“Magic Wormhole -Simple Secure File Transfer”

- Briyan Warner

Securitely moves a file from one computer to another

Easier than all other tools,especially for moving to an unrelated computer

using the command “ pip install magic-wormwhole” you can install it

STEPS

1. Rendezvous message exchange
2. PAKE , key agreement
3. IP address exchange
4. Transit connection
5. Data transfer

Rendezvous Message Exchange

- Two machines find out each other and start exchaning messages
- client exchange messages through the rendezvous server

PAKE

- PAKE means password authentificate key exchange
- PAKE accepts the wormhole code and return the session key. If the these session keys are equal they will start transmitting the data

Wormhole code

- These codes are generated using PGP word list
- There are 256 words in this you can choose 2 words
- so there are 65536 possible codes,equaly likely

IP Address Exchange

- Find IP addresss with ifconfig
- Listen on the TCP ports
- Exchange address+ports
- Try to connect, Trade encrpyted handshake
- First sucessful connction wins

Transist Connection

- Once that handshake is completed the file send through encrypted record pipe
- Data is hashed during the transist
- Final Ack confirms the hash

Data Transfer

- In magic wormwhole screen it show the percenyage level of data transfer
- Finally the reciver confirms all data are recived

"In future it will use GUI application for magic-wormwhole and also add it as a browser extension. It will be port to other languages like JavaScript ,Go and Rust"

Reference

- For codes magic-wormwhole.io
- For video https://www.youtube.com/watch?v=oFrTqQw0_3c