Easy, secure and private data transfer with Magic Wormhole

Ramakrishnan Muthukrishnan

Hi, I am Ram

- Long time free software user and programmer.
- Long time FSF associate member (membership #255).
- Work for Least Authority, which is based in Berlin that focus on security and privacy related projects.
- Have bits and pieces of code contributed to various free software projects like the Debian project, Linux kernel, GNU Emacs and GNU Radio.
- Loves tinkering with electronics and radios - Ham radio callsign VU3RDD.
- Lives in Bangalore, India.

File Transfer

Isn’t this a solved problem?

https://xkcd.com/949/

File Transfer problems

Even in 2022, transferring files from one computer to another computer is “hard”.

- File size limitations.
- Picture quality compromised to reduce size by messaging service providers.
- Slow speed of transfer.
- Not very easy to use.
- Privacy concerns.
- Security Concerns.
- Peer needs the same (often proprietary) application.
- Unreliable.

Magic Wormhole

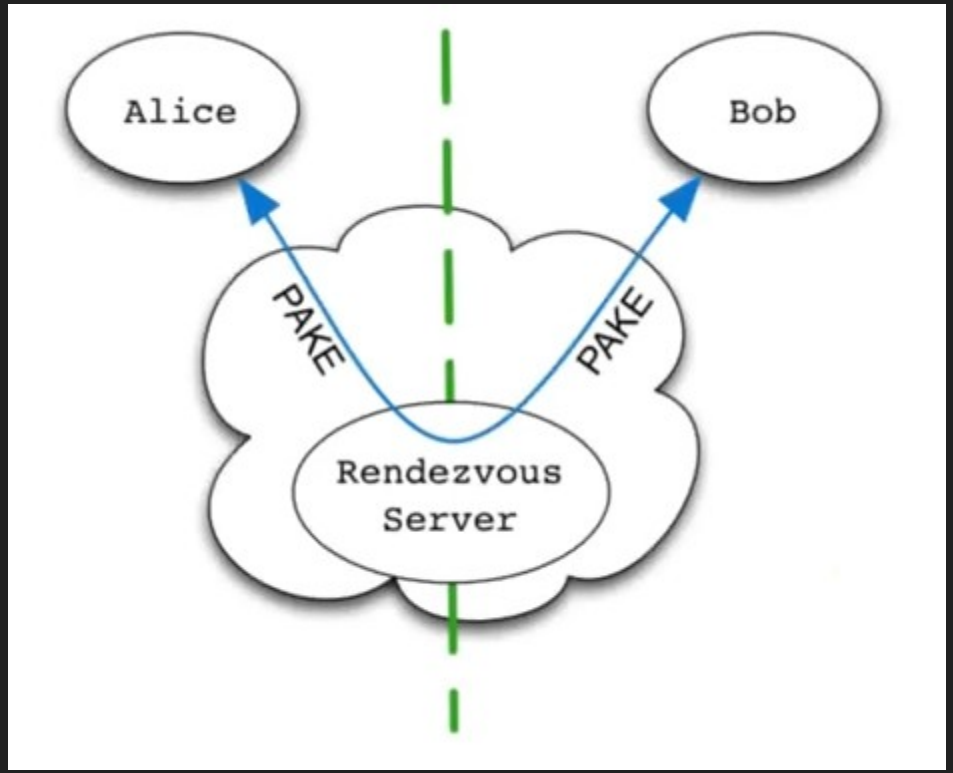
- protocol created by Brian Warner that allows secure file/directory transfer between computers.
- Available as a command line program. Available in most GNU/Linux distributions.
- Multiple implementations of the protocol in different programming languages (Python, Go, Rust, Haskell).
- A few Graphical programs are available as well.
- A few mobile phone clients.
- Various Magic Wormhole related info is under this URL: https://github.com/magic-wormhole/

Features

- Anonymous
  - no need for any user accounts.
  - no need to ask other party's user name, email address or IP address.
  - a short one-time code consisting of English words and a numeral is used for the transfer. (eg: `4-purple-sausages`)
- Connections
  - direct connection between peers when possible.
  - connection via a transit relay server when direct connections are not possible.
  - transfers over Tor supported for greater anonymity.
- Data transfers
  - data that leaves the computer is fully encrypted.
  - no data saved in the cloud.
  - synchronous transfer, so both the parties need to be online during the transfer.

Demo

4-purple-sausages



* Diagram from Brian Warner’s presentation at PyCon 2016.

PAKE

P - Password

A - Authenticated

K - Key

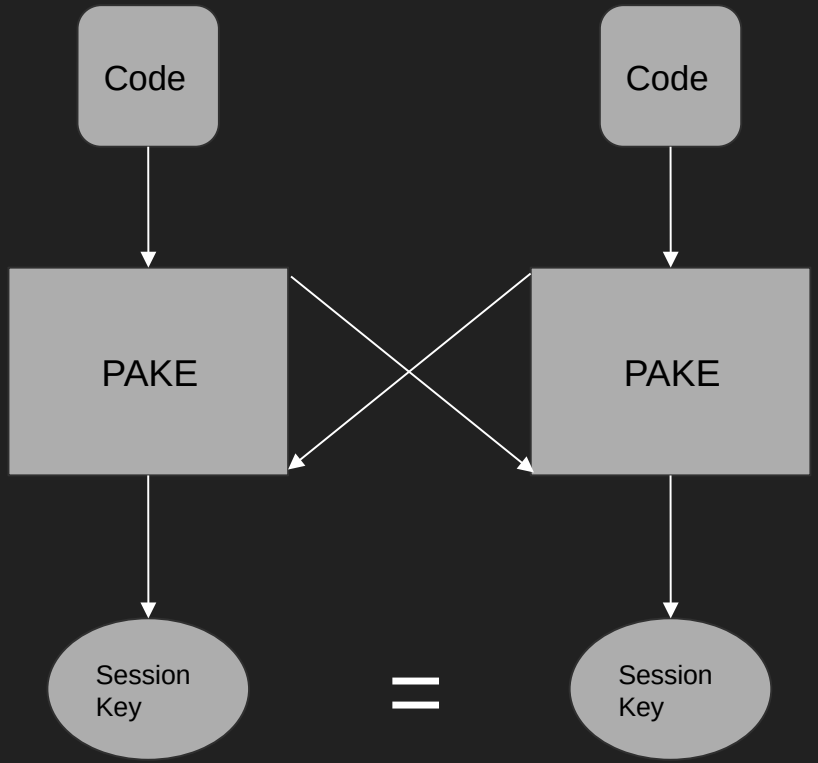
E - Exchange

PAKE based protocols are designed to be secure even though users choose a short password.

Both the parties compute the same resulting high entropy session-key from a low-entropy password.

SPAKE2 (a version of “Balanced PAKE – i.e. the two parties use the same password to authenticate a shared session key) used by magic-wormhole uses an algorithm from Abdalla and Pointcheval.

PAKE



Transit Protocol

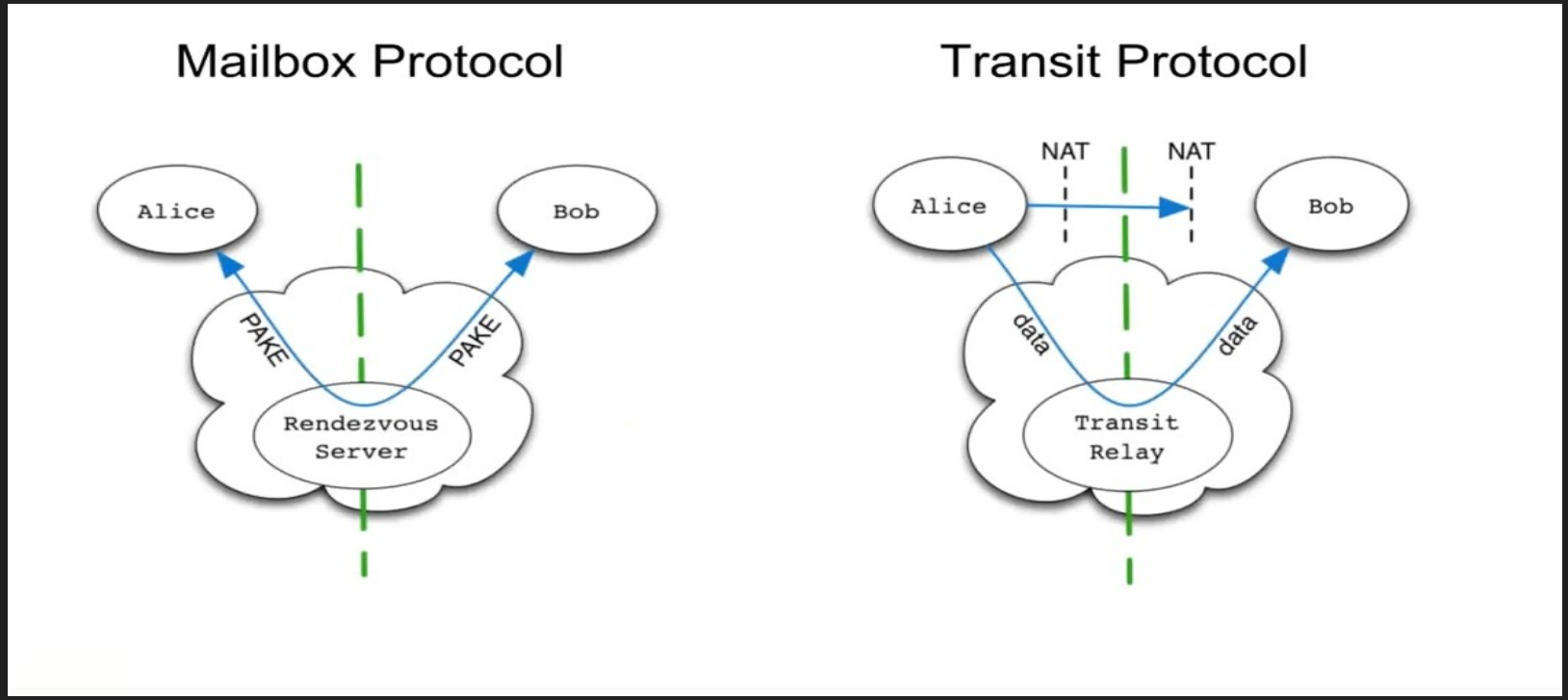


Diagram from Brian Warner’s presentation at PyCon 2016.

Ongoing work

- Availability of clients on more platforms (Desktop and Android)
- Bringing magic-wormhole to the web
  - Cross compile the Go implementation of magic-wormhole protocol to web assembly
  - Websocket support for the transit relay server instead of TCP in order to run the client on a web browser.
  - User friendly browser UI.
  - Improve scalability of the backend.
- Mechanisms for long time association between two devices.
- Dilated wormhole
  - durable connections: file transfers can resume after network disruptions.
  - multiplexed TCP connection.
  - bidirectional initiation.

Resources

- Github Magic wormhole organization: https://github.com/magic-wormhole
- SPAKE2 Algorithm Paper: https://www.di.ens.fr/~mabdalla/papers/AbPo05a-letter.pdf
- Protocol docs: https://magic-wormhole.readthedocs.io/en/latest/index.html
- Python client: https://github.com/magic-wormhole/magic-wormhole
- Rendezvous Server source code: https://github.com/magic-wormhole/magic-wormhole-mailbox-server
- Transit Relay server source code: https://github.com/magic-wormhole/magic-wormhole-transit-relay
- Haskell client source code: https://github.com/LeastAuthority/haskell-magic-wormhole
- Rust client source code: https://github.com/magic-wormhole/magic-wormhole.rs
- Command line Client in Go: https://github.com/psanford/wormhole-william
- Android application: https://github.com/psanford/wormhole-william-mobile
- GUI program: https://github.com/Jacalz/rymdport
- Least Authority's ongoing work on Magic Wormhole: https://leastauthority.com/blog/tag/magic-wormhole/

Questions?

Contact Info

- Email: ram@rkrishnan.org
- Mastodon: https://mastodon.radio/@vu3rdd
- Website: https://rkrishnan.org
- Github: https://github.com/vu3rdd