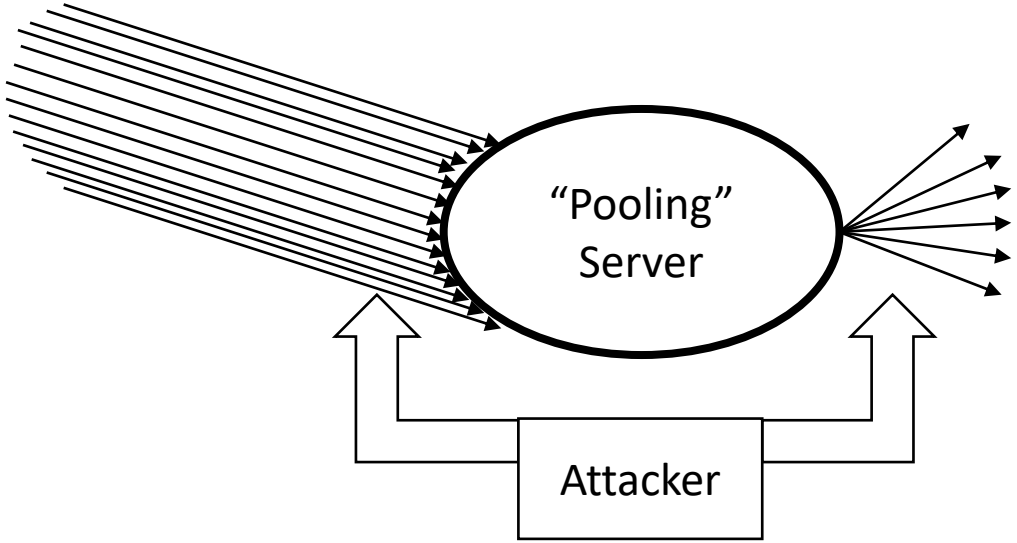
Swimming in shallow anonymity pools

Christian Huitema

PEARG interim, January 19, 2021

Anonymity pools for privacy?



The theory:
Attacker may be able to see incoming and outgoing traffic, but there are so many clients that the attacker cannot match incoming address and outgoing request.

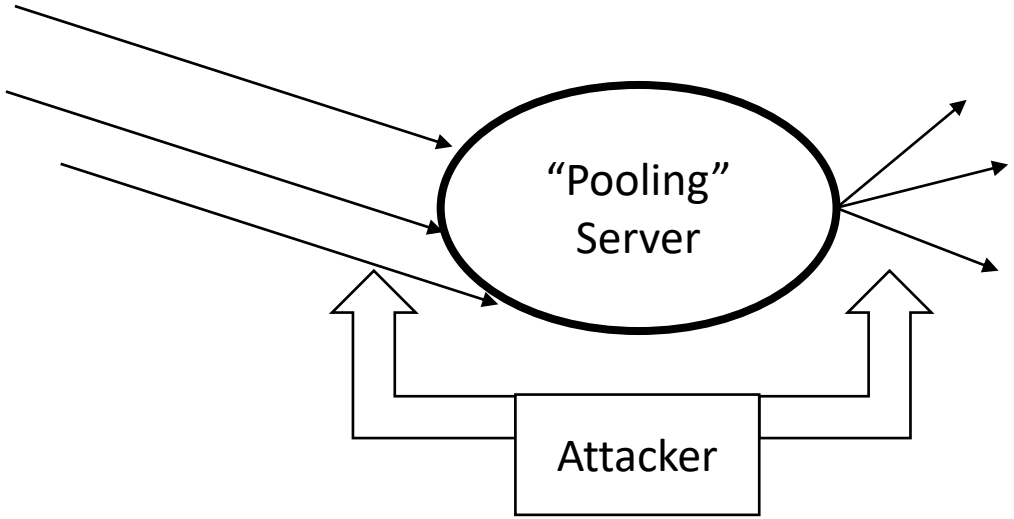
Many privacy functions rely on "anonymity pools":

- Tor nodes
- VPN used for privacy
- DNS over Encryption
- Oblivious DNS
- Encrypted SNI
- …

Classic attacks use correlation between incoming and outgoing traffic: timing, traffic patterns, etc. This is not the subject of this talk.

This talk focuses on the "size of the pool".

Shallow pools do not provide much privacy



The risk:

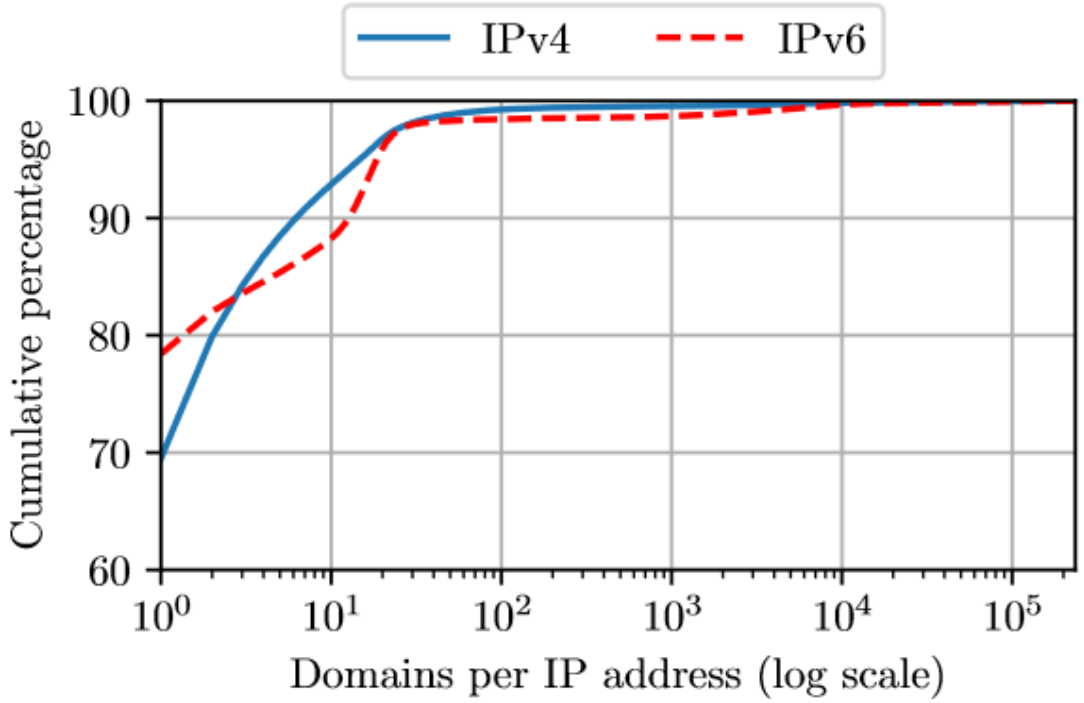
- If there are few clients, timing and correlation attacks become very effective
- If there is just one client, there is no protection at all

The question:

- Do we need to worry in practice?
- …

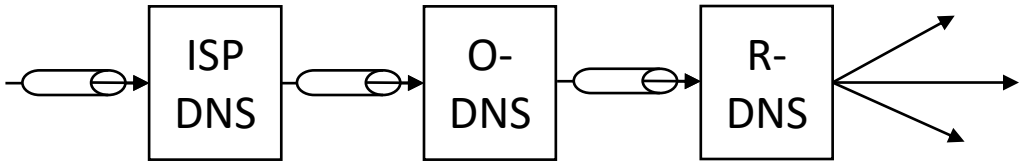
The “ESNI” pools can be very shallow

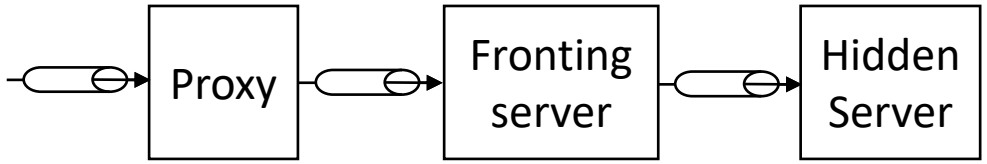
- Several privacy constructs rely on ESNI
  - E.g., DNS privacy ultimately relies on ESNI
- ESNI rely on pool of servers sharing the same IP address
- Per study of top 1 Million domains, 70% of IPv4 addresses are used by a single domain.
- **1 IP per server is the norm**



Hoang, Nguyen Phong & Akhavan Niaki, Arian & Borisov, Nikita & Gill, Phillipa & Polychronakis, Michalis. (2019). Assessing the Privacy Benefits of Domain Name Encryption. 10.1145/3320269.3384728.

Choice, not chance!





"Proxy" could be HTTP-Proxy, QUIC-Masque, or various VPN services

- Example of O-DNS:
  - ISP DNS is a "natural pool"
    - hides source address from O-DNS
  - O-DNS is actively chosen,
    - hides DNS target from ISP DNS
  - Encryption from O-DNS to R-DNS
- Similar approach for E-SNI ?
  - Actively chosen proxy hides IP address from fronting server and third parties
  - ESNI hides final destination from proxy
  - Server should actively choose a fronting server!

Who is going to deploy the proxies?

- Each approach has risks
  - Large tech companies
    - Surveillance capitalism?
    - Walled gardens?
  - Volunteers
    - Is this sustainable?
    - How to deter abuses?
  - Specialized services
    - Need to charge their users, somehow
- Dilemma
  - Open access will invite fraud, make service unsustainable
  - Controlled access requires authentication, breaks privacy
- Are we doomed?

Superior Hiding Services!

At this point, Christian is dreaming

- Chaum, David (1983). "Blind signatures for untraceable payments" (PDF). Advances in Cryptology Proceedings of Crypto. **82** (3): 199–203.
- Can we use that for privacy servers?
  - Proof that client is OK
  - Hide the client actual identity
- Would that enable sustainable privacy services?

Back to the shallow pool…

- One server per IP is pretty much the norm
  - ESNI has limited benefits
  - Encrypted DNS does not protect against on-path observers
- Effective privacy requires hiding the IP address
  - This means one or two relays
- Choice of relay has consequences
  - What if the VPN is spying on you?
  - Choice, not chance!
- Need to look at the business model of proxies
  - Is this sustainable?
- PEARG has work to do.