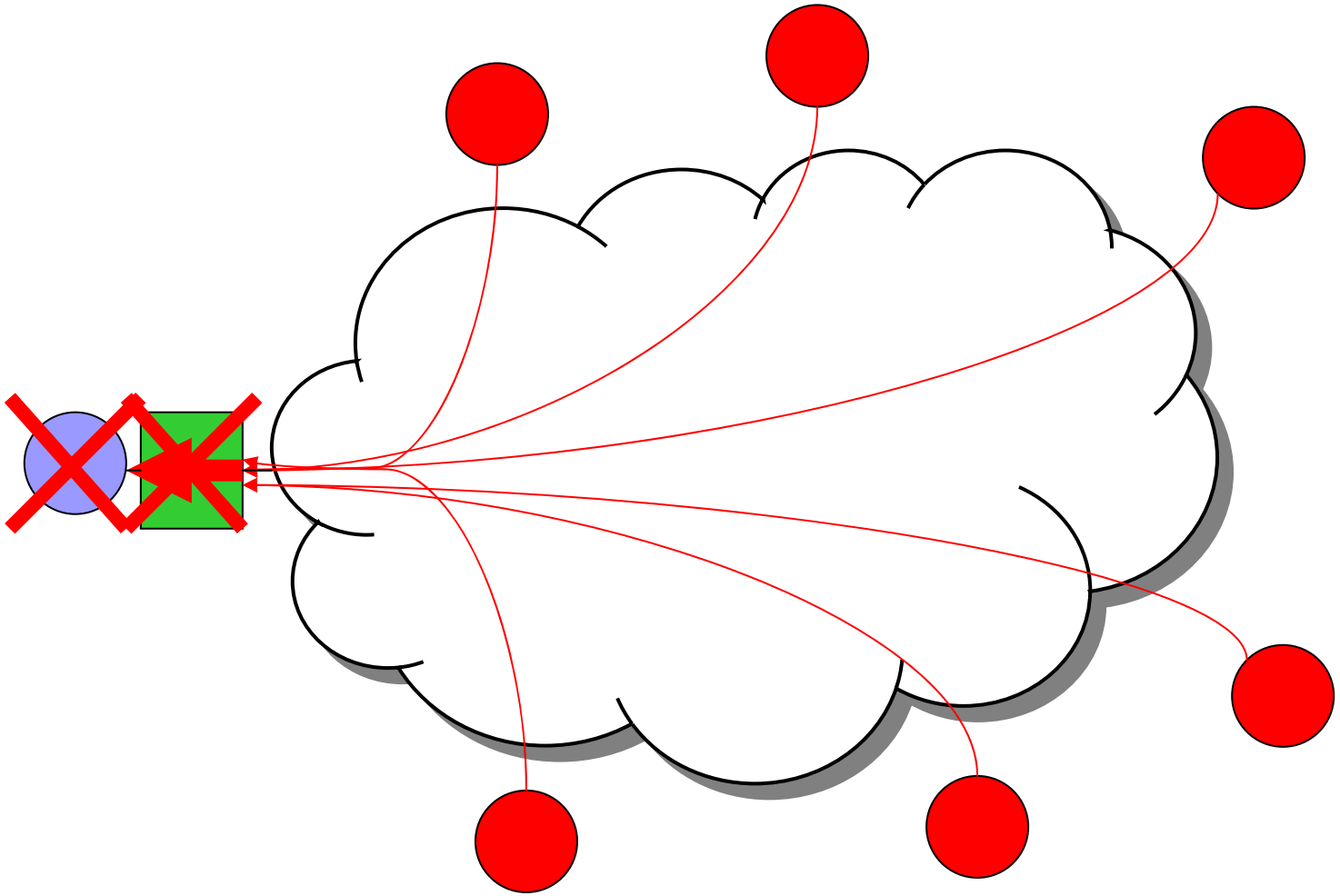
Shield: DoS Filtering Using Traffic Deflection

Erik Kline
UCLA
icebeast@lasr.cs.ucla.edu
Coauthors: Alexander Afanasyev, Peter Reiher

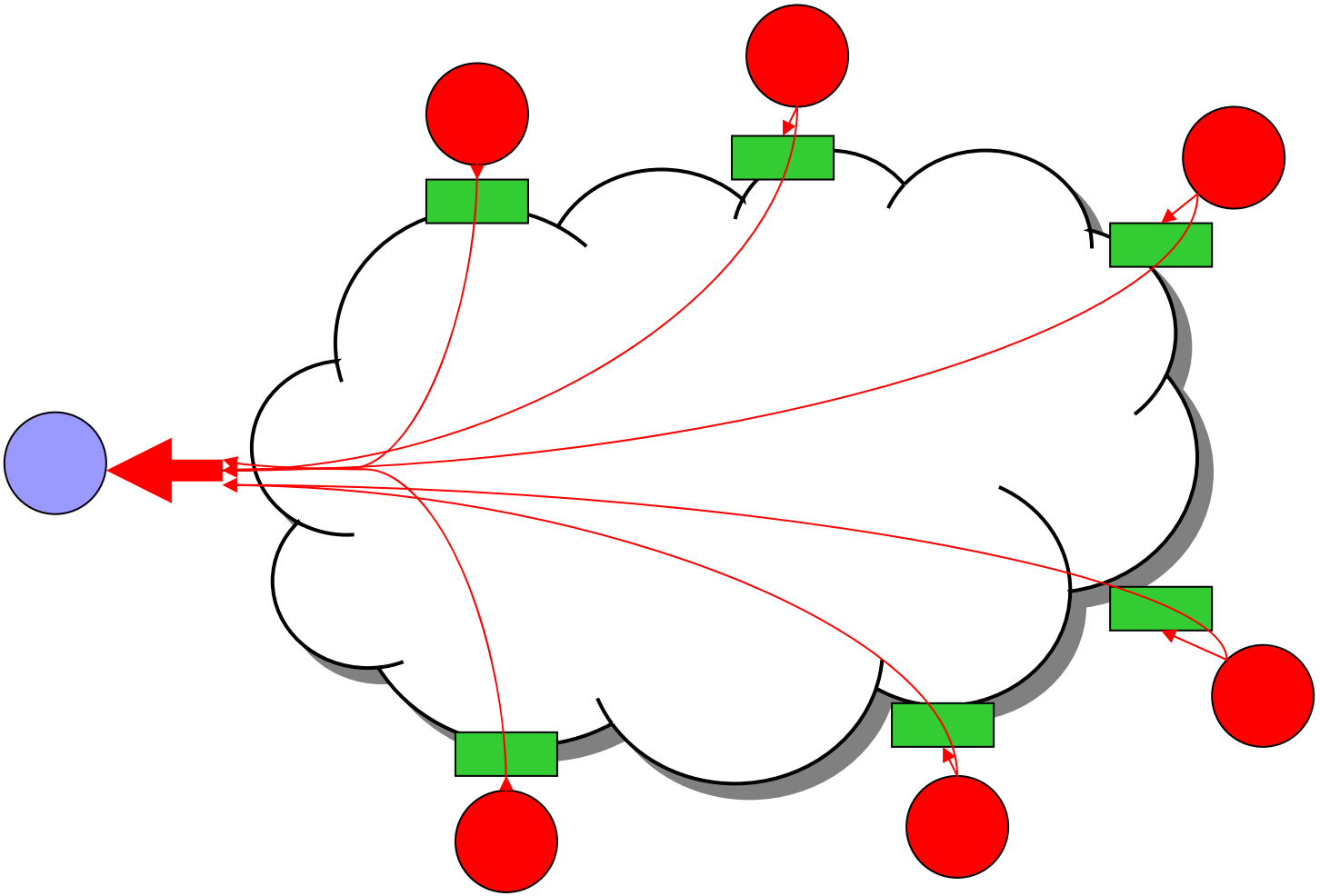
DoS: Still a problem?

- Denial-of-Service attacks still prevalent in today's Internet.
  - But there are several good filtering techniques!
- Deployment is the problem.
  - Where to deploy filters?
  - How to convince people to deploy defenses?
- Over-provisioning and CDNs are good options, but can be expensive.

Near the Victim



Near the Attacker



Where to deploy filters?

- Near the victim
  - Requires each possible victim to deploy filters
  - May be “too late”
- Near the attacker
  - Requires all edge networks to filter egress traffic.
  - May not be enough traffic volume to detect.
- In the core…

Problem

- Most filtering locations are poor
  - Infeasible
  - Limited protection
- Lack of proper incentives to deploy filters

Our Solution: Shield

- Instead of bringing the filter to the traffic, bring the traffic to the filter.
  - Redirect traffic to filtering nodes using routing techniques
  - Deliver filtered traffic to legitimate nodes
- Incentivize deployment via Insurance-like deployment model.

Traffic Deflection

- Two mechanisms
  - IXP-based nodes advertising false paths.
    - All nodes at the IXP send traffic to the filter
    - Filter sends legitimate traffic to the host
  - Filtering nodes legitimately announcing a prefix
    - All traffic is redirected to filtering nodes.
    - Send legitimate traffic to the host.

On Demand

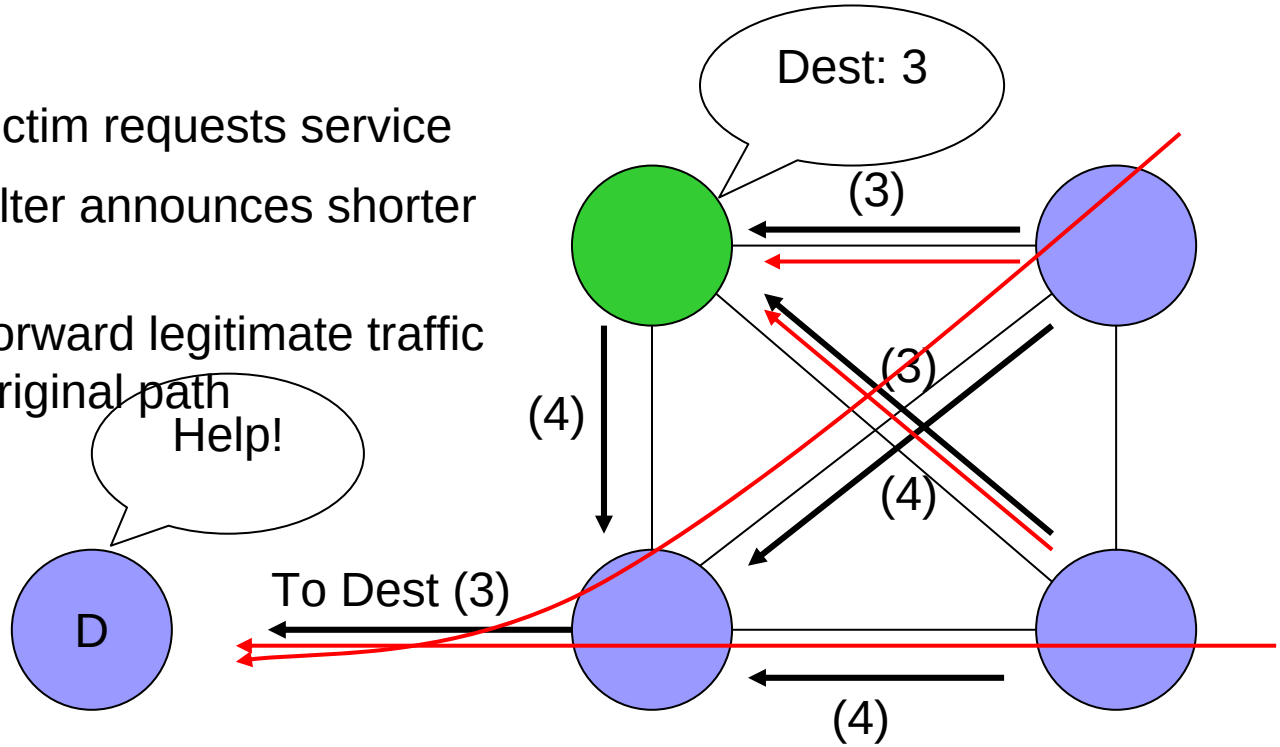
- Service requested only during an attack
  - Automated
  - Manual Request
- Return to service after attack
  - Victim may request termination of service at anytime.

IXP Traffic Deflection

1) Victim requests service

2) Filter announces shorter path

3) Forward legitimate traffic on original path

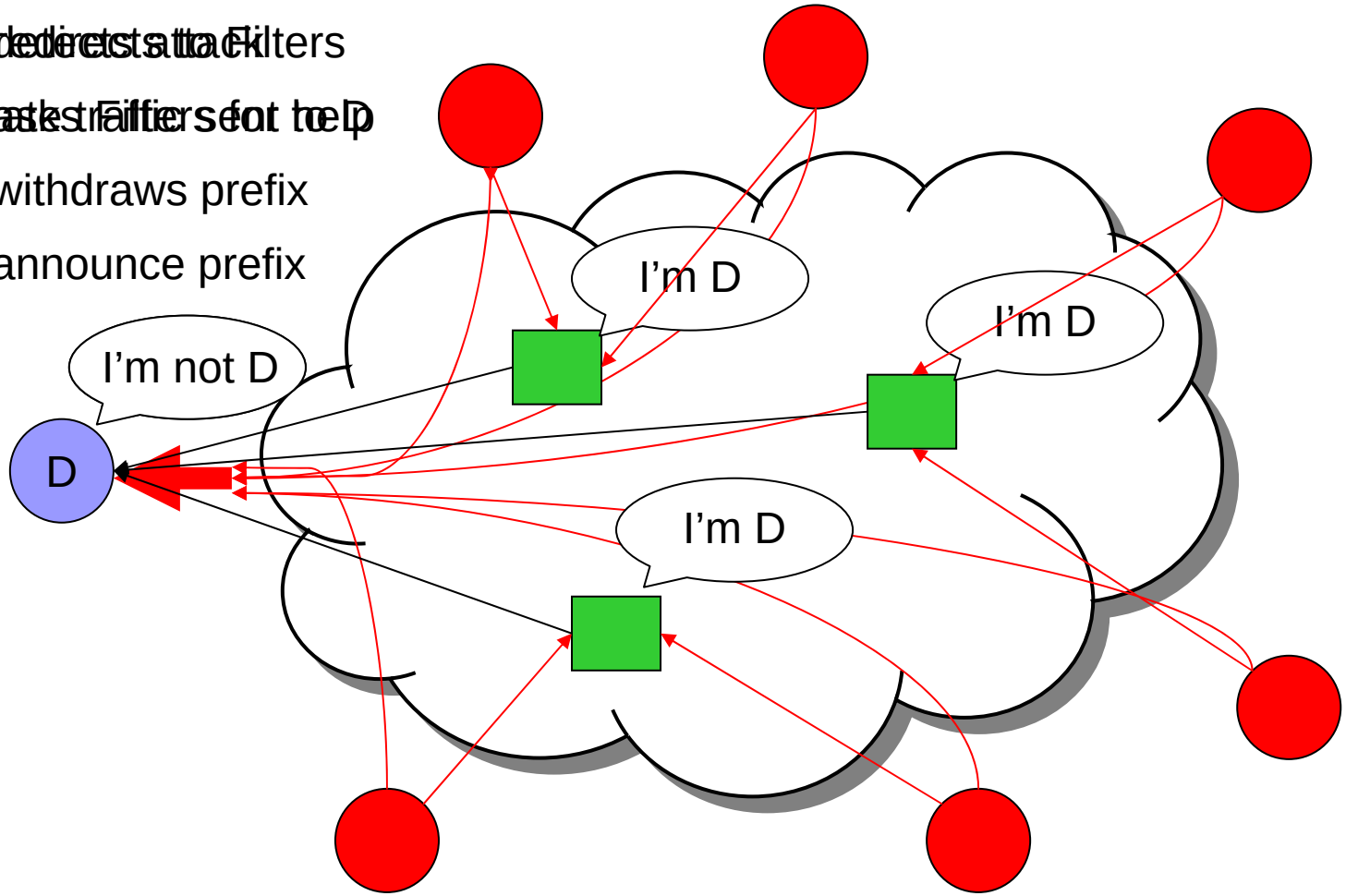


IXP Problems

- Has to be deployed at an IXP
  - Limited deployment options is not much an improvement
- Only protects against DoS traffic that transits an IXP

General Traffic Deflection

1) Victim detects attack
2) Victim asks filters for help
3) Victim withdraws prefix
3) Filters announce prefix



Advantages of Traffic Deflection

- Can be deployed anywhere!
  - IP Anycast allows traffic to be redirected wherever you want it to.
- Agnostic to filtering technique
- Filters can protect multiple victims
  - Traffic redirection makes it possible to defend anyone
- Multiple filters can protect one victim

Deployment Incentives

- Everything previously mentioned
- On-demand Service
  - Only use resources during an attack
  - Can protect more possible victims than resources allow.
- Lends itself to a Insurance-Style Business Model

Wait! How does the traffic get delivered?

- Destination has withdrawn its route!
- Possible Delivery methods
  - Hidden IP addresses
  - Source Routing
  - New Advanced Routing techniques
  - ISP agreements
  - Overlay networks

Delivery Problems

- Hidden IP Addresses
  - Relies on a secret, single point of failure
  - Could use multiple hidden IP addresses or automatic IP changing.
- Source Routing
  - Generally, not widely deployed
  - Adversaries could also use Source Routing

Delivery Problems Cont.

- New Advanced Routing Techniques
  - Still in developmental stages
- ISP Agreements
  - Requires ISP agreements, limiting deployability.
- Overlay Networks
  - Requires the existence of a large, well distributed overlay.

Other Possible Problems

- Attackers purposely causing route flapping
- Attackers trying to do more damage than filters can keep up with.
  - Run on the bank!
- Attackers as insiders

Open Research Questions

- How quickly can this service respond to an attack?
- How quickly can you return to nominal service?
- What is the effect on legitimate traffic?

Questions?