The Onion Unpeeled: User Perceptions vs. Realities of Tor's Security and Privacy Properties

Harel Berger
Georgetown University

Tianjian Hu
Georgetown University

Adam J. Aviv
The George Washington University

Micah Sherr
Georgetown University

Abstract

In the face of growing concerns about online privacy and security, this research delves into the perceptions versus the realities of the Tor network's privacy and security features, as experienced by its users. Through an online survey hosted on an onion site (making it accessible only to Tor users), we seek to uncover the nuances of how users engage with Tor, their understanding of its privacy protections, and their general awareness of online security principles. This exploration not only aims to bridge the knowledge gap regarding user expectations and the technical functionalities of Tor but also to shed light on potential areas for improvement in user education regarding Tor. The insights gained from this study are intended to contribute to the enhancement of Tor's utility as a tool for privacy and security, fostering a more informed and empowered user community.

1 Introduction

As Internet users debate over the practicality and importance of digital privacy [10], Tor [4] offers a path for those seeking a more private Internet experience. It enables users to obscure their IP addresses, offering anonymity and resilience against censorship in certain jurisdictions. Tor helps users achieve anonymity by routing their internet traffic through multiple volunteer-operated servers (relays) worldwide. Tor encrypts the data multiple times before it passes through the network. Each relay decrypts one layer of encryption to reveal only the next relay's IP address until the destination. This layered encryption ensures that no single relay knows both the source and destination of the data. This process also hides the user's IP address from the destination server, making it difficult to trace the origin of the traffic [4]. With approximately eight million daily users [3, 11], Tor has become a cornerstone of privacy-focused Internet usage.

Motivated by the increasing significance of online privacy and security, this research project fills a crucial gap in the literature. While previous studies have extensively examined different aspects of Tor, e.g., measuring its traffic behavior [5,11], analyzing emerging threats on its infrastructure [8, 14], and identifying its communication flows [13, 16], there remains limited exploration into the alignment between user perceptions and Tor's actual capabilities. As concerns surrounding online privacy continue to mount and the utilization of anonymity networks such as Tor grows, understanding this disparity becomes paramount. Existing studies have investigated misconceptions of privacy-enhancing technologies [7, 15, 17]. Also, prior studies explored the motivations of the operators of Tor relays [9] and surveyed end-users about their experiences using Tor [12]. However, a focused work on the differences between the *perceptions* of Tor users regarding the networks security and privacy properties and the *realities* of what Tor provides have not been previously established.

This study explores the divide between the perceived and actual privacy and security features of the Tor network. Our primary aim is to delve into the understanding and expectations of Tor users regarding their privacy and security while utilizing the network. We aim to conduct an incentive-compatible online study with 1000 Prolific participants. During this study, participants share how they use Tor, their understanding of Tor privacy protection, and their general knowledge of security and privacy.

Through an investigation into users' lived experiences and beliefs, this study aims to offer valuable insights into Tor's efficacy from a user-centric standpoint. By shedding light on the intersection of user perceptions and technical functionalities, we aim to inform future enhancements to the Tor network and educational initiatives regarding safe use of the network. In doing so, we contribute to a deeper understanding of Tor's

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

role in preserving online privacy and security, paving the way for a more informed and empowered user base.

1.1 Research Questions

Our study is centered around three main research questions:

RQ1: What are the differences between Tor users' perceptions of its privacy features and its actual privacy capabilities?

RQ2: How do users' expectations of Tor's censorship resistance compare to the service's actual functionalities?

RQ3: How do misconceptions about Tor's functionality affect user behavior and trust in the network?

2 Methodology and Survey Design

To study users' understandings and perceptions of the Tor anonymity network, we conduct an online survey consisting of multiple-choice, Likert scale, and open-ended questions. We self-host the survey on our own infrastructure using an instance of LimeSurvey [1], an open-source online survey tool, and only expose it to the Internet as a Tor Hidden Service (also known as an onion-site or onion service). In this way, we can guarantee that participants have actual experience with Tor. This study has been submitted for review by the Georgetown University Institutional Review Board (IRB).

This study is targeted to people who have at least some experience with Tor. For a higher likelihood of Tor usage, we post advertisements on the `r/Tor` subreddit. We also recruit participants via the study platform Prolific [2].

After completing an informed consent process, participants are given a link to an .onion webpage which they must access with Tor. Upon completion of the survey, they are offered a chance to enter their e-mail address to receive an Amazon gift card. No other personally identifiable information is collected in the survey, and the e-mail address is used solely for the purpose of sending compensation.

The main survey consists of several parts covering different topics:

Motivation To understand participants' motivations for using Tor, we begin the survey by asking participants their main reasons for using it, and when they prefer Tor over regular Internet browsing. They are also asked how they feel other users are using Tor.

Usage patterns We ask participants generally about their usage patterns, including how often and on which devices do they use Tor. Following that, we ask more specifically using Likert scales how often participants use different Tor services (e.g., onion-sites or bridges) and browse for different purposes (e.g., social media or media download).

Understanding We explore participants' basic conceptions about the security and anonymity guarantees that Tor provides, as well as what Tor does *not* protect them from. We ask participants to describe Tor's mechanisms to protect privacy and ask about their degree of agreement on various statements describing whether Tor prevents a certain risk from a certain party or not (e.g., their ISP, their government, the Tor Project, etc.), using Likert scales. Next, we ask participants to compare Tor with VPNs and "incognito" browsing modes and describe their differences.

Deeper knowledge We ask participants about their familiarity with several more in-depth topics. We explore in more detail users' understanding of Internet censorship, onion-sites, and relays.

General security attitudes We use the SA-6 [6] scale to measure participants' general security attitudes towards online security.

Demographics We ask participants to provide demographic information such as age, gender, nationality, and English proficiency.

3 Anticipated Contribution

Our research is poised to reveal a noteworthy divergence between user perceptions and the actual functionalities of Tor's security and privacy features. We expect to clarify these misconceptions, providing a more accurate picture of Tor's operation from the users' viewpoint. The study will generate specific recommendations to improve educational resources. By addressing these gaps between users' understanding of the security and privacy properties offered by Tor and the realities of what the anonymity network provides, our efforts will enhance Tor's true effectiveness in providing security and privacy. These enhancements promise to have a profound impact across the broader security and privacy community, contributing significantly to our understanding and implementation of secure online environments.

Acknowledgments

This work is partially funded by the National Science Foundation through grant 2138078 and the Callahan Family Chair Fund. The opinions and findings are those of the authors and not necessarily that of the funding organizations.

References

[1] Limesurvey - the online survey tool. https://www.limesurvey.org.

[2] Prolific. https://www.prolific.com.

[3] Tor project user statistics. https://metrics.torproject.org/userstats-relay-country.html.

[4] Roger Dingledine, Nick Mathewson, Paul F Syverson, et al. Tor: The second-generation onion router. In *USENIX security symposium*, volume 4, pages 303–320, 2004.

[5] Christoph Döpmann and Florian Tschorsch. Modeling tor network growth by extrapolating consensus data. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pages 1–7, 2023.

[6] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. A Self-Report measure of End-User security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 61–77, Santa Clara, CA, August 2019. USENIX Association.

[7] Matthias Fassl, Alexander Ponticello, Adrian Dabrowski, and Katharina Krombholz. Investigating security folklore: A case study on the tor over vpn phenomenon. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2):1–26, 2023.

[8] Zhong Guan, Chang Liu, Gang Xiong, Zhen Li, and Gaopeng Gou. Flowtracker: Improved flow correlation attacks with denoising and contrastive learning. *Computers & Security*, 125:103018, 2023.

[9] Hsiao-Ying Huang and Masooda Bashir. The onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*, 53(1):1–10, 2016.

[10] Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64:122–134, 2017.

[11] Akshaya Mani, T Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. Understanding tor usage with privacy-preserving measurement. In *Proceedings of the Internet Measurement Conference 2018*, pages 175–187, 2018.

[12] The Tor Project. Tor browser user survey report, November 2021.

[13] Debmalya Sarkar, P Vinod, and Suleiman Y Yerima. Detection of tor traffic using deep learning. In *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, pages 1–8. IEEE, 2020.

[14] Christoph Sendner, Jasper Stang, Alexandra Dmitrienko, Raveen Wijewickrama, and Murtuza Jadliwala. Mirageflow: A new bandwidth inflation attack on tor.

[15] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021.

[16] Ryan Wails, George Arnold Sullivan, Micah Sherr, and Rob Jansen. On precisely detecting censorship circumvention in real-world networks. In *Network and Distributed System Security*, 2024.

[17] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In *Proceedings of the 2018 World Wide Web Conference*, pages 217–226, 2018.