Tor's critique of Ultrasurf: A reply from the Ultrasurf developers

April 16, 2012

Ultrareach would like to thank Jacob Appelbaum and the Tor Project for its work on exploring Ultrasurf. We have attempted to constructively work with them for the last four months, with the ultimate goal of serving our users. However, the Tor project and Jacob Appelbaum published a report today a that amounts to an attack article on the Ultrasurf Internet Freedom product, entitled "Technical Analysis of the Ultrasurf Proxying Software." This is our response.

The Tor paper makes multiple a series of critical assessments about Ultrasurf, but a closer reading reveals:

- Tor has not been able to break Ultrasurf the paper asserts that it is possible to monitor the content of Ultrasurf sessions, but they have not been able to actually demonstrate this.
- Tor has not been able to identify any party who is able to monitor the content of Ultrasurf sessions.
- Tor has only partly understood our security structure, and has failed to break the core mechanisms for protection
- Tor repeatedly and knowingly makes false statements about Ultrasurf.
- In each case where Tor has previously identified a security shortcoming in Ultrasurf, we have moved rapidly to address it.

Tor and Ultrasurf are both Internet Freedom systems. We both require resources to continue our work, and we sometimes compete for resources from similar funding agencies. We wish that Tor had approached us first so that we could use the information in the Tor paper as part of our continuing effort to improve user security.

Instead, Tor's action in this matter is as follows: Jacob Appelbaum went first to meet with our funding agencies – before contacting us – in an effort to stop funding for our project. Tor used a preliminary draft of its paper in an effort to lobby against us. We were only able to meet with Tor after a third-party intervened and arranged a meeting. Even then, it has proved difficult to get any concrete information from Tor. Despite repeated requests, we did not receive a copy of the Appelbaum paper until 4/6/2012.

Tor and Ultrasurf represent fundamentally different approaches solving the censorship challenge. As a result of these different approaches, Tor simply cannot handle the number of users or scale of activities that Ultrasurf can. The bottom line is that Ultrasurf has been serving millions of people for the past decade in over 180 countries. It has been essential during times of humanitarian crises, allowing millions of people to evade government censorship and surveillance. The Chinese government in particular has spent considerable resources and has purchased high-end equipment from top vendors around the world in an attempt to block software like Ultrasurf, yet it has never successfully

1

blocked us for any extended period of time; neither has there been any evidence of monitoring. The same cannot be said for the Tor system, which has been successfully blocked in China on many occasions for extended periods. To the best of our knowledge, Ultrasurf has not been either monitored or blocked in any country.

At Ultrareach we are committed to constantly improving the privacy and security of our product. Ultrasurf faces a rapidly evolving landscape, as censorship practices employed by the Great Chinese Firewall (and similar censorship/monitoring systems in other countries) changes on a daily – sometimes hourly basis. This presents significant security challenges, since our code base must rapidly change in response. We do appreciate Tor's analysis (if not the way Tor handled it), and have – in most cases, months ago – already fixed the issues pointed out by Tor.

As an example of how we are taking security seriously, we have already retained a thirdparty testing and review service at the recommendation of the U.S. State Department to help us identify and remove security vulnerabilities. This is an active exchange and is resulting in continual improvement of our system.

Below, we respond in several places to some specific charges made by Tor in its paper.

Ultrasurf serves different functions than Tor

There are fundamental differences in the philosophy of Ultrasurf and Tor, and the failure to understand these differences is at the root of most of comments in the Tor paper.

Tor: The architecture of the Ultrasurf network is an example of privacy by policy and the protection it offers is extremely weak.

In fact, Ultrasurf does offer a fair number of privacy protections. But it is not designed primarily as a privacy tool. Rather it is designed to be a scalable, high-performance anticensorship tool that allows users in closed societies access to news, political information, religious information, social networks, and other blocked content.

Tor, in contrast, is designed as a high-privacy tool, but the price that it pays is that it lacks the capacity and scalability features that Ultrasurf offers. We believe that within the Internet Freedom community, there is a need for an array of tools to suit different users and environments, including Ultrasurf, Tor, and other emerging tools. We would rather engage in a constructive dialogue to lift the level of the field instead of firing smear attacks at each other.

Tor: UltraReach is subject to US laws such as National Security Letters [20], subpoena and/or so called 2703d notice [14] data production requests.

Ultrareach's primary focus is to provide access to users in closed societies. We do not feel that complying with US law represents a threat to those users.

Tor, by contrast, has a different design philosophy, and attempts to offer strong protection even against the US government. This is a fundamentally a philosophical difference.

Tor: This means that it is possible to extract a list of all sites that are censored by the Ultrasurf network or otherwise unavailable for other reasons. While we found only artistic sites blocked by this filter, we did not extract the entire censorship list; such extraction is trivial and is left as an exercise to the reader. None of the blocked sites were known to be illegal and while adult content was involved, many legal US based websites and companies were censored seemingly based on their content, rather than their legal standing.

Ultrareach's primary objectives are to support users who need access to news, political information, religious information, social networks, etc. We believe that this is the core function of Internet Freedom software—to advance the free flow of information for the betterment of individuals and societies. We do employ internal filters that block access to a certain types of material. Ultrareach has limited resources; we artificially limit the number of people who can use our software, because we do not have the server capacity to meet the demand. This being the case, we make the decision to block access to pornographic material, illicit websites, and other sites deemed offensive. We think this is the right decision – our primary mission is serving users in repressive countries.

Tor, in contrast, has a different design philosophy, and attempts to offer equal access to all sorts of material. The price that Tor pays is that it lacks the capacity and scalability features that Ultrasurf offers.

Tor has not broken Ultrasurf

In several places, the Tor paper seems to imply that it has broken Ultrasurf, but it has not. Tor has admitted to us that it cannot break Ultrasurf traffic. In fact, Ultrasurf uses multiple methods of protection, and Tor has only analyzed some surface mechanisms.

Tor: We find that it is possible to monitor and block the use of Ultrasurf using commercial off-the-shelf software. In particular, BlueCoat sells software and hardware solutions with such capabilities that have been deployed in Syria and other countries.

This assertion is completely unsupported. BlueCoat is mentioned only once in the Tor paper, in the abstract. Tor provides no evidence that BlueCoat sells software and hardware that can break Ultrasurf. This appears to be merely an attack based speculation. These types of vague, unsupported assertions appear throughout the Tor paper.

Tor: The vulnerabilities presented in this paper are not merely theoretical in nature; they may present life-threatening danger in hostile situations. We recommend against the use of Ultrasurf for anonymity, security, privacy and Internet censorship circumvention.

In fact, the vulnerabilities in the Tor paper are theoretical in nature; Tor has admitted to us that it is unable to break Ultrasurf. The suggestion that Ultrasurf is "life-threatening" is pure hyperbole. The fact is that, over the last decade, millions of people have safely used Ultrasurf to circumvent censorship and surveillance online. The tool has been critical during times of human rights crises, and we are not aware of any time when the security of our users has been compromised.

Moreover, we find Tor's approach to be disingenuous; while they purport to want to protect Ultrasurf users, their chosen approach is to publicly release a detailed and explicit description of perceived vulnerabilities. Were it not for the fact that the security vulnerabilities identified have either already been closed or are superficial, this would be tantamount to providing oppressive governments with a roadmap to monitor our users and acquire their information.

Logging

Tor: The proxy systems collect extensive log [6] entries. [...] UltraReach as a corporation has extremely questionable data retention practices that include full logging of all user activity [6]. [...] The Ultrasurf network as a whole appears to log connection information for all clients in a privacy-invasive manner [6]. This data is enough to individually identify every user who uses Ultrasurf as directed and to do so after they cease to use Ultrasurf. When combined with the active content (Section 6.2) and active tagging (Section 6.3) issues we find the issue of data retention to be extremely concerning.

Tor's assertion that "*the proxy systems collect extensive log entries*" is unsupported. In fact, since we receive over two billion hits a day, it is technically impossible for us to collect extensive log entries, even if we wished to.

However, in response to this criticism, we do plan to fully document our data retention policy on our web site.

Misrepresentations by Tor about data release

Tor: Amongst the most alarming admissions from the Ultrasurf team were that log files are indeed being kept, and that they have been disclosed to the US Government without warrants by Ultrasurf.

Sadly, here Tor simply fabricates an "admission." Since many participants in the Ultrasurf team are often not native English speakers, it is perhaps possible that Jacob Appelbaum misunderstood our English.

We wish to clear up the record. Ultrasurf has never disclosed log files to the US government without a warrant. We are not even capable to maintain full logs, as indicated

above. We do some logging for the purpose of checking the efficacy of our system. Those logs are deleted after a month.

In the vast majority of cases, when we do receive search warrants, we simply do not have the data. We are committed to abiding by US law, so in the very rare cases when we do have information and receive a valid warrant from U.S. law enforcement authorities, we would comply.

We have never disclosed original logs to third parties.

Tor's information does not reflect current versions of Ultrasurf

In its paper, Tor makes a number of allegations based on old versions of Ultrasurf. We have pointed out to Tor that the paper does not reflect current versions of Ultrasurf. Unfortunately, the Tor project did not choose to accurately report information in its paper.

Tor: This paper addresses the following claims [27, 28, 29, 30] by UltraReach and other Ultrasurf advocates about the Ultrasurf client and Ultrasurf network:

1. "Ultrasurf enables users to browse any website freely" — refuted in Section 3.1

2. "employs a decoying mechanism to thwart any tracing effort of its communication with its infrastructure." — refuted in Section 5.13

3. "Protect your privacy online with anonymous surfing and browsing. Ultrasurf hides your IP address, clears browsing history, cookies, and more." — refuted in Section 6.2 and Section 6.3.

4. "change IP addresses a million times an hour" —refuted in Section 6.1

5. "Untraceable" — refuted in Section 6.10

6. "Unblockable: Client uses wide array of discovery mechanisms to find an available proxy server and, when necessary, to switch/hop to avoid tracking/blocking" — refuted in Section 6.8

7. "Invisible: Leaves no traces on the user's computer, and its traffic is indistinguishable from normal access to HTTPS sites"— refuted in Section 5.12 8. "Anonymous: No registration is requires [sic], and no personally identifying information collected" — refuted in Section 6.10

9. "Tamperproof: Using privately-signed SSL certificates which dont depend on external, potentially compromised CAs (thus preempting MITM attacks),

Ultrasurf proactively detects attempts by censors to reverse-engineer, sabotage, or otherwise interfere in the secure operation of the tool" —refuted in Section 5.8.

We conclude that each of these claims is false, incorrect, or misleading. We also conclude that Ultrasurf meets many, if not all, of the commonly accepted Snake–Oil [47] critera.

Here Tor quotes from statements on web pages and documents associated with previous versions of Ultrasurf. In some cases, Ultrasurf did make statements that were too broad. However, months ago we completed an effort to correct all of our text with accurate summaries of the Ultrasurf system. Although we pointed out the new text to the Tor Project, it chose to publish its paper based on old descriptions, and not critique our current version.

Tor: The server appears to log this information [6] in addition to setting an HTTP cookie for the Google Analytics service on the actual block page itself.[...] UltraReach appears to tag their users with third party cookies (Google etc) as well as automatically forcing users to load third party resources. A third party may be subject to the same legal concerns as the UltraReach corporation.

All Google Analytics functionality at Ultrasurf was turned off months ago—a fact that we have pointed out to the Tor project. Unfortunately, the Tor project did not choose to accurately report information in its paper.

Tor: Ultrasurf servers are out of date with regard to commonly used software. Users regularly interface with known exploitable software (Section 6.5) that is multiple years out of date. Publically available security patches are seemingly ignored. UltraReach server compromise would be a complete break of all of the security properties offered by the Ultrasurf network with the currently deployed architecture. Ultrasurf server compromise would likely allow an attacker to completely compromise specifically targeted clients as well as all connecting clients in an indiscriminate manner.

We have already updated all server software; a fact that we have pointed out to the Tor project. Unfortunately, the Tor project did not choose to accurately report information in its paper.

Tor: UltraReach claims in Section 1.1 that a user's IP address will change a million times an hour. This amounts to a new server connection 275 times per second and we find that this is not the observed client behavior.

We have long since removed these claims because of the confusion they could cause. This particular claim was never intended to mean that a single client's IP would change a millions times an hour; it was referring to the entire Ultrasurf network. We pointed this out to the Tor project, but they did not choose to accurately report information in its paper.

Blocking

For us, one of the most puzzling claims by the Tor researchers is that Ultrasurf is blocked in China. Because we receive an enormous amount of traffic from China, we know that this is not the case. We suspect that this discrepancy is a result of the Tor group not using our latest release versions. The fact is that Chinese censors, and censors in other countries, are actively trying to block Ultrasurf. Because of this, we release new versions of Ultrasurf often, and older versions may be blocked.

This is, in fact, standard industry practice. Most software vendors release new versions and patches on a regular basis, and to run secure, functional software, users must use the latest versions. As we have shown above, Tor focused on older versions of our software. We would prefer to be evaluated on current versions of the software. At the very least, when declaring whether our software successfully resists blocking, testers should use the most current version of our software.

Obfuscation

Tor: Ultrasurf is primarily protected by security-through-obscurity techniques. This method of protection is well regarded as nearly worthless if it is the primary method of protection. The security economics of analysis by reverse engineering generally lead a novice to think that security-through-obscurity will stop everyone from understanding how a given system works. Generally, the security community understands that the real strength of the system must be the design of the system itself, and not in obscuring how the system itself works. An attacker such as a government has ample resources and it is incentivised to attack tools it finds interesting.

While they are time-consuming to research, we ultimately believe the techniques used by Ultrasurf are severely flawed. This audit was performed with limited time and a limited budget by one person. A censor or dedicated attacker will not be as limited and they will likely be much more skilled with Windows reverse engineering than the authors of this paper.

Obfuscation and secrecy impede researchers, users, and advocates more than they impede most adversaries. Many adversaries have very specific motivations and such adversaries may be willing to engage in unlawful activity that the author of this paper is unwilling to engage in. They may even choose to exploit backdoors that are well intentioned and useful for so-called lawful interception. They may choose to exploit these vulnerabilities technically or socially.

Tor provides no evidence for its claim that "*Ultrasurf is primarily protected by security-through-obscurity techniques.*" In fact, Ultrasurf's primary protection is by use of industry standard encryption: RSA, RC4, etc. However, an obfuscation layer is absolutely required in our system. Otherwise, we would be trapped by a problem that has dogged the Tor Project, among others.

Standard encryption protocols have fingerprints that are traceable and blockable. For example, the Tor Project was successfully blocked in China because it used unobfuscated

OpenSSL, which has a fingerprint that is easily detectible. Chinese censors can now quite easily detect and block most standard encryption protocols. To provide uninterrupted service to our users, we do wrap our standard encryption protocols in an obfuscation layer to avoid leaving fingerprint.

In any case Tor's assertion here is unsupported. These types of vague, unsupported assertions appear throughout the Tor paper. We further regret that Tor had to resort to the name-calling in this paper – e.g., "novice."

Tor: The Ultrasurf client traffic does not appear to be padded, buffered or broken into pieces. This seems to indicate that the traffic would fall to very basic traffic fingerprinting [38]; such an attack would threaten the confidentiality of the traffic and may even allow an attacker to simply block specific content without decryption. Blocking the update process detailed in Section 6.6 seems entirely possible and it would be especially problematic.

First, note all of the qualifiers used above: "does not appear to be," "seems to indicate," "seems entirely possible." In fact, Tor did not carefully analyze or break our client traffic – we use multiple obfuscation mechanisms to avoid detection and blocking.

To a certain extent, the proof is in the pudding. Ultrasurf is widely used in Mainland China, a country that has gone to considerable effort to block its citizen's access to political and religious discussion on the Internet. Yet, China has been unable to block Ultrasurf despite the enormous resources it has brought to bear against us. This alone indicates that Tor's speculative conclusions are flawed: if blocking would be easy to implement based on "very basic" traffic fingerprinting, why has it not happened? Although we see new attempts to try to block on Ultrasurf on a weekly (and sometimes daily) basis, Ultrasurf has not been successfully blocked for any extended period of time in China.

It is instructive to contrast Ultrasurf's situation with Tor's: all anti-censorship tools that we are aware of (including Tor) face regular attempts at blocking by the Chinese government. Tor's use in China is very limited: the Chinese censors have in many cases successfully fingerprinted and blocked Tor traffic.

We do wish to clarify, however, that we do not claim that Ultrasurf is untraceable. Ultrasurf is difficult to trace. Because we have limited resources, we can only afford a limited number of domains and IPs for our system. Censors could potentially collect the domains and IP ranges to identify Ultrasurf traffic. So far, we have successfully used a wide variety of techniques to blunt or evade this form of censorship.

One point that the Tor analysis completely missed is that Ultrasuf is designed with sophisticated mechanisms to defeat the targeted blocking attempts. The design is on demand and progressive, i.e. with more blocking attempts, it will start using more advanced blocking resilient schemes progressively.

Even if Ultrasurf were to be successfully blocked (which has never happened for an extended period of time), no third party would be able to ascertain the URLs and the content of user's communications due to our strong end-to-end encryption.

Tor: Additionally, it appears that the cryptography in use is even weaker than is described in this paper in extremely alarming ways. [...] They admitted that their protocol has no forward secrecy and that they did not apply an integrity check, such as a MAC or HMAC, when they use RC4 as a stream cipher for client and server communication.

Here, Tor simply misrepresents us. We do use industry standard encryption algorithms: RSA, RC4, etc. We have turned on forward security mechanisms in the current version of Ultrasurf. We do implement a full integrity check. However, we use obfuscation (to avoid detection by censors who may try to block Ultrasurf).

Part of Tor's concern here seems to arise from a philosophical difference. Tor is opensource software, which allows anyone to check Tor's protocol and implementation.

But, in Internet Freedom scenarios, there are significant disadvantages to open-source software. Censors routinely examine open-source software to find fingerprints and unique signatures that allow protocols to be blocked. Chinese censors, for example, have repeatedly been able to successfully block Tor.

The concern raised by Tor here is how the community can assure itself of the security of Ultrasurf's protocols if Ultrasurf does not publish them. The path Ultrasurf has taken is to ask a third-party (recommended by the US State Department) to review and inspect its software. We believe that in practice, this yields better results than the open-source approach.

Because this is a philosophical difference, there may never be a meeting of minds on the question of open-source vs. expert review. But the bottom line is that Ultrasurf software has not been broken. Tor's paper presents vague, general, unsupported assertions and rumors, but does not present a method to break Ultrasurf.

Multi-hop

Tor: Although the internal structure of an Ultrasurf server consists of many layers of network proxy software, the server is effectively a single hop proxy and the Ultrasurf network is essentially a single entity; though we find that while UltraReach appears to control the network, they are merely customers of other entities. There are many scenarios where an attacker is able to compromise a single part of the server or network infrastructure. Such a compromise is almost always enough to effectively cancel out any protection that such a system may offer. Single hop or single entity proxy [3] systems such as Anonymizer, SafeWeb, Ultrasurf, and other simple proxy servers are vulnerable to myriad issues: • A proxy server may be compromised by an attacker. • *The proxy system or service may be run by an untrustworthy party.*

• The server or proxy system may be trusted but the servers network may be monitored by an attacker.

Tor's assertion that "*Ultrasurf is a single hop proxy*" is unsupported. The assertion is false, and we have demonstrated this to the Tor project. Since we have demonstrated this to the Tor project, we wish that they had taken the care to accurately describe our system.

In our demonstrations, we showed that the design of Ultrasurf is adaptive, with multi-hop proxy being in countries where danger of monitoring or blocking is particularly high. Ultrasurf is limited by resources, and we do not currently have sufficient resources to always maintain a multi-hop proxy in every single country. We are actively seeking resources that would allow us to maintain that.

Update process

Tor criticizes our update mechanism, although it has not been able to successfully break it (because we use some security measures that Tor did not detect.) However, in response to Tor's comments, we have already made substantial improvements to our update process, including using a digital signature in the update. We are continuing to improve this part of our system.

Third-party software

Tor: We find that Ultrasurf incorporates third party software in violation of their respective licenses.

Here Tor points out a valid issue for Ultrasurf. We are actively working to fix all these issues.

Final comments

The Ultrasurf team appreciates feedback on our security mechanisms. Our ultimate goal is to support and provide access to users. Currently Ultrasurf is used widely in closed societies, and represents what we think is a vital part of providing Internet Freedom capabilities to those users: access to news, political information, social networks, etc. We are constantly improving our system. Tor's paper has already led to substantial improvements to parts of our system, and we have plans for further upgrades. We have also engaged with outside parties to get their feedback to improve our system.

Other anti-censorship tools, such as Tor, serve different purposes, and together these tools represent the Internet Freedom ecosystem. Tools like Ultrasurf serve a different function than Tor. Ultrasurf is designed with capacity and scalability in mind. It

processes more than two billion hits a day. Tor has not demonstrated that it can even begin to approach the scale of users and load that Ultrasurf can.

While honest and accurate technical critique is always welcome, we regret the context in which this paper appeared. Tor did not respond to our requests to correct obvious errors in its paper, to accurately describe the current system, or even to share the paper in a timely fashion. Instead, Tor used this paper primarily in an attempt to persuade funding sponsors to cancel our funding. (Ironically, if their attempt had been successful, it would have meant that we would not have had resources to make the security improvements we have implemented in the last half-year.) The current paper misquotes us, makes representations that Tor knows to be incorrect, and includes vague, general assertions that are not supported.

As the Internet Freedom community continues to grow and evolve, we hope that we can see more scientific rigor in the field. We do not think that name-calling and unsubstantiated attacks is the best way to serve our users.