FreeDOM

- Cooperative Storage
- Resilient Communication
- Work Scheduling
Cooperative Storage

- DHTs
- ramcloud
- Freenet
Ramcloud

1000 – 100,000 Application Servers

Appl. Library

Appl. Library

Appl. Library

Appl. Library

Datacenter Network

Commodity Servers

Master Backup

Master Backup

Master Backup

Master Backup

Coordinator

High-speed networking:
- 5 μs round-trip
- Full bisection bwidth

32-256 GB per server

1000 – 10,000 Storage Servers
Freenet
Communication Resilience

- RON
- Tor
- Diaspora
<table>
<thead>
<tr>
<th>RON was able to successfully detect and recover from 100% (in $RON_1$) and 60% (in $RON_2$) of all complete outages and all periods of sustained high loss rates of 30% or more.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RON takes 18 seconds, on average, to route around a failure and can do so in the face of a flooding attack.</td>
</tr>
<tr>
<td>RON successfully routed around bad throughput failures, doubling TCP throughput in 5% of all samples.</td>
</tr>
<tr>
<td>In 5% of the samples, RON reduced the loss probability by 0.05 or more.</td>
</tr>
<tr>
<td>Single-hop route indirection captured the majority of benefits in our RON deployment, for both outage recovery and latency optimization.</td>
</tr>
</tbody>
</table>
Threat model: what can the attacker do?

Alice
watch Alice!

Anonymity network
Control part of the network!

Bob
watch (or be!) Bob!
Anonymity isn't cryptography: Cryptography just protects contents.
You can't get anonymity on your own: private solutions are ineffective...

Citizen Alice → Alice's small anonymity net → Investigated suspect → "One of the 25 users on AliceNet."

Officer Alice → Municipal anonymity net → Investigated suspect → "Looks like a cop."

AliceCorp → AliceCorp anonymity net → Competitor → "It's somebody at AliceCorp!"
... so, anonymity loves company!

Citizen Alice → Shared anonymity net → Investigated suspect → “???”

Officer Alice → Shared anonymity net → Competitor → “???”

AliceCorp → Shared anonymity net → “???”
Yes, bad people need anonymity too. But they are *already* doing well.

Evil Criminal Alice

- Compromised botnet
- Stolen mobile phones
- Open wireless nets
- .....
Current situation: Bad people on the Internet are doing fine

- Trojans
- Viruses
- Exploits
- Botnets
- Zombies
- Espionage
- DDoS
- Extortion
- Spam
- Phishing
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a single relay (or eavesdropper!) is a single point of failure.
... or a single point of bypass.

Timing analysis bridges all connections through relay ⇒ An attractive fat target
So, add multiple relays so that no single one can betray Alice.
A corrupt first hop can tell that Alice is talking, but not to whom.
A corrupt final hop can tell that somebody is talking to Bob, but not who.
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Diaspora
Work Offloading

• COMET
• CloneCloud
• Maul
COMET: Code Offload by Migrating Execution Transparently

Diagram showing:
- Unmodified & multi-threaded Mobile application
- Memory states
- Distributed memory synchronization
- PhoneOS
- Executes concurrently with non-offloaded threads
- Offloaded threads
- Memory states
- Distributed memory synchronization
- RemoteOS
- in-sync
- via network
Web Security & Isolation Model

- Currently: Both parties should both agree to communication.
- Previously: Including party should agree to communication.