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
Tor’s **Hidden Services**

![Diagram of Tor’s Hidden Services](image)
Tor’s Hidden Services

Diagram showing the connection between a client, circuit, and server in Tor's hidden services.
Tor’s **Hidden Services**
Rendezvous Protocol
Rendezvous Protocol
Rendezvous Protocol
Rendezvous Protocol

Client

Server

Introduction

Introduction

Introduction
Rendezvous Protocol
Rendezvous Protocol
Rendezvous Protocol

Client

Directory

Server

Introduction

Rendezvous

Introduction

Introduction
Rendezvous Protocol

- Client
- Directory
- Server
- Introduction
- Rendezvous
Rendezvous Protocol
Rendezvous Protocol
Rendezvous Protocol

Client

Directory

Server

Rendezvous

Introduction
Rendezvous Protocol
Rendezvous Protocol
The **Attack**
The **Attack**

Original:
The **Attack**

Original:
The **Attack**

**Original:**

- Client
- Circuit
- Rendezvous
- Circuit
- Server

**Objective:**

- Rendezvous
- Client
- Server
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.

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

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>
<thead>
<tr>
<th>Test</th>
<th>Total circuits completed</th>
<th>Matched circuits</th>
<th>Largest single IP</th>
<th>Second largest</th>
<th>Third largest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1</td>
<td>292</td>
<td>8</td>
<td>7</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Test 2</td>
<td>106</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Test 3</td>
<td>296</td>
<td>13</td>
<td>12</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Test 4</td>
<td>292</td>
<td>10</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
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.**

<table>
<thead>
<tr>
<th>Test</th>
<th>Total circuits completed</th>
<th>Matched circuits</th>
<th>Largest single IP</th>
<th>Second largest</th>
<th>Third largest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1</td>
<td>292</td>
<td>8</td>
<td>7</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Test 2</td>
<td>106</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Test 3</td>
<td>296</td>
<td>13</td>
<td>12</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Test 4</td>
<td>292</td>
<td>10</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>