

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Anonymous Communication Networks

Dejaeghere, Jules

Publication date:
2022

[Link to publication](#)

Citation for published version (HARVARD):

Dejaeghere, J 2022, 'Anonymous Communication Networks', CyberExcellence: Première journée des chercheurs, Mons, Belgium, 8/11/22 - 8/11/22.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

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 on-line 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



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

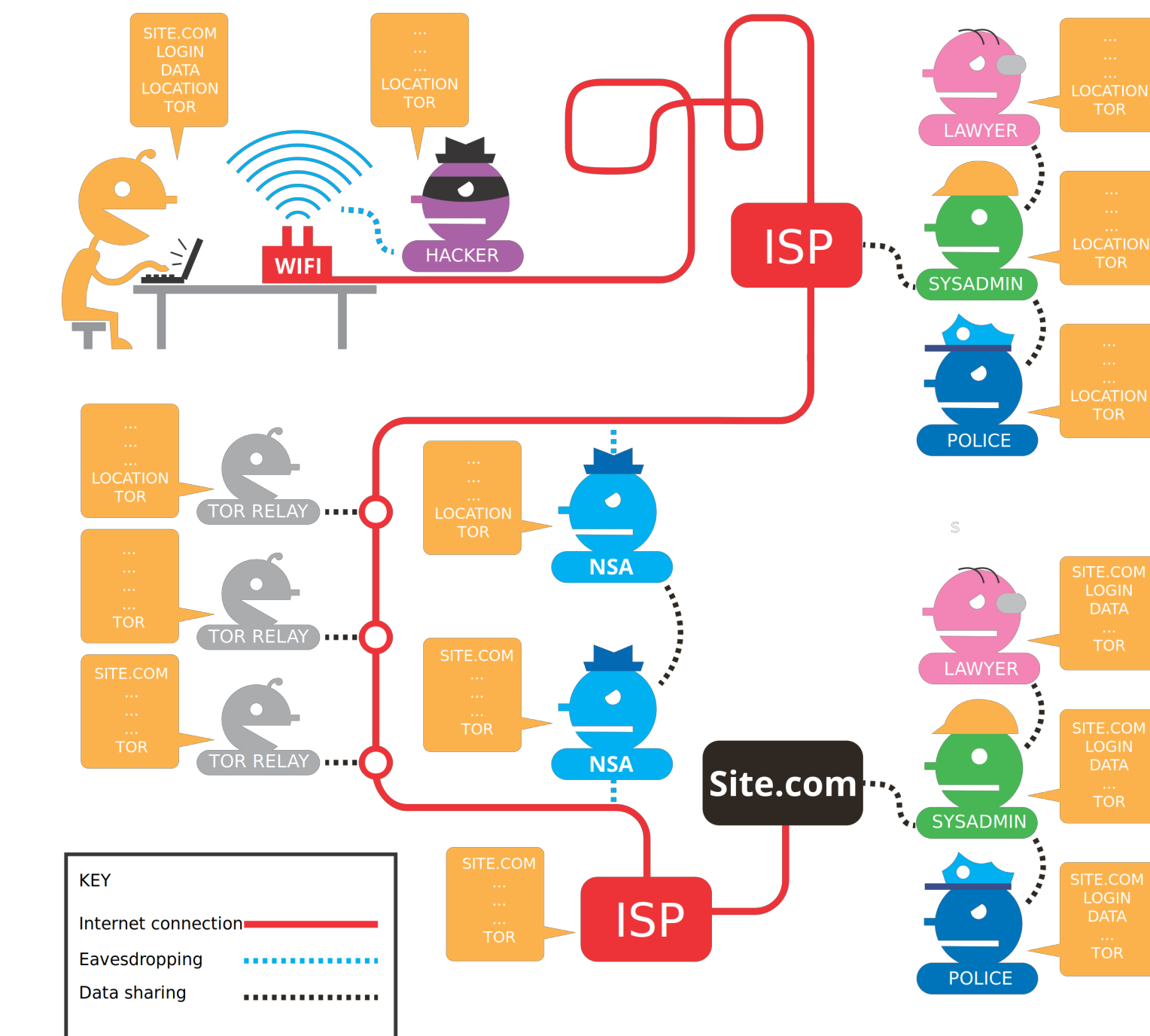


Figure 1. Data journey when using Tor.

<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

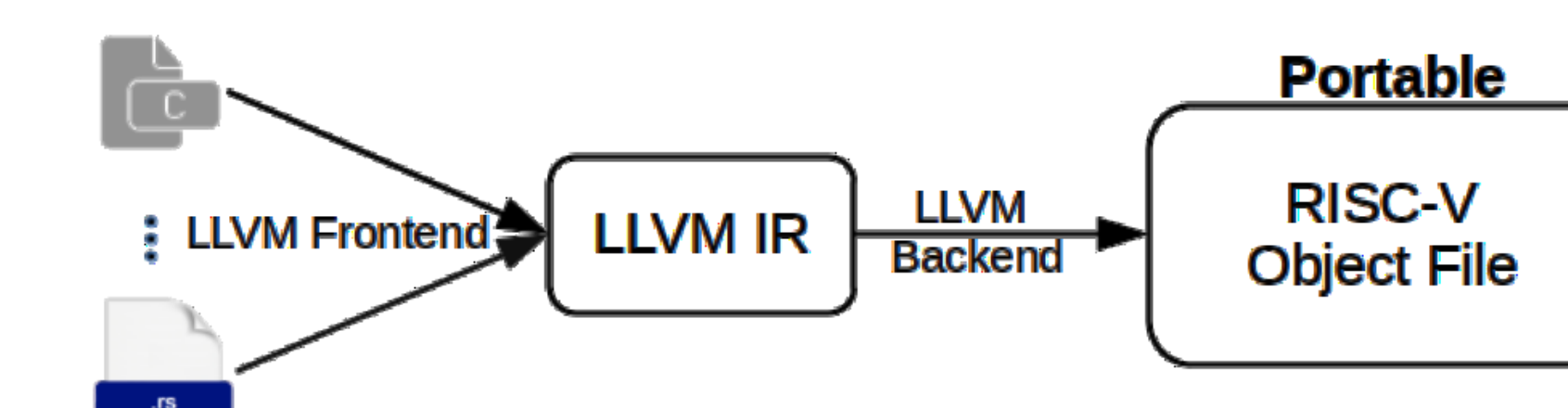
Current Tor approach

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

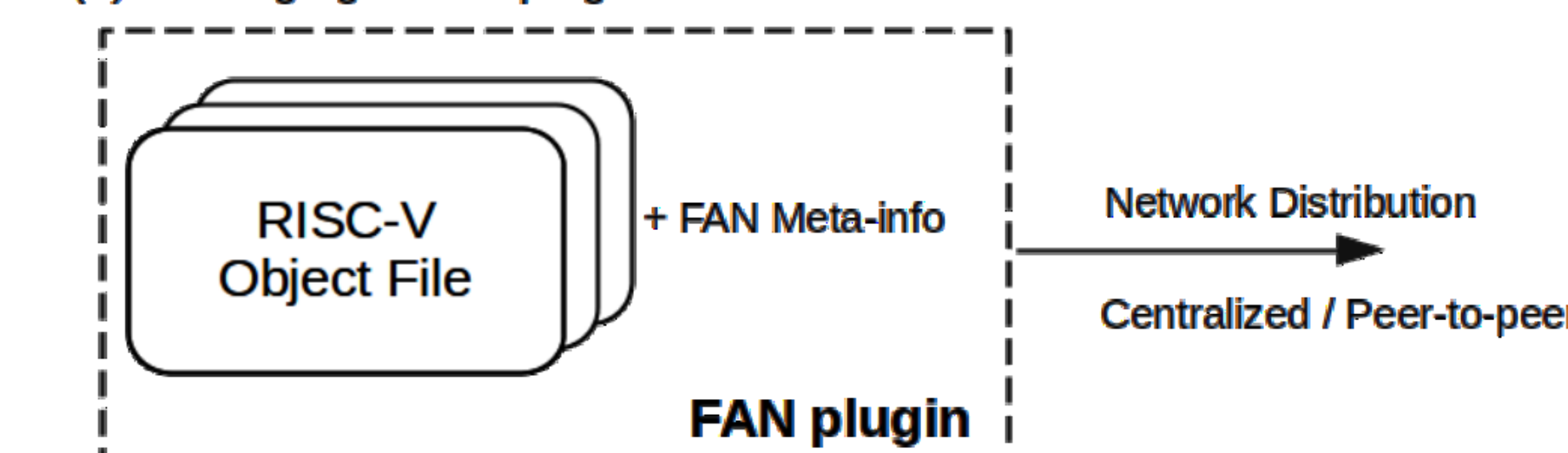
Investigating a new software architecture

- 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

(1) Compiling New Functionalities to Bytecode



(2) Packaging a FAN plugin



(3) Loading a FAN plugin

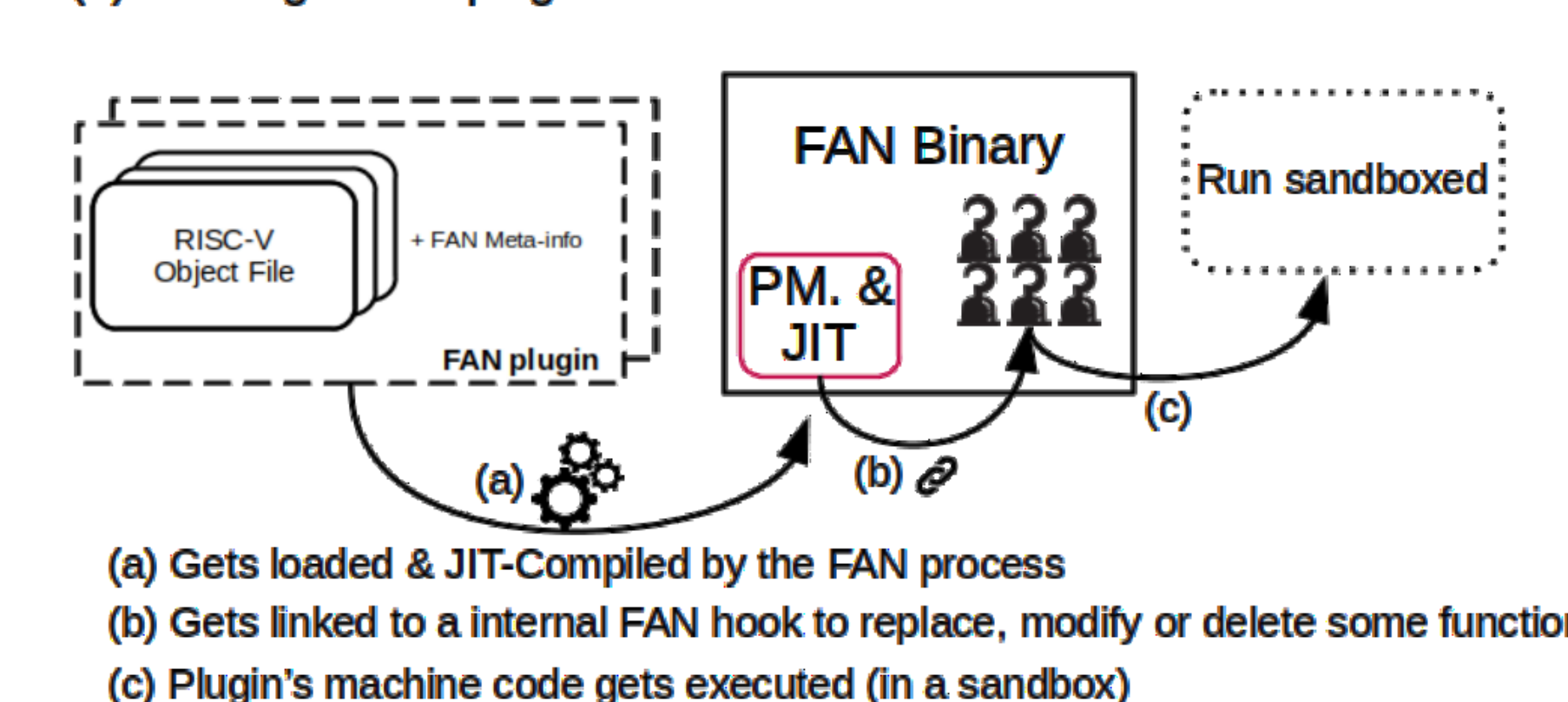


Figure 2. Overview of the process. Rochet, F., & Elahi, T. (2022). Towards Flexible Anonymous Networks. arXiv preprint <https://arxiv.org/abs/2203.03764>