
{inc}ognito
I2P Product
Whitepaper

Overview

{inc}ognito is a recently launched decentralized crypto currency project based on CryptoNote / Monero (private, secure, untraceable and fungible). The key differentiator of {inc}ognito is that it will introduce an enhanced anonymity layer though I2P to enhance the privacy and security of users.

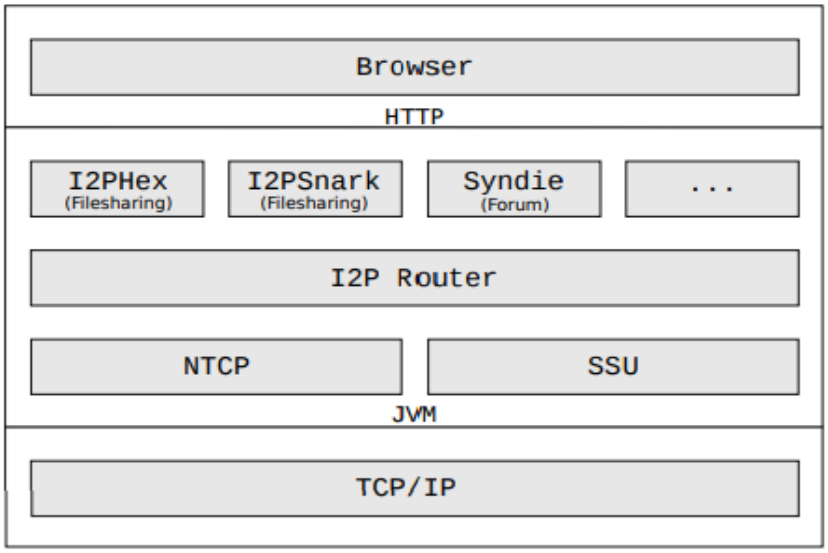
I2P – what is it?

Invisible Internet Project or I2P is a network within an anonymous layer, allowing protected communication free from surveillance and external monitoring. I2P is widely used by people who need complete privacy for their online communication such as journalists, whistle blowers, and activists. It was launched in early 2000 by a group of open source developers with the intention of protecting online communication from surveillance by Government or any other external parties.

Since its launch, I2P has found uses in many different avenues such as emails, websites browsing, blogging and especially across the darknet where people prefer using I2P with its garlic routing over Tor's onion routing. While onion routing transmits a single message as it passes through the network, garlic routing messages are sent encrypted, which are called cloves, breaking off as they reach multiple destinations.

In short, I2P achieves a higher level of anonymity than alternatives such as Tor, because of its garlic routing, decentralised setup and unilateral tunnels.

Diagram



I2P is a multi-application framework for anonymous P2P networking written in Java. On top of the native Internet protocol, I2P specifies the use of two different peer-to-peer transport protocols. The first is called NIO-based TCP (NTCP), where NIO refers to the Java New I/O library. The second is called Secure Semi-reliable UDP (SSU), providing UDP-based message transfer.

Illustration Reference: Michael Herrmann and Christian Grothof
https://www.freehaven.net/anonbib/papers/pets2011/p9-herrmann.pdf

Why incorporate I2P into {inc}ognito?

Security and privacy issues are a major concern for cryptocurrency users and increasingly, news of hacking and theft in vulnerable wallets is worrying. Users of common cryptocurrencies like bitcoin are now seeking more privacy and are moving to alternative privacy focused coins. {inc}ognito aims to address these users through releasing I2P, as one of several key development releases over 2018.

Extra layer of privacy

While CryptoNote/Monero is a leading privacy coin, there is merit in providing an additional layer of protection through I2P ensuring {inc}ognito complete anonymity.

Anonymity will strengthen as the network grows, scaling over time across devices including desktops, mobile and embedded systems. Cryptographic identifiers will ensure the sender and recipients using {inc}ognito will remain anonymous.

Four layer encryption

Four-layer encryption and unilateral tunnel architecture will ensure that time attacks on {inc}ognito are extremely difficult. Typically in a timing attack, the eavesdropper or attacker will monitor the outbound tunnel or exit nodes for traffic, trying to 'time' certain messages while looking for patterns. Due to the strong tunnel encryption in I2P and because users can customize duration and length of a tunnel, the attacker or eavesdropper will have difficulty generating timing patterns. Unilateral proxy tunnels will also increase the efficacy.

Another possible threat is the 'man-in-the-middle' attack where an attacker poses as an authentic receiver trying to decrypt messages before transferring to the subsequent destination. However, I2P's garlic routing is a much stronger defence against this type of attack, as it is much more challenging to decrypt than the onion routing of Tor network.

References & further reading

{1} *The Onion Name System: Tor-powered Decentralized DNS for Tor Onion Services* by Jesse Victors, Ming Li, and Xinwen Fu.

{2} *In Proceedings on Privacy Enhancing Technologies* 2017(1), January 2017

{3} *A Path-Hidden Lightweight Anonymity Protocol at Network Layer* by Chen Chen and Adrian Perrig.

{4} *In Proceedings on Privacy Enhancing Technologies* 2017(1), January 2017

{5} Kubieziel, J. *To Be or I2P: An introduction into anonymous communication with I2P*. Lecture at 24C3 (2007).

{6} *The Waterfall of Liberty: Decoy Routing Circumvention that Resists Routing Attacks* by Milad Nasr, Hadi Zolfaghari, and Amir Houmansadr.

{7} *Effects of Shared Bandwidth on Anonymity of the I2P Network Users* by Khalid Shahbar and A. Nur Zincir-Heywood

{8} *Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study using I2P* by Michael Herrmann and Christian Grothof

{9} *The Dark side of I2P, a forensic analysis case study* by Wilson Bazli and Hurst

{10} *Analysis of the I2P Network - Information Gathering and Attack Evaluations* by Jens Müller.

{11} *Defending Eclipse Attack in I2P using Structured Overlay Network* by Hasib Vhora and Girish Khilari

{12} *The Invisible Internet Project: Cryptograph*

{13} *The Invisible Internet Project: Tor / Onion Routing*