Brian Warner - Magic Wormhole- Simple Secure File Transfer - PyCon 2016

At Pycon 2016 in Portland, Oregon, Brian Warner , who created Buildbot and one of the developers of the Tahoe – LAFS distributed data store gave a presentation about his most recent project: **Magic Wormhole**. It is a way to securely transfer files over an encrypted channel.

Magic Wormhole is a file-transfer program, though it can also be used to transfer simple strings or directories. Over the years, people have been using SSH, email, or shared directories for transferring files, but he claim Magic Wormhole is easier than other security tools especially for moving to an unrelated computers.

The package can be installed using the command "pip install magic-wormhole".The sender then simply does a "wormhole send file name"which prepares to send the file and provides a code that
is used by the receiver. That code is transmitted to the receiver via some other mechanism (e.g. over the phone); the receiver runs "wormhole receive", types in the code, and the file is transferred.The code is a way to "make two computers meet each other", once the humans using them have met through some means.

File transfer may seem like a solved problem , but he likes to characterize the solutions by both their safety from eavesdroppers and the amount of data that a sender or receiver needs in order to do the transfer.

Magic Wormhole has a few different phases that it steps through to handle the transfer. It starts with a "rendezvous message" exchange using a central rendezvous server. That establishes the channel that will be used for the transfer, which is identified by a channel ID that is the number at the beginning of the code. Then it uses password authenticated key exchange (PAKE) to agree on keys. After that, IP addresses are exchanged between the endpoints, an encrypted transit connection is made, and the data is transferred. Once that happens, the channel is closed, so only one transfer to one other endpoint is done; other transfers require new channels and codes.

There is a rendezvous server that he runs, which doesn't participate in the transfer, but just facilitates finding the other endpoint and establishing a key by passing messages between the endpoints using a given channel ID.The magic wormhole uses SPAKE2 PAKE protocol. He has written a pure-Python implementation of SPAKE2 using the Ed25519 elliptic curve that is quite fast. The idea behind PAKE is that a weak secret coupled with interaction (message exchange) can produce a strong secret (the session key).

The local IP address is discovered using ifconfig, then a listening connection is set up. Both sides exchange their address and port number and, once they have received that information, try to connect with the other side to trade encrypted handshakes. The first successful connection is the one that gets used. The data is encrypted using libsodium with the crypto_secretbox interface, which uses the Salsa20 stream cipher and the Poly1305 message-authentication code (MAC). The data is also hashed using SHA256 and the final ACK confirms the hash value.
Magic Wormhole has a library API that can be used to programmatically exchange data using the system. In the future, he would like to add a GUI application and a browser extension to make it easier to use.

Magic wormhole can be used anywhere there is a need to deliver a credential or to get a key from one application to another.In addition, messaging applications could use it to exchange keys directly between participants. Rather than having Alice upload her public key to a server and requiring Bob to get it from there, Alice could just provide Bob with a Wormhole code and he can retrieve it directly from her system. But the real reason behind building the tool is to get more developers to add PAKE to their toolbox.