Award identification number: S-LMAQM-17-GR-1121
Recipient Organization: The Tor Project Inc.
DUNS Number: 809211100
EIN: 1208096820A1
Final Report: July 31, 2017 - December 31, 2018

Tor Project

Final Report - S-LMAQM-17-GR-1121

Gabriela Rodriguez
Maria Pilar Guerra
Project Manager
The Tor Project
gaba@torproject.org
pili@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:	Final Report: July 31, 2017 - December 31, 2018
Reporting date:	March 30, 2019
Reporting frequency:	Final
Email contact:	grants@torproject.org

Summary

Tor Browser for Android

We are very happy to say that we now have a Tor Browser for Android, in parity with our desktop browser, that can connect to the Tor network without the need of Orbot app. With anti-censorship configuration options in case Tor is blocked for the user. Our Android browser contains all the usability improvements built in the past year, such as our new user onboarding.

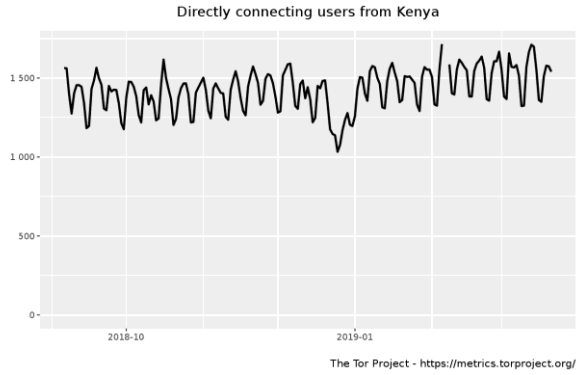
As of the time of writing this final report, since the release of the first Tor Browser for Android Alpha, (September 2018 - March 2019), we have achieved over 2M installs by unique users. We are currently at just over 650k total installs on active devices as of March 21, 2019 with a retention rate of ~30%. This is very good considering this is an alpha release and the average retention rate for mobile apps is around 29%.[1]

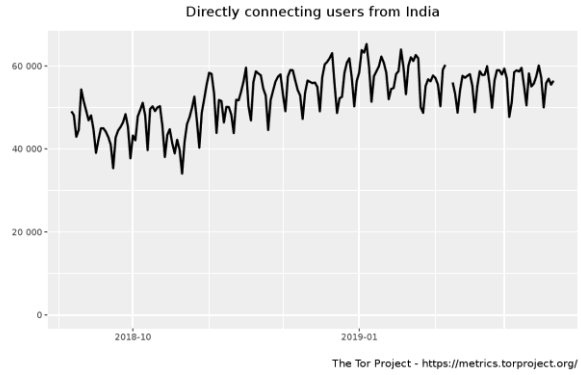
Of the countries in the Global South targeted for this project, India has the second highest number of installs at 13% of installs followed by Brazil in fourth place with 6% of installs. It's also worth mentioning that Bangladesh is in sixth place with the highest number of installs at 4% of installs, Indonesia in eighth place with 2% of installs, and Iran in fifteenth place with 1% of installs. These numbers do not take into account direct apk downloads from the Tor Project website[2] which we are not yet tracking on our metrics.

Tor network optimization for mobile users

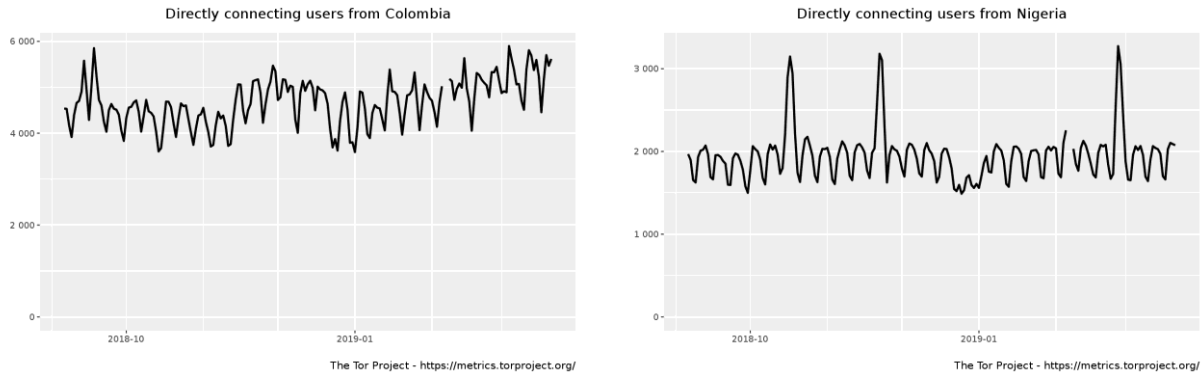
Since this project started, we have managed to significantly reduce memory usage, mostly in mobile and clients, and improved how Tor reports about bootstrapping status.

While we can't directly track the number of connections to the Tor network that come from mobile users, we have seen a steady increase in the number of connections to the Tor network for our target countries since the start of this project.





[1] http://info.localytics.com/blog/mobile-apps-whats-a-good-retention-rate
[2] https://www.torproject.org/download/#android



Tor usage trend from target countries

Although network utilisation varies throughout time, and there are always peaks and troughs in usage due to different events happening in the country. We can see that in general, from the time of the first Tor Browser for Android alpha launch, the peaks and spikes in network usage are getting higher, as well as the troughs.[3]

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.

Accomplishments

Throughout this project, we worked on integrating the existing Orfox code into our Tor Browser code to build a Tor Browser for Android that closely resembles our desktop version, in terms of

[3] https://metrics.torproject.org/userstats-relay-country.html?start=2018-09-06&end=2019-03-21&country=co
https://metrics.torproject.org/userstats-relay-country.html?start=2018-09-06&end=2019-03-21&country=in
https://metrics.torproject.org/userstats-relay-country.html?start=2018-09-06&end=2019-03-21&country=ke
https://metrics.torproject.org/userstats-relay-country.html?start=2018-09-06&end=2019-03-21&country=ng

feature and brand parity. At the same time, we have kept up with the Firefox ESR60 series and the corresponding security fixes from Firefox and have been on 60.6ESR since March 19, 2019.

By the end of this project, we were happy to achieve build process parity with desktop which enables us to release new versions of our alpha series for all platforms at the same time. This is an important step as we move towards making Tor Browser for Android part of our upcoming 8.5 stable series.

This allowed us to bring notable usability features that are currently the same across mobile and desktop include the on-boarding experience and Tor Launcher configuration wizard for bridges and pluggable transports. Other notable features are the same proxy safety protections that we offer on desktop[4] as well as first-party isolation[5].

Impact

By taking over development of Orfox and re-branding it to Tor Browser for Android, we are ensuring a consistent experience for our users throughout platforms, as well as an improved experience on Android when compared to Orfox.

There is currently no other internet browser for the Android platform which achieves the level of security and privacy afforded by Tor Browser for Android.

Challenges

We had a couple of delays at the beginning of this project that forced us to ask for a no-cost extension and adjust our timeline accordingly. A large part of this delay was caused by the time it took for us to put together the best team to develop for Android. We had to hire three new developers, a process which took some time to finalise. An additional delay was caused by unexpected challenges in the Firefox version we had planned to use as a base for Tor Browser for Android. We had to re-evaluate and adjust our work plan and priorities—this caused a delay in producing our first deliverable.

In addition to the extended hiring timeline, one of our core developers had to take an unexpected leave of absence at the end of 2018 and is still out, which impacted our timeline further. As a result of this, we haven't yet merged the "New Identity" or "Current Circuit" functionality to Tor Browser for Android for the upcoming stable release.

[4] https://www.torproject.org/projects/torbrowser/design/#proxy-obedience
[5] https://www.torproject.org/projects/torbrowser/design/#identifier-linkability

However, we have reached out to our developer on leave and plan on re-assigning it within the team so it's ready by the time of our stable release or shortly after.

ACTIVITY O1.2: RESEARCH AND DEVELOP ANDROID SPECIFIC FINGERPRINTING DEFENSES FOR TOR BROWSER.

Accomplishments

We started this activity by auditing any Android-specific potential fingerprintability vectors as well as evaluating existing defenses on our desktop version for potential overlaps. We now have a good process for identifying these situations and iterating on building and testing our fixes until we are satisfied we have resolved any potential proxy-bypass and fingerprinting issues.

By the time of our first alpha release, we achieved a good level of fingerprinting defenses, although the desktop and mobile versions are not yet on parity.

Impact

There is currently no other internet browser for the Android platform which has these fingerprinting defenses in place.

Challenges

Although our browser currently has more protection than any other Android browser, we do recognize that anti-fingerprinting work is constantly evolving.

Through the course of this project we had to decide where to make a cut and how to better utilize our resources to ensure high priority patches were the focus of our team. Of the fingerprintability bugs we currently have documented for Tor Browser for Android, several are low priority and were thus not completed by the time of writing this report. The other mobile-only fingerprinting defense bugs that were not resolved by the end of this project should be addressed with new Mozilla releases. We made the decision not to resolve these bugs because the platform-independent code is already solving underlying issues.

Additionally, as new Android versions and features are released, we will need to continue evaluating any potential new situations and continuously patch Tor Browser for Android accordingly. This will also be the case for any new Firefox versions.

ACTIVITY O1.3: WORK WITH MOZILLA TO MERGE AND BUILT DEFENSES BACK INTO FIREFOX MOBILE

Accomplishments

We have an excellent relationship with Mozilla and the Firefox mobile team and have been collaborating closely throughout this project. We hope to continue this relationship beyond the end of this project. We have standing weekly and monthly online meetings to share progress and discuss issues as well as face-to-face meetings, both when Tor Project members are invited to attend Mozilla's bi-annual All Hands meetings as well as when members of their Fusion ("Firefox USIng ONions") team are invited to our bi-annual meetings.

Throughout the course of this project, we have uplifted a number of patches[6] to Mozilla and will continue working with the team to help them build and merge our defenses back into Firefox for mobile.

Impact

Collaborating with Mozilla in this way allows us both to benefit from each other's expertise and together make better, more secure, privacy-focused tools for mobile phones.

Challenges

Although we have a good level of communication and collaboration with Mozilla, we are still dependent on them to prioritise and merge our patches into their codebase.

Additionally, we had to slightly de-prioritise this work in the lead up to the alpha and stable releases in order to concentrate on building out features to bring Tor Browser for Android on feature parity with the desktop version. However, we will continue working with Mozilla on this activity beyond the end of this project.

[6] https://bugzilla.mozilla.org/show_bug.cgi?id=1459420
https://bugzilla.mozilla.org/show_bug.cgi?id=1459089
https://bugzilla.mozilla.org/show_bug.cgi?id=1455165
https://bugzilla.mozilla.org/show_bug.cgi?id=1440789
https://bugzilla.mozilla.org/show_bug.cgi?id=1480877
https://bugzilla.mozilla.org/show_bug.cgi?id=1474306

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

Accomplishments

We began this activity with the development of an API for the tor controller to allow Tor Browser for Android to connect to the Tor network directly. While this is useful for other Android application developers, we found that this was not necessary to achieve our goals. We ended up building Orbot into Tor Browser for Android, starting with our 8.5a5 release.

Since then, we have continued improving the user interface and working on building a more seamless and intuitive experience for users to configure their connection to the Tor network. For our stable release, we are planning to integrate the Tor Onion Proxy Library (TOPL).[7]

We are confident that this process has allowed us to come up with the best approach for achieving this goal. We are planning for this improved experience to be ready in time for our stable release.

Impact

Having a Tor Browser for Android that directly connects to the Tor network without the need for a separate Orbot installation lowers the usability barrier for users with low power devices and limited technical skills. As we mentioned, Iran is fifteenth in the download rank in our Play Store stats, and we know Tor is censored there. These users in particular are our target for this feature. Additionally, having a direct connection to the Tor network increases the browser's security, stability under stress, and responsiveness.

Some comments from the Google Play Store on this activity include:

> More convenient than a separate bot and browser. We are waiting for release.

[7] https://github.com/thaliproject/Tor_Onion_Proxy_Library

Challenges

As before, we were set back quite a bit on this task due to the time spent in hiring our Android developers. Additionally, we had quite a number of alternative options to achieve this goal which meant that we invested significant time in exploring all of the different options to allow direct connection to the Tor network from within Tor Browser for Android.

ACTIVITY O2.2: IMPROVE USABILITY OF TOR BROWSER FOR ANDROID, RELATIVE TO ORFOX, INCLUDING ANTI-CENSORSHIP BRIDGES.

Accomplishments

When we first started this project, we were in the process of implementing a number of UX improvements on Tor Browser for desktop which we hoped to develop on Android in parallel. As part of the effort to clarify in-app terminology, we have created an on-boarding guide for new users, similar to the one available on desktop, on Tor Browser for Android.

As part of improvements to the configuration UI[8] for our latest Alpha release,[9] we have implemented a number of changes to the application launch screen to allow users to explicitly connect to the Tor Network by clicking "Connect." This means that Android users now don't need to also download the Orbot app in order for the Tor Browser for Android to connect to Tor.

Although there is no automatic censorship circumvention happening if the connection to the Tor Network fails, we have implemented pluggable transport support for our mobile users, allowing them to configure obfs3, obfs4, and meek from the application launch screen.

Additionally, during the bootstrapping process, we are now showing much more accurate and fine-grained information about the progress of the app connecting to the Tor network. We are also giving users the ability to look at connection logs to allow for easier troubleshooting of issues when connecting to the Tor Network.

In addition to the above, Tor Browser for Android is localised to all of the languages supported by our desktop version.

Impact

[8] https://trac.torproject.org/projects/tor/ticket/28329
[9] https://blog.torproject.org/new-release-tor-browser-85a9

We believe that the biggest impact of this work is the fact that users don't need to download yet another app anymore in order to use our Browser. Furthermore, the inclusion of anti-censorship bridges and pluggable transports will enable Android users to easily circumvent censorship when using Tor Browser for Android.

Some relevant comments from the Google Play store include:

> No wonder I waited! The application after the last update just flies and the design has become more attractive. I am glad that I decided to switch from Orfox to this no longer crude and excellent project.
>
> Dear developers, the program works in my opinion, even more stable than the Orbot + Orfox bundle. Thank you very much for the program. :)
>
> better than installing the tor and orbox separately very good

Challenges

This was another activity which was impacted by the Android developer hiring process.
It is extremely hard to implement an automatic circumvention process for users as censorship techniques are different depending where you are and it could be risky to guess that for the user. Therefore, users experiencing censorship still need to do some manual configuration in order for the connection to be established successfully.

The Tor Project is investing a lot in resolving this problem by putting together an anti-censorship team and building projects where our censorship measurement team, OONI, can work closely with our browser and usability teams in order to achieve better usability in this step of the user experience.

We still have some work to do to keep improving usability and we will keep reviewing user comments in the Google Play Store to ensure we keep usability high. Some relevant comments to keep an eye on include the following:

> Tor still doesn't work with Linkedin in Russia (through bridge too) but with Orbot does. I can't open Linkedin program via Tor. Why?
>
> Very good program, no problems establishing and maintaining a connection to the Tor Network and accessing restricted websites. There are a few small bugs: -I wish there was an option in the settings to automatically connect to the Tor Network when the application is started, instead of requiring the user manually click the onion-shaped "START" button. I only launch this app on my device when I intend to connect to the Tor Network, it would make sense to connect-on-launch. -There is an option in the settings the user can uncheck to disable Always-On Notifications, but the option does not seem to work. -The "save file" or "save image as" options on webpages does not work. Maybe the application is saving the images somewhere deep in the applications folder, I don't know. But there is nothing in the standard downloads

folder in Android, this is inconvenient for most users. Overall though this application does the job, and does it much more smoothly that having to use Orbot and Orfox separately.

orbot with orfox is better, not to mention that using this it is not possible to activate the function in Android 9 that blocks connection without the vpn

ACTIVITY O2.3: IMPROVE SOFTWARE AND TOR NETWORK ARCHITECTURE TO IMPROVE USABILITY FOR LOW-SPEED NETWORKS AND LOW-POWER, LOW-RAM DEVICES.

Accomplishments

As part of this work, we managed to **reduce tor memory usage between ~50% to ~73%** depending on the type of profile for the 0.3.5 Core Tor release.

In order to reduce the Core Tor binary size for app developers, we began separating modules, and began extracting modules to be enabled as compile time options. This allows application developers wanting to include Tor to only choose what they want and need and make their resulting apps smaller.

Impact

These improvements will make it easier to run Tor-enabled applications on a larger number of devices, especially low-end ones that have less memory. Better responsiveness and improved usability should increase adoption of Core Tor for mobile applications.

Challenges

One of the improvements requires all relays to update to our Core Tor 0.4.0 version. So it will take some time until it's rolled out to all relays in our network to really be able to see the results. Our challenge here will be to ensure this 'roll out' period is as short as possible so the results are seen sooner.

ACTIVITY O2.4: IMPROVE THE TOR NETWORK'S CONTROLLER INTERFACE TO ALLOW MOBILE APPS TO REDUCE BANDWIDTH AND BATTERY USE.

Accomplishments

For this activity we were happy to be able to work closely with mobile application developers from our community to develop an API[10] (tor-api) to allow them to embed Tor within a process. This API was first published as part of our Core Tor 0.3.3 release and we have been continuously improving on it since then.

In order to further reduce battery usage by Core Tor, we implemented changes to reduce the number of CPU wake ups and the resulting battery drain, which are now enabled through a new "dormant" mode which is now supported by Tor 0.4.0.

Impact

We have made it easier for mobile developers to embed Tor in their apps without undesirable side effects such as application crashes or excessive resource consumption of battery, and RAM.

In particular, some improvements to the in-process interface for developers to use the API[11] were welcomed by developers who sent us the following 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.*

Challenges

We were very reliant on mobile developers to use our code and provide feedback on needs and requirements. At times we found it hard to get this feedback to help us validate our approach. Additionally, we had to be careful that the optimizations introduced did not break other functionality or create security issues for the network.

ACTIVITY O2.5: ENABLE BETTER REPORTING OF NETWORK AND CONNECTION ERRORS TO APPS THAT USE TOR NETWORK

Accomplishments

One of the biggest improvements included under this activity was the improvement in the reporting of bootstrapping errors. From a usability perspective, this improvement makes it much

[10] https://trac.torproject.org/projects/tor/ticket/25510

[11] "#24204 (Improve the in-process Tor API: create owning control port ...." https://trac.torproject.org/projects/tor/ticket/24204. Accessed 15 Mar. 2019.

easier for applications to automatically attempt to self-correct or give the user instructions on what to try next.

This improved reporting enabled us to fix a major bug related to users setting the wrong timezone on their devices, which was encountered by a large amount of users.

We also worked on improved reporting for pluggable transport bootstrapping status, which allows users to see when a pluggable transport is not working to connect to the Tor network and potentially debug the problem.

All improvements related to this activity will be included in Core Tor 0.4.0, scheduled for release in April 2019.[12]

Impact

We have made it easier for application users and developers to troubleshoot issues when using Core Tor to connect to the Tor Network. This results in increased confidence in the software that we ship and, as a result, increased adoption of the technology by developers and end users. We also managed to fix a major bug that was affecting many users when trying to use our browser (desktop and Android).

Challenges

When introducing such changes, it was important for us to be very thorough at analyzing and documenting the potential security impact of changes in this area. This evaluation process is not something we had done very well in the past and it took us some time to do so for this project.

[12] https://blog.torproject.org/new-release-tor-0401-alpha