

ΤΕΧΝΟΛΟΓΙΑ RFID ΠΡΟΚΛΗΣΕΙΣ & ΑΠΕΙΛΕΣ



Μιχαήλ Μαβής

Προϊστάμενος Υποδ/νσης Ελέγχου Ασφαλείας
& Τηλεπικοινωνιακής Απάτης ΟΤΕ

Αντιπρόεδρος ΕΦΤΑ (Ελληνικού Φορέα πρόληψης Τηλεπικοινωνιακής Απάτης)

Email: [mmavis @ ote.gr](mailto:mmavis@ote.gr)



ΠΕΡΙΕΧΟΜΕΝΑ

- Τι είναι η τεχνολογία RFID και ποιες οι κύριες εφαρμογές της.
- Η χρήση της σε αντικείμενα, ζώα & ανθρώπους.
- Ποιοι οι βασικοί κίνδυνοι της τεχνολογίας RFID στην ασφάλεια και στην ιδιωτικότητα.
- Εφαρμογή της τεχνολογίας RFID στα νέα βιομετρικά διαβατήρια.
- Κίνδυνοι και απειλές.
- ΣΥΜΠΕΡΑΣΜΑΤΑ

Μερικές από τις πιο γνωστές μορφές ασύρματης επικοινωνίας

- Δορυφορικές επικοινωνίες
- Κινητές επικοινωνίες (GSM / DCS1800 / UMTS - 3 G)
- GPRS
- WiMax
- WiFi
- Bluetooth
- RFID



Τι είναι η τεχνολογία RFID ;

- **Radio Frequency Identification (RFID)** είναι τεχνολογία που επιτρέπει την αυτόματη αναγνώριση αντικειμένων. Βασίζεται στην αποθήκευση και ασύρματη ανάκτηση δεδομένων μέσω μικροσκοπικών συσκευών, τα ονομαζόμενα **RFID tags ή transponders**.

ΜΙΑ ΓΝΩΣΤΗ ΕΦΑΡΜΟΓΗ



- Τα e-Pass της Αττικής Οδού
- Τα ΤΕΟ-Pass των Εθνικών Οδών της χώρας

Πως λειτουργεί ;

Που τοποθετούνται τα RFID tags και τι περιέχουν ;

- Τοποθετούνται σε προϊόντα, ζώα ή ακόμη και σε ανθρώπους. Περιλαμβάνουν μικροσκοπικά chips με κεραίες, τα οποία τους επιτρέπουν να λαμβάνουν σήματα και να ανταποκρίνονται σε ραδιοσυχνότητες, οι οποίες εκπέμπονται από ένα RFID πομποδέκτη.
- Τα παθητικά tags δεν χρειάζονται καθόλου ηλεκτρική τροφοδοσία, ενώ τα ενεργητικά χρειάζονται μπαταρία.

ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ;

- Ένα σύστημα RFID αποτελείται από δύο μέρη.
 - **To tag** (microchip με κεραία)
 - **Τον αναγνώστη** (RFID reader με κεραία).
- Η κεραία είναι συντονισμένη να λαμβάνει τα ηλεκτρομαγνητικά κύματα που εκπέμπονται από τον αναγνώστη (Reader). Όταν το παθητικό tag λάβει ένα κατάλληλο κύμα διεγείρεται (λαμβάνει ενέργεια από το εν λόγω ηλεκτρομαγνητικό κύμα) και απαντά στέλνοντας μία απάντηση, η οποία λαμβάνεται από τον αναγνώστη (RFID reader).

Σε τι συχνότητες λειτουργούν τα συστήματα RFID ?

Οι πιο κοινές συχνότητες που χρησιμοποιούνται είναι :

- Χαμηλές συχνότητες (γύρω στα 125 KHz)
- Υψηλές συχνότητες (13,56 MHz) αυτή τη συχνότητα χρησιμοποιούν τα νέα ηλεκτρονικά βιομετρικά διαβατήρια.
- Λίαν Υψηλές συχνότητες ή UHF (860-960 MHz)
- Μικροκύματα (2.45 GHz)

Τι μέγεθος πληροφορίας μπορεί να ενταμιεύσει ένα RFID tag ?

- Εξαρτάται από την εφαρμογή. Συνήθως μεταφέρει λιγότερα από 2KB δεδομένων, αρκεί για την εφαρμογή που χρησιμοποιούνται. Τα απλά – μικρής χωρητικότητας παθητικά tags είναι και φθηνά και έτσι μπορούν να παραχθούν σε πολύ μεγάλες ποσότητες.

Ποια η διαφορά των Read-Only & των Read-Write RFID tags ;

- Τα μικροτσίπς των RFID tags μπορεί να είναι ενός από τους παρακάτω τύπους :
 - Read only
 - Read - write
 - Write once – read many (WORM)
- Τα Read – write tags επιτρέπουν την εγγραφή πληροφοριών στο εσωτερικό τους όταν βρίσκονται μέσα στην περιοχή ευθύνης κατάλληλου RFID reader.
- Αντίθετα τα Read Only tags εγγράφονται στο εργοστάσιο και δεν μπορεί να αλλάξει το περιεχόμενό τους αργότερα.
- Τα WORMs επιτρέπουν μόνο μία φορά εγγραφή χωρίς στη συνέχεια να είναι δυνατή η αλλαγή του περιεχομένου τους.

Ποια η εμβέλεια εργασίας ενός τυπικού RFID tag ;

- Δεν υπάρχει τυπικό παθητικό tag. Όλα εξαρτώνται από ποικίλους παράγοντες, όπως η συχνότητα λειτουργίας, η ισχύς του reader, αν το περιβάλλον είναι καθαρό ραδιοηλεκτρικά και ένα σωρό άλλους παράγοντες.
- Tags χαμηλής συχνότητας διαβάζονται από απόσταση 30 cm. Υψηλής συχνότητας tags διαβάζονται από 1 μέτρο, ενώ UHF tags διαβάζονται από 3 – 6 μέτρα.
- Σε περίπτωση που απαιτούνται μεγαλύτερες αποστάσεις (για παράδειγμα για εντοπισμό-αναγνώριση από απόσταση των βαγονιών ενός τραίνου), τότε ενεργά tags με μπαταρία μπορούν να διαβαστούν από απόσταση μέχρι 100 μέτρα ή περισσότερο.

Ποια η διαφορά της τεχνολογίας RFID με τα συστήματα βασισμένα σε Bar Code

- Δεν είναι υποχρεωτικά καλύτερα τα RFID tags. Είναι μία διαφορετική τεχνολογία και έχει διαφορετικές εφαρμογές, ενώ μερικές από αυτές συμπίπτουν. Η μεγαλύτερη διαφορά συνίσταται στο ότι τα συστήματα που βασίζονται στην τεχνολογία bar code απαιτούν οπτική επαφή μεταξύ τους (line of sight technology), δηλ. ο scanner θα πρέπει να «δει» το bar code για να το αναγνώσει.
- Αντίθετα τα RFID tags μπορούν να αναγνωστούν από μεγάλη απόσταση αρκεί να βρίσκονται στην περιοχή κάλυψης του αναγνώστη (RFID reader).
- Μία άλλη διαφορά είναι η εξής: Δύο κουτιά γάλα έχουν ακριβώς το ίδιο bar code ενώ αν χρησιμοποιείται η τεχνολογία RFID μπορεί να ενταμιευτεί ακόμη και η ημερομηνία λήξης του προϊόντος και να γίνεται αυτό άμεσα αντιληπτό από ένα «έξυπνο ψυγείο» το οποίο θα μας ενημερώνει ποια από τα είδη που έχει μέσα του έχουν πλέον λήξει !!!

Ποια η η ιστορία των RFID tags ;

- Το 1945 ο Leon Theremin ανακάλυψε ένα κατασκοπευτικό εργαλείο για τη Σοβιετική κυβέρνηση (ένα τύπο κοριού). Η συσκευή επανεξέπεμπε ραδιοκύματα με πληροφορίες συνομιλιών (audio information). Παρόλον ότι η συσκευή ήταν μία κρυφή παθητική συσκευή υποκλοπών και όχι ένα tag αναγνώρισης θεωρείται ως ο πρόδρομος της τεχνολογίας RFID.
- Άλλοι αναφέρουν ότι τα πρώτα RFID συστήματα σχετίζονται με την τεχνολογία των Radars για εντοπισμό εχθρικών αεροπλάνων και ήταν γνωστά από το 1920.

Τύποι των RFID tags

- Παθητικά
- Ημι-παθητικά &
- Ενεργητικά

Τα παθητικά RFID tags

- Δεν έχουν εσωτερική τροφοδοσία. Το στιγμιαίο ηλεκτρικό σήμα που επάγεται στην κεραία του παθητικού RFID tag από την εισερχόμενη ραδιοσυχνότητα παρέχει την απαραίτητη ισχύ στο CMOS ολοκληρωμένο κύκλωμα (IC) του tag για να επανειπέμψει ένα σήμα (backscattering). Το παθητικό RFID tag μπορεί να περιέχει EEPROM για ενταμίευση δεδομένων και έτσι να επανειπέμψει περισσότερες πληροφορίες από ένα απλό ID number (αριθμός σειράς).

Τα πλεονεκτήματα των παθητικών tags

- Μη έχοντας ηλεκτρική τροφοδοσία, το tag είναι μικρό ώστε να μπορεί να μπει ακόμμη και κάτω από την επιδερμίδα (ζώων ή ανθρώπων). Από το 2006 παράγονται μικρές τέτοιες συσκευές διαστάσεων 0,15 mm x 0,15 mm και έχουν πάχος μικρότερο από ένα φύλλο χαρτιού (7,5 μm).
- Τα παθητικά tags διαβάζονται από αποστάσεις 2 mm (ISO 14443) έως μερικά μέτρα (ISO 18000-6) ανάλογα με την κατασκευή και το μέγεθος της κεραίας τους και την χρησιμοποιούμενη συχνότητα.
- **ΧΡΟΝΟΣ ΖΩΗΣ:** Έχουν θεωρητικά άπειρο χρόνο ζωής (αφού δεν χρειάζονται μπαταρία).

Microchips από πολυμερές υλικό στη συχνότητα 13.56 MHz έχουν ήδη παραχθεί από διάφορες εταιρίες όπως η Philips στη Ολλανδία και η PolyC (Γερμανία). Τα περισσότερα tags σήμερα είναι παθητικού τύπου λόγω ευκολίας κατασκευής, μη ανάγκης για μπαταρία και μικρού κόστους.

Το κόστος των παθητικών RFID tags

- Το 2005 για ποσότητες 10 εκατομμ. κομματιών το κόστος ήταν κάτω από 0,072 € (~ 7 cents του €) το τεμάχιο.
- Οι τιμές αναμένεται να πέσουν δραστικά στο άμεσο μέλλον.

Ημι-παθητικά & Ενεργητικά tags

- Τα ημι-παθητικά RFID tags

Είναι ίδια με τα παθητικά με εξαίρεση μία μικρή μπαταρία. και είναι ταχύτερα στην ανάγνωση.

- Τα ενεργητικά RFID tags

Αυτά έχουν τη δική τους μπαταρία και εκπέμπουν δικό τους σήμα (ονομάζονται και beacons). Έχουν μεγαλύτερη ζώνη κάλυψης (μεγαλύτερες αποστάσεις – δεκάδες μέτρα), μεγαλύτερη μνήμη από ότι τα παθητικά tags,

Το μέγεθός τους σήμερα είναι παρόμοιο με ένα νόμισμα. Η μπαταρία τους έχει χρόνο ζωής μέχρι 5 χρόνια. Είναι όμως ακριβότερα από τα παθητικά.

Από τι αποτελείται ένα RFID σύστημα ;

Από πολλές συνιστώσες όπως:

- Tags,
- tag readers,
- edge servers,
- middleware και
- application software.

Ο σκοπός του συστήματος είναι να διευκολύνει την ασύρματη μετάδοση δεδομένων από μία φορητή συσκευή το tag, σε ένα RFID reader και στη συνέχεια να επιτρέψει την επεξεργασία των δεδομένων για τις ανάγκες της συγκεκριμένης εφαρμογής.

Χρήσεις της τεχνολογίας RFID

- Τα δεδομένα που εκπέμπονται από το tag μπορεί να δώσουν πληροφορίες αναγνώρισης είδους, ή πληροφορίες θέσης, ή ιδιότητες του είδους που το περιέχουν όπως για παράδειγμα τιμή, χρώμα, ημερομηνία λήξης κλπ. Η χρήση της τεχνολογίας RFID για εντοπισμό (tracking) και εφαρμογές πρόσβασης (access applications) πρωτοεμφανίστηκε το 1980.
- Σε ένα τυπικό RFID σύστημα, διαφορετικά αντικείμενα φέρουν ένα φθηνό παθητικό tag με ένα κωδικό είδους, ο οποίος αναγνωρίζεται από τον RFID reader, όταν αυτό διέλθει από το χώρο κάλυψης του αναγνώστη (ηλεκτρομαγνητική ζώνη). Ο αναγνώστης αποκωδικοποιεί τα δεδομένα του tag και αυτά με τη σειρά τους επεξεργάζονται σε έναν υπολογιστή ή υπολογιστικό σύστημα (εκτελώντας τις εργασίες συγκεκριμένης εφαρμογής).

«Ηλεκτρονική» Βιβλιοθήκη & Shipping Containers

- Οι πόρτες ασφαλείας της βιβλιοθήκης με κατάλληλους RFID readers μπορεί να αναγνωρίσουν αν το βιβλίο που φέρει ανά χείρας ο εξερχόμενος (με το αντίστοιχο tag) πέρασε από τον έλεγχο και δανείστηκε κανονικά. Επίσης στην επιστροφή μπορεί αυτόματα να γίνει ηλεκτρονική καταχώρηση επιστροφής του βιβλίου.

Shipping Containers:

- Εξάλλου UHF RFID tags συνήθως χρησιμοποιούνται για τον εντοπισμό **παλετών** σε shipping containers (πλοία)

Ηλεκτρονικό Χρήμα - micropayments

- Smart cards μέσα σε RFID chips μπορούν να χρησιμοποιηθούν για ηλεκτρονική πληρωμή χρημάτων (micropayments – ηλεκτρονικό πορτοφόλι). Για παράδειγμα αναφέρουμε ήδη λειτουργούσες εφαρμογές όπως:
- SmarTrip στην Washington DC, USA,
- EasyCard στην Taiwan,
- Suica στην Ιαπωνία,
- T-Money στη Νότιο Κορέα,
- Octopus Card στο Hong Kong, και την Ολλανδία
- Oyster Card στον υπόγειο του Λονδίνου για πληρωμή εισιτηρίων στα μέσα μαζικής μεταφοράς. Αυτή είναι μία πιστωτική τύπου κάρτα για την είσοδο στα λεωφορεία και τον υπόγειο (παρόμοια με τη χρήση του e-pass, TEO-pass στους ελληνικούς αυτοκινητόδρομους). Αφορά ανθρώπους αντί για αυτοκίνητα.

RFID τεχνολογία στα αυτοκίνητα:

- Τα ηλεκτρονικά κλειδιά μηχανής (smart keys/smart start) στα αυτοκίνητα Toyota & Lexus από τα μοντέλα του 2004 είναι τεχνολογίας RFID. Αναγνωρίζουν την παρουσία του κατόχου του αυτοκινήτου από απόσταση 1 μέτρου από τον αναγνώστη (sensor). Ο οδηγός μπορεί να ανοίξει την πόρτα και την μηχανή ενώ το κλειδί παραμένει στην τσέπη του.



Διαχείριση ζώων (RFID in livestock)

- Τον Απρίλιο του 2006 η Ταιβανέζικη κυβέρνηση υλοποίησε ένα μεγάλο Project με την εταιρία Advanced ID Corporation για την εισαγωγή RFID tags στα αποδημητικά πουλιά, στην προσπάθεια να αντιμετωπίσει την γρίπη των πτηνών. Μελέτες γίνονται συνεχώς σε πολλές Ασιατικές χώρες όπως η Κίνα, η Ταϊλάνδη και η Ιαπωνία

Εμφύτευση RFID

- Το 1998 ο Άγγλος καθηγητής της Κυβερνητικής Kevin Warwick, τοποθέτησε (έκανε implanted - εμφύτευση) ένα microchip τεχνολογίας RFID στον βραχίονα του. Εταιρίες και Οργανισμοί προτείνουν τη χρήση της τεχνολογίας RFID under the skin (κάτω από το δέρμα) σαν λύση για τον έλεγχο πλαστοπροσωπίας (identify theft), ασφαλούς εισόδου στα κτίρια, πρόσβαση σε υπολογιστές, αποθήκευση ιατρικών δεδομένων, μέσο εναντίον των απαγωγών και σε ένα σωρό άλλες εφαρμογές σχετιζόμενες με τις αρχές ασφαλείας.

RFID σε ανθρώπους

- Ειδικές συσκευές όπως η προτεινόμενη Digital Angel, έχουν διάφορες ιατρικές εφαρμογές για συνεχή καταγραφή δεδομένων υγείας του ασθενούς (πίεση, ζάχαρο, παλμοί καρδιάς κλπ). Διάφορα clubs όπως το Baja Beach Club ένα night club στη Βαρκελώνη της Ισπανίας και στο Rotterdam της Ολλανδίας χρησιμοποιεί το VeriChip RFID tag το οποίο έχει τοποθετηθεί κάτω από το δέρμα των VIP πελατών του, για την είσοδο και πληρωμή των ποτών και αναψυκτικών.
- Το 2004, ο Μεξικανός Γενικός Εισαγγελέας υποχρέωσε 18 μέλη του προσωπικού του να τοποθετήσουν στο σώμα τους Verichip RFID tags για την είσοδο στα υψηλής ασφάλειας δωμάτια με τα αρχεία της υπηρεσίας.

**Αναγνώστης της εταιρείας VERICHIP για ανάγνωση
RFID chips που είναι εμφυτευμένα στο ανθρώπινο σώμα
(implanted).**



RFID σε ιατρικές εφαρμογές

- **Ιούλιος-2003** Η Αμερικανική Υπηρεσία FDA (Food and Drug Administration) που έχει έργο παρόμοιο με τις Ελληνικές Υπηρεσίες ΕΦΕΤ & ΕΟΦ μαζί, ξεκίνησε τη μελέτη χρήσης της τεχνολογίας RFID για αναγνώριση ασθενών και έλεγχο εισόδου του νοσηλευτικού προσωπικού στις εμπιστευτικές πληροφορίες που αφορούν την υγεία.
- **Οκτώβριος-2004** Η FDA ενέκρινε το πρώτα RFID chips τα οποία μπορούν να εμφυτευθούν στο ανθρώπινο σώμα. Τα σχετικά RFID chips (σε συχνότητα 134 KHz) από την εταιρία VeriChip Corp. μία θυγατρική της εταιρίας Applied Digital Solutions έλαβαν τη έγκριση τύπου από το Αμερικανικό FDA για χρήση σε ανθρώπους (για ιατρικές εφαρμογές).

Πρώτες αντιδράσεις

- Ας σημειωθεί ότι αρκετοί anti-RFID αντιβιστές όπως οι Κατερίνα Άλπρεχτ και η Λίζα Μακ Ιντιρε αποκάλυψαν εμπιστευτικές επιστολές στελεχών του FDA, στις οποίες αναφερόταν οι κίνδυνοι στην υγεία από τη χρήση των εμφυτευμένων RFID chips στο ανθρώπινο σώμα, τις οποίες όμως δεν έλαβαν υπόψη οι αρμόδιοι για την έγκριση.

RDIF traffic & positioning:

- Μία πολύ κοινή χρήση της τεχνολογίας RFID είναι στην πληρωμή διοδίων.
- Επίσης η λεγόμενη RBS εφαρμογή (Road Beacon Systems). Αντί για τη χρήση δορυφορικών συστημάτων για την αποστολή μηνυμάτων κινδύνου στους οδηγούς, γίνεται χρήση της τεχνολογίας RFID από tags που είναι κρυμμένα στο πεζοδρόμιο και επικοινωνούν με αντίστοιχο αναγνώστη στο αυτοκίνητο μεταφράζοντας το σήμα σε ηχητικές συμβουλές στους οδηγούς (voice messages).
- Ιδιαίτερα χρήσιμη υπηρεσία μέσα σε τούνελ (όπου τα ραδιοσήματα από δορυφόρους ή άλλα επίγεια μέσα δεν είναι αποτελεσματικά).

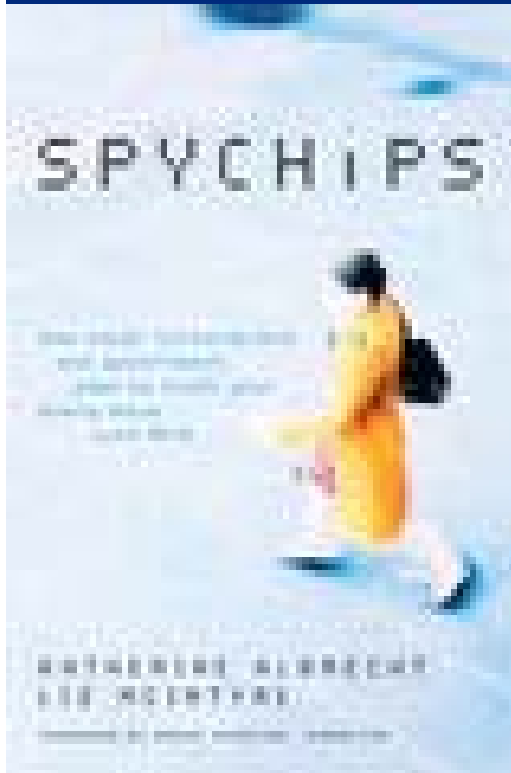
Απειλές από την τεχνολογία RFID:

- Η βασική απειλή συνίσταται στον παράνομο εντοπισμό (tracking) των RFID tags. Έτσι μπορεί να γίνει παράνομος εντοπισμός (location) αντικειμένων – ή ανθρώπων από τα RFID tags που έχουν επάνω τους χωρίς να το γνωρίζουν (πχ. πάνω στα ρούχα τους) ή τα φέρουν ενσυνείδητα (πχ. βιομετρικά διαβατήρια).
- Ιδιαίτερα για τους ανθρώπους πρέπει να σημειωθεί ότι μπορεί να έχουν επάνω τους δεινάδες tags χωρίς να το γνωρίζουν (στα ρούχα, στη τσάντα τους, στο στυλό τους, στο κινητό τους κλπ). Η εταιρία RFIDsec (www.rfidsec.com) είναι ενεργή στην υλοποίηση πρακτικών για την ασφαλή χρήση της τεχνολογίας RFID.

Προβλήματα του tag:

- Το πρόβλημα με τα tags που χρησιμοποιούν κρυπτογραφία είναι το υψηλότερο κόστος και η ανάγκη για ηλεκτρική τροφοδοσία, πράγμα που ελαττώνει την χρησιμότητά τους. Για το λόγο αυτό οι κατασκευαστές δημιουργούν tags με ασθενείς ή proprietary αλγορίθμους κρυπτογράφησης, οι οποίοι όμως δεν είναι ιδιαίτερα ανθεκτικοί σε επιθέσεις.
- Το βασικό πρόβλημα είναι η έλλειψη υπολογιστικών πόρων πάνω στο tag, γιατί τότε γίνεται δύσχρηστο και κυρίως ακριβό (ιδιαίτερα όταν μιλάμε για τεράστιους όγκους παραγωγής).

Προβλήματα στην ιδιωτικότητα



- Οι αντιθέμενοι στην τεχνολογία RFID παρουσιάζουν τους κινδύνους στην ιδιωτικότητα από τη χρήση των tags. Προβάλλουν τη δυνατότητα κυβερνήσεων και μεγάλων οργανισμών να **παρακολουθούν κάθε μας κίνηση** από μακριά με τη χρήση της τεχνολογίας RFID (Τα tags ονομάζονται Spsychips = chips κατάσκοποι).
- Το πρόβλημα είναι ότι μετά την αγορά των προϊόντων τα tags παραμένουν στα προϊόντα που αγοράστηκαν (ρούχα – παπούτσια ή άλλα είδη) με αποτέλεσμα να αποτελούν μία ασύρματη μέθοδο αναγνώρισης του κατόχου τους ! Παρόλον ότι η τεχνολογία RFID έχει μικρή εμβέλεια, η πραγματικότητα είναι ότι κάποιος με μία πολύ ισχυρή κεραία μπορεί να διαβάσει όλα τα είδη που είναι μαρκαρισμένα με tags μέσα σε ένα σπίτι από μακριά. Το σενάριο θυμίζει ταινία Όργουελ !
- Ακόμη και αν τα ρούχα ή άλλα είδη πεταχτούν ή χαριστούν, το RFID code μπορεί να δώσει πληροφορίες σχετικά με τον κοινωνικό περίγυρο και τις επαφές (με ποιους σχετίζεται) ενός συγκεκριμένου ατόμου.

Τα νέα βιομετρικά διαβατήρια:

- Όλα αυτά θα ήταν θεωρητικά και δυνητικά προβληματικά, αν δεν υπήρχε η πιο σημαντική εφαρμογή της τεχνολογίας RFID η οποία επηρεάζει όλους μας. Πρόκειται για τα νέα βιομετρικά διαβατήρια, τα οποία περιλαμβάνουν πολλά προσωπικά δεδομένα του κατόχου τους.
- Ο Bruce Schneier, ένας από τους επιφανέστερους ειδήμονες σε θέματα ασφάλειας στις ΗΠΑ ανέφερε καθαρά: « Πρόκειται για μία καθαρή απειλή στην προσωπική ασφάλεια και στην ιδιωτικότητα. Είναι απλά μια πολύ κακή ιδέα.
- Ευαίσθητες πληροφορίες αναγνώσιμες από μηχανήματα μπορεί να εκτεθούν σε κίνδυνο (όπως για παράδειγμα η εθνικότητα ενός ατόμου). » Ένας τρομοκράτης σε ένα αεροδρόμιο μπορεί να προγραμματίσει ένα αναγνώστη RFID σε μία βαλίτσα, ο οποίος να ενεργοποιεί ένα εκρηκτικό μηχανισμό όταν κοντά του διέρχεται άτομο με **Αμερικανικό ή Εβραϊκό διαβατήριο....**

Ευρωπαϊκά βιομετρικά διαβατήρια

- Η Σουηδία άρχισε την έκδοση βιομετρικών διαβατηρίων με την τεχνολογία RFID, από τις 19 Οκτ. 2005. Κάθε διαβατήριο περιλαμβάνει προσωπικές πληροφορίες όπως ύψος, χρώμα μαλλιών κεφαλής και ματιών όπως επίσης και μία ψηφιακή φωτογραφία του κατόχου του.
- Σε συνέχεια απαίτησης από την Σουηδική Αστυνομική Διεύθυνση, η εταιρία Arcontia AB που υλοποίησε το έργο των διαβατηρίων κατασκεύασε αναγνώστες κατάλληλους για να μπορούν να διαβάσουν εκτός από τα διαβατήρια και τις νέες ηλεκτρονικές ταυτότητες που διαθέτουν επίσης RFID tags. Οι αναγνώστες σε κάθε αστυνομικό σταθμό συνδέονται με τους υπολογιστές του δικτύου της αστυνομίας μέσω USB port και κατάλληλους software drivers. Μέσω δε αυτών με τις τράπεζες πληροφοριών της Σουηδικής αστυνομίας.
- **Μετά τη Σουηδία, η Γαλλία** άρχισε να εκδίδει βιομετρικά διαβατήρια από τις **17 Απριλίου 2006.**

Οι απειλές στα διαβατήρια:

Η αρχική απόφαση των ΗΠΑ να μην κρυπτογραφήσουν τα δεδομένα που περιέχονται στα RFID chips των διαβατηρίων εξέθετε τους κατόχους τους στις γνωστές απειλές με την ονομασία **skimming & Eavesdropping**.

- **Skimming (ξάφρισμα) :**

Skimming συμβαίνει ότι ένας εισβολέας με ένα λαθραίο αναγνώστη βρίσκεται στην περιοχή όπου περνά ο ανυποψίαστος κάτοχος του διαβατηρίου. Ο εισβολέας τότε διαβάει το περιεχόμενο του διαβατηρίου χωρίς ο κάτοχός του να καταλάβει τίποτε.

- **Eavesdropping**

Eavesdropping συμβαίνει όταν ένας εισβολέας υποκλέπτει τα δεδομένα, τα οποία εκπέμπονται από το RFID chip του διαβατηρίου προς ένα κανονικό αναγνώστη.

Επί πλέον προβλήματα στην ιδιωτικότητα:

- Ένα άλλο πολύ σημαντικό θέμα που θίγει την ιδιωτικότητα αφορά το πρωτόκολλο μέσω του οποίου ο αναγνώστης μπορεί να παρακολουθήσει πολλά tags, τα οποία βρίσκονται στην περιοχή του και απαντούν όλα μαζί στο ραδιο-σήμα του.
- Η δομή του πρωτοκόλλου είναι τέτοια ώστε όλα εκτός του τελευταίου bit του σειριακού αριθμού του tag μπορούν να υπολογιστούν απλά και μόνο με παθητική υποκλοπή του σήματος (passive eavesdropping) που ανταλλάσσεται μεταξύ αναγνώστη και tag. Έτσι η απόσταση από την οποία μπορεί να γίνει υποκλοπή του σήματος που εκπέμπει το tag δεν έχει σημασία. Αυτό που μετράει είναι η απόσταση από την οποία το σήμα ενός πολύ ισχυρού αναγνώστη μπορεί να διαβαστεί από το tag. Μερικοί αναγνώστες έχουν μεγάλη ισχύ (π.χ. 4 Watts), ώστε να μπορούν να στείλουν το σήμα τους, το οποίο να μπορεί να διαβαστεί από tags, **ακόμη και από δεκάδες χιλιόμετρα μακριά !!!**

Οι ΗΠΑ αλλάζουν πλάνο ασφαλείας στα διαβατήρια

- Μετά τη μεγάλη κριτική από ειδήμονες ασφαλείας και από οργανώσεις που ενεργοποιούνται στα ανθρώπινα δικαιώματα, σχετικά με τους κινδύνους της τεχνολογίας RFID στα νέα διαβατήρια, η Αμερικανική κυβέρνηση αναθεώρησε το πλάνο της σχετικά με τα διαβατήρια, αποδεχόμενη λύσεις που πριν είχε απορρίψει, για την προστασία των δεδομένων που υπάρχουν στα βιομετρικά διαβατήρια.
- Η λύση ασφαλείας απαιτεί ο αναγνώστης RFID να δίνει ένα κλειδί ή password πριν του επιτραπεί να αναγνώσει τα δεδομένα που βρίσκονται στο RFID chip του διαβατηρίου. Σύμφωνα με τη λύση ασφαλείας τα δεδομένα που ανταλλάσσονται μεταξύ του chip του διαβατηρίου (tag) και του αναγνώστη θα είναι κρυπτογραφημένα, ώστε να μην είναι αναγνώσιμα από κάποιον που υποκλέπτει την επικοινωνία.

Οι προδιαγραφές των διαβατηρίων και ο ICAO

- Ο ICAO (International Civil Aviation Organization), που δημιούργησε τις διεθνείς προδιαγραφές για όλες τις χώρες που προτίθενται να εφαρμόσουν τα νέα RFID διαβατήρια, δημιούργησε προδιαγραφές για μία διαδικασία ασφαλείας που ονομάζεται BAC (Basic Access Control).
- Ο μηχανισμός BAC δουλεύει ως εξής: Τα δεδομένα στο διαβατήριο τοποθετούνται σε ένα RFID chip, μέσα στο σώμα του διαβατηρίου, αλλά τα δεδομένα είναι «κλειδωμένα» και μη διαθέσιμα σε ένα αναγνώστη, ο οποίος δεν διαθέτει το μυστικό κλειδί για να ξεκλειδώσει τα δεδομένα του διαβατηρίου.

Ο μηχανισμός BAC (Basic Access Control)

- Ένας αστυνομικός στο χώρο ελέγχου διαβατηρίων για να πάρει το κλειδί και να διαβάσει τα βιομετρικά δεδομένα του διαβατηρίου θα πρέπει να σκανάρει ηλεκτρονικά (OCR-B) το κείμενο που βρίσκεται κάτω από την φωτογραφία του κατόχου του και περιλαμβάνει τις παρακάτω πληροφορίες:
 - Ημερομηνία γέννησης
 - Αριθμός διαβατηρίου
 - Ημερομηνία λήξης του διαβατηρίου.
- Στη συνέχεια μετά την οπτική ανάγνωση των παραπάνω δεδομένων, ο εσωτερικός αλγόριθμος του αναγνώστη (RFID Reader) δημιουργεί ένα μοναδικό κλειδί (με μηχανισμό hash) με το οποίο στη συνέχεια «ξεκλειδώνει» το RFID chip του διαβατηρίου.

Τα θετικά του μηχανισμού BAC



Facial image has been read

Security of Systems, Radboud University Nijmegen Ronny Wichers Schreur

```
Record length: 14882
Number of images: 1
Gender: Unspecified
Eye colour: Unspecified
Hair colour: Unspecified
Expression: Neutral
Angle yaw: 0 deg
Angle pitch: 0 deg
Angle roll: 0 deg
Angle yaw uncertainty: +-5 deg
Angle pitch uncertainty: +-5 deg
Angle roll uncertainty: +-0 deg
Feature points: 2
code 12.2, x: 179, y: 288
code 12.1, x: 299, y: 288
Image type: Full Frontal
Image data type: JPEG2000
Width: 480
Height: 640
ColourSpace: 24 bit RGB
Source: Photo still
Device type: Unspecified
Quality: 0
Image data: <<14820 bytes>>
```

Details facial image

Security of Systems, Radboud University Nijmegen Ronny Wichers Schreur

- Ο μηχανισμός BAC δεν επιτρέπει το skimming επειδή απαγορεύει σε απομακρυσμένους αναγνώστες να ανακτήσουν τα δεδομένα του διαβατηρίου, πριν το διαβατήριο «ανοίξει» μετά το σκανάρισμα του οπτικού αναγνώστη. Επίσης απαγορεύει το eavesdropping αφού το κανάλι επικοινωνίας μεταξύ chip tag & αναγνώστη είναι κρυπτογραφημένο.

Χαρακτηριστικά του BAC

- Η χρήση επομένως του BAC δίνει μία επιπρόσθετη ασφάλεια στο διαβατήριο. Τα μέλη της Ευρωπαϊκής Ένωσης αποδέχτηκαν τον μηχανισμό BAC, επειδή είχαν στόχο να περιλάβουν επί πλέον δεδομένα στο ηλεκτρονικό διαβατήριο (όπως δύο ηλεκτρονικά δακτυλικά αποτυπώματα).
- Το chip που χρησιμοποιείται στα νέα ηλεκτρονικά διαβατήρια ακολουθεί το πρότυπο ISO 14443 και περιέχει πληροφορίες όπως το όνομα του κατόχου, **την εθνικότητα**, το φύλλο, την ημερομηνία γέννησης, και μία ψηφιακή φωτογραφία (κατ' ελάχιστο). Επίσης τον αριθμό του διαβατηρίου, την ημερομηνία έκδοσης, την ημερομηνία λήξης, και τον τύπο του διαβατηρίου. Σύμφωνα με το πρότυπο το διαβατήριο θα πρέπει να βρίσκεται σε απόσταση 10 εκατοστών από τον αναγνώστη για να διαβαστεί.

Τέστ στην Ολλανδία ...

- Η Αμερικανική κυβέρνηση υπολόγιζε ότι τα δεδομένα δεν θα μπορούν να διαβαστούν από απόσταση πάνω από 10 cm. Σχετικά τεστς όμως έδειξαν ότι ένας κατάλληλος αναγνώστης σε απόσταση μέχρι 10 μέτρα μπορεί να διαβάσει άνετα το περιεχόμενο των βιομετρικών δεδομένων ενός διαβατηρίου.
- Τα σχετικά τεστς έγιναν στην Ολλανδία στο Πανεπιστήμιο του Delft.
- Το χειρότερο ήταν ότι ο μηχανισμός BAC έσπασε μέσα σε δύο ώρες με πολύ φθηνό εξοπλισμό.

Πανεπιστήμιο του Delft (NL)

Για περισσότερες πληροφορίες ο καθένας μπορεί να επικοινωνήσει με τον κ. Harko Robroch

■ Τηλ: +31 64843 2222

■ Email: robroch@riscure.com

Ταχυδρομική Διεύθυνση :

Riscure BV

Radex Innovation Centre

Rotterdamseweg 183/C

2629HD Delft

The Netherlands.

Το σπάσιμο των βιομετρικών διαβατηρίων

- Ο Παρουσιαστής της Ολλανδικής TV που αποκάλυψε στο τέλος Ιανουαρίου 2006, το σπάσιμο της κρυπτογραφίας των νέων βιομετρικών διαβατηρίων. Δείτε περισσότερες πληροφορίες στο site :
- http://www.theregister.co.uk/2006/01/30/dutch_biometric_passport_crack



Λύσεις στο πρόβλημα του tag

Η Ακαδημαϊκή Κοινότητα πρότεινε ήδη μερικές λύσεις στο πρόβλημα της ασφάλειας :

- Προτάθηκε να μεγαλώσει ο αριθμός των ψηφίων (εντροπία) της κλείδας του μηχανισμού BAC.
- Τα διαβατήρια να τοποθετούνται σε ειδικά πορτοφόλια (κλωβοί Faraday).
- Τεχνικές Hash Locks.
- Backward channel XORing
- Third Party privacy agents
- LPN authentication
- Η εταιρία RSA Security έχει πατεντάρει μία πρότυπη συσκευή η οποία παρεμβάλλει (δημιουργεί σήματα παρεμβολής – jamming) στα RFID σήματα, διακόπτοντας το standard collision avoidance protocol, επιτρέποντας στον χρήστη να εμποδίσει μία μη εγκεκριμένη αναγνώριση και διάβασμα του περιεχομένου του tag.

Τα Σουηδικά διαβατήρια

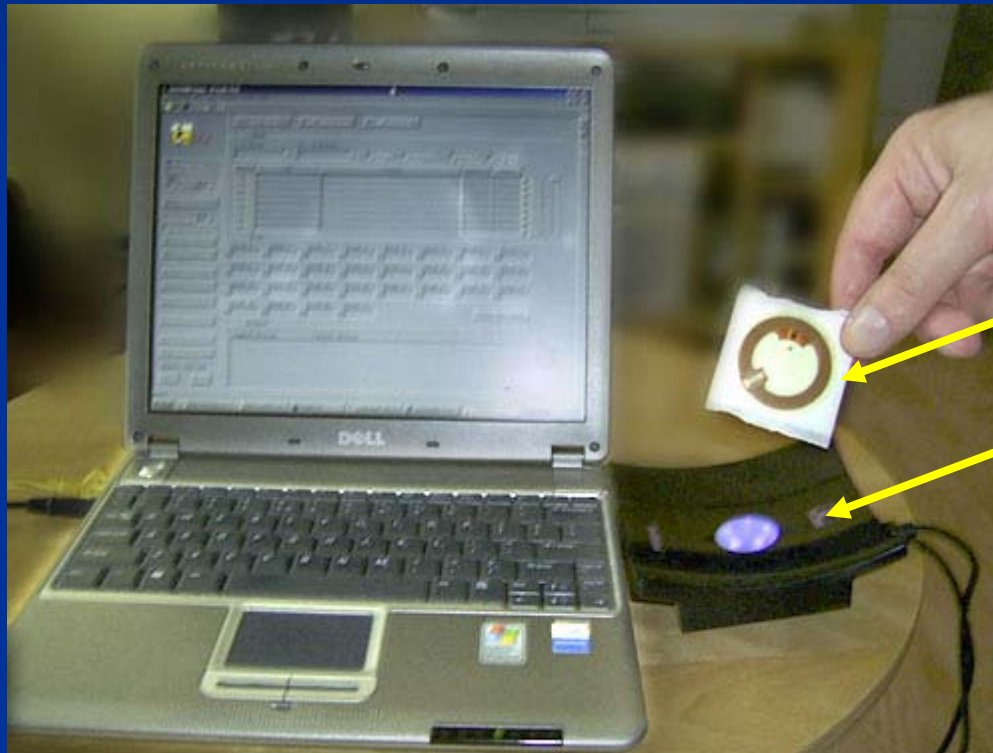
- Τα tags των Σουηδικών διαβατηρίων και των Σουηδικών Ταυτοτήτων λειτουργούν στη συχνότητα των 13.56 MHz και ακολουθούν τα πρότυπα του ISO 7816 και ISO 1443A
- Τα tags έχουν ενεργοποιημένο τον μηχανισμό BAC. Ο μυστικός κωδικός παράγεται μετά από οπτική ανάγνωση (OCR) της σχετικής σελίδας του διαβατηρίου ή τυπώνεται χειροκίνητα στη σχετική οθόνη του υπολογιστή με τον RFID αναγνώστη. Αν υπάρχει σύμπτωση των κωδικών το διαβατήριό διαβάζεται.



Ασφάλεια (tag-location & cloning)

- Η κρυπτογραφία μπορεί να χρησιμοποιηθεί για να αποτρέψει την κλωνοποίηση του tag. Εξάλλου μερικά tags έχουν δυνατότητα αλλαγής του κωδικού αναγνώρισής τους με το χρόνο, ώστε οι ενταμιευμένες πληροφορίες που ανταλλάσει το tag με κάποιο νόμιμο αναγνώστη (reader) να αλλάζουν μετά από κάθε σκανάρισμα, αποτρέποντας έτσι τη χρήση του υποκλοπέντος σήματος επικοινωνιών.
- Πιο εξελιγμένες τεχνικές επιτρέπουν χρήση πρωτοκόλλων του τύπου challenge-response, όπου το tag αλληλοεπιδρά με τον αναγνώστη. Στις περιπτώσεις αυτές μυστικές πληροφορίες του tag δεν αποστέλλονται ποτέ ακρυπτογραφητές στο ανασφαλές κανάλι επικοινωνίας tag-reader. Αντ' αυτού χρησιμοποιείται συμμετρική ή ασύμμετρη κρυπτογραφία.

Αναγνώστης RFID tags



Tag

Αναγνώστης
(reader)

Προστασία διαρροής πληροφοριών από τα ηλεκτρονικά διαβατήρια με τη βοήθεια κλωβού Faraday & ειδικών πορτοφολιών

- Η εταιρία Difrwear (www.difrwear.com) παράγει ειδικά πορτοφόλια με κλωβό faraday, ο οποίος προστατεύει από την διαρροή εμπιστευτικών πληροφοριών το RFID chip που βρίσκεται στο ηλεκτρονικό διαβατήριο από το κίνδυνο του skimming.
- Τα εμπιστευτικά δεδομένα δεν μπορούν να διαρρεύσουν όταν το πορτοφόλι είναι κλειστό. Τι γίνεται όμως όταν το διαβατήριο βγει από το πορτοφόλι προστασίας για να διαβαστεί από ένα νόμιμο αναγνώστη στον έλεγχο διαβατηρίων ?

Το πορτοφόλι προστασίας του διαβατηρίου



Το πορτοφόλι προστασίας που αποτελεί κλωβό Faraday
της εταιρίας Difwear (www.difrwear.com)

Πόσο ασφαλή είναι τα RFID cards ;



Σύμφωνα με τους παραπάνω φοιτητές ενός Αμερικανικού Κολλεγίου **ΚΑΘΟΛΟΥ ΑΣΦΑΛΗ**

Η κλωνοποίηση των πληροφοριών που βρίσκονται στο RFID card είναι εύκολη υπόθεση.

Η ενεργή περιοχή των RFID tags μπορεί να μεγαλώσει. Οι παραπάνω φοιτητές κατάφεραν να επεκτείνουν την ενεργή ζώνη στα 69 πόδια (23 μέτρα), πολύ πάνω από τα 10 εκατοστά που αναφέρει το πρότυπο του ICAO. Στη συνέχεια τα RFID cards μπορούν με μικρή προσπάθεια να αντιγραφούν (κλωνοποιηθούν) από τον επιτιθέμενο.

Οι μέθοδοι κρυπτογράφησης είναι ιδιοκατασκευής εταιριών (proprietary) και το σπάσιμο της κρυπτογραφίας εύκολη υπόθεση.

Πολλές εταιρίες και οργανισμοί αντιλαμβάνονται την έλλειψη ασφάλειας στην τεχνολογία RFID δεν προχώρησαν στην υλοποίηση εφαρμογών πριν λυθούν βασικά θέματα ασφαλείας.

Κλωνοποίηση RFID tags

- Τα RFID tags είναι υποκείμενα επιθέσεων για ανάκτηση εμπιστευτικών πληροφοριών, ή κλωνοποίηση (με πολύ απλές και φθηνές συσκευές όπως οι παρακάτω).



Δείτε περισσότερα στο site <http://cq.cx/index.pl>

ΣΥΜΠΕΡΑΣΜΑΤΑ

- Η Τεχνολογία RFID έχει πολλές χρήσιμες εφαρμογές.
- Δεν είναι απόλυτα ώριμη σήμερα ως προς την ασφάλεια. Υπάρχουν πολλές δυνατότητες, οι οποίες όμως αυξάνουν το κόστος του RFID tag.
- Ο κίνδυνος διαρροής εμπιστευτικών πληροφοριών ή κλωνοποίησης είναι υπαρκτός. Αυτό είναι ιδιαίτερα σημαντικό όσον αφορά τα δεδομένα των βιομετρικών διαβατηρίων.
- Υπάρχουν πολύ σοβαρά θέματα που αφορούν την προστασία της ιδιωτικότητας (privacy), τα οποία και θα πρέπει να ληφθούν σοβαρά υπόψη κατά την χρήση της τεχνολογίας, από τους Νομικούς και τις Αρχές Προστασίας Προσωπικών Δεδομένων (Data Protections Authorities).