I2P Research

Background and Context

Based on Q&A with idk and Sadie

Why I2P Exists

I know that there is need for I2P because the fact that exists is due to a reaction.

It was/is a solution people saw need for with more surveillance, government and big tech overreach and censorship possibilities and realities.

Interviews with original dev: http://invisibleip.sourceforge.net/iip/mediaDCInterview1.php

Basically it was 2 things : one was a better version of Freenet, and the other was the fallout from 911 and how that started roots for enhanced surveillance and profiling.

Technically it was supposed an obfuscated onion-routed transport for Freenet at one point, but the two projects sort of diverged too far to be rejoined and now they're fundamentally very different.

What Users Can Do on I2P

The I2P network allows you to do most things that you can do on the internet.

For any casual user (like me) I can use the apps that ship with the software to torrent content, or I can use email, or use the static webpage to build my own small site.

For devs, the sky is the limit- make apps, SSH, create more robust sites, host forums, and more.

What is missing from the Product is this story - clearly showing what the software allows a person using it to do.

For journalists, yes, using nyms and keeping their traffic / activities confined to the i2P network would be the best for risk management. They could use email, torrents, and even host private non-discoverable sites if they wanted.

Improving the Website

I'd like it if the website facilitated **more sucessful use of I2P, i.e. more users, happier, more comfortable users.**

Honour the 20 years of work by creating **better onboarding funnels for new users, new contributors (maintainers), new devs** who want to build out the application ecosystem, and the next generation of protocol and network researchers and builders. So **product definition and happier users, and clear paths to info** for our creatives, devs, researchers. Also, **clear use cases** since that is not present.

It should be **more engaging** too. There is a rich history of humans making things here with care and thought for people who want or need this technology. That aspect and communication should be realized in a way that makes a more tactile experience for new users and existing community.

Measuring Success

- When people start asking different questions on forums. There are a few common ones that may indicate that our docs are not visible in straight forward way.
- When I stop hearing that people cannot find things
- When doing marketing is easier because I have a product to point too and more engaging docs and processes to share
- When we see more downloads
- Maybe more mac users

What We Know So Far

Overall, I2P users are privacy maximalists. Giving them a survey is hard because they are distrustful of Google forms (survey on I2P?)

Can be hard to get access to certain users for interviews because of sensitive privacy nature.

Quality of data not great. Technical vs user conflict. New user is intimidated by website. Whereas Linux people love obscure tech and want more configuration!

Tor is not a competitor, it’s just different. They should be complementary.

Research Goals and Questions

Research Goals

Define the personas

Figure out typical use cases and user stories

Improve the new user download/onboarding process and experience (priority)

Improve contributor experience

Improve developer experience

Questions We Have

- If we conducted interviews, do we want to talk to people that already use I2P or not?
- What types of threat surfaces do users face? What are they most concerned about?
- Why would someone be looking at I2P? What brought them there?
- Talk to people that care about “privacy.” What does privacy mean?
- How does a new user navigate the download and installation process? What is their experience like?
- What is the contributor’s and developer’s experience like?

Regarding user research - **if there was a way to conduct some interviews with specific groups in order to get their feedback on the software and to get an idea of where it fits or does not fit certain threat surfaces**, that would be wonderful

Threat surfaces: things that people need to be concerned about - like specific people or groups that may target their data, instances where local governments may actually seize hard drives, also, emotional/anxiety aspects of doing certain work

I2P may not be a great fit for people who are on the move or need immediate communication. For a person who has time, it may be a great option if you are collecting and sharing data with other I2P users.

Types of Users

New User
Retention supporting docs (Getting Started and Troubleshooting, Community Links)

Contributor Onboarding
Translators, Reseed Operators, Network Support (Mirror operators, etc)

Dev Onboarding
Application Builders, Network / Cryptographers

Researchers

Onboarding new users / adoption is the priority. People need to have a proper intro in order to take interest in contributing to the project I think.

New users would be people who have some sort of knowledge of privacy tools. As for specific groups (i.e., journalists or activists) I do not feel that creating onboarding for specific use cases is a thing we can do without finding out if either of those groups

1. use I2P so we can talk to them and how they do risk assessment.

2. understand their environment and security or connection ability.

3. think it is a good idea at all to create specific personas. I feel conflicted about saying "use I2P if you are this person" since it an easy way for bad actors to more easily target specific people.

So in the end, it is maybe more about **providing robust and clear product info and letting people figure out their use case** beyond some simple things that we can provide. Like we can say "get your friends to join I2P and create your own secret sharing circle!" But I would not really feel comfortable saying "are you an activist - use I2P" since I cannot also provide proper security advice if that is needed.

I think that there is an opportunity here to do some research though for the needs of journalists, maybe do some user testing with them.

The other thing I did not mention is that **the more mundane user traffic, the better**. it adds to everyone's traffic protection.

Metrics / Demographics

https://i2p-metrics.np-tokumei.net/overview

Most users in the US, followed by Russia, UK.

User Stories & Use Cases

Based off past research

Pulled from Github UX

User Story: A small org activist group

- They are global
- They need to have same communication and file sharing but have not much funding to invest in or maintain infrastructure.
- For email they could use Bote to ensure secure email
- They can use snark for file sharing
- They can host a private irc or forum as a service for invite only.

In this way I2P can be used as secure communication infra for org that wish to lock down some or all of their work to minimize spam, phishing, or a centralized service being shut down or hacked.

A better social media

- I want to start a small forum where my friends and i can post pics, chat without it being public.

- I do not want to use a platform that encourages gamification or allows people to randomly join

- I want it to be a trusted invite only space where people feel safe and can collaborate and share

- I want it to not be dependent on a corporation that can shut it down or collect our data or make members use phone numbers to create an account.

A private service on I2P with a non public b32 address that is only shared when a new person is invited to join.

For Journalists - Scope & Considerations

Some good points raised here, https://internews.org/blog/charting-the-security-needs-of-central-european-journalists/ highlighting some :

- What are the basics of digital security?
- What are high risk or low risk security strategies?
- Interesting to think about if as the article suggests that some journalists do not consider themselves high risk targets for hackers, etc due to what they cover, but often they are simply due to this reduced security posture. In this case an attacker can gain access to other assets through this target.
- Workflows and organizational security strategies
- Journalists often work under tight deadlines and rarely have the luxury of time for self-study or to tweak their workflows. As one interviewee explained, “I’m a busy parent, and a journalist. So, I have to choose between cooking and learning about security, and cooking always wins.”

Proto-personas

https://www.hyperakt.com/insights/proto-personas

Who is this individual? Write a short description about this individual. Keep it simple:
I'm somebody that cares about privacy and is curious about private internet. VPNs and other apps like ProtonMail, Signal, DuckDuckGo, and private browsers are not enough.

Why would they want to engage with your work? What might their goals and aspirations be?
I want to feel safer on the internet. I don't want to be tracked or identified. I may not like my data being used for monetization purposes. I may be based in a country that has firewalls and/or censorship. I want to participate in a space where I can do connect with people doing basic activities like emailing, blogging, and file sharing.

What obstacles and challenges might they face?
I am not knowledgable in technical concepts that comes with more advanced privacy tools, such as I2P. I don't know the difference between I2P, Tor, Freenet and which one to choose. I don't know if I2P is right for me.

Who is this individual? Write a short description about this individual. Keep it simple:

Why would they want to engage with your work? What might their goals and aspirations be?

What obstacles and challenges might they face?