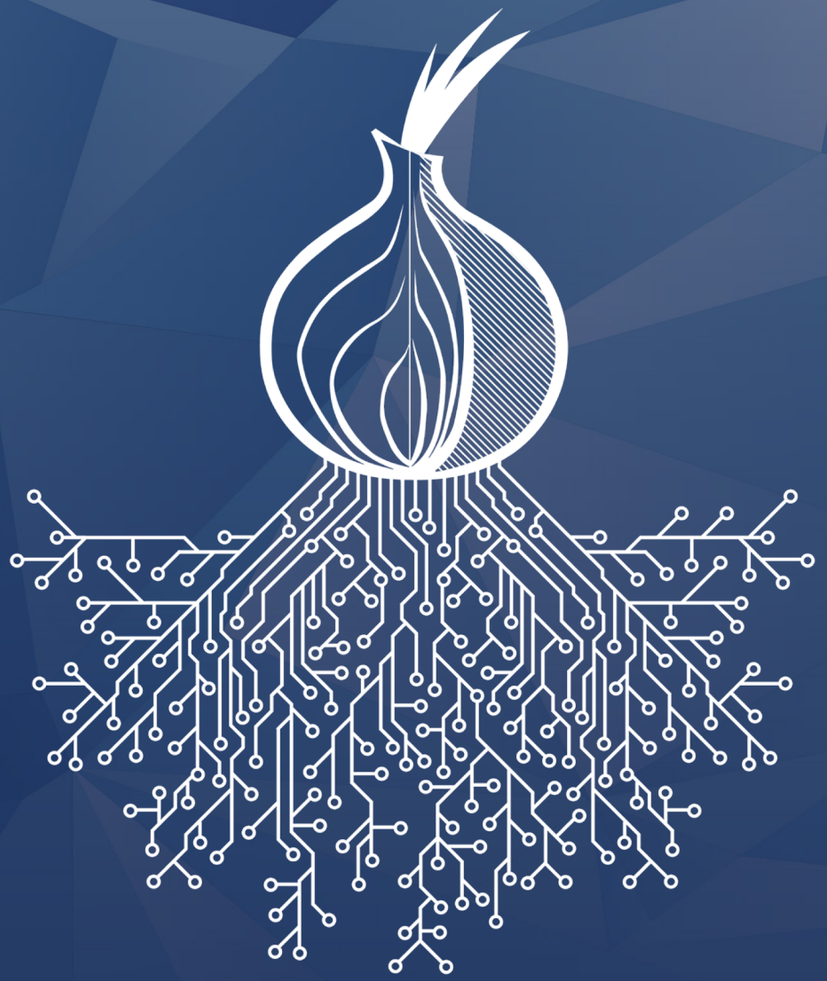
U.S. NAVAL RESEARCH LABORATORY

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



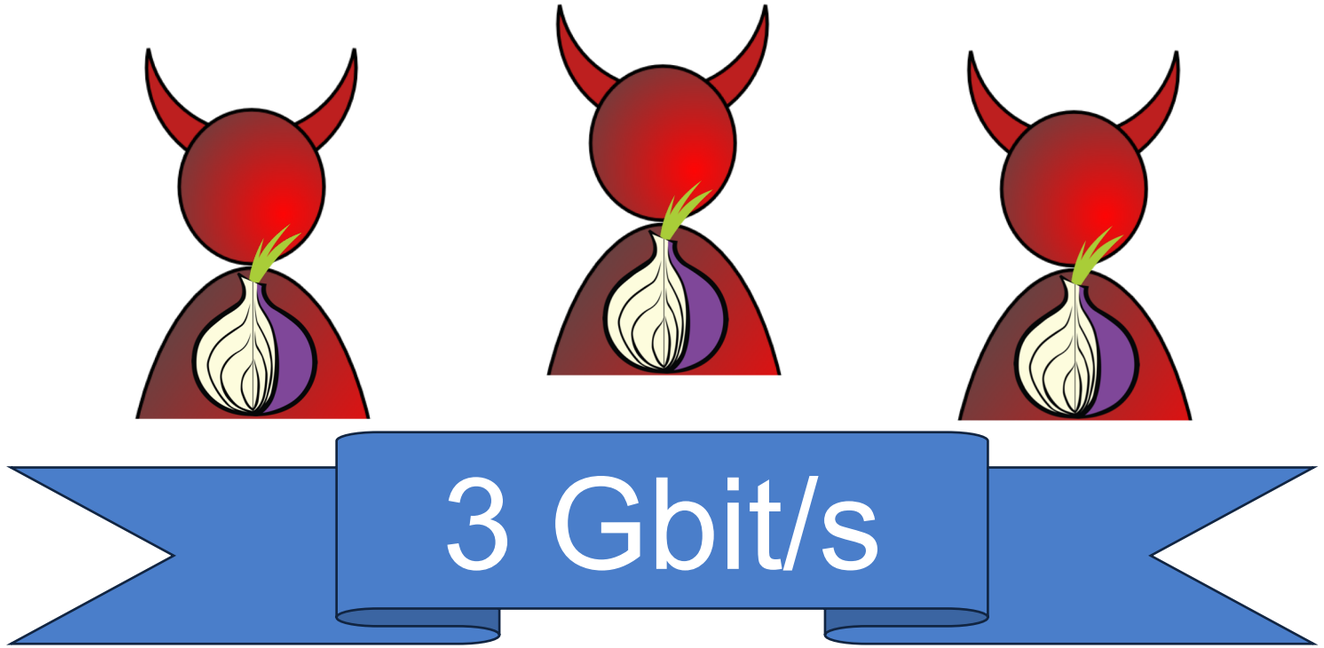
Rob Jansen, U.S. Naval Research Laboratory
Tavish Vaidya, Georgetown University
Micah Sherr, Georgetown University

Rob Jansen
Center for High Assurance Computer Systems
U.S. Naval Research Laboratory

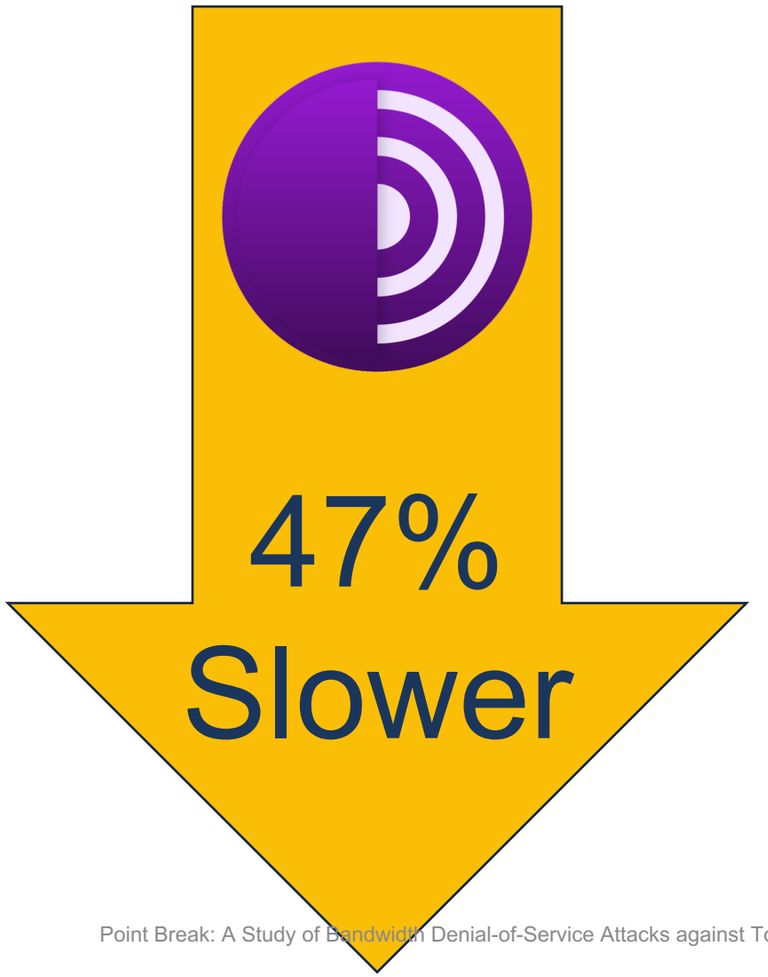
28th USENIX Security Symposium
Hyatt Regency, Santa Clara, CA, USA
August 16th, 2019

Most Exciting Contribution

Explore the costs and effects of bandwidth denial-of-service attacks on Tor



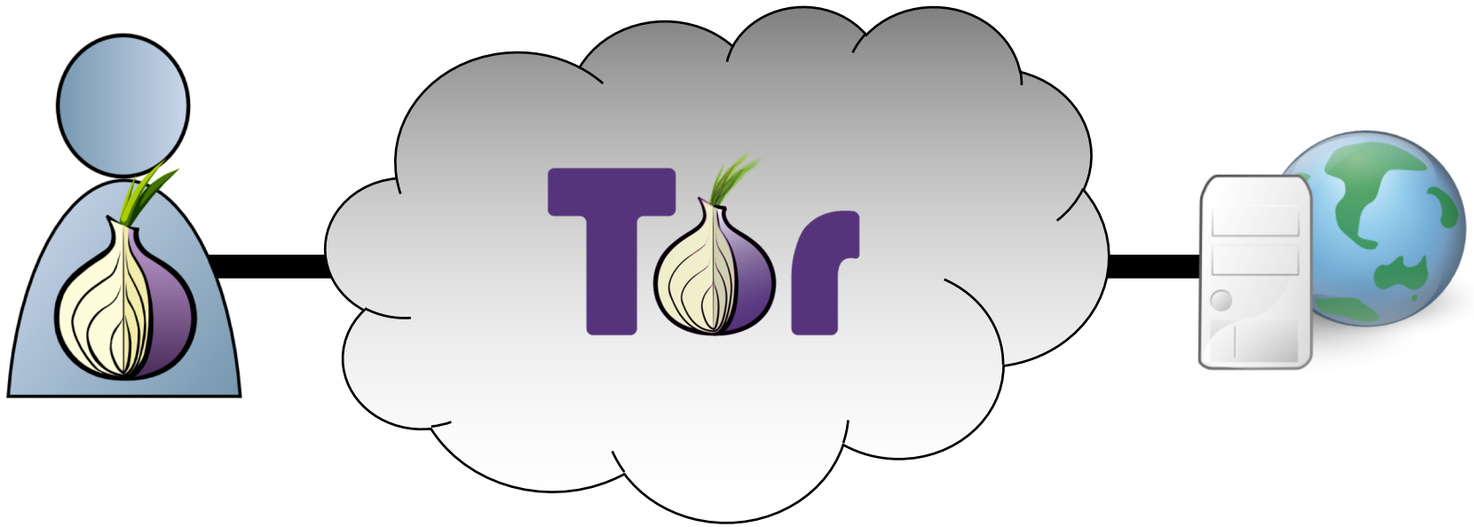
$140 - $1.6K / mo.



Tor Protects Users

Anonymous Communication

- Separates identification from routing
- Provides unlinkable communication
- Protects user privacy and safety online



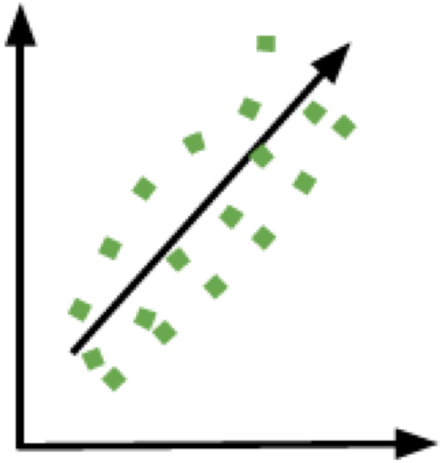
Tor is Popular

- ~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



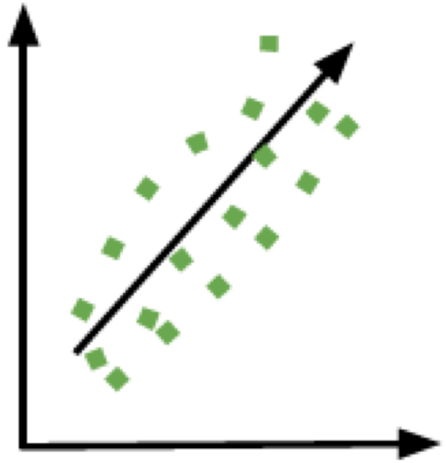
Traffic correlation attacks

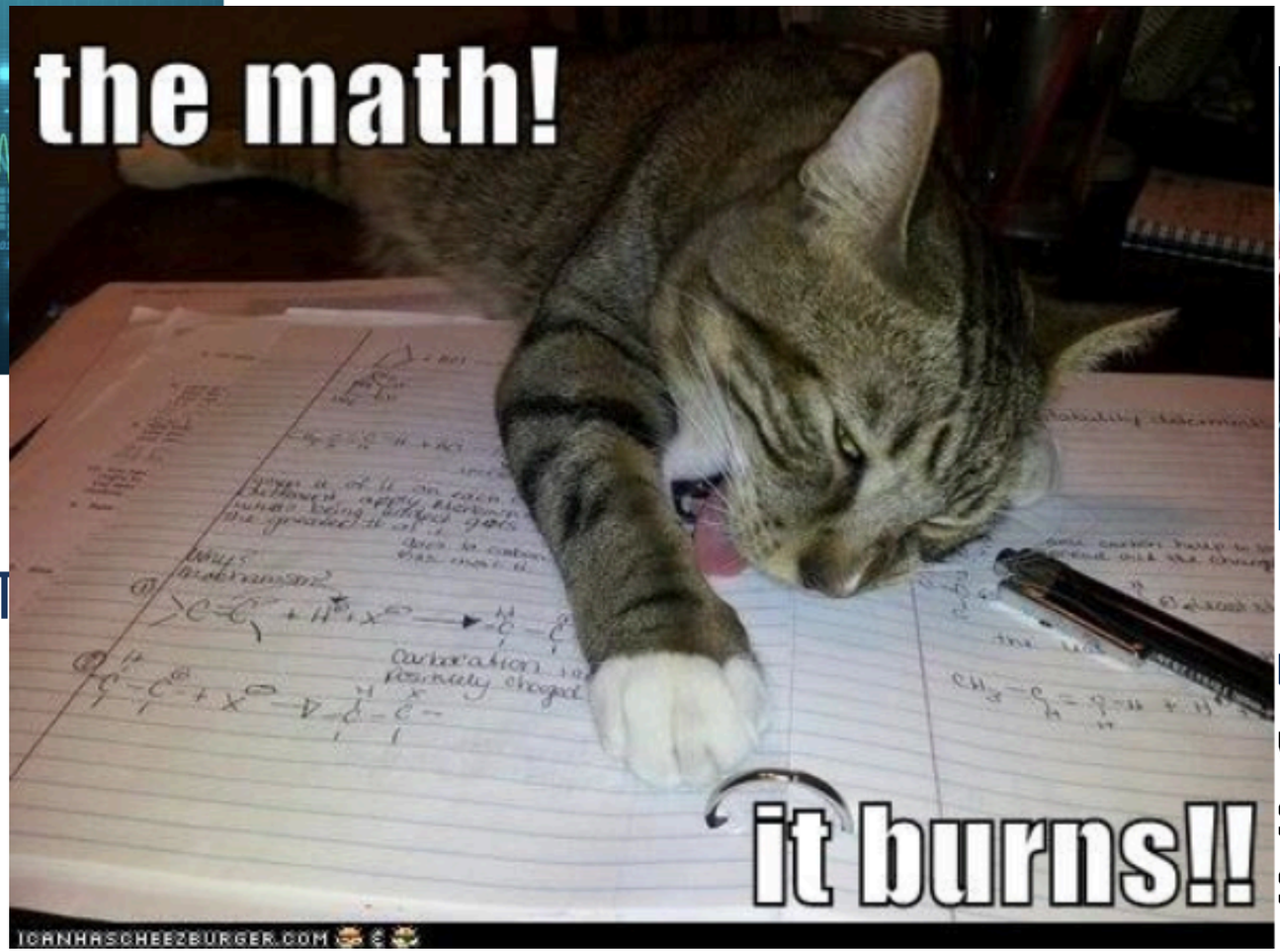
- S&P'05, PET'07, Sec'09, CCS'09, TISSEC'10, CCS'11, PETS'13, CCS'13, CN'13, NDSS'14, CCS'18,

Routing attacks

- WPES'07, CCS'07, Sec'15, PETS'16, S&P'17, PETS'18

Anonymity Attacks against Tor





uting attacks

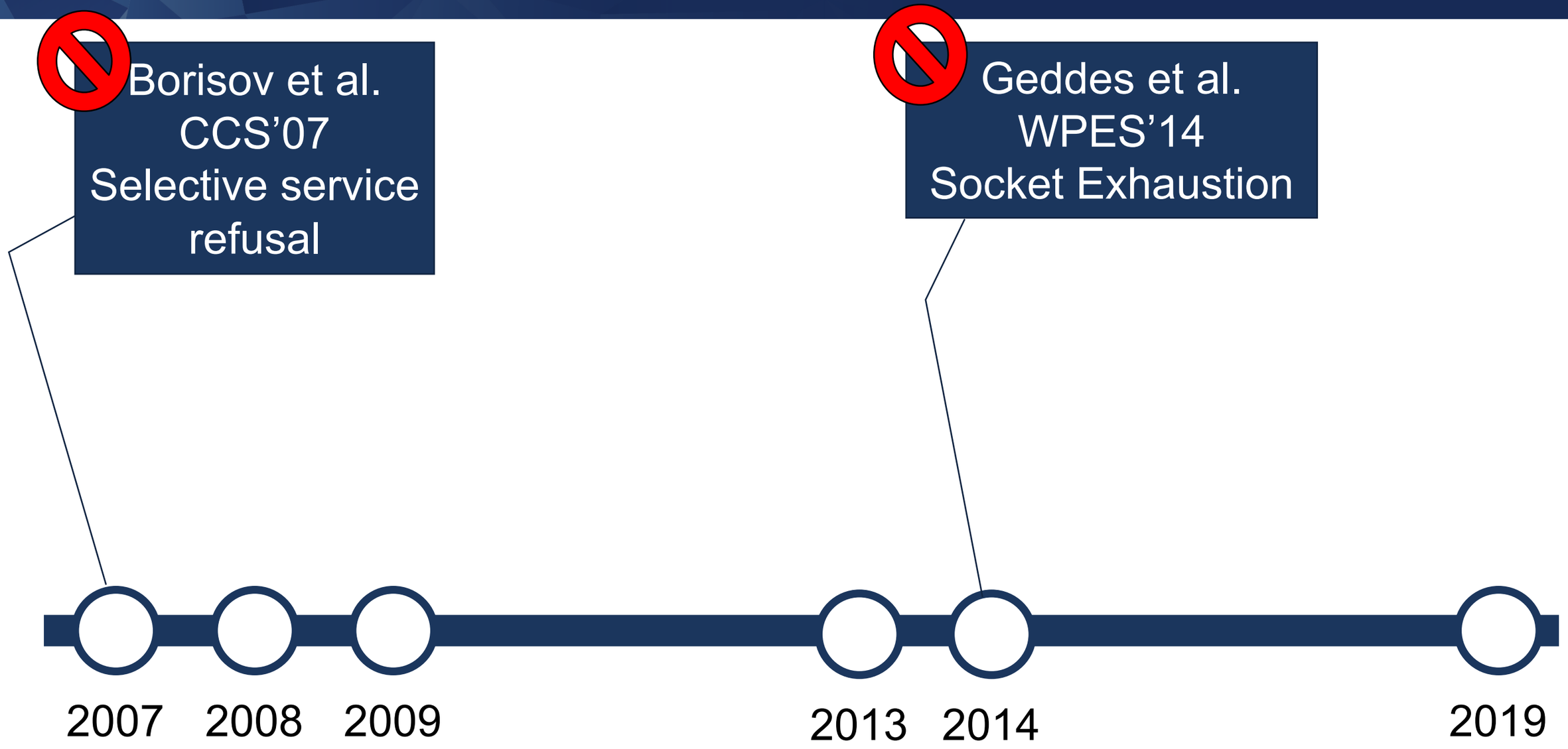
WPES'07, CCS'07, Sec'15, PETS'16, S&P'17, PETS'18

U.S. NAVAL RESEARCH LABORATORY

Our Focus: Denial-of-Service Attacks

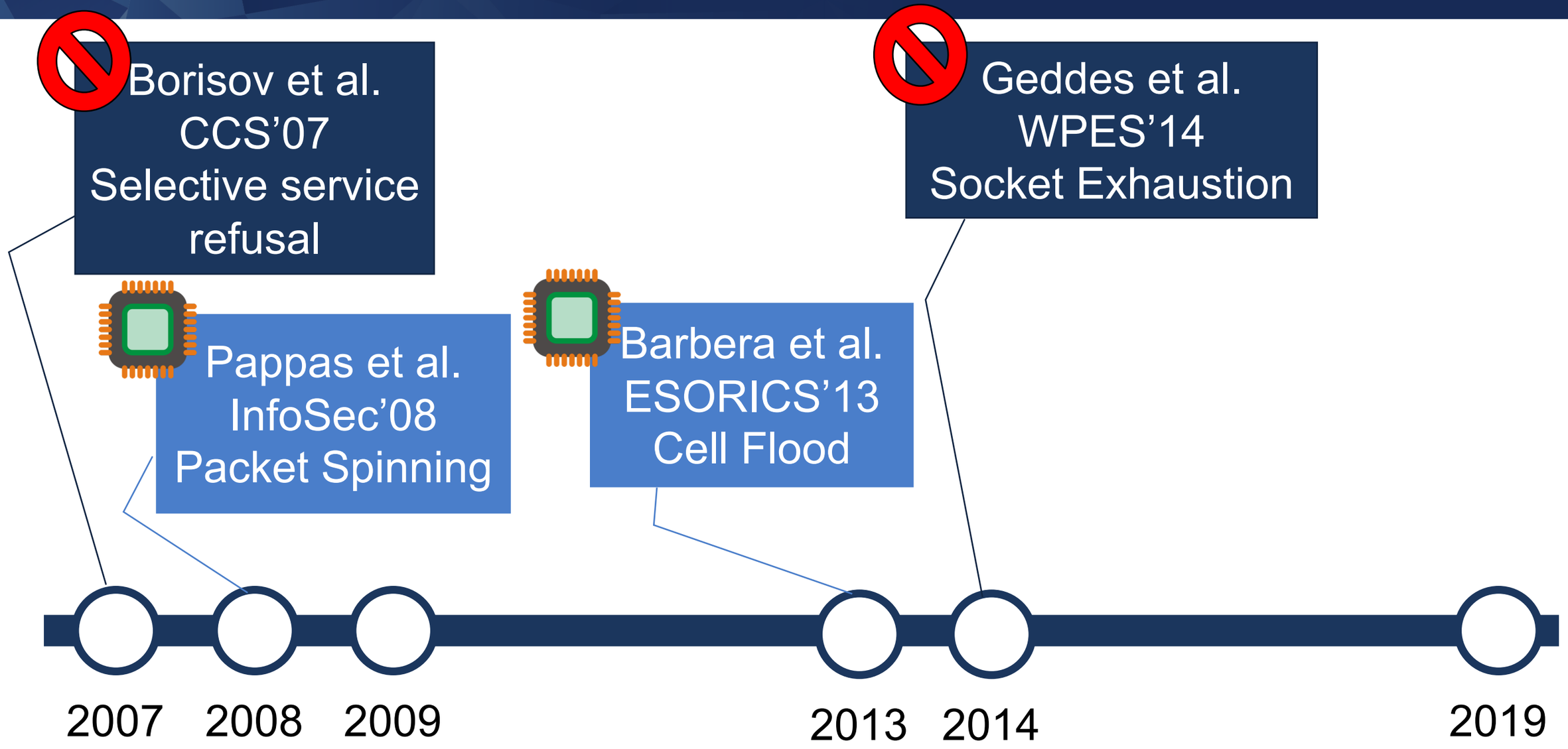
Our Focus: Denial-of-Service Attacks

Our Focus: Denial-of-Service Attacks



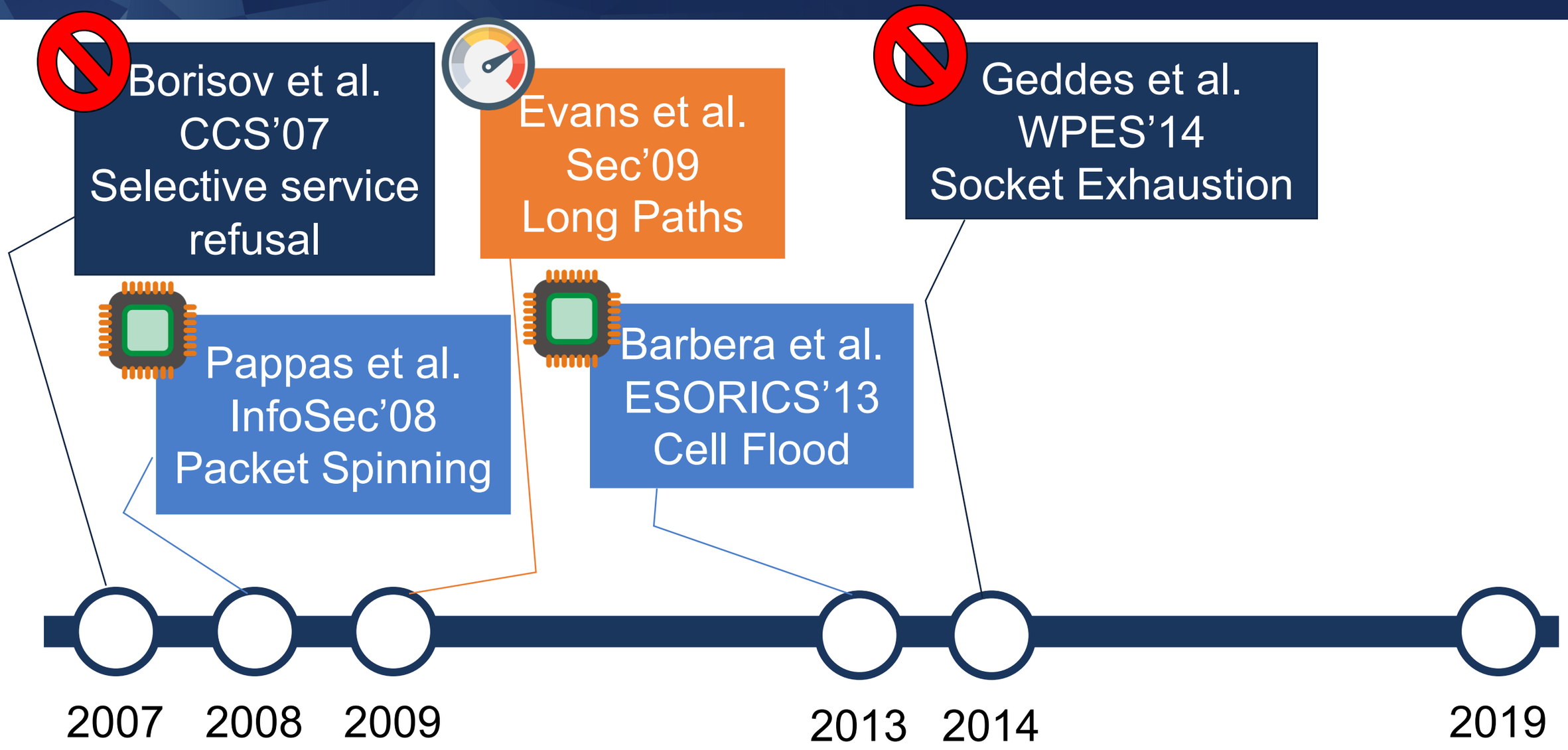
U.S. NAVAL RESEARCH LABORATORY

Our Focus: Denial-of-Service Attacks



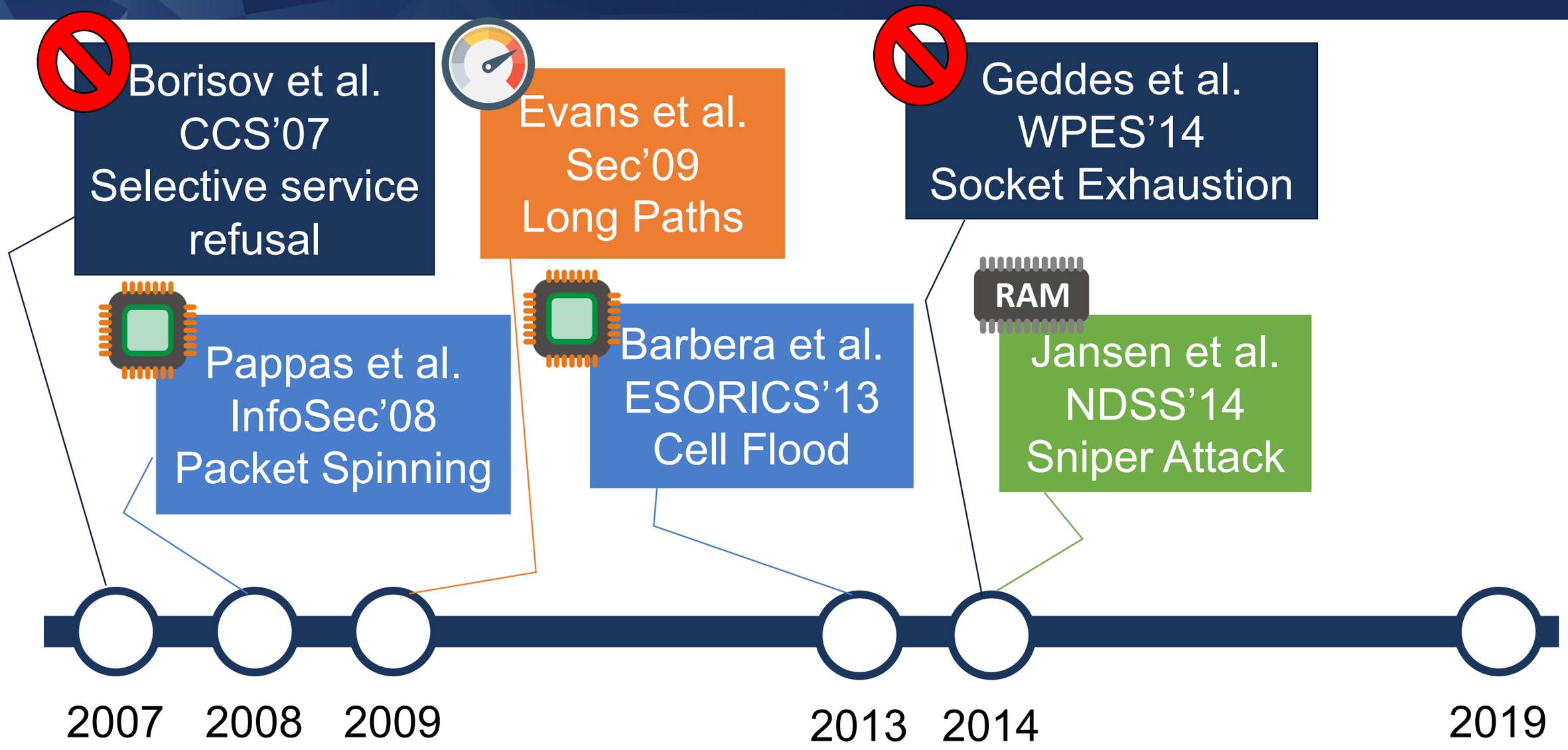
U.S. NAVAL RESEARCH LABORATORY

Our Focus: Denial-of-Service Attacks



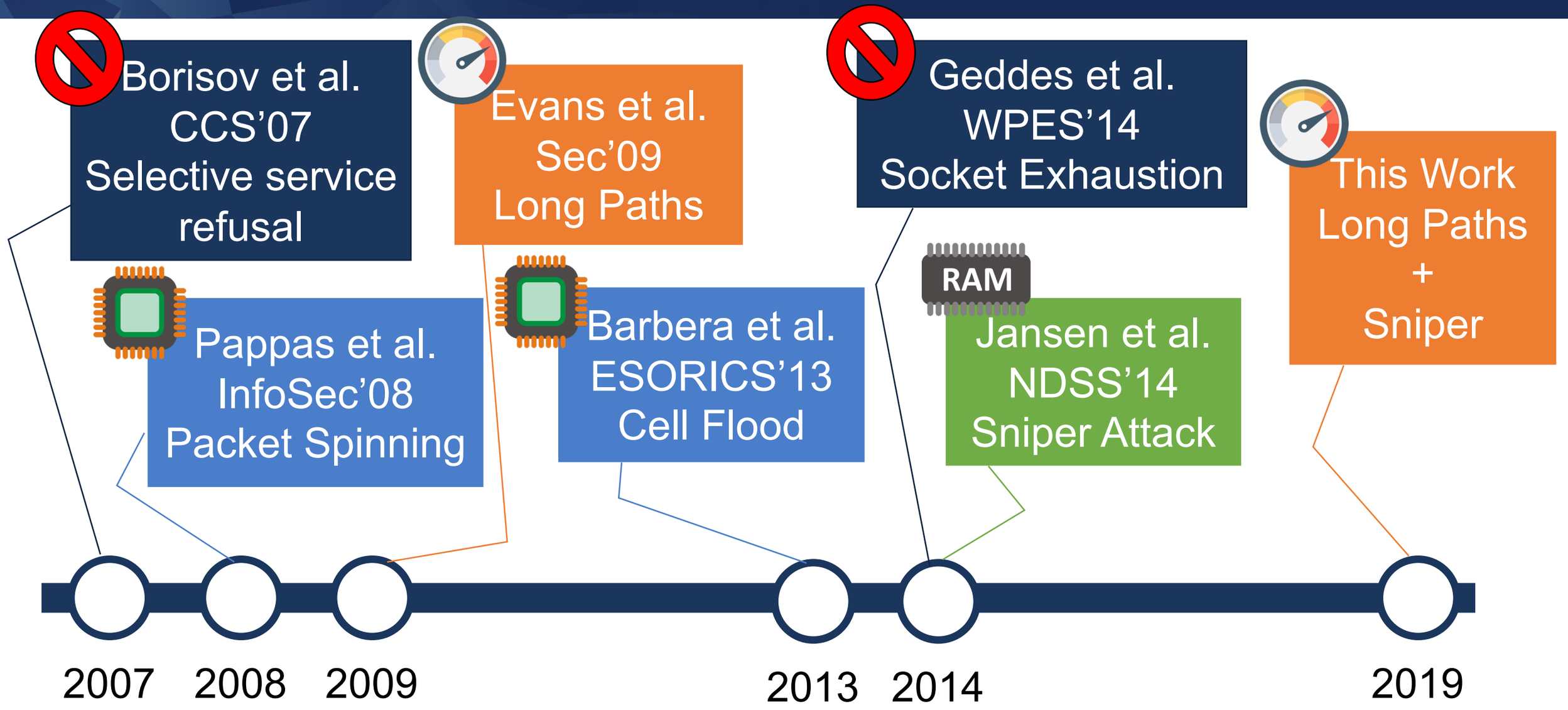
U.S. NAVAL RESEARCH LABORATORY

Our Focus: Denial-of-Service Attacks



U.S. NAVAL RESEARCH LABORATORY

Our Focus: Denial-of-Service Attacks



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

#24902 closed enhancement (fixed)

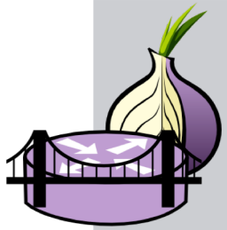
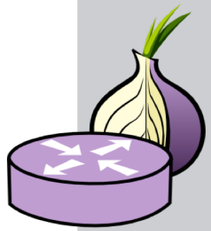
Opened 19 months ago
Closed 17 months ago
Last modified 4 months ago

Denial of Service mitigation subsystem

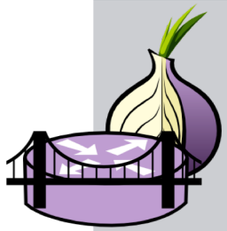
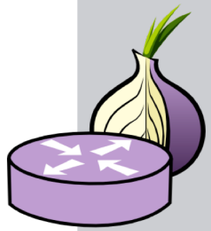
https://trac.torproject.org/projects/tor/ticket/24902

U.S. NAVAL RESEARCH LABORATORY

Research Questions and Summary of Results

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

Research Questions and Summary of Results

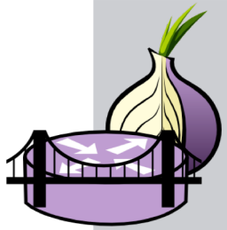
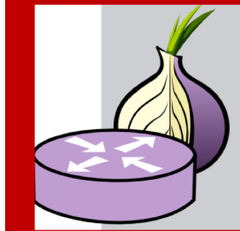
Component	Cost	Effect
 Bridge		% slower
 TorFlow Scanne		% slower
 Relay	$0,500 / mo.	120 % slower

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

U.S. NAVAL RESEARCH LABORATORY

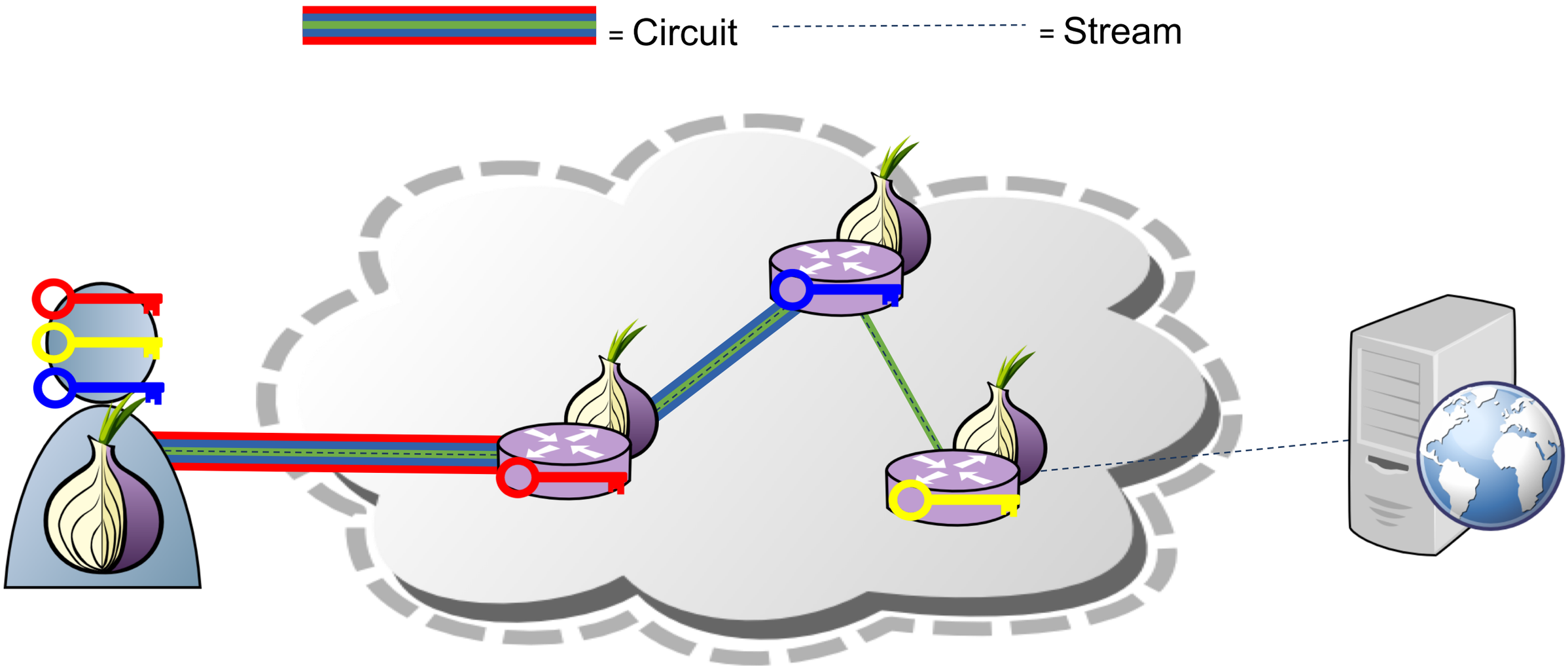
Research Questions and Summary of Results

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

Attack

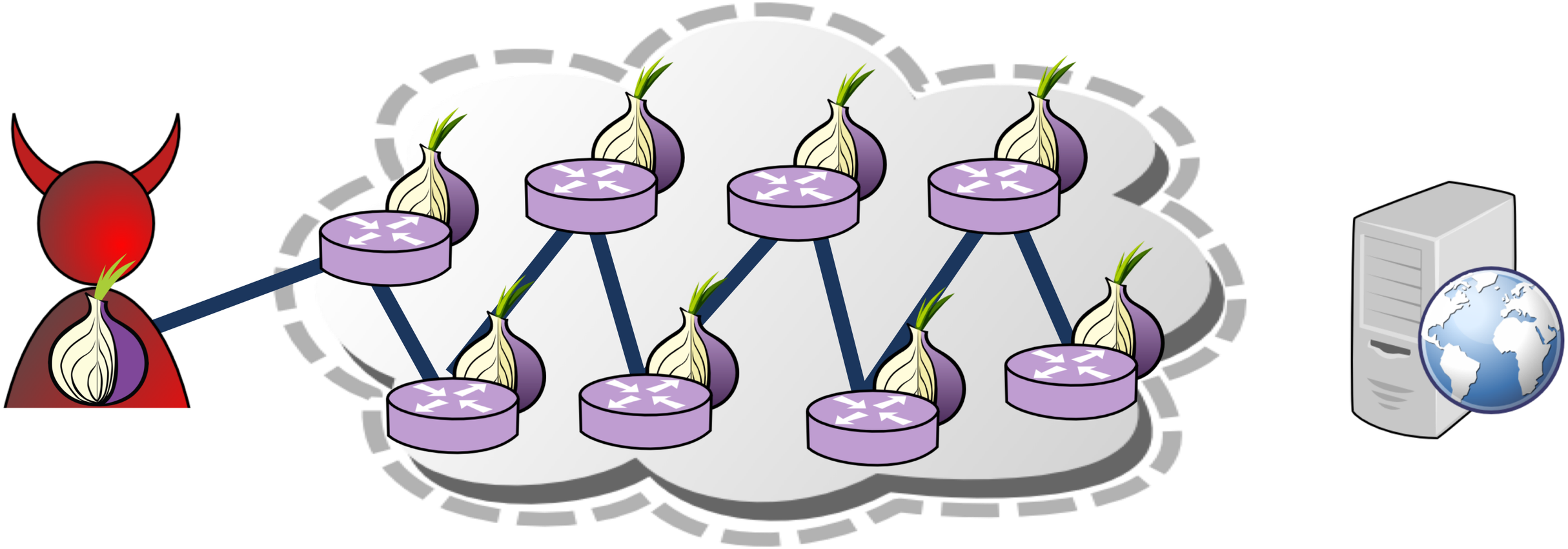
U.S. NAVAL RESEARCH LABORATORY

How Tor Works



The Relay Congestion Attack

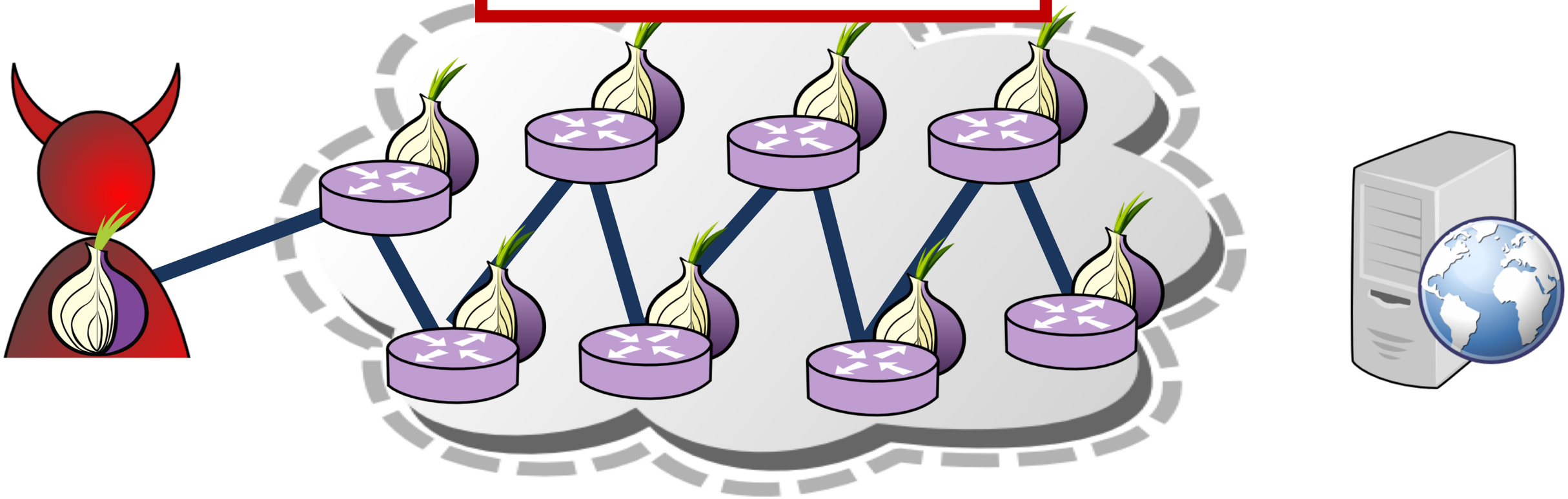
Step 1:
Build 8-hop circuit



The Relay Congestion Attack

Step 1:
Build 8-hop circuit

Can be targeted or indiscriminate

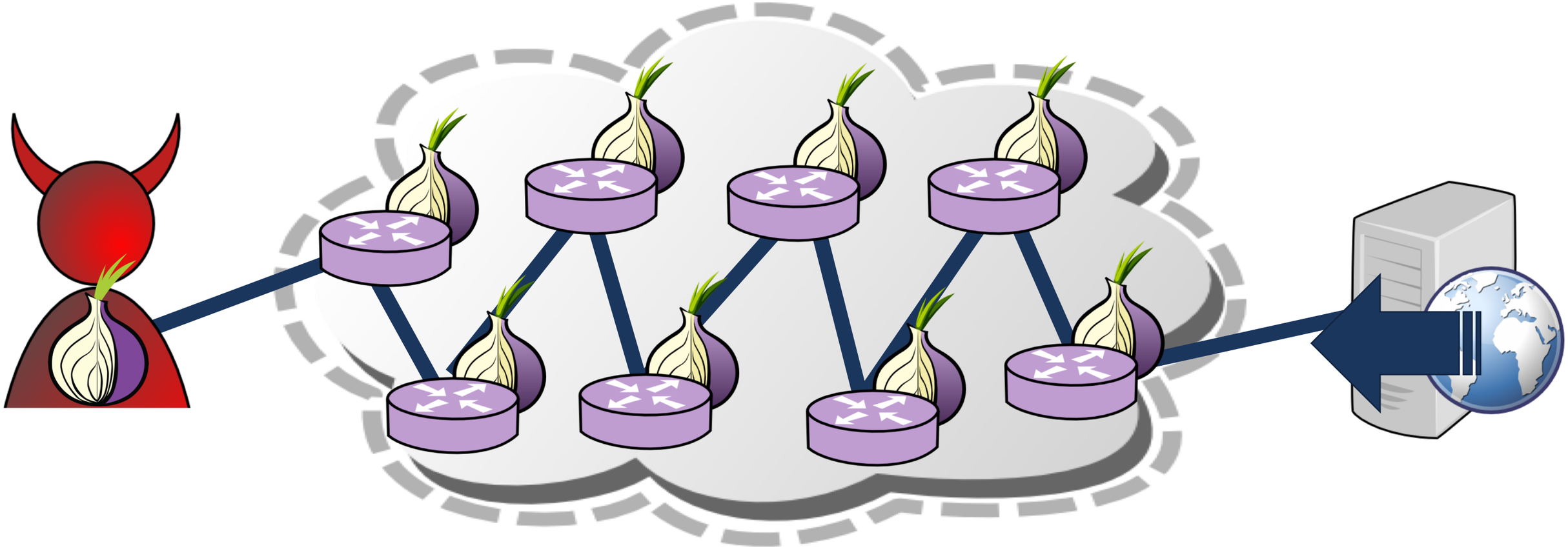


U.S. NAVAL RESEARCH LABORATORY

The Relay Congestion Attack

Step 1:
Build 8-hop circuit

Step 2:
GET large files



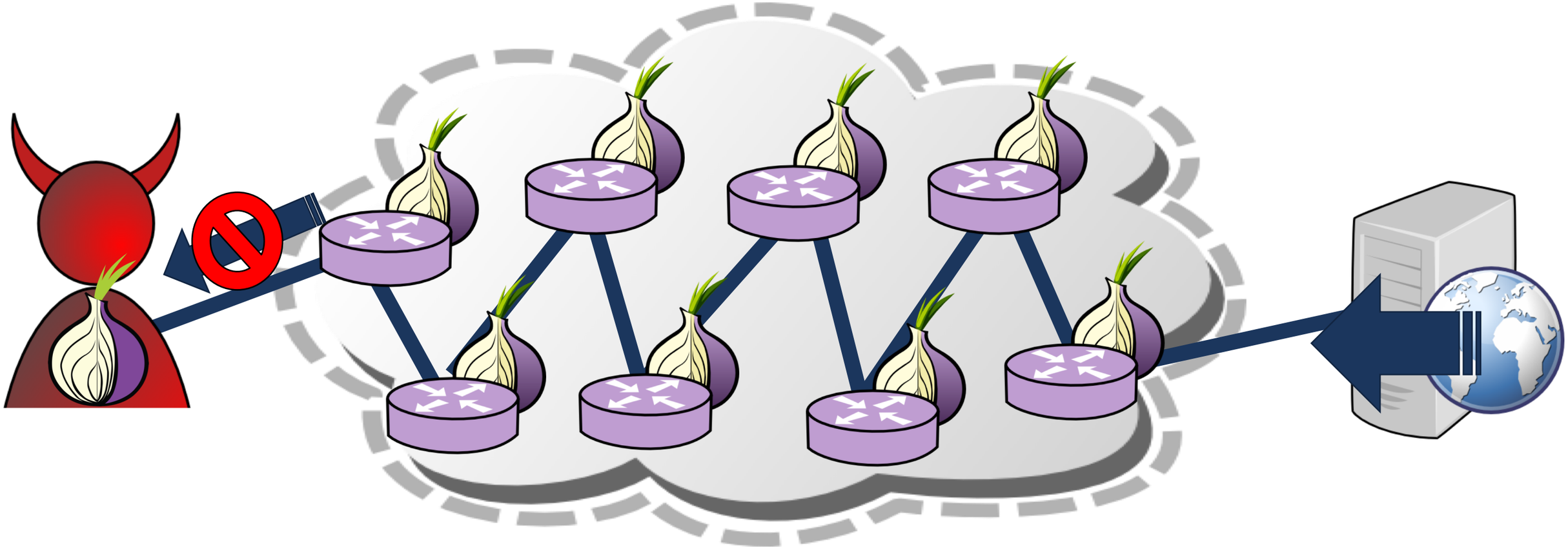
U.S. NAVAL RESEARCH LABORATORY

The Relay Congestion Attack

Step 1:
Build 8-hop circuit

Step 2:
GET large files

Step 3:
Stop reading



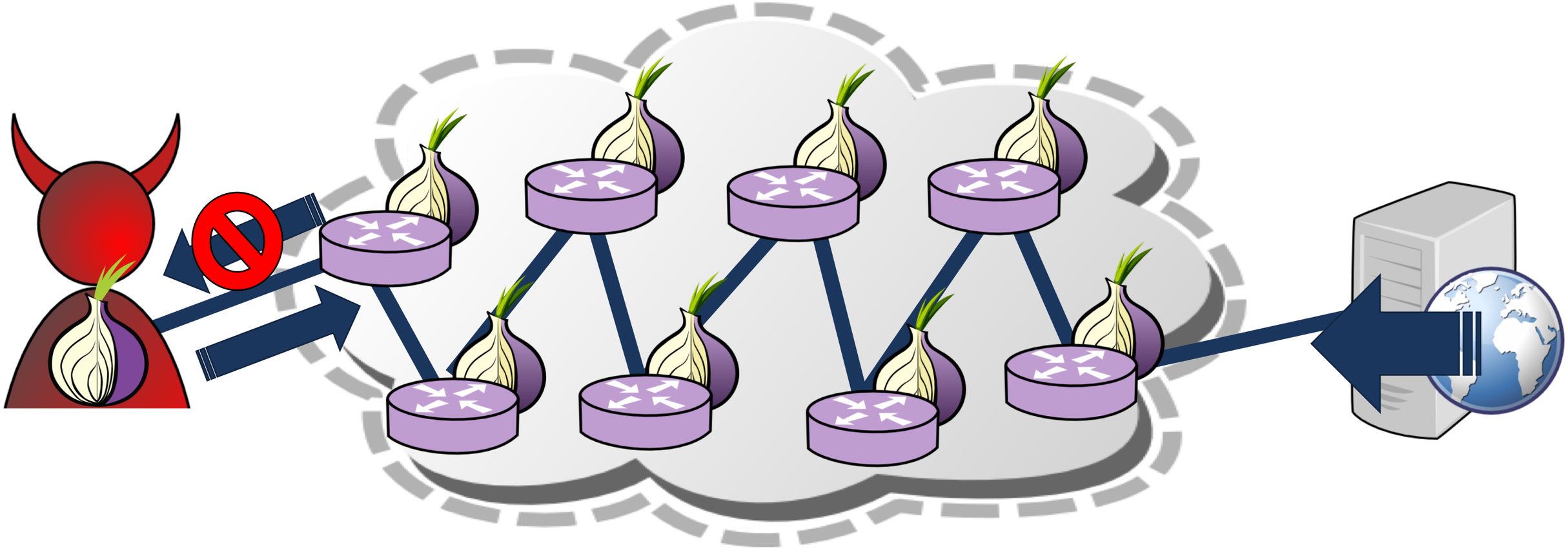
The Relay Congestion Attack

Step 1:
Build 8-hop circuit

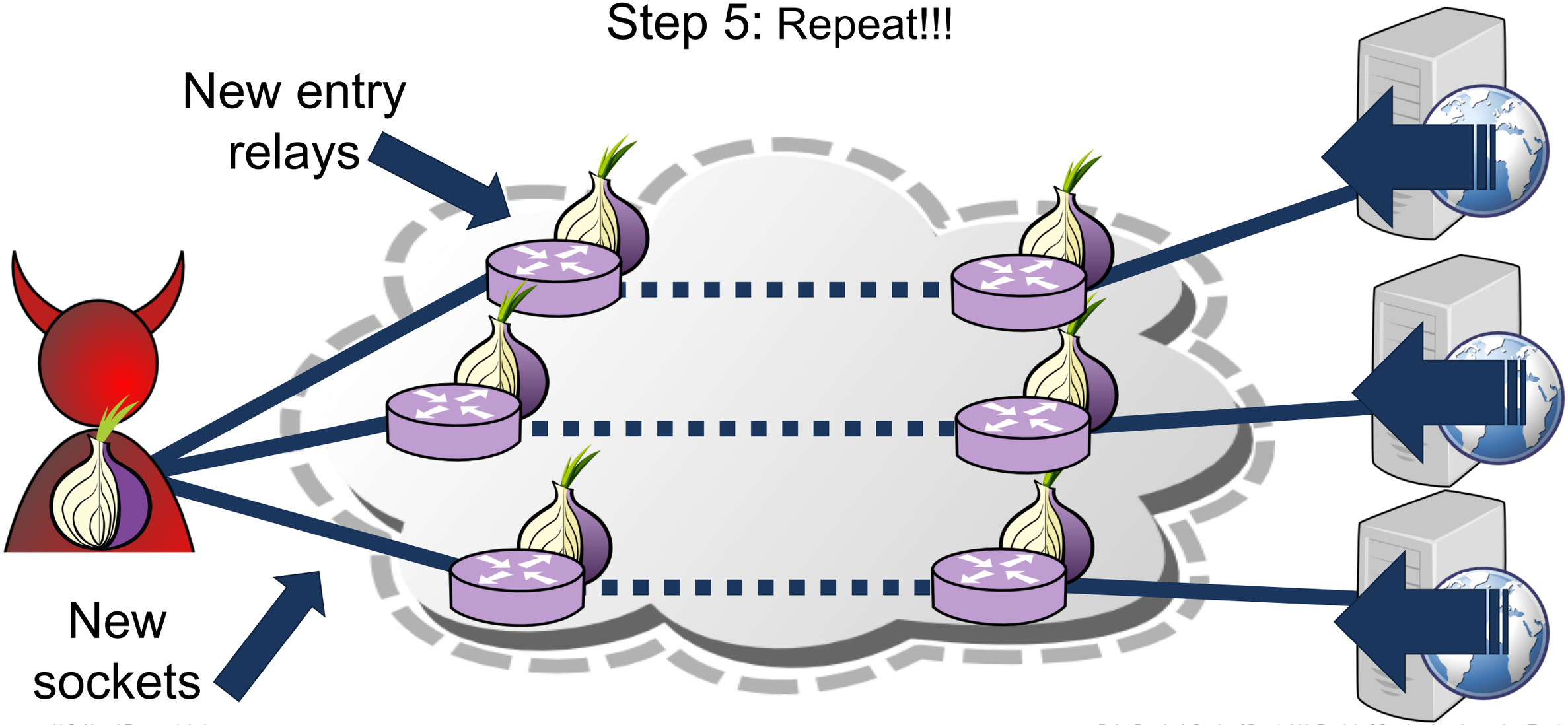
Step 2:
GET large files

Step 3:
Stop reading

Step 4:
Send flow control cells



The Relay Congestion Attack



Evaluation

U.S. NAVAL RESEARCH LABORATORY

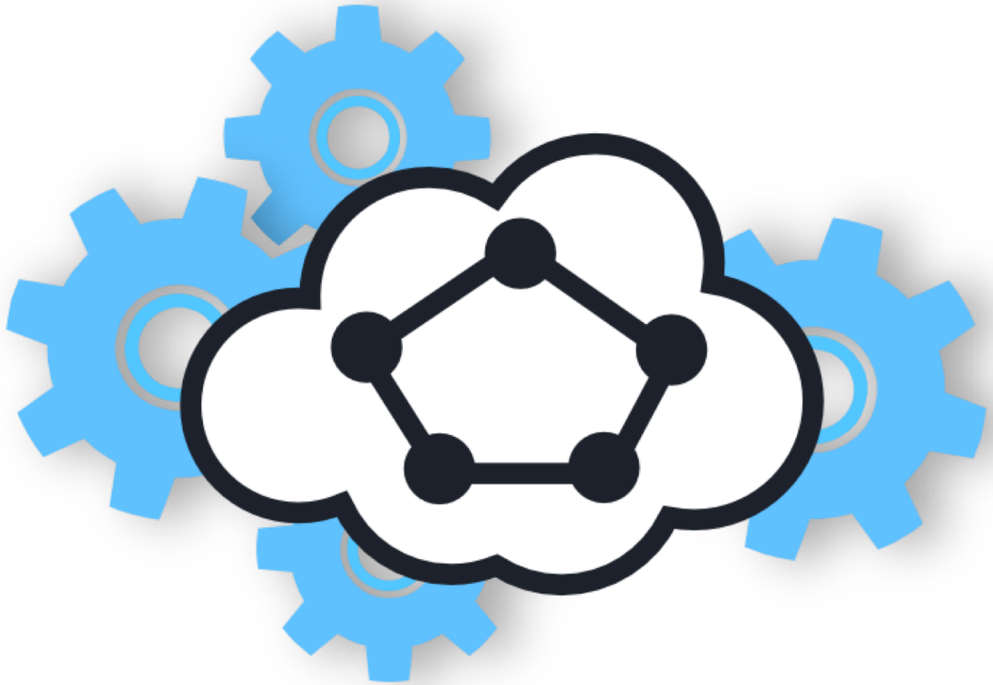
Evaluation Setup

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

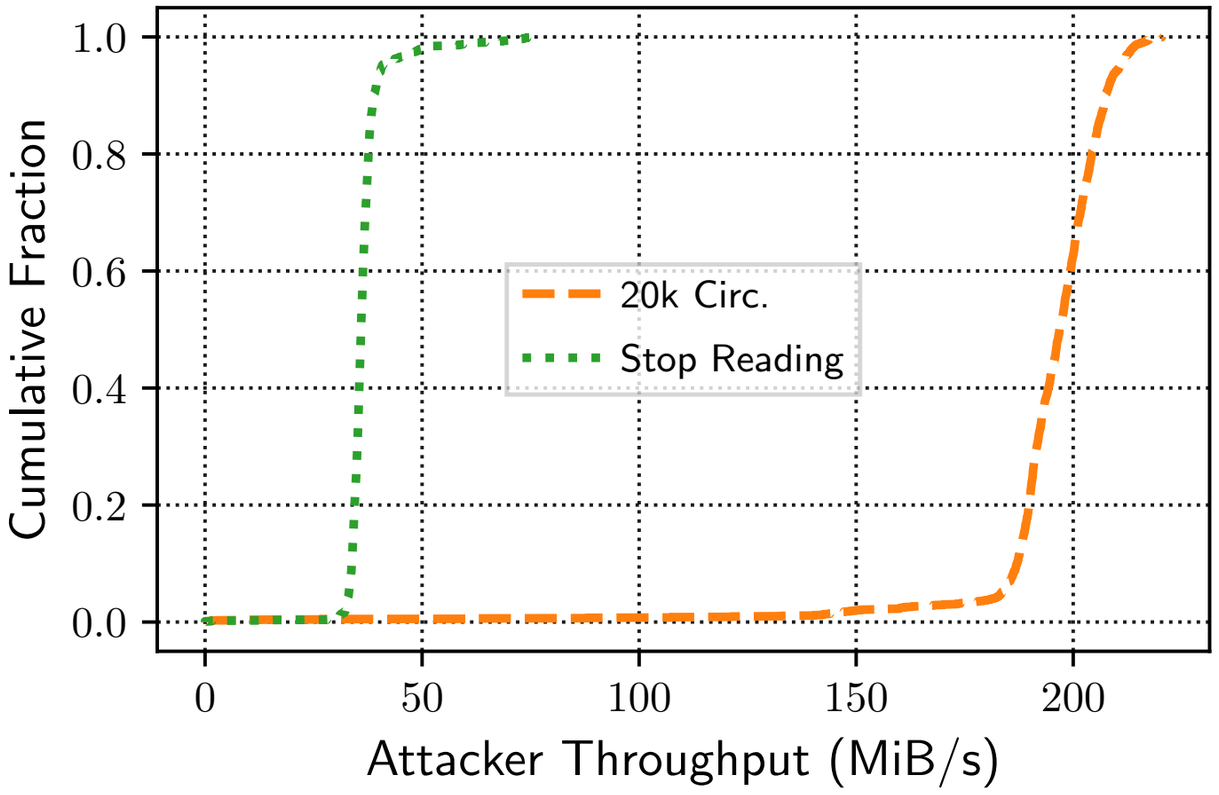
- Attack strength (num. attack circuits)
- Network load, attacker resource usage, client performance

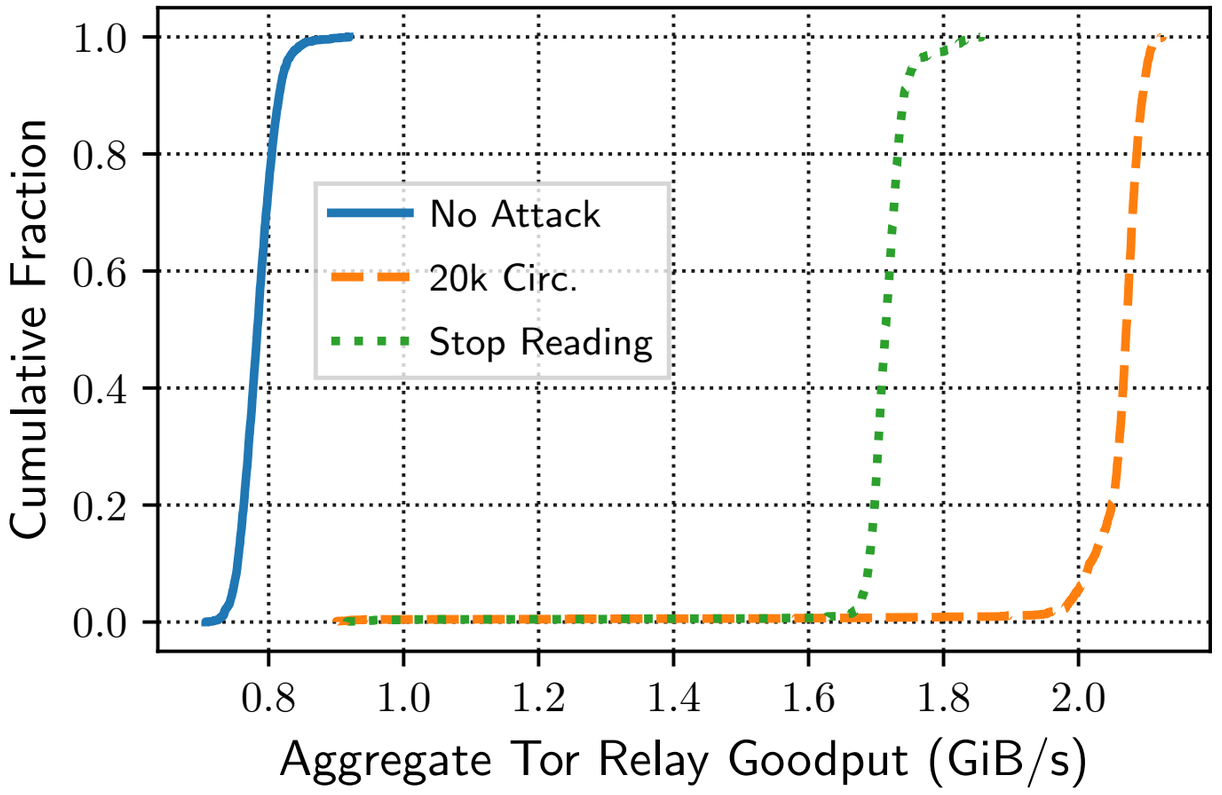


https://github.com/shadow/shadow

U.S. NAVAL RESEARCH LABORATORY

Bandwidth Used by Attacker and Tor Network



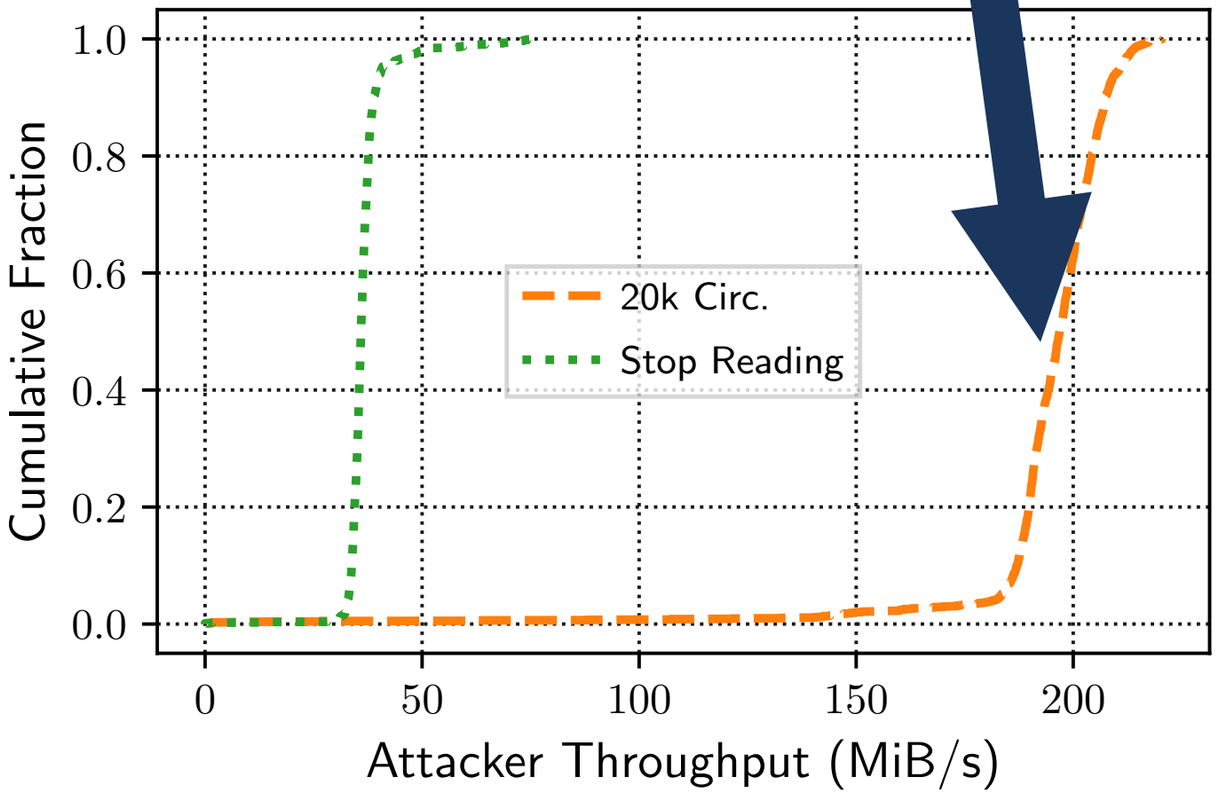


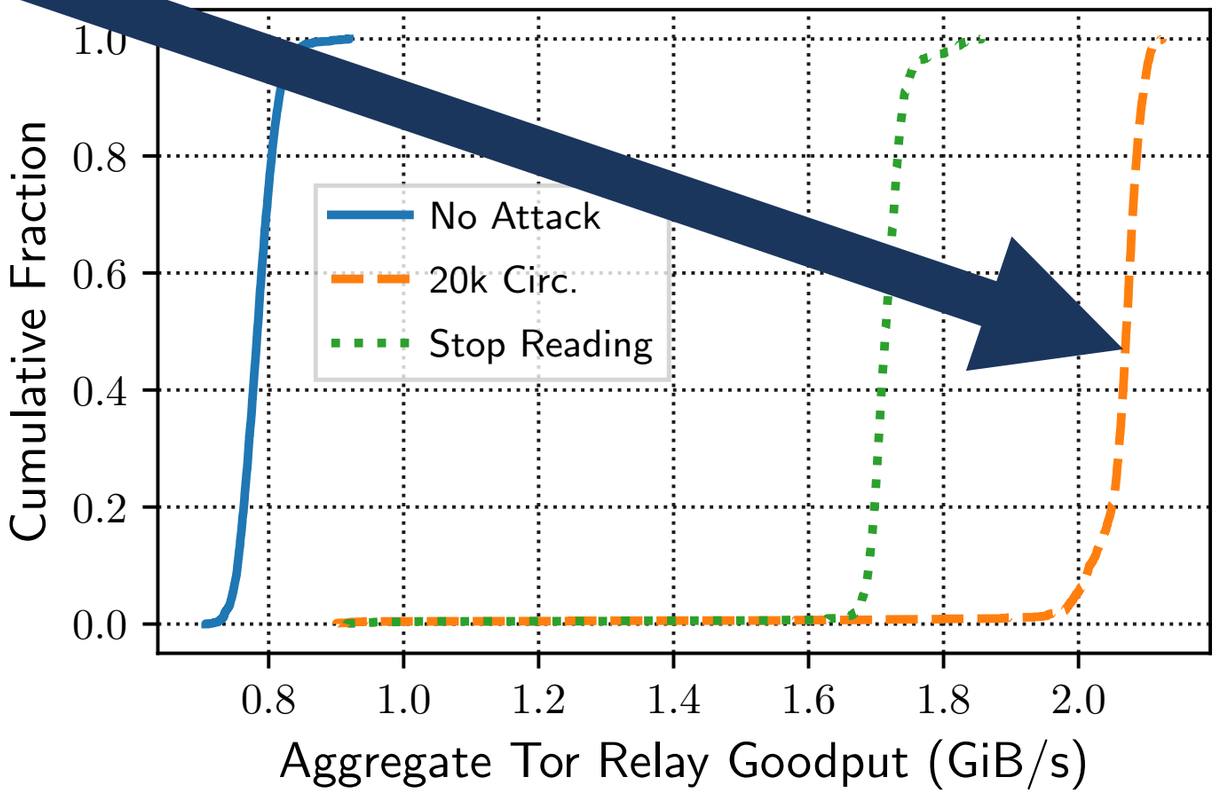
Bandwidth Used by Attacker and Tor Network

Bandwidth Amplification Factors:

20k Circuits

6.7





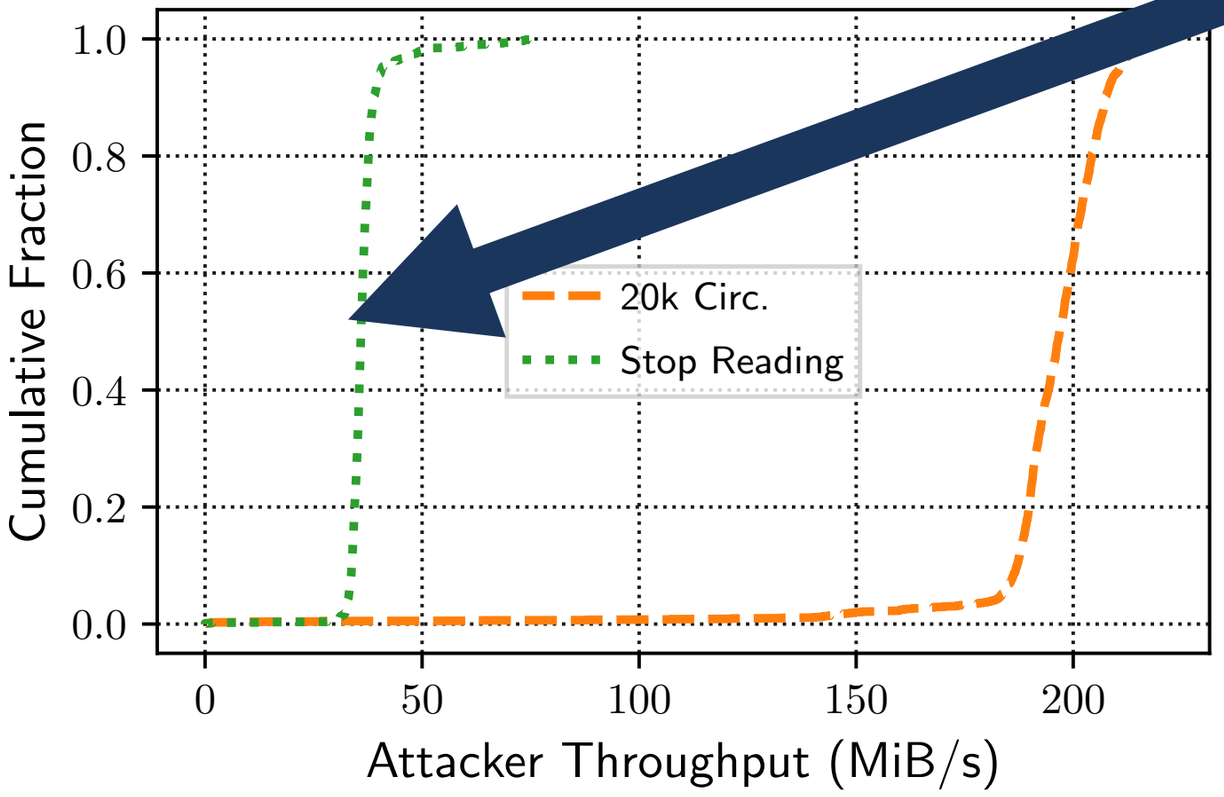
U.S. NAVAL RESEARCH LABORATORY

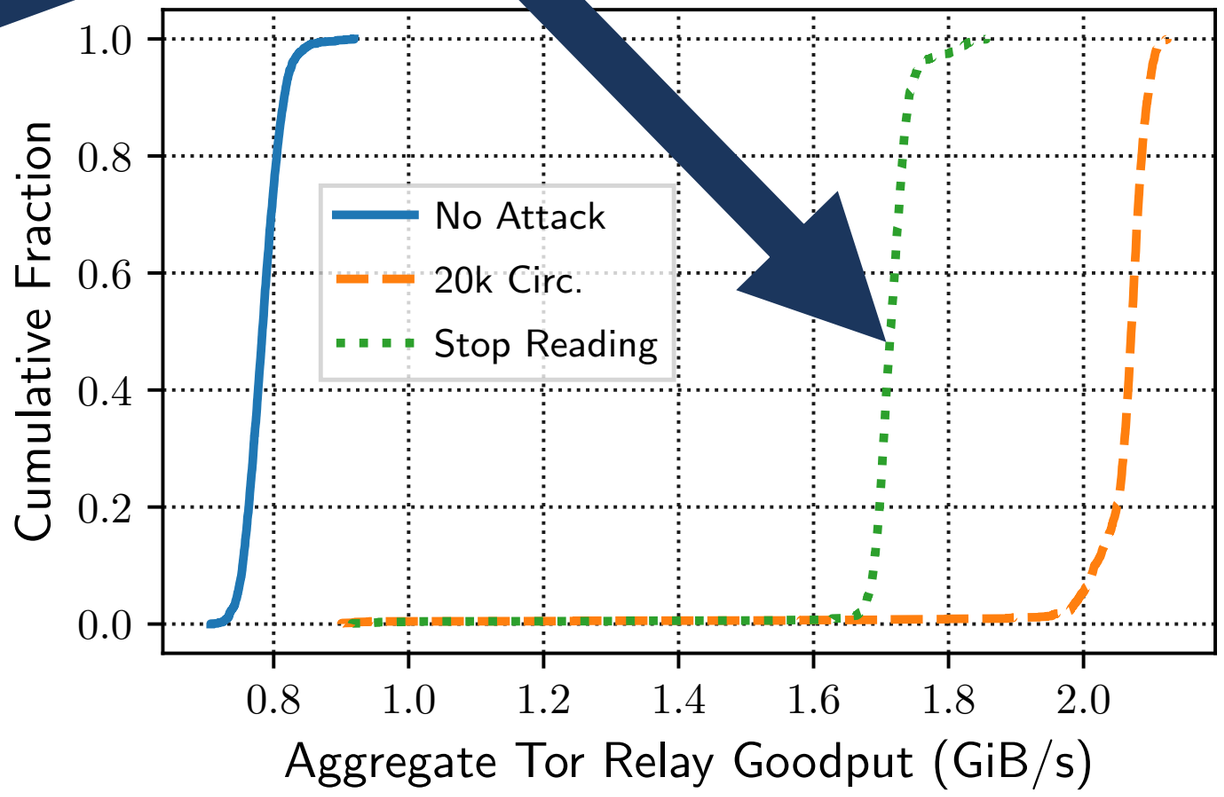
Bandwidth Used by Attacker and Tor Network

Bandwidth Amplification Factors:

20k Circuits
6.7

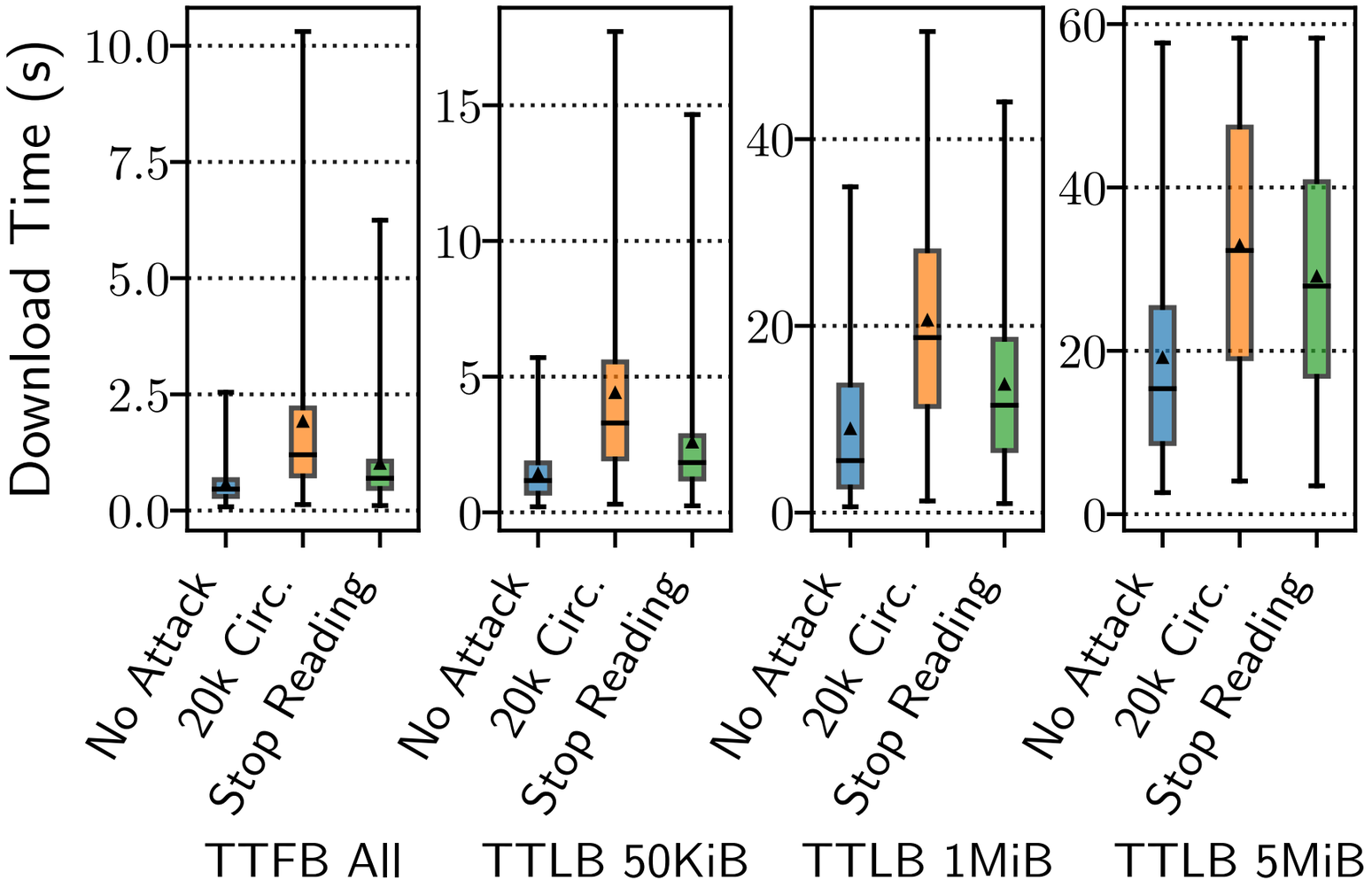
Stop Reading
26





U.S. NAVAL RESEARCH LABORATORY

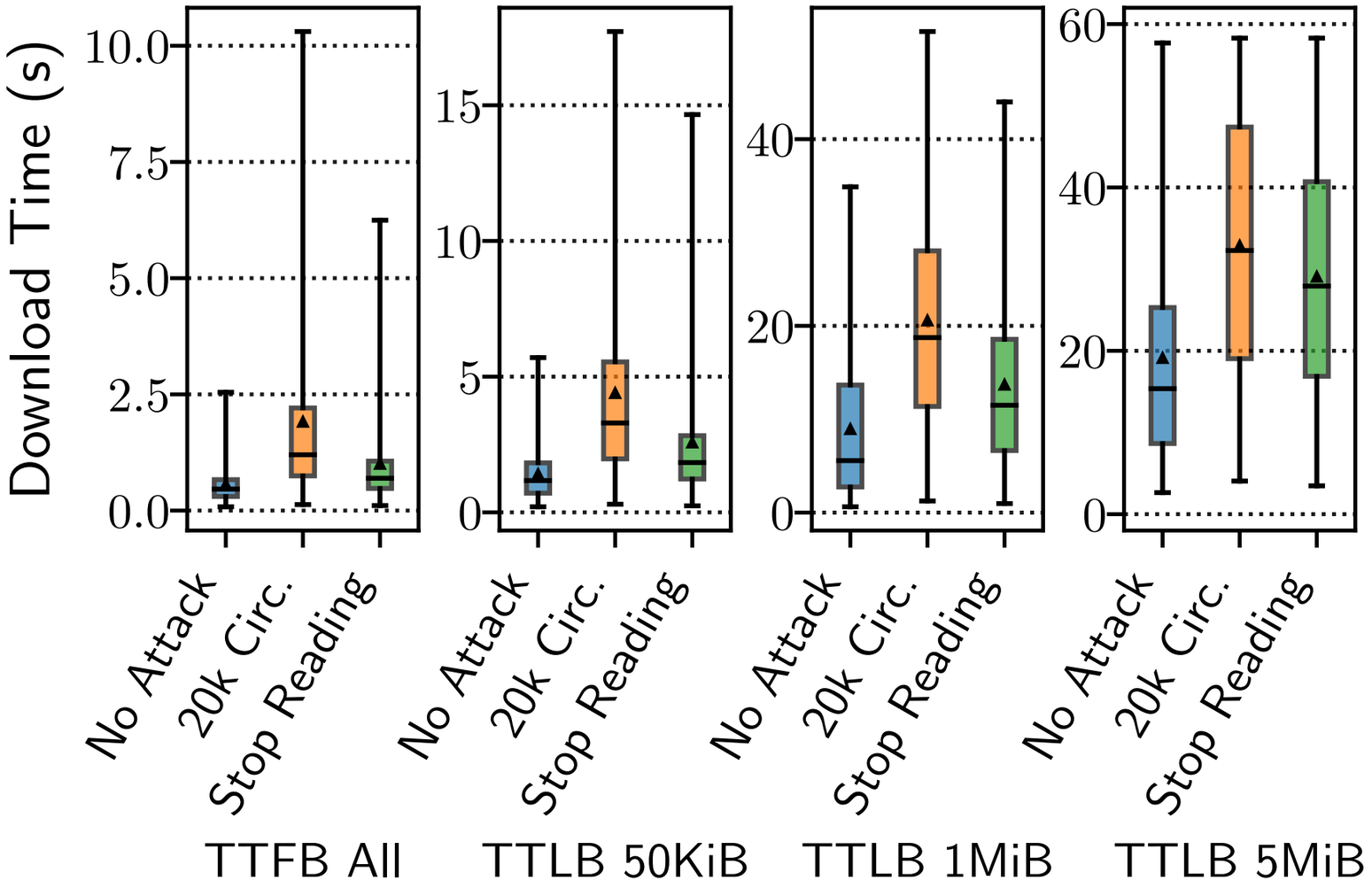
Effect on Client Performance



U.S. NAVAL RESEARCH LABORATORY

Effect on Client Performance

20k Circuits
TTFB:
+138%

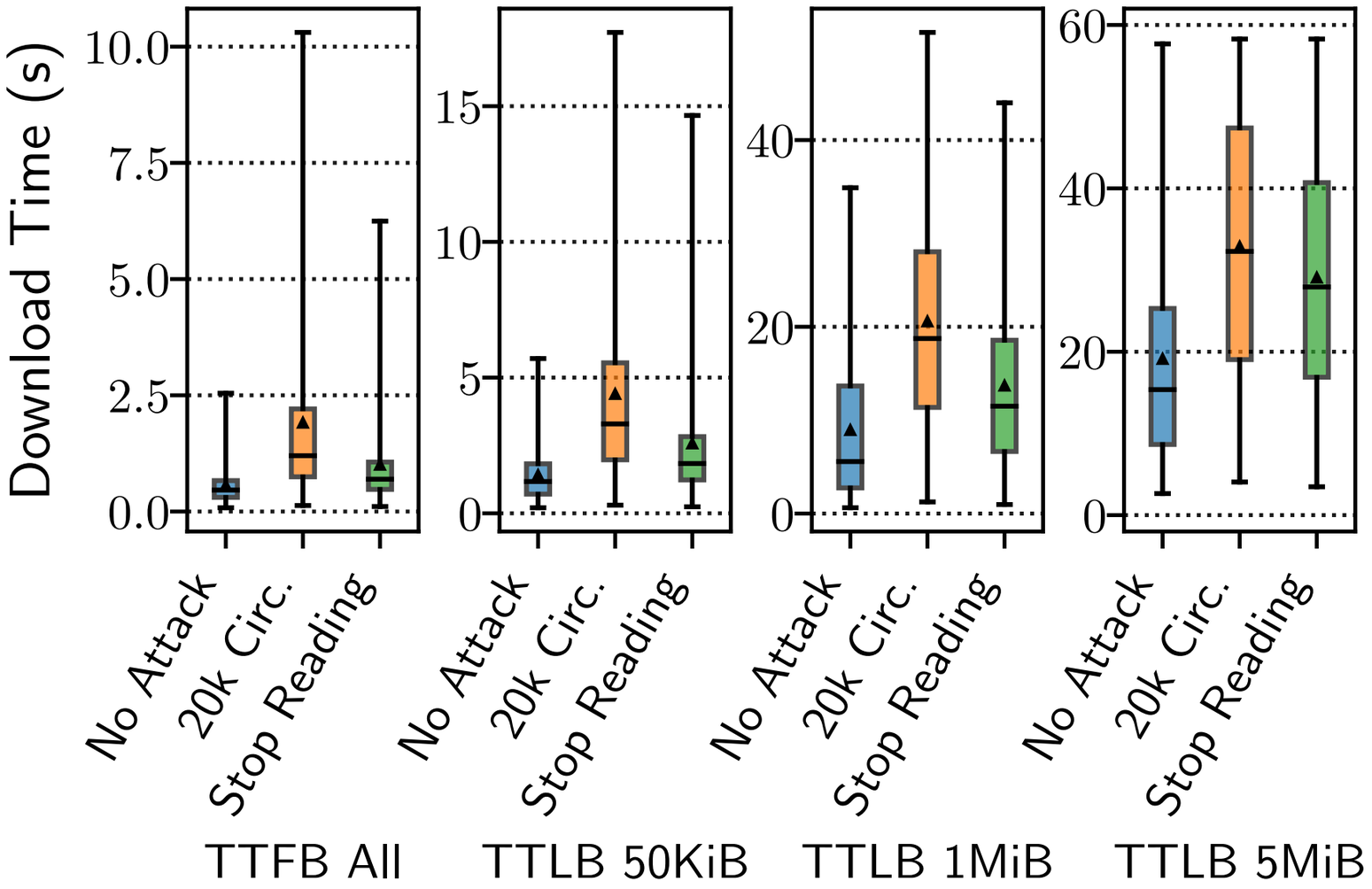


20k Circuits
TTLB:
+120%

Effect on Client Performance

20k Circuits
TTFB:
+138%

Stop Reading
TTFB:
+48%



20k Circuits
TTLB:
+120%

Stop Reading
TTLB:
+47%

U.S. NAVAL RESEARCH LABORATORY

Cost to Conduct Relay Congestion Attack

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)

Table 2: The estimated mean hourly cost to flood a single target with 1 Gbit/s using various dedicated server providers. The amortized cost is the hourly price per Gbit/s of traffic. Prices include 4 CPU cores with minimum 16 GB RAM and 500 GB storage.

Service	Speed (Gbit/s)	Quota (TB)	$/mo. (USD)	Amort. (USD)
Liquid Web	1.00	5	$ 249.00	$ 0.35
InMotion	1.00	10	$ 166.59	$ 0.23
DreamHost	Unkn.	Unmet.	$ 249.00	–
GoDaddy	1.00	Unmet.	$ 239.99	$ 0.33
BlueHost	0.10	15	$ 249.99	$ 3.47
1&1	1.00	Unmet.	$ 130.00	$ 0.18
FatCow	Unkn.	15	$ 239.99	–
OVH	0.50	Unmet.	$ 119.99	$ 0.33
SiteGround	1.00	10	$ 269.00	$ 0.37
YesUpHost	1.00	100	$ 249.00	$ 0.35
Mean amortized cost ($/hour/Gbit/s):				**$ 0.70**

U.S. NAVAL RESEARCH LABORATORY

Comparison to Sybil Attacks

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

Sybil DoS Attack

Sybil Deanonymization Attack

U.S. NAVAL RESEARCH LABORATORY

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

Sybil Deanonymization Attack

U.S. NAVAL RESEARCH LABORATORY

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

Sybil Deanonymization Attack

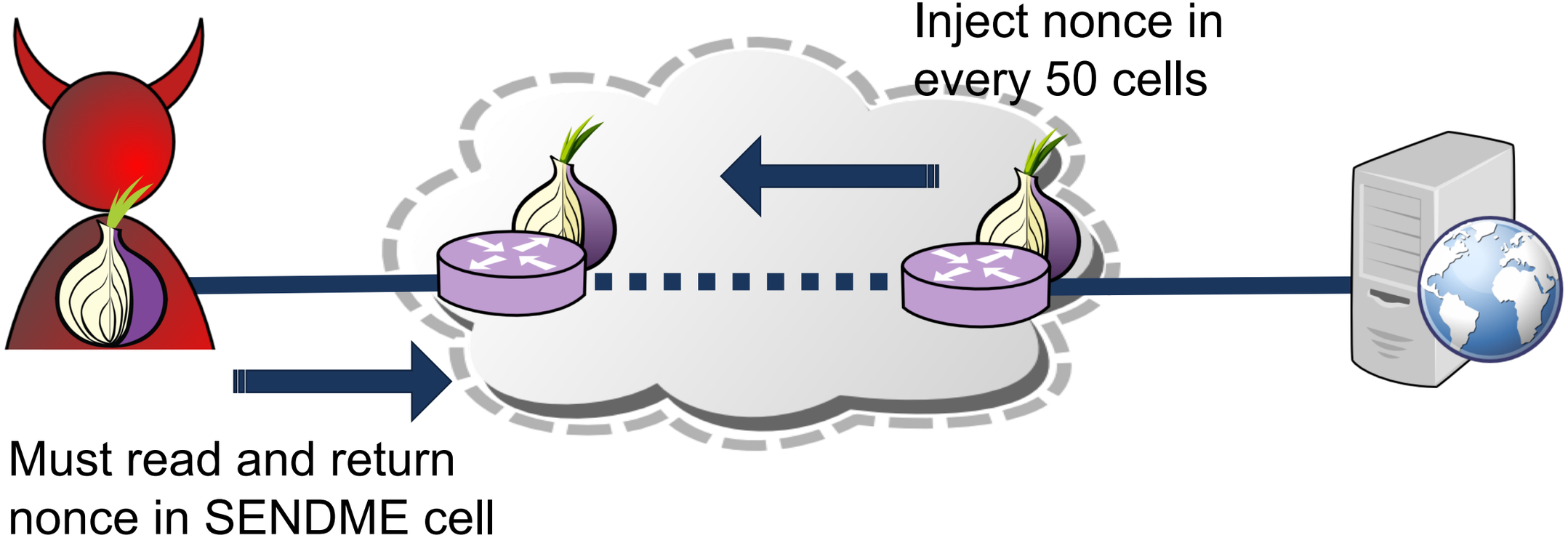
- Goal: appear on both ends of circuits to compromise anonymity
- 5:1 guard-to-exit BW allocation
- 2.8% guard * 0.8% exit = 0.02% total circuits compromised

Mitigation

Mitigations to Relay Congestion Attack

Ability to stop reading from circuits

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



U.S. NAVAL RESEARCH LABORATORY

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

U.S. NAVAL RESEARCH LABORATORY

Mitigations to Relay Congestion Attack

Ability to stop reading from circuits

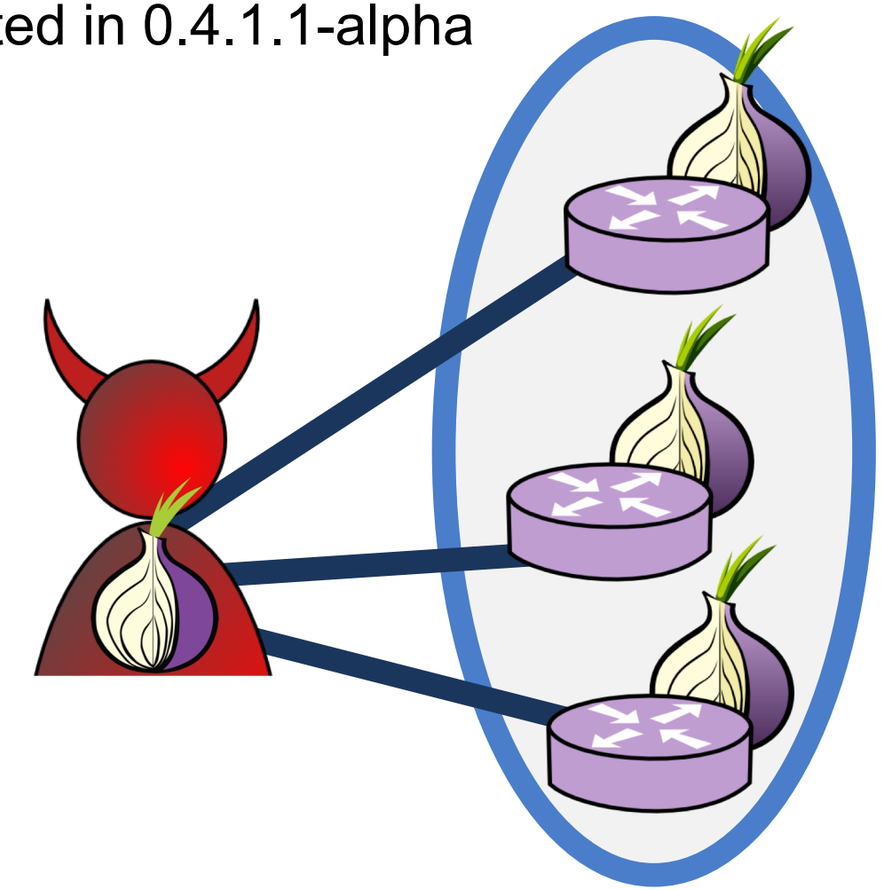
- Authenticated SENDMEs, Tor Proposal 289, implemented in 0.4.1.1-alpha

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



U.S. NAVAL RESEARCH LABORATORY

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