Poster: Blink: A moving-target approach to fingerprint diversification

Pierre Laperdrix
INSA-Rennes & INRIA
Rennes, France
pierre.laperdrix@insa-rennes.fr

Walter Rudametkin
University of Lille & INRIA
Lille, France
walter.rudametkin@univ-lille1.fr

Benoit Baudry
INRIA
Rennes, France
benoit.baudry@inria.fr

***Abstract*—Browser fingerprinting has emerged in the past five years has a new method to track users on the web. With the incredible diversity of both software and hardware to browse the web, the smallest difference can be exploited to identify one device in a pool of thousands. We claim that this diversity which is the source of the fingerprinting problem is also its solution. We present Blink, a constantly changing platform that enables its users to stealthily browse the web while evading tracking through fingerprinting. By assembling different system layers at runtime, we create a disposable environment that breaks one fundamental property of browser fingerprinting: their stability over time.**

I. Introduction

The Internet has never been so rich and dynamic and browsers keep evolving to push the boundaries of what is possible online. An incredible diversity of operating systems and browsers exists to support the standards that is now powering the modern web and to offer the best experience possible to users. However, to support such powerful features, browsers have become a natural extension of the operating system on which they run. With a simple script, anyone can collect specific device information like the name of the browser and its version, the screen resolution, the list of plugins or the list of fonts. One of the downside of that diversity is that it created a privacy issue: browser fingerprinting. By collecting enough information, it has been shown that it is possible to uniquely identify a device [1] and it even gets easier as time goes by thanks to the inclusion of new powerful APIs in browsers [2] Studies also showed that fingerprinting is already used on the web by tracking companies alongside cookies to identify devices [3], [4].

With Blink, we use this incredible diversity to build the foundations for a counter measure to browser fingerprint tracking. We propose an original application of dynamic software reconfiguration techniques to establish a moving target defense that assembles components on-the-fly to exhibit an always-changing fingerprint to trackers online.

II. Approach

We propose to automatically reconfigure a users platform to exhibit different fingerprints over time that cannot easily be linked to one another. Figure 1 shows the elements of a browsing platform that affect the fingerprint: configuration data at different levels (HW, OS, browser); software components that are assembled at different levels (e.g., apt-get, browser plugins, fonts); hardware components, such as the graphics card; cross-level dynamic attributes collectable only at runtime, such as through the HTML5 canvas.

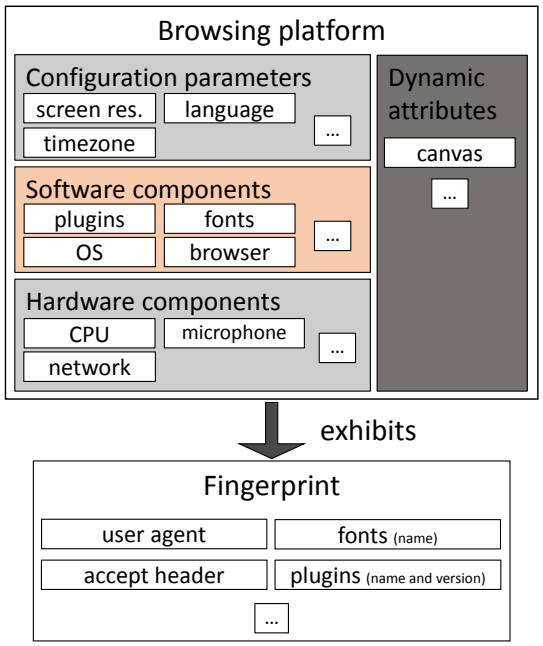

Fig. 1. User platform elements involved in web browsing and exhibited in the browser fingerprint

Once a user starts browsing the web, these data are used to create a fingerprint. We say that a platform exhibits said fingerprint. Our approach reconfigures components that affect the exhibited fingerprint. Studies on fingerprinting [1], [3] including our most recent one [2] found the most distinguishing attributes of a fingerprint to be fonts, plugins and user agents. For this reason, we decided to focus on the reconfiguration of the following elements: fonts, plugins, browsers and the operating system.

Our moving target defense relies on an essential characteristic needed for reconfiguration: the modular architecture of systems and browsers. Modularity makes it possible to reconfigure the browsing platform, on demand, by automatically assembling components. This also allows us to progressively assemble configurations instead of building them beforehand.

Our approach is characterized by three essential properties: (i) the assembled platforms always exhibit consistent fingerprints because the platforms are genuine and we do not lie about any attributes; (ii) we assemble correct platforms, i.e., platforms composed of compatible components and which run correctly; and (iii) each reconfiguration causes the exhibited fingerprints to change. This approach falls into the family of dynamic platforms, a specific form of moving target approaches, as described by Okhravi et al. in [5].

III. Implementation

Blink assembles components at multiple levels to form the browsing platform shown in Figure 2.

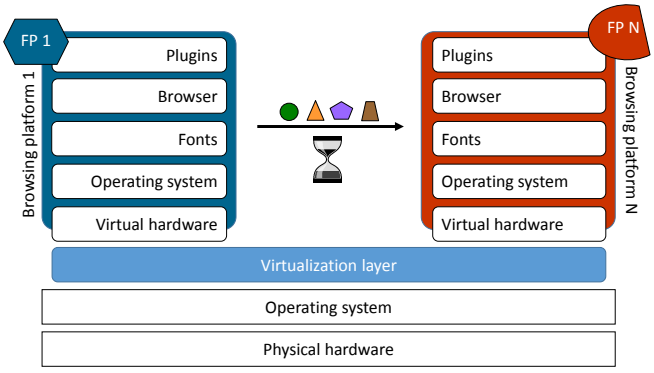

Fig. 2. A multi-level view of browsing platforms. Virtualization isolates the users system

Docker is the underlying technology behind Blink and it enables us to quickly assemble components at runtime while isolating the platform from the host system. With Blink, the components that we assemble are:

- Operating systems: Thanks to official images from DockerHub, numerous operating systems are available right out of the box and ready to be used.
- Browsers: Either downloaded directly from the web or from official package repositories, a wealth of browsers is available to exhibit diverse fingerprints.
- Fonts and plugins: We created a diversity reservoir in which Blink can pick its fonts and plugins when it creates a browsing platform. For the current version of Blink, the reservoir is composed of more than 2,700 fonts and more than 30 plugins.

In a matter of seconds, a web browser is opened with a completely new fingerprint and you can interact with it like a native browser.

In order to avoid creating artificial fingerprints that could not be found in the wild, we have created realistic profiles from the data that we collected on https://amiunique.org to bias the choice of elements when Blink assembles components. The result is that Blink creates platforms with fingerprints that could statistically be found on the Internet.

Assembling components at runtime only addresses the fingerprinting problem by breaking the fingerprint stability over time. Since other methods of tracking exist, what are the other techniques to guarantee stealth browsing? In order to prevent cookie tracing, all the temporary data that has been generated while browsing the web is removed when the user finishes his browsing session. To prevent IP tracing, Blink is fully compatible with the Tor network. With the click of a simple button, all the Internet traffic with Blink can be redirected through the Tor network.

Finally, to guarantee a comfortable browsing experience for users, we developed an offline cross-browser tool that is responsible for transferring essential user parameters between browsing platforms. These parameters include data such as bookmarks, open tabs or passwords and the advantage is that they have no impact on fingerprinting or tracking so they can easily be shared and transferred.

You can find the complete source code of Blink in the following repository https://github.com/plaperdr/blink-docker.

IV. Conclusion

This work explores the opportunity of exploiting automatic, multi-level reconfiguration and the natural diversity of software components in order to create a moving target defense against browser fingerprint tracking. We leverage virtualization and modular architectures at various levels (OS and browser) to modify, over time, the parts of a user platform that are the most identifying in a fingerprint. This new approach allows users to exhibit a diversity of fingerprints without lying. Thanks to the technology behind Docker, we can launch browsing platforms in seconds while providing a comfortable browsing experience.

V. Acknowledgments

This work is partially supported by the EU FP7-ICT-2011-9 No. 600654 DIVERSIFY and the CNRS INS2I JCJC 2016 FPDefendor projects.

References

[1] P. Eckersley, "How unique is your web browser?" in *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*, ser. PETS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 1–18. [Online]. Available: http://dl.acm.org/citation.cfm?id=1881151.1881152

[2] P. Laperdrix, W. Rudametkin, and B. Baudry, "Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints," in *37th IEEE Symposium on Security and Privacy (S&P 2016)*, San Jose, United States, May 2016. [Online]. Available: https://hal.inria.fr/hal-01285470

[3] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna, "Cookieless monster: Exploring the ecosystem of web-based device fingerprinting," in *Proc. of the Symp. on Security and Privacy*, 2013, pp. 541–555.

[4] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, "The web never forgets: Persistent tracking mechanisms in the wild," in *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS 2014)*. ACM, 2014.

[5] H. Okhravi, T. Hobson, D. Bigelow, and W. Streilein, "Finding focus in the blur of moving-target techniques," *Security Privacy, IEEE*, vol. 12, no. 2, pp. 16–26, Mar 2014.