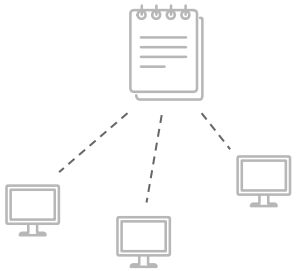
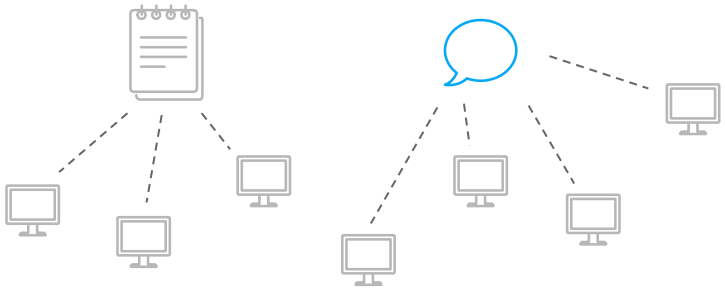
TOR
LOCATING HIDDEN SERVERS

Lasse Øverlier & Paul Syverson
Presented by Andy Zeng

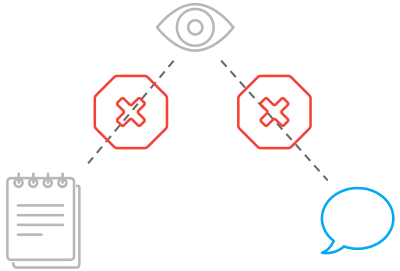
Tor's Hidden Services



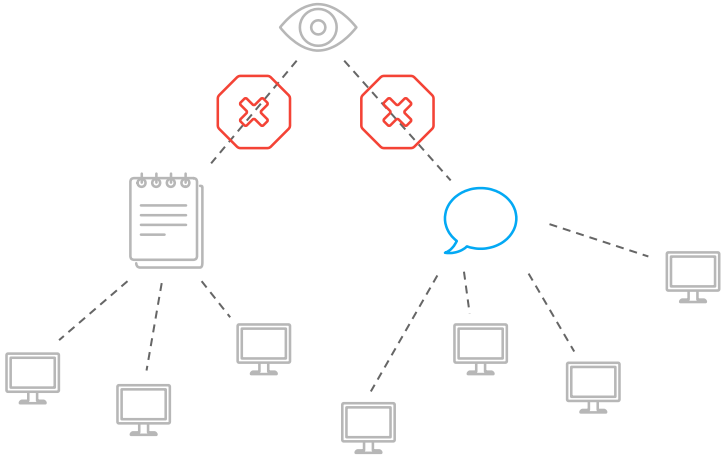
Tor's Hidden Services



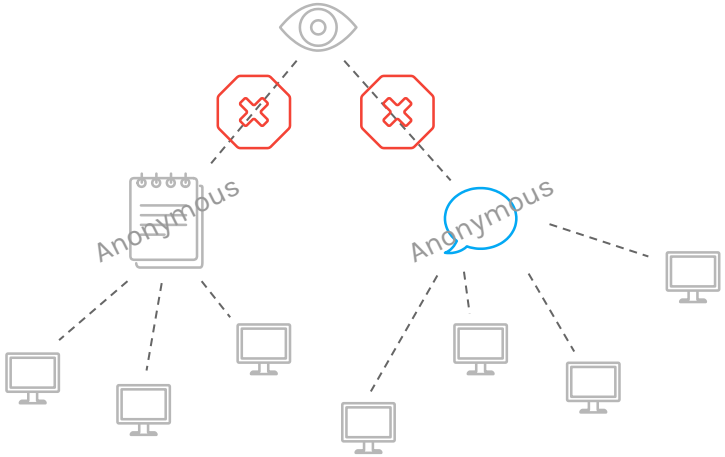
Tor's Hidden Services



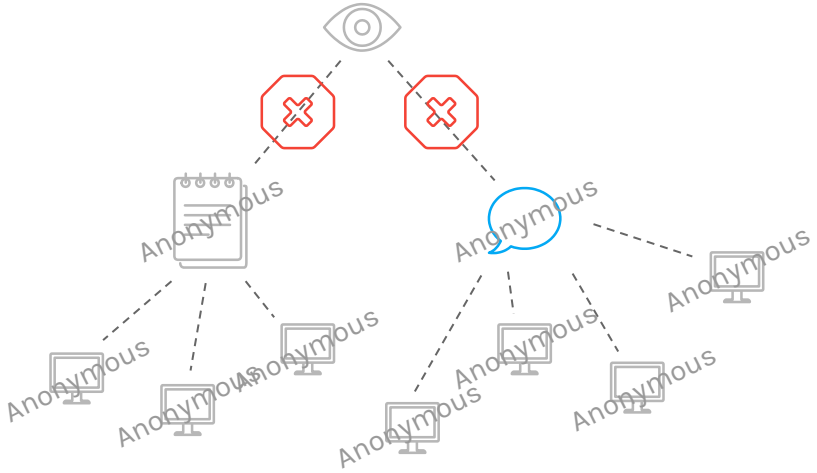
Tor's Hidden Services



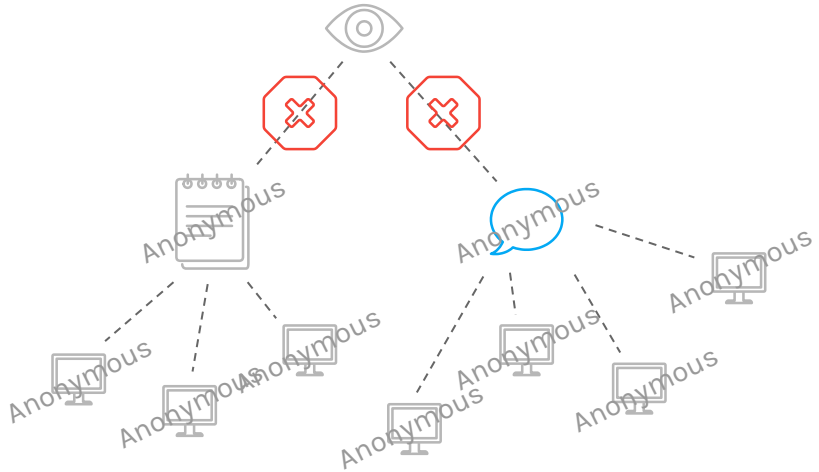
Tor's Hidden Services



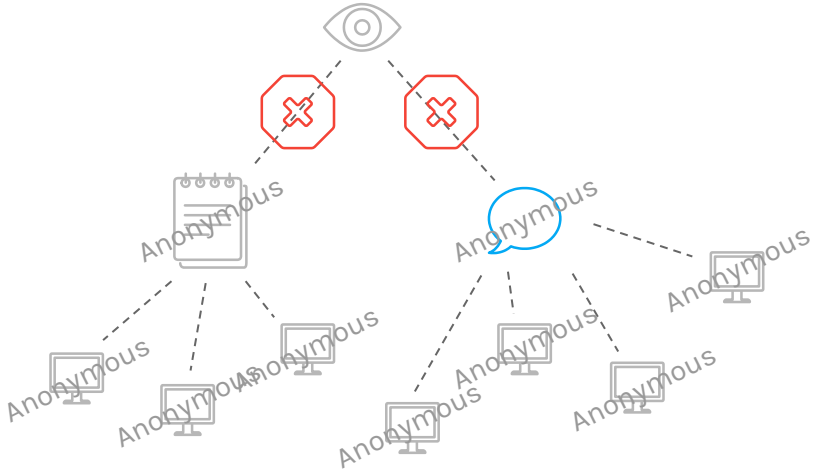
Tor's Hidden Services



Tor's Hidden Services



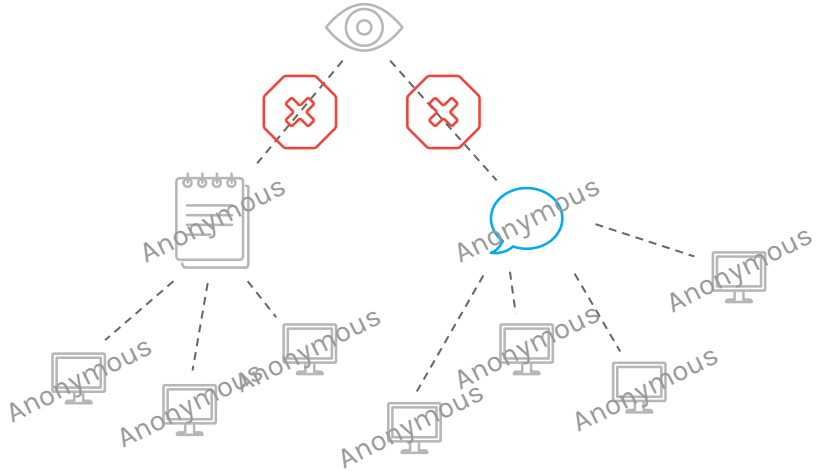
Tor's Hidden Services



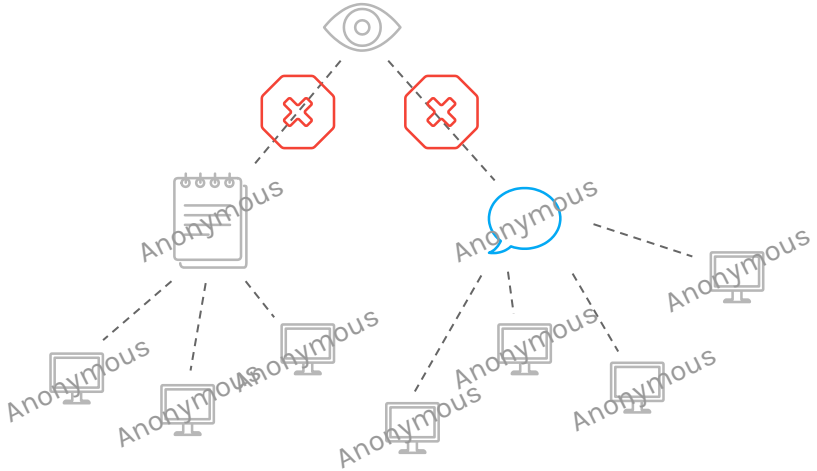
Client

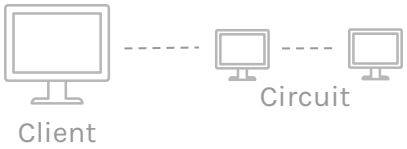
Server

Tor's Hidden Services

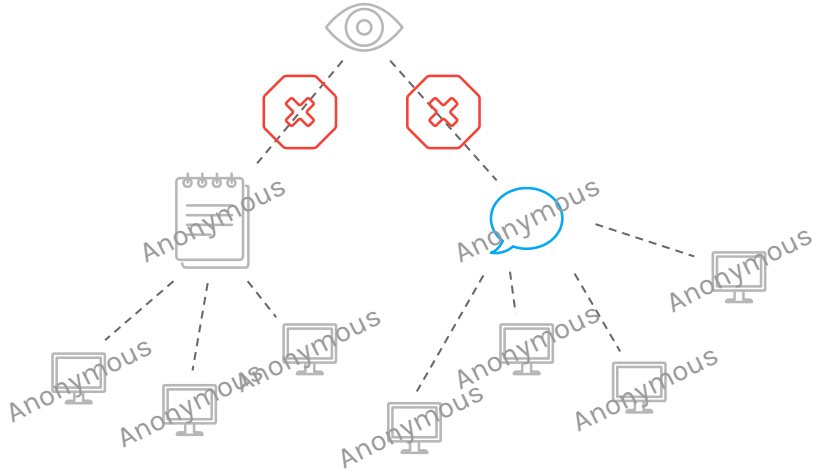


Tor's Hidden Services





Tor's Hidden Services

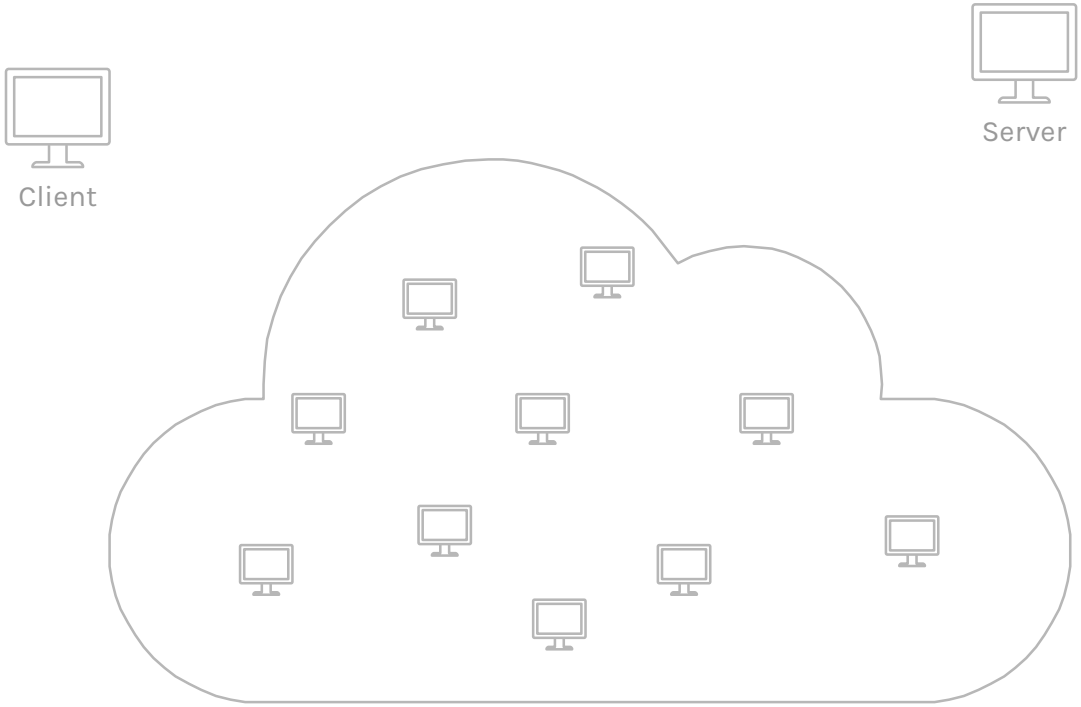


Rendezvous **Protocol**

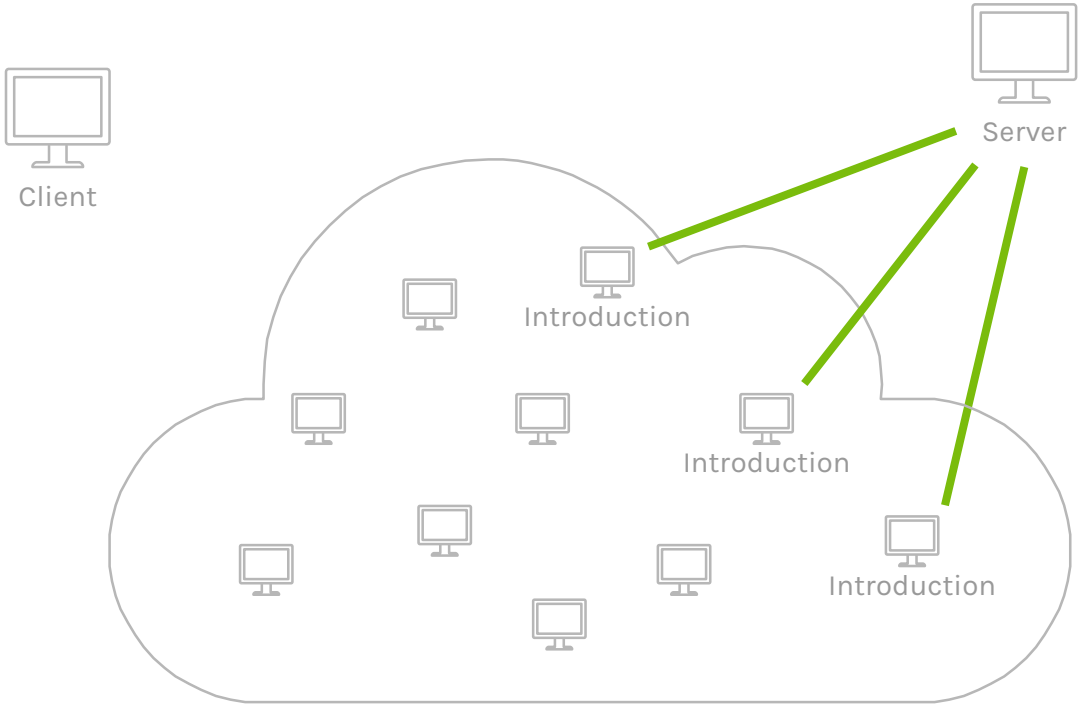
Client

Server

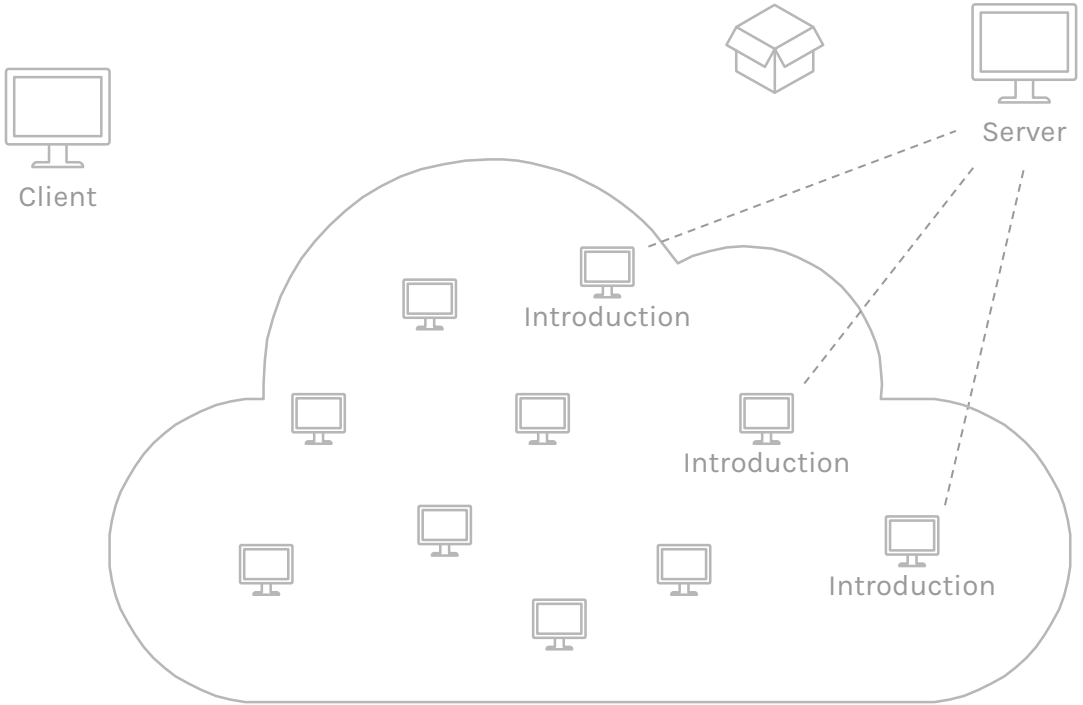
Rendezvous **Protocol**



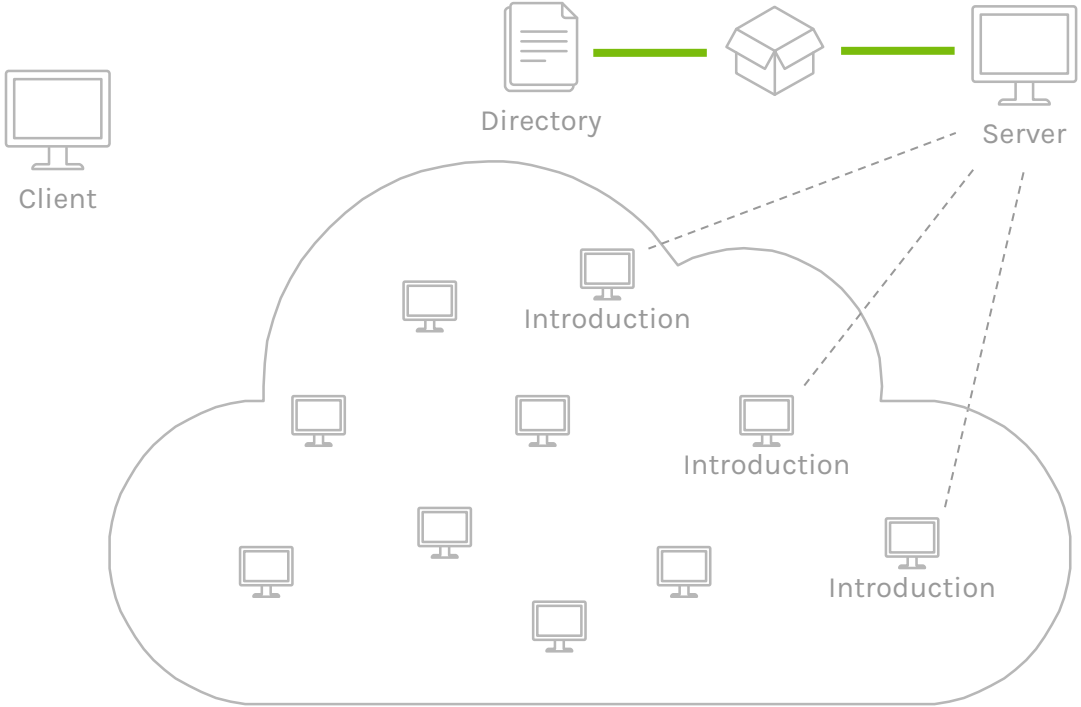
Rendezvous **Protocol**



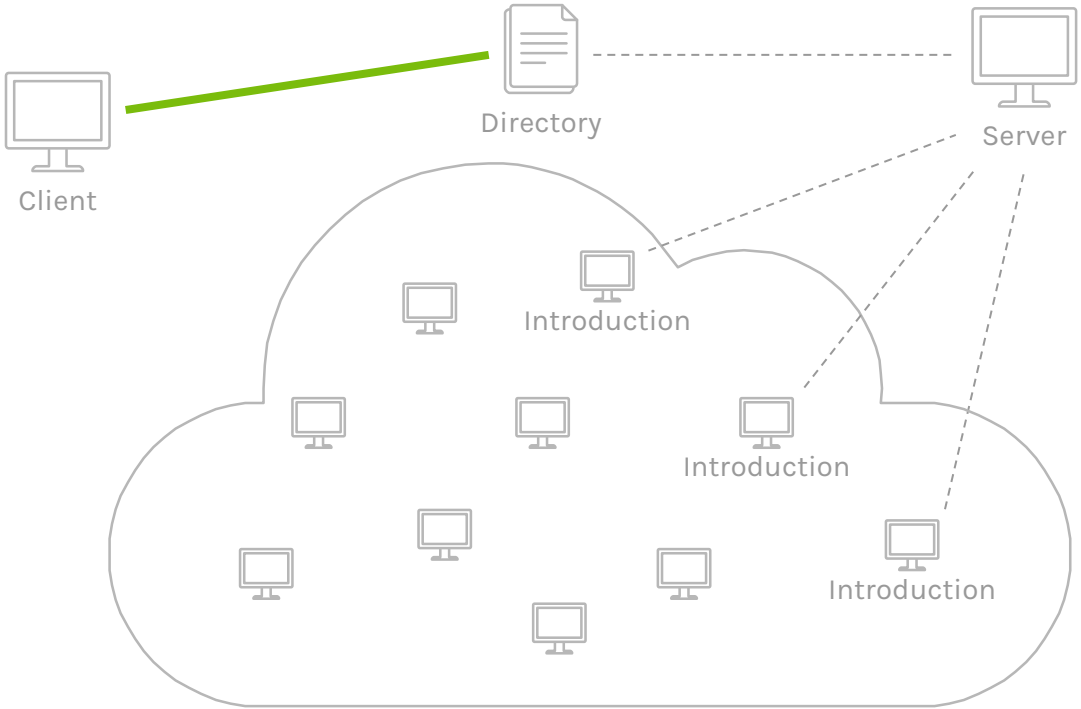
Rendezvous **Protocol**



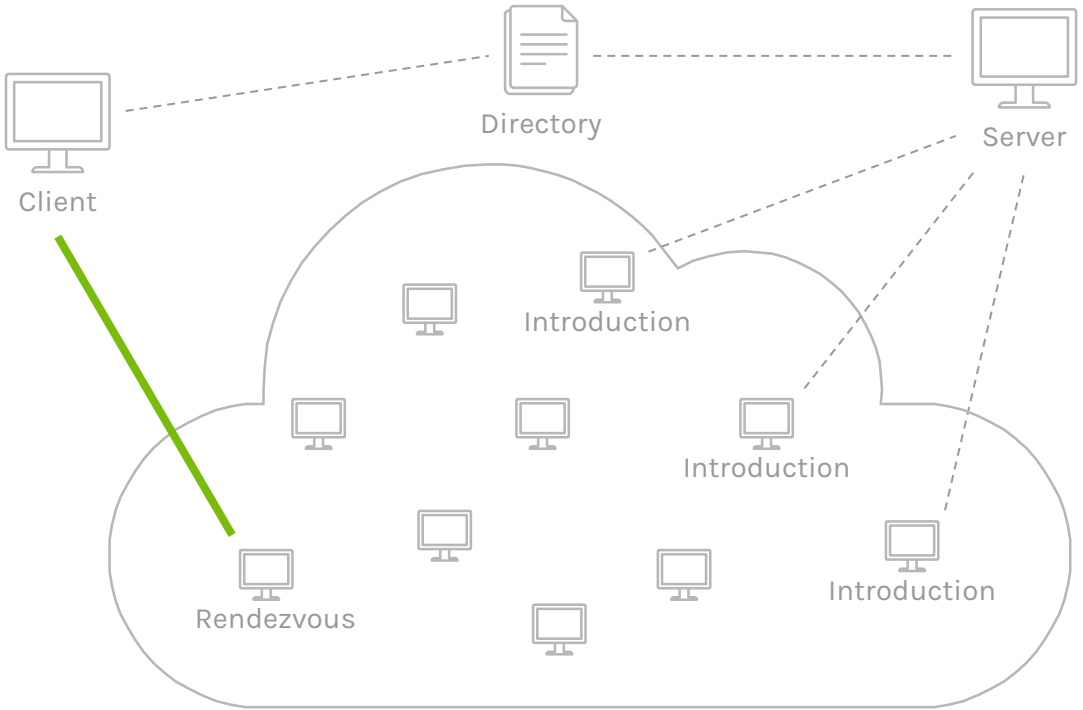
Rendezvous Protocol



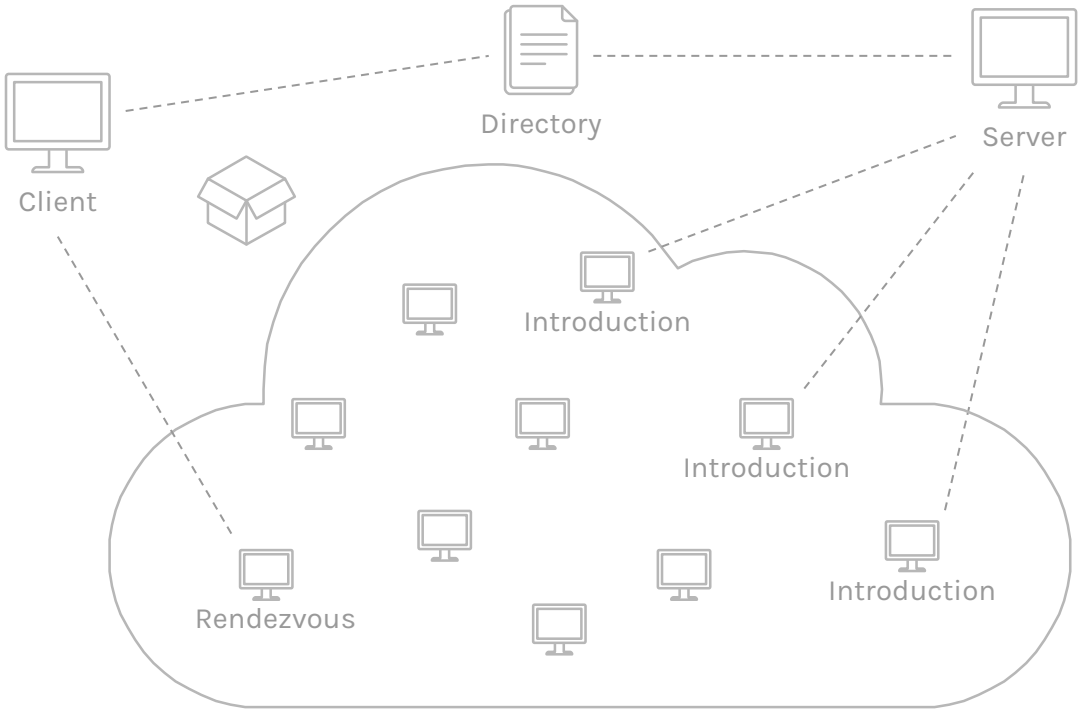
Rendezvous **Protocol**



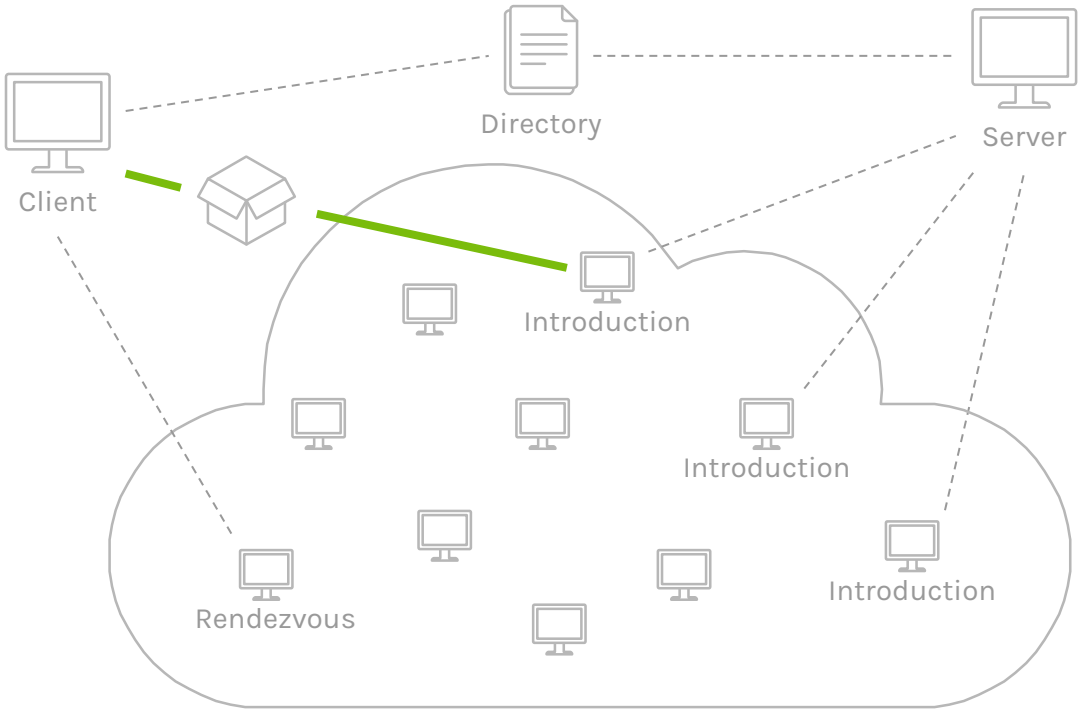
Rendezvous Protocol



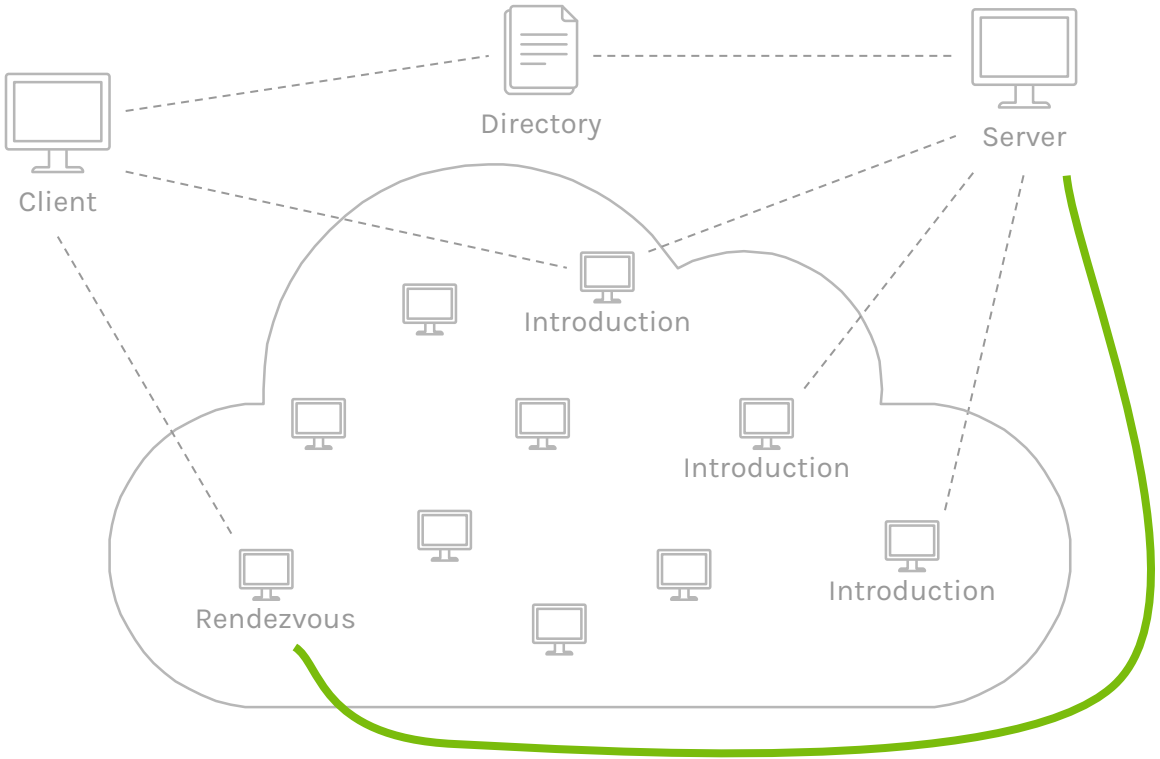
Rendezvous Protocol



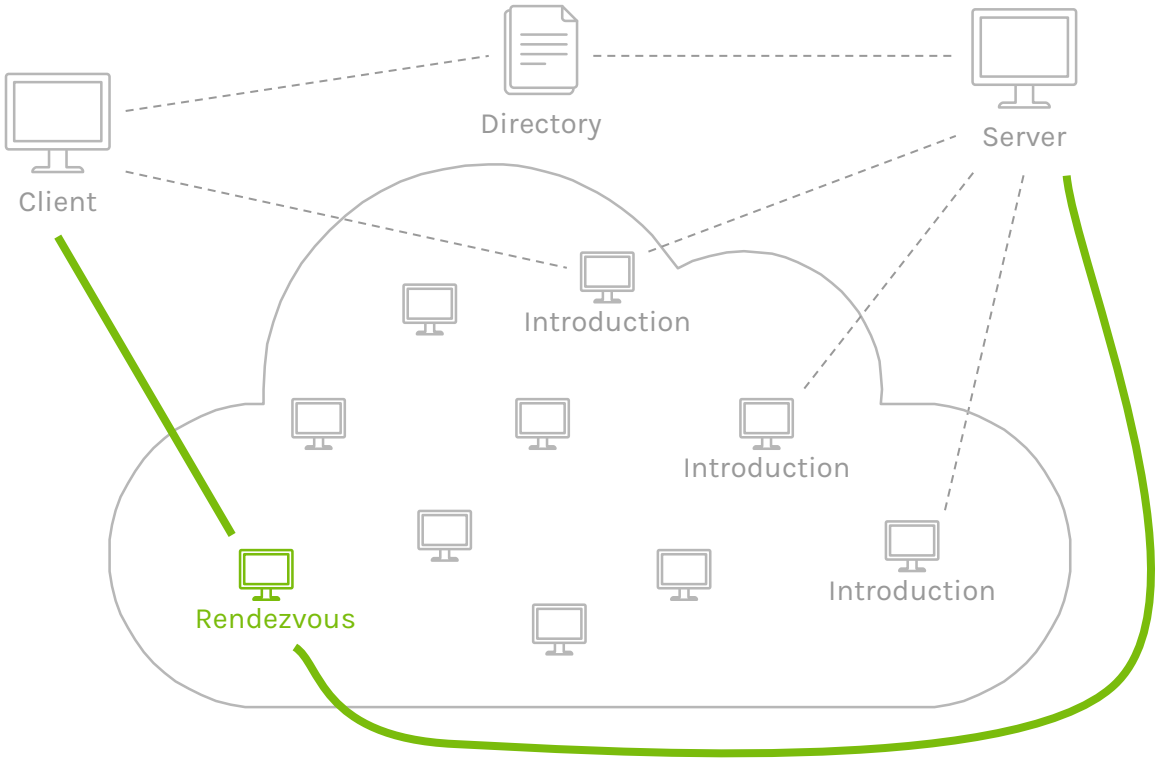
Rendezvous Protocol



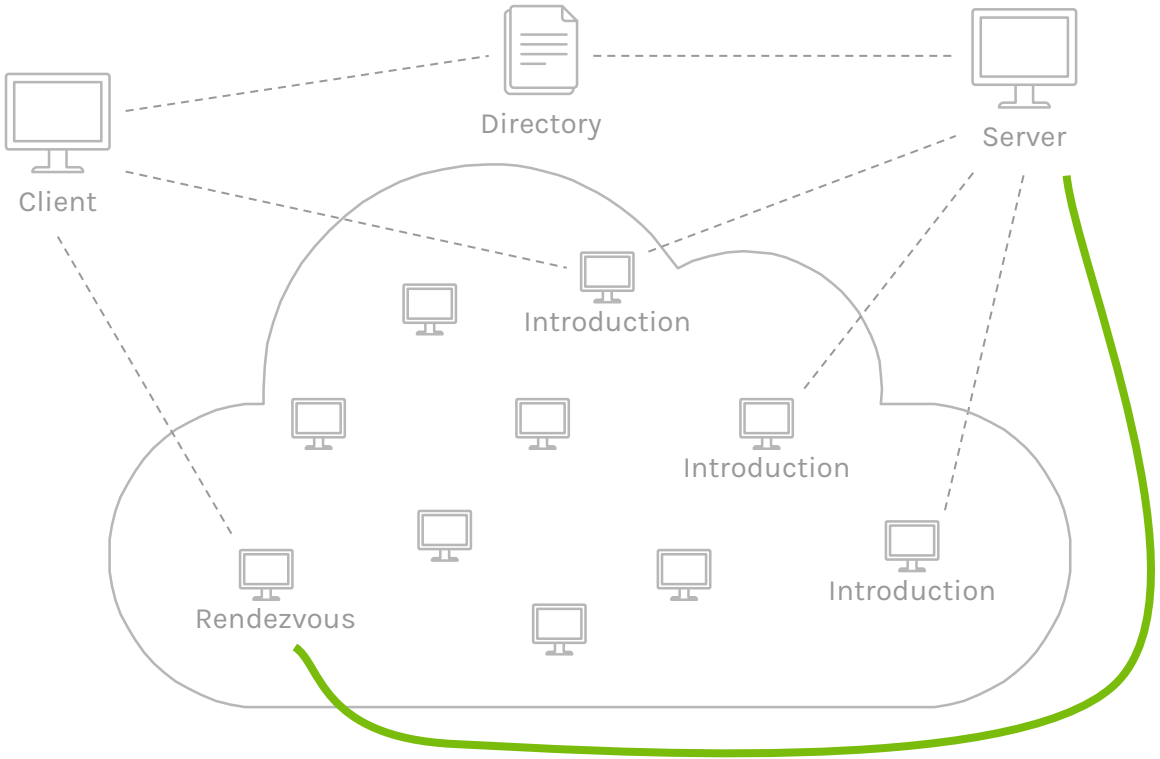
Rendezvous Protocol



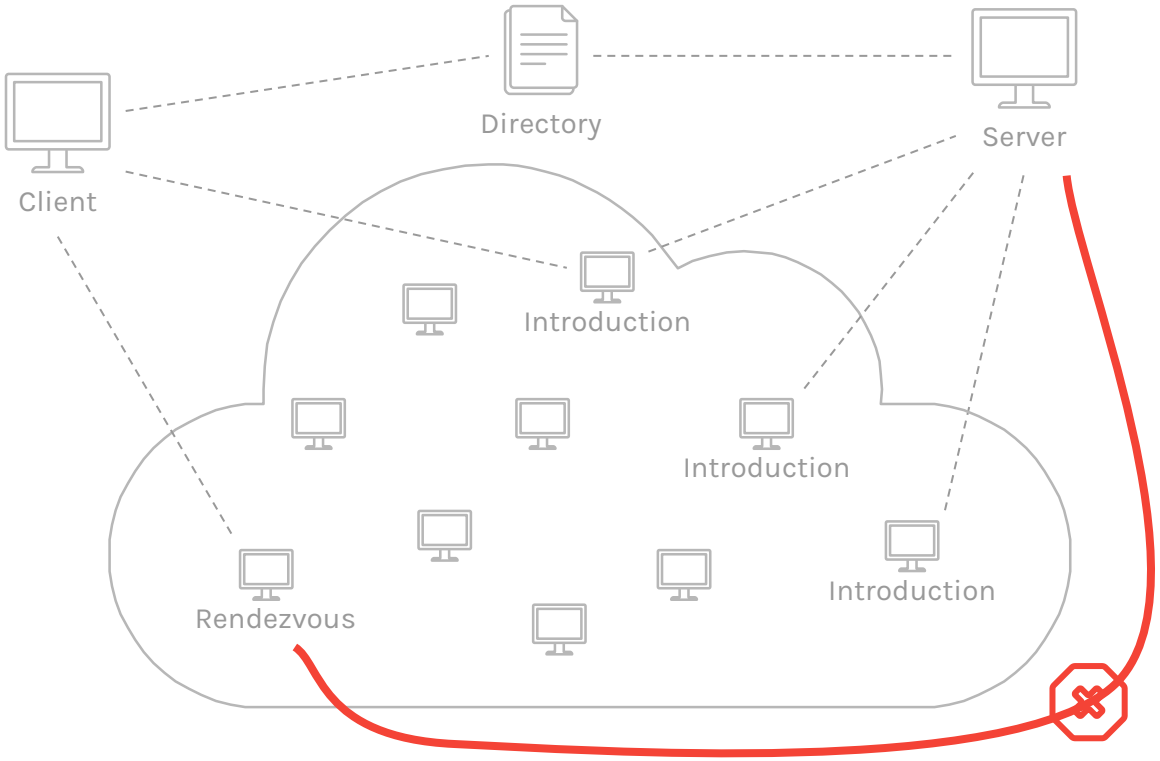
Rendezvous Protocol



Rendezvous Protocol



Rendezvous Protocol

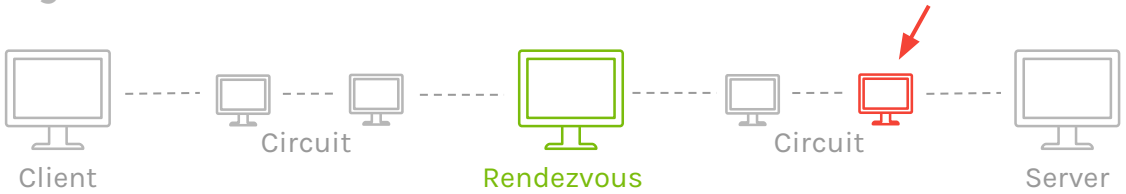


The Attack

Original:

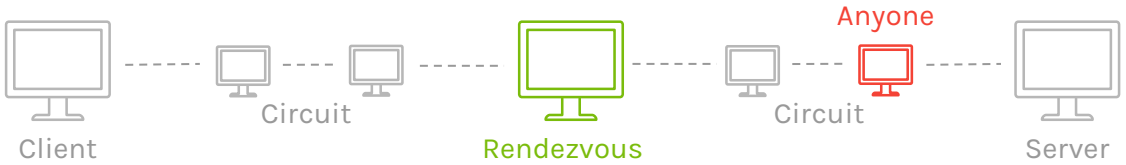
The Attack

Original:



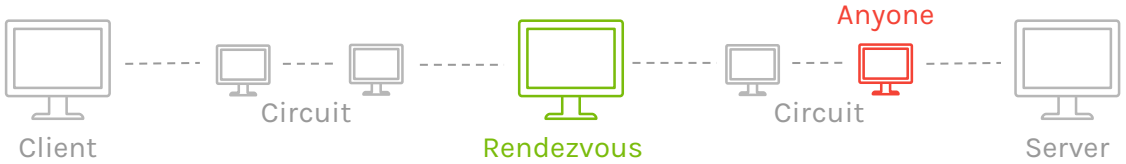
The Attack

Original:

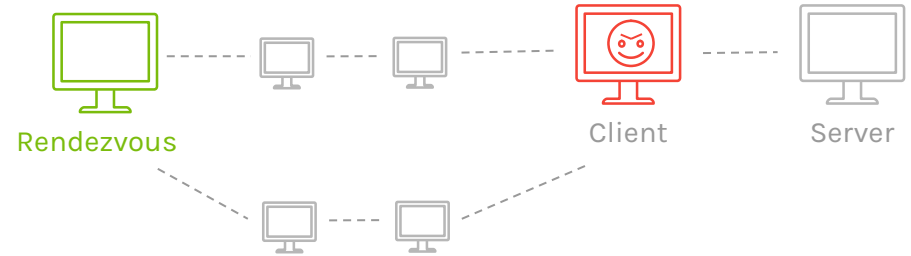


The Attack

Original:



Objective:

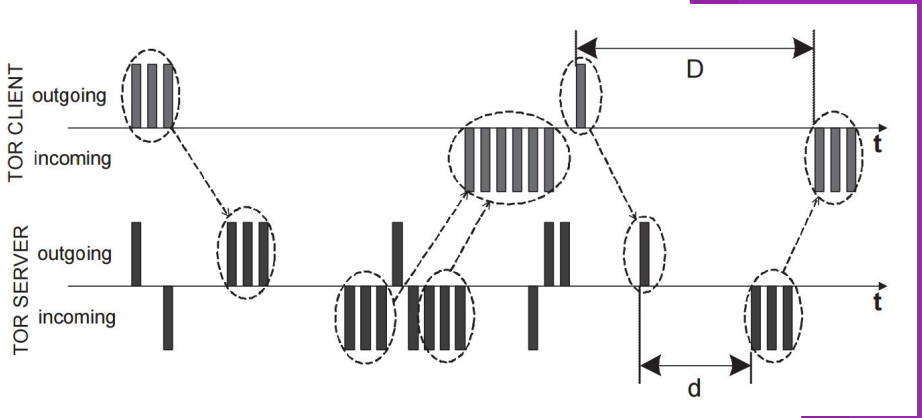


EXPERIMENTAL **SETUP**

- 2 hidden services on Tor
- Changes to client application code
  - Client -> 1 hop -> Rendezvous point
  - Easily create/destroy circuits to hidden server
  - Middleman node
  - Make middleman node trust-worthy to others

MODES OF **ATTACK**

- Timing analysis
- Service location attack
- Predecessory attack
- Distance attack



Owning the Rendezvous Point

MODES OF **ATTACK**

- Timing analysis
- Service location attack
- Predecessory attack
- Distance attack

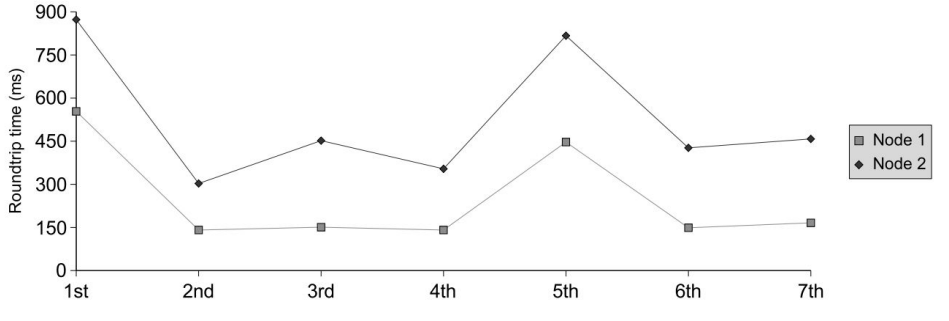
Table 1. Experimental results of our attacks.

	Sample time	Time to first match	Circuits completed	Matched circuits	Largest single IP	Second largest
Server 1	7.8h	15 min	676	37	46%	5%
Server 1	6.8h	3 min	432	26	54%	7%
Server 2	4.9h	28 min	447	31	71%	3%
Server 2	10.6h	3 min	990	56	54%	7%

Owning the Rendezvous Point

MODES OF **ATTACK**

- Timing analysis
- Service location attack
- Predecessory attack
- Distance attack



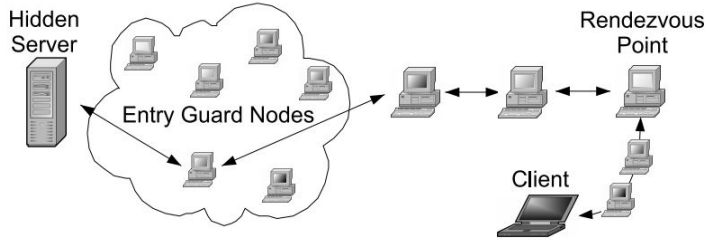
Owning the Rendezvous Point

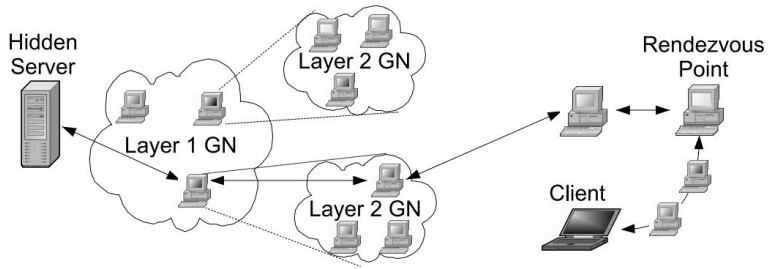
COUNTERMEASURES

- Dummy traffic
- Extend path between hidden server and rendezvous point
- Entry guard nodes (best)

Table 2. Experimental results when Hidden Server is using Entry Guard Nodes.

	Total circuits completed	Matched circuits	Largest single IP	Second largest	Third largest
Test 1	292	8	7	1	0
Test 2	106	6	5	1	0
Test 3	296	13	12	1	0
Test 4	292	10	4	3	3





WEAKNESSES

- Little address on edge cases
  - Dummy traffic vs timing signatures
  - Distance attack vs latency
  - Number of hidden services for experiments
- Solution is not perfect

Table 2. Experimental results when Hidden Server is using Entry Guard Nodes.

	Total circuits completed	Matched circuits	Largest single IP	Second largest	Third largest
Test 1	292	8	7	1	0
Test 2	106	6	5	1	0
Test 3	296	13	12	1	0
Test 4	292	10	4	3	3