Invisible Matrix Services
White Paper

Originally Published April 26, 2018
Last Updated August 12, 2019

1 Abstract

Invisible Matrix Service (1M5 using leet) is the first decentralized services platform with intelligent routing between anonymity networks to bypass censorship. This is required as a base level for electronic communications to ensure freedom of speech, expression, association, and assembly using electronics.

Censorship resistance is currently accomplished using Tor and I2P. In the future, it will include 1DN (a direct wireless ad-hoc network using Radio and LiFi) as well as other future anonymity networks. When a user's device gets blocked on one network, other networks are used to route around the block until another node can make the request.

To ensure this effort doesn't get shut down, it is not an organization nor registered in any jurisdiction and thus is only a shared global mission between those that wish to support freedom of speech, expression, association, and assembly among all beings. Aligning with and following any laws of a particular jurisdiction would create a leverage over the mission ending its ability to sustain it. A call for operating the mission with common ethical principles such as the non-aggression principle and voluntaryism (voluntary relationships) is key. Working with any entity known for aggression, especially of the systemic sort, is a compromise of those ethics.

2 Introduction

1M5's mission is to protect freedom of speech, expression, association, and assembly over electronic communications for all beings by ethical sustainable means.

When the Berlin wall was opened in November 1989, expectations of a more open human society sprang forward. Yet several decades later we are experiencing digital walls being raised by governments and large corporations in the name of protection. These walls promote segregation and censorship of information while harming creativity, innovative technology, and freedom of speech.

Freedom of Speech is a principle that supports the freedom of an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship, or sanction. The term "freedom of expression" is sometimes used synonymously but includes any act of seeking, receiving, and imparting information or ideas, regardless of the medium used.

Censorship is the suppression of speech, public communication, or other information, on the basis that such material is considered objectionable, harmful, sensitive, politically incorrect or "inconvenient" as determined by government authorities or by community consensus.

Constraining the free flow of information between people is a direct threat to our freedom and censorship of communications on-line is growing world-wide.

- https://internetfreedomwatch.org/timeline/
- https://www.wired.com/2017/04/internet-censorship-is-advancing-under-trump/
- https://rsf.org/en/news/more-100-websites-blocked-growing-wave-online-censorship

On-line communications are censored at the point of entrance by Internet Service Providers (ISP). They act as gateways to the internet providing these corporations and goverments control over speech by having the ability to restrict usage and track people's usage via their leased IP addresses. In order to make tracking usage much more difficult, tools have come out that provide techniques called onion-/garlic-routing where the source and destinations of internet routes can not be determined without breaking encryption, a very expensive feat, quite impossible today when considering the encryption algorithms used.

Many governments are using IP (Internet Protocol) geo-fencing (e.g. China's Great Firewall) to isolate people from global information and mass surveillance (e.g. the US' NSA Prism and China's Social Credit System) to increase self-censorship. These systems are now being replicated by many other governments worldwide working together to spy on the masses globally (e.g. Five/Fourteen Eyes).

Privacy, the bedrock of freedom, is being lost at an alarming rate and few know how to maintain it today. Most large organizations (e.g. tech giants, the banking industry, governments) track, persist and use our behavior for their profit, not ours. Whistleblowers, the abused, visible minorities, and a myriad of other people could be emboldened by anonymity to speak out in a manner that would otherwise be unavailable if they were forced to identify themselves. Decentralized applications like Bitcoin are helping to wrestle some control from centralized organizations although they are difficult to maintain anonymity at the network layer. Smartphones, our primary means of global communication and collaboration, are weak in maintaining our anonymity and privacy - critical to ensuring individual freedom.

Two primary tools today that support anonymity are Tor and I2P, both internet overlays. Tor provides a browser that makes it easier to use while I2P is much less known. Both are complementary in that Tor was designed for browsing today's current web sites anonymously while I2P was designed for peer-to-peer communications within I2P. Neither have good APIs for developers to embed in their products making uptake slow for many applications.

A third tool on the horizon is one that completely circumvents ISPs by not using them. They're called direct wireless ad-hoc networks and they can communicate directly between personal devices using technologies such as WiFi Direct. Firechat is an example used during the 2014 Hong Kong protests after the Chinese government threatened to shutdown the internet in that area.

Meshing solutions provide access to multiple networks to benefit from each network's strengths but none provide an anonymous mesh. New mesh solutions are popping up that seek to improve on earlier designs. But the technology is still in its infancy and needs to be pulled into ever day applications more easily once they've matured.

Even getting these technologies in wide use doesn't solve the problem of online censorship. Many people are constantly finding ways to circumvent these technologies to censor and steal information.

Tech-savvy people can normally find a way to bypass censorship and maintain privacy, but the overwhelming majority can not thus preventing a critical mass to make positive change on a political level globally. What's needed is to bring censorship resistance and data privacy to this overwhelming majority so that all people are not only able to become free, but that they can remain so.

3 Mission

1M5 is at its core a mission to ensure free speech, expression, association, and assembly. What's our core beliefs that drive us?

- EVERYONE, including criminals and unethical people, has a natural right to Freedom of Speech, Expression, Association, and Assembly
- All relationships must be voluntary
- Privacy is the bedrock of freedom - we should be able to communicate as we please privately - anonymity as a base
- Transparency in code/governance
- We own our data and should be the ones that profit from it
- Self-sovereign identity – people must establish and maintain their own identities, not by 3rd parties
- Self-sovereign money – people must be their own bank indebted to no one with the keys to their money

4 Objectives

What do we try to achieve? Prioritized...

1. Support sharing of and access to information without being censored.
2. Support sharing of and access to information without fear of being persecuted.
3. Support person-to-person/peer-to-peer (P2P) communication without the need to depend on servers nor the internet - The People's Direct Network - cut the cord to ISPs for good.
4. Provide a self-sovereign identification system so that reputation can be established where necessary while the keys are owned and maintained by the individual.
5. When information about a user is desired from a 3rd party (e.g. marketer, government consensus), that information can be sold to the 3rd party by the owner yet with/without personally identifiable information (PII) being transferred by choice.
6. Provide a platform that monetizes itself to ensure sustainability.

5 Solution

The internet was not designed for anonymity, it must be baked into a more open system from the beginning at the lowest of levels to ensure it can be provided under all circumstances.

Provide a decentralized application (Dapp) platform that is fully open-source in the public domain with absolutely no copyright (to avoid states claiming copyright protection), both software and hardware, for decentralized applications that run without depending on servers sharing only what the owner specifically allows while also being created outside of manufacturers influenced by bad actors (e.g. open-source hardware / 3D printing) to ensure privacy while maintaining code and hardware transparency. Targeted hardware for dapps should be recommended based on openness and/or provided by 1M5.

Dapp platform supports a base level of services for running its framework and the minimal services for ensuring mission success. This includes a Sensors Service that provides intelligent routing across anonymity networks. It should be pluggable as new sensors come online. The platform should also support pluggable services for providing additional functionality as dapps require, e.g. a decentralized content distribution network (DCDN).

The identification system will be self-sovereign and reputation based to ensure privacy is maintained while allowing relaxation of privacy incrementally as desired as trust grows. Both machines and people can have identities. Both should be able to use identities anonymously, psuedo-anonymously, selectively, or fully open to everyone (public). Identities can be generated by the platform or brought to the platform as well as the ability to use those identities with other platforms – open standard identity technology will be well supported, e.g. OpenPGP.

Support individuals voluntarily selling parts of their personal information while ensuring it remains secure on their flash drives. If a user loses their device, their new device will be able to restore itself with no loss of data.

Ensure the platform can monetize itself by monetizing resources - network bandwidth, cpu cycles, and persistent storage - through the use of an internal token to represent them. Donations are fine for getting the core on its feet, but long-term sustainability requires self-monetization.

5.1 Context

1M5 works to provide private censorship-resistant communications as a base layer for decentralized applications far and above anything in the marketplace.

5.2 Platform

The platform consists of the components required in support of its censorship-resistance routing service as well as a core set of services each focusing on a different responsibility considered necessary for basic dapp support.

5.2.1 Censorship Resistance Routing

The first layer in a secure highly network-based application must be a layer supporting anonymity. This is accomplished by 1M5's Sensor Service by using I2P (Invisible Internet Project) as the basis for routing over the internet, 1DN (Invisible Direct Network) comprising Radio & LiFi when the internet is not accessible, and Tor for communicating with non-anonymous nodes in the clearnet like Bitcoin nodes. This routing is managed intelligently using a peer graph across all supported anonymous networks.

- **I2P**: an overlay network over the internet using garlic routing to provide anonymity and end-to-end encryption for privacy using a volunteer network of approximately 65k nodes. Garlic routing encrypts multiple messages together using multiple levels of encryption so that each node that performs routing is only aware of the previous node and the next node but no other nodes especially the originating node. Endpoints are cryptographic identifiers (public keys).
- **1DN**: a wireless ad-hoc network as a sensor to provide private communications outside of the internet using WiFi Direct, the full Radio spectrum (Software Defined Radio – SDR), and LiFi (Light Fidelity). As of 2019, LiFi is an emerging technology.
- **Tor**: directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis using onion routing. Primary focus is on private browsing of clearnet sites and providing hidden service sites.

5.2.2 Orchestration

This component provides application orchestration through simple content-based routing (CBR) with support for Enterprise Application Integration (EAI) pattern routing and decentralized algorithms as the code base grows. Current routing uses by default a Dynamic (https://www.enterpriseintegrationpatterns.com/patterns/messaging/DynamicRouter.html) Routing Slip (https://www.enterpriseintegrationpatterns.com/patterns/messaging/RoutingTable.html) implemented as a stack. It's dynamic in that each service can push additional routes onto the stack at any point in the current routing of the message. For example, an end-user may wish to access Service A but when it gets to that service, Service A requires authentication, so Service A adds a call to the Authentication Service and a call back to Service A with the results. Once the results return to Service A, it will perform the service as desired. Other likely examples include data service requests whereby a service needs additional data to satisfy the service request.

5.2.3 Key Ring

Encryption and Signing keys kept safe on specialized flash drives that when added they can not be read nor changed. Encryption and signing happen on-drive only. OpenPGP used for standards support.

5.2.4 DID - Decentralized IDentifier

Self-Sovereign Identity, RepBAC (Reputation Based Access Control), and Circles of Influence. The DID service works with the Key Ring service to provide identity services. Anyone can get on by providing a DID, but can be restricted in what they can do based on reputation. As of mid-2019, only Self-Sovereign Identity is implemented with OpenPGP and only minimally.

Requirements

- Identity through Correlation
    - https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/final-documents/identity-crisis.pdf
- Reputation Based Access Control (RepBAC)
- Identity Recovery
    - Private key sharded, duplicated, & encrypted with random peer disbursement; 12 words used to rebuild key

Self-Sovereign Identity
Provide means for importing, generating, using, and exporting cryptographic identities supporting well known and used standards.

Reputation Based Access Control (RepBAC)
Not to be confused with Role-Based Access Control (RBAC), RepBAC supports users in placing restrictions on access based on reputation parameters.

Circles of Influence
Build groups of identities automatically based on a set of defined reputation parameters. Aids in quickly building groups on known reputation parameters.

5.2.5 Info-Vault

Keeps personal information confidential and available on personal flash drives.

5.2.6 Monetization (Aten & Prana)

Currently, 1M5 is funded by donations, no monetization is in progress. If/when monetization is decided on, we envision it to monetize people's hardware resources (network, CPU, storage) and users' personal information, all on a voluntary basis. Tokens will be used in this network to keep track of usage, just like a utility provider. End users could offer their resources for tokens to others who desire additional resources on-demand or scheduled in the future. They could also exchange tokens with others in the applications to receive additional resources on-demand or scheduled in the future. All transactions would incur a transaction fee to fund development and maintenance of the network based on current approved budget requirements (should be less than 1% if not much lower). Further details are to be expected through future design. Monetization subject to change at any time as the design below is in a very rough draft. Exchanges will be supported using the Komodo DEX.

Prana – User Tokens: These are limited to the end-users' resources brought to the network. They can be used within the 1M5 network of Dapps for services if the Dapp supports it.

Aten – Development Tokens: These are limited to developer (mission and system) hours and/or funds used in building, maintaining, and supporting the network. Percent ownership of Aten tokens out of total outstanding Aten tokens determines the percent of the distributions from the transaction fees. Transaction fees are paid in Prana.

KMD Tokens: Komodo (KMD) tokens are collected when User and/or Development tokens are exchanged with KMD tokens.

5.3 ManCon

1M5 dynamically bypasses attempts to censor communications within application in which 1M5 is implemented. It does so by maneuvering against blocks and attacks on the internet as well as direct mesh networks. This maneuvering experiences varying levels of situational conditions called MANCON.

MANCON is an alert state signalling the maneuvering required to achieve the mission. It can change at any time in response to new conditions arising. The base MANCON recommended for a claimed jurisdiction is largely based on the Press Freedom Index.

End-users can at any time select the MANCON they feel they need to protect their privacy.

5 – Low
No expected censorship or privacy intrusion attempts.

- Web: will use HTTPS. Failures will assume the site is down.
- Tor for .onion addresses
- I2P for .i2p addresses
- I2P is used for peer-to-peer services such as messaging
- No additional latencies

4 – Medium
Typical censorship attempts by states on reading news (public web sites getting blocked, government shutdown of cloud cdn content). No fear of circumventing censorship expected.

- Web: When an HTTPS clearnet site appears down, other nodes will be used to attempt access. If these fail, the site will be assumed to be down.
- All other routing remains unchanged.
- Expect latencies of 500 milliseconds to 2 seconds.

3 – High
Strong censorship attempts are being made with freedom of speech getting little support. Borderline police state is emerging. Potential retaliation for circumvention of censorship attempts. This is the default setting for 1M5.

- Web: will use Tor as default access to clearnet sites. When Tor gets blocked, will use I2P/1DN to route around blocks.
- All other routing remains unchanged.
- Expect latencies of 1-10 seconds.

2 – Very High
Police state emerging. Prison likely for censorship circumvention attempts.

- Web: will use an I2P peer with random delays that has access to Tor to make the request.
- P2P: direct comms with I2P but with random delays up to 90 seconds per I2P relay node.
- Expect latencies of 4 seconds to 3 minutes.

1 – Extreme
Full on police state / dictatorship. Local cellular service towers shutdown. Death likely for censorship circumvention attempts.

- Web: a 1DN peer will be used to access Tor and/or I2P.

- P2P: 1DN peers will be used until a peer with I2P access can route the request.
- Intentional random delays 90 seconds to 5 minutes per 1M5 relay node (up to 90 seconds per I2P relay node) will be used to help protect end-users.
- Expect latencies of 4-30 minutes when in large cities with many 1M5 nodes.

6 Roadmap

- ~~**0.6.0 – Infrastructure**~~
  - ~~0.5.0 – Core: Framework (April 2018)~~
  - ~~0.5.2 – I2P: Embedded Router (July 2018)~~
  - ~~0.5.4 – DID: OpenPGP (Oct 2018)~~
  - ~~0.6.0 – KeyRing: Encrypt/Decrypt (Jan 2019)~~
- **0.7.0 - Censorship Resistance**
  - ~~0.6.1 – Tor: External Router Integration (June 2019)~~
  - 0.6.2 – Sensors: Uncensored Routing (Testing)
  - 0.6.4 – Sensors: Peer Graph (Integration)
  - 0.6.6 – Proxy: Uncensored Browsing (Development)
  - 0.7.0 – KeyRing, InfoVault: External Drives
- **0.8.0 – Sustainability**
  - 0.7.2 – Komodo: Integration
  - 0.7.4 – Prana: Monetization
  - 0.7.6 – Aten: Monetization
  - 08.0 – DID: Reputation
- **0.9.0 – Outernet**
  - 0.8.2 – Radio: WiFi Direct
  - 0.8.4 – Radio: Full Spectrum
  - 0.8.6 – Radio: Blockstream Satellite
  - 0.9.0 – Radio: Electronic Counter Measures (ECM)
- **1.0.0 – Advanced Decentralized Mesh**
  - 0.9.2 – LiFi: Static Host
  - 0.9.4 – LiFi: Mobile Host
  - 1.0.0 – LiFi: Drone Host

7 FAQ

8 Legal

The following general information applies to this document.

8.1 General

This effort is a mission not confined to any jurisdiction as it would risk alienating individuals and providing a vector for attack. This doesn’t mean that others will not attempt to exercise control over it, that is to be expected as free speech is given more lip service world-wide than actual support. No one person speaks for the natural right to free speech, expression, association, and assembly and this mission seeks to uphold that natural right.

8.2 Risks

Decentralized autonomous missions are new efforts having no state supporting them and therefore none of the protections that come along with registering with a state. Each jurisdiction may come up with laws on dealing with these missions or similar efforts in the future. It is the responsibility of each member to handle these relationships as they see best to protect themselves and their families.

8.3 Representation and Warranties

Security is never a guarantee. It is a constant effort for us all to prevent theft by others. Therefore, no warranties can be offered. Know the limitations of the system and use at your own risk.

8.4 Governing Law and Arbitration

This is not an effort specific to any jurisdiction. There will be no internal disputes as this is not an organization of any kind.