Title: TWC: Option: Small: Collaborative: New Encryption Paradigms to Circumvent Internet Censorship

Principal Investigator: Thomas Shrimpton (Portland State University)
Principal Investigator: Thomas Ristenpart (University of Wisconsin)

---

1 Transitions Supplement

In a world of increasing Internet censorship by nation-states, the academic community can play a role in safeguarding free and open access to information. This supplement lays out a plan for how we intend to transition the proposed research from the lab to everyday users targeted by censorship. This will require overcoming a broad assortment of challenges, ranging from engineering, integration, and testing to engagement with the activist communities. The result of overcoming them will be circumvention tools that can resist attempts to use deep-packet-inspection (DPI) to block them.

Background: a censorship arms race. There exists a broad assortment of in-use censorship circumvention tools. We will concretely focus on Tor [6], a mature, actively supported circumvention tool and with whose maintainers we already have active dialog. Currently, over half a million users across the world every day access the Internet via Tor. It has, in particular, played a vital role in allowing dissidents living under censoring governments such as Iran [3, 5, 9, 11], China [1, 4, 8, 10, 15, 16] and Syria [12] to obtain access to Internet resources (without lessened fear of reprisal).

But Tor is locked in an arms race with censors. Figure 1 shows the results of the use of DPI by Iran against the Tor protocol. The DPI system targeted, in this case, Tor's use of TLS certificates with long expiration dates [5]. Almost all "normal" web sites using TLS have certificates with short expirations, and so this provided an easy DPI-based distinguisher. The Tor maintainers released a patch that ameliorated the problem, but updates to Tor proxies took some time. Ethiopia, China, and Kazakhstan have likewise used DPI to selectively attempt to block Tor. As in the case of Iran, Tor reacts to these attacks via ad-hoc changes to the protocol [5]. More recently, they have introduced pluggable transports [2], which are encoding/decoding mechanisms, sitting below the encryption algorithms of Tor, that seek to more robustly obfuscate traffic from DPI. A limited set of pluggable transports currently exist [13, 14], and their security has yet to be thoroughly analyzed.

The transition plan. Our proposed research will produce a set of new encryption technologies that can, in theory, help Tor and other circumvention tools evade DPI-based detection. We will seek to make practical this theory. As mentioned, we will target our transition on the Tor system, but expect that the lessons learned will be readily transferable to other circumvention tools and applied cryptography at large. We will:

- Implement an optimized cryptographic library for FTE and DME
- Build new pluggable transports that use the library
- Perform extensive security analyses of the modified Tor tool
- Work with the Tor project to deploy these new tools
- Educate and engage students and the broader public about censorship and circumvention

Together these activities tackle the problem of technology transfer across multiple fronts, including, perhaps most importantly, outreach activities aimed at improving awareness of censorship issues and fostering support for deployment of circumvention tools. We view this as critical to a successful transition.

We discuss the proposed transition activities along four broad areas: engineering and integration, security analysis, system dissemination, and education and public engagement.

Engineering and integration. This theme will involve two tasks. First will be optimized implementations of the secure FTE and DME schemes produced by our main proposal. We will hire senior undergraduate to work, with supervision by the graduate students and PIs, on development of this optimized code. This will require combination of existing optimized cryptographic implementations (e.g., openssl cryptographic

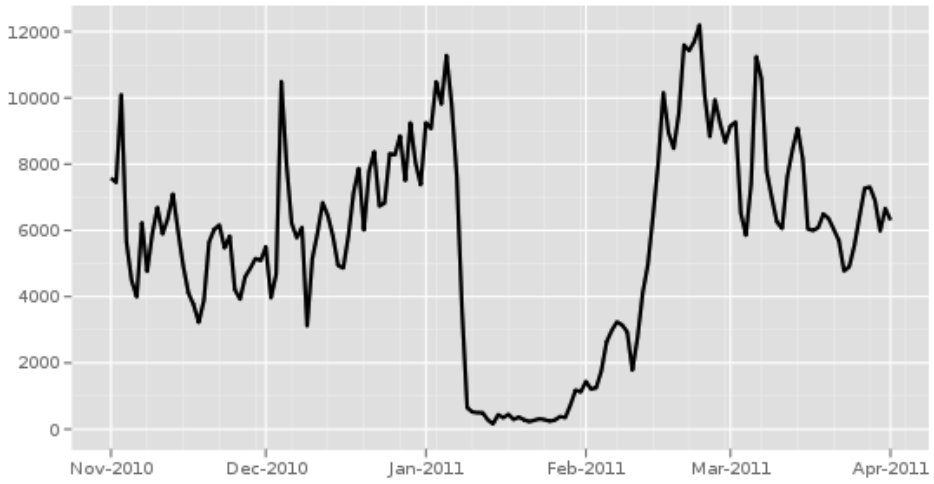

Figure 1: Approximate number of daily Tor users in Iran, starting from November 2010 through April 2011. In January, Iran deployed DPI-based detection of Tor. Source: `http://metrics.torproject.org`

routines) with our new algorithms for ranking and unranking (FTE) and rejection-sampling-type mechanisms (DME). The result will be a fast C library that exposes simple interfaces for use of FTE and DME and which can be of use in a broad variety of contexts.

The integration task will proceed along two lines. The first is building a new pluggable transport using the FTE/DME library. Beyond development to provide suitable wrappers that enable FTE/DME usage within a pluggable transport module, this will likely require tweaking the underlying FTE/DME implementations to ensure high performance for the network dynamics of Tor connections. For this we will, initially use a shared secret key and then will implement a lightweight key-transport mechanism similar to the one used by [14]. The public-key used will be the proxy's.

Initial results on a very preliminary prototype that uses FTE suggests that performance can be obtained, with as little as 5% overhead compared to a conventional encryption layer.

We will follow standard best practices in this work, including unit tests and producing well-documented code. These systems will be open-sourced and made publicly available. We suspect that the code will find use in many further contexts beyond Tor.

Analyzing security. In addition to using industry best practices for secure code development, including code reviews, application of commercial vulnerability auditing tools, and unit testing, we will additionally analyze the security of our systems via red teaming exercises. These will take two forms. First, the PIs will include in their classes a project that will seek ad-hoc student involvement in penetration testing. This will not be mandatory in classes, but rather one of several choices of projects and/or provide a route to improve grades by way of a "bug bounty" extra credit program. (For each bug found, the student will receive some number of extra credit points towards the class.)

Second, we will have officially organized red teaming with one or more hired undergraduates. Suitable undergraduates will be identified by way of the class projects or in other manners. PI Ristenpart has, particularly, already had success in enlisting bright undergraduates to help find attacks in commercial-grade systems [7]. The scope here will not just be our pluggable transport, but the entire Tor protocol and implementation. The goal will be to suss out vulnerabilities in both implementation as well as in design. Discovered problems will be fixed in our code directly, or disclosed privately to the appropriate Tor maintainer(s).

Dissemination. As mentioned, we will open-source and make public the software resulting from this project. To ensure deployability, however, we will develop further our relationship with the Tor project

and its maintainers, and in particular work with them to integrate our technologies as suitable into the Tor system. This will involve any necessary tweaking of our designs to match their deployment requirements, responding to feature requests by Tor project members, responding to bug fixes, and, critically, evaluating the usability of the system.

Education and public engagement. We feel that deployment of circumvention technologies, including our new research, can only be successful given societal support or the endeavor. As such, we view that successfully transitioning our technologies requires a campaign of education and public engagement. PI Ristenpart has already initiated this on several fronts. First, he targets a broad audience on campus for educational activities. In particular, arranging at least yearly lecture swaps with Prof. Alan Rubel (philosopher and JD) of the School of Library and Information Studies (SLIS). Ristenpart gives a lecture on the technical aspects of Internet surveillance and censorship (at an appropriate level of depth) in Rubel's SLIS class, while Rubel gives a lecture on legal issues related to censorship in Ristenpart's security class. Students from a diverse background are educated and engaged on the censorship issue.

Ristenpart, together with Prof. Alan Rubel and Prof. Kristin Eschenfelder (also in SLIS), has also recently been awarded a Holtz Center for Science & Technology Studies Outreach Fellowship to invite speakers that can engage the general Madison public on the topic of computer networks, surveillance, and the state. Roger Dingledine, president and founder of the Tor project, has graciously agreed to give a lecture at University of Wisconsin. We will use this opportunity to educate the public at large about the issues of censorship and circumvention, and to excite students about the opportunities to play a role in helping ensure a free and open Internet.

PI Shrimpton has likewise promoted educational and engagement activities, including discussion of the topic in his classes and hosting at Portland State visitors from the Tor project, including Roger Dingledine, for discussion of circumvention technical challenges.

If funded, a portion of the transitions money will go to support travel by students and PIs. This will facilitate engagement with the Tor community, for example by joining in their "hack fests" (meetings to provide rapid development of Tor features) and giving talks about our technologies. It will also be used to travel to universities, companies, and other organizations to give talks about the transitional work in order to increase visibility and public awareness.

Timeline and milestones. We will organize the transitions work according to the timeline shown in Figure 2. Note that this aims to complement development of the basic science research schedule in the main proposal. The first activity will be to gather requirements from the Tor project team. This will include feedback on both performance and other usability requirements, as well as other implementation matters such as preferred coding styles, language tools, and project team best practices. We will then design the architecture for our FTE/DME library, taking into account said requirements. This design process will be relatively independent of the research activities, as the library API should, inline with the principle of modularity, not rely on the details of the underlying implementations. Implementation will then begin in the next year, and continue throughout the project on a rolling basis. We will ensure that early research results are implemented early, so as to leave plenty of time in the final year for testing, security analysis, and deployment activities. New results will get folded into the codebase as they arise. In the final year a large focus will be on security analysis and polishing the codebase for production use in the Tor network. We will split the red teaming into two sessions, each a semester long. This will allow us to line up red teaming activities with class projects and, students engaged via exposure in class in the first semester, can be hired part time to followup with deeper analysis in the next semester. Documentation and outreach activities will be ongoing throughout the entire project lifetime.

Budget and personnel. A breakdown of the requested transitions budget appears in Figure 3. The budget will support student funding at two levels. One will be a years worth of graduate student funding. This funding will not be for a continues year, but rather to fund the student for months at a time that will be interwoven throughout the three years. This reflects the tight integration between the graduate student's research and transitions work. At Wisconsin, we plan to hire at least two undergraduates full time for the second summer 2015 to particularly aid in the pluggable transport module development and any remaining library development. We will also hire undergraduate students part time during the school year for red teaming activities. At Portland, we will hire an undergraduate for the first summer in order to help with

Activity	Timeline
Gather requirements	June 2013 – June 2014
Library architecture	May 2014 – August 2014
Library implementation	August 2014 – May 2015
Pluggable transport module	May 2015 – October 2015
Performance testing	October 2015 – December 2015
Red teaming part 1	September 2015 – December 2015
Red teaming part 2	February 2016 – June 2016
Documentation	Ongoing
Outreach activities	Ongoing

Figure 2: Timeline for project activities.

Budget Item	Approximate cost	Activities supported
Wisconsin GRA	$70,753	Cumulative year of grad student support
Wisconsin Undergraduates	$20,000	Support for hourly undergraduate researchers
PSU Undergraduates	$20,000	Support for hourly undergraduate researchers
Travel	$15,000	Travel to support outreach, education efforts
Experimental equipment	$20,000	Computing equipment to support testing
Total	$145,753	

Figure 3: Approximate transitions budget, including approximated overheads

sorting through the requirements and to gather necessary tools, and development environments. We will also hire an undergraduate at Portland during the second summer to help with setting up an environment for red teaming. This lab setup will consist of several Tor nodes running our system, setup on an an internal LAN. This testbed will initially be unavailable to the Internet but, as the code matures, it will be used to host public Tor nodes. The equipment budget reflects the necessary specialized computing equipment, including 5 servers, a network switch, and packet capture mechanisms. We will setup one of the servers as a proxy for a DPI system, and the others as Tor nodes and/or systems for use by the red teams. Finally, we have budgeted $15,000 dollars to support significant travel activities. Due to the nature of this project, we intend for undergraduates, graduate students, and the PIs all to travel several times over the three years to universities, workshops/conferences, and to Tor "hack fests", some of these are abroad.

References

[1] Anonymous. Torproject.org blocked by gfw in china: Sooner or later? Available at: `https://blog.torproject.org/blog/torprojectorg-blocked-gfw-china-sooner-or-later`, June 2008. 1

[2] Jacob Appelbaum and Nick Mathewson. Pluggable transports for circumvention. Available at: `https://gitweb.torproject.org/torspec.git/HEAD:/proposals/180-pluggable-transport.txt`, 2010. 1

[3] Jon Brodkin. Iran reportedly blocking encrypted internet traffic. Available at: `http://arstechnica.com/tech-policy/2012/02/iran-reportedly-blocking-encrypted-internet-traffic/`, 2012. 1

[4] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. Ignoring the great firewall of china. In *in G. Danezis & P. Golle, eds, Privacy Enhancing Technologies workshop (PET 2006), LNCS*. Springer-Verlag, 2006. 1

[5] Roger Dingledine. Iran blocks Tor; Tor releases same-day fix. Available at: `https://blog.torproject.org/blog/iran-blocks-tor-tor-releases- same-day-fix`, 2011. 1

[6] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *In Proceedings of the 13th USENIX Security Symposium*, pages 303–320, 2004. 1

[7] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail. In *Oakland' 12: Proceedings of the 33nd IEEE Symposium on Security and Privacy*, Oakland, CA, 05/2012 In Press. IEEE. 2

[8] Andrew Lewman. China block Tor: Round Two. Available at: `https://blog.torproject.org/blog/china-blocking-tor-round-two`, 2010. 1

[9] Andrew Lewman. Update on Internet Censorship in Iran. Available at: `https://blog.torproject.org/blog/update-internet-censorship-iran`, 2011. 1

[10] Jack McCarthy. China bans skype. Available at: `http://www.infoworld.com/t/business/china-bans-skype-911`, 2005. 1

[11] Phobos. Iran partially blocks encrypted network traffic. Available at: `https://blog.torproject.org/blog/iran-partially-blocks-encrypted- network-traffic`, 2012. 1

[12] Tor Metrics Portal. Usage of tor in syria. Available at: `https://metrics.torproject.org/`, 2012. 1

[13] Tor obfsproxy. Available at: `https://gitweb.torproject.org/obfsproxy.git`, 2012. 1

[14] Zachary Weinberg, Jeffrey Wang, Vinod Yegneswaran, Linda Briesemeister, Steven Cheung, Frank Wang, and Dan Boneh. Stegotorus: a camouflage proxy for the tor anonymity system. In *ACM Conference on Computer and Communications Security*, pages 109–120, 2012. 1, 2

[15] Tim Wilde. Knock Knock Knockin' on Bridges' Doors. Available at: `https://blog.torproject.org/blog/knock-knock-knockin-bridges-doors`, 2012. 1

[16] Philipp Winter and Stefan Lindskog. How the Great Firewall of China is Blocking Tor. In *Free and Open Communications on the Internet*, Bellevue, WA, USA, 2012. USENIX Association. 1