SCALABLE ANONYMOUS OVERLAY NETWORKS

NICK HOPPER

with

JON McLACHLAN
ANDREW TRAN
YONGDAE KIM
ANONYMITY

Alice

Francine

Eve

N.H.

facebook.com/bob

facebook.com/charlie

facebook.com/dave

www.SuperSecretEvilPlanToTakeOverTheWorld.com
ONI 2009 CENSORSHIP MAP

Levels of Filtering:  
- Pervasive
- Substantial
- Selective
- Suspected
- No evidence
UNSCALABLE ANONYMITY

\[ X_F = M_F \oplus K_{AF} \oplus \ldots \oplus K_{EF} \]

\[ M = X_A \oplus \ldots \oplus X_F \]

Bandwidth cost (bits/time) of a DC-NET: \( \Omega(n^2) \)
RELAY-BASED ANONYMITY

Well-known example: Tor

Security goal: best attacks are \((f, f^2)\)-attackers

Bandwidth cost = \(O(n)\)?
RELAY DISCOVERY

Bandwidth cost = $\Omega(n^2)$

Directory Service

| R_1  | 1.2.3.4 | 0xFEED |
| R_2  | 10.1.3.5| 0x03D5 |
| R_3  | 3.1.4.1 | 0x15DE |
| R_4  | 1.5.9.6 | 0xAD11 |
| :    | :      | :     |
| R_N  | 2.7.8.3 | 0xFFFF |

Signed,

-Dir. Service
DISCOVERY OVERHEAD

![Graph showing bandwidth (GB/s) vs. users (Millions)]

- Exit Traffic
- v2 DS Traffic
- v3 DS Traffic
- Torsk Traffic
Random node discovery cost: $O(\log n)$
I2P organizes peers into a Kademlia (iterative) DHT. To build circuits, a peer searches for a random key $k$. 

ID$_5 = \text{hash}(PK)$
The closest nodes form the circuit.

What happens if a query hits an adversarial node?

The next query is run through the last circuit.
Pr[compromised circuit] = 
\[ f(f + f(1-q)(1-f) + f(1-q)^2(1-f)^2 + \ldots) = \frac{f^2}{q+f-qf} \]
Probability that a query hits only "good" peers

![Graph showing probability vs. size of network for different network sizes: 5%, 10%, 15%, and 20%.]
I2P allows **route capture**: routes check in, not out.
OTHERS

“Salsa” (Nambiar and Wright, CCS 06)
“Bluemoon” (Puttaswamy et al, ICNP 08)
“Information Slicing” (Katti et al, NSDI 07)
“Cashmere” (Zhao et al, NSDI 05)
“AP3” (Mislove et al, Eurosys 04)
CORE, TAP, GAP, WonGoo, NEBLO,…
Peers form a Chord (recursive) DHT. Every peer belongs to a **group** of size 16.
A single “first-stage” node can capture the route!
If a query hits a faulty node, it can be dropped.

“most” queries hit a faulty node $\Rightarrow \Pr[\text{compromise}] > 3f$
Probability that a completed tunnel is compromised

Number of peers (n)

Probability:
- 5%
- 10%
- 15%
- 20%
DESIGN GOALS

Design a circuit creation algorithm for Tor that has:

- Bandwidth scalable to $10^8$ clients
- Low bootstrapping costs
- Low state at relays
- Incremental deployability
- Resistance to attacks:
  - Fingerprinting
  - Route capture
  - Passive Logging
  - Selective Dropping
TORSK

ID_1

ID_2

ID_3

ID_4

ID_5

ID_6

ID_7

ID_8

Key: 0xBADD00D

nList: ID_3, ID_4, ID_6, ID_7

N. Authority
BUILDING CIRCUITS

extend(k) ID₁

ID₈
ID₂
ID₃
ID₄
ID₅
ID₆
ID₇
ID₈

N. Authority
A query fails at hop $i$ if all neighbors of the $i^{th}$ hop are faulty.

A query fails if it fails at some hop.

Let $|n_{\text{List}}| \geq \frac{(\log \log r) + (\log 1/\delta)}{\log 1/f}$

$\Pr[\text{lookup failure}] \leq \sum_i \Pr[\text{failure at hop } i] \leq (\log r) \cdot f^{n_{\text{List}}} \leq \delta$

Cost of discovery = $O((n \log r) \cdot |n_{\text{List}}|)$
BUDDIES

extend(k) ID₁ → ID₈

lookup(k) ID₈ (buddy)

N. Authority
FINDING BUDDIES

Key: 0xBADD00D

nList: ID₇, ID₈, ID₂, ID₃
rList: ID₈, ID₃, ID₆, ID₂

N. Authority

ID₁
ID₂
ID₃
ID₄
ID₅
ID₆ (buddy)
ID₇
ID₈

get

k
buddies “batch” lookups and mix in random keys

extend(k)

-cover lookups

N. Authority
SELECTIVE DROPPING

- --- Torsk
- ★ 2 buddy
- •• Tor

Compromised Tunnels vs. Malicious Nodes ($f$)
About 2K lines Python, uses eMule Kad DHT

Incrementally deployable: Routers can be Torsk and Tor nodes with one executable.
DISCOVERY OVERHEAD

![Graph showing the relationship between Bytes and Routers for different types: Torsk-Routers, Tor-Routers, Tor-Clients, and Torsk-Clients. The graph illustrates the discovery overhead in bytes as the number of routers increases.]
AUTHORITY OVERHEAD

Graph showing the relationship between nCerts/Hour and Routers, with lines indicating average and maximum values.

- **x-axis (Horizontal)**: Routers
- **y-axis (Vertical)**: nCerts/Hour

Legend:
- Blue line: Average
- Red line: Max
PERFORMANCE

Circuit building times,
64-node Torsk deployment on PlanetLab
CONCLUSIONS

“List of all nodes” relay discovery scales poorly.

DHTs are scalable but easy to get wrong:

  Most queries encounter adversarial nodes

  Mitigation mechanisms can lead to attacks:
  DHT security ≠ Anonymity

Torsk is scalable and incrementally deployable while resisting attacks.