Award identification number: S-LMAQM-17-GR-1121
Recipient Organization: Tor Project Inc.
DUNS Number: 809211100
EIN: 1208096820A1
Period covered by report: FYQ4 2018

Tor Project

Progress Report Q3 2018 - 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:	Q3 of the year -July 1st 2018 - September 31st 2018
Reporting date:	October 30th, 2018
Reporting frequency:	Quarterly
Email contact:	isabela@torproject.org

Summary

Work related to Tor Browser for Android

We are happy to report that we have launched Tor Browser for Android alpha with the following features:

- BLOCK TRACKERS - Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies automatically clear when you're done browsing.
- DEFEND AGAINST SURVEILLANCE - Prevent someone watching your connection from knowing what websites you visit. All anyone monitoring your browsing habits can see is that you're using Tor.
- RESIST FINGERPRINTING - Tor aims to make all users look the same, so Tor Browser for Android makes it difficult for you to be fingerprinted based on your browser and device information.
- MULTI-LAYERED ENCRYPTION - When you use Tor Browser for Android, your traffic is relayed and encrypted three times as it passes over the Tor network.
- BROWSE FREELY - With Tor Browser for Android, you are free to access sites your local internet service provider may have blocked.

Since we launch on Google Play Store alone, the app has ~204k downloads on active devices, with a retention rate of ~40% for over 30 days. Giving this is just our first alpha, the retention rate is very good.

Work related to Tor network optimization for mobile users

We feel very good with our achievements on this front as well. Our core tor bundle has been optimized for mobile environments, consuming less memory, CPU and battery as well as space in the disk. More than that, at our Tor Project Meeting in Mexico we met with mobile developers who gave great feedback on our controller API and do find it very useful for them. For the last

quarter of this project we will just try to see what else we can be adding to these efforts and finalize our error reporting activity.

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:

For our first alpha release, we finished bringing the minimum protections we wanted our users to have while using our alpha.

We finished rebasing our mobile patches to ESR60, then ensured that App sotres were not allowed to execute things we didn't control. We also set up a secure way for our app to update itself on Android. We did another audit for proxy bypass and applied patches for all the leak identified during the audit.[1]

We also worked on bringing reproducible builds to our mobile release process to make sure its in parity with our desktop release security standards[2].

[1] https://trac.torproject.org/projects/tor/ticket/26401
https://trac.torproject.org/projects/tor/ticket/26018
https://trac.torproject.org/projects/tor/ticket/25790
https://trac.torproject.org/projects/tor/ticket/26028
https://trac.torproject.org/projects/tor/ticket/26613
https://trac.torproject.org/projects/tor/ticket/26528
https://trac.torproject.org/projects/tor/ticket/26574
https://trac.torproject.org/projects/tor/ticket/24796
https://trac.torproject.org/projects/tor/ticket/26826
https://trac.torproject.org/projects/tor/ticket/26825
https://trac.torproject.org/projects/tor/ticket/24855
https://trac.torproject.org/projects/tor/ticket/27271
https://trac.torproject.org/projects/tor/ticket/27220
https://trac.torproject.org/projects/tor/ticket/27013
https://trac.torproject.org/projects/tor/ticket/27016
https://trac.torproject.org/projects/tor/ticket/22170
https://trac.torproject.org/projects/tor/ticket/27305
https://trac.torproject.org/projects/tor/ticket/26531
https://trac.torproject.org/projects/tor/ticket/27400
https://trac.torproject.org/projects/tor/ticket/27473
https://trac.torproject.org/projects/tor/ticket/27459

[2] **https://trac.torproject.org/projects/tor/ticket/26695**
https://trac.torproject.org/projects/tor/ticket/26693

Risks Assessments:

As we are entering the last quarter of the project, our main risk assessment is the 'unknowns', the issues that might arise as we finish this activity. These 'unknowns', bugs or dependencies that might appear in this last phase, might cause delays and as we are at the end of the project any delay is a risk. So we want to pay attention to this so we can manage any delay if they happen.

Next Report [Q4 2018]:

Our goal is to finish bringing all the features from Tor Browser desktop to Android, a good example would be our security settings (Security Slider) which we still need to update the experience to be in parity with our desktop application.

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

Progress Report:

During Q3 we closed the remaining finigerprinting defense tickets that we want to be part of our first alpha release.

We closed all cross origin fingerprinting vulnerabilities found on our audit[3]:

- Orfox lists external apps when the user clicks and holds an Android URI in a WebPage
- Disable Firefox Mobile accessibility services (Firefox Android Accessibility services (GeckoAccessibility) can be used by an external app to track user interaction in a web page)
- intl.accept_languages leaks information about OS language

We also disabled 3rd party frameworks that are collecting analytics on mobile usage for Mozilla (Adjust and Leanplum) to ensure our users were not being tracked by that[4].

Finally we did a lastpass on another patch that Orfox team used to do for AccountManager and Sync code that would leak fingerprinting information and addressed any remaining leak that the new version still had related to these functions[5].

Risks Assessments:

N/A

Next Report [Q4 2018]:

Fingerprinting investigation will continue as we move towards stable release. We are very satisfied with our work in this front and feel we are on target to accomplished a level of fingerprint defense in parity to the one we have for desktop.

[3] https://trac.torproject.org/projects/tor/ticket/25703
[4] https://trac.torproject.org/projects/tor/ticket/25906
[5] https://trac.torproject.org/projects/tor/ticket/26858

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

Progress Report:

We had just a couple of patches upstreamed to Mozilla:

- Delete RECEIVE_BOOT_COMPLETED permission[6]
- Fix typo in the extension optionsType handler[7]

At the end of this quarter we had our Tor Project Meeting in Mexico and a big team from Mozilla came and participated in different discussion sessions throughout the meeting.

Risks Assessments:

N/A

Next Report [Q4 2018]:

We will continue to submit our patches upstream to Mozilla as we work on fixing Android specific fingerprinting and other privacy protection features. We will also attend Mozilla All Hands in December, in Orlando.

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:

We start to evaluate the best way to integrate Tor to Tor Browser for Android so our users don't need to install Orbot. For now, with our alpha release, our users sees a notification when they launch Tor Browser for Android and don't have Orbot installed, the notification let them know they will need to install Orbot. When they click on 'ok' to go install it, the Orbot Play Store page opens so they can easily download and install the app.

As part of our project to improve mobile experience with Tor in general, our network team created an API for our core tor controller so mobile developers could easily embed Tor to their app. During this quarter we evaluated this API and gave feedback to the Tor network team on features we believe to be nice to have.

[6] https://bugzilla.mozilla.org/show_bug.cgi?id=1480877
[7] https://bugzilla.mozilla.org/show_bug.cgi?id=1474306

The evaluation was very useful for the team to learn what the API can do and we can see how this API can help other developers. But in general for our case, the controller itself already does all the things we need in a nice way, so we don't need to use this API for our implementation.[8]

Risks Assessments:

As we are entering the last quarter of the project, our main risk assessment is the 'unknowns', the issues that might arise as we finish this activity. These 'unknowns', bugs or dependencies that might appear in this last phase, might cause delays and as we are at the end of the project any delay is a risk. So we want to pay attention to this so we can manage any delay if they happen.

Next Report [Q4 2018]:

We will continue the integration of Tor connection to the network to our browser, using core tor controller, so our users don't need to download Orbot.

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

Progress Report:

We finally launch our first Tor Browser for Android Alpha:
https://blog.torproject.org/new-alpha-release-tor-browser-android

[8] https://trac.torproject.org/projects/tor/ticket/26653

We are very happy with our first official alpha release, we manage to bring to our users a browser almost in parity with Tor Browser desktop' features and new UI.

This new experience aim to fix main usability issues we collected from meeting our users face to face to collection of tickets at our issue tracking system where users were complaining about it.

We brought to our alpha on mobile this whole new user experience we created for Tor Browser desktop 8.0, which includes a new user onboarding that teaches our users about the different features Tor Browser has to protect their privacy, what is the Tor network and some tips on what to expect as you browse the web using Tor Browser.[9]

[9] https://trac.torproject.org/projects/tor/ticket/25696
https://trac.torproject.org/projects/tor/ticket/26690

We also applied internationalization and start to localize our mobile browser so it can support the same set of languages our desktop browser supports (including new languages that came out with desktop 8.0 release).
The alpha is available as an apk at our download page, as well as Google Play Store. As we work towards our stable release we will also have it available at FDroid store.

https://trac.torproject.org/projects/tor/ticket/26884
https://trac.torproject.org/projects/tor/ticket/27611
https://trac.torproject.org/projects/tor/ticket/27111
https://trac.torproject.org/projects/tor/ticket/26782

Risks Assessments:

As we are entering the last quarter of the project, our main risk assessment is the ‘unknowns’, the issues that might arise as we finish this activity. These ‘unknowns’, bugs or dependencies that might appear in this last phase, might cause delays and as we are at the end of the project any delay is a risk. So we want to pay attention to this so we can manage any delay if they happen.

Next Report [Q4 2018]:

We will finalize the integration of all UI changes we applied for desktop 8.0, including the new bridge request/selection experience, where our users can receive obfs4 bridges to bypass censorship by just solving a captcha challenge.

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

Progress Report:

Architectural improvements - via dividing Tor into more modules, to make it easier to make them optional in the future.

We split and reorganized our code to make it easier for developers to choose what they want and only use that to build their packages making the binary smaller. Part of this work involved some refactoring of the code as well. These are the areas of the code which we made architectural changes during this quarter:

- split src/common into src/lib[10]
- router.c and routerkeys.c into separate modules[11]
- common/client/cache/authority parts of directory.c and dirserv.c[12]
- non-stats part of the stats module into different modules[13]

Another part of the code that we changed so it can be optional when building Tor with an app was all the OpenSSL part. This way if an app is using NSS the developer can build Tor withouting having to compile OpenSSL with it[14][15][16].

RAM usage reductions and improvements: We fixed 3 issues that were causing unnecessary memory consumption.

- We removed --enable-openbsd-malloc which was also affecting CPU consumption[17].
- We also reduced the space used by RSA onion keys on clients, in our experiments we used 5.9MB out of 24.7MB total for storing crypto_pk_t and its contents, a 15% decrease of space used in our total memory[18].
- Another change done was to remove an unnecessary object being cached. In experiments we saw that this cached object adds up to 5.7 MB out of a total of 24.7 MB used for directory allocations. By removing it, or replacing it with something mmaped, we can save about 23% of our total client memory usage[19].

CPU usage reduction:

[10] https://trac.torproject.org/projects/tor/ticket/26481
[11] https://trac.torproject.org/projects/tor/ticket/27864
[12] https://trac.torproject.org/projects/tor/ticket/26744
[13] https://trac.torproject.org/projects/tor/ticket/27892
[14] https://trac.torproject.org/projects/tor/ticket/26631
[15] https://trac.torproject.org/projects/tor/ticket/26815
[16] https://trac.torproject.org/projects/tor/ticket/26816
[17] https://trac.torproject.org/projects/tor/ticket/20424
[18] https://trac.torproject.org/projects/tor/ticket/27246
[19] https://trac.torproject.org/projects/tor/ticket/27247

Some of the changes we did last quarter generated some bugs that we had to fix, most of them were detected by chutney, one of our testing applications[20].

Risks Assessments:
N/A

Next Report [Q4 2018]:
We are very happy with the results of this activity and could call it completed but as we are entering our last quarter, we decided to continue to investigate any possible improvements left that we can implement on this front.

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

Progress Report:
We are very happy with our controller API and so far the general feedback from developers has been positive, for this quarter we continue to document feedback received on a master ticket: https://trac.torproject.org/projects/tor/ticket/25510

And we continue to address each one to improve our API. This quarter we work to improve the in-process interface for developers to use the API[21]. Here is a quote from Arturo, tech lead of OONI, one of the mobile projects that we reached out for feedback:

> *The main advantages I see for a mobile app developer use-case, is the fact that:*
> 1. *You can create out of this an event telling you that the Tor control port is ready to receive messages without relying on polling to see if the port is open.*
> 2. *You can use it to signal tor to shutdown cleanly, by simply closing the socket.*

We added a function for reporting the tor version in tor_api.h - this will be very useful for an user that wishes to check if they have linked to the right Tor version without having to start Tor creating significant overhead[22].

Risks Assessments:
N/A

[20] https://trac.torproject.org/projects/tor/ticket/27146
https://trac.torproject.org/projects/tor/ticket/27300
https://trac.torproject.org/projects/tor/ticket/27303
[21] https://trac.torproject.org/projects/tor/ticket/24204
[22] https://trac.torproject.org/projects/tor/ticket/26947

Next Report [Q4 2018]:
For our final quarter we will continue to implement the feedback received from developers, our goal is to improve our API to be as useful as possible to our developer community.

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

Progress Report:
To improve the error messages when a client is establishing a connection with the Tor network we abstract out the current monitoring of bootstrap directory information progress, so we can track it state more independently. This way we were able not to treat cached directory information as meaning that the network is reachable and report the right state of the connection attempt[23].

We continue to work to display the earliest connection to a relay or bridge as the first steps in the connection bootstrap process[24]. We to work improvements in Pluggable Transports error reporting[25].

Risks Assessments:
N/A

Next Report [Q4 2018]:
We are aiming to finalize the relay/bridge connection report and PT error report tasks at the last quarter of this project.

[23] https://trac.torproject.org/projects/tor/ticket/27169
[24] https://trac.torproject.org/projects/tor/ticket/27167
[25] https://trac.torproject.org/projects/tor/ticket/25502