9 Ιανουαρίου 2016

Οι κίνδυνοι του Mobile Banking

/ Πεμπτουσία

Image not found or type unknown

Κατά τη διάρκεια των τριών τελευταίων ετών, ο ερευνητής ασφαλείας Ariel Sanchez από την IOActive, πραγματοποιεί ελέγχους στις Mobile Banking εφαρμογές που έχουν σχεδιαστεί για συσκευές με iOS, αναδεικνύοντας μια σειρά από ζητήματα που σχετίζονται με την ασφάλεια.

Η έρευνά του εστιάζει στην αναζήτηση cleartext traffic, μη σωστά επικυρωμένων πιστοποιητικών SSL, λανθασμένου ή ανεπαρκούς χειρισμού συνεδριών (sessions), ελέγχους σχετικά με την ασφάλεια του compiler, θέματα UIWebViews, προβληματικά logging, ανάλυση δυαδικών αρχείων, και αναζήτηση για μη ασφαλείς πρακτικές αποθήκευσης δεδομένων.

Σύμφωνα με την πιο πρόσφατη έρευνα του, από τις 40 iOS Mobile Banking

εφαρμογές που εξετάστηκαν, το 12,5% δεν επικυρώνουν τα πιστοποιητικά SSL πριν από την έναρξη των συνδέσεων HTTPS, αφήνοντας τους χρήστες εκτεθειμένους σε MITM (Man-in-the-middle) επιθέσεις. Επιπλέον, το 35% των εφαρμογών περιλαμβάνουν links στο περιεχόμενό τους που δεν καλούνται μέσω HTTPS, εκθέτοντας τους χρήστες σε αυθαίρετη έκχυση HTML ή/και JavaScript κώδικα. Τέλος το 30% των εφαρμογών δεν επικυρώνει τα εισερχόμενα δεδομένα, πράγμα που σημαίνει ότι οι επιτιθέμενοι μπορούν να στείλουν ψεύτικο κώδικα JavaScript και να επιτεθούν στον χρήστη μέσω του συστατικού UIWebView.

Τα καλά νέα είναι ότι οι περισσότερες εφαρμογές (40%) έχουν αρχίσει να παρέχουν εναλλακτικές λύσεις ελέγχου ταυτότητας χρήστη. Τα κακά νέα είναι ότι το 42,5% από τις εφαρμογές εκθέτουν επίσης κάποιου είδους προσωπικές πληροφορίες μέσω των system ή custom logs.

Προχωρώντας σε ανάλυση των binarys και των filesystems, ο ερευνητές ανακάλυψε επίσης ότι το 7,5% των apps δεν διαθέτει ακόμα κάποιου είδους compiler protection, επιτρέποντας στους επιτιθέμενους να κάνουν εύκολα decompile και να αποκτήσουν πρόσβαση στον κώδικα τους. 15% από τις εφαρμογές έχουν προστασία για jailbreak, ενώ το 17,5% από τις εφαρμογές αποθηκεύουν κάποια μόνιμη πληροφορία στα δυαδικά τους αρχεία.

Επιπλέον, ο κ Sanchez ανακάλυψε ότι το 15% των εφαρμογών εξακολουθεί να αποθηκεύει μη κρυπτογραφημένες ή / και ευαίσθητες πληροφορίες στο τηλέφωνο, είτε σε κάποια βάση δεδομένων SQLite, είτε ως απλό plaintext αρχείο.

Παρόλο που τα παραπάνω στατιστικά έχουν σημειώνουν πτώση σε σύγκριση με το 2013, εξακολουθούν να μην είναι ικανοποιητικά σε λαμβάνοντας υπόψη το πλήθος των αποτελεσματικών τεχνικών κωδικοποίησης και ασφάλειας που έχουν κυκλοφορήσει αυτά τα χρόνια για τους iOS προγραμματιστές.

«Ενώ η συνολική ασφάλεια έχει αυξηθεί κατά τη διάρκεια των δύο ετών, δεν είναι αρκετό, και πολλές εφαρμογές παραμένουν ευάλωτες,» καταλήγει ο ερευνητής.

Πηγή: secnews.gr