοί χρησιμοποιούνται, το οποίο δίνει έναν υψηλό βαθμό προστασίας ενάντια στην μη εξουσιοδοτημένη πρόσβαση. Ούτε μπορεί η καταγραφή και ως επακόλουθο η επανάληψη της μονογραφής της σειράς (επίθεση επανάληψης) να αποκτήσει πρόσβαση στο tag ή στον reader. Χώρια από τις διαδικασίες επικύρωσης βασισμένες στο συμμετρικό σύστημα κρυπτογραφίας, που περιγράφονται εδώ, διαδικασίες βασισμένες στο ασυμμετρικό σύστημα κρυπτογραφίας είναι επίσης πιθανές για χρήση μέσα στα συστήματα RFID. Το Σχήμα 5.1 απεικονίζει την διαδικασία challenge-response για την αμοιβαία επικύρωση.



Σχήμα 5.1. Η διαδικασία challenge-response για αμοιβαία επικύρωση

5.3. Κρυπτογράφηση

Η κρυπτογράφηση των δεδομένων που διαβιβάζονται είναι μια μέθοδος προστασίας εναντίων του κρυφακούσματος στην επικοινωνία μέσω της διεπαφής αέρα. Η κρυπτογράφηση συνδέεται στενά με την επικύρωση. Εάν ένας transponder σχεδιάζεται για ισχυρές κρυπτογραφικές διαδικασίες, όχι μόνο ισχυρή αμοιβαία επικύρωση αλλά και ασφαλής κρυπτογράφηση των δεδομένων που διαβιβάζονται μπορούν να επιτευχθεί. Ειδικότερα, η διαδικασία επικύρωσης three-pass που περιγράφεται ανωτέρω μπορεί να χρησιμοποιηθεί για να παράγει ένα κοινό προσωρινό κλειδί (session key) από τους τυχαίους αριθμούς της ακολουθίας μονογράφησης για να κρυπτογραφήσει τα δεδομένα που θα διαβιβαστούν στη συνέχεια.

Εάν, εντούτοις, ο transponder δεν υποστηρίζει ισχυρές κρυπτογραφικές διαδικασίες, μόνο η αδύναμη επικύρωση είναι δυνατή. Για τους ίδιους λόγους, η αξιόπιστη κρυπτογράφηση των μεταδιδόμενων δεδομένων δεν είναι έπειτα δυνατή ούτε τότε.
Το πιο αποτελεσματικό μέτρο προστασίας εναντίων μιας επίθεσης με χαρακτηριστικό το κρυφάκουσμα στη διεπαφή του αέρα είναι, ωστόσο, όχι να αποθηκεύσει οποιοδήποτε περιεχόμενο στο ίδιο το tag και αντί γι αυτό να διαβάσει μόνο την ταυτότητα ID του tag. Τα δεδομένα που συνδέονται με το tag ανακτώνται από μια βάση δεδομένων backend.

Αυτό το μέτρο, που συχνότερα συστήνεται στην τεχνική βιβλιογραφία και που υποτίθεται από την EPCglobal προσφέρει τα πρόσθετα πλεονεκτήματα το ότι

λιγότερο ακριβά tags μπορούν να χρησιμοποιηθούν, η μνήμη με τα σχετιζόμενα δεδομένα στο backend είναι σχεδόν απεριόριστη, και οι συνηθισμένες διαδικασίες για την διαχείριση των δεδομένων και ασφάλειας IT μπορούν να χρησιμοποιηθούν.

Το πρόβλημα της προστασίας της διεπαφής του αέρα από το κρυφάκουσμα περιορίζεται στη διαδικασία επικύρωσης και στη μετάδοση του αριθμού ταυτότητας ID. Το πρόβλημα επικύρωσης λύνεται με την εφαρμογή των διαδικασιών επικύρωσης, και το να κρυφακούσει για να λάβει την ταυτότητα δεν αποτελεί μια απειλή σε πολλές εφαρμογές, παραδείγματος χάριν σε μια διαδικασία παραγωγής. Στην περίπτωση των διαδεδομένων εφαρμογών, εντούτοις, το κρυφάκουσμα της ταυτότητας μπορεί να απειλήσει την ιδιωτικότητα θέσης των προσώπων που φέρνουν αντικείμενα ενσωματωμένα με tag και μπορεί έτσι να προκαλέσει προβλήματα προστασίας των δεδομένων.

Σε τέτοιες καταστάσεις μέτρα όπως τα πρωτόκολλα αντι-σύγκρουσης και η ψευδωνυμία των tag θα μπορούσαν να προσφέρουν μια λύση. Για εφαρμογές όπου τα περιεχόμενα πρέπει να αποθηκευτούν στα tag , μόνο οι ισχυρές διαδικασίες κρυπτογράφησης μπορούν να παρέχουν αξιόπιστη προστασία ενάντια στο κρυφάκουσμα.

5.4. Πρωτόκολλα αντι-σύγκρουσης τα οποία είναι ασφαλή από το κρυφάκουσμα

Με τα αντι-σύγκρουσης πρωτόκολλα βασισμένα σε μια δυαδική αναζήτηση δέντρων (tree walking), οι αριθμοί ταυτότητας ID των tags μπορούν να συναχθούν από τα σήματα του reader, ακόμη και από μια σημαντική απόσταση. Για αυτόν τον λόγο, εναλλακτικές λύσεις της διαδικασίας tree-walking έχουν προταθεί που θα απέκλειαν την εξαγωγή των αριθμών ταυτότητας ID μέσω κρυφακούσματος στο downlink (μετάδοση δεδομένων από τον reader στο tag).

Κανένα από τα μέτρα που αναφέρθηκαν δεν έχει οποιαδήποτε επιρροή στις δυνατότητες που υπάρχουν για τη λήψη των αριθμών ταυτότητας ID μέσω του κρυφακούσματος στο uplink (μετάδοση δεδομένων από το tag στο reader). Η χρησιμότητά τους προέρχεται από το γεγονός ότι, λόγω της χαμηλής ισχύς μετάδοσης του passive transponder και λόγω της υπέρθεσης των ισχυρών σημάτων από τον reader, το uplink μπορεί κανονικά μόνο να ελεγχθεί σε μια πιο σύντομη απόσταση από το downlink. Εντούτοις, αυτή η αξιολόγηση τίθεται υπό αμφισβήτηση από τις πιο πρόσφατες έρευνες που διεξάγονται από το BSI, τουλάχιστον για τους επαγωγικά συνδεμένους transponders στο φάσμα των 13,56 MHz.

5.4.1. Silent Tree-Walking

Αυτή η τροποποίηση της διαδικασίας του tree-walking προτάθηκε από τον Weis. Αντί "να προκαλέσει" ενεργά στο σαφές κείμενο τον επόμενο κλάδο στο δυαδικό δέντρο, ο reader μεταδίδει όλο και όλο στα tags στον τομέα ανάγνωσης το αίτημα να μεταδώσουν τα επόμενα bits των αριθμών ταυτότητάς τους ID. Ο reader εξετάζει τις περιοχές των αντίστοιχων ακολουθιών bits όλων των tag με την κατιούσα σειρά έως ότου εμφανίζεται μια σύγκρουση στο σημείο i. Σε αυτό το σημείο ο reader διακλαδίζει το ερώτημα στα sub-trees με τη βοήθεια της εντολής SELECT. Κατόπιν, σε αντίθεση με το κανονικό δέντρο tree walking, δεν είναι το όλο ήδη γνωστό τμήμα του διαστήματος διευθύνσεων που μεταδίδεται, αλλά μάλλον μια τιμή XOR που αποτελείται από το τρέχον bit στο σημείο i μαζί με το προηγούμενο bit. Τα tags διαμορφώνουν στη συνέχεια μια τιμή XOR έξω από αυτήν την ιδιαίτερη τιμή και το δικό τους bit και συγκρίνουν το αποτέλεσμα με το επόμενο ψηφίο του αριθμού ταυτότητάς τους ID. Εάν υπάρχει μια αντιστοιχία, επιλέγονται και μεταδίδεται το επόμενο bit. Ένας επιτιθέμενος που λειτουργεί από μια απόσταση, που μπορεί μόνο να κρυφακούσει στο downlink από τον reader στο tag, δεν μπορεί να ανακαλύψει τον πλήρη αριθμό ταυτότητας ID. Εκείνες οι περιοχές των αριθμών ταυτότητας ID όπου καμία σύγκρουση δεν συμβαίνει παραμένουν κρυμμένες στον επιτιθέμενο και έτσι, δεν μπορεί να ανακαλύψει το επιλεγμένο sub-tree, ούτε μπορεί, με την αντιστροφή της λειτουργίας XOR, να εξακριβώσει τις τιμές bit που διαβιβάζονται από τον reader.

Σε αντίθεση με το κανονικό δέντρο tree walking, αυτή η διαδικασία δεν μπορεί να εφαρμοστεί με τα read-only tags, επειδή απαιτείται μια δυναμική μνήμη. Αυτό καθιστά το silent tree walking ακριβότερο από το απλό tree walking.

5.4.2. Aloha διαδικασία με προσωρινά IDs

Οι προσδιορισμοί του κέντρου Auto ID για τα tags της Class 0 περιέχουν μία εναλλακτική διαδικασία από το tree walking στην οποία οι ID αριθμοί των tags δεν μεταδίδονται στο εμπρόσθιο κανάλι (downlink), το οποίο υπόκειται στο κρυφάκουσμα:

Αντί του προσδιορισμού τους με τους αριθμούς ταυτότητάς τους, τα tags αρχικά προσδιορίζονται με έναν τυχαίο αριθμό ο οποίος παράγεται σε κάθε κύκλο ανάγνωσης και χρησιμεύει ως ένας προσωρινός αριθμός ταυτότητας ID. Ο reader χρησιμοποιεί αυτόν τον αριθμό προκειμένου να αμβλύνει ένα αναγνωρισμένο tag εξατομικευμένα. Αφότου έχουν αναγνωριστεί όλα τα tags στον τομέα ανάγνωσης , οι πραγματικοί αριθμοί ταυτότητάς τους ID ερωτώνται μεταδίδοντας την προσωρινή ταυτότητα ID.

Με αυτήν την διαδικασία, ένας επιτιθέμενος που κρυφακούει στο downlink μπορεί μόνο να ανιχνεύσει τους τυχαίους αριθμούς που χρησιμοποιούνται για την προσωρινή ταυτοποίηση. Ως απαραίτητη προϋπόθεση γι αυτή την διαδικασία, τα tags πρέπει να έχουν μια τυχαία γεννήτρια αριθμού και να κατέχουν επίσης μια λειτουργία για να αμβλύνονται.

.

5.5. Ψευδωνυμία

Η ψευδωνυμία μπορεί να αποκρύψει την ταυτότητα ενός tag έτσι ώστε μόνο οι εξουσιοδοτημένοι readers μπορούν να ανακαλύψουν τη "αληθινή" ταυτότητα του tag. Η διαδικασία hash lock που περιγράφεται παραπάνω είναι βασισμένη στα ψευδώνυμα (meta IDs) που προσδίδονται. Ωστόσο, δεδομένου ότι ένα tag διατηρεί την ίδια μετα ταυτότητα ID πέρα από ολόκληρη την διάρκεια ζωής του, αυτή η διαδικασία δεν προσφέρει οποιαδήποτε προστασία ενάντια της καταδίωξης των tags.

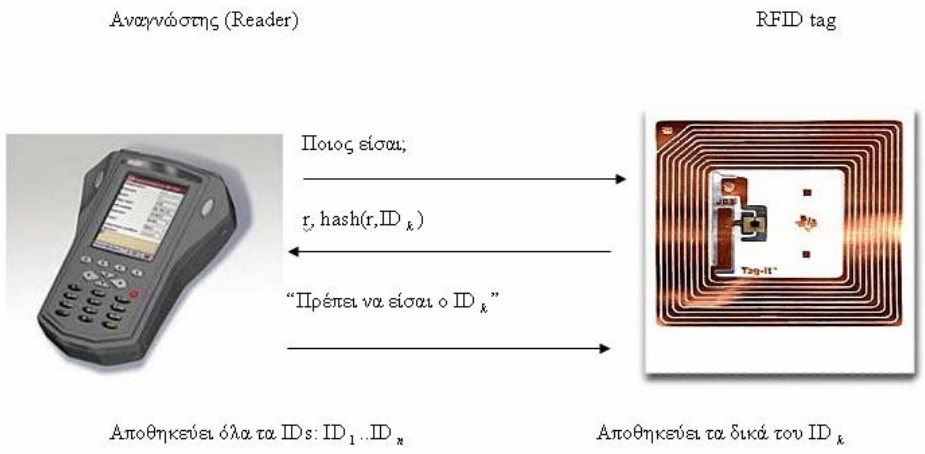
Η διαδικασία hash lock μπορεί έτσι να συμβάλει στην προστασία της ιδιωτικότητας των δεδομένων αλλά δεν βοηθάει στο να βελτιωθεί η ιδιωτικότητα θέσης. Για αυτόν τον λόγο, διάφορες επεκτάσεις της διαδικασίας hash lock έχουν προταθεί.

5.5.1. Τυχαία hash-lock

Αυτή η διαδικασία, που προτείνεται από τον Weis, είναι βασισμένη στη δυναμική παραγωγή μιας νέας μετα-ταυτότητας ID κάθε φορά που εμφανίζεται ένα γεγονός ανάγνωσης. Για αυτό το σκοπό, σε κάθε ενεργοποίηση το tag παράγει έναν τυχαίο αριθμό r που γίνεται hashed με τον αληθινό αριθμό ταυτότητας ID του tag. Ο τυχαίος αριθμός και η hash τιμή μεταδίδονται στον reader από το tag. Προκειμένου να υπολογιστεί ο αληθινός αριθμός ταυτότητας ID του tag, ο χειριστής του reader πρέπει να ξέρει όλους τους αριθμούς ταυτότητας ID που ανήκουν στην εν λόγω εφαρμογή. Ο reader ή ο κεντρικός υπολογιστής του παράγει τις hash τιμές όλων των γνωστών αριθμών ταυτότητας ID, χρησιμοποιώντας τον τυχαίο αριθμό που

παράγεται από το tag, έως ότου μια αντίστοιχη hash τιμή βρεθεί. Σε εκείνο το σημείο ο αριθμός ταυτότητας ID του tag έχει βρεθεί.

Εάν υπάρχει ένας μεγάλος αριθμός από tags, αυτή η διαδικασία δεν είναι πραγματικά εφαρμόσιμη. Αλλά παρά αυτούς τους περιορισμούς είναι ενδιαφέρον για τη χρήση με ένα σύστημα RFID, επειδή μπορεί να εφαρμοστεί με το ελάχιστο κόστος. Εντούτοις, προϋποθέτει ότι τα tags έχουν μια γεννήτρια τυχαία αριθμού. Στο Σχήμα 5.2 απεικονίζεται η τυχαία hash-lock διαδικασία.



Σχήμα 5.2. Τυχαία hash-lock διαδικασία

5.5.2. Chained Hashes

Ο Ohkubo προτείνει την αλυσοδετή hash διαδικασία ως μια κρυπτογραφημένη ακμαία εναλλακτική λύση. Σε κάθε ενεργοποίηση το tag υπολογίζει μια νέα μετα-ταυτότητα, χρησιμοποιώντας δύο διαφορετικές hash λειτουργίες. Πρώτα η τρέχουσα μετα-ταυτότητα γίνεται hashed προκειμένου να παραχθεί μια νέα μετα ταυτότητα ID που έπειτα πάλι γίνεται hashed με την ενίσχυση της δεύτερης λειτουργίας. Είναι αυτή η δεύτερη μετα-ταυτότητα που μεταδίδεται στον reader. Με σκοπό την αποκωδικοποίηση, ο reader πρέπει να κάνει hash έως ότου βρεθεί μια αντιστοιχία με την μετα-ταυτότητα που μεταδίδεται από το tag. Το πλεονέκτημα αυτής της διαδικασίας είναι ότι δεν είναι ευαίσθητη στις επαναλαμβανόμενες προσπάθειες να κατασκοπευθεί η μετα-ταυτότητα κατά τη διάρκεια της μετάδοσης μέσω της διεπαφής του αέρα. Ένας επιτιθέμενος δεν θα ήταν σε θέση να υποστηρίξει και να υπολογίσει τον αριθμό των meta IDs που έχουν κατασκοπευθεί, με αποτέλεσμα η ανωνυμία όλων των προηγούμενων καταχωρημένων δεδομένων του εν λόγω tag στην βάση (log entries) να συντηρείται.

5.5.3. Διαδικασία από τον Henrici και τον Muller

Ο Henrici και ο Muller προτείνουν μια διαδικασία που καθιστούν πιθανή την αμοιβαία επικύρωση του tag και του reader, καθώς επίσης και την κρυπτογράφηση της επικοινωνίας, και που εξασφαλίζει επίσης την προστασία της "ιδιωτικότητας θέσης". Επιπλέον, κανένα κλειδί ή άλλα χρησιμοποιήσιμα δεδομένα δεν αποθηκεύονται για οποιοδήποτε χρονικό διάστημα σε ένα tag, καθιστώντας κατά

συνέπεια τις φυσικές επιθέσεις στο hardware του τσιπ χωρίς ενδιαφέρον. Η διαδικασία τα φέρνει βόλτα με μια ελάχιστη ανταλλαγή των πληροφοριών και είναι επίσης ανθεκτική στην παρέμβαση στο κανάλι μετάδοσης (διεπαφή αέρα). Προκειμένου να διασφαλιστεί η ιδιωτικότητα θέσης, η ταυτότητα ID του tag αλλάζει τακτικά. Το tag δεν αποκαλύπτει ποτέ την τρέχουσα ταυτότητα ID αλλά μόνο την hash τιμή του. Η τελευταία υπολογίζεται από το tag υπό την προϋπόθεση ότι νέοι διεξαγόμενοι αριθμοί συγχρονίζονται με το backend του reader. Αυτά τα χαρακτηριστικά γνωρίσματα αποτρέπουν τις επιθέσεις όπως οι επιθέσεις επανάληψης και ανιχνεύουν τις απώλειες πληροφοριών. Δύο καταχωρήσεις ανά tag αποθηκεύονται στη backend βάση δεδομένων, επειδή η πιθανότητα να χαθεί το τελευταίο μήνυμα από το backend στο tag πρέπει να ληφθεί υπόψη. Η πιο περίπλοκη διαχείριση δεδομένων και ο συγχρονισμός στη backend περιοχή δεν αντιπροσωπεύει οποιοδήποτε σημαντικό περιορισμό, επειδή υπάρχουν ικανοποιητικοί πόροι. Σε αντίθεση, οι σχετικά μέτριες απαιτήσεις γίνονται αναφορικά με το hardware του tag . Το τσιπ πρέπει να είναι ικανό να υπολογίζει τις hash τιμές, ενώ μια γεννήτρια τυχαία αριθμού δεν απαιτείται.

5.6. Παρεμπόδιση της ανάγνωσης

Σε αντίθεση με τα άλλα ηλεκτρονικά προϊόντα τα RFID tags δεν έχουν κάποιο διακόπτη on/off .Γι αυτό το λόγο μπορούν να ενεργοποιηθούν και απέξω χωρίς ο ιδιοκτήτης τους να το γνωρίζει ότι συνέβη.

Τα blocker tags είναι μία μέθοδος η οποία εμποδίζει την εξουσιοδοτημένη ή μη εξουσιοδοτημένη μέθοδο ανάγνωσης ενός tag.

5.6.1. Χρήση των Blocker tags

Ένα blocker tag είναι ένας transponder ή ένα κομμάτι εξοπλισμού με έναν υψηλό βαθμό λειτουργίας το οποίο παριστάνει ότι είναι ένας transponder και παριστάνει όλους τους πιθανούς αριθμούς ταυτότητας ID σε έναν reader. Με το να προσπαθεί να απαντήσει σε κάθε απαίτηση του reader να μεταδώσει δεδομένα, ο blocker tag το καθιστά αδύνατο να ανιχνεύσει τα tags τα οποία είναι ταυτόχρονα στο περιβάλλον του. Τα tags τα οποία είναι πραγματικά παρόν είναι αποτελεσματικά κρυμμένα μέσα σε μία μάζα εικονικών tags (στην πραγματικότητα, αρκετά εκατομμύρια από tags).

Ο Juels έχει προτείνει ένα εξοπλισμένο blocker tag με δυο κεραίες έτσι ώστε οποιαδήποτε μοναδικότητα προθέματος να μπορεί να απαντηθεί ταυτόχρονα από 0 και 1. Αυτό το είδος των blocker tags μπορεί αποτελεσματικά να φράξει τους readers που λειτουργούν σύμφωνα με τη δυαδική διαδικασία δέντρων (binary tree procedure). Προκειμένου να εμποδίσουν τα blocker tags από το να προκαλέσουν μία ολοκληρωτική παρεμπόδιση στην πράξη όλων των εφαρμογών RFID, έχουν προταθεί κάποιες διαδικασίες που θα επέτρεπαν στα blocker tags να εμποδίζουν μόνο ορισμένους περιοχές του χώρου των διευθύνσεων ταυτότητας ID . Με αυτόν τον τρόπο χώροι διευθύνσεων μπορούν να ιδρυθούν εκεί όπου η ανάγνωση εμποδίζεται χωρίς άλλες εφαρμογές να φθείρονται.

Η αξιοπιστία των passive blocker tags είναι φτωχή. Από την στιγμή που το blocker tag ενεργοποιείται μέσω της ενέργειας του ηλεκτρομαγνητικού πεδίου του reader που εμποδίζεται, η αξιοπιστία της προστασίας περιορίζεται από τον τυχαίο χρονικό προσανατολισμό, από τα θωρακισμένα αποτελέσματα και από την απόσταση μεταξύ του blocker tag και του reader. Επιπλέον, ο χρήστης είναι ανίκανος να εξακριβώσει ότι το blocker tag λειτουργεί σωστά. Η ανεπιθύμητη παρέμβαση από τις επιθυμητές εφαρμογές RFID στην περιοχή δεν μπορεί να αποκλειστεί και δεν μπορεί επίσης να ανιχνευθεί άμεσα.

5.7. Οριστική απενεργοποίηση

Η μόνιμη απενεργοποίηση του transponder μετά το τέλος της χρησιμοποίησης του είναι η πιο αξιόπιστη μέθοδος για την προστασία από μία κάθε είδους μελλοντική κακομεταχείριση.

5.7.1. Διαταγή θανάτωσης

Η διαταγή θανάτωσης επιτρέπει την ανωνυμία των transponders. Αυτό το κάνουν με το να καταστούν την ανάγνωση των tags μόνιμα αδύνατη. Αυτό έχει σαν αποτέλεσμα να προστατεύει τα άτομα από την κρυφή αναγνώριση και ως επακόλουθο από την καταδίωξή τους.

Η τρέχουσα προδιαγραφή του EPCglobal καθορίζει μία εντολή θανάτωσης των 8-bit η οποία προστατεύεται από έναν κωδικό πρόσβασης. Έτσι λοιπόν σύμφωνα με την

προδιαγραφή τα προσαρμοσμένα tags δεν μπορούν να αντιδράσουν στο σήμα του reader όταν απενεργοποιηθούν από την εντολή θανάτωσης.

Η εντολή θανάτωσης συζητείται ως πιθανό μέτρο για την απενεργοποίηση των έξυπνων ετικετών στα καταναλωτικά αγαθά στον τομέα των πωλήσεων. Από την πλευρά των καταναλωτών είναι δύσκολο γι αυτούς κάθε φορά να ελέγχουν εάν οι ετικέτες έχουν απενεργοποιηθεί .Από την πλευρά της προστασίας των δεδομένων η αποτελεσματικότητα της διαταγής θανάτωσης παραμένει αμφισβητήσιμη εξαιτίας του ότι οι διαδικασίες θανάτωσης που χρησιμοποιούνται μέχρι τώρα διαγράφουν μόνο τα μεταβλητά κύτταρα μνήμης στον transponder αλλά όχι το μοναδικό αριθμό ταυτότητας ID. Επιπλέον, η απενεργοποίηση με τη βοήθεια ενός κωδικού πρόσβασης δεν είναι πολύ πρακτική εάν, μετά από τα ψώνια, οι καταναλωτές πρέπει να απενεργοποιήσουν τα tags ένα-ένα με το χέρι.

5.7.2. Τομέας τεχνικής απενεργοποίησης

Η ηλεκτρομαγνητική απενεργοποίηση του hardware μέσω ενός προκαθορισμένου σημείου ρήξης, όπως χρησιμοποιείται στα γνωστά αντικλεπτικά συστήματα (1 bit transponders) θα ήταν επίσης εφικτή αλλά μέχρι τώρα δεν προσφέρεται.

5.8. Μετασχηματίζοντας πρακτικές δίκαιων πληροφοριών σε RFID πρωτόκολλα

Ξεκινώντας με τις αρχές του FIP (Fair Information Practices) που είναι οι βάσεις για πολλά άλλα πράγματα ο Flörkemeier προτείνει μέτρα που σκοπό έχουν να δημιουργήσουν διαφάνεια σχετικά με τους χειριστές ενός reader και την χρήση με την οποία τα δεδομένα τοποθετούνται. Ξεκινώντας με την υπόθεση ότι τα τρέχοντα RFID πρωτόκολλα βελτιστοποιήθηκαν σύμφωνα με τεχνικά κριτήρια και τις δαπάνες απόδοσης και όχι με την προστασία της ιδιωτικότητας, οι προτάσεις αφορούν τροποποιήσεις των τρεχόντων RFID πρωτοκόλλων που θα ήταν εύκολο να εφαρμοστούν. Οι βασικές αρχές του FIP σχετικά με το σκοπό, την περιορισμένη χρήση, τη διαφάνεια και την ευθύνη μπορούν να εφαρμοστούν μέσω ελάχιστων αλλαγών στα υπάρχοντα RFID πρωτόκολλα.

Αυτό επίσης σημαίνει ότι οι ερωτήσεις από τους readers δεν πρέπει να παραμείνουν ανώνυμες αλλά πρέπει να παρουσιάζουν την σαφή ταυτότητα του reader. Εάν οι αρχές προστασίας των δεδομένων παραβιάζονται, ο χειριστής του reader μπορεί να αναγνωριστεί και να θεωρηθεί υπεύθυνος. Επίσης, σε κάθε περίπτωση ο σκοπός της συγκέντρωσης των δεδομένων θα πρέπει να εκφραστεί από τον reader, παραδείγματος χάριν μια ανάγνωση των σειριακών αριθμών για λόγους αγοράς. Οι RFID transponders θα μπορούσαν να προγραμματιστούν με τέτοιο τρόπο ώστε να απαντούν μόνο δίνοντας τους σειριακούς αριθμούς όταν ρωτώνται για να παρέχουν την επιθυμητή δήλωση όπως π.χ. για την πληρωμή.

Οι πρόσθετες πληροφορίες για το χειριστή του reader και το σκοπό των δεδομένων που συλλέγουν αποκρυπτογραφούνται με την ενίσχυση μιας ειδικής συσκευής επίδειξης και γίνονται ορατές στον ιδιοκτήτη των tags. Με αυτόν τον τρόπο στον χρήστη των tags δίνεται η δυνατότητα να ελέγξει την λειτουργία των tags και της κατανόησης της χρήσης των δεδομένων που μπορεί να γίνει των δεδομένων που έχουν διαβαστεί. Το πλεονέκτημα αυτής της διαδικασίας είναι ότι ελάχιστη προσπάθεια απαιτείται προκειμένου να εφαρμοστεί στα υπάρχοντα συστήματα RFID. Η διαφάνεια που δημιουργήθηκε έτσι, θα μπορούσε να συμβάλει στη διατήρηση ή την επανάκτηση της εμπιστοσύνης του passive party.

ΚΕΦΑΛΑΙΟ 6

6.1. Εκτίμηση των απειλών και συζήτηση για τα μέτρα ασφάλειας

Στον Πίνακα 6.1 φαίνονται οι επιθέσεις στα RFID συστήματα και τα αντίστοιχα μέτρα τους. Ανταποκρίνονται στις επιθέσεις που αναφέραμε στο active party.

Οι δαπάνες που ο επιτιθέμενος πρέπει να αναλάβει καθώς επίσης και οι δαπάνες που προκύπτουν από τα αντίμετρα είναι απαραίτητα στοιχεία σε οποιαδήποτε αξιολόγηση των κινδύνων που προκύπτουν από τις επιθέσεις. Μπορούμε να κάνουμε μόνο μια ποιοτική εκτίμηση αυτών των δαπανών.

Τα αντίμετρα που ενσωματώνονται στο tag μπορούν συχνά να εφαρμοστούν φτηνά κατά τη διάρκεια της παραγωγής. Σε αυτό το πλαίσιο, οι συμπληρωματικές δαπάνες για τα μέτρα ασφάλειας που είναι στο ίδιο μέγεθος με τις δαπάνες για το σύστημα χωρίς πρόσθετη ασφάλεια υποδεικνύονται ως μεσαίας ακτίνας δαπάνες (medium-range costs). Τα υψηλού κόστους (high cost) αντίμετρα είναι εκείνα που δεν μπορούν να εφαρμοστούν στην πραγματικότητα χωρίς μια παραγωγική αλλαγή στην τεχνολογία.

Επίθεση	**Μέτρα**
Κρυφάκουσμα στην επικοινωνία μεταξύ του tag και του reader	Μετατόπιση όλων των δεδομένων στο backend. Θωράκιση
Μη εξουσιοδοτημένη ανάγνωση των δεδομένων	Ανιχνευτές Επικύρωση
Μη εξουσιοδοτημένη τροποποίηση των δεδομένων	Read-only tags Ανιχνευτές Επικύρωση
Κλωνοποίηση και μίμηση	Αναγνώριση των αντιγράφων Επικύρωση
Αποσύνδεση του tag από το τεμάχιο ενσωματωμένο με tag	Μηχανική σύνδεση Λειτουργία συναγερμού (active tags) Πρόσθετα χαρακτηριστικά γνωρίσματα
Μηχανική ή χημική καταστροφή	Μηχανική σύνδεση
Καταστροφή από την έκθεση σε ένα ηλεκτρομαγνητικό πεδίο	Αυτοθεραπευόμενο φυτίλι (περιορισμένη αποτελεσματικότητα)
Καταστροφή από την κακή χρήση μιας εντολής	Επικύρωση
Εκφόρτιση της μπαταρίας (μόνο στην περίπτωση των active tags)	Τρόπος ύπνου
Φράξιμο	Απαγορευμένο στα πρότυπα των όρων των επιχειρησιακών (Banned in standard business conditions)

Πομποί μπλοκαρίσματος	Μετρήσεις, διαίρεση συχνότητας (Duplex) (FDD)
Ακύρωση πεδίων	Κανένα
Αποσυντονισμός συχνότητας	Ενεργός έλεγχος συχνότητας
Θωράκιση	Βελτιωμένοι σταθμοί ανάγνωσης (περιορισμένη αποτελεσματικότητα)

Πίνακας 6.1. Οι επιθέσεις στα RFID συστήματα και τα αντίστοιχα μέτρα τους

Κρυφάκουσμα στην επικοινωνία μεταξύ του tag και του reader (Eavesdropping on the communication between the tag and the reader)

Το κρυφάκουσμα στην διεπαφή του αέρα είναι σε γενικές γραμμές δυνατό να συμβεί. Αυτό εξαρτάται σε μεγάλο βαθμό από την απόσταση. Εάν για παράδειγμα για την κανονική διαδικασία ανάγνωσης απαιτείται μεγάλη απόσταση ανάγνωσης ο κίνδυνος αυξάνεται. Ενώ είναι μικρότερος ο κίνδυνος για transponders μικρότερου φάσματος. Στην περίπτωση των επαγωγικά συνδεδεμένων συστημάτων δηλ των συστημάτων κάτω από 135 kHz, 13,56 MHz το κρυφάκουσμα στο downlink είναι δυνατό σε μια απόσταση δεκάδων μέτρων. Ενώ στο uplink είναι δυνατό σε μία απόσταση μικρότερη κατά πέντε φορές της μέγιστης απόστασης ανάγνωσης του reader.

Αυτές είναι θεωρητικές εκτιμήσεις οι οποίες βασίζονται στη σχέση της μεταδιδόμενης ισχύς του reader και του tag. Στα πειράματά τους ο Finke και ο Kelter

έδειξαν ότι το κρυφάκουσμα στις επικοινωνίες των RFID καρτών σύμφωνα με το ISO14443 (13,56 MHz, λειτουργικό φάσμα 10 έως 15 εκατοστά) είναι δυνατό σε μία απόσταση μέχρι τουλάχιστον δυο μέτρων. Η διαφορά μεταξύ της μεταδιδόμενης ισχύς του reader και αυτής του tag αποδείχθηκε μη σημαντική για τους σκοπούς του κρυφακούσματος.

Στην περίπτωση των backscatter συστημάτων (868 MHz και 2,45 GHz) το κρυφάκουσμα στο downlink είναι δυνατό μέχρι μια απόσταση 100 έως 200 μ, σε μια ισχύς παραγωγής 2 Watt. Με τη βοήθεια μιας κατευθυντικής κεραίας, αυτός ο τύπος κρυφακούσματος είναι δυνατός μέχρι μια απόσταση των 500 έως 1000 μέτρων. Γενικά, όταν το κρυφάκουσμα συμβαίνει από μία απόσταση υπάρχει πρόβλημα στις χωρική κατανομή των σημάτων, επειδή τα σήματα από διαφορετικές πηγές επιβάλλονται το ένα στο άλλο. Αυτό κάνει το κρυφάκουσμα από μία μεγάλη απόσταση ακόμα πιο δύσκολο.

Οι δαπάνες για τον επιτιθέμενο είναι υψηλές, δεδομένου ότι σε κάθε περίπτωση ο επαγγελματικός εξοπλισμός και η τεχνογνωσία για την αποκωδικοποίηση των στοιχείων απαιτούνται. Η οικοδόμηση μιας κανονικά λειτουργούσας διαμόρφωσης συστημάτων RFID δεν είναι επίσης ένα τετριμμένο θέμα, επειδή η αξιοπιστία της εξαρτάται από ένα πλήθος παραγόντων που επηρεάζουν (αντανακλάσεις, προστατευτικό κάλυμμα, SNR, κ.λπ.). Για μια επίθεση κρυφακούσματος από μια μεγάλη απόσταση οι όροι θα ήταν ευνοϊκότεροι, ειδικά στα υψηλά εύρη ζώνης όπως 106 –848 Kbit/s στα συστήματα σύμφωνα με τον ISO 14443.

Μέτρα:

- Μετατόπιση όλων των δεδομένων εκτός από την ταυτότητα ID στο backend. Αυτό θα προταθεί και για την διαχείριση δεδομένων.
- Ζώνες προστασίας όπου οι readers χρησιμοποιούνται εναντίων της ηλεκτρομαγνητικής ακτινοβολίας (μεταλλική λεπτή ταπετσαρία)
- Κρυπτογραφημένη μετάδοση δεδομένων

Υπό κανονικές συνθήκες, οι δαπάνες για τα αντίμετρα δεν χρειάζονται να είναι υψηλές προκειμένου να παρασχεθεί η καλή προστασία ενάντια του κρυφακούσματος στη διεπαφή αέρα.

Μη εξουσιοδοτημένη ανάγνωση των δεδομένων (Unauthorized reading of the data)

Αυτό το είδος επίθεσης απαιτεί έναν reader που μπορεί να επεκταθεί συγκεκαλυμμένα, χωρίς να εντοπιστεί. Για τη συνήθη απόσταση ανάγνωσης, αυτό είναι εφικτό χωρίς να υποβάλλονται αδικαιολόγητες δαπάνες. Ο επιτιθέμενος πρέπει να αποκτήσει έναν reader και να αναλάβει ενδεχομένως το πρόβλημα της λαθραίας εγκατάστασής του. Τα προϊόντα λογισμικού που χρησιμοποιούνται στους κινητούς readers διαφημίζονται ήδη και είναι ικανά για ανάγνωση και γράψιμο στα απλά tags, π.χ. στα σουπερμάρκετ.

Το ενδεχόμενο αυτών των επιθέσεων είναι περιορισμένο λόγω του μικρού φάσματος και μπορούν να ελεγχθούν σε ένα ελεγχόμενο περιβάλλον. Η ειδική κατασκευή των readers με μεγαλύτερο φάσμα είναι δυνατή σε στενά περιορισμένα όρια και δαπανηρή. Στην περίπτωση των επαγωγικών συστημάτων, το φάσμα μπορεί να διπλασιαστεί. Το ένα μέτρο θεωρείται ως το τελικό ανώτατο όριο στην περίπτωση των επαγωγικής σύζευξης.

Στο UHF φάσμα, η ισχύς που μεταδίδεται περιορίζεται από το νόμο στα δύο Watt, το οποίο επιτρέπει στους readers να λειτουργούν σε μια μέγιστη απόσταση τριών έως πέντε μέτρων. Για να μπορεί να διαβάσει σε μία απόσταση δέκα μέτρων, η μεταδιδόμενη ισχύς που απαιτείται είναι γύρω στα 30 Watts ενώ για μια απόσταση 20 μέτρων απαιτείται μεταδιδόμενη ισχύς τουλάχιστον 500 Watts. Αυτό είναι το είδος της ισχύος που τίθεται από τους πομπούς εκπομπής και δεν θα ήταν πρακτικό για μια συγκεκαλυμμένη λειτουργία. Η αύξηση της απόστασης ανάγνωσης είναι περίπλοκη επειδή το αδύνατο σήμα των tags όλο και περισσότερο "κατατροπώνεται" από το ισχυρό σήμα του reader. Για λειτουργικούς λόγους μόνο, πολλές εφαρμογές RFID θα χρησιμοποιήσουν tags με πολύ μικρές αποστάσεις ανάγνωσης, παραδείγματος χάριν τις έξυπνες κάρτες ή τα τραπεζογραμμάτια.

Κατά συνέπεια, οι πιθανότητες να διαβάσει κρυφά τους passive transponders είναι πολύ περιορισμένες. Η κατάσταση είναι διαφορετική όταν πρόκειται για τους active transponders, αλλά τις περισσότερες φορές δεν είναι απαραίτητο να χρησιμοποιηθούν τα active tag για αναγνωριστικούς σκοπούς (μια χαρακτηριστική εφαρμογή βρίσκει τη θέση των αντικειμένων). Κατά συνέπεια, αυτές οι εφαρμογές υπόκεινται στην κατηγορία RFID.

Μέτρα:

- Μετατόπιση των δεδομένων στο backend
- Ανιχνευτές οι οποίοι αναγνωρίζουν το πεδίο ισχύος του reader
- Επικύρωση (Οι διάφορες μέθοδοι επικύρωσης του reader με σεβασμό στο tag είναι πιθανές)

Οι δαπάνες των αντίμετρων μπορούν να είναι χαμηλές, εάν ο επιθυμητός στόχος μπορεί να επιτευχθεί με τη χρησιμοποίηση μόνο μερικών ανιχνευτών. Μια πιο αδύναμη παραλλαγή θα μπορούσε επίσης να είναι να διεξαχθεί μια τυχαία αναζήτηση των readers. Η επικύρωση θα αύξανε την τιμή των tags σημαντικά σε περιπτώσεις όπου τα ούτως ή άλλως απλά read-only tags θα ήταν αρκετά. Σύμφωνα με τις ειδικές εκτιμήσεις αναμένεται ότι τα παραγμένα μαζικά tags που χρησιμοποιούν τη διαδικασία πρόκληση-απάντησης θα παραμείνουν τρεις έως πέντε φορές ακριβότερα από τα απλούστερα tags.

Σύμφωνα με την Infineon, εντούτοις, η διαφορά τιμών δεν πρέπει να είναι μεγαλύτερη από 20 τοις εκατό.

Μη εξουσιοδοτημένη τροποποίηση των δεδομένων (Unauthorized modification of data)

Στην περίπτωση των επαναγράψιμων tags οι πιθανότητες για επίθεση και τροποποίηση των δεδομένων καθώς και τα αντίμετρα είναι τα ίδια με την προηγούμενη περίπτωση της αναρμόδιας ανάγνωσης.

Εάν, αφ' ετέρου, χρησιμοποιούνται τα read only tags, η μη εξουσιοδοτημένη τροποποίηση των δεδομένων είναι πραγματικά αδύνατη. Αυτό είναι ένα πλεονέκτημα ενάντια στα άλλα μειονεκτήματα ασφάλειας των read-only tags, τα οποία δεν επιτρέπουν οποιαδήποτε κρυπτογράφηση και επιτρέπουν στην καλύτερη περίπτωση μόνο την αδύναμη επικύρωση (κωδικός πρόσβασης χωρίς προστασία ενάντια στις επιθέσεις επανάληψης).

Κλωνοποίηση και μίμηση (Cloning and emulation)

Στην κλωνοποίηση το περιεχόμενο του tag διαβάζεται η ανακαλύπτεται με σκοπό να γραφτεί σε ένα νέο tag το οποίο θα παριστάνει την ταυτότητα του αρχικού tag.

Πιθανότατα να χρησιμοποιούνται μικρές συσκευές όπως ο emulator (εξομοιωτής), οι οποίες χρησιμοποιούνται για να μιμούνται οποιοδήποτε tag. Εάν ο emulator χειροκίνητα βρεθεί κοντά στον reader, τότε διατίθενται ιδιαίτερα ευέλικτα μέσα παραποίησης: Κάποιος αφαιρεί ένα στοιχείο από μία σειρά προϊόντων. Το tag του στοιχείου διαβάζεται χρησιμοποιώντας έναν φορητό reader (που μπορεί επίσης να ενσωματωθεί στον emulator). Έπειτα, το πρόσωπο πηγαίνει στον προοριζόμενο reader όπου, με τη βοήθεια του emulator, διακριτικά μιμείται ότι το στοιχείο έχει περάσει αυτό το σημείο. Ένα αντιγραμμένο tag θα μπορούσε να χρησιμοποιηθεί κατά τον ίδιο τρόπο, παραδείγματος χάριν να παρθεί ένα στοιχείο από το "έξυπνο ράφι" και να αντικατασταθεί με το αντίγραφό του, και έτσι τα αντικλεπτικά μέτρα να μην έχουν αποτέλεσμα.

Η κλωνοποίηση και η μίμηση απαιτούν προγενέστερη ανάγνωση ή κρυφάκουσμα. Για αυτό το λόγο τα αντίμετρα είναι τα ίδια με εκείνα που χρησιμοποιούνται ενάντια σε αυτές τις επιθέσεις (βλ. ανωτέρω). Και οι δύο τύποι επιθέσεων πρέπει να αποτραπούν προκειμένου να αποκλειστεί η δυνατότητα κλωνοποίησης και μίμησης . Ένα άλλο αντίμετρο θα μπορούσε να ήταν οι έλεγχοι στο backend οι οποίοι θα ανίχνευαν τα αντίγραφα.

Αποσύνδεση του tag από το τεμάχιο ενσωματωμένο με tag (Detaching the tag from the tagged item)

Αυτή η επίθεση εμφανίζεται σπάνια. Η διακοπή των tags ("switching") με δόλια πρόθεση ή μοναχά με την πρόθεση της δημιουργίας σύγχυσης είναι μία προφανής μεθόδευση.

Η μηχανική μεθόδευση δεν εμπεριέχει ειδικές απαιτήσεις γι αυτό τείνει να πραγματοποιείται φθηνά.

Μέτρα:

- Ένας σφιχτός μηχανικός δεσμός μεταξύ του tag και του στοιχείου ενσωματωμένου με tag εξασφαλίζει ότι η αφαίρεση του tag θα βλάψει επίσης το προϊόν (π.χ. όταν υφαίνεται στα κλωστοϋφαντουργικά προϊόντα ή ενσωματώνεται στα πλαστικά μέρη).
- Τα tags μπορούν να εγκατασταθούν κατά τέτοιο τρόπο σε μερικές εφαρμογές ώστε είναι δύσκολο να βρεθούν ή είναι απρόσιτα.
- Στα active tags, υπάρχει μια λειτουργία συναγερμών: Ένας αισθητήρας καθορίζει ότι ο transponder έχει μεθοδευτεί. Ο αισθητήρας αποθηκεύει αυτές

τις πληροφορίες και μεταδίδει έναν συναγερμό σε έναν reader μόλις έρχεται μέσα στο φάσμα.

- Πρόσθετα χαρακτηριστικά όπως για παράδειγμα ένα barcode ή ένα δυσδιάκριτο σημάδι παράσχονται στα τεμάχια που ενσωματώνονται με tag όταν αυτά έχουν μεγάλη αξία και να ελέγχεται έτσι εάν το tag είναι ενσωματωμένο στο σωστό τεμάχιο. Η σχέση μεταξύ των πρόσθετων χαρακτηριστικών και της ταυτότητας ID του tag αποθηκεύονται στο backend.

Μηχανική ή χημική καταστροφή (Mechanical or chemical destruction)

Τα RFID tags μπορούν μηχανικά ή χημικά να καταστραφούν. Ειδικότερα οι κεραίες είναι τρωτές.

Μέτρα:

- Μία μηχανική σύνδεση μεταξύ του tag και του στοιχείου το οποίο είναι ενσωματωμένο με tag βοηθά στο να μην καταστραφεί το tag χωρίς την καταστροφή του στοιχείου.
- Σε μερικές εφαρμογές, τα tags μπορεί να είναι συνδέονται με τέτοιο τρόπο ώστε να είναι δύσκολο να βρεθούν ή να είναι απρόσιτα.

Καταστροφή από την έκθεση σε ένα ηλεκτρομαγνητικό πεδίο (Destruction by exposure to an electromagnetic field)

Η καταστροφή από την έκθεση σε ένα ηλεκτρομαγνητικό πεδίο είναι τυποποιημένη πρακτική στην περίπτωση των αντικλεπτικών EAS tags (1 bit transponders) που απενεργοποιούνται στο σημείο της πώλησης. Αν και η απενεργοποίηση θα μπορούσε να πραγματοποιηθεί με σχετικά απλά μέσα από τον πελάτη ενώ είναι στο κατάστημα, αυτό δεν φαίνεται να συμβαίνει στην πράξη.

Αυτός ο τύπος απενεργοποίησης είναι πλήρως δυνατός στην περίπτωση όλων των επαγωγικά συνδεμένων tags, ακόμα και όταν δεν παρέχεται κανένα προκαθορισμένο σημείο ρήξης (ουδετεροποίηση), όπως στην περίπτωση EAS. Κανονικά, οι δίοδοι Zener ή τα εσωτερικά στοιχεία κυκλώματος σταθεροποίησης περιορίζουν την τάση που προκαλείται στην κεραία στην προοριζόμενη λειτουργούσα τάση. Εντούτοις, εάν η τάση που προκαλείται στη σπείρα υπερβαίνει το όριο φορτίων του συστήματος σταθεροποίησης της τάσης, το τσιπ μπορεί να καταστραφεί αμετάκλητα. Μόνο η περιορισμένη προστασία είναι δυνατή ενάντια στην παραπάνω τάση επειδή η δυνατότητα του κυκλώματος σταθεροποίησης να απορροφηθεί η υπερβολική ενέργεια μέσω της επιφάνειάς του (αφαίρεση θερμότητας) είναι περιορισμένη στο τσιπ.

Λόγω της υψηλής δύναμης πεδίου που απαιτείται, αυτή η επίθεση μπορεί μόνο να πραγματοποιηθεί σε πολύ μικρό φάσμα. Το ίδιο πράγμα ισχύει για τα UHF tags.

Επειδή η δύναμη του πεδίου μειώνεται με τον κύβο της απόστασης, ένας πομπός με μια πολύ μεγάλη κεραία και μια πολύ υψηλή παραγωγή ισχύος θα απαιτούνταν για

τη μαζική καταστροφή των tags σε απόσταση αρκετών μέτρων. Αυτό θα ήταν μόλις και μετά βίας πρακτικό για έναν επιτιθέμενο να το επιτύχει.

Σε γενικές γραμμές, τα tags θα μπορούσαν να καταστραφούν με έναν φούρνο μικροκυμάτων, αλλά όχι αξιόπιστα. Εάν το tag συνδέεται κοντά με το στοιχείο που το φέρει (και αυτός είναι ένας καλός λόγος για το βάλεις σε έναν φούρνο μικροκυμάτων) η υψηλή θέρμανση του tag μπορεί να βλάψει το προϊόν.

Επιπλέον, υπάρχει ένας καλός λόγος να υποψιαστούμε ότι οι σπείρες επαγωγής και τα γεγονότα μετατροπής υψηλής τάσης που εμφανίζονται στην κοντινή κλίμακα θα προέτρεπαν αρκετά τις αιχμές υψηλής τάσης στο tag για να βλάψουν το τσιπ. Τα πειράματα σε αυτό το θέμα πραγματοποιούνται αυτή τη στιγμή στο EMPA.

Τα αυτοθεραπευόμενα φιτίλια θα μπορούσαν να θεωρηθούν ως πιθανό αντίμετρο ενάντια στην καταστρεπτική επίδραση ενός ηλεκτρομαγνητικού πεδίου. Μέχρι τώρα, αυτά δεν έχουν περιληφθεί στα πρότυπα. Εντούτοις, αυτό το αντίμετρο δεν θα άλλαζε το γεγονός ότι η ικανότητα να απορροφηθεί η περιττή προκληθείσα ενέργεια περιορίζεται από την περιοχή επιφάνειας πέρα από την οποία η θερμότητα μπορεί να εκπεμφθεί. Επομένως, σε γενικές γραμμές, δεν υπάρχει καμία απόλυτη προστασία ενάντια στην καταστροφή από την έκθεση σε ένα ηλεκτρομαγνητικό πεδίο.

Καταστροφή από την κακή χρήση μιας εντολής θανάτωσης (Destruction by misuse of a kill command)

Εάν, για λόγους ιδιωτικότητας των δεδομένων, τα tags είναι εξοπλισμένα με μια λειτουργία θανάτωσης που μερικώς ή συνολικά σβήνει το περιεχόμενο των δεδομένων, αυτή η λειτουργία μπορεί να χρησιμοποιηθεί κατ' άσχημο τρόπο.

Ένα μέτρο είναι να παρασχεθεί επικύρωση για την εντολή θανάτωσης (π.χ. προστασία κωδικού πρόσβασης). Σχετικά περίπλοκα οργανωτικά μέτρα απαιτούνται προκειμένου να διαβιβαστεί ο κωδικός πρόσβασης στα εξουσιοδοτημένα πρόσωπα (π.χ. ο αγοραστής του στοιχείου που φέρει το tag), αλλά να τον κρατήσουν μυστικό από άλλους. Αυτή η διαδικασία είναι συγκρίσιμη με την έκδοση μιας κάρτας τσιπ με PIN.

Εκφόρτιση της μπαταρίας (μόνο στην περίπτωση των active tags) (Discharging the battery (only in the case of active tags))

Η εκφόρτιση της μπαταρίας γίνεται μόνο στην περίπτωση των active tags. Πως το κάνουν; Με το να προκαλούν το tag να μεταδίδει συχνά απαντήσεις σε μία πληθώρα ερωτήσεων.

Ένα πιθανό μέτρο σε αυτήν την περίπτωση θα ήταν ένας "τρόπος ύπνου (sleep mode") που αναγκάζει μια μικρή διακοπή αφότου έχει εμφανιστεί μια αλληλεπίδραση. Αυτό θα περιόριζε τον αριθμό πιθανών αλληλεπιδράσεων ανά

μονάδα του χρόνου. Παρόμοιες λειτουργίες υπάρχουν ήδη για να αποτρέψουν ήδη τις διπλές αναγνώσεις.

Φράξιμο (Blocking)

Η χρήση των blocker tags δεν απαγορεύεται από το νόμο, επειδή δεν είναι συστήματα μετάδοσης. Εντούτοις, η χρήση τους θα μπορούσε να απαγορευθεί στους τυποποιημένους επιχειρησιακούς όρους, π.χ. των σουπερμάρκετ. Αλλά αυτό δεν θα απέτρεπε το φράξιμο από τον σκοπό της διάπραξης απάτης.

Ένα πλεονέκτημα των blocker tags είναι το γεγονός ότι το φάσμα φραξίματός τους είναι εξελικτικό και μπορούν να διαμορφωθούν για ορισμένα διαστήματα διευθύνσεων. Κατά συνέπεια, η προστασία μυστικότητας μπορεί να ρυθμιστεί επιλεκτικά. Εντούτοις, είναι ακριβώς αυτές οι μεμονωμένες ρυθμίσεις που επιτρέπουν στους ανθρώπους να ακολουθηθούν, έτσι ώστε ο πραγματικός στόχος ιδιωτικότητας θέσης γίνεται παράλογος.

Το blocker τσιπ το οποίο είναι διαθέσιμο στην αγορά από την RSA είναι αποτελεσματικό μόνο στην διαδικασία αντι-σύγκρουσης tree walking. Εντούτοις, τα blocker tags μπορούν επίσης να αναπτυχθούν ενάντια στο πρωτόκολλο Aloha. Σε γενικές γραμμές, δεν υπάρχει καμία απόλυτη προστασία ενάντια στο φράξιμο μέσα σε ένα δεδομένο πρωτόκολλο. Δεδομένου ότι τα διάφορα πρωτόκολλα είναι σε χρήση, ο χρήστης του blocker tag πρέπει να φέρει διάφορα τέτοια tags μαζί του προκειμένου να καλυφθούν όλα τα πιθανά πρωτόκολλα, είτε πρέπει να

χρησιμοποιήσει μια ενιαία (ελαφρώς μεγαλύτερη) blocker συσκευή η οποία αντιμετωπίζει όλα αυτά τα πρωτόκολλα.

Το μόνο μέτρο ενάντια στα blocker tags είναι να απαγορευθεί η χρήση τους στους τυποποιημένους όρους και στους όρους της επιχείρησης – δεν υπάρχει κανένα τεχνικό μέτρο που μπορεί να ληφθεί.

Πομποί μπλοκαρίσματος (Jamming transmitters)

Η αποτελεσματική παρέμβαση της λειτουργίας σε μια απόσταση απαιτεί ισχυρούς πομπούς.

Η ενεργοποίηση τέτοιων jamming transmitters είναι παράνομη και είναι δύσκολη για τους άπειρους τεχνικά: Αλλά οι ραδιοερασιτέχνες έχουν πρόσβαση σε αυτήν την τεχνολογία. Το μποκάρισμα σε κοντινό φάσμα είναι δυνατό χρησιμοποιώντας αδύναμους πομπούς ή επίσης μέσω των αλληλεπιδράσεων με άλλες ηλεκτρονικές συσκευές (παρεμβάσεις, συγκρούσεις πρωτοκόλλου), αλλά είναι δύσκολο να υιοθετηθούν τέτοια αποτελέσματα σοβαρά με έναν στοχοθετημένο τρόπο.

Μέτρα:

- Ανίχνευση των jamming transmitters με την εκτέλεση τυχαίων μετρήσεων ή με τη χρησιμοποίηση μόνιμα εγκατεστημένων ανιχνευτών πεδίων.
- Στις μελλοντικές γενιές RFID υιοθέτηση της μεθόδου διαίρεσης συχνότητας. Αυτό το κατά γενική ομολογία πολύ εκτεταμένο μέτρο θα έλεγχε επίσης το

αυξανόμενο πρόβλημα που δημιουργείται από τις κανονικές πηγές μπλοκαρίσματος.

Ακύρωση πεδίων (Field cancellation)

Οι ζώνες ακύρωσης είναι ένα κανονικό φαινόμενο στο UHF φάσμα, αλλά είναι δύσκολο να διαμορφωθούν. Επομένως φαίνεται απίθανο ότι ένας επιτιθέμενος θα πετύχει να χρησιμοποιήσει αυτή την επίδραση με έναν στοχοθετημένο τρόπο, π.χ. με τη σύσταση των ανακλαστήρων.

Δεν υπάρχουν γενικά και προληπτικά μέτρα. Εάν η στοχοθετημένη ακύρωση πεδίου, εντούτοις, γίνεται ένα στοιχείο των επιθέσεων, θα είναι απαραίτητο να βρεθούν μέτρα προσαρμοσμένα σε κάθε μεμονωμένη περίπτωση.

Αποσυντονισμός συχνότητας (Frequency detuning)

Αυτή η επίθεση πραγματοποιείται φέρνοντας ποσότητες, παραδείγματος χάριν, νερού, μετάλλου ή φερρίτη κοντά στο πεδίο ή στην κεραία του tag. Ίσως να είναι αρκετά απλό να καλυφθεί το tag με το χέρι. Εντούτοις, ο αποσυντονισμός συχνότητας είναι λιγότερο αξιόπιστος στην επίδρασή του σε σύγκριση με την θωράκιση.

Σε γενικές γραμμές, είναι εφικτό να αντιμετωπιστεί αυτός ο τύπος επίθεσης με τη χρησιμοποίηση του ενεργού ελέγχου συχνότητας. Εντούτοις, η τεχνική προσπάθεια

που απαιτείται φαίνεται δυσανάλογη επειδή άλλες, ευκολότερες μορφές επίθεσης, όπως η θωράκιση, δεν αποτρέπονται από αυτό το μέτρο. Επιπλέον, υπό ορισμένες συνθήκες, οι απαιτήσεις χορήγησης αδειών υψηλής συχνότητας για τέτοια συστήματα θα παραβιάζονταν.

Θωράκιση (Shielding)

Τα tags μπορούν να προστατευθούν τυλίγοντάς τα σε μεταλλικό φύλλο αλουμινίου (π.χ. αλουμινόχαρτο) ή με την τοποθέτηση τους σε ψυκτικές τσάντες τυλιγμένες με αλουμίνιο, ή σε τσάντες που εξοπλίζονται με λουρίδες μετάλλων.

Σαν μέτρο, είναι πιθανό στην περίπτωση των επαγωγικά συνδεμένων συστημάτων, να χρησιμοποιούν βελτιωμένους σταθμούς ανάγνωσης που είναι λιγότερο ευαίσθητοι στη θωράκιση. Οι διάφορες κεραίες σε διαφορετικές γωνίες μπορούν να καταστήσουν τη θωράκιση δύσκολη. Δεν υπάρχει καμία αξιόπιστη προστασία ενάντια στην θωράκιση.

6.2. Εκτίμηση των απειλών κατά της ιδιωτικότητας και συζήτηση για τα μέτρα

Αν και το θέμα το οποίο διαπραγματεύεται η διπλωματική αυτή είναι για την ασφάλεια στο RFID παρόλα ταύτα χρήσιμο θα ήταν να αναφερθούμε στις απειλές κατά της ιδιωτικότητας και τα μέτρα που μπορούν να παρθούν. Αυτές οι απειλές και τα μέτρα τους παρουσιάζονται στον Πίνακα 6.2.

Επίθεση	**Μέτρα**
Κρυφάκουσμα στην επικοινωνία μεταξύ του tag και του reader	Μετατόπιση των δεδομένων στο backend Θωράκιση Κρυπτογράφηση Επιθέσεις για αυτοπροστασία: Αποσύνδεση του tag Καταστροφή του tag Tag φραξίματος Πομπός μπλοκαρίσματος Ακύρωση πεδίου Αποσυντονισμός πεδίου Θωράκιση
Μη εξουσιοδοτημένη ανάγνωση των δεδομένων	Ανιχνευτές Επικύρωση Επιθέσεις για αυτοπροστασία: Αποσύνδεση του tag Καταστροφή του tag Tag φραξίματος Πομπός μπλοκαρίσματος Ακύρωση πεδίου Αποσυντονισμός πεδίου Θωράκιση του tag
Παρακολούθηση των ανθρώπων	Μεταβλητοί αριθμοί ταυτοτήτων

	ID Επιθέσεις για αυτοπροστασία: Αποσύνδεση του tag Καταστροφή του tag Tag φραξίματος Πομπός μπλοκαρίσματος Ακύρωση πεδίου Αποσυντονισμός πεδίου Θωράκιση του tag
Χειρισμός των δεδομένων εις βάρος του passive party	Επικύρωση Ανίχνευση των αντιγράφων
Αντικανονική εκτίμηση των στο δεδομένων	Κανένα τεχνικό μέτρο

Πίνακας 6.2. Απειλές κατά της ιδιωτικότητας και τα μέτρα προστασίας

Κρυφάκουσμα στην επικοινωνία μεταξύ του tag και του reader (Eavesdropping on communication between tag and reader)

Αυτή είναι μία επίθεση που απειλεί το active και το passive party με τον ίδιο τρόπο.

Μέτρα:

- Μετατόπιση των δεδομένων στο backend
- Θωράκιση
- Κρυπτογράφηση της μετάδοσης δεδομένων

Αυτά τα μέτρα πρέπει, εντούτοις, να εφαρμοστούν κατά τέτοιο τρόπο ώστε το passive party να έχει εξουσιοδοτημένη πρόσβαση στα δεδομένα που το αφορούν. Διαφορετικά, η μετατόπιση των δεδομένων στο backend ή η κρυπτογράφηση, θα μείωνε τη διαφάνεια του συστήματος για το passive party.

Μη εξουσιοδοτημένη ανάγνωση των δεδομένων (Unauthorized readout of data)

Αυτή είναι μία επίθεση που απειλεί το active και το passive party με τον ίδιο τρόπο.

Μέτρα:

- Οι ανιχνευτές που παρουσιάζουν το πεδίο ενεργειακού ανεφοδιασμού ενός reader μπορούν επίσης να χρησιμοποιηθούν από το passive party.
- Εάν οι διαδικασίες επικύρωσης χρησιμοποιούνται, στο passive party θα πρέπει να δοθούν τα δικαιώματα πρόσβασης στα δεδομένα που το αφορούν. Αλλιώς οι διαδικασίες επικύρωσης θα μείωναν την διαφάνεια του συστήματος για το passive party και αυτό είναι αντίθετο σε αυτό που χρειάζεται το party δηλαδή να έχει τον έλεγχο των δεδομένων.

Παρακολούθηση των ανθρώπων (Tracking of people)

Οι γνώμες ποικίλουν στους κινδύνους στους οποίους οι άνθρωποι ίσως να υφίστανται από την παρακολούθηση.

Η παρακολούθηση χρησιμοποιώντας τις συγκεκαλυμμένες διαδικασίες ανάγνωσης (κρυφάκουσμα, μη εξουσιοδοτημένη ανάγνωση) είναι μάλλον απίθανη λόγω των τεχνικών δυσκολιών και είναι πιθανότερο ότι η κανονική συλλογή δεδομένων θα αποτελέσει τη βάση για την ίδρυση σχεδιαγραμμάτων μετακίνησης.
Εντούτοις, οι γνώμες διαφέρουν για την συμβολή του RFID στον κίνδυνο των ανθρώπων οι οποίοι παρακολουθούνται.

Από την μία υποστηρίζεται ότι τα δεδομένα που θα επέτρεπαν τέτοια παρακολούθηση συλλέγονται ήδη σήμερα (π.χ. μέσω των καρτών πελατών), αλλά δεν χρησιμοποιούνται για αυτόν το λόγο. Εφαρμογές RFID που θα συνέβαλλαν αποφασιστικά σε αυτήν την περιοχή δεν προγραμματίζονται, ούτε θα ήταν πρακτικές. Ειδικότερα, καμία εταιρία δεν θεωρεί αυτήν την περίοδο τα στοιχεία RFID έξω από την αλυσίδα διοικητικών μεριμνών. Οι υποθετικές εφαρμογές, όπως ο αυτόματος-έλεγχος στην υπεραγορά δεν θα χρησιμοποιηθούν σε μια μεγάλη κλίμακα στα επόμενα 10 έτη. Οι δαπάνες ενός tag (> 5 λεπτά του ευρώ) και των τεχνικών δυσκολιών στο φυσικό επίπεδο αποτρέπουν τα tags να χρησιμοποιηθούν επικερδώς για αυτήν την εφαρμογή. Ούτε οι επιχειρήσεις θα επιθυμούσαν να διακινδυνεύσουν τη φήμη τους και την εμπιστοσύνη των πελατών τους. Ο σκοπός των παρουσών προσπαθειών εξυγίανσης είναι απλώς να βελτιστοποιηθεί η εφοδιαστική αλυσίδα από το ράφι στο κατάστημα (έξυπνο ράφι). Και ακόμα και τότε, τα RFID tag πιθανώς μόνο θα χρησιμοποιηθούν στα μεμονωμένα μεγάλης αξίας προϊόντα, ενώ στις

περισσότερες περιπτώσεις τα tags θα χρησιμοποιηθούν απλά στη συσκευασία παράδοσης (π.χ. παλέτα). Αυτό δεν προκαλεί οποιοδήποτε πρόσθετο κίνδυνο για τους

ανθρώπους που παρακολουθούνται μέσω των αγαθών. Ακόμα κι αν κάποιος χρησιμοποιήσει RFID για λόγους παρακολούθησης, θα ήταν πολύ δύσκολο να αντληθούν τα σχεδιαγράμματα μετακίνησης από τα εξαιρετικά τεμαχισμένα δεδομένα. Θα ήταν πάρα πολύ ακριβό να παραχθεί μια γενική εικόνα. Δεν υπάρχει κανένα οικονομικό συμφέρον να γίνει αυτό. Ακόμη και τα τρέχοντα δεδομένα των καρτών των πελατών μετατρέπεται ως επί το πλείστον σε νεκροταφεία δεδομένων επειδή δεν αξίζουν να δημιουργηθούν τα σχεδιαγράμματα πελατών.

Αφ' ετέρου επισημαίνεται ότι εάν το RFID χρησιμοποιείται σε μία διαδεδομένη βάση, σημαντικά περισσότερα γεγονότα (ακόμα κι αν όχι κάθε αγορά ενός φτηνού μαζικού προϊόντος) θα καταγράφονται ψηφιακά, και περισσότερα ίχνη δεδομένων θα παραχθούν που προσφέρουν επίσης περισσότερες ευκαιρίες για αξιολόγηση. Αυτό θα δημιουργήσει νέες επιθυμίες, π.χ. στις κυβερνητικές αντιπροσωπείες, για να εκτελέσουν τις αξιολογήσεις. Επιπλέον, οι λιανοπωλητές ενδιαφέρονται για τα σχεδιαγράμματα μετακίνησης των πελατών μέσα στα καταστήματά τους. Η συγκεκαλυμμένη ανάγνωση θα παραμείνει η εξαίρεση, αλλά δεν μπορεί να αποκλειστεί εντελώς. Εάν τα RFID tag δεν απενεργοποιούνται οριστικά όταν τα προϊόντα απορρίπτονται, ίσως να είναι δυνατό να συναχθούν τα συμπεράσματα για το σημείο και το χρόνο της πώλησης και επίσης για τον αγοραστή του προϊόντος με την ανάγνωση των δεδομένων από τα tags στα απορρίμματα. Το ιδιαίτερο του RFID έναντι των άλλων συστημάτων αναγνώρισης είναι ότι αυτή η τεχνολογία έχει τη δυνατότητα να περιορίσει την ειδάλλως ανώνυμη φύση της διαδικασίας διάθεσης αποβλήτων. Επιπλέον, είναι ένα ιδιαίτερα λεπτό θέμα, αποθηκεύοντας τα βιομετρικά χαρακτηριστικά στους transponders. Ένα πιθανό μέτρο θα ήταν να χρησιμοποιηθούν

οι μεταβλητοί αριθμοί ταυτότητας ID, π.χ. βασισμένοι στην εκτεταμένη διαδικασία hash-lock.

Χειρισμός των δεδομένων εις βάρος του passive party (Manipulation of data to the disadvantage of the passive party)

Όχι μόνο η μη εξουσιοδοτημένη ανάγνωση, αλλά οποιοσδήποτε τύπος χειρισμού των δεδομένων από το third party μπορεί να είναι μια απειλή στο passive party, ιδιαίτερα εάν το τελευταίο δεν έχει κανένα μέσο παρακολούθησης τέτοιου μηχανισμού. Επαρκής ασφαλείς διαδικασίες επικύρωσης απαιτούνται για να αποτραπεί το third party από το να προσεγγίσουν τα δεδομένα. Προκειμένου να αποτραπεί ο χειρισμός, είναι ιδιαίτερα σημαντικό για τα passive parties να έχουν εξουσιοδοτημένη πρόσβαση στα δεδομένα που τους αφορούν, προκειμένου να είναι σε θέση να ελέγξουν ότι είναι σωστά.

Σε αυτήν την περίπτωση, επίσης, νόμιμες ή παράνομες αυτοπροστατευόμενες επιθέσεις, στο σύστημα RFID από το passive party, θα μπορούσαν να θεωρηθούν ως πρόσθετο μέτρο.

ΚΕΦΑΛΑΙΟ 7

7.1. ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα Radio Frequency Identification (RFID) είναι συστήματα για αυτοματοποιημένη αναγνώριση και για εφαρμογή στην εφοδιαστική αλυσίδα. Ένα RFID αποτελείται κυρίως από τα tags και από τους readers.

Αναμένεται ότι αυτή η τεχνολογία τουλάχιστον θα αντικαταστήσει μερικώς τα barcodes στο μέλλον. Μία μεγάλη ανάπτυξη της αγοράς RFID προβλέπεται για το μέλλον. Σε αυτό θα συντελέσει η όλο και περισσότερο πτώση των τιμών των RFID tag. Το RFID χρησιμοποιείται σε πολλές εφαρμογές, όπως π.χ. στα νοσοκομεία, και στις βιβλιοθήκες κτλ.

Η ασφάλεια και η ιδιωτικότητα των RFID συστημάτων αποτελούν ένα πολύ σημαντικό ζήτημα γι΄ αυτό η εύρεση των επιθέσεων αλλά και των μέτρων εναντίων αυτών των επιθέσεων αποτελούν καίριο ζήτημα για να διασφαλιστεί η ασφάλεια των RFID.

Βιβλιογραφικές Αναφορές

[1] http://www.go-online.gr/ebusiness/specials/article.html?article_id=1592

[2] C.M. Roberts, Radio frequency identification (RFID), Departement of Information Sciences, Otago University, New Zealand, ScienceDirect, Computers & Security, vol.25, 2006.

[3] Security and privacy in radio-frequency identification devices, Stephen August Weis, Massachusetts Institute Of Technology, May 2003.

[4] Auto-ID Center, Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag, 23 February 2003.

[5] Prof.Dr.Heiko Knospe, University of Applied Sciences, Prof.Dr. Hartmut Pohl, University of Applied Sciences Bonn-Rhein-Sieg, RFID Security

[6] Finkenzeller, K.,RFID-HandBook, Fundamentals and Applications in Contactless Smart Cards and Identification,2nd edition,Wiley and Sons,2003

[7] Garfimkel.S, RFID Bill of Rights. Technology Review 10,35,2002.

[8] Juels. A, Minimalist cryptography for RFID tags for low-cost RFID tags. In submission,2003

[9] Pohl.H, Taxonomie und Modellbildung in der Informationssicherheit. Datenschutz und Datensicherung 11, 2004.

[10] Weis.S, Sarma.S, Rivest.R, Engels.D, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: security in pervasive computing, Lecture notes in Computer Science, Vol 2802, p 201-212, Berlin 2003

[11] Alireza Pirayesh Sabzevar, Security in RFID Systems. Project report for GMU ECE 646.

[12] Frank Thornton, Brad Haines, Anand M.Das, Hersh Bhargava, Anita Campbell, John Kleinschmidt, Rfid Security, 2006

[13] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Phillips, Guidelines for Securing Radio Frequency Identification (RFID) Systems, National Institute of Standards and Technology (NIST).

[14] Federal Office for Information Security, Security Aspects and Prospective Applications of RFID Systems.

[15] AUTO-ID CENTER: 860 MHz – 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification. Auto-ID Center /EPCglobal, Cambridge, MA, USA..

[16] AUTO-ID CENTER: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. Auto-ID Center/EPCglobal, Cambridge, MA, USA.

[17] EUROPEAN COMMISSION: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[18] EPCGLOBAL INC.: http://www.epcglobalinc.org, Abruf vom

[19] FINKE, T., KELTER, H.: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443- Systems. BSI, http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

[20] Die Ohrmarke bekommt elektronische Konkurrenz. In: fleischwirtschaft.de vom http://www.fleischwirtschaft.de/dokumentation/onlinearchiv/pages/protected/show.prl?params=keyword%3DITeK%26all%0320D%26type%3D1%26laufzeit%3D0&id=4454&currPage=1

[21] HENRICI, D. und MÜLLER, P. (2004): Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha A., Mattern F.: Pervasive Computing (Proceedings of PERVASIVE 2004, Second International Conference on Pervasive Computing). Springer-Verlag, LNCS 3001: 219-224

[22] HENRICI, D., MÜLLER J. und MÜLLER P. (in press): Sicherheit und Privatsphäre in RFIDSystemen. AG Integrierte Kommunikationssysteme, Technische

Universität Kaiserslautern, 18. DFN-Arbeitstagung über Kommunikationsnetze, Springer, Lecture Notes in Informatics. 1.-4. Juni 2004, Düsseldorf

[23] JUELS, A., RIVEST, R.L. und SZYDLO, M.: The Blocker Tag: Selective Blocking of RFID-Tags for Consumer Privacy.

[24] KLAß, C.: Einkaufsbetrug mit RFIDUmprogrammierung http://www.golem.de/0407/32666.html

[25] LAW, C., LEE, K. und SIU, K.Y.: Efficient Memoryless Protocol for Tag Identification. Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Boston, MA, USA. 75-84, verfügbar unter: http://portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal

[26] OHKUBO, M., SUZUKI, K. und KINOSHITA, S.: Cryptographic Approach to „Privacy- Friendly“ Tags. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA.

[27] Kevin FU, Building RFID Applications with Security and Privacy, Department of Computer Science University of Massachusetts at Amherst, USA, http://events.iaik.tugraz.at/RFIDSec06/Program/slides/014%20%20Invited%20Talk%20-%20Kevin%20Fu.pdf

[28] Gildas Avoine, Security and Privacy Issues in RFID Systems, EPFL, Lausanne, Switzerland, http://avoine.net/download/slides/Avoine-2006-emse-handout.pdf

[29] Vitaly Shmatikov, RFID Security and Privacy,

http://www.cs.utexas.edu/~shmat/courses/cs378_spring05/14rfid.ppt

[30]EUROSMART,http://www.eurosmart.com/Update/07-10/Eurosmart_White_paper_on_RFID_Oct07.pdf

[31] Leonid Bolotnyy and Gabriel Robins, New Directions in Detection. Security and Privacy for RFID, Departement of Computer Science, UVa, http://www.cs.virginia.edu/~robins/posters_and_presentations/Leonid_proposal_2007.ppt

[32] Ari Juels, RFID: Security and Privacy for Five-Cent Computers, Principal Research Scientist RSA Laboratories USENIX Security 2004.

[33] Steven Shepard, RFID: The Promise of a Strategic Technology, http://www.shepardcomm.com/RFID-whitepaper-wp.pdf

[34] Kevin Fu, RFID Security & Privacy Applications, Department of Computer Science University of Massachusetts at Amherst, USA http://prisms.cs.umass.edu/~kevinfu/talks/rfid-tutorial/usenix-fu-applications.pdf

[35] FREY, H. und STURM, P. (Universität Trier): UBICOMP Episode 14. http://www.syssoft.unitrier.de/systemsoftware/Download/Sommersemester_2004/Vorlesungen/Ubiquitous_Computing/14%20RFID.pdf