University of Hamburg
Department of Computer Science

Exposé

Implementing browser fingerprinting recognition using OpenWPM

Tronje Krabbe

July 4, 2017

This is an overview of the author's thesis. It describes the user identification and tracking technique 'browser fingerprinting', and explores the detection possibilities of wether it is employed by a website or not.

Contents

1 Introduction **4**

1.0.1 Leading Question and Goals 4

1.0.2 Methods and Approach 4

2 Implementation **5**

2.0.1 Technology 5

1 Introduction

When browsing the web, users can be tracked through the use of cookies, which store information on the user's computer. If the user wishes not to be trackable, they can modify or delete any cookie as they see fit. This interaction gives operators of websites the ability to track users only if they wish to be tracked. There are, however, other methods of uniquely identifying a user and tracking them during their use of the internet, which is not as easily mitigated as a cookie.[1] On of these methods is called 'browser fingerprinting', and it will be the focus of this thesis.

Tracking a user does not simply mean recognizing wether a visitor to one's website is a new or an existing user. Identifying information can be passed on or sold to partners, advertisers, or even governments, in order to construct a rich browsing history of a user.

Browser fingerprinting, also known as device fingerprinting, works by analyzing a web browser's configuration and settings, such as installed fonts, language settings, time zone settings, installed add-ons, to name a few.[3]

1.0.1 Leading Question and Goals

The thesis presents the assertion that techniques to identify and track users across different websites without their knowledge or their ability to easily intervene, violates their privacy. The author will therefore attempt to implement a technique to recognize when a website is deploying browser fingerprinting, and along the way explore the techniques used to do so. The ultimate goal is to integrate the implementation into `https://privacyscore.org`, a web-service to test and rank websites according to the extent to which they respect their users' privacy.

1.0.2 Methods and Approach

TODO

2 Implementation

TODO

2.0.1 Technology

TODO

OpenWPM

“OpenWPM is a web privacy measurement framework which makes it easy to collect data for privacy studies on a scale of thousands to millions of site”[1]. The author is planning to build upon OpenWPM to create a software that can detect browser fingerprinting.[2]

[1] `https://github.com/citp/OpenWPM`

Bibliography

[1] *Am I Unique?* URL: https://amiunique.org/ (visited on July 4, 2017).

[2] Steven Englehardt and Arvind Narayanan. “Online tracking: A 1-million-site measurement and analysis”. In: *Proceedings of ACM CCS 2016*. 2016.

[3] Electronic Frontier Foundation. *Panopticlick*. URL: https://panopticlick.eff.org/ (visited on July 4, 2017).