Οι ετικέτες RFID ατενίζουν το μέλλον

Μία σύντομη ανασκόπηση των ετικετών RFID

Ενας υπάλληλος της εταιρείας "Metro" (στην Ελλάδα Macro) που οδηγεί μία παλέτα με πάνες μέσα από μία πύλη ανάγνωσης RFID, όπου γίνεται με ταχύτητα ανάγνωση των δεδομένων που περιέχονται στα ολοκληρωμένα. Οι κεραίες του αναγνώστη είναι τοποθετημένες δεξιά και αριστερά (στην φωτογραφία φαίνονται αυτές της δεξιάς πλευράς). (Φωτ. Phlips)

Από τον Renke Bienert

Οι ετικέτες RFID είναι πλέον δυνατόν να χρησιμοποιηθούν από την σήμανση καθαρόαιμων αλόγων, μέχρι την σήμανση κιβωτίων μεταφοράς προϊόντων (τα γνωστά container), δικύκλων ή συσκευασιών με αρώματα. Ακόμη και τα διαβατήρια ή τα εισιτήρια αγώνων εξοπλίζονται πια με ετικέτες RFID. Η τεχνολογία που τις υποστηρίζει διαφοροποιείται τόσο πολύ, όσο και το ίδιο το εύρος των πιθανών τους εφαρμογών.

Τόσο τα άψυχα αντικείμενα όσο και τα έμβια όντα (όπως επίσης και οι άνθρωποι), είναι δυνατόν να αναγνωρισθούν αυτόματα χωρίς να υπάρχει άμεση επαφή με αυτά, εφ' όσον είναι εξοπλισμένα με ένα μικρό σύστημα ταυτοποίησης μέσω ραδιο-συχνοτήτων (radio-frequency identification, [RFID]). Η συγκεκριμένη τεχνολογία αναμένεται μέσα στην τρέχουσα χρονιά να κατακτήσει πολλούς νέους τομείς. Στο άμεσο μέλλον το κόστος των ετικετών RFID θα είναι τόσο μικρό, ώστε να μπορούν να χρησιμοποιηθούν για την σήμανση ακόμη και προϊόντων με χαμηλή τιμή.

Με τον τρόπο αυτό η διαδρομή που ακολουθεί το κάθε μπουκάλι γάλα, το κάθε κουτί ασπιρίνης, ή η κάθε εφημερίδα, από την παραγωγή μέχρι τον τελικό καταναλωτή (ή και ακόμη παραπέρα) θα μπορούσε να παρακολουθείται ηλεκτρονικά. Οι ειδικοί επί των θεμάτων παρακολούθησης αποθηκών και παραγγελιών (logistics) δηλώνουν ικανοποιημένοι από την εν λόγω τεχνολογία δεδομένου ότι μπορεί να συνεισφέρει σημαντικά στην μείωση του κόστους μεταφοράς και αποθήκευσης, αλλά υπάρχουν από την άλλη πολλές ενώσεις προστασίας καταναλωτών οι οποίες εκφράζουν προβληματισμό σχετικά με την προστασία του απορρήτου των επιλογών των καταναλωτών.

Ευλογία ή κατάρα;

Όπως φάνηκε και από το μικρό δημοψήφισμα που πραγματοποιήσαμε στον δικτυακό τόπο του περιοδικού Ελεκτορ, οι απόψεις του κόσμου είναι ανάλογα διχασμένες. Το 80 % για παράδειγμα όσων μετείχαν στο δημοψήφισμα εξέφρασε την άποψη ότι η χρήση των ετικετών RFID θα διευκολύνει την καθημερινή τους ζωή, αλλά ένα εξ ίσου μεγάλο ποσοστό θεωρεί ότι το απόρρητο και η προστασία προσωπικών δεδομένων "απειλούνται". Αυτό το μεγάλο ποσοστό ανασφάλειας δικαιολογείται ίσως από το γεγονός ότι η ανίχνευση μέσω ραδιοσυχνοτήτων, παρόμοια με το ηλεκτρονέφος δεν είναι δυνατόν να γίνει αντιληπτή ούτε ακουστικά, αλλά ούτε και οπτικά.

Το γεγονός ότι μία ετικέτα RFID την οποία μεταφέρουμε (εν γνώσει μας ή εν αγνοίας μας), μπορεί ενδεχομένως να ανιχνευτεί από κάποια κυβερνητική αρχή, εταιρεία ή ακόμη και από κάποιο κακόβουλο άτομο, αποτελεί ένα φόβο, τον οποίο όσοι ασχολούνται με την συγκεκριμένη τεχνολογία, θα πρέπει να λάβουν σοβαρά υπ' όψη τους.

Ο εν λόγω φόβος μπορεί επίσης να τροφοδοτείται και από διάφορες ιστο-

ρίες "τρόμου", όπως για παράδειγμα η ιστορία σχετικά με μία εταιρεία προστασίας (security) η οποία επέβαλλε στους υπαλλήλους της να εμφυτεύσουν κάτω από το δέρμα τους ολοκληρωμένα RFID.

Παρ' όλα αυτά βέβαια αντιδράσεις θα υπάρχουν όπως και με όλες τις επαναστατικές τεχνολογίες, και καλό θα ήταν η εν λόγω τεχνολογία να μην καταδικαστεί λόγω κάποιων ακραίων εφαρμογών. Ούτως ή άλλως, υπάρχουν πολλές διαφορετικές μορφές ετικετών RFID. Οι δημόσιες κατά συνέπεια αναφορές εμφάνισης ιών RFID μαζί με την ταυτόχρονη παρουσία ετικετών της εν λόγω τεχνολογίας στα εισιτήρια του Παγκοσμίου Κυπέλλου Ποδοσφαίρου ή στα διαβατήρια, δεν σημαίνει απαραίτητα ότι μέσω των διαβατηρίων ή των εισιτηρίων ο κόσμος θα γεμίσει με "μοχθηρούς" ιούς (επισκεφθείτε και τους σχετικούς συνδέσμους στο διαδίκτυο που αναφέρονται στο τέλος του άρθρου). Προσοχή όμως χρειάζεται.

Μία περιγραφή του RFID

Πρώτα απ' όλα ας δώσουμε μία σύντομη ερμηνεία της ορολογίας: το "RF" στον όρο RFID σημαίνει ραδιο-συχνότητες (Radio Frequencies), οι οποίες χρησιμοποιούνται για την εκπομπή δεδομένων και ενδεχομένως και ενέργειας. Ο όρος "ID" μπορεί να αναφέρεται σε ένα μεγάλο εύρος εφαρμογών, οι οποίες κυμαίνονται από την απλή ανάγνωση δεδομένων μέχρι την ανταλλαγή κρυπτογραφημένων δεδομένων ή σε σύνθετους υπολογισμούς για την πιστοποίηση της αυθεντικότητας κάποιου εγγράφου ταυτοποίησης.

Ένα σύστημα RFID αποτελείται συνήθως από ένα πομποδέκτη (ή αναγνώστη) και ένα πλήθος αποκριτών RFID οι οποίοι συχνά καλούνται "ετικέτες" ή "transponder" (όρος ο οποίος είναι λανθασμένος), ή απλά "κάρτες".

Θα πρέπει επίσης να κάνουμε τον διαχωρισμό μεταξύ ενεργών και παθητικών καρτών. Οι ενεργές κάρτες τροφοδοτούνται οι ίδιες από κάποια μπαταρία, ενώ οι παθητικές λαμβάνουν ενέργεια από το ίδιο το πεδίο που δημιουργεί ο πομπός.

Στο συγκεκριμένο άρθρο θα περιορίσουμε την προσοχή μας στις παθητικές κάρτες, διότι είναι μικρότερες και φθηνότερες από τις ενεργές κάρτες και κατά συνέπεια πιο ενδιαφέρουσες για εφαρμογές καθημερινής χρήσης.

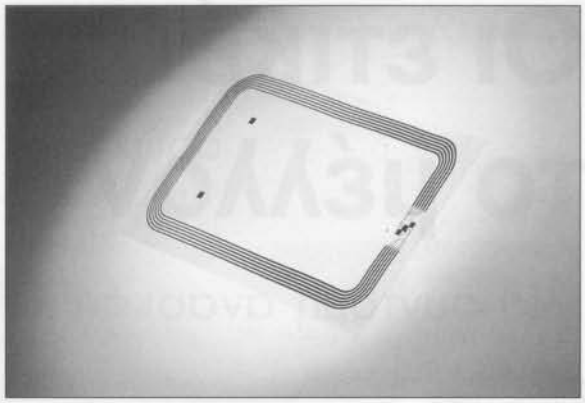
Μέθοδοι σύζευξης

Για την αποστολή δεδομένων μεταξύ κάρτας και του αναγνώστη μπορούν να χρησιμοποιηθούν τρεις διαφορετικές μέθοδοι ζεύξης: η χωρητική, η επαγωγική και η ηλεκτρομαγνητική, με την τελευταία να αποτελεί και την πλέον σημαντική στις σχετικά υψηλές συχνότητες.

Η χωρητική σύζευξη χρησιμοποιεί το ηλεκτρικό πεδίο και περιορίζεται σε ένα σχετικά μικρό ρυθμό μεταφοράς δεδομένων, για τον λόγο αυτό και είναι μάλλον μη ενδιαφέρουσα στην πράξη.

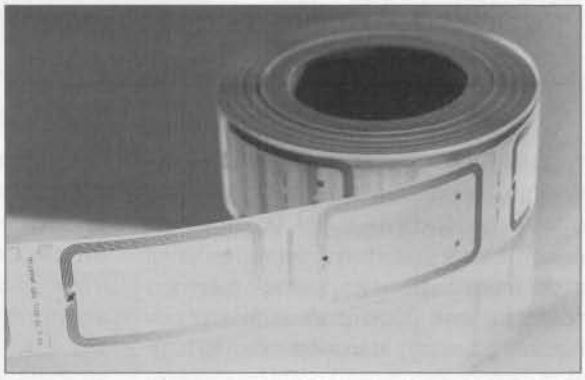
Η επαγωγική σύζευξη χρησιμοποιεί για την μεταφορά δεδομένων και ενέργειας ένα μαγνητικό πεδίο, όπου ένα πηνίο έχει τον ρόλο της κεραίας (Σχήμα 1). Στην κατηγορία αυτή, ευρείας χρήσης τυγχάνουν τα συστήματα που λειτουργούν στα 125 ή 135 kHz, όπως επίσης και στα 13,56 MHz. Η επιλογή των συγκεκριμένων συχνοτήτων δεν έχει να κάνει με την τεχνολογία αλλά βασίζεται στην εκάστοτε νομοθεσία και στις συχνότητες που είναι διαθέσιμες για εφαρμογές RFID. Οι εφαρμογές πάντως που χρησιμοποιούν επαγωγική σύζευξη είναι αρκετά διαδεδομένες.

Σε υψηλότερες συχνότητες όπως είναι τα 434 MHz, 862-956 MHz και 2,45 GHz, η σύζευξη παύει να είναι απλά επαγωγική ή χωρητική, διότι το μήκος κύματος είναι μικρό σε σχέση με το μέγεθος των εξαρτημάτων. Στις περιπτώσεις αυτές, για την μεταφορά ενέργειας και δεδομένων χρησιμοποιείται η διάδοση των ηλεκτρομαγνητικών πεδίων στον χώρο.



Σχήμα 1. Μία ετικέτα RFID με κεραία και ολοκληρωμένο.

Σχήμα 2. Ετικέτες σε ρολό. Το εσωτερικό στρώμα αποτελείται από ένα ολοκληρωμένο, το πηνίο της κεραίας και ένα υπόστρωμα (από χαρτί ή πλαστικό).



Σχήμα 3. Κατασκευή ετικετών RFID. Εάν παρατηρήσει κανείς στο βάθος πίσω από το ρολό, θα προσέξει μέσα από το βασικό στρώμα την γυαλάδα των πηνίων των κεραιών.

Σήμανση

Υπάρχει μία σημαντική διαφοροποίηση μεταξύ των εφαρμογών που έχουν να κάνουν με αντικείμενα και αυτών που έχουν να κάνουν με άτομα.

Στην πρώτη περίπτωση η κάρτα έχει την μορφή μίας ετικέτας που προσαρμόζεται επάνω στο αντικείμενο (δείτε τα Σχήματα 2 και 3). Οι συγκεκριμένες κάρτες που τοποθετούνται στα προϊόντα, καλούνται συχνά και ως "ετικέτες" RFID.

Όσοι ασχολούνται με την διαχείριση παραγγελιών θέλουν πολλές φορές να

Συχνότητες για ετικέτες RFID

	100-150kHz	13.56MHz	UHF	2.45GHz
Επίδραση του νερού και της υγρασίας	Χαμηλή	Χαμηλή	Υψηλή	Πολύ υψηλή
Επίδραση των μετάλλων	Χαμηλή	Υψηλή	Υψηλή*	Υψηλή*
Σχέδιο ανταποκριτή	Απλό	Απλό	Σύνθετο	Πολύ σύνθετο
Ακτίνα ανίχνευσης	Μικρό	Μεσαίο	Μεγάλο	Μεγάλο
Αριθμός αναγνωστών ανά δευτερόλεπτο	Μικρό	Μεγάλο	Μεγάλο	Μεγάλο

* Είναι δυνατό να μειωθεί με κατάλληλη σχεδίαση της ετικέτας

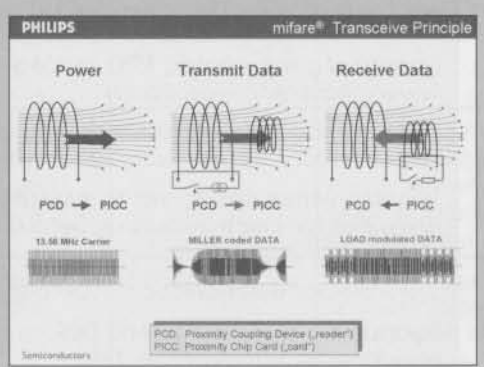
Ενδιάμεσο χωρίς επαφή, όπως καθορίζεται από το ISO/IEC 14443

Αναλογικό μέρος

Η τεχνολογία της Mifare χρησιμοποιεί ένα ενδιάμεσο χωρίς επαφές η οποία είναι συμβατή με το πρότυπο ISO/IEC 14443. Για την μεταφορά της ενέργειας και των δεδομένων μεταξύ της κάρτας και του αναγνώστη, χρησιμοποιείται ένα φέρον στα 13,56 MHz. Η ακτίνα ανάγνωσης-εγγραφής περιορίζεται σε μία απόσταση μικρότερη από 10 cm.

Όπως φαίνεται και από το Σχήμα η λειτουργία χωρίς επαφές, είναι δυνατόν να ερμηνευτεί με απλούς όρους εάν χρησιμοποιήσουμε την αρχή λειτουργίας του μετασχηματιστή. Το πηνίο κεραίας του αναγνώστη παράγει ένα εναλλασσόμενο μαγνητικό πεδίο στα 13,56 MHz. Πιο απλά, η κεραία του αναγνώστη μπορεί να θεωρηθεί ως το πρωτεύον τύλιγμα ενός μετασχηματιστή με χαλαρή ζεύξη. Το πηνίο της κάρτας αποτελεί το δευτερεύον τύλιγμα το οποίο εισέρχεται σε ένα μέρος του παραγόμενου μαγνητικού πεδίου. Με τον τρόπο αυτό το ολοκληρωμένο της κάρτας μπορεί να λάβει την απαιτούμενη για την λειτουργία του ενέργεια. (Οι όροι "PCD" και "PICC" που χρησιμοποιούνται στο σχήμα, προέρχονται από το πρότυπο ISO και ερμηνεύονται στο γλωσσάρι).

Το παραγόμενο από τον αναγνώστη μαγνητικό πεδίο είναι διαμορφωμένο κατά πλάτος και μεταφέρει δεδομένα από αυτόν προς την κάρτα μέσω μίας κωδικοποιημένης ακολουθίας σύμφωνα με τον κώδικα Miller και με 100% ψηφιακή διαμόρφωση σύμφωνα με το πρότυπο ISO/IEC 14443A. Για την μεταφορά δεδομένων στην αντίθετη κατεύθυνση (από την κάρτα δηλ. προς τον αναγνώστη), χρησιμοποιείται διαμόρφωση φορτίου. Αυτό σημαίνει ότι η κάρτα χρησιμοποιεί το διαμορφωμένο σήμα δεδομένων για να μεταγει εντός ή εκτός ένα φορτίο. Οι διακυμάνσεις φορτίου στο "δευτερεύον" τύλιγμα του μετασχηματιστή γίνονται αντιληπτές από τον αναγνώστη στην πλευρά του "πρωτεύοντος".



Ο ρυθμός μεταφοράς δεδομένων και προς τις δύο κατευθύνσεις είναι 106 kbit/s (ενώ προαιρετικά μπορεί να φθάσει μέχρι τα 847,5 kbit/s). Η ενέργεια που παρέχεται από τον αναγνώστη, είναι αρκετή για να λειτουργήσει κανονικά ο μικροελεγκτής.

Δεδομένου ότι εκ των πραγμάτων είναι αδύνατο να γνωρίζει το σύστημα εκ των προτέρων εάν εντός της περιοχής ανίχνευσης του αναγνώστη υπάρχουν περισσότερες της μίας κάρτες, πριν ξεκινήσει οποιαδήποτε ανταλλαγή δεδομένων θα πρέπει να προηγείται μία διαδικασία ταυτοποίησης για να εξασφαλίζεται με τον τρόπο αυτό ότι η επικοινωνία γίνεται με μία μόνον κάρτα (προστασία σύγκρουσης).

Ψηφιακό μέρος

Η μεταφορά δεδομένων (συμπεριλαμβανομένων των δεδομένων χρήσης), ξεκινά μετά της επιλογή της κάρτας. Στην διαδικασία αυτή ισχύουν οι παρακάτω κανόνες:

- Ο αναγνώστης "μιλά" πάντα πρώτος: πρώτα εκπέμπει ο πομποδέκτης και στην συνέχεια απαντά η κάρτα.
- Η κάρτα απαντά πάντοτε εντός κάποιου προκαθορισμένου χρόνου, ενώ ο πομποδέκτης δεν έχει κανένα περιορισμό.

Στην απλούστερη περίπτωση (όπως για παράδειγμα η κάρτα Ultralight της Mifare που χρησιμοποιούμε στην κατασκευή RFID), αυτό επιτυγχάνεται με άμεση χρήση των κατάλληλων εντολών της κάρτας (Read και Write στην περίπτωση της κάρτας Ultralight της Mifare).

Αυτό σημαίνει ότι υπάρχει ένα απλό και ξεκάθαρο πρωτόκολλο, και τα οποιαδήποτε σφάλματα οδηγούν σε διακοπή της επικοινωνίας. Κάτι τέτοιο βέβαια δεν είναι εφικτό για σχετικά σύνθετες εφαρμογές, οπότε υπάρχει και ένα πιο ευέλικτο πρωτόκολλο εκπομπής για έξυπνες κάρτες με μικροελεγκτή.

Το συγκεκριμένο πρωτόκολλο καθορίζεται στο Τέταρτο Μέρος του προτύπου ISO/IEC 14443 και:

- επιτρέπει διαφορετικά μεγέθη πακέτων δεδομένων (ανάλογα με το μέγεθος ενδιάμεσης μνήμης στον αναγνώστη ή την κάρτα).
- καθορίζει μία διαδικασία διαχείρισης σφαλμάτων (ανίχνευση και διόρθωση σφαλμάτων).
- επιτρέπει την σύνδεση ομάδων δεδομένων με σκοπό την μεταφορά σχετικά μεγάλου όγκου δεδομένων.
- υποστηρίζει ευέλικτο χρονισμό (το οποίον σημαίνει ότι η κάρτα μπορεί να ζητήσει περισσότερο χρόνο για την εκτέλεση μίας εντολής.

γνωρίζουν το πότε κάποιο προϊόν βρίσκεται σε μία συγκεκριμένη θέση. Με την βοήθεια των ετικετών RFID, είναι δυνατόν να έχουν μία αυτόματη ενημέρωση σχετικά με την παράδοση προϊόντων που βρίσκονται σε παλέτες ή σε κιβώτια. Η συγκεκριμένη διαδικασία διευκολύνει την απογραφή, συντελεί στην αποφυγή των κλοπών, ενώ επίσης βοηθάει στον διαχωρισμό των γνήσιων προϊόντων από τα πλαστά.

Στις συγκεκριμένες εφαρμογές, μεγάλη σημασία έχει η μέγιστη δυνατή απόσταση ανίχνευσης καθώς και η ευκολία στην χρήση των συστημάτων. Δεν χρειάζεται σημαντική υπολογιστική διεργασία επί των ετικετών RFID ή διαχείριση μεγάλου όγκου δεδομένων, αλλά όμως απαιτείται η ανάγνωση ενός μεγάλου πλήθους ετικετών σχεδόν ταυτόχρονα. Η ανάγνωση μερικών εκατοντάδων ή ακόμη και χιλιάδων ετικετών σε μία απόσταση μερικών δεκάδων εκατοστών ή μερικών μέτρων (μπορεί να φθάσει και τα 5 μέτρα), μπορεί να γίνει με σχετική ευκολία.

Ο τεράστιος όγκος των ετικετών αντισταθμίζεται από μικρούς όγκους δεδομένων (μερικές ψηφιολέξεις) και ένα ρυθμό μεταφοράς δεδομένων της τάξης των kb/s. Η πληροφορία που φέρει η ετικέτα είναι συνήθως ένας αριθμός, ο οποίος σε μία βάση δεδομένων χαρακτηρίζει κάποιο συγκεκριμένο προϊόν. Σε πολλές περιπτώσεις η πρόσβαση στην βάση δεδομένων γίνεται μέσω του διαδικτύου, το οποίον σημαίνει ότι το σύστημα μπορεί εύκολα να λειτουργήσει από το Πεκίνο μέχρι το Σαν Φρανσίσκο.

Το νέο πρότυπο Ηλεκτρονικής Κωδικοποίησης Προϊόντων (Electronic Product Code [EPC]) εξασφαλίζει μοναδικούς κωδικούς αριθμούς προϊόντων σε διεθνές επίπεδο, λειτουργώντας κατά κάποιο τρόπο σαν ηλεκτρονικός γραμμικός κώδικας (barcode).

Έξυπνες κάρτες

Οι "προσωπικές" κάρτες επιβάλλουν κάποιες διαφορετικές τεχνικές απαιτήσεις. Στην συγκεκριμένη περίπτωση αντί για "ετικέτες" αναφέρονται ως "έξυπνες κάρτες". Σε μία έξυπνη κάρτα, ο χρήστης θα πρέπει να ξεκινήσει ενεργά μία διαδικασία εγγραφής-ανάγνωσης φέροντας την κάρτα κοντά στον πομποδέκτη.

Στην συγκεκριμένη περίπτωση, η μεγάλη ακτίνα λειτουργίας όχι μόνον δεν είναι απαραίτητη, αλλά επί της ουσίας είναι ανεπιθύμητη. Η μη εξουσιοδοτη-

Αποτροπή Αναπαραγωγής

Μία τυπική εφαρμογή των έξυπνων καρτών χωρίς επαφές είναι τα συστήματα ελέγχου πρόσβασης, όπως για παράδειγμα αυτά που χρησιμοποιούν διάφορες εταιρείες. Ο κάθε υπάλληλος που έχει δικαίωμα πρόσβασης σε κάποιο ελεγχόμενο χώρο φέρει μία κονκάρδα η οποία περιέχει μία έξυπνη κάρτα. Πριν ο υπάλληλος εισέλθει στην ελεγχόμενη περιοχή, φέρει την κάρτα μπροστά στον αναγνώστη, ο οποίος αφού αναγνωρίσει τα δεδομένα απελευθερώνει την είσοδο.
Τα δεδομένα μεταξύ τη κάρτας και του αναγνώστη εκπέμπονται σε κωδικοποιημένη μορφή. Σε κάθε όμως διέλευση υπάρχει και ένα διαφορετικό "κλειδί" το οποίο αποτρέπει την δυνατότητα απλής καταγραφής των εκπεμπόμενων δεδομένων και αναπαραγωγής τους με σκοπό να παραβιαστεί η είσοδος (παραβίαση μέσω αναπαραγωγής).
Στην μέθοδο "αμοιβαίας αναγνώρισης τριών βημάτων", επιβεβαιώνεται η ορθότητα του μυστικού κλειδιού για να δημιουργηθεί στην συνέχεια ένα κλειδί διέλευσης. Το σύστημα λειτουργεί ως εξής:

1) Η κάρτα παράγει ένα τυχαίο αριθμό RndB, ο οποίος κρυπτογραφείται με την βοήθεια του μυστικού κλειδιού και αποστέλλεται προς τον αναγνώστη.
2) Στην περίπτωση όπου ο αναγνώστης χρησιμοποιεί το ίδιο μυστικό κλειδί, η αποκρυπτογράφηση σε αυτόν δημιουργεί τον ίδιο τυχαίο αριθμό RndB. Ο αποκρυπτογραφημένος αριθμός RndB αναδομείται για να σχηματίσει τον RndB*. Στην συνέχεια ο RndB* μαζί με ένα RndA κρυπτογραφούνται και αποστέλλονται προς την κάρτα.
3) Η κάρτα ανακτά τους δύο τυχαίους αριθμούς μέσω αποκρυπτογράφησης και αναστρέφει την αναδόμηση του RndB. Εάν το αποτέλεσμα είναι το ίδιο με τον τυχαίο αριθμό που είχε αρχικά δημιουργήσει η κάρτα, τα κλειδιά που χρησιμοποιούν η κάρτα και ο αναγνώστης πρέπει να είναι τα ίδια. Στην συνέχεια η κάρτα αναδομεί τον RndA για να δημιουργήσει τον RndA*, τον οποίο στέλνει πίσω στον αναγνώστη.
4) Ο αναγνώστης τώρα είναι σε θέση να αποκρυπτογραφήσει τον RndA* και να τον μετατρέψει στον RndA, για να διαπιστώσει την ορθότητα του κλειδιού που χρησιμοποίησε η κάρτα. Εάν και η τελευταία αυτή δοκιμή είναι επιτυχής, ο αναγνώστης είναι σε θέση να γνωρίζει ότι και η κάρτα είναι γνήσια.

Μετά λοιπόν από την παραπάνω διαδικασία εξακρίβωσης, και τα δύο μέρη είναι σε θέση να γνωρίζουν ότι χρησιμοποιούν το ίδιο κλειδί, έστω και εάν το κλειδί ποτέ δεν εκπέμφθηκε από κανένα. Από τους τυχαίους αριθμούς μπορεί να δημιουργηθεί πλέον ένα προσωρινό κλειδί επικοινωνίας, το οποίο θα είναι γνωστό μόνον στον αναγνώστη και την κάρτα αφού μεταδόθηκε σε κρυπτογραφημένη μορφή. Το συγκεκριμένο κλειδί επικοινωνίας θα χρησιμοποιηθεί στην συνέχεια για την κρυπτογράφηση των δεδομένων που θα ανταλλάξουν οι δύο μονάδες στην εξέλιξη της επικοινωνίας τους. Το πλεονέκτημα του εν λόγω κλειδιού είναι ότι βασίζεται σε τυχαίους αριθμούς, το οποίο σημαίνει ότι για κάθε επικοινωνία χρησιμοποιείται ένα νέο κλειδί. Η διαδικασία αυτή παρέχει μία αποτελεσματική προστασία έναντι των παραβιάσεων αναπαραγωγής.

Διευθύνσεις στο διαδίκτυο

Εφαρμογές της κάρτας RFID σε όλο τον κόσμο:
www.mifare.net/news/#press

Εισιτήριο του Παγκοσμίου Κυπέλλου με ολοκληρωμένα RFID:
www.elektor-electronics.co.uk/Default.aspx?tabid=27&art=53048&PN=On

Τεχνικές λεπτομέρειες για τα ηλεκτρονικά διαβατήρια:
www.elektor-electronics.co.uk/Default.aspx?tabid=27&art=53049&PN=On

Ιοί RFID:
www.elektor-electronics.co.uk/Default.aspx?tabid=27&art=53050&PN=On

Εφαρμογές των DES Τριπλού DES:
en.wikipedia.org/wiki/Triple_Des

Σχήμα 4. Τα πλεονέκτημα της τεχνολογίας RFID αναδεικνύονται στην περίπτωση των αναλώσιμων προϊόντων, όπου επιταχύνονται οι διαδικασίες μεταφοράς.

μένη ανάγνωση της κάρτας μπορεί να αποτραπεί από το στάδιο της σχεδίασης, περιορίζοντας κατά το δυνατόν την ακτίνα ανίχνευσης της κάρτας. Το πρότυπο που περιγράφει το ενδιάμεσο για τις έξυπνες κάρτες χωρίς επαφές (ISO/IEC 14443), καθορίζει τις τεχνικές παραμέτρους έτσι ώστε η μέγιστη δυνατή ακτίνα ανίχνευσης να περιορίζεται στα 10 cm (δείτε το ένθετο άρθρο).

Στις κάρτες όμως αυτές, ενδέχεται να απαιτείται η ανταλλαγή μεγάλου όγκου δεδομένων (μέχρι και αρκετά Kb), οπότε επιβάλλεται και η αντίστοιχη ασφάλεια κατά την ανταλλαγή των δεδομένων. Το ενδιάμεσο χωρίς επαφές είναι σχεδιασμένο με τέτοιο τρόπο, ώστε να παρέχεται ενέργεια στους μικροελεγκτές που είναι ενσωματωμένοι στις έξυπνες κάρτες και να επιτυγχάνεται η μεταφορά μεγάλου όγκου δεδομένων με ρυθμούς μεταφοράς που φθάνουν μέχρι τις εκατοντάδες KB/s.

Παραδείγματα ανάλογων εφαρμογών είναι το νέο ηλεκτρονικό διαβατήριο (δείτε τους συνδέσμους στο διαδίκτυο) και τα ηλεκτρονικά εισιτήρια για τα τοπικά μέσα μαζικής μεταφοράς, όπως είναι το σύστημα Oyster στον υπόγειο του Λονδίνου).

Ποια συχνότητα για τι;

Οι έξυπνες κάρτες χωρίς επαφές λειτουργούν γενικά στα 13,56 MHz και συμφωνούν με το πρότυπο ISO/IEC 14443 (δείτε το ένθετο άρθρο). Η τεχνολογία Mifare που περιγράφεται στην κατασκευή αναγνώστη RFID σε άλλο σημείο του περιοδικού, είναι η πλέον συνήθης τεχνολογία που χρησιμοποιείται για εφαρμογές έξυπνων καρτών RFID σε παγκόσμια κλίμακα.

Η επιλογή της κατάλληλης συχνότητας είναι αρκετά σύνθετη διαδικασία. Όπως φαίνεται και από τον πίνακα, στις διάφορες συχνότητες υπάρχουν διαφορετικοί παράγοντες οι οποίοι εμπλέκονται. Στις χαμηλές συχνότητες η επίδραση του νερού είναι αμελητέα, αλλά αυξάνει σημαντικά στις υψηλότερες συχνότητες. Δεδομένου ότι για παράδειγμα στα 2,5 GHz το νερό απορροφά σημαντικά ποσά ενέργειας, για συστήματα τα οποία αναμένεται να λειτουργήσουν σε συνθήκες υψηλής σχετικής υγρασίας, είναι καλύτερα να επιλέξουμε την συχνότητα των 135 KHz.

Σε ένα μεταλλικό περιβάλλον όπως είναι οι ετικέτες RFID για μεταλλικά βαρέλια μπύρας, είναι προτιμότερη η χρήση μίας χαμηλής συχνότητας, ή η σχεδίαση μίας ετικέτας στα UHF με την κατάλληλη όμως κεραία. Η σχεδίαση της κεραίας για ετικέτες που χρησιμοποιούν επαγωγική σύζευξη είναι ευκολότερη

Γλωσσάρι RFID			
Tagging	Η ανίχνευση ετικετών (συμπεριλαμβανομένων ετικετών RFID)	UHF	Υπέρ Υψηλές Συχνότητες (Ultra High Frequency): στην συγκεκριμένη περίπτωση συχνότητες στην περιοχή 862-956 kHz.
ISO	Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization)	Eavesdropping	Ανεπιθύμητη υποκοπή επικοινωνιών RFID.
IEC	Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission)	Skimming	Ανεπιθύμητη χρήση ετικετών RFID ή έξυπνων καρτών χωρίς επαφές
ISO/IEC 14443	Διεθνές Πρότυπο για την διεπαφή χωρίς επαφές έξυπνων καρτών, με μέγιστη ακτίνα ανίχνευσης 10 cm και συχνότητα στα 13,56 MHz.	Παραβίαση μέσω αναπαραγωγής	Μη εξουσιοδοτημένη συναλλαγή δημιουργούμενη από την αναπαραγωγή προηγούμενης εκπομπής η οποία κατεγράφη μέσω "eavesdropping"
PCD	Συσκευή Ζεύξης με Προσέγγιση (Proximity Coupling Device): ένας πομποδέκτης για έξυπνες κάρτες χωρίς επαφές (συμβατός με το πρότυπο ISO/IEC 14443)	Τροποποιημένη κωδικοποίηση Miller	Κωδικοποίηση κατά θέση παλμού, στην οποία συγκεκριμένοι παλμοί έχουν παραληφθεί για εξοικονόμηση ενέργειας
PICC	Κάρτα προσέγγισης με ολοκληρωμένο (Proximity Chip Card): μία έξυπνη κάρτα χωρίς επαφές (συμβατή με το πρότυπο ISO/IEC 14443)	DES	Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard): μία συμμετρική μέθοδος κρυπτογράφησης για πακέτα δεδομένων 8 ψηφιολέξεων με μήκος κλειδιού 56 ψηφία (8 ψηφιολέξεις χωρίς ψηφία ισοτιμίας). Δείτε τον σύνδεσμο στο διαδίκτυο.
ISO/IEC 15693	Διεθνές Πρότυπο για την διεπαφή χωρίς επαφές ετικετών, με μέγιστη ακτίνα ανίχνευσης 1,5 m και συχνότητα στα 13,56 MHz.	3-DES,	Μία τυποποιημένη μέθοδος κρυπτογράφησης αποτελούμενη από τρεις βρόγχους DES με σκοπό την αυξημένη ασφάλεια. Εδώ το κλειδί είναι 112 ή 168 ψηφία. Δείτε τον σύνδεσμο στο διαδίκτυο.

σε σχέση με αυτή των ετικετών υψηλών συχνοτήτων. Από την άλλη, οι ετικέτες UHF παρουσιάζουν μεγαλύτερη ακτίνα ανίχνευσης, η οποία μπορεί να περιοριστεί ουσιαστικά μόνον μέσω θωράκισης. Εννοείται βέβαια ότι το πλήθος των ετικετών που μπορούν να αναγνωστούν το δευτερόλεπτο είναι μεγαλύτερο για ετικέτες που λειτουργούν σε υψηλές συχνότητες, λόγω του μεγαλύτερου διαθέσιμου εύρους ζώνης.

Ασφάλεια

Πριν ένα σύστημα δοθεί σε λειτουργία, θα πρέπει να έχουν μελετηθεί με προσοχή η ασφάλεια του ίδιου του συστήματος αλλά και των δεδομένων. Οι απαιτήσεις βέβαια εξαρτώνται και από την φύση της εφαρμογής. Σε ένα σύστημα για παράδειγμα που χρησιμοποιεί ετικέτες RFID επάνω σε αντικείμενα, οι οποίες ετικέτες στην απλούστερη περίπτωση αντικαθιστούν τον γραμμικό κώδικα, αρκεί η ασφάλεια που προβλέπεται για τους γραμμικούς κώδικες (αλλά σίγουρα όχι λιγότερη!). Τα δεδομένα αποθηκεύονται σύμφωνα με κάποιο πρότυπο και είναι δυνατόν να διαθέτουν και προστασία κατά της εγγραφής.

Παρ' όλα αυτά βέβαια, οποιοσδήποτε έχει πρόσβαση στην ετικέτα είναι σε θέση να διαβάσει ή να αντιγράψει τα αποθηκευμένα δεδομένα, όπως ακριβώς συμβαίνει και με τον γραμμικό κώδικα. Σε αντίθεση όμως με τα συστήματα γραμμικού κώδικα, η ασφάλεια και λειτουργικότητα των συστημάτων RFID είναι πολύ εύκολο να επεκταθεί. Το πρώτο βήμα αφορά την προστασία έναντι αντιγραφής των δεδομένων. Ένας τρόπος για να επιτευχθεί αυτό είναι να αποδοθεί σε κάθε ετικέτα RFID ένας μοναδικός αριθμός ταυτοποίησης (unique identification number [UID]). Ο συγκεκριμένος αριθμός UID αποθηκεύεται από τον κατασκευαστή του ολοκληρωμένου στην μνήμη της ετικέτας RFID χωρίς δυνατότητα τροποποίησης, παρέχοντας με τον τρόπο αυτό μία βασική προστασία έναντι αντιγραφής.

Μυστικά κλειδιά

Το επόμενο βήμα είναι η χρήση μίας παρόμοιας μεθόδου για την προστασία κάποιας εγγράψιμης (ή επαν-εγγράψιμης) περιοχής μνήμης από κακόβουλη χρήση.

Εδώ ο αριθμός UID χρησιμοποιείται για την δημιουργία ενός μυστικού κλειδιού που είναι ξεχωριστό για κάθε ολοκληρωμένο, και το οποίο εξυπηρετεί στην κρυπτογράφηση των δεδομένων. Για να μπορέσει να διαβάσει ο χρήστης τα δεδομένα που είναι αποθηκευμένα σε μία τέτοια ετικέτα χρειάζεται απαραιτήτως τα ακόλουθα:

- τον αριθμό UID
- ένα μυστικό κλειδί
- γνώση της χρησιμοποιούμενης μεθόδου κρυπτογράφησης

Άλλες μέθοδοι προστασίας των δεδομένων περιλαμβάνουν την χρήση κωδικών λέξεων (password) και αποκλειστικές διαδικασίες κρυπτογράφησης των δεδομένων της ετικέτας αλλά και των εκπεμπόμενων δεδομένων. Παρότι σε τεχνικό επίπεδο υπάρχουν πολύ πιο σύνθετες διαδικασίες προστασίας, συνήθως δεν χρησιμοποιούνται σε απλά συστήματα για να μην ανέβει πολύ το κόστος.

Ασφαλή δεδομένα

Οι έξυπνες κάρτες απαιτούν κατά κανόνα σχετικά υψηλή στάθμη ασφάλειας διότι σε αυτές αποθηκεύονται σημαντικά προσωπικά (όπως το διαβατήριο) ή οικονομικά (όπως οι τραπεζικές κάρτες) δεδομένα. Τα επίπεδα ασφάλειας που είναι δυνατόν να επιτευχθούν, είναι τα ίδια τόσο στις έξυπνες κάρτες χωρίς επαφές, όσο και αυτές με επαφές.

Το πρώτο βέβαια βήμα αφορά την προστασία των εκπεμπόμενων δεδομένων. Για τον σκοπό αυτό υπάρχουν διάφορα πρότυπα, όπου ο βαθμός ασφαλείας εξαρτάται από το μήκος του κλειδιού.

Με απλά λόγια, το μήκος του κλειδιού αντιστοιχεί στο στατιστικό πλήθος ανεπιτυχών δοκιμών εντοπισμού ενός μυστικού κλειδιού. Στην περίπτωση του αλγορίθμου DES όπου το κλειδί έχεις μήκος οκτώ ψηφιολέξεις και για το κλείδωμα χρησιμοποιούνται μόνον 56 ψηφία, το μοναδικό κλειδί αποτελεί ένα από τα 72.000.000 δισεκατομμύριο πιθανά κλειδιά.

Ο παραπάνω αριθμός μπορεί να ακούγεται πολύ μεγάλος, αλλά στην εποχή των δικτυωμένων υπολογιστικών συστημάτων υπάρχουν πολλές εφαρμογές για τις οποίες η παρεχόμενη ασφάλεια δεν θεωρείται επαρκής. Οι εναλλακτικές λύσεις είναι να χρησιμοποιηθεί μεγαλύτερο κλειδί όπως στα 112 ψηφία με τριπλό DES, ή να επιλεγεί κάποια διαφορετική μέθοδος κρυπτογράφησης.

Και στην περίπτωση αυτή, το κόστος λειτουργεί εις βάρος της ασφάλειας, και για τον λόγο αυτό υπάρχουν πολλές διαφορετικές απόψεις. Η ασφάλεια βέβαια ενός συστήματος αποτελεί την συνισταμένη πολλών παραμέτρων, και στο σύνολό της εξαρτάται από τον πλέον αδύναμο κρίκο του συστήματος. Δεν έχει λοιπόν τόσο μεγάλη σημασία η αυξημένη κρυπτογράφηση των δεδομένων που είναι αποθηκευμένα στην κάρτα, εάν υπάρχει δυνατότητα υποκλοπής κάποιας επικοινωνίας και εξομοίωσης αυτής στην συνέχεια. Υπάρχουν βέβαια κάποιες αποτελεσματικές μέθοδοι προστασίας από αυτόν ή άλλους παρόμοιους κινδύνους (δείτε το ένθετο "Αποτροπή Αναπαραγωγής"). Οι υποκλοπές ειδικά σε ασύρματες ζεύξεις πάντα θα υπάρχουν. Όσο για τα ασφαλή διαβατήρια κάποιος πριν λίγες ημέρες απέδειξε ότι είναι εύκολο να υποκλέψεις τα δεδομένα. Μια κάποια ασφάλεια δίνει η θήκη που περιέχει σαν περίβλημα αλουμίνιο ή άλλο μεταλικό φύλλο.

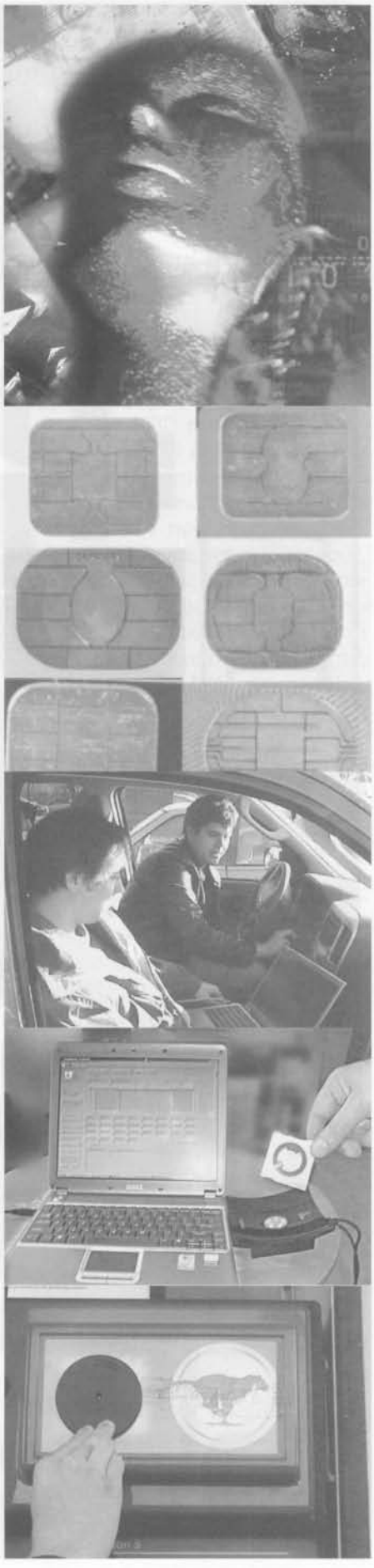
(060204-1)

RFID και ασφάλεια

Οι ιοί απειλούν τις ετικέτες RFID

Από τον Paul Goossens

Οι ετικέτες RFID έχουν αρχίσει να χρησιμοποιούνται σε ένα διαρκώς αυξανόμενο πεδίο εφαρμογών. Τις εντοπίζουμε για παράδειγμα στα συστήματα πληρωμής των δημόσιων μέσων μεταφοράς πολλών Ευρωπαϊκών πόλεων, σε βιβλιοθήκες κ.λ.π. Στο άρθρο που ακολουθεί θα εξετάσουμε ορισμένα ζητήματα ασφάλειας και προστασίας προσωπικού απορρήτου, που ανακύπτουν από την χρήση των ετικετών αυτών.



Μία ετικέτα RFID αποτελεί συνδυασμό ενός ολοκληρωμένου και μίας μικρής κεραίας. Μόλις μία τέτοια ετικέτα βρεθεί στην περιοχή μιας συσκευής ανάγνωσης, το ολοκληρωμένο RFID λαμβάνει ισχύ από την ενέργεια που εκπέμπει η συσκευή, και στην συνέχεια αυτή και το ολοκληρωμένο αρχίζουν μία αμφίδρομη επικοινωνία μέσω ραδιο-κυμάτων.

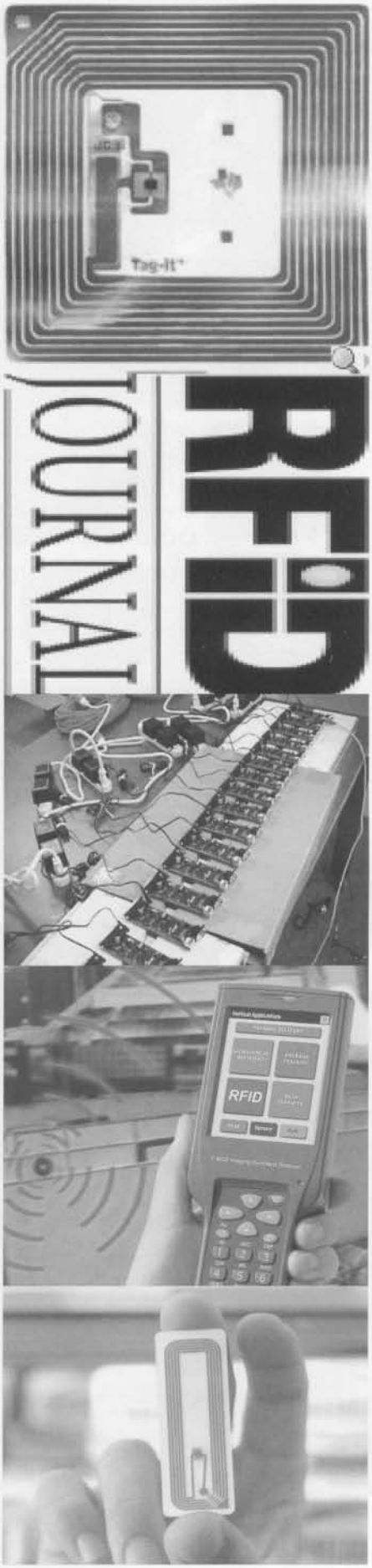
Οι ετικέτες RFID μπορούν να χρησιμοποιηθούν σε πολλές και διαφορετικές εφαρμογές, κυρίως λόγω του πλεονεκτήματος ότι αποτελούν ασύρματες μονάδες. Μία ετικέτα μπορεί να επικοινωνήσει με την συσκευή ανάγνωσης, χωρίς καν να έχει οπτική επαφή με αυτόν. Το γεγονός βέβαια αυτό δημιουργεί και κάποια μειονεκτήματα. Οι χρήστες των ετικετών RFID δεν αντιλαμβάνονται το γεγονός ότι η κάρτα που κατέχουν ανταλλάσσει δεδομένα, όπως επίσης δεν πρόκειται να αντιληφθούν εάν κάποιος τρίτος υποκλέπτει μία κανονική ανταλλαγή δεδομένων της κάρτας του.

Τα μειονεκτήματα

Ας φανταστούμε ότι ψωνίζουμε στο super-market και μέσα στο καρότσι μας έχουμε και ένα λαχταριστό κομμάτι βοδινού (το οποίο διαθέτει την δική του κάρτα RFID). Περνώντας από τον διάδρομο με τα κρασιά, το καρότσι μας (το οποίο διαθέτει συσκευή ανάγνωσης RFID) μας ενημερώνει για το ποια κρασιά ταιριάζουν με το κρέας που έχουμε διαλέξει. Ένα όμορφο, ανώδυνο και "high-tec" σενάριο. Δυστυχώς όμως υπάρχουν και πολλές άλλες περιπτώσεις όπου το έργο δεν εξελίσσεται τόσο ανώδυνα. Ας υποθέσουμε λοιπόν ότι κάποιος μπορεί να διαβάσει και να αντιγράψει τις πληροφορίες που είναι αποθηκευμένες στο διαβατήριο μας χωρίς εμείς να το γνωρίζουμε, ή να γεμίσει το δικό του αυτοκίνητο με βενζίνα την οποία χρεώνει στον δικό μας λογαριασμό. Σε τέτοιες περιπτώσεις, είναι σίγουρο ότι δεν επιθυμούμε εν αγνοία μας να πέσουμε θύματα κακόβουλων ατόμων ή εταιρειών.

Αυτή τη στιγμή υπάρχουν διάφορες ομάδες οι οποίες ασχολούνται με τους κινδύνους χρήσης των ετικετών RFID, κάνοντας πλήθος δημοσιεύσεων σχετικά με την προσοχή που θα πρέπει να δοθεί στην χρήση της συγκεκριμένης τεχνολογίας και της ασφάλειας που θα πρέπει να εξασφαλίσουν οι διάφοροι κατασκευαστές και οργανισμοί.

Μία ομάδα Αμερικάνων φοιτητών για παράδειγμα παραβίασε το σύστημα RFID της "Exxon Mobile Speed Pass", το οποίο χρησιμοποιείται στα συστήματα πληρωμής καυσίμων στα βενζινάδικα της Αμερικής που φέρουν το εμπορικό σήμα της Exxon. Οι ετικέτες RFID του συγκεκριμένου συστήματος είναι εξοπλισμένες με ένα κρυπτογραφικό σύστημα, το οποίο όμως δεν ήταν αρκετό για να εμποδίσει του φοιτητές να πραγματοποιήσουν μία αγορά χρησιμοποιώντας μία ιδιο-κατασκευασμένη ετικέτα RFID, αντίγραφο μίας κανονικής ετικέτας. Η διαδικασία υποκλοπής είχε ως εξής: μία συσκευή (ιδιο-κατασκευή και αυτή) υπέκλεπτε την επικοινωνία μεταξύ της κανονικής κάρτας RFID και της αντίστοιχης συσκευής ανάγνωσης από απόσταση, χωρίς αυτό να γίνεται



αντιληπτό. Στην συνέχεια ανάλυσαν τα δεδομένα της επικοινωνίας, κατάφεραν να σπάσουν την προστασία και δημιούργησαν ένα αντίγραφο της κανονικής κάρτας RFID. Για να βεβαιωθούν για την λειτουργία της κάρτας-αντιγράφου γέμισαν το αυτοκίνητο με βενζίνη και χωρίς κανένα πρόβλημα πλήρωσαν με την κάρτα αυτή. Η αρχική βέβαια κάρτα RFID της οποίας δημιούργησαν αντίγραφο ανήκε σε ένα μέλος της ομάδας, οπότε δεν υπήρχε περίπτωση να κατηγορηθούν για εγκληματική ενέργεια.

Μετά από αυτό το συμβάν, δημιουργήθηκε και ο πρώτος ιός RFID από ένα μέλος μίας ερευνητικής ομάδας στο Ελεύθερο Πανεπιστήμιο του Άμστερνταμ. Ο ιός γράφτηκε για ένα δικό τους σύστημα RFID το οποίο δεν κυκλοφορεί στο εμπόριο, αλλά ούτως ή άλλως αποδεικνύεται ξεκάθαρα ότι η τεχνολογία RFID χρειάζεται μεγάλη προσοχή.

Η Melanie Rieback

Το άτομο το οποίο δημιούργησε τον ιό ήταν η Melanie Rieback, η οποία προχώρησε στην ενέργεια αυτή για προκαλέσει ένα θόρυβο σχετικά με την ασφάλεια των συστημάτων RFID. Κατά την άποψη της το θέμα της ασφάλειας και των προσωπικών δεδομένων δεν είναι μόνον πρόβλημα των καταναλωτών αλλά και των εταιρειών που χρησιμοποιούν την συγκεκριμένη τεχνολογία. Το πλήθος των άρθρων που έχουν δημοσιευτεί σχετικά με το εν λόγω ζήτημα, αποδεικνύει ότι σίγουρα πέτυχε τον σκοπό της. Αποτέλεσμα λοιπόν όλων αυτών ήταν αρκετές εταιρείες να προσεγγίσουν την Melanie για να της ζητήσουν να τις βοηθήσει στην βελτίωση του λογισμικού RFID που παράγουν. Δυστυχώς όμως, κάποιες άλλες εταιρείες που κινούνται στον χώρο του RFID αντιμετώπισαν αρνητικά την κίνηση της, την οποία μάλιστα χαρακτήρισαν εντελώς άστοχη.

Εκτός από την παραβίαση των συστημάτων της Exxon Mobile Speed Pass που αναφέραμε νωρίτερα, η Melanie δήλωσε ότι το νέο Ολλανδικό διαβατήριο δεν είναι εντελώς ασφαλές έναντι παραβιάσεων. Μία εταιρεία στο Ντελφτ ονομαζόμενη Riscure απέδειξε ότι η προτεινόμενη τεχνολογία RFID παρουσιάζει κενά ασφάλειας. Οι τεχνικοί λοιπόν της εν λόγω εταιρείας κατάφεραν να σπάσουν το κλειδί ενός τέτοιου διαβατηρίου μέσα σε λίγες ώρες, γεγονός το οποίο στην συνέχεια τους έδωσε την δυνατότητα να διαβάσουν την ημερομηνία γεννήσεως, την φωτογραφία του διαβατηρίου και τα δακτυλικά αποτυπώματα χωρίς να γίνουν αντιληπτοί. Απαντώντας στο συγκεκριμένο συμβάν το Ολλανδικό Υπουργείο Εσωτερικών ανακοίνωσε ότι θα προχωρήσει σε νέα μέτρα βελτίωσης της ασφάλειας των διαβατηρίων.

Το Ολλανδικό διαβατήριο βέβαια δεν είναι το μόνο που υποφέρει από προβλήματα ασφάλειας σχετιζόμενα με την ετικέτα RFID. Έντονες κριτικές έχει δεχτεί και το Αμερικάνικο διαβατήριο. Στο πρόσφατο συνέδριο Ελευθερίας και Ιδιωτικού απορρήτου από τους Υπολογιστές (Computer, Freedom and Privacy), ένα μέλος της Αμερικάνικης Ένωσης Ατομικών Ελευθεριών (American Civil Liberties Union) απέδειξε ότι το νέο Αμερικάνικο διαβατήριο μπορεί να αναγνωσθεί από απόσταση ενός μέτρου, την στιγμή που οι κατασκευαστές δήλωναν ότι η μέγιστη απόσταση ανάγνωσης είναι μερικά εκατοστά.

Ανησυχία

Έχοντας δεδομένα τα προαναφερθέντα παραδείγματα, η Melanie διερωτάται για το κατά πόσον οι εταιρείες του χώρου έχουν όντως λάβει σοβαρά υπ' όψη τις καταγγελίες τους. "Οι βιομηχανίες αυτοκινήτων υποβάλλουν σε εξαντλητικές δοκιμές τα αυτοκίνητά τους πριν τα παραδώσουν στην κυκλοφορία. Γατί να μην συμβαίνει το ίδιο και με τις τεχνολογίες που εκθέτουν σε απειλές το ιδιωτικό απόρρητο;" Πως είναι δυνατόν ο κόσμος να αποδεχτεί και να εμπιστευτεί κάποια νέα προϊόντα όταν αποδεικνύεται ότι δεν έχουν δοκιμαστεί αρκετά; Μέχρι στιγμής την τεχνολογία RFID την έχουν παραβιάσει ορισμένα ινστιτούτα ερευνών, αλλά ποιος μας εξασφαλίζει ότι κάποια κακόβουλα άτομα δεν πρόκειται να κάνουν το ίδιο; Μόλις κυκλοφορήσουν αρκετά συστήματα RFID, η έλευση της κανονικής δοκιμής αντοχής είναι απλά θέμα χρόνου : της δοκιμής στην πράξη. Δυστυχώς, τότε θα είναι αργά.

Ακόμη και τα ολοκληρωμένα RFID που χρησιμοποιούνται αντί του γραμμικού κώδικα, είναι δυνατόν να χρησιμοποιηθούν για την συλλογή πληροφοριών που σχετίζονται με το ιδιωτικό απόρρητο. Το κάθε ολοκληρωμένο RFID που περιλαμβάνει ένα σειριακό αριθμό μπορεί να χρησιμοποιηθεί για να ελέγξει το που πηγαίνει ο κόσμος, ποια είναι η αγοραστική του συμπεριφορά κ.ο.κ. Εδώ και αρκετά χρόνια, πολλοί οργανισμοί προειδοποιούν τους αρμόδιους για τα

ανεπιθύμητα αποτελέσματα των συστημάτων RFID. Η άποψη βέβαια της βιομηχανίας σχετικά με τις αναφορές αυτές, είναι ότι αποσκοπούν στην δημιουργία ενός γενικότερου κλίματος δυσπιστίας στην τεχνολογία RFID, την οποία η ίδια δεν θεωρεί ιδιαίτερα επικίνδυνη.

Λύσεις και φραγμοί

Ευτυχώς, υπάρχουν και κάποια μέσα αντιμετώπισης των συγκεκριμένων απειλών. Υπάρχουν για παράδειγμα συσκευές δημιουργίας παρεμβολών οι οποίες είναι σχεδιασμένες έτσι ώστε να παρεμβάλλονται στην επικοινωνία μεταξύ των ετικετών RFID και των αντίστοιχων συσκευών ανάγνωσης. Εάν κάποιος φέρει μία τέτοια συσκευή παρεμβολών, η επικοινωνία μεταξύ της ετικέτας και οποιασδήποτε συσκευής ανάγνωσης στην περιοχή της, είναι αδύνατη. Η Melanie είναι μέλος μίας ερευνητικής ομάδας η οποία μελετά την ανάπτυξη αυτού που οι ίδιοι καλούν "Σωματοφύλακα RFID", μίας συσκευής δηλαδή η οποία είναι πολύ πιο σύνθετη από την απλή δημιουργία παρεμβολών.

Ο "Σωματοφύλακας RFID" θα δίνει στον κάτοχο την δυνατότητα να επιλέγει ο ίδιος ποιες ετικέτες RFID είναι αναγνώσιμες και ποιες όχι. Η συσκευή δηλαδή θα είναι σε θέση να αναλύει τα ερωτήματα που προέρχονται από τις συσκευές ανάγνωσης RFID, και από το αποτέλεσμα της ανάλυσης να αποφασίζει εάν θα επιτρέψει ή θα αποτρέψει την επικοινωνία. Με τον τρόπο αυτό μπορούμε να επιτρέπουμε για παράδειγμα την επικοινωνία της RFID κάρτας για τα δημόσια μέσα μεταφοράς και να αποκλείουμε την χρήση όλων των υπολοίπων. Ένα τέτοιο σύστημα θα μπορούσαμε να το παρομοιάσουμε με το τοίχος προστασίας (firewall) του υπολογιστή μας

Μία φωνή

Σύμφωνα με την Melanie είναι σημαντικό να αντιδράσουν οι καταναλωτές και να απαιτήσουν μεγαλύτερη ασφάλεια. Έχουν ήδη γίνει κάποιες δοκιμές με ολοκληρωμένα RFID με μεγαλύτερο επίπεδο ασφάλειας, αλλά ακόμη βρίσκονται σε πειραματικό στάδιο. Είναι γεγονός πως για να επιτευχθεί η ασφάλεια σε ευρεία κλίμακα, θα πρέπει να επενδυθούν αρκετά χρήματα στην έρευνα. Όσο οι καταναλωτές δείχνουν με την συμπεριφορά τους ότι μπορούν να συμβιβαστούν και με μικρότερη ασφάλεια, οι εταιρείες δεν πρόκειται να ενδιαφερθούν για την έρευνα και βέβαια δεν πρόκειται να επενδύσουν τα όποια ποσά χρειάζονται για να αυξήσουν την ασφάλεια.

Αυτή την στιγμή υπάρχουν πολλές επιτροπές οι οποίες σχεδιάζουν πρότυπα για τα συστήματα RFID. Ελπίζουμε ότι τα πρότυπα που θα προκύψουν θα ορίζουν αυστηρότερες απαιτήσεις σχετικά με την ασφάλεια συστημάτων RFID, σε σχέση με το καθεστώς που ισχύει σήμερα. Στις συγκεκριμένες επιτροπές εκπροσωπούνται βέβαια και οι κατασκευαστές, και αυτό που τους "καίει" είναι να μπορέσουν να συνεχίσουν με την υπάρχουσα τεχνολογία, διαφορετικά θα υποχρεωθούν να επενδύσουν αρκετά χρήματα στην βελτίωση των προϊόντων τους.

Η άλλη πλευρά

Βασιζόμενοι σε αυτά τα δεδομένα, ζητήσαμε από την Philips (έναν από τους μεγαλύτερους κατασκευαστικές συσκευών RFID στον κόσμο), να μας πει την άποψη της σχετικά με το συγκεκριμένο ζήτημα.

Η Philips λοιπόν μας απάντησε ότι γνωρίζουν ήδη τους κινδύνους που σχετίζονται με την τεχνολογία RFID. Πιστεύουν πως είναι σημαντικό να παρακολουθούν τις εξελίξεις, ενώ επίσης ενδιαφέρονται να διευκρινίσουν τις μορφές των κινδύνων στους οποίους είναι εκτεθειμένη η τεχνολογία RFID. Παρ' όλα αυτά όμως η Philips τόνισε ότι είναι σημαντικό να γνωρίζει τον τρόπο με τον οποίο ελέγχθηκε ο ιός, καθώς και ότι στην συγκεκριμένη περίπτωση είχαμε ένα σύστημα το οποίο ήταν διαμορφωμένο έτσι ώστε να αποτελέσει στόχο παραβίασης.

Σύμφωνα πάντα με την Philips ο κίνδυνος που ενέχουν οι αναφορές αυτής της μορφής, είναι ότι διαβάζονται επίσης από άτομα τα οποία δεν είναι και τόσο καλά ενημερωμένα σχετικά με την μέθοδο που χρησιμοποιήθηκε. Το γεγονός αυτό μπορεί να οδηγήσει σε λανθασμένη ερμηνεία των δεδομένων και να δημιουργήσει εσφαλμένες εντυπώσεις στους καταναλωτές.

Όπως μας είπαν οι εκπρόσωποι της Philips, οι ετικέτες RFID που έχουν αναπτύξει για τα διαβατήρια και τα συστήματα πληρωμών είναι τόσο καλά προστατευμένες, που είναι ασφαλέστερες από οποιαδήποτε οικονομική συναλλαγή στο διαδίκτυο. Η Philips για παράδειγμα προμηθεύει ετικέτες RFID μεταξύ άλλων και στην Visa, η οποία τις χρησιμοποιεί στις τραπεζικές κάρτες.

Ένα άλλο σημείο το οποίο τόνισαν, είναι ότι η ασφάλεια ενός συστήματος εξαρτάται αποκλειστικά από την μορφή της εφαρμογής για την οποία χρησιμοποιείται η ετικέτα RFID. Για παράδειγμα η Philips έχει πουλήσει πάνω από 500 εκατομμύρια ολοκληρωμένα RFID Mifare από το 1994, τα οποία μεταξύ άλλων χρησιμοποιούνται σε συστήματα πληρωμών και δημόσια μέσα μεταφοράς. Μέχρι σήμερα, δεν είχαν καμία ενημέρωση ότι τα συγκεκριμένα ολοκληρωμένα RFID υπέστησαν κάποια παραβίαση.

Συμπέρασμα

Οι ετικέτες RFID αναμένεται να παίξουν ένα σημαντικό ρόλο στην κοινωνίας μας. Αυτή την στιγμή δεν μπορούμε παρά να κάνουμε υποθέσεις σχετικά με το μέγεθος των προβλημάτων ασφάλειας που ενδέχεται να προκαλέσουν, αλλά είναι απολύτως σαφές ότι το συγκεκριμένο ζήτημα θα πρέπει να εξεταστεί πολύ προσεκτικά. Ειδικά μάλιστα εάν αρχίσουμε να αποθηκεύουμε στις ετικέτες RFID τραπεζικές πληροφορίες, ιατρικά δεδομένα και άλλες ευαίσθητες πληροφορίες, είναι εξαιρετικά σημαντικό να θωρακίσουμε τα δεδομένα αυτά από μη εξουσιοδοτημένα ή κακόβουλα άτομα.

Από την μία πλευρά έχουμε τους κατασκευαστές RFID, οι οποίοι μας υπόσχονται πολυτέλεια και άνεση μέσω της τεχνολογίας RFID. Από την άλλη, έχουμε τις ομάδες των ανθρώπων που αντιμετωπίζουν την έλευση των συστημάτων RFID ως πρελούδιο της αποκάλυψης. Ποια από τις δύο πλευρές έχει δίκιο; Όπως συνήθως συμβαίνει, η αλήθεια θα βρίσκεται κάπου στην μέση. Σε κάθε πάντως περίπτωση, οι αναγνώστες του περιοδικού Ελεκτορ μπορούν να είναι σίγουροι ότι εμείς θα παρακολουθούμε τις εξελίξεις από κοντά και θα τους ενημερώνουμε.

(060174-1)

Σύνδεσμοι στο διαδίκτυο

http://rfidanalysis.org/
www.rfidvirus.org/
www.riscure.com/
www.rfidjournal.com