
Tor Bridge Distribution

Statement of Work

Isis Lovecruft

1 Tor Bridge Distribution

Tor Bridge Distribution includes the maintenance of critical infrastructural systems such as BridgeDB, while also working to improve the robustness, scalability, and maintainability of those systems. It also includes the development of more secure and user-friendly mechanisms for bridge distribution. Without this essential work, much of the Tor Projects' efforts in the area of censorship circumvention would be unusable.

1.1 Background

For additional background information, please see the additional Reference materials, Exhibit A. [16]

BridgeDB has been a free and publicly available service since 2006. Since its inception, BridgeDB has consistently held a number of bridges between half and two-thirds the number of total relays in the Tor network, with its databases currently holding over 4,000 bridges relays [1] and over 12,000 Pluggable-Transport bridges for distribution to users in censored regions. There are approximately 12,000 to 15,000 Tor bridge users per day, using bridges which BridgeDB has distributed. (Please see additional Reference materials [2] and [3].)

BridgeDB's website (see additional Reference material [4]) sees 4.5 million initial page hits per day, and hands out Tor bridges over HTTPS to users roughly 75,000 times per day. BridgeDB's email autoresponder receives 525,000

Isis Lovecruft
Lead Developer
The Tor Project, Inc.
E-mail: isis@torproject.org

emails per day, replies to users with help and configuration assistance 350,000 times per day, and emails Tor bridges to users roughly 50,000 times per day. All of BridgeDB's user interfaces are translated and localised into 45 different languages and dialects.

1.2 Background Information for Primary Developer

The technical lead for this project will be Isis Lovecraft. Isis has been a developer for The Tor Project for the past five years. The first two years were spent working on the Open Observatory of Network Interference (OONI), a platform for a global censorship detection system, as well as tools for the OONI platform which detect various types of network anomalies and censorship events.

After developing OONI, Isis spent the next three years as the Lead Developer and Maintainer of BridgeDB, however, due to lack of funding, much of this time was volunteered. At the same time, Isis also worked for the LEAP Encryption Access Project (LEAP), developing a transparently encrypting remailer in an effort to provide better communications security. Isis has volunteered for, and contributed to, several other projects, including Open Whispersystems, Briar Project, Tahoe-LAFS, and others.

1.3 Terminology

Throughout this and the following sections, the grant applicant for the Open Technology Fund's (OTF) Emerging Technologies Fellowship Program (ETFP) shall be referred to as "The ETFP Fellow" or, simply, "The Fellow". The recipient of the goods and/or services provided by The ETFP Fellow will simply be referred to as "OTF".

2 Scope of Work

The Fellowship's Scope of Work shall consists of a full-time effort to:

- Maintain BridgeDB and other Tor Bridge Distribution infrastructure,
- Mitigate any reported or discovered vulnerabilities within the components of said infrastructure,
- Develop improved solutions for distributing Tor Bridges to end-user clients, and
- Improve the reliability, scalability, and future maintainability of the underlying systems and their codebases.

2.1 Objectives

The Fellow shall strive to ensure that all code and operational procedures are developed with the end-user's security, privacy, and usability prioritised above all other improvements.

Additionally, The Fellow shall, at all times, strive to make BridgeDB and other codebases concerning Tor Bridge Distribution as maintainable, comprehensible, and easily extensible as possible.

3 Statement of Work (SOW)

3.1 Tasks and Deliverables

With respect to the maintenance and improvement of Tor Bridge Distribution, The ETFP Fellow shall undertake the following Tasks within the duration of the Fellowship:

SOW.1. The Fellow shall migrate BridgeDB's cluster of servers to a new host machine. This new host has already been graciously donated to The Tor Project, however, the migration process will require some time and may require some possible development work to complete. This server migration will result in increased server resources, improved uptime, and will enable development of the more resource intensive processes necessary for the future scalability improvements.

SOW.2. The Fellow shall refactor legacy sections of BridgeDB's codebase to utilise a new Tor parser library. This library is commonly-maintained by several developers and volunteers at The Tor Project, thus, this initial refactoring will result in a great reduction in future efforts spent maintaining the BridgeDB's codebase, as well as additional speed improvements and increased uptime for the production servers which distribute Tor bridges to clients. (See additional Reference materials [5] [6] [7] [8].)

SOW.3. The Fellow shall implement scalability improvements to Tor Bridge Distribution backend infrastructure, including but not limited to:

SOW.3.1. Migration of BridgeDB's databases to a distributed, asynchronous database system and add support for using a caching key-value store (see additional Reference materials, Exhibit X, for further details regarding proposed implementation, and see also [9] [10] [11]), and,

SOW.3.2. Improvements to sections of the core Tor codebase which determine the behaviours of the Directory Authorities and Bridge Authority, when necessary.

SOW.4. The Fellow shall provide continued maintenance of infrastructure related to Tor Bridge Distribution, including but not limited to:

SOW.4.1. Systems administration maintenance and supervision regarding production systems used by The Tor Project, Inc., for Tor Bridge Distribution to end-user clients.

SOW.4.2. Timely response and mitigation to any reported or discovered vulnerabilities within production systems used by The Tor Project, Inc., for Tor Bridge Distribution to end-user clients, including code review and vulnerability mitigation for underlying software infrastructure required for maintaining said systems.

SOW.5. The Fellow shall continue to publicly interface with the general Tor volunteer community to review submitted patches, and shall provide assistance and mentorship to new volunteers interested in contributing to any portions of codebases belonging to The Tor Project, Inc., which concern Tor Bridge Distribution and closely-related systems such as Pluggable Transport development.

SOW.6. The Fellow shall create an Application Programming Interface (API) to enable easier and more rapid future developments of additional Tor Bridge Distribution mechanisms (commonly referred to as "Bridge Distributors").

This API shall allow Bridge Distributors to be run on production servers separate from the database systems, increasing the security, integrity, and auditability of both the Bridge Distributors and the backend databases. This API shall also provide for easy development of novel Bridge Distributors, for example, such as a Twitter bot which distributes Tor Bridges, or a Tor Browser Bundle (TBB) Firefox extension which automatically retrieves new Tor Bridges for clients after detecting that some threshold of the client's current set of Tor Bridges are not reachable or not functioning correctly. (See additional Reference materials [11] [12], and SOW.9.1.)

SOW.7. The Fellow shall produce additional documentation, both developer- and user-facing, for Tor Bridges, BridgeDB, and various Pluggable Transports, and shall improve the clarity and update existing documentation when necessary.

SOW.8. The Fellow shall develop improved User Interfaces (UIs) for interacting with clients to distribute Tor Bridges. (See additional Reference materials [13], although additional tasks are likely to arise.)

SOW.9. The Fellow shall research potential future improvements concerning Tor Bridge Distribution, and shall publicly report on these research efforts and their proposed implementations.

SOW.9.1 The Fellow shall research the feasibility and implementation difficulty of creating a new TBB Firefox extension to automatically distribute bridges to clients who have few remaining reachable or functional bridges remaining in their Tor configuration file.

SOW.9.1.2 The Fellow shall research, design, and document a proposed implementation of an Inter-Process Communication (IPC) channel between TBB and BridgeDB. (See additional Reference materials, Exhibit Y, [18] for a Work Breakdown Structure (WBS) diagram of the systems components involved.)

SOW.10. The Fellow shall research the implementation difficulty and costs associated with implementing a modified version of the "Social Distributor" defined in the rBridge paper. (See additional Reference materials, Exhibit Z, [19] for the rBridge paper, and additional Reference materials [14] for a ticket discussing previous, not-yet-complete, research.)

This research will stand as the basis for later implementation of an automated, privacy-preserving, Tor Bridge Distributor that uses measurements of a user's "good behaviour" (i.e. the user's bridges have not been blocked by a censoring party), as well as invite tokens, to create a highly censorship-resistant Tor Bridge distribution mechanism, wherein censoring parties and their sibiyls are "locked out" of the system and unable to obtain bridges. The results of this research shall be publicly documented as an implementation proposal.

SOW.10.1. The Fellow shall investigate the current implementation feasibility, and server-side efficiency, of the underlying cryptographic primitives required by the design of the "Social Distributor" contained within the rBridge paper, including, but not limited to, anonymous credentials and oblivious transfer. (See additional Reference materials [15])

SOW.10.1.1. The Fellow shall investigate the reusability of any previously-published implementations of these requisite cryptographic primitives.

SOW.10.1.2. The Fellow shall consult with cryptologic experts concerning the safest implementation strategy for these primitives, should no acceptable implementations already exist.

SOW.10.1.3. The Fellow shall consult with cryptologic experts concerning any modifications made to the original design of the "Social Distributor" defined in the rBridge paper in order to evaluate their ramifications for security, privacy, and anonymity.

SOW.10.2. The Fellow shall investigate the feasibility of implementing the client-side portion of the codebase for the "Social Distributor" on top of the TBB Firefox extension defined in SOW.9.1.

SOW.10.2.1. The Fellow shall consult with the TBB development team to arrive at a design that is satisfactory to the TBB development team.

3.1.1 Acceptance Criteria

Due to The Fellow being the Team Lead for the Tor Bridge component of the software and hardware Tor ecosystem, as well as the Lead Developer and Lead Maintainer of BridgeDB, the satisfactory acceptance of the efforts and work concerning the above Deliverables, and the determination of their completion status, shall, to some extent, be under the review and recommendation of The Fellow. However, The Fellow shall routinely consult with other Team Leads within The Tor Project, Inc., as well as with any Technical Reviewers, etc., at OTF, to assess that the Deliverable are satisfied in a manner which meets the approval of all parties.

3.1.2 Payment

Provided that the Tasks and Deliverables defined in this SOW meet the Acceptance Criteria defined in 3.1.1, and The Fellow continually meets the provisions for Monitoring defined in 3.4, OTF will provide The Fellow with a monthly stipend of \$4,200 USD, for a period up to twelve (12) months, for a total sum of no more than \$50,400 USD.

3.2 Schedule

The ETFP Fellowship is defined to endure for a duration of one (1) year. The end of The ETFP Fellowship is to be interpreted relative to the start of the ETFP Fellowship, where the start of The ETFP Fellowship is defined as the date when both parties (i.e. OTF and The Fellow) have established a Contract and agreed to any required Terms and Conditions.

The Tasks defined in this SOW have been given in an estimated chronological order, such that Tasks assigned a lower SOW number are to be completed prior to tasks which have been assigned a higher number. Tasks comprised mostly of research, namely SOW.8-10, may be completed by The Fellow at any time throughout the duration of The ETFP Fellowship.

3.3 Assumptions

All work included within this SOW shall be executed by The ETFP Fellow, or by volunteer developers who are external to The Tor Project and whose contributions are subject to the review, approval, and supervision of The Fellow. The Fellow shall not subcontract any of the Deliverables detailed herein to any other party without the explicit written permission of OTF.

3.3.1 Location of Work

The Fellow is unrestricted concerning the location of work, provided that The Fellow is reasonably capable of efficiently and productively communicating with OTF and other colleagues, including colleagues at The Tor Project, Inc., and other institutions and organisations with experts concerned with the surrounding subject matter.

3.3.2 Time Requirements

The Fellow shall make a time commit equivalent to that of provincial and lawful full-time employment in the region(s) which The Fellow inhabits or completes the Tasks as defined in the SOW within.

3.4 Monitoring

The Fellow shall create monthly status reports, which shall be sent to both OTF's and The Tor Project's mailing lists. The Fellow shall, when necessary for either collaboration or reporting, schedule, organise, and conduct online meetings, in open public channels, with colleagues to ensure that progress is made in a satisfactory and timely manner. The Fellow will request regular code reviews and shall carefully consider the recommendations of the reviewers.

4 References

References

1. <https://metrics.torproject.org/networksize.html?graph=networksize&start=2008-10-06&end=2008-10-06>
2. <https://metrics.torproject.org/users.html?graph=userstats-bridge-country&start=2013-01-01&end=&country=all#userstats-bridge-country>
3. <https://metrics.torproject.org/userstats-bridge-transport.html?graph=userstats-bridge-transport&start=2014-10-06&end=&transport=%3COR%3E&transport=obfs2&transport=obfs3&transport=obfs4&transport=fte&transport=meek>
4. BridgeDB
5. Trac Ticket #9380
6. Trac Ticket #12872
7. Trac Ticket #11216
8. Trac Ticket #12505
9. Trac Ticket #12031
10. Trac Ticket #12030
11. Trac Ticket #12506
12. Trac Ticket #12029
13. Trac Ticket #10831
14. Trac Ticket #7520
15. Trac Ticket #12807
16. Original OTF ETFP Application for the Tor Bridge Distribution project
17. Tor Project Proposal #226: BridgeDB Database Improvements
18. BridgeDB and Tor Browser Systems Interaction Diagram
19. Wang, Q., Lin, Z., Borisov, N., & Hopper, N. (2013). rBridge: User Reputation based Tor Bridge Distribution with Privacy Preservation. In NDSS. PDF