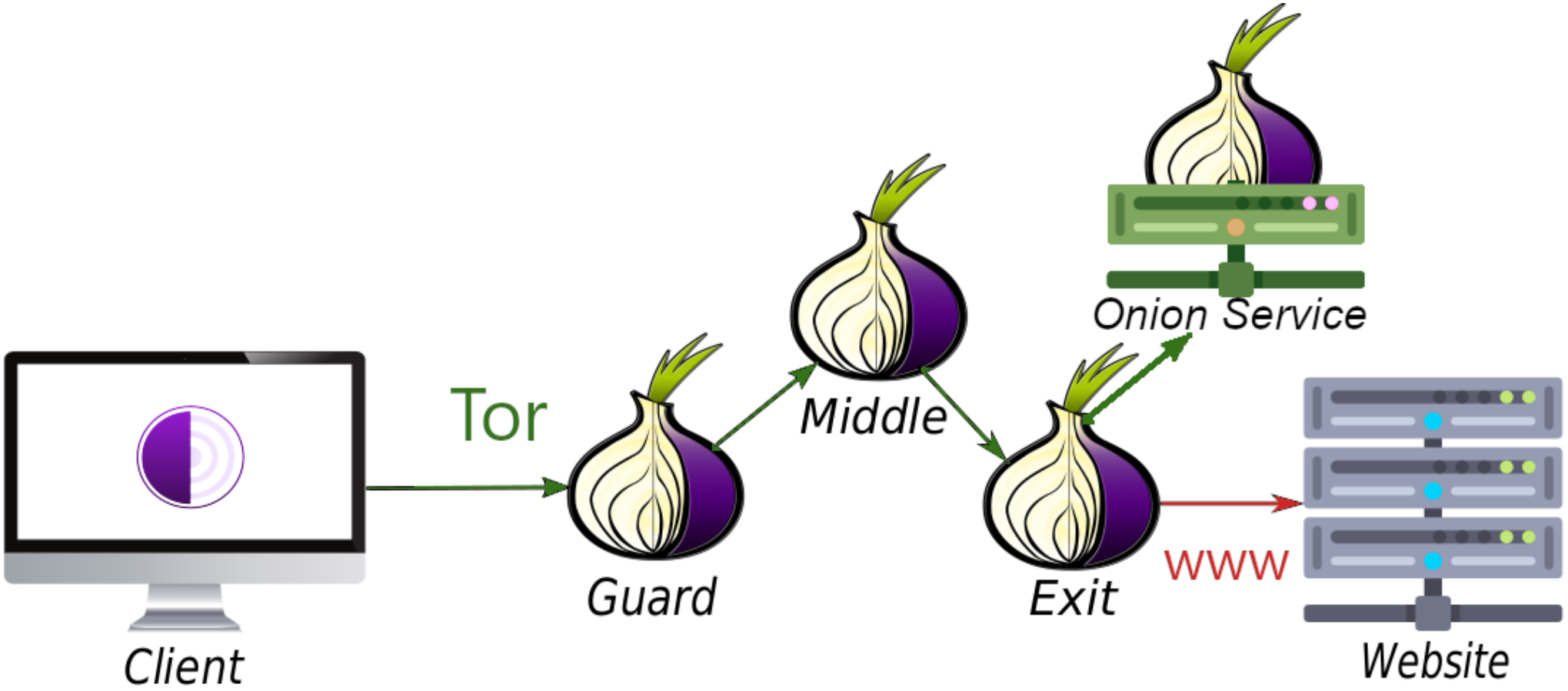
Tor incontra l'IA in attacco e in difesa

Giorgio Maone (ma1)
torproject.org

Di che parliamo?

- Cosa c’entrano le cipolle
- Cosa difende Tor
- Intelligenza artificiale nemica
- Intelligenza artificiale alleata

Cosa c’entrano le cipolle


Onion Service
Tor
Middle
Guard
Exit
www
Client
Website

Cosa difende Tor

Digital Rights = Human Rights

- Chi sono
  - Privacy, anonimato
- Dove vado / cosa vedo / cosa sento
  - Circolazione
  - Informazione
- Con chi sono / cosa dico
  - Associazione
  - Espressione

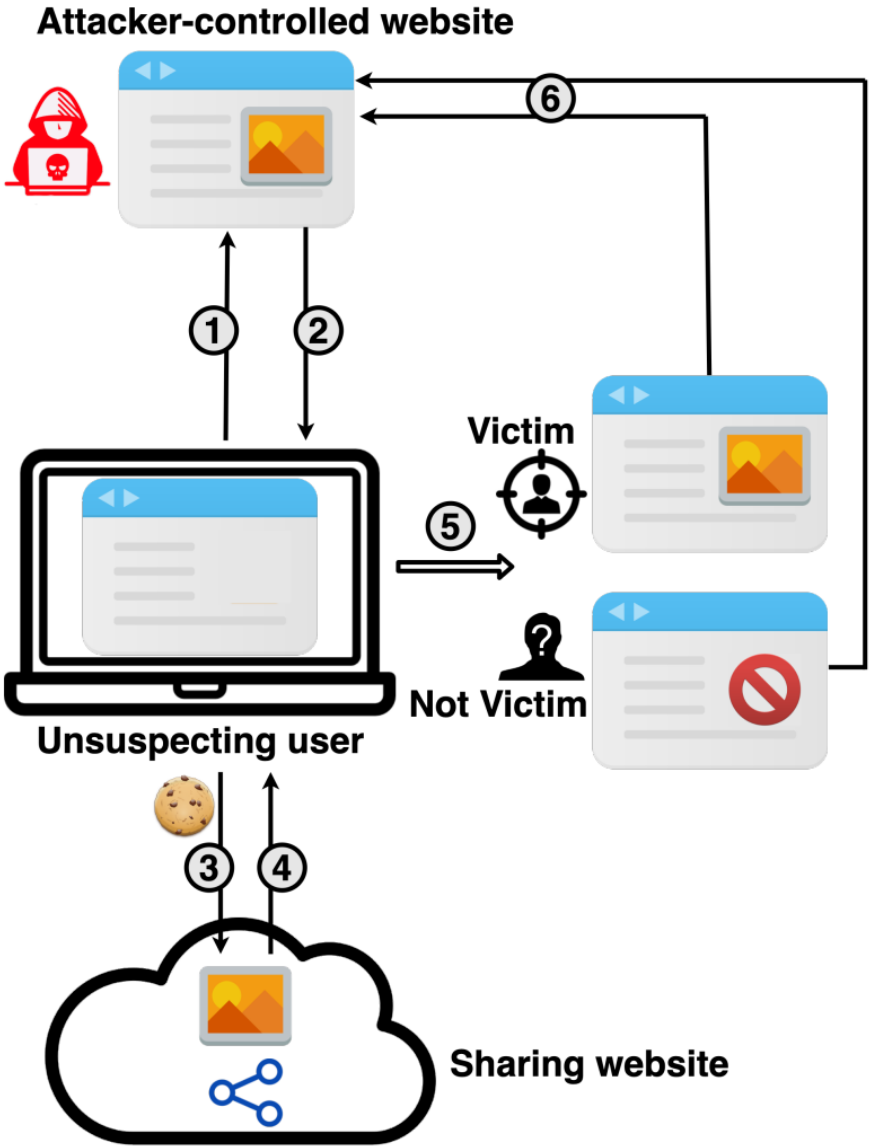
I. A. nemica

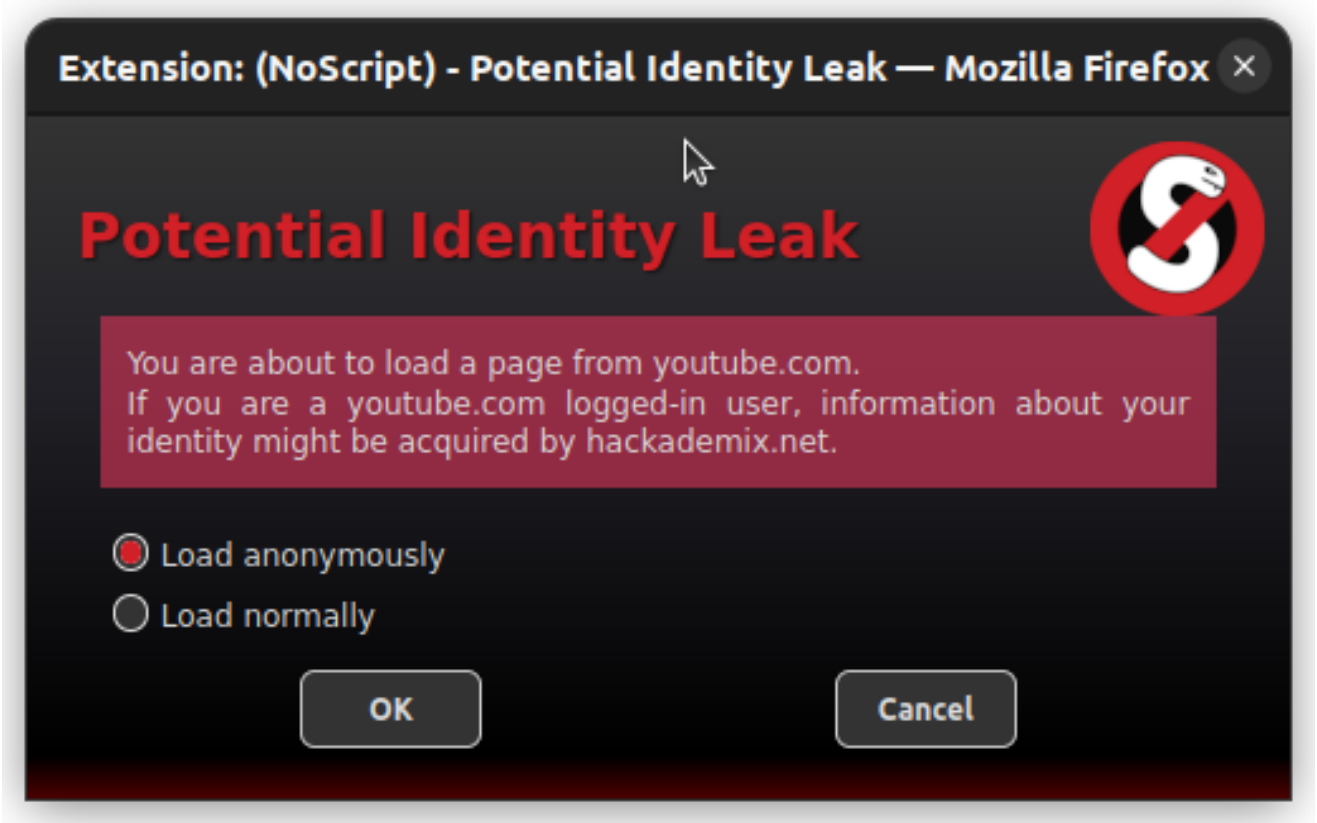
Chi sono

Targeted

Deanonymization

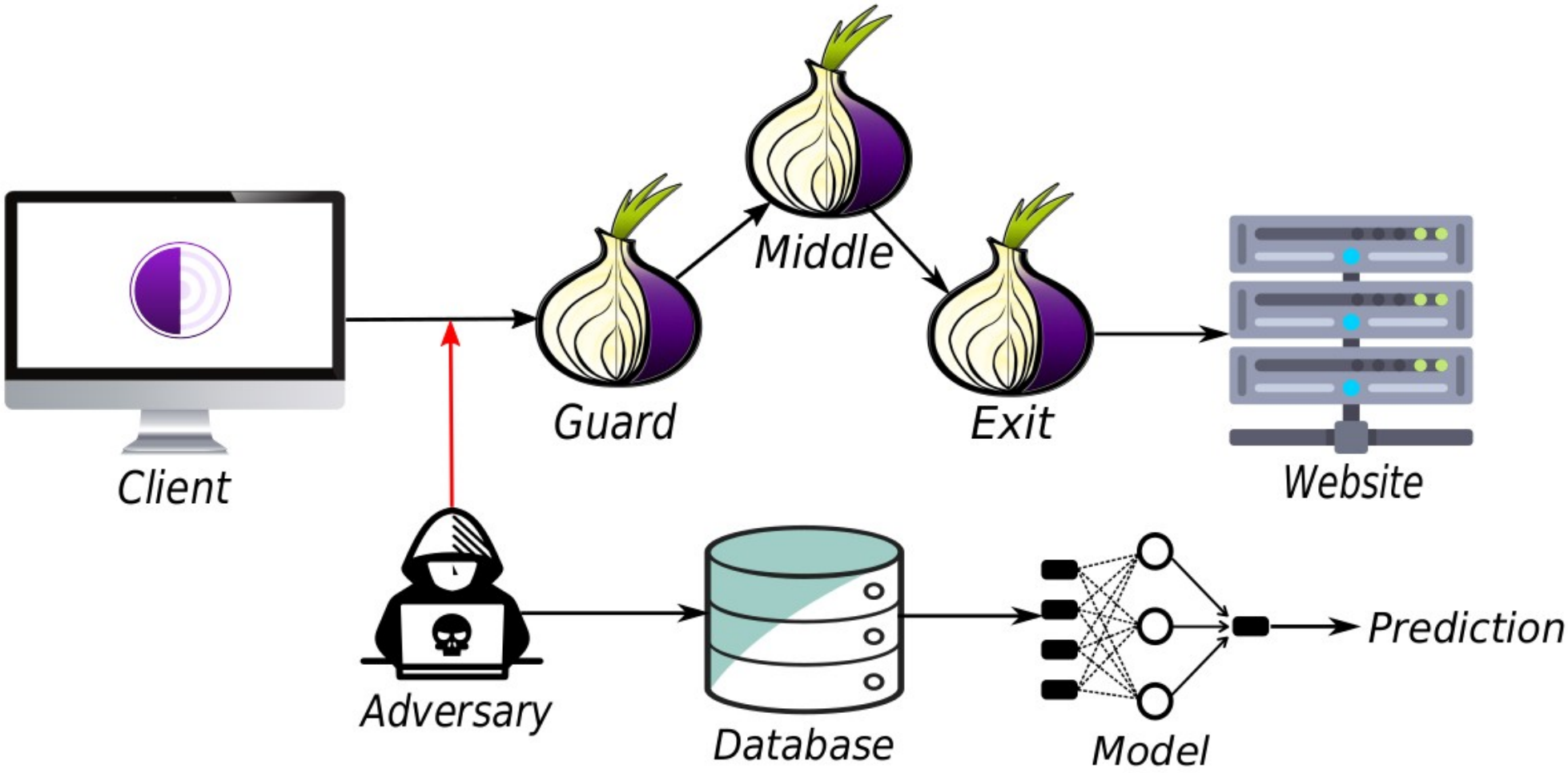
(via the Cache Side Channel)


Attacker-controlled website
6
1
2
Victim
5
Not Victim
Unsuspecting user
3
4
Sharing website


Extension: (NoScript) - Potential Identity Leak — Mozilla Firefox
Potential Identity Leak
You are about to load a page from youtube.com.
If you are a youtube.com logged-in user, information about your identity might be acquired by hackademix.net.
Load anonymously
Load normally
OK
Cancel

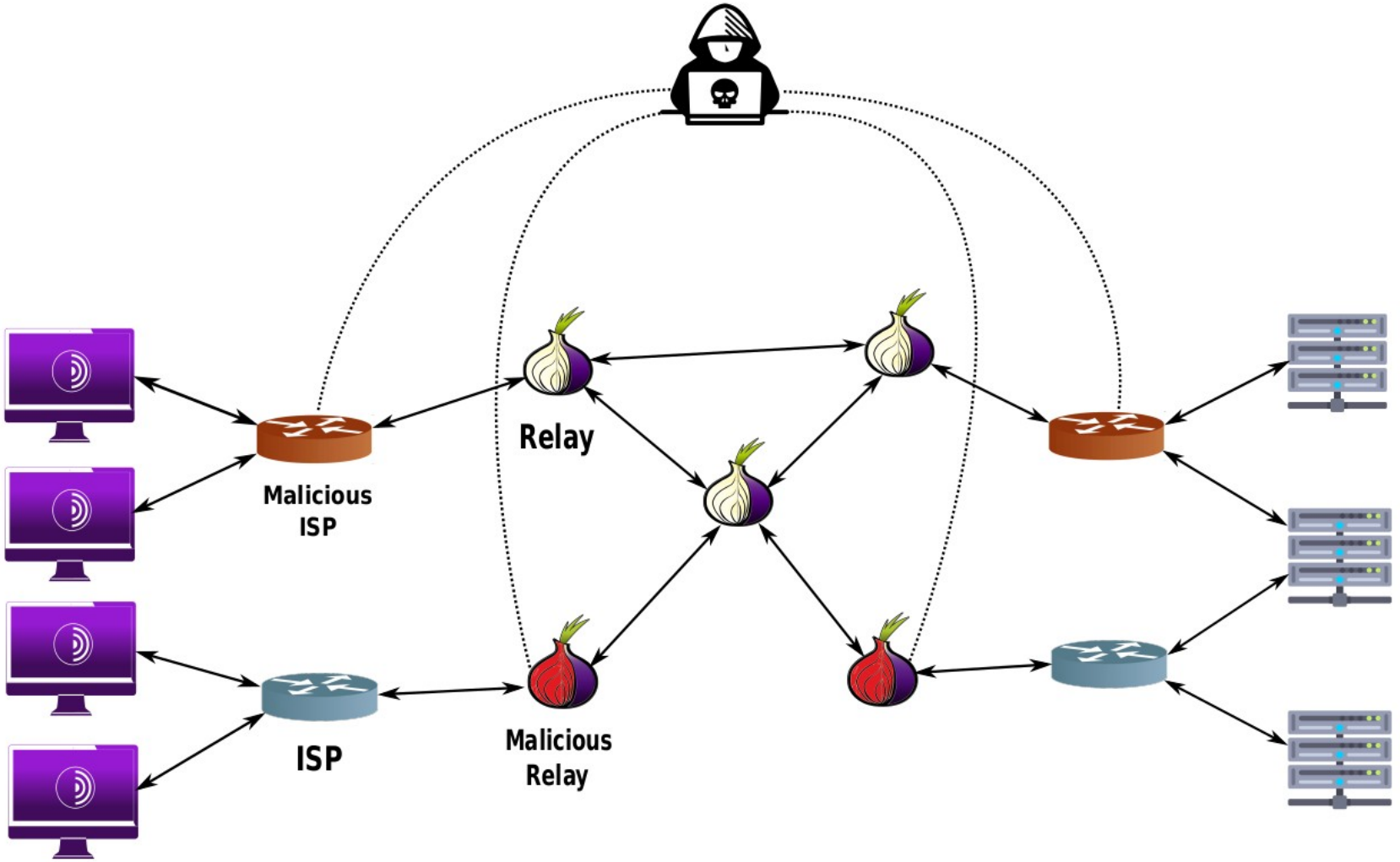
Dove sono / cosa vedo / cosa sento

Website Fingerprinting


Client
Guard
Middle
Exit
Website
Adversary
Database
Model
Prediction

Con chi sono / cosa dico

Flow Correlation

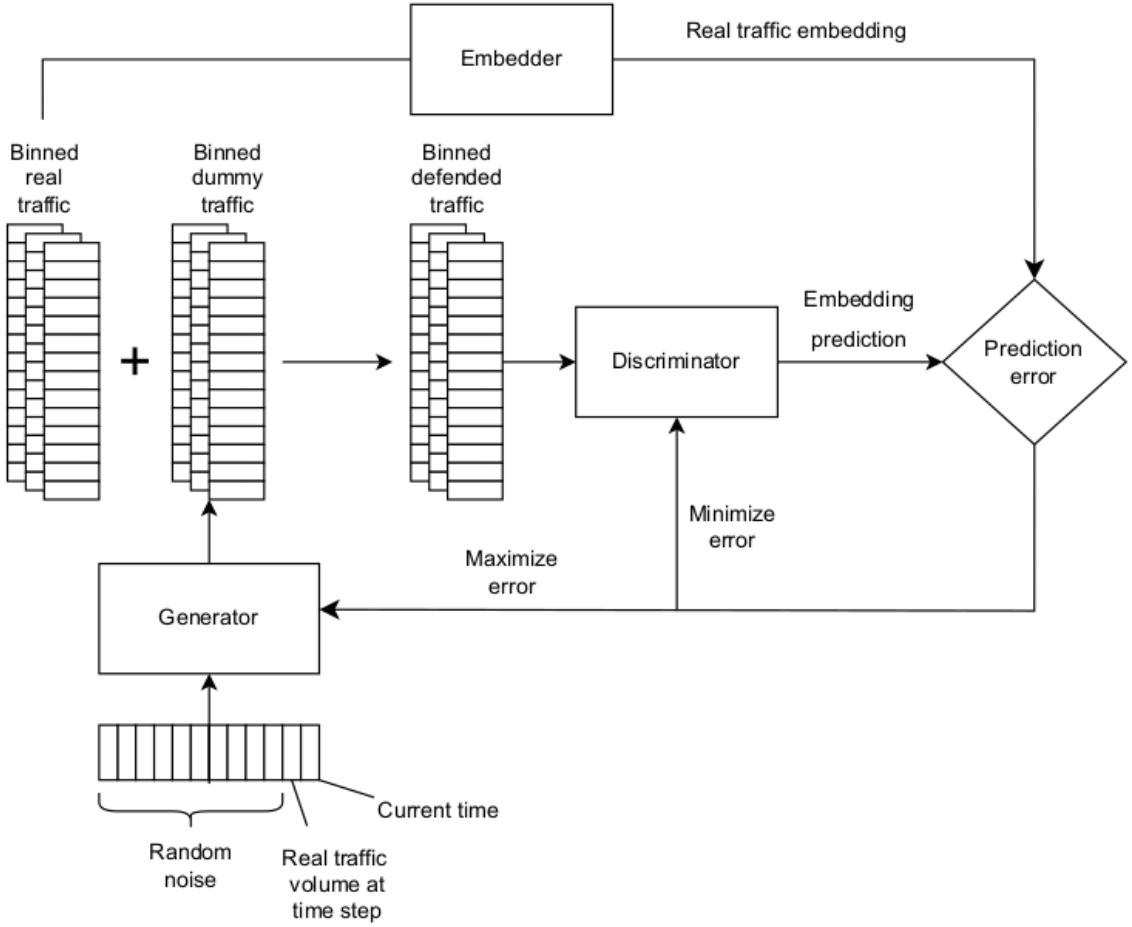

Malicious
ISP
Relay
ISP
Malicious
Relay

I. A. alleata

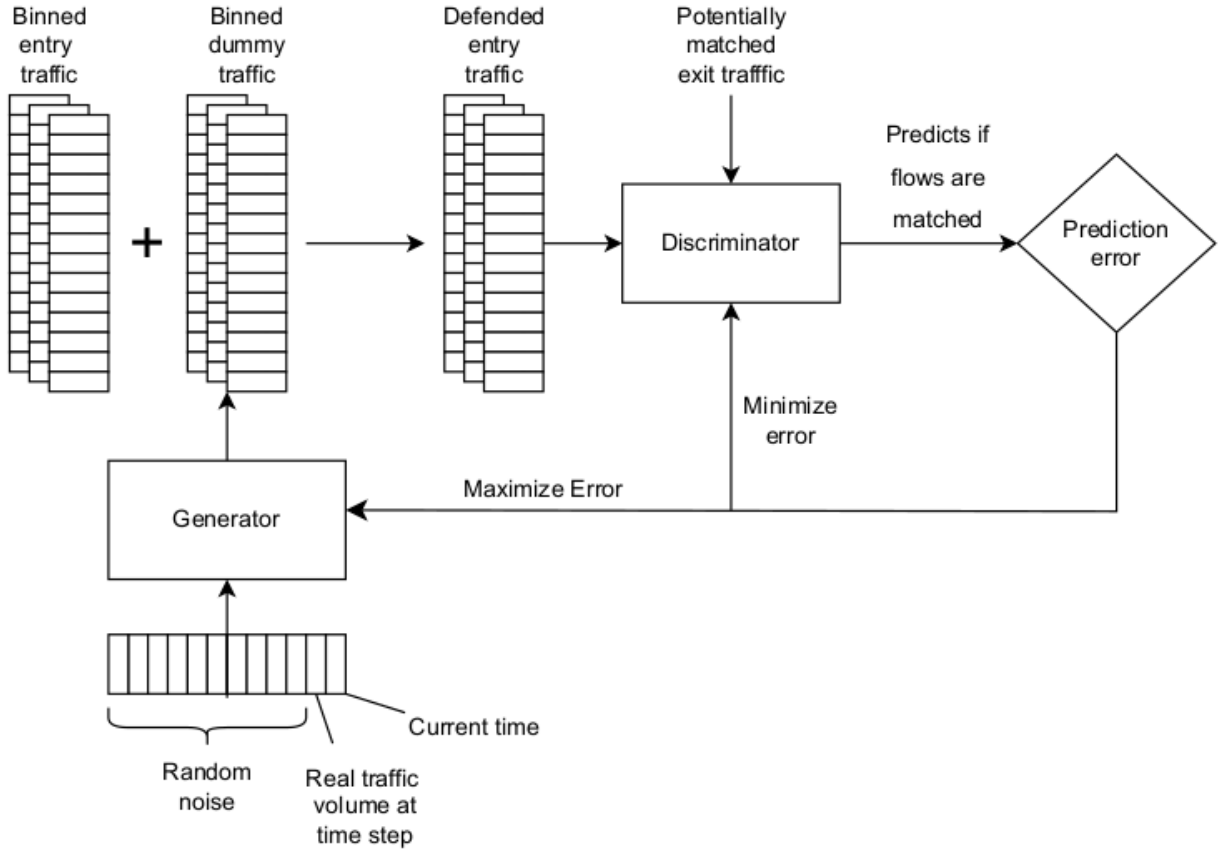
DeTorrent

- Traffic analysis defense
- Padding-only
- Generative Adversarial Network (GAN)
- Long Short-Term Memory (LSTM)
- Pluggable transport

WF DeTorrent



FC DeTorrent



Per approfondire

- Tor:
  torproject.org
- Targeted Deanonymization via the Side Channel:
  usenix.org/conference/usenixsecurity22/presentation/zaheri
- NoScript:
  noscript.net
- DeTorrent:
  arxiv.org/pdf/2302.02012.pdf

Thank You

Giorgio Maone
giorgio@maone.net
@ma1