Eclipse and Re-Emergence of Anonymous P2P Storage Network Overlay Services

Marios Isaakidis
m.isaakidis@cs.ucl.ac.uk

George Danezis
g.danezis@ucl.ac.uk

Department of Computer Science
University College London

HotPETs - July 22, 2016
Network-level Anonymity
Low-latency Anonymity Networks
Routing traffic to a hidden server

https://www.torproject.org/docs/hidden-services.html.en
https://geti2p.net
The “Tor Swiss Army knife”

Onion service developers have to cope with:

- Scalability
- Availability
- Observability
- Platform Security

---

1 Bryan Ford, ECRYPT CSA 2016
The “Tor Swiss Army knife”\textsuperscript{1}

Onion service developers have to cope with:

- Scalability
- Availability
- Observability
- Platform Security

... are there any alternatives?

\textsuperscript{1}Bryan Ford, ECRYPT CSA 2016
CENO
Experimenting with the client-server paradigm over Freenet

CeNO Components
- Darknet node
- CeNO node
- Malicious node
- Bridge node

CeNO inserts websites

https://censorship.no
https://equalit.ie
Anonymous P2P Storage Networks

Decentralized information storage and retrieval systems where nodes:

- Provide resources – bandwidth and storage
- Replicate the files
- Route requests

Two operations available: INSERTIONS and RETRIEVALS
Anonymous P2P Storage Networks

Decentralized information storage and retrieval systems where nodes:
- Provide resources – bandwidth and storage
- Replicate the files
- Route requests

Two operations available: **INSERTIONS** and **RETRIEVALS**

Security Guarantees

- Anonymity for both producers and consumers of information
- Plausible deniability
- High availability and persistence of the information inserted
- Censorship resistance
- Global adversary resistance
A diverse ecosystem of Freenet services

- Communication
  - *Frost* bulletin board
  - *Freemail* asynchronous communication without leaking metadata
  - *FLIP-IRC* synchronous messaging (experienced long delays)

https://freenetproject.org
A diverse ecosystem of Freenet services

- Communication
  - *Frost* bulletin board
  - *Freemail* asynchronous communication without leaking metadata
  - *FLIP-IRC* synchronous messaging (experienced long delays)

- Collaboration
  - *Wiki* systems
  - *Infocalypse* source code management

https://freenetproject.org
A diverse ecosystem of Freenet services

- **Communication**
  - *Frost* bulletin board
  - *Freemail* asynchronous communication without leaking metadata
  - *FLIP-IRC* synchronous messaging (experienced long delays)

- **Collaboration**
  - *Wiki* systems
  - *Infocalypse* source code management

- **Library “distributed search engine”**
  - Maintainers crawl websites and publish indexes
  - Users retrieve the indexes and perform term matching locally

[https://freenetproject.org]
Using public key crypto, Freenet provides an abstraction that allows:
- the owner of the private key to insert and update information
- others to discover what the owner has inserted

The *Web of Trust* is a spam resistance mechanism inspired by Levien’s attack resistant trust metrics.
CENO Deployment Topology
Scaling by allocating tasks and by using High Trust Links
Censorship Circumvention over P2P Storage Networks

- No need to publish proxy/bridges addresses
- Self-versioned Internet archive
- A messaging mechanism with strong privacy guarantees
- Requests need to be handled by an Insertion node only once, then are served directly via the distributed storage
- Content remains available via the distributed cache when a country throttles Internet access to the rest of the world
Censorship Circumvention over P2P Storage Networks

- No need to publish proxy/bridges addresses
- Self-versioned Internet archive
- A messaging mechanism with strong privacy guarantees
- Requests need to be handled by an Insertion node only once, then are served directly via the distributed storage
- Content remains available via the distributed cache when a country throttles Internet access to the rest of the world

**The CENO paradox**

CENO becomes *faster* and requires *fewer request handling nodes* as it gets widely adopted
Freenet as an Anonymity Platform

- “Anonymity as a Service”
  - APIs for developing plugins
  - Existing user base (and storage capacity)
  - Freenet security properties
- Resistant to traffic analysis attacks
Freenet Services Open Challenges
Are we there yet?

- Dynamic content
- Synchronous messaging
- Performance
- Availability of unpopular content
- Spam resistance
- Scaling
Thank you

Marios Isaakidis
m.isaakidis@cs.ucl.ac.uk
@misaakidis
github.com/equalitie/ceno