Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Ασφάλεια και ιδιωτικότητα σε RFID δίκτυα

Αντώνιος Ανατολίτης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Αύγουστος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ασφάλεια και ιδιωτικότητα σε RFID δίκτυα

Αντώνιος Ανατολίτης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Αύγουστος 2014

Περίληψη

Αντικείμενο της διατριβής είναι η επισκόπηση των δικτύων RFID (Radio Frequency Identification) ως προς την πλευρά της ασφάλειας, αλλά και της ιδιωτικότητας. Η τεχνολογία RFID είναι πλέον ευρέως διαδεδομένη, με ποικίλες εφαρμογές, όπου όμως ακριβώς λόγω των ιδιαίτερων χαρακτηριστικών της ανακύπτουν κρίσιμα ζητήματα τόσο ως προς την ασφάλεια (εμπιστευτικότητα/ακεραιότητα των δεδομένων, δεδομένου ότι απαιτούνται αλγόριθμοι με απαιτήσεις για χαμηλή κατανάλωση ισχύος) όσο και ως προς την ιδιωτικότητα (παρακολούθηση ("tracking") προσώπων).

Ειδικότερα, στη διατριβή μελετώνται τα βασικά χαρακτηριστικά της τεχνολογίας RFID, με έμφαση στους κινδύνους ασφαλείας που ανακύπτουν και στους τρόπους αντιμετώπισής τους. Περιγράφονται αναλυτικά κρυπτογραφικά πρωτόκολλα που έχουν προταθεί για εφαρμογή σε RFID δίκτυα προκειμένου να διασφαλίζεται η αυθεντικοποίηση, ενώ επίσης γίνεται αποτίμηση των πρωτοκόλλων αυτών βάσει γνωστών επιθέσεων που έχουν καταγραφεί στη βιβλιογραφία.

Επιπλέον, πέρα από τα αμιγώς τεχνολογικά ζητήματα, στην παρούσα διατριβή μελετώνται οι κοινωνικοί προβληματισμοί που ενέχει η χρήση των RFID και έχουν σχέση με τα θέματα ιδιωτικότητας και προστασίας των προσωπικών δεδομένων. Με το εν λόγω ζήτημα έχουν ασχοληθεί, λόγω της σπουδαιότητάς του, οι αρχές προστασίας δεδομένων στην Ευρωπαϊκή Ένωση, έχοντας εκδώσει σχετικά γνωμοδοτικά κείμενα στο πλαίσιο της νομοθεσίας για την προστασία προσωπικών δεδομένων. Η παρούσα διατριβή καταγράφει την υπάρχουσα κατάσταση, με απώτερο στόχο την εξαγωγή συμπερασμάτων ως προς την επιλογή της βέλτιστης, κάθε φοράς, επιλογής RFID τεχνολογίας για την εκάστοτε εφαρμογή.

Summary

Purpose of this paper is to review the network RFID (Radio Frequency Identification) on the side of safety and privacy. The RFID technology is now widespread, with a variety of applications, but where exactly because of the special characteristics of critical issues arise as to the security (confidentiality / integrity of data, as required low power algorithms) as well as to privacy (tracking persons).

In particular, we study the key technology features RFID, focusing on the security risks that arise and how to tackle them. Detailing cryptographic protocols have been proposed for application in RFID networks to ensure authentication and also are valued protocols on attacks that have been recorded in the literature.

Moreover, beyond of the purely technological issues, in this paper we study the social concerns associated with the use of RFID and related issues of privacy and protection of personal data. Because of its importance, with this issue have been worked the data protection authorities in the European Union, having adopted on advisory texts under the law for the protection of personal data. This paper records the current situation, with the ultimate aim of drawing conclusions as to the choice of the best, every time, RFID technology selection for any application.

Ευχαριστίες

Ευχαριστώ την οικογένεια μου και ιδιαίτερα τους γονείς μου για την υποστήριξη τους σε κάθε επιλογή που έχω κάνει. Πραγματικά χωρίς αυτούς δεν μπορώ να φανταστώ πως θα τα είχα καταφέρει.

Επίσης ευχαριστώ την αρραβωνιαστικιά μου για την υποστήριξη, αλλά και την υπομονή που έδειξε κατά την διάρκεια της περάτωσης αυτής της διατριβής.

Ακόμα θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή αυτής της διατριβής Δρ. Κωνσταντίνο Λιμνιώτη, καθώς χωρίς την πολύτιμη και καθοριστική συμβολή του, δεν θα ήταν δυνατή η υλοποίηση της παρούσας διατριβής..

Αφιέρωση

Η διατριβή αυτή είναι ιδιαίτερα αφιερωμένη στον αείμνηστο καθηγητή μου Κώστα Καραπούλιο που καθ' όλη την διάρκεια της πορείας μου στην επιστήμη της πληροφορικής ήταν κοντά μου και με συμβούλευε σαν δεύτερος πατέρας.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Το RFID (Radio Frequency Identification) στα ελληνικά ορίζεται ως Ταυτοποίηση ή Αναγνώριση Μέσω Ραδιοσυχνοτήτων. Αν και θεωρείται πρωτοποριακή και κατά πολλούς τεχνολογία από το μέλλον, μετρά 70 και πλέον χρόνια ύπαρξης. Για την ακρίβεια χρησιμοποιήθηκε για πρώτη φορά κατά τη διάρκεια του Β' Παγκοσμίου, από την πολεμική αεροπορία της Αγγλίας, για την αναγνώριση και τη διάκριση των εχθρικών από τα φιλικά αεροπλάνα.

Από εκεί και πέρα άρχισε να εδραιώνεται η χρήση και εκμετάλλευσή της. Αρχικά σε πειραματικό στάδιο και σε εργαστηριακό επίπεδο, για να φτάσουμε στο σήμερα, όπου γίνεται εφαρμογή της τεχνολογίας RFID στην καθημερινή μας ζωή, κυρίως μέσω της χρήσης της στην διακίνηση, τον έλεγχο και την ασφάλεια εμπορικών προϊόντων.

Βέβαια καθημερινά και λόγω της φιλοσοφίας του Διαδικτύου των Πραγμάτων (Internet of Things, εφεξής IoT) παρουσιάζονται όλο και νέες καινοτόμες υλοποιήσεις των RFID παγκοσμίως. Παράλληλα αναπτύσσεται το ενδεχόμενο της ευρείας εφαρμογής του, με την καθιέρωση προτύπων και την λειτουργία τους σε παγκόσμιο επίπεδο.

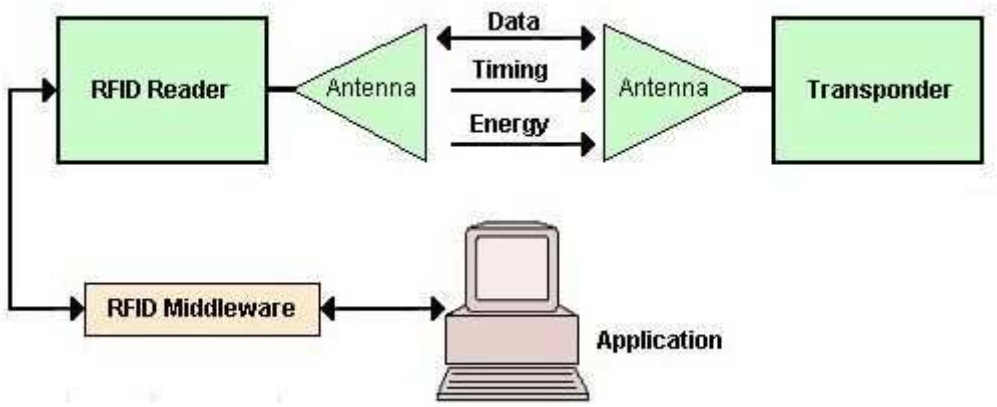
1.1 Δομή διατριβής

Στην παρούσα διατριβή θα δούμε στο 2ο κεφάλαιο μια αναλυτική παρουσίαση της RFID τεχνολογίας και των στοιχείων που την αποτελούν. Στο 3ο κεφάλαιο παρουσιάζονται εφαρμογές που υλοποιούνται χάρη στην RFID τεχνολογία και οι τομείς που επωφελούνται από αυτές. Στο 4ο κεφάλαιο διαπιστώνουμε τις απειλές και τις ευπάθειες των RFID συστημάτων, ενώ στο 5ο κεφάλαιο θα παρουσιαστούν οι τρόποι αντιμετώπισης των απειλών των RFID συστημάτων. Στο 6ο κεφάλαιο αναλύονται κρυπτογραφίες τεχνικές και πρωτόκολλα αυθεντικοποίησης και στο 7ο κεφάλαιο θα δούμε προβλήματα ιδιωτικότητας στα RFID συστήματα, το νομικό πλαίσιο για την προστασία της ιδιωτικότητας στα RFID συστήματα και τις κοινωνικές αντιδράσεις που προκαλούν οι RFID εφαρμογές. Τέλος στο 8ο κεφάλαιο θα δούμε τον επίλογο και τα συμπεράσματα της διατριβής.

Κεφάλαιο 2
Η τεχνολογία RFID

Για να ορίσουμε κατά πολλούς ένα σύστημα αρκεί να το παρουσιάσουμε. Βέβαια η αλήθεια είναι ότι και με το RFID δεν μπορούμε να κάνουμε αλλιώς. Αλλά στην περίπτωση μας θα κάνουμε μια προσπάθεια λέγοντας αρχικά ότι το RFID είναι ένα σύστημα το οποίο μεταδίδει την ταυτότητα και σημαντικές πληροφορίες ενός αντικειμένου ή ατόμου κάνοντας χρήση ραδιοσυχνοτήτων, πράγμα που είναι απόλυτα σαφές, αλλά πάλι στο ευρύ κοινό ακατανόητο. Για αυτό ας δούμε αναλυτικά την τεχνολογία RFID και τα μέρη που την αποτελούν.

Ένα τυπικό RFID σύστημα αποτελείται λοιπόν από δυο κύρια μέρη: την ετικέτα (tag), τον αναγνώστη (reader) και δυο δευτερεύοντα ή συνεπικουρούμενα μέρη: ένα υπολογιστικό σύστημα, που υποστηρίζει τα αλλά δυο μέρη και ένα ενδιάμεσο λογισμικό, που κατανοεί τις πληροφορίες που έρχονται από τον αναγνώστη στο υπολογιστικό σύστημα. Πολλές φορές βέβαια κατά περιπτώσεις έχουμε και επιπλέον δευτερεύοντα μέρη που εξαρτώνται άμεσα από τις παραμέτρους υλοποίησης.



Εικόνα 2.1: τυπικό RFID σύστημα

Η λειτουργία του συστήματος RFID είναι απλή και βασίζεται στην αμφίδρομη επικοινωνία των ετικετών με τους αναγνώστες. Όταν μια ετικέτα RFID βρεθεί στην εμβέλεια της κεραίας του αναγνώστη, ο αναγνώστης επικοινωνεί με ραδιοκύματα (συνήθως) με την κεραία της ετικέτας. Η ετικέτα ενεργοποιείται με τη σειρά της και επιστρέφει τα απαιτούμενα δεδομένα στον αναγνώστη. Η επικοινωνία μπορεί να συνεχιστεί και να επαναληφτεί ανάλογα με τις απαιτήσεις που υπάρχουν από και προς την ετικέτα. Στη συνέχεια παρεμβαίνει ένα ενδιάμεσο λογισμικό, το οποίο κατανοεί τις πληροφορίες, οι οποίες αποστέλλονται από τον αναγνώστη στο υπολογιστικό σύστημα .

2.1 Ετικέτα (RFID tag)

Μία RFID ετικέτα είναι μία ραδιοσυσκευή συνήθως μικρή, που εμφυτεύεται ή επικολλάται στο αντικείμενο που θέλουμε να ταυτοποιήσουμε. Η ετικέτα αποτελείται από ένα ολοκληρωμένο κύκλωμα, το οποίο είναι προσκολλημένο σε μία μικρή κεραία και τοποθετημένο σε μια επιφάνεια. Η όλη συσκευή μπορεί να καλυφθεί από ένα προστατευτικό π.χ. γυαλί ή πλαστικό ή ανάλογα με την κάθε περίπτωση ότι άλλο υλικό μπορεί να μας εξυπηρετεί. Η ετικέτα, πέρα από τις επεξεργαστικές ικανότητες που έχει, διαθέτει και μνήμη, στην οποία μπορούν να αποθηκευτούν περιορισμένου μεγέθους δεδομένα, όπως ένας μοναδικός αναγνωριστικός κωδικός EPC (Electronic Product Code) ο οποίος και αποτελεί την ταυτότητα για κάθε RFID ετικέτα. Είναι πολύ σημαντικό να αναφέρουμε ότι το μέγεθος μιας ετικέτας (αν και ποικίλει ανάλογα με τις απαιτήσεις) μπορεί να είναι 0,3 χιλιοστά, τόσο μικρό, όσο το μισό ενός κόκκου άμμου .

Εικόνα 2.2: RFID ετικέτα

Η πληθώρα των εφαρμογών που έχουν προκύψει για τα RFID συστήματα, έχει οδηγήσει στην ανάπτυξη RFID ετικετών με διαφορετικά χαρακτηριστικά καθώς και δυνατότητες, δίνοντας μας την ευχέρεια να τις ομαδοποιήσουμε ανάλογα με αυτά τα χαρακτηριστικά και τις δυνατότητες τους, όπως για παράδειγμα, την επεξεργαστική τους ισχύ, το μέγεθός τους, την ικανότητα εγγραφής τους στη μνήμη ή το δίαυλο επικοινωνίας που χρησιμοποιούν για να αλληλεπιδρούν (π.χ. συχνότητες ραδιοκυμάτων ή ηλεκτρομαγνητική επαγωγή).

Μια συνηθισμένη κατηγοριοποίηση είναι σε παθητικές (passive) και ενεργές (active) ετικέτες.

2.1.1 Παθητικές ετικέτες

Οι παθητικές RFID ετικέτες διαθέτουν ένα ολοκληρωμένο κύκλωμα (microchip) και μια κεραία. Η επικοινωνία γίνεται επειδή ο αναγνώστης στέλνει ραδιοκύματα, τα οποία μέσω της κεραίας, μεταδίδουν ηλεκτρικό ρεύμα στο κύκλωμα της RFID ετικέτας. Αυτή στη συνέχεια στέλνει τα δεδομένα, τα οποία έχουν αποθηκευτεί, στο ολοκληρωμένο κύκλωμα της για απάντηση.

Λόγω του τρόπου συλλογής της ενέργειας, οι παθητικές RFID ετικέτες έχουν περιορισμό τόσο στην απόσταση εκπομπής, δυνατότητα μετάδοσης σήματος μέχρι και 5 μέτρα, όσο και στο μέγεθος της μνήμης που μπορούν να έχουν. Όμως, λόγω της μεγάλη διάρκεια ζωής τους, καθώς και του χαμηλού τους κόστους, γίνονται πιο ελκυστικές για ένα μεγάλο κομμάτι εφαρμογών. Οι

παθητικές ετικέτες λειτουργούν στις συχνότητες των UHF, καθώς και των μικροκυμάτων LF και HF συχνότητες.

2.1.2 Ενεργές ετικέτες

Οι ενεργές RFID ετικέτες λειτουργούν με τον ίδιο τρόπο που λειτουργούν και οι παθητικές. Η διαφορά τους βρίσκεται στην τροφοδοσία του κυκλώματος που μεταδίδει τα δεδομένα, αφού οι ενεργές ετικέτες διαθέτουν μπαταρίες και έτσι μπορούν από μόνες τους να τροφοδοτήσουν την μετάδοση δεδομένων.

Μπορούν να στείλουν ένα σήμα στον αναγνώστη από μεγάλη απόσταση, η απόσταση αυτή μπορεί να είναι μερικές φορές αρκετές εκατοντάδες μέτρα. Για αυτό το λόγο χρησιμοποιούνται για την παρακολούθηση αγαθών μεγάλης αξίας, όπως εμπορεύματα, οχήματα και συνήθως λειτουργούν στις συχνότητες UHF και των μικροκυμάτων.

Οι ενεργές RFID ετικέτες έχουν ορισμένα πλεονεκτήματα έναντι των παθητικών. Ένα σημαντικό πλεονέκτημα το οποίο και ήδη προαναφέραμε, είναι ότι το σήμα εκπομπής των ενεργών ετικετών είναι πιο ισχυρό και άρα μπορούν να επικοινωνήσουν από μεγαλύτερες αποστάσεις με τον αναγνώστη. Επιπλέον, οι αναγνώστες δεν είναι υποχρεωμένοι να τροφοδοτούν με ισχύ τις ετικέτες, όπως συμβαίνει στις παθητικές RFID ετικέτες και έτσι μπορούν να χρησιμοποιούν σήμα χαμηλότερης ισχύος. Ακόμα χάρη στο ότι οι ενεργές RFID ετικέτες είναι ενεργειακά αυτόνομες, τους δίνεται η δυνατότητα να ξεκινούν μία επικοινωνία, κάτι που μπορεί να είναι απαραίτητο σε κάποιες εφαρμογές, όπως για παράδειγμα σε εφαρμογές που απαιτείται από την RFID ετικέτα να ενημερώσει, ότι μία ένδειξη έχει φτάσει κάποια τιμή.

Όμως λόγω της χρήσης της μπαταρίας, στις ενεργές RFID ετικέτες, προκαλείται μεγαλύτερο κόστος παραγωγής, επομένως και διάθεσης, ενώ συνήθως αυξάνεται και ο όγκος. Συμπερασματικά θα μπορούσαμε να πούμε ότι οι ενεργές ετικέτες καθίστανται επικρατέστερες για το μέλλον, με μόνη προϋπόθεση την μείωση του κόστους και του όγκου τους.

2.2 Αναγνώστης (RFID reader)

Ο αναγνώστη (reader) είναι μια συσκευή, συνήθως φορητή, η οποία αναλαμβάνει να επικοινωνήσει με τις RFID ετικέτες, μεταδίδοντας ραδιοκύματα. Αποτελείται από μια κεραία η

οποία μεταδίδει και λαμβάνει τα σήματα από και προς τις ετικέτες, καθώς και την μονάδα ελέγχου που καθορίζει τις ενέργειες, τις οποίες αναλαμβάνει να εκτελέσει ο αναγνώστης. Τα δεδομένα που φτάνουν στον αναγνώστη είναι συνήθως ο μοναδικός αναγνωριστικός κωδικός EPC που αποστέλλει η RFID ετικέτα, στη συνέχεια προωθούνται στο υπολογιστικό σύστημα, ώστε το υπολογιστικό σύστημα να τα επεξεργαστεί και να παράγει χρήσιμες πληροφορίες. Στις μέρες μας ο αναγνώστης και το υπολογιστικό σύστημα είναι συνήθως ενοποιημένα είτε σε μια κινητή συσκευή (πχ. υπολογιστής παλάμης), είτε σε μια σταθερή (πχ. σταθερός υπολογιστής).

Εικόνα 2.3: RFID αναγνώστης

2.3 Προτυποποίηση

Είναι φυσικό ότι έχοντας μια τόσο πρωτοποριακή τεχνολογία υπάρχει η ανάγκη προτυποποίησης, ώστε μια ετικέτα να μπορεί να είναι ικανή να αναγνωστεί σε οποιοδήποτε μέρος του πλανήτη. Ακόμα όμως δεν μπορούμε να πούμε ότι αυτό έχει γίνει, στο βαθμό που προσδοκούμε. Βέβαια υπάρχουν οι κατάλληλοι οργανισμοί που εκδίδουν πρότυπα για τα RFID.

Στην Ευρώπη υπάρχει το ETSI (European Telecommunications Standards Institute) που ορίζει τα τεχνικά χαρακτηριστικά των συσκευών Πανευρωπαϊκά.

Επίσης υπάρχουν δύο πολύ σημαντικοί οργανισμοί προτυποποίησης διεθνώς: ο Διεθνής Οργανισμός Προτυποποίησης ISO - International Organization for Standardization και ο EPC global που σε συνεργασία με τους κυριότερους κατασκευαστές RFID ορίζουν πρότυπα για το σύνολο της τεχνολογίας RFID, από γενικές οδηγίες για ασύρματες συσκευές (ISO/IEC 18000-1)

και τις τεχνικές προδιαγραφές για τις συχνότητες (ISO/IEC 18000-2 έως ISO/IEC 18000-7) έως την κωδικοποίηση δεδομένων (ISO 15962) και τα πρωτόκολλα επικοινωνίας (ISO 15961).

Ένα διαφορετικό πρότυπο είναι αυτό που σχετίζεται με τα δεδομένα του Ηλεκτρονικού Κωδικού Προϊόντος (Electronic Product Code – EPC) του EPC global. Το EPC είναι μία ομάδα διατάξεων κωδικοποίησης που δημιουργήθηκαν ως αντικαταστάτες των ραβδωτών κωδικών (barcodes). Οι διατάξεις αυτές σχεδιάστηκαν προκειμένου να διασφαλίζουν τη μοναδικότητα κάθε RFID ετικέτας, συμβατής με το πρότυπο EPC. Συνεπώς κάθε RFID ετικέτα που ακολουθεί το πρότυπο EPC, μπορεί να ταυτοποιεί μοναδικά το αντικείμενο στο οποίο έχει επικολληθεί και όχι απλώς τον τύπο του προϊόντος, όπως συμβαίνει με το ραβδωτό κώδικα.

Βέβαια για την αναγνώριση των αντικειμένων, αρκετές διατάξεις ονοματοθεσίας και κωδικοποίησης προτείνουν τη χρήση του συστήματος αρίθμησης του IPv6 [49], η χρήση του οποίου στην αρχή προτάθηκε για τα συστήματα του στρατού των ΗΠΑ, σε περίπτωση που για τις στρατιωτικές εφαρμογές, τα πρότυπα του EPC global κρίνονταν ανεπαρκή.

2.4 Αλγόριθμοι επικοινωνίας

Οι απλοί RFID αναγνώστες τις περισσότερες φορές μπορούν να επικοινωνήσουν με μία μόνο ετικέτα κάθε φορά. Επομένως εάν περισσότερες από μια ετικέτα ανταποκριθούν στο αίτημα, τότε ο αναγνώστης, λόγω της σύγκρουσης θα δυσκολευτεί να διαβάσει κάποια από τις ετικέτες, με αποτέλεσμα να δημιουργηθεί πρόβλημα, το οποίο προκειμένου να επιλυθεί, έχουν προταθεί μία σειρά από τεχνικές απομόνωσης (singulation)[44], οι οποίες δίνουν τη δυνατότητα στον αναγνώστη να επικοινωνήσει με όλες τις RFID ετικέτες. Οι δυο βασικότερες τεχνικές που χρησιμοποιούνται είναι ο αλγόριθμος διάσχισης δυαδικού δένδρου, και ένας αλγόριθμος που βάση του είναι η φιλοσοφία του αλγόριθμου ALOHA.

2.4.1 Αλγόριθμος Διάσχισης Δυαδικού Δένδρου (Binary Tree-Walking)

Η Διάσχιση Δυαδικών Δένδρων είναι ένας ντετερμινιστικός αλγόριθμος ο οποίος χρησιμοποιώντας μία διαδικασία bit προς bit ερωτημάτων, που θυμίζει αναζήτηση κατά βάθος ενός δυαδικού δένδρου, επιτρέπει την αναγνώριση μεμονωμένων RFID ετικετών. Ο κλασσικός αλγόριθμος απαιτεί από τον αναγνώστη τη μετάδοση του προθέματος, τα αρχικά bits δηλαδή, του μοναδικού αναγνωριστικού της RFID ετικέτας που θέλει να διαβάσει. Βέβαια το πλήθος των

bits που πρέπει ο αναγνώστης να μεταδώσει, εξαρτάται από το αριθμό των συγκρούσεων που θα εντοπίσει. Με αυτό τον αλγόριθμο όμως υπάρχει κίνδυνος μια πληροφορία, να αξιοποιηθεί από έναν κακόβουλο ωτακουστή, αφού για παράδειγμα εάν υπάρχουν δύο RFID ετικέτες που διαφέρουν όμως μόνο στα τρία τελευταία bits του μοναδικού αναγνωριστικού κωδικού τους, τότε ο αναγνώστης για να επιλέξει μία από τις δυο, θα πρέπει να μεταδώσει όλα τα αρχικά bits μέχρι και το προτελευταίο.

2.4.2 Αλγόριθμος ALOHA

Στα πρωτόκολλα αποφυγής σύγκρουσης (anti-collision) που βασίζονται στον αλγόριθμο Aloha, κάθε ετικέτα προτού απαντήσει σε ένα ερώτημα, καθυστερεί κατά ένα τυχαίο χρονικό διάστημα, σε σχέση με το σήμα του αναγνώστη. Έτσι λοιπόν εάν συμβεί μία σύγκρουση, οι ετικέτες που βρίσκονται εντός της εμβέλειάς του αναγνώστη, ενημερώνονται από αυτόν και αναγκάζονται προτού απαντήσουν, να καθυστερήσουν για ένα ακόμη τυχαίο χρονικό διάστημα. Τέτοιου είδους αλγόριθμοι, λειτουργούν χωρίς ο αναγνώστης να χρειάζεται να μεταδώσει καμία σημαντική πληροφορία (π.χ. μοναδικά αναγνωριστικά ετικετών), παρά μόνο εντολές. Σαφέστατα όμως, υπάρχουν και τροποποιήσεις, που επιτυγχάνουν καλύτερη αξιοποίηση της επικοινωνίας, ορίζοντας ότι ο αναγνώστης πρέπει να έχει τη δυνατότητα να σιωπήσει κάθε ετικέτα που έχει ήδη αναγνωριστεί. Όμως με ένας τέτοιο μηχανισμό επιλογής, μπορούμε να οδηγηθούμε σε διαρροή πληροφοριών από τον αναγνώστη, αφού η ισχύς του σήματος του είναι τέτοια που μπορεί να επιτρέψει την υποκλοπή των μοναδικών αναγνωριστικών των RFID ετικετών.

Κεφάλαιο 3
Εφαρμογές RFID

Τα RFID μπορούν χρησιμοποιηθούν για πολλές και χρήσιμες εφαρμογές που συμβάλουν στην πρόοδο της κοινωνίας και στον εκσυγχρονισμό της. Χαρακτηριστικό τους είναι ότι μπορούν να χρησιμοποιούνται είτε αυτόνομα είτε σε συνδυασμό με άλλες συσκευές ή εφαρμογές. Στο Κεφάλαιο αυτό θα δούμε τις κυριότερες εφαρμογές των RFID κατανοώντας την αξία τους και τις καινοτόμες λύσεις που προσφέρουν.

3.1 Εφοδιαστική αλυσίδα

Η κυριότερη χρήση των RFID συστημάτων σήμερα θα λέγαμε ότι είναι στο εμπόριο προϊόντων αντικαθιστώντας την τεχνολογία των ραβδοειδών κωδικών (barcodes), αν και τα RFID συστήματα χρησιμοποιούνταν και παλιότερα στην διαδικασία μεταφοράς και ασφάλειας υψηλής αξίας εμπορευμάτων, με πρώτες αναφορές στις ένοπλες δυνάμεις των Ηνωμένων Πολιτειών. Κυριότερο πλεονέκτημα σε σχέση με τους ραβδοειδείς κωδικούς είναι η μονοσήμαντη αναφορά στο αγαθό μέσα από τον μοναδικό αναγνωριστικό κωδικό (EPC) και όχι η αναφορά στον τύπο του αγαθού.

Θα λέγαμε λοιπόν ότι πλέον τα RFID έχουν επεκταθεί σε όλα τα προϊόντα, πολλές φορές όμως χωρίς να είναι ιδιαίτερης αξίας σαν τιμή, μονάδας προϊόντος, αλλά αξία μπορεί να δίνει η ομαλή μεταφορά τους και για αυτό βλέπουμε ότι τα RFID καθημερινά όλο και περισσότερο, χρησιμοποιούνται στην εφοδιαστική αλυσίδα.

Τα οφέλη σε αυτό τον κλάδο της οικονομίας μπορούμε να πούμε ότι είναι τεράστια αφού λόγω των RFID έχουμε:

- **Μείωση του κόστους μεταφορών και αποδοτικότερη διαχείριση εμπορευμάτων**. Είναι σημαντικό τα μέλη της εφοδιαστικής αλυσίδας να γνωρίζουν οποτεδήποτε, το ακριβές απόθεμα εμπορευμάτων τους και να μπορούν να προσδιορίσουν την πορεία των παραγγελθέντων προϊόντων. Επομένως χάρις σε αυτό μπορούμε να οδηγηθούμε σε πιο στοχευόμενες παραγγελίες, με αποτέλεσμα να μειώνεται η ανάγκη για διατήρηση μεγάλου όγκου προϊόντων, να μειώνεται το κόστος αποθήκευσης, αλλά και η απώλεια ευπαθών προϊόντων.

- **Μείωση των κλοπών.** Χάρη στον ακριβή εντοπισμό των προϊόντων, ελαχιστοποιείται η μη δυνατότητα εύρεσης ενός αγαθού, που τις περισσότερες φορές μπορεί να είναι και μπροστά μας και παρουσιάζεται μεγάλη μείωση των κλοπών από επιτηδείους.

- **Ευκολότερη δυνατότητα ανάκληση προϊόντων.** Πολλές φορές μας έχει τύχει να πάρουμε ένα προϊόν που η ημερομηνία λήξης του να έχει παρέλθει. Με τις RFID ετικέτες είναι δυνατόν να εντοπιστεί και να ανακαλεστεί το σύνολο των ληξιπρόθεσμων προϊόντων που δεν έχουν πωληθεί, καθώς και παρτίδα προϊόντων που για διαφόρους λόγους πρέπει να αποσυρθεί.

- **Συνεχείς ελέγχους των προϊόντων.** Η RFID τεχνολογία δίνει την ικανότητα στους συσκευαστές να τοποθετούν ετικέτες στα προϊόντα τους, οι οποίες κατά την διάρκεια της πορείας τους μέσα στην εφοδιαστική αλυσίδα, θα μπορούν να αποθηκεύουν δεδομένα, αλλά και να κατέχουν άμεσα δεδομένα για αυτά. Για παράδειγμα, ο καταναλωτής μπορεί να ελέγχει την θερμοκρασία του γάλακτος την στιγμή που το αγοράζει, αλλά και τη θερμοκρασία του κατά την διάρκεια της μεταφοράς του από τον παραγωγό, μέχρι και το ράφι του καταστήματος στο οποίο πωλείται.

3.2 Ασφάλεια

Στον τομέα της ασφάλειας, τα RFID, τα βρίσκουμε σε πολλές εφαρμογές. Εξαιτίας λοιπόν της ικανότητας εντοπισμού των ετικετών και της μοναδικής ταυτοποίησης αυτών, καθίστανται λειτουργικές για τον έλεγχο περιοχών περιορισμένης πρόσβασης και τον έλεγχο των ατόμων που έχουν πρόσβαση, με την χρήση «έξυπνων καρτών» (RFID ετικετών). Επιπλέον, η χρήση τους με σκοπό την μείωση των κλοπών στα καταστήματα λιανικής, με την προσάρτηση απλών ετικετών στα προϊόντα και την χρήση συστήματος ειδοποίησης, όταν εξέρχεται από το κατάστημα κάποια ετικέτα, εφαρμόζεται ήδη εδώ και αρκετά χρόνια με το φαινόμενο να είναι σύνηθες σε σχεδόν όλα τα καταστήματα λιανικού εμπορείου. Ποιος άλλωστε δεν έχει παρατηρήσει την ετικέτα που αφαιρείται σε ένα κατάστημα πώλησης ενδυμάτων;

Επίσης χρησιμοποιούνται και στα αυτοκίνητα για την ταυτοποίηση του ιδιοκτήτη και την αποφυγή της κλοπής μέσα από «έξυπνες κάρτες» ή των κλειδιών τους, με πρώτη γνωστή στο ευρύ κοινό εφαρμογή του immobilizer, που αν το κλειδί που μπαίνει στην μίζα του αυτοκινήτου δεν ταυτοποιηθεί, δηλαδή αν δεν υπάρχει επικοινωνία μεταξύ του αναγνώστη του αυτοκινήτου και του «έξυπνου κλειδιού» του ιδιοκτήτη, ο κινητήρας δεν εκκινεί.

Άλλη εφαρμογή είναι στη διαχείριση των αποσκευών, όπου εκεί τοποθετούνται οι RFID ετικέτες με στόχο την ελαχιστοποίηση των χαμένων αποσκευών. Ταυτόχρονα χρησιμοποιούνται και στην προστασία πολύτιμων εγγράφων, επικολλώντας πάνω σε αυτά RFID ετικέτες. Τέτοιου τύπου εφαρμογές συναντάμε πολλές φορές, σε δανειστικές βιβλιοθήκες ή βιβλιοθήκες που είναι ανοικτές για το κοινό.

3.3 Δημόσιος τομέας

Στον δημόσιο τομέα εκτός από εφαρμογές ασφάλειας δημόσιων κτηρίων και έλεγχου πρόσβασης που αναφέραμε και παραπάνω, έχουμε τις λεγόμενες κάρτες του πολίτη, ήδη σε πολλές χώρες (και της Ευρωπαϊκής Ένωσης) έχουν αντικαταστήσει τις αστυνομικές ταυτότητες και τα διαβατήρια, καθώς επίσης και άλλα δημόσια έγγραφα που πλέον θα περιέχονται σε μια «έξυπνη κάρτα» (smart card) που θα περιλαμβάνει μια RFID ετικέτα, μειώνοντας έτσι την γραφειοκρατία και ελέγχοντας αποδοτικότερα τους πολίτες του κράτους.

Παρόμοιες θα είναι και οι αλλαγές στην ταυτοποίηση των αυτοκινήτων. Η τοποθέτηση μιας RFID ετικέτας σε αυτά, θα αρκεί για να καταργηθούν οι αριθμοί πλαισίου και οι πινακίδες, καθώς επίσης και τα σήματα των ειδικών τελών, αφού τα απαραίτητα στοιχεία θα περιλαμβάνονται στα δεδομένα της ετικέτας.

3.4 Σύστημα υγείας

Στον τομέα της υγείας, όπως και με τα άλλα εμπορικά αγαθά έτσι και με τα φάρμακα, θα μπορεί να γίνεται καλύτερος έλεγχος, προσαρμόζοντας ετικέτες RFID σε αυτά, δίνοντας μας την δυνατότητα έλεγχου σε όλα τα στάδια παραγωγής και διακίνησης, καθώς και την άμεση απόσυρση τους αν αυτό χρειαστεί, είτε για λόγους λήξης τους, είτε λόγω άλλου προβλήματος.

Άλλη μια δυνατότητα που έχουμε με την RFID τεχνολογία στην υγεία, είναι η πιο αξιόπιστη εξέταση αίματος, ιστών και οργάνων που λαμβάνονται από τους ασθενείς και η παράλληλη ενίσχυση της προστασία της ιδιωτικότητας και των προσωπικών δεδομένων των ασθενών, μέσω του μοναδικού κωδικού ταυτοποίησης τους.

Επίσης ο εντοπισμός και η ταυτοποίηση των ασθενών ώστε να αποφεύγονται τα ιατρικά λάθη, αλλά κυριότερα η παρακολούθηση της κατάστασης τους, είναι ένα μεγάλο πλεονέκτημα που χάρη στην RFID τεχνολογία πραγματοποιείται με μεγαλύτερη ευκολία και φυσικά σώζει ζωές. Εσχάτως με τη εισαγωγή των RFID εφαρμογών στην μεταμόσχευση μελών το ιατρικό επιτελείο μπορεί να έχει πρόσβαση σε δεδομένα που πριν δεν ήταν διαθέσιμα, επίσης μπορεί να ελέγχει την κατάσταση του μοσχεύματος και να καλεί τον ασθενή στο νοσοκομείο πριν την εκδήλωση προβλημάτων με αποτέλεσμα να αποφεύγονται απρόοπτες επιπλοκές.

3.5 Άλλες εφαρμογές

Μία άλλη δημοφιλής εφαρμογή είναι η εμφύτευση RFID ετικετών σε κατοικίδια ή αγροτικά ζώα, που διαθέτουν πληροφορίες για το ιατρικό ιστορικό τους αλλά και τον ιδιοκτήτη τους, ώστε να είναι δυνατός ο εντοπισμός του ζώου άμεσα.

Ακόμα στα μέσα μεταφοράς με την αντικατάσταση των κλασσικών εισιτηρίων με εισιτήρια που περιέχουν ετικέτες RFID, γίνεται ταχύτερη η πρόσβαση των επιβατών, μειώνεται το κόστος του εισιτηρίου, ενώ με κατάλληλο εξοπλισμό και τοποθέτηση ετικετών και στα ίδια τα μέσα και

τοποθέτηση αναγνωστών στις στάσεις, οι πολίτες μπορούν να ενημερώνονται για την πορεία των μέσων, τον ακριβή χρόνο αναμονής, αλλά και την πληρότητα των μέσων στα οποία θέλουν να επιβιβαστούν, πριν ακόμα αυτά έρθουν στην στάση.

Επίσης η είσπραξη των διοδίων στους αυτοκινητόδρομους γίνεται ταχύτερη, ευκολότερη, και φθηνότερη, καθώς γίνεται αυτόματα, δίχως την ανάγκη ύπαρξης προσωπικού για την πραγματοποίηση της συναλλαγής, απλά και μόνο με την αγορά από τον οδηγό μιας RFID ετικέτας, η οποία θα χρεώνεται κάθε φορά που περνάει από τα διόδια. Βέβαια, η τεχνολογία αυτή έχει ακόμα μεγαλύτερες δυνατότητες, αφού μελλοντικά θα μπορούσε να γίνεται η χρέωση στην RFID ετικέτα που θα έχει το αυτοκίνητο και η πληρωμή να γίνεται μέσω της φορολογικής δήλωσης του πολίτη, ενώ μέσω αυτής θα μπορούσε να γίνεται και η πληρωμή των προστίμων που θα επιβάλλονται σε κατόχους αυτοκινήτων, για τα οποία βεβαιώνονται παραβάσεις.

Τέλος θα λέγαμε ότι υπάρχουν και αμφιλεγόμενες εφαρμογές. Μερικά παραδείγματα είναι: το γραφείο του Γενικού Εισαγγελέα του Μεξικό, που χρησιμοποιεί RFID εμφυτεύματα για τον έλεγχο της πρόσβασης στο υπολογιστικό κέντρο δίωξης εγκλήματος που είχε προκαλέσει διενέξεις γύρω από τα ηθικά ζητήματα που εγείρονται, ενώ και σε σχολείο στην Osaka της Ιαπωνίας και ένα άλλο στο Doncaster του Ηνωμένου Βασιλείου, ετικέτες RFID έχουν ραφτεί στις σχολικές στολές που χρησιμοποιούνται για τον έλεγχο της θέσης των μαθητών, ενώ το σχολείο στο Doncaster έχει προσθέσει προσωπικά δεδομένα στις ετικέτες, προκειμένου να επιτρέπεται στο εκπαιδευτικό προσωπικό να διαβάζει ασύρματα, τα στοιχεία και την πρόοδο του μαθητή με τη χρήση ενός αναγνώστη. Στο ίδιο πλαίσιο, οι κατασκευαστές ελπίζουν ότι, στο κοντινό μέλλον, η RFID τεχνολογία θα χρησιμοποιείται και για την αναγνώριση των πελατών, στα καταστήματα για την παροχή προσωπικών υπηρεσιών και διαφημίσεων, με στόχο την καλύτερη εξυπηρέτησή τους, εγείροντας όμως έτσι ηθικά θέματα (όπως παραβίαση ιδιωτικότητας – προσωπικών δεδομένων) που θα τα συζητήσουμε σε επόμενο κεφάλαιο αναλυτικότερα.

3.6 Εφαρμογές RFID και IoT

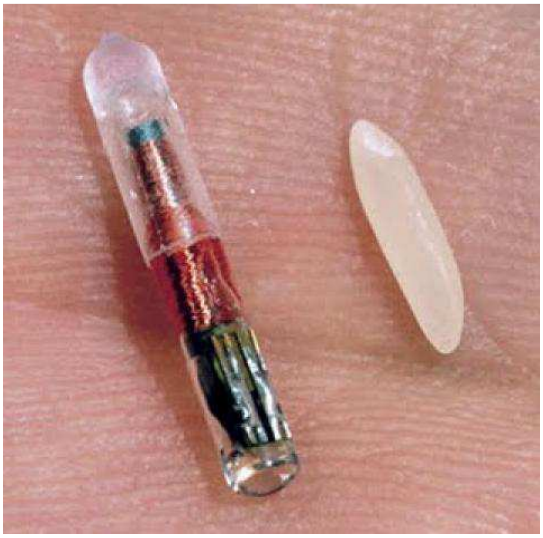
Το Διαδίκτυο των Πραγμάτων (Internet of Things- εφεξής IoT) είναι πλέον μέρος της ζωής μας. Πολλές συσκευές πλέον έχουν αυτή τη φιλοσοφία και σχεδόν όλα τα αντικείμενα γύρω μας σε λίγα χρόνια θα είναι διασυνδεδεμένα με το διαδίκτυο ή θα μπορούν να επικοινωνούν με αυτό. Οι εφαρμογές RFID φυσικά και δεν αποκλίνουν από την φιλοσοφία του IoT. Πολλοί δε μάλιστα ισχυρίζονται ότι οι εφαρμογές RFID κάνουν το IoT να είναι πια μέρος της ζωής μας. Τα

παραδείγματα RFID εφαρμογών με τη φιλοσοφία του IoT είναι πολλά, όπως το «έξυπνο» ψυγείο που μπορεί να αναγιγνώσκει τις RFID ετικέτες των προϊόντων που βρίσκονται μέσα του και όπου υπάρχει έλλειψη κάποιου προϊόντος, να κάνει παραγγελία μέσω του διαδικτύου. Ταυτόχρονα ελέγχει τα προϊόντα του για τυχόν αλλοίωση.

Επίσης άλλη μια εφαρμογή είναι οι «έξυπνες» πόρτες ασφαλείας που διαβάζουν την είσοδο και την έξοδο RFID ετικετών και αναλόγως μπορούν να σβήσουν τα φώτα ή και ακόμα και την θέρμανση του κτιρίου, εάν δεν υπάρχει κανείς.

Οι νέες «έξυπνες» πιστωτικές κάρτες (smart cards) είναι και αυτές στην ίδια φιλοσοφία, αφού πλέον ο πελάτης δεν χρειάζεται να τις βγάλει από το πορτοφόλι του και απλά ο λογαριασμός του χρεώνεται αυτόματα. Όπως πολλοί ισχυρίζονται ίσως είναι το μέλλον στις πληρωμές, μιας και θα είναι δυνατόν αντί των ηλεκτρονικών εισιτηρίων ή άλλων παρόμοιων εφαρμογών να χρεωνόμαστε απευθείας στην RFID πιστωτική μας κάρτα, που φυσικά θα μπορούμε να ελέγχουμε και από τον διαδικτυακό μας λογαριασμό.

Πιο πρόσφατα και στην ίδια φιλοσοφία με τις RFID πιστωτικές κάρτες έχουν δημιουργηθεί επίσης εφαρμογές πληρωμής με τη χρήση της RFID ετικέτας του κινητού μας τηλεφώνου. Επιπλέον παρόμοιες εφαρμογές πληρωμής γίνονται και με ετικέτες RFID εμφυτευμένες σε ανθρώπους για να μην χρειάζεται να κουβαλάμε τίποτα πάνω μας, κάτι που βέβαια κατά πολλούς καταπατά τα ανθρώπινα δικαιώματα και προκαλεί –δικαιολογημένα- κοινωνικές αντιδράσεις.



Εικόνα 3.1: Εμφύτευμα RFID

Όπως μπορούμε να καταλάβουμε λοιπόν, οι RFID εφαρμογές με την φιλοσοφία του IoT είναι πάρα πολύ πρωτοποριακές, ίσως θα λέγαμε από μια άλλη εποχή και το βασικό που θα πρέπει να κατανοήσουμε είναι ότι όλες αυτές οι εφαρμογές είναι μόνο η αρχή, αφού το IoT είναι μόλις στο ξεκίνημά του.

Κεφάλαιο 4
Απειλές και ευπάθειες στα RFID

Τα RFID όπως και κάθε τεχνολογία, έχουν και αυτά τις αδυναμίες τους και τις διάφορες ευπάθειες που κάποιος μπορεί να τις εκμεταλλευτεί και να προκαλέσει προβλήματα.

Τα συστήματα RFID είναι ευάλωτα σε ένα ευρύ φάσμα κακόβουλων επιθέσεων που μπορούμε να πούμε ότι ξεκινούν από την παθητική υποκλοπή και φτάνουν έως στην ενεργή παρέμβαση, σε αντίθεση με τα ενσύρματα δίκτυα, όπου τα υπολογιστικά συστήματα έχουν μέτρα προστασίας κεντρικά, αλλά και στο κάθε ένα σύστημα ξεχωριστά (π.χ. firewalls). Οι επιθέσεις κατά των RFID δικτύων μπορούν να στοχεύσουν σε ένα κομμάτι του συστήματος, δεδομένου ότι οι αναγνώστες και οι ετικέτες RFID λειτουργούν σε ένα ασταθές, θορυβώδες και ενδεχομένως επικίνδυνο περιβάλλον.

Επιπλέον, η τεχνολογία RFID εξελίσσεται γρήγορα - οι ετικέτες πολλαπλασιάζονται και συρρικνώνονται - έτσι και οι απειλές εξελίσσονται και τα συστήματα γίνονται πιο επιρρεπή. Για αυτό λοιπόν καθίσταται συνεχώς και πιο δύσκολο να έχουμε μια σφαιρική άποψη του προβλήματος. Επομένως χρειάζεται ομαδοποίηση των απειλών ώστε να γίνει αποτελεσματική

διαχείριση των κινδύνων, Γι αυτό λοιπόν θα ομαδοποιήσουμε τις επιθέσεις RFID σε επίπεδα (που σχετίζονται , αλλά δεν ταυτίζονται με το μοντέλο OSI).

Παρακάτω θα κατατάξουμε τις επιθέσεις στο επίπεδο που κάθε επίθεση λαμβάνει χώρα, δίνοντας τα ιδιαίτερα χαρακτηριστικά τους. Θα διακρίνουμε τις επιθέσεις στο φυσικό επίπεδο, στο επίπεδο δικτύου και μεταφοράς, στο επίπεδο εφαρμογής και στο στρατηγικό επίπεδο, καθώς και σε πολύεπίπεδες επιθέσεις που επηρεάζουν περισσότερα από ένα επίπεδα .

Άλλες ταξινομήσεις των πιθανών απειλών και κινδύνων σε δίκτυα RFID έχουν επίσης προταθεί ([1] , [2] , [21] , [27]). Avoine, G .κ.ά. [1] , Ayoade, J. κ.ά. [2], και Garfinkel, S. κ.ά. [21] έχουν επικεντρωθεί στις απειλές της ιδιωτικής ζωής , ενώ ο Καρύγιαννης Α. κ.ά. [27] έχουν προτείνει μια λεπτομερή ταξινόμηση σε κινδύνους δικτύων, επιχειρηματικών διαδικασιών και επιχειρηματικής ευφυΐας. Ο Avoine, G .κ.ά. [1] δείχνουν ότι τα ζητήματα προστασίας της ιδιωτικής ζωής δεν μπορούν να επιλυθούν χωρίς να κοιτάμε κάθε επίπεδο ξεχωριστά. Εμείς διευρύνουμε εξετάζοντας και άλλους τύπους απειλών για να δώσουμε μια καλύτερη εικόνα του προβλήματος συμφώνα με την Mitrokotsa A.[34].

4.1 Φυσικό Επίπεδο

Το φυσικό επίπεδο στις επικοινωνίες των RFID αποτελείται από το φυσικό περιβάλλον και τις συσκευές RFID. Ο αντίπαλος σε αυτό το επίπεδο εκμεταλλεύεται τα ασύρματα χαρακτηριστικά των επικοινωνιών RFID, την κακή φυσική τους ασφάλεια και την ανεπαρκή αντοχή τους κατά την φυσική (σωματική) επίθεση. Αυτό το επίπεδο περιλαμβάνει επιθέσεις που έχουν μόνιμη ή προσωρινή απενεργοποίηση των RFID ετικετών, καθώς και τις επιθέσεις αξιοπιστίας.

4.1.1 Μόνιμη Απενεργοποίηση Ετικέτας

Η μόνιμη απενεργοποίηση ετικέτας RFID περιλαμβάνει όλες τις πιθανές ευπάθειες ή απειλές που μπορεί να έχουν ως αποτέλεσμα την ολική καταστροφή ή ουσιαστικά την υποβαθμισμένη λειτουργία μια ετικέτας RFID. Πιθανοί τρόποι με τους οποίους μια ετικέτα RFID είναι οριστικά ακατάλληλη είναι η αφαίρεση της ετικέτας, η καταστροφή της ή η χρήση της εντολής KILL στην ετικέτα.

Αφαίρεση Ετικέτας

Οι RFID ετικέτες έχουν χαμηλή φυσική ασφάλεια, αφού δεν ενσωματώνονται σε αντικείμενα και μπορούν εύκολα να αφαιρεθούν από ένα αντικείμενο και στη συνέχεια μπορούν να τοποθετηθούν σε ένα άλλο. Ένα απλό παράδειγμα είναι η αφαίρεση της ετικέτας από έναν κλέφτη σε ένα σούπερ μάρκετ για να αλλάξει την RFID ετικέτα ενός ακριβού προϊόντος, με εκείνη ενός φτηνότερου προκειμένου να πληρώσει λιγότερο στο ταμείο. Αυτό το είδος της απειλής είναι μια πραγματικότητα που μπορεί εύκολα να πραγματοποιηθεί χωρίς την ύπαρξη ειδικών τεχνικών δεξιοτήτων και θέτει ένα θεμελιώδες πρόβλημα στην ασφάλεια. Ωστόσο, αυτό το είδος της επίθεσης δεν είναι δυνατόν να πραγματοποιηθεί σε μαζική κλίμακα, χωρίς να γίνει αντιληπτό.

Καταστροφή Ετικέτας

Με την ίδια φιλοσοφία της χαμηλής φυσικής ασφάλειας, μία ετικέτα μπορεί να καταστραφεί, ακόμη και αν δεν υπάρχει κέρδος για τον επιτιθέμενο. Ένας βανδαλισμός RFID μπορεί απλά να προκαλεί ενδιαφέρον σε «ενοχλητικά» άτομα. Επίσης μια λειτουργική διαταραχή μπορεί να καταστρέψει εύκολα RFID ετικέτες με χαμηλή φυσική προστασία. Ακόμα όμως και αν οι RFID ετικέτες ξεφύγουν από κακόβουλες προθέσεις βανδαλισμού, εξακολουθούν να είναι ευαίσθητες σε μια πιθανή καταστροφή που προκαλείται από ακραίες περιβαλλοντικές συνθήκες, όπως η πολύ υψηλές ή πολύ χαμηλές θερμοκρασίες ή ακόμα και το γδάρσιμο που μπορεί να προκληθεί από έναν κακό χειρισμό. Επίσης, οι ενεργές ετικέτες RFID μπορούν να αχρηστευθούν με την αφαίρεση ή την απόρριψη των μπαταριών τους. Επιπλέον, οι RFID ετικέτες είναι εξαιρετικά ευαίσθητες στο στατικό ηλεκτρισμό. Ηλεκτρονικά κυκλώματα RFID ετικετών μπορεί να καταστραφούν με ηλεκτροστατική εκκένωση που προκαλείται από την τριβή σε μεταφορικούς ιμάντες ή από υψηλής ενέργειας κύματα.

Εντολή KILL

Το Auto-ID center [9] και ο EPC global δημιούργησαν μια προδιαγραφή που ονομάζεται εντολή KILL που είναι σε θέση να σιωπήσει οριστικά μια RFID ετικέτα. Σύμφωνα με το σύστημα αυτό, κάθε RFID ετικέτα έχει ένα μοναδικό κωδικό ο οποίος ορίζεται από τον κατασκευαστή της ετικέτας και η χρήση του μπορεί να καταστήσει μια ετικέτα RFID οριστικά ακατάλληλη για χρήση. Παρά το γεγονός ότι αυτό το χαρακτηριστικό μπορεί να χρησιμοποιηθεί για λόγους

προστασίας της ιδιωτικότητας, είναι προφανές ότι μπορεί να αξιοποιηθεί από κακόβουλους αντιπάλους, προκειμένου να σαμποτάρουν ένα RFID.

4.1.2 Προσωρινή Απενεργοποίηση Ετικέτας

Ακόμη και αν μια RFID ετικέτα διαφεύγει τον κίνδυνο της μόνιμης απενεργοποίησης, είναι ακόμα δυνατόν να απενεργοποιηθεί προσωρινά, π.χ. ένας κλέφτης μπορεί να χρησιμοποιήσει ένα φύλλο ή μια σακούλα με επένδυση αλουμινίου και να δημιουργήσει έναν απλό κλωβό Faraday, προκειμένου να δημιουργήσει μια ασπίδα απέναντι στα ηλεκτρομαγνητικά κύματα (όπως εκείνα του RFID αναγνώστη) και να κλέψει οποιοδήποτε προϊόν ανενόχλητος. Επίσης οι RFID ετικέτες διατρέχουν τον κίνδυνο της ακούσιας προσωρινής ανικανότητας που προκαλείται από περιβαλλοντικές συνθήκες (π.χ. αν η ετικέτα καλυφθεί με πάγο). Προσωρινή απενεργοποίηση ετικέτας, μπορεί επίσης να είναι αποτέλεσμα των ραδιοηλεκτρικών παρασίτων που είναι είτε παθητικά είτε ενεργητικά.

Παθητικές παρεμβολές (Passive Interference)

Λαμβάνοντας υπόψη το γεγονός ότι τα δίκτυα RFID λειτουργούν σε ένα ασταθές και θορυβώδες περιβάλλον επικοινωνίας, καταλαβαίνουμε ότι καθίστανται ευαίσθητα σε πιθανές παρεμβολές και συγκρούσεις από οποιαδήποτε πηγή ηλεκτρομαγνητικών παρεμβολών, όπως ο ηλεκτρομαγνητικός θόρυβος της ηλεκτρικής γεννήτριας και τα καλώδια υψηλής τάσης. Αυτές οι παρεμβάσεις αποτρέπουν την ακριβή και αποτελεσματική επικοινωνία.

Ενεργητικές παρεμβολές (Active Jamming)

Αν και οι παθητικές παρεμβολές είναι συνήθως ακούσιες, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί το γεγονός ότι μια RFID ετικέτα ακούει αδιακρίτως σε όλα τα ραδιοφωνικά σήματα του εύρους ζώνης της. Έτσι, ο αντίπαλος μπορεί να προκαλέσει ηλεκτρομαγνητικές παρεμβολές δημιουργώντας ένα σήμα στην ίδια περιοχή, όπου εκπέμπει ο RFID αναγνώστης, προκειμένου να εμποδίσει την επικοινωνία των ετικετών με τον αναγνώστη.

4.1.3 Επίθεση Αναμετάδοσης

Σε μια επίθεση αναμετάδοσης ο αντίπαλος ενεργεί ως man-in-the-middle (ενδιάμεσος). Μια συσκευή υποκλοπής τοποθετείται κρυφά ανάμεσα σε μια RFID ετικέτα και τον αναγνώστη.

Αυτή η συσκευή είναι σε θέση να παρεμποδίζει και να τροποποιεί τα ραδιοσήματα μεταξύ της ετικέτας και του αναγνώστη. Η σύνδεση από την ετικέτα στον αναγνώστη γίνεται μέσα από τη συσκευή υποκλοπής προς τον αναγνώστη και το αντίστροφο. Έτσι η ετικέτα και ο αναγνώστης νομίζουν ότι επικοινωνούν απευθείας. Για να γίνει αυτό το είδος της επίθεσης ακόμα πιο εξελιγμένο, μπορούμε να χρησιμοποιήσουμε ξεχωριστές συσκευές υποκλοπής για την επικοινωνία με τον αναγνώστη και για την επικοινωνία με την ετικέτα. Μεγάλη ανησυχία προκαλεί το γεγονός ότι οι επιθέσεις αναμετάδοσης μπορεί να είναι επιτυχημένες ακόμη και από μεγάλες αποστάσεις, για παράδειγμα, μια επίθεση αναμετάδοσης μπορεί να χρησιμοποιηθεί για να φορτωθεί στον λογαριασμό μιας RFID κάρτας, το κόστος μιας συναλλαγής. Μια γερμανική μεταπτυχιακή εργασία σπουδαστή [48] απέδειξε την ευπάθεια της Ολλανδικής εταιρείας δημόσιων συγκοινωνιών, εκτελώντας μια επίθεση αναμετάδοσης στα «ηλεκτρονικά» (RFID) εισιτήρια της. Ο σπουδαστής εφάρμοσε το μοντέλο " ghost and leech", όπως περιγράφεται από τον Kfir και τον Wool [30], δημιουργώντας έντονο προβληματισμό.

4.2 Επίπεδο δικτύου και μεταφοράς

Σε αυτό το επίπεδο περιλαμβάνονται όλες οι επιθέσεις που βασίζονται στο τρόπο που τα RFID συστήματα επικοινωνούν και τον τρόπο που τα δεδομένα μεταφέρονται μεταξύ των δικτύων RFID. Σε αυτή την ενότητα θα περιγράψουμε τις επιθέσεις που επηρεάζουν το επίπεδο δικτύου και μεταφορών και θα γίνει διάκριση σε επιθέσεις που σχετίζονται με τις ετικέτες, σε επιθέσεις που σχετίζονται με RFID αναγνώστες και σε επιθέσεις πρωτόκολλου δικτύου.

4.2.1 Επιθέσεις σε RFID ετικέτες

Κλωνοποίηση

Ακόμα και το πιο σημαντικό και χαρακτηριστικό γνώρισμα των RFID συστημάτων, το μοναδικό αναγνωριστικό τους, είναι επιρρεπές σε επιθέσεις. Αν και θεωρητικά δεν μπορεί να ζητηθεί από ένα κατασκευαστή RFID να δημιουργήσει ένα κλώνο μιας RFID ετικέτας [32], στην πράξη έχει αποδειχθεί ότι η αναπαραγωγή RFID ετικετών δεν χρειάζεται ούτε πολλά χρήματα ούτε πολλή εμπειρία, λαμβάνοντας υπόψη την ευρεία διαθεσιμότητα εύκολα παραμετροποιήσιμων ετικετών. Ένα παράδειγμα είναι η επίδειξη από έναν Γερμανό ερευνητή της τρωτότητας των γερμανικών διαβατηρίων στην κλωνοποίηση [4].

Πλαστογράφηση

Η πλαστογράφηση είναι ουσιαστικά μια παραλλαγή της κλωνοποίησης, που όμως δεν αναπαράγουμε μια RFID ετικέτα. Σε αυτό το είδος των επιθέσεων ο αντίπαλος υποδύεται μια έγκυρη RFID ετικέτα για να κερδίσει τα προνόμιά της. Η πλαστογράφηση απαιτεί πλήρη πρόσβαση στα ίδια κανάλια επικοινωνίας, που έχει και η γνήσια ετικέτα. Αυτό απαιτεί επίσης και τη γνώση των πρωτοκόλλων, των μυστικών κωδικών και των τρόπων που χρησιμοποιούνται σε κάθε έλεγχο ταυτότητας που πρόκειται να λάβει χώρα.

4.2.2 Επιθέσεις σε RFID αναγνώστες

Πλαστογράφηση ταυτότητας

Λαμβάνοντας υπόψη το γεγονός ότι σε πολλές περιπτώσεις η επικοινωνία στα RFID δίκτυα είναι χωρίς έλεγχο ταυτότητας, οι επιτιθέμενοι μπορούν εύκολα να πλαστογραφήσουν την ταυτότητα ενός αυθεντικού RFID αναγνώστη, προκειμένου να αποσπάσουν ευαίσθητες πληροφορίες ή και ακόμα να τροποποιήσουν δεδομένα της RFID ετικέτα.

Υποκλοπή

Η ασύρματη λειτουργία των RFID κάνει τις υποκλοπές μια από τις πιο σοβαρές και διαδεδομένες απειλές. Στις υποκλοπές ένα μη εξουσιοδοτημένο άτομο χρησιμοποιεί μια κεραία, προκειμένου να καταγράψει τις επικοινωνίες μεταξύ των ετικετών και των RFID αναγνωστών. Αυτό το είδος της επίθεσης μπορεί να γίνει και προς τις δύο κατευθύνσεις (ετικέτα - αναγνώστη και αναγνώστη - ετικέτα). Από τους αναγνώστες διαβιβάζουμε πληροφορίες με πολύ μεγαλύτερη ισχύ σήματος από ότι στις ετικέτες, οπότε οι αναγνώστες είναι πιο επιρρεπείς σε αυτό το είδος των επιθέσεων και μάλιστα σε πολύ μεγαλύτερες αποστάσεις. Οι πληροφορίες που καταγράφονται μπορεί να χρησιμοποιηθούν, για να εκτελεστούν πιο εξελιγμένες επιθέσεις μελλοντικά. Η σκοπιμότητα αυτής της επίθεσης εξαρτάται από πολλούς παράγοντες, όπως η απόσταση του επιτιθεμένου από τις RFID συσκευές.

4.2.3 Επιθέσεις πρωτόκολλου δικτύου

Τα RFID συστήματα συχνά συνδέονται με ένα back-end σύστημα βάσεων δεδομένων και με συσκευές δικτύου στο συνολικό δίκτυο λειτουργιάς τους, ωστόσο, αυτές οι συσκευές είναι

ευαίσθητες όπως και οι άλλες συσκευές δικτύου. Ατέλειες του λειτουργικού συστήματος και των πρωτοκόλλων του δικτύου που χρησιμοποιούν, μπορεί να χρησιμοποιηθούν από επιτιθέμενους προκειμένου να εξαπολύσουν επιθέσεις και να θέσουν σε κίνδυνο το σύστημα.

4.3 Επίπεδο Εφαρμογής

Αυτό το επίπεδο περιλαμβάνει όλες τις επιθέσεις που στοχεύουν σε πληροφορίες που σχετίζονται με τις εφαρμογές και τις συνδέσεις στα RFID δίκτυα. Τέτοιες επιθέσεις είναι η μη εξουσιοδοτημένη ανάγνωση RFID ετικέτας, η τροποποίηση των στοιχείων της RFID ετικέτας και οι επιθέσεις σε ενδιάμεσα μέσα.

4.3.1 Μη εξουσιοδοτημένη ανάγνωση ετικέτας

Επειδή δεν υποστηρίζουν όλες οι RFID ετικέτες πρωτόκολλα αυθεντικοποίησης και αναγνώρισης του ατόμου που μπορεί να αναγνώσει μια ετικέτα, οι επιτιθέμενοι μπορούν να διαβάσουν εύκολα τα περιεχόμενα των RFID ετικετών (ακόμη και από μεγάλες αποστάσεις), χωρίς καν να αφήσουν ίχνη.

4.3.2 Τροποποίηση ετικέτας

Λαμβάνοντας υπόψη το γεγονός ότι οι περισσότερες RFID ετικέτες που είναι σε χρήση σήμερα η μνήμη τους τροποποιείται, οι επιτιθέμενοι μπορούν να το εκμεταλλευτούν αυτό και να τροποποιήσουν ή να διαγράψουν πολύτιμες πληροφορίες. Πρέπει να σημειωθεί ότι η ευκολία με την οποία μια τέτοια επίθεση μπορεί να πραγματοποιηθεί, εξαρτάται σε μεγάλο βαθμό από το πρότυπο που χρησιμοποιείται και από τα δικαιώματα ανάγνωσης και εγγραφής που θέτονται.

4.3.3 Επιθέσεις ενδιάμεσου συστήματος (middleware attacks)

Υπερχείλιση μνήμης

Οι Υπερχειλίσεις μνήμης αποτελούν μία από τις κυριότερες απειλές και από τα δυσκολότερα προβλήματα ασφαλείας στο λογισμικό. Η υπερχείλιση μνήμης εκμεταλλεύεται την αποθήκευση δεδομένων ή ένα κώδικα που είναι πάνω από τα όρια των ρυθμίσεων σταθερού μήκους για να προκαλέσει σύγχυση. Οι επιτιθέμενοι μπορούν να χρησιμοποιούν RFID ετικέτες για να

ξεκινήσουν υπερχειλίσεις μνήμης στο back-end RFID ενδιάμεσο σύστημα. Αν και αυτό είναι ασήμαντο, λαμβάνοντας υπόψη την αποθηκευτική μνήμη των RFID ετικετών, υπάρχουν εντολές που επιτρέπουν σε μια RFID ετικέτα να στέλνει το ίδιο μπλοκ δεδομένων επανειλημμένα [40], προκειμένου να υπερχειλίσει το σύστημα. Άλλες επιλογές περιλαμβάνουν τη χρήση συσκευών με περισσότερους πόρους, όπως έξυπνες κάρτες ή συσκευές που είναι σε θέση να μιμηθούν πολλές RFID ετικέτες, ή χρησιμοποιώντας μια ετικέτα με περισσότερη μνήμη από αυτή που αναμένεται.

Κακόβουλος κώδικας (Malicious code injection)

Οι RFID ετικέτες μπορούν να χρησιμοποιηθούν προκειμένου να διαδώσουν επικίνδυνο κώδικα που στη συνέχεια μπορεί να μολύνει τα υπόλοιπα μέρη του RFID δικτύου (RFID αναγνώστες και τα δίκτυα που συνδέονται με το σύστημα)[40]. Σε αυτή την περίπτωση, ο επιτιθέμενος χρησιμοποιεί τη μνήμη των ετικετών RFID για την αποθήκευση και τον ιό που μολύνει το σύστημα. Αν και αυτού του είδους οι επιθέσεις δεν είναι ευρέως διαδεδομένες, εργαστηριακά πειράματα [40] έχουν αποδείξει ότι είναι εφικτές. Λαμβάνοντας υπόψη το γεγονός ότι οι εφαρμογές ενδιάμεσου συστήματος (middleware) χρησιμοποιούν διάφορες γλώσσες προγραμματισμού , όπως η Javascript , PHP , XML κλπ., ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτό και τον κακόβουλο κώδικα, προκειμένου να θέσει σε κίνδυνο το ενδιάμεσο σύστημα. Συγκεκριμένα, οι RFID ετικέτες μπορούν να χρησιμοποιηθούν για την εισαγωγή κακόβουλου κώδικα σε RFID εφαρμογές που χρησιμοποιούν τα πρωτόκολλα του Διαδικτύου και γλώσσες script (κώδικα) . Με τον ίδιο τρόπο , μπορεί επίσης να πραγματοποιηθεί και για γλώσσα SQL [40], όπου ένας κώδικα εισάγεται με πρόθεση εκτέλεσης SQL ερωτήματος που μπορεί να οδηγήσει στη μη εξουσιοδοτημένη πρόσβαση στη back-end βάση δεδομένων και στη συνέχεια να αποκαλύψει ή ακόμη και να τροποποιήσει τα δεδομένα που αποθηκεύονται στο σύστημα.

4.4 Στρατηγικό επίπεδο

Σε αυτό το επίπεδο περιλαμβάνονται επιθέσεις που στοχεύουν σε επιχειρηματικές εφαρμογές, αξιοποιώντας τα λάθη στον σχεδιασμό των υποδομών και των εφαρμογών. Συγκεκριμένα σε αυτό το επίπεδο περιλαμβάνονται η κατασκοπεία, η κοινωνική εξαπάτηση, η παραβίαση των προσωπικών δεδομένων και οι στοχευμένες απειλές ασφάλεια.

4.4.1 Κατασκοπεία

Οι επιτιθέμενοι μπορεί να έχουν συχνά επιχειρηματικούς ανταγωνιστές ως στόχο. Εκμεταλλευόμενοι την δυνατότητα να παρακολουθούν τις ετικέτες, μπορούν να συγκεντρώνουν κρίσιμες και εμπιστευτικές πληροφορίες προκειμένου να σαμποτάρουν τους ανταγωνιστές τους. Οι πληροφορίες αυτές μπορούν να περιλαμβάνουν στρατηγικές και πρακτικές σχετικά με τους στόχου, τις μεταβολές των τιμών, τα χρονοδιαγράμματα παραγωγής [29] ή τα θέματα μάρκετινγκ. Τέτοιες επιθέσεις μπορεί να επιτευχθούν μέσω υποκλοπής, με την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε back-end βάσεις δεδομένων κλπ.

4.4.2 Κοινωνική εξαπάτηση

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει ακόμη και τις κοινωνικές δεξιότητες του, για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα RFID σύστημα και τις πληροφορίες του. Αντί να περάσει από την επίπονη διαδικασία της παρακολούθησης στις επικοινωνίες των RFID, ο επιτιθέμενος χρησιμοποίει ένα απλό τέχνασμα, δημιουργώντας κλίμα εμπιστοσύνης στους ανθρώπους για την αποκάλυψη εμπιστευτικών πληροφοριών. Ο επιτιθέμενος μπορεί απλά να επωφεληθεί από απλές πράξεις της ανθρώπινης καλοσύνης, όπως κρατώντας την πόρτα ανοιχτή (σε μια περιορισμένη περιοχή που κανείς για να εισέλθει χρειάζεται να κάνει χρήση RFID ετικέτας αυθεντικοποίησης) ή να δανειστεί μια ετικέτα RFID (οπότε μπορεί να κάνει ανάκτηση εμπιστευτικών πληροφοριών).

4.4.3 Απειλές στην Προστασία Προσωπικών Δεδομένων

Οι RFID ετικέτες ανταποκρίνονται σε κάθε αναγνώστη, εξουσιοδοτημένο ή μη, χωρίς να δίνουν καμία ένδειξη γι' αυτό στους ιδιοκτήτες τους. Αυτό το ιδιαίτερο χαρακτηριστικό μπορεί να αξιοποιηθεί από τους επιτιθέμενους για να παρακολουθούν το προφίλ των ατόμων. Η πιθανή συλλογή προσωπικών πληροφοριών, από τις αγοραστικές συνήθειες έως και τις ιατρικές πληροφορίες, είναι ένας από τους μεγαλύτερους κινδύνους στα RFID και έχει οδηγήσει σε εκστρατείες κατά της χρήση RFID. Οι απειλές στην ιδιωτικότητα μπορεί να έχουν διάφορες διαστάσεις, ανάλογα με τη συμπεριφορά του ιδιοκτήτη (RFID ετικέτας), από την ταύτιση ενός ατόμου με ένα στοιχείο (RFID ετικέτας), τον προσδιορισμό της θέσης του ιδιοκτήτη, τις προτιμήσεις του ιδιοκτήτη καθώς και την ταύτιση του με ένα σύνολο ετικετών που μπορεί να κατέχει και μπορούν να τον προσδιορίζουν [2].

4.4.4 Στοχευμένες απειλές για την ασφάλεια

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τις πληροφορίες που συλλέγονται από τη συσχέτιση της θέση, προκειμένου να προβεί σε κακόβουλες πράξεις, είτε φυσικές είτε ηλεκτρονικές. Χαρακτηριστικό παράδειγμα αυτής της επίθεσης είναι οι ληστείες σε ανθρώπους ή πολύτιμα αντικείμενα (π.χ. ρολόγια ή κοσμήματα), φορτηγά ή πλοία που μεταφέρουν πολύτιμα ή κρίσιμης σημασίας στοιχεία.

4.5 Πολυεπίπεδες επιθέσεις

Πολλές επιθέσεις που στοχεύουν στην επικοινωνία των RFID συστημάτων δεν περιορίζονται μόνο σε ένα επίπεδο επίθεσης. Στην κατηγορία αυτή περιλαμβάνονται οι επιθέσεις που επηρεάζουν πολλά επίπεδα, συμπεριλαμβανομένου του φυσικού, του δικτυού-μεταφορών, της εφαρμογής και το στρατηγικό επίπεδο. Ειδικότερα, στις πολυεπίπεδες επιθέσεις περιλαμβάνονται τα μυστικά κανάλια, η άρνηση παροχής υπηρεσιών, η ανάλυση της κίνησης, οι κρυπτογραφικές επιθέσεις, οι επιθέσεις παράπλευρου καναλιού και οι επιθέσεις αναμετάδοσης.

4.5.1 Μυστικά κανάλια

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις RFID ετικέτες, προκειμένου να δημιουργήσουν μη εξουσιοδοτημένους διαύλους επικοινωνίας για την κρυφή μεταφορά πληροφοριών. Οι επιτιθέμενοι μπορούν να επωφεληθούν από την αχρησιμοποίητη μνήμη αποθήκευσης πολλών RFID ετικετών, προκειμένου να μεταφέρουν με ασφάλεια δεδομένα με τρόπο τέτοιον ώστε να είναι δύσκολος να ανιχνευθεί [28]. Για παράδειγμα, ένα σύνολο από ετικέτες RFID εμφυτεύονται σε ανθρώπους, των οποίων κανονικά σκοπός θα ήταν να εντοπίσουν το κάθε άτομο, όμως θα μπορούσε στα κρυφά να αναφέρονται προσωπικά δεδομένα που σχετίζονται με ιατρικά θέματα ή κοινωνικές δραστηριότητες των ατόμων αυτών.

4.5.2 Άρνηση παροχής υπηρεσιών

Η κανονική λειτουργία των RFID ετικετών μπορεί να διακόπτεται επίτηδες και να παρεμποδίζεται η πρόσβαση σε αυτές. Ο σκόπιμος αποκλεισμός της πρόσβασης και η επακόλουθη άρνηση της υπηρεσίας για μια RFID ετικέτα μπορεί να προκληθεί από τον επιτιθέμενο με «ετικέτες blocker» (blocker tags)[25] ή από έναν RFID φύλακα (guardian) [41] .

Και οι δύο αυτές προσεγγίσεις έχουν προταθεί για την προστασία των επικοινωνιών στα RFID δίκτυα από τις απειλές κατά της ιδιωτικότητας. Παρ' όλα αυτά, θα μπορούσαν επίσης να χρησιμοποιηθούν από τους επιτιθέμενους για την εκτέλεση μια σκόπιμης άρνησης υπηρεσίας . Μια άλλη άρνηση της υπηρεσίας είναι η μη εξουσιοδοτημένη χρήση των εντολών LOCK. Οι εντολές LOCK [28] περιλαμβάνονται σε πολλά RFID πρότυπα, ώστε να αποτρέπεται η μη εξουσιοδοτημένη εγγραφή δεδομένων στη μνήμη της RFID ετικέτας. Ανάλογα με το πρότυπο που εφαρμόζεται η εντολή κλειδώματος (LOCK) εφαρμόζεται με ένα προκαθορισμένο κωδικό και μπορεί να έχει μόνιμη ή προσωρινή επίδραση. Επιπλέον, δεδομένου ότι τα ενδιάμεσα συστήματα RFID περιλαμβάνουν συσκευές δικτύωσης, ένας επιτιθέμενος μπορεί να επωφεληθεί από τον περιορισμό των πόρων του συστήματος και να προκαλέσει άρνηση εξυπηρέτησης στο ενδιάμεσο σύστημα RFID. Για παράδειγμα, στέλνοντας ένα σύνολο πακέτων στο ενδιάμεσο σύστημα, ώστε η χωρητικότητα του δικτύου ή η επεξεργασία των δεδομένων να κολλήσει και στη συνέχεια να προκληθεί άρνηση της πρόσβαση σε άλλους χρήστες .

4.5.3 Ανάλυση κίνησης

Η επικοινωνία των RFID συστημάτων είναι επίσης ευαίσθητη σε επιθέσεις ανάλυσης κίνησης. Ένας ωτακουστής είναι σε θέση να υποκλέψει μηνύματα και να πάρει πληροφορίες από μια επικοινωνία. Ακόμη και αν η επικοινωνία σε ένα RFID σύστημα προστατεύεται από κρυπτογράφηση και τεχνικές ελέγχου ταυτότητας, εξακολουθεί να είναι ευάλωτη σε επιθέσεις ανάλυσης κίνησης. Όσο μεγαλύτερος είναι ο αριθμός των μηνυμάτων που έχουν υποκλαπεί, τόσο πιο αποτελεσματική είναι η ανάλυση της κίνησης.

4.5.4 Κρυπτογραφικές Επιθέσεις

Όταν σημαντικές πληροφορίες αποθηκεύονται σε RFID ετικέτες, χρησιμοποιούνται τεχνικές κρυπτογράφησης, προκειμένου να διαφυλάξουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Ωστόσο, οι επιτιθέμενοι απασχολούνται με κρυπτογραφικές επιθέσεις για να σπάσουν κρυπτογραφικούς αλγορίθμους και να αποκαλύψουν τις πληροφορίες. Για παράδειγμα, στην Ολλανδία μια εταιρεία ασφαλείας που ονομάζεται Riscure [42] έχει αποδείξει ότι το κλειδί που χρησιμοποιείται σε έναν τύπο ολλανδικού διαβατήριου μπορεί να σπάσει εύκολα, χρησιμοποιώντας ένα τυποποιημένο PC και εκτελώντας μια επίθεση brute-force για δύο ώρες.

4.5.5 Επιθέσεις παράπλευρου καναλιού

Οι Επιθέσεις παράπλευρου καναλιού μπορούν να πλήξουν κρυπτογραφικούς αλγορίθμους ακόμα και αν δεν έχουν, σε θεωρητικό επίπεδο, τρωτά σημεία. Σε αυτό το είδος των επιθέσεων η πληροφορία που αξιοποιείται συνήθως περιλαμβάνει πληροφορίες χρονισμού, κατανάλωση ενέργειας ή ακόμα και ηλεκτρομαγνητικά πεδία. Η αποτελεσματική αξιοποίηση των επιθέσεων παράπλευρου καναλιού απαιτεί βαθιά γνώση του εσωτερικού του συστήματος στο οποίο εφαρμόζονται οι κρυπτογραφικοί αλγόριθμοι. Οι επιθέσεις χρονισμού υλοποιούνται από την εξέταση των διακυμάνσεων στην τιμή του υπολογισμού του στόχου, ενώ η απλή ανάλυση ισχύος (SPA) εξάγει πληροφορίες με βάση τις μεταβολές της κατανάλωσης ισχύος. Η ανάλυση διαφοράς επιπέδου ρεύματος (DPA) είναι ένας ειδικός τύπος των επιθέσεων ανάλυσης ισχύος που βασίζεται στις μεταβολές ηλεκτρομαγνητικού πεδίου που παράγεται , για παράδειγμα, κατά τη διάρκεια της επικοινωνίας μεταξύ ενός RFID αναγνώστη και της ετικέτας. Συγκεκριμένα, οι μεταβολές ηλεκτρομαγνητικού πεδίου όταν μια ετικέτα RFID εκτελεί μια κρυπτογραφική λειτουργία, μπορεί να χρησιμοποιηθεί για την αποκάλυψη των μυστικών κρυπτογραφικών κλειδιών.

4.5.6 Επιθέσεις αναμετάδοσης

Μια κοινή προσέγγιση για την άμυνα σε επιθέσεις όπως παραπάνω, είναι η χρήση ενός πρωτοκόλλου απόκρισης-πρόκλησης. Οι ετικέτες και οι RFID αναγνώστες συνήθως μοιράζονται ένα μυστικό και τη χρήση ενός πρωτοκόλλου απόκρισης πρόκλησης για την πιστοποίηση της ταυτότητάς τους. Παρ' όλα αυτά, πολύ συχνά αυτή η προσέγγιση υπόκειται σε επαναληπτικές επιθέσεις. Σε μια επίθεση επανάληψης, ο επιτιθέμενος μεταδίδει την απάντηση μιας ετικέτας η οποία καταγράφεται από προηγούμενη συναλλαγή, προκειμένου να μιμηθεί την ετικέτα για έναν αναγνώστη. Χαρακτηριστικό παράδειγμα αυτής της επίθεσης είναι η μη εξουσιοδοτημένη πρόσβαση σε ζώνες περιορισμένης πρόσβασης με τη μετάδοση της ακριβής επανάληψης του ραδιοσήματος που αποστάλθηκε από μια αυθεντική ετικέτα στον αναγνώστη που χορηγεί την πρόσβαση.

Κεφάλαιο 5
Τρόποι αντιμετώπισης απειλών στα RFID

Παρατηρώντας στο προηγούμενο κεφάλαιο τις διάφορες απειλές και ευπάθειες στα RFID συστήματα και το τι είναι δυνατόν να προκαλέσουν οι επιθέσεις από άτομα με κακόβουλες διαθέσεις, προκύπτει η ανάγκη παράθεσης τρόπων αντιμετώπισης των απειλών, ώστε αυτές να μειωθούν στο ελάχιστο ή αν είναι δυνατόν να εξαλειφθούν.

Είναι φανερό ότι η παρουσίαση θα πρέπει να ακολουθήσει μια ταξινόμηση. Γι' αυτό το λόγο θα ακολουθήσουμε την ταξινόμηση όπως και στο προηγούμενο κεφάλαιο, δηλαδή σε επίπεδο που η κάθε απειλή λαμβάνει χώρα θα παραθέτουμε τους ανάλογους τρόπους αντιμετώπισης.

5.1 Αντιμετώπιση απειλών φυσικού επίπεδου

Η διαφύλαξη των RFID συστημάτων σε επιθέσεις χαμηλού επιπέδου, όπως η μόνιμη ή προσωρινή απενεργοποίηση ετικετών, τα φυσικά αντίμετρα (π.χ. κλωβός faraday) επιβάλει να

χρησιμοποιηθούν τρόποι, όπως η ασφάλεια με φύλακες, περιφράξεις, προστατευτικές πόρτες και κάμερες [29]. Έτσι, οι εκούσιοι και οι ακούσιοι φυσικοί κίνδυνοι, καθώς και η χρήση των φύλλων αλουμινίου ή των τσαντών υπενδεδυμένων με αλουμίνιο θα μπορούσαν να επαλειφθούν. Επίσης η αφαίρεση των ετικετών θα μπορούσε να προληφθεί με την υιοθέτηση μέτρων, όπως η φυσική επίβλεψη ή η χρήση ισχυρότερων τρόπων, για να αποφύγει την εύκολη αφαίρεση των ετικετών (π.χ. ισχυρότερη κόλλα , η ενσωμάτωση ετικέτας στα προϊόντα). Οι εκούσιες και ακούσιες ράδιο παρεμβολές μπορούν επίσης να περιοριστούν από τεχνικούς τοίχους που τοποθετούνται κατάλληλα εμποδίζοντας κάθε είδος παρεμβολή σήματος [29]. Επιπλέον, η μη εξουσιοδοτημένη χρήση των εντολών KILL θα μπορούσε να αποφευχθεί με την αποτελεσματική χρήση κωδικών πρόσβασης. Για παράδειγμα , η εντολή KILL για Class-1 Gen-2 πρότυπο EPC [17] ετικετών απαιτεί έναν κωδικό πρόσβασης 32-bit.

Για την προστασία από επιθέσεις αναμετάδοσης, θα μπορούσε να χρησιμοποιηθεί η κρυπτογράφηση της επικοινωνίας στα RFID συστήματα ή η προσθήκη μιας δεύτερης μορφής ταυτοποίησης, όπως έναν κωδικό πρόσβασης, ένα PIN ή ένα βιομετρικό στοιχειό έλεγχου. Ωστόσο, η απαίτηση αυτή εξαλείφει την άνεση και τα πλεονεκτήματα της επικοινωνίας στα RFID συστήματα. Ένας άλλος πιθανός τρόπος για την αντιμετώπιση των επιθέσεων αναμετάδοσης, είναι το πρωτόκολλο οριοθέτησης απόστασης που βασίζεται στην επικοινωνία με παλμό ultra-wideband που προτείνουν ο Hancke κ.ά. [23]. Ακόμα μια άλλη ενδιαφέρουσα προσέγγιση που μπορεί να χρησιμοποιηθεί για την προστασία των RFID συστημάτων από επιθέσεις κυρίως στο φυσικό επίπεδο προτάθηκε από τον Bolotnyy κ.ά. [5] . Συγκεκριμένα, έχουν προτείνει μια λύση που βασίζεται σε υλικό και στηρίζεται σε μια συνάρτηση που δεν δυνατόν να κλωνοποιηθεί (pufs), παρέχοντας έτσι ασφάλεια και προστασία της ιδιωτικότητας. Η Pufs παρέχει μια εκθετική επίλυση στο κρίσιμο πρόβλημα της διανομής κλειδών και μπορεί να προστατεύσει την κλωνοποίησης RFID ετικετών, ακόμη και αν ο επιτιθέμενος έχει φυσική πρόσβαση σε αυτές.

5.2 Αντιμετώπιση απειλών επιπέδου δικτύου και μεταφοράς

Μέσα από κατάλληλη συλλογή δεδομένων, είναι δυνατή η ανίχνευση κλωνοποιημένων RFID ετικετών. Εναλλακτικά, οι επιθέσεις κλωνοποίησης μπορούν να μετριαστούν από τα πρωτόκολλα αυθεντικοποίησης απόκρισης - πρόκλησης. Αυτά θα πρέπει όμως να διαθέτουν μηχανισμούς καταπολέμησης των επιθέσεων brute force (εξαντλητικής αναζήτησης). Παρ' όλα

αυτά, οι εγγενείς περιορισμοί των πόρων που οι RFID ετικέτες παρουσιάζουν, μας οδηγούν σε αδύναμα πρωτόκολλα αυθεντικοποίησης που δεν μπορούν να αποτρέψουν τους ικανούς επιτιθέμενους, που είναι αποφασισμένοι να τα καταφέρουν. Ο Juels [27] κατέδειξε κάποιες τεχνικές για την ενίσχυση της αντοχής των EPC των RFID ετικετών σε επιθέσεις κλωνοποίησης, με τη χρήση PIN και τεχνικών απόκρισης πρόκλησης για τη αυθεντικοποίηση της ταυτότητας.

Η ευαισθητοποίηση του κοινού σε θέματα ασφάλειας που σχετίζονται με επιθέσεις κλωνοποίησης, θα πρέπει να είναι βασικό μέλημα για την υπεράσπιση ενάντια σε αυτές. Ωστόσο, το θέμα δεν είναι μόνο το ευρύ κοινό: χαρακτηριστικά αναφέρουμε ότι καμία από τις χώρες που εκδίδουν ηλεκτρονικά διαβατήρια (e-passports) δεν έχουν μηχανισμούς αποφυγής της κλωνοποίησης [32], όπως προτείνεται από το πρότυπο 9303 του ICAO [24].

Για την υπεράσπιση από παθητικές υποκλοπές, μπορεί να χρησιμοποιηθεί κρυπτογράφηση της επικοινωνίας στα RFID δίκτυα. Η πλαστογράφηση, καθώς και η πλαστοπροσωπία θα μπορούσαν να καταπολεμηθούν με τη χρήση πρωτόκολλων αυθεντικοποίησης ή με μία δεύτερη ταυτοποίηση, όπως τα συνθηματικά (passwords), τα PIN ή η χρήση βιομετρικών στοιχείων.

Τέλος οι επιθέσεις στο πρωτόκολλο δικτύου θα μπορούσαν να αντιμετωπιστούν με αύξηση της προστασίας όλων των στοιχείων που υποστηρίζουν την επικοινωνία στα RFID δίκτυα, χρησιμοποιώντας ασφαλή λειτουργικά συστήματα, απενεργοποιώντας ανασφαλή και μη χρησιμοποιούμενα πρωτόκολλα δικτύου και διαμορφώνοντας κατάλληλα τα πρωτοκόλλα που χρησιμοποιούνται, ώστε να έχουν μόνο τα απαραίτητα προνόμια.

5.3 Αντιμετώπιση απειλών επιπέδου εφαρμογής

Για την αντιμετώπιση της απειλής μη εξουσιοδοτημένης ανάγνωσης RFID ετικέτας και τροποποίησής της, τον έλεγχο της πρόσβασης σε RFID ετικέτες, θα πρέπει να εστιάσουμε σε μια προσέγγιση που προτείνει τη χρήση κλωβού faraday για την προστασία των RFID πιστωτικών καρτών και των ηλεκτρονικών διαβατηρίων από τη μη εξουσιοδοτημένη ανάγνωση. Πολλές εταιρείες αγκάλιασαν αυτή τη λύση και πωλούν αυτό το είδος των προϊόντων [33]. Ωστόσο, δεδομένου ότι η κλοπή των εμπιστευτικών δεδομένων μπορεί να πραγματοποιηθεί κατά το χρόνο της χρήσης, η προσέγγιση αυτή δεν φαίνεται να είναι πολύ αποτελεσματική. Τεχνικές κρυπτογράφησης, πρωτόκολλα αυθεντικοποίησης και λίστες ελέγχου πρόσβασης μπορεί να παρέχουν εναλλακτικές λύσεις. Συγκεκριμένα, υπάρχουν προσεγγίσεις που βασίζονται σε

συμμετρικό κλειδί κρυπτογράφησης [31], σε δημόσιο κλειδί κρυπτογράφησης [18], σε συναρτήσεις κατακερματισμού [52] , σε αμοιβαίο έλεγχο ταυτότητας ([35],[14]) ή ακόμα και σε μη κρυπτογραφικές λύσεις, όπως ψευδώνυμα [26]. Ωστόσο, ένας σημαντικός περιορισμός για τη χρησιμοποίηση αυτών των συστημάτων σε συστήματα RFID είναι ότι έχουν εγγενή τρωτά σημεία, όπως η διακοπή της παροχής ρεύματος ή η διακοπή της ασύρματης ζεύξης. Επιπλέον, πρέπει να έχουμε κατά νου ότι θα χρησιμοποιούμε όλες αυτές τις τεχνικές κρυπτογράφησης, ακόμη και σε όχι και τόσο σημαντικές εφαρμογές, όπως τα RFID συστήματα, για αντικείμενα όπως ξυραφάκια, παντόφλες, εσώρουχα ή άλλα είδη χαμηλού κόστος που σίγουρα δεν αξίζει τον κόπο, αλλά πρέπει και αυτά να προφυλαχθούν.

Οι υπερχειλίσεις μνήμης και η προσβολή από κακόβουλο κώδικα στο ενδιάμεσο σύστημα, μπορούν να καταπολεμηθούν με απλά αντίμετρα. Η εκτέλεση τακτικών ελέγχων στον κώδικα του συστήματος μπορεί να εξασφαλίσει την ασφάλεια του συστήματος, ενάντια στα τρωτά σημεία και τα σφάλματα, αρκεί να εξασφαλίσουμε ότι οι έλεγχοι πραγματοποιούνται [40]. Επίσης στις βάσεις δεδομένων, η χρήση των δεσμευμένων παραμέτρων και η όσο το δυνατόν λιγότερη απόδοση προνομίων [20], βοηθούν στην προστασία του συστήματος.

Τέλος, σε γενικές γραμμές, η απενεργοποίηση των περιττών ενδιάμεσων συστημάτων, όπως για παράδειγμα back-end συστήματα για scripting, συμβάλλει περαιτέρω στην ακεραιότητα του συστήματος. Άλλα απλά μέτρα περιλαμβάνουν την απομόνωση του διακομιστή ενδιάμεσου συστήματος RFID, έτσι ώστε σε περίπτωση που το διακύβευμα είναι υψηλό, να μην παρέχεται πρόσβαση στο υπόλοιπο του δικτύου, ελέγχοντας τα δεδομένα εισόδου στο ενδιάμεσο σύστημα και εξαλείφοντας τα ύποπτα στοιχεία.

5.4 Αντιμετώπιση απειλών επιπέδου στρατηγικής

Στις επιθέσεις σε αυτό το επίπεδο μπορούμε να προστατευθούμε με τη χρήση οποιουδήποτε από τα αντίμετρα που χρησιμοποιούνται, κατά τις επιθέσεις που περιλαμβάνονται στα άλλα στρώματα.

Ωστόσο, για την αποτελεσματική αντιμετώπιση των απειλών σε επίπεδο στρατηγικής θα πρέπει να τις αντιμετωπίσουμε ως ένα πρόβλημα που απαιτεί μακρόχρονη προσπάθεια. Οι εταιρείες και οι οργανισμοί που χρησιμοποιούν τα RFID συστήματα πρέπει να καθιερώσουν και να διατηρήσουν μια πολιτική προστασίας της ιδιωτικότητας και της προστασίας των δεδομένων,

εκτελώντας αξιολόγηση κινδύνων, ώστε να καθορίζονται οι απειλές και οι ευπάθειες που σχετίζονται με τις υποδομές που χρησιμοποιούνται για τα RFID συστήματα (βλέπουμε σχετικά και στο κεφάλαιο 7). Είναι σημαντικό να λάβουν καθοδήγηση από υπαλλήλους που είναι ειδικοί σε θέματα ιδιωτικότητας και νομικούς συμβούλους, σχετικά με τις στρατηγικές και τα θέματα προστασίας της ιδιωτικότητας που λαμβάνουν χώρα σε αυτές. Η πολιτική ασφάλειας θα πρέπει να κοινοποιείται σε όλους τους εργαζομένους. Η συνεχής επιμόρφωση και εκπαίδευση του προσωπικού σε θέματα ασφάλειας των RFID συστημάτων και πολιτικών προστασίας της ιδιωτικότητας είναι απαραίτητη, δεδομένου ότι προωθεί την ευαισθητοποίηση και την εποπτεία σε κρίσιμες πληροφορίες. Ο Καρύγιαννης κ.ά. [29] παρέχουν μια πλήρη λίστα των αντισταθμιστικών μέτρων που μπορούν να χρησιμοποιηθούν για την εξάλειψη των κινδύνων ιδιωτικότητας που σχετίζονται με τα RFID συστήματα.

Τα ζητήματα προστασίας της ιδιωτικότητας που σχετίζονται με τις επικοινωνίες στα RFID συστήματα, θα πρέπει επίσης να προσελκύουν την προσοχή από τους νομοθέτες και τις αρχές που μπορεί να δώσουν (όπως θα δούμε και σε επόμενο κεφάλαιο), τις κατευθυντήριες γραμμές, που πρέπει να ακολουθούνται από τους οργανισμούς και τις εταιρείες που χρησιμοποιούν RFID συστήματα.

5.5 Αντιμετώπιση πολυεπίπεδων απειλών

Οι επιθέσεις μυστικού καναλιού είναι δύσκολο να ανιχνευθούν και να αποφευχθούν. Οι ιδιοκτήτες και οι χρήστες των RFID ετικετών δεν έχουν καμία γνώση ότι οι ετικέτες τους έχουν παραβιαστεί και ότι χρησιμοποιούνται για μια συγκαλυμμένη επίθεση καναλιού. Η αποτροπή αυτών των επιθέσεων είναι ακόμα υπό έρευνα. Ωστόσο ένας πιθανός μηχανισμός για την καταπολέμησή τους πρέπει να επικεντρωθεί στη μείωση της διαθεσιμότητας των πόρων μνήμης σε μια RFID ετικέτα.

Οι επιθέσεις άρνησης παροχής υπηρεσίας και ανάλυσης κίνησης είναι σοβαρές απειλές για την ασφάλεια σε όλους τους τύπους των δικτύων, συμπεριλαμβανομένων των ενσύρματων. Ενώ θεωρητικά αυτά τα είδη των επιθέσεων μπορούν να αντιμετωπιστούν με μείωση των πόρων, στις RFID ετικέτες κάνουν την άμυνα προβληματική και παραμένουν ανοικτά σε περεταίρω έρευνα.

Οι κρυπτογραφικές επιθέσεις μπορούν να εξαλειφθούν μέσω της χρήσης των ισχυρών κρυπτογραφικών αλγορίθμων μέσα από κρυπτογραφικά πρότυπα και χρησιμοποιώντας ένα κλειδί με αρκετό μήκος. Έτσι, μπορούμε να αποφεύγουμε γεγονότα, όπως η αποκάλυψη των κενών ασφαλείας στις έξυπνες κάρτες.

Οι Επιθέσεις παράπλευρου καναλιού και πιο συγκεκριμένα οι επιθέσεις DPA, μπορούν να αποφευχθούν με τον περιορισμό των ηλεκτρομαγνητικών εκπομπών του συστήματος. Ωστόσο, αυτό συνεπάγεται συνήθως περιορισμό του εύρους λειτουργίας.

Για την άμυνα ενάντια σε επιθέσεις αναμετάδοσης στα RFID δίκτυα υπάρχουν μερικά απλά αντίμετρα, όπως είναι η χρήση των χρονικών ορίων (timestamps), των κωδικών (passwords) και η τεχνική απόκρισης πρόκλησης. Παρ' όλα αυτά, τα συστήματα αυτά είναι δύσχρηστα και με αμφίβολη αποτελεσματικότητα, λαμβάνοντας υπόψη τα τρωτά σημεία στα οποία τα πρωτόκολλα απόκρισης πρόκλησης είναι επιρρεπή. Μία άλλη περίπτωση είναι η χρήση της RF θωράκιση στους αναγνώστες, προκειμένου να περιοριστεί η εμβέλεια των ραδιοσημάτων [30]. Επίσης μία άλλη προσέγγιση είναι η αυθεντικοποίηση με βάση την απόσταση μεταξύ του αιτουμένου των πληροφοριών και του ιδιοκτήτη των πληροφοριών.

Ο Fishkin κ.ά. [19] ισχυρίζονται ότι ο λόγος σήματος-προς-θόρυβο του σήματος του αναγνώστη σε ένα RFID σύστημα, μπορεί να αποκαλύψει ακόμη και κατά προσέγγιση την απόσταση μεταξύ ενός αναγνώστη και μιας RFID ετικέτας. Η πληροφορία αυτή θα μπορεί σίγουρα να χρησιμοποιηθεί για να γίνει μια διάκριση μεταξύ των εξουσιοδοτημένων και μη εξουσιοδοτημένων αναγνωστών ή ετικετών και στη συνέχεια να μειωθούν οι επιθέσεις αναμετάδοσης.

Κεφάλαιο 6
Τεχνικές Κρυπτογραφίας στα RFID

Η κρυπτογραφία αποτελεί σημαντικό και ίσως αναπόσπαστο κομμάτι των RFID, ειδικά όταν μιλάμε για ασφάλεια. Συγκεκριμένα η διαδικασία αυθεντικοποίησης του αναγνώστη με την ετικέτα κατά μεγάλο μέρος κάνει χρήση κρυπτογραφίας και κρυπτογραφικών τεχνικών γενικότερα.

Ποιο κάτω θα αναλύσουμε τεχνικές και πρωτόκολλα αυθεντικοποίησης με κύριο σκοπό να αναδείξουμε την αποτελεσματικότητα τους, αλλά και να εντοπίσουμε τυχόν κενά που παρουσιάζουν.

6.1 Πρωτόκολλο Song & Mitchell

Το 2008 ο B. Song και ο C. J. Mitchell παρουσίασαν ένα πολύ αποτελεσματικό πρωτόκολλο αυθεντικοποίησης για RFID δίκτυα [45], ένα πρωτόκολλο που σύμφωνα με τους δημιουργούς του απευθύνεται σε χαμηλού κόστους ετικέτες RFID (χωρίς βέβαια να αποκλείει και τις

υπόλοιπες), παρέχει ασφάλεια στις πληροφορίες της ετικέτας, εξασφαλίζει προστασία από πλευράς εντοπισμού της θέσης της ετικέτας και είναι ανθεκτικό σε μια πλειάδα επιθέσεων που ο Song και ο Mitchell τις ταξινομούν σε αδύναμες επιθέσεις και σε ισχυρές επιθέσεις. Στις αδύναμες κατατάσσουν την επίθεση πλαστογράφησης ετικετών (Tag Impersonation), την επίθεση αναμετάδοσης (Replay Attack) και την άρνηση παροχής υπηρεσιών (Denial of Service Attack) ενώ στις ισχυρές επιθέσεις κατατάσσουν την ιχνηλάτηση προς τα πίσω (Backward Traceability), την ιχνηλάτηση προς τα εμπρός (Forward Traceability) και την πλαστοπροσωπία διακομιστή (Server Impersonation).

Για να παρέχει την ασφάλεια στις παραπάνω επιθέσεις το πρωτόκολλο κάνει χρήση μίας συνάρτησης κατακερματισμού, μιας ειδικά διαμορφωμένης συνάρτησης κατακερματισμού (έναν αλγόριθμο αυθεντικοποίησης ταυτότητας του μηνύματος) και μιας γεννήτριας ψευδοτυχαίων αριθμών.

Αναλυτικότερα για τη λειτουργία του πρωτόκολλου πρέπει:
Ένας κατασκευαστής (δημιουργός ετικέτας) να ορίσει μια συμβολοσειρά u_i από l bits για την ετικέτα Ti, να υπολογίσει το t_i που είναι ίσο με $h(u_i)$, το οποίο λέγεται αποτύπωμα του u_i, (όπου h η συνάρτηση κατακερματισμού) και να καταχωρήσει το t_i στην ετικέτα. Το l πρέπει να είναι αρκετά μεγάλο ώστε η εξαντλητική αναζήτηση για τις τιμές των t_i και u_i να είναι υπολογιστικά ανέφικτη. Στην βάση δεδομένων του διακομιστή αποθηκεύονται οι εγγραφές [(u_i, t_i)-νέα , (u_i, t_i)-παλαιά, Di] για κάθε ετικέτα, που διαχειρίζεται το σύστημα. Τα (u_i, t_i)-νέα είναι οι πιο πρόσφατες τιμές των u_i και t_i ενώ τα (u_i, t_i)-παλαιά είναι οι προηγούμενες (δηλαδή οι τιμές πριν την τελευταία απόδοση τιμών). Το Di είναι πληροφορίες για την ετικέτα (πχ. τιμή μονάδας, ημερομηνία λήξης κλπ.). Στην πρώτη ανάθεση τιμών στην βάση δεδομένων το (u_i, t_i)-νέα παίρνει τις τιμές t_i και u_i που πρωτοδημιουργούνται ενώ το (u_i, t_i)-παλαιά παίρνει null.

Στην διαδικασία αυθεντικοποίησης τώρα ο αναγνώστης (Reader) παράγει μια τυχαία συμβολοσειρά από bit, που καλείται r1, και την στέλνει στην ετικέτα. Η ετικέτα Ti παράγει και αυτή μια τυχαία συμβολοσειρά από bit, που με τη σειρά της καλείται r2, καθώς επίσης και τις συμβολοσειρές $M1=t1 \oplus r2$ και $M2=f_{ti}(r1 \oplus r2)$ (οπού $\oplus$ η πράξη xor – αποκλειστική διάζευξη). Ακολούθως στέλνει τα M1 και M2 στον αναγνώστη, ο οποίος με τη σειρά του στέλνει τα M1, M2 και r1 στον διακομιστή.

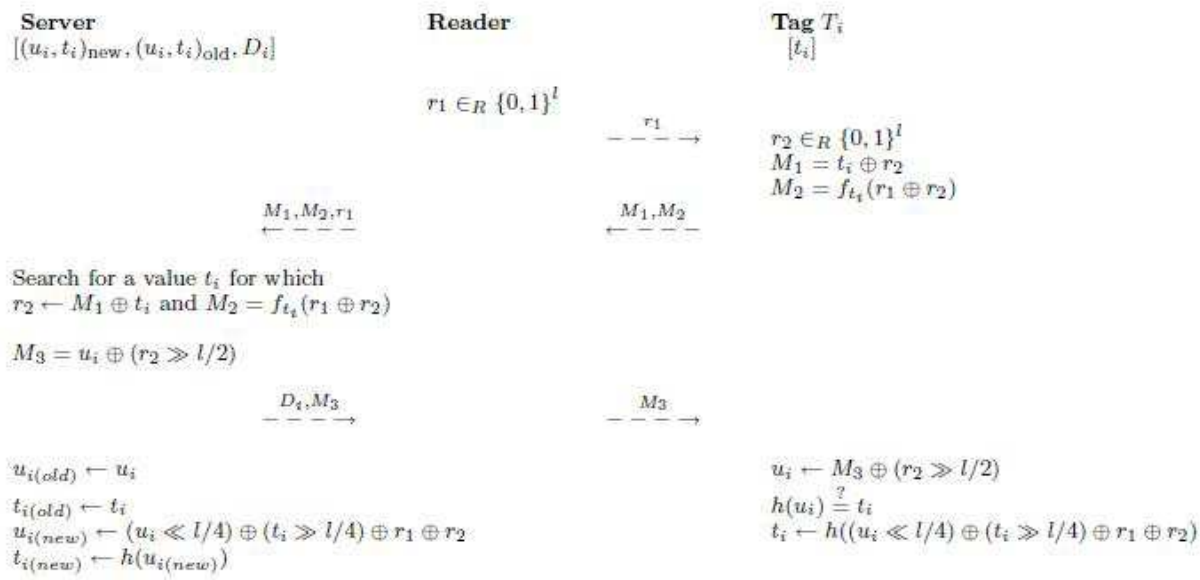
Ο διακομιστής αναζητά στην βάση δεδομένων χρησιμοποιώντας τα M1, M2 και r1 ως εξής: επιλέγει ένα t_i είτε από τις «νέες» εγγραφές {(u_i, t_i)-νέα} είτε από τις «προηγούμενες» { (u_i, t_i)-

παλαιά} που βρίσκονται στην βάση δεδομένων του συστήματος. Δημιουργεί ένα r2 = M1⊕ t_i και υπολογίζει το M2'=f_{ti} (r1⊕ r2) (οπού f_{ti} η ειδικά διαμορφωμένης συνάρτησης κατακερματισμού. Αν M2= M2' έχει βρει την ετικέτα Ti.

Αν M2≠ M2' επαναλαμβάνει τη διαδικασία με άλλο t_i . Αν δεν βρεθεί μετά από την συνολική αναζήτηση η ετικέτα Ti τότε ο διακομιστής στέλνει μήνυμα στον αναγνώστη να διακόψει την επικοινωνία.
Βρίσκοντας το Ti ο διακομιστής υπολογίζει το M3 = u_i⊕(r2 >>l/2) (όπου το σύμβολο >> σημαίνει ολίσθηση προς τα δεξιά) και το στέλνει στον αναγνώστη μαζί με το Di.

Ο διακομιστής ενημερώνει την βάση δεδομένων με τα (u_i, t_i)- παλαιά για την ετικέτα Ti (που ήταν τα προηγούμενα (u_i, t_i)-νέα) και τα (u_i, t_i)-νέα που είναι u_i(νεο)=(u_i <<l/4) ⊕ (t_i >> l/4) ⊕ r1 ⊕ r2 και το t_i(νέο)=h(u_i(νέο)) (όπου το σύμβολο << σημαίνει ολίσθηση προς τα αριστερά). Ο Αναγνώστης προωθεί το M3 στην ετικέτα Ti.

Η ετικέτα Ti υπολογίζει u_i=M3⊕(r2 >>l/2) και ελέγχει h(u_i)=t_i. Αν ο έλεγχος είναι επιτυχής η ετικέτα αυθεντικοποιεί τον αναγνώστη (και τον διακομιστή) και ορίζει t_i = h((u_i<<l/4) ⊕ (t_i >> l/4) ⊕ r1⊕ r2). Αν δεν είναι επιτυχής ο έλεγχος, κρατά την προηγούμενη τιμή του t_i.



Εικόνα 6.1: Πρωτόκολλο αυθεντικοποίησης Song & Mitchell [45]

Η διαδικασία που περιγράφηκε είναι ιδιαίτερα αποδοτική, απαιτώντας ελάχιστο χώρο αποθήκευσης και μικρή επεξεργαστική ικανότητα από πλευράς της ετικέτας, σε σχέση με παρόμοια πρωτόκολλα.

6.2 Πρωτόκολλο μεταβίβασης ιδιοκτησίας

Σε συνέχεια του πρωτοκόλλου αυθεντικοποίησης (Πρωτόκολλο Song & Mitchell) ο B. Song πρότεινε ένα πρωτόκολλο μεταβίβασης ιδιοκτησίας RFID ετικέτας [47] που βασίζεται εξ' ολοκλήρου στο πρωτόκολλο αυθεντικοποίησης.

Σε μια πληθώρα εφαρμογών RFID χρειάζεται να μεταβιβαστεί το δικαίωμα ιδιοκτησίας μιας ετικέτας, όπου μεταβίβαση ιδιοκτησίας μιας ετικέτας σημαίνει ότι ο διακομιστής του νέου ιδιοκτήτη αναλαμβάνει άδεια χρήσης της ετικέτας και έτσι θα πρέπει να δοθούν οι απαραίτητες πληροφορίες για να αλληλεπιδράσει με ασφάλεια και να εντοπίσει την «νέα» ετικέτα. Ωστόσο, κατά τη στιγμή της μεταβίβασης της ιδιοκτησίας της ετικέτας, τόσο οι παλιοί όσο και οι νέοι ιδιοκτήτες έχουν τις απαραίτητες πληροφορίες για την επικύρωση της ετικέτας, γεγονός το οποίο μπορεί να προκαλέσει παραβίαση της ιδιωτικότητας της ιδιοκτησίας της ετικέτας.

Συγκεκριμένα, αν ο προηγούμενος ιδιοκτήτης θελήσει, μπορεί να διαβάσει την ετικέτα, χρησιμοποιώντας τις πληροφορίες που μπορεί να κράτησε πριν ή κατά τη μεταβίβαση της ιδιοκτησίας και να παρακολουθεί τις αλληλεπιδράσεις του νέου ιδιοκτήτη με την ετικέτα. Το ίδιο μπορεί να συμβεί και με τον νέο ιδιοκτήτη που μπορεί να παρατηρήσει την παλαιότερη επικοινωνία της ετικέτας.

Το πρωτόκολλο του Song λοιπόν εξαλείφει το παραπάνω πρόβλημα ιδιωτικότητας και εξασφαλίζει ασφάλεια τόσο στον νέο ιδιοκτήτη, όσο και στον προηγούμενο ιδιοκτήτη, αλλά δίνει και το δικαίωμα ανάκτησης ιδιοκτησίας της ετικέτας, αν αυτό κάποια στιγμή χρειαστεί.

6.3 Πρωτόκολλο ψευδωνυμίας Song & Mitchell

Εκτός από το πρωτόκολλο αυθεντικοποίησης ο B. Song και ο C. J. Mitchell πρότειναν και ένα πρωτόκολλο ψευδωνυμίας [46], που και αυτό βασίζεται στο πρωτόκολλο αυθεντικοποίησης Song & Mitchell.

Η ψευδωνυμία χρησιμοποιείται για να παρέχει ανωνυμία στις ετικέτες. Κάθε φορά που μια ετικέτα ερωτάται, απαντά με ένα διαφορετικό κρυπτογραφικά προερχόμενο ψευδώνυμο. Σε ορισμένα από τα πρωτόκολλα η ψευδωνυμία βασίζεται σε μια γραμμική αναζήτηση της βάσης δεδομένων του back-end συστήματος για να εντοπίσει μια ετικέτα.

Δηλαδή, σε κάθε καταχώρηση ετικέτας στη βάση δεδομένων, υπολογίζεται και παράγεται το ψευδώνυμο που ανήκει στη ετικέτα και συγκρίνεται με το λαμβανόμενο ψευδώνυμο. Η γραμμική αναζήτηση τρέχει σε χρόνο O(n), όπου n είναι ο αριθμός των στοιχείων στη βάση δεδομένων. Μια τέτοια λοιπόν δαπανηρή λειτουργία αναζήτησης θα προκαλέσει δυνητικά θέματα επεκτασιμότητας, καθώς ο πληθυσμός των ετικετών αυξάνεται.

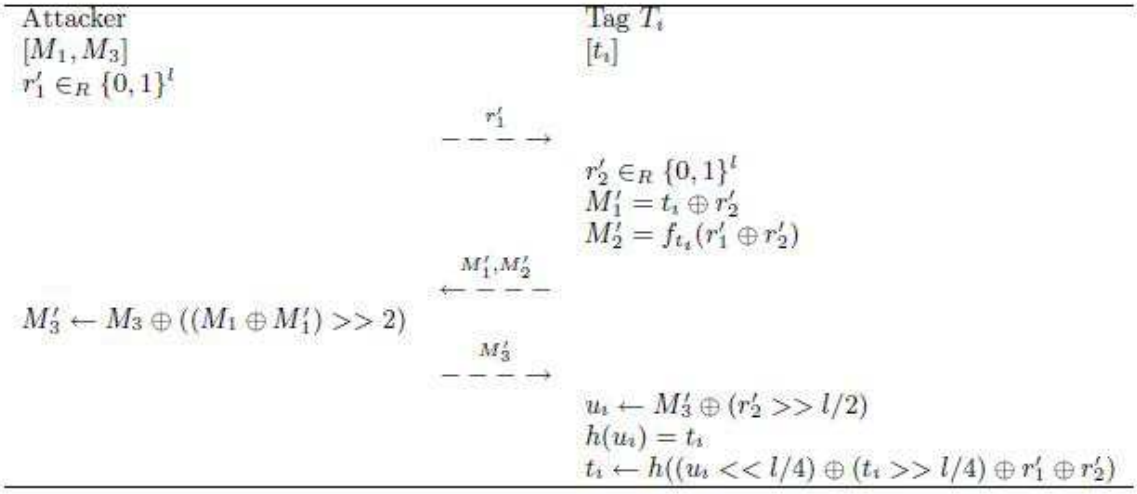
Το πρωτόκολλο ψευδωνυμίας Song & Mitchell παρέχει την επεκτασιμότητα που χρειάζεται, δηλαδή ο χρόνος για τον εντοπισμό μιας ετικέτας στη βάση δεδομένων είναι σταθερός. Παράλληλα υπάρχει ασφάλεια σε θέματα ιδιωτικότητας και οι απαιτήσεις επεξεργασίας και αποθήκευσης στην ετικέτα είναι μικρές, όπως και στο πρωτόκολλο αυθεντικοποίησης.

6.4 Ανάλυση Ασφαλείας του πρωτόκολλου αυθεντικοποίησης Song & Mitchell

Το 2009 οι Π. Ριζομυλιώτης, Ε. Ρεκλείτης και Σ. Γκρίτζαλης [43] εκμεταλλεύθηκαν κάποιες ατέλειες στο σχεδιασμό των μηνυμάτων του πρωτοκόλλου αυθεντικοποίησης για RFID δίκτυα των B. Song και C. J. Mitchell και παρουσίασαν μια επίθεση πλαστοπροσωπίας σε αυτό το πρωτόκολλο που αποσυγχρονίζει την ετικέτα με τον διακομιστή, προκαλώντας σύμφωνα με τους συγγραφείς άρνησης εξυπηρέτησης (denial of service (DoS)).

Συγκεκριμένα όταν το πρωτόκολλο αυθεντικοποίησης Song & Mitchell φτάσει στο 5ο βήμα (δηλαδή στην αποστολή το M3), ο επιτιθέμενος υποκλέπτει το M3 και εμποδίζει να αποσταλεί στην ετικέτα. Έπειτα ο επιτιθέμενος παράγει μια συμβολοσειρά r1' (ίδιου μεγέθους με το r1 του αναγνώστη στο πρωτόκολλο) και την αποστέλλει στην ετικέτα Ti. Η ετικέτα Ti παράγει μια τυχαία συμβολοσειρά r2' και υπολογίζει τα M1'=ti $\oplus$ r2' και M2' = fti(r1'$\oplus$r2') και τα στέλνει στον επιτιθέμενο. Ο επιτιθέμενος έχοντας υποκλέψει το M1 και M3 υπολογίζει M1$\oplus$M1'=ti$\oplus$r2$\oplus$ti$\oplus$r2'=r2$\oplus$r2' και M3'=M3$\oplus$((M1$\oplus$M1')>>l/2) και αποστέλλει στην ετικέτα Ti το M3'. Η ετικέτα Ti υπολογίζει το ui=M3'$\oplus$(r2'>>l/2) και κάνει έλεγχο αν h(u_i)=ti. Αν ο έλεγχος είναι επιτυχής τότε υπολογίζει και καταχωρεί

t_i=h((u_i<<l/4) ⊕(t_i>>l/4)⊕r1'⊕r2' με αποτέλεσμα να αποσυντονίζεται πλήρως από τον διακομιστή, αφού τα δεδομένα της είναι διαφορετικά από αυτά του διακομιστή.



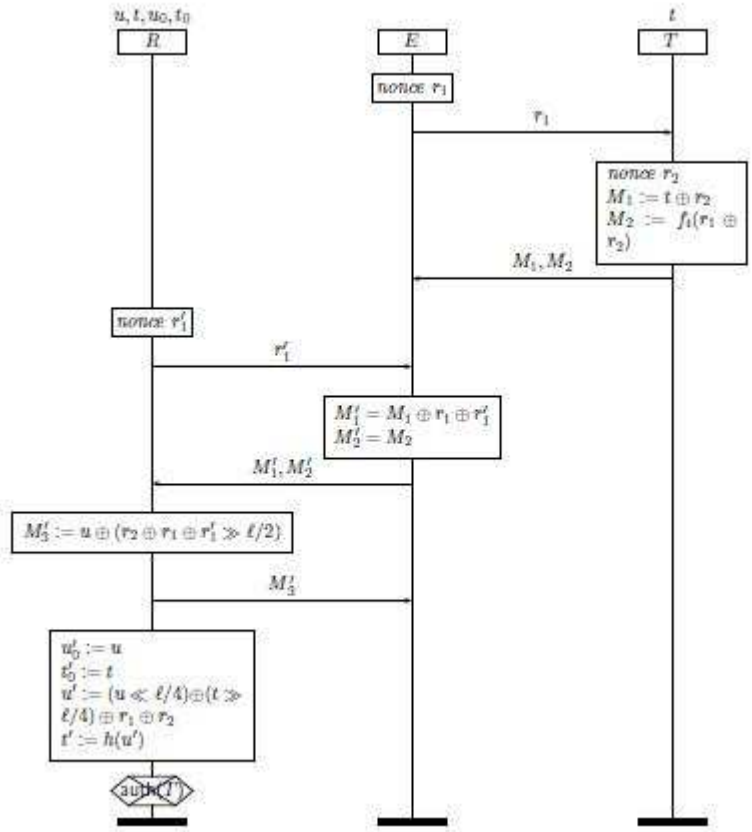
Εικόνα 6.2: Επίθεση πλαστοπροσωπίας στο πρωτόκολλο αυθεντικοποίησης Song & Mitchell [43]

Για αυτό οι συγγραφείς πρότειναν ο υπολογισμός του M3 από τον διακομιστή να υπολογίζεται ως εξής : M3=f_{r2}(u_i) και η ετικέτα Ti να συγκρίνει με f_{r2}(h(t_i). Επομένως αν αυτά είναι ίσα, τότε υπάρχει αυθεντικοποίηση.

Η παραπάνω πρόταση απαιτεί μια παραπάνω χρήση της ειδικά διαμορφωμένης συνάρτησης κατακερματισμού (f_x()) από τον διακομιστή και την ετικέτα, χωρίς όμως να χρειάζεται κάτι επιπλέον από τα συστήματα (διακομιστή- ετικέτας), σε σχέση με αυτή που προτείνει το πρωτόκολλο Song & Mitchell.

Ο Ton van Deursen και ο Sasa Radomirovi [50] παρουσίασαν και αυτοί μια επίθεση στο συγκεκριμένο πρωτόκολλο αυθεντικοποίησης. Συγκεκριμένα ο επιτιθέμενος εκμεταλλεύεται μια πρότερη επικοινωνία του με την ετικέτα T. Στην επικοινωνία του αναγνώστη με την ετικέτα, ο επιτιθέμενος υποκλέπτει το στοιχειό r1 που ο αναγνώστης επιχειρεί να στείλει στην ετικέτα (χωρίς επιτυχία), έχοντας στην διάθεση του από την προηγούμενη επικοινωνία με την ετικέτα τα M1 και M2 τα οποία του είχε στείλει η ετικέτα. Στέλνει λοιπόν στον αναγνώστη τα M1' = M1⊕ r1⊕r1' και M2'=M2. Ο διακομιστής κάνοντας τους υπολογισμούς που προβλέπει το πρωτόκολλο στέλνει το M3' = u ⊕ (r2 ⊕ r1 ⊕ r1' >> l/2) και καταχωρεί u0'=u, t0'=t, u'= (u<<l/4)⊕(t>>l/4)⊕ r1⊕r2 και t'=h(u'). Η διαδικασία αυθεντικοποίησης όμως δεν υλοποιείται ποτέ, αφού η ετικέτα

δεν λαμβάνει το M3' με προφανές αποτέλεσμα την αδυναμία αυθεντικοποιημένης επικοινωνίας διακομιστή – ετικέτας και εκ νέου απαίτηση αυθεντικοποίησης.

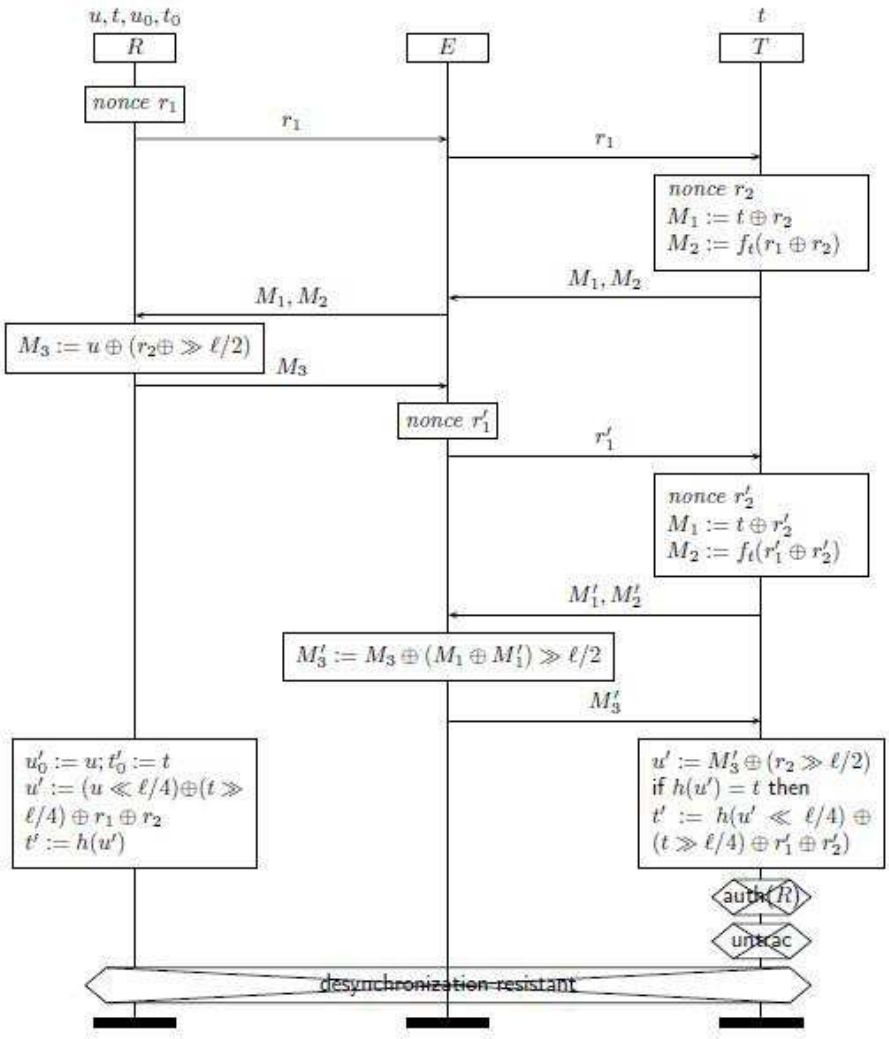


Εικόνα 6.3: Επίθεση την αυθεντικοποίηση της ετικέτας [50]

Επίσης μια άλλη πρόταση των Ton van Deursen και Sasa Radomirovi στο ίδιο άρθρο [50] είναι ο αποσυγχρονισμός, όπου:

Ο αναγνώστης στέλνει το r1 αλλά αυτό υποκλέπτεται από των επιτιθέμενο. Ο επιτιθέμενος προωθεί το r1 στην ετικέτα T, η ετικέτα T αποστέλλει τα M1, M2 αλλά πάλι τα υποκλέπτει ο επιτιθέμενος ο οποίος όμως τα μεταδίδει στον αναγνώστη. Ο διακομιστής δημιουργεί το M3=u⊕ (r2 >> l/2) και το αποστέλλει προς την ετικέτα T. Ο επιτιθέμενος το υποκλέπτει και ταυτόχρονα το εμποδίζει να φτάσει στην ετικέτα T. Ο διακομιστής ακολουθεί την λειτουργία του πρωτόκολλου και αλλάζει τα στοιχεία u0'= u, t0'= t, u'= (u <<l/4)⊕(t>>l/4) ⊕r1⊕r2, t'=h(u'). Ο επιτιθέμενος αποστέλλει ένα νέο r1' στην ετικέτα T και αυτή με την σειρά της αποστέλλει τα M1' και M2' στον επιτιθέμενο. Ο επιτιθέμενος υπολογίζει το M3'=M3⊕(M1⊕M1')>>l/2 και το αποστέλλει στην ετικέτα T για να αυθεντικοποιηθεί. Η ετικέτα ελέγχει το M3 και πιστοποιεί τον

επιτιθέμενο, αλλάζοντας ταυτόχρονα τα στοιχεία της u και t με αποτέλεσμα να αποσυγχρονίζεται από τον διακομιστή.



Εικόνα 6.4: Επίθεση στην αυθεντικοποίηση του αναγνώστη [50]

Τέλος ο Peris-Lopez κ.ά. [37] ολοκληρώνοντας την ανάλυση ασφαλείας του πρωτόκολλου αυθεντικοποίησης Song & Mitchell και του πρωτόκολλου μεταβίβασης ιδιοκτησίας του Song έδειξαν νέα κενά ασφαλείας στα πρωτόκολλα. Απέδειξαν ότι τα πρωτόκολλα αυθεντικοποίησης και ιδιοκτησίας δεν παρέχουν ασφάλεια σε πληροφορίες τοποθεσίας και ιδιωτικότητας. Επιπλέον, απέδειξαν ότι το πρωτόκολλο ενημέρωσης (Secret Update Protocol) που περιλαμβάνεται στο άρθρο του Song για το πρωτόκολλο μεταβίβασης ιδιοκτησίας είναι ευάλωτο σε επιθέσεις αποσυγχρονισμού.

Οπότε είναι προφανές ότι αν και το πρωτόκολλο Song & Mitchell είναι ένα ισχυρό και αποδοτικό πρωτόκολλο αυθεντικοποίησης που θεωρήθηκε ότι επιτυγχάνει μεγάλη ασφάλεια, παρόλα

αυτά εμφανίζει κενά ασφαλείας, τα οποία ένας επιτιθέμενος με καλές γνώσεις μπορεί να εκμεταλλευτεί.

Η αλήθεια είναι ότι το κυριότερο κενό που μπορεί ένας επιτιθέμενος να εκμεταλλευτεί πάντα στην αυθεντικοποίηση, είναι η ασύρματη επικοινωνία που είναι πάντα ευάλωτη σε διακοπές ροής των μηνυμάτων από τον αναγνώστη, στην ετικέτα.

Για αυτό άλλωστε μέχρι τώρα δεν μπορούμε να πούμε ότι υπάρχει ένα πλήρως ασφαλισμένο πρωτόκολλο για RFID δίκτυα που να απευθύνεται σε χαμηλού κόστους ετικέτες και ταυτόχρονα να είναι και αποδοτικό.

6.5 Άλλες κρυπτογραφικές τεχνικές και πρωτόκολλα

Εκτός των παραπάνω πρωτοκόλλων και τεχνικές για RFID συστήματα υπάρχουν και παρά πολλά άλλα πρωτόκολλα και κρυπτογραφικές τεχνικές που εκ των πραγμάτων δεν είναι δυνατόν να αναλυθούν σε αυτή την εργασία, για αυτό και παρακάτω απλά θα παρουσιάσουμε μερικά από αυτά.

6.5.1 Πρωτόκολλο O-FRAP και O-RAP.

Ο M. Burmester, Ο T. van Le, Ο B. De Medeiros και ο G. Tsudik πρότειναν ένα πρωτόκολλο ελέγχου ταυτότητας RFID (O-FRAP) [7] στο οποίο ο διακομιστής αναγνωρίζει και πιστοποιεί τις RFID ετικέτες. Κάθε ετικέτα και ο διακομιστής μοιράζονται ένα κλειδί Ki και ένα ψευδώνυμο ri που ανανεώνονται σε κάθε συνεδρία. Επιπλέον, χρησιμοποιούν μια συνάρτηση F για τον υπολογισμό των μηνυμάτων αυθεντικοποίησης και των νέων μυστικών κλειδιών. Το πρωτόκολλο O-RAP είναι μια απλοποιημένη εκδοχή του πρωτοκόλλου O-FRAP, που ουσιαστικά είναι το O-FRAP, αλλά χωρίς μια βασική διαδικασία ενημέρωσης [7].

Ο K. Ouafi και ο R. Phan παρουσίασαν μια επίθεση ιχνηλάτησης [36] στο O-FRAP προκαλώντας πρόβλημα αποσυγχρονισμού στην ετικέτα. Μια άλλη ανάλυση για O-FRAP και O-RAP έγινε από τον D. Duc και τον K. Kim [15] στην οποία αναφέρθηκαν σε θέματα επεκτασιμότητας των πρωτόκολλων.

6.5.2 Πρωτόκολλο αμοιβαίας αυθεντικοποίησης για συστήματα RFID Cho κ.ά.

Ο Cho κ.ά. πρότειναν ένα πρωτόκολλο αμοιβαίας αυθεντικοποίησης για συστήματα RFID [10]. Το προτεινόμενο πρωτόκολλο χρησιμοποιεί μια συνάρτηση κατακερματισμού που η δομή της παρέχει αρκετή ασφάλεια εναντία σε διάφορες επιθέσεις. Επιπλέον, με τη χρήση της τυχαιότητας σε κάθε συνεδρία αμοιβαίας αυθεντικοποίησης, αυξάνεται η ασφάλεια με την χρησιμοποίηση δύο τυχαίων τιμών Rr και Rt, που παράγονται από τον αναγνώστη και την ετικέτα αντίστοιχα και μίας τιμής που συμβολίζεται με RIdi, η οποία εξαρτάται από Rt. Δεδομένου ότι η μυστική τιμή Sj της ετικέτας ενημερώνεται σε κάθε επιτυχή λειτουργία του πρωτοκόλλου, για να αποφύγει την επίθεση αποσυγχρονισμού η βάση δεδομένων του back-end συστήματος τηρεί τις δύο τελευταίες μυστικές τιμές της ετικέτας, που συμβολίζονται από S-old και S-new αντίστοιχα.

6.5.3 Πρωτόκολλο RFID αμοιβαίας αυθεντικοποίησης με βάση τον αλγόριθμο AES.

Το 2011 ο Tuan Anh Pham, ο Mohammad Hasan S. και ο Hongnian YuIn πρότειναν το πρωτόκολλο αμοιβαίας επαλήθευσης ταυτότητας με βάση το μοντέλο απόκρισης πρόκλησης [38]. Το Πρότυπο Κρυπτογράφησης AES (Advanced Encryption Standard) χρησιμοποιείται για την κρυπτογράφηση, ώστε να είναι ασφαλή τα δεδομένα και είναι ένα πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας που χρησιμοποιεί AES-128 για την κρυπτογράφηση των μηνυμάτων που μεταδίδονται. Το πρωτόκολλο αντιμετωπίζει πολλούς τύπους επιθέσεων όπως διαρροής πληροφοριών, παρακολούθησης ετικέτας κ.λπ.

6.5.4 Πρωτόκολλο αυθεντικοποίησης με βάση το πρότυπο Gen-2 σε σύστημα RFID

Το 2011 ο Liangmin WANG, ο Xiaoluo YI, ο Chao LV, και ο Yuanbo GUOn πρότειναν το πρωτόκολλο που χρησιμοποιεί CRC και PRNG λειτουργίες [51], υποστηρίζοντας το πρότυπο Gen-2, που απαιτεί πολύ μικρή υπολογιστική ισχύ και ελάχιστη επικοινωνία. Χρησιμοποιεί τις ιδέες των λογικών BAN και AVISTA για την ασφάλεια του RFID πρωτοκόλλου. Η λογική BAN δίνει την απόδειξη της ορθότητας του πρωτοκόλλου, και η AVISTA δίνει τις ιδιότητες της αυθεντικοποίησης και του απορρήτου.

6.5.5 Πρωτόκολλο αμοιβαίας αυθεντικοποίησης με βάση την συνάρτηση PUF

Το 2011 ο Ramzi Bassil, ο Wissam El-Beaino, ο Ayman Kayssi και ο Ali Chehab πρότειναν ένα πρωτόκολλο που χρησιμοποιεί μια συνάρτηση που δεν δυνατόν να κλωνοποιηθεί (pufs) για να πετύχει η αμοιβαία αυθεντικοποίηση σε εξαιρετικά «ελαφριές» ετικέτες. Η προτεινόμενη προσέγγιση παρέχει ισχυρές ιδιότητες ασφαλείας, καθώς και καλή απόδοση. Η τεχνική χρησιμοποιεί χαμηλών απαιτήσεων συναρτήσεις και ένα κύκλωμα PUF που απαιτεί ελάχιστη επεξεργαστική ισχύ καθώς και ελάχιστο χώρο αποθήκευσης. [3]

6.5.6 Πρωτόκολλο Δυναμικού Ελέγχου Πρόσβασης και Αξιολόγησης Κινδύνων (DRAAC)

Το 2012 ο Matthew Butler, ο Peter J. Hawrylak και ο John Hale πρότειναν ένα πρωτόκολλο Δυναμικού Ελέγχου Πρόσβασης και Αξιολόγησης Κινδύνων (DRAAC) για την ανίχνευση εισβολών, που μειώνει τα δικαιώματα πρόσβασης στο σύστημα ελέγχου πρόσβασης του RFID συστήματος. Με αυτή τη μέθοδος επιτρέπεται στο διαχειριστή να εξασφαλίσει τις πιο ευαίσθητες περιοχές του συστήματος, ενώ ελαχιστοποιεί την έκταση στην οποία οι χρήστες έχουν πρόσβαση. [8]

6.5.7 Πρωτόκολλο αναγνώρισης κλωνοποιημένης ετικέτας

Το 2012 ο Kai Bu, η Xuan Liu και ο Xiao Bin [6] πρότειναν ένα γρήγορο πρωτόκολλο ταυτοποίησης κλωνοποιημένης ετικέτας, για μεγάλης κλίμακας συστήματα RFID. Το πρωτόκολλο προτείνει μια τεχνική μετάδοσης και σύγκρουσης για τον εντοπισμό κλωνοποιημένων ετικετών. Αυτή η προσέγγιση μειώνει τις προσπάθειες από πολύπλοκες τεχνικές κρυπτογράφησης και μετάδοσης των αναγνωριστικών των ετικετών που καταναλώνουν πολύ χρόνο.

6.5.8 Πρωτόκολλο αμοιβαίας αυθεντικοποίησης σύμφωνα με το πρότυπο ISO 18000-6B

Το 2009 ο YongHao Gu και ο Weiming Wu παρουσίασαν ένα ισχυρό πρωτόκολλο αμοιβαίας αυθεντικοποίησης που ικανοποιεί την απαίτηση του χαμηλού κόστους συστημάτων RFID, συμφώνα με τις απαιτήσεις του πρότυπου ISO 18000-6B. [22]

6.5.9 Ελαφρύ πρωτόκολλο αυθεντικοποίησης

Ο Paolo D'Arco και ο Alfredo De Santis πρότειναν το πρωτόκολλο SASI, που είναι ένα πρωτόκολλο αυθεντικοποίησης RFID, που παρέχει ισχυρή αυθεντικοποίηση και ισχυρή ακεραιότητα (Strong Authentication and Strong Integrity, SASI). Πρόκειται για ένα εξαιρετικά ελαφρύ πρωτόκολλο αυθεντικοποίησης RFID συστημάτων και είναι κατάλληλο για παθητικές ετικέτες και χρησιμοποιεί περιορισμένη υπολογιστική ισχύ, ελάχιστο χώρο αποθήκευσης και περιλαμβάνει απλές δυαδικές λειτουργία, όπως AND, OR, XOR, μοναδιαίες προσθέσεις και λειτουργίες κυκλικής ολίσθησης[12].

6.5.10 Πρωτόκολλο ελέγχου (CHECKER)

Το 2012 η Kaoutar Elkhiyaoui, ο Erik-Oliver Blass και ο Refik Molva εισήγαν ένα νέο πρωτόκολλο ελέγχου (CHECKER) , το οποίο χρησιμοποιείται για την ανίχνευση πλαστών RFID ετικετών στην αλυσίδα εφοδιασμού μέσω επιτόπιου έλεγχου. Με τη βοήθεια αυτού του πρωτοκόλλου οι αναγνώστες RFID ελέγχουν την εγκυρότητα της διαδρομής του προϊόντος και αφού επαληθευθεί η αυθεντικότητα του προϊόντος, το πρωτόκολλο ελέγχου χρησιμοποιεί ένα πολυώνυμο με βάση την κωδικοποίηση, αναπαριστώντας μονοπάτια στην αλυσίδα εφοδιασμού. Κάθε ετικέτα T στο πρωτόκολλο ελέγχου αποθηκεύει το αποτέλεσμα της κρυπτογράφησης IND-CCA της ταυτότητας του αναγνωριστικού (ID) της ετικέτας T και μια υπογραφή του ID, χρησιμοποιώντας πολυωνυμική κωδικοποίηση της διαδρομής της ετικέτας T ως μυστικό κλειδί[16].

Κεφάλαιο 7
Θέματα ιδιωτικότητας των RFID και κοινωνικές προεκτάσεις

Η τεχνολογία RFID όπως είδαμε είναι μια πολύ πρωτοποριακή και χρηστική τεχνολογία που βρίσκει πολλές εφαρμογές σε πάρα πολλές κατηγορίες προϊόντων, αντικειμένων και υπηρεσιών. Παρ' όλα αυτά λόγω της ιδιόμορφης λειτουργίας των RFID συστημάτων (ασύρματη ζεύξη), συνεχώς γίνεται αναφορά σε θέματα ασφάλειας τα οποία και αναλύσαμε σε προηγούμενο κεφάλαιο. Ένα ακόμα πολύ βασικό κομμάτι της ασφάλειας στα RFID δίκτυα είναι η ιδιωτικότητα και η διαχείριση προσωπικών δεδομένων, όπου ο όρος ιδιωτικότητα (privacy) βάσει του ορισμού του Alan F.Westin[53] ορίζεται ως "Η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν για τον εαυτό τους πότε, πώς και σε ποιο ακριβώς βαθμό οι πληροφορίες που τους αφορούν θα γίνονται γνωστές στους υπόλοιπους με τους οποίους επικοινωνούν ".

Όπως αντιλαμβανόμαστε σε ένα μη ασφαλές περιβάλλον, όπως η ασύρματη ζεύξη που τα RFID δίκτυα υλοποιούν, είναι μεγάλος ο κίνδυνος παραβίασης της ιδιωτικότητας.

7.1 Προβλήματα ιδιωτικότητας στα RFID

Κύριο κομμάτι στα προβλήματα ιδιωτικότητας στα RFID συστήματα είναι οι ετικέτες RFID που λόγω του μοναδικού αναγνωριστικού κωδικού (EPC) κάνει εύκολο τον προσδιορισμό τους, αφού οι περισσότερες ετικέτες χαμηλού κόστους ακόμα και τώρα, απαντούν σε αιτήματα με τον μοναδικό αναγνωριστικό κωδικό τους, κάνοντας εύκολο το να εντοπιστούν από τον καθένα. Επίσης οι RFID ετικέτες «φλυαρούν», δηλαδή απαντούν σε όλα τα αιτήματα, χωρίς να κάνουν διακρίσεις και αυτό συμβαίνει λόγω της κατασκευής τους. Επιπλέον ας μην ξεχνάμε ότι βρίσκονται σε ένα μη ασφαλές περιβάλλον, οπότε είναι φανερό ότι υπάρχουν κίνδυνοι για την ιδιωτικότητα που μπορεί να είναι οι εξής:

7.1.1 Διαρροή πληροφοριών

Μια RFID ετικέτα απαντά σε όλα τα ερωτήματα από τους αναγνώστες με το σύνολο των πληροφοριών που βρίσκονται αποθηκευμένα σε αυτή. Οπότε οποιοσδήποτε διαθέτει έναν κατάλληλο RFID αναγνώστη, έχει πρόσβαση στις πληροφορίες της ετικέτας, παραβιάζοντας κάθε έννοια ανωνυμίας και ιδιωτικότητας. Ακόμα όμως και αν η ετικέτα χρησιμοποιεί κάποια προστατευτική τεχνολογία η οποία περιορίζει την πρόσβαση σε μη εξουσιοδοτημένους χρήστες, δεν παύει να υπάρχει θέμα ιδιωτικότητας και αυτό επειδή όποιος έχει πρόσβαση στα δεδομένα της ετικέτας , έχει πρόσβαση στο σύνολο των δεδομένων και όχι σε ένα μέρος αυτών, οδηγώντας πολλές φορές πάλι σε παραβίαση της ιδιωτικότητας επειδή κάποιοι χρειάζονται και πρέπει να έχουν πρόσβαση σε ένα μόνο μέρος των δεδομένων και όχι στο σύνολο. Μια τέτοια επιλογή όμως είναι αρκετά δαπανηρή για να υλοποιηθεί σε μια RFID ετικέτα. Ταυτόχρονα πρέπει να τονιστεί ότι από μόνη της η ηλεκτρονική μορφή των δεδομένων αποτελεί σημαντική απειλή για την ιδιωτικότητα, καθώς διευκολύνει την επεξεργασία των δεδομένων, την εύκολη διάδοση τους και όπως είναι φυσικό και την εύκολη διαρροή τους.

7.1.2 Αδιαφάνεια Επικοινωνίας

Ο κάτοχος μιας RFID ετικέτας έχει πολύ μικρό έλεγχο σε αυτή. Η RFID ετικέτα μπορεί να επικοινωνεί οποτεδήποτε και με οποιονδήποτε χωρίς ο κάτοχος να αντιλαμβάνεται κάτι και χωρίς φυσικά να μπορεί να το ελέγξει, μιας και δεν υπάρχει λίστα επισκέψεων ή κάτι παρόμοιο

για τις RFID ετικέτες, ώστε να γίνεται έλεγχος και να μην δημιουργείται κενό ιδιωτικότητας. Αν και υπάρχουν αρκετές υλοποιήσεις ασφάλειας πάνω σε αυτό το θέμα όπως είδαμε και σε προηγούμενο κεφάλαιο (κλωβός Faraday κλπ.), καμία δεν μπορεί να αντιμετωπίσει το πρόβλημα όταν η ετικέτα πρόκειται να χρησιμοποιηθεί και ουσιαστικά «απενεργοποιείται» η ασφάλεια της, για να είναι ορατή.

7.1.3 Παρακολούθηση δράσης

Μέσω της RFID τεχνολογίας είναι δυνατόν να διαπιστώσουμε τη συμπεριφορά ενός ατόμου από την απλή παρακολούθηση των ενεργειών μιας ομάδας ετικετών. Συγκεκριμένα μπορούμε να υποθέσουμε ή και να εφαρμόσουμε τεχνάσματα για να αποδείξουμε μια κατάσταση που εξαρτάται από την συμπεριφορά μια ετικέτας ή μιας ομάδας ετικετών, για παράδειγμα αν μια ετικέτα βρίσκεται σε κίνηση σε ένα χώρο που δεν πρέπει να κινείται κάνεις, μπορούμε να συμπεράνουμε ότι κάποιος βρίσκεται σε αυτό το χώρο ή ακόμα καλύτερα μπορούμε να ελέγξουμε το χώρο για να εντοπίσουμε το άτομο. Πολλές εφαρμογές έχουν την παραπάνω φιλοσοφία δράσης, με κάποιες από αυτές να παραβιάζουν βασικά δικαιώματα.

7.1.4 Συσχέτιση

Όταν ένας πελάτης αγοράσει ένα προϊόν το οποίο φέρει μια RFID ετικέτα, η ταυτότητα του πελάτη μπορεί να συσχετιστεί με τον Μοναδικό Αναγνωριστικό Κωδικό (EPC) της ετικέτας. Αυτή και μόνο η συσχέτιση RFID ετικέτας και ατόμου πολλές φορές μπορεί να καταπατά την ιδιωτικότητα. Το φαινόμενο αυτό μπορεί να γιγαντωθεί με την χρήση στην συναλλαγή και της πιστωτικής κάρτας οπότε εκεί η συσχέτιση είναι πιο ισχυρή ,καθώς η ταυτότητα του πελάτη γίνεται γνωστή. Όμως υπάρχουν και περιπτώσεις όπου η συσχέτιση γίνεται με λάθος ιδιοκτήτη, όπως στην περίπτωση της αγοράς ενός δώρου, όπου εκεί ο πραγματικός ιδιοκτήτης είναι αυτός που θα λάβει το δώρο και όχι ο αγοραστής, χωρίς βεβαία να μειώνεται η απειλή παραβίασης της ιδιωτικότητας. Βέβαια καλό είναι σε αυτό το σημείο να διευκρινίσουμε ότι η συσχέτιση μιας RFID ετικέτας και ενός πελάτη δεν είναι το ίδιο με τις κάρτες μέλους- προσφοράς που προσφέρουν διάφορες επιχειρήσεις στους πελάτες τους. Εκεί δεν γίνεται άμεση συσχέτιση με το προϊόν αλλά απλή αναφορά της προτίμησης, ενώ σημαντικό είναι ότι υπάρχει η δυνατότητα της μη χρήσης της κάρτας από τον πελάτη.

Τέλος είναι σημαντικό να γνωρίζουμε ότι η χρήση μετρητών στις αγορές, αυξάνει την ανωνυμία αλλά έστω και ανώνυμα η συσχέτιση πελάτη – RFID ετικέτας παραμένει.

7.1.5 Αποκάλυψη προτιμήσεων

Όπως ήδη ξέρουμε μια RFID ετικέτα φέρει πληροφορίες για ένα προϊόν στο οποίο είναι προσαρτημένη. Διαβάζοντας κάποιος αυτές τις πληροφορίες μπορεί να συμπεράνει τις προτιμήσεις του κατόχου – αγοραστή του προϊόντος, καθώς και τυχόν ανάγκες του που μπορεί να εκθέτουν ευαίσθητα προσωπικά δεδομένα (πχ. ιατρικές πληροφορίες από ετικέτες φαρμάκων). Έτσι είναι εύκολα αντιληπτό ότι οι RFID ετικέτες μπορούν να καταδείξουν τις προτιμήσεις μας και δεν μπορούμε να εξακριβώσουμε πότε συμβαίνει αυτό, μιας και η ανάγνωση γίνεται με τρόπο μη αντιληπτό, σε αντίθεση με τις κάρτες μέλους – προσφορών από τις επιχειρήσεις, όπου εκεί είναι επιλογή μας αν θα τις χρησιμοποιήσουμε σε μια αγορά μας. Βασικό βέβαια είναι ότι εκτός από της προτιμήσεις μας, μπορούν να μας θέσουν σε κίνδυνο επειδή ο οποιοσδήποτε μπορεί να γνωρίζει το τι φέρουμε και πόσο πολύτιμο είναι, δημιουργώντας πιθανές απειλές ληστείας.

7.1.6 Αστερισμός Ετικετών

Το σύνολο των RFID ετικετών που διαθέτει ένα άτομο σχηματίζει ένα μοναδικό αστερισμό οπότε ακόμα και αν το άτομο δεν έχει συσχετιστεί με τις ετικέτες, η μοναδικότητα αυτή μπορεί να χρησιμοποιηθεί για να παρακολουθήσουμε και να καταγράψουμε τις κινήσεις αυτού του ατόμου. Βέβαια αν στο άτομο υπάρχει μια συσχέτιση με μια RFID ετικέτα, είναι αρκετή χάρη στον αστερισμό, ώστε να συσχετιστούν και οι άλλες με το ίδιο πρόσωπο. Επίσης μπορεί να υπάρξει περίπτωση κατηγοριοποίησης του ατόμου με βάση το σύνολο ή μέρος των RFID ετικετών του, δείχνοντας μας ότι δεν είναι απαραίτητη η γνώση της ταυτότητας του ατόμου για να το καταδείξουμε.

7.1.7 Αποκάλυψη συναλλαγών

Όταν ένα αντικείμενο που φέρει μια RFID ετικέτα αλλάξει ομάδα – αστερισμό ετικετών, μπορούμε να συμπεράνουμε ότι μια συναλλαγή μεταξύ των ατόμων που συσχετίζονται με τους αστερισμούς RFID ετικετών συνέβη. Η μεγάλη διαφάνεια στις συναλλαγές από πολλούς μπορεί

να θεωρηθεί ωφέλιμο στο να ασκείται καλύτερος έλεγχος στις συναλλαγές, παρόλα αυτά όμως δεν παύει να παραβιάζει την ιδιωτικότητα.

7.1.8 Απαρχαιώμενα στοιχεία

Αν μια συσχέτιση ενός ατόμου με μια RFID ετικέτα αποθηκευτεί σε μια βάση δεδομένων και δεν ενημερωθεί ξανά όταν το άτομο αποκοπεί από την RFID ετικέτα, η συσχέτιση με αυτή την ετικέτα θα συνεχίσει να υφίσταται στο σύστημα, με πιθανή συνέπεια να εξαρθούν πολλές λανθασμένες εκτιμήσεις ή και συμπεράσματα για αυτό το άτομο, με φυσιολογικό αποτέλεσμα πολλές φορές να χρεωθεί κινήσεις ή ακόμα και πράξεις που δεν του ανήκουν. Βέβαια το γεγονός και μόνο ότι μια συσχέτιση του παρελθόντος συνεχίζει να υφίσταται παρά τη θέληση μας, αποτελεί κατάφορη παραβίαση ιδιωτικότητας.

Τέλος καλό είναι να γίνεται αναφορά και στο υπόλοιπο κομμάτι του RFID συστήματος (πλην των RFID ετικετών) για προβλήματα ιδιωτικότητας. Βέβαια ανάλογα με την υλοποίηση του κάθε συστήματος υπάρχουν και οι ανάλογες απαιτήσεις, που όπως θα δούμε και παρακάτω το νομικό πλαίσιο για την προστασία της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες κάνει ειδική αναφορά στην RFID τεχνολογία και προνοεί για όλα.

7.2 Νομικό πλαίσιο για προστασία της ιδιωτικότητας στα RFID

Στην Κύπρο, στην Ελλάδα αλλά και στις υπόλοιπες χώρες που ανήκουν στην Ευρωπαϊκή Ένωση το Νομικό πλαίσιο για την προστασία τις ιδιωτικότητας και των δεδομένων για τις RFID εφαρμογές ορίζεται από την ευρωπαϊκή οδηγία 95/46/ΕΚ [55] για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών που ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο τον Οκτωβρίου του 1995, όπως αυτή έχει τροποποιηθεί (τελευταία τροποποίηση έγινε από την Οδηγία 2009/136/ΕΚ [54]). Η έκδοση της οδηγίας 2009/136/ΕΚ [54] πραγματοποιήθηκε λαμβάνοντας υπόψη την σύσταση της Ευρωπαϊκής Επιτροπής για την εφαρμογή αρχών προστασίας της ιδιωτικότητας και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνοτική αναγνώριση (RFID) [11] που εκδόθηκε στις 12 Μαΐου 2009 και περιέχει μια ισχυρή καινοτομία: απαιτεί από τους φορείς εκμετάλλευσης RFID να εκπονούν «αξιολόγηση των

επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων» πριν από την εγκατάσταση μιας εφαρμογής RFID και να διαθέτουν τα αποτελέσματά της στην αρμόδια αρχή, παρέχοντας έτσι την δυνατότητα αυτορρύθμισης στο κλάδο.

Σκοπός της σύστασης της Ευρωπαϊκής Επιτροπής στις εφαρμογές RFID[11] ήταν επίσης να προωθήσει «πληροφόρηση και διαφάνεια σχετικά με τη χρήση RFID», ιδίως μέσω της ανάπτυξης «μιας κοινής ευρωπαϊκής σήμανσης, που αναπτύσσεται από Ευρωπαϊκούς Οργανισμούς Τυποποίησης, με την υποστήριξη των ενδιαφερόμενων φορέων», με στόχο «την ενημέρωση των φυσικών προσώπων σχετικά με την παρουσία συσκευών αναγνώρισης».

Με όλα τα παραπάνω να μας οδηγούν το 2011 στο πλαίσιο εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων (Privacy Impact Assessment - PIA) [39], το πρώτο τέτοιο πλαίσιο στην Ευρώπη. Το πλαίσιο εισήχθη στην βιομηχανία τον Ιανουάριο του 2011, εγκρίθηκε από την ομάδα εργασίας του άρθρου 29[1] για την προστασία των δεδομένων τον Φεβρουάριο του 2011 και υπογράφηκε στις 6 Απριλίου 2011 από τους βασικούς ενδιαφερόμενους και την Neelie Kroes Αντιπρόεδρο της Ευρωπαϊκής Επιτροπής για την Ψηφιακή Ατζέντα.

Η διαδικασία της εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων, βασίζεται σε μια προσέγγιση διαχείρισης της ιδιωτικότητας και των δεδομένων και προστασίας από κινδύνους με έμφαση κυρίως στην εφαρμογή της σύστασης για RFID[11] της Ευρωπαϊκής Ένωσης. Η διαδικασία έχει σχεδιαστεί για να βοηθήσει τους φορείς εκμετάλλευσης RFID εφαρμογών στην αποκάλυψη των κινδύνων ιδιωτικότητας που συνδέονται με μια RFID εφαρμογή, στην αξιολόγηση τους και στην τεκμηρίωση των μέτρων που λαμβάνονται για την αντιμετώπιση των εν λόγω κινδύνων. Οι επιπτώσεις (αν υπάρχουν) μπορούν να ποικίλουν σημαντικά, ανάλογα με την παρουσία και τον βαθμό της επεξεργασίας προσωπικών δεδομένων από την RFID εφαρμογή.

Το πλαίσιο εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων [39], παρέχει καθοδήγηση στους διαχειριστές των εφαρμογών RFID για τις μεθόδους αξιολόγησης των κινδύνων, συμπεριλαμβανομένων των κατάλληλων μέτρων για την άμβλυνση κάθε πιθανής επίπτωσης στην ιδιωτικότητα ή την προστασία δεδομένων με ένα αποδοτικό, αποτελεσματικό και αναλογικό τρόπο.

[1] Η Ομάδα Εργασίας του Άρθρου 20 προβλέπεται από το άρθρο 29 της Οδηγίας 95/46/ΕΚ και αποτελείται από εκπροσώπους των αρχών Προστασίας Προσωπικών Δεδομένων της Ε.Ε.

Όπως είναι φυσικό το πλαίσιο εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων [39] είναι αρκετά γενικό, ώστε να εφαρμόζεται σε όλες τις RFID εφαρμογές, επιτρέποντας ταυτόχρονα τις ιδιαιτερότητες και τις ιδιομορφίες που μπορεί να αντιμετωπιστούν σε μια εφαρμογή.

Σήμερα το πλαίσιο εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων [39] έχει επεκταθεί και σε άλλους τομείς που σχετίζονται με την ιδιωτικότητα, όπως η πιστοποίηση των συστημάτων ευφυούς μέτρησης (smart metering systems). Πρέπει να σημειωθεί ότι όλα αυτά θα είναι πλέον υποχρεωτικά βάσει των νέων κανόνων προστασίας δεδομένων της Ευρωπαϊκής Ένωσης που πρόκειται άμεσα να θεσπιστούν.

Τέλος μόλις στις 30 Ιουλίου 2014 ανακοινώθηκε το νέο λογότυπο για RFID [13] στην Ευρωπαϊκή Ένωση, με στόχο την ενημέρωση των φυσικών προσώπων σχετικά με την παρουσία συσκευών αναγνώρισης RFID και την κατάδειξη ότι η συσκευή είναι σύννομη με τις απαιτήσεις της Ευρωπαϊκής Ένωσης που αναφέρεται στο πλαίσιο αξιολόγησης των επιπτώσεων, στην προστασία της ιδιωτικότητας και των δεδομένων (PIA).

Εικόνα 7.1: Νέο λογότυπο για RFID στην Ευρωπαϊκή Ένωση [13]

7.3 Κοινωνικές προεκτάσεις και κουλτούρα για την RFID τεχνολογία

Η RFID τεχνολογία είναι μια αμφιλεγόμενη τεχνολογία για την κοινωνία. Αν και οι εφαρμογές που υπάρχουν είναι πολλές και οι περισσότερες κατά γενική ομολογία είναι χρηστικές στο

κοινωνικό σύνολο, υπάρχουν όμως και εφαρμογές που ξεσηκώνουν κοινωνικές ομάδες και δημιουργούν αντιδράσεις.

Κατά κύριο λόγο θα λέγαμε βλέποντας τα προβλήματα ιδιωτικότητας στις RFID εφαρμογές που περιγράφηκαν ανωτέρω, ότι οι εφαρμογές που η χρήση τους καταπατά την ιδιωτικότητα, κάλλιστα – και δικαιολογημένα- θα μπορούσαν να δημιουργήσουν αντιδράσεις και αρνητικά σχόλια. Επίσης λόγω και της κουλτούρας, κατά πολλούς τα RFID συστήματα δεν θα έπρεπε να υλοποιούνται σε καμία εφαρμογή, θεωρία όμως που θεωρείται υπερβολική και μάλλον στερείται επιχειρημάτων.

Πρέπει να παραδεχτούμε ότι η RFID τεχνολογία προσφέρει αρκετές χρήσιμες εφαρμογές που βοηθούν στην βελτίωση του κοινωνικού συνόλου. Αν δούμε την χρήση της RFID τεχνολογίας στις Η.Π.Α. και σε άλλες χώρες που έχουν υιοθετήσει πρώτες την τεχνολογία αυτή, βλέπουμε ότι η προσφορά των RFID συστημάτων στην κοινωνία είναι αρκετά μεγάλη, βελτιώνοντας πολλά κομμάτια της καθημερινότητας, δίνοντας την δυνατότητα να έχουν υπηρεσίες που μέχρι τώρα θεωρούνταν εξωπραγματικές.

Ιδιαίτερα χάρη στην χρήση του IoT (Internet of Things) οι εφαρμογές έχουν βελτιώσει το επίπεδο διαβίωσής μας, μιας και πραγματικά οι υπηρεσίες είναι παρά πολύ χρήσιμες με σημαντικότερο στοιχείο ότι όλα αυτά μπορούν να είναι προσιτά σε ένα μέσο πολίτη μιας χώρας, χωρίς να χρειάζεται να έχει υπερβολικούς οικονομικούς πόρους προκειμένου να τα αποκτήσει. Το κόστος των περισσοτέρων RFID εφαρμογών είναι μικρό και όπως καλά αντιλαμβανόμαστε τα οφέλη είναι μεγάλα, αρκεί βέβαια να δούμε κάποια από τις εφαρμογές που παρουσιάσαμε σε προηγούμενο κεφάλαιο, για να το αντιληφτούμε.

Οι αμφιλεγόμενες βέβαια εφαρμογές από την κοινωνία πρέπει αναμφίβολα να προσεχθούν πχ. οι RFID εφαρμογές ηλεκτρονικού διαβατηρίου σε όλες τις χώρες που έχουν εφαρμοστεί, έχουν ξεσηκώσει κοινωνικές αντιδράσεις με ακρογωνιαίους λίθους των αντιδράσεων, επιστήμονες των RFID εφαρμογών. Ίσως βέβαια να είναι δικαιολογημένη μια τέτοια αντίδραση μιας και καμία RFID εφαρμογή ηλεκτρονικού διαβατηρίου μέχρι τώρα δεν έχει δείξει την ικανότητα να παρέχει πλήρη ασφάλεια της ιδιωτικότητας και διαφύλαξη των προσωπικών δεδομένων. Όμως με το νέο νομικό πλαίσιο στην Ευρωπαϊκή Ένωση για τις RFID εφαρμογές, ίσως οι εφαρμογές ηλεκτρονικού διαβατηρίου να βελτιώσουν την αποτελεσματικότητα τους, αφού καθημερινά παρουσιάζονται επιθέσεις κατά της ιδιωτικότητας σε εφαρμογές RFID ηλεκτρονικού διαβατηρίου.

Εκεί που διαπιστώνεται όμως το πρόβλημα και υπάρχουν και οι μεγαλύτερες αντιδράσεις είναι σε εφαρμογές εμφύτευσης RFID στον άνθρωπο, αν και ακόμα και οι σχεδιαστές RFID εφαρμογών ισχυρίζονται ότι οι μόνες εφαρμογές RFID που δεν πρέπει να υλοποιούνται είναι οι εμφυτεύσεις RFID ετικετών σε ανθρώπους. Το φαινόμενο εμφυτεύσεων RFID ετικετών σε ανθρώπους έχει πάρει διαστάσεις στις Η.Π.Α. Ένας στους τρεις φέρει εμφύτευμα RFID με τις προβλέψεις να κάνουν λόγο πως μέχρι το 2017, κάθε αμερικανός θα έχει αγοράσει ένα εμφύτευμα RFID.

Για τους ειδικούς στα RFID συστήματα το πρόβλημα στα RFID εμφυτεύματα δεν είναι το γεγονός, όπως πολλοί ισχυρίζονται ότι προκαλούν προβλήματα στην ανθρώπινη υγεία, αλλά στο αν αυτά είναι σύννομα με τις διατάξεις για την προστασία της ιδιωτικότητας, πολύ δε μάλιστα αν έχει γίνει δοκιμή αντοχής τους σε επιθέσεις και φυσικά αν έχουν την έγκριση από κάποια αρμόδια αρχή.

Στην Ελλάδα οι RFID εφαρμογές είναι λιγότερες (σε σχέση πάντα με τον υπόλοιπο κόσμο) αλλά οι κοινωνικές αντιδράσεις περισσότερες. Αν και καμία αμφιλεγόμενη RDID εφαρμογή δεν έχει εφαρμοστεί στην χώρα μας, πολλοί είναι αυτοί που καταδικάζουν την RFID τεχνολογία και είναι φανατικά αντίθετη στην χρήση της, έστω και σε απλές εφαρμογές. Το πρόβλημα μάλλον είναι η κουλτούρα μας και οι λίγο συντηρητικές απόψεις μας, σε σχέση με την υπόλοιπη Ευρώπη. Χαρακτηριστικό παράδειγμα της διαφοράς φιλοσοφίας με τους άλλους ευρωπαίους είναι ότι η Καθολική Εκκλησία μέσω του πάπα Φραγκίσκου θεωρεί τα RFID συστήματα ευλογία, ενώ η Ελληνική Ορθόδοξη Εκκλησία θα λέγαμε ότι είναι πιο συγκρατημένη έως και αρνητική, στην χρήση RFID εφαρμογών.

Ας ελπίσουμε ότι με το νέο νομικό πλαίσιο για την προστασία της ιδιωτικότητας και των δεδομένων στις RFID εφαρμογές, με το ειδικό λογότυπο, την υποχρέωση εκπόνησης μελέτης επιπτώσεων στην ιδιωτικότητα η οποία θα οδηγεί στην υλοποίηση κάθε φόρα της πλέον φιλικής προς την ιδιωτικότητα υλοποίησης, καθώς και με ενημέρωση για τα RFID, να μας κάνουν να άρουμε τις όποιες αμφιβολίες για τουλάχιστον κάποιες από τις RFID εφαρμογές.

Κεφάλαιο 8
Επίλογος

Στην παρούσα διατριβή έγινε μια γενική επισκόπηση των δικτύων RFID, κυρίως ως προς την πλευρά της ασφάλειας, αλλά και της ιδιωτικότητας. Παρουσιάσαμε απειλές και ευπάθειες στα RFID, καθώς και τρόπους αντιμετώπισης των απειλών.

Παράλληλα ασχοληθήκαμε και με τις διάφορες κρυπτογραφικές τεχνικές και τα πρωτόκολλα αυθεντικοποίησης στα RFID, αναλύοντας την λειτουργία και τις δυνατότητες τους και παρουσιάζοντας ταυτόχρονα και τις αδυναμίες τους βάση γνωστών επιθέσεων που έχουν καταγραφεί στην βιβλιογραφία.

Επιπλέον παρουσιάσαμε προβλήματα ιδιωτικότητας που μπορεί να προκύψουν από την χρήση RFID εφαρμογών, όπως και το νομικό πλαίσιο που ισχύει στην Ευρωπαϊκή Ένωση για την προστασία της ιδιωτικότητας και των δεδομένων για τις RFID εφαρμογές, αλλά και το πλαίσιο εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων που ουσιαστικά είναι και το εργαλείο για την σχεδίαση και κατασκευή εφαρμογών με γνώμονα την προστασία της ιδιωτικότητας. Επίσης καταγράψαμε διάφορες κοινωνικές αντιδράσεις που εκδηλώνονται, λόγω της χρήσης αμφιλεγόμενων RFID εφαρμογών σε διάφορα κομμάτια της κοινωνίας.

Από όλα τα παραπάνω κατανοούμε ότι η τεχνολογία RFID που είναι αναμφισβήτητα μια πρωτοποριακή τεχνολογία, χρειάζεται ακόμα να διορθώσει αρκετές αδυναμίες της. Βεβαίως η συνεχής έρευνα που γίνεται σίγουρα αναμένεται να εξαλείψει κάποια προβλήματα.

Αν και εμείς βέβαια δούμε τα RFID σαν κάτι καλό για την ανθρωπότητα, πάντα φυσικά με σταθερά και προσεκτικά βήματα και λογικευμένη χρήση σίγουρα θα έχουμε και τα ανάλογα αποτελέσματα. Να μην ξεχνάμε όμως ότι υπάρχουν και εναλλακτικές επιλογές πλην των RFID εφαρμογών, που μπορούν να μας δώσουν λύση σε κάποιες περιπτώσεις.

Βασικές προϋποθέσεις βέβαια για να δούμε την RFID τεχνολογία να κάνει σταθερά βήματα προς το μέλλον, είναι η τήρηση του πλαισίου της Ευρωπαϊκής Ένωσης για εκπόνησης αξιολόγησης των επιπτώσεων στην προστασία της ιδιωτικότητας και των δεδομένων, καθώς και η συνέχιση της χρηματοδότησης ερευνών για νέες κρυπτογραφικές λύσεις στα RFID. Ίσως όμως πρέπει να αναρωτηθούμε αν η χρήση ετικετών RFID υψηλότερων δυνατοτήτων και ίσως λίγο μεγαλύτερου κόστους θα λύσει το πρόβλημα για τις εφαρμογές RFID που περιέχουν προσωπικά δεδομένα.

Τέλος σε μελλοντική εργασία μπορούν να παρουσιαστούν ή και να προταθούν άλλες κρυπτογραφικές τεχνικές και πρωτόκολλα που στόχος τους είναι να διασφαλίσουν την ιδιωτικότητα και τα προσωπικά δεδομένα σε εφαρμογές RFID, καθώς και να αναλυθεί ο τρόπος λειτουργίας και η αποδοτικότητά τους.

Βιβλιογραφία

[01] Avoine, G., Oechslin, P.: RFID Traceability: A Multilayer Problem. In: Patrick, A., Yung,M. (eds.). In: Proc. of the Ninth Int'l Conf. on Financial Cryptography and Data Security (FC'05), Lecture Notes in Computer Science, Vol. 3570,125–140, 2005.

[02] Ayoade, J., Saxby, S.: Roadmap for Solving Security and Privacy Concerns in RFID Systems. In: Computer Law and Security Report, 2007.

[03] Bassil Ramzi, El-Beaino Wissam, Kayssi Ayman, Chehab Ali, "A PUF-Based Ultra-Lightweight Mutual-Authentication RFID Protocol" , 2011 Internet Technology and Secured Transactions (ICITST), International Conference for Computing & Processing (Hardware/Software), pp. 495 – 499, Dec. 2011.

[04] BBC Reports, ePassports 'at risk' from cloning, 2006. http://news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm

[05] Bolotnyy, L., Robins, G.: Physically Unclonable Function-Based Security and Privacy in RFID Systems. In: Proc. of PerCom'07. New York, USA, 211–220, 2007.

[06] Bu Kai , Liu Xuan , Xiao Bin "Fast Cloned-Tag Identifica-tion Protocols for Large-Scale RFID Systems", 2012 IEEE 20th International Workshop on Quality of Service (IWQoS), pp. 1 – 4, June 2012.

[07] Burmester, M., Van Le, T., De Medeiros, B., Tsudik, G.: Universally composable RFID identification and authentication protocols. ACM Transactions on Information and Systems Security 12(4), Article 21, 2009.

[08] Butler Matthew , Hawrylak Peter J. and Hale John, "Grace-ful Privilege Reduction in RFID Security", 2011 CSIIRW Pro-ceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 47, pp. 47+12, Oct 2012.

[09] Center, A.I.: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. In: Draft,http://www.gs1.org/docs/epcglobal/standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf, 2003.

[10] Cho, J.-S., Yeo, S.-S., Kim, S.K.: Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer Communications 34(3), 391–397, 2011.

[11] Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio- frequency identification, Brussels, 12 May 2009

[12] D'Arco Paolo, De Santis Alfredo, "On Ultralight-weight RFID Authentication Protocols" 2011 IEEE Transac-tions on Dependable and Secure Computing, volume. 8, Issue. 4, pp. 548 – 563, Aug. 2011.

[13] Digital privacy: EU-wide logo and "data protection impact assessments" aim to boost the use of RFID systems, Brussels, 30 July 2014

[14] Dimitriou, T.: A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks. In: Proc. of IEEE Conf. on Security and Privacy for Emerging Areas in Communication Networks, 2005.

[15] Duc, D.N., Kim, K.: Defending RFID authentication protocols against DoS attacks.Computer Communications 34(3), 384–390, 2011.

[16] Elkhiyaoui Kaoutar, Blass Erik-Oliver, Molva Refik, "CHECKER: On-site Checking in RFID-based Supply Chains", Proceedings of the fifth ACM conference on Security and Pri-vacy in Wireless and Mobile Networks (WISEC '12), pp: 173-184, 2012.

[17] EPCGlobal: Class-1 generation-2 UHF RFID Protocol for Communications at 860MHz-960 Mhz. In: EPC Radio-Frequency Identity Protocols, Vol. 1.1.0, 2005.

[18] Fedhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems Using the AES Algorithm. In: Proc. of Cryptographic Hardware and Embedded Systems (CHES'04), Vol. 3156. Lecture Notes in Computer Science, 357–370, 2004.

[19] Fishkin, K., Roy, S., Jiang, B.: SomeMethods for Privacy in RFID Communication. In: Proc. of the 1st European Workshop on Security, 42–53, 2004.

[20] Friedl, S.: SQL Injection attacks by example, 2007

[21] Garfinkel, S., Juels, A., Pappu, R.: RFID Privacy: An Overview of Problems and Proposed Solutions. In: IEEE Security & Privacy, Vol. 3. 34–43, 2005.

[22] Gu Yonghao , Wu Weiming "A Light-Weight Mutual Au-thentication Protocol For ISO 18000-6B Standard RFID Sys-tem" 2009 IEEE International Conference on Communications Technology and Applications (ICCTA '09), pp. 21 – 25 , Oct. 2009.

[23] Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: Proc. of the 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks, 2005

[24] ICAO, ICAO Document 9303, 2006.

[25] Juels, A., Rivest, R.,Szydlo,M., The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: Proc. of the 10th ACM Conf. on Computer and Communication Security, 2003.

[26] Juels, A.: Minimalist Cryptography for Low-cost RFID Tags. In: Proc. of the 4th Conf. on Security in Communication Networks (SCN'04), Vol. 3352.Lecture Notes in Computer Science. Springer-Verlag, 2004.

[27] Juels, A.: Stengthening EPC Tags Against Cloning. In: Proc. of ACMWorkshop onWireless Security (WiSe'05). ACM Press, 2005.

[28] Karygiannis, A., Phillips, T., Tsibertzopoulos, A.: RFID Security: A Taxonomy of Risk. In: Proc. of China'Com '06, 2006 .

[29] Karygiannis, T., Eydt, B., Barber, G., Bunn, L., Phillips, T.: Guidelines for Securing Radio Frequency Identification (RFID) Systems. In: NIST Special Publication 800-98, National Institute of Standards and Tecnology, 2007.

[30] Kfir, Z., Wool, A.: Picking Virtual Pockets Using Relay attacks on Contactless Smartcard. In: Proc. of the 1st Int'l Conf. on Security and Privacy, 2005.

[31] Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., Ohkubo, M.: Low-cost RFID Privacy Protection Scheme. In: IPS Journal, Vol. 45., 2003.

[32] Laurie, A.: Practical Attacks Against RFID. In: Network Security, Vol. 2007, No. 9., 2007.

[33] mCloak: mCloak for RFID tags, 2005.

[34] Mitrokotsa A, Rieback M.R, Tanenbaum AS. Classification of RFID Attacks. In Proceedings of the 2nd International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2008), in conjunction 10th International Conference on Enterprise Information Systems, pages 73-86, Barcelona, Spain, 2008.

[35] Molnar, D. and Wagner, D.: Privacy and Security in Library RFID: Issues, Practices and Architectures. In: Proc. of Conf. on Computer and Communications Security, 2004.

[36] Ouafi, K., Phan, R.C.-W.: Traceable Privacy of Recent Provably-Secure RFID Protocols. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 479–489. Springer, Heidelberg , 2008.

[37] Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: Vulnerability analysis of RFID protocols for tag ownership transfer. Computer Networks 54(9), 1502–1508, 2010.

[38] Pham Anh T., Hasan Mohammad S. and Yu Hongnian , "A RFID mutual authentication protocol based on AES algorithm", 2012 UKACC International Conference on Control,pp. 997 – 1002, Sept. 2012.

[39] Privacy and Data Protection Impact Assessment Framework for RFID Applications, EU, 12 January 2011

[40] Rieback, M.R., Bruno, B., Tanenbaum, A.S. Is Your Cat Infected with a Computer Virus? In: Proc. of the 4th IEEE Int'l Conf. on Pervasive Computing and Communications, 169–179, 2006.

[41] Rieback, M.R., Crispo, B., Tanenbaum, A.S.: RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In: Proc. of ACISP'05, 184–194, 2005.

[42] Riscure.: Privacy Issues with New Digital Passport. , July 2005.

[43] Rizomiliotis, P., Rekleitis, E., Gritzalis, S.: Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tags. IEEE Communications Letters 13(4), 274–276, 2009.

[44] Sarma S., Weis S. , Engels Daniel W. , "RFID systems, security and privacy implications", Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[45] Song, B., Mitchell, C.J.: RFID authentication protocol for low-cost tags. In: Gligor,V.D., Hubaux, J., Poovendran, R. (eds.) ACM Conference on Wireless Network Security WiSec 2008, pp. 140–147. ACM Press, New York , 2008.

[46] Song, B., Mitchell, C.J.: Scalable RFID pseudonym protocol. In: Proceedings of the Third International Conference on Network and System Security NSS 2009, pp. 216–224. IEEE Computer Society, 2009.

[47] Song, B.: RFID tag ownership transfer. In: Proceedings of Workshop on RFID Security (RFIDsec 2008), Budapest, Hungary , 2008.

[48] Tanenbaum, A.: Dutch Public Transit Card Broken. In: http://www.cs.vu.nl/~ast/ov-chip-card/, 2007.

[49] Vadhia D., Gupta R. , IPv6 vs. EPC: a face off on the RFID battleground, February 2004. http://www.worldinternetcenter.com/Pubs/Pubs2004/feb05/IPv6vEPC.pdf.

[50] van Deursen, T., Radomirovic, S.: Attacks on RFID protocols. Cryptology ePrint archive, Report 2008/310, 2008. http://eprint.iacr.org/2008/310.pdf.

[51] Wang Liangmin , YI Xiaoluo , LV Chao, Guo Yuanbo , "Security Improvement in Authentication Protocol for Gen-2 Based RFID System", 2011 Journal of Convergence Information Technology, Volume 6, Number 1, pp. 157 to 169. January 2011.

[52] Weis, S., Sarma, S., Rivest, R., Engels, D.: Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. In: Proc. of 1st Int'l Conf. in Security in Pervasive Computing, Vol. 2802, 201–212, 2003.

[53] Westin A. F. , Privacy and Freedom, New York 1967.

[54] Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, 25 Νοεμβρίου 2009.

[55] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, 24 Οκτωβρίου 1995.

Παράρτημα Α
Ορολογία

Αγγλικός όρος	**Ελληνικός όρος**
Active Jamming	Ενεργητική παρεμβολή
Active tag	Ενεργή ετικέτα
Anti-collision	Αποφυγή σύγκρουσης
Attacks	Επιθέσεις
Backward Traceability	Ιχνηλάτηση προς τα πίσω
Barcodes	Ραβδοειδείς κωδικοί
Brute force	Εξαντλητική αναζήτηση
Denial of Service	Άρνηση παροχής υπηρεσιών
Electronic Product Code	Μοναδικός αναγνωριστικός κωδικός
E-passports	Ηλεκτρονικά διαβατήρια
Firewalls	Τείχη προστασίας

Forward Traceability	Ιχνηλάτηση προς τα εμπρός
Guardian	Φύλακας
ID	Αναγνωριστικό
Internet of Things	Διαδικτύου των Πραγμάτων
KILL	Καταστρέφω
Malicious code injection	Κακόβουλος κώδικας
Man-in-the-middle	Ενδιάμεσος
Microchip	Ολοκληρωμένο κύκλωμα
Middleware	Ενδιάμεσο σύστημα
Passive Interference	Παθητική παρεμβολή
Passive tag	Παθητική ετικέτα
Passwords	Συνθηματικά
Privacy	Ιδιωτικότητα
Radio Frequency Identification	Αναγνώριση Μέσω Ραδιοσυχνοτήτων
Reader	Αναγνώστης
Replay Attack	Επίθεση αναμετάδοσης
Script	Κώδικας
Server Impersonation	Πλαστοπροσωπία διακομιστή
Smart card	Έξυπνη κάρτα
Tag	Ετικέτα
Tag Impersonation	Πλαστογράφηση ετικετών
Timestamps	Χρονικά όρια
Tracking	Παρακολούθηση
Xor	Αποκλειστική διάζευξη