

SICO

Surgical Interception Attacks by Manipulating BGP Communities

Henry Birge-Lee

Liang Wang, Jennifer Rexford, Prateek Mittal



PRINCETON
UNIVERSITY

BGP is vulnerable to hijacks

- BGP: Routing protocol used between autonomous systems
- No inherent authentication method
- Networks can falsely claim ownership of IP prefixes and announce malicious routes (i.e., a BGP hijack)

Public DNS in Taiwan the latest victim to BGP hijack

May 15, 2019 by [Aftab Siddiqui](#) [Leave a Comment](#)

DISRUPTIONS ... [view more](#)

April 25, 2018



BGP Hijack of Amazon DNS to Steal Crypto Currency



[Doug Madory](#)

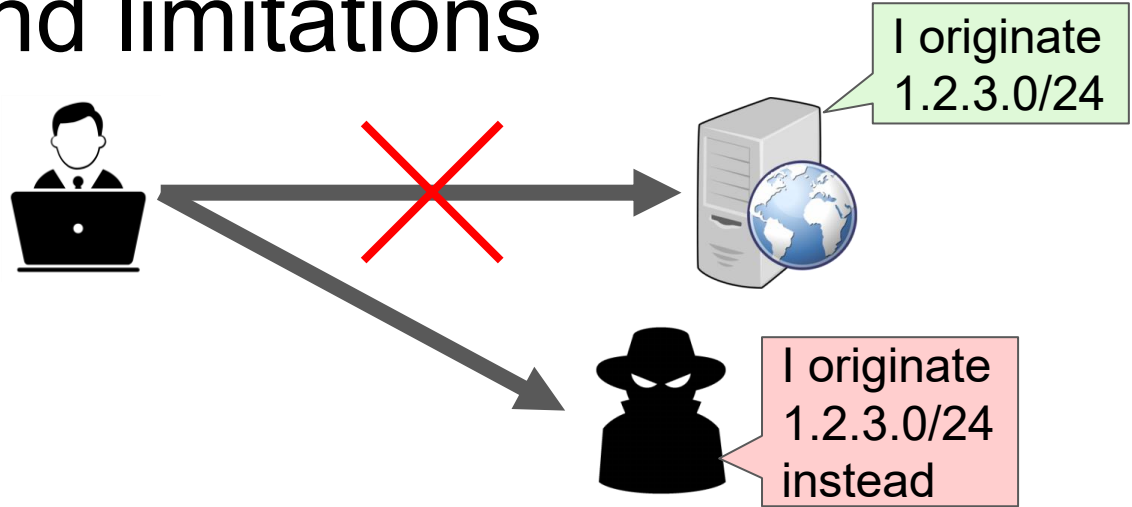
DIRECTOR OF INTERNET ANALYSIS

Pakistan hijacks YouTube

Research // Feb 24, 2008 // [Dyn Guest Blogs](#)

BGP hijacks and limitations

BGP
Hijack:



- Limitation: victim partially loses Internet connectivity (can be detected with monitoring frameworks)
- Limitation: adversary cannot perform passive traffic analysis or full man-in-the-middle attacks

BGP hijack vs interception

BGP
Hijack:

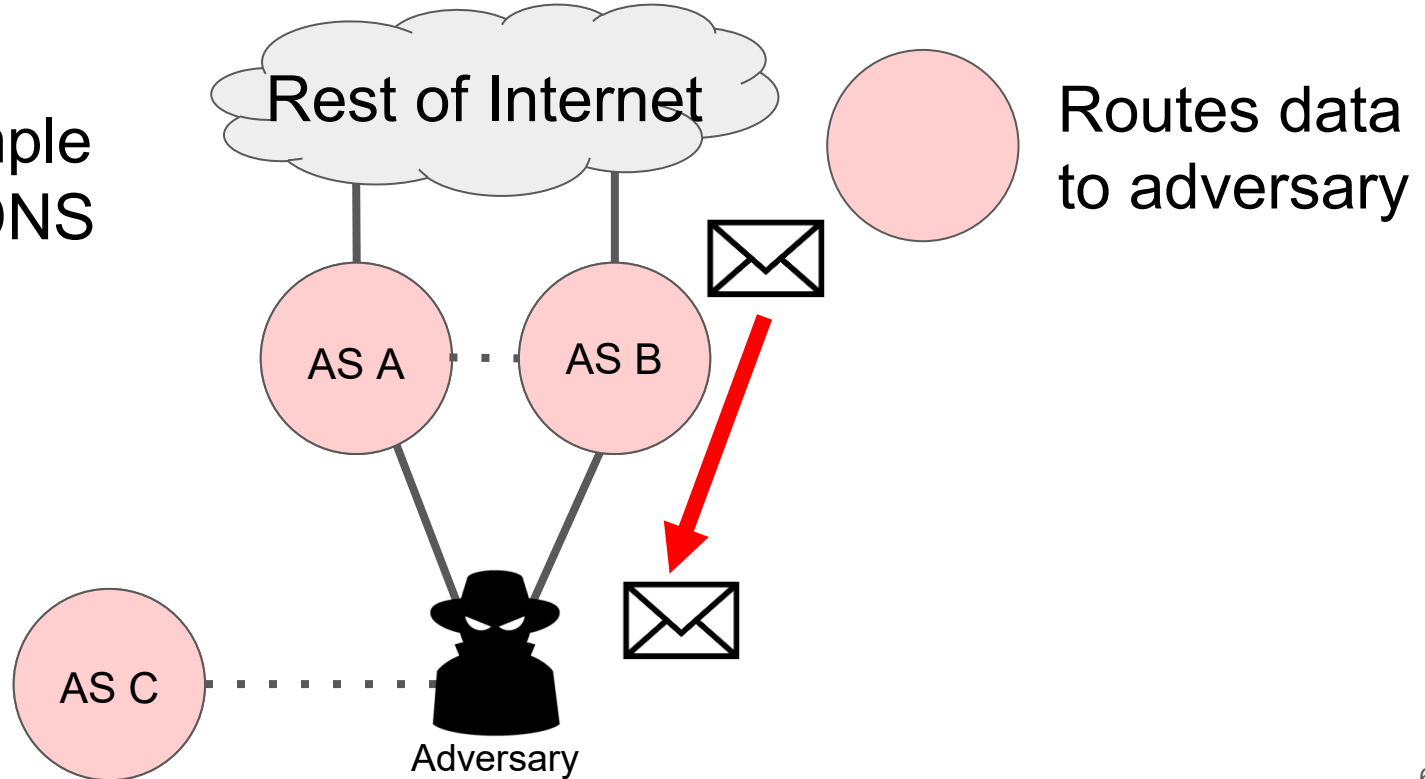


BGP
Interception:



Launching interception is challenging

Real Internet
topology example
from Taiwan DNS
resolver hijack



Previous views on Interception

On average, traffic interception is difficult for stubs, but a manipulator with many customers can quite easily launch an interception attack. Indeed, manipulators

Goldberg et al.

How Secure Are Secure Interdomain Routing Protocols

ACM SIGCOMM '10

84% of ASes on the Internet are stubs

Previous views on Interception

BGP communities allow stub networks to launch interception attacks

G

How Secure Are Secure Interdomain Routing Protocols

ACM SIGCOMM '10

84% of ASes on the Internet are stubs

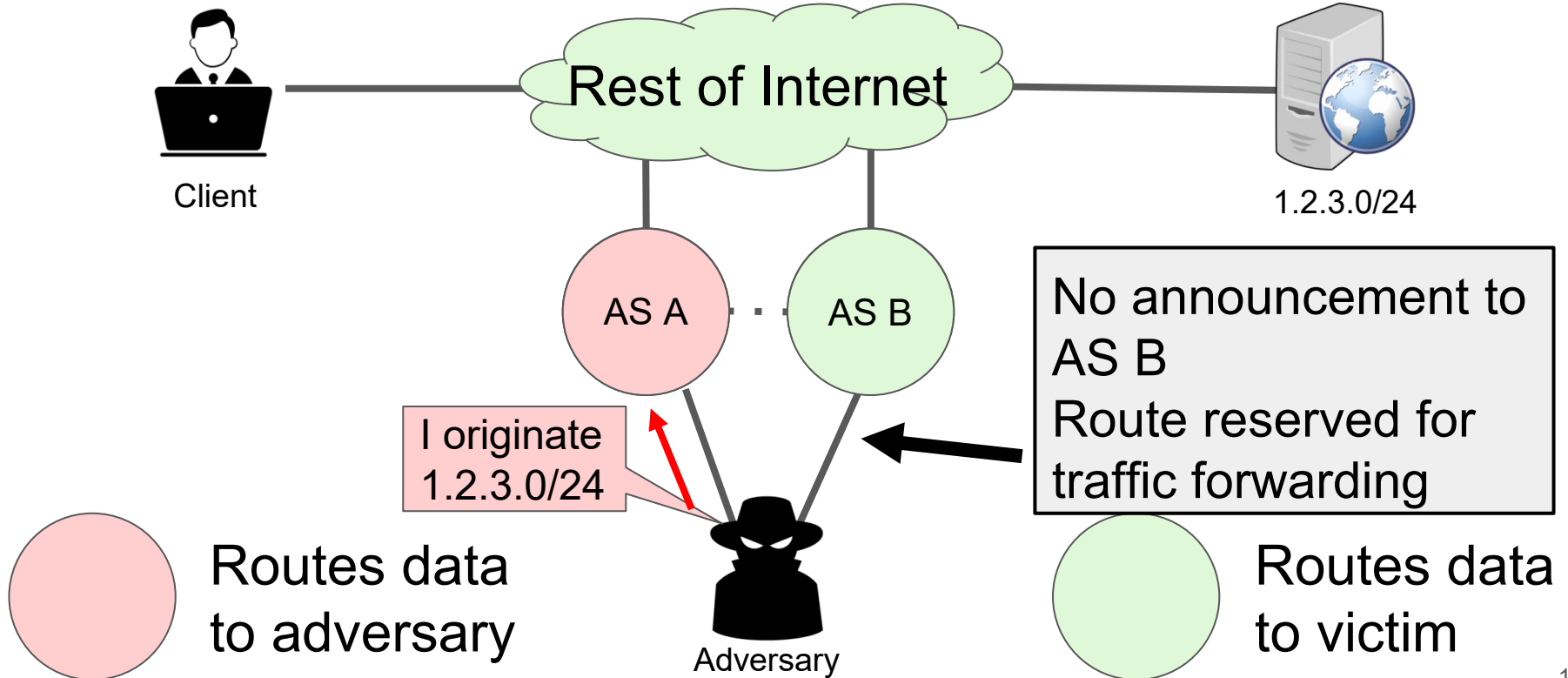
Our Contributions

- Use seemingly benign BGP communities to enable **48%** of ASes (incl. stubs) to launch interception
- Demonstrate **viability** and effectiveness of these attacks in the wild
- Introduce **targeted** BGP attacks that increase stealth and decrease attack cost

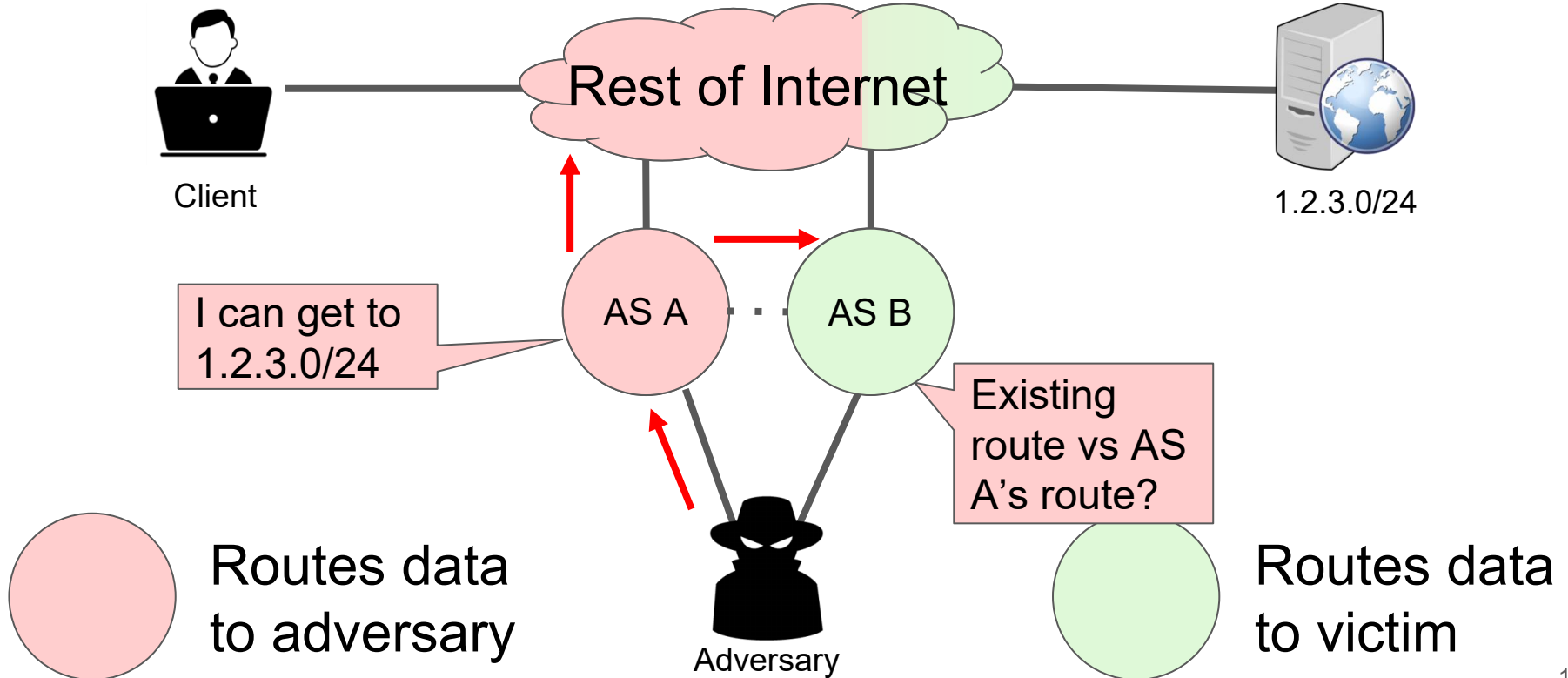
Overview

- How communities enable interception ←
- Real-world evaluation
- Targeted SICO attacks
- Simulation-based evaluation

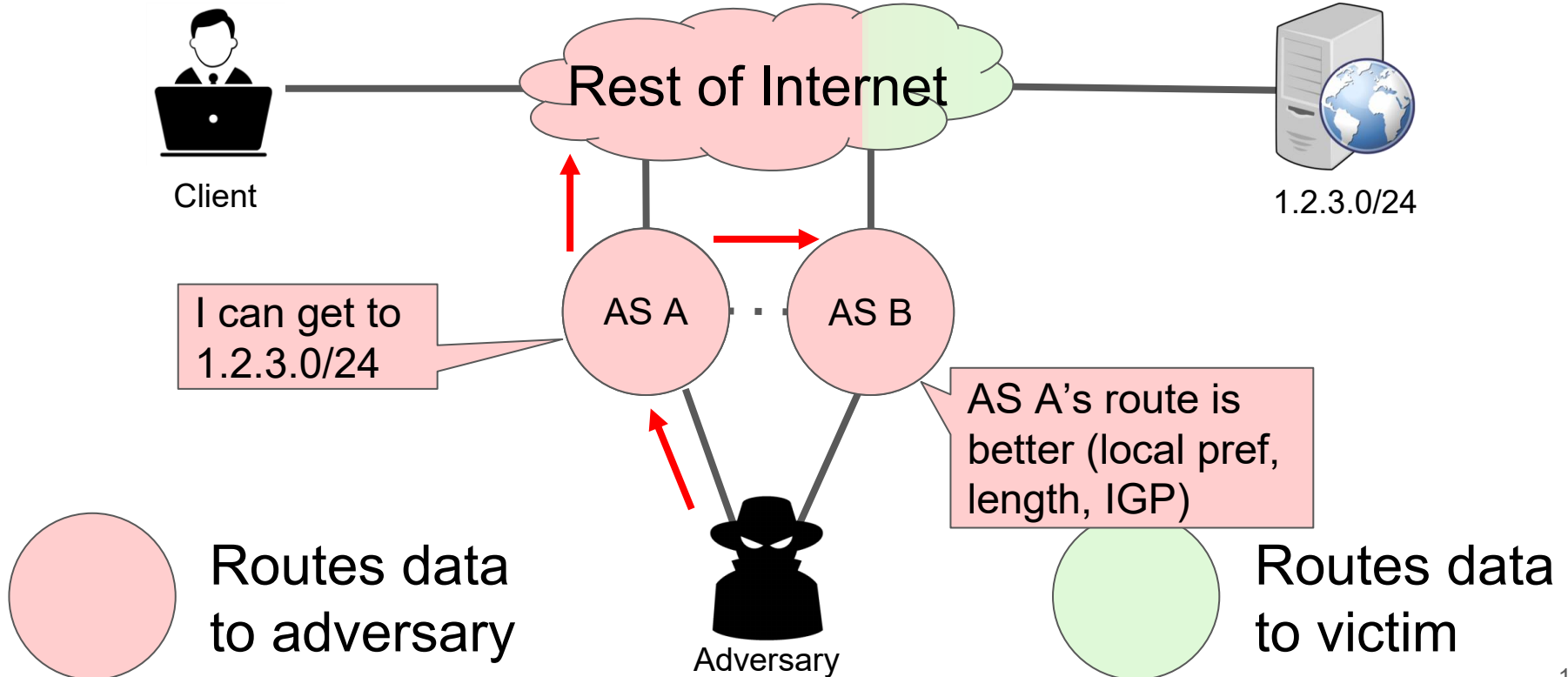
An interception scenario



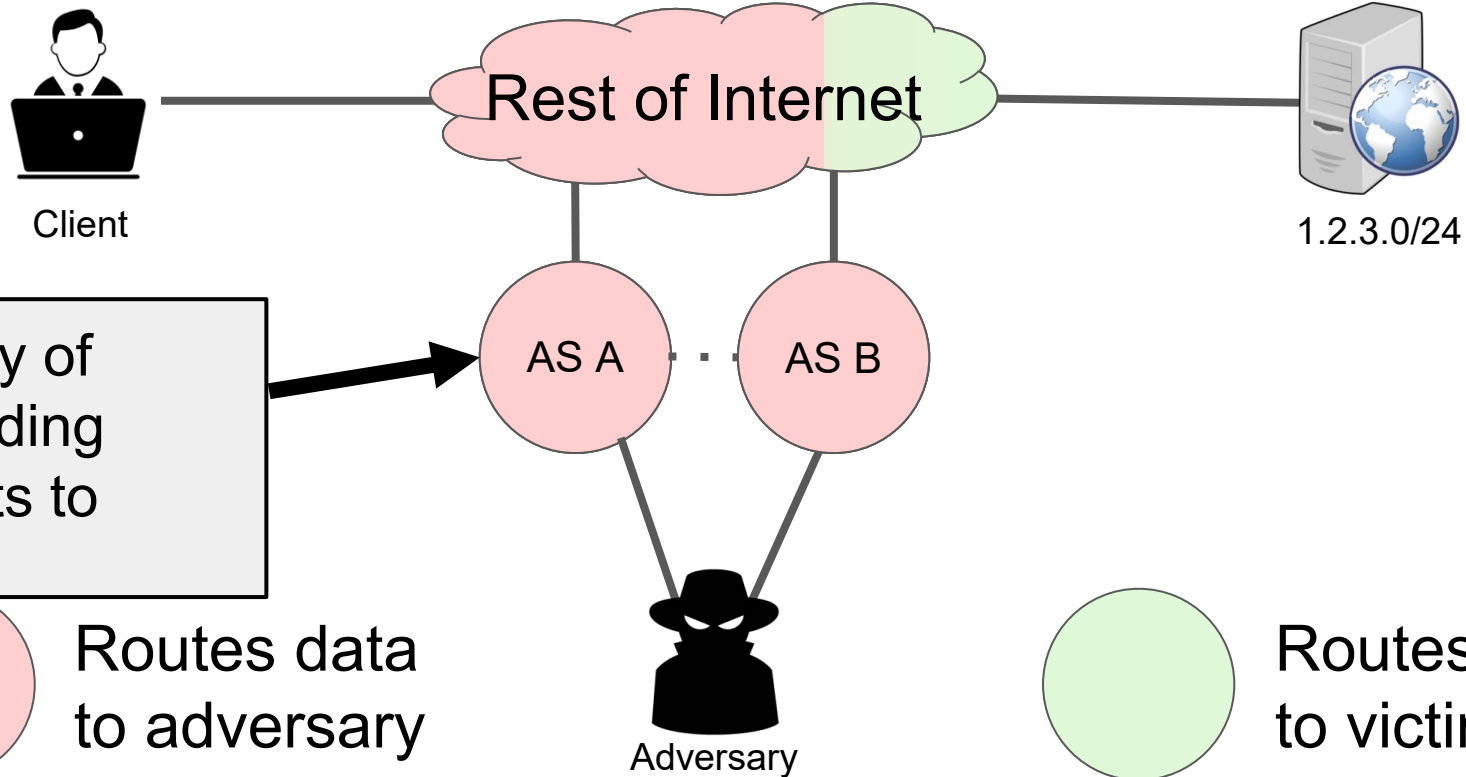
An interception scenario



An interception scenario



A failed interception scenario



SICO Attacks: Exploiting BGP Communities

- BGP communities:
 - Tags attached to BGP announcements
 - Can control announcement propagation (e.g., prevent exporting routes to neighbors)
- Support for propagation controlling communities by 21 of top 30 ISPs (as per as-rank.caida.org)

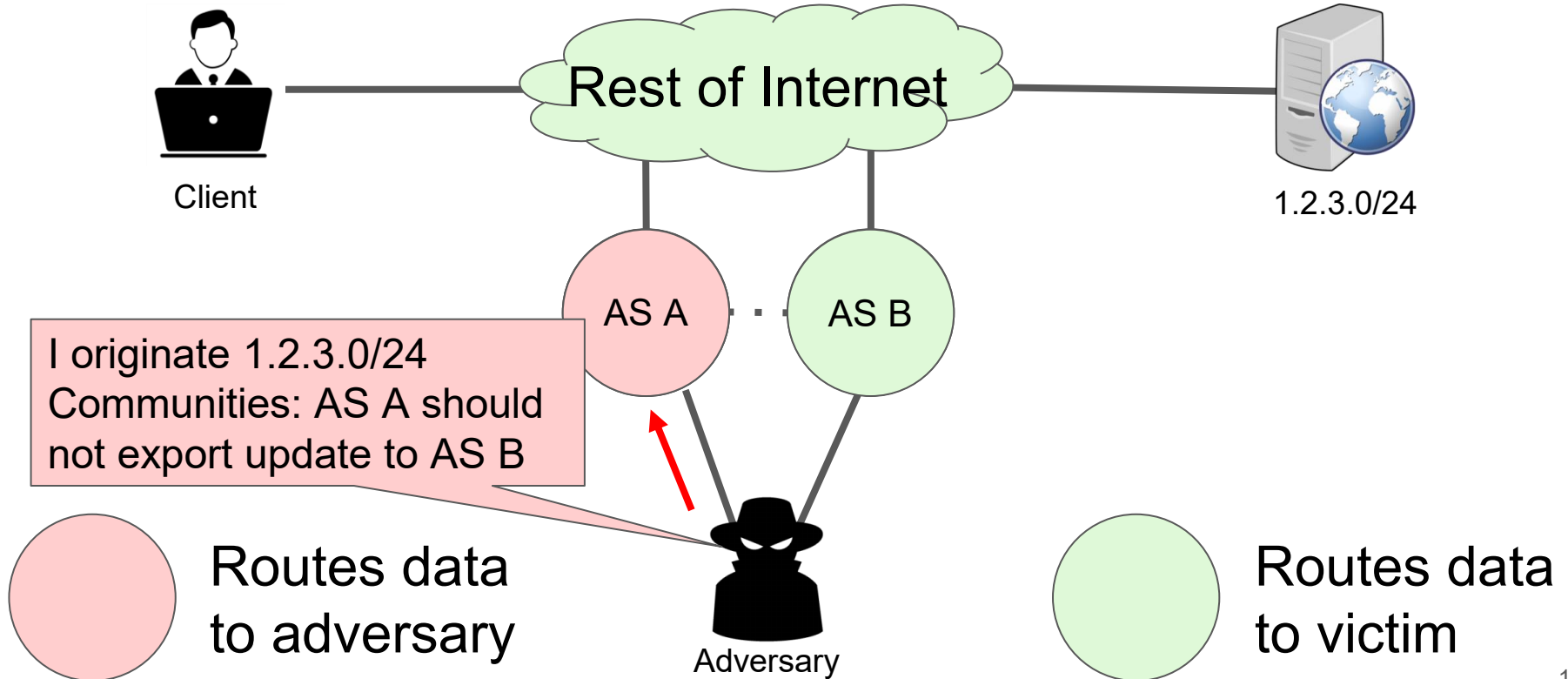
SICO Attacks: Exploiting BGP Communities

- BGP communities:

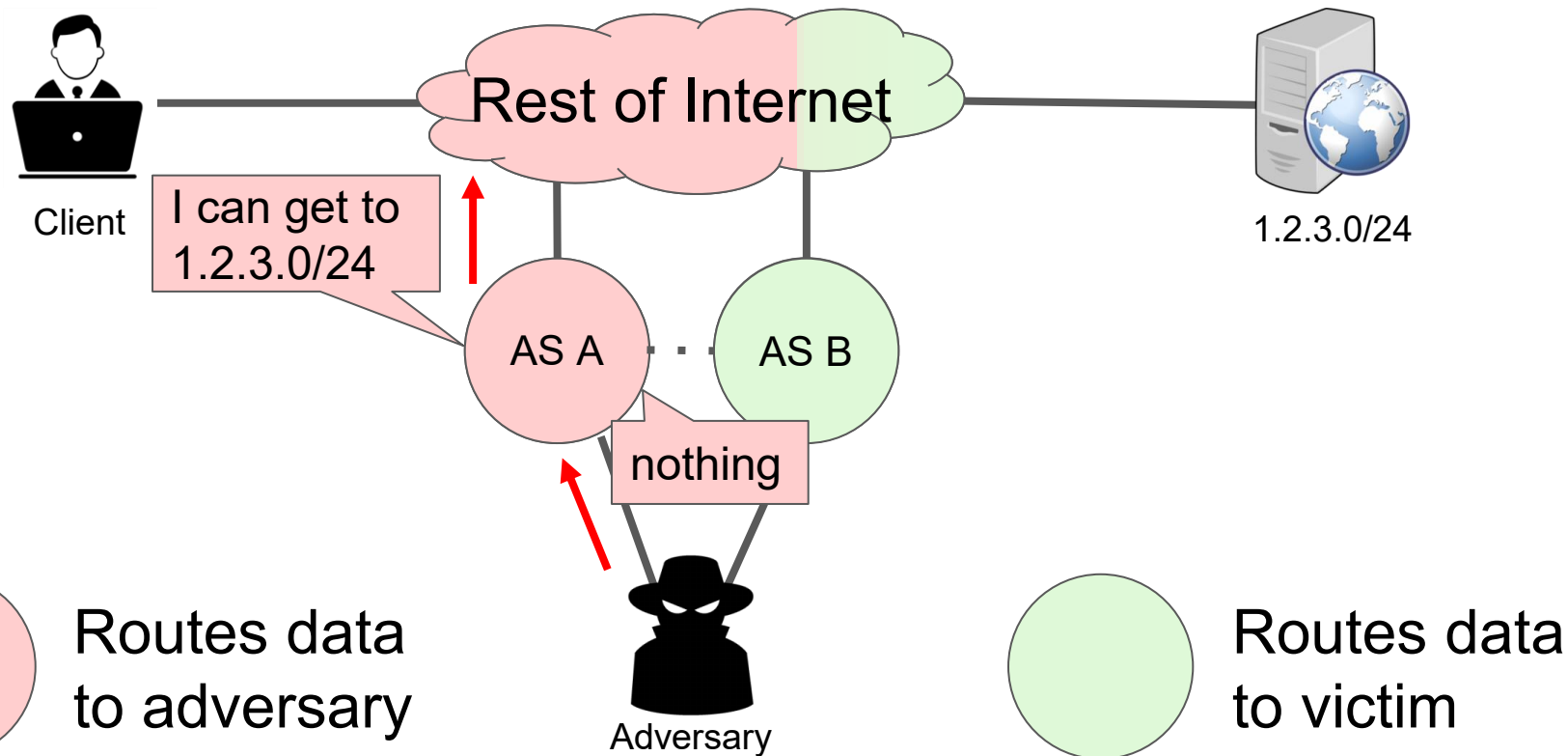
The same communities that allow for benign traffic engineering can be exploited to enable interception!

- Support for propagation controlling communities by 21 of top 30 ISPs (as per asrank.caida.org)

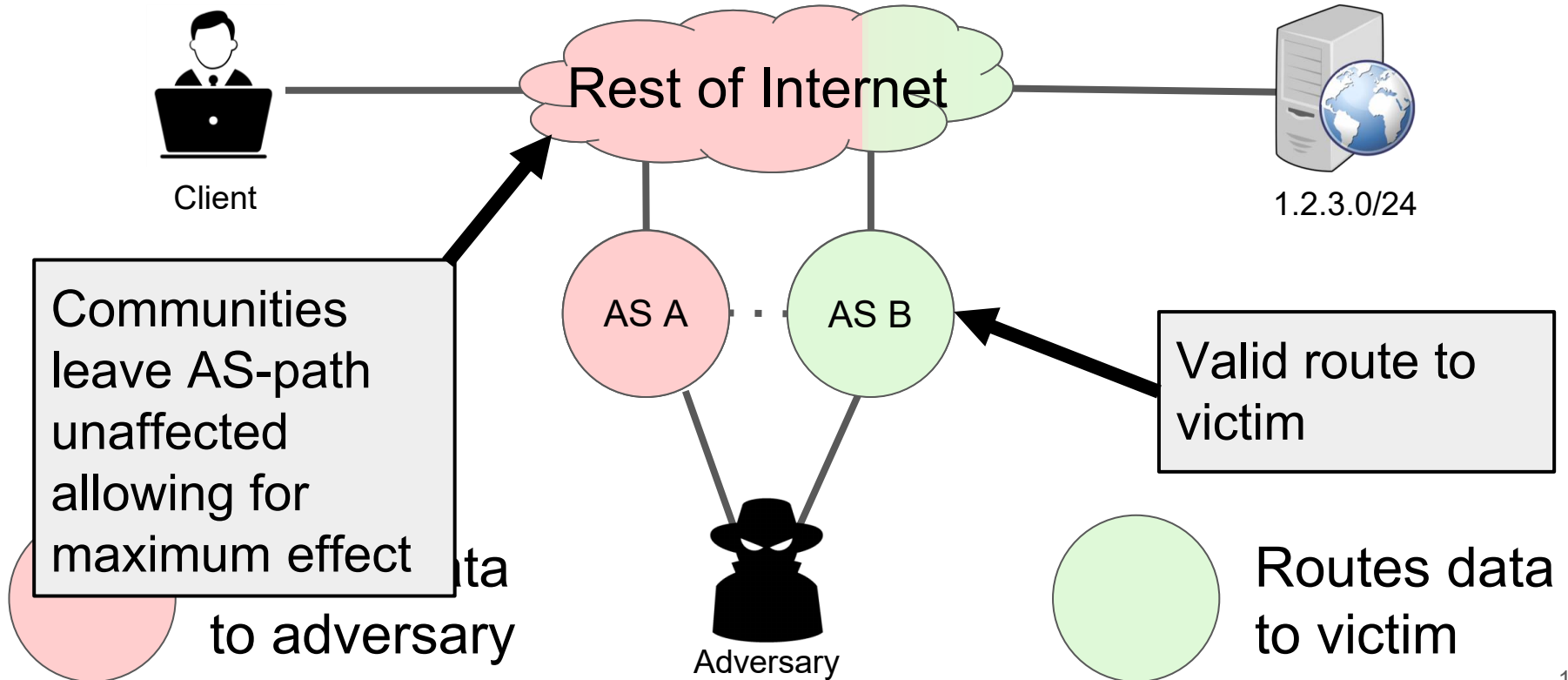
SICO Example



SICO Example

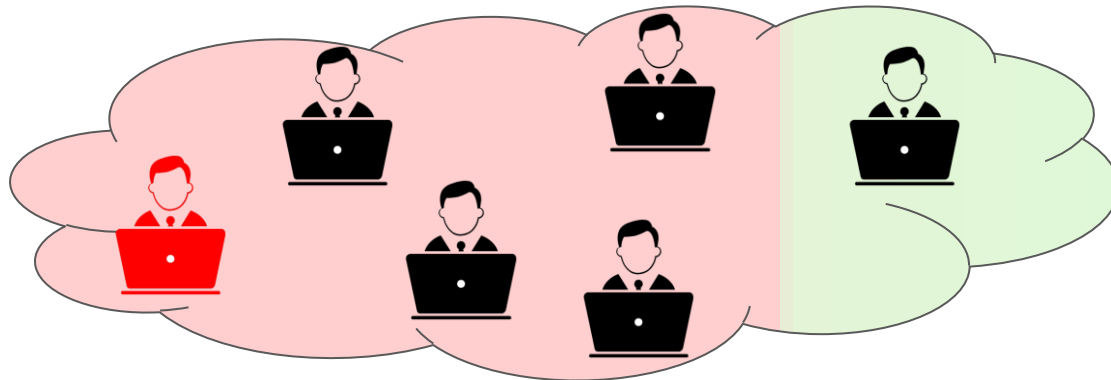


SICO Example



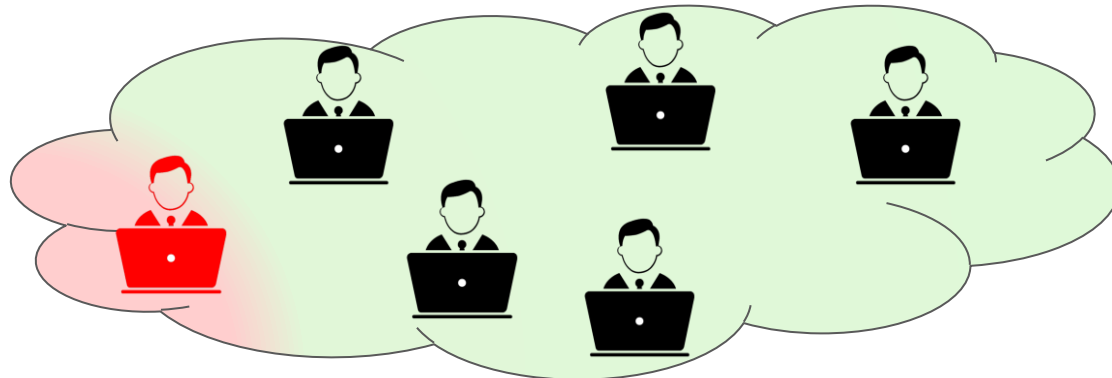
Targeting a BGP attack to specific IPs

Untargeted
interception
attack:



Many irrelevant source addresses affected

Targeted
interception
attack:



Only relevant sources affected

Why target a BGP attack to specific sources?

- **Cheaper:** affecting fewer source addresses reduces traffic volume and cost
- **Stealthier:** unaffected sources cannot detect attack via effect on throughput or latency
- **Greater viability:** viable against high-volume prefixes

Why The deep-dive into how

- Verizon and a BGP Optimizer

Knocked Large Parts of the

- Internet Offline Monday

attacked



Martin J Levy

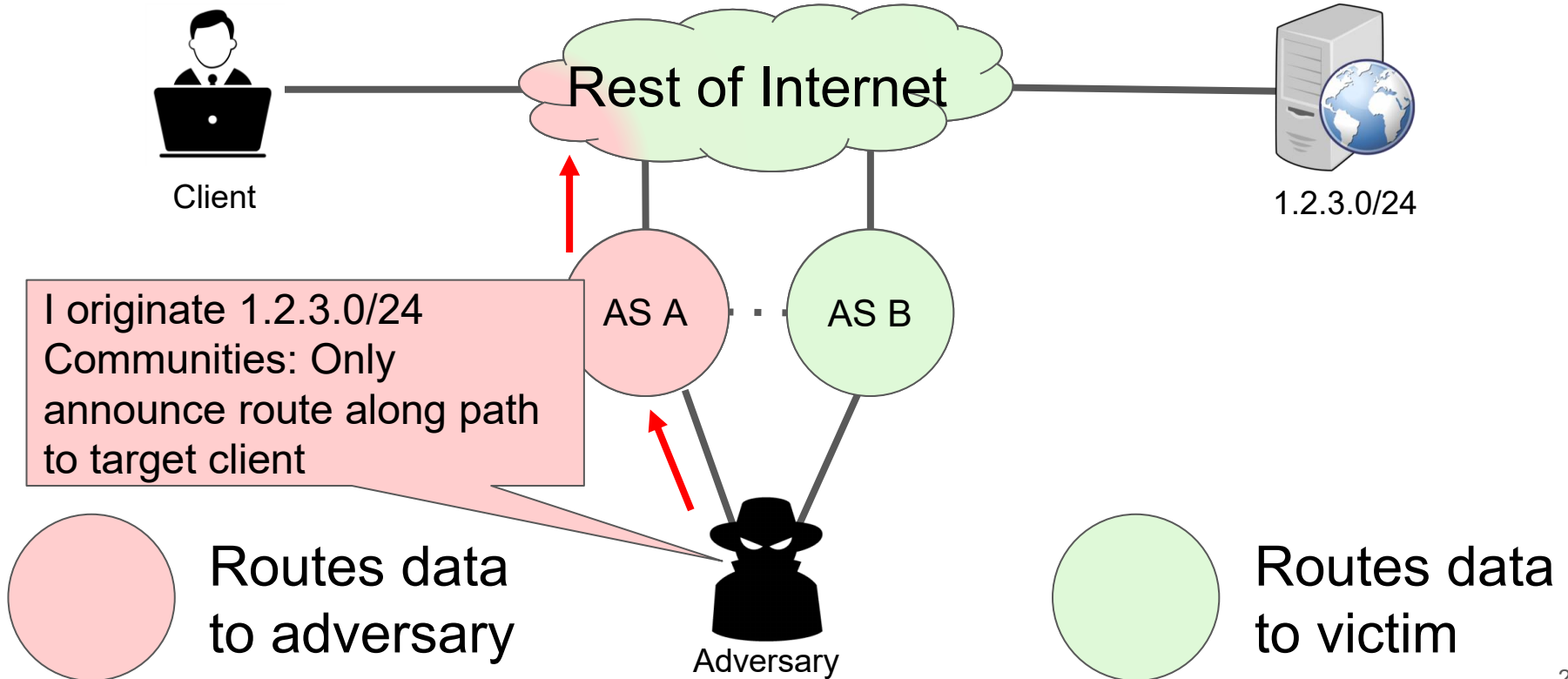
6/26/2019, 3:22:13 PM PDT

- Gre

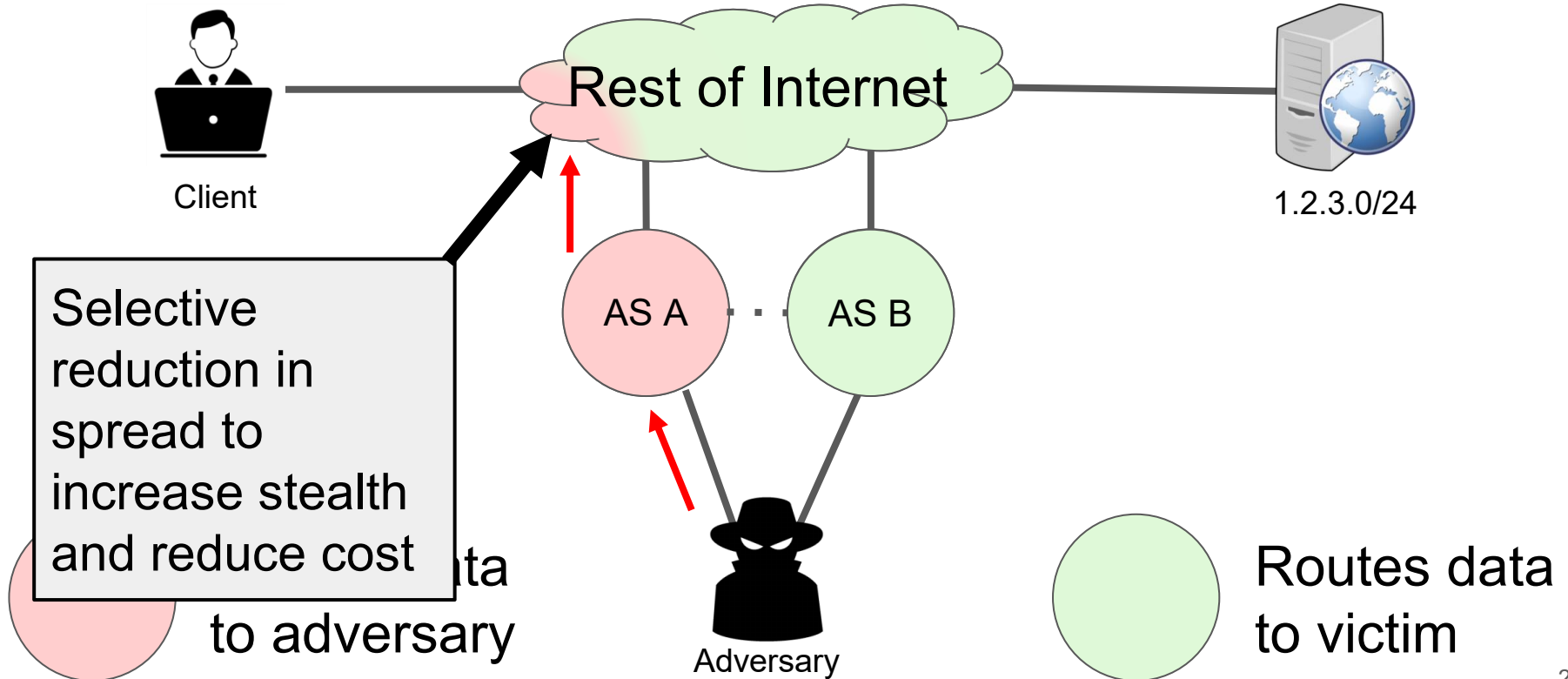
prefixes

An interception is just a DOS if adversary can't handle traffic volume

Targeted SICO Example



Targeted SICO Example



Overview

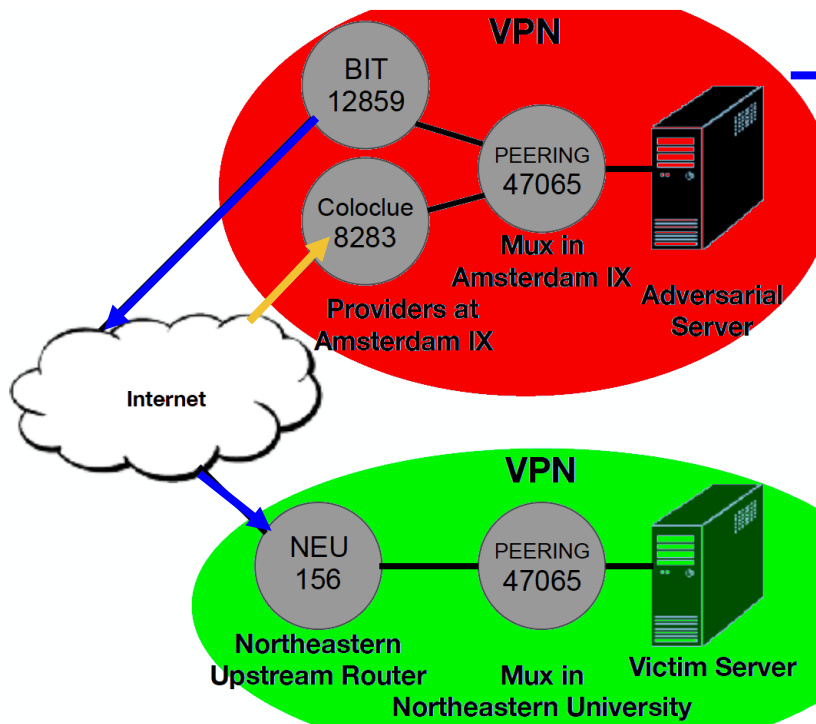
- How communities enable interception
- Real-world evaluation ←
- Targeted SICO attacks
- Simulation-based evaluation

Ethically Launching Attacks

- Used PEERING testbed
- Hijack/intercept only our own prefixes
- Repeated experiments with two different adversaries (Amsterdam and Seattle)

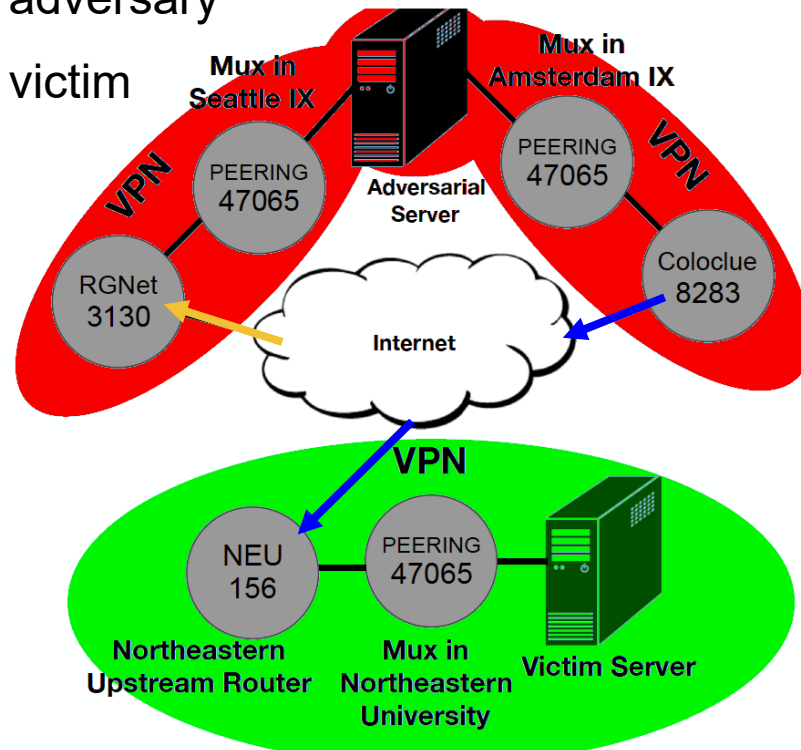
Experimental Setup

Amsterdam



Traffic:
to adversary
to victim

Seattle



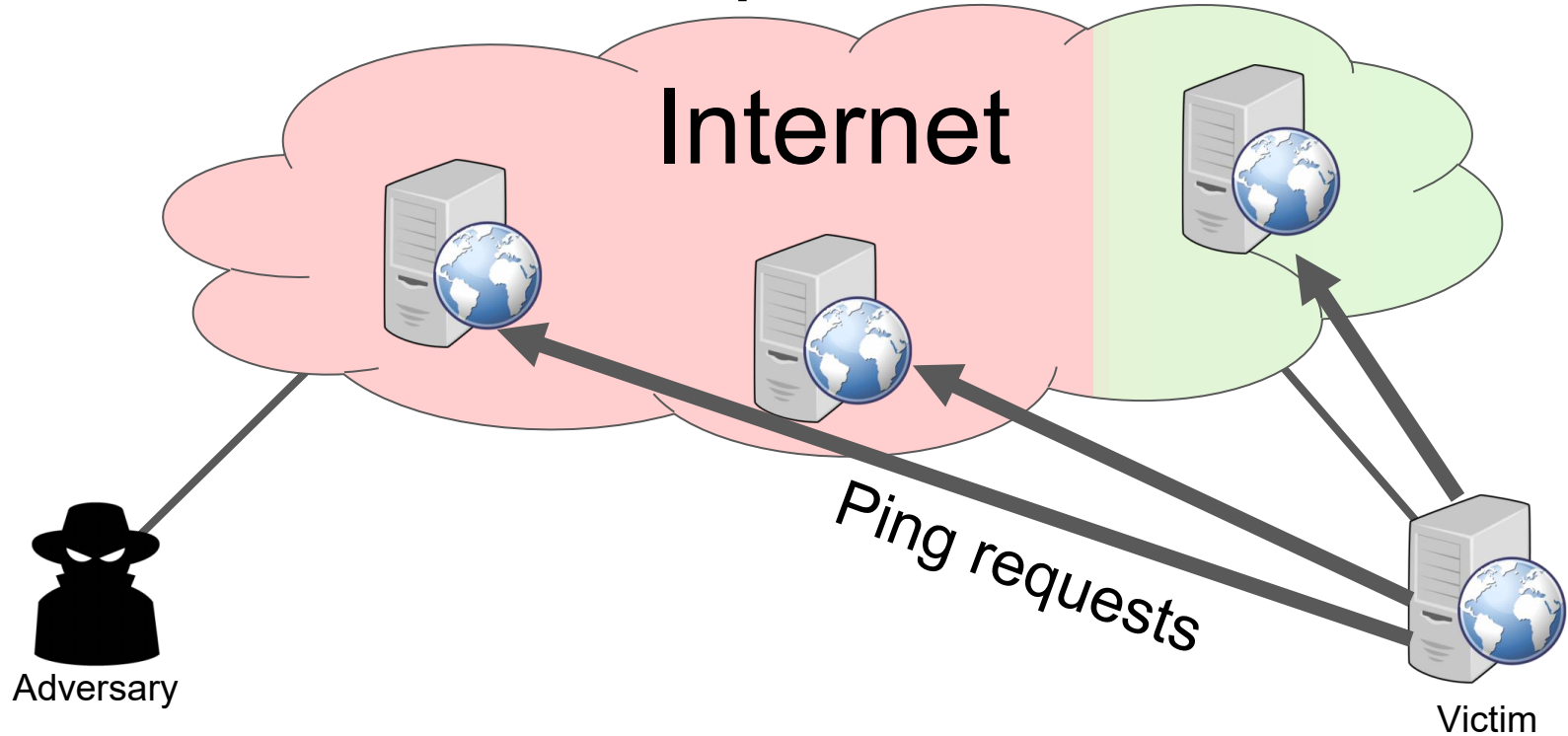
Real-world Evaluation Methodology

1. Engineer interception attack **with BGP communities** at each location
2. Compare with previous works:
 - Test **selective neighbor announcement** (i.e., only announce to one provider)
 - Compare propagation to **AS-path poisoning** (i.e., interception via AS-path manipulation)

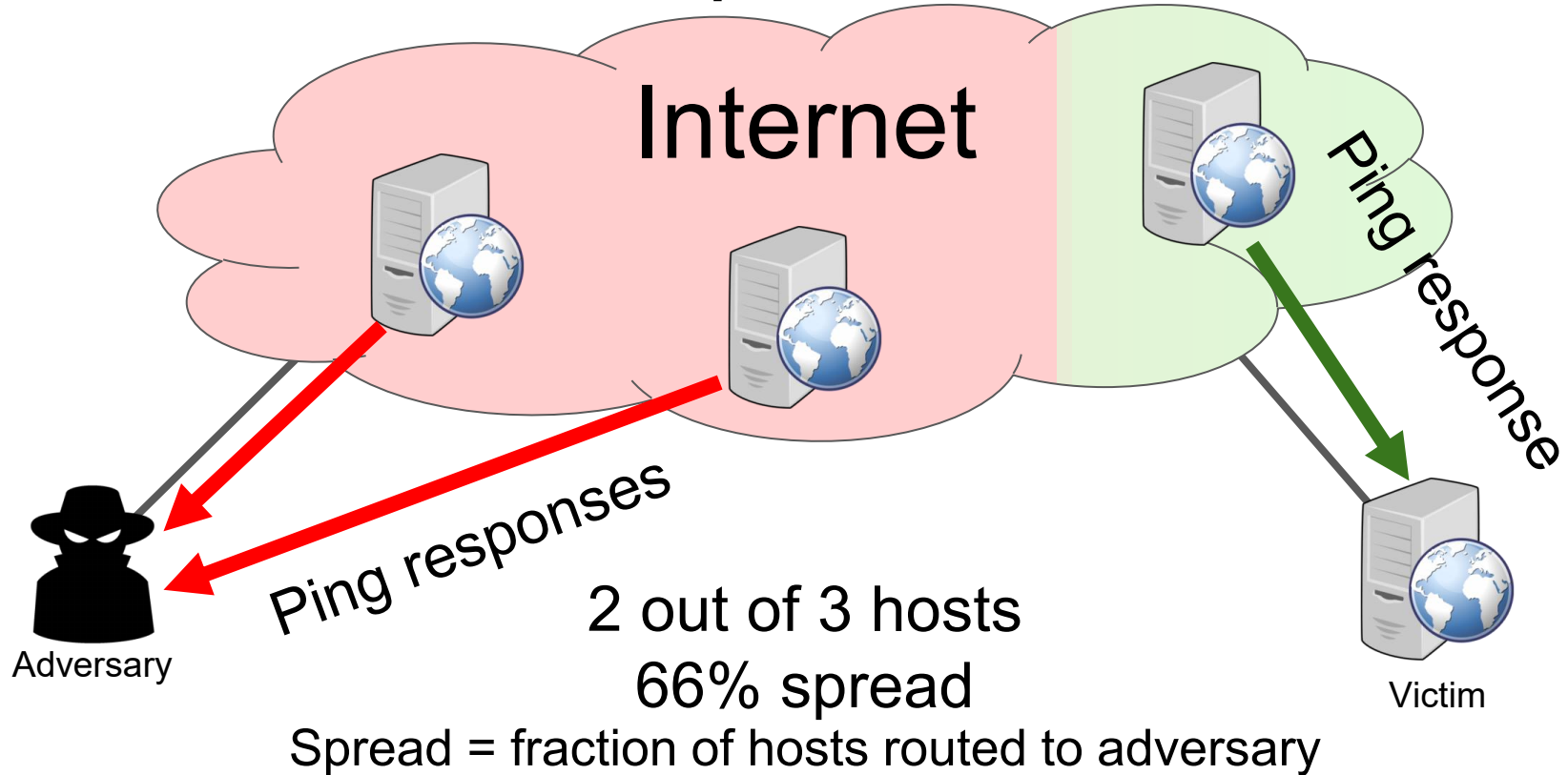
Real-world Evaluation Results

1. **Successfully** launched interception with communities at both locations
2. Selective neighbor announcement **failed to achieve interception** at either location
3. SICO attacks **propagated significantly further** than AS-path poisoning attacks ...

How to measure spread

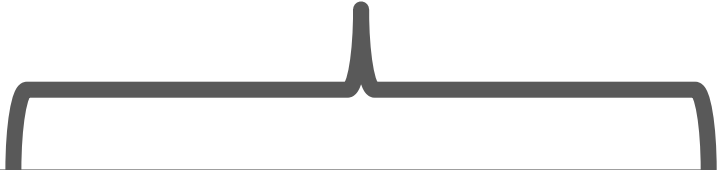


How to measure spread



Spread Comparison

Prior works



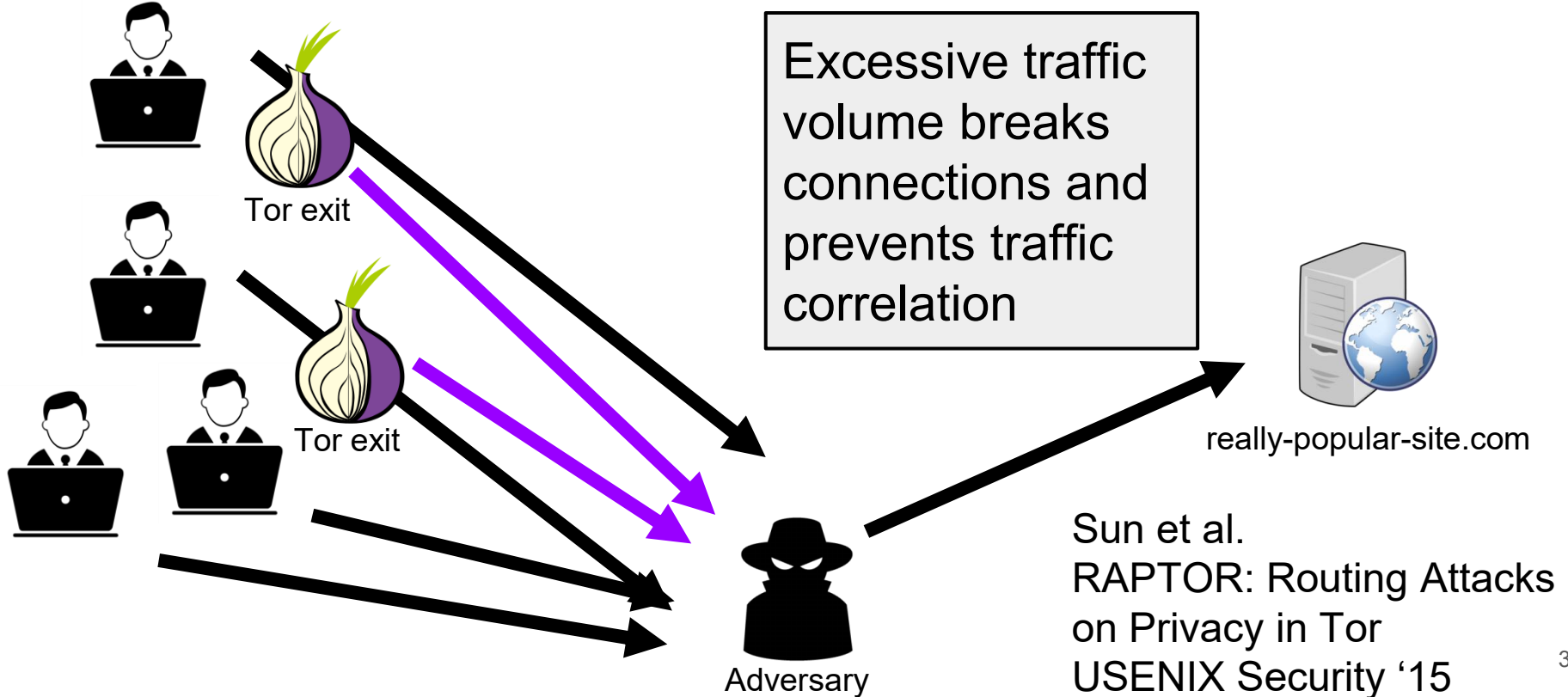
Location	Maximum achievable interception spread	Spread SICO	Spread path poisoning	Selective neighbor announcement
Amsterdam	68.9%	68.8%	52.6%	NA
Seattle	43.9%	38.9%	12.4%	NA

SICO improves spread significantly compared to path poisoning

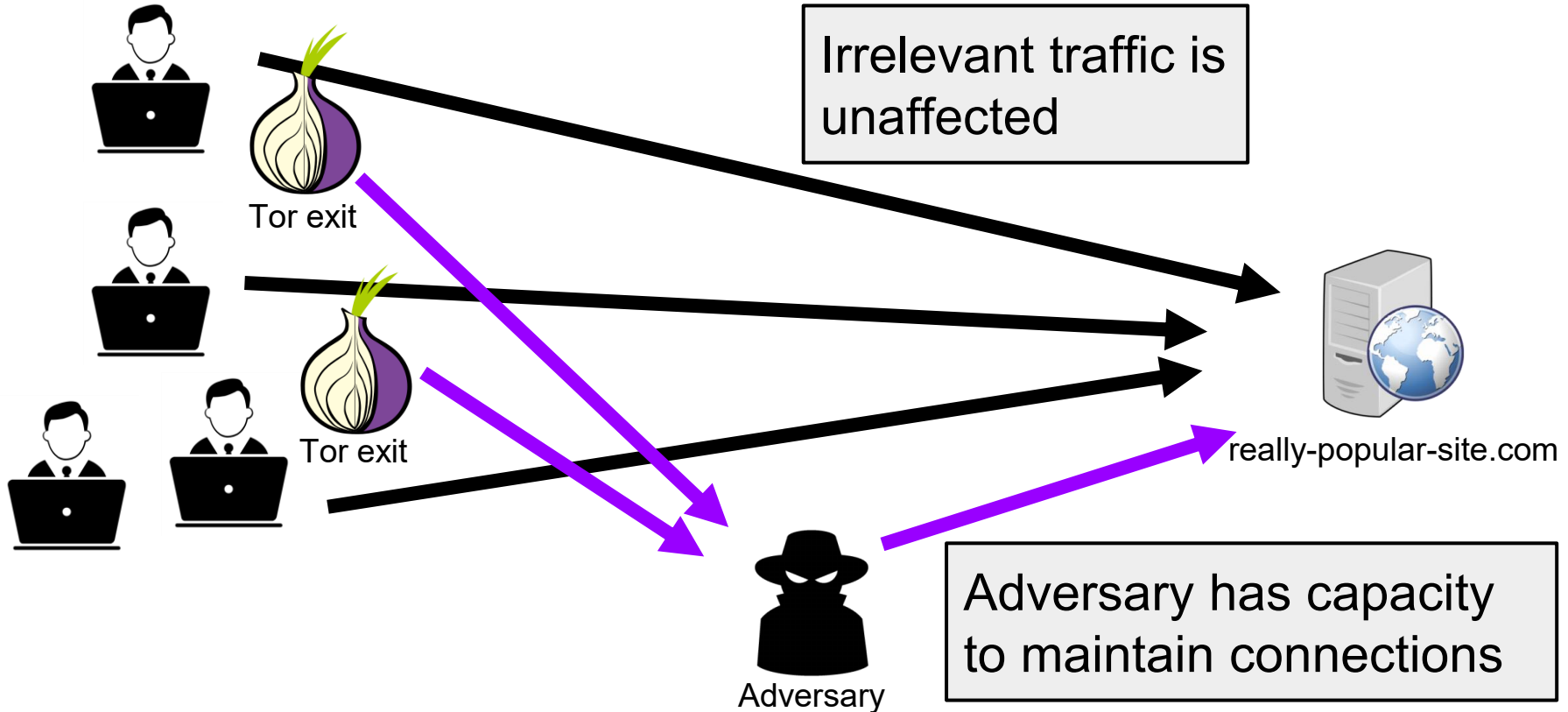
Overview

- How communities enable interception
- Real-world evaluation
- Targeted SICO attacks ←
- Simulation-based evaluation

Use of traditional interception against Tor



Targeted interception against Tor



Targeting top eight Tor exits

Tor exit node IP	Tor node ASN	Targeted attack spread
46.165.245.154	28753	5.5%
94.23.150.81	16276	1.8%
31.220.0.225	206264	0.2%
62.210.177.181	12876	0.5%
199.249.230.72	62744	3.3%
178.32.181.96	16276	1.9%
195.206.105.217	9009	8.0%
176.9.44.232	24940	0.7%
Average	NA	2.7%

Targeting top eight Tor exits

Tor exit node IP	Tor node ASN	Targeted attack spread
46.165.245.154	28753	5.5%
94.23.150.81	16276	1.8%
31.220.0.225	206264	0.2%
Average targeted attack spread was only 2.7% compared to 68.8% from untargeted interception		
176.92.101.55	16276	1.8%
195.206.105.217	9009	8.0%
176.9.44.232	24940	0.7%
Average	NA	2.7%

Overview

- How communities enable interception
- Real-world evaluation
- Targeted SICO attacks
- Simulation-based evaluation ←

Simulation Evaluation Results

- Found community support by **21/top 30 ASes** (by degree) through routing policy inspection
- Studied Internet topology around supporting ASes via **CAIDA AS-relations** data set
- **48%** of ASes capable of launching SICO attacks counting community forwarding

Simulation Evaluation Results

- Only multi-homed ASes are capable of interception
- 48% of all ASes represents 83% of multi-homed ASes

Takeaways Questions?

- BGP communities let adversaries shape malicious announcements
- This enables effective interception
- Even stub ASes can feasibly intercept traffic
- Future threat models should consider adversaries that can launch and target interception attacks

Thanks to support
from



OPEN
TECHNOLOGY
FUND

