ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Παπαδόπουλος Παναγιώτης - Ηλίας
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Καθηγητής, Ε. Μαρκάτος

Τρίτη, 20/02/2018, 14:00
Αίθουσα Β108,Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

" Εντοπισμός, Ανάλυση και Άμυνα Εναντίων Βιβλιοθηκών Ταυτοποίησης Χρηστών σε Φορητές Συσκευές: *Ιστοσελίδες εναντίον Εφαρμογών* "

ΠΕΡΙΛΗΨΗ

Στις μέρες μας, η συντριπτική πλειοψηφία των διαδικτυακών υπηρεσιών παρέχουν ιστοσελίδες και εφαρμογές, σχεδιασμένες για φορητές συσκευές (κινητά τηλέφωνα και τάμπλετ). Οι δύο αυτές επιλογές συνήθως διατίθενται δωρεάν, ενώ τα έσοδά των προγραμματιστών τους προέρχονται κυρίως από διαφημίσεις οι οποίες ενσωματώνουν το δικό τους περιεχόμενο. Προκειμένου να παρέχουν πιο εξατομικευμένες και αποτελεσματικές διαφημίσεις, οι διαφημιστικές εταιρίες, αναπτύσσουν τεχνικές παρακολούθησης και ταυτοποίησης χρηστών, προκαλώντας έτσι σημαντικές ανησυχίες σχετικά με την παραβίαση της ιδιωτικότητάς τους. Συνεπώς, οι χρήστες δεν πρέπει να ενδιαφέρονται μόνο για την ευκολία χρήσης μιας διαδικτυακής υπηρεσίας αλλά και για την λιγότερο δυνατή παραβίαση της ιδιωτικότητάς τους.

Στόχος αυτής της μεταπτυχιακής εργασίας είναι να απαντήσουμε στην ερώτηση *ποια από τις δύο επιλογές προστατεύουν καλύτερα την ιδιωτικότητα του χρήστη, οι*

ιστοσελίδες ή οι εφαρμογές; Για την αντιμετώπιση αυτού του ζητήματος, μελετήσαμε ένα ευρύ φάσμα διαρροών που σχετίζονται με την προστασία της ιδιωτικότητας του χρήστη, συγκρίνοντας πολλές δημοφιλείς εφαρμογές κινητών και του αντίστοιχου ιστότοπού τους. Αυτές οι διαρροές μπορεί να περιέχουν όχι μόνο προσωπικές πληροφορίες ταυτοποίησης (PII) του χρήστη, αλλά και πληροφορίες για την συσκευή που είναι ικανές να επιτρέψουν την αναγνώριση του χρήστη όταν χρησιμοποιεί διαφορετικές εφαρμογές και ιστοτόπους.

Τέλος, προτείνουμε έναν μηχανισμό προστασίας που επιτρέπει την χρήση εφαρμογών για κινητά, χωρίς να διακινδυνεύει την παραβίαση της ιδιωτικότητας των χρηστών. Η αξιολόγηση των αποτελεσμάτων δείχνει ότι η προσέγγισή μας είναι σε θέση να διασφαλίσει την ιδιωτικότητα του χρήστη μειώνοντας τα διαρρέοντα αναγνωριστικά των εφαρμογών σε ποσοστό 27,41%, κατά μέσο όρο, ενώ προσθέτει σχεδόν αμελητέα καθυστέρηση, μικρότερη από 1 χιλιοστό του δευτερολέπτου ανά αίτηση.

Papadopoulos Panagiotis- Ilias
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Professor E. Markatos

Tuesday, 20/02/2018, 14:00
Room B108, Computer Science Dept., University of Crete

"Detection, Measurement and Defense Against Third-party Trackers on Mobile Devices: *Mobile Websites vs Mobile Apps*"

ABSTRACT

The vast majority of online services nowadays, provide both a mobile-friendly website and a mobile application to their users. Both of these choices are usually released for free, with their developers mostly gaining revenue by allowing advertisements from ad networks to be embedded into their content. In order to provide more personalized and thus more effective advertisements, ad networks usually deploy pervasive user tracking,

raising this way significant privacy concerns. As a consequence, the users do not have to think only their convenience before deciding which choice to use while accessing a service: web or app, but also which one harms their privacy the least.

In this master thesis, we aim to respond to this question: which of the two options protects the users' privacy in the best way, websites or apps? To tackle this question, we study a broad range of privacy related leaks comparing several popular apps with their web counterpart. These leaks may contain not only personally identifying information (PII) but also device-specific information, able to cross-application and cross-site track the user into the network, and allow third parties to link web with app sessions.

Finally, we propose an anti-tracking mechanism that enables the users to access an online service through a mobile app without risking their privacy. Our evaluation shows that our approach is able to preserve user privacy by reducing the leaking identifiers of apps by 27.41%, on average, while it introduces a practically negligible latency of less than 1 millisecond per request.