Security Audit of Safeplug

Anna Kornfeld Simpson, Anne Edmundson, Josh Kroll and, Ed Felten
Department of Computer Science
Princeton University, Princeton, NJ 08540-5233

***Abstract*—We present the first public third-party security audit of Pogoplug's Safeplug device, which marketed "complete security and anonymity online" by using Tor technology to protect users' IP addresses. We examine the hardware, software, and network behavior of the Safeplug device, as well as the user experience in comparison to other forms of web browsing. Although the Safeplug appears to use Tor as advertised, lack of user education could easily allow users to be identified in ways that they might not expect. Furthermore, an engineering vulnerability in the Safeplug's settings commands would allow an adversary internal or external to user's home network to silently disable Tor or modify other Safeplug settings, which completely overrules the security claims of the device. Even if the engineering problem is fixed, the user experience challenges of this type of device make it inferior to the existing standard in anonymity methods, particularly the Tor Browser Bundle.**

I. Introduction

User privacy is becoming increasingly important as more Internet users realize how vulnerable they are to attackers and eavesdroppers. This has been exacerbated by the current news about the NSA's surveillance of the Internet [2]. Unfortunately, the average Internet user is not aware of how to protect themselves against malicious users.

II. Background

Tor. The state-of-the-art in online anonymity technology is the open-source project Tor. Tor is a service that provides anonymous communication as an onion router; by encrypting internet traffic and sending it through layers of relays, a user can make it much more difficult to trace their internet use [5]. Instead of appearing to come from a user's IP address, the traffic will reach the destination from one of the relays, that will have received the traffic from another relay, creating a chain back from when the user first sent their traffic to a relay. Tor is known as an onion router because each relay peels back one layer of encryption and no more, allowing it to send the traffic to the next destination but not allowing it to discover the origin or final recipient of the traffic. Tor is open-source software developed by the Tor Project [34]. Users of Tor are highly recommended to use it as part of the **Tor Browser Bundle (TBB)**, which provides a single installation of a browser and the Tor software package. This browser has special settings to prevent deanonymization of the traffic by other means, such as cookies, supercookies, or scripts [34].

Using Tor or the Tor Browser Bundle provides a tradeoff between anonymity, usability, and efficiency. Sending traffic to these relays around the world slows down the traffic significantly, possibly degrading user experience for websites that load a lot of data in real-time. In addition, because the destination website will see the user's request as coming from a new, likely international IP address, websites such as banks that have location-based safeguards may deny users access to their sites. For many users around the world, these troubles are a worthwhile price for access to free and open internet, anonymous communications, and resisting censorship. However, one of the biggest reasons that Tor is not more widespread is that many Internet users do not know about Tor, how it works, or how they would be able to use it to become more anonymous online.

Safeplug. Safeplug is a product that launched in December of 2013 from the cloud storage company Pogoplug, that offers any user the option of using Tor without having to know about it or how it works. It allows users to browse the web from their own standard web browser with complete security and anonymity for the cheap price of $49 [27]. Safeplug offers Tor out of the box, with no additional software installation, by sitting between a user's router and the internet [31]. Pogoplugs marketing pitch centers around the protection of users IP addresses by using Tor [27], [10].

Pogoplug. Pogoplug, a subsidary of Cloud Engines, also offers a box for home network file sharing without needing to use a third-party storage provider. Based on our examination of the box discussed below, we suspect that the Pogoplug box was relabelled as Safeplug and just uses different software to achieve its newly branded purpose.

III. Design and Operation of Safeplug

A. Hardware

Before investigating the software, we took apart one of the two Safeplug devices we purchased in order to see the physical components. Figure **??** shows the top of the board and Figure **??** shows the bottom. The board incorporates: (A) an SD card slot, (B) a power connector, (C) a USB slot, (D) an ethernet connector, (E) ethernet transceiver, (F) lan transformer, (G) an integrated circuit, and (H), (I) flash memory.

B. Software

We determined the software on the device from analyzing network traffic logs of the activation process and accessing the device via SSH.

C. Terms of Service

The Terms of Service (TOS) contains three main points of interest: TOS updates, open source licensing information, and software updates.

TOS updates. Pogoplug suggests that users consistently read the TOS becaues they can update or change them at anytime. Most Safeplug users will likely not read the TOS

Fig. 1: Configuration instructions.

once, let alone on a regular basis; therefore, most users will be blind to any changes. It is also interesting that these TOS are only accessible through a small link at the bottom of the Safeplug website [27]; specifically, there is no documentation, including the TOS, in the package that the device was shipped in.

Open source licensing information. There is a section that acknowledges the use of many open source components in the Safeplug device; this section includes the statement:

> "You agree to abide by the terms of the relevant licenses, as may be updated by Pogoplug from time to time at http://pogoplug.com/home-en-developers-open-source.html. " [27]

The link included is a dead link and takes the user to a web page with a 404 error. This lack of attention to detail or respect for open source licenses does not put Pogoplug in a good light. In fact, the Tor-talk mailing list noted this particularly, since Tor is an open source project [32].

Software updates. Not only can the TOS be updated at any time, so can the software on the device. These udpates will be "automatically delivered" to the user, but the user is not notified of these updates [27]. This should raise a red flag for users because they may not know when the software in their device is being changed or what it is changing to. While Safeplug makes many claims about providing anonymity, users are simply putting their trust in a different entity, namely Pogoplug.

D. Tor Relay Node Option

One of Safeplug's configurations is the use of the device as a Tor relay node in the Tor network. When the device is initially setup, the default setting is to not use it as a relay node.

One of our concerns is how understandable this setting is to the average Internet user. The settings page describes Tor in an extremely basic way:

> "Safeplug uses the Tor network to secure your Internet connection. Tor works by routing your Internet through a series of random destinations, much like driving a twisty, complicated route to throw off someone who is following you, making it impossible for websites and organizations to identify the source or destination of Internet traffic." [27]

On the other hand, it describes the functionality of a Tor relay node in a much more technical manner. This description is shown in Figure 3. If the majority of users can only understand the simpler description, then they likely won't understand the description of a Tor relay node. This could be a problem if users simply decide not to do anything with that setting (i.e. don't change the setting to use Safeplug as a relay node). Then there would be a large increase in use of the Tor network, yet most of the users are not giving back to it.

This could easily be remedied; Safeplug should choose a target audience and have consistent descriptions. The best option is to explain the Tor network and the functionality of a Tor relay node at the same level, preferably a level that normal Internet users can understand. This increases the chances that users will run their Safeplug as a relay node.

E. Software on the Safeplug

The software installed by the activation process on the Safeplug (it is not on the box prior to the activation) is in `/opt/xce` and includes lighttpd, privoxy, and tor. Lighttpd is an open-source webserver, which is serving the settings page on the device - the project's description mentions "security, speed, compliance, and flexibility [... while being] designed and optimized for high perfomance environments" [15]. Privoxy is a "non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying webpage data and HTTP headers, controlling access, and removing ads and other obnoxious Internet junk" and it specifically advertises its "flexible configuration" [28]. Privoxy is also open source. All three pieces of software appear to have default configuration files. The fourth piece of software discovered on the device, which does not seem to be installed during the activation process is the Dropbear SSH server and client, used to support SSH access to the device [13]. The Safeplug uses its own configuration files to determine how these pieces of software are set up and used.

F. Configuration on the Safeplug

The Safeplug configuration files can be found in `/opt/xce/etc` and include `sp.conf` and `sp_version`

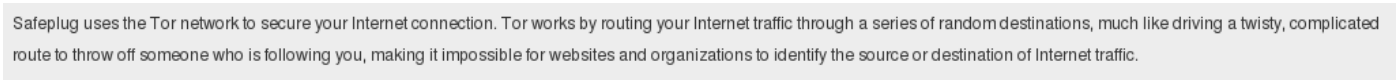

Fig. 2: Description of Tor on Safeplug settings page.

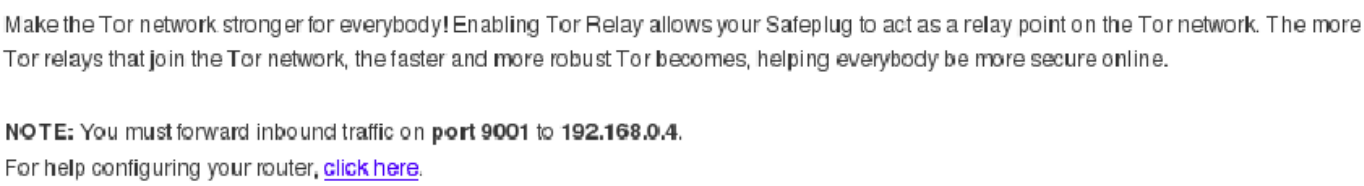

Fig. 3: Description of a Tor relay on Safeplug settings page.

and `sp_torexceptions`. The first contains all of the important details from the configuration page (whether to use Tor, whether to be a relay, whether to adblock) as well as a hidden option about whether to be an exit relay for the Tor network. This is not documented anywhere on the site, so enabling this option would likely require SSH access to discover it, thereby breaking the warranty, but it is interesting that this option is available. The version file is likely used for updates, and the exceptions file is used by the privoxy configuation to control the whitelist of sites not to connect to via Tor.

These configuration files are read by the scripts in `/opt/xce/etc/init.d` which enable lighttpd, privoxy, and tor. As expected, Privoxy looks at the Tor, adblock and exceptions configurations, and Tor reads the `sp.conf` file to set which Tor configuration file (regular, relay or exit relay) to use.

IV. Usability

Many news articles were published to announce the release of the Safeplug in addition to a lengthy discussion on the Tor-talk mailing list [32]. There were many thoughts on the Terms of Service and the option to use the device as a Tor relay node; this inspired us to start our analysis with these items.

A. Activation and Setup

The first step was to plug Safeplug into our router and activate our device. Our instructions are shown in Figure 1. We followed them, activated our device, and then ended on the configurations page. The configurations page has a combination of platforms and browsers, with a different set of proxy configuration instructions for each one. It is interesting to note that the only platform options were: OSX, Windows, Android, and iOS. Figure 4 shows our configuration.

After we finished our configuration, we were taken to our settings page. This page is shown in Figure **??**. This allowed us to turn Tor on/off, add white-listed websites, turn ad-blocking on/off, and turn the ability of our device to be a relay node on/off.

B. Internet Use

Figure **??** shows what a web page looks like before turning Tor and ad-blocking on, while Figure **??** shows the same website after turning Tor and ad-blocking on. Both of these figures show our IP address in the top right corner; due to the change in IP address we can see that our traffic is being routed through Tor.

Next, we wanted to see how usable this would be to a normal Internet user. A user would probably decide not to use Safeplug if they could not read their web pages (if they were not in their native language), or if they could not log into their accounts (some web sites will lock a user out if they try to log in from multiple countries in a short time period). While browsing the Internet, we experienced some pages in German and Swedish, which is expected with Tor; if a user is not familiar with Tor, then they may just get frustrated and stop using Safeplug altogether. We were also prompted with the page in Figure **??** when we tried to log into our Google account, indicating that Google noticed we were trying to login from different locations.

C. Cookies

While browsing the Internet, we logged into a Google Account in a tab, and then subsequently went to a website that had the Google+ logo in a different tab. When we clicked on the Google+ logo, it remember who we are; so we can confirm that we still have first-party cookies. We experienced the same situation with Facebook and its corresponding "like" button.

This is clearly not the perfect "anonymity" that Safeplug promised in their publicity. Although normal use does follow this model of persisting logged in status across browser tabs and sessions, a user concerned about anonymity and seeing each session coming up differently (German vs Swedish) might mistakenly believe that they do not have to log out of their social media accounts to preserve their anonymity when accessing other websites.

More interesting and damaging to the user's control over their anonymity would be third-party cookies because the user cannot remove those just by logging out. It requires a trip to the browser settings to clear cookies (or not have them set in the first place). We used the FourthParty plugin developed by Jonathan Mayer at Stanford to collect information about cookies and other browsing data during the client's use of the

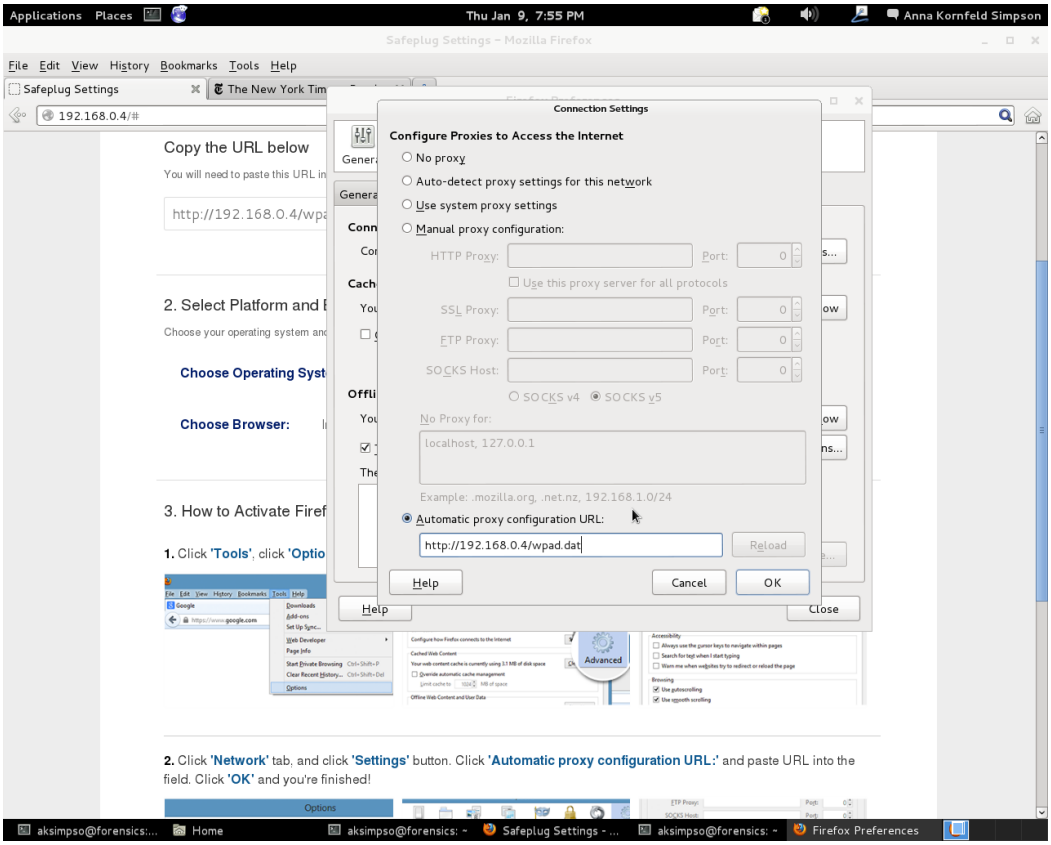

Fig. 4: Proxy Configuration.

Safeplug [19]. When collecting data on the existence of third-party cookies, we analyzed two separate browsing sessions; they were both new sessions with no cookies. One of the sessions used the ad-block feature of the Safeplug and the other did not. After analyzing data from Fourthparty, we found many third-party cookies in both sessions. These included cookies from: abmr.net, bizographics.com, krxd.net, and bluekai.com among many others.

D. Latency

If the latency of web requests using the Safeplug is noticeably longer than that of normal Internet use, users may be deterred from using the device. Similarly, if turning Tor on, but not ad-blocking, adds a significant time delay, the user may only turn on the ad-blocking feature (without Tor). We recorded the time for a web request on the following settings:

- Plain Firefox
- Firefox, no Tor, no ad-blocking
- Firefox, Tor, no ad-blocking
- Firefox, Tor, ad-blocking
- Firefox, no Tor, ad-blocking
- Tor Browser Bundle with Safeplug (all settings turned off)
- Tor Browser Bundle

For each of the settings, we took 20 measurements; Figure **??** shows the average time of a web request on each of the specified settings for three different web pages. When taking these measurements, we loaded the page, but did not scroll; in many cases more objects are loaded when scrolling down a page. The differences between web pages can most likely be attributed to the amount of ads on the web page.

It is interesting to note that the average web request time for accessing www.washingtonpost.com is greatest on the same settings that the average web request time for www.google.com is the least. This setting did not include ad-blocking, and therefore www.washingtonpost.com had to render each ad; www.google.com does not have any ads. This also explains why the average latency was greater than the other settings for www.washingtonpost.com: each ad was requested through Tor.

The latency of using the Safeplug with Firefox, Tor, and ad-blocking is comparable to that of using the Tor Browser Bundle. For all three web pages, the Tor Browser Bundle had slightly lower latency; the Tor Browser Bundle blocks scripts, and for web pages such as www.coca-cola.com, this provides a significant latency decrease. This, in conjunction with the fact that the Tor Browser Bundle is free and is issued directly from The Tor Project, shows a convincing argument to use the Tor Browser Bundle in place of the Safeplug.

V. Implementing Attacks

As we discovered during the software analysis, the Safeplug has a remote procedure call (RPC) capability. This is a script called `xspctrl` found in `/opt/xce/html/svc` and it contains various options. Particularly, functional calls to this script include enable and disable for all of the Safeplug settings, including Tor, ad block, and Tor relay. None of them require any arguments in the POST string.

A. Insider Attack

Since the RPC server does not perform any kind of validation or authentication on the settings strings, it would be easy for anyone inside the local network to send a command and change the settings, for example to disable Tor or adblocking. All the attacker would need to know is the IP of the device. It does not even require SSH or discovering the (publically available) root password, or the user's new root password if they have been well-informed and adept enough to change it. Figure **??** shows an example of this attack.

This attacker could also be any kind of device on the local network, or the local gateway if it is compromised. The NSA "Spymall" catalog leaked in December shows tools for compromising a number of different devices and home routers are traditionally insecure [1]. It is easy to imagine any malicious party, not just one with the resources of a government, (although governments might be some of the most interested parties in attacking a Tor proxy) compromising the gateway and using that access to make a disabling RPC call into the Safeplug. This would occur silently from the perspective of a client unless they happen to check the Settings page for the Safeplug. Instead, the client would continue browsing with a belief that they are protected by their use of the Tor network, while in fact any external adversary can track their traffic.

This seems like a fairly important vulnerability and requires action from Pogoplug to fix. Since the purpose of these RPC operations is unclear without access to more of the source code, it is possible that they could be disabled entirely. If not, perhaps there is some authentication protocol that could be implemented. The challenge of such a protocol from a user's point of view is that valid access would be infrequent so giving a user a password to remember would be a poor experience.

B. CSRF Attack

An external website can also perform this attack by returning a correctly formatted POST string. This executes the same functionality as the Insider Attack, but the attacker does not need to be on the local network or know the IP address of the Safeplug. Instead, the attacker (who could be any malicious actor with access to a web server) can just send a POST request to every IP in the common ranges of local addresses in home networks, 192.168.0.0/24 and 192.168.1.0/24. We implemented this attack with less than 30 lines of Javascript code (See Appendix A). The following steps are necessary for the attack to be successful:

1) Set up a web page with the crafted Javascript code, which will send the POST request of the following format to all addresses in the common ranges: http://⟨IPaddress⟩/svc/xspctrl/disableTor (See Appendix **??**).
2) Send the malicious link to a user in the targeted private network.
3) Once the user clicks the link and loads the malicious site, the correctly formatted POST request will be sent to every IP address in the ranges.
4) Tor is disabled silently. The user must check or refresh her settings page to learn that Tor is turned off.

This exploits the RPC server in the same manner that the Insider Attack does. While this attack requires a greater amount of time because the local IP address of the Safeplug must be guessed via search, the number of private address spaces is small, and the space likely to be occupied by a Safeplug on a home network is even smaller.

The largest observed time to send requests to the 192.168.0.0/24 space was approximately 400 milliseconds; the entire attack costs approximately 800 milliseconds for sending request to both 192.168.0.0/24 and 192.168.1.0/24 ranges - even when the website was being loaded over Tor. In the case of a private network in the range of 172.16.0.0/16, the attack took less than 12 minutes (this generates script timeout warnings in most major browsers, which affects the timing of this attack). This means that it would take a few hours to send requests to the full 172.16.0.0/12 range, which is commonly used in business networks. The final private network space is 10.0.0.0/8 which is too large for an exhaustive search, but some simple optimization might make it feasible as well. For example, using a GET request to get and parse the Safeplug settings page would allow the script to positively identify the safeplug and stop the search. However, the 192.168.0.0/24 and 192.168.1.0/24 ranges are much more common in home networks; because Safeplug is geared towards home network use, in most cases the script will take less than a second, a trivial amount of time for the attacker to spend.

In addition to disabling Tor, the attacker can modify any other settings on the device. This includes: enabling/disabling Tor, enabling/disabling ad-blocking, enabling/disabling the use of the device as a Tor relay node [note: this requires the user to do additional setup], enabling/disabling the use of the device as an exit node (if it is already a relay). Lastly, the attacker can also modify the user's whitelist of sites that should not be routed through Tor. This whitelist attack is particularly dangerous because the change is silent and much harder for the user to notice the addition of a single website to the whitelist than a global loss of Tor. (Removal of a webpage from the whitelist is likely to cause usability problems and be more evident.)

C. Gaining Access through SSH

Safeplug runs an RPC server that allows the enabling of SSH access via HTTP. SSH instructions for Cloud Engine's other device (Pogoplug) are widely available online and an email in the Tor-talk mailing list confirms that the instructions are the same [4]:

Obviously having a publically available root password means that SSH can be done effectively without authentication. We tried the SSH procedure twice, once before the internet

connection and activation, and once afterwards. Before the activation and update procedure, SSH was not available. The simple `Hbplug` software on the box could not accept this RPC call. However, once the box was updated and had lighttpd installed, the SSH procedure was available and we could download the contents of the root filesystem for analysis.

VI. Related Work

To our knowledge, there has been no other study analyzing the security of Pogoplug's Safeplug device. However there has been much prior research on the primary technology that the device uses: Tor. Additionally, the security vulnerabilities that Safeplug attempts to secure users against have been previously studied in great detail; these include fingerprinting and cookies.

Tor. Prior security evaluations of the Tor network reveal a myriad of potential vulnerabilities. A significant area of research on Tor relates to diversity of autonomous systems (ASes). Feamster and Dingledine argue that a user's anonymity may be compromised by using geographically diverse ASes; when analyzing both sides of an anonymous path, it is more likely the same AS will appear in both sides of a long path than in a short path [7]. Murdoch and Zielinski also argue against AS diversity. They state that AS diversity does not improve security because traffic is routed through ASes at Internet exchange points (IXPs); therefore, an IXP can observe traffic that passes through multiple ASes [23]. There has also been proven traffic correlation attacks that are efficient on the Tor network [22], [24]. Johnson, Wacek, Jansen, Sherr, and Syverson evaluated Tor's security against reasonably realistic adversaries and contribute metrics that model security over time. They found that in a period of six months, 80% of all users may be deanonymized by a reasonably realistic Tor-relay adversary. Johnson et al. take into account how the Tor network evolves over time when evaluating Tor's security [12]. While Safeplug does not introduce or modify how Tor is used, it routes all traffic through the Tor network; Safeplug is also vulnerable to the attacks found in prior research on Tor.

Fingerprinting. Website fingerprinting attacks as well as remote physical device fingerprinting attacks have shown they can identify users, even when specific defenses have been used in order to prevent these attacks. Previous research has shown that web page fingerprinting attacks are possible [6], [11], [25]. Cai, Zhang, Joshi, and Johnson introduced both a web page and website fingerprinting attack that defeats many recently proposed defenses, including cover traffic and randomized pipeling. They find that their attack is successful 83.7% of the time when the defense is the use of Tor; the success rate decreases to 52.2% when the defense is the use of Tor, randomized pipelining, padding packets to 1500 bytes, and adding cover traffic at a 1:1 ratio [3]. These results can be extended to the security of Safeplug. Because Safeplug uses only Tor to anonymize users, it may be susceptible to this type of fingerprinting attack.

Cookies There has been much policy and technology debate around the topic of third-party web tracking. Mayer and Mitchell survey recent policy and technology stances on web tracking; while tracking allows for free web content and innovation, it compromises a user's privacy [20]. They discuss the existence and use of stateful tracking by using "supercookies." While many companies use cookies, there has also been work in developing privacy-preserving third-party services, such as Privad, Adnostic, and RePriv [9], [36], [8].

VII. Discussion

A. Engineering Fixes

The most critical engineering fix is authentication in the POST calls to prevent the cross-site request forgery attack. A typical example is a cookie and a hidden form field set in the Settings page the Safeplug hosts; the cookie must be returned by the browser when making the POST request to the RPC server [38]. Although someone doing a cross-site request forgery attack such as the one described above could get the cookie sent, because of the same-origin policy, the adversary would not be able to examine the contents of the cookie to determine what to put in the form field.

B. Structural Problems

However, there are much more significant structural problems with implementing a Tor connection via an HTTP proxy. Several of the usability problems involve user awareness and vigilance. For example, cookies and fingerprinting problems mean that users could still be tracked across websites, regardless of whether the ad-block functionality on the Safeplug is enabled. This poses an unreasonable stress on users who must be aware of their browsing practices and does not bode well for the advertised security and anonymity.

One type of client that deserves special attention is a non-Android mobile phone user. Although the Tor Project publishes an Android app called Orbot on the Android Market [33] which is supported for Android versions 2.3 and later [35], there are no official Tor apps for iPhones or other non-Android devices. Safeplug provides proxy functionality and instructions for Safari on the iPhone; however, this would only work while the user is on that wifi network that the Safeplug routes through. If any data is sent over the cellular network or another wifi network, then the security of Tor is lost. Additionally, the user may have to disable the proxy whenever they move to a different network, and remember to re-enable it when they want to use Tor. This is certainly not transparent usability. Users who are truly concerned about anonymity online should eschew the Safeplug and purchase a device that supports the Tor Browser Bundle or other Tor Project software.

C. Opportunities

Despite all the structural problems, is there a market for a Torifying piece of hardware? Given the security pitfalls in comparison to a piece of software such as the Tor browser bundle, there seems to be no reason for a user that can run the Tor browser bundle to purchase the Safeplug or any other device. For mobile phones, the proxy problems with mobility contribute to an already high usability cost. However, there are an emerging class of "smart home" devices which may connect to the internet. It is possible that some of these devices can be configured to use an HTTP proxy or some other middle box to Torify their traffic to an external service provider. For them, is the benefit of some anonymity via a Safeplug-like device worthwhile? Since the data sent by these devices to the service provider likely contains lots of identifying information, the use

of Tor probably only protects the user's location at the expense of connection time and load on the Tor network. Since proxy configuration on such devices is likely to be difficult and the amount of information hidden is unlikely to be worth the effort, a Torifying box that functions as a proxy has questionable use in this space as well.

Ultimately, the structural concerns of the Safeplug "Torifying proxy-in-a-box" strategy indicate that this is not the correct method for security and anonymity online. It is critical for Safeplug to correct their engineering errors, particularly the vulnerability to silent disabling of Tor in order to protect customers who have already made use of the device, but users who are truly concerned about safety and anonymity online should make use of technologies directly from the Tor Project.

ACKNOWLEDGMENT

We would like to express our gratitude to Ed Felten for helping us procure the Safeplugs and to Josh Kroll for donating a lot of time and his computer to the routing effort. We also thank whoever left the very nice set of screwdrivers on our desks!

REFERENCES

[1] Appelbaum et. al. "Shopping for Spy Gear: Catalog Advertises NSA Toolbox" *Der Spiegel* 29 December 2013 www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

[2] Arther, Charles. "NSA scandal: what data is being monitored and how does it work?" http://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

[3] Cai, Xiang, et al. "Touching from a distance: Website fingerprinting attacks and defenses." *Proceedings of the 2012 ACM conference on Computer and Communications Security (CCS)*, 2012.

[4] Colleton, Lee. "Fwd: SSH on Safeplug" *Tor-talk mailing list* 2 January 2014. http://archives.seul.org/or/talk/Jan-2014/msg00003.html

[5] Dingledine, Roger, et. al. "Tor: The second-generation onion router." *USENIX Security Symposium*, 2004.

[6] Dyer, Kevin P., Coull, Scott E., Ristenpart, Thomas, and Shrimpton, Thomas. "Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail." *In Proceedings of the 33rd Annual IEEE Symposium on Security and Privacy*, 2012.

[7] Feamster, Nick, and Dingledine, Roger. "Location Diversity in Anonymity Networks." *In ACM Workshop on Privacy in the Electronic Society (WPES)*, 2004.

[8] Fredrikson, M., and Livshits, B. "Repriv: Re-envisioning in-browser privacy." *In Proceedings of the 2011 IEEE Symposium on Security and Privacy*, May 2011.

[9] Guha, S., Cheng, B., and Francis, P. "Privad: Practical privacy in online advertising." *In Proceedings of the 2011 USENIX Symposium on Networked Systems Design and Implementation*, April 2011.

[10] Halfacree, Gareth. "Pogoplug launches Tor-powered Safeplug" *bit-tech.net* 25 November 2013, http://www.bit-tech.net/news/hardware/2013/11/25/pogoplug-safeplug/1.

[11] Herrmann, Dominik, Wendolsky, Rolf, and Federrath, Hannes. "Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naive-bayes classifier." *In Proceedings of the 2009 ACM workshop on Cloud computing security*.

[12] Johnson, Aaron, et al. "Users get routed: Traffic correlation on Tor by realistic adversaries." *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security (CCS)*, 2013.

[13] Johnston, Matt. "Dropbear SSH." https://matt.ucc.asn.au/dropbear/dropbear.html

[14] Kohno, Tadayoshi et. al. "Remote physical device fingerprinting." Dependable and Secure Computing, IEEE Transactions on 2.2 (2005): 93-108.

[15] Lighttpd. http://www.lighttpd.net

[16] Marvell, "88F6190 and 88F6192 Integrated Controller Hardware Specifications" 2 December 2008. http://www.marvell.com//embedded-processors/kirkwood/assets/HW_88F619x_OpenSource.pdf

[17] Marvell, "Marvell 88F6192 SoC with Sheeva Technology" 2009. http://www.marvell.com//embedded-processors/kirkwood/assets/88F6192-003_ver1.pdf

[18] Marvell, "Marvell Alaska 88E1116R" 2007. http://www.marvell.com/transceivers/assets/Marvell-Alaska-88E1116R-Single-Port-GbE.pdf

[19] Mayer, Jonathan. "FourthParty" http://fourthparty.info

[20] Mayer, Jonathan R., and John C. Mitchell. "Third-party web tracking: Policy and technology." *IEEE Symposium on Security and Privacy (SP)*, 2012.

[21] Meyer, David. "Say hello to Safeplug, Pogoplugs $49 Tor-in-a-box for anonymous surfing", *GigaOm*, 21 November 2013. http://gigaom.com/2013/11/21/say-hello-to-safeplug-pogoplugs-49-tor-in-a-box-for-anonymous-surfing/.

[22] Murdoch, S.J., Danezis, G. "Low-Cost Traffic Analysis of Tor." *In IEEE Symposium on Security and Privacy (Oakland)*, 2005.

[23] Murdoch, S.J. and Zielinski, P. "Sampled Traffic Analysis by Internet-Exchange-Level Adversaries." *In Privacy Enhancing Technologies (PET)*, 2007.

[24] Overlier, L. and Syverson, P. "Locating Hidden Servers." *In IEEE Symposium on Security and Privacy (Oakland)*, 2006.

[25] Panchenko, Andriy, Niessen, Lukas, Zinnen, Andreas, and Engel, Thomas. "Website fingerprinting in onion routing based anonymization networks." *In Proceedings of the 10th Workshop on Privacy in the Electronic Society*, 2011.

[26] Panopticlick. https://panopticlick.eff.org/.

[27] Pogoplug. "Safeplug", https://pogoplug.com/safeplug.

[28] Privoxy. https://www.privoxy.org

[29] Schneier, Bruce. "Tor Appliance." *Schneier on Security*, 27 November 2013. https://www.schneier.com/blog/archives/2013/11/tor_appliance.html.

[30] Simonite, Tom. "Online Anonymity in a Box, for $49", *MIT Technology Review*, 21 November 2013. http://www.technologyreview.com/news/521676/online-anonymity-in-a-box-for-49/.

[31] Solon, Olivia. "Safeplug makes it super-easy to harness Torś anonymity at home," *Wired UK*, 22 November 2013. http://www.wired.co.uk/news/archive/2013-11/22/safeplug-tor.

[32] Tor Mailing List. https://lists.torproject.org/pipermail/tor-talk/2013-November/031199.html.

[33] "Tor on Android." *Tor Project.* Accessed February 2014. https://torproject.org/docs/android.html.en

[34] The Tor Project. https://www.torproject.org/.

[35] The Tor Project. "Orbot: Proxy with Tor." *Google Android Market*. Accessed 7 February 2014, https://play.google.com/store/apps/details?id=org.torproject.android

[36] Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H., and Barocas, S. "Adnostic: Privacy preserving targeted advertising." *In Proceedings of the 2010 Network and Distributed System Security Symposium*, March 2010.

[37] Wireshark, http://www.wireshark.org/.

[38] Zeller and Felten. "Cross-Site Request Forgeries: Exploitation and Prevention." *Princeton Technical Report*. 2008.