Digital Self Defense for Activist

PufferFish

April 26, 2017

1. Communication
   - End-to-end encryption
   - Signal

2. Anonimity
   - TOR

Communication

What is encryption

Taking plaintext and a random generated key and performing mathematical operations to hide it's original content. Decryption is taking the ciphered test, and WITH THE CORRECT KEY performing mathematical operations to recover the original plaintext.

What does it protect me from?

Maire wants to communicate with Robert a

What does it protect me from?

Maire wants to communicate with Robert a

What does it NOT protect me from? Limits of the encryption

If the device is already compromised (Key logger, surveiled... - Microsoft).

How does it work?

Only the persons taking part on the conversation can decrypt the message, not the service providers.

- Maire and Robert want to hide the content of their conversations
- Marie and Robert will generate a secure key

Why?

End to end encryption Created by a non-profit organization Open source

What does it do?

Messages and calls Encrypt messages BETWEEN SIGNAL USERS Allows group conversations Has a desktop version

It also...

Send disappearing messages Disable lock-screen notifications

Safety numbers...

It allows you to verify that the conversation hasn't been intercepted by someone

What does it doesn't do?

Encrypt old SMS communications Encrypt messages on the phone, this requires disk encryption IT DOES: Store minimum meta-data

It’s useless if the device is already compromised

What is TOR

Software and a network It allows you to hide your IP address, your location

How does it work

The TOR network is composed by servers (nodes) The request traverses three nodes before reaching the final destination It's encrypted between each node

Limits

The global adversary

https://freedom.press/training/preventative-mobile-security-tips-activists/
https://tacticaltech.org/
https://ssd.eff.org/
securityinabox.org/en/