Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Privately Waiting – A Usability Analysis of the Tor Anonymity Network

Benjamin Fabian
Humboldt-Universität zu Berlin, bfabian@wiwi.hu-berlin.de

Florian Goertz
Humboldt-Universität zu Berlin, goertzfl@cms.hu-berlin.de

Steffen Kunz
Humboldt-Universität zu Berlin, Institute of Information Systems, steffen.kunz@wiwi.hu-berlin.de

Sebastian Müller
Humboldt-Universität zu Berlin, sebastian.mueller.4@hu-berlin.de

Mathias Nitzsche
Humboldt-Universität zu Berlin, mathias.nitzsche@student.hu-berlin.de

Privately Waiting – A Usability Analysis of the Tor Anonymity Network

Benjamin Fabian
Institute of Information Systems
Humboldt-Universität zu Berlin
bfabian@wiwi.hu-berlin.de

Florian Goertz
Institute of Information Systems
Humboldt-Universität zu Berlin
goertzfl@cms.hu-berlin.de

Steffen Kunz
Institute of Information Systems
Humboldt-Universität zu Berlin
steffen.kunz@wiwi.hu-berlin.de

Sebastian Müller
Institute of Information Systems
Humboldt-Universität zu Berlin
sebastian.mueller.4@hu-berlin.de

Mathias Nitzsche
Institute of Information Systems
Humboldt-Universität zu Berlin
mathias.nitzsche@student.hu-berlin.de

ABSTRACT

As the Internet is increasingly absorbing information from the real world it becomes more important to prevent unauthorized collection and abuse of personalized information. At the same time, democratic societies should establish an environment helping not only their own people but also people who face repressive censorship to access public information without being identified or traced. Internet anonymization tools such as Tor offer functionalities to meet this demand.

In practice, anonymization of Internet access can only be achieved by accepting higher latency, i.e., a longer waiting time before a Web site is displayed in the browser, and therefore reducing its usability significantly. Since many users may not be willing to accept this loss of usability, they may refrain from or stop using Tor – at the same time decreasing the anonymity of other users, which depends on shared resources in the Tor user community. In this paper[1], we quantify the loss of usability by measuring the additional latency of the Tor software and combine our measurements with metrics of the existing Web usability and performance literature. Our findings indicate that there is still a major usability gap induced by Tor, leading to its possible disuse accompanied by a higher risk exposure of Internet users.

Keywords (Required)

Usability, Latency, Security, Privacy, Anonymity, Tor

INTRODUCTION

Today, information technology allows data analysis to a degree which was unconceivable a few years ago. Simultaneously to the increasing amount and availability of information on the Internet, new information retrieval, data mining, and further technologies allow to automatically collect, filter, and analyze personal information and draw conclusions based on this process. In repressive political regimes, where personal rights, the freedom of speech, and in particular free access to information is restricted, these possibilities of modern data collection can lead to persecution of individuals if their identity is unveiled. Another restraint is censorship, which is used by repressive political regimes to restrict access to unwanted information (Amnesty International 2006).

By using anonymization tools such as the Tor onion routing network (Tor Project 2010a), Internet users can conceal their

[1] This research was funded by the German Federal Ministry of Education and Research under grant number 01IA08001E as part of the Aletheia project (http://www.aletheia-projekt.de/). The responsibility for this publication lies with the authors.

virtual tracks, leading to a non-personalized Internet access. With Tor, application messages are not directly routed to the receiver, but are encrypted and forwarded through ephemeral paths of an overlay network, using more complicated routes that are hard to analyze for an adversary. The more users participate, the harder it is to correlate senders and receivers. The anonymity provided within the Tor network attracts many different groups of users like journalists and activists or business, governmental, military, and private users (Palme and Berglund 2002; Vitone 2008). A recent study showed significant growth in Tor users in China as the governmental censorship increased and also in Iran when the riots after the presidential election took place (Loesing et al. 2009).

Besides one-time installation and configuration efforts, the main usability costs for using an anonymization tool such as Tor consist of an increase in Web latency. Several authors already discussed technically why Tor is slow and proposed how to improve the performance (Dingledine and Murdoch 2009; Loesing 2009; Loesing et al. 2009). In this paper, we compare requests via Tor to direct requests (without Tor) in order to discuss the impact of latency problems and the associated expected user cancelation rate, the percentage of users who abandon the wait during a certain time interval. This metric is an indicator how easy it would be to keep existing users and to attract new, "average" Web users to Tor for increasing their own anonymity as well as the anonymity of the whole user community.

The rest of this paper is structured as follows. In the following section, we focus on the influence of usability in security. Next, we introduce two forms of latency, core and average (technical) latency, which we use as the major usability factor for Web anonymity, followed by a description of our experimental setup. Additionally, we describe the execution and the results of our experiment. Finally, we discuss our major findings as well as related and future work.

USABILITY OF SECURITY

With the increasing need for human rights enforcement in a globalized world, the topic of security has recently gained momentum on the Internet. Security can generally be understood as the prevention of adversary attacks and can be divided in local (system) and communication security (Wright 2004). Local security is well-debated in public as a necessary precondition for privacy. However, the same is also true for communication security, though most Internet users are not aware of the attacks threatening their daily communication links. One potential countermeasure against the adversary attacks on communication security is anonymization (Wright 2004). In our case, the Tor security software provides privacy for Internet users by fundamentally enhancing their anonymity when using the Internet.

The problem associated with most of today's security and privacy solutions is not that the level of security they provide is insufficient, but rather their lack of usability. If the usability for certain security features is too low, end users are not willing to apply them, increasing the users' personal risk exposure to adversary attacks. Recent studies show that too complex security features are not applied if they are not obligatory, see Mannan and van Oorschot (2008) for usage of security in a banking scenario. The amount of time or money users are willing to spend for more security is restricted and differs individually.

There exist two ways to foster a broader application of security mechanisms: either (i) to increase the awareness of security risks in order to raise the willingness to pay money or time, or (ii) to increase the usability of the security features. In the case of Tor, our main hypothesis is that due to its poor usability, i.e., its additional latency, Tor is not frequently and intensively used.

LATENCY AS USABILITY FACTOR

In the area of e-commerce, there is a common understanding that waiting time impedes increasing online commerce (Nielson 1999; Rose et al. 1999; Ryan and Valverde 2003; Stockport et al. 2001), although the authors do not agree on concrete metrics. Due to the fact that in our Tor usability experiment latency has to be classified and finally quantified, we need to define metrics to measure when users cancel their Web page request or in other words, how long users tolerate waiting for a request. Table 1 summarizes the existing literature about critical latency thresholds for Internet users, providing different classifications (e.g., response time below x seconds is acceptable, but response time higher than x seconds is not).

According to these works, we assume that user tolerance for waiting for Web page requests decreases after 2s; it falls sharply within the interval between 7s and 15s, and ends with 50s when the user stops waiting. In our opinion, the research conducted by Nah (2004) is best suited for our experiment due to its empirical grounding and most recent data compared to the other studies. In particular, we apply the results presented in Figure 1 referencing Nah's (2004) *first attempt waiting scenario* in which the user is confronted with a broken link while not getting any feedback from the Web browser. Here, an important metric is introduced: the percentage of users who abandoned the wait during the time interval specified. We label and adopt this *cancelation rate* as a good indicator for the user's waiting tolerance in our setting.

Author	Critical Latency	Description	Year	Source
Nah	2s	For simple information retrieval tasks	2004	Journal
AccountingWEB	8s	Optimal Web page waiting time	2000	Practical advise
Bhatti	8.57s	Tolerable delay by users	2000	Conference
Selvidge	10s	Tolerable delay by users	1999	Practical advise
Nielson	10s	Optimal Web page waiting time	1999	Practical advise
Galetta	12s	Start of significant decrease in user satisfaction	2004	Journal
Nah	15s	Free user from physical and mental captivity	2004	Journal
Ramsay	41s	Suggestion as cut-off for long delays	1998	Journal

Table 1: Classification of Tolerable Waiting Time

In our experiment, we focus on technical latency, i.e., the latency that can be measured while providing reproducible results. In particular, we examine the *core latency*, which is the duration of a single HTTP request without downloading the complete content of the Web page. This latency also entails the time for the Domain Name System (DNS) request which will be discussed later. The *average latency*, on the other hand, refers to the time for downloading the complete content necessary to display the whole page in the Web browser. We do not focus on perceived latency, i.e., how individual users perceive the waiting time, since this metric strongly depends on soft social, cultural, and further context factors as well as individual browser and operating system settings that are difficult to quantify and pose interesting research challenges for future work. Further, at this stage of our research, we have not investigated how much additional latency a user is willing to accept for anonymous browsing. This will be part of future research.

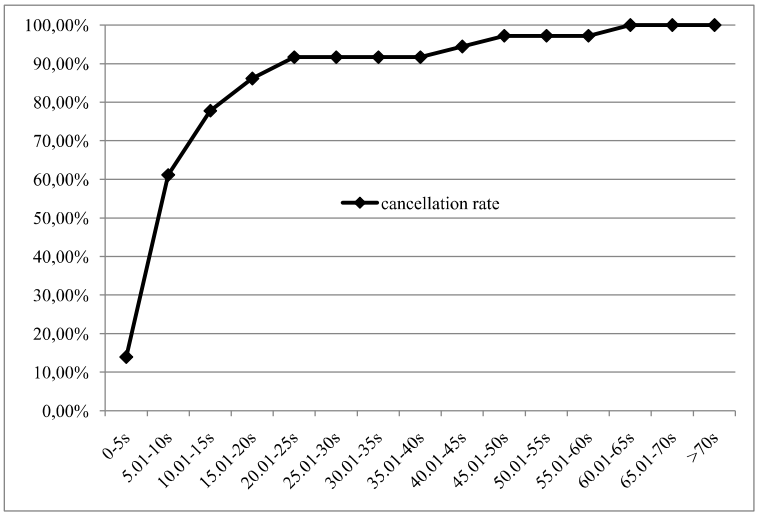

Figure 1: Cancelation Rate of *waiting for broken link in first attempt* (Nah, 2004, p.159)

EXPERIMENT

The experiment was conducted from a standard Internet user's point of view, i.e., the behavior of a user is simulated and modeled as follows: The user is accessing the Internet from his home location via DSL (situated in Europe), requesting

different Web sites over a certain period of time. The 50 Web sites, we sent requests to, were taken from SEOMOZ[2], which provides a list of the 500 most linked Web pages on the Internet. For collecting the empirical data, Perl scripts that simulate user requests were developed. In order to prevent distortion of the results, competing traffic during the experiment was omitted. The experiment itself was conducted within a period of 3 days and the tests took place during different times of the day. Table 2 shows the hardware and software we used for our experiment.

Core Latency

For measuring the *core latency* – the duration of a single HTTP request without downloading the complete content of the Web page –, the time needed for each of altogether 50 *GET* requests to each of the target Web sites was measured. A Perl script using the *LWP library* (Aas 2010) was used to perform these HTTP requests automatically. This library provides methods to dispatch *GET* requests. In each request, only a single HTML Web source was demanded. Additional data or media, like images, videos, or java scripts were not transferred. The Perl script iterated a list of targets, which stores the 50 most linked Web sites. Each target was requested once with Tor and once without Tor in an alternating sequence. All Tor requests were directed over Socks protocol proxy "Privoxy" (Privoxy 2010), which then forwarded the request over the Tor network. After having processed one target, one run was complete. Altogether, 50 runs were executed. Date and time, request duration, and received bytes were logged for each request.

Figure 2 and Figure 3 compare the duration of HTTP requests with and without Tor. All results gained by completing 50 runs are visualized. The 50 different Web sites are shown on the x-axis. Each vertical line displays the maximum and minimum time of the core latency and the 0.25- and 0.75-quantile included as bar. Further analysis showed that 50% of all HTTP requests of the direct connection take between 0.79s and 1.95s, while 50% of all HTTP request with Tor are between 3.9s and 12.4s. This indicates that the core latency of Tor-based requests has a larger deviation. Further, we calculated the median of core latency across all 50 sites for both access methods. The median value was chosen because a high deviation and peak values can distort the arithmetic average. Tor's median of 6.98s compared to 1.37s for direct connection indicates a five times higher core latency.

PC	IBM Lenovo X61s Intel Core 2 Duo 1.60 GHz 2GB memory
Operation System	Windows XP SP3
Software	TorPortable 1.3.1 Privoxy 3.0.12 Vidalia 0.1.15 Strawberry Portable 5.10.0.6 TorDNS v1.7 WiresharkPortable 1.2.5 GNU Wget tool LWP library
Internet Access	ADSL 16 Mbit/s Download, 1 Mbit/s Upload

Table 2: Hardware Deployment for Experiments

[2] http://www.seomoz.org/

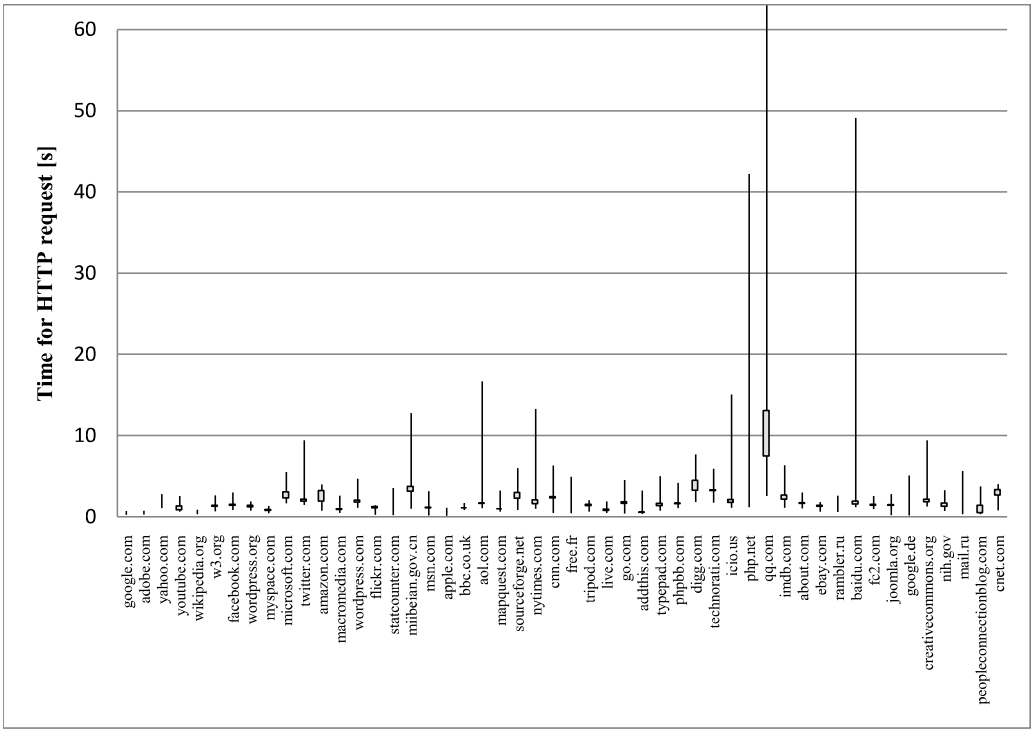

Figure 2: Core Latency for Direct Access (in Seconds)

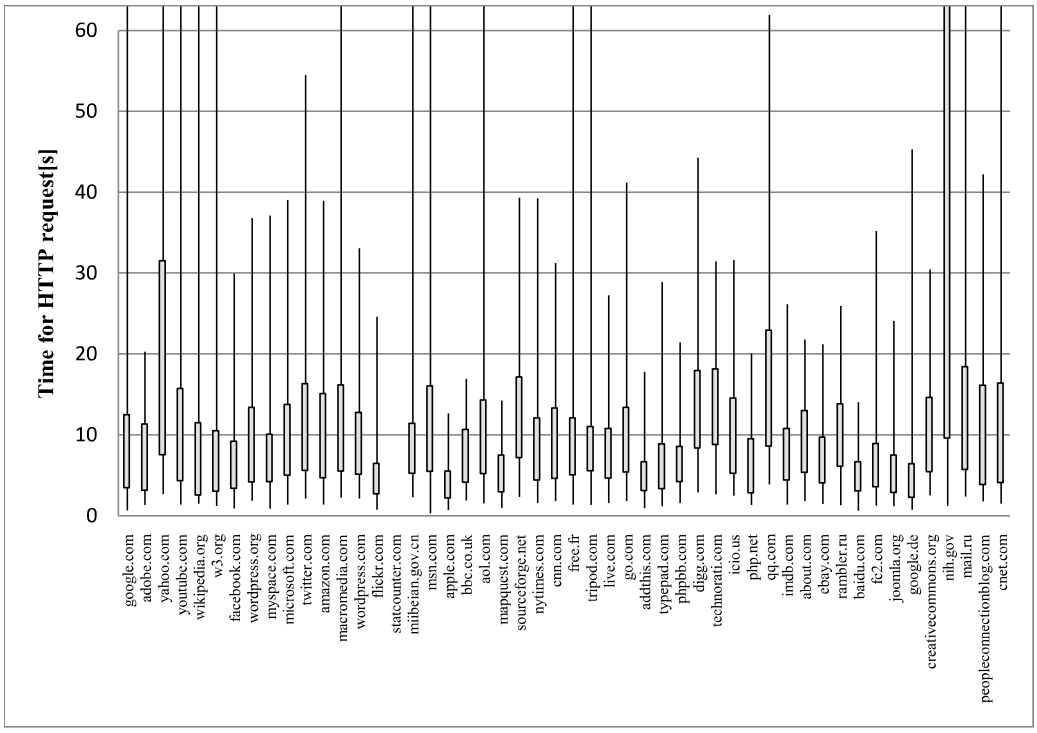

Figure 3: Core Latency with Tor (in Seconds)

DNS Request as a Part of the HTTP Request

In order to break down the core latency, we further investigated the DNS latency of the HTTP request by applying a Perl script that looped over the 50 most linked Web sites and conducted alternating DNS requests with and without Tor using the *dig* command line tool. Instead of the standard DNS Server of the Internet service provider, for direct requests, Google's public DNS server (with IP 8.8.8.8) was used via the User Datagram Protocol (UDP), to make the experiment outcome reproducible for later experiments. For request over the Tor network, a local DNS proxy was used to forward UDP-based DNS requests to Tor as Transmission Control Protocol (TCP) based requests that are currently necessary for Tor. The Tor-DNS-Tool v1.7, which is recommended on the Tor homepage, was used for this purpose.

Figure 4 shows the (rounded) median and the 0.25- and 0.75-quantile included as bar. It reveals that the Tor DNS request in our experiments was around 45 times slower with a much larger span of values compared to a direct DNS request.

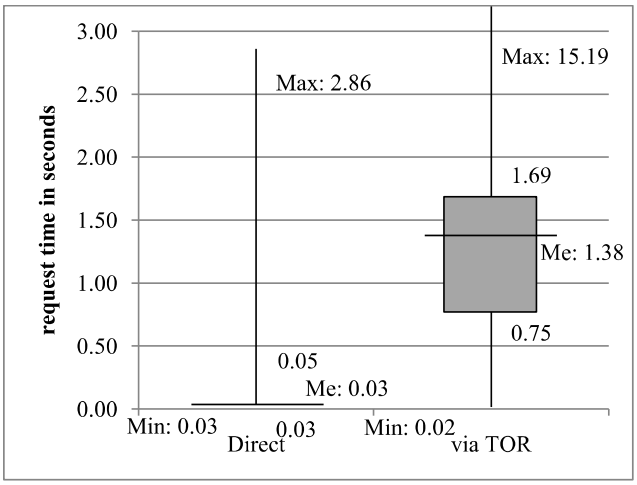

Figure 4: Direct and Tor-Based DNS Requests (in Seconds)

Figure 5 shows the proportion of DNS latency compared to the average latency. We applied the median value for this comparison. It can be noticed that the latency portion of the DNS request was always under 35% and it is therefore not dominant for the whole request time. However, it can also be recognized that the proportion of the Tor DNS latency, as part of the core latency, was disproportionally higher than for direct requests. One possible reason could be that Tor is currently sending DNS requests via the TCP stack instead of using UDP. In future releases, Tor may be able to use the UDP stack for DNS requests.

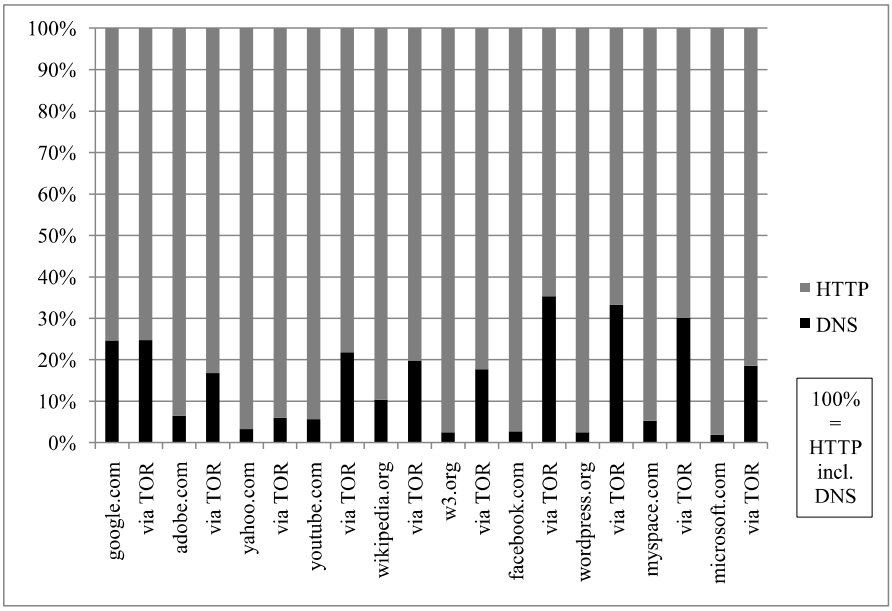

Figure 5: Comparison of Latency Proportions of HTTP and DNS

Average Latency

In the preceding paragraphs, we referred to the latency for a single HTTP request. In order to determine the usability, we have to take the waiting time for a complete Web site into consideration, i.e., to download all the content necessary to display a complete Web site. In order to do so, we tested the top 50 Web sites (the same ones as for the core and DNS latency setting) and found out that downloading a complete Web page, instead of only the first HTML page, raises the core latency by the factor 2.4. We repeated our test three times and the result did not vary more than 15% (upside and downside). We consider this variation as nonsignificant. Accordingly, using this *average latency* as an indicator for downloading entire Web sites, we extrapolate the downloading time of one page by the factor 2.4.

We have to note that this approach, though most suited for our experimental setting, has some limitations: (i) The results vary between different Web sites, while extrapolating does not cover this issue. We do not consider this as crucial due to the fact that we focus on average latency. (ii) When downloading the complete Web page, additional variations in terms of time and coverage for different browsers and individual browser settings may be experienced. In order to provide a most reproducible and browser independent benchmark for the average latency factor, we decided to do the request via the *GNU Wget* tool for downloading Web sites from the command line. Our comparison is based on the *wget* and *wget –p* command, with *wget –p* as estimator for retrieving entire Web sites (including inline images, sounds, and referenced style-sheets). Some parallel control experiments using the *Yslow* plug-in for *Firefox*[3] indicated that this approach provides a good estimation in the average case for our set of Web sites.

The extrapolation by the identified factor 2.4 increases the median of the HTTP Tor request from 7.08s to 16.99s. The median of the HTTP requests without Tor increases from 1.37s to 3.29s. Figure 6 shows the results of our comparison. The extrapolated average latency is referenced by *AVG*, the core latency by *CORE* and the latency of the DNS request by *DNS*, while requests directed via the Tor network are referenced by *TOR* and the direct requests by *Direct*. The bars show the difference between the 0.25-quantile and the 0.75-quantile of the requests' latency. In every bar, there is an additional indicator for the median latency. The 0.75-quantile of the extrapolated download time of whole Web sites via Tor is 30.26 seconds, the median 16.99 seconds, and the 0.25-quantile 9.60 seconds. It can be recognized that every 0.25-quantile of Tor requests is higher than the 0.75-quantile of direct requests of the same request type. Hence, at least 75% of all direct requests are faster than 75% of all Tor requests. Figure 6 also implicates that the variance of different Tor requests is much higher than for direct requests.

[3] http://developer.yahoo.com/yslow/

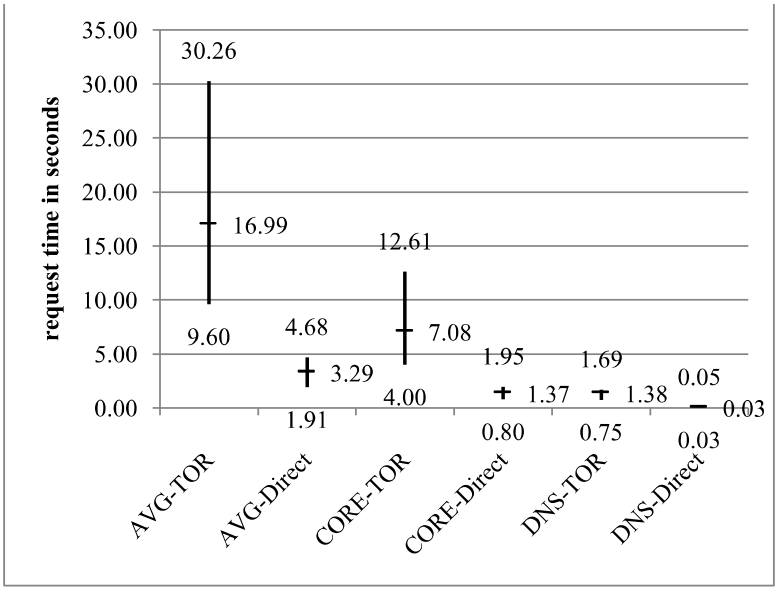

Figure 6: Comparison of Request Times (in Seconds)

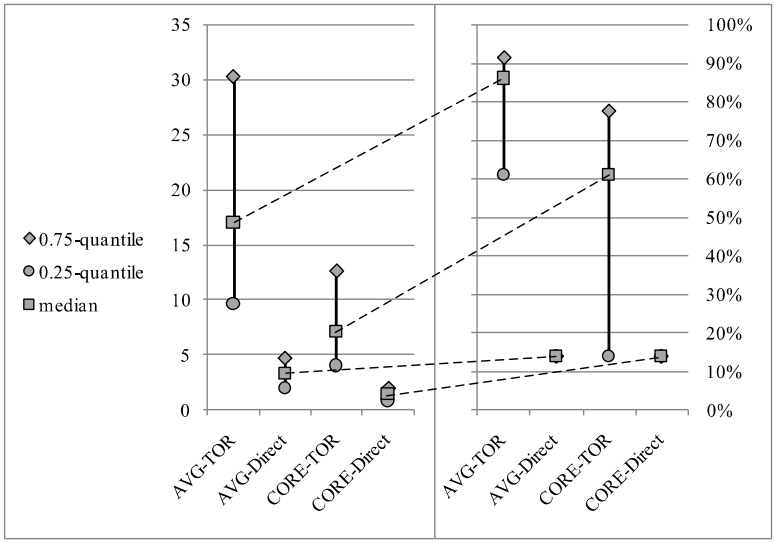

Figure 7: Mapping of Core and Average Latency to Expected Cancelation Rate

Cancelation Rate for Average and Core Latency

In Figure 7, we map our technical latency results to the user cancelation rate of Figure 1. This mapping shows direct and Tor-based core and average latency and the respective cancelation rate. This indicates an expected disproportionate increase in user cancelation when sending requests via TOR. The median of the average latency via Tor maps to a median of 88% cancelation rate, while user frustration for the median of direct average latency maps to 14% cancelation. This expected disproportional increase, which we aim to support by our own set of user studies in future work, indicates a crucial gap in user cancelation when using the Tor software. Lowering the average latency via Tor by 2 seconds would decrease the user cancelation rate by 8%. A reduction of Tor-based average latency by 7 seconds would reduce the cancelation rate by 25% The same cancelation rate for Tor-based and direct request would require reducing the average latency of Tor by 12 seconds.

RELATED WORK

Several authors have already discussed why Tor is slower or have proposed how to improve the performance, e.g., Loesing,

(2009) or Dingledine and Murdoch (2009). In Loesing (2009) the throughput metric from the user's perspective is measured and analyzed. Other research approaches have conducted demographic studies, e.g., number and countries of exit nodes or estimation of user numbers and origin (Loesing et al. 2009). These approaches differ from our approach as this paper focuses on a comparison of performance. In the Tor Metrics subproject (Tor Project 2010b) different users have provided long-term data of the Tor performance. Their results indicate that the performance of Tor is volatile over time, but they do not discuss the latency gap compared to a direct connection. In our paper, we aim to close this research gap by a comparison of Internet access with and without the application of Tor.

In the existing security literature there are other security related technologies that generate additional latency: Fathi et al. (2005) discuss the latency of WLAN security mechanisms, while Zia et al. (2007) focus on the latency of security mechanisms in wireless sensor networks. Lyu and Lau (2000) measure the latency of various firewall security levels. Dinev and Hu (2007) discuss the user behavior toward protective technologies. They mention that awareness of the threats posed by attacks (negative technologies) has a strong impact on the user behavioral intention for using protective technologies.

DISCUSSION AND FUTURE WORK

In our experimental setting, we focused on the 50 most linked Web sites on the Internet. In future work less optimized and less country-specific Web sites should also be taken into consideration. We assume that the average latency between direct and Tor-based requests will even increase in such settings. In addition, a larger number of Web sites could be taken into account. The approach that could reflect a real user's browsing behavior best would be to provide a Tor exit node by ourselves and use the requested Web sites of the exit node for our experiment. We focused on the usability losses, i.e., the costs for gaining anonymity on the Internet. This paper may provide a good starting point for future research focusing on the reasons for high latency caused by Tor – compared to direct requests. Future experimental setups should include a long-term analysis as well as an examination of different user locations, e.g., on different continents. Changing the Internet connection speed from a private DSL connection to a corporate or University Internet connection could also provide interesting data for a sensitivity analysis.

We focused on clear-cut technical metrics that can be measured via automated requests. In the real world, the perceived latency of the user depends on various other aspects. Additional studies about influence factors for perceived latency, e.g., cultural issues, the task at hand, or individual user settings of the browser or operating system could provide valuable information about how latency is experienced by users and what countermeasures could be applied, e.g., introducing a loading progress bar for Tor users. In future work, we plan a set of user studies on capturing those further, more individual or subjective aspects of latency acceptance and influence factors for user willingness to tolerate more latency for anonymity. These studies will be evaluated with the help of structural equation models.

CONCLUSION

In this paper, we addressed an important facet of the general topic of "costs" of security and privacy, i.e., the loss of usability in exchange for improved anonymity while browsing the Web via Tor. In particular, we compared the DNS, core and average technical latency for direct as well as Tor-based HTTP requests for the 50 most linked Web sites on the Internet. In terms of the Tor core latency, the median of all requests was five times higher than the median of the direct connection. Furthermore, the results revealed that Tor HTTP requests seem to be less constant, i.e., the actual duration of the Tor HTTP request is hard to anticipate for the user. As far as the DNS requests are concerned, the Tor response was almost 40 times slower than direct DNS requests. The overall latency that a user finally experiences is approximated by the average latency, simulating the download of a complete Web page. Our results indicate that at least 75% of all direct requests are faster than 75% of all Tor request.

Based on the results of our experiments, we provided a mapping that measures the expected increase in average Web user cancelation rate while using Tor. Comparing the average latency between Tor-based and direct requests, there is a difference of 74% in expected cancelation rate. This is a strong indicator for potentially high user frustration when using the Tor anonymization network. We suggest that a usability improvement in terms of reducing latency will significantly increase the adoption of the Tor anonymization network by new users, and thereby increase the anonymity of current users as well.

REFERENCES

1. Aas, G. (2010). libwww-perl, Online: http://search.cpan.org/dist/libwww-perl/.
2. AccountingWEB. (2000). Is Your Web Site Too Big?, Online: http://www.accountingweb.com/item/29331.

3. Amnesty International (2006). Undermining Freedom of Expression in China – The Role of Yahoo!, Microsoft and Google, Online: http://irrepressible.info/static/pdf/FOE-in-china-2006-lores.pdf.
4. Bhatti, N., Bouch, A., and Kuchinsky, A. (2000). Integrating User-perceived Quality into Web Server Design, *Computer Networks (Amsterdam, Netherlands: 1999)* 33, 1–16.
5. Dinev, T. and Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies, *Journal of the Association for Information Systems*, 8, 7, 386–408.
6. Dingledine, R. and Murdoch, S. J. (2009). Performance Improvements on Tor – or, why Tor is Slow and What we're Going to do about it, Online: http://www.torproject.org/press/presskit/2009-03-11-performance.pdf.
7. Fathi, H., Kobara, K., Chakraborty, S. S., Imai, H., and Prasad, R. (2005). On the Impact of Security on Latency in WLAN 802.11b, *Proceedings of the IEEE Global Telecommunications Conference*, 3.
8. Galletta, D.F., Henry, R., McCoy, S. and Polak, P. (2004). Web Site Delays: How Tolerant are Users?, *Journal of the Association for Information Systems* 5, Online: http://aisel.aisnet.org/jais/vol5/iss1/1.
9. Loesing, K., Murdoch, S.J., and Dingledine, R. (2009). A Case Study on Measuring Statistical Data in the Tor Anonymity Network, *Proceedings of the Workshop on Ethics in Computer Security Research (WECSR 2010)*, Online: http://www.cl.cam.ac.uk/~sjm217/papers/wecsr10measuring.pdf.
10. Loesing, K. (2009). Measuring the Tor Network from Public Directory Information*, 2nd Hot Topics in Privacy Enhancing Technologies (HotPETs),* Online: http://www.freehaven.net/~karsten/metrics/measuring-tor-public-dir-info-final.pdf.
11. Lyu, M.R. and Lau, L.K.Y. (2000). Firewall Security: Policies, Testing and Performance Evaluation, *COMPSAC*, 116-121.
12. Mannan, M. and van Oorschot, P. C. (2008). Security and Usability: The Gap in Real-world Online Banking, *Proceedings of the 2007 Workshop on New Security Paradigms*, 1–14.
13. Nah, F. F. (2004). A study on Tolerable Waiting Time: How Long are Web Users Willing to Wait?, *Behaviour & Information Technology,* 23, 3, 153-163.
14. Nielson, J. (1999). “Top Ten Mistakes" Revisited Three Years Later (Alertbox May 1999), Online: http://www.useit.com/alertbox/990502.html.
15. Palme, J. and Berglund, M. (2002). Anonymity on the Internet, Online: http://people.dsv.su.se/~jpalme/society/anonymity.pdf.
16. Privoxy (2010). Privoxy Home Page, Online: http://www.privoxy.org/.
17. Ramsay, J., Barbesi, A., and Preece, J. (1998). A Psychological Investigation of Long Retrieval Times on the World Wide Web, *Interacting with Computers, 10*, 77-86.
18. Rose, G., Khoo, H., and Straub, D. W. (1999). Current Technological Impediments to Business-to-consumer Electronic Commerce, *Communications of the AIS*, 1, 5, 1.
19. Ryan, G. and Valverde, M. (2003). Waiting Online: a Review and Research Agenda, *Internet Research: Electronic Networking Applications and Policy,* 13, 195-205.
20. Selvidge, P. (1999). How Long is Too Long to Wait for a Website to Load?, *Usability News,* 1, 2, Online: http://www.surl.org/usabilitynews/12/time_delay.asp.
21. Stockport, G. J., Kunnath, G., and Sedick, R. (2001). Boo.com – The Path to Failure, *Journal of Interactive Marketing,* 15, 56-70.
22. Tor Project. (2010a). Tor: Anonymity Online, Online: http://www.torproject.org/.
23. Tor Project. (2010b). Tor Metrics Portal, Online: http://metrics.torproject.org/.
24. Vitone, D. (2008). Anonymous Networks, Online: http://blag.cerebralmind.net/wp-content/uploads/2008/05/tor.pdf
25. Wright, T. (2004). Security, Privacy, and Anonymity, *Crossroads,* 11, 2, 5.
26. Zia, T., Zomaya, A., and Ababneh, N. (2007). Evaluation of Overheads in Security Mechanisms in Wireless Sensor Networks, *Proceedings of the 2007 International Conference on Sensor Technologies and Applications*, 181-185.