Award identification number: S-LMAQM-17-GR-1121
Recipient Organization: Tor Project Inc.
DUNS Number: 809211100
EIN: 1208096820A1
Period covered by report: FYQ2 2018

# Tor Project

## Progress Report Q1 2018j - S-LMAQM-17-GR-1121

Isabela Bagueros
Project Manager
The Tor Project
isabela@torproject.org

# Table of Contents

# Project Information

| | |
|---|---|
| **Grantee:** | The Tor Project, Inc. |
| **Project Title:** | Tor Browser for Android |
| **Award Number** | S-LMAQM-17-GR-1121 |
| **Period of performance:** | Q1 of the year -January 1st 2018 - March 31st 2018 |
| **Reporting date:** | May 17, 2018 |
| **Reporting frequency:** | Quarterly |
| **Email contact:** | isabela@torproject.org |

# Summary

**Work related to Tor Browser for Android**
During this quarter we worked on bringing all Orfox special configuration into the same 'code tree' of Tor Browser as well as addressing some issues related to add-ons Tor Browser needs as part of the security features we provide to our users, such as HTTPS-Everywhere and NoScript. We also start to build Tor Launcher as part of the Tor Browser for Android in order to make it possible for the user to use our browser without the need to download Orbot. We are hoping to have the first alpha release of Tor Browser for Android in Q2 and already did a small Orfox release as a transition of this process from the Guardian Project to the Tor Project team.

**Work related to Tor network optimization for mobile users**

Our 0.3.3 Core Tor release now has a tor-api for controllers which app developers can use to implement Tor to their app as a library. This has been the main request que got from mobile developers and we used our Tor Meeting in Rome to perform extensive tests with mobile developers to collect their feedback to continue iterating with this feature. We also obtained great performance improvements on CPU load by simplifying our overall event loop logic, we worked on 'libevent'[1] to do that and now we are having less 'wake up calls' on our processes which leads to less CPU consumption. We continue to improve our error reporting and fixing small bugs that mobile developers reported such as a bug that was happening on iOS which enabled Tor to shutdown and restart in same process.

# Objective 1: Build a Tor Browser for Android to empower mobile users to safely, anonymously, and securely interact with Internet resources and services.

## Activity O1.1: Build a Tor Browser for Android with functionality and build processes in parity with desktop Tor Browser.

**Progress Report:**

At this quarter we had our first 'Orfox' release completely managed by the Tor Browser Android team, the 1.5.1 Orfox release[2]. This was a nice way for the Guardian Project to hand over things to our Android team and for us to get a handle on how the release process of Orfox is done.

During this period we also worked on merging mobile patches[3] in our Tor Browser tree to centralize all Tor Browser (desktop and mobile) in one single repository tree. We also updated[4] Orfox HTTPS-Everywhere Add-on which was running an old version of it.

We start to work on fixing a prompt for enabling Sync on Orfox[5], Sync is already mostly disabled in Orfox but the UI sometimes appears to user causing confusion. Our work is to ensure that doesn't happen and disable Sync (at compile-time) until we sufficiently audit the implementation and decide it is proxy-safe.

[1] https://trac.torproject.org/projects/tor/ticket/23750
[2] https://github.com/guardianproject/Orfox/releases/tag/Fennec-52.7.2esr%2FTorBrowser-7.5.2%2FOrfox-1.5.1-RC-1
[3] https://trac.torproject.org/projects/tor/ticket/19675
[4] https://trac.torproject.org/projects/tor/ticket/25603
[5] https://trac.torproject.org/projects/tor/ticket/24919

We worked on a patch for a race-condition happening with add-ons[6] (specially HTTPS-Everywhere add-on) to address the issue we are seeing when the user installs the Browser. This first installation also install all the add-ons we need and sometimes the first installation doesn't see the add-ons and when the user launches the app they don't see our special configurations because of this race-condition, where the app doesn't see the add-ons that were installed simultaneously. But at a second launch the app sees them and our special configuration appears. Our patch is currently under review and should be merged soon.

Finally, in parallel to all this work we are building documentation for developers who would like to collaborate with the project on how to do it, our Tor Browser Hacking page now contains specific Orfox information[7].

**Risks Assessments:**

Currently our main risk is that we are still on hiring process for our Android developer. We finished interviewing all candidates and have 2 great options that we are now checking their references and we hope to have a developer for Q2.

**Next Report [Q2 2018]:**

We are targeting to have the first Tor Browser for Android release in July so our Q2 will be focus on doing all the remaining work to get this first alpha release out. We will:

- Create Tor Browser for Android branch based on mozilla-central
- Integrate Torbutton as a systems add-on
- Integrate mobile Tor Browser cross-compilation into tor-browser-build

Between other work necessary for this first alpha release as Tor Browser for Android.

## Activity 01.2: Research and develop Android specific fingerpriting defenses for Tor Browser.

**Progress Report:**

For this activity we start to test how we are in respect to our fingerprinting defenses on Android[8]. In particular, making sure we have some protections from cross-origin tracking on Android by using our patches in Tor Browser for desktop. We have identified some leaking going on such as:

- Firefox Mobile(and Orfox) allows the user to copy the url to another app[9]
    - An user is able to copy URL from the web browser URL bar to another app when both apps are diving the screen(multi window support), violating the no-proxy-bypass rule.
- Orfox lists external apps when the user clicks and holds an Android URI in a WebPage[10]

[6] https://trac.torproject.org/projects/tor/ticket/25659
[7] https://trac.torproject.org/projects/tor/ticket/25562
[8] https://trac.torproject.org/projects/tor/ticket/25703
[9] https://trac.torproject.org/projects/tor/ticket/25635
[10] https://trac.torproject.org/projects/tor/ticket/25790

    - Even if the network.protocol-handler.external-default is false an user can open an external application.
- Disable Firefox Mobile accessibility services[11]
    - Firefox Android Accessibility services (GeckoAccessibility) can be used by an external app to track user interaction in a web page.

**Risks Assessments:**

As we started this work we were concerned with the amount of work that will need to be re-done in comparison to what we can actually use from the desktop protections. But right now we are less worried about it as our findings are showing a few new things that we expected to find as these are different platforms.

**Next Report [Q2 2018]:**

For the next quarter we plan on continue investigating more fingerprinting possibilities on Android and fix them.

### Activity 01.3: Work with Mozilla to merge and built defenses back into Firefox Mobile

**Progress Report:**

This work haven't started yet, although we are going to Mozilla All Hands again in June and hope to have another meeting with their mobile team to better organize this effort.

**Risks Assessments:**

n/a

**Next Report [Q2 2018]:**

We are doing to Mozilla All Hands in June in San Francisco where we will be syncing with Firefox Mobile team and coordinate this upstream effort.

## Objective 2: Specifically Build a Tor Browser for Android to empower mobile users to safely, anonymously, and securely interact with Internet resources and services.

### Activity O2.1: Enable standalone use of Tor Browser for Android without separate Orbot installation

**Progress Report:**

One of the main goals of our project is to include Tor Launcher on our Tor Browser for Android so our users don't need to install Orbot in order to establish a connection with the Tor network. As part of this effort we want to have the same code base used by Tor Browser for desktop as the

[11] https://trac.torproject.org/projects/tor/ticket/25902

one used for Android, in order to do that we will have to modify some parts of how Tor Launcher implementation is done. Our first step was to write a technical proposal[12][13] of how we will do this implementation and work on applying it[14][15].

**Risks Assessments:**

Currently our main risk is that we are still on hiring process for our Android developer. We finished interviewing all candidates and have 2 great options that we are now checking their references and we hope to have a developer for Q2.

**Next Report [Q2 2018]:**

For Q2 we will continue to work on integrating Tor Launcher to Tor Browser for Android as a systems add-on.

### Activity 02.2: Improve usability of Tor Browser for Android, relative to Orfox, including anti-censorship bridges.

**Progress Report:**

The work related to anti-censorship bridges will be done once we have ported Tor Launcher to our Android browser. At our desktop browser we are working on fixing different user problems and changing a lot our UI and the user experience. We are including the experience for Android as part of this process as well and hope to bring all the usability fixes we are doing in the desktop version to mobile. During our Tor Meeting in Rome we spend great time with both teams (desktop and mobile) discussing the different user problems and possible solutions. We are very excited with this coordination at our development process, where we are thinking mobile and desktop together when brainstorming solutions for our users.

**Risks Assessments:**

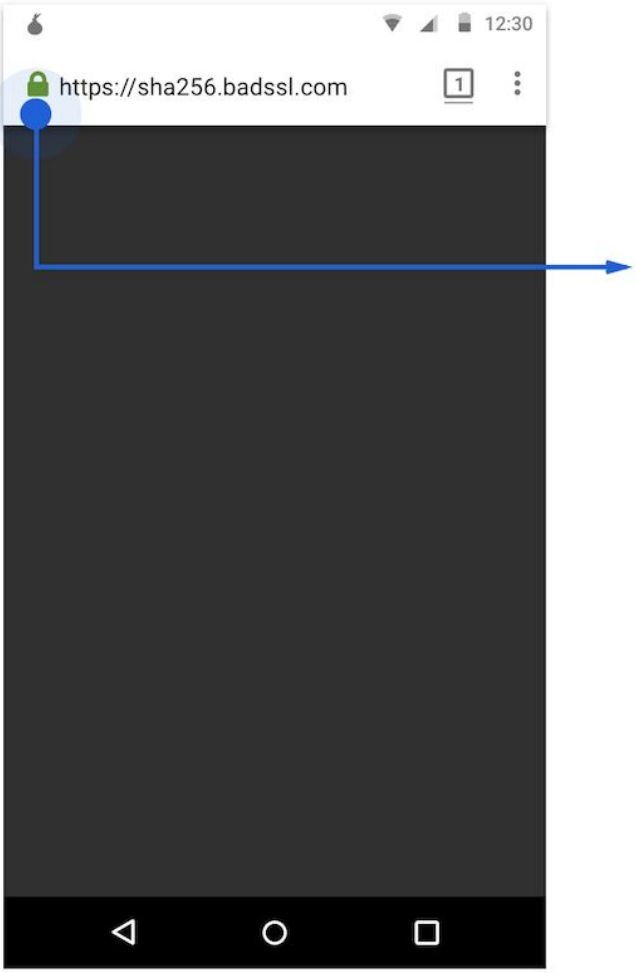
Currently our main risk is that we are still on hiring process for our Android developer. We finished interviewing all candidates and have 2 great options that we are now checking their references and we hope to have a developer for Q2.

**Next Report [Q2 2018]:**

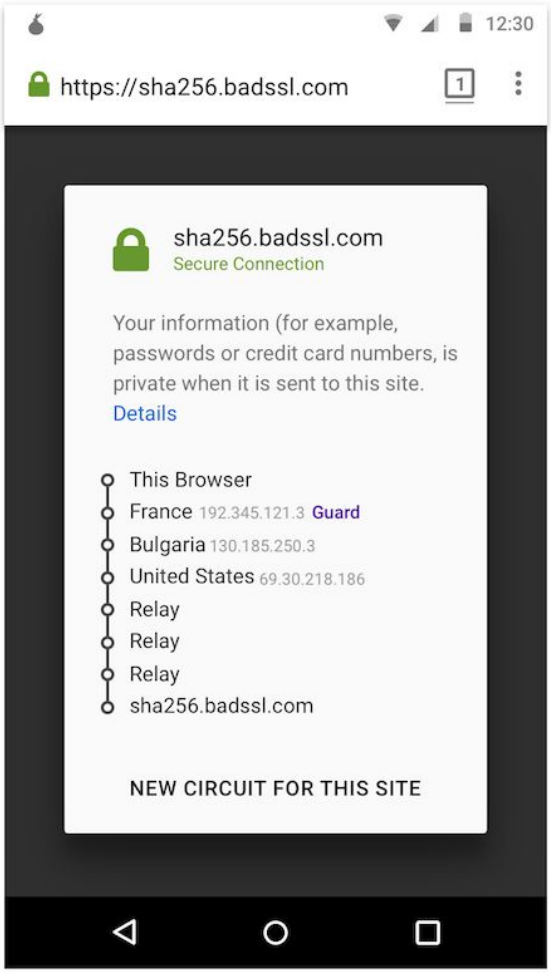
For Q2 we should have all new UI design mocks we are building for the user experience in our desktop browser also created for the Android experience so our developers can implement the same new experience in both platforms.
Here is an example of the new user experience (Tor circuit display) we are creating for desktop and also porting to Android:

[12] https://lists.torproject.org/pipermail/tbb-dev/2018-January/000735.html
[13] https://lists.torproject.org/pipermail/tbb-dev/2018-January/000743.html
[14] https://trac.torproject.org/projects/tor/ticket/24856
[15] https://trac.torproject.org/projects/tor/ticket/25260

00.01 - Padlock tap




01 - Padlock Description + Circuit




## Activity 02.3: Improve software and Tor Network architecture to improve usability for low-speed networks and low-power, low-RAM devices.

**Progress Report:**

**CPU load**

During the past quarter we performed an analyses[16] based on the results from the initial set of measurements[17] collected on Q4 and our main strategy has been to address the leading problems, which are battery drain due to excessive "wake up calls" (#25500), and memory usage due to the directory cache (#25503).

[16] https://trac.torproject.org/projects/tor/ticket/24065
[17] https://docs.google.com/spreadsheets/d/1N4dRCrmvlTME615sODaeTb4lCQWKxgux2l4U7EfYRZc/edit#gid=0

We organized all tasks[18] we identified that can reduce "wake up calls" on mobile and started all the preparatory design work to modify them.

Then we start to work on these tasks and managed to simplify our overall event loop logic[19], and make other event loop simplifications easier. We worked on 'libevent'[20] to do that and now we are having less 'wake up calls' on our processes, these calls were happening too often and therefore consuming more memory and CPU when running Tor on mobile.

**Risks Assessments:**

n/a

**Next Report [Q2 2018]:**

For Q2 we plan to continue working on the tasks we have identified and keep the improvements we want to do on Core Tor to reduce "wake up calls' and memory usage.

### Activity 02.4: Improve the Tor Network's controller interface to allow mobile apps to reduce bandwidth and battery use.

**Progress Report:**

Our Core Tor 0.3.3 was released with supported tor-api for use by controllers for app developers who wish to integrate Tor in their app. At our Tor Meeting in Rome (March, 2018) we worked with OONI and other mobile developers (Guardian Project and Onion Browser) to debug and integrate Tor-as-a-library into their app. All this work is documented on our bug tracker under the ticket #23684[21], together with all of its children tickets.

We also documented all the feedback collected at our Tor Meeting[22] from developers. This will help guide our work to continue improving the experience for developers who want to embed Tor on their apps.

We worked on how to improve memory usage as well, #22703 and its children tickets are part of this effort for better cooperation with cache management on mobile. What we did was to better organize things we storage and created a specific place for cached objects (cached-*), this helped with memory usage on platforms where /var is a tmpfs.

We fixed an issue reported by developers of OnionBrowser (iOS) which enabled Tor to shutdown and restart in same process. See #24581[23] for tracking ticket. Also see #25512[24].

[18] https://trac.torproject.org/projects/tor/ticket/25500
[19] https://trac.torproject.org/projects/tor/ticket/25374
[20] https://trac.torproject.org/projects/tor/ticket/23750
[21] https://trac.torproject.org/projects/tor/ticket/23684
[22] https://trac.torproject.org/projects/tor/ticket/25510
[23] https://trac.torproject.org/projects/tor/ticket/24581

**Risks Assessments:**
N/A

**Next Report [Q2 2018]:**
Work on the feedback given by developers who are testing our tor-api documented as children tickets under: https://trac.torproject.org/projects/tor/ticket/25510

## Activity 02.5: Enable better reporting of network and connection errors to apps that use Tor Network

**Progress Report:**
We fixed a major problem[25] users who had the wrong timezone set in their machines would see when launching an application like Tor Browser that its trying to establish a connection to the Tor network. They would receive an error that their timezone was wrong. This was particular confusing for users who their clock might have the right time but their timezone was not right. We worked on the network side to be smarter about how to deal with this situation and present better messages to the user and/or application launching Tor.

We also improved getrandom() syscall failure to contain[26]:

- The log level should possibly be NOTICE rather than WARN.
- The log message should mention that tor will fall back to alternative sources of randomness.
- Mention header/kernel version mismatches as a specific common reason for this issue.

This will help the developer who is running Tor to know what they need to do to fix this issue.

**Risks Assessments:**
n/a

**Next Report [Q2 2018]:**
For next quarter we plan on continue investigating areas where we can improve our error reporting and fix them.

[24] https://trac.torproject.org/projects/tor/ticket/25512
[25] https://trac.torproject.org/projects/tor/ticket/25511
[26] https://trac.torproject.org/projects/tor/ticket/25120