Abstract

In the recent years, obtaining data about users and their online devices to track their activities and find out about their interests has become standard practice. While browser cookies have been state-of-the-art for user tracking a long time, a new technique evolved and is more and more applied in practice: digital fingerprinting. In contrast to cookies, fingerprinting a digital system reveals information about the system itself. It is possible to learn a systems software or hardware configuration with this technique. Still, it remained unclear to what extent fingerprinting can be utilized and also what risks and opportunities the use of fingerprinting entails.

In the past, there has been researching mostly about fingerprinting a system’s browser—so-called browser fingerprinting. Transferring such methods to fingerprinting whole digital systems may be achieved in different ways and has to be fitted to the exact scenario, including the types of systems like mobile devices, the data available, e.g., browser attributes or hardware measurements, and the overall goal—for instance recognizing a single device among others. Hence, differentiated approaches and determining suitable methods are required to make fingerprinting feasible.

This thesis emphasizes two key aspects: First, we explore the feasibility of fingerprinting in various scenarios, e.g., browser fingerprinting in a Web context or system-based hardware fingerprinting, to investigate which goals can be achieved by this technique. Second, we investigate the impact of fingerprinting, including the risks for user privacy and the chances to enhance existing security mechanisms. In this work, we shift to fingerprinting not only a browser but complete systems by determining the general feasibility of fingerprinting mobile devices, like smartphones and tablets, and also the possibilities to elude fingerprinting methods. Fingerprinting mobile devices is deemed to be hard as these are highly standardized in contrast to desktop computers or browsers and, as a general rule, fingerprinting is less effective in a uniform group of devices. While some methods of browser fingerprinting can be instrumented for fingerprinting mobile devices as well, also new approaches can be developed since modern devices are more complex systems and, for instance, include hardware sensors. Hence, we also examine the feasibility of fingerprinting system hardware, e.g., a mobile device’s sensors and investigate whether or not it is possible to recognize devices just by hardware imperfections of these sensors. We also study whether or not differences in digital fingerprints may lead to triggering online marketing policies. In the media, there have been articles over the past years, claiming that users of specific computer systems experience price differentiation. Since such behavior may be based on digital system fingerprinting, we shed light on the impact of various fingerprints on online pricing. Finally, we take fingerprinting beyond digital systems and analyze whether writing styles may also be fingerprinted.
effectively as an example of the transferability of fingerprinting methods to other research areas.

Our findings reveal both the opportunities of digital fingerprinting as well as its limits. We present various applications for this new technique, investigating its power, risks, and chances.