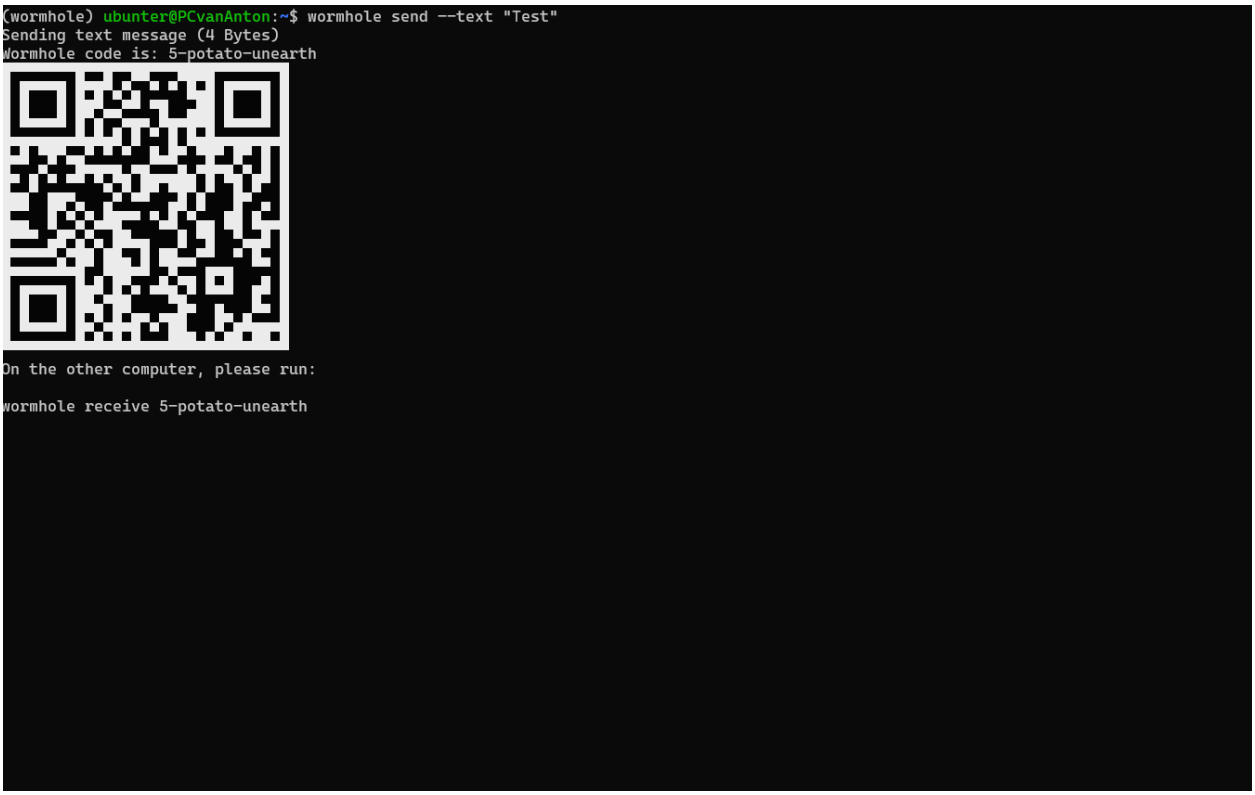
Crypto

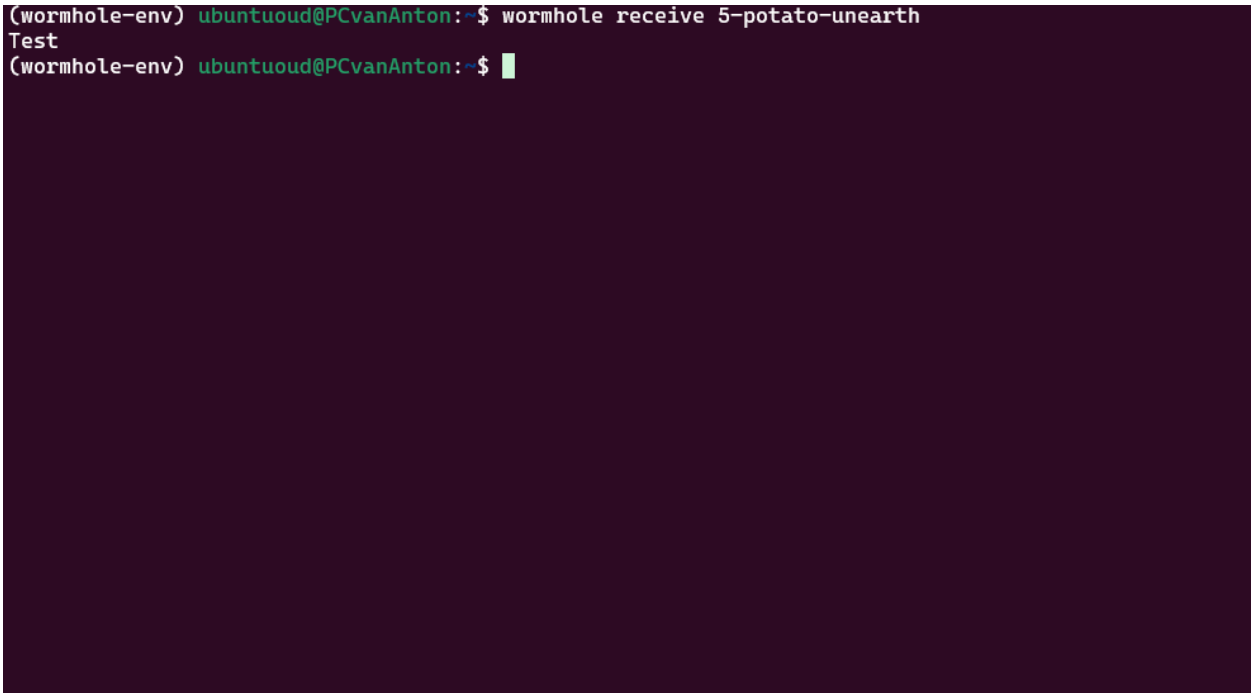
s150359

Anton Doms

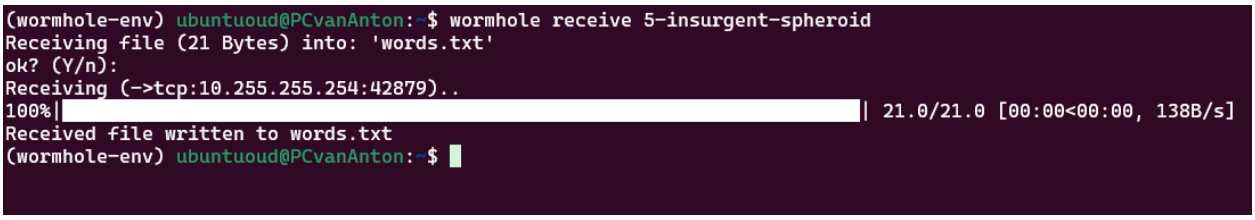
Testing met wormhole

Text




(wormhole-env) ubuntuoud@PCvanAnton:~$ wormhole receive 5-potato-unearth
Test
(wormhole-env) ubuntuoud@PCvanAnton:~$

File



Vragen

- What encryption algorithm is used by wormhole?

Wormhole gebruikt een PAKE om een gedeelde sessiesleutel te maken, en daarna symmetrische authenticated encryption om de data te versleutelen.

- Is the concept of hashing used by wormhole during file transfer? If so, what for?

Ja. Hashfuncties en KDFs worden gebruikt om sleutels af te leiden. Er is ook een kleine verifier die een hash van de sessiesleutel toont zodat gebruikers key confirmation kunnen doen. Integriteit wordt vooral gewaarborgd door de MAC in de authenticated encryption.

- Is a symmetric or asymmetric algorithm (or both) used? Which one?

Beide, in praktijk: asymmetrische groepsbewerkingen in de PAKE-handshake; daarna symmetrische encryptie (secretbox) voor de gegevensstroom.

- How does wormhole ensure that the file or message you receive is from the intended sender?

Alleen wie de code kent kan de PAKE correct uitvoeren en dezelfde sessiesleutel afleiden. Authenticated encryption zorgt ervoor dat berichten niet ongemerkt zijn gewijzigd.

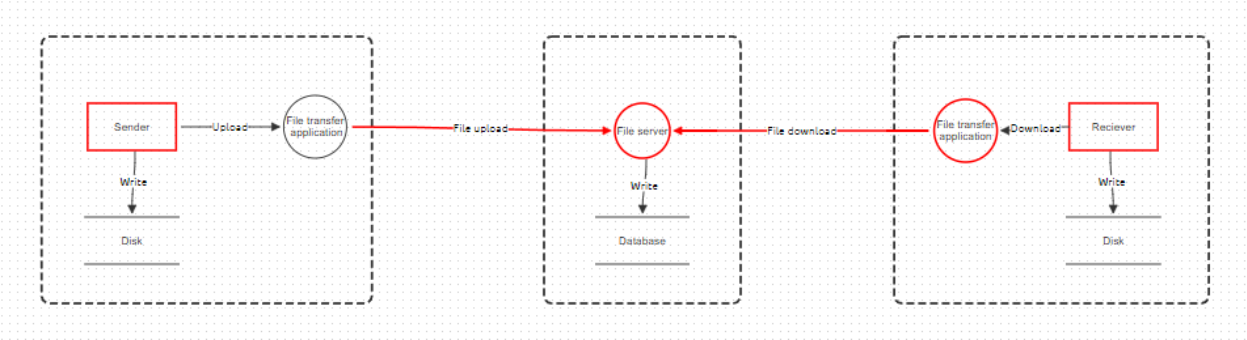
- How does a file transfer through the wormhole solution compare to a file exchange via Signal, from a security point of view?

Beide bieden end-to-end encryptie. Signal biedt echter een langdurig ratchet-mechanisme en identity-management voor langdurige gesprekken. Wormhole is ideaal voor korte, ad-hoc, eenmalige transfers.

- What attacks would be possible if the relay server were malicious?

De relay kan metadata verzamelen (wie, wanneer, grootte), verbindingen blokkeren of brute forcing tegenhouden.

Threat Model


Sender
Upload
File transfer application
File upload
File server
File download
File transfer application
Download
Reciever
Write
Disk
Write
Database
Write
Disk