DIVA.EXCHANGE

Major Changes of the Peer-to-Peer Network

Cryptography of I2P Received a Major Update:
an Overview of the Changes in 2022

Author: Konrad Bächler
Twitter: @DigitalValueX, Web: https://diva.exchange

About diva.exchange

- Non profit association, open to everyone
- A loose bunch of Devs & Researchers - spread all over the world
- «DIVA - Free Banking Technology for Everyone» means: handle all kind of Digital Values under your own control and responsibility and apply your very own philosophy of privacy without being nudged by others
- No centralized business model (pointless); no token/coin.

Agenda

- Short introduction: the I2P network
- Overview of the latest changes
- Focus on the impact of the changes
- Summary and take-outs
- One or two questions

Git repos to fork

I2P: role of diva.exchange

- I2Pd **docker image** maintainer, https://hub.docker.com/u/divax
- One of the official I2P **reseed server** operators, https://reseed.diva.exchange
- I2P application developer, **DIVA software stack**, https://github.com/diva-exchange
- **I2P SAM Library developer** https://www.npmjs.com/package/@diva.exchange/i2p-sam
- **Research cooperations** with academia (mainly Swiss Universities), see some of the videos https://odysee.com/@diva.exchange:d/

Hello I2P Network

- A few basic facts (some are simplified - educational reasons):
  - I2P is an overlay network (misleading name «darknet» is just used by dubious media desperately in need for clicks)
  - It's a peer-to-peer network where every node in the network acts as a router
  - I2P itself has no storage capabilities – it is a transport layer
  - Messages travelling through the network are multiple times encrypted (like a garlic: it has multiple layers) – call it «Confidentiality feature»
  - Messages hop over several routers within the network to their final destination (using «tunnels») – call it «Anonymity feature»
- In a nutshell: I2P = confidential & anonymous message transport

Git repos to fork

Hello I2P Network (2)

- How to get I2P? Three reasonable possibilities:
  - Linux Repos (like Debian repo – probably not the latest version though)
    Project Repos (up-to-date): https://deb.i2p2.de/ and https://repo.i2pd.xyz/
    PPAs: https://launchpad.net/~i2p-maintainers/+archive/ubuntu/i2p/+packages and https://launchpad.net/~purplei2p/+archive/ubuntu/i2pd/+packages
  - https://geti2p.net/ or https://i2pd.website/ (download points to github)
  - Container: https://hub.docker.com/search?q=i2p (use only «SPONSORED OSS» I2P/I2Pd images)
- Why I2P and I2Pd? In short:
  I2P = written in Java with User Interface
  I2Pd = written in C++, daemon only (lean, for «admins»)
  Both are equally valid.
- How do I create my I2Pd binaries since years? Github → build from source → publishing to https://hub.docker.com/u/divax
- ***Warning***: **don't trust any binary-only-stuff** in such a sensitive area. Fact: «no complete source code / no simple local reproducability = stay away!»

Latest Changes / Goals (1)

- I2P supports TCP and UDP on the transport layer
- Simplified: TCP is called NTCP2 (2018) and UDP is called SSU (2005) and SSU2 (2022)
  - UDP/SSU has been modernized and now it's called **SSU2**
  - It's all based on the noise protocol (noiseprotocol.org) and heavily borrowed from WireGuard VPN and QUIC (RFC 9000, 9001 and 9002)
  - Cryptography: Curve25519, RFC 8439

Latest Changes / Goals (2)

- It is all about the transformation from SSU to SSU2
- Motivation: UDP has large performance advantages in **truly and fully** distributed networks.
- Therefore, the major changes focus on UDP:
  - Upgrade of the Cryptography
  - Improve efficiency: CPU, bandwidth, etc.
  - Improve censorship-resistance (aka «obfuscation»)
  - Improve DoS-Attack-Resistance (UDP is vulnerable)

Impact of the Changes (1)

- Challenges of UDP:
  - Message fragmentation
  - Security issues, like address spoofing
- Solutions, provided by SSU2:
  - Strong DoS resistance (token concept)
  - Header encryption: improve obfuscation and increase resistance against pattern recognition
  - Better handling, if peers change their address
  - … and some more (see links at the end for details)

Impact of the Changes (2)

- Performance - estimated improvements for SSU2 vs. SSU:
  - 40% reduction in total handshake packet size
  - 50% or more reduction in handshake CPU
  - 90% or more reduction in ACK overhead
  - 50% reduction in packet fragmentation
  - 10% reduction in data phase overhead

Impact on diva.exchange

- DIVA testnet, based on divachain, https://testnet.diva.exchange:
  - The testnet is more stable
  - It is significantly faster
  - And «gossiping» is more reliable

Summary and Take Outs

- I2P is the leading fully distributed network suitable for a wide range of privacy-by-design-applications
- I2P got even faster and stronger with the latest update
- Get involved today and support privacy-by-design networks and applications

Sources

- 2022 Changes, blog post: https://geti2p.net/en/blog/post/2022/10/11/SSU2-Transport
- Container / Docker images, including documentation: https://hub.docker.com/u/divax
- I2P Research (like de-anonymization approaches): https://github.com/diva-exchange/academia
- Latest release notes (I2P 2.1, java version): https://geti2p.net/en/blog/post/2023/01/09/2.1.0-Release

DIVA.EXCHANGE

Discussion / Links

Web: https://diva.exchange/

Twitter: @DigitalValueX

Mastodon: @social@social.diva.exchange

Telegram Group: https://t.me/diva_exchange_chat_de

Source Code (AGPL3 or better; Apache 2.0) &
Research/Academia: https://github.com/diva-exchange

I2P & Docs: https://geti2p.net