ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Μουστάκας Σεραφείμ
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Επόπτης Μεταπτυχιακής Εργασίας: Καθηγητής, Ε. Μαρκάτος

Παρασκευή, 19 Μαρτίου 2021 , ώρα 15:00 μ.μ.

Join Zoom Meeting

https://zoom.us/j/99219940514

"This Greedy Piggy Went to the Ad Market: Stealing Users' (Input) Data using Mobile Sensors"

Περίληψη

Οι ενσωματωμένοι σένσορες στα κινητά τηλέφωνα έχουν ένα πολύ σημαντικό ρόλο στην συμπόρευση ανθρώπου-υπολογιστή, ενισχύοντας και αλλάζοντας ριζικά την εμπειρία του χρήστη. Ωστόσο, η κακή χρήση τους σε συνδυασμό με την απουσία επαρκών μηχανισμών ελέγχου πρόσβασης παρουσιάζουν μια πληθώρα κινδύνων προσωπικού απορρήτου και ασφάλειας. Όπως έχει ήδη αποδειχθεί, υπάρχει ένα ευρύ φάσμα από επιθέσεις σε κινητές συσκευές χρησιμοποιώντας τα "πλούσια" δεδομένα από τους ενσωματωμένους σένσορες. Ενώ σε προηγούμενες έρευνες αυτές οι επιθέσεις χρειάζονταν μια κακόβουλη εφαρμογή εγκατεστημένη στην συσκευή ή την επίσκεψη μιας κακόβουλης ιστοσελίδας, παρατηρήσαμε ότι υπάρχει μια διαφορετική, πιο αθόρυβη προσέγγιση που επηρεάζει όλους τους Android χρήστες χωρίς καμία προϋπόθεση.

Σε αυτή την εργασία παρουσιάζουμε ένα εναλλακτικό κανάλι επίθεσης, που χρησιμοποιεί το οικοσύστημα της διαφήμισης για να παραδώσει ένα μεγάλο πλήθος από διαφορετικές επιθέσεις χρησιμοποιώντας σένσορες σε κινητά τηλέφωνα. Το συγκεκριμένο μοντέλο απειλής δεν βασίζεται σε συγκεκριμένες "άδειες" εφαρμογών και επηρεάζει όλες τις Android εφαρμογές που δείχνουν διαφημίσεις λόγω του ακατάλληλου μηχανισμού πρόσβασης στους σένσορες. Αναλύουμε τον τρόπο με τον οποίο οι σένσορες κίνησης μπορούν να αποκαλύψουν προσωπικούς κωδικούς και πληροφορίες για την πιστωτική κάρτα σε δύο διαφορετικά σενάρια. Το πρώτο στοχεύει να αποσπάσει πληροφορίες από την εφαρμογή που προβάλει τις διαφημίσεις ενώ το δεύτερο στοχεύει όλες τις εφαρμογές που είναι εγκατεστημένες στο κινητό ενός χρήστη. Το συγκεκριμένο μοντέλο επίθεσης μεγαλώνει καθώς οι ενσωματωμένες διαφημίσεις στις εφαρμογές μπορούν να χρησιμοποιήσουν και άλλους σένσορες όπως την κάμερα, το μικρόφωνο και το GPS αν η εφαρμογή διαθέτει την κατάλληλη "άδεια".
Αξιολογούμε την συγκεκριμένη απειλή, διεξάγοντας μια μεγάλη έρευνα στις διαφημίσεις που προβάλλονται από τις εφαρμογές του Google Play. Τα αποτελέσματά μας δείχνουν ότι οι διαφημίσεις παίρνουν πρόσβαση στους σένσορες κίνησης και διαρρέουν τα αντίστοιχα δεδομένα χωρίς καμία συναίνεση από τον χρήστη. Η έρευνά μας αποδεικνύει την επιτακτική ανάγκη ενός αυστηρού μηχανισμού ελέγχου πρόσβασης στους σένσορες των κινητών συσκευών για την προστασία των χρηστών και του οικοσυστήματος της διαφήμισης.

University of Crete

Computer Science Department

M.Sc. Thesis presentation / examination

Moustakas Serafim

Master's Thesis Supervisor: Professor, E. Markatos

Friday, 29 March 2021, 15:00 p.m.

Join Zoom Meeting

https://zoom.us/j/99219940514

“This Greedy Piggy Went to the Ad Market: Stealing Users' (Input) Data using Mobile Sensors”

Abstract

Mobile sensors in modern smartphones play a crucial role in the human-computer confluence by enhancing and transforming the user experience. However, misuse of mobile sensors combined with the absence of sufficient access control mechanisms introduce a plethora of privacy and security risks. As previously demonstrated, there is a wide range of sensor-based attacks using the rich data captured from mobile sensors and while previous attack paths depended on specific requirements such as malware or visiting a webpage; we found that an alternative and stealthier approach exists and affects all Android users without any requirements.

In this thesis we introduce a novel attack channel, that abuses the advertising ecosystem for delivering a variety of sophisticated and sneaky attacks using mobile sensors. The proposed threat-model does not depend on app permissions or user specific actions and affects all Android apps that contain in-app advertisements due to improper access control for sensor data in WebViews. We explain how motion sensor data can be used to infer user’s sensitive touch input (pin, password, credit card info, etc.) in two distinct attacks scenarios, namely intra and inter-app data exfiltration. The former targets information obtained from the app that display the in-app ads, while the latter targets every other Android app installed on the device. Unfortunately, as in-app ads have the ability to "piggyback" on the permissions obtained for the app’s core functionality they can also obtain information from other sensors such as the camera, the microphone and the GPS.

To provide a comprehensive assessment of this emerging threat, we conduct a large-scale, end-to-end, dynamic analysis of in-app ads that access mobile sensors in applications found in Google Play. We find that in-app ads access and leak data obtained from motion sensors in the wild and emphasize the need for a strict access control policy that should be adopted and standardized to better protect users and the advertising ecosystem.