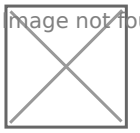
16 Ιουλίου 2016

Τι ανακάλυψαν οι ερευνητές Προσοχή! Το «έξυπνο» ρολόι μπορεί να… προδώσει το PIN σας στα ATM

/ Επιστήμες, Τέχνες & Πολιτισμός



Τη σχετική αποκάλυψη-προειδοποίηση έκαναν για πρώτη φορά ερευνητές από τις ΗΠΑ, οι οποίοι, συνδυάζοντας δεδομένα από τους ενσωματωμένους αισθητήρες σε αυτές τις «φορητές» συσκευές, κατάφεραν -με τη βοήθεια ενός υπολογιστικού αλγόριθμου- να «σπάσουν» τα passwords και τα PIN

Τα «έξυπνα» ρολόγια (smartwatches) και οι άλλες συσκευές που φοριούνται (wearables), όπως όσες καταγράφουν ζωτικούς δείκτες της φυσικής κατάστασης (fitness trackers), μπορούν να προδώσουν τους προσωπικούς κωδικούς των χρηστών, όπως στα ATM των τραπεζών.

Τη σχετική αποκάλυψη-προειδοποίηση έκαναν για πρώτη φορά ερευνητές από τις ΗΠΑ, οι οποίοι, συνδυάζοντας δεδομένα από τους ενσωματωμένους αισθητήρες σε αυτές τις «φορητές» συσκευές, κατάφεραν -με τη βοήθεια ενός υπολογιστικού αλγόριθμου- να «σπάσουν» τα passwords και τα PIN.

Οι ερευνητές πειραματίστηκαν με 20 εθελοντές που φορούσαν στο σώμα τους διάφορες συσκευές επί ένα έτος περίπου. Οι «καλοί» χάκερ της Σχολής Μηχανικών του Πανεπιστημίου Μπινγκχάμπτον και του Ινστιτούτου Τεχνολογίας Στίβενς, είχαν ποσοστό επιτυχίας 80% στην πρώτη προσπάθειά τους, ενώ μετά από τρεις προσπάθειες η ακρίβεια στην κλοπή των κωδικών είχε ξεπεράσει το 90%.

«Οι φορητές συσκευές μπορούν να πέσουν θύμα χάκερ. Οι επιτιθέμενοι είναι δυνατό να αναπαράγουν τις κινήσεις του χεριού του χρήστη και έτσι να υποκλέψουν τους μυστικούς κωδικούς για τα ATM, τις ηλεκτρονικές κλειδαριές θυρών κ.α.», δήλωσε ο επίκουρος καθηγητής επιστήμης των υπολογιστών Γιαν Γουάνγκ και τόνισε ότι «η απειλή είναι πραγματική».

Η υποκλοπή θα μπορούσε να γίνει με «δούρειο ίππο» την εισαγωγή από τους

πραγματικούς χάκερ του κατάλληλου κακόβουλου λογισμικού (malware) μέσα στο smartwatch ή σε άλλη φορετή συσκευή, ώστε να παρακολουθεί πλέον κρυφά τις καταγραφές των ενσωματωμένων ηλεκτρονικών αισθητήρων (επιταχυνσιόμετρου, γυροσκόπιου, μαγνητόμετρου κ.α.).

Έτσι, όταν ο χρήστης πληκτρολογεί τον κωδικό του σε ένα ATM και την ίδια ώρα φορά το «έξυπνο» ρολόι του που διαθέτει το κακόβουλο λογισμικό, το τελευταίο εν αγνοία του στέλνει στους χάκερ τα δεδομένα για τις κινήσεις του χεριού του χρήστη. Με τη βοήθεια ενός άλλου λογισμικού (αλγόριθμου), που διαθέτει ο χάκερ στον υπολογιστή του, είναι σε θέση να μαντέψει τι πληκτρολόγησε ο χρήστης στο ATM, στην ηλεκτρονική κλειδαριά του σπιτιού και του χρηματοκιβωτίου του ή σε όποιο άλλο σύστημα ασφαλείας χρειάζεται η εισαγωγή κωδικού με το χέρι.

Εναλλακτικά, αντί για την εισαγωγή κακόβουλου λογισμικού-δούρειου ίππου στη συσκευή του χρήστη, ο χάκερ μπορεί να τοποθετήσει μια ασύρματη συσκευή υποκλοπής κοντά στο ATM ή όπου αλλού, έτσι ώστε να «κρυφακούει» τα δεδομένα των αισθητήρων, τα οποία στέλνει μέσω Bluetooth το «έξυπνο» ρολόι ή το fitness tracker του χρήστη στο συνδεδεμένο «έξυπνο» κινητό τηλέφωνό (smartphone) του θύματος.

Οι ερευνητές επεσήμαναν ότι επειδή οι φορητές συσκευές έχουν μικρό μέγεθος και σχετικά περιορισμένων δυνατοτήτων επεξεργαστή, δεν είναι δυνατό να εφοδιασθούν με εξελιγμένο σύστημα κυβερνο-ασφάλειας, πράγμα που τις καθιστά πιο ευάλωτες σε χάκερ.

Προς το παρόν, η λύση που προτείνεται στους κατασκευαστές είναι να εισάγουν τεχνηέντως ένα συγκεκριμένο «θόρυβο» στα δεδομένα των αισθητήρων, ώστε να είναι πιο δύσκολο για τους χάκερ να συμπεράνουν τις συγκεκριμένες κινήσεις του χεριού του χρήστη. Στην πορεία όμως, αυτό που πρέπει να γίνει, είναι να δημιουργηθούν καλύτερα συστήματα κρυπτογράφησης στη φορητή συσκευή.

Πηγή: protothema.gr