MEASUREMENT AND IMPROVEMENT OF THE TOR USER EXPERIENCE

DISSERTATION

Submitted in Partial Fulfillment of

the Requirements for

the Degree of

DOCTOR OF PHILOSOPHY (Computer Science)

at the

NEW YORK UNIVERSITY

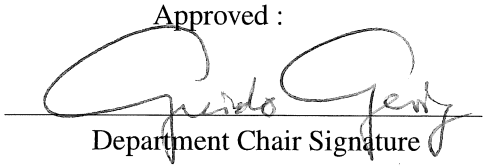
TANDON SCHOOL OF ENGINEERING

by

KEVIN GALLAGHER

January 2020

Approved :



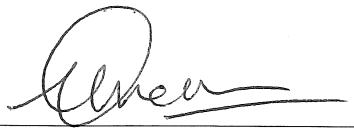
Department Chair Signature

Dec, 18th, 2019

Date

Approved by the Guidance Committee :

Major : Computer Science



Nasir Memon

Professor of
Computer Science and Engineering

Dec 16th 2019

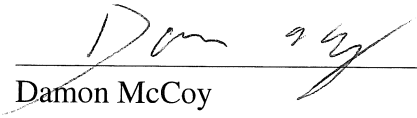
Date

Brendan Dolan-Gavitt

Professor of
Computer Science and Engineering

Dec 16th 2019

Date



Damon McCoy

Professor of
Computer Science and Engineering

Dec 16th 2019

Date

Sameer Patil

Professor of
Computer Science and Engineering

Dec 20th 2019

Date

Vita

Kevin Gallagher was born in New York on March 15th, 1991. He received his Bachelors of Arts in Computer Science from the City University (CUNY) of New York's Hunter College in January 2014 and went on to work as a programmer for CUNY while doing research on Bibliometrics under Professor Theodore Brown at the CUNY Graduate Center. He then began the PhD Program in Computer Science at the New York University (NYU) Tandon School of Engineering in September of 2014 and earned his Masters degree in passing in August of 2016. During his time at NYU he held the positions of Research Assistant, Course Assistant, Teaching Assistant, and Adjunct Professor.

Kevin performed research in Bibliometrics and Usability and User Experience of Anonymity Systems. He focuses his research on the intersection of anonymity, psychology, and human rights. During his time at NYU he has published one peer-reviewed article in Bibliometrics and two peer-reviewed articles in Usability and User Experience of Anonymity Systems. At the time of this writing a fourth article is in preparation for submission.

In addition to these activities, Kevin also lead the Applied Research competition of Cyber-Security Awareness Week in 2016 and performed organizational work for the Tor Project in New York City, The United States and Lisbon, Portugal. He is the co-founder and president of PrivacyLx (officially Defend Our Privacy Association) in Lisbon, Portugal and is a Tor Core Contributor.

Acknowledgements

I would like to express my gratitude to my advisors, who put many hours and effort into guiding me through my research and the various other requirements of my PhD. I would also like to thank Santiago Torress, Zahra Ghodsi, Donna Tincher, Dennis Gallagher, and other friends and family who provided the emotional support to help me get through the difficult times as a PhD student. Finally I would like to thank my funders of my work, the National Science Foundation (under grant DGE-0966187), the Qatar National Research Fund (under grant NPRP 7-1469-1-273), Comcast, and Google.

Kevin Gallagher

Dedicated to Rodrigo de Sousa Rodrigues, who waited patiently for me to complete my studies.

ABSTRACT

Measurement and Improvement of the Tor User Experience

by

Kevin Gallagher

Advisor: Nasir Memon

Coadvisor: Brendan Dolan-Gavitt

Submitted in Partial Fulfillment of the Requirements for

the Degree of Doctor of Philosophy (Computer Science)

January 2020

Anonymity plays a vital role in modern societies. Using the protective cloak of anonymity, whistle-blowers are able to raise concern over worrying activities, journalists are able to protect their sources and investigate the powerful, abuse victims can seek help without fear that they will be discovered by their abusers, immigrants can seek advice on their legal situations, and other at-risk populations can remain safe. The most widely-used anonymity system on the Internet today is Tor, and like all anonymity systems it is dependent on having a large anonymity set, or set of indistinguishable users, in order to provide anonymity. This makes usability and user experience extremely important for anonymity. The more usable a system is, and the better experience it provides to its users, the larger the anonymity set can grow.

In this thesis we examine the usability and user experience of Tor from three perspectives. First we study how well users understand the software that they are using by studying their mental models of the Tor network. We find that experts and non-experts have different understandings of the internal workings of the Tor anonymity network, with experts having a more complete model of it as a complex network and focusing on the networking portion, while non-experts focus on the Tor Browser as a black box service. Both experts and non-experts show gaps in their mental models that can lead to misuse of the software.

Next we examine the User eXperience (UX) flaws of the Tor Browser. We asked

participants that resembled a new, non-technical user base of Tor to use the Tor Browser as their default browser for a period of 7 days. During this time we spawned a survey for them to fill out every time they finished browsing. From these surveys, some semi-structured interviews, and some write-ups we discovered that Tor Browser users face multiple issues, including broken functionality, differential treatment, geo-location issues, and more.

Finally we examined the Tor Browser Friendliness of the Web by creating a suite of tools used to log and examine the creation of DOM trees and the execution of JavaScript scripts on the Tor Browser and on Firefox. We then performed deep-dive analysis on 40 Web sites randomly drawn from 4 categories. From these analyses we discovered many instances in which the Web sites break on the Tor Browser, and use them to better understand what it means to be Tor Browser Friendly. We then present guidelines for how to make a Web service Tor Browser friendly.

The results and insights gained from each of these projects have been reported to the Tor Project, and have influenced decisions in the design of the Tor Browser. Other changes are in discussion for being implemented.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

In his work *The moral character of cryptographic work* [62], Phil Rogaway discusses the current state of cryptographic work as it applies to the influence of power, both governmental and commercial, and to the common person. He spends a large part of the essay discussing mass surveillance and the academic community's unwillingness to solve the issue, and indeed how in some cases it furthers it. He states:

"As computer scientists and cryptographers, we are twice culpable when it comes to mass surveillance: computer science created the technologies that underlie our communications infrastructure, and that are now turning it into an apparatus for surveillance and control; while cryptography contains within it the underused potential to help redirect this tragic turn... [S]cientific and technical work routinely implicates politics. This is an overarching insight from decades of work at the crossroads of science, technology, and society... Technological ideas and technological things are not politically neutral: routinely, they have strong, built-in tendencies. Technological advances are usefully considered not only from the lens of how they work, but also why they came to be as they did, whom they help, and whom they harm."

Though Rogaway's words in his essay do specifically address the cryptography community it does not take much looking to see that they generalize to the rest of the security research world. Many new research projects in security seek to aid commercial power in restricting access to copyrighted material such as in [44], or aid government and corporate power by allowing for easier mass surveillance, such as in [7]. This trend is worrying and inevitably leads to power tightening its grip on the flow of information.

Controls on the flow of information inherently leads to the censoring of ideas, and mass surveillance creates a chilling effect that makes people unwilling to express controversial or radical opinions. Even further, mass surveillance chilling effects can also apply to actions, making people unwilling to do things such as attend protests. In short, mass surveillance helps ensure the status-quo, and that the institutions and systems in power do not lose that power.

Towards the end of his article, Rogaway includes what amounts to an academic call to arms.

"Since cryptography is a tool for shifting power, the people who know this subject well, like it or not, inherit some of that power. As a cryptographer, you can ignore this landscape of power, and all political and moral dimensions of our field. But that won't make them go away. It will just tend to make your work less relevant or socially useful. My hope for this essay is that you will internalize this fact and recognize it as the starting point for developing an ethically driven vision for what you want to accomplish with your scientific work."

Again, this call to arms generalizes beyond cryptography into the security world. Security researchers must consider the implications of their work and ensure that they work on projects that shift the power into the hands of the common person. Through doing this we will move away from contribution to power or to the academic bubble and move towards contribution to societal good.

When it came time to choose a research problem, we[1] heeded Rogaway's words and decided to follow his call to arms. Given the large problem of mass surveillance, we decided to focus on improving anonymity, and to gear this body of work towards an investigation of the User eXperience (UX) of the Tor Browser.

1.2 Problem Statement

Anonymity plays a vital role in modern societies. Using the protective cloak of anonymity, whistle blowers are able to inform the public of malicious behaviors of governments and corporations, journalists are able to contact sources and perform research on subjects of interest, immigrants, abuse victims, and other at-risk individuals are able to seek help and information, and citizens are able to maintain privacy and

[1] Even though this dissertation contains only one author it will follow the academic tradition of using the royal we.

express ideas without fear. Anonymity helps many people protect their rights or keep themselves safe from embarrassment, physical danger, or in some cases, even death.

Though achieving anonymity in the Internet age is becoming increasingly difficult due to the prevalence of tracking mechanisms and metadata collection and requires more advanced tools [48]. One such tool is Tor [12], an overlay network that provides metadata obfuscation by routing Internet traffic through randomly selected, volunteer-run relays, with each relay providing a layer of encryption. Other tools include i2p, freenet, and others. Though surveillance is a problem, there exist many solutions that individuals can turn to. However, all of these solutions have the same limitation.

The strength of an anonymity system depends on the number of indistinguishable users, called its anonymity set [11]. If an anonymity set is low, users of an anonymity system gain very little from using it, even if the cryptographic guarantees of the network are very high. Thus usability and UX must be considered vital parts of any anonymity system, and each anonymity system must provide user-centered security [80] by paying attention to the usability and UX aspects of the system. Poor UX tends to drive users away, thus negatively impacting the strength and quality of anonymity provided by the system. Further, the more diverse the user base, the less an adversary may infer about any individual user of the anonymity system. Those whose anonymity needs may not be strict enough to tolerate UX frustrations and inconveniences may still be willing to use an anonymity system if the UX is improved, thus diversifying the anonymity set.

The Tor Project realizes this. In an effort to strengthen the network and expand the set of indistinguishable Tor users, the Tor Project provides the Tor Browser that makes users less distinguishable by countering some application-layer tracking techniques, such as cookies, `User-agent` strings, or browser fingerprinting mechanisms. Yet, there has been little research on the usability and UX aspects of Tor. Existing work related to the topic is outdated [8], narrow in focus [42], or limited to lab settings and specific tasks [49, 50], thus limiting the utility and impact of the findings.

In this dissertation we study Tor users and Tor UX. Specifically we address the large research question:

How do users perceive and experience use of the Tor Browser?

This is a large question, and to address it we broke it down into three smaller, easier to address questions:

- ***How do users understand the inner workings of the Tor anonymity software?***

- ***How do users experience routine Web browsing when using the Tor Browser?***

- ***What functionality and Web sites break on the Tor Browser and why?***

The first two research questions were addressed in separate projects that were published in top conferences in their field. The last research question is addressed for the first time in this dissertation, but is also described in an article that is under submission. The details of these projects are discussed thoroughly in Chapters 4, 5, and 6.

1.3 Contributions

The first research question we considered was:

Why do people use Tor and how well do they understand the underlying operation of the Tor system?

We addressed this question by performing semi-structured interviews with 17 Tor users recruited from Reddit, New York University, and Craigslist. We then analyzed the text of these interviews using techniques based on grounded theory. Based on this analysis of the interviews we made the following contributions:

- We describe user perceptions and practices regarding Tor, an anonymity tool of growing individual and societal importance.
- We uncover and describe important differences in how experts and non-experts understand and conceptualize Tor. Specifically, we show that gaps and inaccuracies in non-expert understanding of the operation and threat model of Tor could lead to a sense of more or less privacy and security than is actually the case.
- We suggest solutions that can improve the Tor user experience and boost adoption by non-experts, many of whom are in vulnerable situations and/or serve as society's important actors.

After addressing the first research question, we decided to take a look at how Tor users experience everyday, naturalistic use of the Tor browser. Specifically we wanted to know:

How do users experience routine Web browsing when using the Tor Browser?

We addressed this question via a study that examined the use of the Tor Browser in a naturalistic setting for a period of one week, focusing particularly on identifying frustrations, confusions, and problems. To this end, we collected quantitative and qualitative data on the use of the Tor Browser for routine Web browsing and online tasks. Based on 121 questionnaire responses, 11 interviews, and 19 write-ups from 19 study participants, we report on a number of UX issues, such as broken Web sites, latency, lack of common browsing conveniences, differential treatment of Tor traffic, incorrect geolocation, operational opacity, etc. Specifically, we made the following contributions:

- **Detailed accounts of naturalistic use of the Tor Browser.**
  We collected data regarding Tor Browser usage for routine online activities in a naturalistic setting, uncovering a number of important UX issues.
- **Suggestions for improving the Tor Browser UX.**
  Grounded in the UX issues encountered during our study, we identified and outlined several practical solutions and design guidelines to address and mitigate the problems and improve the UX of the Tor Browser.
- **Method for privately collecting naturalistic quantitative data on the Tor Browser UX at scale.**
  The method we used for collecting quantitative UX data on Tor Browser usage could be deployed to allow privately gathering naturalistic data at scales significantly beyond those possible in typical laboratory studies. Thus it is a contribution of this dissertation in addition to the understanding we gleaned from it.

From this work we discovered that users who attempt to use the Tor Browser frequently and for diverse tasks are likely to run across content on the Web that works on other browsers, but does not work correctly on the Tor Browser. This broken content became the subject of our next investigation. Specifically, we addressed the question:

What functionality and Web sites break on the Tor Browser and why?

To address this question we created a tool that scanned a Web page on Firefox (for ground truth data) and the Tor Browser and logged the creation of the DOM tree and all JavaScript executions. We then scanned the home-pages of 1000 Web sites and did a cognitive walk-through of 40 Web sites using this tool. The DOM and JavaScript traces were then analyzed to look for signs of broken functionality. From this work we make the following contributions:

- **Tools for collecting and analyzing information about site functionality on the Tor Browser**
  We created a series of tools and analysis scripts to capture information about the DOM rendering process and the JavaScript executions on both Firefox and the Tor Browser. We then created a series of scripts to analyze this data and determine the difference between the JavaScript execution traces and the DOM Rendering processes of Firefox and the Tor Browser.

- **A data set of 1000 home pages and 40 interactive browsing sessions.**
  We release the data set created in this project so that it can continue to be studied and more information about the differences between Firefox and the Tor Browser can be discovered.

- **Insight about what functionality breaks on the Tor Browser and why.**
  We provide details about what functionality has broken on the Tor Browser, and discuss the root causes for these breaks. These breaks were discovered using a combination of a cognitive walkabout and the logging from the tools we created.

- **Guidelines for creating a Tor Browser Friendly Website.**
  Based on the analysis of our deep dives, we propose some guidelines to creating a more Tor Browser Friendly Website. These guidelines are not exhaustive.

In the chapters that follow we elaborate on these projects. In Chapter 2 we summarize the necessary background information of the fields we contribute to. In Chapter 3 we then discuss the prior related research on the UX, usability, and users of Tor. In Chapter 4 we describe our first project, which addresses user perceptions of Tor. Next

in Chapter 5, we discuss our second project, which discovered UX faults in the Tor Browser during naturalistic usage. In Chapter 6 we discuss our last project, which determined how and why some Web site functionality broke on the Tor Browser. In Chapter 7 we discuss the work that still remains to be done after this dissertation, and how we intend to address that work. In the final chapter we include some closing remarks.

Chapter 2

Background

In this chapter we provide background information on the fields of anonymity, usability and UX that are vital to understand this dissertation. We start by explaining Tor the anonymity network at the center of our investigation, in Section 2.1. We discuss how it operates, the adversary it considers, and a few attacks against it. We discuss its most popular front-end, the Tor Browser, in Section 2.2. We then go on to explain the usability and UX concepts that we use in this dissertation, including grounded theory and coding in Section 2.3, cognitive walk-throughs 2.4 and mental models in Section 2.5.

2.1 Tor

The subjects of the investigations presented in this dissertation are Tor [12] and its users. Tor is an anonymity network that allows individuals to access TCP-based Internet resources anonymously by hiding their IP address using a variant of onion routing [20]. For each connection, Tor will build a circuit of three[1] volunteer-run nodes. Each cell[2] in that circuit will then be encrypted three times, once for each node. The traffic is then forwarded to the first node, which will strip one layer of encryption and forward it to the next layer, which will repeat the process. This process goes on until the last node of the circuit, where the decrypted form of the cell can be seen and the contained packet(s) can be forwarded to the intended destination. The list of nodes is maintained and publicly listed by a set of directory authorities that act as root trust in the system, and agree on the state of the system every hour via a consensus algorithm.

Unlike other anonymity systems, Tor does not defend against an adversary who

[1] Though the default is three, this is a configurable amount

[2] A cell is a construct in Tor that makes all sent information the same fixed-length of 512 bytes. For more information, see the Tor paper.

can see all traffic on the network. Instead, Tor protects against an adversary which can observe a fraction of network traffic, can modify traffic, and who can participate in the protocol maliciously by running nodes or compromising nodes. This adversary was chosen to balance the anonymity needs of users while still remaining a practical, usable system. Unfortunately this leaves Tor vulnerable to certain types of statistical attacks based on timings of traffic, mainly the traffic confirmation attack and Web site fingerprinting attacks. However, since these are not the focus of this dissertation, we do not discuss these attacks further.

The strength of the Tor anonymity system, like any anonymity network, can be linked in part to its anonymity set [11]. The anonymity set is the set of users of an anonymity network that are equally suspected of causing a given communication. The higher this anonymity set is, the more effective the anonymity system is. For this reason usability and UX are extremely important in Tor. The more usable and the more pleasant to use Tor is, the more the anonymity set will grow, and the stronger Tor may become.

2.2 Tor Browser

Although Tor can be used with any application that uses TCP network traffic, Tor is most commonly used for Web browsing [46]. To facilitate easier Tor usage and to decrease the chance of profiling through Browser fingerprinting and other methods, the Tor Project released the Tor Browser. The Tor Browser is a modified Firefox that sends all of the browsing traffic through Tor, and which blocks or otherwise frustrates methods of Browser fingerprinting. For example, on the higher security slider settings the Tor Browser blocks all JavaScript from executing, ensuring that many avenues for browser fingerprinting are eliminated. On lower security slider settings certain JavaScript APIs such as the Web Speech API are disabled by default, since they can open the user to fingerprinting attacks. The introduction of the Tor Browser helped improve Tor's strength by increasing it's anonymity set. It did this by solving a few problems that connecting to Tor previously caused.

- ***Avoiding Proxy Bypass***
  Prior to the release of the Tor Browser, the way that Tor users would use the program to access the Web was to connect a browser of their choice to the Tor SOCKS proxy running on their local machine. This proxy would then pass traffic to the Tor network, anonymizing it. This approach had several issues, the most severe of which was proxy bypassing. Browser add-ons and extensions like

Flash could ignore the proxy settings and send messages over the user's regular network. The release of the Tor Browser fixed these issues by disallowing extensions that could bypass the proxy, ensuring that individuals who were using Tor were not leaking their IP addresses to arbitrary servers online.

- ***Frustrating Browser Fingerprinting***
  Another avenue of attack against anonymity is browser fingerprinting. A browser connecting to a Web service through Tor might have some uniquely identifying characteristics, such as the browser's referrer headers. Even if one piece of information was not uniquely identifying, adding other information such as installed fonts, canvas size, or fingerprinting hardware through timing functions could cause fingerprinting to occur. The Tor Browser frustrates these types of fingerprinting attacks by creating a more uniformity in the browser, such as the referrer headers and the list of fonts installed. In addition it blocks some features that could be used to fingerprint a browser, such as HTML5 Canvas data, and frustrates other features such as timing features by forcing it to return information at a lower granularity.

- ***Making Tor Easier to Use***
  The Tor Browser increased the anonymity set of Tor by making Tor easier to use. Since the Tor Browser can be downloaded as a standalone browser and no longer requires complex configurations, it allows people with less technical skill be access Tor and become anonymous on the net. As the number of users of Tor increases, so too does its anonymity set, and thus its strength.

- ***Fixing Other Issues***
  In addition, the Tor Browser fixed other issues related to anonymity, fingerprinting, and privacy. One example of other fixes includes Disk Avoidance, or the concept of avoiding writing any material from anonymous browsing onto the local disk of the computer. For a full understanding of what changes were made in the Tor Browser, we recommend viewing the Tor Browser Design Document [54].

To keep the Tor Browser usable the Tor Project included in it a "security slider" that activated and deactivated different security functions to meet the needs of the user. The lowest level, "Standard," performs the least changes to Firefox. It routes all traffic through Tor and disables Graphite fonts, remote JAR files, and asm.js while allows JavaScript to run as native C code. The "Safer" security level disables the IonMon-

key JIT compiler, native regular expressions, Baseline JIT, WebAudio, MathML, SVG Opentype font rendering, and makes HTML5 audio and video click-to-play. It also forbids JavaScript over HTTP. On the "Safest" security setting remote fonts are disabled, JavaScript is disabled entirely, and SVG images are disabled. These changes allow the user to choose their level of desired security versus the functionality of their browser.

However, even with all of these positive changes Tor still has issues. There exist user experience issues in the Tor Browser. These are discussed more in Chapter 5. These UX faults can drive users away, shrinking the anonymity set and making Tor less effective. However, some of these UX issues may be caused by the measures that are put in place to protect individuals from fingerprinting and other identifying attacks, potentially creating a tension between expanding the anonymity set and ensuring that individuals within the anonymity set are virtually indistinguishable.

Some of these UX issues can be solved politically. For example, the Cloudflare CDN used to serve Tor users many CAPTCHAs before allowing them to access content being hosted using their services [53,66], justifying their actions with questionable statistics [53, 55]. However, after large amounts of pressure from members of the Tor community and other Internet freedom activists, Cloudflare was forced to develop solutions that did not negatively impact the UX of Tor users [63]. However UX issues need to be discovered before they can be handled in this way, and other UX issues cannot be handled politically.

2.3 Grounded Theory

In addition to Tor, this dissertation relies on knowledge about certain usability and user experience research an analysis methods, including grounded theory [19]. Grounded theory is a method in social sciences that starts with a question, rather than a given hypothesis. Qualitative data is then analyzed through repeating steps until a theory is formed. These steps are

1. ***Open coding***
   First is open coding, where core points of the data are labeled with a code that summarizes them and represents their core meaning.

2. ***Axial coding***
   The second step is axial coding. In this stage codes from the first step are examined and related codes are grouped into categories. Codes can be determined to

be related based on how frequently they appear together, based on similarities in the meanings that they convey, or both.

3. ***Selective coding***
   The third step is selective coding. In selective coding categories are analyzed in an attempt to find a core variable or set of core variables that link them all together.

These steps are performed repeatedly until a theory is formed, and the research questions are answered. This method differs from other methods and from the scientific method specifically in that is begins with research questions but without hypothesis that it is seeking to validate. Instead, the researcher approaches the data without any initial hypothesis and generates understanding from the data alone. Often times theories that are generated from grounded theory are then tested using quantitative data and the scientific method.

In this dissertation we do not use grounded theory, but we do use methods inspired by grounded theory. That is we use the methods of qualitative analysis that grounded theory uses, open coding, axial coding, and selective coding, but we stop short of coming up with a central theory to explain the data. We complete our analysis when we feel we have hit saturation, and provide the insights we have gained from it.

2.4 Cognitive Walk-throughs

In addition to the three steps of grounded theory, we also perform cognitive walk-throughs in this dissertation. A cognitive walk-through is a usability research method in which specific functionality of a site or system is tested by a researcher. The researcher attempts to perform this task as if he or she is a new user of this system. This occurs in two steps: first the researcher breaks the task into a series of steps that the new user needs to perform in order to complete the task, then the researcher attempts to perform this task while answering a set of questions about a user's ease and ability to perform the task. Though these tasks are different for different applications, questions for Web applications may be [5]:

1. Will the user try and achieve the right outcome?
2. Will the user notice that the correct action is available to them?
3. Will the user associate the correct action with the outcome they expect to achieve?

4. If the correct action is performed; will the user see that progress is being made towards their intended outcome?

The answers to the relevant questions are noted at each step and the resulting notes are used in a report to determine usability issues with the given system. In this dissertation we perform cognitive walk-throughs for sites on the Web while using a modified version of the Tor Browser. More information about these walk-throughs is presented in Chapter 6.

2.5 Mental Models

To understand how users viewed the Tor anonymity system, we decided to study their mental models of the Tor software. A mental model is a mental representation of a system, which usually include parts of that system and relationships between them [15]. In terms of technological systems, a mental model is used to guide or drive interaction with the system. It informs decisions of what the user inputs into a system and how, and creates expectations of what will come out of the system and how, and helps the user interpret what output the system does give, even if it is not the expected output.

Mental models are formed through interaction with the system and typically build over time. Individuals can learn about the system they are using through more interactions with it and adjust their mental models accordingly. They are formed based on incomplete, unquantifiable information and as such are often not accurate representations of the system. They are typically flexible, meaning that they can adjust to new information provided by the system. This can serve as both a positive and a negative for the user. However, mental models can also cause selective perception, which can amplify an incorrect or incomplete understanding of the inner operation of a system.

In this work we measure users' mental models of Tor through semi-structured interviews. More information about this work can be found in Chapter 4.

Chapter 3

Related Work

As Dingledine and Mathewson observed [11], the strength of an anonymity system depends on the number of users, thus highlighting the importance of UX and usability for these systems. Yet, in contrast to the large body of work on its technical aspects, such as attacks, defenses, measurements, etc. [23, 27, 29–31, 33, 45, 52, 60, 67, 72, 77], relatively little research has focused on the UX and users of Tor. Existing research on the user aspects falls under three main themes: UX of anonymity systems and the Tor network, UX of the Tor Browser in particular, and attitudes and practices of Tor users.

3.1 User Experience of Tor

As Dingledine and Mathewson [11] observed, user-centered security [80] is important for anonymity systems since improving the user experience attracts more users, which strengthens the network as a whole. To this end, studies of the user experience of Tor have covered software and network operation, user interface, and external factors.

One of the first studies regarding the user experience of anonymity systems introduced latency 'shocks' into the anonymity network *'AN.ON'* over a one month period. A latency shock occurred every 105 minutes and lasted 15 minutes [40]. The results showed that the number of users who leave an anonymity network because of latency is linearly related to the amount of latency, for latency periods lasting less than 60 seconds. Fabian et al. [14] applied metrics from the literature to investigate and quantify such losses in usability caused by the latency within the Tor network. When compared with direct connections, they found that the median load time for a Web page over Tor was 5 times higher and Domain Name System (DNS) requests were 40 times slower. Based on these measurements, they postulated a request cancellation rate of 74%, leading to potential user frustration when using Tor. In 2014, Griffith [21] examined the

data on the Tor Metrics Web site and concluded that Tor achieves less than 2% of the throughput of non-Tor bandwidth which has remained relatively constant for small files (when normalized by non-Tor bandwidth). Tor performance for large files is however steadily improving, albeit slowly.

Due to its importance for an acceptable UX, reducing latency is an important topic of investigation. Jansen et al. [28] implemented KIST, a kernel-informed socket management algorithm which dynamically computes the amount of data to write to a given socket. In a limited trial, KIST was shown to reduce congestion by over 30% and latency by 18%, thus increasing overall network throughput by nearly 10%. Later, Jansen and Traudt [32] confirmed similar performance improvements in a real-world deployment of KIST within a portion of the Tor network. Geddes et al. [18] proposed the Avoiding Bottleneck Relay Algorithm (ABRA) which utilizes messaging between clients and relays to facilitate path selection in a manner that avoids over-utilized nodes, achieving nearly 20% increase in network utilization compared to vanilla Tor. Despite such efforts, latency continues to be an issue for Tor users. Addressing latency in the Tor network is a priority for the Tor Project [13].

Other studies have examined the user experience of the various user interface elements of Tor. Clark et al. [8] performed a cognitive walk-through of four configurations of the Tor software, performing four tasks in each of the configurations. They proposed user interface changes based on the difficulties encountered in completing the tasks. Norcie et al. [50] tried to identify the challenges experienced by individuals in adopting and using Tor, beginning with the step of installing the software. Their study of 25 undergraduates found that 64% of the participants faced various problems in installing and using the Tor Browser Bundle to perform the given tasks. These problems included difficulties finding and downloading the installation program, issues with decompressing the installation file, confusion in distinguishing between the Tor Browser Bundle and Firefox, latency, etc. In a follow-up study, Norcie et al. [49] evaluated the effectiveness of their proposed interface solutions aimed at fixing the problems uncovered in their initial study. They found statistically significant usability improvement in the case of most issues. Similarly, Lee et al. [42] examined the usability of the Tor Launcher that configures Tor connections. They found that the Tor Launcher interface required users to understand technical terms and did not provide appropriate and adequate feedback, thus leading to frustration and errors. They further showed that interface changes to the Tor Launcher were effective in addressing these challenges.

In a different vein, Khattak et al. [38] investigated how the Tor user experience is affected by the actions of external parties. Specifically, they looked at how Tor users are

treated at the application as well as the network layer. They discovered that 1.3 million IPv4 addresses and 3.67% of the Alexa top 1,000 websites offered degraded services to Tor users or blocked them altogether.

On a different note, Victors et al. [71] proposed a DNS for onion services implemented as a Tor Browser plugin called OnioNS. OnioNS utilizes Tor network nodes and the Bitcoin mining system to assign human readable domain names to Tor Onion services, thus improving the UX by allowing individuals to access these services without the need to enter long cryptographically generated onion service names.

3.2 Tor Users

Improving the Tor Browser UX requires understanding the characteristics, attitudes, and needs of the Tor user population. In this regard, McCoy et al. [46] analyzed the traffic from an entry guard and an exit node under their control, finding that many Tor users came from Germany, Turkey, and Italy. They further discovered that a large amount of sensitive information was sent over the Tor network in plain-text. An investigation of the privacy perceptions of Americans following the government surveillance revelations of Edward Snowden found that 34% of those who were aware of the matter made greater efforts to protect their online personal information. Yet, only 2% of these individuals reported using anonymity software such as Tor. [56] Forte et al. [16] reported that maintaining anonymity via Tor is used by some contributors to open collaboration projects (such as Wikipedia) in order to guard against risks, such as surveillance, harassment, violence, reputation loss, etc. Winter et al. [76] found that users struggle to understand onion services and face issues in navigating to these resources and determining their authenticity.

3.3 Tor Research Considering UX

The importance of usability and UX have not been lost on Tor researchers. Recent technical works have been geared towards technical solutions that solve UX problems, such as the work of Victors et. al discussed previously [71]. New attacks also seek to frustrate Tor user experience, such as the attacks proposed by Jansen et. al [34]. These bandwidth denial of service attacks raise the cost of running Tor nodes and reduce bandwidth, both frustrating the Tor node operators and users, and leading to a decrease in UX and potentially driving users away.

In addition to these new attacks, new defenses also keep usability and UX in mind.

Recent work by Kohls et. al examines how to frustrate traffic confirmation attacks without adding latency or using traffic padding [39]. This works by creating a circuit through geographical locations that are not suspected of participating in traffic confirmation attacks and avoiding geographical locations that are expected to participate. The algorithm then attempts to verify that the traffic does not pass through any router in the suspected geographical areas as well. Though not the primary reason for this research, avoiding latency maintains the usability of Tor and provides a better user experience while also increasing the security against confirmation attacks.

3.4 User Experience of Privacy and Security Tools

At a more general level, researchers have devoted attention to the user experience of various commonly used privacy and security tools and mechanisms. We highlight the most salient findings in this domain pertaining to expert and non-expert understanding and behaviors.

Leon et al. [43] studied 9 tools designed to limit or prevent online behavioral advertising and found significant usability problems in all of them, making it difficult, if not impossible, for users to make meaningful opt-out choices. Wash [73] and Wash and Rader [74] described variations in user mental models regarding viruses and hackers and explained that user decisions to follow security guidance from domain experts were influenced by the specifics of these mental models. Ion et al. [26] found that security non-experts deferred or ignored installing software updates, did not employ two-factor authentication, and did not use a password manager. They suggest that better messaging and usability are required to address the lack of adoption of common security tools. This study was then replicated by Busse et. al with similar results [6]. Similarly, Kang et al. [36] reported large differences in the complexity of the mental models of tech savvy participants and others. Yet, they found no link between technical knowledge and attempts to control online privacy. McGregor et al. [47] focused on journalists, a user group that often encounters situations that require anonymity, for sources as well as themselves. Journalists from the US and France indicated resorting to ad-hoc security approaches due to the lack of comprehensive and usable tools and reported difficulties in authenticating sources using existing tools.

Recent research by Wu et. al examined mental models of encryption by performing semi-structured interviews by phone with 19 people from the United States. They find mental models of varying detail, but with common threads, such as the belief in impersonal use of encryption while reserving personal use of encryption for the paranoid

or for criminals [78]. Research by Habib et. al examined user's perceptions of Private Browsing mode by monitoring browsing of 450 participants and collecting survey data from them and found that users overestimate the protection of private browsing against advertising networks and other trackers [22].

Chapter 4

Determining The Mental Model of Tor Users

In order to practice user-centered security and provide a good user experience for software, it is first necessary to know who uses the software, why they use the software, and how they believe the software works. For this reason we decided to begin our investigation into the usability and UX of Tor by studying the Tor users themselves. At this point very little work had been done on the usability or user experience of Tor, and most of the work that existed focused on Tor itself, rather than trying to understand the Tor user. We suspect that this is because of the difficulty of recruiting Tor users for studies about their Tor use.

However, other studies had been published studying the users of other privacy tools and systems and their understandings and perspectives of the tools they were using. Inspired by those projects, we decided to study the mental models of Tor users in an attempt to ascertain how they understood the tool they were using, why they were using the tool, and what benefits they believed the tool was granting them.

We decided on a set of two core research questions that we believed would help us understand how to approach the problem of Tor usability and user experience:

- ***Why do people use Tor?***
- ***How well do users understand the underlying operation of the Tor system?***

We tackled the above research questions by conducting semi-structured interviews with a diverse sample of 17 Tor users. Based on an analysis of the interview responses, we made the following contributions:

- We described user perceptions and practices regarding Tor, an anonymity tool of

Tasks	Internet Service Provider	Government and Law Enforcement	Target Web site or Service	Advertising Networks
Browsing a Web site	Can see one is using Tor	Can potentially see one is using Tor	Can see some Tor user is visiting the site	Can see some Tor user is visiting the site
Reading email	Can see one is using Tor	Can potentially see one is using Tor	Can access identity and data, but not IP	Can see some Tor user is visiting the site
Receiving an advertisement	Can see one is using Tor	Can potentially see one is using Tor	Can see some Tor user is visiting the site	Can see some Tor user is visiting the site

Table 4.1: An empty version of the above table was presented to the participants during the interview. Participants were instructed to fill out the cells indicating which information about them they believed the corresponding entities could access when they performed the listed tasks with the Tor Browser Bundle. The above table shows the correct answers derived from the Tor Project documentation [70].

growing individual and societal importance.

- We uncovered and described important differences in how experts and non-experts understand and conceptualize Tor. Specifically, we showed that gaps and inaccuracies in non-expert understanding of the operation and threat model of Tor could lead to a sense of more or less privacy and security than is actually the case.
- We suggested solutions that could improve the Tor user experience and boost adoption by non-experts, many of whom are in vulnerable situations and/or serve as society's important actors.

In the next section we outline the method we used to conduct our study along with the details of participant recruitment and a description of the sample. Next, we describe our findings followed by a discussion of the insight that emerged. We proceed to apply the insight to suggest a number of potential improvements to Tor and other related aspects. We conclude the chapter by discussing some of the limitations of this work and leaving some closing remarks.

4.1 Method

To address our research questions, we conducted semi-structured interviews with individuals who reported using Tor. The subsections below describe how we recruited participants and provide the details of our study protocol. The protocol was approved by New York University's Institutional Review Board (IRB).

4.1.1 Recruitment

Recruiting Tor users for such a study is difficult because only a small proportion of the population uses Tor. Moreover, Tor users are likely privacy conscious and, as a result, may be unwilling to discuss their attitudes and behaviors, especially pertaining to their use of Tor. Therefore, we cast a wide net and utilized multiple channels to seek study participants. Such an approach was also aimed at increasing the diversity of the sample. Specifically, we advertised the study on the Tor community of Reddit,[1] the 'Et Cetera Jobs' category of Craigslist for the New York City area, and mailing lists and bulletin boards at New York University. When describing the study on Reddit's Tor community and at the university, we mentioned that the research was regarding Tor. In contrast, on Craigslist, we stated that we were studying software use, without specifying our focus on Tor. This dual strategy was adopted partially to overcome the difficulties of attracting Reddit and university participants for a general software study and partially to include participants with varying levels of familiarity and experience with Tor. Our Craigslist advertisement directed potential participants to a brief online screening questionnaire (see Appendix B). Along with age, gender, and email address, the questionnaire asked about the use of 14 technologies and online services, with 'anonymization software' as one of the options in the randomly ordered list. Those who indicated using anonymization software were contacted to ask if they had ever used Tor.

4.1.2 Participants

We set up interviews with the individuals who reported having used Tor and expressed willingness to participate in the study. Overall, we interviewed 17 participants (5, 2, and 10 via Reddit, university channels, and Craigslist, respectively): 10 males, 5 females and 2 who preferred not to reveal their gender. Apart from ensuring that each participant was above the age of 18, we did not collect age information in order to respect the privacy and anonymity of the participants.[2] Participant occupations covered a spectrum of technical sophistication from penetration tester to fitness trainer. As a token of appreciation for participating in the study, we offered each participant a $20 gift card for Starbucks. Many participants declined the reward, likely to preserve their anonymity.

[1] https://reddit.com/r/Tor

[2] Based on the responses to the screening questionnaire and our interactions with the participants, we estimate the age range to be 21–50.

4.1.3 Study Protocol

Prior to participation, we provided the participants with information on the purpose of the study along with the procedures followed for handling the collected data. Specifically, we stated that we would not collect any personally identifiable information and would treat all responses as anonymous and confidential.

After obtaining informed consent for participation (and optionally for audio recording the conversation), we interviewed the participants one-on-one using a semi-structured interview protocol (see Appendix A). When possible, interviews with the participants local to the New York City area were conducted in person at New York University. Others were interviewed via phone or conferencing software, with the exception of one participant interviewed via email[3] and two others interviewed using a text chat program.[4]

Each interview consisted of several open-ended questions. At the beginning, the participants were asked general questions about their occupation to make them feel at ease and establish rapport. After the introductory questions, the interview delved into the participants' use of Tor, beginning with how they discovered Tor and covering the details of why, where, when, and how they used Tor. We further asked the participants to describe their understanding of how Tor works.

For an elicitation of the participants' understanding of the underlying operation of Tor, we asked them to engage in a drawing task as suggested by Kearney et al. [37]. Specifically, we asked the participants to draw a free-form sketch of their views and understanding of Tor, including its various front- and back-end (i.e., visible and invisible) components, processes, and actors. We stated that the sketches may include information about data flows and access controls. As they drew, the participants were encouraged to vocalize their thoughts in order to allow the collection and comprehension of the corresponding detail. Those who were interviewed via phone, conferencing, chat, or email were asked to send a picture of the drawing to the interviewer. When needed, we sought clarification and asked follow-up questions during the task. All drawings were retained for analysis.

We next asked the participants to fill out a table to capture their awareness of the threats countered by Tor (see Table 4.1). The table included a set of tasks along with various entities involved in those tasks. The participants were asked to indicate

[3]The questions were sent to the participant in an initial email, with subsequent emails used to ask follow-up questions as necessary.

[4]These participants did not wish to reveal their voice and demanded a text communication channel with end-to-end encryption.

which pieces of information each of these entities could access when they used the Tor Browser Bundle to carry out each of the listed tasks. We encouraged the participants to think aloud when filling out the table. These answers, coupled with the responses to the other questions, allowed us to determine the participants' understandings of the potential deanonymization risks.

At the end, we asked the participants about the societal role of privacy tools, specifically in relation to contemporary national security debates and discussions in the US and Europe. We concluded the interviews with a brief multiple-choice questionnaire that used 5 questions on cybersecurity and anonymity taken from the 'Technical Knowledge of Privacy Tools Scale' from Kang et al. [36]. We chose this scale due to its topical relevance as well as short length. Participants who provided no more than one incorrect answer were marked as 'experts' with the remaining labeled 'non-experts.' These cutoffs were determined based on prior pilot testing with privacy and cybersecurity domain experts. Overall, 6 of our participants were classified as experts and the other 11 were treated as non-experts.

Most interviews lasted approximately 45 minutes. For the interviews that were audio recorded, the audio files were labeled with an anonymous identifier and destroyed after transcription. We analyzed the text of the interview responses along with the corresponding interviewer notes and the sketches collected during the drawing task. We followed an inductive process, allowing insight to emerge from the collected data. In order to avoid biasing the inductive analysis, we deferred a systematic review of the literature related to mental models of security and privacy tools until after the analysis was completed. The analysis included iterative open coding, axial coding, and selective coding [19] using the Atlas.ti software.

We began the three stages of coding – open, axial, and selective – right after the first interview. The coding proceeded continuously as the interviews were being conducted. During open coding, the text was coded sentence by sentence. Codes were created from the data with no initial hypotheses. For example, the sentence *"curiosity; I heard a lot of different things about it and was wondering how it works"* was labeled with the code 'being curious.' Axial coding examined the collection of codes generated by open coding and grouped related codes into categories. For instance, the codes 'feeling less watched,' 'feeling at ease,' 'evading surveillance,' and a few others were categorized under 'benefits derived from Tor use.' We further examined how frequently codes were mentioned together. Finally, in selective coding, the interactions between the categories and the codes were analyzed qualitatively and, to a smaller extent, quantitatively. The following sections describe the high level insight regarding user perceptions and

understandings of Tor that emerged from the analysis.

4.2 Findings

Unsurprisingly, we found notable and large differences between the experts and the non-experts in terms of understanding of the operation of Tor as well as the threat it counters. The experts exhibited deep knowledge of Tor's underlying operation while the views of the non-experts were simple and abstract. Notably, not all experts were free of gaps in knowledge that could potentially affect anonymity during Tor use. Interestingly, the experts focused on the *technical details* of Tor operation, while the non-experts were much more likely to situate Tor within a broader *sociotechnical* landscape of purposes, actors, and values. We unpack these results by discussing the details of the participants' understanding of Tor operation and threat model, respectively.

4.2.1 Mental Models of Tor Operation

As mentioned above, we uncovered differences in the mental models of the experts and the non-experts pertaining to how Tor operates as a system. However, within each of the two participant groups, the models exhibited common threads.

Experts View Tor as a Complex Network

The experts understood Tor as a complex decentralized network used to move packets of information from one node to another. When describing how Tor works, the experts focused on network related aspects, such as connections, paths between Tor nodes, routing, etc., along with technical details, such as encryption layers. For example, one expert discussed the evolution in his understanding of Tor operation using the technical jargon of computer networks:

"When I started off I understood [Tor] pretty crudely as just kind of a way to get past state firewalls and to hide your identity from Web sites you are visiting. As I continued to use it, it's really good for NAT [Network Address Translation] traversal for example. Like, if you want to host a Web site from your home address and you're behind NAT, a Tor hidden service is a great way to give you that kind of access." (P8, Expert, Male)

Typically, the experts viewed the Tor network as composed of three elements: a sender, a receiver, and a path of decentralized nodes connecting the sender and the receiver. Moreover, they frequently referred to themselves as the sender who uses the network of Tor nodes to send messages to various receivers. For example, consider expert P10's sketches of Tor operation; he drew two diagrams, one depicting a connection

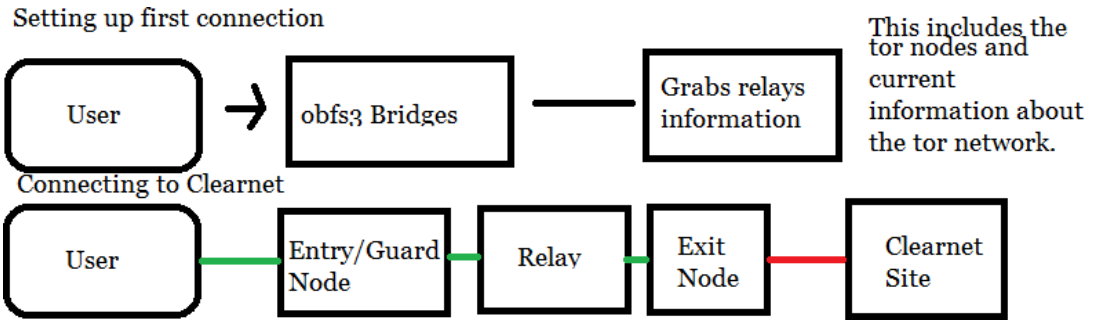


Figure 4.1: An expert's sketch of Tor's connection to a 'clearnet' Web site. (P10, Expert, Male)

from himself to a 'clearnet' site (see Figure 4.1) and another showing his connection to a Tor Onion Service (see Figure 4.2). In the first drawing, P10 indicated how relay information is loaded (including the possibility of a Tor bridge with obfuscation). The bottom half of the drawing shows that the traffic between the client (User) and the exit relay (Exit Node) is encrypted (green) and the traffic between the exit relay (Exit Node) and the Web site (Clearnet Site) is potentially unencrypted (red). In the second drawing, P10 showed the role of Tor Onion Service Directories, Rendezvous Points, and Introduction Points in connecting to a Tor Onion Service (Hidden Service). These drawings and descriptions present a mental model of the Tor network that demonstrates an understanding of the Tor system architecture akin to that of a Tor developer or researcher.

Other experts described Tor operation in varying levels of detail, with P10's being the most descriptive and complete. Despite differences in the level of completeness of the descriptions, all elicitations of the experts referred to the decentralized network nature of the Tor system architecture along with the role played by onion routing and encryption in the operation of Tor. For instance, the experts discussed the workings of Tor in terms of technical mechanisms, such as traffic obfuscation techniques, anti-tracking measures, latency reduction solutions, etc.

Non-experts Treat Tor as a Service

Seven of our non-experts began using Tor out of curiosity. This curiosity took different forms, with four curious about the 'Deep Web' and controversial hidden services and others about the ability to surf anonymously or bypass censorship. Similar to the experts, the non-experts viewed themselves as information senders within the Tor system. However, unlike the experts, the non-experts often treated several key components of Tor's network based architecture as an abstract and opaque 'black box' with certain

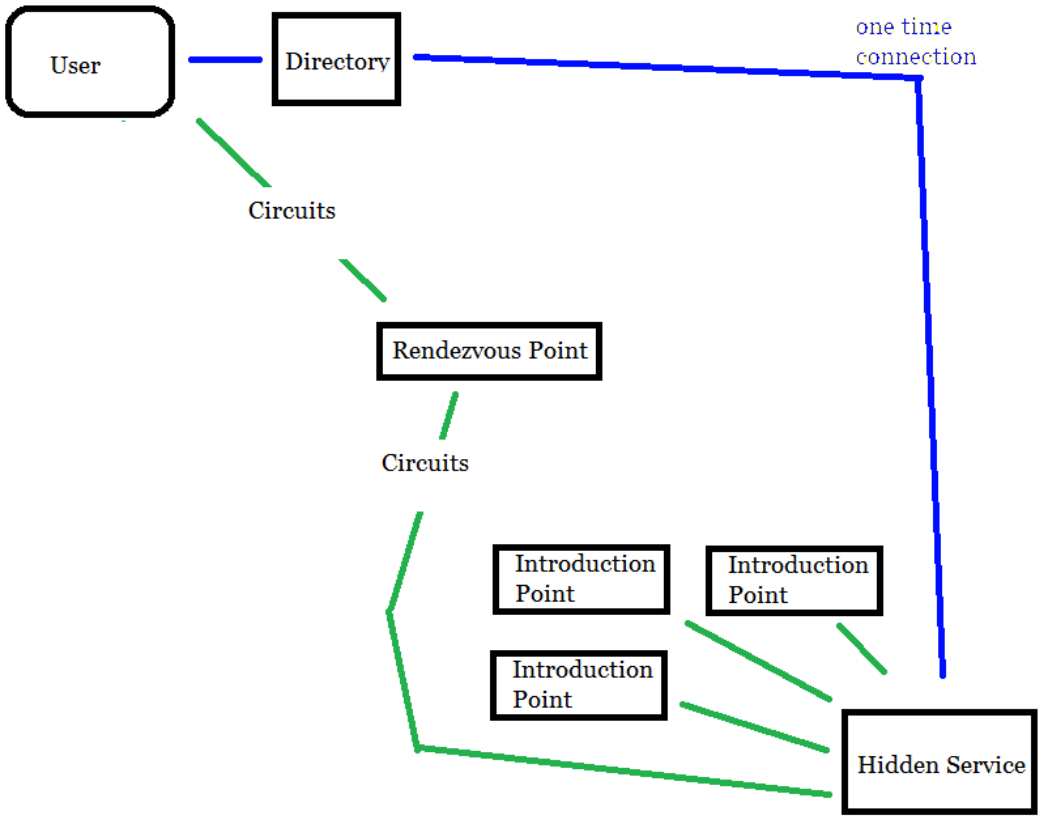


Figure 4.2: An expert's sketch of Tor's connection to a Tor Onion Service (Hidden Service). (P10, Expert, Male)

inputs and outputs. Specifically, we noted that the non-experts tended to treat Tor as a 'service.' They described calling upon the Tor service to perform specific functions, such as "*bouncing signals*" (P3, Non-expert, Male) or "*providing security*" (P11, Non-expert, Male). For instance, non-expert P17 drew his model of Tor as a service that provides a "*new me,*" obscuring his identity from those he is connecting to (see Figure 4.3). Additionally, Figure 4.3 reveals that the non-experts often mistakenly understood the Tor 'service' as *centralized*, with an administrator watching over and controlling the operation of individual Tor nodes. Only one non-expert correctly mentioned the decentralized nature of Tor nodes.

Different non-experts believed that the Tor service performed different functions; some said it provided security, others mentioned it made them anonymous, and still others stated it granted them access to previously inaccessible sites and resources. These functions were seen as enabling Tor to help the user achieve specific goals and tasks.

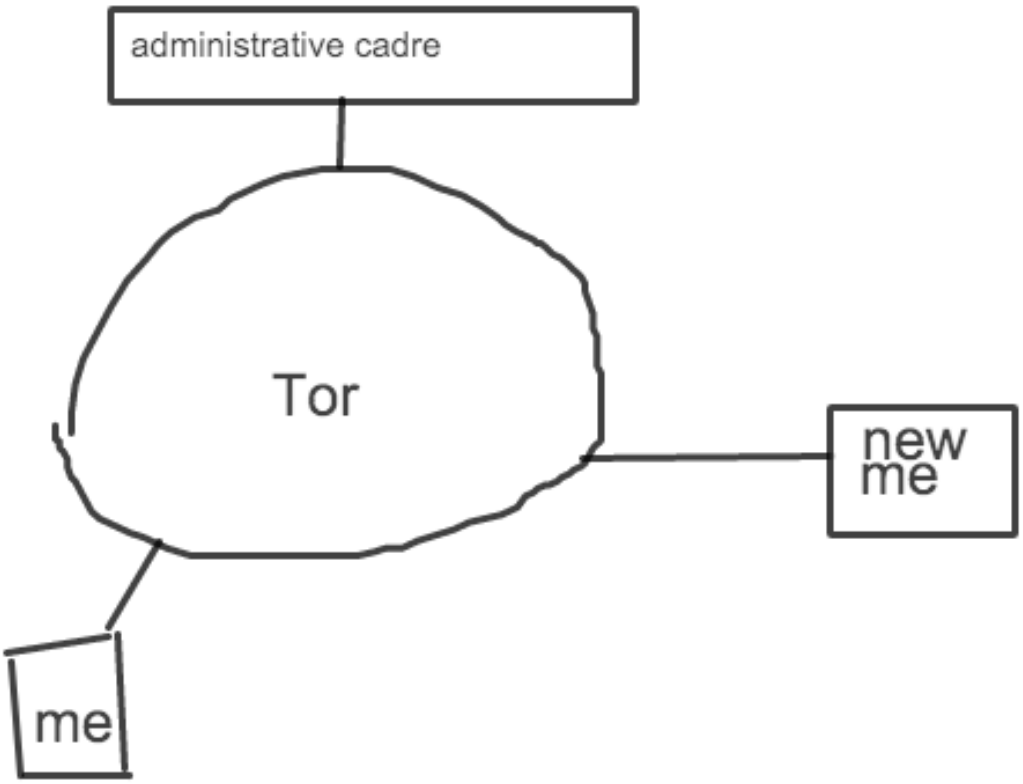


Figure 4.3: One non-expert's sketch describing Tor as a service with an administrative section watching over its inner workings. (P17, Non-expert, Male)

These included tasks such as visiting sites that the participant wished to conceal from the spouse, accessing geographically restricted content, circumventing content restrictions of filters and firewalls, etc.

While all non-experts described Tor as an abstract service, some descriptions exhibited more technical sophistication than others. For example, one participant mentioned that Tor may assign a new IP address, showing some understanding of the role of an IP address as an identifier.

"And then like IP address . . . I don't know . . . does Tor jumble up your IP? Maybe, perhaps it does, perhaps it doesn't. Perhaps it gives you a new IP." (P2, Non-expert, Female)

Three non-experts mentioned cryptography, even though they did not understand the role it played in the operation of Tor. Two non-experts mentioned 'signal bouncing' without explaining how it was accomplished.

"Like, the signal gets split up among other things, that would be cool if that happens, not too sure how that works, but I don't have an extensive knowledge of that."

(P2, Non-expert, Female)

"As far as I'm aware the way it works is it bounces your signal around a lot . . . To various countries and such." (P3, Non-expert, Male)

It should be noted that there was a large degree of uncertainty among the non-experts about their understanding of the operation of Tor. While some non-experts were confident in their answers, five seemed unsure that their understanding was accurate or complete. For instance, when P2 was asked to clarify her idea that Tor performs *"signal dispersion,"* she replied that it works with *"cryptography,"* admitting that she did not know what that meant, indicating confusion between terminology and operation. Other non-experts simply stated that they did not understand how Tor worked, but knew that it did.

"It's one of those things where I know it works, it exists." (P9, Non-expert, Female)

Five non-experts described their understanding of Tor operation through metaphors. For example, one non-expert stated that it worked just like a faucet: *"if one turns the handle, the water appears"* (P9, Non-expert, Female). P11 clarified his sketch of Tor by equating it with Fort Knox, through which his traffic passed in order to become secure. This demonstrates his conception of Tor as a central service meant to secure, rather than anonymize, his traffic.

"Let's say I am like a circle. I am a circle on the left side. Inside of the circle I have for example, let's say I have my laptop and this for example would be down, hanging down. And on this it says it's my computer or it's my laptop. So that's on the left side and above that for example you can put any human picture and I give it a face. In the middle for example you will have a wall like Fort Knox and that would be in the middle obviously with no face because . . . it's not human and on the right side it is also a circle and that would be another computer with another human face." (P11, Non-expert, Male)

Many metaphors utilized by the non-experts described the ideologies and the values that the participants believed Tor stands for. For instance, P14 referred to Tor as the Statue of Liberty, bringing liberty to those who use it.

"Yes, the Statue of Liberty on Ellis Island. So just to describe to you we can probably explain it as giving us liberty to watch what I need, you know, and so at the same time [providing] freedom." (P14, Non-expert, Male)

Another example is a non-expert drawing Tor as the Tree of Knowledge (Figure 4.4), granting access to many different branches of knowledge.

"Tor ties in with the Tree of Knowledge for the simple reason that it's one of the best forms of confronting knowledge. Because there's no filters really on Tor." (P9,

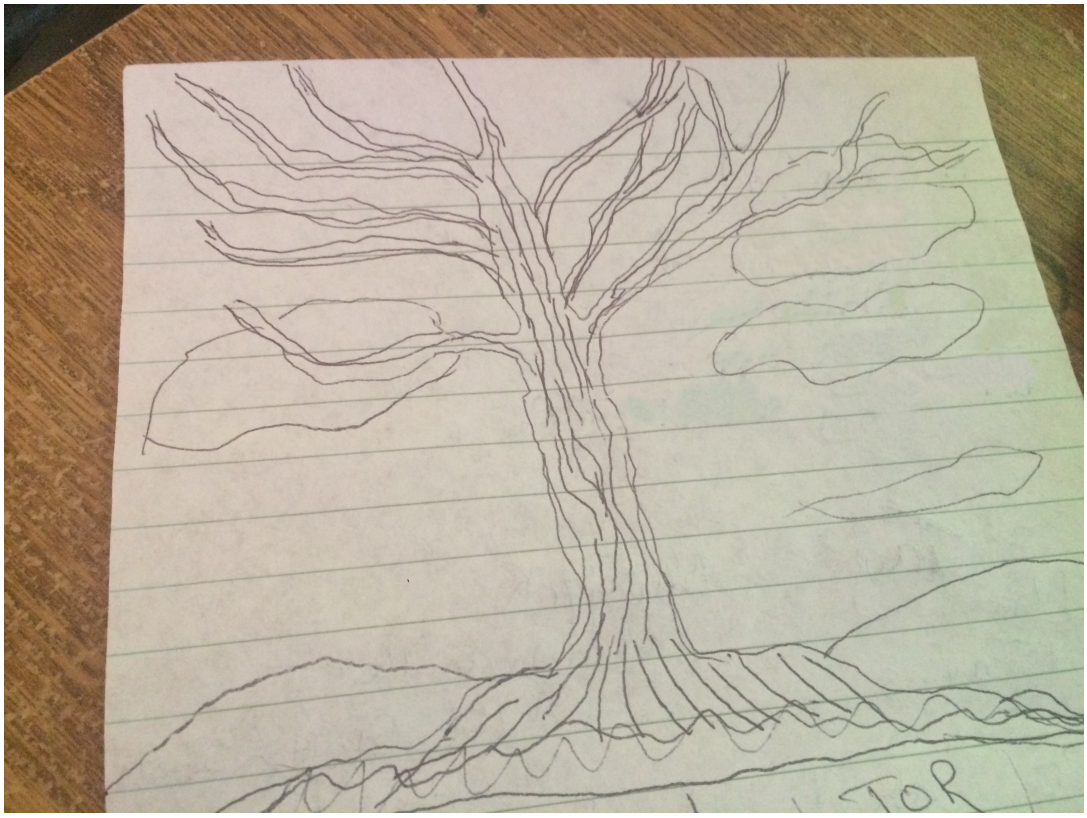


Figure 4.4: One non-expert's sketch depicting Tor as the Tree of Knowledge. (P9, Non-expert, Female)

Non-expert, Female)

Apart from underscoring the non-expert treatment of Tor as a service, these metaphors also reveal that the non-experts often viewed Tor as a tool for social good. This aspect was mentioned in multiple non-expert interviews, with the participants discussing Tor as a tool used by activists, journalists, and ordinary citizens for communicating freely without surveillance, bypassing state censorship, and achieving empowerment in civic engagement.

4.2.2 Threat Model Addressed by Tor

During the interviews, we attempted to discover the participants' understandings of the threat model of Tor. We discovered misunderstandings of the following threats to anonymity on Tor:

1. **Client side scripting:** Client side scripting may place users at risk. For example, Flash code running outside the browser's control can be used to deanonymize users.

Similarly, various vulnerabilities in JavaScript running within the browser can be exploited for deanonymization.

2. **Browser fingerprinting:** When Tor users use a browser other than the Tor Browser Bundle over the Tor network, the browser sends information to visited sites, such as installed add-ons, version, etc. Since the number of people with matching sets of information is likely to be low, the browser fingerprint lowers anonymity, with the worst case being unique identification.

3. **Side channel leaks:** Information provided by users to third parties external to Tor, such as login credentials, credit card numbers, or even language choice, can be used to denanonymize the user to varying degrees. In addition, if users do not ensure the use of encrypted connections, their information can be accessed by the exit node on their Tor circuit.

4. **Node operation:** Tor nodes are independently owned by volunteers. As a result, data flowing within the network is not controlled or seen by any single party, including the owners and the operators of the Tor Project itself. As a result, it is possible for malicious actors to run Tor nodes with the aim of attacking users who utilize the node (which is typically an exit node).

Similar to the operational details of the Tor system, the experts and the non-experts differed in the understanding of the threat model that Tor addresses. We discuss each in turn.

Experts Mostly Grasp the Threat Model

The experts showed a reasonably accurate understanding of the threat that Tor attempts to counter. Importantly, they understood that Tor is not a *complete* solution for all potential anonymity related issues and additional steps may be needed to achieve the desired level of anonymity. For instance, when filling out Table 4.1, expert responses revealed that they understood the complexities of the different browsing tasks and situations. These complexities are tied to the threat model of Tor. For example, all experts understood that logging into a Web site could deanonymize them. When asked whether the email service could access any information when reading email using the Tor Browser Bundle, the response of one expert demonstrated his understanding of the limits of Tor's protection:

"Yes they do, because you have an account with them. Assuming you've provided personal information, they kind of know who you are and, you know, what you've sent,

but they still don't know where you are. You've still obscured your IP address." (P1, Expert, Male)

Further, all experts mentioned that the traffic exiting a Tor exit node may not be encrypted, again demonstrating the limitations of the protection Tor provides.

"Between the laptop and the entry I will write a little note that says ISP can see that I'm using Tor. And then between the entry and the middle I'm going to say 'encrypted traffic.' And then between the middle and the exit I'm going to say 'encrypted traffic' and between the exit and the Web site I'm going to say 'ISP can see requests, but not the originator."' (P1, Expert, Male)

In addition, many experts understood that the threat model of Tor allows a certain number of compromised Tor nodes, and that some of the Tor nodes might be a threat.

"Nodes may be owned/0wned[5] *by governments."* (P5, Expert, Unspecified gender)

Though the experts understood the threat model, all but two of them neglected to mention the Tor Browser Bundle as a part of the Tor system, mentioning only its network elements, such as the nodes, and security elements, such as encryption. Two experts configured their own Web browsers or used other non-standard ways to connect to the Tor network to receive Web content. This makes them vulnerable to fingerprinting attacks mentioned above, thus leading to potential deanonymization. Moreover, using a Web browser other than the Tor Browser Bundle is complicated and could lead to mistakes such as DNS leaks caused by a misconfigured browser resolving DNS requests independent of Tor. One expert stated that he used *wget* (an alternative tool for Web content retrieval) over Tor, which has a similar effect if the user does not anonymize the USER-AGENT string.[6]

Non-experts Conflate Threat Models

Unlike the experts, the responses of the non-experts revealed a lack of consensus regarding the threats that Tor addresses. While some non-experts possessed a complete understandings of the Tor threat model, five believed that Tor provided more security than it actually does. For instance, one non-expert believed that Tor was a tool for protecting sensitive data, such as credit card numbers, in transit on the Internet.

"It's going to something and entering my credit card or some kind of financial or some Web site where I don't want them to have my information because they're going to follow me." (P13, Non-expert, Female)

[5] 0wned here refers to the computing slang term indicating a device being taken over and controlled by an external party, with or without the knowledge of the device owner.

[6] A USER-AGENT string is a line of text containing information about the browser or the program.

Another non-expert believed that Tor kept one anonymous from one's email provider, even when logged into the service. Other non-experts, however, held the view that Tor did not offer complete protection, with four claiming that Tor is effective for privacy protection from entities such as advertising networks, but not from governments and ISPs. Two others believed that the Tor Project has access to all traffic on the Tor network and could provide it to governments and law enforcement agencies. One non-expert argued that the Tor Project does not provide such access only because doing so would be counter to their goals.

"I know that I'm not doing anything dangerous but they don't know that, so I can see why the government would want to have access to that kind of thing. Or maybe they can receive alerts from Tor saying 'hey this person is suspicious by your standards' . . . but that's bad business, so. . . " (P4, Non-expert, Female)

Two non-experts claimed using Tor to circumvent geographical restrictions imposed by Web sites, such as Hulu, Netflix, etc. Yet, many of these sites run Adobe Flash or JavaScript, which can not only deanonymize users but also leave them vulnerable to injection attacks from malicious Tor exit nodes.

In general, the non-experts operated with incomplete, and sometimes inaccurate, understanding of the Tor threat model, often conflating it with other threat models that Tor is not designed to address. These gaps and inaccuracies could lead to a sense of more or less anonymity and privacy than is actually the case.

4.2.3 Discovery and Use of Tor

We examined how the participants discovered Tor, why they used it, and how long they had been using it. There are no real distinctions between the experts and the non-experts regarding the discovery of Tor. Both groups primarily discovered Tor through news articles, and many participants reported discovering it around the time of the initial publication of the Snowden documents. Some exceptions exist, with five participants finding Tor through searches on popular search engines or hearing about it from friends. One participant discovered Tor at a conference, and two participants (both experts) did not remember how they discovered Tor. In terms of use, however, we found significant differences between the experts and the non-experts.

Experts Used Tor for Many Reasons

All experts reported that they used Tor more frequently and for more purposes than the non-experts. A few experts used the Tor Browser Bundle as their primary browser, using it for most tasks and reserving non-anonymous browsers, such as Google Chrome

and Mozilla Firefox, only for tasks which are ill-suited for the latency Tor creates (e.g., video streaming, etc.).

"I use [Tor] primarily as my everyday browser for most of my tasks. But I use regular Firefox if I want to do something, if the Web site is blocking Tor or if I want to do something on localhost that doesn't need outside Internet access." (P1, Expert, Male)

In addition to anonymous browsing and censorship circumvention, the experts mentioned alternative uses of Tor apart from Web browsing, such as downloading via alternative means such as *wget*, circumventing NAT using Onion Services, etc.

"So if I'm at school I can use Tor to ssh into a computer on my home network and it's not a problem. I don't have to deal with all of the IP address stuff." (P8, Expert, Male)

Curiosity differed between the experts and the non-experts. The experts tended to be curious about the network and its components, rather than the information held in Onion Services.

"Pure curiosity drove me toward it. It was just a different way of distributing information systems, so it was like, hmm, if we could do it a bit differently that would be a bit better." (P10, Expert, Male)

Additionally, the experts who started using Tor out of curiosity tended to remain Tor users and become more involved in the Tor community, while the non-experts who started using Tor due to curiosity stopped using it relatively quickly.

Non-experts Have Specific Motivations

Although the non-experts mentioned a variety of reasons for using Tor, all but two used it only within the context of a single specific purpose. Non-expert motivations for using Tor included: satisfying curiosity regarding the content accessible via Tor, bypassing censorship, circumventing geographical restrictions imposed by Digital Rights Management (DRM), countering surveillance by governments as well as other parties such as advertisers, communicating with activists, protecting the discovery of one's visits to pornography and gambling sites, researching sensitive legal matters, etc.

The non-experts who used Tor out of curiosity tended to be more curious about the information available via Tor rather than about the operation of the anonymity system itself. Specifically, the non-experts were drawn to information available on Onion Services, also called the 'Deep Web.'

"To be honest, the Internet black market. Uh, yeah, just to access it and see what's up. Um, the 'Deep Web.' Yes, that's it, the 'Deep Web."' (P2, Non-expert, Female)

Four non-experts believed that Tor was designed primarily in the context of their own specific use case. For example, one non-expert used Tor only when abroad in a country that censored Web sites.

"I was using [Tor] because I was living abroad and I wasn't allowed to access certain sites... I was looking for ways to access these sites or rather looking for ways to get around the countrywide ban." (P4, Non-expert, Female)

She stated that Tor was not very needed in the US because the US government did not block many Web sites.

"I feel like it's less relevant in the US for the average user because the US doesn't block too much. They don't block Facebook and they don't block Google or that sort of thing. Whereas within a lot of foreign countries there's a lot of content that the US would consider benign that the governments wouldn't want you to access." (P4, Non-expert, Female)

Another non-expert used it only when performing credit card transactions, believing Tor to be a tool meant to safeguard data in transit.

Similarly, the non-experts tended to focus on only one adversary while using Tor. For example, one non-expert claimed that she used Tor because she did not want the government to see that she had looked up drugs, contract killer postings, and other such information.

"I just kind of used it those few times to look on the Internet and be like 'look how much acid costs on the Internet' and then like...find all the Web sites that are like oh I'm a hitman and I'm going to kill the president for a few million dollars...I like the president, but ...I was kind of like just lurking and seeing what's up. That was the main purpose and I didn't really want to get like a knock on my door, which they do in China...So that's like something that I'd like to avoid, which I'm sure doesn't happen as frequently in the States but...I don't like want to get arrested for some unrelated incident and then have my record like....my computer searched, and then its like 'You were looking at hitmen, what's up with that?"' (P2, Non-expert, Female)

Lastly, half of the non-experts reported using Tor infrequently or having quit using it altogether, citing a lack of need or fading curiosity for the tool as their reasons.

4.2.4 National Security and Tor

In contrast to other aspects, we found no major differences among the experts and the non-experts regarding the relationship between Tor and national security concerns. When asked about the morality of Tor and its role in national security, most participants stated that Tor was a trade-off between privacy and national security and acknowledged

that it likely made law enforcement more difficult. Yet, all but one participant believed that Tor was a good tool and the balance between individual privacy and national security should be closer to privacy.

"On balance I think that the good parts outweigh the bad parts and that they are necessary regardless of what we might think of the bad parts. So obviously properly implemented secure communication technologies will always be problems for law enforcement and intelligence agencies because they depend on sort of exclusive access to our data as part of their job. But . . . I mean that's fine but there are other things at stake, right? There's individual liberty, there's freedom of speech, there's freedom of association, there's the ability to have secure technologies that will protect really important sensitive information, you know embarrassing stuff or your credit card number." (P8, Expert, Male)

There were some exceptions, however. One participant believed that privacy and national security are synergistic, and the protection of the rights of the people, including privacy, is itself a matter of national security.

"In my opinion, security is directly related to privacy and so is privacy to anonymity. I feel stronger tools are needed and are a benefit to society. Giving up any of the three (security, privacy, anonymity) means you can have none of the above. I understand the national security threat when the 'bad guys' use these tools, but they won't follow the rules anyway." (P6, Expert, Unspecified)

Another participant believed that Tor was detrimental to national security and should include a back door that allows access to the government.

"For national security reasons there is a need to have back hole [back door] access to certain things . . . Tor is something that can be a very positive tool but at the same time it is used by a lot of illegal entities . . . everything from child pornography to black market smuggling to terrorism, finances, planning, and coordination and so in that sense I think that there needs to be a certain degree of control from a government perspective." (P17, Non-expert, Male)

It must be noted that the views of the non-experts on this matter may have been influenced by some of the misunderstandings described in Sections 4.2.1 and 4.2.2. Specifically, a few non-experts believed that intelligence agencies, such as the Central Intelligence Agency (CIA) and the National Security Agency (NSA), are capable of defeating the protection Tor provides and have access to Tor network traffic. As mentioned earlier, one participant believed that Tor was capable of giving notices to the government if a Tor user is deemed suspicious by government standards, but would not do so because of the business implications of such an action. Yet, most non-experts

Category	Expert	Non-Expert
Mental Model	Complex network	On-demand service
Threat Model	Multiple threats	Specific (single) threat
Frequency of Use	Frequent	Mostly for specific uses
Discovery	Varied	Mostly through news
Morality of Tor	Good, positive	Varied, mostly positive

Table 4.2: Comparison of notable aspects of the understanding and the use of Tor across the experts and the non-experts.

believed that Tor helped foster important sociotechnical values, such as freedom of speech, uncensored information access, privacy, and personal security.

4.3 Discussion

Table 4.2 summarizes the notable aspects of our findings across the experts and the non-experts. In addition to the findings related to our research questions, we found that several experts and non-experts mentioned enhancing their anonymity and privacy by engaging in 'compartmentalization' via the use of a separate device for Tor use. Such a practice indicates greater attention to privacy and security among Tor users in comparison with non-users. While the adoption of Tor in the general population remains low, our sample shows that its user base is heterogenous and not composed only of domain experts with deep technical knowledge.

As expected, our findings confirm that the extent to which non-experts grasp the operational details of Tor differs substantially from the level of understanding of experts. Non-expert understanding of the operational details of Tor varied widely, possibly because of the differences in the frequencies and the motivations of use. Our findings

shed light on the nature of these differences in terms of mental models and threat models. Regardless of the technical sophistication of these mental models, Tor, like any privacy enhancing technology, would benefit greatly from understanding and utilizing the mental models of its users [73]. For instance, the user interface as well as the documentation of Tor could draw upon the mental models to present the operational concepts more effectively.

The experts exhibited useful and complete knowledge of the Tor architecture and operation along with a nuanced understanding of its threat model. In contrast, the mental models of the non-experts were incomplete and overly abstract, leaving out or distorting important details that impact anonymity and privacy. For instance, bounding the entire Tor network within a single box may create a false sense of privacy and security by ignoring the potential attacks by malicious exit nodes, such as capturing sensitive information passing through the node via insecure protocols [46]. Moreover, users operating under an assumption of anonymity may engage in behavior they might not want tied back to their identity. In contrast, viewing Tor as a centralized service could lead to the opposite effect. A belief that external parties, such as governments, law enforcement agencies, ISPs, and the Tor Project, can access decrypted Tor traffic has the potential to create a chilling effect, leading to self-censorship as well as unwillingness to use Tor. As mentioned earlier, even some experts exhibited gaps in understanding and engaged in behaviors that left them vulnerable to specific attacks, such as DNS leaks. This underscores that even the smallest of gaps in knowledge has the potential to defeat the anonymity protection a user seeks via Tor. Some of these issues, such as DNS leaks, can be addressed by the Tor software itself,[7] while others can be addressed by explicitly documenting the dangers of non-standard uses of Tor.

Tor is used by experts and non-experts across the world for a variety of purposes. Many of these purposes involve society's important values and causes, such as circumventing censorship, avoiding surveillance, sharing sensitive information of journalistic importance, communicating with informants, and so on. In addition, Tor serves sensitive and valuable personal purposes, such as protecting one's online activities from an abusive partner, avoiding targeted advertising, etc. In a large majority of these situations, the users involved are non-experts. In such circumstances, gaps and inaccuracies in the understanding of the operation and threat model of Tor that lead to deanonymization may hold serious repercussions, including account compromises, identity theft, financial losses (resulting from fraud), surveillance of communication and movements,

[7]For instance, DNS leaks can be addressed by raising a warning when the Tor network proxy receives a numeric IP address instead of a request for resolving a text based domain name.

civil or legal penalties, physical and/or psychological abuse, imprisonment, or, in extreme cases, death.

Interestingly, the responses of our non-experts show that they placed importance on the societal values that Tor aims to promote along with the corresponding usage scenarios tied to those values. Indeed, some of them seemed to be using Tor to make a value statement related to civil liberties and democratic principles, such as privacy, anonymity, freedom from surveillance, personal liberty, censorship circumvention, freedom of expression, etc. While the experts also recognized the connection of Tor to societal values, they preferred to describe Tor in terms of the architectural and engineering details of the software and the network. When considering whether Tor poses a problem for national security, participant opinions ranged from asserting that Tor acts as a force for freedom to believing that Tor is a tool for cybercriminals and terrorists.

Regardless of how they discovered Tor, the experts reported using Tor more frequently and for longer periods. In contrast, the interest of the non-experts tended to fade, with many claiming that they saw no need for the tool. While these usage differences have previously been observed in other privacy tools as well [59], they are especially crucial for an anonymity system such as Tor because the efficacy of its protection improves with an increase in the number of users. Given the awareness of Tor's value proposition exhibited by the non-experts, emphasizing that the use of Tor is a community and societal contribution could potentially boost its adoption.

A typical goal of Human Computer Interaction research is creating user experiences that facilitate effective use of a system without requiring deep knowledge of the underlying operation, thus making it easily accessible to non-experts. As discussed in Section 4.4, our findings can be applied to improve the Tor user experience for non-experts. However, a key aspect where Tor differs from typical systems is its use as a privacy and security tool, sometimes under circumstances of great importance as well as danger. As such, an incomplete or inaccurate understanding of its operational details has the potential for individual as well as societal harm. These risks lead to a tension between the need to promote technical understanding of the operational detail and the goal of making such knowledge unnecessary as a requirement for the correct use of the system. Addressing the issues uncovered by our findings could be a step in the direction of mitigating the potential risks and resolving the tension between the simultaneous needs for revealing as well as abstracting away the technical details of Tor operation.

4.4 Implications

Our findings can be applied to improve the Tor system in a variety of ways. These include refining the design of the user interface and the user experience of the Tor Browser Bundle, targeting specific operational aspects for enhancement and optimization, and facilitating learning, especially for non-experts. We discuss some of these below. In addition to these improvements, our data suggests that Tor users desire a reduction in latency.

4.4.1 Route Information

As discussed earlier, non-experts conceptualize Tor as a centralized service. A possible solution to avoid such a misunderstanding could be displaying information about the ownership of each Tor node in the current connection's route, when such information is available and verifiable. Such a feature would be an extension of the current Tor Browser Bundle functionality that allows clicking the onion logo to display route information, such as the node IP address and the country. It might also be useful to make such information readily available in the background without the need for explicit click-and-seek. The feature could be further expanded to indicate the encryption status of each link within the current route.

4.4.2 Safe Script Execution

Our findings suggest that a notable barrier to the adoption and the use of Tor is the demand and the need for using Web sites and services that utilize JavaScript. JavaScript is so ubiquitous that disabling it makes a large proportion of popular Web sites unusable [68]. As mentioned earlier, enabling JavaScript while using Tor may lead to deanonymization [69]. We advocate investigations of operational and architectural modifications that reduce the attack surfaces opened up by enabling JavaScript within the Tor Browser Bundle. Such technical improvements could facilitate a reasonable balance between preserving anonymity without overly compromising usability and utility.

In addition, the Tor Browser Bundle should be modified to warn users that it defaults to a *low* security level that has JavaScript enabled. In the current release, one must open a menu accessible by two clicks in order to discover this default setting. A prominent visual indicator of the current security level should be available at a glance in the Tor Browser Bundle interface.

4.4.3 Tor Friendly Web sites

In line with the empirical findings of Khattak et al. [38], most of our participants mentioned routinely having trouble due to the restrictions many Web sites place on Tor traffic. These sites typically restrict Tor traffic even under situations that pose minimal risk to the server, such as fetching static Web pages that do not involve user interaction or data input. We recommend that Web sites, especially those providing important information such as government Web sites, provide 'Tor friendly' versions of the pages that allow Tor users to at least fetch information, even if specific mechanisms, such as posting, are disallowed to protect against abuse. In addition, using CAPTCHAs to prevent abuse by Tor users should be limited only to submitting POST data, permitting GET requests without submitted parameters to proceed without such checks.

Moreover, site owners could consider serving an alternative Tor friendly version of the site for connections from Tor exit nodes. The process of creating such a Tor friendly version of a site could be made easier by promoting the creation of plugins for common Web development platforms, such as WordPress and Dreamweaver. Such plugins could ensure that Tor nodes are not blacklisted and automatically create versions of Web pages that reduce the amount of JavaScript to the bare minimum, or possibly none.

4.4.4 Compartmentalization

Our participants reported using the privacy enhancing strategy of compartmentalization by separating different tasks or personas through the use of separate computers and/or software. Yet, most current programs and operating systems make it challenging, if not impossible, to achieve meaningful compartmentalization of digital activities. We advocate explicit attention by system designers and Tor developers to the provision of compartmentalization functionalities as a privacy and security enhancing feature.

4.4.5 Maintaining Workflow

Although many participants in our study compartmentalized their Tor use, some participants indicated frustration at the burden of switching away from Tor in order to complete the tasks that could not be performed via Tor. These tasks included visiting Web sites that depend on flash or Java plugins or those that explicitly block Tor traffic. Currently, when a user wants to perform such tasks he or she must manually switch to another browser and copy/paste the site address. Subsequently, the user must remember to switch back to Tor once the task in the other browser is completed. While the task is ongoing, the user must switch back and forth between Tor and the other browser. The

desire to minimize the disruption caused by the burden and frustration of managing the workflow and task switches can lead users to choose a non-Tor browser as the default. We suggest adding functionality within the Tor Browser Bundle that makes such task switches easier and faster whenever a task necessitates the use of a non-Tor browser. Such functionality has the potential to increase Tor adoption and usage by making it easier for users to stay within the Tor system as much as possible, switching away from Tor only when absolutely necessary for the task at hand. In addition to benefiting the individual user, increasing the time users spend using Tor would boost the overall utility of Tor by increasing the number of active users at any given time.

4.4.6 Contextual and Personalized Training

It would be beneficial to explore training and learning opportunities for non-experts in order to promote the development of useful conceptualization of the operation and threat model of Tor. Training has been shown to be effective in other cybersecurity domains, such as phishing [41]. In addition to an explicit focus on non-experts, training mechanisms could be customized to the person(s) and situation(s) at hand. For instance, different training modules could be developed for common use cases, such as circumventing censorship, avoiding surveillance, communicating securely and anonymously with a journalist, etc. Training activities could even be embedded into the user experience of the Tor Browser Bundle in a manner that utilizes learning theories and techniques, such as gradual knowledge building, periodic repetition, and effective assessment.

4.5 Limitations

A few limitations must be kept in mind when considering the generalizability of these findings. While we continued iterative coding of the interview responses until sufficient understanding emerged, we were unable to engage in purposeful additional sampling aimed at filling gaps. Although such a step is common in inductive qualitative analysis, the difficulties in finding and recruiting unbiased and unprimed Tor users limited our sampling efforts. Despite this limitation, we believe we reached reasonable saturation for the research questions at hand. In addition, the inherent difficulty in recruiting Tor users without bias or priming means that our study has a small sample size compared to other research on mental models. Further, advertising in Tor-specific groups such as Reddit's Tor community may have introduced bias in the sample. For privacy and anonymity, we did not collect demographic data beyond gender. As a result,

we cannot account for cultural differences. Although we cannot be certain, advertising in online and offline communities in English leads us to believe that most of our participants were native residents of the US or Canada. Finally, we point out that our findings are derived from self-reports. Consequently, it is possible that the participants omitted, forgot, or misrepresented their understanding and behavior.

4.6 Conclusions

In this chapter we explored the mental models of Tor users. Specifically we performed semi-structured interviews with 17 participants, 6 experts and 11 non-experts. These interviews sought to understand why individuals used Tor and how they believed Tor worked. Data from these interviews were analyzed using open coding, axial coding, and selective coding as inspired from grounded theory.

From this analysis we saw that experts and non-experts had very different mental models. Experts had a more complete mental model and viewed Tor as a distributed network with many actors. Non-experts had a different view, instead viewing Tor as a centralized service that they could use to achieve anonymity. Reasons for using Tor differed across experts and non-experts, with experts citing more varied reasons for using the Tor software and focusing on the technical elements of the software and non-experts citing specific motivations and only using Tor within that specific purpose.

Perhaps surprisingly, both experts and non-experts showed misunderstandings of the threat model that Tor addresses, potentially leaving both groups vulnerable to attacks. Non-experts had varied misunderstandings of the threat model, with some believing that Tor was stronger than it actually is, and others believe that it is weaker. Some experts stated that they configured an unrelated browser like Firefox to use with Tor, which demonstrates a misunderstanding of the fingerprinting threats that exist at the application level.

Based on these findings we proposed recommendations to the Tor Project to make Tor more usable for both technical and non-technical users. These recommendations included making Tor circuit information easier to find, aiding Tor users in switching their workflow, aiding users in compartmentalization, and other recommendations.

After learning more about Tor users and discovering that there existed both expert and non-expert users of Tor, and learning that some of these users use the Tor Browser as their default browser, we moved on to discover what issues these users face when using the Tor Browser in a naturalistic way. This project is discussed more in the next chapter.

Chapter 5

Measuring the UX Faults of the Tor Browser

Our previous research project had shown us that Tor had two groups of Tor users, a highly technical set of users and a non-technical set of users. These two groups used Tor for different reasons and in different ways, with the highly technical users using Tor beyond just the Tor Browser. Non-technical users, however, mainly interacted with the Tor Browser and used Tor for curiosity or for specific purposes. Though we now understood why and how people used Tor, we did not understand what issues users would run into when using Tor, especially the when using the Tor Browser. Though previous work had discussed the issues that Tor faced on the network level, no recent research existed to study the recent iterations of the Tor Browser. That lead us to ask the question:
How do users experience routine Web browsing when using the Tor Browser?

We addressed this question via a study that examined the use of the Tor Browser in a naturalistic setting for a period of one week, focusing particularly on identifying frustrations, confusions, and problems. To this end, we collected quantitative and qualitative data on the use of the Tor Browser for routine Web browsing and online tasks. Based on 121 questionnaire responses, 11 interviews, and 19 write-ups from 19 study participants, we reported on a number of UX issues, such as broken Web sites, latency, lack of common browsing conveniences, differential treatment of Tor traffic, incorrect geolocation, operational opacity, etc. Specifically, we made the following contributions:

- ***Detailed account of naturalistic use of the Tor Browser.***
  We collected data regarding Tor Browser usage for routine online activities in a naturalistic setting, uncovering a number of important UX issues.
- ***Suggestions for improving the Tor Browser UX.***

Grounded in the UX issues encountered during our study, we identified and outlined several practical solutions and design guidelines to address and mitigate the problems and improve the UX of the Tor Browser.

- ***Method for privately collecting naturalistic quantitative data on the Tor Browser UX at scale.***
  Our method for collecting quantitative UX data on Tor Browser usage could be deployed to allow privately gathering naturalistic data at scales significantly beyond those possible in typical laboratory studies. Thus it is a contribution of this dissertation in addition to the understanding we gleaned from it.

In the sections that follow, we first describe our method, including study setup and sample. Next, we present and discuss the quantitative and qualitative findings on the Tor Browser UX. We discuss application of the findings to derive practical suggestions for improving the UX of the Tor Browser to help expand its user base and support non-experts. Finally, we point out important limitations of our study.

5.1 Method

We tackled our research objective by studying naturalistic use of the Tor Browser. In the following subsections, we describe the rationale behind our study design, details of participant recruitment and study deployment, and approaches used for data analyses, respectively.

5.1.1 Study Design and Instruments

We wished to collect data from individuals as they used Tor Browser for their routine online tasks. To ensure sufficient data quality and quantity, we used three separate data collection mechanisms: opportunistically timed short online questionnaires, open-ended written self reports, and one-on-one semi-structured interviews. Collectively, the three approaches were designed to meet the following requirements:

- Use a lightweight mechanism with minimal burden that does not require instructions.
- Respect privacy by avoiding capturing screens and URLs (unless provided voluntarily).

- Be independent of a specific place or time, thus allowing collection to occur at the participant's convenience.
- Capture sufficiently detailed information (as in a controlled laboratory setting).
- Span a reasonable period that constitutes extended use.

Specifically, we designed three online questionnaires to gather information whenever participants experienced a problem with the Tor Browser. Each questionnaire asked for the nature and details of the problem along with the option to provide the Web site(s) involved. If no problem was encountered, the questionnaire could be closed without answering. The questionnaires respectively targeted the following three circumstances: ending a Tor Browser session (*Tor Browser Questionnaire*), switching from the Tor Browser to another browser (*Switched Browser Questionnaire*), and starting a new browsing session directly with a non-Tor browser (*Other Browser Questionnaire*). The questionnaires are included in Appendix F.

In a laboratory setting, researchers have direct access to the participants and can trigger data collection upon observing relevant participant actions. In contrast, in a naturalistic setting, it is not straightforward to seek questionnaire input at the most opportune time. Relying on participants to remember to fill out a questionnaire each time they encounter a problem is unreliable. However, continually monitoring user activity to detect when an issue is encountered can be invasive and difficult. We addressed this aspect via a process-monitoring Python script that kept track of the creation and termination of the following browser processes: Tor Browser, Firefox, Chrome, Opera, Safari, and Edge. To detect browser processes, we used the `psutil` library [61]. For Windows, simply checking the existence of the browser process was sufficient to know whether the participant closed the application. On Mac computers, however, processes continue to run in the background even after closing the window(s) associated with them. Therefore, the Mac script used the `Quartz` library, which is part of `pyobjc` [51], to monitor active windows associated with each process. If the number of active windows fell below a pre-determined threshold unique to each browser, the browser was marked as closed. The thresholds for each browser were determined by counting the number of active browser windows with visible windows open and closed.

When the script detected that any of the browser processes were terminated, it launched the appropriate questionnaire according to the following rules:

- If Tor Browser was running and no other browsers were running, launch the Tor Browser Questionnaire.

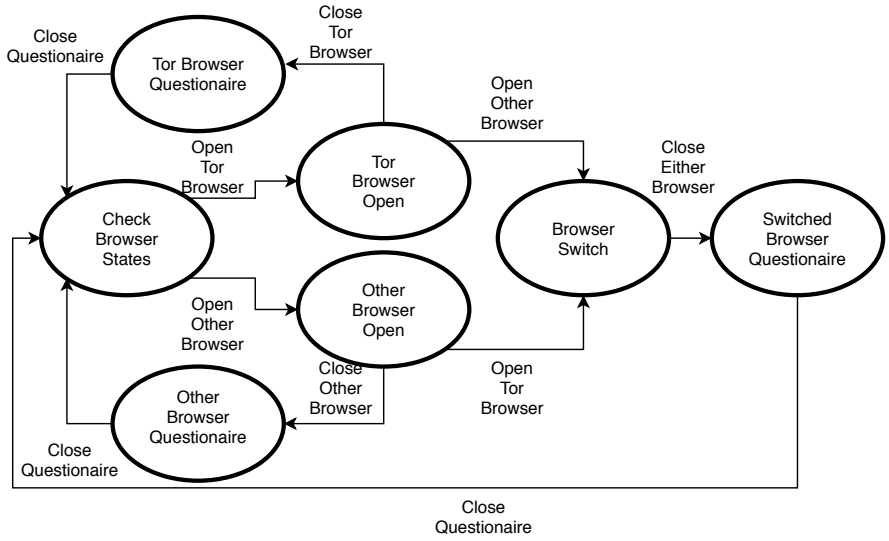


Figure 5.1: State and logic flow of the browser monitoring script used to select and present the appropriate questionnaire.

- If Tor Browser was running along with another browser, launch the Switched Browser Questionnaire.
- If Tor Browser was not running and any other browser was running, launch the Other Browser Questionnaire.

Additionally, if no browser was closed within a 24-hour period, the script launched the Tor Browser Questionnaire. Figure 5.1 shows the script logic used to select the questionnaire to present. Source code for the script is available on GitHub[1] and was made available to study participants.[2]

To complement the insight captured via the questionnaire, we obtained detailed qualitative data in two ways. At the end of the study, participants provided 2-3 page write-ups reflecting on the experience of using the Tor Browser for routine online tasks (see Appendix E for the instructions provided for the write-up). In addition, we conducted brief 10-minute semi-structured interviews asking participants about the UX and challenges of using the Tor Browser (see Appendix D for the semi-structured interview guide). The write-ups and interviews served to provide context, add nuance, and corroborate information gathered via the other mechanisms.

[1] `https://github.com/kcg295/TorUsabilityBrowserSensor`

[2] We recognize that participants without a programming background needed to trust that our code is not malicious or engage a trustworthy individual to audit the code.

5.1.2 Study Procedures

The study was deployed as an assignment within an undergraduate course in the Department of Information and Library Science at Indiana University Bloomington. This sample is similar to those in previous works [17, 49, 50] and is composed of novice and non-expert users of the Tor Browser, a population whose adoption of Tor is particularly important for making Tor more inclusive and diverse in terms of its user base.

While the assignment counted toward 10% of the grade for the course, allowing the assignment data to be used for research purposes was optional and voluntary. Moreover, the grading and research aspects of the assignment were kept completely separate with the course instructor playing no part in the research and the researchers having no involvement in the grading. This separation allowed us to avoid potential coercion for research participation and prevent undue influence of grade considerations on the collected research data. To maintain anonymity during data collection, each participant was assigned a unique identifier composed of an alliterative adjective-noun pair, such as 'elegant eagle,' to be used as the participant ID when providing responses. Participants did not receive any compensation.

We first sought informed consent for study participation via a brief in-class presentation on assignment procedures and requirements followed by answering questions and providing clarifications as needed. Next, participants received detailed instructions to download and install the Tor Browser and our monitoring script. After installation, participants filled out a brief pre-study questionnaire (see Appendix C). Prior to the start of the study, we ensured that all participants had successfully installed the Tor Browser and the monitoring script and set the Tor Browser as default browser on their primary computer.

The study lasted for one week, beginning Monday and ending the following Sunday. For the entire week, participants were asked to use the Tor Browser for all online browsing activities just as they would use any other browser. As described above, our script monitored browser processes, presenting participants with appropriate online questionnaires.[3] In some respects, our approach resembles the Experience Sampling Method [24] used in other studies [9, 10, 58]. At the end of the one-week study period, participants were provided guidance to uninstall our monitoring script and the Tor Browser, if they desired. Within a few days of study completion, participants submitted 2-3 page reports on their use of the Tor Browser during the study. In addition, we interviewed those willing to talk to us about their experiences. Each interview was audio

[3]The questionnaires were hosted on Qualtrics: `https://qualtrics.com`.

recorded, and the audio was destroyed after transcription.

All study procedures were reviewed and approved by the Institutional Review Boards (IRBs) of Indiana University and New York University.

5.1.3 Data Analysis

A total of 19 students consented to participate in our research (8 female, 7 male, and 4 who did not provide demographic information) with ages ranging from 18 to 22 (average 20). Of the 15 participants who provided demographic information, one was Hispanic, two Asian, and the rest Caucasian. Only 3 of the participants indicated having used the Tor Browser prior to the study. Overall, we received 121 questionnaire responses (102 Tor Browser questionnaires, 13 Switched Browser questionnaires, and 6 Other Browser questionnaires) from 13 of the 19 participants (mean: 9.3, median: 6, and mode: 7 per participant across the 13 respondents). All 19 participants provided thorough post-study write-ups, and 11 of the 19 agreed to be interviewed.

Issue Categorization

In addition to choosing from the provided list of categories of issues, the online questionnaires allowed participants to enter open-ended text responses to describe the encountered problems. These open-ended responses were assigned one of the following seventeen labels generated after examining all collected responses:

1. **Broken Web site**
2. **Unresponsive Web site**
3. **Streaming Content**
4. **Reduced Productivity**
5. **Login**
6. **Browser Update Required**
7. **Browser Dependent Content**
8. **Shopping**
9. **Specific File Types**
10. **Latency**

11. **Inconvenience**
12. **Tor Traffic Block**
13. **CAPTCHAs**
14. **Geolocation**
15. **Browser Crash**
16. **Other**
17. **No Perceived Need for the Tor Browser**

The above labels were generated by analyzing all of open-ended text responses across all questionnaires. Voluntarily provided URLs were used along with the open-ended text to generate the labels and them to responses. In 83 cases, the categories selected by the participants matched the labels assigned to the open-ended responses. In 26 cases, the open-ended responses and URLs led us to assign labels more specific than the categories chosen by the participants. In the remaining 12 cases, the text responses did not match the categories the participants selected in the questionnaires. In such cases, we labeled the issues according to the open-ended text.

After assigning labels to questionnaire responses, some labels were combined to reflect a higher-level issues, resulting in the following larger issues:

1. **Broken Functionality**
   The Web site or some functionality within the Web site was not accessible via the Tor Browser.
2. **Latency**
   The Tor Browser was unacceptably slow.
3. **Differential Treatment**
   The Web site treated Tor traffic differently.
4. **Geolocation**
   The Web site provided content based on the locale of the Tor exit node which did not match the participant's locale.
5. **Crash**
   The Tor Browser crashed or encountered an error.
6. **Other**
   The participant reported an issue not specific to the Tor Browser.

For instance, the first 9 labels were combined under the Broken Functionality aspect. Table 5.1 provides the full list of issues along with the respective underlying labels and counts.

Qualitative Coding

Qualitative data collected via write-ups and interviews was analyzed with techniques based on Grounded Theory approaches [19]. We began coding the qualitative data after completing the first interview, continuing the coding process throughout the qualitative data collection activities. The analysis utilized two stages of coding: open and axial. During open coding, data was coded sentence-by-sentence and codes were created without an initial hypothesis. We labeled each sentence with an underlying concept. Although more attention was given to UX-relevant codes, sentences were open coded even if they did not contain a UX issue. Subsequently, the codes were examined for similarity and connections and grouped together into overarching categories via axial coding. These categories were used to generate insight pertaining to UX problems faced by our participants. All coding and categorization was verified independently by a collaborator on the project. RQDA [25] was used for carrying out the qualitative analyses.

5.2 Findings

Table 5.1 provides quantitative details on the various issues reported in the online questionnaires broken down into the various types of problems falling under each issue. In the following subsections, we provide details regarding these issues uncovered by integrating the numeric counts with the insight gained from the analyses of the qualitative data.

5.2.1 Broken Functionality and Latency

As Table 5.1 shows, broken functionality and latency were by far the most frequently and broadly encountered UX issues, with 54/121 questionnaires reporting some type of functional hindrance and 41/121 questionnaires expressing frustration with latency. Of the 13 participants who filled out the online questionnaires, 9 reported functionality breaks while 8 reported slow speeds.

Notably, breaks in desired functionality occurred in a number of different ways, ranging from completely inaccessible Web sites to a lack of support for specific opera-

tions, such as the ability to access streamed content. Seven participants reported sites that did not load within the Tor Browser at all while six mentioned being able to access a site only partially. Participants also encountered more specific functional issues, such as the inability to complete productivity tasks necessary for work or school, problems with logins, or failure in checking out online purchases.

"*Sometimes the Tor browser simply would fail to load the page or just continue to load, never reaching its goal of going to the page that I wanted to go to.*" – (P17, M, unspecified age, write-up)

"*In some cases of using Tor, certain Web sites did not work at all.*" – (P3, F, 19, write-up)

Participants reported experiencing great frustration when they could not access all features of a Web site with reasonable speed. The most common reason for the frustration was the impact on productivity. For instance, a few participants stated that the two-factor authentication scheme deployed at their workplaces did not function within the Tor Browser. Some participants could not load specific files, such as PDFs, while others were unable to access needed translation services. A few were not able to read news.

"*In my opinion, I think the ability to access all sorts of sites needs to be improved in Tor, along with the overall running speed.*" – (P3, F, 19, write-up)

Anonymity can potentially be useful for a variety of individuals, such as journalists, activists, law enforcement, or even ordinary citizens wishing to read the news without fear of retribution. Therefore, losing the ability to access Web sites that aid in productivity, learning, and information acquisition makes many beneficial uses of Tor impossible.

Although slow speeds were found annoying, when we explained that the latency is an artifact of Tor operations required to protects identity, many participants stated during the interviews that in certain circumstances they would be willing to deal with increased latency for anonymity benefits.

"*Yeah, definitely. I didn't know it was that. I knew that Tor was a much more secure way to browse the Internet but I did not know that the slowness of it was part of how it did it. Now that I know that, if for whatever reason I wanted to make sure it was really secure, I would definitely use Tor even though it is slower. I did not know that was a thing!*" – (P5, F, 19, interview)

"*Because, I mean, some things are worth waiting for to make sure I can accomplish*

whatever I need to." – (P7, F, 21, interview)

Yet, no participant provided specifics regarding the amount of tolerable latency or the acceptable level of identity protection, underscoring the difficulties in ascribing precise quantities to these subjective and contextual needs and experiences.

5.2.2 Inconvenience

As two of our participants pointed out, the Tor Browser lacks a number of mechanisms present in other browsers to make browsing more convenient and efficient, such as easy access to bookmarks, password saving capabilities, etc. These two participants often switched to other browsers when they needed to access a bookmarked site or a saved password that they could not easily recall.

"*The Tor browser also does not provide a lot of the ease of access quirks that a traditional browser provides. For example, it does not save your passwords which forces you to put them in manually every time.*" – (P17, M, unspecified age, write-up)

"*To elaborate on what I mean by 'ease of access,' because Google Chrome was my default browser of choice, none of my bookmarks or pre-saved information (i.e., passwords, payment information, etc.) were readily available to me while using the Tor Browser.*" – (P12, M, unspecified age, write-up)

While the questionnaire responses indicated the lack of browser conveniences to be a hindrance and, sometimes, a cause for switching to an alternate browser, we found that many participants understood that these conveniences are often a double-edged sword and including them might compromise Tor's anonymity goals.

"*I know that the goal of Tor is to allow for anonymity and privacy, so it does not store any information or have the capability to save passwords, but it was really inconvenient to have to log back into things whenever I opened the browser again.*" – (P5, F, 19, write-up)

"*I think many of the things the average user would want in a browser to make usage more efficient would counteract the anonymity aspect of Tor — things like having a most visited sites page, having passwords saved for certain sites, and using bookmarks at the top of the page to make navigating faster.*" – (P14 F, 19, write-up)

"*It also did not have some of the useful perks that a normal web browser has. I had to input my passwords in every time which is not bad; it is actually good and more secure, just inconvenient and time consuming.*" – (P17, M, unspecified age, write-up)

5.2.3 Differential Treatment

Two of our participants stumbled onto Web sites that treated Tor traffic differently from other network traffic (5 questionnaire reports). Such differential treatment included total blockage of traffic coming from known Tor exit nodes and an incorrect presumption of automated activity or denial-of-service attempts leading to being presented with CAPTCHAs for verifying that a human was attempting to access the resource.

"*I was going to read articles on the online news site derspiegel.de and I was trying to open articles, but it would not let me read them further.*" – (P14, F, 19, interview)

Yet, the number of incidences reporting differential treatment was much lower than our expectations based on the large amount of differential treatment for Tor traffic measured in the past [38].

5.2.4 Geolocation

Perhaps surprisingly, only two participants reported issues due to Web site features that depend on IP address based geolocation. Interviews and write-ups revealed that wrong geolocation due to the Tor exit node being located in another country was particularly problematic when accessing multimedia content, which is often geographically restricted, or checking email, which is often timestamped with time zone determined via geolocation.

"*When I tried to get on the site, it told me that Pandora was not active in my country just yet, just the United States.* " – (P3, F, 19, write-up)

5.2.5 Web Searching and Operational Messaging

Our qualitative analyses surfaced two aspects not captured in the questionnaire responses: Web searching and operational messaging.

The default search engine for the Tor Browser is DuckDuckGo which claims to provide Web search functionality without user tracking or record keeping. As a participant noted, the switch in the default search engine could potentially be confusing:

"Someone who is using Tor and does not understand IP anonymity may be confused why when they search 'Google' in the search bar it turns into 'DuckDuckGo' which may lead users to believe they are doing something incorrect and feel lost." – (P18, M, 19, write-up)

Issue	Category Labels	Description	Report	Participants	Total Reports	Total Participants
Broken Functionality	Broken Website	Some part of the Web site did not work.	13	6	54	9
	Unresponsive Website	The Web site did not load.	13	7		
	Streaming Content	Video streaming did not work.	9	3		
	Reduced Productivity	A productivity-oriented feature could not be used.	9	3		
	Login	Logging into the Web site failed.	2	1		
	Browser Update Required	Accessing the content required a different browser version.	2	1		
	Browser Dependent Content	Accessing the content required a specific browser.	2	1		
	Shopping	A financial transaction could not be completed.	1	1		
	Specific File Types	A specific file type could not be viewed.	3	1		
Latency	Latency	Access was slow.	41	8	41	8
Inconvenience	Inconvenience	A feature present in other Web browsers was missing.	2	2	2	2
Differential Treatment	Tor Traffic Block	The Web site blocked connections from the Tor network.	2	2	5	2
	CAPTCHAs	The Web site wanted to verify that the access was by a human.	3	1		
Geolocation	Geolocation	The Web site was customized to the locale of the Tor circuit's exit node.	2	2	2	2
Crash	Crash	The Tor Browser crashed.	3	3	3	3
Other	Other	The participant provided no information or reported a non-UX problem.	13	5	14	5
	No Perceived Need	The participant saw no reason to use the Tor Browser for the task at hand.	1	1		

Table 5.1: Participant reported UX issues along with associated report counts and number of reporting participants.

Some participants noted a number of undesirable DuckDuckGo characteristics, such as a lack of auto-complete capability, inability to revisit past search results via the 'Back' button, etc.

"I personally did not care for DuckDuckGo at all. My one big complaint is that when I was searching something it would not autocomplete like Google does. That means I had to know what specifically I was looking for and how to spell it." – (P9, F, 20, write-up)

"I did run into a quirk, and I do not know if this was due to Tor or DuckDuckGo. I use StackOverFlow to get help on coding problems and whenever I clicked back it took me to the main page of Tor and not to the list of search events. This was very frustrating because I had to retype my query and look for it again." – (P6, F, 22, write-up)

The reaction to DuckDuckGo's search results was mixed; some participants liked the results while others found them to have lower relevance and utility compared to those from other search engines.

Participants expressed a need for promoting greater operational transparency and facilitating learning via Tor messaging and communication designed to be accessible to

non-experts. The need for greater and clearer information was perceived in a number of contexts: motivating Tor use, describing Tor functionality, and explaining errors.

Many participants lacked appropriate understanding of how Tor achieved the anonymity it promises and why and when online anonymity is important and useful. For instance, some participants believed that Tor was useful only in countries where freedom of expression is limited, but did not see any benefit to using it in the United States. These findings echo the results of our prior work which pointed out that non-experts typically hold simplistic mental models regarding Tor operation and the threats it counters [17].

"One thing I really wish would be explained at the beginning of the study is the difference between Tor and a VPN service, like HideMyAss or TunnelBear. I tried Googling it (or in the case of the past week, DuckDuckGoing it) but I still do not understand exactly what differentiates them." – (P4, F, unspecified age, write-up)

Several participants ran into situations in which they were puzzled by why the Tor Browser was performing specific operations or encountered error messages full of jargon that they did not comprehend. For instance, many of those who reported unresponsive Web sites stated that they did not understand why the Tor Browser was not able to access sites that seemed to pose no problems for other browsers.

"... at home, the Tor browser would refuse to launch and would have a 'proxy server is refusing connections' message. I was unsure of the cause of this message, but no Web pages would launch." – (P10, M, 20, write-up)

Error messages were often unhelpful for troubleshooting. The error message referred to in the above quote by P10, for example, is full of jargon and could have been caused as a result of any one of multiple problems, such as a lack of Internet connectivity or the failure to launch the Tor daemon. Similar lack of clarity was mentioned regarding messages encountered in a number of situations.

"I went to launch Tor and it got stuck on the 'loading relay information' part of connecting. It said 'this may take several minutes' but it ended up never connecting." – (P4, F, unspecified age, write-up)

5.2.6 Lack of Trust

Importantly, qualitative analyses showed that the lack of a "smooth and polished" UX caused more than mere frustration; it led some participants to associate the problems with a general lack of trustworthiness and reliability.

"*I experienced only two Web sites crashing but it lessened my trust in regards to the reliability of the Tor browser.*" – (P10, M, 20, write-up)

"*This was not always the case but its unreliability also made me not trust the Tor service as much.*" – (P1, M, 22, write-up)

The reduced trust further led to feelings of less security compared to other browser alternatives, thus defeating the central promised benefit of Tor.

"*...it felt less secure and smooth than the official browsing options (Firefox, Safari, Microsoft Edge, Chrome, etc).*" – (P10, M, 20, write-up)

5.2.7 Benefits

On a positive note, qualitative analyses revealed several aspects of the Tor Browser participants deemed beneficial and enjoyable. For instance, participants appreciated that the Tor Browser was easy to install and enjoyed the anti-tracking advertising-free browsing experience in the Tor Browser. For one participant, the Tor Browser solved an `SSL` certificate issue, potentially preventing a Man-in-the-Middle attack.

"For some reason, a few days before the study started, the laptop started tweaking, saying that it did not trust the certificates for [some] sites and would not let me navigate to them. It was incredibly frustrating, but when I accessed the same sites via Tor once the study began, there were no error messages and I could go straight to the sites with no issues." – (P11, F, unspecified age, write-up)

Several participants perceived using the Tor Browser as a learning experience. For instance, some Tor Browser warnings made them aware of threats to anonymity they had not previously considered, such as `HTML5` canvas data, window maximization, etc.

"I really enjoyed that when you resize the Tor window, it notifies you that, while you may choose to do so, it actually makes your device more vulnerable. I had no idea that this was an issue and was very pleased that Tor let me know this." – (P11, F, unspecified age, write-up)

Similarly, participants found it illuminating to consult the circuit information, which many felt was well-presented and useful.

"One really cool tool that Tor offers is the map of where the IP address is being rerouted — seeing that the circuit is being bounced around back and forth to other countries." – (P1, M, 22, write-up)

"I loved that I was able to see the circuit that the browsing session was being routed

through and how it bounced around different countries." – (P5, F, 19, write-up)

Notably, when using the Tor Browser, many participants reported an overall feeling of anonymity and privacy which was typically characterized as desirable.

"Upon starting to use the Tor browser, it felt pretty good and unique to be able to browse the Internet without concern of being watched or surveilled, I felt like I had more liberties and discretion in what Web pages I visited without the concern of surveillance." – (P8, M, unspecified age, write-up)

5.3 Discussion and Implications

Our naturalistic approach was able to uncover a number of UX considerations that were not noted in previous studies of Tor use carried out in the laboratory where the settings and the study designs imposed constraints on the tasks and the time. In the following subsections, we discuss the most salient UX insight derived from our findings and apply it to suggest solutions to tackle the corresponding issues and improve the Tor Browser UX.

5.3.1 Broken Functionality and Latency

Although broken functionality and latency were the most frequently encountered and the most frustrating for our participants, the causes behind the issues were often unknown or unclear. Participants experienced that the site did not load or function as expected but received no explanatory warnings or errors from the Tor Browser. There are, of course, a number of possible reasons behind broken site functionality within the Tor Browser, such as blocked JavaScript, server time outs, dependencies on plug-ins, Tor traffic blocks, etc. The reasons remain opaque since users merely experience that the site failed to operate as desired. Moreover, it is typically unclear to users that many of the issues arise due to the mechanisms needed to provide anonymity or restrictions on Tor imposed by external parties. As a result, users may incorrectly conclude that the Tor Browser is buggy, unreliable, and ineffective compared to alternate browsers. For example, two of our participants were unable to view PDF files. We suspect that the problem arose because of the specifics of the PDF generation and serving mechanisms used by the sites involved. However, in the absence of any information regarding why the files could not be viewed, the participants assumed that the Tor Browser could not handle PDF files.

In anonymity systems such as Tor, there is an inherent trade-off between anonymity

and latency. Much research is devoted to improving access speeds over the Tor network, mostly addressing traffic routing, and the Tor Project engages in outreach aimed at growing the number of volunteer-run relays in order to boost available resources, thus helping reduce latency. Despite these efforts, latency remains a UX challenge. Additional research on sophisticated approaches that alleviate traffic congestion in the Tor network [1–4, 18, 28, 32, 35] may provide noticeable speed improvements. Such approaches involve improved path selection that avoids overloading nodes and fixing the slowness induced by TCP mechanisms, such as head-of-the-line blocking. It may also be fruitful to explore whether the UDP protocol could be incorporated to help reduce latency.

Solution: Inform users about potential causes for broken functionality and latency. Perhaps the most straightforward way to address broken functionality is informing users why a Web site does not work with Tor. If the Tor Browser or a browser extension blocks content, users should be able to determine what was blocked and understand why. Of course, such explanatory information must avoid jargon and technical detail that non-experts may not follow.

A similar approach could be used for latency as well. For example, until a page loads, the Tor Browser could explain latency within a local page that is replaced when the desired page is ready to be rendered (i.e., HTTP 200 is received). Another possibility is to measure Round-Trip Time (RTT) between the client and the exit node by having the exit node acknowledge a Tor cell. If the RTT is above a specified threshold, the user could be alerted that higher latency should be expected as long as RTT remains high. As recommended by Norcie et al. [49], it may be useful to remind users that latency is an artifact of anonymity protection. As mentioned earlier, our participants were more willing to tolerate slower speeds when they understood those as necessary to benefit from the anonymity offered by onion routing. It is important that such messages are delivered unobtrusively, avoiding invasive techniques like pop-ups that are likely to be dismissed as an annoyance.

Solution: Provides means to generate Tor-friendly pages. In order to facilitate content delivery in a manner that fits the constraints imposed by the Tor Browser, content and site developers could be encouraged to support 'Tor-friendly' versions of Web pages. To that end, tools could developed to analyze Web pages and provide a Tor-friendliness rating along with a list of actionable suggestions that could be implemented to improve the rating. Web sites are often built on top of content management systems (CMS), such as Wordpress, that use templates and plug-ins with features that may not work within the Tor Browser. A potential solution is to provide plug-ins and templates

that function in a Tor-friendly manner. For example, a Wordpress login plug-in could be built to handle user authentication without requiring the use of JavaScript. Further, existing CMS plug-ins could be tested and certified as Tor-friendly if they meet the appropriate criteria. These suggestions, however, involve addressing several challenges. First, 'Tor-friendliness' needs to be defined and measured. Second, content and service providers must be encouraged and incentivized to adopt the tools and provide Tor-friendly versions. Third, the tools will need to work in conjunction with other mechanisms that can get around Tor traffic blocks or other forms of Tor censorship.

5.3.2 Inconvenience

Many users have come to rely on common browser features, such as password managers, bookmarks, history, session tracking, cookies, etc., that make browsing convenient and efficient. The amnesiac property of the Tor Browser forgoes such features in order to provide protection against certain adversaries, especially those that could potentially gain access to the user's machine. Against other adversaries, however, a lack of these features creates an inconvenience with no benefit. That said, as our participants correctly discerned, implementation of some of these features could potentially compromise privacy and security. For instance, password managers with lax auto-fill policies have been shown to introduce attacks that otherwise would not have been possible [65]. Additionally, lenient treatment of cookies could cause Web activities to be tracked. More research is needed to determine the potential effects of including these convenience features in the Tor Browser. Such features are particularly important for novices, who often begin using the Tor Browser out of curiosity [17]; inconveniences may make them give up using the Tor Browser before they have had the chance to learn and experience its benefits.

Solution: Modify the security slider settings to allow convenience features at lower anonymity levels. Perhaps a reasonable solution is allowing convenience features when the Tor Browser is set for the lowest level of security, i.e., the security slider setting is set to 'Standard.' This would allow users to maintain many of the familiar browsing conveniences while still allowing those who require stronger protections to disable the features easily by raising the security level via the slider settings. Since the security slider is currently set to 'Standard' by default, an alternative implementation could add another setting level that enables convenience features without affecting the currently implemented settings.

Solution: Provide the ability to specify threats of relevance to the user. The security slider settings within the Tor Browser already address various threat models. How-

ever, most of the differences among the different settings of the slider pertain to user tracking and identification mechanisms and capabilities of remote adversaries. The security slider functionality could be extended to consider other adversaries, such as those with physical access to the user's computer. In addition to being controlled via the security slider, convenience features could be selectively enabled based on user input regarding threats and use cases of importance. For instance, at the time of installation, the Tor Browser could launch a 'threat selection dialog' that allows the user to specify the threat(s) from which protection is desired, e.g., mass surveillance, censorship, advertiser profiling, etc. Based on user selections, and potentially other relevant aspects, such as country of use, features within the browser could be activated to achieve an optimal balance between convenience and privacy. Research is needed to determine the potential anonymity impact of the convenience features and the criteria for achieving the desired balance between convenience and privacy. Further, users should be able to invoke the threat selection dialog as needed in order to account for changes in needs and contexts.

5.3.3 Differential Treatment

A notable portion of the difficulties faced by Tor users are not technical, but political. Many Web site operators as well as powerful corporate and government entities block connections from the Tor network entirely. Moreover, it is not straightforward to determine who is blocking Tor traffic and why. Unless users are able to connect via an unpublished Tor exit node or use a proxy after the Tor exit node, it is difficult to avoid such blocks. Currently, the best countermeasure is working with Web site operators and security software vendors to create exceptions for Tor. However, such a process could be time and resource consuming, especially for a small entity like the Tor project.

Solution: Crowdsource the reporting of differential treatment of Tor traffic. It might be expedient to detect and report Tor traffic blocks by distributing the effort among Tor users via crowdsourcing techniques. For instance, the Tor Browser could include a 'Report connection problem' button that allows users to flag offending resources, thus facilitating monitoring and prioritization based on reporting frequency and problem severity. The crowd could perhaps also be leveraged to monitor and maintain the database of reports. Such reporting mechanisms could be extended to provide lightweight features for collecting and processing voluntary and anonymous user feedback regarding UX issues in general.

Solution: Explore alternative ways to deliver blocked content. When a resource cannot be reached via the Tor Browser, it may still be possible to access the content

through the use of services that archive or cache Internet content. For instance, the Tor Browser could incorporate mechanisms that allow searching for content on Internet archives such as the Wayback Machine [75] and within search engine caches, thus facilitating access to the content without sacrificing anonymity by accessing the blocked content in another browser.

5.3.4 Geolocation

Many Web sites customize content delivery based on the location determined by the user's IP address. For instance, such customization is utilized to set the appropriate language, display prices in the local currency, enforce intellectual property restrictions, etc. If the Tor Browser routes a user's traffic through an exit node in a country other than where the user is located, the delivered content ends up being wrongly customized from the user's point of view. Currently, specifying the desired country for exit nodes requires modifying the Tor run-time configuration file, `torrc`. This file can be complicated to handle and difficult to edit correctly, especially for non-experts.

Solution: Allow easy specification of desired exit node location. The ability to switch the preferred location of the exit node could be included within the set of settings that can be adjusted within the Tor Browser's graphical user interface. Such a feature must be accompanied by clear warnings that choosing to limit exit nodes to a specific country reduces the number of potential circuits, thus reducing the level of anonymity. The ability to set exit node location could be disabled at higher security levels as indicated by the security slider settings or based on the threats and adversaries selected by the user in the threat selection dialog mentioned above.

5.3.5 Operational Messaging

Novices and non-experts lack sophisticated operational understanding of Tor and anonymity compromising mechanisms [17]. As a result, it is important that the UX provide operational transparency and facilitate user learning. However, our participants found messaging within the Tor Browser to be inadequate and inaccessible, leading to confusion, frustration, and lack of trust.

Solution: Deliver contextually relevant information during user sessions. Most users lack the time or the patience to read long manuals or view tutorials. However, short messages relevant to the user's context delivered appropriately during use could be an effective means of communication, as demonstrated by the engagement of our participants with warnings related to screen maximization and `HTML5` can-

vas data extraction and the visualization related to traffic routing. Such mechanisms could be used for further text messages and visual indicators that help users relate the UX with operational detail. Useful information snippets could also be made available when the Tor Browser is first launched as well as on the `about:tor` and `https://check.torproject.org` pages. The UX for the delivery of such messages should be carefully designed to avoid unduly interrupting or distracting the user.

Solution: Craft errors, warnings, and other user communication in language accessible to non-experts. Information provided to users is useful only if they can understand it and take appropriate action. Therefore, messages should be crafted to avoid jargon and ensure understanding without requiring in-depth technical knowledge. To this end, evaluating message text via user studies could help improve its readability for a general audience.

5.4 Limitations

A few limitations must be kept in mind when considering the generalizability of these findings. Our sample is small and homogenous in terms of age, education, and cultural background. Moreover, the research was carried out in the United States where the nature of threats to civil liberties is different from that encountered in other places across the world. Further research is needed to uncover additional UX aspects that might be salient in other types of populations.

Most of our participants were not familiar with Tor prior to the study, thus representing novice and non-expert users. While UX considerations for experts may be somewhat different, increasing Tor adoption and use requires a greater focus on novices and non-experts who constitute the majority of the population.

One participant mentioned changing browsing activities during the study because of the monitoring of browser state transitions by our script. In contrast, it is possible that the privacy protection of Tor led our participants to access resources that they might not otherwise have sought in the course of routine "non-private" browsing. Additionally, given the nature of our study, participants may have been more tolerant of errors than they would be in a typical browsing session. Although such deviations from normal browsing practices may have slightly reduced the naturalistic aspect of our data, we note that only one participant reported engaging in browsing behavior during the study that differed from typical online practices.

Since our browser monitoring script relied on various heuristics to determine browser state transitions, it was prone to the occasional false positives that led to unnecessary

presentation of questionnaires, evoking pop-up fatigue in some participants. Similarly, it is possible that the script missed some browser transitions and failed to present a questionnaire even when warranted, thus missing the opportunity for collecting data. Moreover, the script covered only traditional desktop or laptop computers, missing coverage of browsing activities from mobile devices, such as smartphones and tablets, which are increasingly becoming the dominant mode of online access for a large proportion of the population. A few participants reported that the study did not capture the full extent of their Web use because they utilized their mobile devices for most of their Web browsing activities during the study period. As Web access via mobile devices continues to increase at a rapid pace, our study would need to be replicated in order to capture UX problems specific to Tor based mobile applications.

Additional quantitative data and finer grained information could potentially have shed more light on some of the issues we discovered. For instance, an in-depth analysis of broken functionality issues was infeasible due to the limited information available in participant self-reports. A potential solution could combine self-reports with information collection within the Tor Browser on relevant aspects such as load times, blocked page elements, etc. It is difficult, if not impossible, to collect such data privately, thus leading to a tension between the goals of the research and the Tor Browser.

5.5 Conclusions

In this chapter we discovered and described user experience errors discovered during naturalistic use of the Tor Browser. We collected both qualitative and quantitative data that described issues that our participants encountered while using the Tor Browser, coming from surveys, interviews, and write-ups submitted by 19 participants. This data was analyzed and we discovered issues relating to broken Web sites, slow speeds, geolocation issues, convenience issues, differential treatment and blocking, crashes, insufficient UI cues, and search engine issues. Based on this information we recommend interface changes and tool development, including the threat-model wizard and a Tor-friendliness scanner to improve Tor UX.

This mixed-method study was an important first step in studying the Tor Browser UX in a naturalistic setting. In the upcoming chapter we discuss how we captured more information about naturalistic UX of the Tor Browser, specifically relating to broken content and the Tor friendliness of Web pages.

Chapter 6

Measuring the Tor Friendliness of the World Wide Web

After studying where the Tor Browser fails during naturalistic use and discovering the under-explored issue of broken Web content in the Tor Browser, the questions we were forced to ask ourselves were *"What content was broken by the Tor Browser?"* and *"How Tor Browser Friendly is the World Wide Web?"* Unfortunately these are very large questions, so we narrowed it down to two main research questions:

1. *How different are sites rendered on Firefox and sites rendered on Tor Browser?*
2. *What functionality fails on the Tor Browser and why?*

Answering these research questions allowed us to come closer to answer our two larger questions, which to this day remain open questions (see Chapter 7). We decided to address these two smaller but still significant research questions by examining the difference between the DOM rendering results and JavaScript execution on the Tor Browser and on the Firefox version on which it is based. This allows us to see how frequently sites appear different on the Tor Browser than on normal Firefox, and how frequently the Tor Browser blocks the execution of a JavaScript script or causes a JavaScript script to otherwise not run. With this information from many different sites we can begin to see what frequently crashes on the Tor Browser, and use this to inform better design of Tor Browser friendly Web services in the future, as well as understand the consequences of some Tor Browser design decisions regarding blocking JavaScript execution.

6.1 Our Tool

In order to address our research goal and determine the Tor Browser friendliness of the Web we first needed to create a set of tools to help us collect data about the rendering of DOM elements and the execution of scripts in Firefox and the Tor Browser. This rendering data and execution data are then used in our analysis to determine what breaks on the Tor Browser and why. This analysis is discussed more in Section 6.2.2.

The first tools we created were modified versions of Firefox and the Tor Browser which were changed to log all steps in the creation of the DOM tree and all creations and executions of JavaScript scripts. The edits made to Firefox and Tor Browser are described in Subsections 6.1.1 and 6.1.2. After we get the DOM and JavaScript logs from Firefox and the Tor Browser, we then created scripts to compare their DOM trees and JavaScript execution traces.

6.1.1 Logging DOM Data

The first step of our analysis was to determine how much the DOM rendering process different on Firefox versus the Tor Browser. This gave us an understanding of how different the user may perceive the Web site on Firefox and the Tor Browser. However, to do this we needed to make a few modifications to accommodate our logging. First we added unique identifiers to DOM elements, and added functions that allowed us to store these elements in an easily parsed manner. Next we needed to modify Firefox to log the insertion, removal, and change of any of these elements.

Modifying DOM Elements

In order to make analysis possible, we needed a way to identify and easily find DOM elements. To do this we modified all DOM elements to contain a unique identifier. We did this by adding an integer variable to the class nsINode in the file dom/base/nsINode.h of the Firefox and Tor Browser code. We then modified the constructor of the nsINode class to include a node ID.

In addition to modifying the nsINode class to contain a unique ID, we needed to create functions to log the contents of a DOM element. We therefore added the following functions:

- nsIContent::GetContent
  This function is used to get the text content of a node (HTML Markup) if it exists. It is a virtual function that is implemented in every class that inherited from

nsIContent.

- nsIContent::DumpHash
  This function is used to get the hash of the text content of a node (HTML Markup) if it exists. It is a virtual function that is implemented in every class that inherited from nsIContent. It is used to quickly tell if the content of two nodes is equal.

Logging DOM Elements

In order to determine the difference between the page seen by a user on Firefox and the page seen by a user on the Tor Browser we logged the DOM tree as it rendered on both Firefox and the Tor Browser. To do this we modified Firefox and the Tor Browser to log all content:

- added to the DOM tree
- removed from the DOM tree
- and changed while in the DOM tree.

We achieved this by modifying the functions ContentAppended, ContentInserted, ContentRemoved, and ContentChanged. These functions were modified to simply log the action that was occurring at the time, and did not modify any of the other functionality. This was achieved by using the built in MOZ_LOG macro in Firefox and using a LazyLog called scannerDOM, which was created only to log DOM element creation, modification and removal events. However, this step was far from trivial. These methods were inherited by many different sub-classes, all with different implementations. In some implementations we only wanted to log in some circumstances (when we were certain that the content was not a duplicate, or was indeed added). In other implementations logging was straightforward and simply needed to be added to the beginning or end of the implementation.

Comparing DOM Trees

After the DOM trees were logged for both Firefox and Tor we built a tool in python that retraced the construction of the DOM trees and compared them for differences. This tool took two logs created by our modified browsers, went through and replayed the logs to recreate the DOM tree, and then compared the two resulting trees. Comparison was done using the edit distance of the trees. To calculate the edit distance the trees were flattened into an array of nodes and then the Levenshtein distance of the arrays were taken.

6.1.2 Logging JavaScript Scripts

In order to achieve a better understanding of what worked and what did not work on the Tor Browser, we needed to log the creation and execution of JavaScript scripts as well as DOM elements. This allowed us to determine what scripts were present in the site rendered on Firefox and the Tor Browser, and when both were present, which ones ran and didn't run.

Modifying JavaScript Elements

In order to meaningfully log and analyze the execution of JavaScript we needed to create a modification to the JSScript, JSFunction, GlobalObject, and JSContext classes in the Firefox and Tor Browser code bases. This modification added a script ID to the JSScript and JSFunction classes. However, all JSScript and JSFunction objects also belong to a JSContext object, so we also added a context ID variable to the JSScript and JSFunciton class and added a unique identifier to each JSContext. This allowed us to easily log the unique ID of the JSScript and JSFunciton objects and the JSContext object they belonged to.

JavaScript Logging

After we modified the scripts to contain unique identifiers we modified the code to log the creation and execution of all JavaScript functions in SpiderMonkey. These modifications occurred in seven functions:

- jsapi.cpp:Compile
  This function compiles a JavaScript script from source into Bytecode.
- js::Execute
  This function executes compiled JavaScript by calling the ExecuteKernel function.
- BytecodeCompiler::createScript
  This function creates an instance of the class JSScript using a source code buffer.
- BytecodeCompiler::compileScript
  This function compiles a JavaScript script from source into Bytecode.
- BytecodeCompiler::compileModule
  This function compiles a JavaScript Module from source into Bytecode.

- BytecodeCompiler::compileStandaloneFunction
  This function compiles a standalone JS function, "... which might appear as the value of an event handler in an HTML <INPUT>tag, or in a Function() constructor." [1]

- frontend::CompileLazyFunction
  This function compiles a JavaScript script from source into Bytecode if the source of the function exists.

In functions jsapi.cpp:Compile, BytecodeCompiler::createScript, BytecodeCompiler::compileScrip BytecodeCompiler::compileModule, BytecodeCompiler::compileStandaloneFunction, and frontend::CompileLazyFunction we logged that a script was created. This does not mean that the script was executed, only that the script exists and was not yet run. In the function js::Execute we logged that the script was executed only if the ExecuteKernel function returned without errors. This ensured that only the scripts that did successfully execute were logged.

Matching JavaScript Scripts

In order to meaningfully understand what scripts execute in both Firefox and the Tor Browser we must first match each script in Firefox with a matching script in the Tor Browser. Unfortunately even though IDs were granted sequentially the same scripts were not always granted the same IDs. One potential reason for this could be because of the non-deterministic nature of the order of network requests: some scripts may arrive before others and there is no way of guaranteeing the order of scripts arriving on the network. This made matching scripts between two logs more difficult. Though a potential solution would be to attempt to match based on a value like the hash of the script source, this does not provide a sufficient solution. Scripts may be dynamically generated by the back-end, or by another JavaScript script, and may be slightly different each time the site is loaded. However, as long as the changes are only minor these should still be considered the same scripts.

We addressed this problem by matching scripts using the MinHash locality sensitive hashing (LSH) [57] algorithm. Specifically we used LSH Forests for a top-k similarity search among the set of possible matching script sources. This algorithm worked as follows:

[1] This description is taken from a comment in the Firefox code in file BytecodeCompiler.cpp.

Data: A set of scripts S to match to candidates.
Result: A set of matched script pairs M and a set of unmatched scripts U
F = BuildForest();
$M = \emptyset$;
$U = \emptyset$;
foreach s *in* S **do**
    $c = F$.getClosest(s);
    if *JaccardSimilarity(c, s)* $\geq$ *THRESHOLD* **then**
        $M = M \cup \{(s, c)\}$;
        F.remove(c);
    else
        $U = U \cup \{s\}$;
    end
end
return (M, U);

Algorithm 1: Algorithm used to match scripts.

It made use of another algorithm used to build the Locality Sensitive Hashing Forest. This algorithm worked as follows:

Data: Set of source code candidates C_1
Result: A Locality Sensitive Hashing Forest F
F = initializeForest();
foreach c *in* C_1 **do**
    S =split(c, ' ');
    M = initializeMinHash();
    foreach s *in* S **do**
        M.add(s);
    end
    F.add(M);
end
return F;

Algorithm 2: BuildForest() algorithm to build the LSHForest used in Algorithm 1

We use the datasketch library [79] for Python 3.7 to perform the matching.

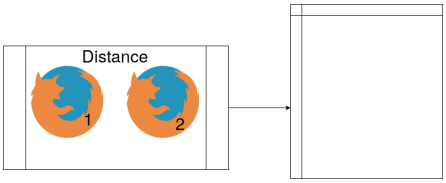


Figure 6.1: For the first step we calculated the distances between render trees and execution traces for two runs of a site on Firefox.

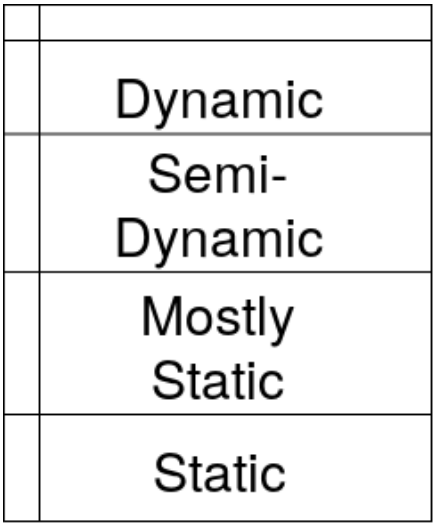


Figure 6.2: For the second step we split the list of sites based on the distances we calculated in the first step.

After functions were matched we were able to determine which functions existed on Firefox and not the Tor Browser, and which functions existed on both but only ran on Firefox. These scripts were considered broken on the Tor Browser. We then parsed these scripts and counted the occurrences of each function in them. We used this information to determine which functions occurred most frequently in scripts that were broken on the Tor Browser.

6.2 Method

In order to get an understanding of how users experience the Web on the Tor Browser and what breakages occur, we collected and collected and analyzed logs of DOM tree creation and JavaScript execution for 1000 home-pages on the World Wide Web using the tool described in Section 6.1. We decided to use the Alexa top 1000 Web sites. We believe that a top list is an appropriate solution for this research question since we are interested in mimicking user click-through traffic [64]

For reach of these Web pages we visited the home page of the site 5 times with our tools. The first two visits were done with the modified Firefox logging code, and the remaining three visits were done with the modified Tor Browser on multiple Security Slider settings. Our tools followed any redirects that were served. The DOM construction logs and JavaScript execution logs were then stored. These connections were done automatically and no interaction with the Web page beyond loading the Web

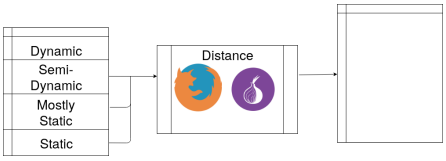


Figure 6.3: We calculated the distances between the Tor Browser and Firefox.

Figure 6.4: We then split the list of sites based on the distances we calculated in the third step.

page occurred.

After collecting the logs we classified the sites as *dynamic*, *semi-dynamic*, *mostly static*, and *static*. We did this by computing the similarity of the DOM trees computed from the two logs captured from the modified Firefox. We then broke these into quartiles. The bottom quartile was considered dynamic, the next quartile was considered *semi-dynamic*, the next *mostly static*, and the top quartile was considered *static*. A graphical depiction of these steps can be seen in Figures 6.1 and 6.2.

For all categories except *dynamic* we then compared the DOM and JavaScript logs of Firefox with the DOM and JavaScript logs of the Tor Browser to classify the level of difference between Tor and Firefox. Based on this we classified sites as *different*, *semi-different*, *mostly similar*, and *similar*, just as we did the classification for the four previous categories. We decided to not perform this analysis for the *dynamic* category because we could not tell if the difference between Tor and Firefox was caused by the browser or by the normal dynamic nature of the Web site. A graphical depiction of these steps can be seen in Figures 6.3 and 6.4.

6.2.1 Deep Dive

To get a better understanding of how sites might break under more detailed usage, we performed in-depth data collections on a subset of 40 Web sites, 10 from the *different* category, 10 from the *semi-different* category, 10 from the *mostly similar* category,

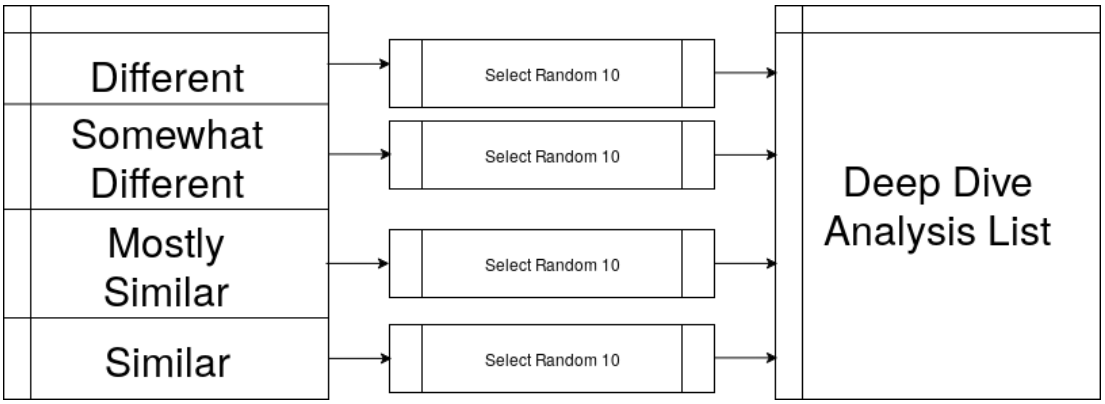


Figure 6.5: We randomly selected 10 Web pages from each of the categories at the end
.

and 10 from the *similar* category. A graphical depiction of this step can be seen in Figure 6.5. We replaced any adult Web site with another randomly chosen site from the same category. For each of these sites we performed a more in-depth scan of the Web site by hand in what we called a *deep dive collection*. The Web sites we performed the deep dive collection on, as well as their classification can be found in Table 6.1.

Before performing our deep dive collection we first visited the Web site using a normal, unmodified browser to understand what the Web site was, how it functioned, and, if necessary, to register for the site. While visiting the site we noted some of the major functionalities of the site in preparation for our deep dive. We then noted the steps that would need to be performed in order to use that functionality of the Web site.

To begin the deep dive we then visited the site on our modified version of Firefox. We performed a cognitive walk-through of the site using the noted steps for each functionality that we discovered from visiting the site previously. This data would become ground-truth data for which Web site functionality worked and which functionality didn't work on normal Firefox.

After collecting the ground truth data we performed the same cognitive walk-through on the modified Tor Browser three times, one time for each setting of the Tor Browser Security Slider. For each feature of the Web site noted previously we performed the same steps as the ground-truth walk-through until we came across an error or break that prohibited us from proceeding with that feature. We then moved on to testing the next feature. During each cognitive walk-through we took notes about what functionality we were attempting to use, on which step the feature became unusable (if applicable) and what effects the break had. This data was then used for analysis.

6.2.2 Analysis

After collecting data from our normal scan and our deep dive we proceeded to analyze the data. As part of this analysis we needed to compute the differences between the DOM trees of two given render traces as well as match JavaScript scripts across runs on both Firefox and the Tor Browser, including matching scripts that have portions that are dynamically generated or contain different values each time. Details about how this was achieved can be found in Section 6.1.

Data collected from the scan of the home pages of the Alexa top 1000 were analyzed for difference in DOM rendering and JavaScript executions. These were computed between all pairings between Firefox, the Tor Browser on Standard, the Tor Browser on Safer, and the Tor Browser on Safest.

Data collected from the deep dive collection method were analyzed for differences between JavaScript executions between Firefox and Tor and directed by notes from the cognitive walk-through. In addition to the differences between JavaScript executions we were able to find information about which JavaScript functions correlated most with broken scripts and broken functionality on the Tor Browser on all three Security Slider settings. This information is presented in Section 6.3.

6.3 Results

After the data was collected, we analyzed the differences between the JavaScript executions of Firefox and Tor on all three security slider settings, guided by the notes from the cognitive walk-through. From this we discovered a few interesting findings.

1. ***We do not find evidence of wide-spread broken functionality on the lowest setting of the security slider.***
   Contrary to the results presented in our second chapter, we do not find evidence of wide-spread broken functionality on the lowest setting of the Tor Browser's security slider. Though we did not discover evidence of this, it may still exist but not show up in our deep-dive analysis. However, we do have an alternative explanation for the reports of broken functionality from this chapter, as reported in Section 6.3.2.

2. ***Differential treatment may be misunderstood as broken content.***
   We discovered evidence that differential treatment may appear as arbitrary errors on Web sites, causing people to believe that certain functionality on the page is

broken by the Tor Browser. This may explain previous reports of broken functionality on the lowest level of the Tor Browser security slider.

3. ***Broken JavaScript functionality may come more from HTTPS errors and loading errors than from specific JavaScript issues.***
   On the "Safer" security slider setting, more issues may occur from HTTPS and loading errors than from specific JavaScript issues or functions. Though the Tor Browser does block unsafe functions and libraries from executing on the second level of the security slider, we only found evidence of broken functionality from blocking JavaScript over HTTP, or from denying third-party cookies.

4. ***Very few sites support the highest level of the Tor Browser's security slider.***
   Perhaps unsurprisingly, very few sites allowed us to complete all of our tasks on the highest setting of the Tor Browser's security slider. This setting disables JavaScript entirely, which breaks a lot of the functionality of the modern Web. However, on eight sites we were able to complete our tasks on the highest setting of the Tor Browser security slider.

In the following subsections we describe these findings in greater detail. In the section that follows we discuss the implications of these findings, and suggest improvements to the Tor Browser to either mitigate these issues or make it clearer what is creating the issue so the user can make more informed decisions about their use of anonymity systems.

6.3.1 Differences in Security Slider Settings

Perhaps unsurprisingly there exist many differences between functionality on different levels of the Tor Browser's security slider. On the first level of the Tor Browser's security slider, "Standard," we did not find evidence of wide-spread broken functionality caused by the Tor Browser. Notes from our cognitive walk-throughs of the 40 Web sites listed in Table 6.1 demonstrate that most Web sites do not cause issues completing tasks on the "Standard" setting of the Tor Browser. Of the sites that do cause issue on the "Standard" setting, none of the them relate to issues caused by the Tor Browser itself, but rather from differential treatment, which was discussed in Chapter 5.

On the second security slider setting, "Safer," we begin to see issues caused by the Tor Browser that prevent us from performing our desired task. This includes JavaScript not being loaded, and media content not playing. There are several reasons for these issues, and each of these reasons are explored in the following subsections.

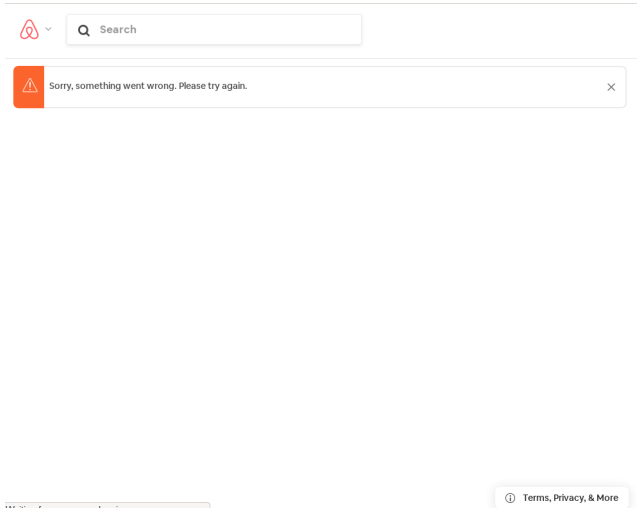


Figure 6.6: An example of the AirBnb error message that is caused by differential treatment.

Perhaps unsurprisingly, most Web sites do not function correctly on the third security slider setting, "Safest." This causes us to fail in most of our desired task. Further, most of the Web sites that we performed our deep dive analysis on do not check if JavaScript is supported or running on the browser that requested it, causing numerous issues with the "Safest" setting of the Tor Security slider. Perhaps surprisingly, however, we were able to complete our tasks on eight Web sites without issue.

In some instances the "Safer" and "Safest" security slider settings provided better load times than the "Standard" security slider setting. We expect this is because many requests for third-party objects are blocked, causing the browser to load less unnecessary elements and code. As long as the functionality of the Web service remains in tact, this can serve as a way to alleviate the latency issue created by the Tor anonymity network.

6.3.2 Differential Treatment May Seem Like Broken Functionality

Though we did not find evidence of broken functionality on the lowest security slider setting, "Standard," that does not mean that we did not come across issues during our cognitive walk-through. In a few instances on the lower security slider setting, we came across issues seemingly related to broken functionality that caused us to abandon the task we were attempting to perform. One example of this was found on Airbnb.com, which returned an error message when we tried to perform a search. This error message can be seen in Figure 6.6.

We analyzed the DOM construction and JavaScript logs to determine what was

causing this error to occur. We suspected that it was an issue with a JavaScript function failing to execute, however we quickly realized that was not the issue. When examining the JavaScript and DOM tree creation logs we saw that the response to our search was not an expected HTTP 200 OK, but rather an HTTP 429 Too Many Requests.

We then attempted to perform the deep dive analysis for Airbnb.com again to ensure that the issue was not many people attempting to use the same Tor exit node to book an Airbnb rental at the same time. After many repeated attempts and the same result, we came to the conclusion that this was not broken functionality, but rather differential treatment of Tor exit nodes.

However, to a user attempting to search for an Airbnb rental using the Tor Browser, this may appear to be broken functionality rather than differential treatment. The error message provided by Airbnb does not give any information about what went wrong, leaving the user to guess what the issue is. Since Airbnb's Web service appears to be working enough to give the user an error message of some sort, a user may believe that the issue lies with the Browser instead.

This issue extends to other sub-resources of a Web service. If a Web service relies on a resource provided by a third-party that blocks network traffic from Tor, or if the Web service blocks Tor user's from accessing some services and not others, users may not understand that the resource they are trying to access is being blocked and may incorrectly attribute the inability to complete their task to the Tor Browser, rather than the Web service.

6.3.3 JavaScript and HTTPS

To protect its users, the Tor Project has strengthened the Tor Browser by blocking JavaScript over HTTP on the "Safer" and "Safest" security slider settings. This, along with the extension HTTPSEverywhere, ensures that JavaScript cannot be modified in transit by a malicious exit node or other network attacker, assuming the attacker does not have an HTTPS certificate for the Web site it is impersonating. However, during our deep dive analysis of go.com, a Web site owned by Disney, we discovered that this can indeed cause problems with functionality on the Web.

When accessing go.com on the "Safer" security slider setting, the user is faced with a blank page as shown in Figure 6.7. The user is given no warning as to why the content doesn't load, or what could have gone wrong. To the user it just seems like the page has no content at all.

To determine why this issue was occurring, we examined the DOM tree creation log and the JavaScript execution log. We saw that many of the JavaScript functions that ran

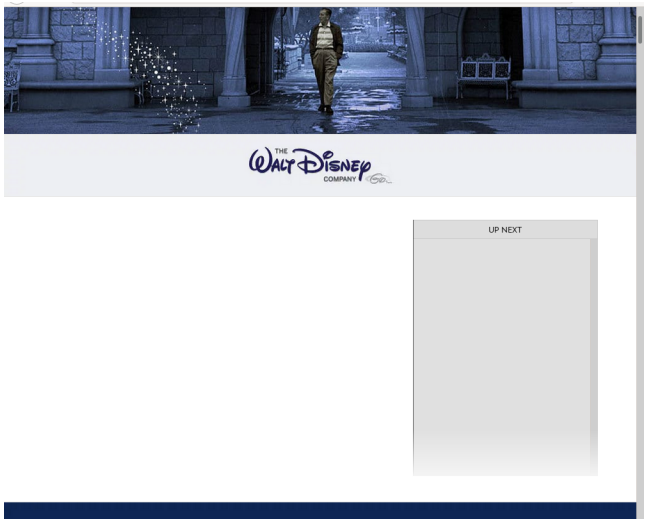


Figure 6.7: The Web site go.com as viewed on the "Safer" setting of the Tor Browser security slider.

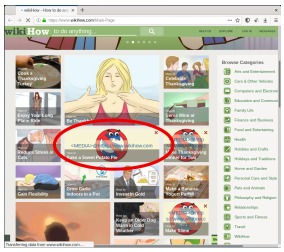


Figure 6.8: The icon used by NoScript for click-to-play media on the Tor Browser.

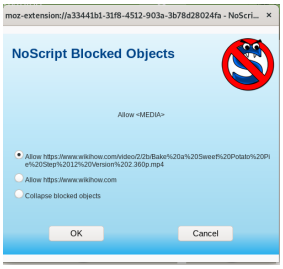


Figure 6.9: The popup that appears when one clicks media to play it.

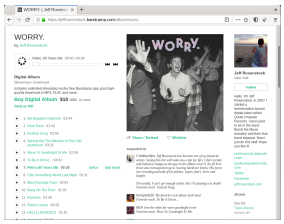


Figure 6.10: Bandcamp.com provides no indication that the media is being blocked.

on Firefox and ran on the "Standard" security slider setting did not run on the current security slider setting, while others had. We could not find any function calls, libraries, etc., that these scripts had in common. One thing they did all have in common was that they were not external scripts. That is, these scripts were defined on the go.com page. After seeing this, we noticed that go.com was served over HTTP, not HTTPS. We then tried to explicitly load the page over HTTPS rather than HTTP, but could not since go.com does not offer HTTPS. [2]

6.3.4 Click-to-play Media and Custom Players

During our deep dive analysis we discovered more issues on the "Safer" and "Safest" security slider settings. The next came while performing the cognitive walk-through of bandcamp.com. When attempting to listen to a song using the "Safer" setting on the Tor Browser, we noticed we could not get the music to play. As for the other issues, we looked towards the JavaScript and DOM construction logs to determine what the issue was. We noticed that the audio files that were fetched would fail to play.

In addition to blocking JavaScript loading over HTTP, the Tor Project has also strengthened the Tor Browser by changing media to click-to-load using NoScript. This provides the user with protection against exploits that may exist in media players and from fingerprinting that may occur through the media player. On the "Safer" and "Safest" security slider settings, the Tor Browser replaces the icon of the media with a NoScript icon. When a user clicks this icon they are presented with a pop-up that allows them to allow the media. This is shown in Figures 6.8 and 6.9.

Though changing media to click-to-load can be obvious to users, such as in Figures 6.8 and 6.9, in other cases media might be loaded and automatically started without being shown to the user. If the media needs to be clicked to be played it would simply fail to start, and the user would not see any icon or reason to expect that the media could be started through their intervention, as in bandcamp.com. As Figure 6.10 demonstrates, the user gets no indication that the media was being blocked unless allowed, and can not easily find a way to intervene and allow the media to play.

6.3.5 Some Web Sites Still Work on "Safest"

The most drastic break in functionality occurred on the "Safest" setting of the Tor Browser security slider. On this setting the Tor Browser disables all JavaScript by default, and "... only allows website features required for static sites and basic services." [3] Many modern Web sites rely on JavaScript to create a more dynamic and perceivably seamless experience, so it is not surprising that this setting breaks many Web sites. A few Web sites did have noscript tags that informed the user that the Web site would not work without JavaScript. A few pages still offered partial functionality and allowed us to complete many of our tasks. Mostly these sites were news sites or older commerce sites. A list of which sites worked and didn't work on this setting can be seen in Table 6.1.

[2] This issue has been reported to Disney.

[3] This is quoted from their Web site, found at https://tb-manual.torproject.org/security-settings/

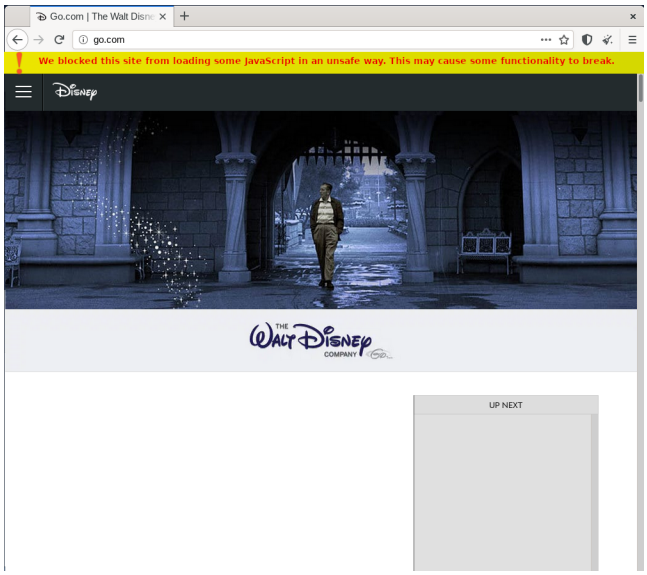


Figure 6.11: An example warning that informs users why functionality may be broken in the case of JavaScript over HTTP.

6.4 Discussion

These findings demonstrate that the problems of broken content on the Tor Browser are both political and technical, and that the current state of the Tor Browser does not communicate to the user exactly when content is broken and what the user can do about it. In this section we discuss the significance of each of our findings and how the Tor Browser can address broken content through better communication with the user.

6.4.1 JavaScript and HTTPS

In our findings we discovered that at least some Web sites exhibit broken functionality because the JavaScript that it is attempting to load over HTTP, rather than HTTPS. This failure to load does not trigger and log that communicates to the user what is occurring. Instead, Web site features may silently fail to load, as shown in Figure 6.7.

This is not an ideal situation. A user who is attempting to use the functionality of a site may get frustrated at being unable to achieve their goal without knowing why they were unable to do so. For this we recommend addressing this issue in one or both of the following ways.

The first problem is that HTTPSEverywhere fails silently when the Web site it is trying to upgrade the connection of does not support HTTPS. One change that can help inform the user of issues on the Tor Browser is to modify HTTPSEverywhere to

present a message to the user whenever a connection cannot be updated to HTTPS. If this message is specifically made for the Tor Browser it can state that the browser may not load some JavaScript on the page for the protection of the user. Though this does not help the user achieve their tasks, it at least lets them know what occurred and why they could not achieve their goal.

The second problem is that the Tor Browser does not notify users when scripts have not loaded on the page. This is understandable; if the Tor Browser were to inform the user when any JavaScript is blocked on higher settings, it is possible that it would inform users of many false positives caused by advertising networks or undesirable tracking code. However, not acknowledging that anything happened when broken functionality has occurred may lead to user frustration.

Ultimately, we recommend detecting the conditions under which an error like this can occur (when scripts are blocked from loading over HTTP) and informing the user that the scripts have been blocked, and that this may lead to broken functionality. An example warning message can be seen in Figure 6.11.

For operators of Web services, we recommend enabling HTTPS on your Web service and requesting all scripts over HTTPS. In addition to making your Web service more Tor friendly, this is also better for security for all clients using your Web service using other, more traditional browsers.

Interestingly, pushes by Google and the Internet Security Research Group to get Websites to adopt HTTPS may lead to an improvement in Tor Browser UX. If these organizations are successful in getting the entire Web to use HTTPS Tor users will no longer come across issues of broken functionality caused by refusal to load JavaScript on the "Standard" security slider setting.

6.4.2 Click-to-load Media

During the deep dive data collection portion of this work, we used many Web sites that contained media, such as bandcamp.com, wikihow.com, wordpress.com, and other. These media played without issue on the "Standard" security slider setting, but media such as audio and video become click-to-play on the "Safer" and "Safest" security slider settings of the Tor Browser. Though the media still works after clicking in some cases, there are some issues with the current click-to-load approach of the Tor Browser.

First, the icon used by NoScript (which enforces the click-to-play policy) may lead users to believe that the media is blocked and cannot load. This icon, shown in Figure 6.8, features the traditional circle with a line through it, which usually indicates that something should not or cannot be done. A different icon may be required to demon-

strate to users that they may run the video or audio if they wish.

In addition to the issue with icons, the current NoScript approach buries the media that the user may wish to access behind a pop-up with confusing options. This pop-up is shown in Figure 6.9. Non-technical users may not understand the consequences of these actions, or may be scared away from the media they wish to access. The user would expect to click the media and have it start, rather than get a pop-up. We recommend changing the click-to-load media functionality to follow the user's expectation, rather than generating a popup that the user may not understand.

There exist cases, such as on bandcamp.com, where media may not be presented as click-to-play at all due to JavaScript handling the starting and stopping of that media. In these cases users have no easy option to access the media they wish to access, and come across broken functionality. This is a very difficult issue to detect and solve, and we leave it to future research.

6.4.3 Differential Treatment and Political Solutions

Though some of these problems can be solved with technology, some of them can be solved more easily through political means. One example of this is the differential treatment demonstrated by AirBnb and other Web sites. Similar problems have occurred in the past with the content delivery network Cloudflare. After it was pointed out that Cloudflare was treating Tor traffic differently from other Web traffic, Cloudflare attacked Tor in a blog post and attempted to justify its decision [55] with questionable statistics [53]. However, after large amounts of pressure from the Tor community Cloudflare was forced to develop solutions that did not negatively impact the UX of Tor users [63].

Similar success stories can occur with individual Web sites and services that provide Tor users with differential treatment, but the inability to determine differential treatment from broken functionality as reported in Section 6.3.2 can frustrate any attempt at pressuring Web services to serve Tor users without differential treatment. If it is not known that a problem is caused by differential treatment, it is hard to mobilize Tor users to pressure Web services to remedy the problem.

To address this we recommend that the Tor Project begin keeping records of Web services that serve Tor users with differential treatment, and begin taking reports of differential treatment from Tor users. However, this can be filled with false positives, and verifying differential treatment is a non-trivial task. We leave solving this problem to future research.

Unfortunately differential treatment is not the only problem that may need to be ad-

dressed with political solutions. In Sections 6.4.1 and 6.3.4 we recommended changes to two extensions that the Tor Browser uses: HTTPSEverywhere and NoScript. If the Tor Project makes the suggested modifications, they then have two choices: to make a pull request to HTTPSEverywhere and NoScript, or to keep a forked version of these software and maintain it. The ideal scenario is that the pull request be accepted and these add-ons be maintained by their creators, but getting a pull request accepted can require a lot of political work. Therefore the technical solutions we recommend also require aid from political solutions to be most effective.

6.4.4 Other Changes in the Tor Browser

The Tor Browser makes many changes from Firefox by default. The changes include:

- **Only allowing a predefined set of fonts.**
  To protect against browser fingerprinting attacks, the Tor Browser only allows a pre-set list of fonts to be used. If this were not done an adversary could attempt to load many different fonts and build up a font-fingerprint which could be use to track Tor users cross-site.

- **Disabling the Web Speech API.**
  By default the Tor Browser disables the Web Speech API. This is done both to avoid fingerprinting based on the installed speech packages and to avoid hardware fingerprinting based on how long a phrase takes to complete.

- **Timing is made more less granular.**
  The Tor Browser makes the timing resolution of many different timing functions down to 100 ms to frustrate hardware fingerprinting attacks.

- **resource:// and chrome:// URI filtering.**
  The Tor Browser filters resource:// and chrome:// URIs to avoid fingerprinting based on extensions, locale, platform, etc.

A full list of changes can be found in the Tor Browser design document [54].

Even with all of these changes, we were unable to find instances of broken functionality in our deep dives related to these issues. This was counter-intuitive to our expectations, as we expected that changes in granularity to timing functions as well as blocking fonts and disabling Web Speech would have large impacts on the Web. We leave it to future work to determine what effect, if any, these changes have on the user experience of the Tor Browser through a larger-scale study.

6.5 Limitations

Like all studies, this study has limitations. These limitations may affect the generalizability of findings, and may also point towards interesting future work. In this work we have three main limitations: site selection, gaps in analysis, and tool limitations.

6.5.1 Site Selection

For our deep-dive analysis we randomly selected forty Web sites from the categories similar, mostly-similar, somewhat-different, and different[4]. These categories ignored highly dynamic Web sites such as YouTube, and as such does not capture issues that may be present on highly dynamic Web services.

In addition to ignoring highly dynamic sites, when we randomly selected adult Web sites we discarded them and randomly selected another Web site from within the same category. This was done because the deep dive analysis was being performed in an office setting, and viewing adult Web sites in an office setting could have put the investigator at risk for disciplinary action, and could have made other office members uncomfortable. This limitation can be addressed with future research.

Last, the Web sites that were randomly selected provided interesting insight to what breaks on the Tor Browser, but the issues we found are far from exhaustive. It is likely that with different Web sites we would run into different issues, and therefore find different results. Future work can perform the same deep dive collection again, but with different sites.

6.5.2 Gaps in Analysis

In addition to limitations that stem from site selection, this work also has limitations relating to gaps in analysis. First, the analysis performed on this work was guided by cognitive walk-throughs that did not attempt to replicate the entire functionality of the Web service we were testing. Instead this cognitive walk-through attempted a subset of tasks that are achievable on the Web service, and may have missed functionality on the Web site that is broken on the Tor Browser.

In some of the tasks that were tested in the cognitive walk-through, we still have breaks in the site functionality that we have not been able to find explanations for in the logs as of yet. Examining the logs created by the tool is a lengthy and potentially

[4]These categories relate to the difference between the Web site on Firefox and on the Tor Browser with the lowest security slider settings. For more information please see Section 6.2.

error-prone process, and future work may focus on narrowing down the logs to only relevant sections of broken functionality.

These two points can be summarized by saying that this examination is non-exhaustive. Though we do have explanations for broken functionality on the Tor Browser that were discovered in our collection, our collection may have missed broken functionality and we have still been unable to explain other phenomenon that our collection had captured. More analysis of our logs and more in-depth dives of Web sties could help provide more insight.

In addition to these gaps, this method of inspection gears itself towards qualitative analysis, rather than quantitative analysis. Therefore, the insight gained from these analyses must be tested at a larger scale using a tool derived from these insights. We intend to perform this as future work.

6.5.3 Tool Limitations

Our tool also has some limitations. One limitation that exists is the method for matching JavaScript. Since dynamically generated scripts can occur in the wild, we needed a solution for matching JavaScript scripts that may differ slightly, but perform the same functionality. We achieved this by using a fuzzy-matching algorithm that relied on the MinHash algorithm. This could have false positives and false negatives, which would make analysis more difficult.

In addition to limitations caused by false positives and false negatives, our tool also had issues with running very slowly. The reduction in speed is caused by large amounts of logging, which often included duplicate logging of the same DOM element or JavaScript script. Future work could reduce the logging time for the tool and duplicate logging by the tool. This would speed up both data collection and analysis, making it possible to collect and analyze data from more Web sites.

6.6 Conclusions

In this chapter we sought to determine what makes a Web service Tor Browser Friendly. To move towards the answer to this question we decided to take a look at what functionality of Web services breaks on the Tor Browser, and why. We tackled these questions by creating a suite of tools that captured the steps of Web site DOM tree creation and JavaScript execution for both Firefox and the Tor Browser. We then used these tools to perform deep-dive analysis on 40 Web sites, randomly chosen from 4 categories of Web sites based on the degree of DOM rendering and JavaScript execution

similarity on Tor and Firefox. We then analyzed the logs of these deep-dive analyses.

In our analysis we do not find that broken functionality appears to be an issue on the lowest level of the Tor Browser security slider. However, we do find that it can be hard to tell the difference between differential treatment and broken functionality on the lowest level of the Tor Browser security slider, since JavaScript can be used to catch HTTP error codes and transform them into error messages on the Web site. Depending on the error message presented to the user, this can cause the user to believe that the Tor Browser is at fault, when in fact it is the Web service that is blocking the Tor network.

On higher security slider settings we find several issues across many Web sites. From examining the logs of these issues we were able to discover a few issues of broken functionality in the wild. One example was an artifact of the Tor Browser refusing to execute JavaScript loaded over HTTP. Another example was an artifact of the Tor Browser refusing third-party cookies that were necessary to load content from a server with a different domain. We were able to complete tasks on eight of the forty Web sites on the highest level of the Tor Browser security slider setting.

Website	Firefox	Tor on Standard	Tor on Safer	Tor on Safest
nypost.com	No issues	No issues	No issues	No task related issues
news18.com	No issues	No issues	No issues	Cannot Search
theepochtimes.com	No issues	No issues	No issues	Cannot Search
esty.com	No issues	No issues	No issues	Initial product load, further products don't
ebay.co.uk	No issues	No issues	No issues	Cannot add to cart or view cart
wayfair.com	No issues	Differential Treatment (CAPTCHA)	Differential Treatment (CAPTCHA)	Unsolvable CAPTCHA
tripadvisor.com	No issues	No issues	No issues	Multiple Issues
fiverr.com	No issues	No issues	Differential Treatment (after search)	Search brings you to Home Page
bandcamp.com	No issues	No issues	Songs won't play	Multiple issues
securecafe.com	No issues	No issues	No issues	Slight issues, can still complete task
wikihow.com	No issues	No issues	Some media blocked	Some media blocked
wordpress.com	No issues	No issues	Some media blocked	Multiple Issues
istockphoto.com	No issues	No issues	No issues	Slight issues, can still complete task
wiktionary.org	No issues	No issues	No issues	No issues
marriott.com	No issues	Differential Treatment	Differential Treatment	Differential Treatment
opera.com	No issues	No issues	No issues	No issues
healthline.com	No issues	No issues	No issues	Slight issues, can still complete task
mayoclinic.com	No issues	No issues	No issues	Multiple issues
justdial.com	No issues	Differential Treatment	Differential Treatment	Differential Treatment
yadi.sk	No issues	No issues	No issues	Completely Blank
google.sk	No issues	Differential Treatment	Differential Treatment	Differential Treatment
go.com	No issues	No issues	Videos won't populate	Many issues
rt.com	No issues	No issues	No issues	Slight issues, can still complete task
rapidgator.net	No issues	No issues	No issues	Cannot log in
linkedin.com	No issues	Differential treatment	Differential treatment	Differential treatment
pixabay.com	No issues	Differential treatment (more CAPTCHAs)	No issues	Results do not load
fidelity.com	No issues	No issues	No issues	Multiple issues
smallpdf.com	No issues	No issues	No issues	Cannot upload file
best2019games.com	Forbidden	Forbidden	Forbidden	Forbidden
thepiratebay.org	No issues	Magnet link doesn't open torrent client	Magnet link doesn't open torrent client	Magnet link doesn't open torrent client
yelp.com	No issues	Differential treatment	Differential treatment	Differential treatment
wondershare.com	No issues	No issues	No issues	Multiple issues
scihub.tw	Articles not found	Articles not found	Articles not found	Search broken
mit.edu	No issues	No issues	Media click-to-play	Media click-to-play
geeksforgeeks.org	No issues	No issues	No issues	No issues
sciencedirect.com	No issues	Differential treatment	Differential treatment	Differential treatment
airbnb.com	No issues	Differential treatment	Differential treatment	Differential treatment
deviantart.com	No issues	No issues	No issues	Multiple issues
netflix.com	No issues	Cannot watch video	Cannot watch video	Multiple issues
hulu.com	No issues	Differential treatment	Differential treatment	Multiple issues

Table 6.1: Summary of results from deep dive analysis.

Chapter 7

Future Work

Though we made contributions to Tor usability and UX in this work, there is still a lot of work remaining. For future work, we plan on continuing to improve the usability and UX of Tor, improving the security of Tor against attacks against it, and addressing usability and UX issues of other software.

7.1 Tor Usability and UX

Though this work contributes to the usability and UX of Tor and the Tor Browser, it also reveals other paths for future research in the area. First, works regarding the usability and UX of the Tor Browser need to be verified and expanded using a larger data set. We will soon begin working with the Tor Project to create a survey about UX issues encountered while using the Tor Browser. This survey is intended for large portions of the Tor Browser user base, and will likely shed light on more issues faced by users of the Tor Browser.

Similarly, the work presented in Chapter 6 can be expanded, and more interesting issues of the Tor Browser can be discovered. Using our tools we can perform deep dive collection on more sites, including highly dynamic sites, to determine what frequently breaks on the Tor Browser. Likely our first analysis of the logs produced by our tools contain more information that was missed during our first pass of analysis.

In addition, we plan on simplifying the tools described in Chapter 6 and releasing a simplified and unified version of the tools that allows Web developers to test the Tor friendliness of their site. This scanner should work only on HTML, CSS and JavaScript source code, and would therefore make large-scale scanning of Web sites for Tor Browser compatability possible. This would lead to a more in-depth understanding of how Tor Friendly the World Wide Web is.

It is also possible to revisit and implement recommendations from the different chapters of this dissertation. For example, in Chapter 5 we recommended the creation of a Tor Adversary wizard that allowed Tor users to decide whether to remove disk avoidance features of the Tor Browser in favor of convenience, or to keep them in favor of security. This recommendation and others can be implemented and lab tested, and the security impact of them can be analyzed.

Finally, Tor has more elements to examine than just the Tor Browser. Usability and UX aspects of other features or aspects of Tor, Tor related software, or software that relies on Tor will be performed. We intend to perform usability analyses of Tor node creation, mobile versions of the Tor Browser, and Tor-relient services such as SecureDrop and Tor-enabled messengers such as Riccochet.

7.2 Tor Security

Each suggestion in this dissertation likely has effects on the anonymity set of Tor. Some suggestions, like the suggestion of displaying route information in an easily accessible way, or creating templates and content management system plugins that create Tor-friendly sites can only serve to make Tor more usable and likely will only expand the anonymity set. Other recommendations, such as the adversary wizard, make Tor more usable for the average person, but may create an opportunity for Browser fingerprinting from a remote adversary. For each of these suggestions the changes to the anonymity set must be measured and presented as future research.

However, expanding the number of Tor users is only part of expanding the anonymity set. These users must be virtually indistinguishable in order to expand the anonymity set. However, traffic analysis attacks like Web site fingerprinting and traffic confirmation attacks still need to be addressed. We will focus on creating traffic padding and traffic mixing techniques that balance the need for anonymity and usability so that Tor can defend more strongly against these attacks.

7.3 OTRv4 Usability

Other software is also in need of usability and UX research and improvement. Currently we are planning research on the usability and UX of Off-the-record version 4 (OTRv4), an end-to-end encryption protocol, with its creators at the Centro de Autonomía Digital. Though no specifics are planned yet, we believe there is a lot of promise for collaboration in this area.

Chapter 8

Conclusion

In this work we addressed the usability and user experience of the Tor anonymity system. We chose this problem both as a topic of interest itself, and because of the viral role that usability and user experience plays in the strength of an anonymity system. By making Tor more usable, one allows the anonymity set of the Tor network to grow [11].

Specifically we address the large research question:

How do users perceive and experience use of the Tor Browser?

This is a large question, and to address it we broke it down into three smaller, easier to address questions:

- ***How do users understand the inner workings of the Tor anonymity software?***
- ***How do users experience routine Web browsing when using the Tor Browser?***
- ***What functionality and Web sites break on the Tor Browser and why?***

The first two research questions were addressed in separate projects that were published in top conferences in their feild. The last research question is addressed for the first time in this dissertation. The details of these projects were discussed thoroughly in Chapters 4, 5, and 6.

8.1 Contributions

The first research question we considered was:

Why do people use Tor and how well do they understand the underlying operation of the Tor system?

We addressed this question by performing semi-structured interviews with 17 Tor users,6 experts and 11 non-experts, recruited from Reddit, New York University, and Craigslist. We then analyzed the text of these interviews using techniques based on grounded theory. Based on this analysis of the interviews we made the following contributions:

- We describe user perceptions and practices regarding Tor, an anonymity tool of growing individual and societal importance.
- We uncover and describe important differences in how experts and non-experts understand and conceptualize Tor. Specifically, we show that gaps and inaccuracies in non-expert understanding of the operation and threat model of Tor could lead to a sense of more or less privacy and security than is actually the case.
- We suggest solutions that can improve the Tor user experience and boost adoption by non-experts, many of whom are in vulnerable situations and/or serve as society's important actors.

Specifically, we found that there was a difference in completeness between experts and non-experts in their understanding of the Tor anonymity software. Experts had more complete mental models that viewed Tor as a complex and decantralized network. Non-experts had a less complete mental model that viewed Tor as a centralized service used for anonymity. Reasons for using Tor differed across experts and non-experts, with expers citing more varied reasons for using the Tor software and focusing on the technical elements of the software and non-experts citing specific motivations and only using Tor within those specific purposes.

Despite these differences, both experts and non-experts showed misunderstandings of Tor's threat model that could lead to attacks against their anonymity. Non-experts had varying understandings of Tor's threat model, with some believing it was wearker than it is, and others beliving it was stronger that it is. Some experts stated that they

configured their own browser to work with Tor, which demonstrates a misunderstanding of the threat model and how fingerprinting attacks could be levied against their browser to deanonymize them on the application level.

After addressing the first research question, we decided to take a look at how Tor users experience everyday, naturalistic use of the Tor browser. Specifically we wanted to know:

How do users experience routine Web browsing when using the Tor Browser?

We addressed this question via a study that examined the use of the Tor Browser in a naturalistic setting for a period of one week, focusing particularly on identifying frustrations, confusions, and problems. To this end, we collected quantitative and qualitative data on the use of the Tor Browser for routine Web browsing and online tasks. Specifically, we made the following contributions:

- **Detailed accounts of naturalistic use of the Tor Browser.**
  We collected data regarding Tor Browser usage for routine online activities in a naturalistic setting, uncovering a number of important UX issues.

- **Suggestions for improving the Tor Browser UX.**
  Grounded in the UX issues encountered during our study, we identified and outlined several practical solutions and design guidelines to address and mitigate the problems and improve the UX of the Tor Browser.

- **Method for privately collecting naturalistic quantitative data on the Tor Browser UX at scale.**
  The method we used for collecting quantitative UX data on Tor Browser usage could be deployed to allow privately gathering naturalistic data at scales significantly beyond those possible in typical laboratory studies. Thus it is a contribution of this dissertation in addition to the understanding we gleaned from it.

Based on 121 questionnaire responses, 11 interviews, and 19 write-ups from 19 study participants, we report on a number of UX issues, such as broken Web sites, latency, lack of common browsing conveniences, differential treatment of Tor traffic, incorrect geolocation, operational opacity, etc. Some of these discoveries were new,

and others reaffirmed issues found by previous work. Based on these discoveries we recommended several changes to the Tor Browser in order to make browsing using Tor more accessible to the common person. Our recommendations included, but were not limited to:

- **Provide the ability to specify threats of relevance to the user.**
  One of our findings was that users dislike the fact that many convenience features that they are fond of, such as built-in password managers and Web history, are unavailable on the Tor Browser. This is because the Tor Browser provides disk-avoidance in order to protect users from local threats. However, not all Tor Browser users are attempting to protect against local adversaries. For this reason, we recommended creating an adversary wizard that would allow users to select the threats they were interested in defending against, and disabling disk-avoidance features if the user is not interested in protecting against a local adversary.

- **Explore alternative ways to deliver blocked content.**
  When a resource cannot be reached via the Tor Browser, it may still be accessible from alternative sources such as Internet archives, etc. For this reason we recommended Tor Browser include a feature that allows for automatic search of Internet archives, search engine caches, and other sources of information for content that is being denied to Tor users.

- **Deliver contextually relevant information during user sessions.**
  Every time the average person buys a new appliance such as a dish washer, they normally do not read the manual before using it. Software is no different. Users do not have the time or patience to read manuals or documentation, so we must supply information to the users when it is contextually relevant. This is especially important in anonymity, where actions can undo the protection provided by tools. For this reason, we recommended that the Tor Browser provide contextually relevant information about ppotentially dangerous behaviors as they happen to help the user learn about how to protect their anonymity.

One of the more important findings of this work was that users who attempt to use the Tor Browser frequenlty and for diverse tasks are likley to run across content on the Web that works on other browsers, but does not work correctly on the Tor Browser.

This broken content became the subject of our next investigation. Specifically, we addressed the question:

What functionality and Web sites break on the Tor Browser and why?

To address this question we created a tool that scanned a Web page on Firefox (for ground truth data) and the Tor Browser and logged the creation of the DOM tree and all JavaScript executions. We then scanned the home-pages of 1000 Web sites and did a cognative walkthrough of 40 Web sites using this tool. The DOM and JavaScript traces were then analyzed to look for signs of broken functionality. From this work we make the following contributions:

- **Tools for collecting and analyzing information about site functionality on the Tor Browser**
  We created a series of tools and analysis scripts to capture information about the DOM rendering process and the JavaScript executions on both Firefox and the Tor Browser. We then created a series of scripts to analyze this data and determine the difference between the JavaScript execution traces and the DOM Rendering processes of Firefox and the Tor Browser.

- **A dataset of 1000 home pages and 40 interactive browsing sessions.**
  We released the dataset created in this project so that it can continue to be studied and more information about the differences between Firefox and the Tor Browser can be discovered.

- **Insight about what functionality breaks on the Tor Browser and why.** We provided details about what functionality breaks on the Tor Browser, and discussed the root causes for these breaks. These breaks were discvoered using a combination of a cognitive walk-through and logging from tools created for this project.

- **Guidelines for creating a Tor Browser Friendly Website.**
  Based on the analysis of our deep dives we proposed some guidelines to create a more Tor Browser Friendly Website. Though these guidelines are data-driven, they are not exhaustive.

We did not find evidence to confirm that broken functionality is a prevalent issue on the lowest setting of the Tor Browser security slider setting. However, we did find some cases in which differential treatment could be misperceived as broken functionality because of the error messages provided by the offending Website. Additionally we discovered issues on the second level of the security slider setting relating to JavaScript not loading over HTTP, and third-party cookies being blocked. Finally, we discovered that a potentially surprising number of Websites allowed us to complete our tasks on the higest level of the Tor Browser security slider setting. Since we only used a subset of the functionality of each Website, this does not guarnatee that some functionality does not break on these sites on the highest level of the Tor Browser security slider.

Based on these findings we provided recommendations for changes to the Tor Browser interface to communicate with the user when funcitonality is being blocked for specific reasons. First we recommended that the Tor Browser automatically detect when a Website is attempting to load JavaScript over HTTP and provide a warning to the user that the site attempted to load scripts in an insecure way and was blocked, potentially leading to broken functionality. We also recommended changes to the NoScript add-on that would change the logo and click-through proceedure for click-to-play media to make it easier for users to use. We also provide feedback to Website operators on how to avoid these pitfalls and remain Tor Browser Friendly.

Depsite the amount that we have achieved in this dissertation, there is still a lot of work that remains to be done. In Chapter 7 we outlined the work we intend on tackling after the completion of this dissertation, including work that is already in the beginning stages. This work includes continued work on the usability and user experience of Tor, work on defenses against traffic confirmation attacks, and work on the usability and user experience of other security and privacy tools.

Appendix A

Interview Protocol

Thank you for taking the time to participate in this interview. The purpose of this interview is to discover your views, opinions, and understanding regarding how Tor works. Many people use Tor everyday for many reasons, from reading their email to accessing blocked Web sites. Please keep in mind that there is no single correct answer to these questions. Please answer the questions based on your own knowledge and experiences.

1. What do you do for a living? What does that entail?
2. What kind of computer(s) or mobile device(s) do you use? What are the differences (if any) in what these device(s) can do and how you use them?
3. On which of these device(s) do you use Tor?
4. When did you start using Tor? Why did you start using Tor?
5. How did you discover Tor?
6. Why do you currently use Tor?
7. This is a drawing exercise. Keeping background processes in mind, please draw what happens when you use the Tor Browser Bundle. Also note of who can access information about you. Please think aloud and explain your thought process while you are drawing.
8. How often do you use Tor?
9. What other browsers do you use?
10. Under which circumstances do you use the Tor Browser Bundle instead of another browser or vice versa?

11. Describe your feelings regarding the advantages and disadvantages of using Tor.

12. In what ways, if any, do you use Tor differently on your mobile device(s) than your computer(s)? (If applicable.)

13. Please fill out the given table of tasks and various entities involved in those tasks. For each of the tasks, mark the entities that you believe can access information about you when you perform the task using Tor. Please also mention what information you believe they can access. (See Table 4.1.)

14. Currently, a debate is going on about the role of privacy tools in matters pertaining to national security. Some people claim that strong privacy tools like Tor are good, while others claim they are bad. This is a part of a larger discussion about the trade-off between privacy and national security concerns. What is your opinion on this matter?

15. Is there anything else you would like to tell us? Is there anything that we should have asked?

Appendix B

Screening questionnaire

We invite you to participate in our study. Your participation will benefit science and help us understand user perceptions of software.

Our study involves a one-on-one interview. You may participate in-person or remotely via telephone or Voice-over-IP solutions, such as Skype. The interview will take a maximum of 45 minutes. Each participant will be compensated with a $20 Starbucks gift card.

To register, please answer the brief questionnaire below. We will contact you if we have an available position. Slots are limited, so if you wish to participate, please sign up as soon as possible.

If you have any questions, please contact us via email.

1) Age

- 18-24
- 25-34
- 35-44
- 45-54
- 55+
- Prefer not to say

2) Gender

- Male
- Female
- Other

- Prefer not to say

3) Email

Please enter your email address. This is the email address we will use to contact you.

4) Which of the devices below do you own and use? (Check all that apply.)

- Desktop Computer
- Laptop Computer
- Smartphone
- Tablet
- Other

5) Which of the technologies and services below have you ever used? (Check all that apply.)

[NOTE: Options were presented in random order.]

- Social Networking (Facebook, Twitter, LinkedIn, etc.)
- Online Audio and Video Conferencing (Skype, Facetime, etc.)
- Anonymization Software (Tor, etc.)
- Office Software (Word, Excel, Powerpoint, etc.)
- Online Music, TV, and Media
- Version Control Software (Git, Subversion, etc.)
- Online File Sharing (Dropbox, OneDrive, etc.)
- Mobile Messaging (Kik, Telegram, Snapchat, etc.)
- Online Banking
- Encryption Software
- Online Communities (Reddit, etc.)
- Computer Programming
- Online Shopping
- Blogging

Appendix C

Prestudy Questionnaire

[Information about Study Procedures]

1. Do you agree to participate in this study?
2. Please enter your participant ID:
3. What is your year of birth?
4. What is your current nationality?
5. How long have you lived in the US?
6. What is your gender?
    - Male
    - Female
    - Other
    - Do not wish to specify
7. What is your ethnicity?
    - American Indian or Native American
    - Asian
    - Black or African American
    - Hispanic
    - Native Hawaiian or Other Pacific Islander
    - White / Caucasian
    - Other

- Do not wish to specify

8. What is your major field of study?
9. What is your current employment status?
    - Employed full time
    - Employed part time
    - Unemployed looking for work
    - Unemployed not looking for work
    - Retired
    - Homemaker
    - Unable to work
    - Do not wish to specify
10. Have you used the Tor Browser before?
    - Yes
    - No
    - Not sure
11. What is the operating system of the computer (desktop or laptop) that you use as your primary computer?
    - Windows
    - MacOS
    - Linux
    - Other
12. What is the operating system of your primary phone?
    - iOS
    - Android
    - Other
13. Have you successfully installed the Tor Browser on your computer(s), and, if you wish, your mobile device(s)?
    - Yes

- No

14. Have you successfully installed our script on your computer?

    - Yes
    - No

Appendix D

Interview Questions

Please keep in mind that there are no incorrect answers to these questions. Any answers you provide will remain strictly confidential with access limited only to the research team unless otherwise required by law. Additionally, you may refuse to answer any question. All questions are optional.

This interview will be recorded to aid in the analysis performed by the researchers. After the interview is transcribed, the audio data will be deleted. Anonymous transcribed data will be retained indefinitely. If you wish, you can request that the recording device be disabled at any time.

Do you consent to the audio recording of this interview?

Do you consent to the indefinite retention of the anonymous transcribed interview data?

1. Please describe your experience using the Tor Browser.
2. Please tell us about some of the issues you encountered using the Tor Browser as your default browser.
   (a) Could you elaborate on the issue?
   (b) Did you encounter this issue more times than you reported it in the online questionnaires?
   (c) On which categories of Web sites did this issue occur?
   (d) Would this issue hinder you from using the Tor Browser in the future?
3. Will you continue using the Tor Browser after this study? Why or why not?
4. In your opinion, which of the issues you encountered while using the Tor Browser caused the most confusion and/or frustration?

5. One issue many Tor Browser users face is long waiting times (high latency). However, this latency can be an artifact of how Tor protects your identity. Indeed, in some instances latency and anonymity are transactional: higher latency can lead to better protection. Knowing this, are there certain tasks for which you would be willing to tolerate latency to gain anonymity?

6. Are there any other issues that you encountered while using the Tor Browser that you wish to report?

7. Is there anything else I should have asked?

Appendix E

Write-up Prompt

Write an essay of about 2-3 single-spaced pages about your experience of using the Tor Browser as your default and primary browser for the duration of one week. Your essay should describe your positive and negative experiences with the user interface and user experience of the Tor Browser. Please provide specific examples along with respective relevant contextual details. Please include a discussion of what you learned specifically about the Tor Browser and Tor as well as generally about Web technology, anonymity, surveillance, etc. Feel free to propose creative solutions or improvements that could have helped you utilize the Tor Browser more effectively. Please also indicate whether your browsing behavior during the study period was typical of your browsing behavior at other times. If your browsing practices during the study period differed from your typical practices, please explain how and why. You may also comment on your study participation experience, such as the questionnaires prompted by the script throughout the week.

Appendix F

Questionnaires

F.1 Tor Browser Questionnaire

1. Please enter your participant ID:
2. Which of the following best describes the issue(s) you encountered? (*Check all that apply.*)
   (a) The Tor Browser was slow.
   (b) Some parts of the Web site I wanted to view did not work.
   (c) Many Web sites wanted to verify that I was human.
   (d) The Tor Browser crashed.
   (e) The Web site I wanted to view did not load in the Tor Browser.
   (f) The Web site blocked the Tor Browser.
   (g) I did not need the Tor Browser for the task at hand.
   (h) I did not know how to proceed via the Tor Browser.
   (i) The Web site I wanted to view was in an incorrect language or currency or showed results for a location far from me.
   (j) The Web site I wanted to view prevented me from performing a specific action (e.g., logging in, posting a comment, etc.).
   (k) I experienced an issue other than those mentioned above.
3. Please provide more details on the above issue(s) you encountered:
4. (*Optional*) Please specify the address (URL(s)) of the Web site(s) that you were browsing when you encountered the above issue(s):

F.2 Switched Browser Questionnaire

1. Please enter your participant ID:
2. Did you encounter any issues with the Tor Browser that caused you to switch to another browser?[1]
   (a) Yes
   (b) No
   (c) Not Applicable: I did not switch to another browser from the Tor Browser.
3. Which of the following best describe the issue(s) you encountered? (*Check all that apply.*)
   (a) The Tor Browser was slow.
   (b) Some parts of the Web site I wanted to view did not work.
   (c) Many Web sites wanted to verify that I was human.
   (d) The Tor Browser crashed.
   (e) The Web site I wanted to view did not load in the Tor Browser.
   (f) The Web site blocked the Tor Browser.
   (g) I did not need the Tor Browser for the task at hand.
   (h) I did not know how to proceed via the Tor Browser.
   (i) The Web site I wanted to view was in an incorrect language or currency or showed results for a location far from me.
   (j) The Web site I wanted to view prevented me from performing a specific action (e.g., logging in, posting a comment, etc.).
   (k) I experienced an issue other than those mentioned above.
4. Please provide more details on the above issue(s) you encountered:
5. (*Optional*) Please specify the address (URL(s)) of the Web site(s) that you were browsing when you encountered the above issue(s):

[1] If the participant did not answer 'Yes,' he or she was not presented further questions.

F.3 Other Browser Questionnaire

1. Please enter your participant ID:
2. Which browser did you use during this browsing session?
   (a) Edge
   (b) Chrome
   (c) Firefox
   (d) Safari
   (e) Opera
   (f) Other. Please specify:
3. Why did you use the above browser instead of the Tor Browser? (*Check all that apply.*)
   (a) I forgot to use the Tor Browser.
   (b) I was annoyed with using the Tor Browser.
   (c) I did not want to use the Tor Browser for this session.
   (d) The Tor Browser was slow.
   (e) Some parts of the Web site I wanted to view did not work in the Tor Browser.
   (f) Many Web sites wanted to verify that I was human.
   (g) The Web site I wanted to view did not load in the Tor Browser.
   (h) The Web site I wanted to view blocked the Tor Browser.
   (i) I did not need the Tor Browser for the task at hand.
   (j) I did not know how to proceed via the Tor Browser.
   (k) The Web site I wanted to view prevented me from performing a specific action (e.g., logging in, posting a comment, etc.).
   (l) None of the above.
4. Please provide more details regarding the above reason(s):
5. Which category of Web sites were you browsing during this session? (*Check all that apply.*)

(a) Adult
(b) Arts
(c) Business
(d) Communication (e.g., emails, chat, conferencing, etc.)
(e) Computers
(f) Games
(g) Health
(h) Home
(i) Kids and Teens
(j) Lifestyle
(k) News
(l) Recreation
(m) Reference
(n) Regional
(o) Social Media
(p) Science
(q) Shopping
(r) Society
(s) Sports
(t) Technology
(u) World

Bibliography

[1] Masoud Akhoondi, Curtis Yu, and Harsha V Madhyastha. Lastor: A low-latency as-aware tor client. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy (S&P 2012)*, pages 476–490. IEEE, 2012.

[2] Mashael AlSabah, Kevin Bauer, Tariq Elahi, and Ian Goldberg. The path less travelled: Overcoming Tor's bottlenecks with traffic splitting. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 143–163. Springer, 2013.

[3] Mashael AlSabah, Kevin Bauer, and Ian Goldberg. Enhancing tor's performance using real-time traffic classification. In *Proceedings of the 2012 ACM conference on Computer and Communications Security (CCS 2012)*, pages 73–84. ACM, 2012.

[4] Mashael AlSabah, Kevin Bauer, Ian Goldberg, Dirk Grunwald, Damon McCoy, Stefan Savage, and Geoffrey M Voelker. Defenestrator: Throwing out windows in tor. In *Proceedings of the 11th Privacy Enhancing Technologies Symposium (PETS 2011)*, pages 134–154. Springer, 2011.

[5] Marilyn Hughes Blackmon, Peter G Polson, Muneo Kitajima, and Clayton Lewis. Cognitive walkthrough for the web. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 463–470. ACM, 2002.

[6] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[7] Yushi Cheng, Xiaoyu Ji, Juchuan Zhang, Wenyuan Xu, and Yi-Chao Chen. Demicpu: Device fingerprinting with magnetic signals radiated by cpu. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1149–1170. ACM, 2019.

[8] Jeremy Clark, P. C. van Oorschot, and Carlisle Adams. Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS 2007)*, pages 41–51. ACM, 2007.

[9] Sunny Consolvo, Frank R Bentley, Eric B Hekler, and Sayali S Phatak. Mobile user research: A practical guide. *Synthesis Lectures on Mobile and Pervasive Computing*, 9(1):i–195, 2017.

[10] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI 2005)*, pages 81–90. ACM, 2005.

[11] Roger Dingledine and Nick Mathewson. Anonymity Loves Company: Usability and the Network Effect. In *Proceedings of Workshop on the Economics of Information Security (WEIS 2006)*, pages 547 – 559. Springer, 2006.

[12] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The Second-generation Onion Router. In *Proceedings of the 13th Conference on USENIX Security Symposium (USENIX Security 2004)*, pages 21–21. USENIX Association, 2004.

[13] Roger Dingledine and Steven J Murdoch. Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it. `https://www.torproject.org/press/presskit/2009-03-11-performance.pdf`. Accessed: 2017-06-15.

[14] Benjamin Fabian, Florian Goertz, Steffen Kunz, Sebastian Müller, and Mathias Nitzsche. Privately Waiting – A Usability Analysis of the Tor Anonymity Network. In *Sustainable e-Business Management: Proceedings of the 16th Americas Conference on Information Systems (AMCIS 2010)*, pages 63–75. Springer, 2010.

[15] Jay W. Forrester. Counterintuitive behavior of social systems. *Technological Forecasting and Social Change*, 3:1–22, January 1971.

[16] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. Privacy, anonymity, and perceived risk in open collaboration: A study of tor users and wikipedians. In *Proceedings of the 20th ACM Conference on Computer-Supported Cooporative Work and Social Computing (CSCW 2017)*, pages 1800–1811, 2017.

[17] Kevin Gallagher, Sameer Patil, and Nasir Memon. New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 385–398. USENIX Association, 2017.

[18] John Geddes, Michael Schliep, and Nicholas Hopper. Abra cadabra: Magically increasing network utilization in tor by avoiding bottlenecks. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2016)*, November 2016.

[19] Barney G Glaser and Anselm L Strauss. *The discovery of grounded theory: Strategies for qualitative research*. Transaction Publishers, 2009.

[20] David M Goldschlag, Michael G Reed, and Paul F Syverson. Hiding routing information. In *Proceedings of the International Workshop on Information Hiding*, pages 137–150. Springer, 1996.

[21] Virgil Griffith. Tor growth rates and improving Torperf throughput. Technical Report 2014-10-001, The Tor Project, October 2014.

[22] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. Away from prying eyes: Analyzing usage and understanding of private browsing. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 159–175, Baltimore, MD, August 2018. USENIX Association.

[23] Hans Hanley, Yixin Sun, Sameer Wagh, and Prateek Mittal. DPSelect: A differential privacy based guard relay selection algorithm for tor. *Proceedings on Privacy Enhancing Technologies*, 2019(2):166–186, April 2019.

[24] Stefan E Hormuth. The sampling of experiences in situ. *Journal of personality*, 54(1):262–293, 1986.

[25] Ronggui Huang. *RQDA: R-based Qualitative Data Analysis*, 2018. R package version 0.3-1.

[26] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Proceedings of Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346. USENIX Association, 2015.

[27] Aaron D Jaggard, Aaron Johnson, Sarah Cortes, Paul Syverson, and Joan Feigenbaum. 20,000 in league under the sea: Anonymous communication, trust, MLATs, and undersea cables. In *Proceedings on Privacy Enhancing Technologies (PoPETS 2015)*, pages 4–24. De Gruyter Open, 2015.

[28] Rob Jansen, John Geddes, Chris Wacek, Micah Sherr, and Paul Syverson. Never been KIST: Tor's congestion management blossoms with kernel-informed socket transport. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 127–142, San Diego, CA, 2014. USENIX Association.

[29] Rob Jansen and Aaron Johnson. Safely measuring Tor. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS 2016)*, pages 1553–1567. ACM, 2016.

[30] Rob Jansen, Marc Juarez, Rafa Gálvez, Tariq Elahi, and Claudia Diaz. Inside job: Applying traffic analysis to measure tor from within. In *Network and Distributed System Security Symposium (NDSS 2017)*. IEEE Internet Society, 2017.

[31] Rob Jansen, Marc Juarez, Rafael Galvez, Tariq Elahi, and Claudia Diaz. Inside job: Applying traffic analysis to measure tor from within. In *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society, 2018.

[32] Rob Jansen and Matthew Traudt. Tor's been kist: A case study of transitioning tor research to practice. *arXiv preprint arXiv:1709.01044*, 2017.

[33] Rob Jansen, Florian Tschorsch, Aaron Johnson, and Björn Scheuermann. The sniper attack: Anonymously deanonymizing and disabling the Tor network. In *Proceedings of the Network and Distributed System Security Symposium 2014 (NDSS 2014)*. Internet Society, 2014.

[34] Rob Jansen, Tavish Vaidya, and Micah Sherr. Point break: A study of bandwidth denial-of-service attacks against tor. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1823–1840, Santa Clara, CA, August 2019. USENIX Association.

[35] Aaron Johnson, Rob Jansen, Nicholas Hopper, Aaron Segal, and Paul Syverson. Peerflow: Secure load balancing in tor. *Proceedings on Privacy Enhancing Technologies (PETS 2017)*, 2017(2), April 2017.

[36] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52. USENIX Association, 2015.

[37] Anne R Kearney and Stephen Kaplan. Toward a methodology for the measurement of knowledge structures of ordinary people: The conceptual content cognitive map (3CM). *Environment and Behavior*, 29(5):579–617, 1997.

[38] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J Murdoch, and Damon McCoy. Do You See What I See? Differential Treatment of Anonymous Users. In *Proceedings of the Network and Distributed System Security Symposium 2016 (NDSS 2016)*. Internet Society, 2016.

[39] Katharina Kohls, Kai Jansen, David Rupprecht, Thorsten Holz, and Christina Popper. On the challenges of geographical avoidance for tor. In *Proceedings 2019 Network and Distributed System Security Symposium*. Internet Society, 2019.

[40] Stefan Köpsell. Low Latency Anonymous Communication – How Long Are Users Willing to Wait? In *Proceedings of Emerging Trends in Information and Communication Security (ETRICS 2006)*, pages 221–237. Springer, 2006.

[41] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS 2009)*, pages 3:1–3:12. ACM, 2009.

[42] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. A Usability Evaluation of Tor Launcher. In *Proceedings on Privacy Enhancing Technologies (PoPETs 2017)*, pages 87–106. De Gruyter Open, 2017.

[43] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. Why Johnny Can't Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, pages 589–598. ACM, 2012.

[44] Zhaofeng Ma, Ming Jiang, Hongmin Gao, and Zhen Wang. Blockchain for digital rights management. *Future Generation Computer Systems*, 89:746–764, December 2018.

[45] Srdjan Matic, Platon Kotzias, and Juan Caballero. CARONTE: Detecting location leaks for deanonymizing Tor hidden services. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS 2015)*, pages 1455–1466. ACM, 2015.

[46] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. Shining Light in Dark Places: Understanding the Tor Network. In *Proceedings of the 8th International Privacy Enhancing Technologies Syposium (PETS 2008)*, pages 63–76. Springer, 2008.

[47] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *Proceedings of the 24th USENIX Security Symposium (USENIX Security 2015)*, pages 399–414. USENIX Association, 2015.

[48] Helen Nissenbaum. The meaning of anonymity in an information age. *The Information Society*, 15(2):141–144, 1999.

[49] Greg Norcie, Jim Blythe, Kelly Caine, and L. Jean Camp. Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. In *Proceedings of the 2014 Workshop on Usable Security (USEC 2014)*. Internet Society, 2014.

[50] Greg Norcie, Kelly Caine, and L Jean Camp. Eliminating Stop-Points in the Installation and Use of Anonymity Systems: A Usability Evaluation of the Tor Browser Bundle. In *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS 2012)*. PETS Symposium, 2012.

[51] Ronald Oussoren. Pyobjc. `https://bitbucket.org/ronaldoussoren/pyobjc/src`, 2018.

[52] Rebekah Overdorf, Mark Juarez, Gunes Acar, Rachel Greenstadt, and Claudia Diaz. How unique is your .onion?: An analysis of the fingerprintability of tor onion services. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017)*, pages 2021–2036. ACM, 2017.

[53] Mike Perry. The trouble with cloudflare. `https://blog.torproject.org/trouble-cloudflare?page=2`, Mar 2016.

[54] Mike Perry, Erinn Clark, Steven Murdoch, and Georg Koppen. The design and implementation of the tor browser [draft]. https://2019.www.torproject.org/projects/torbrowser/design/, Jun 2018.

[55] Matthew Prince. The trouble with tor. https://blog.cloudflare.com/the-trouble-with-tor/, Aug 2018.

[56] Lee Rainie, Martin Shelton, and Mary Madden. Americans' privacy strategies post-Snowden. *Pew Research Center*, March 2015.

[57] Anand Rajaraman and Jeffrey David Ullman. *Mining of massive datasets*. Cambridge University Press, 2011.

[58] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI 2018)*, page 512. ACM, 2018.

[59] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why Doesn't Jane Protect Her Privacy? In *Proceedings of Privacy Enhancing Technologies (PoPETs 2014)*, pages 244–262. Springer, 2014.

[60] Vera Rimmer, Davy Preuveneers, Marc Juarez, Tom Van Goethem, and Wouter Joosen. Automated website fingerprinting through deep learning. *Proceedings 2018 Network and Distributed System Security Symposium*, 2018.

[61] Giampaolo Rodolà. psutil. https://github.com/giampaolo/psutil, 2018.

[62] Phillip Rogaway. The moral character of cryptographic work. *IACR Cryptology ePrint Archive*, 2015:1162, 2015.

[63] Mahrud Sayrafi. Introducing the cloudflare onion service. https://blog.cloudflare.com/cloudflare-onion-service/, Dec 2018.

[64] Quirin Scheitle, Oliver Hohlfeld, Julien Gamba, Jonas Jelten, Torsten Zimmermann, Stephen D Strowes, and Narseo Vallina-Rodriguez. A long way to the top: significance, structure, and stability of internet top lists. In *Proceedings of the Internet Measurement Conference 2018*, pages 478–493. ACM, 2018.

[65] David Silver, Suman Jana, Dan Boneh, Eric Yawei Chen, and Collin Jackson. Password managers: Attacks and defenses. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 2014)*, pages 449–464, 2014.

[66] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. Characterizing the nature and dynamics of tor exit blocking. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 325–341, 2017.

[67] Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang, and Prateek Mittal. RAPTOR: Routing Attacks on Privacy in Tor. In *Proceedings of the 24th USENIX Security Symposium (USENIX Security 2015)*, pages 271–286. USENIX Association, 2015.

[68] The Tor Project. FAQ. `https://www.torproject.org/docs/faq.html.en`. Accessed: 2017-06-15.

[69] The Tor Project. Tor security advisory: Old Tor Browser Bundles vulnerable. `https://blog.torproject.org/blog/tor-security-advisory-old-tor-browser-bundles-vulnerable`. Accessed: 2017-06-15.

[70] The Tor Project. Understanding and Using Tor - An Introduction for the Lay(wo)man. `https://trac.torproject.org/projects/tor/wiki/doc/TorALaymansGuide`. Accessed: 2017-06-15.

[71] Jesse Victors, Ming Li, and Xinwen Fu. The onion name system: Tor-powered decentralized dns for tor onion services. *Proceedings on Privacy Enhancing Technologies (PETS 2017)*, 2017(1), January 2017.

[72] Gerry Wan, Aaron Johnson, Ryan Wails, Sameer Wagh, and Prateek Mittal. Guard placement attacks on path selection algorithms for tor. *Proceedings on Privacy Enhancing Technologies*, 2019(4):272–291, October 2019.

[73] Rick Wash. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*, pages 11:1–11:16. ACM, 2010.

[74] Rick Wash and Emilee Rader. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325. USENIX Association, 2015.

[75] Wayback Machine. Wayback machine, 2018.

[76] Philipp Winter, Anne Edmundson, Laura M. Roberts, Agnieszka Dutkowska-Żuk, Marshini Chetty, and Nick Feamster. How do tor users interact with onion services? In *27th USENIX Security Symposium (USENIX Security 2018)*, pages 411–428, Baltimore, MD, 2018. USENIX Association.

[77] Philipp Winter and Stefan Lindskog. How the Great Firewall of China is Blocking Tor. In *Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet*. USENIX Association, 2012.

[78] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, Baltimore, MD, August 2018. USENIX Association.

[79] Eric Zhu and Vadim Markovtsev. Ekzhu/datasketch: First stable release. https://zenodo.org/record/290602, 2017.

[80] Mary Ellen Zurko and Richard T. Simon. User-centered Security. In *Proceedings of the 1996 Workshop on New Security Paradigms (NSPW 1996)*, pages 27–33. ACM, 1996.