Enhancing Censorship Resistance in the Tor Anonymity Network

Philipp Winter

Faculty of Health, Science and Technology

Computer Science

LICENTIATE THESIS | Karlstad University Studies | 2014:5

Enhancing Censorship Resistance in the Tor Anonymity Network

Philipp Winter

LICENTIATE THESIS | Karlstad University Studies | 2014:5

Enhancing Censorship Resistance in the Tor Anonymity Network

Philipp Winter

LICENTIATE THESIS

Karlstad University Studies | 2014:5

urn:nbn:se:kau:diva-30752

ISSN 1403-8099

ISBN 978-91-7063-534-2

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2014

WWW.KAU.SE

Enhancing Censorship Resistance in the Tor Anonymity Network

Philipp Winter

Department of Mathematics and Computer Science
Karlstad University

Abstract

The Tor network was originally designed as low-latency anonymity network. However, over time Tor earned a reputation as also being a useful tool to circumvent Internet censorship—at times, the network counted 30,000 users only from China. Censors reacted by tightening their grip on the national communication infrastructure. In particular, they developed different techniques to prevent people from being able to access the Tor network. This arms race now counts several iterations and no end is in sight.

This thesis contributes to a censorship-resistant Tor network in two ways. First, it analyses how existing censorship systems work. In particular, the Great Firewall of China is probed in order to obtain a detailed understanding of its capabilities as well as unexplored circumvention opportunities. Second, this thesis proposes practical countermeasures to circumvent Internet censorship. It discusses a novel network protocol which is resistant to the Great Firewall's active probing attacks.

Some of the concepts and results of this thesis led to the creation of software prototypes. All the code is available under a free license. By developing and deploying software, we are not just limited to a theoretical understanding of censorship systems. Rather, we can gain valuable practical experience in the rapidly progressing arms race that is Internet censorship.

Keywords: Tor, censorship, circumvention, anonymity, network measurement

Acknowledgements

I want to thank my family and in particular my parents for their continuous support over the years. Also, I would like to thank both my supervisors, Stefan Lindskog and Simone Fischer-Hübner, as well as the entire PriSec research group for fruitful discussions.

Finally, I want to thank Internetfonden whose research grant made this work possible.

Karlstad, Sweden, January 8, 2014 Philipp Winter

Contents

List of Appended Papers

I. Philipp Winter and Stefan Lindskog. How the Great Firewall of China is Blocking Tor. In *USENIX FOCI*, 2012.

II. Philipp Winter. Towards a Censorship Analyser for Tor. In *USENIX FOCI*, 2013.

III. Philipp Winter and Tobias Pulls and Juergen Fuss. ScrambleSuit: A Polymorphic Network Protocol to Circumvent Censorship. In *ACM WPES*, 2013.

Comments on my Participation

Paper I This paper was joint work with Stefan Lindskog. The bulk part of the work was done by me. Stefan and I met regularly to discuss results, experimental design, and future steps. Stefan also reviewed several draft versions of this paper. Helpful feedback was given by the people listed in the acknowledgements.

Paper II I am the sole author of this paper. Helpful feedback was given by the people listed in the acknowledgements.

Paper III This paper was joint work with Tobias Pulls and Jürgen Fuß. Parts of the cryptographic scheme was designed together with Tobias and Jürgen provided helpful feedback on mathematical aspects and earlier versions of this paper. The experimental part done by me.

Selection of Other Publications

- Philipp Winter and Tobias Pulls and Juergen Fuss. ScrambleSuit: A Polymorph Network Protocol to Circumvent Censorship. *Technical Report*, Karlstad University (May 2013).
- Philipp Winter and Jedidiah R. Crandall. The Great Firewall of China: How it Blocks Tor and Why it is Hard to Pinpoint. In *USENIX ;login: (6)*, 2012, pp. 42–50.
- Philipp Winter and Stefan Lindskog. How China Is Blocking Tor. *Technical Report*, Karlstad University (March 2012).

Introductory Summary

1 Introduction

In 2012, Reporters Without Borders published a report which identifies twelve "enemies of the Internet" [1]. These twelve enemies are in fact countries; namely Burma, China, Cuba, Iran, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan, and Vietnam. What these countries have in common is their tight grip on national communication infrastructure. The report mentions Bahrain's arrest of bloggers, Iran's launch of its "national Internet" and Uzbekistan's Internet monitoring, just to name a few examples. Furthermore, the report identifies 14 countries under surveillance. This list also contains Australia and France which shows that surveillance is also part of the Western world.

The difference between Internet *censorship* and *surveillance* appears significant from a policy point of view. Censorship, which is frequently conducted by repressive regimes and dictatorships, is typically associated with web sites blocks, arrests and harassment of bloggers, and the deletion of regime-critical content. Surveillance, on the other hand, is often seen as a necessary part of democratic countries. It is typically conducted by intelligence agencies with the goal to thwart criminals and terrorists. From a technical point of view, however, Internet surveillance can quickly turn into censorship: Both rely on special equipment which is deployed in national communication infrastructure. Often, the only difference is merely a set of configuration options. Surveillance equipment can be turned into censorship equipment within a matter of minutes. Furthermore, Reporters Without Borders' report identified two countries which made the unfortunate step from a surveillance to a censorship country: Bahrain and Belarus.

Censorship comes in many shapes. It can range from the widespread arrest of political opponents to subtle self-censorship typically done by individuals out of fear. Ultimately, Internet censorship is merely a symptom of severe social and political problems and technology alone is unlikely to solve them. Technology can, however, be a useful tool towards solving these problems. The technological aspect of censorship is the content of this thesis. In particular, this thesis discusses censorship of the *Tor network*.

The Tor anonymity network was designed to thwart many forms of Internet surveillance and censorship [2]. It was originally designed as low-latency anonymity network and as of November 2013, it consists of almost 5,000 volunteer-run Tor relays. In a nutshell, Tor clients first download the *network consensus* from *directory authorities* which is a signed list of all relays which together form the network. After clients obtained the consensus, they can now create *circuits* which are essentially virtual tunnels—consisting of three relays—through the Tor network. An example of a circuit is given in Figure 1.

Tor provides protection against a local adversary such as a user's ISP. A malicious ISP is unable to read a user's transmitted data and cannot tell with whom the user is communicating with. The network further provides anonymity towards communication destinations. A malicious web site should be unable to determine where a Tor user is located on the Inter-

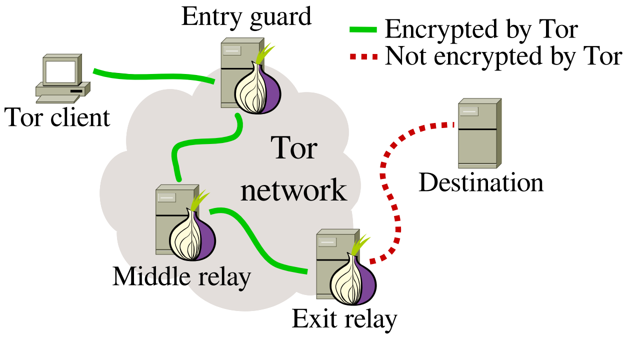


Figure 1: The schematic structure of the Tor network. A client established a three-hop circuit and connects to a destination. All traffic up to the exit relay is encrypted by the Tor protocol. After the exit relay, the user is responsible for encrypted traffic, e.g., by using HTTPS.

net. Given its nature as low-latency anonymity network, Tor cannot protect against a global adversary engaging in traffic analysis [3].

While Tor was originally designed as a pure anonymity tool, an ever increasing set of people began using it to circumvent censorship systems. Censors reacted by blacklisting the small and static set of directory authorities which comprise an ideal choke point for censors. This development led to the creation of *bridges* which are essentially non-public Tor relays. The idea is to give bridges to censored users while trying to keep them secret from censors. In practice, this difficult balancing problem is tackled by making it easy for an individual to obtain a small set of bridges but hard to obtain a large set. Paper I and III discuss censorship-resistance of bridges whereas Paper II proposes a censorship analyser for the Tor network.

This thesis is organised as follows. Section 2 begins by giving an overview of related work. The research questions of this thesis are then asked in Section 3. The research methods which were employed by the appended papers are discussed in Section 4. The contributions are listed in Section 5 and a summary of all appended papers is provided in Section 6. Finally, this thesis is concluded in Section 7.

2 Related Work

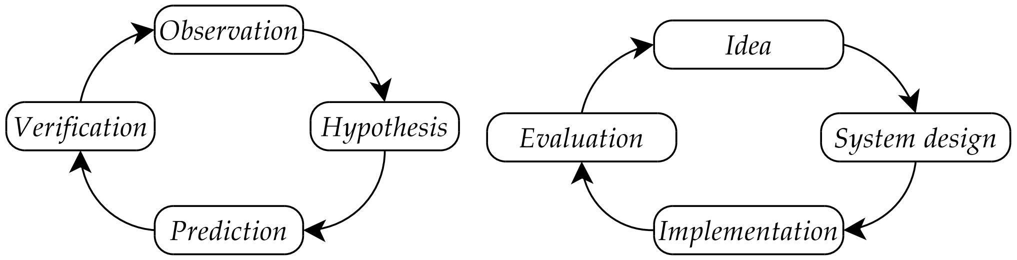
It is convenient to divide related work into censorship *analysis* and *circumvention*. A large variety of censorship-resistant schemes were proposed over the past year. We only discuss low-latency circumvention schemes. Several schemes were proposed to disguise network traffic, e.g., as VoIP [4, 5], email [6, 7], or HTTP [8]. Other systems rely on ordinary web users as proxies [9] or can disguise packet payload as dictated by a well-chosen set of regular expressions [10]. While it is not hard to design systems which can evade a censor's filter at one point in time, it is difficult for systems to be a major obstacle to censors. Accordingly, recent research demonstrated that most traffic obfuscation systems fail in various ways. For example, one class of circumvention systems *mimics* widespread innocuous protocols such as VoIP. This approach was shown to be problematic as it is very difficult to perfectly mimic a given target protocol [11]. Furthermore, a censor is sometimes able to prevent protocol tunneling by breaking the tunneled protocol while leaving the cover protocol mostly intact [12]. Paper III proposes a censorship-resistant protocol which differs from previous work in its ability to change its "protocol shape". Furthermore, it is optimised for throughput rather than for obfuscation.

Another design category requires cooperating backbone routers [13, 14, 15]. The basic idea is that censored users embed a steganographic tag in their network traffic which signals to cooperating backbone routers that they should hijack the client's TCP stream and reroute it to the actual and hidden destination. The rerouting happens after the packets left the censor's network which should make the design undetectable. Later, it was shown that censors are often able to "route around" these decoy routers as they can control their own routing decisions [16].

Compared to circumvention, the field of censorship analysis has received less attention. This is mostly due to the difficulty of probing censorship systems while not being inside the censoring regime. Some systems such as the Great Firewall of China (GFW) operate symmetrically, i.e., censoring ingress as well as egress traffic. This convenient property was exploited in one of the earliest contributions to censorship analysis [17]. This paper was followed by numerous others which investigated how the GFW conducts DNS poisoning [18, 19], how it is structured [20, 21, 22] and how it can be monitored [23]. Paper I expands our knowledge about the GFW by determining how it blocks the Tor network.

Recently, the research community began to focus on other countries. This can be surprisingly difficult as other country-wide censorship systems do not always operate symmetrically which means that access to machines within the country must be obtained first. Aside from China, Iran was subject to recent research efforts which provided an overview [24, 25], analysed traffic throttling as a means of censorship [26], and discussed Iran's infamous Hidden Internet [27]. Further research investigated Internet censorship in Pakistan [28]. Independent of the censoring country, other work investigates side channels in TCP implementations which can be used to detect intentional drops on the Internet [29].

While most censorship analysis work focuses on the address and transport layer, recent work began investigating network services, e.g., how censors interfere with services such as Weibo [30], or Twitter [31]. Finally, concepts to continuously monitor censorship over time were proposed [32, 33]. In Paper II, we propose a similar concept adapted to the Tor network.



(a) The scientific method.

(b) System design experimentation.

Figure 2: A comparison between the scientific method in Figure 2(a) and experimentation in system design in Figure 2(b) (cf. [34]).

3 Research Questions

This thesis provides answers for the following three research questions.

1. *How do real-world censorship systems work?*

   An answer to this question is given in Paper I. It provides an analysis of a nation-scale censorship system, namely the Great Firewall of China. While the GFW is just one system among many, it is commonly regarded as one of the most sophisticated censorship systems and knowledge about one system can frequently be transferred to other systems as well.

2. *How can censorship analysis be "crowdsourced"?*

   Paper II proposes a framework which can assist in analysing censorship systems. It differs from previously proposed systems in that it relies on volunteering users inside the censoring regime. This approach creates new technical challenges which are also addressed in the paper.

3. *How can network protocols be polymorphic and active probing-resistant?*

   A novel censorship-resistant network protocol is proposed in Paper III. It was motivated by the results obtained in Paper I and discusses the design, implementation, and evaluation of a protocol which seeks to disguise Tor traffic from censors.

4 Research Method

Computer science is often divided into the sub-fields *systems* and *theory*. This thesis is part of the systems branch. In particular, the main research methods which were used in this thesis are the *scientific method* and *system design experimentation*.

The scientific method is illustrated in Figure 2(a). It has its origins in the natural sciences and consists of four basic steps even though the details frequently vary. First, *1)* observations about the real world are gathered. Based on these observations, *2)* a hypothesis is formed which should explain the observed phenomena. In the next step, *3)* the hypothesis is used to predict new observations. Finally, *4)* these predictions are verified. If they turn out to be accurate, step 3 is repeated. If not, step 2 is repeated. The scientific method was used in Paper I as it discusses real-world measurements.

In contrast to the natural sciences, the systems branch of computer science also seeks to propose novel systems rather than just measuring and reasoning about them. A popular research method for that is system design experimentation which is illustrated in Figure 2(b). Conceptually, it is similar to the scientific method. First, *1)* a novel system typically starts with an idea. Based on this idea, *2)* a system is designed. In the next step, *3)* the theoretical design leads to a concrete implementation. Finally, *4)* the implementation is evaluated. System design experimentation was used in Paper II and III as these papers propose novel systems.

In the scientific method, an important criteria of the hypothesis is *falsifiability*. It must be possible for a hypothesis to be proven wrong, e.g., by observing real-world examples which are in contrast to the hypothesis' predictions. Accordingly, the experimentation method's system design must be falsifiable as well. Often, a system design aims to supersede a previously proposed system, e.g., by performing better or by providing stronger security properties. As a result, the evaluation has to determine whether the new system design can really provide what it claims. Consequently, falsifiability in the experimentation method means that it must be possible to design experiments to reject a system design.

5 Contributions

This thesis provides the following five contributions.

1. *An understanding of how the Great Firewall of China is blocking the Tor network.*

   Paper I discusses a variety of networking experiments which were designed to shed light on how the Great Firewall of China operates. The experiments made heavy use of decoy Tor connections which originated from a machine in China which was under our control. By doing so, we could attract the GFW's scanners and gather data which was then analysed in detail.

2. *A lightweight circumvention tool to evade the Great Firewall of China.*

   Paper I proposes a lightweight tool which enables server-side evasion of the GFW's fingerprinting. The tool rewrites a server's TCP window size and can be run by bridge operators to prevent active probing attacks.

3. *A design for a lightweight censorship analyser for Tor.*

   Paper II proposes a design for a lightweight censorship analyser for the Tor network. The analyser is meant to assist the Tor developers in debugging censorship incidents. The main contribution is that the analyser is "crowdsourced", meaning that it is supposed to be run by ordinary computer users.

4. *The design and implementation of a blocking-resistant transport protocol.*

   Paper III discusses the design and implementation of a blocking-resistant transport protocol. The protocol proposes two active probing-resistant authentication mechanisms and techniques to change the transported protocol's flow signature. Finally, the paper contains an initial evaluation of the protocol.

5. *Software prototypes.*

   Paper I and III discuss software prototypes for server-side circumvention as well as a prototype of ScrambleSuit, the blocking-resistant transport protocol. All the code is available under a free license at: http://www.cs.kau.se/philwint/.

6 Summary of Appended Papers

This section summarises the three papers which are appended to this thesis.

Paper I – How the Great Firewall of China is Blocking Tor

This paper investigates how the Great Firewall of China is blocking the Tor anonymity network. In particular, experimental data of Chinese network scanners were gathered over a period of several weeks. The data was analysed and additional network experiments were designed and conducted to hypothesise how the block functions.

Paper II – Towards a Censorship Analyser for Tor

This paper discusses the design of a lightweight censorship analyser for the Tor anonymity network. The paper considers both, usability as well as technical requirements as the analyser is meant to be run by non-technical users.

Paper III – ScrambleSuit: A Polymorphic Network Protocol to Circumvent Censorship

This paper introduces a network protocol—ScrambleSuit—which should provide censorship resistance for protocols such as Tor. In particular, ScrambleSuit should provide protection against active probing attacks as well as simple attempts of traffic analysis. Finally, the proposed protocol is evaluated using a prototype.

7 Conclusions and Future Work

There is a strong need for technology which enables the free retrieval of information and the Tor network is one of these tools. This thesis discussed two aspects of Tor's resistance to censorship. First of all, it investigated and proposed censorship *analysis* techniques. Sound analysis techniques are crucial since circumvention technology relies on it. Secondly, this thesis investigated censorship *circumvention* technology which was motivated by our own censorship analysis findings. This thesis proposes several theoretical techniques as well as practical tools that give a better understanding of how real censors block Tor and how these very blocks can be circumvented.

There is lots of space for future work. Several censorship-resistant protocols were proposed in recent years [35]. These protocols are composed of components which are quite useful for other protocols as well. While the Tor project's pluggable transport system clearly decouples anonymity from censorship resistance, there is no decoupling *within* censorship resistance components. As a result, future work could further modularise these protocols which should enable faster prototyping and composition. Furthermore, there is no structured approach to evaluating the *quality* of censorship-resistant protocols. To date, evaluations are based on vague assumptions about censor's capabilities. Future work should investigate frameworks to evaluate and quantify the censorship-resistance of protocols.

References

[1] Reporters Without Borders. *Internet Enemies*. 2012. URL: http://march12.rsf.org/en/.

[2] Roger Dingledine, Nick Mathewson, and Paul Syverson. "Tor: The Second-Generation Onion Router". In: *USENIX Security*. USENIX Association, 2004. URL: http://static.usenix.org/event/sec04/tech/full_papers/dingledine/dingledine.pdf.

[3] Steven J. Murdoch and George Danezis. "Low-Cost Traffic Analysis of Tor". In: *Security & Privacy*. IEEE, 2005. URL: http://www.cl.cam.ac.uk/users/sjm217/papers/oakland05torta.pdf.

[4] Amir Houmansadr et al. "I want my voice to be heard: IP over Voice-over-IP for unobservable censorship circumvention". In: *NDSS*. The Internet Society, 2013. URL: http://www.cs.utexas.edu/~amir/papers/FreeWave.pdf.

[5] Hooman Mohajeri Moghaddam et al. "SkypeMorph: Protocol Obfuscation for Tor Bridges". In: *CCS*. ACM, 2012. URL: http://www.cypherpunks.ca/~iang/pubs/skypemorph-ccs.pdf.

[6] Wenxuan Zhou et al. "SWEET: Serving the Web by Exploiting Email Tunnels". In: *HotPETS*. Springer, 2013. URL: http://petsymposium.org/2013/papers/zhou-censorship.pdf.

[7] Qiyan Wang et al. "CensorSpoofer: Asymmetric Communication using IP Spoofing for Censorship-Resistant Web Browsing". In: *CCS*. ACM, 2012. URL: http://hatswitch.org/~nikita/papers/censorspoofer.pdf.

[8] Zachary Weinberg et al. "StegoTorus: A Camouflage Proxy for the Tor Anonymity System". In: *CCS*. ACM, 2012. URL: http://www.owlfolio.org/media/2010/05/stegotorus.pdf.

[9] David Fifield et al. "Evading Censorship with Browser-Based Proxies". In: *PETS*. Springer, 2012, pp. 239–258. URL: http://crypto.stanford.edu/flashproxy/flashproxy.pdf.

[10] Kevin P. Dyer et al. "Protocol Misidentification Made Easy with Format-Transforming Encryption". In: *CCS*. ACM, 2013. URL: http://eprint.iacr.org/2012/494.pdf.

[11] Amir Houmansadr, Chad Brubaker, and Vitaly Shmatikov. “The Parrot is Dead: Observing Unobservable Network Communications”. In: *Security & Privacy*. IEEE, 2013. URL: http://www.cs.utexas.edu/~amir/papers/parrot.pdf.

[12] John Geddes, Max Schuchard, and Nicholas Hopper. “Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention”. In: *CCS*. ACM, 2013. URL: http://www-users.cs.umn.edu/~hopper/ccs13-cya.pdf.

[13] Amir Houmansadr et al. “Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability”. In: *CCS*. ACM, 2011, pp. 187–200. URL: http://hatswitch.org/~nikita/papers/cirripede-ccs11.pdf.

[14] Eric Wustrow et al. “Telex: Anticensorship in the Network Infrastructure”. In: *USENIX Security*. USENIX Association, 2011. URL: http://www.usenix.org/event/sec11/tech/full_papers/Wustrow.pdf.

[15] Josh Karlin et al. “Decoy Routing: Toward Unblockable Internet Communication”. In: *FOCI*. USENIX Association, 2011. URL: http://static.usenix.org/event/foci11/tech/final_files/Karlin.pdf.

[16] Christopher Thompson Max Schuchard John Geddes and Nicholas Hopper. “Routing Around Decoys”. In: *CCS*. ACM, 2012. URL: http://www-users.cs.umn.edu/~hopper/decoy-ccs12.pdf.

[17] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. “Ignoring the Great Firewall of China”. In: *PETS*. Springer, 2006. URL: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf.

[18] Sparks et al. “The Collateral Damage of Internet Censorship by DNS Injection”. In: *SIGCOMM Computer Communication Review* 42.3 (), pp. 21–27. URL: http://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf.

[19] Graham Lowe, Patrick Winters, and Michael L. Marcus. *The Great DNS Wall of China*. Tech. rep. New York University, 2007. URL: http://cs.nyu.edu/~pcw216/work/nds/final.pdf.

[20] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. “Internet Censorship in China: Where Does the Filtering Occur?” In: *PAM*. Springer, 2011, pp. 133–142. URL: http://www.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf.

[21] Jong Chun Park and Jedidiah R. Crandall. “Empirical Study of a National-Scale Distributed Intrusion Detection System: Backbone-Level Filtering of HTML Responses in China”. In: *Distributed Computing Systems*. IEEE, 2010, pp. 315–326. URL: http://www.cs.unm.edu/~crandall/icdcs2010.pdf.

[22] Sheharbano Khattak et al. “Towards Illuminating a Censorship Monitor’s Model to Facilitate Evasion”. In: *FOCI*. USENIX Association, 2013. URL: https://www.usenix.org/system/files/tech-schedule/foci13-papers-archive.zip.

[23] Jedidiah R. Crandall et al. “ConceptDoppler: A Weather Tracker for Internet Censorship”. In: *CCS*. ACM, 2007, pp. 352–365. URL: http://www.csd.uoc.gr/~hy558/papers/conceptdoppler.pdf.

[24] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. “Internet Censorship in Iran: A First Look”. In: *FOCI*. USENIX Association, 2013. URL: https://www.usenix.org/system/files/tech-schedule/foci13-papers-archive.zip.

[25] John-Paul Verkamp and Minaxi Gupta. “Inferring Mechanics of Web Censorship Around the World”. In: *FOCI*. USENIX Association, 2012. URL: https://www.usenix.org/system/files/conference/foci12/foci12-final1.pdf.

[26] Collin Anderson. *Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran*. Tech. rep. 2013. URL: http://arxiv.org/abs/1306.4361.

[27] Collin Anderson. *The Hidden Internet of Iran: Private Address Allocations on a National Network*. Tech. rep. 2012. URL: http://arxiv.org/pdf/1209.6398v1.

[28] Zubair Nabi. “The Anatomy of Web Censorship in Pakistan”. In: *FOCI*. USENIX Association, 2013. URL: https://www.usenix.org/system/files/tech-schedule/foci13-papers-archive.zip.

[29] Roya Ensafi et al. “Detecting Intentional Packet Drops on the Internet via TCP/IP Side Channels”. In: *PAM*. Springer, 2014.

[30] Tao Zhu et al. “The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions”. In: *USENIX Security*. USENIX Association, 2013. URL: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_zhu.pdf.

[31] John-Paul Verkamp and Minaxi Gupta. “Five Incidents, One Theme: Twitter Spam as a Weapon to Drown Voices of Protest”. In: *FOCI*. USENIX Association, 2013. URL: https://www.usenix.org/system/files/tech-schedule/foci13-papers-archive.zip.

[32] Arturo Filastò and Jacob Appelbaum. “OONI: Open Observatory of Network Interference”. In: *FOCI*. USENIX Association, 2012. URL: https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf.

[33] Andreas Sfakianakis, Elias Athanasopoulos, and Sotiris Ioannidis. "CensMon: A Web Censorship Monitor". In: *FOCI*. USENIX Association, 2011. URL: http://static.usenix.org/event/foci11/tech/final_files/Sfakianakis.pdf.

[34] Dror G. Feitelson. *Experimental Computer Science: The Need for a Cultural Change*. Tech. rep. The Hebrew University of Jerusalem, 2006. URL: http://www.cs.huji.ac.il/~feit/papers/exp05.pdf.

[35] Philipp Winter. *Selected Papers in Censorship*. URL: http://veri.nymity.ch/censorbib/.

Enhancing Censorship Resistance in the Tor Anonymity Network

The Tor network was originally designed as low-latency anonymity network. However, as the years progressed, Tor earned a reputation as also being a useful tool to circumvent Internet censorship. At times, the network counted 30,000 users only from China. Censors reacted by tightening their grip on the national communication infrastructure. In particular, they developed techniques to prevent people from being able to access the Tor network. This arms race now counts several iterations and no end is in sight.

This thesis contributes to a censorship-resistant Tor network in two ways. First, it analyses how existing censorship systems work. In particular, the Great Firewall of China is analysed in order to obtain an understanding of its capabilities as well as to explore circumvention opportunities. Second, this thesis proposes practical countermeasures to circumvent Internet censorship. In particular, it presents a novel network protocol which is resistant to the Great Firewall's active probing attacks.

urn:nbn:se:kau:diva-30752

ISBN 978-91-7063-534-2

ISSN 1403-8099

LICENTIATE THESIS | Karlstad University Studies | 2014:5