The Invisible Internet Project

History

I2P is a project to build, deploy, and maintain a network supporting secure and anonymous communication. The project started in October 2001 as a “desire for instant communication with other Freenet users to talk about Freenet issues, and exchange Freenet keys while still maintaining anonymity, privacy and security.” It was called IIP — the Invisible IRC Project. The Invisible IRC Project was based on the ideals behind another project called The InvisibleNet.

To quote the developer who started the project "I believe most people want this technology so they can express themselves freely. It’s a comfortable feeling when you know you can do that. At the same time we can conquer some of the problems seen within the Internet by changing the way security and privacy is viewed, as well as the extent to what it is valued."

To quote the developer who started the project:

> *I believe most people want this technology so they can express themselves freely. It’s a comfortable feeling when you know you can do that. At the same time we can conquer some of the problems seen within the Internet by changing the way security and privacy is viewed, as well as the extent to what it is valued.*

More information about the history of the project can be found in the blog post 20 Years of Privacy: A Brief History of I2P.

What is the Invisible Internet?

The Invisible Internet is a fully encrypted private network layer that has been developed with privacy and security by design in order to provide protection for your activity, location and your identity.

People using the I2P network are in control of the tradeoffs between anonymity, reliability, bandwidth usage, and latency. There is no central point in the network on which pressure can be exerted to compromise the integrity, security, or anonymity of the system. The network supports dynamic reconfiguration in response to various attacks, and has been designed to make use of additional resources as they become available.

I2P is designed to allow peers using I2P to communicate with each other anonymously. Both sender and recipient are unidentifiable to each other as well as to third parties.

The I2P network is designed for privacy and resilience to censorship

I2P hides the server from the user and the user from the server. All I2P traffic is internal to the I2P network. Traffic inside I2P does not interact with the Internet directly. It is a layer on top of the Internet. It uses encrypted unidirectional tunnels between you and your peers. No one can see where traffic is coming from, where it is going, or what the contents are. Additionally I2P offers resistance to pattern recognition and blocking by censors. Because the network relies on peers to route traffic, location blocking is also reduced.

An essential part of designing, developing, and testing an anonymizing network is to define the threat model. There is no such thing as "true" anonymity, just increasingly expensive costs to identify someone. I2P's intent is to allow people to communicate in environments or situations where protected communication and identity is needed, by providing good anonymity, mixed in with sufficient cover traffic provided by the activity of people who require less anonymity. This way, some users can avoid detection when a personal threat model requires it alongside others with different privacy needs. On the I2P network all of these messages are essentially indistinguishable from the others.

The I2P Software

The Invisible Internet Project provides software to download that connects you to the network. In addition to the network privacy benefits, I2P provides an application layer that allows people to use and create familiar apps for daily use. I2P provides its own unique DNS so that you can self host or mirror content on the network. You can create and own your own platform that you can add to the I2P directory or only invite your friends. The I2P network functions the same way the Internet does. When you download the I2P software, it includes everything you need to connect, share, and create content on the I2P network.

A Brief Technical Overview of the Network

I2P uses cryptography to achieve a variety of properties for the tunnels it builds and the communications it transports. I2P tunnels use transports, NTCP2 and SSU, to hide the nature of the traffic being transported over it. Connections are encrypted from router-to-router, and from client-to-client(end-to-end). Forward-secrecy is provided for all connections. Because I2P is cryptographically addressed, I2P addresses are self-authenticating and only belong to the user who generated them.

I2P is a secure and traffic protecting Internet-like layer. The network is made up of peers ("routers") and unidirectional inbound and outbound virtual tunnels. Routers communicate with each other using protocols built on existing transport mechanisms (TCP, UDP, etc), passing messages. Client applications have their own cryptographic identifier ("Destination") which enables it to send and receive messages. These clients can connect to any router and authorize the temporary allocation ("lease") of some tunnels that will be used for sending and receiving messages through the network. I2P has its own internal network database (using a modification of the Kademlia DHT) for distributing routing and contact information securely.

About Decentralization and I2P

The I2P network is almost completely decentralized, with exception to what are called "Reseed Servers," which is how you first join the network. This is to deal with the DHT (Distributed Hash Table) bootstrap problem. Basically, there's not a good and reliable way to get out of running at least one permanent bootstrap node that non-network users can find to get started. Once you're connected to the network, you only discover peers by building "exploratory" tunnels, but to make your initial connection, you need to get a peer set from somewhere. The reseed servers, which you can see listed on http://127.0.0.1:7657/configreseed in the Java I2P router, provide you with those peers. You then connect to them with the I2P router until you find one who you can reach and build exploratory tunnels through. Reseed servers can tell that you bootstrapped from them, but nothing else about your traffic on the I2P network.

I2P is Peer-to-Peer

You will see IP addresses of other I2P nodes in the software router console. This is how a fully distributed peer-to-peer network works. Every node participates in routing packets for others, so your IP address must be known to establish connections. While the fact that your computer runs I2P is public, nobody can see your activities in it. You can't say if a user behind this IP address is sharing files, hosting a website, doing research or just running a node to contribute bandwidth to the project.

What I2P Does Not Do

The I2P network does not officially "Exit" traffic. It has outproxies to the Internet run by volunteers, which are centralized services. I2P is primarily a hidden service network and outproxying is not an official function, nor is it advised. The privacy benefits you get from participating in the the I2P network come from remaining in the network and not accessing the internet. I2P recommends that you use Tor Browser or a trusted VPN when you want to browse the Internet privately.

I2P is Free Open Source

The entire system is open source. The router and most of the SDK (software development kit) are public domain with some BSD and Cryptix licensed code. Some applications like I2PTunnel and I2PSnark are GPL. Almost everything is written in Java (1.5+), though some third party applications are being written in Python and other languages. The code works on Sun Java SE and other Java Virtual Machines.

View the project on Gitlab.

For more in-depth information about the network, its protocols and encryption methods, please see the I2P Technical Docs.