11 Οκτωβρίου 2014

Η πιθανή απειλή του «χακαρίσματος» συσκευών μέσω… φωνής

/ Επιστήμες, Τέχνες & Πολιτισμός

Τον κίνδυνο που συνιστά η διεύρυνση της χρήσης τεχνολογιών ενεργοποίησης μέσω φωνής οι οποίες μπορεί να μην είναι τόσο ασφαλείς επισημαίνει ερευνητής της AVG σε ανάρτησή του στο blog της εταιρείας.

Όπως αναφέρει ο Γιουβάλ Μπεν- Ιτζάκ, chief technology officer της εταιρείας, σε κείμενο υπό τον τίτλο «What if smart devices could be hacked with just a voice?», η άνοδος των smartphones και των wearables έφερε επανάσταση στον τρόπο αλληλεπίδρασης μεταξύ ανθρώπων και υπολογιστών, καθώς μειώθηκε σημαντικά η ανάγκη χρήσης περιφερειακών όπως το πληκτρολόγιο και το ποντίκι – που, επί της προκειμένης, αντικαθίστανται από τα χέρια ή ακόμη και τις φωνές.

Αυτό με τη σειρά του, συμπληρώνει, έφερε την έλευση του ενεργοποιούμενου μέσω φωνής personal assistant. «Καθώς ενεργοποιούνται απλά από τις φωνές μας, υπόσχονται να μας βοηθήσουν σε βασικές εργασίες με hands-free τρόπο. Τόσο η Apple όσο και η Google πρόσθεσαν τεχνολογίες αναγνώρισης φωνής στις ‘έξυπνες’ συσκευές τους. Το Siri και το Google Now αποτελούν όντως personal assistants για την καθημερινή ζωή μας. Τόσο το Siri όσο και το Google Now μπορούν να

καταγράψουν τη φωνή μας, να τη μεταφράζουν σε κείμενο και να εκτελούν συσκευές στη συσκευή μας…ωστόσο αυτές οι τεχνολογίες αναγνώρισης φωνής – οι οποίες είναι τόσο απαραίτητες στις ‘έξυπνες’ συσκευές- ίσως να μην είναι τόσο ασφαλείς όσο τις θεωρούμε. Σε τελική ανάλυση, δεν είναι ρυθμισμένες για τις συγκεκριμένες μας φωνές. Ο καθένας μπορεί να ζητήσει από το Google Now να πραγματοποιήσει μια κλήση ή να στείλει ένα μήνυμα κειμένου και αυτό θα υπακούσει- ακόμα και αν δεν είναι η φωνή σας που το ζητάει».

Το ερώτημα το οποίο θέτει ο Μπεν-Ιτζάκ είναι το εάν μια συσκευή είναι «τρωτή» σε φωνητικές εντολές από κάποιον άλλον. «Οι over-the-air επιθέσεις σε τεχνολογίες αναγνώρισης φωνής είναι πραγματικότητα, και δεν περιορίζονται μόνο στα smartphones. Οι τεχνολογίες ενεργοποίησης μέσω φωνής έρχονται επίσης σε ‘έξυπνες’ διασυνδεδεμένες συσκευές στο σπίτι, όπως η smart TV».

Σε βίντεο που ανέβασε στο YouTube, ο ερευνητής της AVG επιδεικνύει ότι οι «έξυπνες» συσκευές στο σπίτι του ανταποκρίνονται στη φωνή του- ωστόσο ανταποκρίνονται και σε οποιαδήποτε φωνητική εντολή, «ακόμα και μία που έχει συντεθεί από μία άλλη συσκευή στο σπίτι μου». Συνεχίζοντας, υπογραμμίζει την ανάγκη για πρόοδο στον τομέα της ταυτοποίησης της πηγής της φωνής, θέτοντας και το ζήτημα της πρόσβασης παιδιών σε ακατάλληλο υλικό εάν μια συσκευή δεν μπορεί να «καταλάβει» εάν μιλά το παιδί ή ο γονιός του. Παράλληλα, επισημαίνει ότι νέες «έξυπνες» συσκευές εμφανίζονται καθημερινά, στο πλαίσιο της «έκρηξης» του «Internet of Things». «Μπορεί να μην είναι πρόβλημα η αλλαγή σταθμού στην τηλεόρασή μου, αλλά η δυνατότητα για εντολές σε διασυνδεδεμένα οικιακά συστήματα ασφαλείας, smart home assistance, οχήματα και διασυνδεδεμένους χώρους εργασίας δεν είναι πολύ μακριά. Η αξιοποίηση της τεχνολογίας ενεργοποίησης μέσω φωνής στο Internet of Things χωρίς ταυτοποίηση της πηγής της φωνής είναι σαν να αφήνεις τον υπολογιστή σου χωρίς κωδικό- ο καθένας μπορεί να τον χρησιμοποιήσει και να δώσει εντολές» σημειώνει.

Κλείνοντας, ο Μπεν-Ιτζάκ διευκρινίζει ότι μέχρι τώρα δεν έχουν βρεθεί «ελεύθερα» δείγματα malware που εκμεταλλεύονται αυτή την «αχίλλειο πτέρνα», ωστόσο προσθέτει ότι «πρόκειται για έναν προβληματισμό που οι κατασκευαστές συσκευών και οι developers λειτουργικών συστημάτων θα έπρεπε να λάβουν υπόψιν στα σχέδιά τους για το μέλλον. Όπως συμβαίνει συχνά με την τεχνολογία, η άνεση μπορεί να έρχεται με κινδύνους για την ιδιωτικότητα ή την ασφάλεια- και φαίνεται ότι η ενεργοποίηση μέσω φωνής δεν διαφέρει».

Πηγή: naftemporiki.gr