Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor

Rob Jansen, U.S. Naval Research Laboratory
Tavish Vaidya, Georgetown University
Micah Sherr, Georgetown University
Explore the costs and effects of bandwidth denial-of-service attacks on Tor

3 Gbit/s

$140 - $1.6K / mo.

47% Slower
Anonymous Communication
- Separates identification from routing
- Provides unlinkable communication
- Protects user privacy and safety online

Tor is Popular
- ~2-8 million daily active users
- ~6,500 volunteer relays
- Transferring ~200 Gbit/s
Anonymity Attacks against Tor

Website fingerprinting attacks
• CCSW’09, WPES’11, CCS’12, WPES’13, Sec’14, NDSS’16, Sec’16, NDSS’18, CCS’18

Traffic correlation attacks
• S&P’05, PET’07, Sec’09, CCS’09, TISSEC’10, CCS’11, PETS’13, CCS’13, CN’13, NDSS’14, CCS’18,

Routing attacks
• WPES’07, CCS’07, Sec’15, PETS’16, S&P’17, PETS’18
Anonymity Attacks against Tor

Website fingerprinting attacks
- CCSW'09, WPES'11, CCS'12, WPES'13, Sec'14, NDSS'16, Sec'16, NDSS'18, CCS'18

Traffic correlation attacks
- S&P'05, PET'07, Sec'09, CCS'09, TISSEC'10, CCS'11, PETS'13, CCS'13, CN'13, NDSS'14, CCS'18

Routing attacks
- WPES'07, CCS'07, Sec'15, PETS'16, S&P'17, PETS'18
Our Focus: Denial-of-Service Attacks
Our Focus: Denial-of-Service Attacks
Our Focus: Denial-of-Service Attacks

Borisov et al. CCS’07
Selective service refusal

Geddes et al. WPES’14
Socket Exhaustion

2007 2008 2009 2013 2014 2019
Our Focus: Denial-of-Service Attacks

- Borisov et al. CCS’07
  Selective service refusal

- Pappas et al. InfoSec’08
  Packet Spinning

- Barbera et al. ESORICS’13
  Cell Flood

- Geddes et al. WPES’14
  Socket Exhaustion

2007 2008 2009 2013 2014 2019
Our Focus: Denial-of-Service Attacks

- Borisov et al. CCS’07 Selective service refusal
- Evans et al. Sec’09 Long Paths
- Geddes et al. WPES’14 Socket Exhaustion
- Pappas et al. InfoSec’08 Packet Spinning
- Barbera et al. ESORICS’13 Cell Flood
Our Focus: Denial-of-Service Attacks

- Borisov et al. CCS’07
  Selective service refusal

- Pappas et al. InfoSec’08
  Packet Spinning

- Evans et al. Sec’09
  Long Paths

- Barbera et al. ESORICS’13
  Cell Flood

- Geddes et al. WPES’14
  Socket Exhaustion

- Jansen et al. NDSS’14
  Sniper Attack

2007 2008 2009 2013 2014 2019
Our Focus: Denial-of-Service Attacks

- Borisov et al. CCS’07
  Selective service refusal
- Pappas et al. InfoSec’08
  Packet Spinning
- Evans et al. Sec’09
  Long Paths
- Barbera et al. ESORICS’13
  Cell Flood
- Geddes et al. WPES’14
  Socket Exhaustion
- Jansen et al. NDSS’14
  Sniper Attack
- This Work
  Long Paths + Sniper

Timeline:
- 2007
- 2008
- 2009
- 2013
- 2014
- 2019
DoS against Tor – A Realistic Threat

[tor-project] Ongoing DDoS on the Network - Status

David Goulet dgoulet at torproject.org
Wed Dec 20 16:15:39 UTC 2017

[tor-relays] could Tor devs provide an update on DOS attacks?

Roger Dingledine arma at mit.edu
Tue Jan 16 08:27:21 UTC 2018

https://trac.torproject.org/projects/tor/ticket/24902
### Research Questions and Summary of Results

<table>
<thead>
<tr>
<th>Component</th>
<th>Cost</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridges</td>
<td>$17,000 / mo.</td>
<td>44% slower</td>
</tr>
<tr>
<td>TorFlow BW Scanners</td>
<td>$2,800 / mo.</td>
<td>80% slower</td>
</tr>
<tr>
<td>Relays</td>
<td>$140 - $1,600 / mo. or</td>
<td>47% slower or</td>
</tr>
<tr>
<td></td>
<td>$6,300 / mo.</td>
<td>120% slower</td>
</tr>
</tbody>
</table>
### Component | Cost | Effect
--- | --- | ---
Bridges | $17,000 / mo. | 44% slower
TorFlow BW Scanners | $2,800 / mo. | 80% slower
Relays | $140 - $1,600 / mo. or $6,300 / mo. | 47% slower or 120% slower

**Ethical research:**
- No attacks on the public Tor network
- Analyzed performance effects with Shadow
- Conducted some Tor measurements as client, stored no information about users
## Research Questions and Summary of Results

<table>
<thead>
<tr>
<th>Component</th>
<th>Cost</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridges</td>
<td>$17,000 / mo.</td>
<td>44% slower</td>
</tr>
<tr>
<td>TorFlow BW Scanners</td>
<td>$2,800 / mo.</td>
<td>80% slower</td>
</tr>
<tr>
<td>Relays</td>
<td>$140 - $1,600 / mo. or</td>
<td>47% slower or</td>
</tr>
<tr>
<td></td>
<td>$6,300 / mo.</td>
<td>120% slower</td>
</tr>
</tbody>
</table>
Attack
How Tor Works

= Circuit

= Stream
Step 1: Build 8-hop circuit
The Relay Congestion Attack

Step 1: Build 8-hop circuit

Can be targeted or indiscriminate
The Relay Congestion Attack

Step 1: Build 8-hop circuit
Step 2: GET large files
The Relay Congestion Attack

Step 1: Build 8-hop circuit
Step 2: GET large files
Step 3: Stop reading
The Relay Congestion Attack

Step 1: Build 8-hop circuit
Step 2: GET large files
Step 3: Stop reading
Step 4: Send flow control cells
The Relay Congestion Attack

Step 5: Repeat!!!

New entry relays

New sockets
Evaluation
Use Shadow for evaluation
· Private Tor network for safety
· 634 relays (10% size, capacity of Tor)
· 15,000 clients and 2,000 servers generating traffic through Tor

Explore network effects
· Attack strength (num. attack circuits)
· Network load, attacker resource usage, client performance

https://github.com/shadow/shadow
Bandwidth Used by Attacker and Tor Network

![Graph showing Bandwidth Used by Attacker and Tor Network](graph.png)
Bandwidth Used by Attacker and Tor Network

Bandwidth Amplification Factors:

20k Circuits

Cumulative Fraction

Attacker Throughput (MiB/s)

0 50 100 150 200

0 0.2 0.4 0.6 0.8 1.0

Stop Reading

20k Circ.

No Attack

Aggregate Tor Relay Goodput (GiB/s)

0.0 0.2 0.4 0.6 0.8 1.0

0.8 1.0 1.2 1.4 1.6 1.8 2.0

Cumulative Fraction

Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor | 29
Bandwidth Amplification Factors:

20k Circuits: 6.7

Stop Reading: 26
Effect on Client Performance

20k Circuits

**TTFB:** +138%

**TTLB:** +120%

Download Time (s)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>TTFB All</th>
<th>TTLB 50KiB</th>
<th>TTLB 1MiB</th>
<th>TTLB 5MiB</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20k Circ. Stop Reading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Effect on Client Performance

20k Circuits

TTFB: +138%

Stop Reading
TTFB: +48%

TTLB: +120%

TTLB: +47%
Requirements for “stop reading” attack
- 200,000 circuits
- 3 Gbit/s, 20 IP addresses

Cost of Bandwidth and IP addresses
- 3 dedicated servers at 1 Gbit/s each, amortized cost of 0.70 $/hour/Gbit/s
- 17 additional IPs at $5 each, $85 total

Total Cost Estimates
- Conservative: $1,647 per month
- Optimistic: $140 per month ($7 * 20 VPSes)
Comparison to relay Sybil attacks with the same bandwidth budget (3 Gbit/s)

Sybil DoS Attack

Sybil Deanonymization Attack
Comparison to Sybil Attacks

Comparison to relay Sybil attacks with the same bandwidth budget (3 Gbit/s)

Sybil DoS Attack

- Goal: drop all circuits containing Sybil relays
- Exit BW is scarcest and gives highest probability of selection
- 3 Gbit/s = 4.5% dropped circuits
Comparison to relay Sybil attacks with the same bandwidth budget (3 Gbit/s)

**Sybil DoS Attack**
- Goal: drop all circuits containing Sybil relays
- Exit BW is scarcest and gives highest probability of selection
- 3 Gbit/s = 4.5% dropped circuits

**Sybil Deanonymization Attack**
- Goal: appear on both ends of circuits to compromise anonymity
- 5:1 guard-to-exit BW allocation
- 2.8% guard * 0.8% exit = 0.02% total circuits compromised
Mitigation
Mitigations to Relay Congestion Attack

Ability to stop reading from circuits

- Authenticated SENDMEs, Tor Proposal 289, implemented in 0.4.1.1-alpha

Inject nonce in every 50 cells

Must read and return nonce in SENDME cell
Mitigations to Relay Congestion Attack

Ability to stop reading from circuits
• Authenticated SENDMEs, Tor Proposal 289, implemented in 0.4.1.1-alpha

Ability to build 8 hop circuits
• Reduce to 4 hops to reduce BW amplification factor
Mitigations to Relay Congestion Attack

Ability to stop reading from circuits
- Authenticated SENDMEs, Tor Proposal 289, implemented in 0.4.1.1-alpha

Ability to build 8 hop circuits
- Reduce to 4 hops to reduce BW amplification factor

Ability to use any relay as entry
- Privacy-preserving defense against Sybil attacks
- Detect, measure, and prevent such attacks
Summary

Contributions

• Bridge congestion attack: $17K/mo., 44% slower
• Bandwidth authority attack: $2.6K/mo., 80% slower
• Relay congestion attack: $140-$1.6K/mo., 47% slower (or $6.3K/mo., 120% slower)

Future Work

• Deploy simple mitigation techniques in short term
• Need research in Sybil attack detection, measurement, and prevention

Contact

• <rob.g.jansen@nrl.navy.mil>, robgjansen.com, @robgjansen