Toward Proactive Mobile Tracking Management

Hella Kaffel Ben Ayed, National School of Computer Science, University of Manouba, Manouba, Tunisia

Asma Hamed, National School of Computer Science, University of Manouba, Manouba, Tunisia

ABSTRACT

This paper presents an experimental study on mobile Web and mobile applications tracking. The study on Mobile Web tracking has been conducted on datasets collected by TrackScoreMobile, a Firefox add-on that has been developed and distributed to a set of Tunisian students and researchers. Results identify the factors that increase the privacy risk. The study on mobile applications tracking focuses on the permissions required by android applications. The findings point out on the mostly required permissions and the mostly tracked application categories. The originality of this work is summarized as follows: 1) identification and measurement of the parameters to quantify Web tracking, 2) identification of risky association between mobile applications permissions and associations between permissions and tracking components. The goal of this paper is to better understand how trackers rely on tracking components and on permissions for the purpose of tracking mobile users.

Keywords: Mobile Applications, Permissions, Privacy, Tracking, Tracking Components

INTRODUCTION

Pervasive Web has to cope with privacy threats resulting from Web tracking and from tracking performed by mobile applications as well. Mobile Web tracking is implemented using various tracking components which permit users’ identification, observation, monitoring as well as the leakage of their browsing activities and personal information to third parties. Tracking on mobile devices is also made possible to mobile applications using permissions granted by the users during the installation of the application. These permissions allow the applications to access the mobile device resources such as the Internet access, the device ID, and users’ accounts. Mobile Web and mobile applications tracking raises a privacy concern if data related to users’ activities and personal information is revealed to third parties without their awareness and consent. This constitutes an issue to informational privacy.

Researchers conducted various studies to measure mobile Web tracking and in-applications tracking as well (Liu & Terzi, 2010). Some studies stressed the risk of privacy violations resulting from Web tracking (Krishnamurthy & Willis, 2009a, 2009b). Others developed tools to quantify
tracking over mobile devices (Self-destructing cookies, 2013; Vold, 2013). However, to the best of our knowledge there is no approach that addresses users’ awareness and privacy scoring proactively by identifying the risk just when tracking elements are detected.

This paper addresses the privacy issue from users’ perspective in a proactive manner, i.e. before the leakage occurs. The goal of the present work is to go toward risk identification and estimation. In a first step, the focus is made on mobile Web tracking. An intuitive privacy scoring model is proposed to measure the users’ privacy risk due to the presence of tracking components in the visited Webpages. An experimental study permits to collect and analyze datasets focusing on various tracking parameters. The datasets have been collected via a new android Firefox add-on that has been distributed to Tunisian volunteers (students and researchers). The add-on computes the privacy score and alerts users about the risk of personal information disclosure.

In a second step, the present study addresses tracking by mobile apps via the permissions granted by users. The study focuses first on the permission distribution considering different Website categories. Potential correlations and associations between the permission required by applications are identified. The possible associations’ rules between the tracking components used by websites and the permissions required by their mobile application are also identified.

LITERATURE REVIEW

In this section, related works on Web tracking are presented first. Second, related works on mobile apps tracking are depicted.

Related Work on Web Tracking

Various browsers add-ons have been developed to reduce privacy-violating information flows on the Web. Self-Destructing Cookies is a Firefox add-on which detects and removes cookies (Self-destructing cookies, 2013). No Google Analytics is also a Firefox add-on that implements a content policy which blocks all network requests from Googleanalytics.com; such as JavaScript and gif images (Self-destructing cookies, 2013; Vold, 2013). Ghostery detects and blocks trackers (Signanini & Shnir, 2013). Similarly, Privacy Defense permits trackers detection based on their signatures (Privacy defense, 2013). Privacyscore detects trackers present in the visited Websites (Waugh, 2012). Lightbeam creates a real-time graph of all tracking cookies stored on users’ browser as they move around the Web. One of the inconveniences of lightbeam is that after visiting about four or five sites, the graph tends to get really confusing (Fowler, 2013).

Experimental studies addressed the issue related to third party trackers. The study in (Krishnamurthy & Willis, 2009a) explores more than 1200 popular Websites. It shows that the penetration of the top-10 third-party tracking servers viewing user habits has increased from 40% in Oct’05 to 70% in Sep’08. The same authors demonstrate in another work (Krishnamurthy & Wills, 2009b) that personally identifiable information belonging to any user, such as name, gender or OSN (Online Social Network) unique ID, are leaked to third-party servers via the OSN. Thus, besides viewing the surfing habit of users, third parties potentially gather much more personal information. The work in (Roesner, Kohno, & Wetherall, 2012) shows that the most commercial Webpages are tracked by multiple parties. Trackers vary widely in their coverage with a small number being largely deployed. Other trackers rely on combinations of tracking behaviors. Web search traces taken from AOL data show that each tracker can capture more than 20% of a user’s browsing behavior. A study of the tracking in the most popular Websites through different countries highlights the dominance of US trackers in China and Europe while in Russia, the dominance of local trackers is observed (Castelluccia, Grumbach, & Olejnik, 2013).
Critical Video Surveillance and Identification of Human Behavior Analysis of ATM Security Systems

Cybersecurity and Data Breaches at Schools
www.igi-global.com/chapter/cybersecurity-and-data-breaches-at-schools/173132?camid=4v1a