Tor Project – Onion Services
Final Report
Contract No: 1002-2018-060

Introduction

Onion Services enable websites and other web services to offer anonymous locations for users to visit. The service operator can setup an onion service as a place inside the Tor network that the users can access to without revealing information about where the service is located. For example, a NGO in Brazil that provides information about abortions could set up an onion site without fear of being discovered by any possible threat to their services. The information they provide would be encrypted, and the information about how to access that data (i.e., the metadata) would be obscured.

Onion Services are also used by different tools from the Tor ecosystem to help people connect in a private way. For example, Onionshare, uses Onion Services to make a connection between a person who sends a file and the person who receives it to have the whole exchange inside the Tor network. There are other tools like Briar and SecureDrop that also use Onion Services. We expect more applications to use Tor this way in the future with the improvements that we achieved through this project.

Onion Services are used by different media organizations to help people around the world to reach their content without being censored. For example New York Times, Facebook and ProPublica. They are also used at other places like the Central Intelligence Agency. They have adopted Tor's onion services to make it easier for users in internet-repressive regimes, as well as whistleblowers and activists, to access their sites safely and securely without the negative consequences that metadata and content exposure bring.

Summary

Objective 1: Enhance onion services and make v3 the default version on Core Tor, so it can scale and be more stable, with the goal of enabling more organizations to adopt it for their users.

Activity 1.1 - Make v3 the default on Core Tor stable **- 100% completed**

Progress

In May we released Tor 0.4.3.5 that includes the work we finish with this activity[1] [2].

Activity 1.2 - Adopt OnionBalance features into onion services v3 **- 100% completed**

Progress

During this last month, we worked on producing OnionBalance packages for Debian and pip[3].

[1] https://blog.torproject.org/node/1872
[2] https://trac.torproject.org/projects/tor/ticket/29995
[3] https://pypi.org/project/OnionBalance/

Additional Work

Now that we have OnionBalance v3, the Tor Project as an organization can start to use this as we upgrade our onion services to v3[4]. This is something that will happen in the next year when we have the capacity to do it. Other organizations that heavily relay on Onion Services (like SecureDrop to connect whistleblowers with news organizations) will be updating it soon too.

We will continue to solicit feedback from users on this new version and future versions of OnionBalance and fix bugs as they are found. For more details on next steps for OnionBalance v3, check out the blog post[5] which we will write upon release.

We are talking with other funders to write Onion Guides that will help the community have a place where they can consult how to use Onions. OnionBalance has a section in the guide to help service operators learn how to use it, or for those who are already using it, how to migrate to HSv3.

Activity 2 - Denial of service defenses **- 100% completed**

Progress

This activity was to develop an “onion cannon" to reproduce DoS attacks in order to take measurements and understand how these attacks work. We completed this work.

Challenges or Changes

Thanks to the work on this activity measuring how DoS attacks work, we found that taking down a big .onion site with a DoS attack requires an extremely low number of resources- basically a couple of servers, good bandwidth, and a few minutes.

We also found out that ongoing attacks are greatly affecting the health of the network and the reliability and performance of all Tor users. Thus, to make the biggest impact for the most users, we decided we needed to focus on safeguarding the health of the network so that ongoing attacks don't cause so many reconnects and failed connections. We wanted to be sure that one DoS attack on an onion service did not take down the entire network. We also gave options that smaller onion services can use to defend against aggressive DoS attacks, like client authorization. For this work, we asked for an extension that got converted into an amendment for this project.

Objective 2: Improve the end user experience of onion services with the goal of increasing user adoption and retention.

[4] https://trac.torproject.org/projects/tor/ticket/32824
[5] https://blog.torproject.org/cooking-onions-reclaiming-onionbalance

Tor Project – Onion Services
Final Report
Contract No: 1002-2018-060

Activity 1 - Integrating client-side authorization to onion services v3 **- 100% completed**

Progress

We released Tor Browser 9.5[6] last week which includes the ability for users to manage authorization keys in Tor Browser[7].

Activity 2 - Notify users about typo errors when entering .onion addresses **- 100% completed**

Progress

Now Tor Browser 9.5 will show a notificaiton that informs users when a failed connection to an onion service is due to a mistyped v3 address[8].

Activity 3 - Notify users if a current website they are visiting on Tor Browser has an onion service version **- 100% completed**

Progress

Tor Browser 9.5 now notifies the user when there is an onion service version.

Activity 4 - Better client-side errors ***- 100% completed***

Additional Work

As a follow up to this project, we are planning to work on implementing validation in Tor Browser for Same Origin Onion Certificates[9]. With the recent approval of DV certificates for v3 onion services by the CA/B forum[10], we are also working on mapping the existing and future alternatives for adding a TLS certificate to an onion service and pushing for wider adoption and implementation of these in the wild.

Activity 5 - POC for Human-memorable addresses for .onion services **- 100% completed**

Progress

Tor Browser 9.5 now includes human memorable names[11] in HTTPS-Everywhere through a SecureDrop update channel[12].

Additional Work

Now that we have a implementation of this work, we will continue iterating on the expected behavior and collecting feedback from any Tor Browser user. We will continue exploring alternative solutions to this problem by mapping out all of the different existing solutions and evaluating their effectiveness.

---

[6] https://blog.torproject.org/new-release-tor-browser-95
[7] https://trac.torproject.org/projects/tor/ticket/19757
[8] https://trac.torproject.org/projects/tor/ticket/23545
[9] https://trac.torproject.org/projects/tor/ticket/13410
[10] https://cabforum.org/pipermail/servercert-wg/2020-March/001791.html
[11] https://trac.torproject.org/projects/tor/ticket/30029
[12] https://trac.torproject.org/projects/tor/ticket/28005

Amendment: Address DoS attacks against onion sites and the Tor network. **100% completed**

Progress

This amendment allowed us to spend time researching how to solve the DoS attack problem and we brainstormed some important ideas[13]. We explored different short and long term solutions[14] and considered that it was worth it to focus on evaluating an optional dynamic proof of work scheme for the onion services to specify. From this work we wrote a Tor proposal "A First Take at PoW Over Introduction Circuits[15]" posted it and discussed.

Challenges or Changes

As an extension of objective 1, activity 2 we asked to meet in person to discuss short, medium and long term solutions to DoS attacks and find a way to make decisions fast. We understand that face-to-face meetings are the faster way to focus on a problem and collaborate to find a solution. When we were planning the face-to-face meeting, the lock-down and travel cancellations happened related to the covid-19 pandemic. We had to change plans and look for other ways to connect and figure out how to move forward. We switched to meeting online for a couple of hours over several days and designated a couple of our engineers to explore several short and medium term solutions.

Additional Work

As next steps, we are planning to implement DoS defenses based on proof-of-work (PoW) and anonymous credentials [16] to provide more options to onion service administrators for defending their services. To achieve this, we are reaching out to other funders to sponsor this work.

Conclusion & Outlook

Until this project, Onion Services have been poorly maintained as we haven't had many funds to focus on this. We needed to make version 3 the default in the Tor network to be able to reduce onion services exposure to malicious relays and create faster and more reliable client connections. Now v3 is the default since Tor 0.3.5.1 and is on feature parity with v2, something that this project allowed us to do. Onion Services v3 has Onion Balance support and the entire network supports v3. Thanks to this work, we can now initiate the process of deprecating v2 and on October 2021 we will have only v3 in the Tor network.

As next step for Onion Services v3, we need metrics to know the number of Onions using v3. Right now we only have metrics for v2[17] and we can't differentiate v2 and v3 traffic[18] on the

[13] https://trac.torproject.org/projects/tor/ticket/29999
[14] https://trac.torproject.org/projects/tor/ticket/31223
[15] https://lists.torproject.org/pipermail/tor-dev/2020-April/014215.html
[16] https://lists.torproject.org/pipermail/tor-dev/2020-March/014198.html
[17] https://metrics.torproject.org/hidserv-dir-onions-seen.html
[18] https://metrics.torproject.org/hidserv-rend-relayed-cells.html

network. We are looking for support to continue the implementation of Privcount[19], that is a distributed counting system which relies on multiple nodes and entities to achieve privacy and security, and through that improve our metrics for Onion Services.

Denial of services have been a problem for many Onion Services in the last couple of years. With this project we focused on understanding how denial of services attacks work. While working on this project we found out that taking down an Onion services with a DoS attacks requires low number of resources. And we found out that DoS attacks also slow down the rest of the Tor network. We asked for an extension to research on defenses and its implementation. The extension was to cover an in-person meeting so we could brainstorm possible approaches. As Covid-19 lock-downs started, we had to change the travel plans to a series of audio calls and use the extension to do more research.

As a next step for denial of services defenses we will be implementing PoW and anonymous credentials, that are the approaches we evaluated during the extension of this project.

With this project, we worked cross-team (Tor Browser, Tor Network, Community and UX teams) on improving the user experience of onion services in Tor Browser for end-users aiming to increase adoption and retention. We saw a significant increase of traffic on onion services only two days after releasing Onion Location, this shows how the feature helped with the discover-ability of onion services[20] . Tor Browser 9.5 allowed users to opt-in for a safernetwork connection through the redirection option to an onion version of a website. The next steps for onion location are 1) to understand how we can improve the developer experience implementing onion-location on their services, 2) move forward with becoming a header standard, and 3) deploy new features in the header such an alias or a load balancing. Another important usability improvement on Tor Browser 9.5 is the way onion errors are exposed to users. By relying on a step-by-step graphic, we teach users about where the error was happening and give them straightforward information about the error and the chance to recover. The next step in onion errors includes offering localized strings for our supported languages and increase the number of network errors that we did not contemplate for this first version.

As a next step we are going to write guides to help service providers and users to implement onion services as well as connecting with partner organizations to help shape this documentation.

This project allowed the Tor Project to bring Onion Services v3 in parity with v2 and brought v3 support to Onion Balance, both things that were blocking developers from migrating to v3, a secure version of Onion Services. We were able to invest on critical usability improvements, including the biggest challenge of solving human readability of onion services addresses. We also could create mechanisms (Onion Cannon) to better investigate DDoS attacks and could create a strategy from short to long term solutions to defend onion services and the network from these attacks. All of it has marked an important milestone in popularizing this important censorship circumvention and surveillance protection technology. We are very thankful to Open Technology Fund for helping us achieve this milestone.

[19] https://www.robgjansen.com/talks/privcount-uoregon-20161004.pdf

[20] https://metrics.torproject.org/hidserv-rend-relayed-cells.html?start=2020-05-20&end=2020-06-26