Anonymous Communication Networks

Dejaeghere, Jules

Publication date:
2022

Anonymous Communication Networks

Jules Dejaeghere

University of Namur

Jules Dejaeghere

Researcher at the Computer Science Faculty of University of Namur.

- Master in cybersecurity
- Joined CyberExcellence project in September 2022
- Research under the supervision of Florentin Rochet

Research direction

Focus on anonymous communication networks: how to provide anonymity to Internet users? Tor aims to provide online anonymity.

- Nodes of the network are run by volunteers
- Nodes are distributed around the world
- Challenging to maintain because of the diversity in the network components

UNIVERSITÉ DE NAMUR

Overview of Tor - `https://www.torproject.org/`

Protections provided by Tor

- Tor prevents websites and other services from learning your location
- Tor prevents people from watching your traffic
- Tor routes your connection through more than one Tor relay so no single relay can learn what you're up to

Protections not provided by Tor

- Tor does not protect against global passive adversaries
- Tor does not defend against timing analysis to correlate and link traffic to a specific user

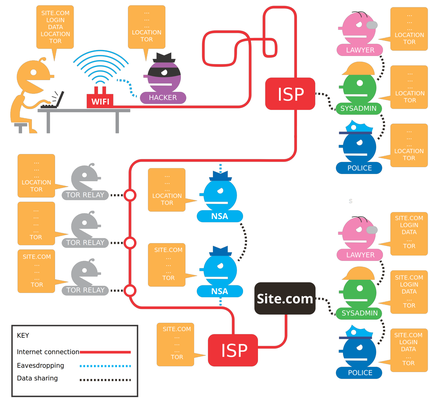

Figure 1. Data journey when using Tor.
`https://support.torproject.org/https/https-1/`

Keeping Tor up to date for everyone: a challenge

Key points of today's Tor network

- Around 6000 relays running, operated by volunteers
- Relay operators may not always update the software

Current Tor approach

- Build a flexible protocol that is forward compatible
- Enable unknown messages to be processed without breaking functionality

Investigating a new software architecture

- Do not rely on protocol flexibility for forward compatibility
- Allow developers to push updates to the network without the intervention of the operators
- Define where updates can be plugged in the main software and use just-in-time compilation

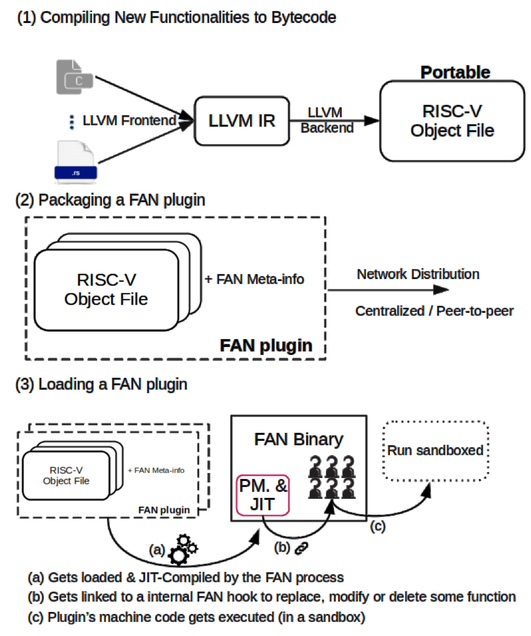

Figure 2. Overview of the process. *Rochet, F., & Elahi, T. (2022). Towards Flexible Anonymous Networks. arXiv preprint* `https://arxiv.org/abs/2203.03764`