Ασφάλεια Rfid Τεχνολογίας

Μεταπτυχιακός Φοιτητής
Μελετίου Διομήδης

Μεταπτυχιακή Εργασία

Επιβλέπων: Κάτσικας Σωκράτης, Καθηγητής

Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ Διδακτική της Τεχνολογίας και Ψηφιακά Συστήματα
Κατεύθυνση Δικτυοκεντρικών Συστημάτων

Πανεπιστήμιο Πειραιώς

Πειραιάς 2010

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΣΦΑΛΕΙΑ ΤΕΧΝΟΛΟΓΙΑΣ RFID

ΕΙΣΑΓΩΓΗ

Το RFID είναι μια τεχνολογία που συνεχώς εξελίσσεται τραβώντας ολοένα και περισσότερο το ενδιαφέρον της αγοράς. Η βασική της δυνατότητα να ταυτοποιεί μοναδικά αντικείμενα στα οποία εφαρμόζεται χωρίς την ύπαρξη οπτικής επαφής επαυξάνεται σε συνδυασμό με τεχνολογικώς προηγμένα στοιχεία, όπως ολοκληρωμένα κυκλώματα και αισθητήρες. Έτσι καθίσταται ικανή στο να αποθηκεύει, να ανανεώνει και τελικά να παρέχει δεδομένα σχετικά με ανθρώπους, ζώα, αντικείμενα και εμπορεύματα με τρόπο ξεκάθαρο και αυστηρά δομημένο ώστε να επεξεργάζονται περαιτέρω από τα πληροφοριακά συστήματα.

Το όραμα για αποδοτικότερη διαχείριση της εφοδιαστικής αλυσίδας σε παγκόσμιο επίπεδο κινεί την τεχνολογία RFID με ένα μεγάλο αριθμό επενδύσεων σε πιλοτικά προγράμματα. Όμως οι δυνατότητες της δεν αφήνουν αδιάφορους και άλλους τομείς όπως αυτόν της υγείας (π.χ. φορείς βιομετρικών στοιχείων) και της ασφάλειας (π.χ. πιστοποιητικά ταυτοποίησης ατόμων) όπου η τεχνολογία RFID βρίσκει εφαρμογή. Μολαταύτα οι τεχνολογικές, οικονομικές και κοινωνικές αλλαγές που συνοδεύουν την συγκεκριμένη τεχνολογία εγείρουν όχι μόνο ερωτήσεις σχετικά με τις δυνατότητες αλλά και με τους κινδύνους που ελλοχεύουν. Το βασικό θέμα που τίθεται είναι κατά πόσο είναι ασφαλή τα συστήματα αυτά σε θέματα επικοινωνίας και δεδομένων και κατά πόσο θα μπορέσει η κοινωνία να τα αποδεχτεί. Αυτό θα αποτελέσει και το κλειδί της επιτυχίας των συστημάτων RFID.

Ο σκοπός αυτής της διπλωματικής εργασίας είναι να παρουσιάσει τα βασικά χαρακτηριστικά των RFID συστημάτων δίνοντας έμφαση στον τομέα της ασφάλειας.

Στο 1ο κεφάλαιο γίνεται μια γενική περιγραφή των βασικών χαρακτηριστικών της RFID τεχνολογίας και των εφαρμογών στις οποίες χρησιμοποιείται.

Στο 2ο κεφάλαιο γίνεται μια κατηγοριοποίηση των πιο κοινών επιθέσεων στα RFID σε στρώματα (περίπου σαν του ISO), παρουσιάζονται απειλές και πιθανές πολιτικές άμυνας για κάθε στρώμα.

Στο 3ο κεφάλαιο παρατίθεται μια συλλογή επιθέσεων κατά των RFID πρωτοκόλλων που μπορεί να χρησιμεύσει ως μια γρήγορη και εύκολη αναφορά.

Στο 4ο κεφάλαιο παρουσιάστηκαν τρία πρωτόκολλα ως λύσεις σε διαφορετικά ζητήματα πάνω στην ασφάλεια της RFID τεχνολογίας.

ΚΕΦΑΛΑΙΟ 1

ΕΠΙΣΚΟΠΗΣΗ ΤΕΧΝΟΛΟΓΙΑΣ RFID

1.1 Εισαγωγή

Η τεχνολογία RFID (Radio Frequency Identification), είναι η τεχνολογία που χρησιμοποιεί τα ραδιοκύματα (radio waves) με σκοπό αυτόματα να αναγνωρίζει (identify), να εντοπίζει (track), να συλλέγει και να αποθηκεύει πληροφορίες (data capture) έμψυχων και άψυχων αντικειμένων. Οι συχνότητες των ραδιοκυμάτων και τα αντικείμενα στα οποία εφαρμόζεται, η τεχνολογία RFID, ποικίλουν ανάλογα με την εφαρμογή και τους σκοπούς της.

Για παράδειγμαώ, στην εφοδιαστική αλυσίδα (Supply Chain) χρησιμοποιούνται πολύ υψηλές συχνότητες (UHF, Ultra High Frequency), τα αντικείμενα είναι άψυχα και είναι τα μεμονωμένα προϊόντα (π.χ. ένα κουτάκι αναψυκτικού), η συσκευασία κιβωτίου μεμονωμένων προϊόντων (π.χ. κιβώτιο με κουτάκια αναψυκτικών) και η συσκευασία παλέτας κιβωτίων μεμονωμένων προϊόντων (π.χ. παλέτα με πολλά κιβώτια με κουτάκια αναψυκτικών). Ένα άλλο παράδειγμα είναι τα εκτροφεία βοοειδών στα οποία χρησιμοποιούνται χαμηλές συχνότητες (LF, Low Frequency) και τα αντικείμενα είναι έμψυχα (βοοειδή) [Feder 2004].

Η τεχνολογία RFID είναι μέλος της οικογένειας τεχνολογιών Αυτόματης Αναγνώρισης και Συλλογής Δεδομένων (AIDC, Automatic Identification and Data Capture) και αποτελεί την τεχνολογική εξέλιξη των γραμμωτών κωδικών. Οι δυνατότητες που δίνει η τεχνολογία RFID είναι πολύ μεγάλες και αυτό θα προσπαθήσουμε να αναδείξουμε στο κεφάλαιο αυτό παράλληλα με την περιγραφή του τρόπου λειτουργίας της τεχνολογίας RFID και των ιδιαίτερων χαρακτηριστικών της.

1.2 Αρχιτεκτονική

Η τεχνολογία RFID βρίσκεται στα άκρα ενός πληροφοριακού συστήματος. Είναι στην ουσία ένας διαφορετικός τρόπος διασύνδεσης με αντικείμενα που επιθυμούμε να αναγνωρίζουμε, να εντοπίζουμε και να συλλέγουμε πληροφορίες για αυτά. Η διασύνδεση είναι ασύρματη και βασίζεται στα ραδιοκύματα τα οποία μεταδίδονται στον αέρα. Παράλληλα η αναγνώριση αντικειμένων δεν απαιτεί οπτική επαφή (σε αντίθεση με τον γραμμωτό κώδικα που έχει μέσο διασύνδεσης τις υπέρυθρες και απαιτεί οπτική επαφή).

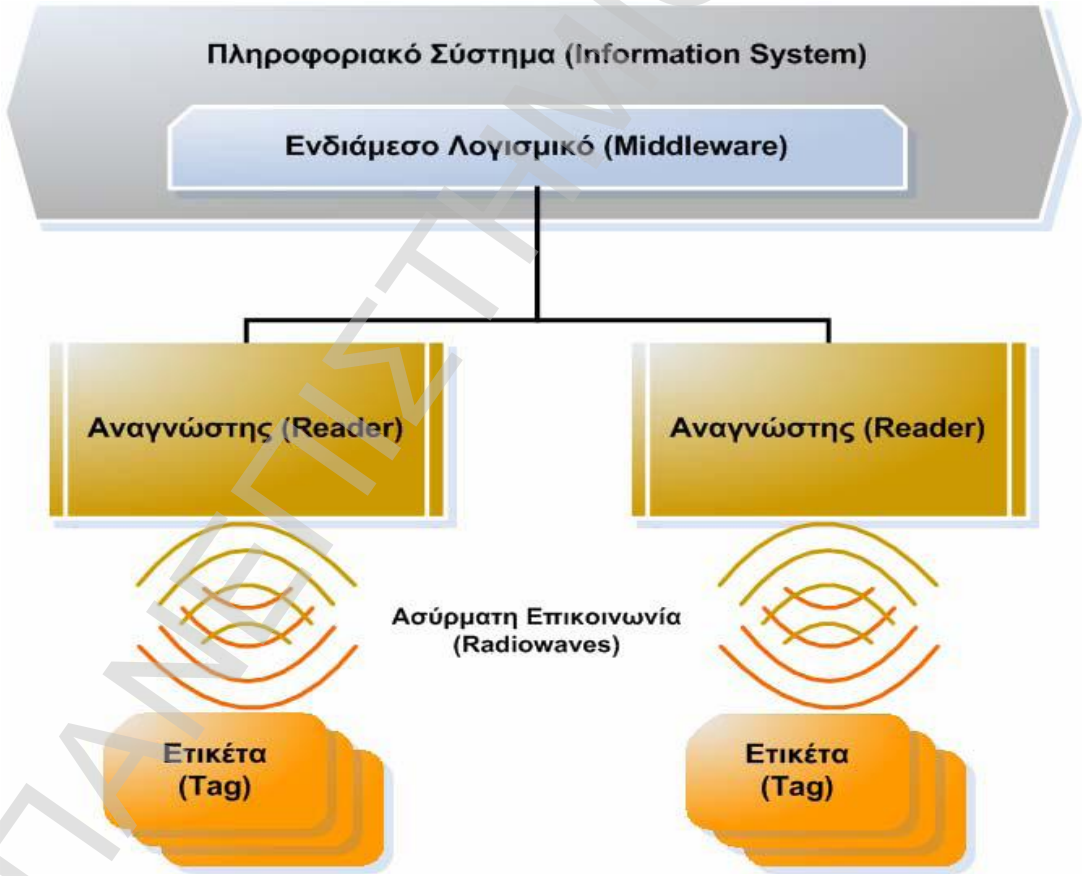
Ένα σύστημα RFID περιλαμβάνει τρία βασικά στοιχεία:

1. την Ετικέτα (tag), η οποία αναφέρεται στην βιβλιογραφία και ως πομποδέκτης (transponder)

2. τον Αναγνώστη (reader), ο οποίος αποτελείται από την κεραία (antenna) και την μονάδα ελέγχου (control unit)

3. το Ενδιάμεσο Λογισμικό (Middleware), το οποίο λειτουργεί ως «γέφυρα» επικοινωνίας μεταξύ του αναγνώστη και του πληροφοριακού συστήματος

Η αρχιτεκτονική του συστήματος RFID απεικονίζεται στην εικόνα 1.1 και αφορά στις τρεις οντότητες που αναφέραμε δηλαδή τις ετικέτες, τους αναγνώστες και το ενδιάμεσο λογισμικό. Τα υπόλοιπα μέρη του πληροφοριακού συστήματος (εξυπηρετητές, δίκτυα, τερματικά κ.α.) παραλείπονται καθώς είναι πέρα από την οπτική αυτού του κεφαλαίου.



Εικόνα 1. 1 Αρχιτεκτονική συστήματος RFID

1.2.1 Πώς λειτουργεί ένα σύστημα RFID

Η λειτουργία ενός RFID συστήματος βασίζεται στην δυναμική και αμφίδρομη επικοινωνία μεταξύ των μερών που απαρτίζουν το σύστημα, τα οποία περιγράψαμε παραπάνω. Ας δούμε όμως μέσω ενός παραδείγματος ένα τρόπο χρήσης ενός RFID συστήματος σε μια ξενοδοχειακή μονάδα.

Η RFID ετικέτα βρίσκεται προσκολλημένη πάνω σε κάποιο αντικείμενο (π.χ. μια κάρτα εισόδου σε δωμάτιο ξενοδοχείου) και περιέχει συγκεκριμένες πληροφορίες οι οποίες ποικίλουν ανάλογα με τον σκοπό της χρήσης του συστήματος RFID (π.χ. ένα μοναδικό κωδικό για τον προσδιορισμό του δωματίου και ένα μοναδικό κωδικό για τον προσδιορισμό του πελάτη). Ο πελάτης του ξενοδοχείου κρατώντας την κάρτα πλησιάζει στην πόρτα του δωματίου του όπου είναι εγκατεστημένος ένας RFID αναγνώστης. Όταν η κάρτα βρεθεί εντός της εμβέλειας της κεραίας του αναγνώστη αυτόματα η μονάδα ελέγχου επικοινωνεί, με ραδιοκύματα, με την ετικέτα και παίρνει τις πληροφορίες που χρειάζεται. Εδώ διευκρινίζεται ότι η ετικέτα έχει και αυτή ενσωματωμένη μια κεραία (περισσότερες πληροφορίες για τις ετικέτες θα ειπωθούν στην ενότητα 1.1.1). Στην συνέχεια το ενδιάμεσο λογισμικό, που κατανοεί τα δεδομένα που στέλνει η μονάδα ελέγχου του αναγνώστη, περνάει τις πληροφορίες στη σωστή μορφή στο πληροφοριακό σύστημα του ξενοδοχείου και ελέγχεται αν ο πελάτης μένει στο δωμάτιο με τον συγκεκριμένο αναγνώστη. Τελικά και εφόσον διαπιστωθεί ότι ο συγκεκριμένος πελάτης μένει στο συγκεκριμένο δωμάτιο η πόρτα του δωματίου ξεκλειδώνεται.

Όπως θα διαπιστώσατε η χρήση του RFID αφορά στην επικοινωνία αναγνώστη – ετικέτας και στην συνέχεια στην μεταφορά των δεδομένων από το ενδιάμεσο λογισμικό στο πληροφοριακό σύστημα. Το παράδειγμά μας είναι αρκετά απλοϊκό καθώς σε πραγματικές εφαρμογές επιτελούνται εργασίες εκατέρωθεν μεταξύ πληροφοριακού συστήματος και αναγνώστη – ετικέτας. Για παράδειγμα, θα μπορούσε να γίνει μια εγγραφή στην ετικέτα με την χρέωση του πελάτη. Στην περίπτωση αυτή το πληροφοριακό σύστημα δίνει την εντολή στο ενδιάμεσο λογισμικό να γίνει η εγγραφή της ετικέτας, το ενδιάμεσο λογισμικό μεταφέρει σε κατάλληλη μορφή την εντολή αυτή στην μονάδα ελέγχου του αναγνώστη ο οποίος επικοινωνεί με την ετικέτα και γράφει τα δεδομένα που του ζητήθηκαν στην ετικέτα ανανεώνοντας έτσι τα δεδομένα της.

Η αρχιτεκτονική του συστήματος RFID είναι σταθερή ως προς την ροή των δεδομένων (ετικέτα ↔ αναγνώστης ↔ ενδιάμεσο λογισμικό ↔ πληροφοριακό σύστημα) αλλά όχι και ως προς την διακριτότητα των επιμέρους στοιχείων. Συγκεκριμένα παρατηρείται μια τάση για ολοκλήρωση της κεραίας, της μονάδας ελέγχου και του ενδιάμεσου λογισμικού σε μια συσκευή που ονομάζεται αναγνώστης. Σε κάθε περίπτωση η ετικέτα είναι αυτόνομη οντότητα.

1.3 Βασικά Στοιχεία του Συστήματος RFID

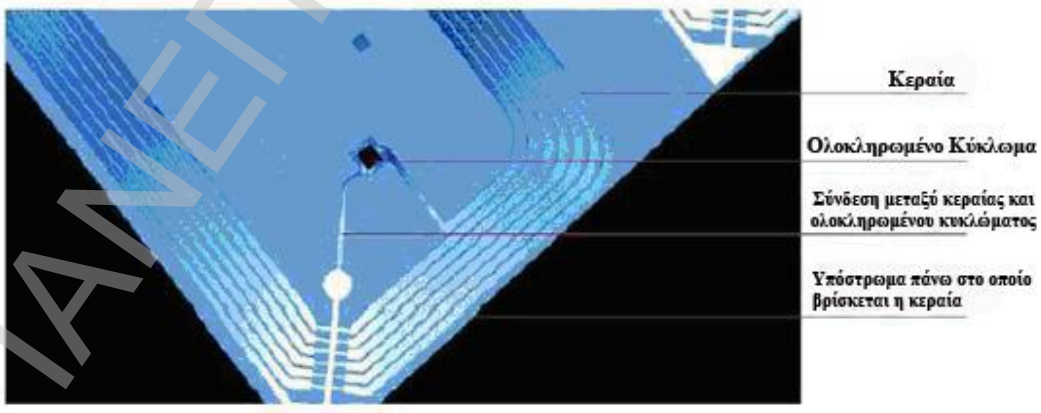
Όπως προαναφέρθηκε τα βασικά στοιχεία του συστήματος RFID είναι τρία: η ετικέτα, ο αναγνώστης και το ενδιάμεσο λογισμικό. Τα στοιχεία αυτά ανάλογα με τις ιδιότητες τους καθορίζουν για ποια εφαρμογή είναι κατάλληλα και ποιες είναι οι δυνατότητες της εφαρμογής.

1.3.1 Ετικέτα (Tag)

Η ετικέτα RFID περιλαμβάνει μια κεραία (antenna) και ένα ολοκληρωμένο κύκλωμα (IC), βλέπε Εικόνα 1.2. Η κεραία χρησιμοποιείται για την αμφίδρομη αποστολή σημάτων μέσω των ραδιοκυμάτων με τον αναγνώστη. Το ολοκληρωμένο κύκλωμα είναι αυτό που καθορίζει κάθε φορά αν θα γίνει εκπομπή ή λήψη δεδομένων και έχει την δυνατότητα να τα αποθηκεύει στην μνήμη του. Η μνήμη κυμαίνεται από 4 μέχρι 128KB.

Οι ετικέτες κατηγοριοποιούνται σε:

- παθητικές (passive), ημιπαθητικές-ημιενεργητικές (semi-passive or semiactive) και ενεργητικές (active)
- αναγνώσιμες (Read only), μίας εγγραφής-πολλών αναγνώσεων (Write Once Read Many) και επανεγράψιμες (Read - Write)

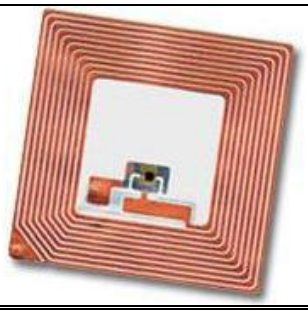


Εικόνα 1. 2 Ετικέτα RFID

Εν γένει θα μπορούσαν να κατηγοριοποιηθούν ακόμα ως προς τις φυσικές τους διαστάσεις, την κατασκευή τους και ως προς την εφαρμογή τους. Στην συνέχεια του κεφαλαίου θα μιλήσουμε και γι' αυτές τις κατηγοριοποιήσεις.

1.3.1.1 Παθητικές, ημιπαθητικές-ημιενεργητικές και ενεργητικές ετικέτες

Οι ετικέτες κατηγοριοποιούνται κυρίως σε παθητικές και ενεργητικές ανάλογα με την πηγή ενέργειάς τους. Οι ενεργητικές ετικέτες διαθέτουν μπαταρία, η οποία είναι ενσωματωμένη στην ετικέτα ενώ οι παθητικές ετικέτες αντλούν την ενέργεια τους από το σήμα που στέλνει ο αναγνώστης (βλέπε Παράρτημα Α). Στον πίνακα 1.1 παρουσιάζονται συνολικά οι διαφορές μεταξύ παθητικών και ενεργητικών ετικετών.

Ετικέτες	**Παθητικές (*Passive*)**	**Ενεργητικές (*Active*)**
Πηγή Ενέργειας	Λειτουργούν χωρίς μπαταρία. Κατά την είσοδο τους στο πεδίο εκπομπής του αναγνώστη ενεργοποιούνται λαμβάνοντας ενέργεια από τα σήματα του αναγνώστη	Απαιτούν μπαταρία για την λειτουργία τους. Όταν εισέρχονται στο πεδίο του αναγνώστη αυτοενεργοποιούνται
Χρόνος Ζωής	Απεριόριστος	Περιορισμένος (*battery-dependent*)
Μέγεθος	Μικρό (προσαρμοζόμενο)	Μεγάλο (απουσία ευελιξίας)
Κόστος	Χαμηλό (20 λεπτά - 3€)	Υψηλό (20€ και άνω)
Ισχύς Εκπομπής Αναγνωστών	Ισχυρή εκπομπή	Όχι ιδιαίτερες απαιτήσεις εκπομπής
Απόσταση Ανάγνωσης	Μικρή (20cm – 6m)	Μεγάλη (30m – 40m)
Φωτογραφία		

Πίνακας 1. 1 Παθητικές και ενεργητικές ετικέτες

Επίσης υπάρχει και μια τρίτη υποκατηγορία ετικετών που ονομάζονται ημιπαθητικές ή ημιενεργητικές ετικέτες. Οι ετικέτες αυτές περιέχουν μπαταρία η οποία όμως δεν χρησιμοποιείται για τη μετάδοση ραδιοκυμάτων στον αναγνώστη παρά μόνο για τη λειτουργία του ολοκληρωμένου κυκλώματος τους (π.χ. μπορούν να έχουν ενσωματωμένο ένα αισθητήρα θερμοκρασίας μετρώντας την θερμοκρασία του περιβάλλοντος ανά τακτά χρονικά διαστήματα και όταν εισέλθουν στο πεδίο εκπομπής του αναγνώστη μεταδίδουν τα δεδομένα που έχουν αποθηκεύσει). Στην βιβλιογραφία αναφέρονται συνήθως ως ενεργητικές ετικέτες καθώς περιέχουν μπαταρία. Όμως λόγω των μικρότερων απαιτήσεων τους σε ισχύ η μπαταρία άρα και το μέγεθος τους είναι σημαντικά μικρότερο γεγονός που τις κάνει και φθηνότερες από τις ενεργητικές ετικέτες.

Η απαιτούμενη απόσταση ανάγνωσης των ημιπαθητικών ή ημιενεργητικών ετικετών είναι μεγαλύτερη από αυτή των παθητικών και μικρότερη από αυτή των ενεργητικών ετικετών. Τέλος οι ετικέτες αυτές είναι συνήθως μιας χρήσης, δηλαδή όταν αποφορτιστεί η μπαταρία τους αχρηστεύονται.

1.3.1.2 Αναγνώσιμες, μίας εγγραφής-πολλών αναγνώσεων και επανεγράψιμες Ετικέτες

Όπως προαναφέρθηκε οι ετικέτες έχουν μνήμη, λόγω του ολοκληρωμένου κυκλώματος που περιέχουν. Επομένως οι ετικέτες κατηγοριοποιούνται ανάλογα με την δυνατότητα επανεγγραφής τους σε αναγνώσιμες, μίας εγγραφής-πολλών αναγνώσεων και επανεγράψιμες.

Οι αναγνώσιμες ετικέτες εγγράφονται μία φορά με τα κατάλληλα δεδομένα κατά την κατασκευή τους (συνήθως ένα σειριακό αριθμό και ένα ψηφίο ελέγχου) και οι αναγνώστες μπορούν μόνο να διαβάσουν τα δεδομένα και όχι να τα τροποποιήσουν. Οι ετικέτες μίας εγγραφής-πολλών αναγνώσεων εγγράφονται κατά την κατασκευή τους, μπορούν όμως να εγγραφούν και από τον χρήστη μόνο μια φορά ακόμα. Έπειτα μετατρέπονται σε αναγνώσιμες ετικέτες.

Οι επανεγράψιμες ετικέτες εγγράφονται κατά την κατασκευή τους, όμως οι αναγνώστες έχουν την δυνατότητα εκτός από το να διαβάζουν τα δεδομένα τους, να τα τροποποιούν (εισαγωγή, διαγραφή) απεριόριστα. Στον πίνακα 1.2 παρουσιάζονται συνολικά οι διαφορές μεταξύ αναγνώσιμων και επανεγράψιμων ετικετών.

Ετικέτες	**Αναγνώσιμες (*Read Only*)**	**Μίας εγγραφής – Πολλών Αναγνώσεων (*WORM*)**	**Επανεγράψιμες (*Read - Write*)**
Ανάγνωση	Απεριόριστα	Απεριόριστα	Απεριόριστα
Εγγραφή κατά την κατασκευή	Ναι	Ναι	Ναι
Εγγραφή κατά	Όχι	Μία φορά μόνο	Απεριόριστα

την χρήση			
Ευελιξία	Μικρή	**ß ---------- à**	Μεγάλη
Ασφάλεια	Μεγάλη	**ß ---------- à**	Μικρή
Κόστος	Μικρό	**ß ---------- à**	Μεγάλο
Εφαρμογές	Έλεγχος πρόσβασης	Διαχείριση εφοδιαστικής αλυσίδας	Αυτόματη συλλογή διοδίων, έλεγχος βιομηχανικής παραγωγής

Πίνακας 1. 2 Αναγνώσιμες, μίας εγγραφής-πολλών αναγνώσεων και επανεγγράψιμες ετικέτες

1.3.1.3 Κατηγοριοποίηση ετικετών σύμφωνα με την κατασκευή και την εφαρμογή τους

Οι εφαρμογές των RFID συστημάτων ποικίλλουν μεταξύ τους ως προς τις απαιτήσεις που έχουν από τις ετικέτες. Για το λόγο αυτό η κατασκευή των ετικετών αλλάζει αναλόγως την εφαρμογή και τις ανάγκες της. Με τον όρο κατασκευή ετικετών αναφερόμαστε στην ενσωμάτωση της κεραίας και του ολοκληρωμένου κυκλώματος στην ετικέτα καθώς και τον τρόπο με τον οποίο αυτή τοποθετείται πάνω στο αντικείμενο που πρέπει να αναγνωριστεί.

Κάποια από τα είδη ετικετών που χρησιμοποιούνται σήμερα είναι:

- Ένα ευρέως χρησιμοποιούμενο είδος ετικέτας είναι οι έξυπνες ετικέτες (Smart Labels) που είναι κοινές χάρτινες ή πλαστικές ετικέτες στις οποίες εκτυπώνεται ο γραμμωτός κώδικας (bar code) και ενσωματώνεται μια ετικέτα RFID τύπου επιφανειακής τοποθέτησης (inlay). Η ετικέτα RFID τύπου επιφανειακής τοποθέτησης έχει την μορφή ενός πλαστικού αυτοκόλλητου στο οποίο τυπώνεται το ολοκληρωμένο κύκλωμα και η κεραία με μεταξοτυπία ή χάραξη. Για την δουλειά αυτή υπάρχουν ειδικοί εκτυπωτές εμπορίου που αναλαμβάνουν τόσο την εκτύπωση της έξυπνης ετικέτας όσο και τον προγραμματισμό της ετικέτας RFID που ενσωματώνεται. Οι ετικέτες αυτές χρησιμοποιούνται κυρίως στην διαχείριση της εφοδιαστικής αλυσίδας. Επίσης ετικέτες RFID τύπου επιφανειακής τοποθέτησης ενσωματώνονται σε κάρτες που ονομάζονται έξυπνες κάρτες μη επαφής (contactless smart cards) και χρησιμοποιούνται κυρίως σε εφαρμογές ελέγχου πρόσβασης (π.χ. κάρτες που χρησιμοποιούνται σε θεματικά πάρκα για την χρέωση των πελατών κατά την είσοδο τους στα διάφορα θεάματα).

- Ένα επίσης ευρέως χρησιμοποιούμενο είδος ετικέτας είναι ο δίσκος (disk), μια στρογγυλή θερμοπλαστικά διαμορφωμένη κατασκευή προκειμένου να λειτουργεί κάτω από ένα εύρος θερμοκρασιών. Κύριο χαρακτηριστικό τους είναι η μεγάλη τους αντοχή σε ακραίες θερμοκρασίες και χτυπήματα και για το λόγο αυτό τοποθετούνται κυρίως σε

παλέτες τοποθετώντας μια βίδα στερέωσης στην οπή στο κέντρο της ετικέτας. Οι μικρότερες εκ αυτών ράβονται ως κουμπιά σε πουκάμισα και άλλα ρούχα.

- Ένα επόμενο είδος ετικέτας είναι αυτό για τον εντοπισμό ζώων και ανθρώπων. Ονομάζονται γυάλινοι σωλήνες (glass tubes) και πρόκειται για συσκευές πολύ μικρές, 30mm μήκος περίπου, που προορίζονται να τοποθετηθούν κάτω από το δέρμα του ζώου ή του ανθρώπου με ένεση. Σκοπός της χρήσης τους είναι ο εντοπισμός (κυρίως στην περίπτωση των ζώων) και η ταυτοποίηση.

- Παρόμοιο με το παραπάνω είδος είναι η ετικέτα ενωτίου (ear tag) που προορίζεται για τον εντοπισμό ζώων κυρίως εκτροφείων, όπως βοοειδών και χοιρινών. Οι ετικέτες αυτές, όπως δηλώνει και το όνομα τους, τοποθετούνται στο αυτί του ζώου. Άλλες ετικέτες παρόμοιας χρήσης είναι οι κεραμικές ετικέτες (ceramic tags) τις οποίες καταπίνουν τα ζώα και παραμένουν στον μόνιμα στον προστόμαχο τους καθώς και οι ετικέτες περιλαίμιου (collar tags).

1.3.2 Αναγνώστης (Reader)

Ο αναγνώστης είναι μια συσκευή που αναλαμβάνει να επικοινωνήσει με την ετικέτα μέσω των ραδιοκυμάτων και για το λόγο αυτό ενσωματώνει κεραία. Επίσης περιέχει μια μονάδα ελέγχου που καθορίζει τις ενέργειες που κάνει ο αναγνώστης (αποστολή/λήψη σημάτων, ανάγνωση/ εγγραφή ετικετών κ.α.), ενέργειες που καθορίζονται από το ενδιάμεσο λογισμικό. Επίσης η μονάδα ελέγχου αναλαμβάνει την επικοινωνία με το πληροφορικό σύστημα μέσω του ενδιάμεσου λογισμικού που παίζει το ρόλο μεταφραστή και για τις δύο πλευρές.

Εικόνα 1. 3 Ο Αναγνώστης

Ανάλογα με την εφαρμογή, τις τεχνικές ιδιότητες και τις φυσικές διαστάσεις τους, οι αναγνώστες κατηγοριοποιούνται σε:

1. Σταθερούς Αναγνώστες

2. Ολοκληρωμένους Αναγνώστες

3. Αναγνώστες Χειρός

4. Ενσωματωμένους Αναγνώστες

Στους πίνακες 1.3, 1.4 που ακλουθούν περιγράφονται οι ιδιότητες για κάθε μία από τις κατηγορίες των αναγνωστών.

Αναγνώστες	**Σταθεροί**	**Ολοκληρωμένοι**
Γενικά Χαρακτηριστικά	Περιέχουν 2 – 8 κεραίες	Περιέχουν 1 κεραία
Εφαρμογές	Χρησιμοποιούνται κυρίως στην εφοδιαστική αλυσίδα (σε εισόδους αποβάθρων φόρτωσης/ εκφόρτωσης, σε ταινίες μεταφοράς προϊόντων)	Χρησιμοποιούνται κυρίως σε εφαρμογές ελέγχου πρόσβασης (σε εισόδους/ εξόδους κρίσιμων υποδομών)
Τεχνικά Χαρακτηριστικά	16-bit/ 32-bit επεξεργαστές, περιέχουν λειτουργικό σύστημα, δυνατότητα επεξεργασίας σήματος	16-bit επεξεργαστές, περιέχουν λειτουργικό σύστημα, αυξημένες δυνατότητες ανάγνωσης εγγραφής
Δικτύωση	TCP/ IP ανεξάρτητοι κόμβοι, κατέχουν δικό τους API, χρησιμοποιούν μια σειρά από πρωτόκολλα (DHCP, HTTP, Telnet or SSH, NTP, SNMP)	Σπάνια TCP/ IP ανεξάρτητοι κόμβοι, συνήθως χρησιμοποιούν σύνδεση σειριακή (RS-232) ή USB

Φωτογραφία		

Πίνακας 1. 3 Σταθεροί και ολοκληρωμένοι αναγνώστες RFID

Αναγνώστες	**Χειρός**	**Ενσωματωμένοι**
Γενικά Χαρακτηριστικά	Περιέχουν 1 κεραία	Περιέχουν 1 κεραία
Εφαρμογές	Χρησιμοποιούνται κυρίως στην εφοδιαστική αλυσίδα για ελέγχους αποθέματος	Χρησιμοποιούνται κυρίως για ενσωμάτωση σε συσκευές όπως οι εκτυπωτές ετικετών RFID, ταξινομητές κιβωτίων, τερματικά POS
Τεχνικά Χαρακτηριστικά	16-bit/ 32-bit επεξεργαστές, περιέχουν λειτουργικό σύστημα, δυνατότητα επεξεργασίας σήματος	Δεν περιέχουν επεξεργαστή, δεν περιέχουν λειτουργικό
Δικτύωση	Ασύρματοι TCP/ IP κόμβοι, συνδέονται απευθείας με εξυπηρετητές (συνήθως περιοδικά) χρησιμοποιώντας εφαρμογές μεταφοράς δεδομένων	Δεν έχουν ικανότητες δικτύωσης, χρησιμοποιούν σύνδεση USB, Σειριακή (RS-232) or PCMCIA
Φωτογραφία		

Πίνακας 1. 4 Χειρός και ενσωματωμένοι αναγνώστες RFID

1.3.3 Ενδιάμεσο Λογισμικό (Middleware)

Το ενδιάμεσο λογισμικό είναι ο «αντιπρόσωπος» του RFID αναγνώστη στο πληροφοριακό σύστημα της εκάστοτε εταιρίας. Αναλαμβάνει να προωθεί τόσο προς τον αναγνώστη τα δεδομένα και τις εντολές που δέχεται από το πληροφοριακό σύστημα όσο και τα δεδομένα και τις εντολές που δέχεται από τον αναγνώστη προς το πληροφοριακό σύστημα.

Οι εντολές προς τον αναγνώστη αφορούν κυρίως πράξεις που πρέπει να γίνουν πάνω σε μια ετικέτα (εύρεση ετικέτας, ανάγνωση κωδικού ετικέτας, ανάγνωση δεδομένων ετικέτας, εγγραφή δεδομένων στην ετικέτα, καταστροφή ετικέτας κ.α.) αλλά και πράξεις που αφορούν τον ίδιο τον αναγνώστη (ανάγνωση κατάστασης αναγνώστη, αλλαγή ρυθμίσεων αναγνώστη, ανάγνωση κωδικού αναγνώστη κ.α.) και ονομάζονται ως εντολές αναγνώστη. Τα δεδομένα που μεταφέρονται εκατέρωθεν μεταξύ αναγνώστη και πληροφοριακού συστήματος αφορούν είτε τα δεδομένα που αποθηκεύονται σε μια ετικέτα είτε δεδομένα που απαιτούνται για την επικοινωνία
μεταξύ Π.Σ. και αναγνώστη.

1.4 Συχνότητες

Οι ζώνες συχνοτήτων που χρησιμοποιούν τα συστήματα RFID διακρίνονται σε:

1. Ζώνη χαμηλών συχνοτήτων (LF, low frequency) στα 125/134 KHz

2. Ζώνη υψηλών συχνοτήτων (HF, high frequency) στα 13.56 MHz

3. Ζώνη πολύ υψηλών συχνοτήτων (UHF, Ultra high frequency) στα
433/869/915 MHz
4. Ζώνη μικροκυμάτων (mW, micro-wave) στα 2.45/5.8GHz
Στον πίνακα 1.5 που ακολουθεί περιγράφονται ιδιότητες και χαρακτηριστικά των τεσσάρων ζωνών συχνοτήτων καθώς και σε ποιες εφαρμογές χρησιμοποιούνται.

Ζώνες Συχνοτήτων	**LF 125 KHz**	**HF 13.56 MHz**	**UHF 869 (EU) 915 (USA) MHz**	**Microwave 2.45 GHz & 5.8 GHz**
Μέγιστη απόσταση ανάγνωσης	< 0.5 m	- 1 m	- 6 m	- 1 m
Γενικά Χαρακτηριστικά	Σχετικά ακριβά ακόμα και για μεγάλες παραγγελίες. Οι	Λιγότερο ακριβές σε σχέση με τις επαγωγικές LF ετικέτες.	Σε μεγάλες ποσότητες οι UHF ετικέτες είναι	Παρόμοια χαρακτηριστικά με τις UHF ετικέτες

	LF συχνότητες απαιτούν μια μεγαλύτερη και ακριβότερη κεραία. Οι επαγωγικές ετικέτες είναι ακριβότερες από τις χωρητικές.	Κατάλληλες για εφαρμογές που δεν απαιτούν μεγάλη απόσταση ανάγνωσης πολλαπλών ετικετών.	φθηνότερες από LF και HF. Καλή ισορροπία μεταξύ απόσταση ανάγνωσης – επιδόσεων κυρίως για ανάγνωση πολλαπλών ετικετών.	αλλά με μεγαλύτερο ρυθμό ανάγνωσης Είναι ευαίσθητες στην απόδοσή τους λόγω της παρουσίας μετάλλων, υγρών και άλλων υλικών.
Πηγή ενέργειας για την ετικέτα	Γενικά παθητικές ετικέτες που χρησιμοποιούν επαγωγική σύζευξη	Γενικά παθητικές ετικέτες που χρησιμοποιούν επαγωγική ή χωρητική σύζευξη	Ενεργές ετικέτες με εσωτερική μπαταρία ή παθητικές ετικέτες που χρησιμοποιούν χωρητική σύζευξη	Ενεργές ετικέτες με εσωτερική μπαταρία ή παθητικές ετικέτες που χρησιμοποιούν χωρητική σύζευξη
Τυπικές Εφαρμογές	Έλεγχος πρόσβασης, εντοπισμός ζώων, immobilizer οχημάτων, εφαρμογές POS	Έξυπνες κάρτες, εντοπισμός σε επίπεδο τεμαχίου, χειρισμός βαλιτσών , βιβλιοθήκες	Εντοπισμός σε επίπεδο παλέτας, αυτόματη είσπραξη διοδίων, διαχείριση βαλιτσών	Αυτόματη είσπραξη διοδίων
Ρυθμός Ανάγνωσης Δεδομένων	Αργός	**ß ---------- à**	**ß ---------- à**	Γρήγορος
Ανάγνωση σε μεταλλικές και υγρές επιφάνειες	Ικανοποιητική	**ß ---------- à**	**ß ---------- à**	Μη ικανοποιητική
Μέγεθος ετικέτας	Μεγάλο	**ß ---------- à**	**ß ---------- à**	Μικρό

Πίνακας 1.5 Συχνότητες τεχνολογίας RFID

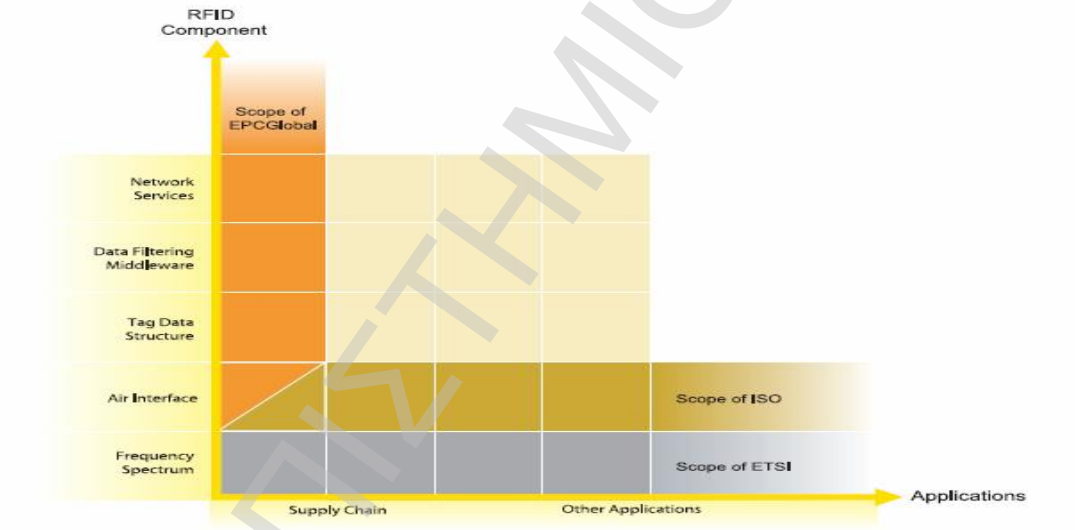
1.5 Πρότυπα

Η τεχνολογία RFID χρησιμοποιεί τις ραδιοσυχνότητες και για το λόγο αυτό απαιτούνται πρότυπα που θα καθορίζουν ποιο κομμάτι του φάσματος συχνοτήτων θα δεσμεύει, τα επίπεδα εκπομπής και θέματα παρεμβολών με άλλες ράδιο-υπηρεσίες. Επίσης η ύπαρξη πολλών κατασκευαστών - προμηθευτών τεχνολογίας RFID δημιουργεί πρόβλημα στον καταναλωτή (στην συγκεκριμένη περίπτωση ο καταναλωτής είναι η εταιρία που θα εγκαταστήσει ένα σύστημα RFID) που καλείται να επικοινωνήσει με διαφορετικά συστήματα RFID (π.χ. πως θα γνωρίζει μια εταιρία ποιο είναι το κατάλληλο σύστημα RFID για μια εφαρμογή ελέγχου πρόσβασης).

Παράλληλα το όραμα της αγοράς για ένα ανοικτό και παγκόσμιο σύστημα διαχείρισης της εφοδιαστικής αλυσίδας, με χρήση της τεχνολογίας RFID, απαιτεί πρότυπα προκειμένου αυτό να γίνει πραγματικότητα. Για τους παραπάνω λόγους έχουν αναπτυχθεί μια σειρά από πρότυπα από συγκεκριμένους οργανισμούς που είναι οι:

- Παγκόσμιος Οργανισμός Προτυποποίησης (ISO, International Organization for Standardization)
- Παγκόσμιο Ηλεκτροτεχνικό Συμβούλιο (IEC , International Electrotechnical Council)
- Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών (ETSI, European Telecommunications Standards Institute)
- EPC global

Ο κάθε οργανισμός στοχεύει σε μια διαφορετική πτυχή της τεχνολογίας RFID και αναπτύσσει πρότυπα για αυτή. Στο Διάγραμμα 2.1 φαίνονται οι σχέσεις μεταξύ τεχνολογίας RFID και οργανισμών.



Διάγραμμα 1. 1 Σύγκριση προτύπων για την τεχνολογία RFID

1.6 EPC και EPCglobal Network

Η EPC global είναι μια ένωση που διοικείται από αντιπρόσωπους από διάφορους χώρους (αναφέρονται παρακάτω) και αναπτύσσει πρότυπα που στοχεύουν στην παροχή κατάλληλης τεχνολογίας για την αύξηση της αποτελεσματικότητας και την μείωση των λαθών στην λειτουργία της εφοδιαστικής αλυσίδας. Ενδεικτικά οι μετέχοντες στην EPC global είναι:

- Οργανισμοί Εμπορίου: UCC, EAN
- Προμηθευτές προϊόντων: Gillette, Johnson & Johnson, Procter & Gamble
- Λιανέμποροι: Wal-Mart, Metro AG
- Κυβέρνηση: Υπουργείο Αμύνης ΗΠΑ (US Department of Defence)
- Τεχνολογία: Hewlett-Packard, Cisco Systems
- Ακαδημαϊκός χώρος: Ινστιτούτο Τεχνολογίας Μασαχουσέτης (MIT)

Η EPC global πιστεύει ότι θα επιτύχει τους στόχους της με την αυτοματοποίηση του εντοπισμού προϊόντων μέσω της τεχνολογίας RFID και συγκεκριμένα με την χρήση φθηνών RFID ετικετών και τον ορισμό ενός παγκόσμιο πλαισίου ανταλλαγής πληροφοριών. Για το λόγο αυτό έχει αναπτύξει το EPCglobal Network, ένα κατανεμημένο δίκτυο υπηρεσιών, και έχει ορίσει έξι κλάσεις RFID ετικετών με αύξουσα λειτουργικότητα.

Το EPCglobal Network είναι ένα δίκτυο που καθιστά δυνατή την άμεση, μονοσήμαντη και αυτόματη αναγνώριση τεμαχίων στην εφοδιαστική αλυσίδα και τον διαμοιρασμό των δεδομένων τους. Στόχος του είναι η «πραγματική» ορατότητα (visibility) της εφοδιαστικής αλυσίδας, με την παροχή αναγνώρισης οποιουδήποτε τεμαχίου (κωδικός και Serial Number), οποιασδήποτε εταιρίας, οποιασδήποτε βιομηχανίας, οπουδήποτε στον κόσμο με σκοπό να κάνει τις εταιρίες περισσότερο αποτελεσματικές. Το EPCglobal Network αποτελείται από πέντε βασικά στοιχεία:

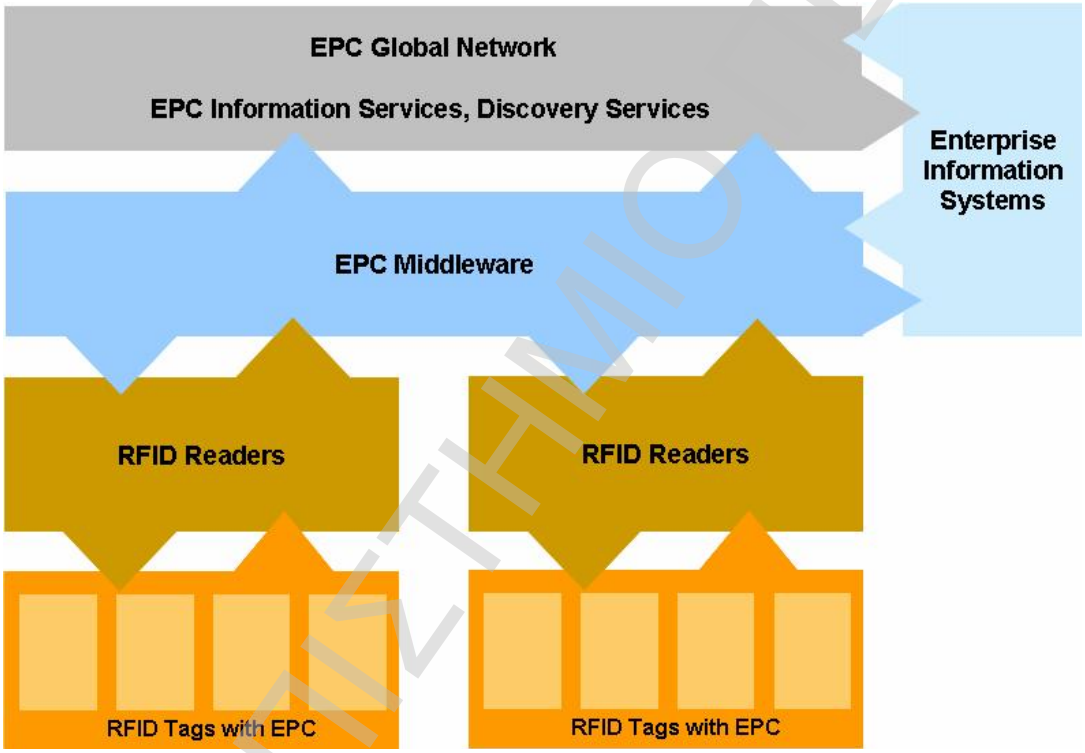
1. Ηλεκτρονικός Κωδικός Προϊόντος (EPC, Electronic Product Code): Ο EPC είναι ένας μοναδικός αριθμός ταυτοποίησης προϊόντος σε επίπεδο τεμαχίου που αποτελείται από 64 - 256 bits.

2. Σύστημα Αναγνώρισης (ID System): Το Σύστημα Αναγνώρισης (ID System) αποτελείται από RFID αναγνώστες και ετικέτες. Οι RFID ετικέτες είναι παθητικές και περιέχουν μόνο τον κωδικό EPC του αντικειμένου στο οποίο επικολλούνται. Οι RFID αναγνώστες διαβάζουν το EPC και το στέλνουν στα τοπικά πληροφοριακά συστήματα της επιχείρησης μέσω του EPC λογισμικού (EPC Middleware).

3. Λογισμικό EPC (EPC Middleware): Το Λογισμικό EPC (EPC Middleware) διαχειρίζεται γεγονότα ανάγνωσης πραγματικού χρόνου και αναλαμβάνει να επικοινωνήσει τις πληροφορίες που δέχεται στις Υπηρεσίες Πληροφοριών EPC και στα τοπικά πληροφοριακά συστήματα της επιχείρησης. Η EPCglobal αναπτύσσει μια πρότυπη διεπαφή εφαρμογής για υπηρεσίες, επιτρέποντας την ανταλλαγή δεδομένων μεταξύ αναγνωστών EPC και πληροφοριακών συστημάτων.

4. Υπηρεσίες Πληροφοριών EPC (EPCIS ,EPC Information Services): Οι Υπηρεσίες Πληροφοριών EPC (EPCIS, EPC Information Services) επιτρέπουν σε χρήστες την ανταλλαγή EPC δεδομένων με εμπορικούς συνεργάτες μέσω του EPCglobal Network.

5. Υπηρεσίες Ανακάλυψης (Discovery Services): Οι υπηρεσίες Ανακάλυψης (Discovery Services) είναι ένα σετ υπηρεσιών που επιτρέπουν στους χρήστες να αναζητήσουν παγκοσμίως, δεδομένα σχετικά με ένα συγκεκριμένο κωδικό EPC και αποκτήσουν πρόσβαση σε αυτά. Μία από τις υπηρεσίες ανακάλυψης είναι η Υπηρεσία Ονοματοδοσίας Αντικειμένων (ONS, Object Naming Service).

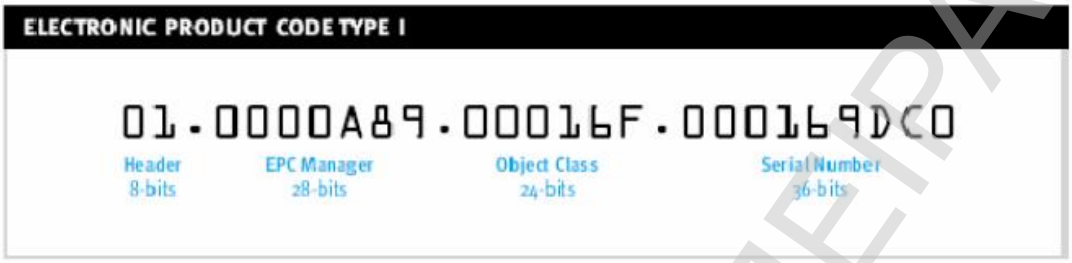


Εικόνα 1. 4 Αρχιτεκτονική EPCglobal Network

1.6.1 Ηλεκτρονικός Κωδικός Προϊόντος

Ο Ηλεκτρονικός Κώδικας Προϊόντος (EPC, Electronic Product Code) χρησιμοποιείται σε συνδυασμό με την τεχνολογία RFID προκειμένου 'Ε7 να βελτιώσει κυρίως την αποτελεσματική διαχείριση της εφοδιαστικής αλυσίδας και να μειώσει τα λειτουργικά κόστη. Ο EPC είναι αποτέλεσμα ενός παγκόσμιου εγχειρήματος

προκειμένου να επιτευχθεί καλύτερη συνεννόηση μεταξύ των μελών της εφοδιαστικής αλυσίδας. Αυτός ο κώδικας παρέχει γρήγορες και λεπτομερείς πληροφορίες για ένα προϊόν σε οποιοδήποτε σημείο της εφοδιαστικής αλυσίδας. Ο EPC είναι παρόμοιος του Παγκόσμιου Κώδικα Προϊόντος (UPC, Universal Product Code), ο οποίος χρησιμοποιείται στους γραμμωτούς κωδικούς.



Εικόνα 1. 5 Παράδειγμα EPC

Ο EPC είναι ένας μοναδικός αριθμός αποτελούμενος από 64 - 256 bits και περιλαμβάνει τέσσερα διακριτά πεδία (βλ. Εικόνα 1.4):

- Επικεφαλίδα (Header): Η επικεφαλίδα αποτελείται από 8-bits και προσδιορίζει το μήκος του Ηλεκτρονικού Κωδικού Προϊόντος
- Διαχειριστής Ηλεκτρονικού Κωδικού Προϊόντος (EPC manager): Προσδιορίζει τον κατασκευαστή του προϊόντος
- Κλάση του αντικειμένου (Object Class): Αναφέρεται στον ακριβή τύπο του αντικειμένου, με τον ίδιο τρόπο όπως η Μονάδα Διατήρησης Αποθέματος SKU (Stock Keeping Unit)
- Σειριακός Αριθμός (Serial Number): Πρόκειται για το συγκεκριμένο σειριακό αριθμό που προσδιορίζει το αντικείμενο

1.7 Κατηγοριοποίηση εφαρμογών RFID

Στον παρακάτω πίνακα γίνεται μια προσπάθεια κατηγοριοποίησης των πεδίων εφαρμογής της τεχνολογίας RFID με βάση το βαθμό εξέλιξης και ανάπτυξης.

Παραδοσιακές εφαρμογές RFID	**Αναδυόμενες εφαρμογές RFID**
1. Έλεγχος ασφάλειας /πρόσβασης	1. Διαχείριση αποθήκης
2. Ηλεκτρονική επιτήρηση άρθρων	2. Διοίκηση εφοδιαστικής αλυσίδας
3. Διαχείριση ενεργητικού	3. Αντίστροφη εφοδιαστική αλυσίδα
4. Μαζική μεταφορά	4. Παρακολούθηση αποστολών
5. Πρόσβαση σε βιβλιοθήκες	5. Παρακολούθηση παγίων στοιχείων

6. Είσπραξη διοδίων	6. Διοίκηση λιανικού εμπορίου
7. Ταυτοποίηση ζώων	7. Παρακολούθηση εγγράφων
	8. Καταπολέμηση της παραχάραξης
	9. Προηγμένος έλεγχος εισόδου
	10. Μαζική μεταφορά
	11. Διαχείριση αεροπορικών αποσκευών
	12. Εφαρμογή σε μέρη και εργαλεία αεροσκαφών
	13. Εφαρμογές υγειονομικής περίθαλψης
	14. Ρυθμιστική συμμόρφωση
	15. Πληρωμές

Πίνακας 1.6: RFID εφαρμογές (παραδοσιακές - αναδυόμενες)

Στην συνέχεια παρατίθεται διάφοροι τομείς εφαρμογής της τεχνολογίας RFID. Η κατηγοριοποίηση βασίζεται στο είδος των ετικετών που χρησιμοποιούνται καθώς επίσης και στους κλάδους που τίθενται σε εφαρμογή.

• **Αδιάκοπη παρακολούθηση τικ pone των προϊόντων (Object ID-Tracking)**
Βασίζονται σε: Ετικέτες / Αυτοκόλλητα. Hard-Tags
Εφαρμογές: Ιατρεία, Νοσοκομεία. Φαρμακευτική βιομηχανία. Διαχείριση λημμάτων. Τράπεζες, Εμπόριο και επιχειρήσεις. Αεροπορικές εταιρίες (παρακολούθηση αποσκευών)

• **Παρακολούθηση Coxov (Animal Tracking)**
Βασίζονται σε: Hard-Tags, Μοσχεύματα
Εφαρμογές: Γεωργία, Αγροτικές δραστηριότητες, Βιομηχανία τροφίμων

• **Παρακολούθηση ανθρώπων (Human-Tracking)**
Βασίζονται σε: Hard-Tags
Εφαρμογές: Ιατρικός κλάδος. Νοσοκομεία. Συστήματα ασφαλείας. Δικαστήρια. Χώρους ψυχαγωγίας και αναψυχής

• **Παρακολούθηση εγγράφων και βιβλίων (Document / Book-Tracking)**

Βασίζονται σε: Ετικέτες / Αυτοκόλλητα, RFID-Tags ενσωματωμένα σε χαρτί
Εφαρμογές: Δημόσιες υπηρεσίες. Κρατικούς φορείς, Μεγάλες εταιρείες. Τράπεζες. Βιβλιοθήκες. Τεχνικά γραφεία

• **Συστήματα εισιτηρίων για ελέγχους εισόδων / ασύρματη μετάδοση πληροφοριών (Ticketing Solutions)**
Βασίζονται σε: Χάρτινα εισιτήρια. Πλαστικές κάρτες. Hard-tags Εφαρμογές: Διόδια, Μεταφορικά μέσα. Δημόσιους χώρους στάθμευσης. Δημόσιες υπηρεσίες. Κρατικούς φορείς, Μεγάλες εταιρείες, Εισιτήρια θεαμάτων. Χιονοδρομικά κέντρα

• **Ηλεκτρονική προστασία προϊόντων. Πρόληψη πειρατείας (Electronic Product Protection)**
Βασίζονται σε: Ετικέτες / Αυτοκόλλητα, Hard-Tags
Εφαρμογές: Λιανικό και χονδρικό εμπόριο. Κατασκευαστές

• **Αυτόματη απογραφή αποθεμάτων (Automatic Inventory)**
Βασίζονται σε: Ετικέτες / Αυτοκόλλητα, Hard-Tags Εφαρμογές: Λιανικό και χονδρικό εμπόριο. Κατασκευαστές

• **Υπολογισμός και καταγραφή θερμοκρασιών (Temperature Data Collection)**
Βασίζονται σε: Ετικέτες / Αυτοκόλλητα, Hard-Tags
Εφαρμογές: Λιανικό και χονδρικό εμπόριο. Φαρμακευτική βιομηχανία. Βιομηχανία τροφίμων

• **Συστήματα πρόσβασης για εισόδους (Entrance Solutions)**
Βασίζονται σε: Ετικέτες / Αυτοκόλλητα, Hard-Tags
Εφαρμογές: Ξενοδοχεία, διαμερίσματα και άλλους χώρους

• **Συλλογή δεδομένων εξ αποστάσεως (Remote Data Collection)**
Βασίζονται σε: Αισθητήρες
Εφαρμογές: Επιστημονικές εφαρμογές (π.χ. σεισμολογία), Συστήματα ασφαλείας. Λιανικό και χονδρικό εμπόριο. Φαρμακευτική βιομηχανία, Βιομηχανία τροφίμων

1.7.1 Εφαρμογές RFID στην παραγωγική διαδικασία και την εφοδιαστική αλυσίδα.

Η χρήση της τεχνολογίας RFID στην εφοδιαστική αλυσίδα υπόσχεται να φέρει επανάσταση στον τρόπο με τον οποίο τα προϊόντα περνούν από τον κατασκευαστή στο λιανοπωλητή και έπειτα στον καταναλωτή.

Το ενδιαφέρον για την τεχνολογία RFID παραμένει υψηλό και αυτό οφείλεται στις συνεχείς βελτιώσεις της τεχνολογίας και στα ιδιαίτερα χαρακτηριστικά της, τα οποία της επιτρέπουν να προσφέρει καινοτόμες λύσεις τόσο κατά μήκος της εφοδιαστικής

αλυσίδας (συστήματα ανοικτού βρόγχου) όσο και εντός των επιχειρήσεων (συστήματα κλειστού βρόγχου).

Παρακάτω ακολουθούν παραδείγματα εφαρμογών κατά την παραγωγική διαδικασία:

- **Το μαρκάρισμα ελαττωματικών προϊόντων**

Ένα ιδιαίτερο χαρακτηριστικό της RFID ετικέτας είναι ότι έχει την ικανότητα να «διαφημίζει» την παρουσία της. Είναι δηλαδή δυνατό να γνωρίζει κανείς πού βρίσκεται ή πού δεν βρίσκεται ένα προϊόν. Αυτό το χαρακτηριστικό αξιοποιείται από επιχειρήσεις για το μαρκάρισμα των ελαττωματικών προϊόντων κατά την ανάλωση τους ώστε να εξασφαλιστεί ότι δεν θα προχωρήσουν ελαττωματικά προϊόντα στα επόμενα στάδια της παραγωγικής διαδικασίας. Η ανάκληση προϊόντων αποτελεί ίσως την πιο σημαντική πηγή απώλειας στην εφοδιαστική αλυσίδα. Αυτό συμβαίνει συχνά επειδή είναι εξαιρετικά δύσκολο για τις επιχειρήσεις να εντοπίσουν μεμονωμένα το συγκεκριμένο ελαττωματικό προϊόν ή παρτίδα και συχνά οδηγούνται στην καταστροφή και μη ελαττωματικών προϊόντων. Μέσω των RFID συστημάτων όμως και του EPC (Electronic Product Code) μπορεί να επιτευχθεί η αποκλειστική αναγνώριση κάθε επιμέρους σημείου της εφοδιαστικής αλυσίδας, επιτρέποντας στους κατασκευαστές να αποκτήσουν άμεση πρόσβαση σε πληροφορίες που τους επιτρέπουν να εντοπίζουν τα ελαττωματικά μόνο προϊόντα και να τα αποσύρουν.

- **Η ταυτοποίηση εξαρτημάτων κατά την συναρμολόγηση**

Για να λειτουργήσει το RFID. δεν απαιτείται οπτική επαφή μεταξύ της ετικέτας και του πομποδέκτη, αντίθετα με τις ετικέτες barcode όπου χρειάζεται να επικολλούνται στην εξωτερική επιφάνεια των συσκευασιών. Το χαρακτηριστικό αυτό του RFID είναι χρήσιμο σε εφαρμογές που για διάφορους λόγους (marketing, προστασία ετικέτας από φθορά) δεν μπορεί να υπάρχει barcode στη συσκευασία. Για παράδειγμα, η τεχνολογία χρησιμοποιείται για την καταγραφή των σειριακών αριθμών των εξαρτημάτων τα οποία προστίθενται σε διάφορα στάδια της επεξεργασίας και συναρμολογούνται σε ένα τελικό προϊόν. Με τη χρήση του RFID. μπορεί να επιβεβαιωθεί η ενσωμάτωση ή όχι των απαραίτητων εξαρτημάτων στο τελικό προϊόν και να εξασφαλιστεί η ιχνηλασιμότητά τους μέσω κωδικών παρτίδας.

- **Η δυναμική διαχείριση αποθήκης και αποθεμάτων**

Με τη χρήση του RFID. ένα σύστημα διαχείρισης αποθήκης (WMS), μπορεί να αποκτήσει καλύτερη ορατότητα στην χωροταξική κατανομή. Με τα barcodes, απαιτείται η επικόλληση ετικετών σε κάθε ράφι. ενώ με το RFID το WMS ενημερώνεται δυναμικά και βοηθά έτσι στην βέλτιστη σχεδίαση και διαχείριση του διαθέσιμου χώρου αποθήκευσης. Επιπλέον μέσω της RFID τεχνολογίας μπορεί να ενισχυθεί η διαχείριση των αποθεμάτων με μια σειρά τρόπους, για παράδειγμα, με συστήματα RFID που μπορεί να βελτιώσουν κατά 10-20% την ικανότητα πρόβλεψης του προϊόντος που απαιτείται συγκριτικά με τα παραδοσιακά συστήματα. Εκτός από αυτό, τα συστήματα RFID μπορούν να βοηθήσουν στη διατήρηση χαμηλότερου επίπεδου αποθεμάτων της τάξεως του 10 έως 30% και αύξηση πωλήσεων κατά 1-2% μέσω της μειωμένης συχνότητας εμφάνισης έλλειψης αποθεμάτων.

- **Η διαχείριση εξοπλισμού**

Η χρήση ενεργών ετικετών RFID βοηθά τις επιχειρήσεις να εντοπίσουν ανά πάσα στιγμή ευκολότερα τον διαθέσιμο εξοπλισμό τους. Για παράδειγμα, ένα σύστημα RFID μπορεί να εντοπίσει την τοποθεσία ενός εργαλείου που είναι κρίσιμο μια δεδομένη στιγμή σε μια γραμμή παραγωγής, χωρίς να απαιτείται μια χρονοβόρα παύση για την αναζήτηση του.

Οι εφαρμογές κατά μήκος της εφοδιαστικής αλυσίδας είναι:

- **Η παρακολούθηση επαναχρησιμοποιούμενων συσκευασιών (reverse logistics)**

Η δυνατότητα της RFID ετικέτας να επικοινωνήσει με το δέκτη χωρίς οπτική επαφή, επιτρέπει στις επιχειρήσεις να παρακολουθήσουν τις επαναχρησιμοποιούμενες συσκευασίες κατά μήκος της εφοδιαστικής αλυσίδας. Έτσι, οι επιχειρήσεις είναι σε θέση να γνωρίζουν το ιστορικό κάθε συγκεκριμένης συσκευασίας (τι περιεχόμενο είχε, πόσες φορές χρησιμοποιήθηκε, σε ποιόν πελάτη εστάλη, αν πρέπει να αποσυρθεί, κτλ). Επίσης, η δυνατότητα για ενσωμάτωση επιπλέον πληροφοριών σε μια ετικέτα RFID. επιτρέπει την ανανέωση της πληροφορίας, ώστε να ταυτίζεται με το εκάστοτε περιεχόμενο της συσκευασίας (κωδικό προϊόντος, κωδικός παρτίδας ημερομηνία λήξης, κτλ) σε κάθε στάδιο της αλυσίδας.

- **Ο Έλεγχος Ποιότητας**

Η προαναφερθείσα δυνατότητα για ανανέωση της πληροφορίας που αποθηκεύεται σε μια ετικέτα επιτρέπει την επίγνωση του πλήρους ιστορικού των συνθηκών αποθήκευσης και διακίνησης ευπαθών προϊόντων (νωπά και κατεψυγμένα). Έτσι, για παράδειγμα, τα τμήματα Ποιότητας των αλυσίδων λιανεμπορίου μπορούν να γνωρίζουν αν το παρελθφθέν φορτίο βρέθηκε εκτός των προβλεπόμενων συνθηκών (π.χ. θερμοκρασία).

- **Η αντιμετώπιση μη γνήσιων προϊόντων**

Το πρόβλημα των πλαστών προϊόντων (counterfeiting) είναι από τα πιο κρίσιμα ζητήματα που αντιμετωπίζει η Βιομηχανία ,και κυρίως η Φαρμακοβιομηχανία σήμερα. Ο Παγκόσμιος Οργανισμός Υγείας υπολογίζει ότι 5-8% των φαρμάκων που διακινούνται παγκοσμίως είναι πλαστά. Στην Αμερική, ο FDA συστήνει την προσέγγιση του «Mass Serialization)), δηλαδή την ταυτοποίηση κάθε μονάδας μεταφοράς με έναν μοναδικό σειριακό αριθμό και την καταχώρηση του αριθμού αυτού σε ένα κεντρικό σύστημα. Έτσι, όλοι οι εμπλεκόμενοι στην φαρμακευτική εφοδιαστική αλυσίδα, από τον παραγωγό έως το φαρμακείο, μπορούν να επιβεβαιώσουν την γνησιότητα του σκευάσματος. Ο FDA προτείνει τη χρήση RFID για την υλοποίηση αυτής της ιδέας διότι ένα σύστημα γνησιότητας με βάση το RFID αντιγράφεται πολύ δύσκολα .

1.7.2 Η ολοκλήρωση των διαδικασιών της εφοδιαστικής αλυσίδας μέσω της RFID τεχνολογίας

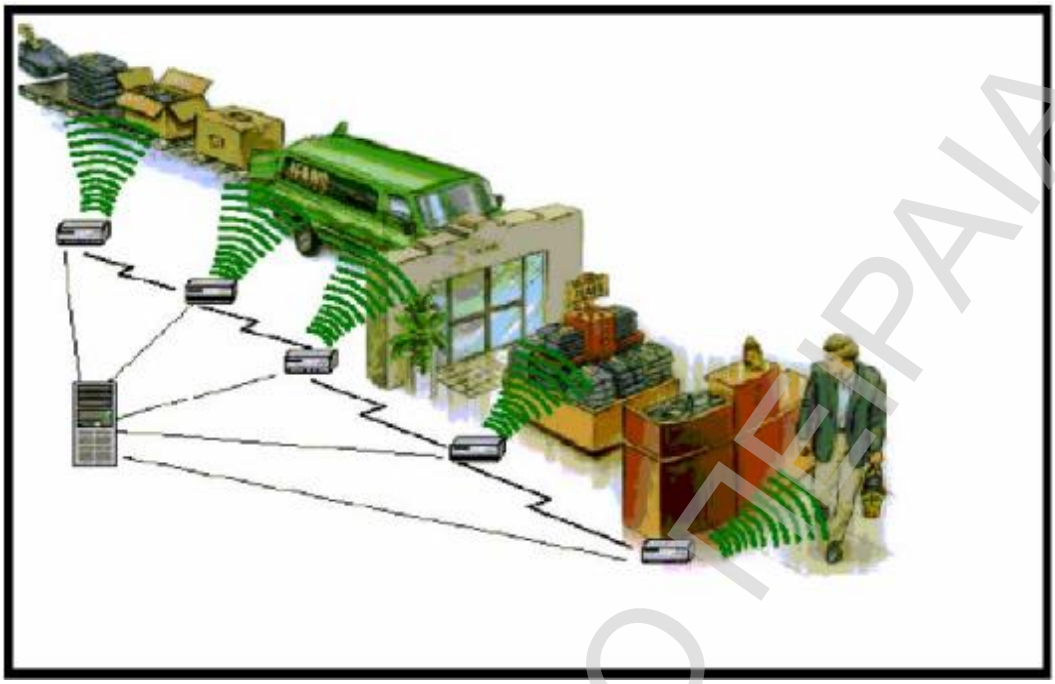
Οι δυνατότητες του RFID είναι απεριόριστες. Η συγκεκριμένη τεχνολογία παρέχει στις επιχειρήσεις ποικιλία υλικού και λογισμικού, εναλλακτικές διαδικασίες και νέες μορφές συνεργασίας. Οι επιχειρήσεις που εξετάζουν τη χρήση του RFID συχνά αναρωτιούνται: «Από πού αρχίζω; Πώς μπορώ να χρησιμοποιήσω αυτήν την τεχνολογία για να βελτιώσω την επιχείρηση μου;»

Η χρήση της τεχνολογίας RFID κατά μήκος της εφοδιαστικής αλυσίδας θα προσδώσει σημαντικά οφέλη που αφορούν κυρίως τη μείωση τον λειτουργικών δαπανών και κατά συνέπεια την αύξηση κερδών. Πολλοί αναλυτές πιστεύουν ότι αυτό θα συμβεί αρχικά μέσα από:

- Το μειωμένο απόθεμα
- Την εξάλειψη φυσικών φθορών
- Τις μειωμένες δαπάνες εργασίας σε καταστήματα και αποθήκες εμπορευμάτων
- Τις μειωμένες ελλείψεις εμπορευμάτων (out-of-stock)

Σε αυτή την ενότητα παρουσιάζεται μία σύντομη επισκόπηση της ροής των προϊόντων σε μια «χαρακτηριστική» εφοδιαστική αλυσίδα λιανεμπορίου.

Στις εγκαταστάσεις του κατασκευαστή, οι παλέτες συγκεντρώνονται αμέσως μετά από τη γραμμή παραγωγής και είτε αποθηκεύονται στην αποθήκη, είτε προωθούνται προς ένα από τα κέντρα διανομής. Για την εφοδιαστική αλυσίδα που θα εξεταστεί, οι περισσότερες παραδόσεις προϊόντων που φθάνουν τελικά στο κατάστημα στέλνονται απευθείας από την αποθήκη των εργοστασίων στο κατάστημα λιανικής πώλησης. Προκειμένου να ετοιμαστεί μια παράδοση εμπορευμάτων για ένα κέντρο διανομής, οι παλέτες μεταφέρονται από την περιοχή αποθήκευσης των εμπορευμάτων και τοποθετούνται στην περιοχή δρομολόγησης όπου φορτώνονται επάνω στα φορτηγά. Όταν τα φορτηγά φθάνουν στο κέντρο διανομής τα εμπορεύματα ξεφορτώνονται, ελέγχονται και αποθηκεύονται. Μερικές από τις παλέτες στέλνονται από το κέντρο διανομής στα καταστήματα ως πλήρεις (περιέχουν προϊόντα του ίδιου είδους), αλλά η πλειοψηφία των παλετών είναι μικτές (περιέχουν διαφορετικά είδη προϊόντων). Πριν από την αποστολή, οι παλέτες που ανήκουν σε μια παραγγελία συγκεντρώνονται στην περιοχή δρομολόγησης και όταν το φορτηγό φθάνει, αυτές φορτώνονται και αποστέλλονται στο κατάστημα λιανικής. Το κατάστημα παραλαμβάνει εμπορεύματα από περισσότερα του ενός κέντρα διανομής ή ακόμη κι άμεσα από τους κατασκευαστές. Οι υπάλληλοι των καταστημάτων ελέγχουν τις παλέτες και τις τοποθετούν στην αποθήκη του καταστήματος μέχρι να χρειαστεί να μεταφερθούν στο χώρο του καταστήματος προς πώληση. Σε μερικές περιπτώσεις, ο λιανοπωλητής εντοπίζει ελλιπή ή πρόσθετα προϊόντα σε μια παράδοση ή ελαττωματικά προϊόντα, γεγονός το οποίο δημιουργεί προβλήματα επιστροφών ή επαναποστολής. Η ροή των αγαθών από τη γραμμή παραγωγής μέχρι την αγορά του τελικού προϊόντος από τον καταναλωτή φαίνεται στην παρακάτω εικόνα .



Εικόνα 1.6: Η ροή των Προϊόντων σε μια τυπική εφοδιαστική αλυσίδα

Στη συνέχεια γίνεται μια σύντομη περιγραφή του τρόπου με τον οποίο η τεχνολογία RFID μπορεί να χρησιμοποιηθεί σε κάθε μια από τις κοινές διαδικασίες που εμφανίζονται τόσο στις αποθήκες όσο και στα κέντρα διανομής.

Παραλαβή των προϊόντων

Η μείωση της εργασίας κατά την παραλαβή είναι αποδεδειγμένα μια πολύ μεγάλη κινητήρια δύναμη για τις επιχειρήσεις που αναζητούν ή και απαιτούν την εφαρμογή των RFID ετικετών από τους προμηθευτές τους κατά την αποστολή των εμπορευμάτων. Οι παλέτες και τα κιβώτια αναγνωρίζονται αυτόματα καθώς αυτά ξεφορτώνονται από το φορτηγό, είτε μέσω Fixed RFID αναγνωστών που είναι τοποθετημένοι στην πόρτα παραλαβής , είτε μέσω mobile RFID αναγνωστών που είναι τοποθετημένοι στα διάφορα παλετοφόρα. Τα δεδομένα που διαβάζονται από τις ετικέτες της παλέτας ή του κουτιού, μεταφέρονται στο πληροφοριακό σύστημα της αποθήκης (WMS) και αναβαθμίζουν τη βάση δεδομένων. Το σύστημα στη συνέχεια ρυθμίζει την παραγγελία και στέλνει προς τον αναγνώστη τις απαραίτητες πληροφορίες που θα επιτρέψουν σε μερικά εμπορεύματα να μεταφορτωθούν άμεσα σε άλλη παραγγελία, ενώ σε άλλα να αποθηκευτούν. Μέσω της εφαρμογής της τεχνολογίας RFID. σε αυτή τη διαδικασία, η εργασία αυτή είναι λιγότερο χρονοβόρα και δύσχρηστη για το προσωπικό απ' ότι η ίδια διαδικασία με την χρήση του barcode συστήματος.

Τοποθέτηση των προϊόντων στους χώρους αποθήκευσης

Μέσω της αυτόματης σύνδεσης των «προς αποθήκευση» εμπορευμάτων και της πραγματικής τους θέσης τοποθέτησης, η τεχνολογία RFID. μπορεί να βελτιώσει την ακρίβεια της διαδικασίας τοποθέτησης των εμπορευμάτων μέσα στην αποθήκη χωρίς την απαίτηση για περαιτέρω καταχώριση δεδομένων ή την ανίχνευση του barcode . Όταν ένα κιβώτιο ή μια παλέτα πραγματικά τοποθετείται σε μια θέση ο αναγνώστης του παλετοφόρου αυτόματα καταγράφει την κίνηση και αντιστοιχίζει τη θέση αποθήκευσης με το ID του κιβωτίου ή της παλέτας, μέσω μιας προεγκατεστημένης ετικέτας στη θέση αποθήκευσης. Κατά αυτό τον τρόπο, οι χειριστές μειώνουν το χρόνο τοποθέτησης των εμπορευμάτων καθώς δεν απαιτείται στόχευση και ανίχνευση του barcode, ενώ επίσης, εξαλείφεται η πιθανότητα λάθους αντιστοίχησης του κωδικού της θέσης τοποθέτησης με το εμπόρευμα.

Ασφάλιση της περιοχής αποθήκευσης και φύλαξη σημαντικών εγγράφων

Η αρχή της αυτόματης τοποθέτησης, όπως παρουσιάστηκε στην προηγούμενη παράγραφο, μπορεί να τροποποιηθεί κατά τέτοιο τρόπο προκειμένου να παρέχει τον έλεγχο αφύλακτων θέσεων. Σε αυτή την εφαρμογή γίνεται χρήση κυρίως σταθερών RFID αναγνωστών για να παρακολουθείται μια συγκεκριμένη τοποθεσία, όπως μια πύλη ή μια ξεχωριστή περιοχή αποθήκευσης. Η εφαρμογή αυτή είναι χρήσιμη για καταστάσεις όπου η περιοχή αποθήκευσης χρησιμοποιείται για ασφάλεια ή και για φύλαξη σημαντικών εγγράφων. Για παράδειγμα, σε μια περιοχή όπου τοποθετούνται προϊόντα υψηλής αξίας, η χρήση της τεχνολογίας RFID για συνεχή παρακολούθηση ασφαλίζει την εν λόγω περιοχή από πιθανές κλοπές.

Συλλογή των προϊόντων

Η χρήση της τεχνολογίας RFID στη διαδικασία της συλλογής των εμπορευμάτων από μια θέση της αποθήκης, όπως και στην περίπτωση της τοποθέτησης, ελαχιστοποιεί τις λανθασμένες εντολές. Τα εμπορεύματα αναγνωρίζονται αυτόματα, από ένα σταθερό αναγνώστη ή κάποιον άλλο κινητό αναγνώστη, καθώς αυτά συλλέγονται, ενώ τα δεδομένα αυτόματα μεταφέρονται και ελέγχονται από το WMS ή από ένα σύστημα διαχείρισης παραγγελιών προκειμένου να επιβεβαιωθεί ότι το συγκεκριμένο εμπόρευμα που συλλέγεται ανήκει στην παραγγελία που εκτελείται. Επίσης, στην περίπτωση της χρήσης παλετών, οι ετικέτες των εμπορευμάτων μπορούν ταυτόχρονα να συνδέονται και να ενημερώνουν και τα δεδομένα της ετικέτας της παλέτας στην οποία είναι τοποθετημένα, εξασφαλίζοντας έτσι μείωση στο χρόνο της καταχώρησης δεδομένων σε ένα σύστημα βασισμένο σε επίπεδο παλέτας.

Φόρτωση των προϊόντων

Με τη χρήση της τεχνολογίας RFID. στο στάδιο της αποστολής των εμπορευμάτων, ελέγχονται οι παλέτες που φορτώνονται και βελτιώνεται η ακρίβεια της φόρτωσης, ακόμα και αν μια παλέτα δεν έχει περάσει από τη διαδικασία της συλλογής. Μια παλέτα με κιβώτια που έχουν RFID ετικέτες μπορεί να αναγνωριστεί είτε από ένα αναγνώστη που βρίσκεται σε μια πύλη ή από μια συσκευή ανάγνωσης χειρός. Στη συνέχεια το σύστημα διαχείρισης αποθήκης ή και το σύστημα διαχείρισης των παραγγελιών μπορεί να αντιστοιχήσει τα δεδομένα που έχουν αναγνωσθεί με αυτά της παραγγελίας του πελάτη, προκειμένου να βεβαιωθεί ότι κανένα κιβώτιο δεν έχει χαθεί και ότι οι ποσότητες είναι σωστές. Μια τελευταία αναγνώριση των ετικετών στην πόρτα εκφόρτωσης προσφέρει μια αναβάθμιση στη βάση δεδομένων και καταγράφει την αφαίρεση των εμπορευμάτων από το σύστημα αποθέματος.

Παρακολούθηση πάγιου εξοπλισμού

Η τοποθέτηση μιας RFID ετικέτας σε ένα εμπορευματοκιβώτιο ή μια παλέτα που συνοδεύει μια παραγγελία προς τον πελάτη, εξυπηρετεί την ιχνηλασιμότητα του εν λόγω εξοπλισμού όταν πρόκειται για πάγιο εξοπλισμό που επιστρέφεται και ξαναχρησιμοποιείται. Κατά αυτό τον τρόπο δημιουργείται μια ακριβής διαδρομή από πληροφορίες για την ανάκτηση του παγίου εξοπλισμού και τη διαχείριση τους πιο αποτελεσματικά. Παράδειγμα της χρήσης τον RFID ετικετών στην παρακολούθηση της θέσης του πάγιου εξοπλισμού, αποτελεί η εφαρμογή της εταιρίας Marks and Spencer. Η εταιρία χρησιμοποιεί συσκευές ανάγνωσης χειρός για να αναγνωρίζει τις RFID ετικέτες που έχουν τοποθετηθεί στον εξοπλισμό και διακινούνται μεταξύ των 6 διαφορετικών κέντρων διανομής. Η εταιρία χρησιμοποιεί πάνω από 4,5 εκατομμύρια RFID ετικέτες για τις διαδικασίες διακίνησης των προϊόντων της. Με την ακριβή ιχνηλασιμότητα του εξοπλισμού καθώς αυτά κινούνται μέσα στις εγκαταστάσεις και την εφοδιαστική αλυσίδα, η εταιρία βελτιώνει το σχεδιασμό της αυξάνοντας τη χρησιμοποίηση του εξοπλισμού και μειώνοντας το κόστος διαχείρισης.

Πέρα από τα πλεονεκτήματα που προσφέρει η τεχνολογία RFID στην παρακολούθηση του πάγιου εξοπλισμού μέσα από τις διαδικασίες logistics, ο εξοπλισμός της αποθήκης όπως τα παλετοφόρα, τα εργαλεία και λοιπές μηχανές, μπορούν να επωφεληθούν από τα πλεονεκτήματα της χρήσης των RFID ετικετών βελτιώνοντας τη διαφάνεια και τη διαθεσιμότητα, μειώνοντας τις απώλειες και παρέχοντας ακριβείς πληροφορίες για τη διαχείριση του εξοπλισμού.

Όπως διαφαίνεται στις παραπάνω αναφορές, υπάρχει πληθώρα εφαρμογών και χρήσεων της τεχνολογίας RFID στις λειτουργίες της αποθήκης και ενός κέντρου διανομής. Ως προς την προσαρμογή και υλοποίηση της τεχνολογίας RFID στην αποθήκη, πολλοί προμηθευτές hardware και software εξοπλισμού ερευνούν τον τρόπο με τον οποίο μπορούν να προσαρμόσουν τη RFID τεχνολογία στα διάφορα πληροφοριακά συστήματα για να παρέχουν πιο αποτελεσματική απόδοση στις λειτουργίες της αποθήκης. Έτσι

πολλά σύγχρονα WMS πλέον υποστηρίζουν και την RFID εισαγωγή δεδομένων στο λογισμικό τους.

1.7.3 Πλεονεκτήματα και μειονεκτήματα της RFID στην εφοδιαστική αλυσίδα

Καθώς οι διάφορες βιομηχανίες της εφοδιαστικής αλυσίδας (supply chain) συνεχίζουν να εργάζονται με γνώμονα τη συνεχή βελτίωση της ροής των πληροφοριών-δεδομένων μέσα στις γραμμές παραγωγής τους, αναπτύσσονται όλο και περισσότερο διάφορες εφαρμογές, προσφέροντας πολλά τεχνολογικά πλεονεκτήματα. Έτσι και η τεχνολογία RFID. λόγω του ότι προσφέρει περισσότερη διαφάνεια-ορατότητα (visibility) και αποτελεσματικότερη διαχείριση των δαπανών, θεωρείται μια από τις πλέον ενδιαφέρουσες επιλογές για την συλλογή δεδομένων και την αναγνώριση των προϊόντων στην εφοδιαστική αλυσίδα.

Παρακάτω παρατίθενται τα πλεονεκτήματα και τα μειονεκτήματα της τεχνολογίας RFID στην εφοδιαστική αλυσίδα.

Πλεονεκτήματα

- Συντόμευση των διαδικασιών και τη μείωση του συνολικού κόστους προσφοράς και παραγγελίας
- Καλύτερη ροή πληροφοριών
- Σημαντική αύξηση στην παραγωγικότητα της αποθήκης
- Καλύτερη αξιοποίηση των αποθηκευτικών χώρων
- Πλήρης έλεγχος του αποθηκευτικού κυκλώματος και την τεκμηριωμένη διοίκηση της εφοδιαστικής αλυσίδας
- Μείωση stock εμπορεύματος άρα την οικονομία κλίμακος που σχετίζεται με το προσωπικό της αποθήκης αλλά και με το κόστος της παραγωγικής διαδικασίας
- Έλεγχος και την αυτοματοποίηση της ροής πληροφορίας άρα τη μείωση των λειτουργικών εξόδων
- Μείωση απωλειών λόγω παλαίωσης των ειδών
- Δυνατότητα ανάκλησης και ανίχνευσης συγκεκριμένων παρτίδων
- Ακριβή καταμέτρηση του stock
- Βελτίωση του customer service
- Κατάργηση των χειρόγραφων δελτίων
- Διαχείριση ηλεκτρονικού καταλόγου

Μειονεκτήματα

- Ανάγκη ανασχεδιασμού και επέκτασης της υπολογιστικής υποδομής
- Υψηλό κόστος εξοπλισμού.

Προκειμένου να γίνουν κατανοητά τα οφέλη που μπορεί να απορρέουν από τη χρήση της τεχνολογίας RFID στις παλέτες και τα κιβώτια των προϊόντων, χρειάζεται να εξεταστεί η τρέχουσα διαδικασία και τί αλλάζει με την υιοθέτηση του RFID. Αυτό απαιτεί ένα ελαφρώς υψηλότερο επίπεδο λεπτομέρειας από την επισκόπηση που δίνεται ανωτέρω.

Η πλειοψηφία των οφελών προκύπτει από την αυτοματοποίηση των βημάτων των διαδικασιών που μέχρι σήμερα πραγματοποιούνται χειροκίνητα. Συχνά, αυτές οι διαδικασίες αφορούν το χειρωνακτικό έλεγχο των προϊόντων ή τον έλεγχο με την ανίχνευση γραμμωτού κώδικα. Σε μερικές περιπτώσεις, το RFID οδηγεί σε μια βελτιστοποίηση των τρεχουσών διαδικασιών ή σε νέες διαδικασίες. Υπάρχει περίπτωση οι κατασκευαστές να έχουν την εντύπωση ότι η πλειοψηφία των οφελών από την επικόλληση ετικετών RFID στα κιβώτια πηγαίνει μόνο στο λιανοπωλητή. Καθώς τα προϊόντα, και κατά συνέπεια τα κιβώτια που τα περιέχουν, αποτελούν διαχειριζόμενη μονάδα και των κατασκευαστών, ορισμένα οφέλη που προκύπτουν από την εφαρμογή ετικετών στα κιβώτια είναι και δικά τους οφέλη. Αυτό οφείλεται στο ότι οι ετικέτες RFID στα κιβώτια μπορούν να οδηγήσουν σε βελτιωμένη διαθεσιμότητα προϊόντων στο λιανοπωλητή και κατ' επέκταση σε αυξημένες πωλήσεις των προϊόντων με ό,τι αυτό συνεπάγεται.

Η τεχνολογία RFID μπορεί να χρησιμοποιηθεί σε πολλές διαφορετικές αποθήκες και κέντρα διανομής, στις διάφορες λειτουργίες διαχείρισης αποθεμάτων, συμπεριλαμβανομένων της παραλαβής και τοποθέτησης των εμπορευμάτων, της συλλογής και αποστολής των προϊόντων. Η τεχνολογία RFID παρέχει προοπτικές υψηλής επένδυσης, εφόσον η εφαρμογή της προσφέρει πλεονεκτήματα και λύσεις στα αναγνωρισμένα προβλήματα και περιορισμούς των προηγούμενων τεχνικών και προσδίδει τη δυνατότητα εφαρμογής νέων επιχειρηματικών διεργασιών.

Με τη χρήση της τεχνολογίας RFID. τα προϊόντα μπορούν να παρακολουθούνται και να αναγνωρίζονται σε όλες τις φάσεις των διαδικασιών μέσα στην αποθήκη, εκεί που άλλες εφαρμογές αδυνατούν λόγω περιβαλλοντικών περιορισμών κόστους. Προσφέροντας τη δυνατότητα κωδικοποίησης και χρήσης ασφαλών σειριακών αριθμών στις ετικέτες, αρχίζει να γίνεται εμφανής ο τρόπος με τον οποίο η τεχνολογία RFID μπορεί να οδηγήσει σε νέα επίπεδα διαφάνειας στη διαχείριση των αποθεμάτων και των λειτουργιών της εφοδιαστικής αλυσίδας. Μειώνοντας τόσο τα επίπεδα των αποθεμάτων, όσο και το χρόνο αποθήκευσης, τις δαπάνες διαχείρισης και το logistics.

Καθώς η τεχνολογία RFID προχωρεί σε περαιτέρω ανάπτυξη και εφαρμογές, θα υπάρξουν τεράστιες ευκαιρίες μέσα στην επόμενη δεκαετία για τους ερευνητές με τη μελέτη όχι μόνο της προόδου της τεχνολογίας αυτής, αλλά και την εξέταση των επιπτώσεων της στη μεγάλη ποικιλία προοπτικών και εφαρμογών. Πράγματι, αυτό αποτελεί μια τεράστια ευκαιρία αναξιοποίητης έρευνας, που σπάνια είχε παρατηρηθεί στο παρελθόν, δίνοντας τέτοιου είδους δείγματα από την απαρχή της δηλαδή την ξεχωριστή δυνατότητα που έχει να αναμορφώσει ριζικά τον επιχειρηματικό κόσμο και

την οικονομία γενικότερα κατά τουλάχιστον μια δεκαετία και πέραν αυτής. Υπάρχουν τρία μεγάλα πεδία επιπλέον έρευνας για τους ερευνητές σε ό.τι αφορά την τεχνολογία RFID. Το πρώτο πεδίο αποτελείται από την εξέταση και έρευνα των περιοχών που ήδη εφαρμόζεται και χρησιμοποιείται σήμερα η εν λόγω τεχνολογία από τις εταιρίες. Μια τέτοια έρευνα θα μπορούσε να εμπεριέχει τα εξής πεδία, χωρίς αυτό να αποτελεί και περιορισμό για περαιτέρω έρευνα και σε άλλους τομείς εφαρμογής:

- Μεταφορές και logistics
- Διοίκηση εφοδιαστικής αλυσίδας
- Διοίκηση λειτουργιών
- Διοίκηση υγειονομικής περίθαλψης
- Σχεδιασμός επιχειρηματικών- παραγωγικών διαδικασιών .

Η έμφαση της έρευνας αυτής θα είναι, για το εγγύς μέλλον, προς την εξής κατεύθυνση: της ανακάλυψης και της εξέτασης ορθών πρακτικών στη χρήση και εφαρμογή της τεχνολογίας RFID καθώς επίσης και της δυναμικής για πολλαπλή αξιοποίηση των εννοιών αυτών σε διαφορετικά περιβάλλοντα.

Βραχυπρόθεσμα, μεγάλο μέρος της ερευνητικής δραστηριότητας στον τομέα αυτό θα βρίσκεται σε πρώιμο επίπεδο. Για τα επόμενα πέντε έως δέκα ετών-ίσως και πλέον, θα υπάρχει μεγάλη ανάγκη για μια πιο επισταμένη και βαθιά έρευνα σχετικά με το πώς η τεχνολογία RFID μπορεί να χρησιμοποιηθεί σε περισσότερες εφαρμογές. Για αυτό το σκοπό είναι αναγκαίο να δοθεί απάντηση σε θεμελιώδη ερωτήματα, όπως:

- Πώς και πού θα πρέπει να εφαρμόζονται οι ετικέτες σε παλέτες, κιβώτια, και μεμονωμένα αντικείμενα ώστε να μεγιστοποιείται η αναγνωσιμότητα τους;
- Πώς θα πρέπει οι μεμονωμένοι RFID αναγνώστες να τοποθετούνται έτσι ώστε να μεγιστοποιείται η ικανότητα τους να σαρώνουν τις ετικέτες, καθώς και πώς θα πρέπει οι συστοιχίες των αναγνωστών να εγκαθίστανται ώστε να εξασφαλίζεται;
- Τι μπορεί να γίνει για να αμβλυνθούν οι επιπτώσεις των μετάλλων, των υδάτων και άλλων περιβαλλοντικών όρων στην ικανότητα ανάγνωσης των ετικετών;

Βέβαια, το μεγαλύτερο μέρος της έρευνας αυτής διεξάγεται από τις ίδιες τις εταιρίες, επιβαρυνόμενες οι ίδιες το κόστος, μιας και τέτοιου είδους έρευνα έχει σκοπό την βελτίωση και ανάπτυξη των δικών τους λειτουργιών. Αυτό που είναι επιθυμητό σήμερα αλλά και μελλοντικά είναι να παραμείνει ανοιχτή και συνεχής η επικοινωνία τόσο των εταιριών όσο και των κυβερνητικών υπηρεσιών στην ανταλλαγή βέλτιστων πρακτικών και εμπειριών με την ευρύτερη κοινότητα RFID. μέσω παρουσιάσεων και γραπτών εκθέσεων (μελέτες περιπτώσεων) καθώς με αυτόν τον τρόπο διαμορφώνονται και επίσημα τα στάδια της RFID επανάστασης. Ένα από τα χαρακτηριστικά της ανάπτυξης της RFID τεχνολογίας μέχρι σήμερα, που θεωρείται και το σήμα κατατεθέν της είναι η προθυμία των εταιριών, των στελεχών και των ακαδημαϊκών φορέων να μοιραστούν την ερευνητική τους δραστηριότητα, τις εμπειρίες και τα συμπεράσματα των βέλτιστων πρακτικών τους.

Όσον αφορά στο δεύτερο πεδίο έρευνας, οι ερευνητές θα μπορούσαν να επιστήσουν την προσοχή τους στον αντίκτυπο της RFID στις επιχειρηματικές διαδικασίες και πώς αυτές επηρεάζουν τους οργανισμούς-επιχειρήσεις γενικότερα.. Η δεύτερη κατηγορία της έρευνας θα εξετάσει τον αντίκτυπο της RFID που μπορεί και έχει στην ευρύτερη εικόνα των οργανισμών-επιχειρήσεων τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα. Η έρευνα θα μπορούσε να επεκταθεί σε τομείς που περιλαμβάνουν:

- Διοίκηση στρατηγικών
- Διοίκηση της τεχνολογίας
- Διοίκηση πληροφοριακών συστημάτων
- Επιχειρησιακή συνείδηση
- Οικονομική διοίκηση
- Διοίκηση της γνώσης.

Η περιοχή αυτή της έρευνας θα επικεντρωθεί στον τρόπο με τον οποίο η RFID τεχνολογία θα επηρεάσει τους οργανισμούς, τόσο σε σχέση με τα εσωτερικά τους συστήματα / λειτουργίες / δυνατότητες όσο και στις ενδοεπηχειρησιακές τους σχέσεις. Σύμφωνα με την τελευταία αυτή άποψη, η έρευνα θα πρέπει να μην εστιάζει μόνο στις σχέσεις μέσα στην εφοδιαστική αλυσίδα, αλλά και το πώς επηρεάζει η ανταλλαγή δεδομένων σε πραγματικό χρόνο όλους τους τομείς, όπως τη παροχή υπηρεσιών, τη χρηματοδότηση και τις πληρωμές, καθώς και την εξυπηρέτηση των πελατών.
Τέλος, το επίκεντρο της έρευνας που αποτελεί και τον τρίτο πεδίο αναφοράς θα μπορούσε να είναι οι συνέπειες της τεχνολογίας RFID για τους ανθρώπους, τις διεργασίες, και την κοινωνία . Αυτό περιλαμβάνει, αλλά δεν πρέπει να περιοριστεί σε τομείς όπως:

- Δεοντολογία / Ιδιωτικότητα
- Επιχειρήσεις και την κοινωνία
- Επιχειρηματικό δίκαιο
- Διοίκηση ανθρώπινων πόρων.

Ο τελευταίος τομέας της έρευνας θα μπορούσε να χαρακτηριστεί ως «οι διακλαδώσεις και παραλλαγές» της RFID καθώς επικεντρώνεται στον αντίκτυπο της στην κοινωνία, τις επιχειρήσεις, το δίκαιο, την προστασία της ιδιωτικής ζωής, και τη δεοντολογία.

Το πεδίο αυτό έρευνας περιλαμβάνει την έρευνα για το πώς η τεχνολογία RFID προκαλεί και αλλάζει τα όρια, τους κανόνες και τους νόμους σε συγκεκριμένους τομείς των επιχειρήσεων, της κυβέρνησης, και της κοινωνίας. Μπορεί μερικές φορές να είναι αντιφατική και να φέρει στο φως ποικίλες προοπτικές για τις επιπτώσεις αυτής της νέας τεχνολογίας. Συμπερασματικά, η τεχνολογία RFID αποτελεί έναν σπινθήρα στη μεγάλη ερευνητική δραστηριότητα, καθώς είναι πολλά υποσχόμενη με κάθε τομέα να συμπληρώνει και να βοηθάει στην οικοδόμηση των θεμελίων της σημερινής RFID επανάστασης.

1.7.4 Οι ανασταλτικοί παράγοντες της τεχνολογίας RFID

Παρ' όλα τα οφέλη που μπορούν να επέλθουν για. την επιχείρηση με την εφαρμογή της τεχνολογίας RFID. στην πράξη υπάρχουν πολλά προβλήματα που λειτουργούν ανασταλτικά στην υιοθέτηση ενός τέτοιου συστήματος. Για αυτό το λόγο πολλές επιχειρήσεις τηρούν στάση αναμονής παρακολουθώντας τις εξελίξεις στην τεχνολογία RFID. Αναλυτικότερα οι παράγοντες που παίζουν ανασταλτικό ρόλο μπορούν να διακριθούν στις παρακάτω δυο κατηγορίες :

- **Τεχνολογικοί περιορισμοί**

Πολλές από τις αρχικές πιλοτικές εφαρμογές σχεδιάστηκαν με βάση υπερεκτιμημένες δυνατότητες των συστημάτων RFID. Για παράδειγμα, είχε προβλεφθεί ότι η συσκευασία της παλέτας και η καταγραφή των περιεχομένων προϊόντων από ένα σύστημα RFID θα αρκούσε για την διαδικασία της προετοιμασίας και αποστολής μιας παραγγελίας. Στην πράξη όμως αυτό δεν είναι εφικτό: ένα σύστημα RFID δεν μπορεί ακόμα να καταγράψει αξιόπιστα τα περιεχόμενα μίας παλέτας. Στις τρέχουσες εφαρμογές, τα συστήματα RFID χρησιμοποιούνται μόνο για την επιβεβαίωση περιεχομένου παλετών.

Η μη εκπλήρωση των υψηλών προσδοκιών οφείλεται κυρίως σε προβλήματα τεχνικής φύσεως που αναδείχθηκαν κατά την εφαρμογή της τεχνολογίας.

- **Μη συμβατότητα προτύπων**

Για να λειτουργήσει ένα RFID σύστημα σε μια εφοδιαστική αλυσίδα, απαιτείται όλοι οι εμπλεκόμενοι να χρησιμοποιούν κοινά πρότυπα. Όμως δεν υπάρχει ένα κοινό πρότυπο για τις ετικέτες και τους αναγνώστες και οι συχνότητες λειτουργίας διαφέρουν: υπάρχουν προϊόντα που λειτουργούν σε UHF και σε HF. Έτσι, δεν μπορεί να είναι κανείς σίγουρος ότι μια ετικέτα θα αναγνωστεί σε όλο το μήκος της εφοδιαστικής αλυσίδας. Ακόμα και με την εισαγωγή του διεθνούς προτύπου Gen2 το 2004, η επικοινωνία μεταξύ των προϊόντων RFID παραμένει δύσκολη. Η Ευρωπαϊκή Ένωση έχει ορίσει για τις επιχειρήσεις ένα εύρος Ccovnc UHF (2MHz") πολύ μικρότερο από αυτό της Αμερικής (26MHZ). Από αυτή την ασυμβατότητα προκύπτουν προβλήματα ευελιξίας και κόστους: αν μια εταιρία τροφίμων που έχει επενδύσει σε τεχνολογία UHF λάβει οδηγία από κάποιον πελάτη της στο εξωτερικό να παραδίδει τις παλέτες με RFID σε HF. θα χρειαστεί να επενδύσει εκ νέου σε εξοπλισμό. Η παρούσα κατάσταση που επικρατεί στα πρότυπα δημιουργεί σοβαρή σύγχυση, δημιουργώντας συστήματα μη συμβατά μεταξύ τους. Για παράδειγμα, μία συσκευή ανάγνωσης δεν μπορεί να διαβάσει ετικέτες που προέρχονται από διαφορετικό κατασκευαστή. Η προτυποποίηση θα επιτρέψει την επικοινωνία ετικετών και συσκευών ανάγνωσης που προέρχονται από διαφορετικούς προμηθευτές. Η ύπαρξη κοινών προτύπων θα παίξει σημαντικό ρόλο στην ευρεία

αποδοχή της τεχνολογίας από τις επιχειρήσεις και θα συντελέσει στην πτώση του συνολικού κόστους της.

- **Ιδιαιτερότητες υλικών**

Τα προϊόντα RFID είναι ηλεκτρομαγνητικές συσκευές. Η πληροφορία μεταφέρεται με ΗΜ κύματα, η διάδοση των οποίων εξαρτάται από παράγοντες όπως από το υλικό πάνω στο οποίο είναι προσκολλημένες οι ετικέτες, από το υλικό που παρεμβάλλεται και από την ύπαρξη ΗΜ θορύβου. Για παράδειγμα, τα μέταλλα και τα υγρά δυσχεραίνουν την επικοινωνία των ετικετών με τις κεραίες των αναγνωστών.

- **Δυσκολίες εγκατάστασης και λειτουργίας**

Στην περίπτωση των barcodes, η προετοιμασία για μια εγκατάσταση μπορεί να περιοριστεί στην εξασφάλιση της οπτικής επαφής μεταξύ αναγνώστη και barcode και στον συνυπολογισμό της ταχύτητας με την οποία κινείται το barcode ως προς τον αναγνώστη. Αντίθετα, στις εφαρμογές RFID απαιτείται επί τόπου επίσκεψη, δοκιμές με τα προτεινόμενα υλικά, δοκιμαστικές τοποθετήσεις εξοπλισμού (αναγνώστες, δικτύωση) και πιθανόν η διεξαγωγή μιας πιλοτικής εφαρμογής. Όσον αφορά στην λειτουργία, οι ετικέτες RFID δεν είναι τόσο "ανεκτικές" στην κακομεταχείριση όσο οι ετικέτες barcodes: το τσάκισμα μιας ετικέτας RFID μπορεί να σημάνει την πλήρη καταστροφή της πληροφορίας, ενώ κάτω από τις ίδιες συνθήκες μια ετικέτα barcode παραμένει αναγνώσιμη.

Πολλά από τα παραπάνω προβλήματα μπορούν να λυθούν με την τοποθέτηση των αντικειμένων με συγκεκριμένο τρόπο, έτσι ώστε να λειτουργεί αποτελεσματικά το σύστημα π.χ. το πρόβλημα ανάγνωσης σε κιβώτιο που περιέχει μπουκάλια με υγρό περιεχόμενο μπορεί να λυθεί με τη τοποθέτηση της ετικέτας στο επάνω μέρος του κιβωτίου.

Τέλος, οι συνεχείς αλλαγές στην τεχνολογία RFID λειτουργούν ανασταλτικά στην υιοθέτηση της από τις επιχειρήσεις. Λόγω των συχνών αλλαγών και αναμένοντας την τεχνολογία δεύτερης γενιάς, οι επιχειρήσεις φοβούμενες ότι θα απαρχαιωθεί και θα αχρηστευθεί ο τεχνολογικός εξοπλισμός που θα αγοράσουν δεν εφαρμόζουν συστήματα RFID. Το πρόβλημα αυτό μπορεί να λυθεί εάν οι επιχειρήσεις εξοπλιστούν με ετικέτες και συσκευές ανάγνωσης που μπορούν να αναβαθμιστούν, έτσι ώστε να μπορούν να λειτουργούν και στο μέλλον.

- **Επιχειρηματικοί περιορισμοί**

Ο αρχικός σχεδιασμός της ανάπτυξης της τεχνολογίας RFID έγινε με βάση την υπόθεση ότι η ζήτηση θα μείωνε σταδιακά τα κόστη της τεχνολογίας. Όμως, οι παραπάνω τεχνικοί περιορισμοί καθυστερούν την πτώση των τιμών που απαιτείται για την ευρύτερη αποδοχή της. Ενώ η έρευνα σήμερα προσανατολίζεται στις λύσεις αυτών των τεχνικών ζητημάτων, οι επιχειρήσεις που εξετάζουν το ενδεχόμενο υλοποίησης ενός

συστήματος RFID προβληματίζονται κυρίως από τον παράγοντα «κόστος», ο οποίος σχετίζεται με την απόκτηση και λειτουργία του απαιτούμενου εξοπλισμού.

- **Μη βέλτιστη σχέση κόστους /οφέλους**

Για εταιρίες κολοσσούς όπως η Wal-Mart, έχει αποδειχθεί ότι η διαχείριση αποθεμάτων με την χρήση RFID μπορεί να μειώσει τα κόστη διευκολύνοντας τις διαδικασίες παραλαβών και αποστολών. Για τους προμηθευτές της Wal-Mart όμως, και γενικά για όσες επιχειρήσεις τροφίμων προμηθεύουν με προϊόντα αλυσίδες λιανεμπορίου, τα οφέλη είναι λιγότερο εμφανή, ειδικά για όσες εταιρίες έχουν ήδη επενδύσει σε συστήματα barcode.

- **Υψηλό κόστος απόκτησης και λειτουργίας**

Οι εφαρμογές RFID έχουν υψηλότερο κόστος λειτουργίας. Οι πρώτες εφαρμογές σχεδιάστηκαν με την προϋπόθεση ότι οι ετικέτες RFID θα κόστιζαν έως και 5 cents. Επτά χρόνια μετά. τα 5 cents παραμένουν ζητούμενο, ενώ το αντίστοιχο κόστος για μια ετικέτα barcode είναι 0,2 cents. Πέρα από το κόστος της ετικέτας εμπεριέχει και το κόστος απόκτησης των πομποδεκτών. Αυτό σημαίνει ότι μια ενδεχόμενη επέκταση εφαρμογής RFID θα αυξήσει πολύ περισσότερο το συνολικό κόστος.

- **Κουλτούρα**

Σύμφωνα με μία μελέτη, ο δεύτερος σημαντικότερος παράγοντας που συμβάλει στην καθυστέρηση διάδοσης της τεχνολογίας RFID. μετά τα τεχνολογικά προβλήματα, είναι τα προβλήματα κουλτούρας. Το 30% των ερωτηθέντων μιας έρευνας φοβάται τις αλλαγές που θα επέλθουν στο εσωτερικό της επιχείρησης. Πολλές επιχειρήσεις αδυνατούν να προσαρμόσουν την οργανωσιακή τους κουλτούρα στις ανάγκες ενός συστήματος RFID.

- **Κατάρτιση ανθρώπινου δυναμικού**

Η εισαγωγή ενός συστήματος RFID επιφέρει σημαντικές αλλαγές στις διαδικασίες παραλαβών, αποθήκευσης και αποστολής των προϊόντων, οι οποίες επηρεάζουν τις μέχρι τώρα καθημερινές εργασίες των εργαζομένων. Επιπλέον, είναι δυνατόν να απαιτηθεί καταρτισμένο ανθρώπινο δυναμικό. Για τη μετάβαση λοιπόν σε ένα σύστημα RFID. απαιτείται εκπαίδευση του υπάρχοντος ανθρώπινου δυναμικού και πιθανόν επένδυση σε νέο.

- **Απουσία οφέλους μετάβασης από barcode σε RFID**

Από την άλλη πλευρά, η ταυτοποίηση προϊόντων με χρήση barcode είναι ακριβής σε ποσοστό 99.90%. Με την χρήση RFID το ποσοστό αυτό μπορεί, υπό προϋποθέσεις, να ανέβει σε 99.99%. Αναρωτιέται κανείς, εάν μία βελτίωση της τάξης του 0.09% επαρκεί για να δικαιολογήσει το κόστος της εισαγωγής μιας νέας τεχνολογίας. Πόσο μάλιστα που στην πράξη αποδεικνύεται ότι το RFID δεν είναι όσο αξιόπιστο είναι το barcode.

1.7.5 Οι κίνδυνοι την άκριτης χρήσης της RFID τεχνολογίας

Όπως και οι περισσότερες άλλες τεχνολογίες, έτσι και τα RFID συστήματα έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους. Στις πιο κοινές εφαρμογές, οι παθητικές RFID ετικέτες κάνουν δυνατό και γρήγορο τον προσδιορισμό του αύξοντα αριθμού των ετικετών (χωρίς να είναι αναγκαία η επαφή) συμβάλλοντας έτσι στη μείωση εσφαλμένων αναγνωρίσεων. Ωστόσο, η τεχνολογία αυτή μπορεί να καταστεί επικίνδυνη όταν ο δεσμός μεταξύ της ετικέτας και του περιεχομένου χρήσης της είναι υπό αμφισβήτηση. Η κατάσταση αυτή είναι παρόμοια με αυτήν των Social Security Numbers, τα οποία είναι χρήσιμα ως στοιχεία αναγνώρισης, αλλά όχι ως στοιχεία γνησιότητας, με ένα ευρύ φάσμα αποδεδειγμένων καταχρήσεων να έχει καταγραφεί.

Τα RFID οφέλη μπορούν να εξουδετερωθούν πολύ εύκολα με τυχαία ή εκ προθέσεως κατάχρηση της τεχνολογίας και των συστημάτων υποστήριξης της. Ένα ευρύ φάσμα θεμάτων που σχετίζονται με το σύστημα και την ακεραιότητα των δεδομένων, την προσωπική ευημερία, την ασφάλεια και την ιδιωτική ζωή βρίσκονται σε κίνδυνο. Οι ετικέτες μπορούν να παραποιηθούν, κλωνοποιηθούν, αναστραφούν, καταστραφούν εκ προθέσεως (σε ορισμένες περιπτώσεις ακόμη και εξ αποστάσεως), ή να αποτελέσουν αντικείμενο κατάχρησης. Η τεχνολογία RFID μπορεί να λειτουργήσει εξίσου αποτελεσματικά ακόμη και σε επισφαλή συστήματα. Αυτό είναι ιδιαίτερα προβληματικό σε ευαίσθητα περιβάλλοντα αν γίνει χρήση RFID ετικετών ή πρωτοκόλλων χωρίς ή με ασθενή κρυπτογράφηση.

Πολλά θέματα ιδιωτικού απορρήτου που υπάρχουν, μερικά από τα οποία μπορεί να έχουν σοβαρές συνέπειες, έχουν αγνοηθεί ή υποβαθμιστεί ως δευτερεύοντα.. Έρευνες δείχνουν ότι ακόμα και παθητικές RFID ετικέτες μπορεί να αναγνωστούν από πολύ μεγαλύτερες αποστάσεις από ό,τι είχε αρχικά προβλεφθεί. Οι συνέπειες από αυτά τα προβλήματα είναι τεράστια για τα άτομα που φέρουν πιστωτικές κάρτες ή διαβατήρια, που κάνουν χρήση της εν λόγω τεχνολογίας, και κυρίως για άτομα με ενσωματωμένα υποδόρια εμφυτεύματα RFID που δεν θα έχουν καμία δυνατότητα ελέγχου από πού και πότε τα εμφυτεύματα μπορούν να αναγνωστούν.

Επιπλέον, διάφορα ζητήματα που σχετίζονται με τα διάχυτα προβλήματα ασφάλειας μπορεί να οδηγήσουν σε αύξηση των παραβάσεων της ιδιωτικής ζωής που διαπράττονται από ξένους που κατέχουν εμπιστευτικές πληροφορίες, όπως είναι η κακή χρήση των βάσεων δεδομένων που σχετίζονται με την ετικέτα RFID ή πληροφορίες που προέρχονται από το περιεχόμενο στο οποίο χρησιμοποιούνται οι ετικέτες. Παραδείγματα

που σχετίζονται με το σύστημα είναι: οι εγγενείς ευπάθειες ασφαλείας των βοηθητικών συστημάτων του υπολογιστή, ο ανεπαρκής έλεγχος ταυτότητας χρήστη και φορέα, και η υπερβολικά ευρεία βάση δεδομένων και του συστήματος αδειών. Τέτοιες καταστάσεις μπορεί να δημιουργήσουν ευκαιρίες για ανεξέλεγκτη κατάχρηση των πληροφοριών της βάσης δεδομένων. Υπάρχουν πολλές περιπτώσεις αύξησης τέτοιου είδους θυμάτων, με ευρεία ή επιλεκτική «εξόρυξη» δεδομένων, μέχρι και ολόκληρη σάρωση βάσεων δεδομένων. Πιθανές προθέσεις για μια τέτοια κακή χρήση θα μπορούσε για παράδειγμα, να. περιλαμβάνει τη ληστεία, την κλοπή ταυτότητας, την απάτη, την παρενόχληση και τον εκβιασμό.

Με το εύρος των πιθανών προβλημάτων που συνδέονται με τα συστήματα RFID. το ζήτημα της εθελοντικής έναντι της ακούσιας χρήσης της γίνεται υψίστης σημασίας. «Όταν κάτι πάει στραβά, κάποιος είναι πιθανό να επιβαρυνθεί οικονομικά ή με άλλους τρόπους». Είναι πιθανό λοιπόν η ακούσια, εμφύτευση μικροτσίπ σε ανυποψίαστους ανθρώπους να δικαιολογείται στο εγγύς μέλλον από την κοινωνία, τις οργανώσεις και τις αρχές προφασιζόμενες την ασφάλεια, οικονομικούς, ή άλλους φαινομενικά αξιέπαινους στόχους.

Σε επίπεδο τεχνολογικής επιστήμης, η ανεπαρκής ασφάλεια στα. λειτουργικά συστήματα, τα συστήματα διαχείρισης βάσεων δεδομένων, τη δικτύωση κ.α, που υποστηρίζουν τη χρήση της τεχνολογίας RFID. οδηγεί στην απολύτως απαραίτητη και επιτακτική περαιτέρω βελτίωση τους. Συνεπείς, σωστές και ενημερωμένες βάσεις δεδομένων είναι ουσιαστικής σημασίας για τη διαθεσιμότητα του συστήματος και την ικανότητα επιβίωσης του. Πολλές προσπάθειες στον τομέα Έρευνας και Ανάπτυξης μπορεί να είναι χρήσιμες, αν και αυτές δεν περιορίζονται στις συνέπειες της τεχνολογίας RFID. Ιδιαίτερα είναι αναγκαία η ανάπτυξη αξιόπιστων συστημάτων, με κατάλληλη ασφάλεια, λογοδοσία, έλεγχο, που δεσμεύουν την ακεραιότητα, την προστασία της ιδιωτικής ζωής, τη διατήρηση της κρυπτογράφησης, και ούτω καθεξής.

Οι RFID τεχνολογίες μπορούν να έχουν σημαντικά πλεονεκτήματα σε ορισμένες καταστάσεις όταν οροθετούνται προσεκτικά. Ωστόσο, σε όλες τις περιπτώσεις, τεχνικοί κίνδυνοι καθώς και κίνδυνοι παραβίασης της ιδιωτικότητας πρέπει να λογιστούν ως αντικειμενικοί και υπαρκτοί στα επιχειρησιακά περιβάλλοντα.

Ακόμη πιο σημαντικό και ζωτικής σημασίας είναι να ξεκινήσει σήμερα ένας εκτεταμένος, σε ολόκληρη την κοινωνία, διάλογος σχετικά με τις συνθήκες και τα περιβάλλοντα εντός των οποίων τα συστήματα RFID πρέπει ή δεν πρέπει να χρησιμοποιούνται, και τα δικαιώματα των ατόμων και των οργανώσεων να ελέγχουν αν θα υπόκεινται ή όχι σε διάφορες χρήσεις των συστημάτων αυτών. Αυτό είναι ένα ιδιαίτερα δύσκολο έργο, διότι πολλές από τις υποτιθέμενες εφαρμογές μπορεί να είναι συναισθηματικά φορτισμένες, και οι RFID δυνατότητες και οι δήθεν παροχές σε ορισμένες περιπτώσεις να μεγεθύνονται κατά πολύ από αυτό που είναι ρεαλιστικό. Ωστόσο, είναι τόσο κρίσιμα αυτά τα θέματα που είναι πιθανό να επηρεάσουν το αν η RFID θα αναπτυχθεί κυρίως ως χρήσιμο εργαλείο, ή ως μέσο κατάχρησης.

- **Πιθανά προβλήματα ασφαλείας από τη χρήση της τεχνολογίας RFID**

Οι ετικέτες RFID που χρησιμοποιούνται στην εφοδιαστική αλυσίδα περιέχουν δεδομένα όπως οι απλοί αριθμοί αναγνώρισης (EPC) αλλά και οι σημαντικότερες πληροφορίες για ένα προϊόν. Για παράδειγμα, στον κλάδο της υγείας, θα μπορούσε να είναι ο τύπος αίματος ενός δείγματος. Ο κύριος στόχος ασφάλειας οποιουδήποτε συστήματος που έχει σκοπό να προστατεύσει τις πληροφορίες που αποθηκεύονται στα διάφορα μέσα αποθήκευσης που χρησιμοποιούνται, όπως οι ετικέτες, οι δίσκοι των υπολογιστών, ή οι έξυπνες κάρτες, είναι βασικά να αποτραπεί οποιοδήποτε αναρμόδιο πρόσωπο από το να:

α) αποκτήσει πρόσβαση και να μάθει το περιεχόμενο των πληροφοριών,
β) αποκτήσει πρόσβαση και να παραποιήσει, να προσθέσει ή να διαγράψει δεδομένα.
γ) αντιγράψει το περιεχόμενο των πληροφοριών.

Σε ένα ολοκληρωμένο σύστημα, η ασφάλεια των δεδομένων όπως περιγράφηκε παραπάνω, συμπεριλαμβάνει όχι μόνο το μέσο αποθήκευσης, αλλά και τον τρόπο που τα δεδομένα δημιουργούνται και μεταφέρονται από την κεντρική μονάδα διαχείρισης στο αποθηκευτικό μέσο (ή αντίστροφα). Παραδείγματος χάριν, όταν ένας μηχανικός «έσπασε» την ασφάλεια μιας πιστωτικής κάρτας γαλλικής τράπεζας μερικά χρόνια πριν το έκανε όχι αποκωδικοποιώντας το αντίστοιχο τσιπ ασφαλείας, αλλά με την παραβίαση των κωδικών ασφαλείας του τερματικού ανάγνωσης todv καρτών (ATM).

Τα ακόλουθα είναι σενάρια παρανομίας και γενικά μη εξουσιοδοτημένης χρήσης που θα μπορούσαν να συμβούν στην εφοδιαστική αλυσίδα:

1) Σαμποτάζ: κάποιος που είναι αντίθετος με τις δραστηριότητες μιας επιχείρησης μπορεί να παραποιήσει τα δεδομένα στις ετικέτες χρησιμοποιώντας μια χειροκίνητη συσκευή και να σβήσει ή να τροποποιήσει το περιεχόμενο τους.

2) Κατασκοπεία: ένας ανταγωνιστής μπορεί να επιθυμεί να μάθει πόσα και τι είδους προϊόντα κατασκευάζει και δρομολογεί ο «αντίπαλος» του. Θα μπορούσε ενδεχομένως να μάθει αυτά που τον ενδιαφέρουν με τους ακόλουθους παράνομους τρόπους:
α) Κρυφακούγοντας, να ακούσει μέσα από τηλεπικοινωνιακά συστήματα μεγάλου εύρους, όπως το UHF, που μεταδίδουν ραδιοφωνικά σήματα (αν και συνήθως αυτά είναι αρκετά αδύναμα) σε αποστάσεις μέχρι 100 μέτρων.
β) Τοποθετώντας καλά κρυμμένες συσκευές ανάγνωσης που θα συνδέονται με έναν Η/Υ κάπου εντός του εύρους των ετικετών που κινούνται μέσω της γραμμής παραγωγής.
γ) Χρησιμοποιώντας διάφορες άλλες χειροκίνητες συσκευές.

3) Πλαστογράφηση: κάποιος μπορεί να επιδιώξει να διαβάσει τα στοιχεία που αναγράφονται σε μια ετικέτα και τα οποία προσδιορίζουν μοναδικά ή πιστοποιούν την ταυτότητα ενός προϊόντος. Μόλις τα στοιχεία αυτά γίνουν γνωστά, ο «πλαστογράφος»

θα μπορούσε να αγοράσει παρόμοιες ετικέτες ανάγνωσης / γραφής και να τις ενημερώσει με αυθεντικά στοιχεία, δημιουργώντας έτσι πλαστά προϊόντα τα οποία θα προστατεύονται από μια γνήσια ετικέτα. Όλα τα παραπάνω σενάρια αποτελούν πιθανούς κινδύνους εάν δεν εφαρμόζεται καμία ασφάλεια στην ετικέτα και τη συσκευή ανάγνωσης RFID.

Η σημασία, προστασίας των δεδομένων κατά μήκος της εφοδιαστικής αλυσίδας θα εξαρτηθεί από την ίδια την εφαρμογή του RFID και τη στρατηγική που θα ακολουθήσουν οι επιχειρήσεις σχετικά με την ασφάλεια. Σε μερικές περιπτώσεις, ο τρόπος που θα γίνουν αυτά θα επιβληθεί από κατάλληλη νομοθεσία. Φυσικά, οι γραμμωτοί κώδικες που χρησιμοποιούνται σήμερα, μπορούν εύκολα να διαβαστούν, να αποκρυπτογραφηθούν ακόμη και να καταστραφούν, αλλά όχι τόσο αυτοματοποιημένα και σε τόσο μεγάλη κλίμακα όσο πιθανώς θα μπορεί να συμβεί με το RFID. Όμως. ακόμα και η απλούστερη μορφή ασφάλειας απαιτεί επιπλέον δαπάνες για τοποθέτηση πυριτίου στις ετικέτες, πράγμα που αυξάνει την τελική τιμή των ετικετών. Αυτό εμποδίζει τις πρόσφατες προσπάθειες που γίνονται να παραχθεί η φθηνότερη δυνατή ετικέτα. Κάθε επιχείρηση επομένως βρίσκεται αντιμέτωπη με το ζήτημα των φθηνότερων αλλά ακάλυπτων από άποψη ασφάλειας ετικετών και τους πιθανούς κινδύνους ασφάλειας που αυτό συνεπάγεται.

- **Θέματα ιδιωτικού απορρήτου**

Ένας από τους βασικούς φόβους των επικριτών της τεχνολογίας RFID είναι η ευρεία, εξάπλωση της και η δημιουργία με αυτόν τον τρόπο ενός ασύρματου δικτύου παρακολούθησης των δραστηριοτήτων όλων των πολιτών. Πιστεύουν ότι χρησιμοποιώντας ως «Δούρειο Ίππο» τις πρακτικές εφαρμογές των RFID οι εταιρίες θα δράσουν καταλυτικά για την εξάπλωση των ετικετών RFID με στόχο την παρακολούθηση και την κατάργηση των προσοοπικών ελευθεριών.

Η χρήση πάντως εμφυτευμάτων με μικροτσίπ ραδιοσυχνοτήκον έχει εγκριθεί από την αμερικανική Υπηρεσία Τροφίμων και Φαρμάκων, όταν συντρέχουν λόγοι ασφαλείας ή υγείας. Το εμφύτευμα είναι υποδόριο και περιέχει κωδικό αριθμό τον οποίο μπορεί να διαβάσει κάθε αρμόδιος σκανάροντας το μπράτσο του ατόμου. Ύστερα, ο κωδικός εισάγεται σε ένα κομπιούτερ και ανοίγει αυτόματα ο ατομικός φάκελος με τα προσωπικά δεδομένα.

Αξίζει να σημειωθεί ότι τελευταία, άρχισαν να λειτουργούν οι λεγόμενες ελεγχόμενες ζώνες δραστηριότητας «Safe zones», όπου οι γονείς εφοδιάζουν τα παιδιά τους με λουράκια στο χέρι που είναι εφοδιασμένα με μικροτσίπ RFID. ώστε να έχουν τον άμεσο έλεγχο των παιδιών τους σε περίπτωση που αυτό χαθεί ή απαχθεί.

Στον αντίποδα ο αντιπρόεδρος της Gillette, Dick Cantwell, είχε δηλώσει ότι οι ετικέτες RFID θα απενεργοποιούνται στο ταμείο των καταστημάτων μόνο όταν το ζητήσει ο πελάτης. Η σύγχυση αυτή στις δηλώσεις των εκπροσώπων των εταιριών ανησυχεί ιδιαίτερα τους επικριτές της τεχνολογίας RFID. Όσον αφορά στην ακτίνα δράσης των ετικετών RFID. η Alien Technology υποστηρίζει ότι σήμερα είναι της τάξης των 3-5 μέτρων. Μπορεί λοιπόν εύκολα να φανταστεί κανείς έναν κόσμο όπου ένα

αόρατο μάτι θα παρακολουθεί κάθε κίνηση. Όπου κάθε αντικείμενο, από την μπλούζα έως το περιεχόμενο μιας τσάντας, θα στέλνει, χάρη στην «ετικέτα-κατάσκοπο» που θα φέρει πληροφορίες του κατόχου της.

Από ό,τι φαίνεται ο «Μεγάλος Αδελφός» μοιάζει να έχει βρει ήδη αρωγούς κάποιες μεγάλες εταιρίες. Οι κατασκευαστές, βέβαια, δεν τις αποκαλούν «ετικέτες-κατασκόπους», αλλά «έξυπνες ετικέτες» ή αλλιώς «Ετικέτες Εντοπισμού με Ραδιοσυχνότητες - RFID». Υποστηρίζουν πως μοναδικός σκοπός τους είναι η «παρακολούθηση» όλων των προϊόντων, από το εργοστάσιο έως το ταμείο του καταστήματος, για τον καλύτερο έλεγχο των αποθεμάτων. Δεν πείθουν, ωστόσο, τις οργανώσεις για την προστασία των καταναλωτών και πιο συγκεκριμένα για την προστασία της ιδιωτικής ζωής (ή ιδιωτικότητας) των καταναλωτών.

Η πιο γνωστή τέτοια οργάνωση, είναι η CASPIAN, τα αρχικά της οποίας σημαίνουν «Καταναλωτές Εναντίον της Παραβίασης της Ιδιωτικότητας και της Αριθμοποίησης». Η επικεφαλής της, η Κάθριν Άλμπρεχτ (Katkerine Albreckt), έχει κηρύξει τον «πόλεμο» ενάντια σε πολυάριθμες εταιρίες. Ανάμεσα τους. η Gillette, η Benetton, η βρετανική αλυσίδα σούπερ μάρκετ Tesco, η αμερικάνικη αλυσίδα πολυκαταστημάτων Wal - Mart και πρόσφατα η γνωστή αλυσίδα Marcs & Spencer. Μαζί με την συνεργάτιδα, της, Liz Mcintyre, έγραψε το βιβλίο "SPYCHIPS" «Τσίπ Κατάσκοποι – Πως οι μεγάλες Εταιρίες και η κυβέρνηση θέλουν να καταγράψουν κάθε κίνηση σου με το RFID». Το βιβλίο κέρδισε το Νοέμβριο του 2005 το βραβείο Lysander Spooner για την βοήθεια που προσφέρει στην λογοτεχνία της ελευθερίας.

Τα θέματα ιδιωτικού απορρήτου που εγείρει η εφαρμογή της τεχνολογίας RFID τείνουν να καταδεικνύουν πως σε αρχικό τουλάχιστον επίπεδο, οι επιχειρήσεις δεν θα πρέπει να έχουν ως στόχο να παρέχουν end-to-end λύσεις στις οποίες συμμετέχει ενεργά ο τελικός καταναλωτής.

1.8 Το κόστος του απαιτούμενου εξοπλισμού

Το μεγαλύτερο πρόβλημα, μαζί με την έλλειψη κοινών προτύπων, για την επιτάχυνση της υιοθέτησης της τεχνολογίας RFID είναι το κόστος του εξοπλισμού. Όσον αφορά στις ετικέτες, οι περισσότερες εταιρίες που πωλούν RFID tags δεν αναφέρουν τιμές, αφού αυτές εξαρτώνται από τον όγκο των πωλήσεων, την ποσότητα μνήμης της ετικέτας και τη συσκευασία της (αν δηλαδή είναι κλεισμένη σε πλαστικό, ενσωματωμένη, κ.λπ.). Σε γενικές γραμμές, στις ΗΠΑ μια 96-bit ετικέτα EPC κοστίζει από 0,20 έως 0,40. Οι πομποί χαμηλής συχνότητας σε γυάλινες κάψουλες κοστίζουν περίπου 0,5 και σε πλαστική κάρτα και άνω, ενώ οι υψηλής συχνότητας κυμαίνονται από 0,5 έως . Πάντως, ο στόχος της EPCglobal για μαζική παραγωγή ετικετών κόστους 0,05 δεν φαντάζει εφικτός για το άμεσο μέλλον.

Οι περισσότεροι αναγνώστες UHF κοστίζουν από 500 έως 1000, ανάλογα με τα χαρακτηριστικά τους (οι τιμές τους πάντως αναμένεται να μειωθούν με την αύξηση της μαζικής ζήτησης από τις εταιρίες). Οι επιχειρήσεις θα πρέπει επίσης να αγοράσουν κάθε κεραία ξεχωριστά μαζί με τα καλώδια. Πιο προσιτοί είναι οι αναγνώστες χαμηλής και υψηλής συχνότητας.

ΚΕΦΑΛΑΙΟ 2

Ταξινόμηση Rfid Επιθέσεων

2.1 Εισαγωγή

Τα δίκτυα RFID υπάρχουν σε μια ευρεία σειρά περιβάλλοντων και η γρήγορη εξάπλωση τους είναι εν εξελίξει εδώ και αρκετό καιρό. Τα συστήματα RFID αποτελούνται από τα μικροσκοπικά ολοκληρωμένα κυκλώματα που εξοπλίζονται με ετικέτες T RFID, οι οποίες επικοινωνούν με τις συσκευές ανάγνωσής τους αναγνώστες R RFID χρησιμοποιώντας τους ηλεκτρομαγνητικούς τομείς σε μια από διάφορες τυποποιημένες ραδιοσυχνότητες. Επιπλέον, υπάρχει συνήθως μια back-end βάση δεδομένων που συλλέγει τις πληροφορίες σχετικές με τα φυσικά αντικείμενα που περιέχουν ετικέτα T.

Τα συστήματα RFID είναι τρωτά σε μια ευρεία σειρά κακόβουλων επιθέσεων . Αντίθετα από τα συνδεμένα με καλώδιο δίκτυα, όπου τα συστήματα υπολογισμού διαθέτουν και κεντρικά σχεδιασμένη και κατά χρήστη προστασία (πχ. Firewall) , οι επιθέσεις ενάντια στα δίκτυα RFID μπορούν να στοχεύσουν στα αποκεντρωμένα μέρη της υποδομής συστημάτων, δεδομένου ότι οι αναγνώστες και οι ετικέτες λειτουργούν σε ασταθές και ενδεχομένως θορυβώδες περιβάλλον.

Παρακάτω θα κατηγοριοποιήσουμε τις πιο κοινές επιθέσεις RFID σε στρώματα (περίπου σαν το ISO αλλά όχι ακριβώς τα ίδια στρώματα), θα παρουσιάσουμε απειλές και θα αναφέρουμε πιθανές πολιτικές άμυνες για κάθε στρώμα.

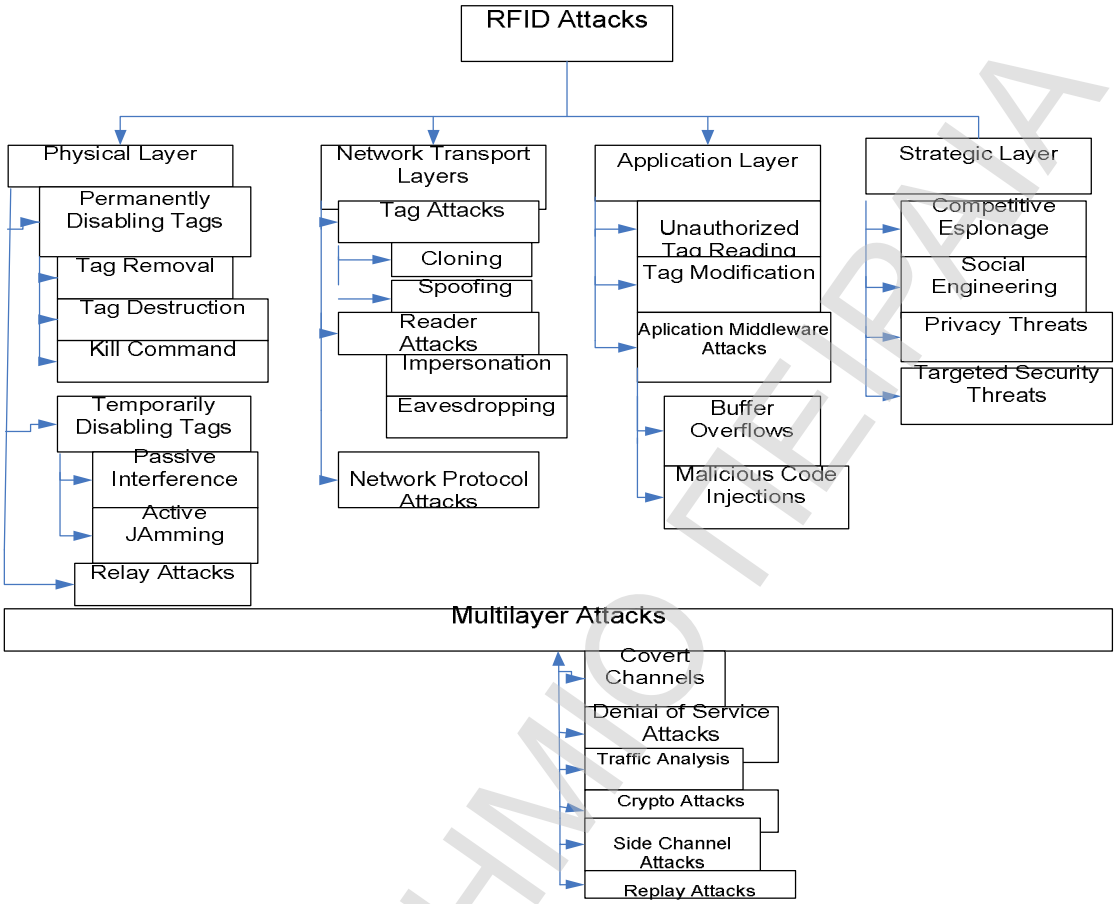
<table>
<tr><td colspan="2">Costs vs.Utility tradeoffs</td><td colspan="2">Logical Factors</td><td>Real-World constraints</td><td>Strategic LAyer</td></tr>
<tr><td colspan="2">APCIS/ ONS</td><td colspan="2">Oracle/ SAP</td><td colspan="2">Commercial/ enterprise middleware</td><td>Aplication Layer</td></tr>
<tr><td colspan="2">ISO 15693/ 14443</td><td colspan="2">EPC 800 Gen-2</td><td colspan="2">Proprietary RFID Protocols</td><td>Network-Transport Layer</td></tr>
<tr><td>RF</td><td colspan="3">Reader HW</td><td>RFID tags</td><td>Physical layer</td></tr>
</table>

Εικόνα 2.1: Στρώματα RFID επικοινωνίας

2.2 Κατηγοριοποίηση

Η κατηγοριοποίηση θα γίνει με βάση το στρώμα που λαμβάνει χώρα κάθε επίθεση, αναφέροντας και τα χαρακτηριστικά κάθε επίθεσης ενώ θα παρατεθούν και πιθανές λύσεις που μπορούν να χρησιμοποιηθούν ώστε να αντιμετωπιστούν αυτές οι επιθέσεις. Θα γίνει διαχωρισμός των επιθέσεων όπως φαίνεται στην εικόνα 2.1 στο φυσικό στρώμα (physical layer), στο στρώμα δικτύου και μεταφοράς (network-transport layer), στο στρώμα εφαρμογής (application layer) και στο στρατηγικό στρώμα (strategic layer), καθώς θα αναφερθούν και επιθέσεις που επιδρούν συγχρόνως σε παραπάνω του ενός στρώματα.

Ειδικότερα στο φυσικό στρώμα περιέχονται επιθέσεις που επηρεάζουν της ραδιοσυχνότητες (RF), το υλικό των αναγνωστών R και των ετικετών T ως φυσικές συσκευές. Στο στρώμα δικτύου-μεταφοράς περιγράφονται επιθέσεις οι οποίες εκμεταλλεύονται την δομή των RFID πρωτοκόλλων όπως τα πρότυπα ISO 15693/14443/18000, το EPC Gen-2 και άλλα ιδιόκτητα πρωτόκολλα. Στο στρώμα εφαρμογής συμπεριλαμβάνονται επιθέσεις που εκμεταλλεύονται τις ευπάθειες εμπορικών εταιρικών εφαρμογών όπως η Oracle, SAP η EPCIS/ONS Servers. Το στρατηγικό στρώμα σχετίζεται με λογιστικούς παράγοντες, με περιορισμούς του πραγματικού κόσμου και με συσχετίσεις όπως κόστος – χρησιμότητα. Σε αυτό το στρώμα εμπεριέχονται επιθέσεις οι οποίες εκμεταλλεύονται τις κρίσιμες πληροφορίες που συσχετίζονται με την παραγωγή, την οργάνωση και τις πολιτικές επέκτασης που υιοθετούνται στα ανταγωνιστικά επιχειρησιακά περιβάλλοντα καθώς επίσης και τη μυστικότητα και τις στοχοθετημένες απειλές ασφάλειας. Τέλος δημιουργούμε μια χωριστή κατηγορία πολυστρωματικών επιθέσεων που εκμεταλλεύονται τις ευπάθειες από παραπάνω από ένα στρώματα. Μια πιο λεπτομερής ταξινόμηση παρουσιάζεται στην εικόνα 2.



Εικόνα 2.2 Ταξινόμηση RFID επιθέσεων

2.3 Φυσικό στρώμα

Το φυσικό στρώμα στις επικοινωνίες RFID αποτελείται από τη φυσική διεπαφή και τις συσκευές RFID. Ο επιτιθέμενος σε αυτό το στρώμα εκμεταλλεύεται την ασύρματη φύση των επικοινωνιών RFID, της φτωχής φυσικής ασφάλειάς τους και της ανεπαρκούς ανθεκτικότητάς τους ενάντια στο συνεχή χειρισμό. Αυτό το στρώμα περιλαμβάνει τις επιθέσεις οι οποίες θέτουν μόνιμα ή προσωρινά εκτός λειτουργίας τις ετικέτες RFID καθώς επίσης και relay επιθέσεις.

2.3.1 Μόνιμη απενεργοποίηση Ετικέτας Τ

Η **μόνιμη απενεργοποίηση των RFID ετικετών** περιλαμβάνει όλους τους πιθανούς κινδύνους οι οποίοι έχουν ως αποτέλεσμα την ολική καταστροφή ή την ουσιαστική αλλοίωση της λειτουργίας της RFID ετικέτας. Πιθανοί τρόποι για να καταστεί μια ετικέτα μόνιμα μη λειτουργική είναι είτε η μετακίνηση της ετικέτας είτε η καταστροφή της ετικέτας είτε χρησιμοποιώντας την εντολή KILL.

Μετακίνηση ετικέτας Τ. Από τη στιγμή που οι RFID συσκευές παρέχουν φτωχή φυσική ασφάλεια, οι RFID ετικέτες που δεν είναι ενσωματωμένες μπορούν εύκολα να μετακινηθούν και να τοποθετηθούν αλλού (πχ. Αλλαγή RFID ετικετών που δείχνουν την τιμή του προϊόντος). Ένα χαρακτηριστικό παράδειγμα είναι η αλλαγή ετικετών σε κατάστημα με ρούχα όπου μπορεί κάποιος να αλλάξει τις ετικέτες RFID ενός ακριβού ρούχου με αυτή ενός φτηνού ρούχου. Αυτού του τύπου η εξαπάτηση είναι εύκολο να επιτευχθεί χωρίς κάποιος να έχει ειδικές γνώσεις.

Καταστροφή ετικέτας Τ. Με βάση την φτωχή φυσική ασφάλεια που προσφέρει, μια ετικέτα μπορεί εύκολα να καταστραφεί ακόμα και αν δεν υπάρχει κάποιο προφανές κέρδος για τον επιτιθέμενο. Ένας επιτιθέμενος που απλά τον ενδιαφέρει να αναστατώσει μια διαδικασία. Ακόμα και αν οι ετικέτες δεν καταστραφούν επίτηδες παραμένουν ευαίσθητες σε ακραίες περιβαντολλογικές συνθήκες και στην απροσεξία (λάθος χρήση) αυτού που τις χρησιμοποιεί. Οι RFID ετικέτες μπορούν εύκολα να γίνουν μη λειτουργικές βγάζοντας ή αλλάζοντας τις μπαταρίες της. Επιπλέον, οι RFID ετικέτες είναι πολύ ευαίσθητες στον στατικό ηλεκτρισμό. Τα ηλεκτρικά κυκλώματα των RFID ετικετών μπορούν να καταστραφούν ξαφνικά από ηλεκτρική δυσαναλογία λόγω κυμάτων υψηλής ενέργειας .

Εντολή KILL. Η Auto-ID center και η EPC global δημιούργησαν μια εντολή η οποία ονομάζεται KILL και η οποία είναι ικανή να σταματάει μόνιμα την RFID ετικέτα. Συμφώνα με την παραπάνω προδιαγραφή κάθε RFID συσκευή έχει μοναδικό μυστικό κωδικό το οποίο τις δίνεται από τον κατασκευαστή της και χρησιμοποιώντας το μπορεί να καταστήσει μία ετικέτα μόνιμα μη λειτουργική. Αν και αυτή η δυνατότητα συνήθως χρησιμοποιείται για λόγους ασφαλείας είναι προφανές ότι μπορεί να χρησιμοποιηθεί και από επιτιθέμενους με σκοπό να σαμποτάρουν τις RFID επικοινωνίες.

2.3.2 Προσωρινή απενεργοποίηση ετικέτας Τ

Ακόμα και αν μια ετικέτα RFID αποφύγει τον κίνδυνο μόνιμης απενεργοποίησης πάντα υπάρχει ο κίνδυνος της προσωρινής αναστολής λειτουργίας. Ένας επιτιθέμενος μπορεί εύκολα με μία τσάντα αλουμινίου να εμποδίσει την επικοινωνία της ετικέτας με τα ηλεκτρομαγνητικά κύματα και έτσι να κλέψει οτιδήποτε χωρίς ενόχληση. Οι ετικέτες διατρέχουν τον κίνδυνο να καταστούν προσωρινά μη ενεργές λόγω των περιβαντολλογικών συνθηκών (πχ, ετικέτα καλυμμένη με πάγο). Προσωρινή απενεργοποίηση μπορεί να προκληθεί από ράδιο παρεμβολές είτε ενεργητικές είτε παθητικές.

Παθητική παρεμβολή. Λαμβάνοντας υπόψη ότι τα RFID δίκτυα λειτουργούν σ' ένα ασταθές και θορυβώδες περιβάλλον η επικοινωνία τους καθίσταται ευάλωτη σε πιθανές παρεμβολές και σε συγκρούσεις από οποιαδήποτε πηγή ράδιο παρεμβολών όπως θορυβώδεις ηλεκτρικές γεννήτριες και πηγές μετατροπής ενέργειας. Αυτή η παρεμβολή εμποδίζει την ορθή και αποδοτική επικοινωνία.

Ενεργητική παρεμβολή (μπλοκάρισμα). Αν και η παθητική παρέμβαση είναι συνήθως ακούσια, ένας επιτιθέμενος μπορεί να εκμεταλλευτεί το γεγονός ότι μια ετικέτα RFID ακούει αδιακρίτως όλα τα ράδιο σήματα στην εμβέλεια της. Κατά συνέπεια, ένας αντίπαλος μπορεί να προκαλέσει το ηλεκτρομαγνητικό μπλοκάρισμα με τη δημιουργία ενός σήματος στην ίδια εμβέλεια με τον αναγνώστη προκειμένου να αποτραπούν οι ετικέτες από την επικοινωνία με τους αναγνώστες.

2.3.3 Relay Επιθέσεις

Σε μια Relay επίθεση ο επιτιθέμενος λειτουργεί σαν συσκευή ανάμεσα σε μια ετικέτα και έναν αναγνώστη. Η επιτιθέμενη συσκευή είναι τοποθετημένη παράνομα ανάμεσα στη νόμιμη ετικέτα και το νόμιμο αναγνώστη. Αυτή η συσκευή είναι σε θέση να παρεμποδίσει και να τροποποιήσει το ραδιο σήμα μεταξύ της νόμιμης ετικέτας και του νόμιμου αναγνώστη. Στη συνέχεια, μια προσωρινή (παραπλανητική) σύνδεση αναμεταδίδεται από τα νόμιμα ετικέτα / αναγνώστη μέσω της επιτιθέμενης συσκευής στα νόμιμα αναγνώστη / ετικέτα. Έτσι τα νόμιμα αναγνώστης και ετικέτα νομίζουν λανθασμένα ότι επικοινωνούν απευθείας μεταξύ τους. Για να γίνει αυτού του είδους η επίθεση ακόμη πιο πολύπλοκη μπορούν να χρησιμοποιηθούν ξεχωριστές συσκευές, μία για την επικοινωνία με τον αναγνώστη R και μία για την επικοινωνία με την ετικέτα Τ. Ανησυχητικό είναι το γεγονός ότι αυτού του είδους η επίθεση μπορεί να είναι επιτυχής και από μεγάλες αποστάσεις. Για παράδειγμα μια relay επίθεση μπορεί να χρησιμοποιηθεί για να χρεώσει την RFID κάρτα του θύματος. Πρόσφατα ένας Γερμανός μεταπτυχιακός φοιτητής απέδειξε την ευπάθεια τον Ολλανδικών μεταφορών εκτελώντας το μοντέλο "ghost and leech", μοντέλο που έχει περιγραφή από τους Kfir και Wool και

δημιούργησε μεγάλο μπλέξιμο στο αξίας 2 δισεκατομμυρίων δολαρίων δημόσιο σύστημα μεταφοράς της Ολλανδίας.

2.3.4 Άμυνες απέναντι στις επιθέσεις στο Φυσικό στρώμα

Με σκοπό την διασφάλιση των RFID συστημάτων από τις τεχνικού επιπέδου επιθέσεις όπως η μόνιμη ή η παροδική απενεργοποίηση ετικέτας Τ, παραδοσιακά αντίμετρα πρέπει να χρησιμοποιηθούν, όπως η αυξανόμενη φυσική ασφάλεια με φρουρές, φράκτες, πύλες, κλειδωμένες πόρτες και κάμερες.

Κατά συνέπεια, η σκόπιμη και ακούσια φυσική καταστροφή καθώς επίσης και η χρήση των τσαντών με επένδυση από αλουμίνιο θα μπορούσαν να μετριαστούν. Η μετακίνηση της ετικέτας θα μπορούσε να αποφευχθεί υιοθετώντας τις παραπάνω πρακτικές φυσικής επίβλεψης χρησιμοποιώντας ισχυρότερους τρόπους να αποφευχθεί η εύκολη μετακίνηση ετικετών (πχ. Δυνατότερη κόλα, ενσωματωμένη ετικέτα Τ στα προϊόντα). Σκόπιμη και ακούσια ράδιο παρεμβολή μπορεί επίσης να παρεμποδιστεί με την χρήση αδιαφανών τοίχων στις σχετικές ραδιοσυχνότητες. Επιπλέον, η μη εξουσιοδοτημένη χρήση της εντολής KILL θα μπορούσε να αποτραπεί με την αποτελεσματική διαχείριση κωδικού πρόσβασης. Για παράδειγμα, η εντολή KILL για Class-1 GEN-2 τυποποιημένων ετικετών EPC απαιτεί έναν τριανταδυάμπιτο κωδικό πρόσβασης. Για την προστασία από τις Relay επιθέσεις οι πιθανές προσεγγίσεις θα μπορούσαν να είναι η κρυπτογράφηση της επικοινωνίας RFID ή της προσθήκης μιας δεύτερης μορφής επικύρωσης όπως ένας κωδικός πρόσβασης, ένα PIN ή βιομετρικές πληροφορίες. Εντούτοις, αυτές οι απαιτήσεις μειώνουν την ευκολία και τα πλεονεκτήματα της επικοινωνίας RFID. Ένας άλλος πιθανός τρόπος να αντιμετωπιστούν οι Relay επιθέσεις είναι το distance bounding πρωτόκολλο βασισμένο στην εξαιρετικά ευρείας ζώνης παλμική επικοινωνία που προτείνεται από τον Hancke. Μια άλλη ενδιαφέρουσα προσέγγιση που μπορεί να χρησιμοποιηθεί για να προστατεύσει τα RFID συστήματα ενάντια στις επιθέσεις (συμπεριλαμβανομένων των φυσικών επιθέσεων στρώματος) προτάθηκε από τον Bolotny. Συγκεκριμένα έκανε μια πιο τεχνική προσέγγιση βασισμένη σε φυσικές μη δυνατές να κλωνοποιηθούν λειτουργίες (PUFs) για την παροχή ασφάλειας και μυστικότητας. Οι λειτουργίες PUFs δίνουν μια λύση στο κρίσιμο βασικό πρόβλημα διανομής και μπορούν να προστατεύσουν από την κλωνοποίηση ακόμα κι αν ένας επιτιθέμενος έχει φυσική πρόσβαση στις ετικέτες RFID.

2.4 Στρώμα Δικτύου και Μεταφοράς

Αυτό το στρώμα εμπεριέχει όλες τις επιθέσεις οι οποίες βασίζονται στον τρόπο με τον οποίο τα RFID συστήματα επικοινωνούν και στον τρόπο με τον οποίο τα δεδομένα μεταφέρονται μεταξύ ολόκληρου του RFID δικτύου (Ετικέτες, Αναγνώστες). Σε αυτή την ενότητα περιγράφονται επιθέσεις που επιδρούν στο στρώμα Δικτύου-Μεταφοράς και διακρίνουμε αυτές σε επιθέσεις στις ετικέτες, στους αναγνώστες και επιθέσεις στο

πρωτόκολλο δικτύου. Επίσης παρέχονται πιθανοί τρόποι για να αντιμετωπιστούν αυτές οι επιθέσεις.

2.4.1 Επιθέσεις στις ετικέτες Τ

Κλωνοποίηση. Ακόμη και το σημαντικότερο και πιο χαρακτηριστικό γνώρισμα των RFID συστημάτων, το μοναδικό προσδιοριστικό τους (ταυτότητα) , είναι ευαίσθητο σε επιθέσεις. Αν και θεωρητικά δεν μπορεί να ζητήσεις από έναν κατασκευαστή RFID να δημιουργήσει ένα κλώνο ετικέτας, στην πράξη αποδεικνύεται ότι το να δημιουργήσεις μια ψεύτικη αντιγραφή δεν χρειάζεται πολλά χρήματα και πείρα από την στιγμή που υπάρχει ευρέως μεγάλη ποικιλία από επαναγράψιμες και εύκολα επαναπρογραμματίσιμες RFID. Ένα αντιπροσωπευτικό παράδειγμα είναι μια έκθεση ενός Γερμανού Ερευνητή που παρουσιάζει την ευπάθεια των γερμανικών διαβατηρίων στην επίθεση της κλωνοποίησης.

Εξαπάτηση(spoofing). Η εξαπάτηση είναι ουσιαστικά μια παραλλαγή της κλωνοποίησης η οποία δεν δημιουργεί φυσικό αντίγραφο της RFID ετικέτας. Σε αυτή την επίθεση ο επιτιθέμενος προσποιείται μια νόμιμη ετικέτα έτσι ώστε να κερδίζει τη εμπιστοσύνη και προνόμια. Αυτή η προσποίηση απαιτεί ολοκληρωμένη πρόσβαση στα κοινά κανάλια επικοινωνίας όπως ακριβώς έχει η νόμιμη ετικέτα. Αυτό προϋποθέτει γνώση των πρωτοκόλλων και των μυστικών που χρησιμοποιούνται κατά την πιστοποίηση (αυθεντικοποίηση).

2.4.2 Επιθέσεις στους Αναγνώστες

Προσποίηση (Impersonation). Λαμβάνοντας υπόψη ότι πολλές φορές η RFID επικοινωνία διεξάγεται χωρίς ταυτοποίηση χρήστη, οι επιτιθέμενοι μπορούν εύκολα να πλαστογραφήσουν την ταυτότητα του νόμιμου αναγνώστη με σκοπό να συλλέξουν ευαίσθητες πληροφορίες ή να αλλάξουν τα δεδομένα στις RFID ετικέτες.

Υποκλοπή (Eavesdroping). Η ασύρματη φύση της RFID τεχνολογίας κάνει την υποκλοπή μία από τις πιο επικίνδυνες και τις πιο ευρέως διαδεδομένες απειλές. Στην υποκλοπή ένα μη εξουσιοδοτημένο άτομο χρησιμοποιεί μία κεραία με σκοπό να καταγράψει δεδομένα, μεταξύ των γνήσιων αναγνώστη και ετικέτας. Αυτός ο τύπος επίθεσης μπορεί να γίνει από και προς τις δύο κατευθύνσεις από την ετικέτα προς τον αναγνώστη και το αντίθετο. Δεδομένου ότι οι αναγνώστες διαβιβάζουν τις πληροφορίες με πολύ υψηλότερη ισχύ από τις ετικέτες, είναι ευαίσθητοι σε αυτόν τον τύπο επιθέσεων από πολύ μεγαλύτερες αποστάσεις και συνεπώς σε μεγαλύτερο βαθμό. Οι πληροφορίες που καταγράφονται από τις επιθέσεις αυτές μπορούν να χρησιμοποιηθούν για να εκτελέσουν περιπλοκότερες αργότερα. Η δυνατότητα πραγματοποίησης αυτής της

επίθεσης εξαρτάται από πολλούς παράγοντες, όπως η απόσταση του επιτιθεμένου από τις νόμιμες συσκευές RFID.

2.4.3 Επιθέσεις στο Πρωτόκολλο Δικτύου

Τα RFID συστήματα συχνά συνδέονται με κεντρικές βάσεις δεδομένων και συσκευές δικτύου που βρίσκονται στην κεντρική διαχείριση της εταιρείας. Παρόλα αυτά αυτές οι συσκευές είναι ευαίσθητες σε ευπάθειες που έχουν γενικά οι συσκευές δικτύωσης. Τρύπες στο λειτουργικό σύστημα και τα πρωτόκολλα δικτύων, μπορούν να χρησιμοποιηθούν από τους επιτιθεμένους προκειμένου να ξεκινήσουν επιθέσεις με σκοπό να προσπελάσουν την βασική δομή του συστήματος.

2.4.4 Άμυνες ενάντια στις επιθέσεις του στρώματος Δικτύου- Μεταφοράς

Με κατάλληλη συλλογή δεδομένων είναι πιθανό να ανιχνευθούν κλωνοποιημένες ετικέτες RFID. Εναλλακτικά, οι επιθέσεις κλωνοποίησης μπορούν να μετριαστούν μέσω των πρωτοκόλλων αυθεντικοποίησης πρόκλησης-απάντησης (challenge-response authentication protocols). Αυτά πρέπει επίσης να υποστηρίξουν δυνατούς μηχανισμούς κατά των “brute-force” επιθέσεων. Εντούτοις, οι περιορισμοί υλικών στην κατασκευή των RFID ετικετών οδηγούν σε αδύνατα πρωτόκολλα επικύρωσης που πολλές φορές είναι ανεπαρκή ενάντια στους επιτιθεμένους. Ο Juels έχει καταδείξει μερικές τεχνικές για μεγαλύτερη αντίσταση των EPC ετικετών ενάντια στις επιθέσεις κλωνοποίησης, χρησιμοποιώντας την πρόσβαση με βάση μυστικό κωδικό (PIN) για να επιτύχει αυθεντικοποίηση με την διαδικασία πρόκλησης-απάντησης.

Η Δημόσια συναίσθηση της ασφάλειας και οι επιπτώσεις σχετικές με τις επιθέσεις κλωνοποίησης πρέπει να είναι η βασική πολιτική ενάντια σε αυτό τον τύπο επίθεσης. Εντούτοις, αυτό δεν φέρνει πάντα το επιθυμητό αποτέλεσμα.. Για παράδειγμα καμία από τις χώρες στις οποίες χρησιμοποιείται το ηλεκτρονικό διαβατήριο δεν έχει μηχανισμούς που να αποτρέπουν την κλωνοποίηση όπως προβλέπεται με βάση το πρότυπο ICAO 9303. Με σκοπό την αποφυγή της παθητικής υποκλοπής δεδομένων μπορούν να χρησιμοποιηθούν τεχνικές απόκρυψης οι οποίες θα εξασφαλίζουν τις RFID επικοινωνίες. Η εξαπάτηση και η προσωποποίηση θα μπορούσαν να καταπολεμηθούν με τη χρησιμοποίηση πρωτοκόλλων επικύρωσης ή μιας δεύτερης μορφής επικύρωσης όπως οι one-time κωδικοί πρόσβασης, τα PIN ή τα βιομετρικά

Οι επιθέσεις στο πρωτόκολλο δικτύου θα μπορούσαν να αντιμετωπιστούν σκληραίνοντας την πολιτική ασφάλειας όσον αφορά τα συστατικά που υποστηρίζουν την επικοινωνία RFID, χρησιμοποιώντας ασφαλή λειτουργικά συστήματα, απενεργοποιώντας τα επισφαλή και αχρησιμοποίητα πρωτόκολλα δικτύων και διαμορφώνοντας τα πρωτόκολλα ώστε χρησιμοποιούνται με τα λιγότερα πιθανά προνόμια.

2.5 Στρώμα Εφαρμογής (Application Layer)

Αυτό το στρώμα περιλαμβάνει όλες τις επιθέσεις που στοχεύουν στις πληροφορίες σχετικές με τις εφαρμογές και τη σύνδεση μεταξύ των χρηστών και των ετικετών RFID. Τέτοιες επιθέσεις υιοθετούν την χωρίς επικύρωση ανάγνωση ετικετών, την τροποποίηση των στοιχείων των ετικετών Τ και των επίθεση στο υλικολογισμικό των εφαρμογών. Περιγράφουμε αυτές τις επιθέσεις καθώς επίσης και τους πιθανούς τρόπους να τις καταπολεμήσουμε.

2.5.1 Μη εξουσιοδοτημένη ανάγνωση αναγνώστη R

Λόγω του ότι δεν υποστηρίζουν όλες οι ετικέτες RFID λειτουργίες αυθεντικοποίησης, ο επιτιθέμενος μπορεί εύκολα να διαβάσει τα περιεχόμενα των RFID ετικετών Τ (ακόμα και από μεγάλες αποστάσεις) χωρίς να αφήσει κανένα ίχνος.

2.5.2 Τροποποίηση ετικέτας

Λόγω του γεγονότος ότι οι RFID συσκευές είναι ευρέως διαδεδομένες και χρησιμοποιούνται σήμερα από εργαζόμενους ως μνήμη καταχώρησης δεδομένων, είναι σχετικά εύκολο για τον επιτιθέμενο να τροποποιήσει ή να διαγράψει μια πολύτιμη πληροφορία. Εδώ πρέπει να σημειώσουμε ότι το πόσο εύκολα θα επιτύχει η επίθεση εξαρτάται από το πρότυπο που χρησιμοποιείται στην εγγραφή/ανάγνωση για την προστασία των δεδομένων.

2.5.3 Επίθεση στο ενδιάμεσο των εφαρμογών (middleware)

Υπερχείλιση μνήμης. Η υπερχείλιση μνήμης αποτελεί μιας από τις σημαντικότερες απειλές και μεταξύ των σημαντικότερων προβλημάτων ασφαλείας στο λογισμικό. Η υπερχείλιση εκμεταλλεύεται τα στοιχεία ή τον κώδικα πέρα από τα όρια του καθορισμένου μήκους της μνήμης. Οι αντίπαλοι μπορούν να χρησιμοποιήσουν τις ετικέτες RFID για να εξαπολύσουν επίθεση υπερχείλισης μνήμης στο οπίσθιο μέρος του λογισμικού των RFID εφαρμογών.

Λαμβάνοντας υπόψη την αποθήκευση των δεδομένων στις ετικέτες RFID, υπάρχουν ακόμα εντολές οι οποίες επιτρέπουν σε μια RFID ετικέτα Το να στέλνει μια αλληλουχία δεδομένων επαναλαμβανόμενα με σκοπό να υπερχειλίσει η μνήμη στο οπίσθιο μέρος του λογισμικού των εφαρμογών. Άλλες επιλογές είναι η χρησιμοποίηση άλλων συσκευών με περισσότερους πόρους όπως έξυπνες κάρτες ή συσκευές που είναι

ικανές να χειριστούν πολλαπλές RFID ετικέτες (πχ RFID guardian) ή χρησιμοποιώντας ετικέτες T με περισσότερη μνήμη από την αναμενομένη.

Έγχυση κακόβουλου κώδικα. Οι ετικέτες RFID μπορούν να χρησιμοποιηθούν προκειμένου να διαδοθεί ο εχθρικός κώδικας που θα μπορούσε στη συνέχεια να μολύνει άλλες οντότητες του δικτύου RFID (αναγνώστες R και συνδέοντας δίκτυα).

Σε αυτό το σενάριο, ένας αντίπαλος χρησιμοποιεί το διάστημα μνήμης των ετικετών T RFID με σκοπό να αποθηκευτούν και να διαδοθούν ιοί. Αν και αυτός ο τύπος επιθέσεων δεν είναι διαδεδομένος, εργαστηριακά πειράματα έχουν αποδείξει ότι είναι εφικτός. Λαμβάνοντας υπόψη το γεγονός ότι οι εφαρμογές ενδιάμεσου λογισμικού χρησιμοποιούν τις πολλαπλές script γλώσσες όπως Javascript, PHP, XML κ.α. ο επιτιθέμενος μπορεί να το εκμεταλλευτεί αυτό και να διαδώσει τον κακόβουλο κώδικα προκειμένου να "μολυνθούν" τα συστήματα ενδιάμεσου λογισμικού. Πιο συγκεκριμένα, οι ετικέτες RFID μπορούν να χρησιμοποιηθούν προκειμένου να εκτελεστεί η εισαγωγή κώδικα στις εφαρμογές RFID που χρησιμοποιούν τα πρωτόκολλα Ιστού και τις γλώσσες script που είναι γραμμένα. Με τον ίδιο τρόπο, μπορεί επίσης να διενεργηθεί διάδοση κακόβουλου λογισμικού σε SQL, μια επίθεση εισαγωγής κώδικα με σκοπό να εκτελέσει τις αναφορές που βγάζει η SQL και που μπορούν να οδηγήσουν την αναρμόδια πρόσβαση στις βάσεις δεδομένων οπίσθιου μέρους και να αποκαλύψει ή να τροποποιήσει στοιχεία που αποθηκεύονται στο οπίσθιο μέρος του ενδιάμεσου RFID λογισμικού.

2.5.4 Άμυνες κατά του στρώματος εφαρμογής

Με σκοπό την προστασία ενάντια στη μη-εξουσιοδοτημένη ανάγνωση η τροποποίηση ετικέτας, θα πρέπει να εστιάσουμε στον έλεγχο πρόσβασης στις ετικέτες RFID. Μια προσέγγιση είναι η χρήση προστατευτικού από αλουμίνιο για την κάλυψη των καρτών πληρωμής ή των διαβατηρίων. Πολλές εταιρείες έχουν υιοθετήσει αυτή τη λύση και διανέμουν αυτού του είδους προϊόντα. Οι τεχνικές κρυπτογράφησης, τα πρωτόκολλα επικύρωσης και οι κατάλογοι ελέγχου προσπέλασης μπορούν να παρέχουν μια εναλλακτική λύση. Πιο συγκεκριμένα, προσεγγίσεις βασισμένες στη συμμετρική κρυπτογράφηση κλειδιού, στη κρυπτογράφηση δημόσιου κλειδιού, σε hash συναρτήσεις, σε αμοιβαία επικύρωση ή ακόμα και μη κρυπτογραφημένες λύσεις όπως τα ψευδώνυμα , έχουν προταθεί.

Εντούτοις, ο σημαντικός περιορισμός στην υιοθέτηση αυτών των σχεδίων στα συστήματα RFID είναι ότι αυτά έχουν δομικές ευπάθειες όπως οι πιθανές διακοπές ισχύος ή διακοπές στην ασύρματη επικοινωνία. Θα πρέπει να σημειώσουμε ότι δεν χρειάζεται η χρήση όλων αυτών των τεχνικών κρυπτογράφησης σε εφαρμογές που δεν είναι άμεσος ο κίνδυνος υποκλοπής των δεδομένων.

Οι υπερχειλίσεις της μνήμης και η κακόβουλη έγχυση κώδικα στο ενδιάμεσο των εφαρμογών μπορούν να καταπολεμηθούν με τα απλά αντίμετρα. Με εκτέλεση κώδικα

επαναληπτικά μπορούμε να διαπιστώσουμε την ασφάλεια του συστήματος ενάντια στις ευπάθειες και λάθη, για παράδειγμα να εξασφαλιστεί ότι ο έλεγχος ορίων πραγματοποιείται. Για τις βάσεις δεδομένων, η χρήση παραμέτρων ορίων και η ισχύ λιγότερων προνομίων μεταξύ άλλων βοηθούν στο να προστατευθεί το σύστημα.

Τέλος, απενεργοποιώντας τα περιττά χαρακτηριστικά γνωρίσματα ενδιάμεσων εφαρμογών όπως ο προγραμματισμός οπίσθιου μέρους, προωθείται περαιτέρω την ακεραιότητα συστημάτων. Άλλα απλά μέτρα περιλαμβάνουν την απομόνωση του RFID Server ενδιάμεσων εφαρμογών έτσι ώστε σε περίπτωση εκτίθεται σε κίνδυνο, να μην παρέχεται πρόσβαση στο υπόλοιπο του δικτύου. Έτσι θα γίνεται έλεγχος στα δεδομένα εισόδου των ενδιάμεσων εφαρμογών RFID και θα αποβάλλονται οι πρόσθετοι και ύποπτοι χαρακτήρες.

2.6 Στρατηγικό στρώμα

Αυτό το στρώμα περιλαμβάνει τις επιθέσεις που στοχεύουν στην οργάνωση και τις επιχειρηματικές εφαρμογές, που αξιοποιούν απροσεξία των υποδομών και των εφαρμογών. Πιο συγκεκριμένα σε αυτό το στρώμα συμπεριλαμβάνεται η κατασκοπεία για λόγους ανταγωνισμού, μηχανική εξαπάτησης με σκοπό την αποκάλυψη πληροφορίας, μυστικότητα και στοχοθετημένες απειλές ασφάλειας. Θα περιγράψουμε αυτές τις απειλές και θα παραθέσουμε πιθανούς τρόπους που μπορούν να χρησιμοποιηθούν για να την αντιμετώπιση των απειλών.

2.6.1 Κατασκοπεία για λόγους ανταγωνισμού

Επιτιθέμενοι έχουν συχνά επιχειρηματικούς ή βιομηχανικούς ανταγωνιστές ως στόχο. Εκμεταλλευόμενοι τη δυνατότητα να ακολουθήσουν και να ανιχνεύσουν μαρκαρισμένες συσκευές, μπορούν να συλλέξουν κρίσιμες και εμπιστευτικές πληροφορίες προκειμένου να υπονομευθούν οι ανταγωνιστές τους. Τέτοιες πληροφορίες μπορούν να περιλαμβάνουν τις στρατηγικές και πρακτικές του θύματος σχετικά με τις μεταβαλλόμενες τιμές, τα προγράμματα παραγωγής ή τα σενάρια μάρκετινγκ. Τέτοιες επιθέσεις μπορούν να επιτευχθούν κρυφακούγοντας ή αποκτώντας αναρμόδια πρόσβαση στις βάσεις δεδομένων.

2.6.2 Κοινωνική Μηχανική (μηχανική εξαπάτησης με σκοπό την αποκάλυψη πληροφορίας)

Ένας επιτιθέμενος μπορεί ακόμη και να χρησιμοποιήσει τις δεξιότητες της μηχανικής εξαπάτησης για να παρακάμψει ένα σύστημα RFID και να κερδίσει την αναρμόδια πρόσβαση σε απαγορευμένες θέσεις ή σε πληροφορίες. Αντί να περάσει από την επίπονη διαδικασία του να αποκωδικοποιήσει προγραμματιστικά την επικοινωνία RFID, ένας επιτιθέμενος χρησιμοποιεί απλά ένα τέχνασμα εμπιστοσύνης ώστε να καταφέρει να του αποκαλυφθεί από τους ανθρώπους η εμπιστευτική πληροφορία.

Ένας επιτιθέμενος μπορεί απλά να εκμεταλλευτεί τις απλές πράξεις της ανθρώπινης καθημερινότητας, όπως το κράτημα της πόρτας ανοικτής (όπου μπορεί κάποιος να εισαχθεί χωρίς ένα διακριτικό RFID σε μια ειδάλλως περιορισμένη περιοχή) ή ο δανεισμός μιας ετικέτας RFID (όπου μπορεί κάποιος να ανακτήσει όλη τη εμπιστευτική πληροφορία).

2.6.3 Απειλές στη μυστικότητα

Οι ετικέτες RFID αποκρίνονται σε οποιοδήποτε αναγνώστη, πιστοποιημένο και μη πιστοποιημένο, χωρίς οποιασδήποτε ένδειξη για αυτήν την απόκριση στους ιδιοκτήτες τους. Αυτό το πρόσθετο χαρακτηριστικό γνώρισμα μπορεί να χρησιμοποιηθεί από τους αντιπάλους ώστε να κρατηθούν ίχνη με σκοπό την αποκάλυψη της δομής της επικοινωνίας. Η πιθανή συλλογή της προσωπικής πληροφορίας που κυμαίνεται από τις αγοραστικές συνήθειες των καταναλωτών έως ιατρικές πληροφορίες είναι ένας από τους μέγιστους κινδύνους στα συστήματα RFID.

2.6.4 Στοχοθετημένες απειλές ασφάλειας

Ένας αντίπαλος μπορεί να χρησιμοποιήσει τις πληροφορίες που συλλέγονται από μια εταιρεία προκειμένου να προκληθούν κακόβουλες φυσικές ή ηλεκτρονικές επιθέσεις. Το χαρακτηριστικό παράδειγμα αυτής της επίθεσης στοχεύει και ληστεύει ανθρώπους που συλλέγουν πολύτιμα στοιχεία (πχ. ρολόγια ή κοσμήματα).

2.6.5 Άμυνες εναντίον επιθέσεων στο στρατηγικό στρώμα

Οι επιθέσεις σε αυτό το στρώμα μπορούν να αποτραπούν με οποιοδήποτε από τα αντίμετρα που υιοθετούνται ενάντια στις επιθέσεις που περιλαμβάνονται στα άλλα

στρώματα. Ακριβέστερα, για τη μυστικότητα και τις στοχοθετημένες απειλές ασφάλειας μια ευρεία σειρά τεχνικών λύσεων έχει προταθεί, συμπεριλαμβανομένων της οριστικής ή προσωρινής σίγασης των ετικετών, κάτι που εμποδίζει την πρόσβαση στους αναρμόδιους αναγνώστες, επαναονοματοδοσία με ψευδώνυμα, την μετρήση της απόστασης εκπομπής και τις τεχνικές κρυπτογράφησης.

Εντούτοις, για να αντιμετωπίσουμε αποτελεσματικά τις στρατηγικές απειλές πρέπει να τις αντιμετωπίσουμε ως πρόβλημα που απαιτεί μακροπρόθεσμη προσπάθεια. Οι επιχειρήσεις και οι οργανώσεις που χρησιμοποιούν τα συστήματα RFID πρέπει να καθιερώσουν και να διατηρήσουν μια πολιτική μυστικότητας και προστασίας δεδομένων και να εκτελέσουν αξιολόγηση κινδύνου για να καθορίσουν τις απειλές και τους κινδύνους που συνδέονται με την υιοθετημένη υποδομή RFID. Γι' αυτό είναι σημαντικό να λάβει κανείς κατευθύνσεις από έναν ειδικό στην μυστικότητα και προστασία πληροφοριών και έναν νομικό σύμβουλο σχετικά με τα υιοθετημένα στρατηγικά σενάρια και σχετικά με τα ζητήματα μυστικότητα και προστασίας. Η πολιτική ασφαλείας πρέπει να κοινοποιηθεί σε όλους τους υπαλλήλους. Η συνεχής κατάρτιση και η εκπαίδευση του προσωπικού της οργάνωσης στις πολιτικές ασφάλειας RFID είναι ουσιαστική, δεδομένου ότι προωθεί τη συνειδητοποίηση για την προστασία των κρίσιμων πληροφοριών. Τα ζητήματα προστασίας σχετικά με την επικοινωνία RFID πρέπει επίσης να ληφθούν σοβαρά υπόψη από τους νομοθέτες και τις αρχές που δίνουν τις οδηγίες που πρέπει να ακολουθηθούν από τις οργανώσεις και τις επιχειρήσεις που χρησιμοποιούν τα συστήματα RFID. Το κέντρο για τη δημοκρατία και την τεχνολογία και το EPC global έχουν ήδη αναπτύξει ένα σύνολο οδηγιών και αρχών που μπορεί να χρησιμοποιηθεί από τις οργανώσεις για να αντιμετωπιστούν προβλήματα στην προστασία και μυστικότητα πληροφοριών.

2.7 Επιθέσεις σε παραπάνω από ένα στρώματα

Πολλές επιθέσεις που έχουν ως στόχο την επικοινωνία RFID δεν είναι περιορισμένες μόνο σε ένα στρώμα. Σε αυτό η κατηγορία συμπεριλαμβάνονται επιθέσεις που έχουν επιπτώσεις συγχρόνως σε παραπάνω από ένα στρώμα συμπεριλαμβανομένων όλων όσων αναλύσαμε στις προηγούμενες ενότητες. Συγκεκριμένα σε αυτό το στρώμα συμπεριλαμβάνονται επιθέσεις συγκεκαλυμμένων καναλιών, άρνησης υπηρεσιών, ανάλυσης κυκλοφορίας και επιθέσεων σε δευτερεύοντα κανάλια. Στη συνέχεια θα περιγράψουμε αυτές τις επιθέσεις, καθώς επίσης και τους πιθανούς τρόπους άμυνας ενάντια σε αυτές.

2.7.1 Συγκεκαλυμμένα κανάλια

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις ετικέτες RFID προκειμένου να δημιουργηθούν αναρμόδια κανάλια επικοινωνίας για να μεταφέρουν πληροφορίες με κάλυψη. Οι αντίπαλοι μπορούν να εκμεταλλευτούν την αχρησιμοποίητη υποθηκευμένη μνήμη των ετικετών RFID προκειμένου να μεταφερθούν ασφαλώς τα στοιχεία με έναν τρόπο που είναι δύσκολο να ανιχνευθεί. Για παράδειγμα, ετικέτες RFID που εμφυτεύθηκαν στα ανθρώπινα σώματα, των οποίων κανονικός σκοπός θα ήταν να προσδιοριστεί ένα πρόσωπο, θα μπορούσε κρυφά να εκθέσει τις ιδιωτικές πληροφορίες σχετικές με τα ιατρικά στοιχεία ή τις κοινωνικές δραστηριότητες.

2.7.2 Επιθέσεις άρνησης υπηρεσιών

Η λειτουργία των ετικετών RFID μπορεί να διακοπεί σκόπιμα ώστε να εμποδιστεί η πρόσβαση σε αυτές. Η σκόπιμη παρεμπόδιση πρόσβασης και η κατά συνέπεια άρνηση της υπηρεσίας των ετικετών RFID μπορούν να προκληθούν από τις κακόβουλες χρήσεις των «blocker tags» ή του guardian RFID. Και οι δύο προσεγγίσεις προτάθηκαν αρχικά για να προστατεύσουν τις επικοινωνίες RFID ενάντια στις απειλές μυστικότητας.
Εντούτοις, θα μπορούσαν επίσης να υιοθετηθούν από τους επιτιθέμενους για να εκτελέσουν μια σκόπιμη άρνηση της υπηρεσίας. Μια άλλη άρνηση της τεχνολογίας υπηρεσιών είναι η μη εξουσιοδοτημένη χρήση των εντολών κλειδώματος. Οι εντολές κλειδώματος εμπεριέχονται σε διάφορα RFID πρότυπα με σκοπό να εμποδίσουν την μη πιστοποιημένη εγγραφή στην μνήμη των ετικετών RFID. Ανάλογα με το πρότυπο η εντολή κλειδώματος μπορεί να περιλαμβάνει ένα προκαθορισμένο μυστικό κωδικό και μπορεί να έχει μόνιμες ή παροδικές επιδράσεις.

Επιπλέον, δεδομένου ότι το ενδιάμεσο των εφαρμογών RFID περιλαμβάνει τις συσκευές δικτύωσης, ένας αντίπαλος μπορεί να εκμεταλλευτεί τους περιορισμένους φυσικούς πόρους του συστήματος και να προκαλέσει μια άρνηση υπηρεσιών στο ενδιάμεσο των εφαρμογών RFID. Για παράδειγμα, στέλνοντας ακολουθία πακέτων στο ενδιάμεσο των εφαρμογών ώστε η δικτυακή και επεξεργαστική ικανότητα να είναι στα ανώτατα ανεκτά επίπεδα στην συνέχεια θα έχουμε άρνηση πρόσβαση στους κανονικούς πελάτες.

2.7.3 Επιθέσεις Ανάλυση Κίνησης

Η επικοινωνία RFID είναι επίσης ευαίσθητη στις επιθέσεις ανάλυσης κίνησης. Ένας επιτιθέμενος που ακούει χωρίς άδεια είναι σε θέση να παρεμποδίζει κομμάτια πληροφοριών από ένα σχέδιο επικοινωνίας. Ακόμα κι αν η επικοινωνία RFID προστατεύεται από τις τεχνικές κρυπτογράφησης και επικύρωσης, είναι ακόμα τρωτό

στις επιθέσεις ανάλυσης κυκλοφορίας. Όσο μεγαλύτερος ο αριθμός μηνυμάτων που παρεμποδίζονται, τόσο αποτελεσματικότερη θα είναι και η ανάλυση κυκλοφορίας.

2.7.4 Crypto Επιθέσεις

Όταν οι πληροφορίες αποθηκεύονται στις ετικέτες RFID, οι τεχνικές κρυπτογράφησης υιοθετούνται προκειμένου να προστατευθούν η ακεραιότητα και η εμπιστευτικότητα των δεδομένων. Ωστόσο οι επιτιθέμενοι διεξάγουν crypto επιθέσεις για να σπάσουν τους κρυπτογραφικούς αλγορίθμους και να αποκαλύψουν ή να χειριστούν τη ευαίσθητη πληροφορία. Για παράδειγμα, στην Ολλανδία μια εταιρία ασφάλειας που ονομάζεται Riscure έχει αποδείξει ότι το κλειδί που χρησιμοποιείται στο Ολλανδικό διαβατήριο μπορεί εύκολα να σπάσει χρησιμοποιώντας ένα απλό PC και εκτελώντας “brute force” επίθεση για δύο ώρες.

2.7.5 Επιθέσεις σε δευτερεύοντα κανάλια

Οι δευτερεύουσες επιθέσεις καναλιών εκμεταλλεύονται τη φυσική υλοποίηση ενός κρυπτογραφικού αλγορίθμου παρά τις θεωρητικές ευπάθειές της. Σε αυτόν τον τύπο επιθέσεων οι πληροφορίες που αξιοποιούνται συνήθως περιλαμβάνουν πληροφορίες συγχρονισμού, την κατανάλωση ισχύος ή ακόμα και τα ηλεκτρομαγνητικά πεδία. Η αποδοτική επέκταση των επιθέσεων δευτερευόντων καναλιών απαιτεί τη βαθιά γνώση του εσωτερικού συστήματος στο οποίο οι κρυπτογραφικοί αλγόριθμοι εφαρμόζονται.

2.7.6 Επιθέσεις επανάληψης

Μια απλή αμυντική προσέγγιση σε επιθέσεις όπως η παραπάνω, είναι η χρήση ενός πρωτοκόλλου πρόκλησης-απάντησης. Οι ετικέτες RFID και οι αναγνώστες μοιράζονται συνήθως ένα μυστικό κωδικό και χρησιμοποιούν ένα πρωτόκολλο πρόκλησης-απάντησης για να επικυρώσουν τις ταυτότητές τους. Εντούτοις, πολύ συχνά αυτή η προσέγγιση υπόκειται σε επιθέσεις επανάληψης. Σε μια επίθεση επανάληψης, ένας επιτιθέμενος μεταδίδει ραδιοφωνικά την απάντηση μιας ετικέτας που καταγράφεται από μια προηγούμενη συναλλαγή προκειμένου υποδυθεί την ετικέτα σε έναν αναγνώστη. Χαρακτηριστικό παράδειγμα αυτής της επίθεσης είναι η αναρμόδια πρόσβαση στις περιορισμένες περιοχές με την αναμετάδοση ακριβούς επανάληψης του ράδιο σήματος που στάλθηκε από μια νόμιμη ετικέτα στον αναγνώστη που χορηγεί την πρόσβαση.

2.7.7 Άμυνες εναντίον επιθέσεων που δρουν σε παραπάνω από ένα στρώματα

Οι επιθέσεις σε παραπάνω από ένα στρώματα είναι δύσκολο να ανιχνευθούν και να αντιμετωπιστούν. Οι ιδιοκτήτες και οι χρήστες των ετικετών RFID δεν έχουν καμία γνώση ότι οι ετικέτες τους έχουν εκτεθεί στον επιτιθέμενο και ότι χρησιμοποιούνται για μια συγκαλυμμένη επίθεση. Αυτές οι επιθέσεις είναι ένα ανοικτό ερευνητικό ζήτημα. Ένας πιθανός μηχανισμός για να τους καταπολεμήσει θα πρέπει να εστιάσει στη μείωση της διαθεσιμότητας των πόρων μνήμης σε μια ετικέτα RFID (π.χ. καθαρίζοντας την αχρησιμοποίητη μνήμη κάθε λίγα δευτερόλεπτα ή τυχαία τοποθέτηση ανά μικρό χρονικό διάστημα των δεδομένων σε διαφορετικές θέσεις).

Οι επιθέσεις άρνησης υπηρεσιών και ανάλυσης κυκλοφορίας είναι σοβαρές απειλές ασφάλειας για όλους τους τύπους δικτύων. Ενώ θεωρητικά αυτοί οι τύποι επιθέσεων μπορούν να αντιμετωπιστούν οι λιγοστοί πόροι των ετικετών RFID καθιστούν την υπεράσπισή τους προβληματική. Οι Crypto επιθέσεις μπορούν να αντιμετωπιστούν μέσω της χρήσης ισχυρών κρυπτογραφικών αλγορίθμων ακολουθώντας ανοικτά κρυπτογραφικά πρότυπα και τη χρησιμοποίηση ενός κλειδιών με μεγάλο μήκος.

Οι επιθέσεις σε δευτερεύοντα κανάλια και ακριβέστερα οι DPA επιθέσεις, μπορούν να προστατευθούν με περιορισμό των ηλεκτρομαγνητικών εκπομπών του συστήματος. Προκειμένου να προστατευθούν ενάντια στις επιθέσεις επανάληψης RFID υπάρχουν μερικά απλά αντίμετρα όπως η χρήση χρονικών αποτυπωμάτων (timestamps), των κωδικών πρόσβασης μίας φοράς και του συστήματος κρυπτογραφίας πρόκλησης απάντησης.

Εντούτοις, αυτά τα σχέδια δεν είναι εύκολα εφαρμόσιμα και η αποδοτικότητα τους είναι αμφισβητήσιμη. Μια άλλη προσέγγιση είναι η χρήση του προστατευτικού καλύμματος RF στους αναγνώστες προκειμένου να περιοριστεί η κατευθυντικότητα των ραδιοσημάτων και στη συνέχεια η εμφάνιση ενός επιτιθέμενου. Μια άλλη προσέγγιση βασίζεται στην απόσταση μεταξύ του αιτούντος και του παραγωγού της πληροφορίας. Οι Fishkin et. Al υπονόησαν ότι η αναλογία σήματος προς θόρυβο για το σήμα του αναγνώστη σε ένα σύστημα RFID μπορεί να αποκαλύψει ακόμα και κατά προσέγγιση την απόσταση μεταξύ ενός αναγνώστη και μιας ετικέτας. Αυτές οι πληροφορίες θα μπορούσαν σίγουρα να χρησιμοποιηθούν προκειμένου να γίνει μια αναγνωστών ή των ετικετών έτσι ώστε να μετριαστούν στη συνέχεια οι επιθέσεις επανάληψης.

2.8 Συμπεράσματα

Λόγω της όλο και περισσότερο ευρείας επέκτασης των συστημάτων RFID, το ζήτημα της ασφάλειας τους είναι πιο σημαντικό από ποτέ. Σε αυτό το κεφάλαιο, προσπαθήσαμε να ανακαλύψουμε κάποια δομή μέσα στο σύνολο των πιθανών επιθέσεων που επιδρούν και έχουν επιπτώσεις σε τέτοια συστήματα. Με το να εξετάζουμε το σημείο της επίθεσης, τα αποτελέσματα που έχουν στο σύστημα και τα αντίμετρα της επίθεσης από κοινού, μπορούμε να λάβουμε μια συνεπέστερη άποψη των απειλών και των πιθανών τρόπων αντιμετώπισης των απειλών.

Σε αυτό το κεφάλαιο, ταξινομήσαμε τις επιθέσεις βασισμένες στο στρώμα το οποίο κάθε επίθεση πραγματοποιείται και συζητήσαμε τα πιθανά αντίμετρα που μπορούν να χρησιμοποιηθούν για να καταπολεμήσουν αυτές τις επιθέσεις. Κάναμε διακρίσεις στις επιθέσεις που επεκτάθηκαν στο φυσικό στρώμα, το στρώμα εφαρμογής, το στρατηγικό στρώμα και τις επιθέσεις που δρούν σε παρά πάνω από ένα στρώμα. Τέλος, επισημαίνουμε για ποιες επιθέσεις η περαιτέρω έρευνα είναι απαραίτητη προκειμένου να επιτευχθεί η επαρκής υπεράσπιση ενάντια στους επιτιθέμενους.

ΚΕΦΑΛΑΙΟ 3

Επιθέσεις σε RFID πρωτόκολλα

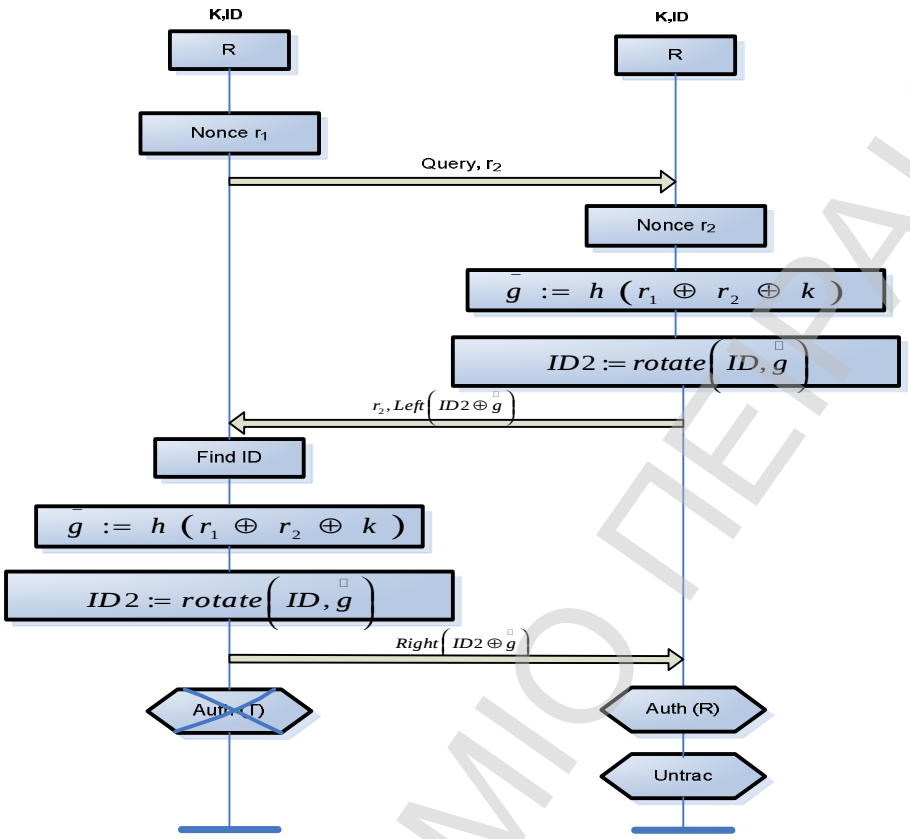
3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα παρουσιαστεί μια συλλογή επιθέσεων σε RFID πρωτόκολλα. Για την απλούστευση των αναφορών τα ονόματα των πρωτόκολλων θα γράφονται κωδικοποιημένα βάση των συντακτών του πρωτοκόλλου και της χρονιάς που δημοσιεύτηκε.

3.2 [CH07]

3.2.1 Περιγραφή

Ο αναγνώστης R και η ετικέτα T μοιράζονται το μυστικό k και την ταυτότητα ID. Ο αναγνώστης ξεκινά με την αποστολή μιας τυχαίας bit σειράς. Η ετικέτα παράγει τυχαίο αλφαριθμητικό και διαχωρίζει τυχαία με την μέθοδο κρυπτογράφησης XOR τα, και το μυστικό k. Το αποτέλεσμα του διαχωρισμού αυτού και η ταυτότητα ID χρησιμοποιούνται ως εισαγωγή για μια λειτουργία στην οποία η ταυτότητα περιστρέφεται από μια τιμή σύμφωνα με την τυχαία ακολουθία (hash). Η ετικέτα υπολογίζει το XOR της περιστρεφόμενης ταυτότητας ID και την τυχαία ακολουθία κατακερματισμού hash, πριν στείλει το αριστερό μισό των προκυπτόντων bits και το στον αναγνώστη. Ο αναγνώστης εκτελεί τις ίδιες διαδικασίες σε κάθε ζευγάρι της ταυτότητας και του k ώσπου να βρει την αντίστοιχη ετικέτα. Στέλνει έπειτα το σωστό μισό των αντίστοιχων bits στην ετικέτα.



Εικόνα 3.1: Το πρωτόκολλο

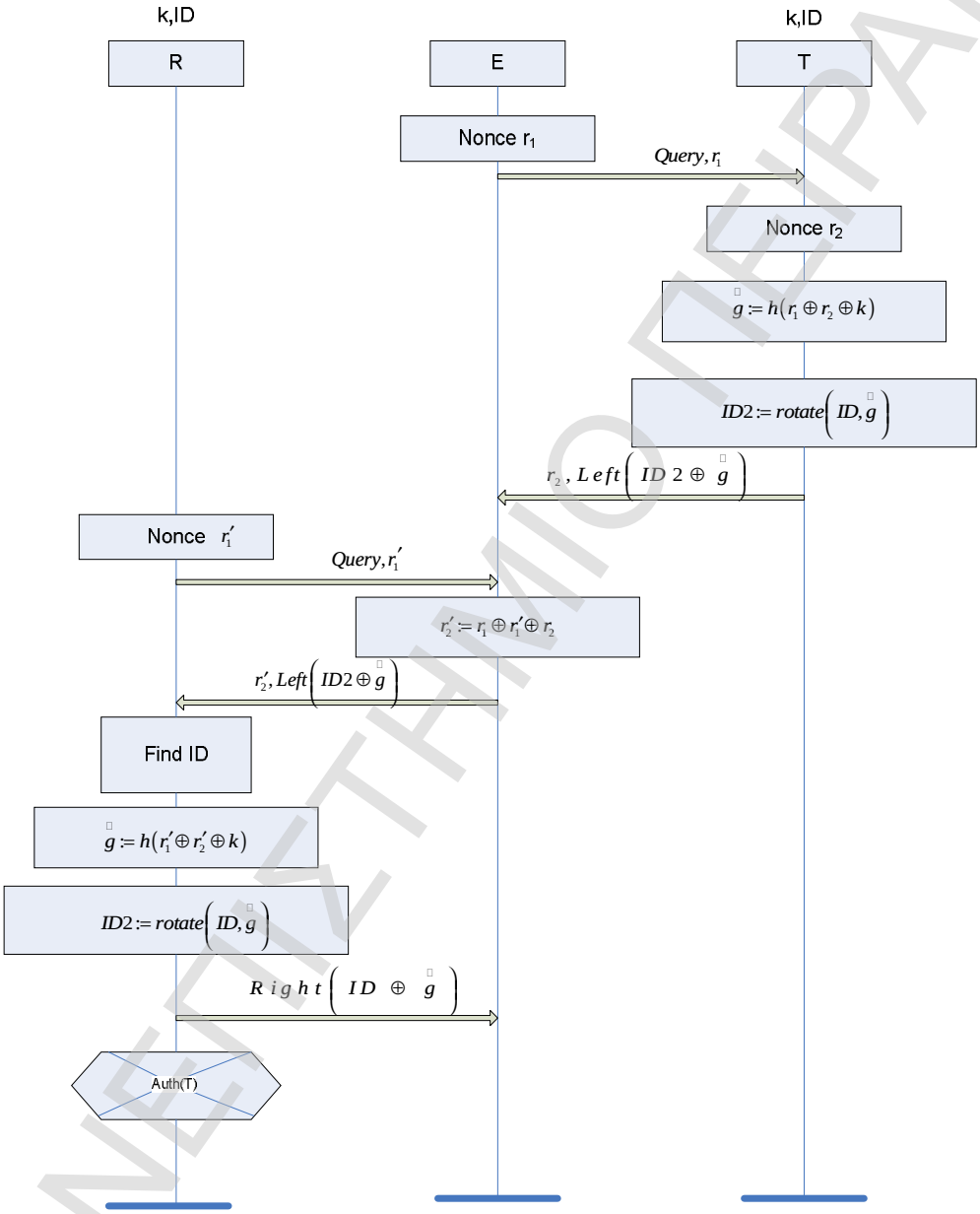
3.2.2 Επιθέσεις

3.2.2.1 Πιστοποίηση ετικέτας

Για να παραπλανηθεί μια ετικέτα, αρκεί να σημειωθεί ότι η απάντηση της ετικέτας στην πρόκληση του αναγνώστη εξαρτάται μόνο από $r_1 \oplus r_2$ και ένα κοινό μυστικό k. Ο επιτιθέμενος μπορεί προκαλέσει μια ετικέτα για να αποκτήσει έναν έγκυρο συνδυασμό $r_1, r_2, Left\left(ID \oplus \bar{g}\right)$. Αυτές οι πληροφορίες αρκούν για τον επιτιθέμενο να είναι σε θέση να ανταποκριθεί σε οποιαδήποτε μελλοντική πρόκληση r_1' που παραλαμβάνεται από έναν αναγνώστη. Όταν προκαλείται το παραπάνω, ο αντίπαλος θέτει $r_2' = r_1' \oplus r_1 \oplus r_2$ και στέλνει τα r_2', $Left\left(ID_2 \oplus \bar{g}\right)$.

3.2.3 Σχετικά Πρωτόκολλα

Έχουν βρεθεί ίδιε επιθέσεις και στα πρωτόκολλα [LAK06],[KCLL06],[SM08].



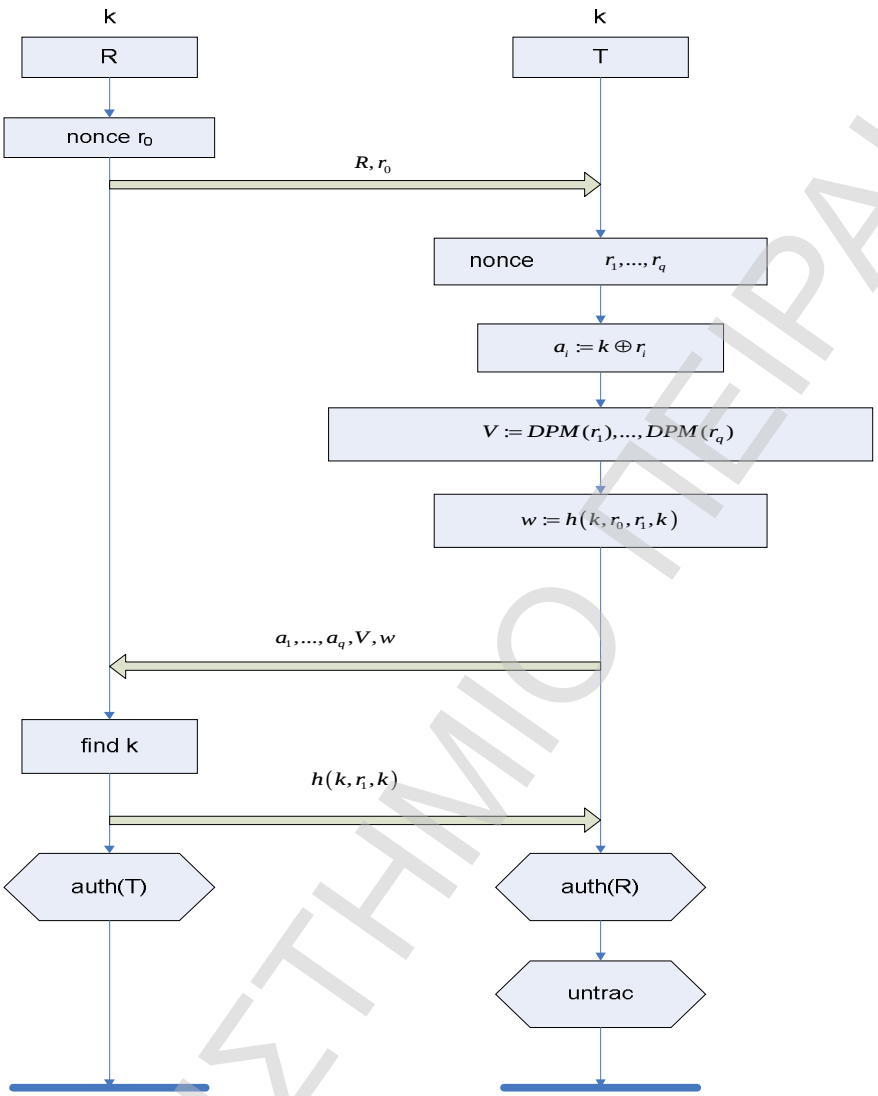
Εικόνα 3.2: Επίθεση στην επικύρωση της ετικέτας

3.3 [DM07]

3.3.1 Περιγραφή

Αυτό είναι ένα πρωτόκολλο αυθεντικοποίησης που στοχεύει όχι μόνο να κρατήσει τις ετικέτες μη δυνάμενες να αντιγραφούν, αλλά και να περιορίσει τη ζημία που ένας εκτεθειμένος αναγνώστης μπορεί να προκαλέσει.

Στο πρωτόκολλο, που απεικονίζεται στην εικόνα 3, η λειτουργία $DPM(x)$ ορίζεται ως η ισοδυναμία των λειτουργιών των διαδοχικών bit-τριπλετών του x. Το μέγεθος της εξόδου ως εκ τούτου είναι 1 bit. Το πρωτόκολλο αρχίζει με τον αναγνώστη να στέλνει το όνομά του και ένα μοναδικό r_0 στην ετικέτα. Η ετικέτα απαντά με το μήνυμα $a_1,...,a_q,V,w$ όπου $a_i = k \oplus r_i$ για τυχαία επιλεγμένο r_i (μια bit-σειρά μήκους ℓ, ℓ = 117 που προτείνονται από τους συντάκτες), το i-οστό bit του V (μια σειρά bit μήκους q) είναι $DPM(r_i)$ και $w = h(k, r_0, r_1, k)$. Ο αναγνώστης έχει μια βάση δεδομένων των κλειδιών όλων των ετικετών που εξουσιοδοτείται να αναγνωρίζει. Ο αναγνώστης μπορεί να βρει το ειδικό κλειδί k μιας ετικέτας με τη βοήθεια των διανυσμάτων a_i και να υπολογίζει το $DPM(r_i)$ περνώντας όλα τα κλειδιά στη βάση δεδομένων του, επαναληπτικά αποκλείοντας τα αδύνατα, δηλαδή εκείνα για τα οποία $DPM(k \oplus a_i) \neq DPM(r_i)$. Αναμένεται ότι κάθε επανάληψη μειώνει τον αριθμό πιθανών κλειδιών περίπου στο μισό. Τέλος, ο αναγνώστης χρησιμοποιεί ω για να προσδιορίσει μοναδικά το σωστό κλειδί και να πιστοποιήσει την ετικέτα. Το τελευταίο μήνυμα του πρωτοκόλλου επιτρέπει στην ετικέτα να πιστοποιήσει τον αναγνώστη.



Εικόνα 3.3: Το πρωτόκολλο

3.3.2 Επιθέσεις

3.3.2.1 Πιστοποίηση και μη ανιχνευσιμότητα

Παρακάτω δείχνουμε ότι μετά από κάποιες επαναλήψεις, το πρωτόκολλο έχει απώλεια $\frac{2l}{3}$ bit του k. Αυτό επιτρέπει σε έναν επιτιθέμενο να επιτεθεί με την μέθοδο «brute-force» στα υπόλοιπα bit του k για την προτεινόμενη παράμετρο ℓ = 117.

Έστω ότι ακολουθία $x = x_1, x_2 ... x_l$ από bit μήκους ℓ, για κάποιο θετικό ακέραιο αριθμό ℓ διαιρέσιμο δια τρία.

Κατόπιν $DPM(x) = M(x_1, x_2, x_3) \oplus ... \oplus M(x_{l-2}, x_{l-1}, x_l)$ όπου το $M(a,b,c)$ είναι η ακέραιη πλειοψηφία μεταξύ των τριών bits. Έστω ότι $\bar{x}_i$ το συμπλήρωμα του bit x_i. Είναι εύκολο να δούμε ότι το $M\left(\bar{x}_1, x_2, x_3\right) = M(x_1, x_2, x_3)$ εάν και μόνο εάν $x_2 = x_3$. Οι ανάλογες εξισώσεις ισχύουν για τα συμπληρώματα x_2 και x_3. Ακολουθεί η παρακάτω εξίσωση

$$DPM\left(\bar{x}_1, x_2, x_3\right) = DPM(x_1, x_2, x_3) \Leftrightarrow x_2 = x_3 \qquad (1)$$

με τις ανάλογες εξισώσεις για οποιοδήποτε bit του x.

Ο επιτιθέμενος μπορεί να εκμεταλλευτεί την εξίσωση (1) ως εξής. Υποθέτουμε ότι ο επιτιθέμενος παρεμποδίζει το μήνυμα της ετικέτας, αντιστρέφει το πρώτο bit $a_2 = r_2 \oplus k$ για να λάβει $\bar{a}$ και να διαβιβάσει το τροποποιημένο μήνυμα στον αναγνώστη. Εάν το δεύτερο και τρίτο bit r_2 είναι ίσο, τότε $DPM\left(k \oplus \bar{a}_2\right) = DPM(k \oplus a_2) = DPM(r_2)$. Σε αυτήν την περίπτωση, ο αναγνώστης θα είναι σε θέση ακόμα να βρει το σωστό κλειδί k και να απαντήσει στην ετικέτα με ένα τρίτο μήνυμα του πρωτοκόλλου. Ωστόσο, εάν το δεύτερο και τρίτο bit του r_2 δεν είναι ίσα, τότε $DPM\left(k \oplus \bar{a}_2\right) \neq DPM(r_2)$ και ο αναγνώστης θα αφαιρέσει το κλειδί k από τον κατάλογο των πιθανών κλειδιών. Κανένα άλλο κλειδί δεν θα περάσει την επαλήθευση με ω, έτσι ο αναγνώστης R δεν θα απαντήσει με τρίτο μήνυμα. Επομένως ο επιτιθέμενος μπορεί να διακρίνει τις δύο περιπτώσεις.

Παρακάτω βλέπουμε ότι αναστρέφοντας επιλεκτικά bit του a_2 μπορεί, ο εχθρός, μετά από κάποιες εκτελέσεις του πρωτοκόλλου, να καθορίσει για κάθε διαδοχική bit τριπλέτα του k ποια bit είναι ίσα τα ένα με το άλλο. Με άλλα λόγια, ο επιτιθέμενος μπορεί να καθορίσει τα bit του k μέχρι τα συμπληρώματα των διαδοχικών bit-τριπλετών.

Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να μειώσουν την πολυπλοκότητα του υπολογισμού όλων των bit του k σε μια αναζήτηση “brute-force” ενός διαστήματος του οποίου το μέγεθος είναι η κυβική ρίζα ολόκληρου του διαστήματος του κλειδιού. Για την παραμετροποίηση του συστήματος που προτείνεται από τους Di Pietro και Molva, αυτή η “brute force” αναζήτηση είναι εφικτή με (2^{39}) κλειδιά. Η γνώση του μυστικού κλειδιού k επιτρέπει ακόμη στον επιτιθέμενο να υποδυθεί την ετικέτα στον αναγνώστη, σπάζοντας κατά συνέπεια την αλυσίδα αυθεντικοποίησης του πρωτοκόλλου. Με αρκετή αύξηση του μήκους του κλειδιού k αυτή η επίθεση γίνεται ανέφικτη.

Για να σπάσει η μη ανιχνευσιμότητα , η αναζήτηση «brute-force» δεν είναι απαραίτητη. Η πιθανότητα ότι δύο κλειδιά είναι ίσα μέχρι τα συμπληρώματα των διαδοχικών bit-τριδύμων είναι πραγματικά μηδαμινή **[DMR08]**. Η αύξηση του μήκους του κλειδιού δεν αποτρέπει αυτήν την επίθεση.

Η επίθεση που περιγράφεται παραπάνω δεν είναι αποδοτική. Στο **[DMR08]** περιγράφουμε μια αποδοτική ποιοτικά και χρονικά επίθεση σε αυτό το πρωτόκολλο που αποκαλύπτει τις ίδιες πληροφορίες για το k με την επίθεση που περιγράφεται ανωτέρω.

3.3.3 Σχετικά Πρωτόκολλα

Η επίθεση που παρουσιάστηκε είναι παρόμοια με την ενεργό επίθεση στο HB+ πρωτόκολλο [JW05] που ανακαλύφθηκε από το [GRS05] δεδομένου ότι εκμεταλλεύεται μια αλγεβρική ιδιότητα τροποποιώντας μηνύματα και παρατηρώντας την συμπεριφορά του αναγνώστη R.

3.4 [HMNB07a]

3.4.1 Περιγραφή

Το πρωτόκολλο ξεκινά με τον αναγνώστη να ρωτά την ετικέτα με ένα μοναδικό r_1. Η απάντηση της ετικέτας εξαρτάται από την τιμή την οποία έχει η μεταβλητή S. Σε περίπτωση που το προηγούμενο διαδικασία τελείωσε επιτυχώς η αξία του S είναι 0 και η ετικέτα θα αποκριθεί με το h(ID). Σε περίπτωση που δεν τελείωσε επιτυχώς η αξία του S είναι 1 και η ετικέτα θα αποκριθεί με το h (ID, r_2, r_1). Σε καθεμία περίπτωση, η ετικέτα θα θέσει το S της σε 1. Ο αναγνώστης θα επικυρώσει την ετικέτα εάν η απάντηση είναι ίση με HID, h(ID,r_2,r_1) ή το h(PID, r2, r1) για οποιαδήποτε αποθηκευμένη αξία του HID,ID ή PID. Ο αναγνώστης θα ενημερώσει έπειτα τις πληροφορίες για την ιδιαίτερη ετικέτα σύμφωνα με τον πίνακα 2. Έπειτα ο αναγνώστης στέλνει το h(PID, r_2) στην ετικέτα, και μετά η ετικέτα αντικαθιστά το δικό της ID από το h(PID, r_1) και θέτει το S σε 0. Το πρωτόκολλο απεικονίζεται στο σχήμα 4.

Tag Response	Reader Action
$h\ (ID\ ), r_2$	$ID' := h(ID, r_1) : HID' := h(ID) : PID' := ID :$
$h(ID, r_2, r_1), r_2$	$ID' := h(ID, r_1) : HID' := h(ID) : PID' := ID :$
$h(PID, r_2, r_1), r_2$	$ID' := h(PID, r_1) := HID' := h(ID) : PID' := PID :$
Other	Reject tag

Πίνακας 3.1: Επαλήθευση από τον αναγνώστη και ανανέωση της διαδικασίας

3.4.2 Επιθέσεις

3.4.2.1 Επικύρωση Ετικετών

Σημειώνουμε ότι εάν κανένα μήνυμα δεν εμποδιστεί ή χαθεί, η ετικέτα θα αποκρίνεται πάντα με το h(ID) κάτι που συντελεί στο να είναι αποδοτική η διαδικασία από τον αναγνώστη. Ένας επιτιθέμενος μπορεί έτσι να προσποιηθεί σε οποιαδήποτε ετικέτα που είναι σε κατάσταση 0 στέλνοντας μια ερώτηση σε αυτήν και απαντώντας στην απόκριση της ετικέτας προσποιούμενος έναν εξουσιοδοτημένο αναγνώστη. Ο πραγματικός εξουσιοδοτημένος αναγνώστης δεν θα έχει προλάβει να αποκριθεί. Η επίθεση απεικονίζεται στο σχήμα 6.

3.4.2.2 Μη ανιχνευσιμότητα

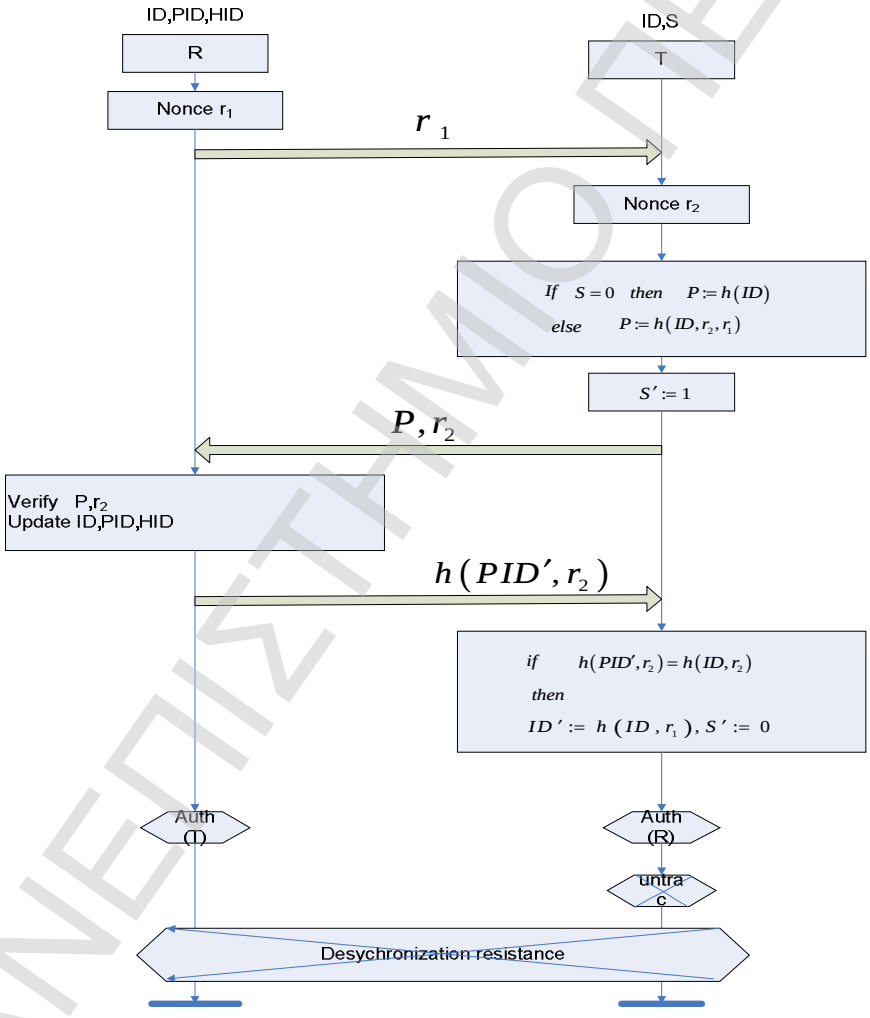
Η απάντηση της ετικέτας εξαρτάται από την αξία του S, δηλ. την κατάσταση που η ετικέτα βρίσκεται. Εάν S = 0 η ετικέτα απαντά με h(ID), r_2 ειδάλλως η ετικέτα αποκρίνεται με το h(ID, r_1, r_2). Επειδή ο επιτιθέμενος δεν ξέρει την ID, δεν μπορεί να βγάλει συμπέρασμα από την απάντηση για το σε ποια κατάσταση βρίσκεται η ετικέτα. Ωστόσο, ο επιτιθέμενος μπορεί επωφεληθεί από το γεγονός ότι εάν η ετικέτα είναι σε κατάσταση 0, η αλλαγή του r_2 δεν οδηγεί σε μια απόρριψη της απάντησης από τον αναγνώστη. Εάν η ετικέτα είναι σε κατάσταση 1, η αλλαγή r_2 οδηγεί σε απόρριψη της απάντησης και σε τερματισμό της εκτέλεσης του αναγνώστη.

3.4.2.3 Αντίσταση Αποσυγχρονισμού (Desynchronization resistance)

Οποιαδήποτε ετικέτα που είναι σε κατάσταση S = 0 μπορεί να αποσυγχρονιστεί από έναν αναγνώστη από μια “man-in-the-middle” επίθεση. Κατά την επικοινωνία μεταξύ του αναγνώστη και ετικέτας, ο εχθρός παρεμποδίζει και τροποποιεί την

πρόκληση του αναγνώστη r_1 σε οποιαδήποτε αξία $r'_1 \neq r_1$. Ο επιτιθέμενος στέλνει έπειτα την τροποποιημένη τιμή στην ετικέτα και προωθεί όλα τα άλλα μηνύματα μεταξύ του αναγνώστη και της ετικέτας χωρίς τροποποίηση. Δεδομένου ότι στην υπόθεση S = 0 ο αναγνώστης δεν ελέγχει ότι η ετικέτα έλαβε τη σωστή αξία r_1, η προσποίηση του αντιπάλου περνάει απαρατήρητη.

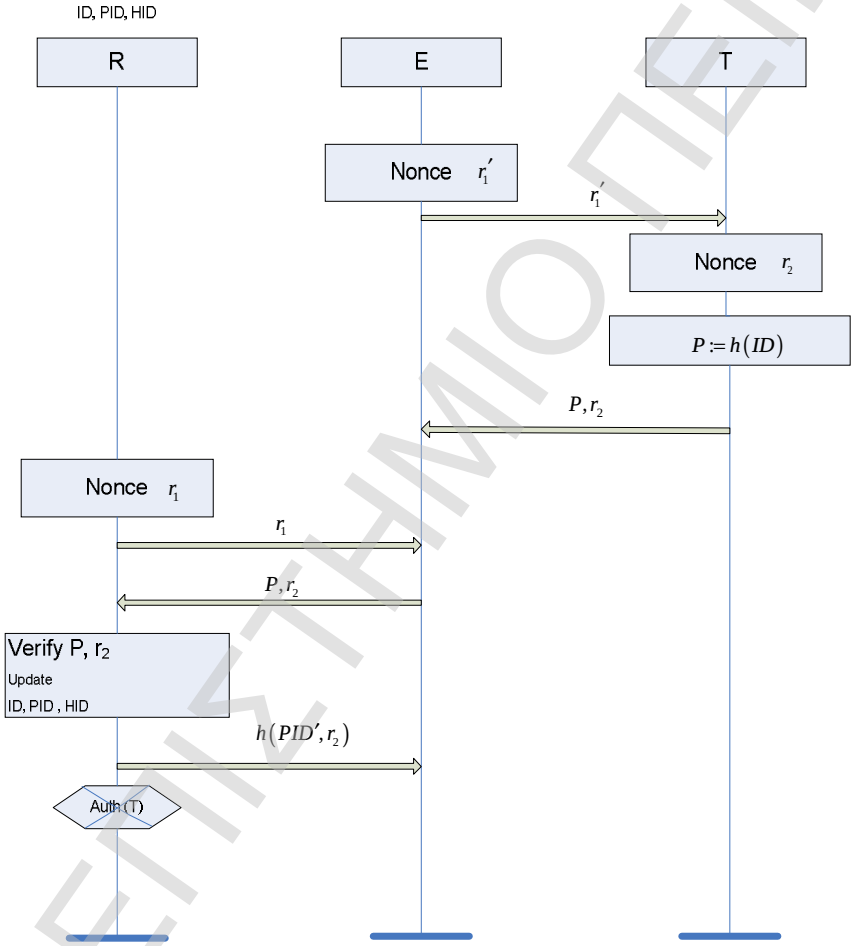
Έτσι, στο τέλος της εκτέλεσης του πρωτοκόλλου, αναγνώστης και ετικέτα ανανεώνουν το ID σε διαφορετικές τιμές. Ο αναγνώστης αποθηκεύει h(ID, r_1), ενώ η ετικέτα αποθηκεύει h(ID, r'_1). Επομένως, ο αναγνώστης και η ετικέτα θα είναι σε μη συγχρονισμένη κατάσταση και η μελλοντική αυθεντικοποίηση της ετικέτας γίνεται αδύνατη. Η επίθεση απεικονίζεται στο σχήμα 6.



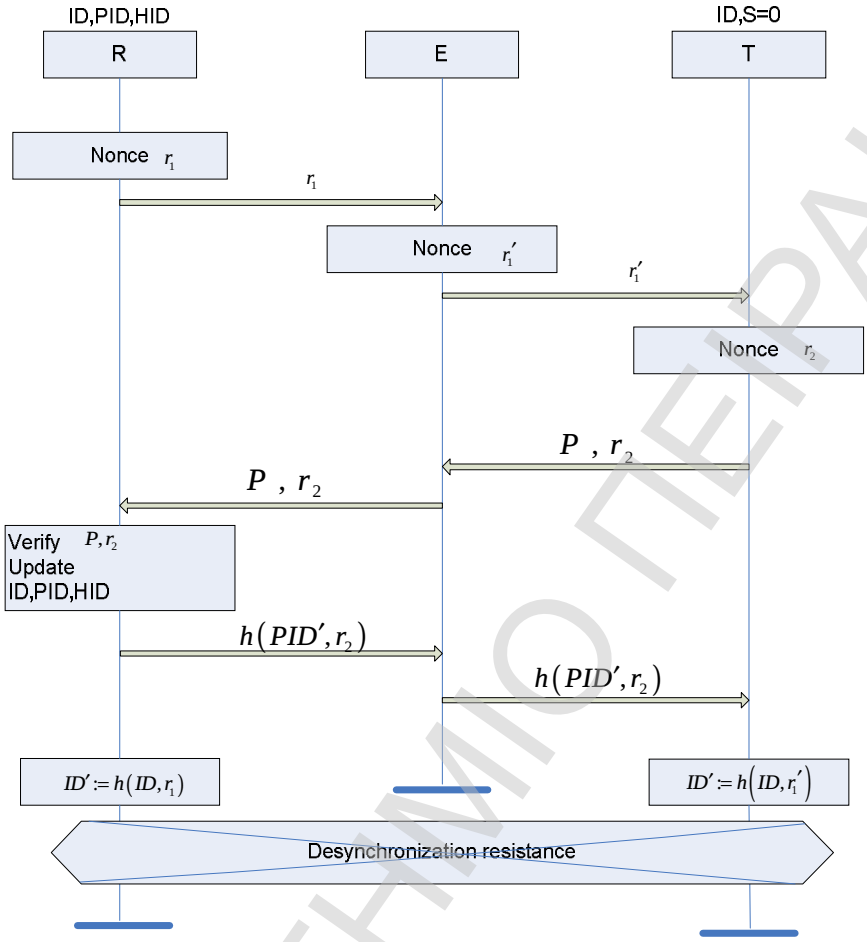
Εικόνα 3.4: Το Πρωτόκολλο

3.4.3 Σχετικά Πρωτόκολλα

Τα πρωτόκολλα [LY07c, LY07a, LY07b, HM04] είναι πρωτόκολλα τα οποία **βασίζονται σε ενέργεια πρόκλησης-απάντησης και έχουν παρόμοιο πρόβλημα** αυθεντικοποίησης. Ένα παρόμοιο μη ανιχνεύσιμο πρόβλημα στο [HM04] βρέθηκε από [Avo05]. Εκεί μια επίθεση ποιότητας χρόνου χρησιμοποιείται για να αυξήσει τον εσωτερικό μετρητή μιας ετικέτας σε ένα μη φυσιολογικό επίπεδο προκειμένου στην συνέχεια να γίνει αναγνώριση της ετικέτας T.



Εικόνα 3.5: Επίθεση στην επικύρωση της ετικέτας

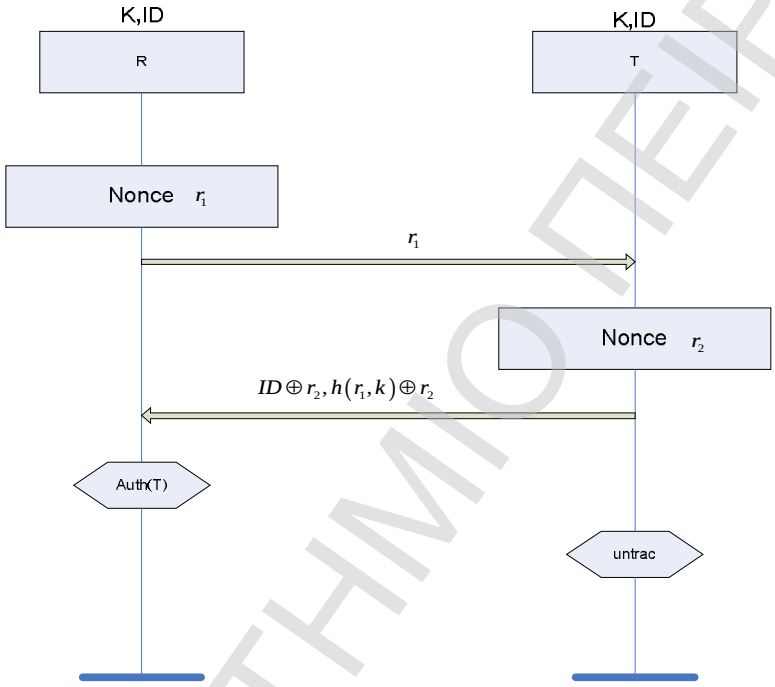


Εικόνα 3.6: Επίθεση στην αντίσταση αποσυνγχρονισμού

3.5 [KCL07]

3.5.1 Περιγραφή

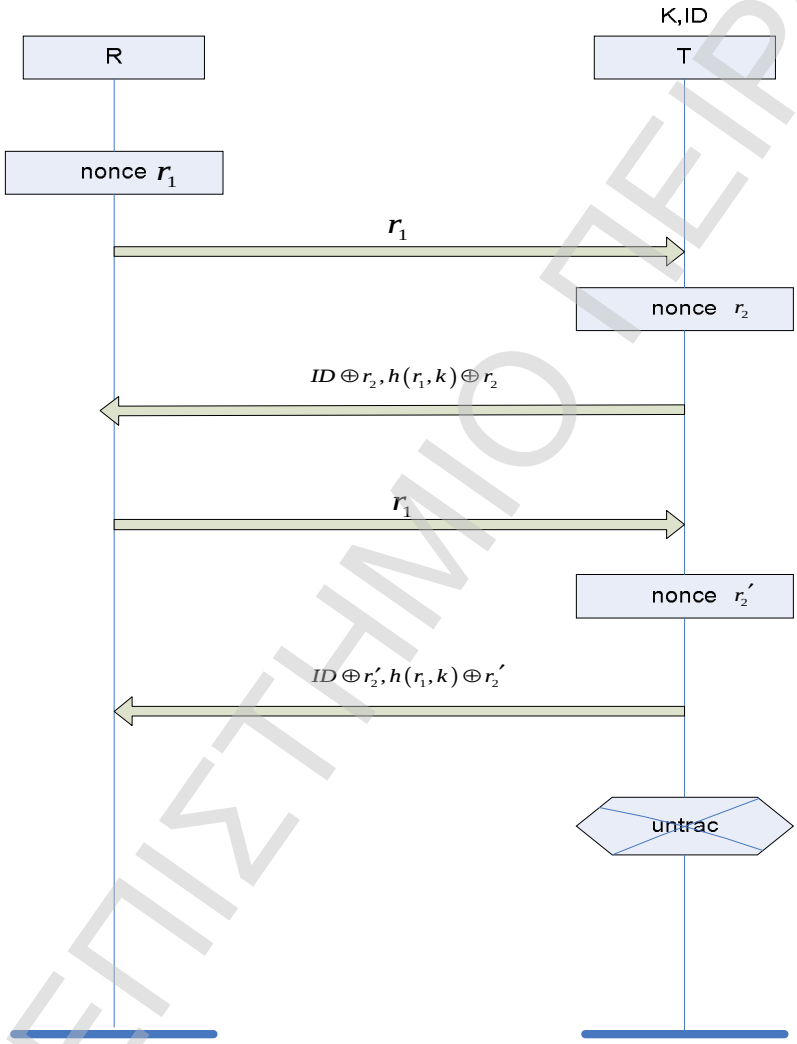
Το πρωτόκολλο παρουσιάζεται στην εικόνα 7.



Εικόνα 7: Το πρωτόκολλο KCL07

3.5.2 Επιθέσεις (claimed attacks)

3.5.2.1 Μη ανιχνευσιμότητα (μη δυνάμενο να αντιγραφεί)



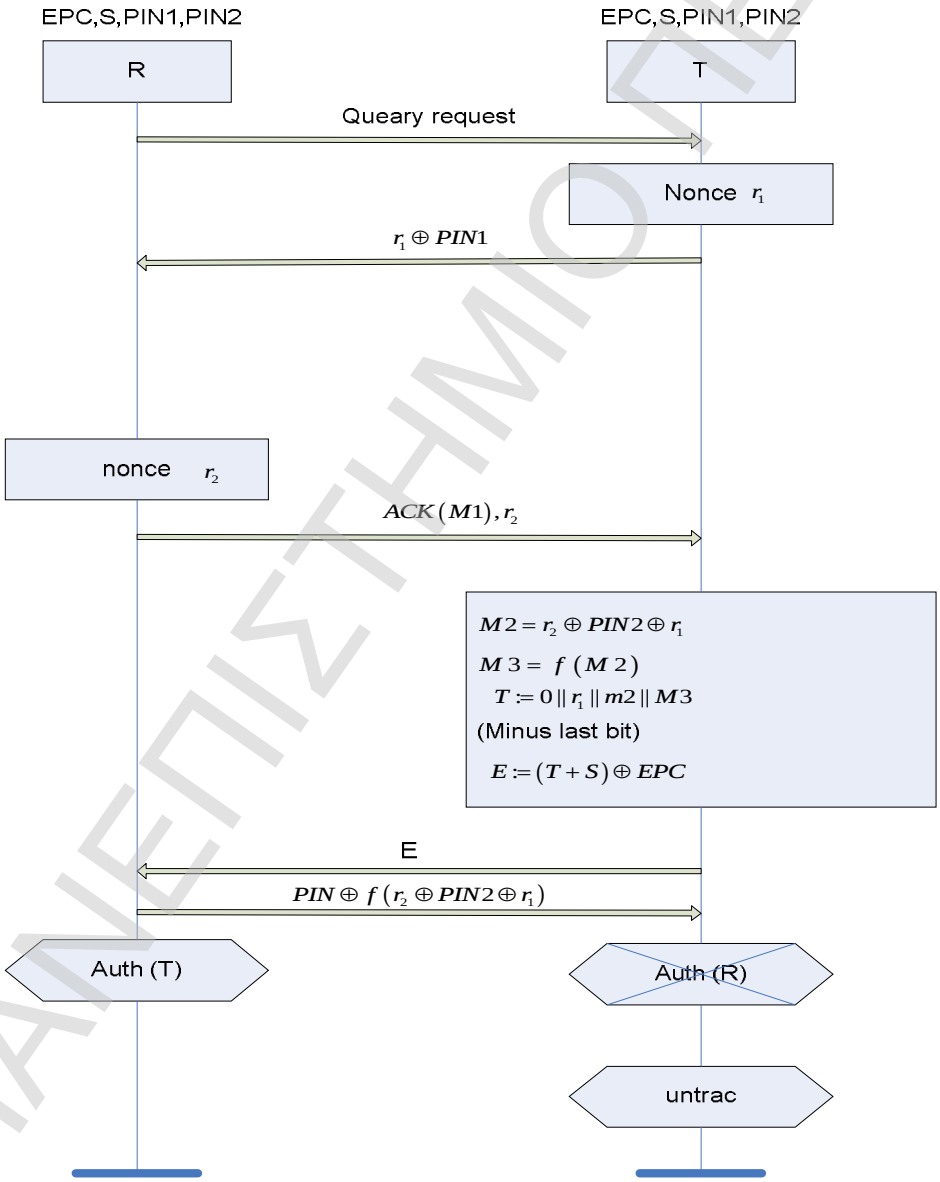
Εικόνα 8: Επίθεση στην μη ανιχνευσιμότητα

Ο επιτιθέμενος προκαλεί την ετικέτα δύο φορές με το ίδιο μοναδιαίο. Υπολογίζει στη συνέχεια την *XOR* συνάρτηση από τις δύο απαντήσεις $ID \oplus r_2$ και $h(r_1,k) \oplus r_2$. Ο επιτιθέμενος λαμβάνει $ID \oplus h(r_1,k)$, εάν και μόνο ήταν δύο φορές η ίδια ετικέτα που έχει προσβληθεί. Η επίθεση αυτή απεικονίζεται στο σχήμα 9.

3.6 [KCLL06]

3.6.1 Περιγραφή

Το πρωτόκολλο απεικονίζεται στο σχήμα 9. Στην αρχική προδιαγραφή, τα bit ελέγχου του πρωτοκόλλου (PC) και ένας μηχανισμός ανίχνευσης και ελέγχου (CRC) διαβιβάζονται στο τέταρτο μήνυμα. Αυτά είναι άσχετα με οποιεσδήποτε από τις εξεταζόμενες ιδιότητες ασφάλειας και επομένως δεν λαμβάνονται υπόψη.



Εικόνα 3.9 : Το πρωτόκολλο

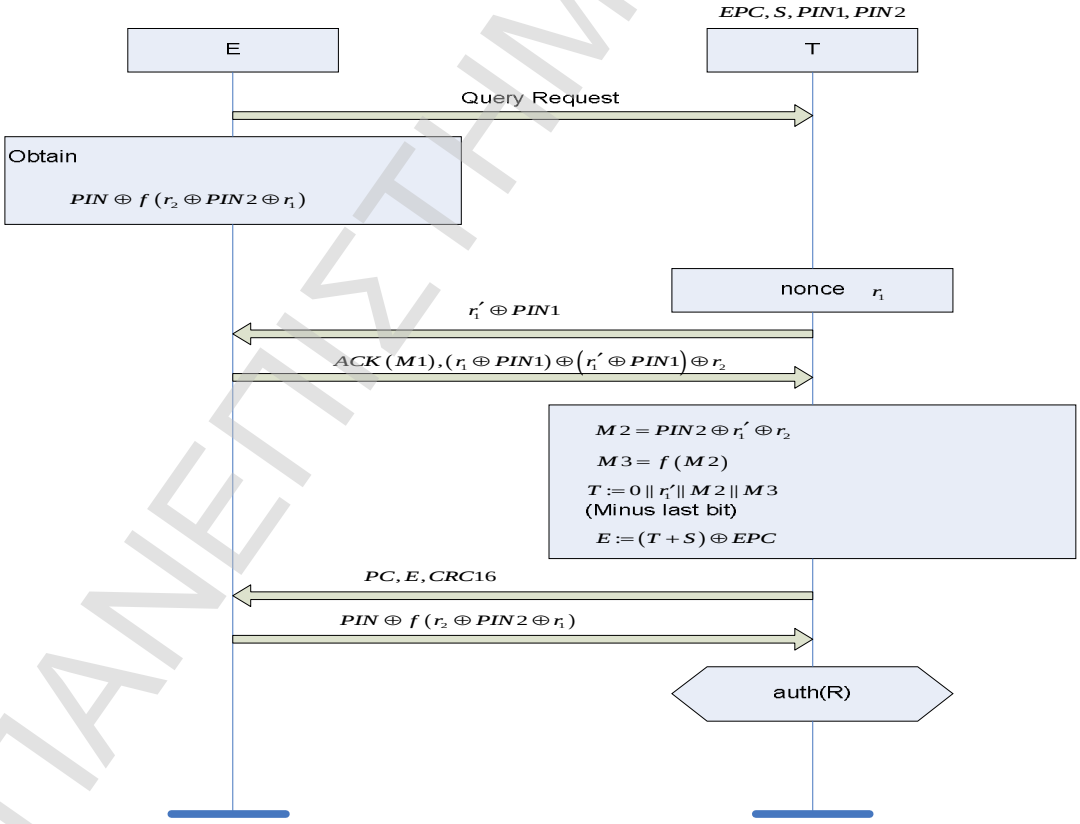
3.6.2 Σχετικά Πρωτόκολλα

3.6.2.1 Επικύρωση Αναγνώστη

Ο επιτιθέμενος μπορεί να προσποιηθεί ένα νόμιμο αναγνώστη στέλνοντας ένα μοναδικό r_2' που επιτρέπει σε αυτόν να επαναλάβει ένα μήνυμα που παρατήρησε προηγουμένως ως τελευταίο μήνυμα. Προκειμένου να είναι σε θέση να επαναλάβει την $PIN \oplus f\left(r_2 \oplus PIN2 \oplus r_1\right)$ σε μια άλλη επικοινωνία, πρέπει να ικανοποιείται: $r_1 \oplus r_2 = r_1' \oplus r_2'$. Αυτό μπορεί να επιτευχθεί θέτοντας r_2' σε $r_1 \oplus r_2 \oplus r_1'$. Η επίθεση απεικονίζεται στο σχήμα 10.

3.6.3 Σχετικά Πρωτόκολλα

Έχουμε παρόμοιες επιθέσεις στα πρωτόκολλα [CH07,LAK06,SM08].

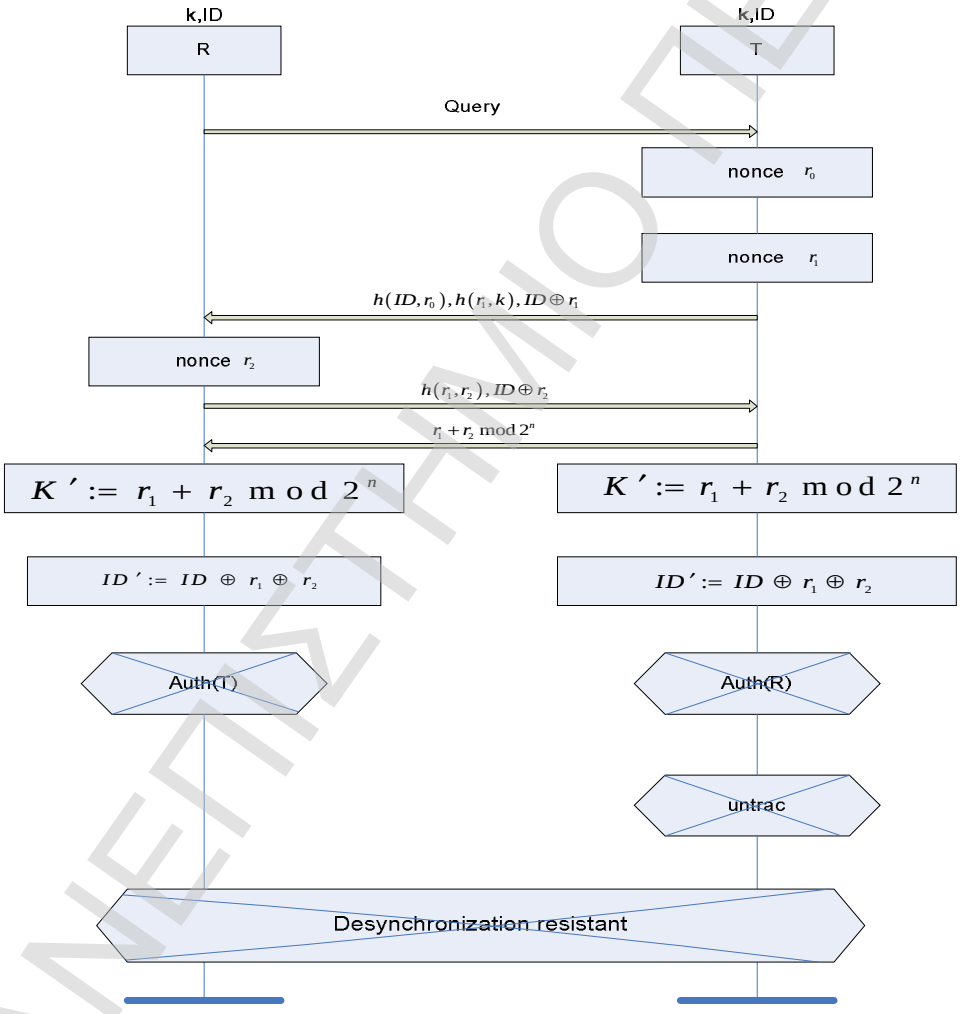


Εικόνα 3.10: Επίθεση στην επικύρωση της ετικέτας

3.7 [KN05]

3.7.1 Περιγραφή

Το πρωτόκολλο απεικονίζεται στην εικόνα 11. Σημειώνουμε ότι το r_0 επιλέγεται από μια μικρή περιοχή, και μπορεί επομένως να δεχθεί επίθεση «brute-force» από $h(ID, r_0)$ εάν το ID είναι γνωστό.



Εικόνα 3.11 : Το πρωτόκολλο

3.7.2 Επιθέσεις

3.7.2.1 Επικύρωση ετικέτας T

Ένας επιτιθέμενος ο οποίος υποκλέπτει είναι σε θέση να βρει bit της ID συνδυάζοντας $h(ID, r_0)$, $ID \oplus r_1$, $ID \oplus r_2$, και $r_1 + r_2 \bmod 2^n$ που παρατηρείται στα τελευταία τρία μηνύματα του πρωτοκόλλου. Για δική μας ευκολία θέτουμε $V = r_1 + r_2 \bmod 2^n$ και $W = ID \oplus r_1 \oplus ID \oplus r_2 = r_1 \oplus r_2$. Συγκρίνουμε το ι-στο bit $V[i]$ του V με το ι-στο bit $W[i]$ του W, για $1 \le i < n$, όπου τα bit $V[1]$ και $W[1]$ είναι τα λιγότερο σημαντικά κομμάτια των V και W, αντίστοιχα. Κατά την σύγκριση αυτών των δύο με κρυπτογράφηση XOR, αποδεικνύεται ότι $V[i+1] \neq W[i+1]$ μόνο εάν ο υπολογισμός του $V[i]$ οδηγεί σε μεταφερόμενο bit. Σε αυτήν την περίπτωση $r_1[i] \neq r_2[i]$ εάν και μόνο εάν $W[i] = 1$ και $r_1[i] = r_2[i] = 1$ εάν και μόνο εάν $W[i] = 0$. Δεδομένου ότι η τελευταία περίπτωση καθορίζει τα $r_1[i]$ και $r_2[i]$ μεμονωμένα, σημαίνει ότι μπορεί να χρησιμοποιηθεί για να βρεθεί το ι-οστό bit της ταυτότητας ID. Περισσότερα bit από την ID μπορούν να ληφθούν με την σημείωση ότι μεταφέρουν bit στο $V[i]$ ακολουθούμενο από τα μη μεταφερόμενα bit στο $V[i+1]$ που συνεπάγεται $r_1[i+1] = r_2[i+1] = 0$.

Δεδομένου ότι r_1 και r_2 επιλέγονται τυχαία, κατά μέσον όρο, κάθε σύναψη επικοινωνίας έχει έλλειμμα περίπου $\frac{n-1}{4}$ bit της ID. Αποκάλυψη όλων των bit της ταυτότητας ID, από την στιγμή που πολλά bit είναι γνωστά, μπορεί να επιτευχθεί με μια αναζήτηση «brute force» πέρα από τις πιθανές τιμές της ταυτότητας ID και του r_0 και συγκρίνοντας την συνάρτηση κατακερματισμού τους (hash) με το χ (ταυτότητα, r0). Η αποκάλυψη όλων bit της ταυτότητας περιπλέκεται από το γεγονός ότι ο αναγνώστης και η ετικέτα ανανεώνουν την ταυτότητα στο τέλος κάθε εκτέλεσης του πρωτοκόλλου θέτοντας την $ID \oplus r_1 \oplus r_2$. Ο επιτιθέμενος θα πρέπει να παρακολουθήσει περίπου τέσσερις διαδοχικές εκτελέσεις του πρωτοκόλλου μεταξύ της ετικέτας και του αναγνώστη πριν εκτελέσει μια εξαντλητική αναζήτηση προκειμένου να αποκαλυφθεί εντελώς η ταυτότητα της ετικέτας. Αποκαλύπτοντας την ταυτότητα της ετικέτας, σπάει η αυθεντικοποίηση του πρωτοκόλλου.

3.7.2.2 Αυθεντικοποίηση Αναγνώστη

Αποκαλύπτοντας την ταυτότητα της ετικέτας όπως είδαμε στην παράγραφο 6.2.1 σπάει η αυθεντικοποίηση του πρωτοκόλλου.

3.7.2.3 Μη ανιχνευσιμότητα

Αποκαλύπτοντας την ταυτότητα της ετικέτας όπως είδαμε στην παράγραφο 3.6.2.1 σπάει επίσης και η μη-ανιχνευσιμότητα του πρωτοκόλλου.

3.7.2.4 Αντίσταση Αποσυγχρονισμού

Αποκαλύπτοντας την ταυτότητα της ετικέτας όπως στην παράγραφο 6.2.1 σπάει και η αντίσταση αποσυγχρονισμού δεδομένου ότι ο αντίπαλος μπορεί ψευδώς να επικυρώσει είτε στον αναγνώστη είτε την ετικέτα. Το αποτέλεσμα είναι ότι ο αναγνώστης και η ετικέτα δεν είναι συγχρονισμένοι.

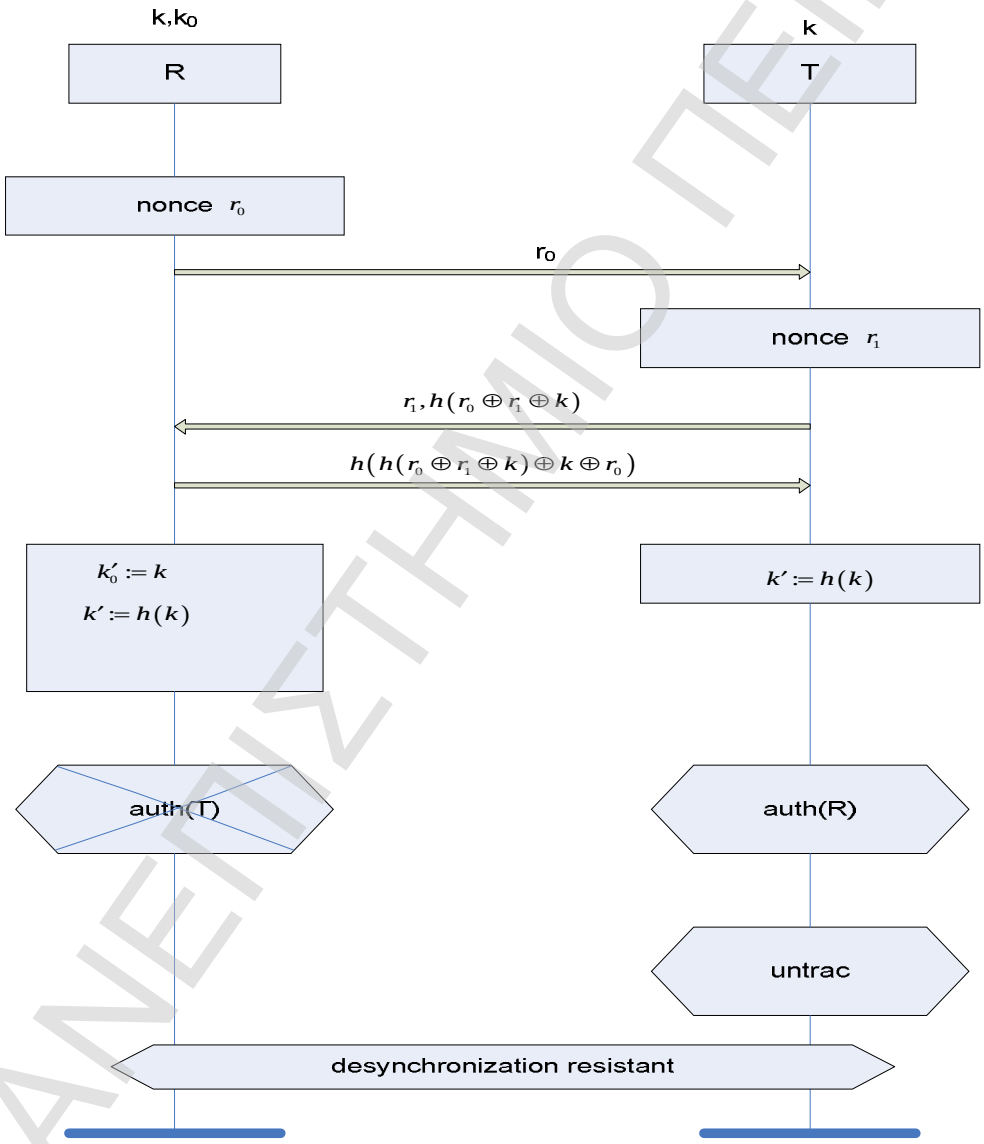
3.7.3 Σχετιζόμενα Πρωτόκολλα

Πολλές παρόμοια προβληματικά σημεία έχουν τεκμηριωθεί. Το πρωτόκολλο [CLL05] χρησιμοποιεί έναν μετρητή από κοινού με xor κρυπτογράφηση. Στο πρωτόκολλο [HMNB07b] η προβλεψιμότητα του μετρητή και η αλληλεπίδρασή του με το XOR χρησιμοποιείται για να σπάσει το πρωτόκολλο. Στα πρωτόκολλα [PLCETR06b, PLCETR06a, PLHCETR06] τα λογικά AND και OR χρησιμοποιούνται μαζί με το XOR και τη συναρτησιακή αριθμητική και οδηγούν προβληματικά σημεία που περιγράφονται στα [ALP07, LW07]. Η λειτουργία ελέγχου κυκλικού πλεονασμού χρησιμοποιείται με xor στο πρωτόκολλο [CC07] καταστώντας το προτεινόμενο πρωτόκολλο τρωτό στην προσωποποίηση των ετικετών και των αναγνωστών, και την ανιχνευσιμότητα των ετικετών κάτι που ανακαλύπτεται από το [PLHCETR07]. Τέλος, το [DFJ07] πρωτόκολλο σπάει την επικύρωση στο [VB03] όπου τοXOR χρησιμοποιείται με διάφορους bit-συνδυασμούς.

3.8 [LAK06]

3.8.1 Περιγραφή

Το πρωτόκολλο απεικονίζεται στην εικόνα 12.



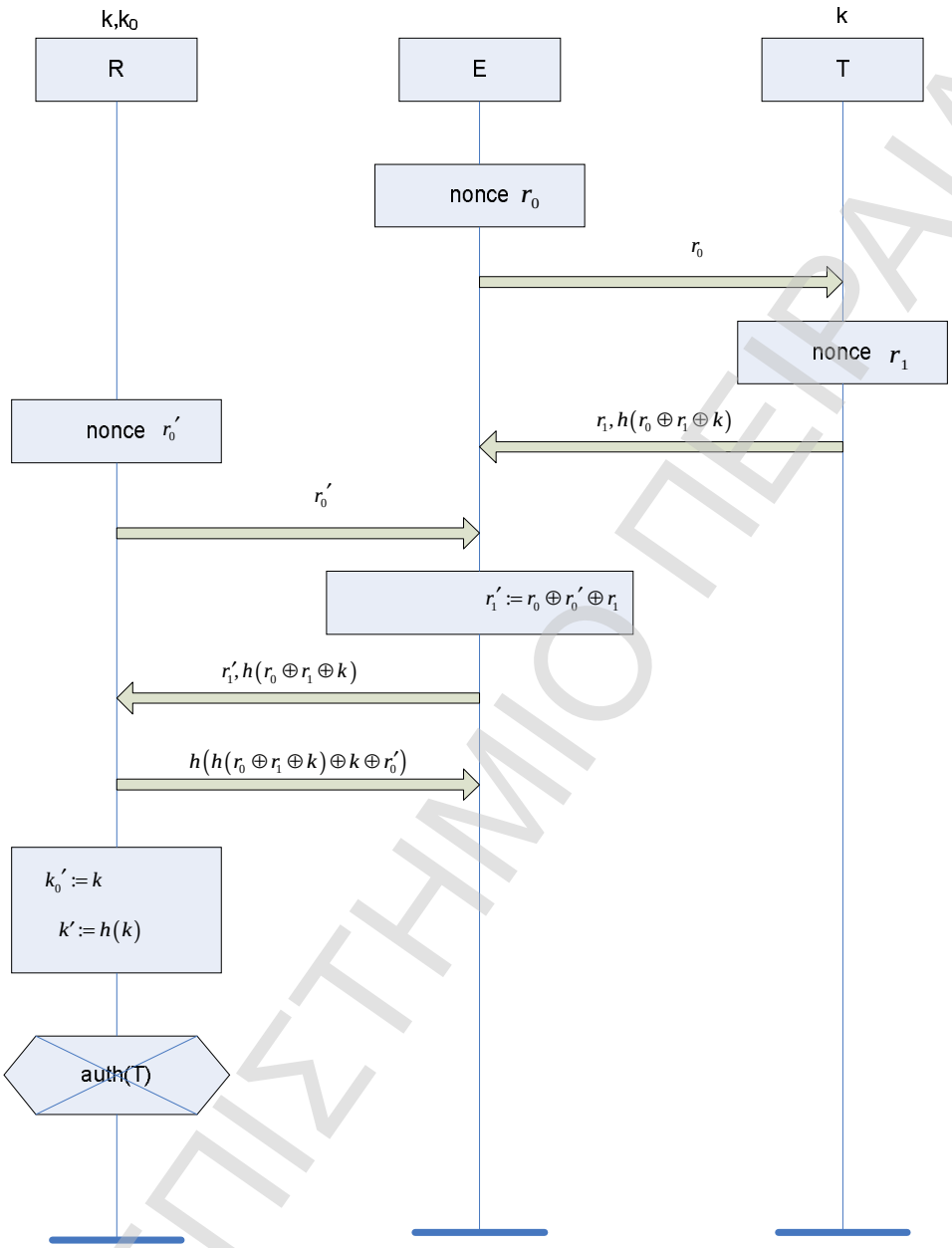
Εικόνα 3.12: Το πρωτόκολλο

3.8.2 Επιθέσεις

Η επίθεση απεικονίζεται στο σχήμα 13. Ο επιτιθέμενος μπορεί να επαναλάβει το $r_0 \oplus r_1 = r_0' \oplus r_1'$. Για να ικανοποιήσει αυτόν τον όρο ο επιτιθέμενος θέτει το r_1' σε $r_0 \oplus r_1 \oplus r_1'$

3.8.3 Σχετιζόμενα Πρωτόκολλα

Έχουν βρεθεί παρόμοιες επιθέσεις στα πρωτόκολλα [CH07, KCLL06, SM08].



Εικόνα 3.13: Επίθεση στην επικύρωση της ετικέτας

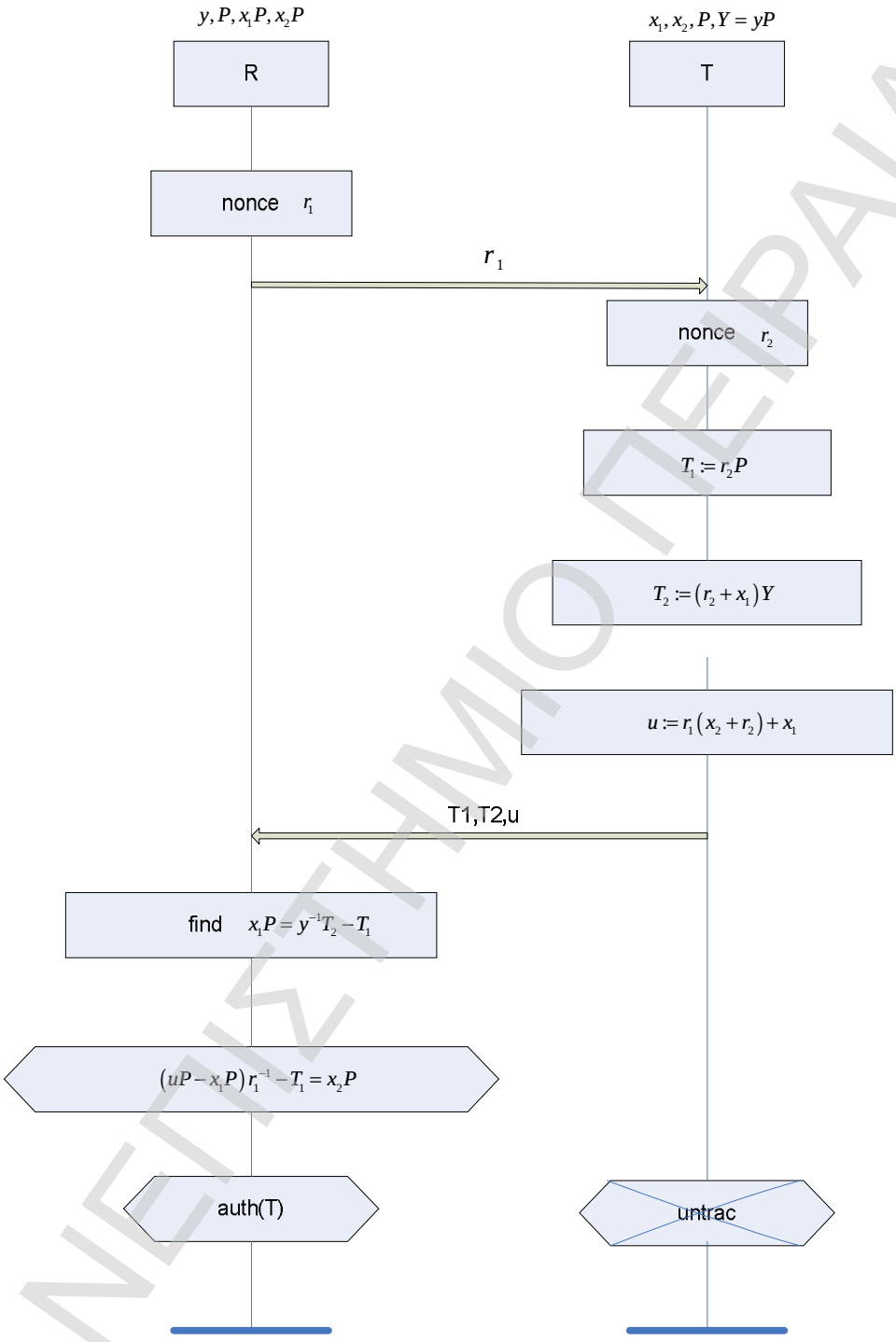
3.9 [LBV07]

3.9.1 Περιγραφή

Το πρωτόκολλο, που παρουσιάζεται στο σχήμα 16 στοχεύει να επικυρώσει αποτελεσματικά μια ετικέτα σε έναν αναγνώστη κρατώντας την ετικέτα μη ανιχνεύσιμή. Το πρωτόκολλο είναι βασισμένο σε μια σταθερή, σε όλο το σύστημα ελλειπτική καμπύλη πέρα από έναν πεπερασμένο τομέα.

Τα P , ${}_yP$, ${}_{x_1}P$, ${}_{x_2}P$ είναι δημόσια γνωστά σημεία πάνω στην ελλειπτική καμπύλη, το κλιμακωτό y είναι γνωστό μόνο στον αναγνώστη και τα κλιμακωτά x_1, x_2 είναι μοναδικά σε κάθε ετικέτα και γνωστά μόνο σε αυτήν. Η ελλειπτική καμπύλη υποτίθεται ότι είχε επιλεχτεί έτσι ώστε να είναι δύσκολο να υπολογιστούν τα x_1, x_2, y από τα ${}_{x_1}P$, ${}_{x_2}P$, ${}_yP$. Ο αναγνώστης προκαλεί την ετικέτα με έναν τυχαίο αριθμό r_1, η ετικέτα αποκρίνεται με δύο σημεία $T_1 = {}_{r_2}P$, στη $T_2 = {}_{(r_2+x_1)}Y$ πάνω στην ελλειπτική καμπύλη και ένα κλιμακωτό $u = r_1(x_2 + r_2) + x_1$.

Ο αναγνώστης συμπεραίνει την ταυτότητα της ετικέτας και την επικυρώνει από τα σημεία και τον κλιμακωτό ως εξής. Δεδομένου ότι ο αναγνώστης ξέρει το y μπορεί να υπολογίσει $y^{-1}T_2 - T_1 = X_1P$ για να λάβει την ταυτότητα της ετικέτας και να υπολογίσει έπειτα $(uP - x_1P)r_1^{-1} - T_1 = x_2P$ για να επικυρώσει την ετικέτα.



Εικόνα 3.14: Το πρωτόκολλο

3.9.2 Επιθέσεις

3.9.2.1 Μη ανιχνευσιμότητα

- Εάν η ετικέτα προκαλείται με $r_1 = 0$ η ετικέτα αποκρίνεται πάντα με $u = x_1$.
- Εάν η ετικέτα προκαλείται με $r_1 = 1$, οι πληροφορίες που λαμβάνονται από την απάντηση της ετικέτας, $T_1 = r_2 P$, $T_2 = (x_1 + 1)_y P$, $u = (x_2 + r_2) + x_1$ μπορούν να χρησιμοποιηθούν για να υπολογιστεί μια σταθερή, μοναδική τιμή για την ετικέτα $uP - T_1 = (x_1 + x_2) P$.
- Εάν μια ετικέτα προκαλείται δύο φορές, μία φορά με ένα τυχαίο r_1 και μία φορά με το $r_1' = r_1 + 1$, έπειτα οι πληροφορίες που παραλαμβάνονται από την ετικέτα στα δύο τρεξίματα μπορεί να χρησιμοποιηθούν για να υπολογιστεί ο σταθερός όρος $-x_2 P$ ως εξής. Οι πιο βασικοί όροι διαφαίνονται κατά το δεύτερο τρέξιμο. Παρατηρούμε ότι

$$u - u' = r_1 (x_2 + r_2) - (r_1 + 1)\left(x_2 + r_2'\right) = -x_2 - r_2' + r_1\left(r_2 - r_2'\right)$$

Έτσι μπορούμε να υπολογίσουμε

$$-x_2 P = (u - u') P + T_1' - r_1\left(T_1 - T_1'\right)$$

Από την στιγμή που οι όροι της δεξιάς μεριάς είναι γνωστοί.

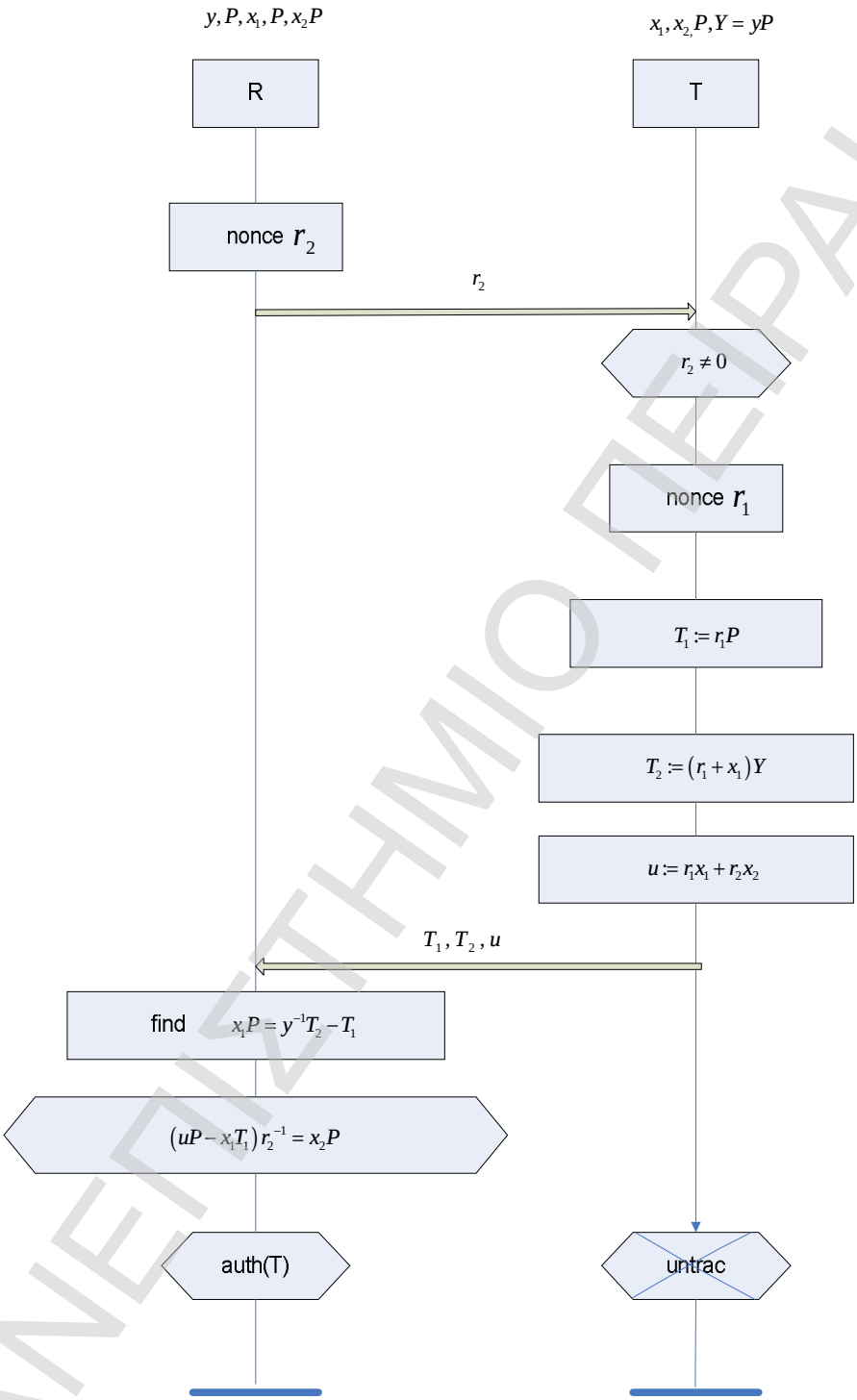
3.9.3 Σχετιζόμενα Πρωτόκολλα

Το [LBV08] είναι μια βελτίωση του πρωτοκόλλου [LBV07] αλλά εξετάζει μόνο τις πρώτα δύο προβληματικά σημεία που απαριθμούνται στην παράγραφο 8.2.1 και όχι το τρίτο.

3.10 [LBV08]

3.10.1 Περιγραφή

Το πρωτόκολλο, που παρουσιάζεται στο σχήμα 15 στοχεύει να επικυρώσει αποτελεσματικά μια ετικέτα σε έναν αναγνώστη διατηρώντας την ετικέτα μη ανιχνεύσιμη. Το πρωτόκολλο είναι βασισμένο σε μια σταθερή, σε ολόκληρο το σύστημα ελλειπτική καμπύλη πέρα από έναν πεπερασμένο πεδίο. Τα $P, Y = {}_{y}P, {}_{x_1}P, {}_{x_2}P$ είναι δημόσια γνωστά σημεία στην ελλειπτική καμπύλη, το κλιμακωτό Y είναι γνωστό μόνο στον αναγνώστη, τα κλιμακωτά x_1, x_2 είναι μοναδικά σε κάθε ετικέτα και είναι γνωστά μόνο σε αυτήν. Η ελλειπτική καμπύλη υποτίθεται ότι είχε επιλεχτεί έτσι ώστε να είναι δύσκολο να υπολογιστούν τα x_1, x_2, y από τα ${}_{x_1}P, {}_{x_2}P, {}_{y}P$.



Εικόνα 3.15: Το πρωτόκολλο

3.10.2 Επιθέσεις

3.10.2.1 Μη Ανιχνευσιμότητα

Ο επιτιθέμενος πραγματοποιεί δύο συνδέσεις με την ετικέτα και στέλνει το ίδιο μοναδικό r_2 και στις δύο. Στην συνέχεια υπολογίζει $u-u'=\left(r_1-r_1'\right)x_1$ και $T_1-T_1'=\left(r_1-r_1'\right)P$. Υπολογίζοντας κατά συνέπεια το αντίστροφο του $u-u'$ στα πλαίσια της ελλειπτικής καμπύλης, ο επιτιθέμενος λαμβάνει $x_1^{-1}P$ κάτι που προσδιορίζει την ετικέτα μοναδικά.

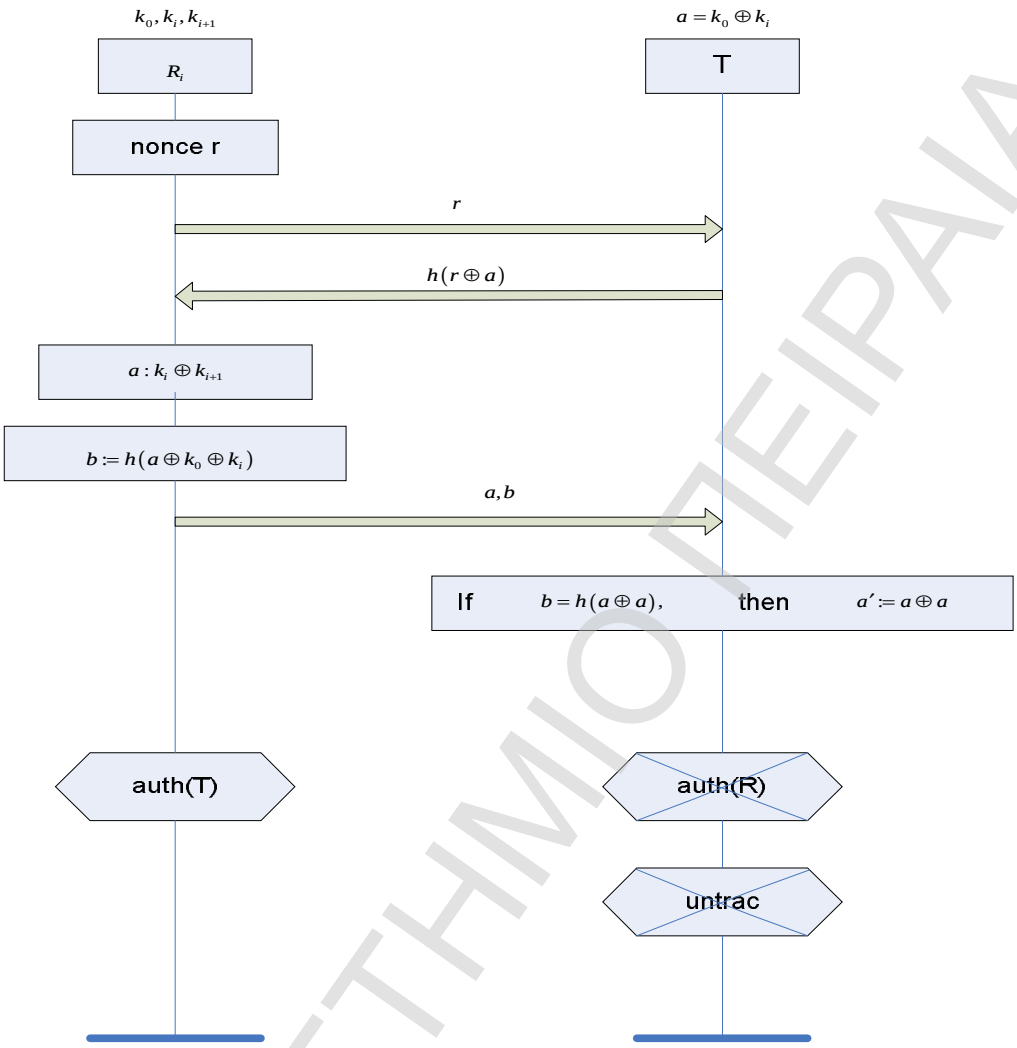
3.10.3 Σχετιζόμενα Πρωτόκολλα

Αυτό είναι μια βελτίωση του πρωτοκόλλου [LBV07].

3.11 [LD07]

3.11.1 Περιγραφή

Το [LD07] πρωτόκολλο σχεδιάστηκε για τη χρήση στις αλυσίδες εφοδιασμού. Κάθε αλυσίδα εφοδιασμού αποτελείται από μια αλυσίδα συνεργατών, κάθε μια από τις οποίες αντιπροσωπεύεται από έναν αναγνώστη. Ο αναγνώστης R_i και η ετικέτα μοιράζονται τον μυστικό κωδικό k_0. Επιπλέον, ο αναγνώστης R_i ξέρει τα μυστικά k_i και k_{i+1}.



Εικόνα 3.16: Το πρωτόκολλο

3.11.2 Επιθέσεις

3.11.2.1 Μη Ανιχνευσιμότητα

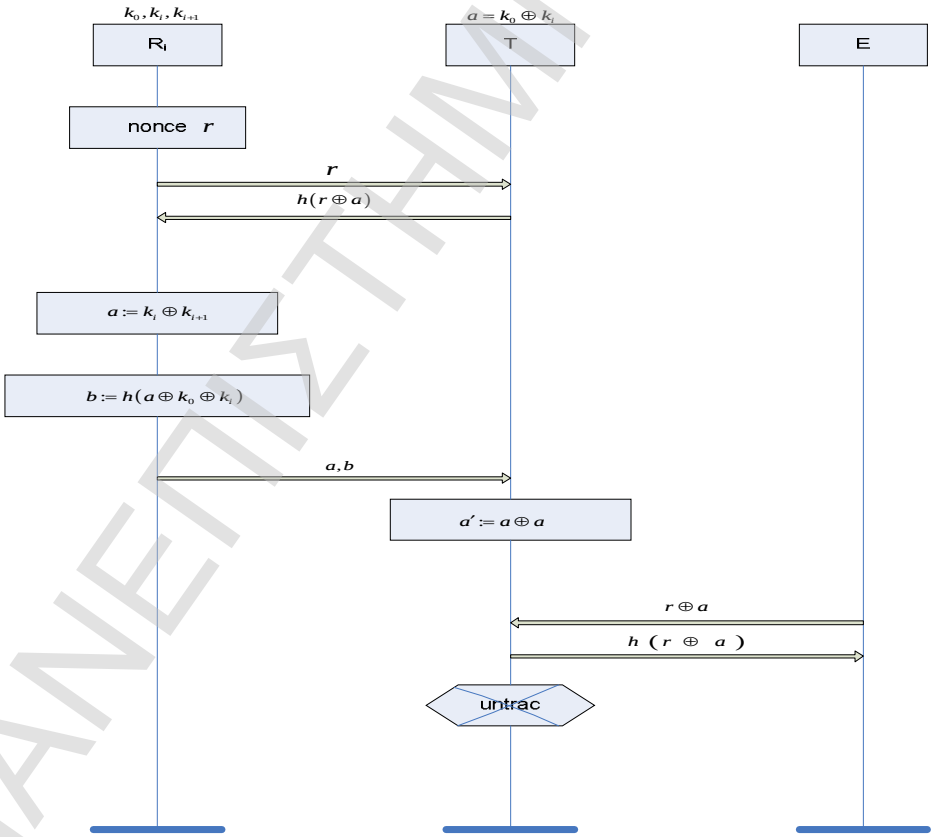
Το πρωτόκολλο δεν ικανοποιεί την μη ανιχνευσιμότητα όσον αφορά στις ετικέτες, των οποίων ο ρόλος είναι να αναγνωρίζουν τους συντάκτες του πρωτοκόλλου και ως εκ τούτου να μην πέφτουν σε απάτη. Αυτό γίνεται επειδή μεταξύ οποιωνδήποτε δύο ανανεώσεων του a, ένας επιτιθέμενος που στέλνει δύο φορές την ίδια πρόκληση r στην ίδια ετικέτα, θα λάβει δύο φορές την ίδια απάντηση.

Ο συντάκτης προσπαθεί να πετύχει μη ανιχνευσιμότητα, αν και αδύναμη, η οποία δημιουργείται από τις συνεχείς ανανεώσεις. Η επίθεση παρουσιάζεται στο σχήμα 18 και επιτυγχάνεται ως εξής. Παρακολουθώντας την σύνδεση επικύρωσης ο αντίπαλος μαθαίνει το $r, h(r \oplus a), a$ και το b. Ο επιτιθέμενος μπορεί τώρα να ρωτήσει την ετικέτα με $r' = r \oplus a$, στο οποίο η ετικέτα θα αποκριθεί με το $h(r' \oplus a')$. Αυτή η απάντηση είναι ίση με αυτήν που παρατηρήσαμε προηγουμένως.:

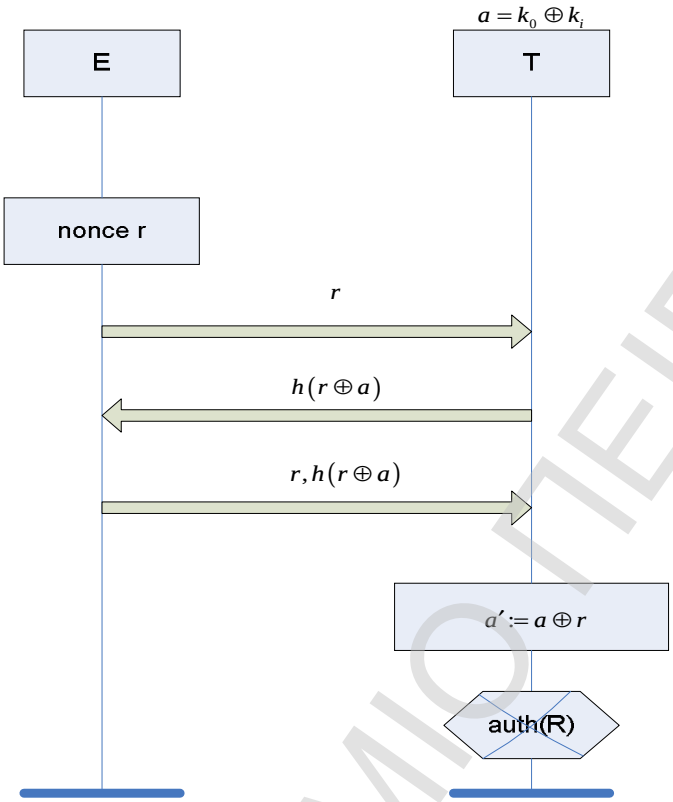
$$h(r' \oplus a') = h(r \oplus a \oplus a \oplus a) = h(r \oplus a) \qquad (2)$$

3.11.2.2 Ταυτοποίηση Αναγνώστη

Η επικύρωση αναγνωστών μπορεί να σπάσει θέτοντας $a = r$ και $b = h(r \oplus a)$. Η ετικέτα δέχεται το a και το b, επειδή $b = h(a \oplus a) = h(r \oplus a)$. Η επίθεση παρουσιάζεται στην εικόνα 18. Αυτή η επίθεση οδηγεί επίσης σε αποσυγχρονισμό της βάσης δεδομένων και της ετικέτας.



Εικόνα 3.17: Επίθεση στην μη ανιχνευσιμότητα



Εικόνα 3.18: Επίθεση στην ταυτοποίηση του Αναγνώστη

3.11.3 Σχετιζόμενα Πρωτόκολλα

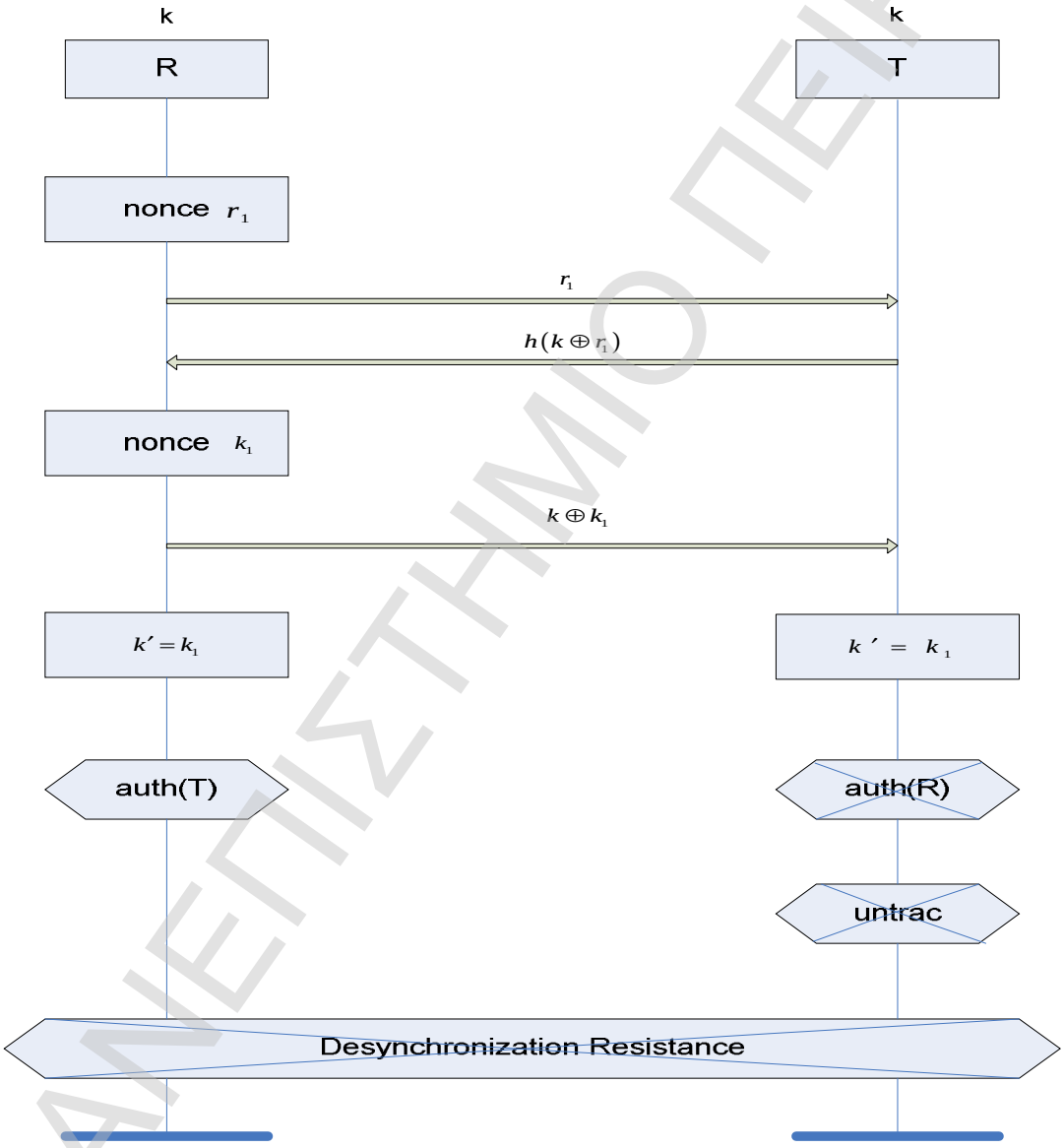
Έχουν βρεθεί παρόμοιες επιθέσεις στην μη ανιχνευσιμότητα στα [YPL+05, OTYT06, KCL07].

Το πρωτόκολλο [LCUL06] είναι τρωτό σε μια απλούστερη μορφή αυτής της επίθεσης που έχει παρουσιαστεί στο [CH07].

3.12 [OTYT06]

3.12.1 Περιγραφή

Το πρωτόκολλο παρουσιάζεται στην εικόνα 19.



Εικόνα 3.19: Το πρωτόκολλο

3.12.2 Επιθέσεις

3.12.2.1 Ταυτοποίηση Αναγνώστη

Δεδομένου ότι η ετικέτα δεν ξέρει το νέο κλειδί k_1, η ετικέτα δεν είναι ικανή να ελέγξει εάν το τρίτο μήνυμα είναι πράγματι $k \oplus k_1$. Δεδομένου ότι κανένας έλεγχος δεν μπορεί να εκτελεστεί από την ετικέτα, ο επιτιθέμενος μπορεί να στείλει ένα τυχαίο μήνυμα r στην ετικέτα που θα αναγκάσει την ετικέτα να αντικαταστήσει το k από το $k \oplus r$.

3.12.2.2 Αντίσταση Αποσυνχρονισμού

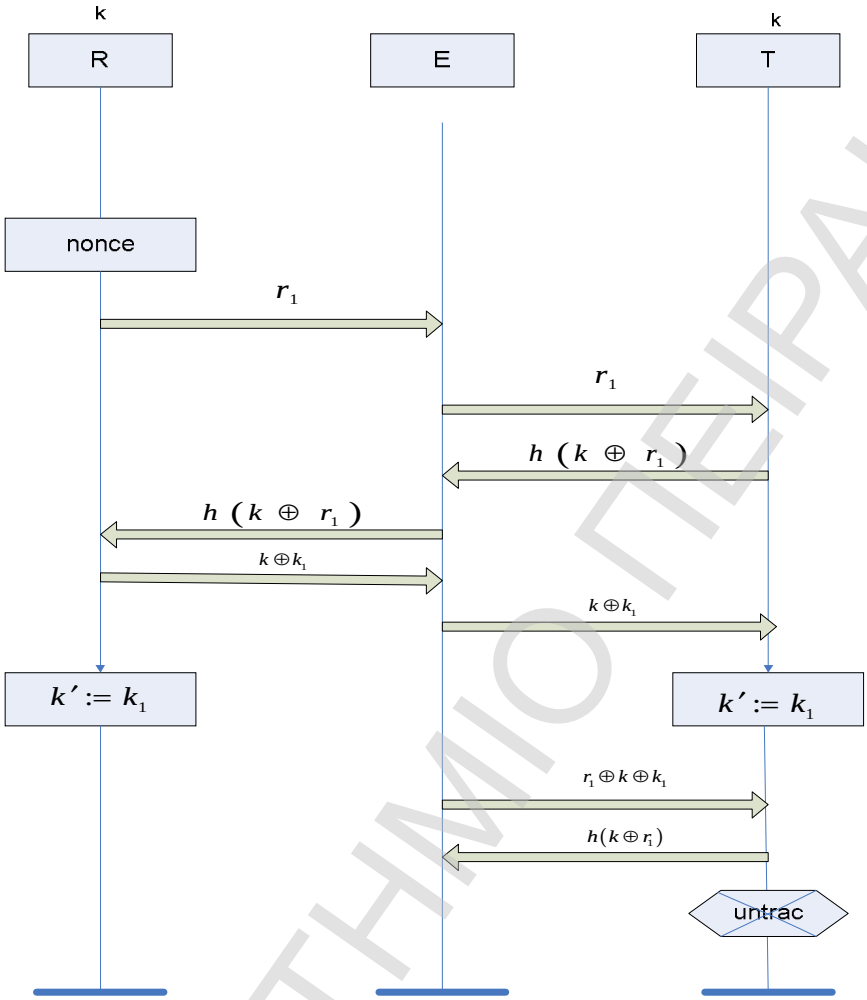
- Η επίθεση στην επικύρωση αναγνωστών αποσυγχρονίζει το μυστικό κλειδί k, το οποίο είναι κοινό μεταξύ της ετικέτας και του αναγνώστη, καθιστώντας τη μελλοντική επικύρωση αδύνατη. Σημειώστε ότι ο επιτιθέμενος είναι το μόνο πρόσωπο που μπορεί να επανασυγχρονίσει τις μυστικές πληροφορίες μεταξύ του αναγνώστη και της ετικέτας δεδομένου ότι είναι το μόνο πρόσωπο που ξέρει το $k \oplus r$.

- Τροποποιώντας το τρίτο μήνυμα μεταξύ ετικέτας και αναγνώστη οδηγούνται στο να έχουν διαφορετικές ενημερώσεις στο μυστικό κλειδί, παραμένοντας αποσυγρονισμένα.

- Μην επιτρέποντας το τελευταίο μήνυμα να φτάσει από τον αναγνώστη στην ετικέτα, έχουμε ως αποτέλεσμα να έχει ανανεώσει ο αναγνώστης το k, ενώ η ετικέτα δεν διαθέτει αυτή την πληροφορία κάτι που οδηγεί σε μη συγχρονισμένη κατάσταση .

3.12.2.3 Μη Ανιχνευσιμότητα

Ένας επιτιθέμενος που παρατηρεί μια ολοκληρωμένη διαδικασία του πρωτοκόλλου λαμβάνει ένα τριπλό στοιχείο $\left(r, h\left(k \oplus r\right), k \oplus k_1\right)$. Μπορεί τώρα να προκαλέσει μια ετικέτα με $r \oplus k \oplus k_1$ δίνοντας της την ίδια απάντηση που παρατήρησε ήδη, υπό τον όρο ότι η ετικέτα είναι η ίδια με αυτήν που είχε υποκλέψει πιο πριν. Η επίθεση απεικονίζεται στο σχήμα 20 .



Εικόνα 3.20: Επίθεση στην μη ανιχνευσιμότητα

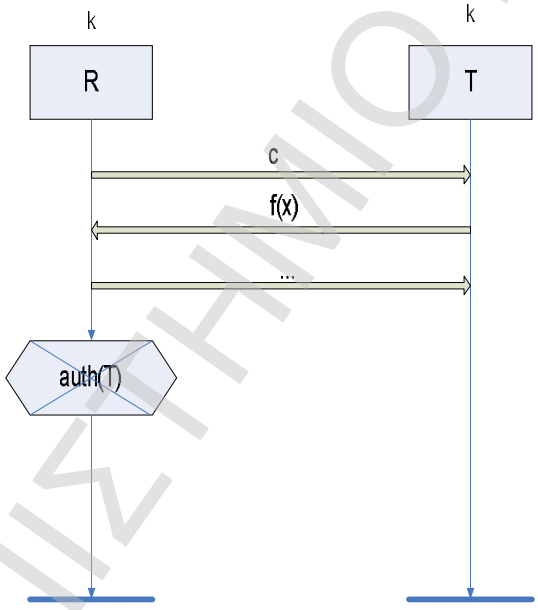
3.13 Σχετιζόμενα Πρωτόκολλα

Έχουν παρατηρηθεί παρόμοια προβλήματα στα πρωτόκολλα [YPL+05, KCL07]

3.14 [LY07a, LY07c, LY07b, HM04]

3.14.1 Περιγραφή

Όπως απεικονίζεται στην εικόνα 21 τα πρωτόκολλα έχουν μια δομή πρόκλησης-απάντησης. Ο αναγνώστης προκαλεί την ετικέτα, η ετικέτα υπολογίζει μια συνάρτηση με έναν ή περισσότερους όρους και στέλνει το αποτέλεσμα στον αναγνώστη. Εντούτοις, η πρόκληση δεν χρησιμοποιείται από την ετικέτα ως δεδομένο της συνάρτησης.



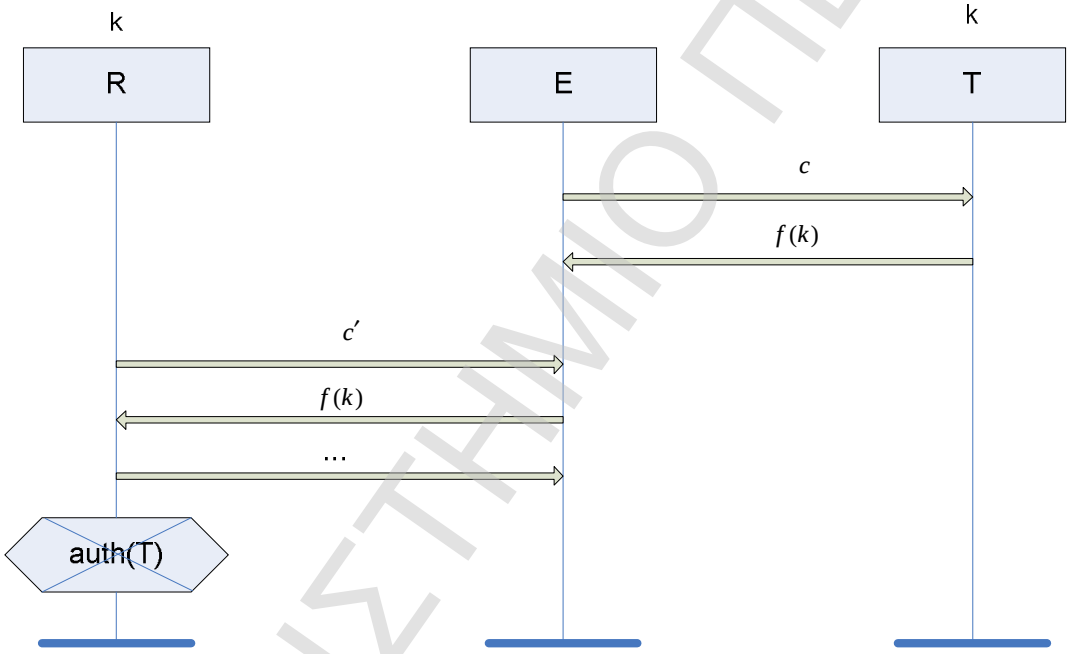
Εικόνα 3.21: Γενική δομή πρωτοκόλλου

3.14.2 Επιθέσεις

3.14.2.1 Επικύρωση Ετικέτας

Επειδή η απάντηση της ετικέτας δεν εξαρτάται από την πρόκληση του αναγνώστη, ένας επιτιθέμενος μπορεί να ρωτήσει μια ετικέτα και να χρησιμοποιήσει την απάντηση σε πιθανή μελλοντική ερώτηση του αναγνώστη.

Επομένως, κανένα από αυτά τα πρωτόκολλα δεν ικανοποιεί την αξίωση της ζωτικότητας όσον αφορά στο ρόλο των ετικετών. Η γενική δομή της επίθεσης απεικονίζεται στο σχήμα 22.



Εικόνα 3.22: Επίθεση στην επικύρωση της ετικέτας.

3.14.3 Σχετιζόμενα Πρωτόκολλα

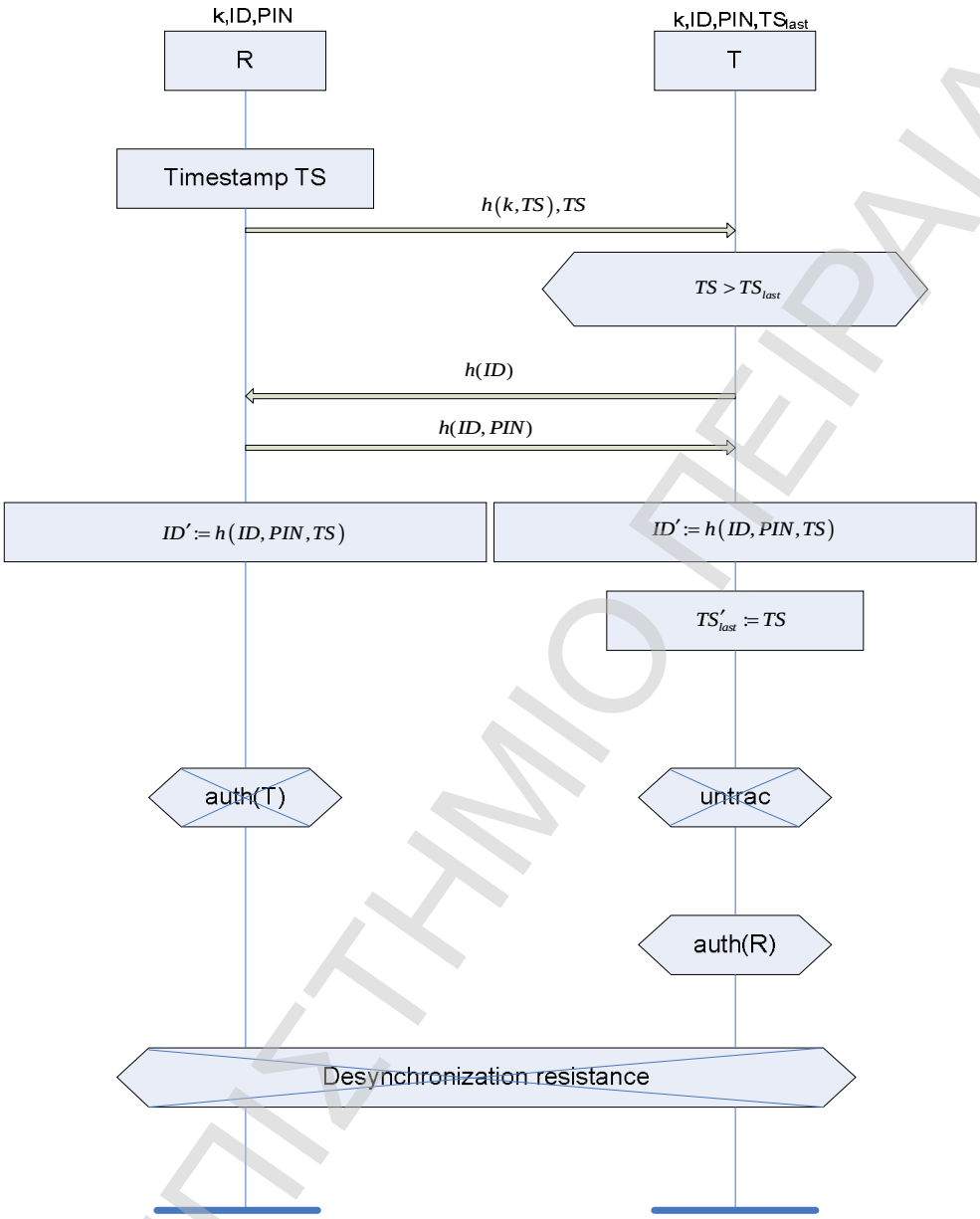
Τα πρωτόκολλα [SLK06, HMNB07a] υποφέρουν από το ίδιο πρόβλημα

3.15 [SLK06]

3.15.1 Περίληψη

Το πρωτόκολλο υποθέτει ότι ο αναγνώστης και η ετικέτα μοιράζονται τα μυστικά k, ταυτότητα ID, και ένα κωδικό (PIN).

Ενώ η ταυτότητα ID και το PIN είναι μοναδικά σε κάθε ετικέτα, το k είναι ίδιο για όλες τις ετικέτες που ο αναγνώστης έχει την άδεια να επικυρώσει. Η ετικέτα αποθηκεύει ακόμα την χρονική στιγμή TS_{last} της τελευταίας επιτυχούς αμοιβαίας επικύρωσης που αρχικοποιείται σε 0 στο εργοστάσιο. Το πρωτόκολλο απεικονίζεται στην εικόνα 23 .



Εικόνα 3.23: Το πρωτόκολλο

3.15.2 Επιθέσεις

3.15.2.1 Επικύρωση Ετικέτας

Για την επίθεση στο πρωτόκολλο, αρκεί να σημειωθεί ότι η πρόκληση του αναγνώστη και η απάντηση της ετικέτας δεν συσχετίζονται. (ενότητα 12) .

3.15.2.2 Αντίσταση Αποσυγχρονισμού

Η επίθεση που περιγράφεται στην παράγραφο της 13.2.1 οδηγεί σε μια κατάσταση στην οποία ο αναγνώστης ενημερώνει την ταυτότητα, αλλά η ετικέτα όχι. Το ίδιο αποτέλεσμα μπορεί να επιτευχθεί με το φράξιμο του τελευταίου μηνύματος από έναν αναγνώστη σε μια ετικέτα. Αυτό σκοτώνει ουσιαστικά την ετικέτα δεδομένου ότι ο αναγνώστης δεν θα δεχτεί το μήνυμα $h(ID)$ της ετικέτας (ταυτότητα) σε ένα μελλοντικό τρέξιμο πρωτοκόλλου.

3.15.2.3 Μη Ανιχνευσιμότητα

Το γεγονός ότι ένας αναγνώστης και η ετικέτα δεν συμφωνούν σχετικά με την τιμή της ταυτότητας, δηλ. είναι μη συγχρονισμένα, είναι εύκολο να παρατηρηθεί, δεδομένου ότι σε αυτή την περίπτωση ο αναγνώστης ολοκληρώνει το πρωτόκολλο νωρίς. Κατά συνέπεια ο αντίπαλος μπορεί να επισημάνει τέτοιες ετικέτες. Επιπλέον, όταν μια ετικέτα δεν συγχρονίζεται, δεν θα είναι σε θέση να ενημερώσει την ταυτότητα ID και το TS_{last} άλλο, κατά συνέπεια η απάντησή της σε οποιαδήποτε έγκυρη πρόκληση $h(k,TS),TS$ με $TS > TS_{last}$ θα παραμείνει ότι σταθερή αφήνοντας τον επιτιθέμενο να διακρίνει μεταξύ πρόσφατα αποσυγχρονισμένες ετικέτες και πιο παλιά μη συγχρονισμένες ετικέτες.

3.15.3 Σχετιζόμενα Πρωτόκολλα

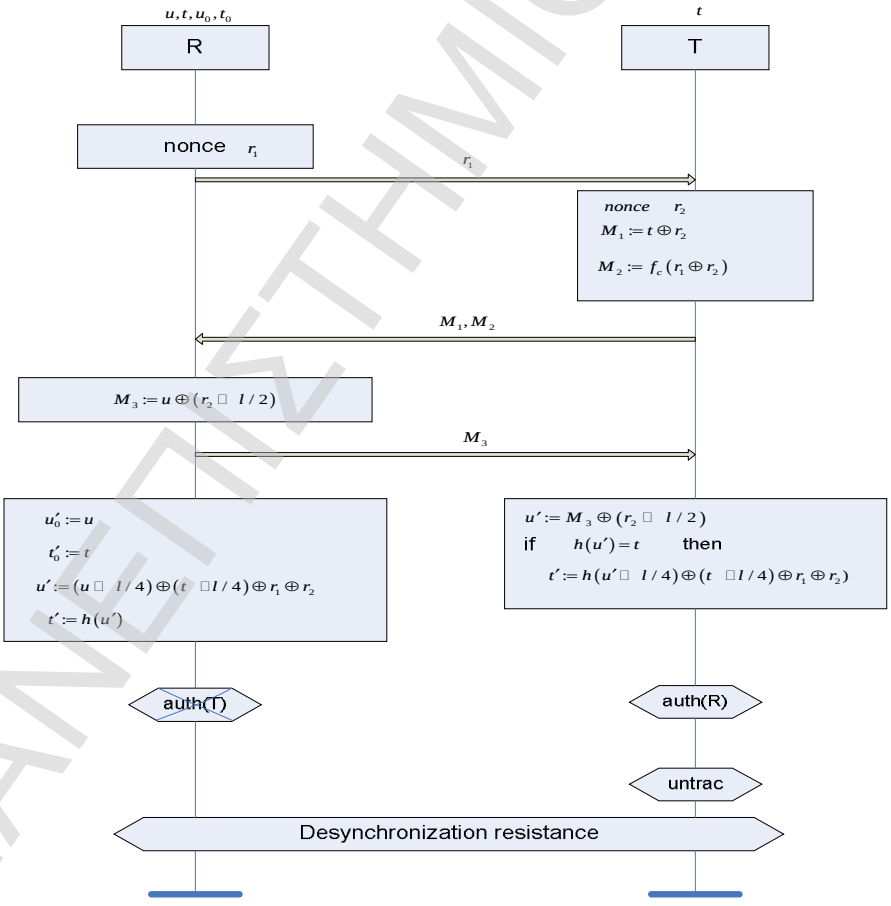
Τα ίδια προβλήματα επικύρωσης παραουσιάζονται στα πρωτόκολλα [LY07e, Ly07a,LY07b,HMNB07a**]**

Στο [Avo05] παρουσιάζεται. μια ποιοτική χρονική επίθεση στην προσπάθεια μη ανιχνευσιμότητας του σταθερού πρωτοκόλλου [HM04]. Η επίθεση περιλαμβάνει την αύξηση του εσωτερικού μετρητή μιας ετικέτας προς μη ομαλό επίπεδο προκειμένου να αναγνωριστεί η ετικέτα αργότερα.

3.16 [SM08]

3.16.1 Επικύρωση Ετικέτας

Το πρωτόκολλο απεικονίζεται στο σχήμα 24. Οι περιστροφές bit δείχνονται από και όπου το a b σημαίνει ότι το a έχει μετατοπιστεί κυκλικά δεξιόστροφα από τα b bits. Η συνάρτηση f_t που χρησιμοποιούνται για να υπολογιστεί το M_2 είναι μια hash λειτουργία, όπου t είναι το κλειδί.



Εικόνα 24 : Το πρωτόκολλο

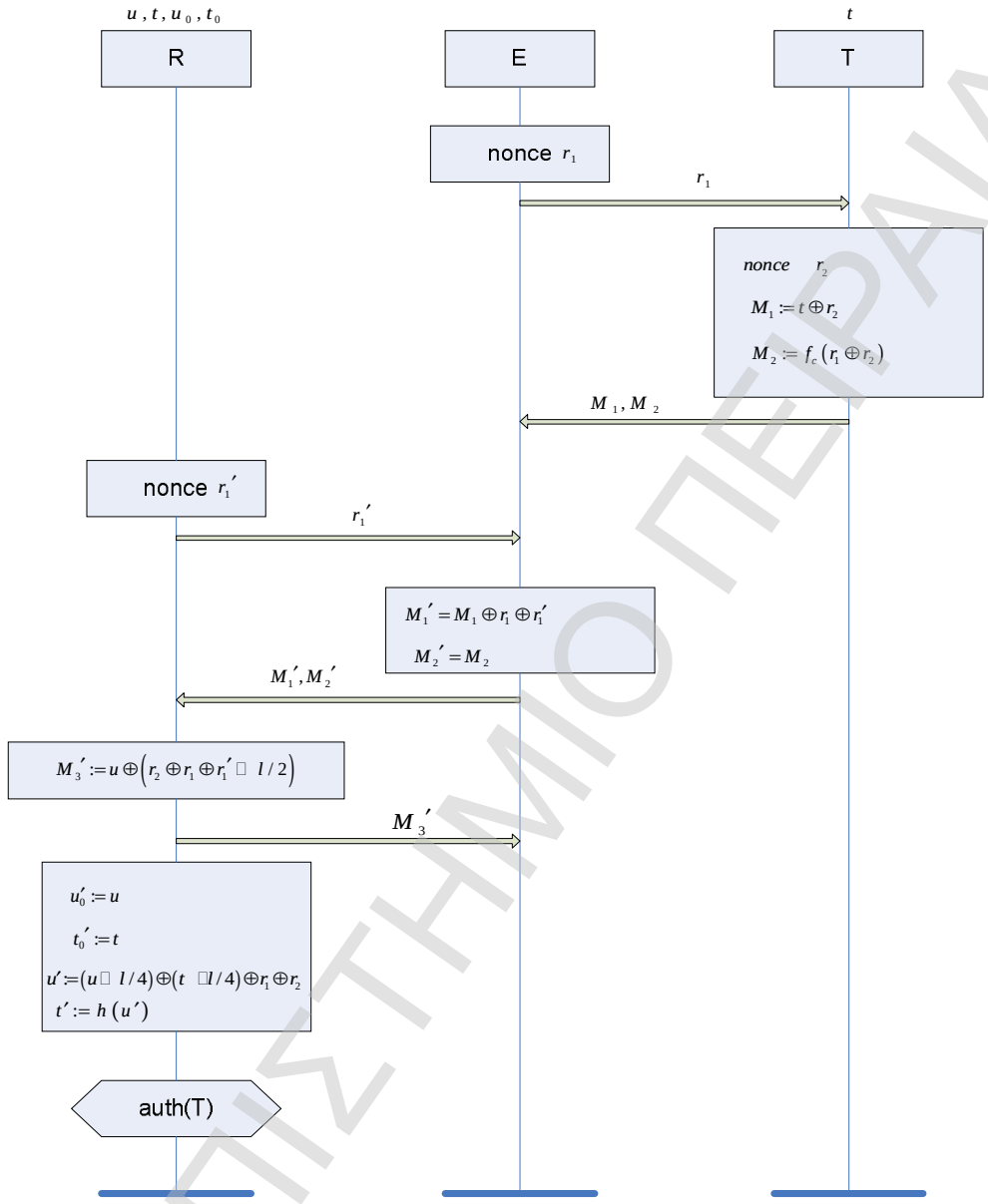
3.16.2 Επιθέσεις

3.16.2.1 Επικύρωση Ετικέτας

Η επίθεση στην επικύρωση ετικετών απεικονίζεται στο σχήμα 26. Ο επιτιθέμενος χρησιμοποιεί το γεγονός ότι μπορεί να επαναλάβει M_2 για το M_2' εάν είναι σίγουρος ότι $r_1 \oplus r_2 = r_1' \oplus r_2'$. Για να ικανοποιείται αυτός ο όρος θέτει M_1' σε $M_1 \oplus r_1 \oplus r_1'$.

3.16.3 Σχετιζόμενα Πρωτόκολλα

Έχουν παρατηρηθεί παρόμοιες επιθέσεις στα πρωτόκολλα [CH07, LAK06, KCLL06].

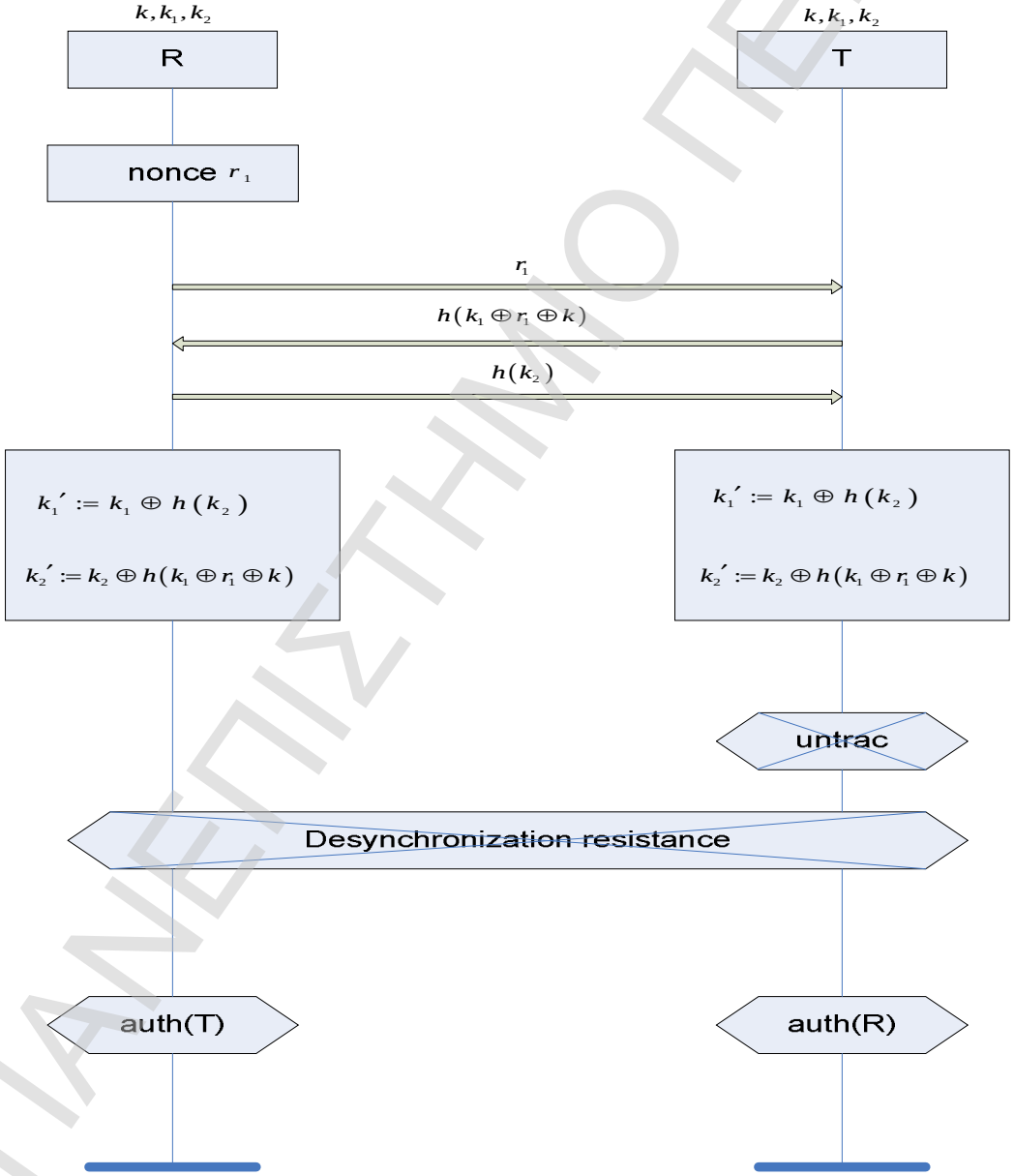


Εικόνα 3.25: Επίθεση στην επικύρωση της ετικέτας

3.17 [YPL+05]

3.17.1 Περιγραφή

Η Εικόνα 26 απεικονίζει το πρωτόκολλο.



Εικόνα 3.26: Το πρωτόκολλο

3.17.2 Επιθέσεις

3.17.2.1 Μη Ανιχνευσιμότητα

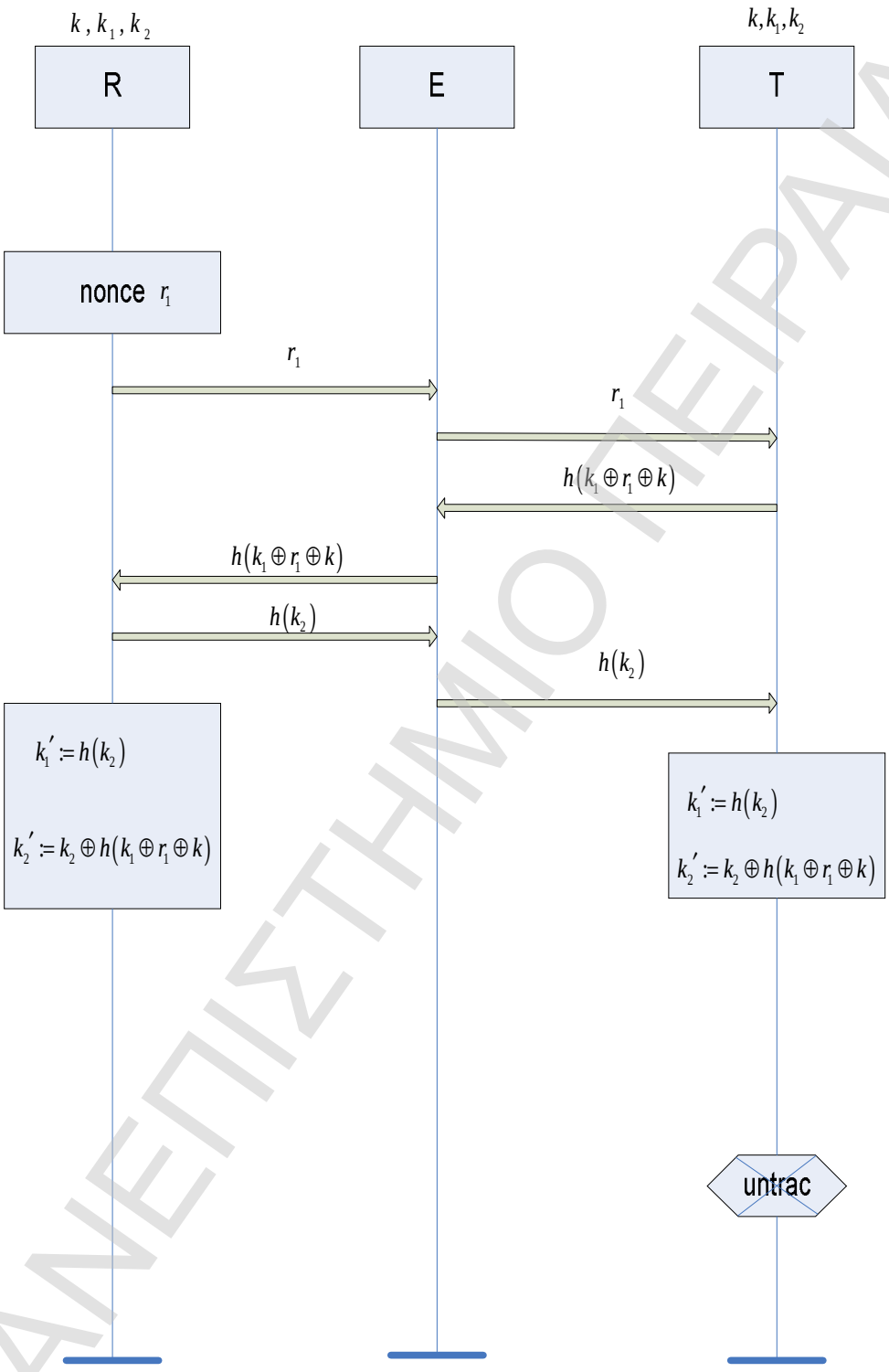
Ένας επιτιθέμενος που υποκλέπτει μια σύνοδο επικοινωνίας του πρωτοκόλλου λαμβάνει τα μηνύματα $r_1, h(k_1 \oplus r_1 \oplus k), h(k_2)$. Ο αναγνώστης και η ετικέτα ενημερώνουν έπειτα τους μυστικούς κωδικούς τους. Ο επιτιθέμενος μπορεί να αναγνωρίσει την ετικέτα προκαλώντας την με $r_1 \oplus h(k_2)$ στο οποίο η προηγουμένως παρατηρηθείσα ετικέτα θα αποκριθεί με $h(k_1 \oplus r_1 \oplus k)$. Το σχήμα 27 απεικονίζει την επίθεση.

3.17.2.2 Αντίσταση Αποσυγχρονισμού

Το μπλοκάρισμα του τρίτου μηνύματος του πρωτοκόλλου από τον αναγνώστη στην ετικέτα, οδηγεί τον αναγνώστη στην ενημέρωση του μυστικών του ενώ η ετικέτα δεν τους ενημερώνει. Επομένως, οι μυστικές πληροφορίες μεταξύ του αναγνώστη και της ετικέτας θα είναι μη συγχρονισμένες, καθιστώντας τη μελλοντική επικύρωση αδύνατη.

3.17.3 Σχετιζόμενα Πρωτόκολλα

Καταγράφονται παρόμοια προβλήματα στα πρωτόκολλα [ΟΤΥΤ06,ΚΨΛ07]



Εικόνα 3.27: Επίθεση στη μη ανιχνευσιμότητα

ΚΕΦΑΛΑΙΟ 4

ΠΑΡΑΓΡΑΦΟΣ 4.1

Ένα βέλτιστο πρωτόκολλο επικύρωσης RFID ενάντια στις Relay επιθέσεις

4.1.1 Περίληψη

Οι Relay επιθέσεις είναι ένα σημαντικό πρόβλημα για τα συστήματα RFID: κατά τη διάρκεια μιας διαδικασίας επικύρωσης ένας επιτιθέμενος αναμεταδίδει χωρίς να φαίνονται, τα μηνύματα μεταξύ ενός ελεγκτή.

Παρακάτω παρουσιάζεται ένα πρωτόκολλο επικύρωσης το οποίο ταιριάζει με τα συστήματα RFID. Η λύση αυτή είναι η πρώτη που αποτρέπει τις Relay επιθέσεις χωρίς υποβάθμιση του επιπέδου ασφάλειας επικύρωσης: ελαχιστοποιεί την πιθανότητα να δέχεται ο ελεγκτής πλαστή απόδειξη της ταυτότητας, εάν μια Relay επίθεση συμβαίνει ή όχι.

4.1.2 Εισαγωγή

Η RFID επικοινωνία επιτρέπει την αναγνώριση αντικειμένων χωρίς οποιαδήποτε φυσική ή οπτική επαφή, χρησιμοποιώντας αναμεταδότες-μικροκυκλώματα με μια κεραία που επικοινωνεί με τους αναγνώστες μέσω ενός καναλιού ραδιοσυχνότητας. Αυτή η τεχνολογία είναι μια από τις πλέον πολλά υποσχόμενες αυτής της δεκαετίας και ήδη χρησιμοποιείται ευρέως στις εφαρμογές όπως οι κάρτες πρόσβασης σε κτήρια, οι κάρτες επιβίβασης-αποβίβασης στις μεταφορές, οι κάρτες πληρωμής, και τα διαβατήρια. Αυτή η ευρεία αποδοχή οφείλεται εν μέρει στην σταθερή μείωση του μεγέθους και του κόστους των παθητικών αναμεταδοτών που αποκαλούνται ετικέτες.

Η Relay επίθεση η οποία για πρώτη φορά συζητήθηκε από τους Desmedt, Goutier, και Bengio πρόσφατα έγινε ένα σημαντικό θέμα ανησυχίας για τα πρωτόκολλα επικύρωσης RFID. Ο επιτιθέμενος προσποιείται ότι συμμετέχει νόμιμα, αναμεταδίδοντας μηνύματα που ανταλλάσσονται κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου. Αυτό μπορεί να διαπιστωθεί μέσω του ακόλουθου παραδείγματος.

Θεωρούμε ότι υπάρχει μια μηχανή πώλησης εισιτηρίων που βασίζεται στην τεχνολογία RFID. Για να αγοράσει ένα εισιτήριο, ο πελάτης δεν πρέπει για να

παρουσιάσει την θεατρική του κάρτα (πάσο), μια ετικέτα RFID. Ο πελάτης πρέπει να πλησιάσει αρκετά κοντά στη μηχανή (ελεγκτής) έτσι ώστε η ετικέτα να επικοινωνήσει με τον αναγνώστη. Η RFID κάρτα μπορεί να παραμείνει στην τσέπη του πελάτη κατά την επικοινωνία. Θεωρούμε ακόμα ότι υπάρχει μια μεγάλη ουρά με πελάτες που θέλουν να προμηθευτούν εισιτήρια. Δυο άτομα διεξάγουν την Relay επίθεση. Έστω ο Νίκος και ο Κώστας. Ο Νίκος βρίσκεται μπροστά στην μηχανή ενώ ο Κώστας πίσω στην ουρά δίπλα στην Μαρία, το θύμα. Μόλις η μηχανή αρχικοποιήσει την συναλλαγή με την κάρτα του Νίκου, ο Νίκος θα προωθήσει το λαμβανόμενο σήμα στον Κώστα, ο οποίος με την σειρά του θα το μεταδώσει στην Μαρία. Η ετικέτα της κάρτας του θύματος θα απαντήσει αυτόματα μιας και οι παθητικές RFID ετικέτες που χρησιμοποιούνται συνήθως για αυτές τις εφαρμογές απαντούν χωρίς να χρειάζονται την εξουσιοδότηση του κατόχου. Η απάντηση στην συνέχεια αναμεταδίδεται στο μηχάνημα αγοράς μέσω του Κώστα και του Νίκου οι οποίοι δρουν σαν ενδιάμεσοι. Ολόκληρη η επικοινωνία ολοκληρώνεται διαφανώς και η επίθεση πετυχαίνει τελικά: Η Μαρία πληρώνει το εισιτήριο του Νίκου.

Όταν αρχικά εισήχθη προς το τέλος της δεκαετίας του '80, η Relay επίθεση χαρακτηρίστηκε μη ρεαλιστική. Σήμερα, η Relay επίθεση είναι μια από τις αποτελεσματικότερες επιθέσεις ενάντια στα συστήματα RFID. Μπορεί να εφαρμοστεί εύκολα δεδομένου ότι ο αναγνώστης και η ετικέτα επικοινωνούν ασύρματα, και δεν είναι εύκολα ανιχνεύσιμη από το θύμα επειδή οι ενεργοποιημένες (παθητικές) ετικέτες απαντούν αυτόματα στα αιτήματα των αναγνωστών χωρίς κάποια περαιτέρω επικύρωση. Πρόσφατα, οι Halvac και Rosa παρατήρησαν ότι το πρότυπο ISO 14443, το οποίο είναι σχετικό με τις κάρτες πιστοποίησης προσώπου και που επεκτείνεται ευρέως στα βιομετρικά διαβατήρια μπορεί εύκολα να προσβληθεί από μια Relay επίθεση λόγω τον μη ασφαλισμένων διαλειμμάτων στην επικοινωνία.

Όλα τα τρέχοντα πρωτόκολλα επικύρωσης ενάντια στις Relay επιθέσεις αποδίδουν μάλλον κακώς ενάντια σε έναν επιτιθέμενο που δεν αναμεταδίδει τα μηνύματα. Εγγυώνται το ίδιο επίπεδο ασφάλειας ανεξάρτητα από τη δυνατότητα του επιτιθέμενου να αναμεταδώσει τα μηνύματα. Αυτό μπορεί να θεωρηθεί ως αδυναμία, και ιδιαίτερα στις καταστάσεις όπου οι Relay επιθέσεις είναι δύσκολο να εκτελεστούν.

Στην συνέχεια παρουσιάζεται ένα πρωτόκολλο επικύρωσης με το πλεονέκτημα ότι ελαχιστοποιεί την πιθανότητα ψεύτικης αποδοχής εάν μια Relay επίθεση εμφανίζεται ή όχι. Στην παράγραφο 2 παρουσιάζεται το πρωτόκολλό. Η παράγραφος 3 αφιερώνεται στην ανάλυση ασφάλειας. Η παράγραφος 4 εξετάζει την βελτιστοποίηση της λύσης αυτής. Στην παράγραφο 5 συγκρίνουμε το πρωτόκολλό με τα σχετικά πρωτόκολλα επικύρωσης.

4.1.3 Πρωτόκολλο

4.1.3.1 Απαιτήσεις και υποθέσεις πρωτοκόλλου

Παρουσία του νόμιμου δικαιούχου, το πρωτόκολλο επικύρωσης πρέπει να εγγυηθεί ότι ο ελεγκτής δέχεται πάντα την απόδειξη ταυτότητάς. Το πρωτόκολλο πρέπει επίσης να αποτρέψει έναν επιτιθέμενο να παρουσιάσει ψευδή στοιχεία με σκοπό να συμμετέχει είτε παθητικά είτε ενεργά στις εκτελέσεις πρωτοκόλλου ξεχωριστά με τον δικαιούχο, ξεχωριστά με τον ελεγκτή η και με τους δυο μαζί.

Αυτό σημαίνει ότι ο επιτιθέμενος μπορεί 1) να κρυφακούει τις εκτελέσεις του πρωτοκόλλου μεταξύ του νόμιμου δικαιούχου και του ελεγκτή (παθητική επίθεση), 2) να συμμετέχει χωρίς άδεια στις εκτελέσεις του πρωτοκόλλου ξεχωριστά με τον δικαιούχο, ξεχωριστά με τον ελεγκτή ή και με τους δυο μαζί (ενεργός επίθεση). Υποθέτουμε ότι ούτε ο νόμιμος δικαιούχος ούτε ο ελεγκτής δεν συνεργεί με τον επιτιθέμενο, δηλ., οι μόνες πληροφορίες που ο αντίπαλος μπορεί να λάβει είναι μέσω των εκτελέσεων πρωτοκόλλου. Τέλος, υποθέτουμε ότι δικαιούχος και επιτιθέμενος δεν τυχαίνει ποτέ να θέλουν να αυθεντικοποιηθούν την ίδια στιγμή.

Λαμβάνοντας υπόψη έναν ακέραιο αριθμό $N \geq 1$, θεωρούμε ότι ο επιτιθέμενος είναι επιτυχής εάν είναι σε θέση να υποδυθεί το νόμιμο δικαιούχο μέσα σε N εκτελέσεις του πρωτοκόλλου είτε με παθητικές είτε με ενεργητικές επιθέσεις. Σε αυτό το κεφάλαιο το N θα θεωρείται μη μεταβλητή σταθερά και στο RFID περιβάλλον, μπορεί να ερμηνευθεί ως χαρακτηριστικός αριθμός επικυρώσεων που η ετικέτα μπορεί να υποστηρίξει κατά τη διάρκεια της ζωής της.

4.1.3.1 Περιγραφή πρωτοκόλλου

Πριν από την εκτέλεση πρωτοκόλλου, ο νόμιμος δικαιούχος και ο ελεγκτής συμφωνούν σε ένα κοινό μυστικό κωδικό (κλειδί) k το οποίο είναι σε μορφή δυαδικής ακολουθίας μήκους $n \geq 1$, όπου n ακέραιος αριθμός.

$$l_k = 2^{n+2} - 2 \qquad (1)$$

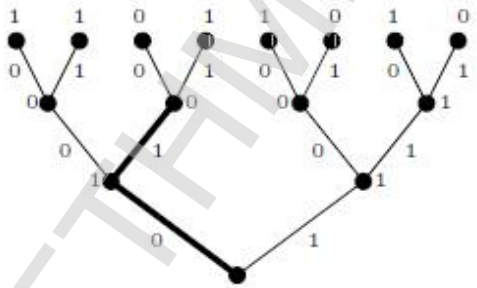
Το πρωτόκολλο αποτελείται από τρία μέρη: **έναρξη**, **επικύρωση** και **έλεγχος** εγκυρότητας. Η έναρξη και τα μέρη της επικύρωσης εκτελούνται κατά τη διάρκεια μιας «αργής φάσης» όπου δεν υπάρχει κανένα χρονικό μέτρο. Σε αντίθεση ο έλεγχος εγκυρότητας, περιλαμβάνει χρονικό μέτρο και αναφέρεται συχνά ως «γρήγορη φάση.»

Εκτός από το l_k, το πρωτόκολλο περιλαμβάνει δύο θετικούς ακέραιους αριθμούς l_a και l_b των οποίων οι τιμές θα διευκρινιστούν παρακάτω.

Εναρξή

Ο δικαιούχος στέλνει μια τυχαία σειρά l_a bit a και μια τυχαία σειρά l_b bit b στον ελεγκτή. Με τα a και b, και το κοινό μυστικό κλειδί k, ο ελεγκτής και ο δικαιούχος παράγουν ένα πλήρες δυαδικό δέντρο $_T(a,b,k)$ βάθους n + 1 που φαίνεται παρακάτω (εικόνα 4.1). Οι αριστερές και δεξιές άκρες παίρνουν τις τιμές 0 και 1, αντίστοιχα, και κάθε κόμβος (εκτός από τη ρίζα) παίρνουν την αξία 0 ή 1 ανάλογα με το a, το b, και το k.

Η λειτουργία $_T(a,b,k)$ είναι μια ένα προς ένα λειτουργία όποτε δύο από τις τρεις μεταβλητές a, b, k κράτιουνται σταθερές. (Αυτό για να είναι δυνατό, θα πρέπει τα l_a και l_b να είναι το μέγιστο ίσα με l_k δεδομένου ότι ο συνολικός αριθμός των πληρών δυαδικών δέντρων βάθους n + 1 είναι ίσος με $2^{2^{n+2}-2} = 2^{l_k}$.



Εικόνα 4.1: γράφημα απόφασης με την μορφή δέντρου με n=2 και l_k =14. Η μαυρισμένη γραμμή στο δέντρο αντιστοιχεί στις προκλήσεις του ελεγκτή 0, 1 και οι στις αντίστοιχες απαντήσεις 1, 0 από τον δικαιούχο.

Επικύρωση

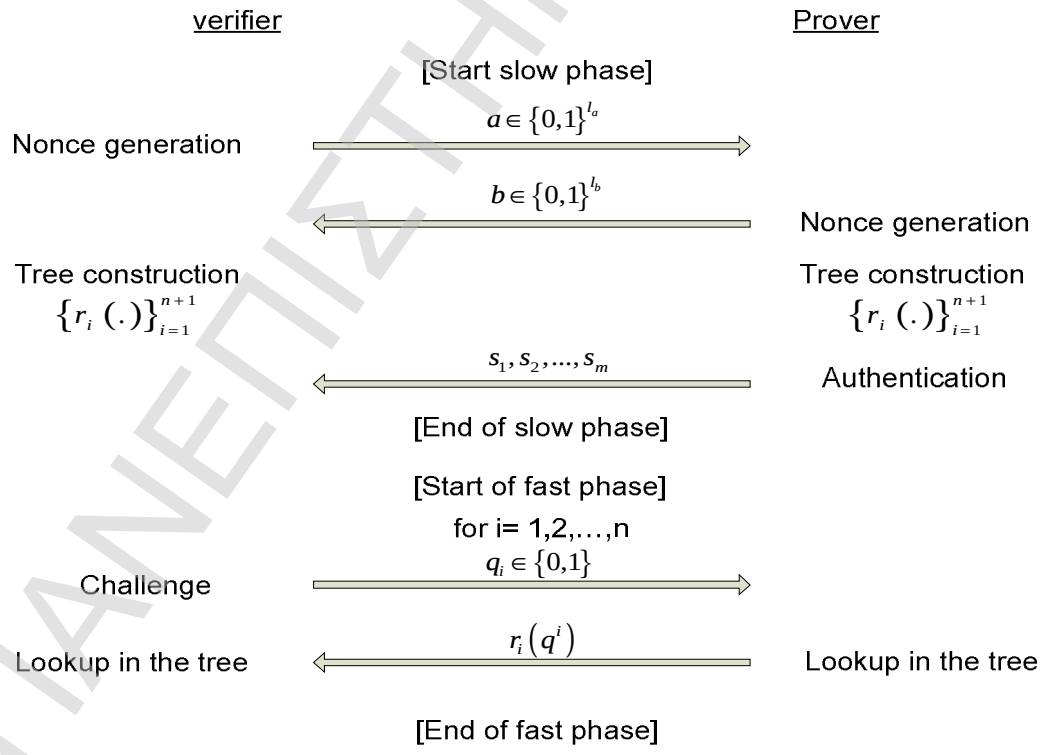
Ο δικαιούχος διαβιβάζει m bit που αντιστοιχούν σε m φύλλα του δέντρου ξεκινώντας από το αριστερό άκρο. Η τιμή του m θα διευκρινιστεί στην παράγραφο 3. Για τώρα, το m θα είναι κάποια τιμή μικρότερη από 2^{n+1}, το οποίο είναι και ο συνολικός αριθμός των φύλλων.

Έλεγχος εγκυρότητας

Μια n επαναλήψεων γρήγορη ανταλλαγή bit μεταξύ του ελεγκτή και του ελεγκτή που χρησιμοποιούν το δέντρο. Οι άκρες και οι τιμές στους κόμβους αντιπροσωπεύουν τις «προκλήσεις του ελεγκτή» και τις «απαντήσεις των δικαιούχων» αντίστοιχα. Σε κάθε βήμα $i \in \{1, 2, ..., n\}$ ο ελεγκτής παράγει μια πρόκληση υπό μορφή τυχαίων bit q_i και την στέλνει στον δικαιούχο. Ο δικαιούχος απαντά στέλνοντας την τιμή του κόμβου στο δέντρο του οποίου η πορεία των ακρών από τη ρίζα είναι $q^i = q_1, q_2, \ldots q_i$.Αυτή η απάντηση υποδηλώνεται από τον τύπο $r_i\left(q^i\right)$.

Στο παράδειγμα που εμφανίζεται στην εικόνα 1, ο ελεγκτής απαντά πάντα με 0 στο δεύτερο κύκλο εκτός αν οι πρώτες και δεύτερες προκλήσεις είναι ίσες με 1 οπότε σ' αυτή την περίπτωση ο ελεγκτής απαντά με 1, δηλ., $r_2\left(q^2\right) = 0$ για q^2=1. Τέλος για κάθε $i \in \{1, 2, ..., n\}$, ο ελεγκτής μετρά το χρονικό διάστημα μεταξύ του στιγμιαίου q_i που στέλνεται έως ότου παραληφθεί το $r_i\left(q^i\right)$.

Ο χρόνος επιστροφής για κάθε πρόκληση-απάντηση δίνει εγγυήσεις ότι ο δικαιούχος θα είναι σε πολύ κοντινή απόσταση με τον ελεγκτή. Ως εκ τούτου, ένα χαρακτηριστικό κατώτατο όριο είναι μια τιμή κοντά 2d/c όπου το d δείχνει την απόσταση του δικαιούχου από τον ελεγκτή ενώ το c είναι η ταχύτητα του φωτός.



Εικόνα 4.2: Πρωτόκολλο περιορισμού 2-φάσεων.

Τελική απόφαση

Ο ελεγκτής δέχεται την ταυτότητα του δικαιούχου μόνο εάν τα m bit επικύρωσης είναι σωστά και εάν οι απαντήσεις n της γρήγορης φάσης είναι σωστές σε συνδυασμό με το χρονικό περιορισμό πρόκληση-απάντησης. Το πρωτόκολλο εμφανίζεται στο στην εικόνα 4.2.

4.1.4 Ανάλυση Ασφαλείας

Εξετάζουμε την πιθανότητα να ισχύει το ακόλουθο σενάριο "μετά από N εκτελέσεις πρωτοκόλλου, ο ελεγκτής να δεχτεί την απόδειξη της ταυτότητας του επιτιθεμένου ως έγκυρη τουλάχιστον μια φορά.". Για να υπολογιστεί αυτή η ποσότητα, κάνουμε την ακόλουθη υπόθεση: μια εκτέλεση πρωτοκόλλου δεν παρέχει καμία πληροφορία στον επιτιθέμενο για το μυστικό κλειδί k. Αποτέλεσμα αυτού είναι ότι η γνώση μόνο του a και του b δεν αποκαλύπτουν τίποτα για την ανάθεση κάθε κόμβου που, ανεξάρτητα, μπορεί να πάρει τις τιμές 0 ή 1 με πιθανότητα 1/2.

Αρχικά, η παραπάνω υπόθεση μπορεί να δημιουργήσει κάποιες αμφιβολίες δεδομένου ότι τα m κομμάτια επικύρωσης και τα n κομμάτια που στέλνονται κατά τη διάρκεια της γρήγορης φάσης από τον δικαιούχο εξαρτώνται από το μυστικό κλειδί. Πρακτικά, αυτή η υπόθεση μπορεί να δικαιολογηθεί διατυπώνοντας ότι εάν m + n είναι πολύ μικρότερα από το μέγεθος του κλειδιού, $l_k = 2^{n+2} - 2$, μια εκτέλεση πρωτοκόλλου δεν αποκαλύπτει σχεδόν καμία πληροφορία για το μυστικό κλειδί. Για να υπάρχει συμφωνία με την υπόθεσή μας, από τώρα υποθέτουμε $m = m(n) = o(l_k)$, δηλ., το m θα αυξάνεται σχεδόν εκθετικά με το n .

Για να υπολογίσουμε την πιθανότητα της ψεύτικης επικύρωσης, διακρίνουμε δύο περιπτώσεις ανάλογα με το εάν κατά τη διάρκεια των N εκτελέσεων του πρωτοκόλλου ο επιτιθέμενος ενεργεί μόνος του ή όχι, δηλ., χωρίς αλληλεπίδραση είτε παθητικά είτε ενεργά με τον νόμιμο δικαιούχο.

4.1.4.1 Επίθεση χωρίς την ανάμειξη του νόμιμου δικαιούχου

Αυξάνουμε και χαμηλώνουμε τα όρια της πιθανότητας ψεύτικης επικύρωσης (f-a) όπως

$$\Pr(f-a|E)\Pr(E) \le \Pr(f-a) \le \Pr(f-a|E) + \Pr(E^c) \quad (2)$$

όπου το E δείχνει ότι «μετά από N εκτελέσεις του πρωτοκόλλου όλα τα δέντρα είναι διαφορετικά» και όπου το E_c δείχνει το συμπλήρωμα του E. Επομένως, για κάθε

εκτέλεση πρωτοκόλλου ο επιτιθέμενος λαμβάνει μια πιθανότητα για την επιτυχία (στην καλύτερη περίπτωση) ίση με $2^{-(m+n)}$, που αντιστοιχεί σε τυχαίους υπολογισμούς.

Ακολουθεί

$$\Pr\left(f - a \,|E \right) = N \times 2^{-(m+n)} + o\left(2^{-(m+n)}\right) \quad (n \to \infty) \quad (3)$$

Ο υπολογισμός $\Pr\left(E^c\right)$ αναφέρεται στο παράδοξο των γενεθλίων. Αφήνοντας $l_a = m+n$, ένας τυποποιημένος υπολογισμός αποκαλύπτει το παρακάτω[2]

$$\Pr\left(E^c\right) \le \frac{N(N-1)}{2^{m+n+1}} + o\left(2^{-2(m+n)}\right) \qquad (n \to \infty) \qquad (4)$$

Από τις εξισώσεις (2) , (3) και (4) θα έχουμε

$$\Pr(f - a) = \Theta\left(2^{-(m+n)}\right) \qquad (n \to \infty) \qquad (5)$$

4.1.4.2 Επίθεση με ανάμειξη του νόμιμου δικαιούχου

Αυτή την περίπτωση την διακρίνουμε σε δύο υποπεριπτώσεις, ανάλογα με εάν ο αντίπαλος μπορεί ή όχι να αναμεταδώσει μηνύματα.

<u>Με αναμετάδοση μηνυμάτων</u>

Σε αυτήν την περίπτωση, ο αντίπαλος μπορεί να εκτελέσει επιθέσεις με ενδιάμεσο άτομο (man-in-the-middle) για να περάσει το βήμα επικύρωσης για κάθε μια από τις N εκτελέσεις πρωτοκόλλου. Ο επιτιθέμενος αρχίζει το πρωτόκολλο με τον ελεγκτή και αναμεταδίδει τα παρόντα a,b και μια σειρά επικύρωσης s_1, s_2,…, s_m. Εντούτοις, για να πετύχει ο επιτιθέμενος πρέπει να περάσει τον έλεγχο εγγύτητας. Υπολογίζουμε τη πιθανότητα της ψεύτικης-αποδοχής (f-a) υποθέτοντας ότι ο επιτιθέμενος πέρασε το βήμα επικύρωσης.

Ομοίως όπως και στην σχέση (2), αυξάνουμε και χαμηλώνουμε τα όρια της πιθανότητας ψεύτικης επικύρωσης (f-a)

$$\Pr\left(f-a\middle|E_b\right)\Pr\left(E_b\right)\le\Pr\left(f-a\right)\le\Pr\left(f-a\middle|E_b\right)+\Pr\left(E_b^c\right) \qquad (6)$$

Όπου το E_b δείχνει το γεγονός «μετά από τις N εκτελέσεις πρωτοκόλλου όλα τα b είναι διαφορετικά.»

Υπολογίζουμε αρχικά το $\Pr\left(f-a\middle|E_b\right)$. Λόγω του χρονικού περιορισμού, ο επιτιθέμενος δεν μπορεί να αναμεταδώσει τις πληροφορίες μεταξύ του ελεγκτή και του δικαιούχου κατά τη διάρκεια της γρήγορης φάσης. Αυτό σημαίνει ότι η απάντηση του επιτιθέμενου στο χρόνο πρέπει να είναι ανεξάρτητη από την πρόκληση του ελεγκτή στο χρόνο i, για οποιοδήποτε $i\in\{1,2,...,n\}$. Επειδή δεν υπάρχει κανένα χρονικό μέτρο πριν από τη γρήγορη φάση, ο αντίπαλος μπορεί να ρωτήσει το νόμιμο δικαιούχο με μια ακολουθία προκλήσεων $\tilde{q}^n$, ελπίζοντας αυτές να αντιστοιχούν στις προκλήσεις q^n που παρέχονται από τον ελεγκτή κατά τη διάρκεια της γρήγορης φάσης. Επειδή τα q^n και $\tilde{q}^n$ επιλέγεται ανεξάρτητα, η πιθανότητα του περάσματος του ελέγχου εγγύτητας είναι η ίδια για οποιοδήποτε $\tilde{q}^n$. Ως εκ τούτου, χωρίς απώλεια γενικότητας, υποθέτουμε ότι ο επιτιθέμενος έχει πρόσβαση $r_i\left(\tilde{q}^i\right)$ για $\tilde{q}^n = (0, 0,\ldots, 0) \triangleq 0^n$. Ο επιτιθέμενος θα είναι επιτυχής μόνο εάν $r_i\left(0^i\right)=r_i\left(q^i\right)$ για κάθε $i\in\{1,2,...,n\}$. Για συντομία, από τώρα και στο εξής θα γράφουμε r_i αντί για $r_i\left(q^i\right)$ και $\tilde{r}_i$ αντί για $r_i\left(\tilde{q}^i\right)$.

Θέτοντας το t να είναι την πρώτη φορά $i\ge 1$ όταν $q_i = 1$, θα έχουμε $\tilde{r}_i = r_i$ για κάθε $i\in\{1,2,...,t-1\}$, και $\tilde{r}_i = r_i$ με την πιθανότητα 1/2 για κάθε $i\in\{t,t+1,...,n\}$.

Επομένως, αφήνοντας το $r^n \triangleq r_1, r_2, ..., r_n$, η πιθανότητα μιας επιτυχούς επίθεσης με παραπάνω της μίας εκτέλεσης του πρωτοκόλλου μπορεί να υπολογιστεί όπως παρακάτω:

$$\Pr(\tilde{r}^n = r^n)\sum_{i=1}^{n}\Pr(\tilde{r}^n = r^n \,|\, t=i)\Pr(t=i) +$$

$$\Pr\left(\tilde{r}^n = r^n \,\middle|\, q^n = 0^n\right)\Pr\left(q^n = 0^n\right) =$$

$$\sum_{i=1}^{n} 2^{-(n-i+1)} 2^{-i} + 2^{-n}$$

$$= 2^{-n}\left(\frac{n}{2}+1\right)$$

και έχουμε

$$\Pr\left(f - a \,|\, Eb\right) = 2^{-n+o(1)} \qquad (n \to \infty) \qquad (7)$$

Παρόμοια με την σχέση (4) έχουμε :

$$\Pr\left(E_b^c\right) \le \frac{N(N-1)}{2^{l_b+1}} + O\left(2^{-2l_b}\right) \quad (l_b \to \infty) \qquad (8)$$

Θέτοντας $l_b \ge n$, από τις σχέσεις (6), (7), και (8) η υψηλότερη πιθανότητα ψεύτικης επικύρωσης που μπορεί να επιτευχθεί από έναν επιτιθέμενο ο οποίος μπορεί να αναμεταδώσει μηνύματα ικανοποιείται από την παρακάτω σχέση:

$$\Pr\left(f - a\right) = 2^{-n(1+o(1))} \qquad (n \to \infty) \qquad (9)$$

<u>Χωρίς αναμετάδοση μηνυμάτων</u>

Όπως κάποιος μπορεί να παρατηρήσει, η ανάλυση ασφάλειας στην ανωτέρω περίπτωση **«με αναμετάδοση»** δεν χρησιμοποιεί ποτέ το μοναδικό a. Υποθέτει δηλαδή ότι ο επιτιθέμενος δεν μπορεί να αναμεταδώσει σήματα. Χωρίς τη χρησιμοποίηση του μοναδικού a, ο αντίπαλος μπορεί εύκολα να περάσει το βήμα επικύρωσης αφού πρώτα λάβει το μοναδικό b και την αντίστοιχη σειρά επικύρωσης από το νόμιμο δικαιούχο, παρουσιάζοντας τα στοιχεία που συνέλλεξε στον ελεγκτή.

Η ασφάλεια είναι έπειτα βασισμένη μόνο στον έλεγχο εγγύτητας. Σε αντίθεση, με την χρησιμοποίηση ενός μοναδικού a, αυτή η επίθεση είναι λιγότερο πιθανό να πετύχει. Μπορεί εύκολα να δει κάποιος ότι με $l_a = m+n$, η πιθανότητα της ψεύτικης αποδοχής είναι τόσο μικρή όσο στην περίπτωση των επιθέσεων χωρίς νόμιμο δικαιούχο που δίνεται από την σχέση (5).

4.1.5 Βελτιστοποίηση του προτεινόμενου πρωτοκόλλου

Παρατίθεται παρακάτω η βελτιστοποίηση του πρωτοκόλλου αυτού περιορίζοντας την προσοχή μας σε πρωτόκολλα ανταλλαγής bit που ικανοποιούν τις ακόλουθες γενικές ιδιότητες:

- Ο ελεγκτής και ο νόμιμος δικαιούχος μοιράζονται ένα κοινό μυστικό υπό μορφή σειράς bit μήκους l_k
- Ο ελεγκτής δέχεται πάντα την απόδειξη της ταυτότητας ενός νόμιμου δικαιούχου.
- Ούτε ο ελεγκτής ούτε ο νόμιμος δικαιούχος δεν συνεργεί με τον επιτιθέμενο.

Εξετάζουμε ένα πρωτόκολλο επικύρωσης που ικανοποιεί τις παραπάνω ιδιότητες. Μεταξύ των bit που στέλνονται από τον δικαιούχο κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου, μερικά εξαρτώνται από το κοινό μυστικό, και μερικά όχι. Εάν m+n δείχνει τον αριθμό μυστικών εξαρτώμενων κομματιών, η πιθανότητα ψεύτικης αποδοχής (ανά προσπάθεια του επιτιθέμενου) του πρωτοκόλλου είναι στην καλύτερη περίπτωση

$$2^{-(m+n)}$$

ανεξάρτητα από τον τύπο επίθεσης.

Για να υπερνικηθούν οι Relay επιθέσεις, είναι απαραίτητο ο ελεγκτής να καθορίζει επιτυχώς εάν ο δικαιούχος είναι κοντά σε αυτόν - στην περίπτωσή μας με χρονικό περιορισμό.

Εάν το n δείχνει τον αριθμό των βασικών εξαρτώμενων bit που στέλνονται από τον δικαιούχο με βάση τα οποία ο ελεγκτής αξιολογεί την εγγύτητά του, η πιθανότητα ψεύτικης αποδοχής (ανά προσπάθεια του επιτιθέμενου) παρουσία των Relay επιθέσεων είναι στην καλύτερη περίπτωση

$$2^{-n}$$

Λαμβάνοντας υπόψη τις σχέσεις (5) και (9), το πρωτόκολλο αυτό είναι ασυμπτωτικά βέλτιστο υπό την έννοια ότι το εκθετικό ποσοστό στο οποίο η πιθανότητα ψεύτικης αποδοχής τείνει στο μηδέν όσο τα m και n τείνουν στο άπειρο είναι ό,τι καλύτερο μπορεί να επιτευχθεί μεταξύ όλων των πρωτοκόλλων με τις ίδιες παραμέτρους.

4.1.6 Παρατηρήσεις

Σε αυτό το κεφάλαιο παρουσιάστηκε ένα πρωτόκολλο επικύρωσης που είναι ασυμπτωτικά βέλτιστο από την άποψη της πιθανότητας της ψεύτικης αποδοχής από κοινού στις περιπτώσεις αποστολής μηνυμάτων και μη αποστολής μηνυμάτων, σε αντίθεση με όλα τα προηγούμενα πρωτόκολλα.

Η απόδοση του πρωτοκόλλου, έρχεται εις βάρος των πρόσθετων ικανοτήτων αποθήκευσης προκειμένου να υπολογιστεί ολόκληρο το δέντρο απόφασης πριν εκτελεστεί η γρήγορη φάση. Αυτό καθιστά το πρωτόκολλο συνήθως κατάλληλο στις εφαρμογές όπου ο αριθμός των κύκλων γρήγορης φάσης μπορεί να είναι μικρός - για παράδειγμα, στις καταστάσεις όπου οι Relay επιθέσεις αναμένεται να εμφανιστούν σπάνια. Αριθμητικά, θέτοντας το n = 11 , απαιτείται ένα 1KByte μνήμη. Οι περισσότερες ετικέτες T RFID που χρησιμοποιούνται για την ασφαλή χρήση εφαρμογών διαθέτουν αυτή την μνήμη. Η κλασική τυποποιημένη ετικέτα NXP Mifare παρέχει μνήμη 1KByte και τα ICAO ηλεκτρονικά διαβατήρια (συμμορφωμένα με τους κανονισμούς) ενσωματώνουν μια ετικέτα μνήμης τουλάχιστον 30KByte.

Τέλος, σημειώνουμε ότι διάφορα άλλα κριτήρια βελτιστοποίησης μπορούν να εξεταστούν εκτός από αυτά που προτείνονται στην παράγραφο 4. Μια ενδιαφέρουσα κατεύθυνση που μπορεί να εξεταστεί είναι, λαμβάνοντας υπόψη το μέγεθος του μυστικού κλειδιού K, να επιδιωχθεί η διερεύνηση των πιθανοτήτων της ψεύτικης αποδοχής με μετάδοση και χωρίς μετάδοση μηνυμάτων .

ΠΑΡΑΓΡΑΦΟΣ 4.2

Ασφάλεια Rfid συστημάτων με ανίχνευση της κλωνοποιημένης ετικέτας

4.2.1 Εισαγωγή

Το RFID παίρνει τη θέση του ως κυρίαρχο καθημερινό εργαλείο για το αυτόματη ταυτοποίηση των φυσικών αντικειμένων. Πολλές βιομηχανίες το χρησιμοποιούν για να διευκολύνουν το χειρισμό των φυσικών αγαθών. Η RFID είναι επίσης μια τεχνολογία που βοηθά την διακίνηση των αγαθών στο διαδίκτυο. Το διαδίκτυο των αγαθών (IoT) συνδέει τα φυσικά αντικείμενα σε δίκτυα και βάσεις δεδομένων έτσι ώστε να μπορούν να εξαχθούν τα επίπεδα μέτρησης και επεξεργασίας της ακρίβειας διαδικασιών που συμβαίνουν στον πραγματικό κόσμο.

Το RFID αλλάζει τον τρόπο που κατασκευάζεται η ασφάλεια στις εφαρμογές αυτόματης επικύρωσης ταυτότητας (Auto-ID). Αφενός, το RFID φέρνει βελτιώσεις στην ασφάλεια έναντι των παλαιότερων τεχνολογιών αυτόματης επικύρωσης με την παροχή αυξανόμενης διαφάνειας και της δυνατότητας να χρησιμοποιηθεί κρυπτογραφία. Ένα αντικείμενο στο οποίο προσκολλιέται ένα μη-καθορισμένο barcode μπορεί να επικυρωθεί μόνο με τη βοήθεια μιας πρόσθετης ιδιότητας ασφαλείας, όπως ένα ολόγραμμα ή κάποιοι πρόσθετοι δείκτες, μια ετικέτα RFID μπορεί να επιτρέψει την επικύρωση και την πιστοποίηση του προσκολλημένου αντικειμένου. Από την άλλη, η ασφάλεια χρειάζεται σε πολλές RFID εφαρμογές.

Οι ετικέτες RFID χρησιμοποιούνται για να παρέχουν πρόσβαση σε κτήρια, χιονοδρομικά κέντρα και εθνικές οδούς, ως εισιτήρια στις δημόσιες συγκοινωνίες και τους Ολυμπιακούς Αγώνες ακόμα και για την πληρωμή κινητής τηλεφωνίας. Επιπλέον, το RFID υιοθετείται ως τεχνολογία επικύρωσης για να εξασφαλίσει τις αλυσίδες εφοδιασμού από τα πλαστά προϊόντα. Σε όλες αυτές τις εφαρμογές κλωνοποίηση και η πλαστογραφία των ετικετών RFID θα μπορούσαν να είναι οικονομικά προσοδοφόρα τακτική για περιστασιακούς χάκερ ή για επαγγελματίες του οικονομικού εγκλήματος, κάτι που σημαίνει σοβαρή καταστροφή για τα εισοδήματα και τη φήμη των επιχειρήσεων. Οι πιθανές απώλειες λόγω των παραβιάσεων της ασφαλείας είναι επιπλέον αυξανόμενες από το υψηλό επίπεδο αυτοματοποίησης που επιτρέπεται από την τεχνολογία. Επομένως η ασφάλεια είναι όχι μόνο προστιθέμενη αξία την οποία το RFID παρέχει έναντι των παλαιότερων αυτοματοποιημένων τεχνολογιών, αλλά μία απαίτηση για την περαιτέρω εξέλιξη τους.

Για την τεχνολογία RFID, οι πιο προκλητικές απειλές ασφάλειας στις εμπορικές εφαρμογές RFID είναι η κλωνοποίηση και η πλαστογράφηση ετικετών. Η ερευνητική κοινότητα εξετάζει αυτές τις απειλές πρώτιστως με την προσπάθεια να γίνει η κλωνοποίηση ετικετών πολύ δύσκολη, κυρίως με τη χρησιμοποίηση κρυπτογραφικών πρωτοκόλλων επικύρωσης ετικετών.

Οι θεμελιώδης δυσκολίες αυτής της έρευνας περιστρέφονται γύρω από το εμπόριο μεταξύ του κόστους ετικετών, του επιπέδου ασφάλειας, και της απόδοσης από την άποψη της ταχύτητας ανάγνωσης και της απόστασης. Δεν είναι πολύ δύσκολο να προστατευθεί μια συσκευή Ράδιο Συχνότητας (RF) από την κλωνοποιήση σήμερα, αλλά είναι εξαιρετικά δύσκολο να γίνει χρησιμοποιώντας μια χαμηλού κόστους ετικέτα RFID τύπου barcode. Αυτές οι ετικέτες θα παραχθούν κατά εκατομμύρια κομμάτια και οι επιχειρήσεις θα έχουν έναν ισχυρό το οικονομικό κίνητρο για να ελαχιστοποιηθεί το κόστος της ετικέτας χωρίς να μειωθούν τα χαρακτηριστικά ασφάλειας τα οποία οι ετικέτες παρέχουν. Σύμφωνα με τον Sanjay Sarma, συνιδρυτή του τμήματος αυτοματοποίησης του MIT, δεν μπορείς να κάνεις τίποτα στις παθητικές ετικέτες εκτός από το να εφαρμόσεις συναρτήσεις κατακερματισμού (hashes).

Αν και η ερευνητική κοινότητα παρέχει πάντα αυξημένες βελτιώσεις, υπάρχουν λόγοι να θεωρείται ότι οι χαμηλού κόστους ετικέτες RFID δεν θα μπορούν να προστατευθούν εντελώς από την κλωνοποίηση στο εγγύς μέλλον. Μία ημέρα περίπου παίρνει η υπολογιστική και φυσική πολυπλοκότητα μιας έξυπνης κάρτας ώστε να εφαρμοστεί σε μια κινητή συσκευή που θα μπορεί να θεωρηθεί εύλογα εξασφαλισμένη ενάντια στις περισσότερες γνωστές απειλές, συμπεριλαμβανομένων των επιθέσεων δευτερευόντων καναλιών και των φυσικών επιθέσεων. Οι χαμηλού κόστους ετικέτες είναι υπολογιστικά πολύ πιο αδύνατες συσκευές από τις έξυπνες κάρτες, μπορούν να χρησιμοποιήσουν μόνο ένα μέρος της ενέργειας και του προϋπολογισμού δύναμης μιας έξυπνης κάρτας και στερούνται τη φυσική προστασία. Κατά συνέπεια, είναι αμφισβητήσιμο, εάν είναι δυνατό βρούμε μια αληθινά ασφαλή συσκευή RFID που εξετάζει όλα τα γνωστά τρωτά σημεία χωρίς να συνδυάζεται με μια συσκευή η οποία θα έχει επίδραση και στο κόστος και στην απόδοση (δηλ. ταχύτητα και απόσταση ανάγνωσης), όπως μια ασύρματη έξυπνη κάρτα.

Σε αυτό το κεφάλαιο θα ερευνηθεί μια προσέγγιση για ασφαλή χαμηλού κόστους συστήματα RFID ενάντια στην κλωνοποίηση και στην πλαστογράφηση ετικετών βασισμένη στην ανίχνευση των επιθέσεων κλωνοποίησης. Αντί να στηριχθούμε στην αποτελεσματικότητα που μπορεί να προσφέρουν αυτές αδύνατες και φτηνότερες συσκευές, σε αυτή τη προσέγγιση θα στηριχθούμε στη διαφάνεια που οι ετικέτες παρέχουν.

Η εστίασή σε χαμηλού κόστους RFID γίνεται για δύο λόγους. Ο πρώτος είναι ότι οι χαμηλού κόστους ετικέτες χρησιμοποιούνται για την ασφάλεια ευαίσθητων εφαρμογών όπου η κλωνοποίηση των ετικετών μπορεί να οδηγήσει σε μεγάλη ζημία. Για παράδειγμα, η εταιρεία φαρμάκων Pfizer χρησιμοποιεί χαμηλού κόστους HF και UHF ετικέτες για την επικύρωση για του πλέον πλαστού προϊόντος της, το Viagra .

Δεύτερον, εάν οι χαμηλού κόστους ετικέτες μπορούν να ασφαλιστούν κατάλληλα, το RFID θα μπορούσε να εφαρμοστεί επίσης σε ευαίσθητες περιοχές ασφάλειας όπου το μεγάλο κόστος των κρυπτογραφικών ετικετών δεν μπορεί να αιτιολογηθεί.

4.2.2 Εισαγωγή στο RFID

Τα συστήματα RFID περιλαμβάνουν τις ετικέτες που είναι προσκολλημένες στα αντικείμενα, συσκευές που διαβάζουν και γράφουν τα στοιχεία όσον αφορά τις ετικέτες, και τα συστήματα οπίσθιου μέρους στα οποία αποθηκεύονται και διαμοιράζονται τα δεδομένα. Οι παθητικές ετικέτες παίρνουν όλη τη δύναμή τους από τον αναγνώστη ενώ οι ακριβότερες ενεργές ετικέτες έχουν μπαταρία.

Τα σημαντικότερα πρότυπα για το RFID επιτηρούνται από την EPCglobal που αναφέρθηκε στο πρώτο κεφάλαιο. Τα πρότυπα EPC οδηγούνται από τη βιομηχανία και εστιάζουν στις χαμηλού κόστους παθητικές UHF ετικέτες. Οι UHF ετικέτες είναι σημαντικές στις εφαρμογές διοικητικής μέριμνας λόγω της μεγαλύτερης περιοχής διαβάσματος που παρέχουν έναντι των ετικετών LF και HF.

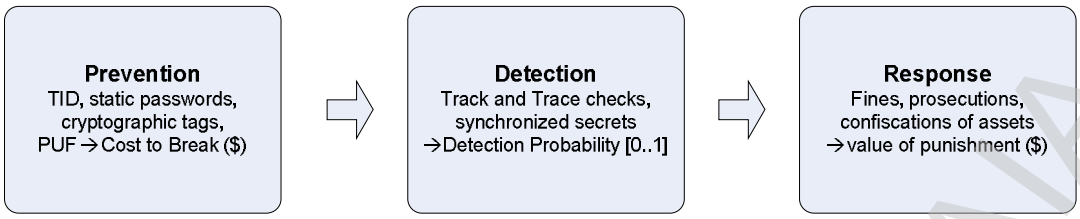
Ενώ οι κρυπτογραφικές ετικέτες RFID είναι αυτήν την περίοδο ευρέως διαθέσιμες στη ζώνη HF, σήμερα δεν υπάρχει καμία κρυπτογραφική ετικέτα διαθέσιμη στο εμπόριο στην UHF ζώνη. Εντούτοις, η ανάγκη για ασφάλεια των προϊόντων στην UHF αγορά φαίνεται ξεκάθαρα και οι πρώτες εφαρμογές ήδη υπάρχουν.

4.2.3 Σχετική Εργασία

Σε πολύ γενικές γραμμές, ασφάλεια είναι η διαδικασία προστασίας περιουσιακών στοιχείων από τους επιτιθέμενους και περιλαμβάνει τα βήματα της πρόληψης, της ανίχνευσης, και της απάντησης. Στην συνέχεια παρουσιάζεται η χαρτογράφηση των αντίμετρων στα τρία βήματα στο στάδιο της εξασφάλισης ενός συστήματος RFID ενάντια στην κλωνοποίηση και την πλαστογράφηση των ετικετών. Αυτή η γενική διαδικασία προβάλλεται στην εικόνα 4.3.

Πρόληψη

Η πρόληψη αναφέρεται στην οικοδόμηση εμποδίων που πρέπει να σπάσουν ή να παρακαμφτούν ώστε να υλοποιηθεί μια απειλή. Αποτελεί το πρώτο επίπεδο υπεράσπισης και τον πιο προφανή στόχο επίθεσης από τους αντιπάλους. Ένα παράδειγμα των προληπτικών μέτρων ασφάλειας είναι μια κλειδαριά στη εξώπορτα ενός σπιτιού. Η δύναμη των προληπτικών μέτρων χαρακτηρίζεται από το κόστος που χρειάζεται για να σπάσουν (Cost to Break-CtB), δηλαδή είναι η ελάχιστη προσπάθεια για να βρεθεί και γίνει εκμεταλλεύσιμη μια ευπάθεια. Μόλις σπάσουν τα προληπτικά μέτρα, η εκμετάλλευση μπορεί να επαναληφθεί με μια μικρή πρόσθετη προσπάθεια.



Εικόνα 4.3: Διαδικασία ασφάλειας ενός RFID συστήματος ενάντια στην κλωνοποίηση και την πλαστογράφηση ετικετών (τα μικρά βέλη δείχνουν την έκβαση και το μετρικό σύστημα κάθε βήματος).

Τα βασικά προληπτικά μέτρα των τυποποιημένων ετικετών της EPC περιλαμβάνουν μοναδικό εργοστασιακό προγραμματισμό, μόνο για ανάγνωση, αριθμούς ταυτότητας αναμεταδοτών (TID) που είναι κάπως παρόμοιοι με τις διευθύνσεις MAC των καρτών που χρησιμοποιούνται στα δίκτυα υπολογιστών και κωδικούς πρόσβασης για την προστασία των εντολών ΠΡΟΣΒΑΣΗΣ (ACCESS) και ΘΑΝΑΤΩΣΗΣ (KILL). Τα βασικά μέτρα, ωστόσο, είναι τρωτά όταν ο επιτιθέμενος "ακούει" κρυφά και έτσι παρέχεται μέτρια προστασία ενάντια στην κλωνοποίηση ετικετών.

Τα κρυπτογραφικά μέτρα περιλαμβάνουν την διαδικασία επικύρωσης από τον αναγνώστη στην ετικέτα και το αντίθετο. Διάφορα πρωτόκολλα επικύρωσης από την ετικέτα στον αναγνώστη έχουν προταθεί, συνήθως βασισμένα σε ξεπερασμένες κρυπτογραφικούς τεχνικές όπως οι διαδικασίες βασισμένες σε bit, οι ψευδοτυχαίοι αριθμοί και οι λειτουργίες που στηρίζονται στις συναρτήσεις κατακερματισμού (hash). Επίσης υπάρχουν διαφορετικά συμμετρικά πρωτόκολλα επικύρωσης βασισμένα στην κρυπτογράφηση των ετικετών, για παράδειγμα ετικέτες βασισμένες στον αλγόριθμο AES.

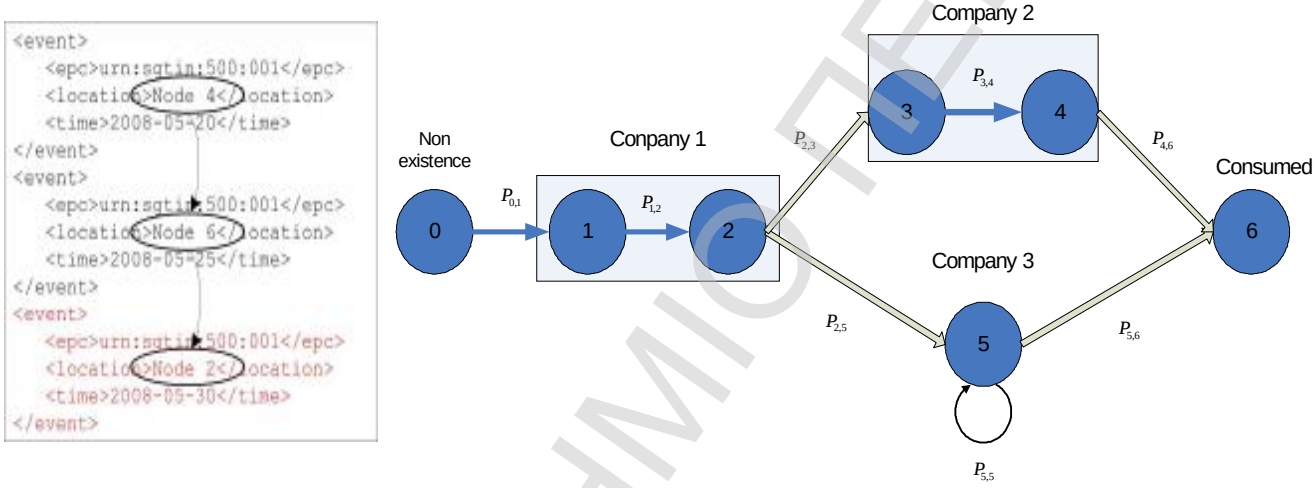
Η ασύμμετρη κρυπτογράφηση είναι αυτήν την περίοδο μια μεγάλη πρόκληση για τις RFID ετικέτες αλλά λόγω των προόδων ελλειπτικού συστήματος καμπύλων κρυπτογράφησης (ECC), ως λύση για το άμεσο μέλλον κρίνεται εφικτή. Ένας άλλος τρόπος να επικυρωθεί μια ετικέτα RFID είναι να χρησιμοποιηθεί μια φυσική λειτουργία μη κλωνοποίησης (PUF) η οποία είναι μια μονόδρομη λειτουργία που εφαρμόζεται και χρησιμοποιεί ελάχιστες φυσικές δαπάνες.

Ανίχνευση

Η ανίχνευση χρειάζεται για να ελαχιστοποιηθούν οι αρνητικές επιδράσεις των υπαρχουσών απειλών και για να αυξηθεί η πιθανότητα να πιαστούν οι αντίπαλοι. Ένα τηλεοπτικό σύστημα παρακολούθησης είναι ένα χαρακτηριστικό παράδειγμα μέτρων. Σε μερικές περιπτώσεις η ανίχνευση ενεργοποιεί μια άμεση απάντηση η οποία ακυρώνει τις αρνητικές επιδράσεις της επίθεσης και ως αποτέλεσμα έχουμε την αποτροπή της. Αυτό είναι κάτι ανάλογο με ένα σύστημα ανίχνευσης παρείσφρησης (intrusion detection system) που ανιχνεύει τον εισβολέα αμέσως όταν η παρείσφρηση εμφανίζεται και τον εμποδίζει προτού να μπορέσει να κάνει οποιαδήποτε ζημιά. Σε άλλες περιπτώσεις υπάρχει καθυστέρηση πριν η ανίχνευση οδηγήσει σε απάντηση και έτσι οι

επιθέσεις οδηγούν σε επιβλαβή αποτελέσματα. Για παράδειγμα, αυτό συμβαίνει με το διαρρήκτη όταν ο συναγερμός δεν καταλάβει αμέσως την ενέργεια του.

Στα RFID συστήματα, τα μέτρα που βασίζονται στην ανίχνευση δεν απαιτούν κρυπτογραφικές διαδικασίες από τις ετικέτες αλλά χρησιμοποιούν τη διαφάνεια για να ανιχνεύσουν τις κλωνοποιημένες ετικέτες ή τις αλλαγές στην ιδιοκτησία ετικετών. Η αποτελεσματικότητα ενός βασισμένου στην ανίχνευση μέτρου χαρακτηρίζεται από το πόσο μεγάλη είναι η πιθανότητα ανίχνευσης της απειλής. Σε αντίθεση με τα προληπτικά μέτρα, τα μέτρα ανίχνευσης μπορούν να παραγάγουν ψεύτικους συναγερμούς όπου μια γνήσια ετικέτα χαρακτηρίζεται ως μιμητής.



Εικόνα 4.4: Απεικόνιση για το πώς οι κλωνοποιημένες ετικέτες μπορούν να ανιχνευθούν από τα στοιχεία και τα ίχνη της διαδρομής (αριστερά): η μετάβαση από τον κόμβο 6 στον κόμβο 2 $\left(p_{6,2}\right)$ δεν είναι δυνατή σύμφωνα με το πρότυπο αλυσίδων εφοδιασμού (δεξιά), το τελευταίο συμβάν στον κόμβο 2 πρέπει να έχει παραχθεί από μια κλωνοποιημένη ετικέτα.

Ο Juels τόνισε ότι το τμηματικό επίπεδο επικύρωσης από μόνο του χωρίς ασφαλή επαλήθευση των ταυτοτήτων μπορεί να είναι ένα ισχυρό εργαλείο ενάντια στην πλαστογράφηση. Ο Koh χρησιμοποίησε αυτήν την υπόθεση για να ασφαλίσει τις φαρμακευτικές αλυσίδες εφοδιασμού με την βοήθεια ενός κεντρικού υπολογιστή επικύρωσης που δημοσίευε έναν κατάλογο γνήσιων προϊόντων με της ταυτότητες τους (ID).

Ο Staake ήταν από τους πρώτους που συζήτησε τη δυνατότητα της επικύρωσης βασισμένη στο ίχνος και τα στοιχεία της διαδρομής των προϊόντων μέσα στο δίκτυο EPC και επισήμανε μερικά προβλήματα που εμφανίζονται, όταν το οπίσθιο μέρος δεν ξέρει πλέον που βρίσκεται το γνήσιο αντικείμενο. Οι Mirowski και Hartnett ανέπτυξαν ένα σύστημα που ανιχνεύει ουσιαστικά τις κλωνοποιημένες ετικέτες RFID ή αλλαγές στην ιδιοκτησία ετικετών με μια εφαρμογή ελέγχου πρόσβασης χρησιμοποιώντας τις μεθόδους ανίχνευσης παρείσφρησης. Για να αντιμετωπιστεί το πρόβλημα της περιορισμένης ορατότητας, ο Lehtonen και η ομάδα του χρησιμοποίησαν μηχανές οι οποίες μαθαίνουν

τεχνικές που ανιχνεύουν αυτόματα τις κλωνοποιημένες ετικέτες από τα ελλιπή στοιχεία θέσης (βλ. εικόνα 4.4).

Ο Ilic και η ομάδα του χρησιμοποίησε μια παρόμοια συγχρονισμένη προσέγγιση μυστικών κωδικών, αλλά η εστίαση της εφαρμογής ήταν στη μεταφορά της ιδιοκτησίας και στον έλεγχο προσπέλασης. Επίσης ο Grummt και ο Ackermann παρουσίασαν μια ιδέα πίσω από τη συγχρονισμένη προσέγγιση μυστικών κωδικών σε μια εφαρμογή RFID ελέγχου προσπέλασης σε ένα σχέδιο το οποίο αποκάλεσαν «επιλεγμένοι, προσωρινοί έγκυρα μυστικοί κωδικοί».

Επιπλέον, ο Koscher και οι συνεργάτες του περιγράψανε την ίδια αρχή σε μια τεχνική έκθεση σαν έναν τρόπο για να αύξησης της ασφάλειας ΠΡΟΣΒΑΣΗΣ η οποία βασίζεται στον κώδικα επικύρωσης των ετικετών EPC. Εντούτοις, κανένας από τους συντάκτες δεν συζήτησε και αξιολόγησε πώς η συγχρονισμένη προσέγγιση μυστικών θα μπορούσε να εφαρμοστεί για να αντιμετωπίσει τις επιθέσεις κλωνοποίησης ετικετών.

Απάντηση

Η απάντηση είναι ό,τι συμβαίνει αφότου ανιχνεύεται μια απειλή. Περιλαμβάνει όλες τις ενέργειες που ελαχιστοποιούν τις αρνητικές επιπτώσεις για τον νόμιμο ιδιοκτήτη και μεγιστοποιούν τις αρνητικές επιπτώσεις για τον επιτιθέμενο από την άποψη της τιμωρίας. Στις εμπορικές εφαρμογές RFID αυτό μπορεί να σημαίνει, παραδείγματος χάριν, κατάσχεση των παράνομων αγαθών, ποινική δίωξη των παράνομων φορέων λόγω παραβιάσεων των συμβάσεων ή λόγω παράνομων δραστηριοτήτων και το τελείωμα των επιχειρησιακών δραστηριοτήτων.

Η έλλειψη αποδοτικής επιβολής του νόμου μπορεί μειώσει σοβαρά τη δύναμη των απαντητικών μέτρων, ειδικά στις αναπτυσσόμενες χώρες. Επιπλέον, οι μικρές εταιρίες έχουν λιγότερη δύναμη στο να αποδώσουν βαριά τιμωρία σε σχέση με τις μεγάλες επιχειρήσεις, κάτι που τις κάνει ενδεχομένως πιο προσοδοφόρους και εύκολους στόχους. Τα απαντητικά μέτρα ορίζουν το πόσο σκληρή θα είναι η τιμωρία και χρηματικά και υλικά και συμβάλλουν αποτρεπτικά.

4.2.4 Επίδραση της Ασφάλειας

Λαμβάνοντας υπόψη τη δομημένη άποψη της ασφάλειας, μπορούμε τώρα να διαμορφώσουμε μια γενική εικόνα των μέτρων ασφάλειας ενός συστήματος, κατά του επιτιθέμενου. Μια τέτοια τοποθέτηση μπορεί να χρησιμοποιηθεί για να αξιολογήσει την αποτελεσματικότητα της ασφάλειας όσον αφορά στους κατ'εξακολούθηση παράνομους οι οποίοι έχουν υποκινηθεί από οικονομικά κίνητρα, αλλά αυτή η προσέγγιση είναι λιγότερο χρήσιμη για περιστασιακούς χάκερ που παρακινούνται από διανοητικές προκλήσεις ή για λόγους φήμης. Το E θα δείχνει την αναμενόμενη καθαρή αξία της προσπάθειας επίθεσης από τον επιτιθέμενο, το CtB θα είναι το κόστος για να σπάσουν

τα προληπτικά μέτρα, P_{det} θα είναι η πιθανότητα να εντοπιστεί μια επίθεση από τα μέτρα ανίχνευσης, P_{pun} η δυνατότητα να τιμωρηθεί ο παράνομος εάν η επίθεση ανιχνευθεί, F η αξία της τιμωρίας και L η αξία του λάφυρου, η διαδικασία της ασφάλειας θα επηρεάζει το όφελος του επιτιθέμενου όπως φαίνεται και στην εξίσωση 1.

$$E = (1 - P_{\text{det}})(L - CtB) - P_{\text{det}} P_{pun} (F + CtB) \qquad (1)$$

Αυτό το πρότυπο βασίζεται στην εργασία του Schechter και αφορά το πόση ασφάλεια είναι αρκετή για να σταματήσει έναν κλέφτη και επιδεικνύει πώς και τα μέτρα πρόληψης και ανίχνευσης μπορούν να καταστήσουν το όφελος ενός αντιπάλου αρνητικό μέσω του υψηλού CtB ή του υψηλού P_{det}, αντίστοιχα. Ειδικότερα, εξαιτίας του κινδύνου τιμωρίας, ένα μέτρο πρόληψης δεν χρειάζεται να έχει ένα 100% P_{det} προκειμένου να έχουμε E < 0. Αυτό σημαίνει ότι ένα μεγάλο ποσοστό ανίχνευσης είναι αρκετό να καταστρέψει το επιχειρησιακό σχεδιασμό ενός κλέφτη.

4.2.5 Ανίχνευση κλωνοποιημένων ετικετών με τη χρήση συγχρονισμένων μυστικών κωδικών

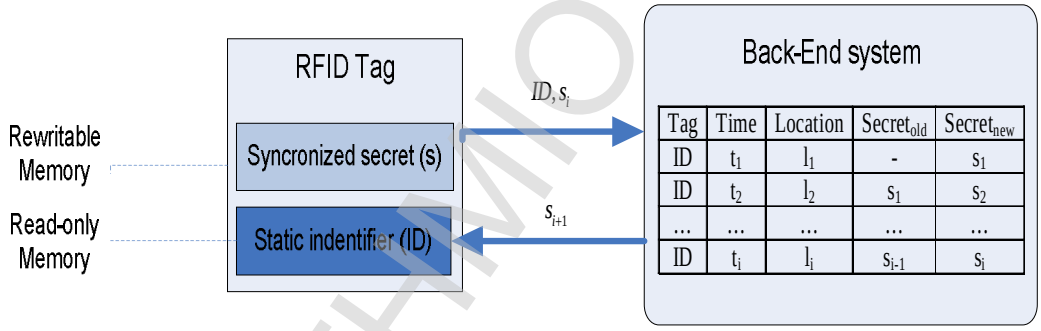
Οι διαθέσιμες μέθοδοι για την ασφάλεια των RFID ετικετών χαμηλού κόστους από την κλωνοποίηση είναι περιορισμένες. Ειδικότερα, οι κρυπτογραφικές προσεγγίσεις που έχουν προταθεί δεν μπορούν να χρησιμοποιηθούν με τις υπάρχουσες τυποποιημένες UHF ετικέτες δεδομένου ότι απαιτούν αλλαγές στο ολοκληρωμένο κύκλωμα του τσιπ, και τα υπάρχοντα μέτρα ανίχνευσης δεν αποδίδουν καλά κάτω από περιορισμένη ορατότητα. Η μέθοδος που θα παρουσιαστεί παρακάτω είναι απλή και έχει προταθεί ήδη σε άλλες εφαρμογές RFID, δεν έχει εφαρμοστεί ακόμα και δεν έχει αξιολογηθεί για την αντιμετώπιση επιθέσεων κλωνοποίησης ετικετών.

Προτεινόμενη Μέθοδος

Η παρούσα μέθοδος χρησιμοποιεί την επαναγράψιμη μνήμη των ετικετών. Σε αντίθεση με τα στατικά αντικείμενα επικύρωσης και τους αναμεταδοτες (π.χ EPC, TID), οι ετικέτες αποθηκεύουν έναν τυχαίο αριθμό ο οποίος αλλάζει κάθε φορά που διαβάζεται η ετικέτα. Αντιστοιχούμε αυτόν τον αριθμό με ένα συγχρονισμένο μυστικό κωδικό δεδομένου ότι είναι άγνωστος σε όλους που δεν έχουν πρόσβαση στην ετικέτα και μπορεί επίσης να γίνει κατανοηθεί ως κωδικός πρόσβασης ενός περάσματος. Ένα συγκεντρωτικό σύστημα οπίσθιου μέρους εκδίδει αυτούς τους αριθμούς και κρατά την αντιστοιχία ποιος αριθμός γράφεται σε ποια ετικέτα έτσι ώστε να μπορεί να ανιχνεύσει λάθη συγχρονισμού.

Κάθε φορά που διαβάζεται μια ετικέτα, το σύστημα οπίσθιου μέρους αρχικά επαληθεύει το στατικό αναγνωριστικό της ετικέτας. Εάν αυτός ο αριθμός ισχύει, το σύστημα οπίσθιου μέρους συγκρίνει το συγχρονισμένο μυστικό κωδικό της ετικέτας με έναν άλλο που αποθηκεύεται για εκείνη την ιδιαίτερη ετικέτα. Εάν αυτοί οι αριθμοί ταιριάζουν με, η ετικέτα περνά τον έλεγχο, σε αντίθετη περίπτωση προκαλείται συναγερμός. Μετά από τον έλεγχο αυτό, το οπίσθιο μέρος παράγει ένα νέο συγχρονισμένο μυστικό κωδικό τον οποίο η συσκευή του αναγνώστη γράφει στην ετικέτα. Αυτή η διαδικασία περιγράφεται στην Εικόνα 4.5.

Διακρίνουμε περιπτώσεις όπως μια ετικέτα να έχει ένα περασμένο χρονικά συγχρονισμένο μυστικό κωδικό, είτε η ετικέτα να είναι γνήσια αλλά να μην έχει ενημερωθεί σωστά (desynchronization) ή κάποιος να έχει επέμβει σκόπιμα και έχει να έχει γράψει έναν παλαιό κωδικό στη γνήσια ετικέτα ή η γνήσια ετικέτα να έχει κλωνοποιηθεί και η κλωνοποιημένη ετικέτα να έχει ανιχνευθεί.



Εικόνα 4.5: Εικονογράφηση του πρωτοκόλλου

Από τότε που τα ακούσια προβλήματα μη-συγχρονισμού μπορούν να αντιμετωπιστούν με bit αναγνώρισης (acknowledgments) και η παραπάνω μορφή βανδαλισμού εμφανίζεται κάπως μη ρεαλιστική στις σημερινές εμπορικές εφαρμογές RFID, ένας περασμένος χρονικά συγχρονισμένος μυστικό κωδικός είναι μια δυνατή ένδειξη επίθεσης κλωνοποίησης ετικετών. Εάν μια ετικέτα έχει ένα έγκυρο κωδικό αλλά ένα συγχρονισμένο μυστικό που δεν έχει εκδοθεί ποτέ από το σύστημα οπίσθιου μέρους, η ετικέτα είναι πιθανό να ακυρωθεί.

Ένας ξεπερασμένος συγχρονισμένος μυστικός κωδικός από μόνος του δεν αποδεικνύει ότι μια ετικέτα είναι η κλωνοποιημένη. Εάν η κλωνοποιημένη ετικέτα διαβάζεται πριν από τη γνήσια ετικέτα τότε μόλις αναγνωριστεί η απάτη, θα είναι η γνήσια ετικέτα που έχει ένα περασμένο συγχρονισμένο μυστικό. Για να γίνει σωστή εύρεση της κλωνοποιημένης ετικέτας εκτός από όλα τα αλλά χρειάζεται και χειρωνακτική η οπτική επιθεώρηση των ετικετών.

Για να προστατευτεί το πλάνο αυτό από τις επιθέσεις ενδιάμεσου ατόμου (MITM) και από τα κακόβουλα συστήματα οπίσθιου μέρους και τους αναγνώστες, τα συστήματα

οπίσθιου μέρους και οι αναγνώστες χρειάζονται έναν αξιόπιστο τρόπο να αποδεικνύεται η αυθεντικότητά μεταξύ τους. Αυτό μπορεί να γίνει χρησιμοποιώντας παραδείγματος χάριν μια έμπιστη πλατφόρμα αναγνωστών και την τυποποιημένη βασική υποδομή δημόσιου κλειδιού (PKI).

Εκτός από τη γνώση ότι μια επίθεση κλωνοποίησης έχει εμφανιστεί, το σύστημα οπίσθιου μέρους μπορεί να επισημάνει ένα χρονικό παράθυρο και ένα παράθυρο θέσης όπου η επίθεση κλωνοποίησης συνέβη.

Επίπεδο Ασφαλείας

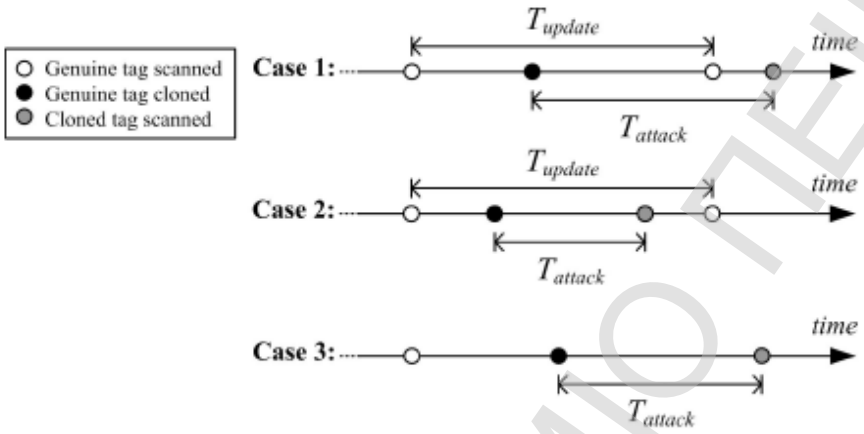
Το επίπεδο ασφάλειας ενός βασισμένου στην ανίχνευση μέτρου ασφάλειας χαρακτηρίζεται από το ποσοστό ανίχνευσής του. Σε αυτήν την υπό-ενότητα θα αξιολογήσουμε το επίπεδο ασφάλειας της παρουσιασμένης μεθόδου με ένα στατιστικό πρότυπο.

Υποθέτουμε ότι ένα σύστημα αποτελείται από έναν μεγάλο αριθμό ετικετών που έχουν ένα στατικό αναγνωριστικό και αμετάβλητη μνήμη για το συγχρονισμένο μυστικό κωδικό. Οι ετικέτες επανειλημμένως ανιχνεύονται από τους αναγνώστες οι οποίοι συνδέονται με το σύστημα οπίσθιου μέρους. Η πιθανότητα ότι μια ετικέτα θα ανιχνευθεί στο μέλλον τουλάχιστον ακόμα μια φορά είναι σταθερή και υποδηλώνεται με Θ. Όταν μια ετικέτα ανιχνεύεται, ο συγχρονισμένος μυστικός κωδικός της ανανεώνεται και στην ετικέτα και στο σύστημα οπίσθιου μέρους όπως περιγράφεται και στην υποενότητα 3.1. Ο χρόνος μεταξύ αυτών των αναπροσαρμογών για μια ετικέτα υποδηλώνεται από μία τυχαία μεταβλητή T_{update}. Ένας επιτιθέμενος μπορεί να αντιγράψει οποιαδήποτε ετικέτα του συστήματος και στην συνέχεια να εγχύσει την κλωνοποιημένη ετικέτα στο σύστημα. Η χρονική καθυστέρηση από την στιγμή που παρουσιάζεται μια επίθεση αντιγραφής έως ότου να ανιχνευθεί η αντιγραμμένη ετικέτα υποδηλώνεται μια τυχαία μεταβλητή T_{attack}. Επιπλέον, να σημειώσουμε ότι ο επιτιθέμενος θα προσπαθήσει να υποθέσει την τιμή του συγχρονισμένου μυστικού.

Οι απαντήσεις του συστήματος μπορούν να αναλυθούν στατιστικά. Η πιθανότητα για να βρεθεί επιτυχώς το συγχρονισμένο μυστικό μιας γνήσιας ετικέτας είναι $1/\left(2^N\right)$, όπου το N δείχνει το μήκος του συγχρονισμένου μυστικού σε bit. Ακόμη με μικρό αριθμό, π.χ. N = 32, το να μαντέψει κάποιος τον συγχρονισμένο μυστικό κωδικό είναι δύσκολο (2×10^{-9}), έτσι το σύστημα μπορεί να θεωρηθεί ασφαλές ενάντια στην επίθεση που στηρίζεται στο μάντεμα του μυστικού κωδικού. Δεύτερον, όταν εμφανίζεται μια επίθεση αντιγραφής, τρία πιθανά σενάρια είναι δυνατά (εικόνα 4).

- **Περίπτωση 1:** Η γνήσια ετικέτα ανιχνεύεται πριν από την αντιγραμμένη ετικέτα και προκαλείται συναγερμός, όταν ανιχνεύεται η αντιγραμμένη ετικέτα.
- **Περίπτωση 2:** Η αντιγραμμένη ετικέτα ανιχνεύεται πριν από τη γνήσια ετικέτα και προκαλείται συναγερμός, όταν ανιχνεύεται η γνήσια ετικέτα.
- **Περίπτωση 3:** Η γνήσια ετικέτα δεν ανιχνεύεται και έτσι κανένας συναγερμός δεν προκαλείται για την αντιγραμμένη ετικέτα.

Στην πρώτη περίπτωση η κλωνοποιημένη ετικέτα εντοπίζεται αμέσως μόλις ανιχνευθεί και η αρνητική επίπτωση της επίθεσης μπορεί να αποτραπεί. Στην δεύτερη περίπτωση η κλωνοποιημένη ετικέτα δεν προκαλεί συναγερμό κάτι που γίνεται με το πέρασμα της γνήσιας ετικέτας. Στην τρίτη περίπτωση η ασφάλεια αποτυγχάνει και η επίθεση κλωνοποίησης περνά απαρατήρητη. Το επίπεδο ασφάλειας χαρακτηρίζεται από την πιθανότητα της πρώτης υπόθεσης όπου η επίθεση αποτρέπεται και από την υπόθεση της δεύτερης επίθεσης όπου η επίθεση ανιχνεύεται.



Εικόνα 4.6: σχηματική επεξήγηση των πιθανών αποτελεσμάτων μια επίθεσης κλωνοποίησης

$$\text{Πιθανότητα Αποτροπής} = \Pr(case1) \qquad (2)$$

$$\text{Πιθανότητα Ανίχνευσης} = \Pr(case1 \vee case2) \qquad (3)$$

Η πιθανότητα της πρώτης περίπτωσης είναι ίση με την πιθανότητα ότι η γνήσια ετικέτα ανιχνεύεται τουλάχιστον ακόμα μια φορά, Θ, που πολλαπλασιασμένη με την πιθανότητα ότι η γνήσια ετικέτα ανιχνεύεται πριν από την κλωνοποιημένη ετικέτα.Υποθέτουμε ότι ο χρόνος που η επίθεση κλωνοποίησης εμφανίζεται είναι ανεξάρτητος από τον χρόνο που ανιχνεύεται η γνήσια ετικέτα και κατανέμεται ομοιόμορφα το χρονικό άξονα, έτσι ο μέσος χρόνος πριν ανιχνευθεί η γνήσια ετικέτα ανιχνεύεται μετά την επίθεση αντιγραφής και είναι T_{update}=2. Μπορούμε τώρα να υπολογίσουμε την πιθανότητα της περίπτωσης 1 ως εξής:

$$\Pr(Case1) = \Theta \times \Pr\left(\frac{T_{update}}{2} - T_{attack} < 0\right) \qquad (4)$$

Θεωρούμε $T_{update} \sim N\left(m_{update}, s^2_{update}\right)$ και $T_{attack} \sim N\left(m_{attack}, s^2_{attack}\right)$ ότι, μπορούμε να υπολογίσουμε την πιθανότητα της πρώτης υπόθεσης χρησιμοποιώντας μία τυχαία μεταβλητή $Z = \frac{T_{update}}{2} - T_{attack}$ όπως παρακάτω:

$$\Pr(Case1) = \Theta \times \Pr\left(Z < 0\right) \qquad (5)$$

Η κανονική κατανομή του Z μπορεί να υπολογιστεί χρησιμοποιώντας τους ακόλουθους κανόνες: Εάν $X \sim N\left(n, t^2\right)$, τότε $aX \sim N\left(an, \left(at^2\right)\right)$ και εάν $Y \sim N\left(k, l^2\right)$, τότε $X + Y \sim N\left(n + k, t^2 + l^2\right)$

$$Z \sim N\left(\frac{m_{update}}{2} - m_{attack}, \frac{s^2_{update}}{4} + s^2_{attack}\right) \qquad (6)$$

Η εξίσωση 4 δείχνει ότι το επίπεδο ασφάλειας της συγχρονισμένης μεθόδου μυστικών κωδικών εξαρτάται από τη συχνότητα στην οποία οι γνήσιες ετικέτες ανιχνεύονται όσον αφορά στη χρονική καθυστέρηση της επίθεσης, και από την πιθανότητα η γνήσια ετικέτα να ανιχνευτεί ακόμα μια φορά. Το ίδιο πράγμα επιβεβαιώνεται από τις εξισώσεις 5 και 6 οι οποίες παρουσιάζουν πιο σαφώς ότι, στην περίπτωση των κανονικά διανεμημένων χρονικών μεταβλητών, $\lim_{m_{attack} - m_{update} \to \infty} \Pr\left(Case1\right) = \Theta$.

Μετά από την τελευταία συναλλαγή της γνήσιας ετικέτας, μια απλή κλωνοποιημένη ετικέτα θα περάσει πάντα απαρατήρητη (περίπτωση 3). Υποθέσαμε τα παραπάνω από έναν στατιστικά μέσο επιτιθέμενο ο οποίος δεν εκμεταλλεύεται συστηματικά αυτήν την ευπάθεια. Εντούτοις, ένας πραγματικός επιτιθέμενος ο οποίος ξέρει το σύστημα δεν υπάρχει μεγάλη πιθανότητα να συμπεριφερθεί κατά αυτόν τον τρόπο. Επομένως αυτή η ευπάθεια πρέπει να επιδιορθωθεί με ετικέτες που θα έχουν σημανθεί και που είναι γνωστές για να τις αφήνει το σύστημα.

4.2.6 Εφαρμογή

Σε αυτό το σημείο θα παρουσιαστεί η πειραματική εφαρμογή της μεθόδου χρησιμοποιώντας ετικέτες UHF που προσαρμόζονται στα πρότυπα EPC. Αυτές οι

ετικέτες είναι πραγματικά χαμηλού κόστους (περίπου 0.10-0.20$), παρέχουν μόνο βασικές λειτουργίες (π.χ. 96-bit επαναγράψιμο προσδιοριστικό, πρόσβαση προστατευμένη με κωδικό, 16-bit ψευδό τυχαία αριθμό-γεννήτρια), επομένως αναμένεται να χρησιμοποιηθούν σε μεγάλες ποσότητες για την αποθήκευση πληροφοριών.

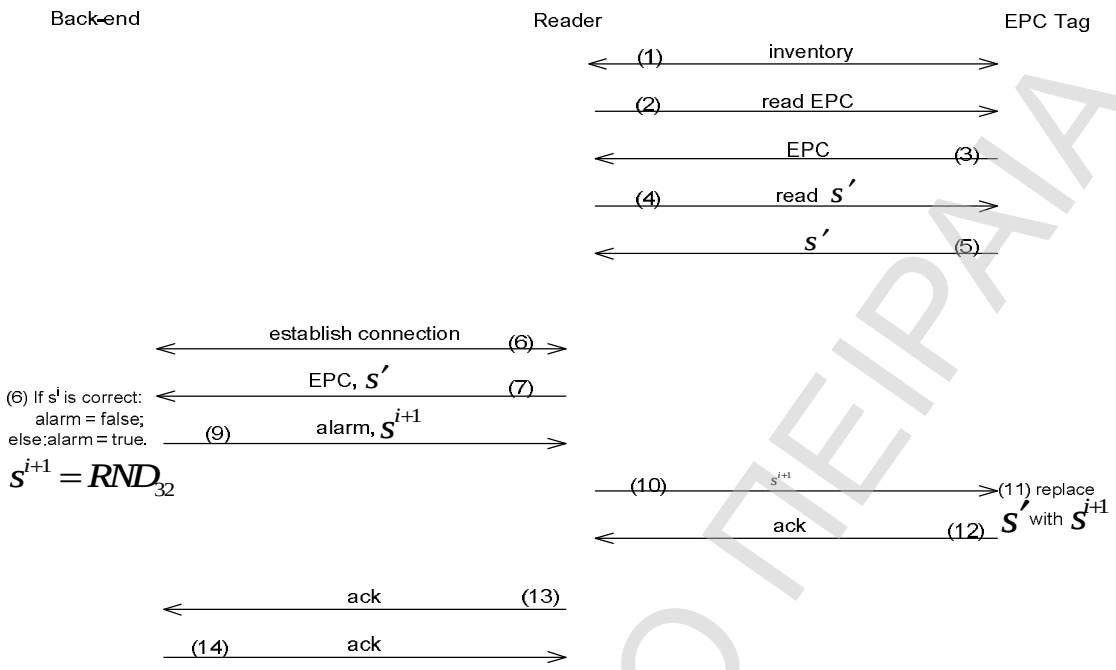
Τα πρότυπα EPC ορίζουν μια «τράπεζα» μνήμης χρηστών για την αποθήκευση του συγχρονισμένου μυστικού κωδικού. Για να διαφανούν οι πραγματικοί περιορισμοί υλικού λόγω του χαμηλού κόστους ετικετών RFID, αρκεί να τονίσουμε ότι πολλές υπάρχουσες ετικέτες EPC δεν έχουν οποιαδήποτε μνήμη χρηστών. Για να παρακάμψει αυτό το πρόβλημα, μία ετικέτα μπορεί εναλλακτικά να ξαναγράψει τον 32-bit κωδικό πρόσβασης στη διατηρημένη τράπεζα μνήμης και να υποθηκεύσει το συγχρονισμένο μυστικό ή να χρησιμοποιήσει ένα μέρος της «τράπεζας» μνήμης EPC εάν δεν απαιτείται εντελώς για το προσδιοριστικό του αντικειμένου.

Το πρωτόκολλο μεταξύ του συστήματος οπίσθιου μέρους, του αναγνώστη, και της ετικέτας παρουσιάζεται στην εικόνα 4.7. Στην απεικόνιση, το s^i δείχνει το τρέχον συγχρονισμένο μυστικό, $s^i + 1$ το νέο συγχρονισμένο μυστικό, RND_{32} ένας νέος 32-bit τυχαίος αριθμός, *alarm* μια μεταβλητή η οποία δέχεται 0 η 1 έτσι ώστε να προκαλείται ή όχι ένας συναγερμός, και ACK ένας αριθμός της βεβαίωσης επιτυχούς ανανέωσης του συγχρονισμένου μυστικού κωδικού.

Το βήμα 6 αφιερώνεται στην εγκατάσταση μιας ασφαλούς σύνδεσης μεταξύ του αναγνώστη και του συστήματος οπίσθιου μέρους για να αντιμετωπιστεί η επίθεση ενδιάμεσου στην ετικέτα και τον αναγνώστη επιτιθέμενου (MITM), για να αντιμετωπιστούν κακόβουλα συστήματα οπίσθιου μέρους, και για να προστατευτεί η ακεραιότητα του οπίσθιου μέρους.

4.2.6.1 Εγκατάσταση

Έχει εφαρμοστεί η παραπάνω μέθοδος χρησιμοποιώντας GEN-2 ετικέτες EPC κατηγορίας 1 από UPM Raflatac το οποίο χρησιμοποιεί τσιπ Monza 1A που κατασκευάζονται από την εταιρεία Impinj. Η συσκευή του αναγνώστη είναι UHF A828EU από το CAEN και ελέγχεται από ένα laptop το οποίο έχει εγκατεστημένο ένα τοπικό πρόγραμμα σύνδεσης (client program). Το σύστημα οπίσθιου μέρους εφαρμόστηκε ως κεντρικός υπολογιστής (server) που αποθηκεύει αριθμούς EPC, συγχρονισμένους μυστικούς κωδικούς και χρονικά σημάδια σε μια MySQL βάση δεδομένων. Η οργάνωση υλικού παρουσιάζεται στην εικόνα 4.8 .



Εικόνα 4.7: Εφαρμοσμένο πρωτόκολλο

Δεδομένου ότι μια υποδομή RFID είναι σε ισχύ και οι ετικέτες έχουν ένα μέτριο ποσό μνήμης, το μόνο άμεσο κόστος της μεθόδου είναι η χρονική καθυστέρηση της επαλήθευσης και της ενημέρωσης των συγχρονισμένων μυστικών κωδικών, δηλ. βήματα 4-14 του πρωτοκόλλου (βλ. εικόνα 5). Έχουμε μετρήσει αυτόν τον παραπάνω χρόνο για 100 “διαβάσματα” όπου το προϊόν με την ετικέτα έχει την κεραία σε απόσταση 5 εκατοστών.

4.2.6.2 Εκτέλεση

Ο μέσος χρόνος επεξεργασίας μιας ετικέτας ήταν 864 ms. Αυτό περιλαμβάνει 128 ms για την εντολή καταλόγων, 181 ms για την ανάγνωση του αριθμού EPC και τα υπόλοιπα 555 ms είναι η χρονικά επιβάρυνση του συγχρονισμένου πρωτοκόλλου μυστικών κωδικών. Οι μετρημένοι μέσοι χρόνοι και οι σταθερές αποκλίσεις παρουσιάζονται στην εικόνα 4.9. Τα αποτελέσματα δείχνουν ότι η χρονική επιβάρυνση του πρωτοκόλλου αυξάνει τον χρόνο επεξεργασίας της ετικέτας κατά 300%, μετά από την εντολή καταλόγων.

Παρά το γεγονός ότι η χρονική επιβάρυνση είναι μικρή σε απόλυτες τιμές, κάνει την διαφορά στη μαζική ανάγνωση όπου τα παραπλήσια προϊόντα ανιχνεύονται αμέσως.

Μια προσεκτικότερη ματιά στα χρονικά διαστήματα των βημάτων αποκαλύπτει ότι το γράψιμο ενός νέου συγχρονισμένου μυστικού κωδικού στην ετικέτα είναι ελαφρώς πιο αργό από το διάβασμα ενός μυστικού κωδικού από την ετικέτα, και ότι η μεγαλύτερη διαφορά υπάρχει στην πρόσβαση του συστήματος οπίσθιου μέρους (βήματα 6-9).

Η απόδοση εξαρτάται από την εφαρμογή και έχει τη δυνατότητα να καλυτερεύσει μέσω της βελτιστοποίησης του αναγνώστη και του λογισμικού οπίσθιου μέρους. Επιπλέον, η διαφορά στη λανθάνουσα κατάσταση των κεντρικών υπολογιστών κάνει την χρονική επιβάρυνση δύσκολο να προβλεφθεί.

Παρά τους περιορισμούς, αυτό το απλό πείραμα παρέχει το στοιχείο ότι ο παραπάνω χρόνος μπορεί να περιορίσει τη δυνατότητα χρησιμοποίησης της συγκεκριμένης μεθόδου στην περίπτωση μιας χρονικά περιορισμένης μαζικής ανάγνωσης.

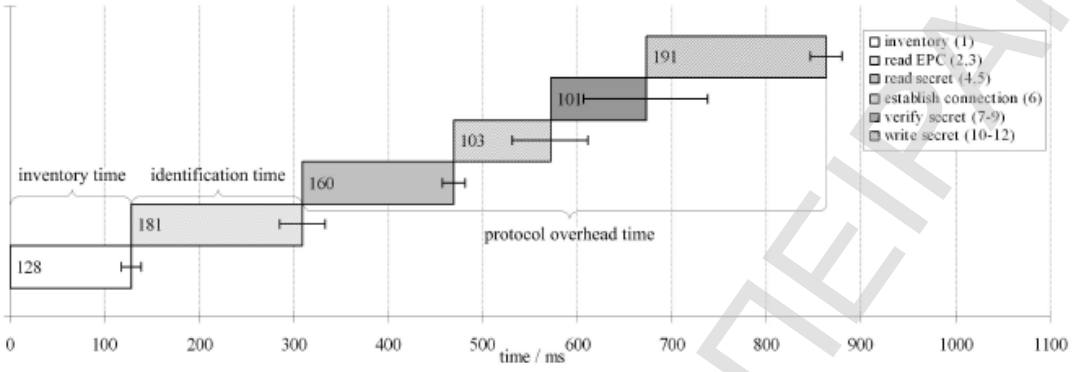
Εικόνα 4.8: Εγκατάσταση εξοπλισμού

4.2.6.3 Συζήτηση

Η πρόκληση των σχεδιαστών συστημάτων είναι να κατασκευάζουν συστήματα τα οποία να μπορούν να αντισταθούν όχι μόνο στους περιστασιακούς χάκερ, αλλά και στο «νόμο της πλεονεξίας» που λέει ότι εάν υπάρχει μια δυνατότητα να κερδίσει κάποιος κάτι από απρομελέτητη ή παράνομη χρήση, αργά ή γρήγορα κάποιος θα βρεθεί που θα το κάνει. Δεδομένου ότι RFID χρησιμοποιείται κυρίως ως αναγνωριστικό αντικειμένων, το πρώτο βήμα προστασίας είναι η σιγουριά ότι τα αντικείμενα είναι αυτό που ισχυρίζονται ότι είναι. Τέτοιες επιθέσεις παραπέμπουν σε επιθέσεις κλωνοποίησης της διεύθυνσης ή σε επιθέσεις πλαστογραφίας των ετικετών.

Η αβεβαιότητα που αφορά τους συναγερμούς είναι έμφυτη στα μέτρα ασφάλειας που βασίζονται στην ανίχνευση και είναι ένας σημαντικός παράγοντας δαπανών της συνολικής λύσης δεδομένου ότι χρειάζεται χειρονακτική εργασία. Στα χαρακτηριστικά συστήματα παρείσφρησης-ανίχνευσης ένας συναγερμός δείχνει ότι μια παρείσφρηση πρέπει να έχει συμβεί και στη συγχρονισμένη μέθοδο μυστικού κωδικού ένας συναγερμός δείχνει ότι ένα από τα αντικείμενα με την ίδια ταυτότητα δεν είναι γνήσιο.

Επομένως οι τελικοί χρήστες των μέτρων ασφάλειας ανίχνευσης θα πρέπει να εφαρμόσουν μια διαδικασία για να ειδοποιούνται από κάθε συναγερμό.



Εικόνα 4.9: Μετρημένοι μέσοι χρόνοι και σταθερές αποκλίσεις (φραγμοί λάθους) των διαφορετικών βημάτων (αριθμοί στα κουτάκια) στο εφαρμοσμένο πρωτόκολλο

Για την μέθοδο αυτή η διαδικασία περιλαμβάνει τον εντοπισμό όλων των φυσικών αντικειμένων με την ίδια ταυτότητα και χειρονακτική επαλήθευση αυτών των αντικειμένων. Σε σύγκριση με άλλα μέτρα ασφάλειας που βασίζονται στην ανίχνευση η συγχρονισμένη μέθοδος μυστικών κωδικών έχει ένα σημαντικό πλεονέκτημα σχετικά με τον χρόνο αναγκαίας χειρωνακτικής επαλήθευσης, από την στιγμή που έχουμε συναγερμό στην μέθοδο συγχρονισμένων μυστικών κωδικών θα υπάρχει πάντα μια επίθεση κλωνοποίησης. Όσον αφορά στις μεθόδους που βασίζονται στην διαδρομή και στα ίχνη που αφήνουν οι ετικέτες, συναγερμοί μπορούν να παραχθούν από οποιοδήποτε μη ομαλό γεγονός στις αλυσίδες εφοδιασμού. Αυτό το πλεονέκτημα θα επεξηγηθεί με ένα αριθμητικό παράδειγμα στην υπό-ενότητα, παρακάτω.

Η συγχρονισμένη μέθοδος μυστικών κωδικών δεν απαιτεί τη διανομή των στοιχείων της διαδρομής και των ιχνών αυτής κάτι το οποίο είναι πολύ σημαντικό για τις επιχειρήσεις που χειρίζονται πολύ ευαίσθητα δεδομένα. Εντούτοις, εάν υπάρχουν μεγάλες καθυστερήσεις μεταξύ των ανιχνεύσεων, η συγχρονισμένη μέθοδος μυστικών κωδικών μπορεί να προκαλέσει έναν συναγερμό για πιθανή κλωνοποιημένη ετικέτα, μόνο όμως μετά από μια μεγάλη καθυστέρηση. Σε μερικές εφαρμογές αυτή η καθυστέρηση δεν μπορεί να υπάρχει, παραδείγματος χάριν, ένα πλαστό φάρμακο θα έχει ήδη πουληθεί και καταναλωθεί. Στη μέθοδο που βασίζεται στη διαδρομή και στα ίχνη ο συναγερμός προκαλείται αμέσως μόλις ανιχνευθεί η κλωνοποιημένη ετικέτα και έτσι παρόμοιες καθυστερήσεις είναι λιγότερο πιθανό να εμφανιστούν.

Ένα φυσικό σύστημα οπίσθιου μέρους είναι απίθανο να είναι αρκετά γρήγορο σε επεξεργαστική ισχύ ώστε να τρέξει το συγχρονισμένο πρωτόκολλο μυστικών κωδικών για πολύ μεγάλους αριθμούς αντικειμένων στους οποίους θα επικολληθούν ετικέτες. Το σύστημα οπίσθιου μέρους μπορεί να είναι διαμοιρασμένο ουσιαστικά σε έναν απεριόριστο αριθμό κεντρικών υπολογιστών, παραδείγματος χάριν, ενός κεντρικού

υπολογιστή οπίσθιου μέρους ανά οικογένεια προϊόντων, ανά τύπο προϊόντων, ανά γεωγραφική περιοχή, ή ανά υποσύνολο ορισμένων ειδών προϊόντων. Αυτό μπορεί να εφαρμοστεί είτε με στατικούς καταλόγους που χαρτογραφούν τους αριθμούς EPC στα συστήματα οπίσθιου μέρους και που είναι γνωστοί από τους αναγνώστες ή με τη βοήθεια της υπηρεσίας ονοματοδοσίας αντικειμένων EPC (Object Naming Service, ONS) ή της υπηρεσίας ανακαλύψεων (Discovery Services, DS) που παρέχουν ένα κεντρικό σημείο για ερωτήσεις, πληροφορίες και υπηρεσίες σχετικά με ένα προϊόν. Επιπλέον, η εξελιξιμότητα σχετικά με τις απαιτήσεις της παρούσας μεθόδου είναι η ίδια όπως σε οποιοδήποτε σύστημα RFID όπου το σύστημα οπίσθιου μέρους γνωρίζει την τρέχουσα θέση και κατάσταση των στοιχείων. Πρόσθετες απαιτήσεις για παρούσα μέθοδο περιλαμβάνουν την ισχυρή επικύρωση μεταξύ των συσκευών αναγνωστών και του συστήματος οπίσθιου μέρους για να εξασφαλίσουν το πρωτόκολλο ενάντια στις επιθέσεις ενδιάμεσου (επιτιθέμενου) μεταξύ αναγνώστη και ετικέτας (Man In The Middle, MITM).

Όλες οι ετικέτες EPC είναι ενδεχομένως τρωτές στο να αλλάξουν τα στοιχεία τους από τον επιτιθέμενο κάτι που μπορεί να χρησιμοποιηθεί ως επίθεση άρνησης υπηρεσιών (DOS) ενάντια στην παρούσα μέθοδο. Αυτή η ευπάθεια στις επιθέσεις άρνησης υπηρεσιών (DOS) μπορεί να μετριαστεί με κωδικούς πρόσβασης EPC. Ο αναγνώστης θα ανακτά τον κωδικό πρόσβασης και ξεκλειδώνει την ετικέτα μετά από ταυτοποίηση (βλ. βήμα 2 στην εικόνα 5) και θα κλειδώνει την ετικέτα αφού ανανεωθεί ο συγχρονισμένος μυστικός κωδικός. Επιπλέον, η προστασία γραφής και ανάγνωσης της μνήμης χρηστών στην οποία ο συγχρονισμένος μυστικό κωδικός αποθηκεύεται μπορεί να χρησιμοποιηθεί ως συμπληρωματικό μέτρο ασφάλειας για να αποτραπεί η κλωνοποίηση και η αλλαγή στοιχείων στην ετικέτα. Επιπλέον, η χρήση των συγχρονισμένων μυστικών ανοίγει ένα παράθυρο για επίθεση άρνησης υπηρεσιών (DOS) κάνοντας μια γνήσια ετικέτα να προκαλέσει συναγερμό ακόμα και όταν δεν υπάρχει κλωνοποιημένη ετικέτα στο σύστημα. Ένας επιτιθέμενος που βρίσκεται κοντά σε έναν εξουσιοδοτημένο αναγνώστη μπορεί να κρυφακούσει το στατικό αριθμό ταυτότητας και το συγχρονισμένο μυστικό κωδικό μιας γνήσιας ετικέτας και να προσποιηθεί αυτή την ετικέτα σε ένα αναγνώστη πριν η γνήσια ετικέτα εμφανιστεί.

Έτσι η γνήσια ετικέτα θα ενεργοποιήσει έναν συναγερμό την επόμενη φορά που θα ανιχνευθεί. Αυτό οδηγεί σε μια περιττή χειρωνακτική επιθεώρηση της γνήσιας ετικέτας (που θα αποκαλύψει το χρόνο και τη θέση της επίθεσης προσωποποίησης). Αυτή η επίθεση άρνησης υπηρεσιών (DOS) είναι δυνατή μόνο όταν έχουν οι επιτιθέμενοι πρόσβαση σε μια εξουσιοδοτημένη συσκευή αναγνωστών, κάτι που δεν είναι χαρακτηριστικό στην περίπτωση των εφαρμογών αλυσίδων εφοδιασμού όπως η αντι-πλαστογράφηση. Επιπλέον, ο χρόνος και η θέση της επίθεσης άρνησης υπηρεσιών (DOS) καταχωρείται, ενώ υπάρχουν απλούστερες επιθέσεις που επιτυγχάνουν την ίδια έκβαση χωρίς να αφήνουν οποιοδήποτε ίχνος, δηλαδή φυσική ή ηλεκτρομαγνητική καταστροφή των ετικετών.

4.2.7 Αντί-πλαστογράφηση

Η παρούσα μέθοδος, ολοκληρώνεται βάζοντας ταμπέλες σε όλα τα παραγόμενα προϊόντα, κάνει έτσι την εισχώρηση των πλαστών προϊόντων στην προστατευμένη αλυσίδα εφοδιασμού πολύ δύσκολη. Πλαστά προϊόντα που δεν έχουν τις ετικέτες RFID ή που έχουν τις ετικέτες RFID με τους άκυρους αριθμούς ταυτότητας χαρακτηρίζονται ως πλαστά. Τα πλαστά προϊόντα με τις κλωνοποιημένες ετικέτες RFID προκαλούν από-συγχρονισμό τον οποίο το σύστημα οπισθίου μέρους ανιχνεύει (περίπτωση 1 ή περίπτωση 2).

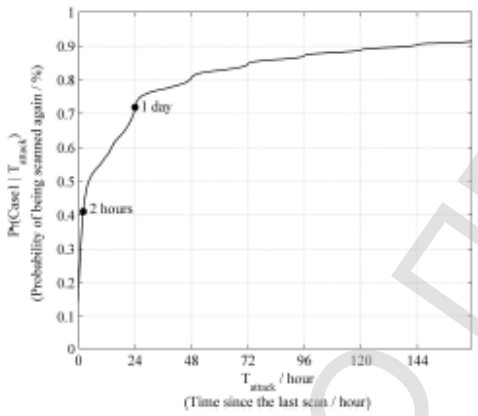
Σε κάθε περίπτωση, δεν υπάρχει τίποτα που ένας επιτιθέμενος να μπορεί να κάνει σε μια κλωνοποιημένη ετικέτα που θα απέτρεπε το σύστημα από την ανίχνευση της επίθεσης κλωνοποίησης, δεδομένου ότι οι γνήσιες και κλωνοποιημένες ετικέτες θα ανιχνευθούν. Εκτός από την προστασία του συστήματος από την κλωνοποίηση ετικετών, η μέθοδος αυτή χορηγεί επίσης μια απόδειξη του πότε χρονικά κλωνοποιούνται οι ετικέτες. Αυτό βοηθά περαιτέρω στην επισήμανση ίσως των παράνομων φορέων και των προβληματικών θέσεων . Δεδομένου ότι οι αναγνώστες και τα προϊόντα βρίσκονται σε εγκαταστάσεις συνεργατών οι οποίοι συνεισφέρουν στην παραγωγή των αλυσίδων εφοδιασμού, ο κίνδυνος των προαναφερθεισών επιθέσεων άρνησης υπηρεσιών (DOS) είναι χαμηλός. Από τα παραπάνω καταλαβαίνουμε ότι η συγκεκριμένη μέθοδος παρέχει μια ιδιαίτερη αύξηση στην ασφάλεια συγκριτικά με αυτή που καθορίζεται στις πρότυπες EPC /RFID αλυσίδες εφοδιασμού όπου η επίθεση κλωνοποίησης ετικετών δεν εξετάζεται.

4.2.8 Έλεγχος Πρόσβασης

Το επίπεδο ασφάλειας της παρουσιασμένης μεθόδου εξαρτάται από πόσο συχνά οι ετικέτες ανιχνεύονται και σε πόσο χρόνο ο αντίπαλος πρέπει να διευθύνει την επίθεση κλωνοποίησης και πλαστοπροσωπίας. Μελετάμε τα ποσοστά ανίχνευσης γνήσιων ετικετών βασισμένων σε ένα σύνολο στοιχείων ελέγχου δημόσια πρόσβασης. Αυτό το σύνολο στοιχείων είναι ένα αρχείο στο οποίο αποθηκεύεται η δραστηριότητα των καρτών εγγύτητας μέσα σε ένα σύστημα ελέγχου πρόσβασης που ελέγχει την είσοδο στα μέρη ενός κτηρίου.

Η πιθανότητα μια ετικέτα να ανιχνεύθηκε πάλι μέσα σε αυτό το σύνολο στοιχείων παρουσιάζεται στην εικόνα 4.10 ως η λειτουργία της χρονικής καθυστέρησης από την προηγούμενη ανίχνευση. Αυτή η τιμή είναι ίση με την πιθανότητα ότι μια αυθαίρετη εκτεθειμένη κλωνοποιημένη ετικέτα ενεργοποιεί έναν συναγερμό (περίπτωση 1) δεδομένης της καθυστέρημένης επίθεσης. Παραδείγματος χάριν, ένας αντίπαλος ο οποίος κλωνοποιεί μια γνήσια ετικέτα και ανιχνεύεται, μετά από 2 ή 24 ώρες αφότου γίνει η κλωνοποίηση υπάρχει 41% ή 72% πιθανότητα αντίστοιχα να δημιουργηθεί συναγερμός λόγω πλαστοπροσωπίας. Η συνολική πιθανότητα μία ετικέτα να ανιχνευθεί και πάλι είναι Θ, το οποίο ήταν 99,15% και αντιστοιχεί στο ποσοστό ανίχνευσης της τρίτης περίπτωσης.

Τα ευρήματα δείχνουν ότι μόνο πολύ λίγες επιθέσεις κλωνοποίησης θα πήγαιναν ενδεχομένως απολύτως απαρατήρητες στη μελετημένη εφαρμογή, και ότι ένας επιτιθέμενος πρέπει να διευθύνει την επίθεση πλαστοπροσωπίας μέσα σε μερικές ώρες μετά από την κλωνοποίηση ετικετών για να έχει μια σχετική καλή πιθανότητα να αποφύγει έναν συναγερμό.



Εικόνα 4.11: Η χρονική καθυστέρηση μεταξύ διαδοχικών διαβάσμάτων σε ένα σύνολο στοιχείων ελέγχου πρόσβασης

Τέλος, θα συγκριθεί η απόδοση της συγχρονισμένης μεθόδου μυστικών κωδικών με αυτήν του Deckard, ένα σύστημα που σχεδιάστηκε για να ανιχνεύει κλωνοποιημένες ετικέτες μέσα στο προαναφερθέν σύνολο στοιχείων βασισμένο στις στατιστικές ανωμαλίες. Κατά μέσο όρο, ο Deckard ήταν σε θέση να ανιχνεύσει 76% των κλωνοποιημένων ετικετών με ένα 8% ψεύτικων συναγερμών από τα προσομοιωμένα σενάρια επίθεσης μέσα στο προαναφερθέν σύνολο στοιχείων.

Αν υποθέσουμε ότι το 1% των ενέργειών παράγονται από κλωνοποιημένες ετικέτες, αυτό σημαίνει ότι για κάθε συναγερμό που προκαλείται από μια κλωνοποιημένη ετικέτα υπάρχουν περίπου 11 ψεύτικοι συναγερμοί που προκαλούνται από τις γνήσιες ετικέτες. Κατά συνέπεια η πιθανότητα ότι μια ετικέτα που προκαλεί έναν συναγερμό είναι πραγματικά κλωνοποιημένη είναι μόνο 8.4%. Σύμφωνα με τη συγχρονισμένη μέθοδο μυστικών κωδικών, κάθε συναγερμός δείχνει μια επίθεση κλωνοποίησης και η πιθανότητα ότι μια ετικέτα που προκαλεί έναν συναγερμό είναι πραγματικά κλωνοποιημένη είναι 50%, έναντι μόνο 8.4% με την μέθοδο Deckard. Ακόμη ένας συναγερμός θα προκαλούταν στο 99.15% των κλωνοποιημένων ετικετών, έναντι στο 76% που μας δίνει η μέθοδος του Deckard. Αυτό το αριθμητικό παράδειγμα επεξηγεί την βελτιωμένη αξιοπιστία της συγχρονισμένης μεθόδου μυστικών κωδικών έναντι σε οποιοδήποτε μέτρο βασισμένο στην ανίχνευση για την ασφάλεια RFID.

ΠΑΡΑΓΡΑΦΟΣ 4.3

Ένα υβριδικό πρωτόκολλο RFID ενάντια στις Tracking επιθέσεις

4.3.1 Εισαγωγή

Η RFID είναι μια τεχνολογία με την οποία κάποιος μπορεί να προσδιορίσει αντικείμενα ή και ανθρώπους με την ενσωμάτωση των ετικετών, ένα μικρό τσίπ ικανό να διεξάγει ασύρματη μετάδοση στοιχείων. Με την επικόλληση των ετικετών στα εμπορεύματα των καταστημάτων, κάποιος μπορεί να επιτευχθεί γρηγορότερα η διαδικασία καταγραφής απλά με μια ασύρματη ανίχνευση. Οι ετικέτες RFID έχουν διάφορα χαρακτηριστικά. Καταρχήν, κάθε ετικέτα έχει ένα προσδιοριστικό για να αντιπροσωπευθεί. Επιπλέον, τέτοια προσδιοριστικά έχουν αρκετά μακρύ κώδικα έτσι ώστε να είναι μοναδικός. Επιπλέον, κάθε μικροσκοπική ετικέτα εμφυτεύεται μέσα σε ένα αντικείμενο. Κατά συνέπεια, η εύρεση της ετικέτας σημαίνει το αντίστοιχο αντικείμενο. Δεύτερον, ο προσδιορισμός ετικετών μέσω της ραδιοσυχνότητας επιτρέπει στα αντικείμενα να διαβαστούν σε μια αρκετά μεγάλη απόσταση. Αυτά τα χαρακτηριστικά εισάγουν ζητήματα μυστικότητας, π.χ. ανιχνευσιμότητα των ετικετών από τους παράνομους επιτιθεμένους.

Ένα από τα πολύ σημαντικά ζητήματα μυστικότητας είναι η προστασία των προσωπικών δεδομένων των χρηστών. Τα αντικείμενα που ενσωματώνονται με τις επισφαλείς ετικέτες μπορούν να αποκαλύψουν ιδιωτικές πληροφορίες κατά την διάρκεια της επικοινωνίας τους από τους αναγνώστες. Ένα άλλο σημαντικό ζήτημα μυστικότητας είναι η αποκάλυψη της θέσης στην οποία βρίσκεται ο χρήστης. Αντικείμενα στα οποία ενσωματώνονται ετικέτες οι οποίες δεν αποκαλύπτουν οποιαδήποτε ευαίσθητη πληροφορία μπορούν να παρακολουθηθούν από άλλες εμφυτευμένες ετικέτες. Αυτό γίνεται λόγω του ότι οι απαντήσεις των ετικετών στις αιτήσεις των αναγνωστών είναι δυνατό να βοηθήσουν στον εντοπισμό των αντικειμένων με την ανάλυση των στοιχείων είτε από τους νόμιμους είτε από παράνομους αναγνώστες από μια σταθερή θέση. Αυτό μπορεί να αναγκάσει τα αντικείμενα να αποκαλύψουν τα ιδιωτικά, μυστικά τους στοιχεία όπως προσδιοριστικά στοιχεία (πχ. ταυτότητα) που θα έχουν στο άμεσο μέλλον. Το άλλο σημαντικό ζήτημα μυστικότητας είναι η αποκαλούμενη μπροστινή μυστικότητα που καθορίζεται ως εξής. Σε μια τυχαία χρονική στιγμή t, υποθέτουμε ότι στον επιτιθέμενο δίνονται όλες οι πληροφορίες μεταξύ των ετικετών και των αναγνωστών, συμπεριλαμβανομένων όλων των πληροφοριών που αποθηκεύονται σε μια ετικέτα η οποία έχει καταληφθεί από τον επιτιθέμενο. Η μπροστινή μυστικότητα επιβάλει στον επιτιθέμενο να μην είναι σε θέση να προσπελάσει οποιαδήποτε προηγούμενη

επικοινωνία μεταξύ της κατελημένης ετικέτας και των αναγνωστών για ένα χρονικό διάστημα $t' < t$.

4.3.2 Προεπισκόπηση παλαιότερων σχετικών εργασιών

Πολλά RFID πρωτόκολλα έχουν προταθεί για να αντιμετωπίσουν τα διάφορα ζητήματα μυστικότητας. Ο Weis πρότεινε το αποκαλούμενο "Hash Lock" σχέδιο στο οποίο χρησιμοποίησαν τη συναρτήσεις κατακερματισμού (hash) h για να κομματιάσουν ένα τυχαίο κλειδί K έτσι ώστε η τιμή που θα προκύπτει να χρησιμοποιείται ως ταυτότητα της ετικέτας, ID=h(K).

Όταν ένας αναγνώστης ρωτά μια ετικέτα, η ετικέτα αποκρίνεται με μια ταυτότητα ID και στην συνέχεια ο αναγνώστης στέλνει αυτή την ID στη βάση δεδομένων οπίσθιου μέρους (η οποία δημιουργείται συνήθως από hash συναρτήσεις) για να ανατρέξει το κατάλληλο βασικό K' έτσι ώστε $h(K') = h(K)$. Μόλις βρει ο αναγνώστης το κλειδί K', το διαβιβάζει πίσω στην ετικέτα και η ετικέτα κομματιάζει το κλειδί K' και το συγκρίνει με το $h(K)$. Εάν οι τιμές ταιριάζουν, η ετικέτα ξεκλειδώνεται. Σημειώνουμε ότι ακολουθώντας αυτή τη πολιτική μεσολαβεί ένα σύντομο χρονικό διάστημα έρευνας στη βάση δεδομένων λόγω του ότι για να δημιουργηθεί ο πίνακας εφαρμόζονται συναρτήσεις κατακερματισμού (hash). Η ετικέτα που προκύπτει από αυτό το σχέδιο μπορεί να ακολουθηθεί εύκολα από έναν επιτιθέμενο μέσω της αντιστοιχίας των ID. Επιπλέον, κρυφακούγοντας την επικοινωνία μεταξύ του νόμιμου αναγνώστη και της στοχοθετημένης ετικέτας, ο επιτιθέμενος μπορεί να πάρει το επιθυμητό κλειδί K δεδομένου ότι το K θα στέλνεται με επισφαλής ασύρματη επικοινωνία.

Ο Weis επίσης έδωσε μια τυχαία έκδοση του σχεδίου "Hash Lock" στο οποίο μια ετικέτα κομματιάζει την ταυτότητά της σε μια μακριά τυχαία σειρά δεδομένων έτσι ώστε η παραγωγή της να φαίνεται τυχαία και ως εκ τούτου μεταβλητή. Αυτό αποτρέπει την επίθεση στην ετικέτα. Ακριβώς, όταν ρωτιέται από τον αναγνώστη, η ετικέτα παράγει μια τυχαία σειρά δεδομένων R, υπολογίζει τη τιμή της με συνάρτηση κατακερματισμού (hash) $h(R \| ID)$, και μεταδίδει $(R, h(R \| ID))$ στον αναγνώστη. Καθώς λαμβάνει $(R, h(R \| ID))$, ο αναγνώστης αρχίζει μια αναζήτηση "Brute Force" στα αποθηκεμένα ID στη βάση δεδομένων έως ότου να βρει μια εγγραφή που να ταιριάζει με την πρόκληση της ετικέτας $(R, h(R \| ID))$. Αν και οι ετικέτες με αυτό τον τρόπο εξασφαλίζουν την πλήρη μυστικότητα, δεν είναι δόκιμο ο τρόπος δεδομένου ότι ένας τεράστιος αριθμός διαδικασιών κατακερματισμού πρέπει να εκτελεστεί στη βάση δεδομένων. Επιπλέον, αυτό το πρωτόκολλο δεν εγγυάται την μπροστινή μυστικότητα δεδομένου ότι οι αποθηκεμένες πληροφορίες σε μια κατελημένη από τον επιτιθέμενο ετικέτα αποκαλύπτουν πολλές πληροφορίες της προηγούμενης επικοινωνίας της ίδιας ετικέτας.

Μια πρόσθετη εκτεταμένη έκδοση του τυχαίου "Hash Lock" σχεδίου που εξασφαλίζει μπροστινή μυστικότητα προτάθηκε από τον Ohkubo. Για να εγγυηθεί την μπροστινή μυστικότητα, η βασική ιδέα τους είναι επαναπροσδιορισμός της ταυτότητας

των ετικετών κάθε φορά που ρωτιέται η ετικέτα από έναν αναγνώστη. Το σχέδιο μπορεί να επιτευχθεί μέσω ενός μηχανισμού χαμηλού κόστους αλυσίδων συναρτήσεων κατακερματισμού. Ωστόσο, αυτό το σχέδιο δεν είναι επίσης δόκιμο δεδομένου ότι απαιτεί εξαντλητική αναζήτηση. Για να μειώσουν την πολυπλοκότητα στην αναζήτηση, ο Avoine και ο Oechslin χρησιμοποίησαν μια χορό-χρονική τεχνική ανταλλαγή μνήμης έτσι ώστε να κερδηθεί χρόνος αναζήτησης. Αν και έλαβαν καλύτερο χρόνο αναζήτησης το προτεινόμενο σχέδιό απαιτεί ένα πρόσθετο συγχρονισμό συντηρήσεων μεταξύ μιας μεμονωμένης ετικέτας και της βάσης δεδομένων οπίσθιου μέρους κάτι που συνιστά μειονέκτημα.

Ο Δημητρίου χρησιμοποίησε ένα αμοιβαίο σχέδιο επικύρωσης μεταξύ των ετικετών και των αναγνωστών για να διευθετήσει το ζήτημα του μη συγχρονισμού. Πρότεινε ένα τριών φάσεων πρωτόκολλο όπως περιγράφεται παρακάτω. Ενώ ο αναγνώστης ξεκινά ένα αίτημα στην ετικέτα, επισυνάπτει επίσης μια τυχαία αλφαρηρμιτική σειρά K_R.

Μόλις λαμβάνει το K_R, η ετικέτα υπολογίζει μια τιμή με συνάρτηση κατακερματισμού (hash) στο προσωρινό προσδιοριστικό ID_i, δηλ. το $h(ID_i)$, στην συνέχεια παράγει μια νέα τυχαία σειρά K_t, και υπολογίζει τη hash αξία ολόκληρης της σειράς (ID_i, K_R, K_T), δηλ. $h(ID_i \| K_R \| K_T)$. Κατόπιν η ετικέτα διαβιβάζει το $h(ID_i)$, K_T, και το $h(ID_i \| K_R \| K_T)$ πίσω στον αναγνώστη και χρησιμοποιεί μια συσκευή βασισμένη σε συνάρτηση κατακερματισμού για να ανανεώσει το προσδιοριστικό του σε $ID_i + 1$. Ο νόμιμος αναγνώστης γνωρίζει το προσωρινό προσδιοριστικό της ετικέτας ID_i μέσω μιας γρήγορης αναζήτησης της hash αξίας $h(ID_i)$ που είναι αποθηκεμένη στη βάση δεδομένων. Αφού υπολογίσει το ID_i , η βάση δεδομένων μπορεί επίσης να ανανεώσει το προσδιοριστικό της ετικέτας σε $ID_i + 1$ με τον ίδιο μηχανισμό όπως η ετικέτα. Τώρα, ο νόμιμος αναγνώστης μπορεί να περάσει επιτυχώς την πρόκληση της ετικέτας. Υπολογίζει ακριβώς την αξία ολόκληρης της σειράς $ID_i + 1$, του K_R, και K_T και το στέλνει πίσω στην ετικέτα.

Τέλος, η ετικέτα μπορεί να ελέγξει την ισχύ της αξίας με υπολογισμό του $h(ID_i + 1 \| K_R \| K_T)$ και συγκρίνοντας το με το μήνυμα που στάλθηκε από τον αναγνώστη. Αυτό το πρωτόκολλο επιτρέπει και στους αναγνώστες και στις ετικέτες πάντα τον τέλειο συγχρονισμό, και ως εκ τούτου εγγυάται την μπροστινή μυστικότητα. Εντούτοις, εάν κανένας εξουσιοδοτημένος αναγνώστης δεν ανανεώνει το προσωρινό προσδιοριστικό της ετικέτας, τότε αυτό παραμένει σταθερό και μπορεί έτσι να ακολουθηθεί από τον επιτιθέμενο. Ακόμη και μεταξύ της σύνδεσης για ταυτοποίηση με έναν νόμιμο αναγνώστη, η παραγωγή της ετικέτας παραμένει στατική. Οι ετικέτες μπορούν να ακολουθηθούν από τον επιτιθέμενο κατά τη διάρκεια αυτής της περιόδου.

Από τα παραπάνω, μπορεί κάποιος να αναρωτηθεί εάν είναι δυνατό να υπάρξει πλήρη μυστικότητα που να βασίζεται σε συναρτήσεις κατακερματισμού ως σχέδιο επικύρωσης RFID με μια αποδοτική διαδικασία προσδιορισμού που απαιτεί μόνο τον υπολογισμό $o(n)$ της βάσης δεδομένων οπίσθιου μέρους όπου το n είναι ο αριθμός ετικετών.

4.3.3 Τεχνική Πρωτοκόλλου

Σε αυτό το πρωτόκολλο δίνεται ένα σχέδιο για την πλήρη διατήρηση της ιδιωτικότητας βασισμένο σε συναρτήσεις κατακερματισμού (hash) στο οποίο η χρονική πολυπλοκότητα είναι κατά το ήμισυ γραμμική υπό μια αποσβησμένη έννοια.

Εδώ, δίνεται εν συντομία το πλάνο κατασκευής. Η ιδέα πίσω από το πρωτόκολλό αυτό είναι να συνδυαστεί ομαλά το μη συστηματικό (τυχαίο) με βάση τις συναρτήσεις κατακερματισμού σχέδιο κλειδώματος και το αμοιβαίο σχέδιο επικύρωσης που είχε προτείνει ο Δημητρίου. Όπως αναφέρεται στο προηγούμενο τμήμα, το πρωτόκολλο που πρότεινε ο Δημητρίου διατηρεί πλήρως την ιδιωτικότητα εκτός από τις θέσεις οι οποίες παρακολουθούνται από μη εξουσιοδοτημένες ομάδες.

Το κύριο μειονέκτημα είναι ότι η παραγωγή $h(ID_i)$ από την στοχοποιημένη ετικέτα είναι πάντα σταθερή (ως εκ τούτου είναι εύκολο να ακολουθηθούν τα ίχνη της) όταν την προσελκύουν συνεχώς παράνομοι αναγνώστες. Για να υπερνικήσουμε αυτό το πρόβλημα, εφαρμόζουμε την τυχαία hash τεχνική κλειδώματος με μια σχετικά μικρή τυχαία σειρά αλφαριθμητικών. Παρόλα αυτά, αυτό οδηγεί σε μια "brute force" αναζήτηση στη βάση δεδομένων οπίσθιου μέρους. Για να λύσουμε αυτό το δίλημμα, παρατηρούμε τα ακόλουθα. Από την στιγμή που η τυχαία σειρά αλφαριθμητικών που επιλέγουμε είναι σχετικά μικρή, για κάθε ετικέτα, μπορούμε να αποθηκεύουμε όλες τις πιθανές hash τιμές του προσδιοριστικού της ετικέτας που συνδέεται με όλες τις πιθανές τυχαίες αλφαριθμητικές σειρές στη βάση δεδομένων. Δεν Απαιτείται πάρα πολύ χώρος για να εφαρμοστεί κατι τέτοιο στη βάση δεδομένων. Κατά συνέπεια η χρονική πολυπλοκότητα της αναζήτησης βάσεων δεδομένων οπίσθιου μέρους είναι πιο αποδοτική από το πλήρως τυχαίο hash σχέδιο κλειδώματος. Απ' την άλλη το προτεινόμενο σχέδιο φαίνεται να αντέχει στην πίεση από τις συνεχείς ερωτήσεις των παράνομων αναγνωστών.

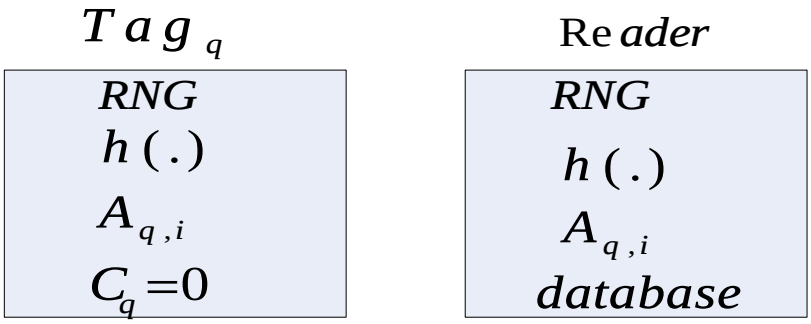
Εντούτοις, μια επίθεση γενεθλίων (Birthday attack) μπορεί να έχει ως αποτέλεσμα η ετικέτα να ακολουθείται και πάλι ανεξάρτητα από τις εξουσιοδοτημένες ή μη εξουσιοδοτημένες προκλήσεις. Για παρακάμψουμε και αυτό το πρόβλημα, σε κάθε ετικέτα χρησιμοποιούμε ένα μετρητή a που θα καταγράφει τον αριθμό παράνομων ερωτήσεων. Μόλις ο αριθμός παράνομων ερωτήσεων είναι μεγαλύτερος από κάποιο σταθερό όριο που έχει συμφωνηθεί, το πρωτόκολλο προχωρά και εκτελεί το αρχικό τυχαίο βασισμένο σε συναρτήσεις κατακερματισμού σχέδιο κλειδώματος ώστε να ανανεωθεί το προσδιοριστικό της ετικέτας. Όπως μπορούμε να δούμε, το σχήμα που προτείνεται έχει χαμηλότερη απόσβεση κόστους κατά την διαδικασία ταυτοποίησης ενώ προσδίδει πλήρη μυστικότητα. Παρακάτω, παρουσιάζεται το αμοιβαίο σχέδιο επικύρωσής και η ανάλυση ασφάλειάς του.

4.3.4 Το Πρωτόκολλο

Σε αυτό το σημείο παρουσιάζεται το σχήμα επικύρωσης. Για περισσότερη ευκολία θα χρησιμοποιούμε την παρακάτω σήμανση για το υπόλοιπο της περιγραφής.

Σήμανση	**Αντίστοιχη σημασία**
N	Αριθμός των ετικετών που συμμετέχουν στο RFID σύστημα
Tag_q	Η q-οστή ετικέτα
Reader	Ο νόμιμος Αναγνώστης
RNG	Η γεννήτρια τυχαίου αριθμού
$A_{q,i}$	Το προσωρινό αναγνωριστικό της ετικέτας Tag_q κατά την διάρκεια της i-οστής νόμιμης πρόκλησης
$M_1 \| M_2$	Αλληλουχία των μηνυμάτων M_1 και M_2
H	Η συνάρτηση κατακερματισμού που χρησιμοποιείται στο πρωτόκολλο
K_R	Το τυχαίο αλφαριθμητικό που παράγεται από τον αναγνώστη
K_T	Το τυχαίο αλφαριθμητικό που παράγεται από την ετικέτα
R	Το κοντό τυχαίο αλφαριθμητικό που παράγεται από την ετικέτα
C_q	Ο μετρητής που καταγράφει των αριθμό των μη νόμιμων προκλήσεων

4.3.4.1 Αρχικοποίηση



Εικόνα 4.12: Στάδιο αρχικοποίησης για Αναγνώστη και ετικέτα

Καταρχήν, θα περιγράψουμε την οργάνωση των ετικετών και των αναγνωστών. Κάθε ετικέτα και κάθε αναγνώστης έχουν γεννήτριες τυχαίων αριθμών και μια συνάρτηση κατακερματισμού h. Όπως έχει αναφερθεί, το πρωτόκολλό αυτό στηρίζεται στην ύπαρξη ενός τυχαίου κοινού μυστικού κωδικού σε ετικέτα και αναγνώστη. Για την q-οστή ετικέτα, έστω $A_{q,i}$ δείχνει το κοινό μυστικό που αποθηκεύεται επίσης στη βάση δεδομένων. Επιπλέον, για να εγγυηθούμε την μπροστινή μυστικότητα, επιτρέπουμε στην q-οστή ετικέτα και στον αναγνώστη έναν μη αναστρέψιμο υπολογισμός ώστε να ανανεωθεί το προσδιοριστικό σε $A_{q,i+1}$ με έναν συγχρονισμένο τρόπο κάθε φορά που η διαδικασία επικύρωσης είναι επιτυχής.

Τέλος, προκειμένου να αποτραπεί μια επίθεση γενεθλίων, θέτουμε ένα μετρητή Cq για να καταγράψουμε τον αριθμό των παράνομων ερωτήσεων. Σημειώνεται ότι υποθέτουμε ότι η ετικέτα φορτώνεται με ένα αρχικό προσδιοριστικό ID_0 που επιλέγεται τυχαία. Για να είναι πιο επεξηγηματική, η οργάνωση πρωτοκόλλου παρουσιάζεται η εικόνα 4.12.

Στην συνέχεια θα εξετάσουμε την εφαρμογή της βάσης δεδομένων οπίσθιου μέρους. Σημειώνεται ότι συνδυάζουμε το σχετικά μικρό τυχαίο αλφαριθμητικό r και το προσωρινό προσδιοριστικό $A_{q,i}$(metaID) με μια hash λειτουργία h. Έστω ότι $r_1,...,r_m$ απαριθμεί όλες τις πιθανές τυχαίες σειρών r μήκους $\log_m$. Για να είμαστε αποδοτικοί στο να βρούμε το metaID, αποθηκεύουμε το δείκτη $h\left(r_k \| A_{q,i}\right)$ για όλο το $k \in \{1,...,m\}$ όπως φαίνεται στην εικόνα 4.13.

4.3.4.2 Διαδικασία Επικύρωσης

Παρακάτω θα παρουσιαστεί η διαδικασία επικύρωσης και τα στάδια τα οποία ακολουθεί, όπως φαίνεται στην εικόνα 4.13.

Back –end Database	
index	metaID
$h\left(r_1 \| A_{q,i}\right)$	$A_{q,i}$
…	
$h\left(r_m \| A_{q,i}\right)$	
	…

$h\left(r_1 \left\| A_{p,i}\right.\right)$	$A_{p,i}$
…	
$h\left(r_m \left\| A_{p,i}\right.\right)$	

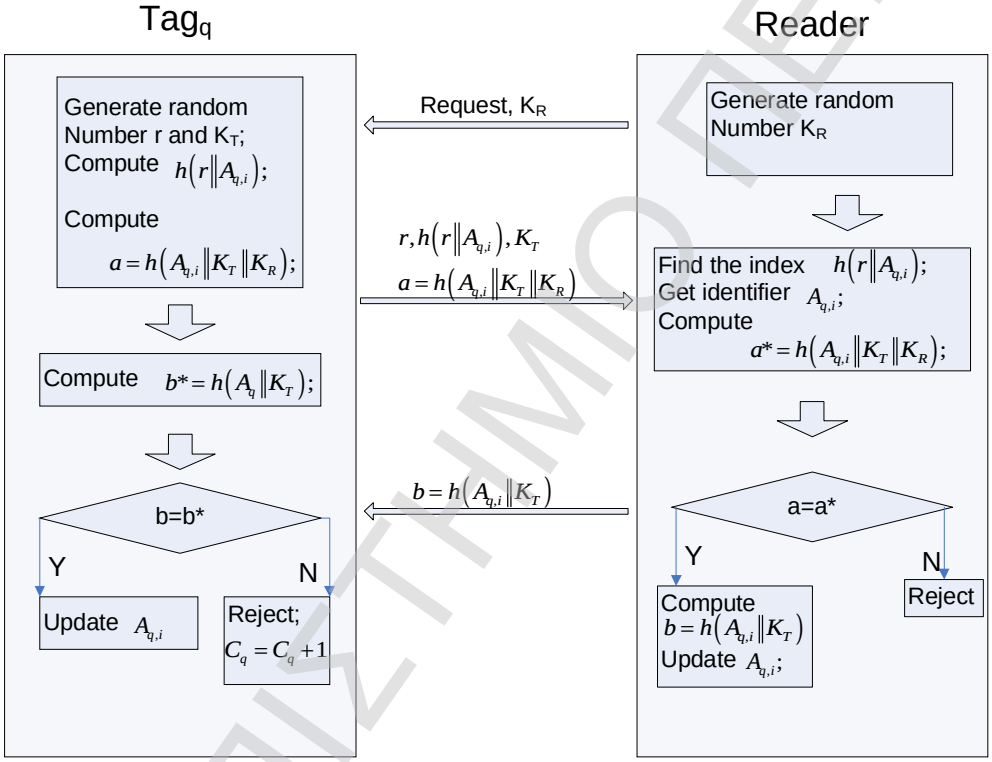
Εικόνα 4.13: Η δομή της βάσης δεδομένων οπισθίου μέρους

1. Ο αναγνώστης κάνει αίτημα στην ετικέτα και στέλνει ένα μακρύ τυχαίο αλφαριθμητικό K_R σε αυτήν.
2. Η ετικέτα παράγει ένα σχετικά μικρό τυχαίο αλφαριθμητικό r και ένα μακρύ τυχαίο αλφαριθμητικό K_T. Κατόπιν υπολογίζει τις δύο τιμές με συναρτήσεις κατακερματισμού $h\left(r \left\| A_{q,i}\right.\right)$ και $h\left(A_{q,i} \left\| K_T \right\| K_R\right)$. Έπειτα η ετικέτα στέλνει τις δυο τιμές καθώς επίσης το r και το K_T στον αναγνώστη.
3. Ο πρώτος στόχος του αναγνώστη είναι να αναγνωρίσει την ετικέτα. Χρησιμοποιεί την τιμή $h\left(r \left\| A_{q,i}\right.\right)$ για να ψάξει γρήγορα για το δείκτη στη βάση δεδομένων και να ανακαλύψει της ετικέτας το metaID = $A_{q,i}$. Υπολογίζει έπειτα τη hash τιμή $h\left(A_{q,i} \left\| K_T \right\| K_R\right)$ και ελέγχει εάν αυτή η τιμή είναι ίση με αυτή που έστειλε η ετικέτα. Εάν ταιριάζουν οι δύο τιμές, ο αναγνώστης υπολογίζει τη hash τιμή $h\left(A_{q,i} \left\| K_T\right.\right)$, στέλνει στην ετικέτα αυτήν την τιμή, και ανανεώνει το $A_{q,i}$ σε $A_{q,i+1}$. Ενώ ο αναγνώστης ανανεώνει το προσδιοριστικό, ενημερώνει επίσης όλους τους σχετικούς δείκτες για το χρησιμοποιημένο αναγνωριστικό $A_{q,i}$ το οποίο υπάρχει στον hash πίνακα .
4. Αφού λάβει την τιμή $h\left(A_{q,i} \left\| K_T\right.\right)$ η ετικέτα ελέγχει εάν είναι αληθινή η τιμή. Εάν ταιριάζουν, έπειτα επιτρέπει στον αναγνώστη να χρησιμοποιήσει όλες τις λειτουργίες του και ανανεώνει το $A_{q,i}$ σε $A_{q,i+1}$. Εάν η τιμές δεν ταιριάζουν ετικέτα απορρίπτει και καταγράφει αυτήν την παράνομη ερώτηση με την βοήθεια του μετρητή C_q.

Μόλις ο αριθμός που καταγράφεται στον δείκτη C_q είναι μεγαλύτερος από κάποια τιμή ορίου (έστω $m^{1/3}$), τότε η ετικέτα ξεκινά να τρέχει το τυχαίο hash πρωτόκολλο κλειδώματος σε συνεργασία με τους αναγνώστες. Απεικονίζουμε το διάγραμμα ροής στην εικόνα 4.14.

4.3.4.3 Πολυπλοκότητα και Ανάλυση Ασφαλείας

Εδώ θα αναλυθεί η υπολογιστική πολυπλοκότητα του πρωτοκόλλου. Υποθέτουμε ότι η ετικέτα δεν εισάγει το τυχαίο hash σχέδιο κλειδώματος. Η διαδικασία επικύρωσης μπορεί να γίνει σε χρόνο $O(\log n)$. Μόλις επιτευχθούν οι αμοιβαίες ταυτοποιήσεις, ανανεώνονται οι σχετικοί δείκτες που σχετίζονται με το χρησιμοποιημένο προσδιοριστικό κάτι που απαιτεί χρόνο m όπου logm είναι το μήκος του σχετικά μικρού τυχαίου αλφαριθμητικού που παράγεται από την ετικέτα. Κατά συνέπεια ο υπολογισμός μιας επιτυχούς επικύρωσης απαιτεί χρόνο $m+O(\log n)$.



Εικόνα 4.14: Το πρωτόκολλο επικύρωσης ανάμεσα σε ετικέτα και αναγνώστη.

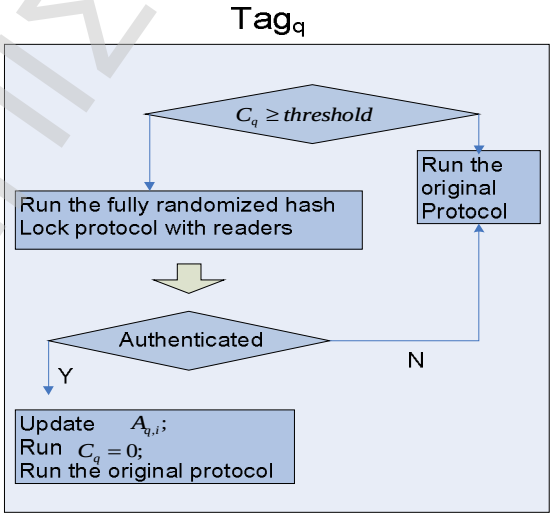
Απ' την άλλη, εάν η ετικέτα αρχίζει το τυχαίο hash σχέδιο κλειδώματος, αυτό απαιτεί το χρόνο $O(n)$. Έτσι στη χειρότερη περίπτωση, δεν βελτιώνουμε το σχέδιο που είχε προτείνει ο Weis. Εντούτοις, από μια άποψη, το πρωτόκολλό τρέχει σε πολύ λιγότερο χρόνο από ότι έχουν δείξει όλα τα προηγούμενα αποτελέσματα. Δεδομένου ότι θέτουμε ένα μετρητή C_q για την q-οστή ετικέτα, η ετικέτα ξεκινά να στέλνει το πλήρες τυχαίο hash σχέδιο κλειδώματος μόνο όταν το C_q είναι μεγαλύτερο από μια τιμή ορίου T. Κατά συνέπεια το αποσβεσμένο κόστος κάθε επιτυχούς επικύρωσης είναι το μέγιστο $m+O(\log n)+O(n/T)$. Εάν θέσουμε $m=n^{3/4}$ και $T=m^{1/3}$, το αποσβεσμένο κόστος θα

είναι το μέγιστο $O\left(n^{3/4}\right)$ που είναι σημαντικά λιγότερο από το n. Το τελευταίο βήμα είναι η εγγύηση της ασφάλειας με αυτές τις παραμέτρους.

Παρόμοια με την ανάλυση ασφάλειας του πρωτοκόλλου που είχε προτείνει ο Δημητρίου, το πρωτόκολλό αυτό μπορεί να αποτρέψει τους αντιπάλους όχι μόνο από τις προαναφερθείσες επιθέσεις αλλά και από τις ακόλουθες.

- *Επίθεση στην ιδιωτικότητα της θέσης*. Αντίθετα από το πρωτόκολλο που πρότεινε ο Δημητρίου, το πρωτόκολλό αυτό εξασφαλίζει την ιδιωτικότητα θέσης όχι μόνο για τις νόμιμες ερωτήσεις αναγνωστών αλλά και για τις παράνομες. Σημειώνουμε ότι όπως αναφέρεται στην εισαγωγή, το πρωτόκολλο του Δημητρίου δεν μπορεί να αποτρέψει την ιδιωτικότητα θέσης από τα παράνομα αιτήματα από τη στιγμή που η ερωτωμένη ετικέτα παράγει σταθερά την ίδια τιμή και ως εκ τούτου μπορεί να ακολουθηθεί από τον επιτιθέμενο.

- ***Birthday attack*** *(Επίθεση γενεθλίων) στην συνάρτηση κατακερματισμού*. Η ετικέτα κατακερματίζει ένα τυχαίο αλφαριθμητικό r σε αρκετά μικρά σε μήκος κομμάτια τα οποία συνδέονται από το προσωρινό προσδιοριστικό της ετικέτας και το οποίο στέλνει έπειτα στον αναγνώστη. Ένας τεράστιος αριθμός των αναρμόδιων ερωτήσεων μπορεί να προκαλέσει την ετικέτα και να αποκαλύψει πληροφορίες μυστικότητας λόγω μιας επίθεσης γενεθλίων. Για να αποτραπεί αυτό, έχουμε έναν μετρητή a που καταγράφει τον αριθμό των αναρμόδιων ερωτήσεων. Μόλις ο αριθμός στο μετρητή είναι μεγαλύτερος από $m^{1/3} = n^{1/4}$, από εκεί και έπειτα η ετικέτα ξεκινάει και τρέχει το τυχαίο hash πρωτόκολλο κλειδώματος σε συνεργασία με τους αναγνώστες



Εικόνα 4.15: Άμυνα εναντίον του μεγάλου αριθμούν παράνομων προκλήσεων

Από την στιγμή που το μήκος του σχετικά κοντού αλφαριθμητικού είναι $3\log n/4$, η πιθανότητα μια επίθεση γενεθλίων με $n^{1/4}$ ερωτήσεις να επιτύχει, είναι αμελητέα. Σημειώνουμε ότι, μπαίνοντας στην κατάσταση να προχωρήσει η ετικέτα σε έναρξη του πλήρως τυχαίου σχεδίου, σημαίνει ότι παρόλο που υπάρχουν πολλές παράνομες προκλήσεις και πάλι επιτυγχάνεται να διατηρείται η ιδιωτικότητα θέσης.

4.3.5 Συμπέρασμα

Σε αυτό το κεφάλαιο, παρουσιάζεται ένα πρωτόκολλο επικύρωσης το οποίο συντηρεί πλήρως την ιδιωτικότητα μεταξύ των ετικετών RFID και των αναγνωστών. Η χρονική πολυπλοκότητα μιας επιτυχούς αμοιβαίας επικύρωσης μεταξύ μιας ετικέτας και ενός αναγνώστη απαιτεί το χρόνο $O\left(n^{3/4}\right)$ σε μια αποσβεσμένη ανάλυση όπου το n είναι ο αριθμός ετικετών που συμμετέχουν στο σύστημα RFID. Αυτό απαντά μερικώς στο ανοικτό πρόβλημα που είχε λεχθεί και το οποίο έλεγε εάν υπάρχει ένα πρωτόκολλο RFID που να διατηρεί πλήρως την ιδιωτικότητα και στο οποίο η χρονική πολυπλοκότητα είναι στη χειρότερη περίπτωση $O(n)$

Επιπλέον, το πρωτόκολλό μας βελτιώνει το πρωτόκολλο που προτείνεται από τον Δημητρίου στο οποίο δεν μπορεί να αποτρέψει την δυνατότητα που έχει ο επιτιθέμενος να ακολουθεί την ετικέτα RFID. Η κύρια συμβολή του πρωτοκόλλου αυτού είναι αποτροπή αυτού του είδους της επίθεσης κρατώντας την αποσβεσμένη χρονική πολυπλοκότητα μέσα στο $O(n)$ όπου το n είναι ο αριθμός ετικετών που περιλαμβάνει το σύστημα RFID.

ΣΥΜΠΕΡΑΣΜΑΤΑ-ΠΑΡΑΤΗΡΗΣΕΙΣ

Λόγω της όλο και περισσότερο ευρείας επέκτασης των συστημάτων RFID, το ζήτημα της ασφάλειας τους είναι πιο σημαντικό από ποτέ.

Στο 1^{ο} κεφάλαιο έγινε μια εισαγωγή στην τεχνολογία RFID. Παρουσιαστήκαν τα βασικά αρχιτεκτονικά χαρακτηριστικά, ο τρόπος λειτουργίας και διάφορες εφαρμογές στις οποίες συναντάμε τα RFID συστήματα.

Στο 2^{ο} κεφάλαιο, προσπαθήσαμε να ανακαλύψουμε κάποια δομή μέσα στο σύνολο των πιθανών επιθέσεων που επιδρούν και έχουν επιπτώσεις σε συστήματα RFID. Με το να εξετάζουμε το σημείο της επίθεσης, τα αποτελέσματα που έχουν στο σύστημα και τα αντίμετρα της επίθεσης, μπορούμε να λάβουμε μια συνεπέστερη άποψη των απειλών και των πιθανών τρόπων αντιμετώπισης των απειλών. Ταξινομήθηκαν οι επιθέσεις βάση του στρώματος στο οποίο κάθε επίθεση πραγματοποιείται και συζητήσαμε τα πιθανά αντίμετρα που μπορούν να χρησιμοποιηθούν για να καταπολεμηθούν αυτές τις επιθέσεις. Έγινε διάκριση των επιθέσεων που δρουν στο φυσικό στρώμα, το στρώμα εφαρμογής, το στρατηγικό στρώμα και τις επιθέσεις που συνδυάζουν σε παραπάνω από ένα στρώμα. Τέλος, επισημάνθηκε για ποιες περιπτώσεις η περαιτέρω έρευνα είναι απαραίτητη προκειμένου να επιτευχθεί η επαρκής υπεράσπιση ενάντια στις επιθέσεις.

Στο 3^{ο} κεφάλαιο παρατίθεται μια συλλογή επιθέσεων κατά των RFID πρωτοκόλλων που μπορεί να χρησιμεύσει ως μια γρήγορη και εύκολη αναφορά.

Στο 4^{ο} κεφάλαιο παρουσιάστηκαν τρία πρωτόκολλα ως λύσεις σε διαφορετικά ζητήματα πάνω στην ασφάλεια της RFID τεχνολογίας. Παρουσιάστηκε αρχικά ένα πρωτόκολλο επικύρωσης που είναι ασυμπτωτικά βέλτιστο από την άποψη της πιθανότητας της ψεύτικης αποδοχής από κοινού στις περιπτώσεις αποστολής μηνυμάτων και μη αποστολής μηνυμάτων, σε αντίθεση με όλα τα προηγούμενα πρωτόκολλα. Η απόδοση του πρωτοκόλλου αυτού, έρχεται εις βάρος των πρόσθετων ικανοτήτων αποθήκευσης προκειμένου να υπολογιστεί ολόκληρο το δέντρο απόφασης πριν εκτελεστεί η γρήγορη φάση. Αυτό καθιστά το πρωτόκολλο συνήθως κατάλληλο στις εφαρμογές όπου ο αριθμός των κύκλων γρήγορης φάσης μπορεί να είναι μικρός - για παράδειγμα, στις καταστάσεις όπου οι Relay επιθέσεις αναμένεται να εμφανιστούν σπάνια. Αριθμητικά, θέτοντας το n = 11 , απαιτείται ένα 1KByte μνήμη. Οι περισσότερες ετικέτες T RFID που χρησιμοποιούνται για την ασφαλή χρήση εφαρμογών διαθέτουν αυτή την μνήμη. Η κλασική τυποποιημένη ετικέτα NXP Mifare παρέχει μνήμη 1KByte και τα ICAO ηλεκτρονικά διαβατήρια (συμμορφωμένα με τους κανονισμούς) ενσωματώνουν μια ετικέτα μνήμης τουλάχιστον 30KByte. Σημειώνουμε ότι διάφορα άλλα κριτήρια βελτιστοποίησης μπορούν να εξεταστούν εκτός από αυτά που προτείνονται στην παράγραφο 4.1. Μια ενδιαφέρουσα κατεύθυνση που μπορεί να εξεταστεί είναι, λαμβάνοντας υπόψη το μέγεθος του μυστικού κλειδιού K, να επιδιωχθεί η διερεύνηση των πιθανοτήτων της ψεύτικης αποδοχής με μετάδοση και χωρίς μετάδοση μηνυμάτων.

Στην συνέχεια παρουσιάστηκε μια συγχρονισμένη μέθοδος μυστικών κωδικών η οποία ανιχνεύει επιθέσεις κλωνοποίησης και επισημαίνει διαφορετικές ετικέτες οι οποίες έχουν την ίδια ταυτότητα. Η ανίχνευση των κλωνοποιημένων ετικετών RFID εμφανίζεται ελκυστική για την εξασφάλιση των εμπορικών εφαρμογών RFID δεδομένου ότι δεν απαιτεί πολύ ακριβές ετικέτες και ετικέτες που να θέλουν συνεχώς παροχή

ενέργειας. Η μέθοδος που παρουσιάστηκε απαιτεί μια μικρής ποσότητας επαναγράψιμη μνήμη για την ετικέτα και παρέχει μια μεγάλη αύξηση στο επίπεδο της ασφάλειας για τα συστήματα που χρησιμοποιούν μη προστατευμένες ετικέτες. Ένα σημαντικό πλεονέκτημα της μεθόδου αυτής είναι ότι μπορεί και χρησιμοποιείται με τις υπάρχουσες τυποποιημένες χαμηλού κόστους ετικέτες RFID, όπως το EPC GEN-2, και μπορεί να εφαρμοστεί σε όλες τις εφαρμογές RFID όπου οι ετικέτες ανιχνεύονται επανειλημμένα. Η συμπληρωματική δαπάνη της παρουσιασμένης μεθόδου είναι η χειρωνακτική εργασία που απαιτείται για να εξακριβωθεί ποια εκ των ετικετών με τον ίδιο αριθμό ταυτότητας είναι η αυθεντική και ποια η κλωνοποιημένη. Ο αριθμός αναγκαίων επαληθεύσεων για την παρουσιασμένη μέθοδο είναι αρκετά μικρότερος από όλες τις συγκρίσιμες μεθόδους ασφάλειας ανίχνευσης. Συνολικά, η μέθοδος αυτή έχει τη δυνατότητα να καταστήσει την επιβλαβή εισαγωγή δεδομένων στις κλωνοποιημένες ετικέτες, στα συστήματα RFID, αρκετά πιο δύσκολη υπόθεση χρησιμοποιώντας μόνο ελάχιστα έξοδα στο υλικό.

Τέλος παρουσιάστηκε ένα υβριδικό πρωτόκολλο RFID ενάντια στις Tracking επιθέσεις. Το πρωτόκολλο αυτό είναι ένα πρωτόκολλο επικύρωσης το οποίο συντηρεί πλήρως την ιδιωτικότητα μεταξύ των ετικετών RFID και των αναγνωστών. Η χρονική πολυπλοκότητα μιας επιτυχούς αμοιβαίας επικύρωσης μεταξύ μιας ετικέτας και ενός αναγνώστη απαιτεί το χρόνο $O\left(n^{3/4}\right)$ σε μια αποσβεσμένη ανάλυση όπου το n είναι ο αριθμός ετικετών που συμμετέχουν στο σύστημα RFID. Αυτό απαντά μερικώς στο ανοικτό πρόβλημα που είχε λεχθεί και το οποίο έλεγε εάν υπάρχει ένα πρωτόκολλο RFID που να διατηρεί πλήρως την ιδιωτικότητα και στο οποίο η χρονική πολυπλοκότητα είναι στη χειρότερη περίπτωση $O(n)$. Επιπλέον, το πρωτόκολλό αυτό βελτιώνει το πρωτόκολλο που προτείνεται από τον Δημητρίου στο οποίο δεν μπορεί να αποτρέψει την δυνατότητα που έχει ο επιτιθέμενος να ακολουθεί την ετικέτα RFID. Η κύρια συμβολή του πρωτοκόλλου αυτού είναι αποτροπή αυτού του είδους της επίθεσης κρατώντας την αποσβεσμένη χρονική πολυπλοκότητα μέσα στο $O(n)$ όπου το n είναι ο αριθμός ετικετών που περιλαμβάνει το σύστημα RFID. Όσον αφορά στο πρόβλημα που διατυπώθηκε από τον Juels απομένει ακόμα να καθοριστεί εάν κάποιο πρωτόκολλο μπορεί να διατηρήσει πλήρη ιδιωτικότητα, του οποίου η μη αποσβησμένη χρονική πολυπλοκότητα θα είναι μέσα στον ημι-γραμμικό χρόνο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Aim Global *org.(2008),«RFID: What is RFID»* www.aiinglobal.org/teclinologies/rfid

2. Autoid.org.(2002), *«Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility-)).*

3. Angeles R.(2007), *«RFID Technologies: Supply-Chain Applications and Implementation Issues»,* IEEE Engineering Management Review. Vol.35. No 2

4. Ayoade, J., Saxby, S. (2007), «Roadmap for Solving Security and Privacy Concerns in RFID Systems», In: *Computer Law and Security Report*

5. CDT: CDT Working Group on RFID. (2006), «Privacy Best Practices for Deployement of RFID Technology», In: Interim Draft, http://www.cdt.org/privacy/20060501rfid-best-practices.php

6. Dimitriou T. (2005), «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.

7. Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum. (2007), «Classification of RFID Attacks Department of Computer Science», Amsterdam.

8. Ton van Deursen, Saˇsa Radomirovi´c. (2008), «Attacks on RFID Protocols» (v1.0).

9. Srdjan Capkun and Jean-Pierre Hubaux. (Feb 2006), «Secure positioning in wireless networks», IEEE Journal on Selected Areas in Communications: Special Issue on Security in Wireless Ad Hoc Networks, 24(2):221–232.

10. Thomas Beth and Yvo Desmedt. (Aug 1990), «Identification tokens – or: Solving the chess grandmaster problem», In Alfred Menezes and Scott Vanstone, editors, Advances in Cryptology – CRYPTO'90, volume 537 of Lecture Notes in Computer Science, pages 169–176, Santa Barbara, California, USA,. IACR, Springer-Verlag.

11. Jorge Munilla, Andres Ortiz, and Alberto Peinado. (July 2006), «Distance bounding protocols with voidchallenges for RFID», Printed handout of Workshop on RFID Security – RFIDSec 06.

12. Gildas Avoine and Aslan Tchamkerten.(Sep 2008), «An Asymptotically Optimal RFID Authentication Protocol Against Relay Attacks», Universit´e Catholique de Louvain TELECOM ParisTech.

13. Fleisch, E. & Mattern, F. (2005), Das Internet der Dinge: «Ubiquitous Computing Und RFID in Der Praxis»: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Springer, Berlin.

14. Juels A.(2006), RFID security and privacy: A research survey. IEEE Journal of Selected Areas of Communication, 24(2), pp. 381{894}.

15. Mirowski, L., Hartnett. (2007), J.: Deckard: A System to Detect Change of RFID Tag Ownership. International Journal of Computer Science and Network Security, 7(7)

16. Michahelles, F., Florkemeier C., Lehtonen M., Hinske S. (2006), «An RFID-tag in Every Ski Item-Level Tagging in the Ski Industry», In: Pervasive Technology Applied - Real-World Experiences with RFID and Sensor Networks, Proceedings of the Pervasive 2006 Workshops, Dublin.

17. Swedberg, C. (2004), RFID Drives Highway Tra_c Reports. RFID Journal

18. Mikko Lehtonen, Daniel Ostojic, Alexander Ilic and Florian Michahelles. (May 2009), «Securing RFID systems by detecting tag cloning», Zurich.

19. Gildas Avoine and Philippe Oechslin. (March 2005), «A scalable and provably secure hash based RFID protocol», In International Workshop on Pervasive Computing and Communication Security – PerSec 2005, pages 110–114, Kauai Island, Hawaii, USA, IEEE, IEEE Computer Society Press.

20. Ari Juels. (2006), «RFID security and privacy: a research survey», IEEE Journal on Selected Areas in Communications, 24(2):381–394,.

21. Ari Juels and Stephen A. Weis. (2007), «Defining strong privacy for RFID», In PerCom Workshops, pages 342–347. IEEE Computer Society.

22. Marc Langheinrich. (Oct 2008), A survey of RFID privacy approaches. Personal and Ubiquitous Computing,. Online First Edition, available from http://www.springerlink.com/content/p71246k75029v715/.

23. Jen-Chun Chang, Hsin-Lung Wu. (March 2009), «A Hybrid RFID Protocol against Tracking Attacks».