Resources

General Topics

Introduction

Learn about I2P and how to get started

Using I2P Software

Learn how to use I2P software

Support

News, updates, and release notes

Contributor Guides

For contributors and volunteers

Developer Resources

Developer guidelines and applications

Research

Academic papers and peer reviews

Advanced Connections

I2P Software

Tagline goes here

I2P Network

Tagline goes here

Resources

General Topics

Introduction

Learn about I2P and how to get started

Using I2P Software

Learn how to use I2P software

Support

News, updates, and release notes

Get Involved

Contributor Guides

For contributors and volunteers

Developer Resources

Developer guidelines and applications

Research

Academic papers and peer reviews

Advanced Connections

I2P Software

Tagline goes here

I2P Network

Tagline goes here

Resources > Introduction

Version 1. Separate pages organized under sub-categories

Overview

What is I2P?
How to Get Started
What I2P Does Not Do
Tour I2P Software
Privacy & Safety
Uninstalling

Comparisons

There are a great many other applications and projects working on anonymous communication and I2P has been inspired by much of their efforts. This is not a comprehensive list of anonymity resources - both freehaven's Anonymity Bibliography and GNUnet's related projects serve that purpose well. That said, a few systems stand out for further comparison.

Tor / Onion Routing
Freenet
Other Networks

Extras

How to Connect to the I2P Network
About Decentralization and I2P
Peer to Peer
Licenses

Resources > Introduction

Version 2.
Separate pages

- What is I2P?
- How to Get Started
- Privacy & Safety
- Comparisons with Tor, Freenet
- Licenses
- Uninstalling

Version 3. One page with all the info and anchor links.

Introduction

What is I2P?

The Invisible Internet Project (I2P) 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. The software ships with a router that connects you to the network and applications for sharing, communicating and building.

I2P Cares About Privacy

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.

How to Connect to the I2P Network

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 privately.

An 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.

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.

Comparisons

There are a great many other applications and projects working on anonymous communication and I2P has been inspired by much of their efforts. This is not a comprehensive list of anonymity resources - both freehaven's Anonymity Bibliography and GNUnet's related projects serve that purpose well. That said, a few systems stand out for further comparison. The following have individual comparison pages:

- Tor / Onion Routing
- Freenet

The following are discussed on the other networks page:

- RetroShare
- Morphmix / Tarzan
- Mixminion / Mixmaster
- JAP
- MUTE / AntsP2P
- Haystack

Version 4. One page with all the info and sidebar with anchor links.

What is I2P?

The Invisible Internet Project (I2P) is a fully encrypted private network layer that has been developed wi
security by design in order to provide protection for your activity, location and your identity. The software
router that connects you to the network and applications for sharing, communicating and building.

I2P Cares About Privacy

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.

How to Connect to the I2P Network

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 privately.

An 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.

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.

Comparisons

There are a great many other applications and projects working on anonymous communication and I2P has been inspired by much of their efforts. This is not a comprehensive list of anonymity resources - both freehaven's Anonymity Bibliography and GNUnet's related projects serve that purpose well. That said, a few systems stand out for further comparison. The following have individual comparison pages:

- Tor / Onion Routing
- Freenet

The following are discussed on the other networks page:

- RetroShare
- Morphmix / Tarzan
- Mixminion / Mixmaster
- JAP
- MUTE / AntsP2P
- Haystack

What is Included

This section is quite long (https://geti2p.net/en/about/software) *might need its own page for it. Or condense the information for this section and offer more details elsewhere.*

Tour I2P Software

Click here to see more of I2P and how it works and how you can use it. (Or embed a video here)

Getting Started

There are 3 basic steps to getting started: download, install, and configure. Follow those steps and instructions at the Getting Started page. It will walk you through choosing your operating system for the download(s) required. You'll then follow the step-by-step installation instructions for getting it running and opening I2P software. Finally, you will configure your browser. You can also continue to learn more about how to use I2P here.

Installing Java

There are three operating systems that require Java: Mac, Windows, and Linux. If you are downloading I2P, you must download and install Java first. You can follow instructions for how to install Java here.

Advanced Connections

What is I2P?

The Invisible Internet Project (I2P) 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. The software ships with a router that connects you to the network and applications for sharing, communicating and building.

I2P Cares About Privacy

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.

How to Connect to the I2P Network

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 privately.

An 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.

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.

Comparisons

There are a great many other applications and projects working on anonymous communication and I2P has been inspired by much of their efforts. This is not a comprehensive list of anonymity resources - both freehaven's Anonymity Bibliography and GNUnet's related projects serve that purpose well. That said, a few systems stand out for further comparison. The following have individual comparison pages:

- Tor / Onion Routing
- Freenet

The following are discussed on the other networks page:

- RetroShare
- Morphmix / Tarzan
- Mixminion / Mixmaster