Unpeeling the Onion

Tor Browser Browser-Fingerprinting Threat Model Analysis

Jared Stemper, Vafa Andalibi
School of Informatics, Computing, and Engineering, UROC, Indiana University Bloomington

Introduction

Browser-Fingerprinting (BF) refers to information collected about a computing device for the purpose of identification [1]. BF allows for more accurate services, but also brings privacy threats.

Tor Browser

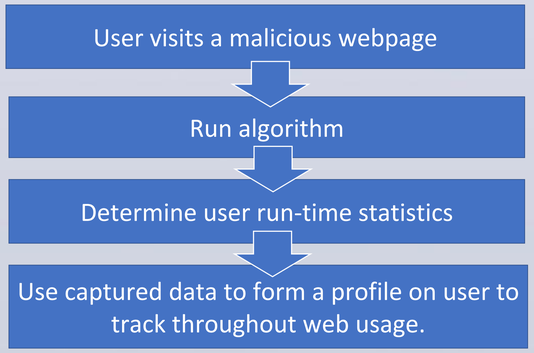
Tor Browser attemps to make it harder to obtain user data by obscuring data. Our research test to find our how breakable these attempts are and the security flaws that could potentially be present in the services in order to help protect people's privacy.

Research Question

Can we break the Tor Browser-Fingerprinting?
By break we mean:

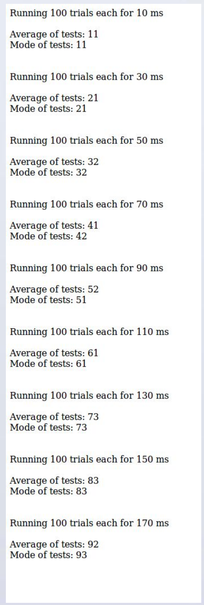
- **Reveal user data without authorization**
- **Unapproved web-based location tracking**
- **Potential for harmful activity**

Threat Model



Methodology

- **Create Apache 2 server**
- **Form initial attack vector**
- **Research vector for previous attempts**
- **Refine Threat Model**
- **Create algorithm to test quantitative measurements**
- **Analyze/observe data findings**
- **Refine algorithm**
- **Form final threat models**


Running 100 trials each for 10 ms

Average of tests: 11
Mode of tests: 11

Running 100 trials each for 30 ms

Average of tests: 21
Mode of tests: 21

Running 100 trials each for 50 ms

Average of tests: 32
Mode of tests: 32

Running 100 trials each for 70 ms

Average of tests: 41
Mode of tests: 42

Running 100 trials each for 90 ms

Average of tests: 52
Mode of tests: 51

Running 100 trials each for 110 ms

Average of tests: 61
Mode of tests: 61

Running 100 trials each for 130 ms

Average of tests: 73
Mode of tests: 73

Running 100 trials each for 150 ms

Average of tests: 83
Mode of tests: 83

Running 100 trials each for 170 ms

Average of tests: 92
Mode of tests: 93

Firefox user analytics


Running 100 trials each for 10 ms

Average of tests: 8
Mode of tests: 0

Running 100 trials each for 30 ms

Average of tests: 17
Mode of tests: 0

Running 100 trials each for 50 ms

Average of tests: 26
Mode of tests: 0

Running 100 trials each for 70 ms

Average of tests: 35
Mode of tests: 0

Running 100 trials each for 90 ms

Average of tests: 44
Mode of tests: 0

Running 100 trials each for 110 ms

Average of tests: 53
Mode of tests: 0

Running 100 trials each for 130 ms

Average of tests: 61
Mode of tests: 100

Running 100 trials each for 150 ms

Average of tests: 72
Mode of tests: 100

Running 100 trials each for 170 ms

Average of tests: 78
Mode of tests: 100

Tor user analytics

Results/Findings

- **Unauthorized user tracking**
- **Able to use data to track user in a network**
- **Verified user data captured**

Conclusion

We were able to access user data without authorization, identify the user on the Tor browser, and track the web-based location of the user. Many people depend on Tor Browser for anonymity, but this anonymity can be broken by a determined attacker.

Future Works

- **Proper reporting of this issue to Tor security develops, advising change to current algorithm for BF**
- **Some level of user education to notify users of this threat**
- **Test other attack vectors to verify the same security issues**
- **Combine attack vectors to create a full profile of a user**

References

[1]InfoSec Resources, 19-6-2014, Web, 6-12-2018, https://resources.infosecinstitute.com/must-know-os-fingerprinting/.
[2] The Tor Project, Inc..“Tor logo.”, media.torproject.org, n.p.,19-6-2011, Web, 6-12-2018, https://commons.wikimedia.org/wiki/File:Tor-logo-2011-flat.svg.

Acknowledgements

I would like to thank Vafa Andalibi for this research opportunity and guidance. I would also like to acknowledge Joshua Streiff for their technical assistance. Special thanks to UROC program for this great opportunity.

Contact Information: jaastemp@iu.edu