

Πόσο ασφαλείς είναι οι πιστωτικές κάρτες;

Το σύστημα κρυπτογράφησης RFID αποδείχθηκε ευάλωτο στους χάκερς



Με ένα «ηλεκτρονικό στηθοσκόπιο» γερμανοί ερευνητές υπέκλεψαν τα στοιχεία πιστωτικής κάρτας και έδειξαν ότι «ο βασιλιάς είναι γυμνός».

8

Έχουν περάσει κάπου 2.500 χρόνια αφότου «της γειτονιάς μας ο τρελός», ο Πυθαγόρας, διακήρυξε ότι «η γλώσσα του Σύμπαντος είναι τα μαθηματικά». Από τότε η όλη πρόοδος της επιστήμης κατατείνει στο να αποδείξει πως «τα είχε τετρακόσια». Αλλά και χωρίς να περιμένουμε τις επιστημονικές αποδείξεις, ο κόσμος μας έχει ήδη εμπιστευθεί το βίος του στην ασφάλεια των μαθηματικών: όλες οι τραπεζικές συναλλαγές γίνονται ψηφιακά, μέσω κρυπτογράφησης με μαθηματικούς αλγορίθμους, και όλες οι αγοραπωλησίες με «πλαστικό χρήμα» γίνονται μέσω καρτών που επίσης διασφαλίζουν τη συναλλαγή με μαθηματικούς αλγορίθμους.{AR}

Θεωρητικά η κρυπτογράφηση αυτή είναι απολύτως ασφαλής. Στην πράξη, όμως, η υλοποίησή της σκοντάφτει στην πειρατική αντιστροφή της τεχνολογίας εφαρμογής της. Και τα πιο γνωστά θύματα αυτής της πειρατείας είναι οι πιστωτικές ή χρεωστικές κάρτες που όλοι χρησιμοποιούμε.

Όλοι μας έχουμε ακούσει ή διαβάσει το πώς οι κάρτες με μαγνητική λωρίδα μπορούν να «διαβαστούν» από μηχανάκια αντίστοιχα εκείνων που έχουν όλα τα

καταστήματα που δέχονται τις κάρτες μας. Με ένα τέτοιο «γκάτζετ» κρυμμένο στην τσέπη του, ο κάθε σερβιτόρος μπορεί να υποκλέψει τα στοιχεία μας. Όμως η ευκολία που μας παρέχουν οι κάρτες είναι τόσο μεγάλη ώστε να συνεχίζουμε ακάθεκτοι την καταναλωτική μας δράση με αυτές. Μάλιστα ο ραγδαίος μετασχηματισμός της Κοινωνίας της Πληροφορίας σε «Ασύρματη Κοινωνία» έχει ωθήσει τους εκδότες τέτοιων καρτών στην υιοθέτηση μιας ακόμη μεγαλύτερης καινοτομίας: στην ενσωμάτωση στις κάρτες κυκλωμάτων «ταυτοποίησης μέσω ραδιοσυχνότητων» (Radio Frequency Identification, εν συντομία RFID).

Η υπόσχεση των RFID

Τη RFID την πρωτογνωρίσαμε στη μορφή ενός λεπτού και χάλκινου τετράγωνου σπινάλ, με ένα τσιπάκι στο κέντρο του. Το σπινάλ είναι η κεραία που εκπέμπει την ταυτότητα του προϊόντος στις αντίστοιχες συσκευές ανάγνωσης του κάθε καταστήματος ώστε το προσωπικό του να ελέγχει το πού βρίσκεται το προϊόν και αν βγήκε από το κατάστημα εξοφλημένο ή «σουφρωμένο». Με την ενσωμάτωση αυτής της τεχνολογίας στις πιστωτικές κάρτες ο κάτοχός τους μπορεί να ενημερώνει από απόσταση για το ποιος είναι και αν διαθέτει το απαιτούμενο βαλάντιο ώστε να γίνεται αποδεκτή ή όχι η συναλλαγή που επιθυμεί.

Η πρώτη υλοποίηση αυτής της τεχνολογίας στις κάρτες έγινε το 1994 από μια εταιρεία ονόματι Mikron, υπό το όνομα MIFARE Classic. Η Mikron εξαγοράστηκε το 1998 από τη Philips, η οποία μετεξέλιξε την τεχνολογία στην επανομαζόμενη DESFire MF3ICD40 και μετέτρεψε τον κλάδο παραγωγής της σε αυτόνομη εταιρεία ονόματι NXP. Η NXP κατόρθωσε να πείσει τόσο κυβερνητικές υπηρεσίες (όπως η Υπηρεσία Εσωτερικής Ασφάλειας των ΗΠΑ) όσο και συγκοινωνιακά μέσα (όπως τα περισσότερα μετρό σε Ευρώπη και Ασία) να μπολιάσουν τις κάρτες διόδου που παρείχαν στο κοινό τους με τέτοια ασύρματα επικοινωνία. Τη σκυτάλη παρέλαβαν στη συνέχεια οι γνωστές εκδότριες καρτών VISA και MasterCard, που από το 2007 προωθούν τέτοιες κάρτες υπό τις εμπορικές επωνυμίες Visa payWave και MasterCard PayPass. Ήδη υπολογίζεται ότι έχουν διατεθεί πάνω από τρία δισεκατομμύρια τέτοιες κάρτες με RFID διεθνώς. Σε αυτές θα πρέπει να προσθέσει κανείς και τον αριθμό των βιομετρικών διαβατηρίων που επίσης ενσωματώνουν RFID.

Η τάση υιοθέτησης της ασύρματης συναλλαγής αναμένεται να γιγαντωθεί μέσω των... κινητών τηλεφώνων: βάζοντας ένα τέτοιο μικροκύκλωμα στο εσωτερικό των «έξυπνων τηλεφώνων» μπορεί ο κάθε χρήστης τους να κυκλοφορεί χωρίς καν ταυτότητα, χρήματα ή πιστωτικές κάρτες στην τσέπη του. Αρκεί να πλησιάσει το κινητό του στο ATM, την ετικέτα ενός μουσειακού εκθέματος, το μηχάνημα ακύρωσης του εισιτηρίου ή τον έλεγχο διαβατηρίων στο αεροδρόμιο, για να ταυτοποιηθεί, να διαβάσει την περιγραφή του εκθέματος, να προχωρήσει

σε συναλλαγή ή να του επιτραπεί η είσοδος αντίστοιχα. Τεχνολογικά η δυνατότητα αυτή έγινε εφικτή το 2002 χάρη σε μια ευρεσιτεχνία που ανέπτυξαν από κοινού η NXP και η Sony. Η πρώτη εφαρμογή της όμως ανακοινώθηκε στις 26 Μαΐου 2011 από την Google, η οποία την ενσωμάτωσε στο κινητό της Google Nexus S συνεργαζόμενη με τη MasterCard PayPass.

Η τεχνολογία επιτρέπει πλέον τη διέλευσή μας ή τη συναλλαγή ασύρματα, αλλά είναι ασφαλής;

Πώς δούλεψαν οι «χάκερς»

Οι προοπτικές λοιπόν εμφανίζονται ρόδινες για τους «νομάδες» της ψηφιακής εποχής μας και ακόμη πιο ρόδινες για τους παρόχους της εν λόγω τεχνολογίας και τους εκδότες πιστωτικών καρτών. Από το 2008 όμως άρχισαν να εκφράζονται αμφιβολίες για το απαραβίαστο αυτής της τεχνολογίας, αμφιβολίες που πρόσφατα αποδείχθηκαν επιστημονικά: στις 3 Νοεμβρίου 2011 ο καθηγητής Christof Paar, του γερμανικού πανεπιστημίου Ruhr-Bochum, ανακοίνωσε πως η ομάδα του μπόρεσε να εκμαιεύσει τον πλήρη κλειδάριθμο 112 ψηφίων κάρτας τύπου Mifare DESFire MF3ICD40 σε διάστημα τριών ως επτά ωρών. Η τεχνική που εφάρμοσε αυτή η ομάδα «επίσημων διαρρηκτών» έμοιαζε πολύ με εκείνη ενός γιατρού που μας ακούει με στηθοσκόπιο: «διάβασαν» την κατανάλωση ενέργειας του μικροκυκλώματος RFID της κάρτας και από τις διαταραχές του ηλεκτρομαγνητικού πεδίου εξήγαγαν τα στοιχεία. Τα εργαλεία που χρησιμοποίησαν ήταν ένας αναγνώστης RFID (που πωλείται στο Διαδίκτυο έναντι 15 δολαρίων), μία ακκίδα μέτρησης πεδίου και ένας ταλαντογράφος. Με τα στοιχεία που συνέλεξαν ήταν σε θέση – αν ήθελαν – να αναπαραγάγουν άπειρες πλαστές κάρτες. Οπως δήλωσε ο καθηγητής Paar, ενημέρωσαν την κατασκευάστρια NXP, η οποία αποδέχθηκε την «τρύπα ασφαλείας» και σύστησε στους πελάτες της να αναβαθμίσουν τις κάρτες της με το νέο της μοντέλο κυκλώματος, το MIFARE DESFire EV1.

Τόσο απλά... Δισεκατομμύρια κάρτες και διαβατήρια στον κόσμο πρέπει να αλλαχτούν, γιατί όλα ήταν μια «τεχνολογική φούσκα». Και ώσπου να γίνει η αλλαγή, τι κάνουμε; Εντάξει, εμείς στην Ελλάδα δεν έχουμε αρχίσει ακόμη να χρησιμοποιούμε ασύρματες κάρτες, αλλά τα διαβατήριά μας έχουν το παραβιάσιμο τσιπάκι!

Η λύση υπάρχει στην αγορά υπό τη μορφή «θήκης αποκοπής σήματος». Θα τη βρείτε στο Διαδίκτυο με τις λέξεις «secure sleeves» και κόστος από 15 ως 40 δολάρια. Αλλά και χωρίς να πληρώσετε σέντσι, μπορείτε να τυλίξετε το διαβατήριό σας ή την επόμενη κάρτα σας με ένα αλουμινόχαρτο. Αυτό αρκεί, εφόσον δεν τα αφήσετε στα χέρια άλλων για πάνω από τρεις ώρες.

