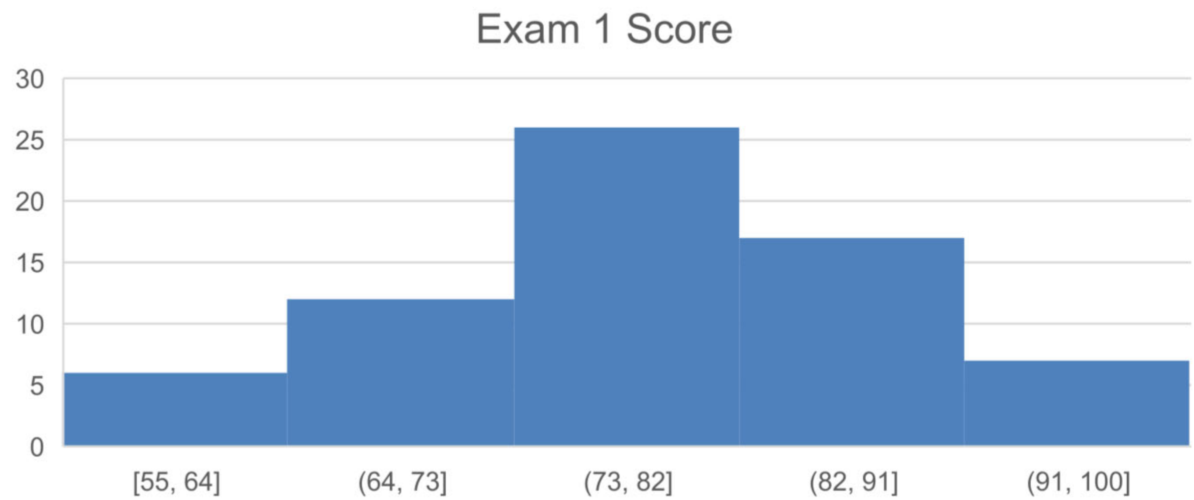
Announcement

- Take-home Exam 1 example answer is uploaded.
  - Average: 78.7



- Quiz 4
  - Opens at 9am on 14 Mar, 2023
  - Closes at 6:30pm on 20 March 2023
  - Covers Week 7 and 8 lecture slides

CS5321 Network Security
Week9: DoS Attacks

Daisuke MASHIMA

http://www.mashima.us/daisuke/index.html

2022/23 Sem 2

Agenda

- **(Traditional) Denial-of-service attacks and defence**
- **SIFF (IEEE S&P 2004)**
  - Enabling receiver to stop misbehaving senders
- **Crossfire (IEEE S&P 2013)**
  - How to disrupt the Internet itself with botnets?

Denial-of-service (DoS) attacks

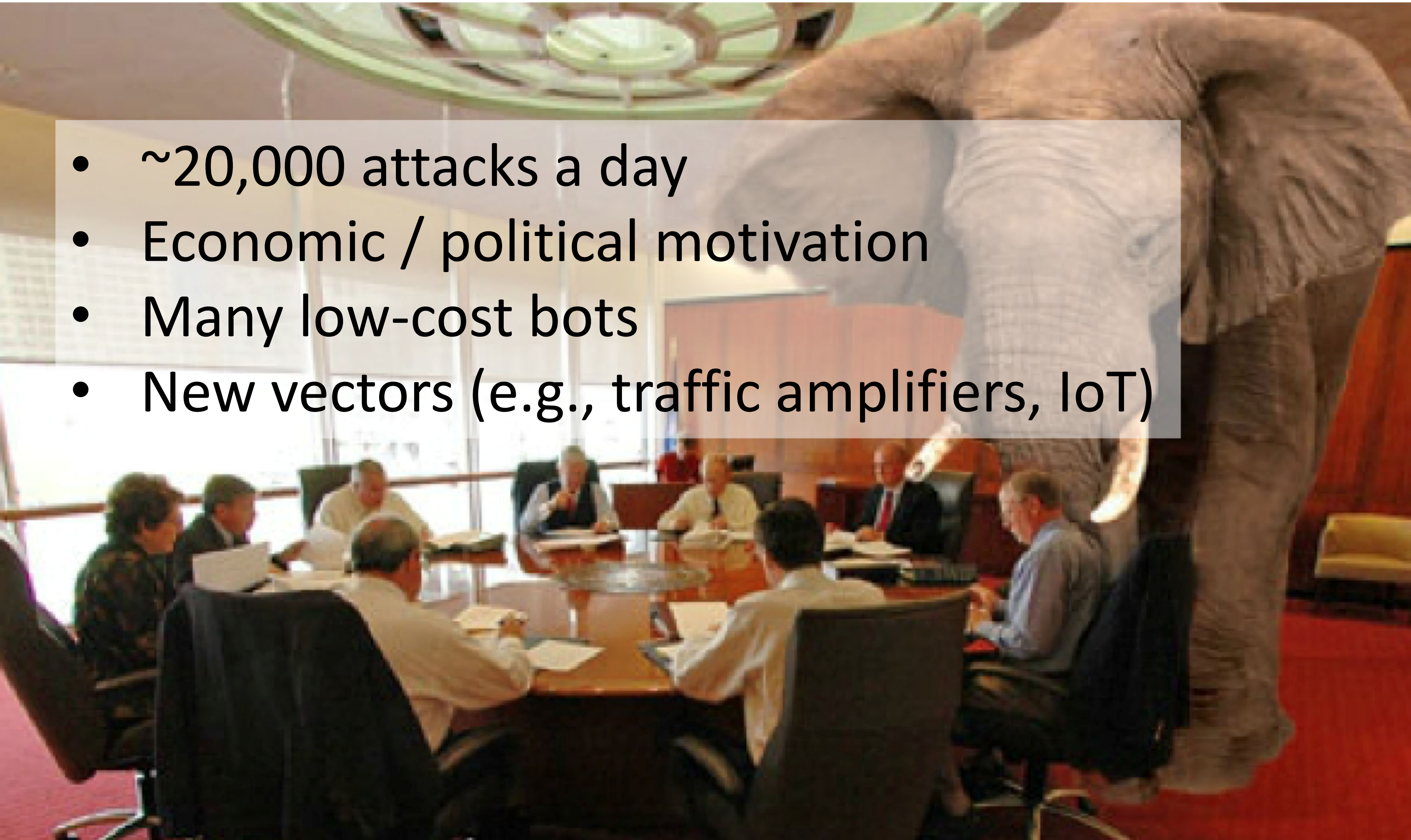
- **Definition** of the **denial-of-service problem**
  - A group of ***authorized*** users of a ***specified service*** is said to ***deny service*** to ***another*** group of ***authorized*** users if the former group makes the specified service ***unavailable*** to the latter group for a period of time which exceeds the intended (and advertised) service ***maximum-waiting time***

    Gligor, "A NOTE ON THE DENIAL-OF-SERVICE PROBLEM," IEEE Security & Privacy, 1983

  - Not considered as a security problem until late 80s

Elephant in the room

- ~20,000 attacks a day
- Economic / political motivation
- Many low-cost bots
- New vectors (e.g., traffic amplifiers, IoT)



Recent news

SingCERT
Singapore Computer Emergency Response Team

W

Global Ransom DDoS Campaig

Published on 04 Sep 2020
Updated on 02 Jul 2021

There have been reports of a new global ransom distr
finance, travel and e-commerce industries.

Targeted organisations may receive an extortion email
infrastructure if the ransom was not paid. The threat ac
demands have gone up from 1 BTC or 2 BTC in 2019,

TECH

Cyberattack hits Ukrainian banks and government websites

PUBLISHED WED, FEB 23 2022•11:08 AM EST | UPDATED WED, FEB 23 2022•6:15 PM EST

Lauren Feiner
@LAUREN_FEINER

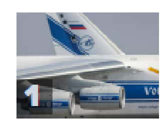
SHARE

KEY POINTS

- Several Ukrainian government websites were offline on Wednesday as a result of a mass distributed denial of service attack, a Ukrainian official said.
- A DDoS attack is when a hacker floods a victim's network or server with traffic so that others are unable to access it.
- The source of the attack is not yet confirmed but the outages come as Russia has positioned troops to be able to invade Ukraine.

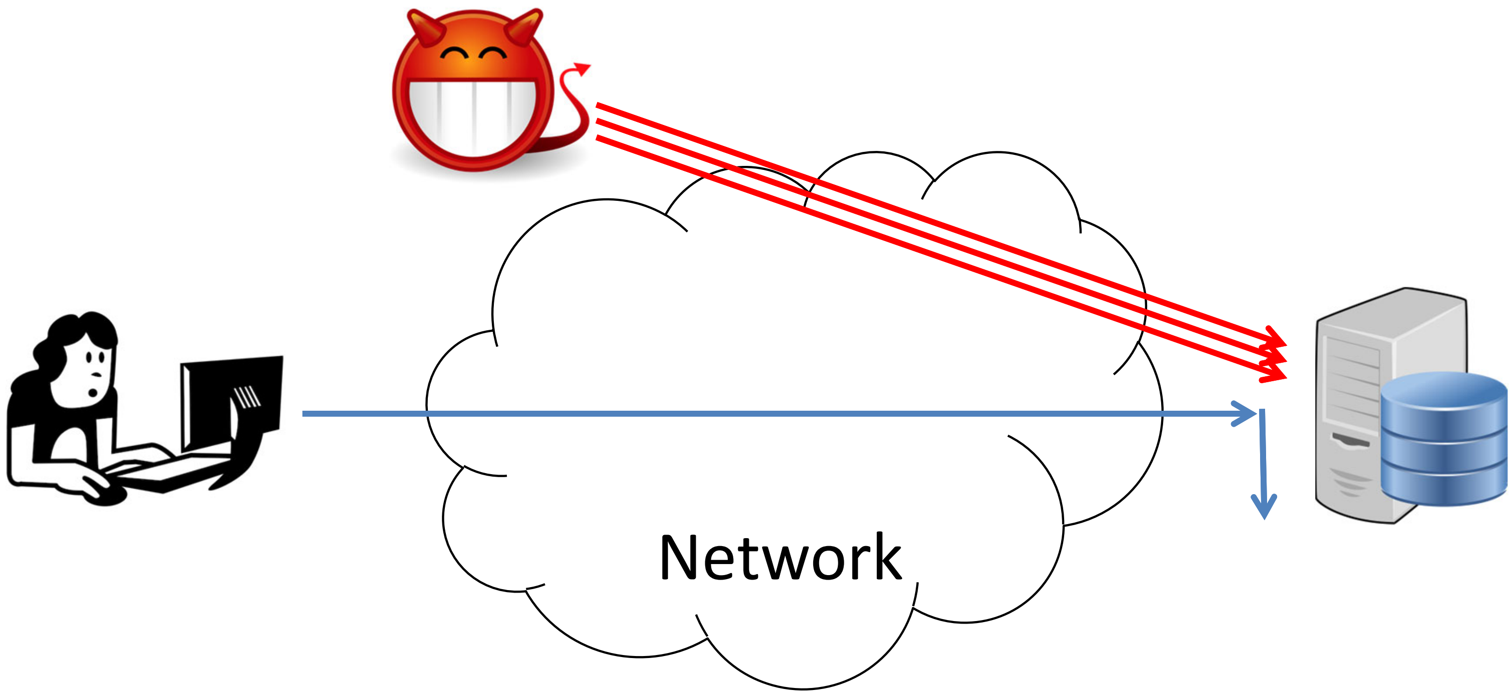
TV
The News With Shepard Smith
UP NEXT | **Shark Tank** 08:00

TRENDING NOW



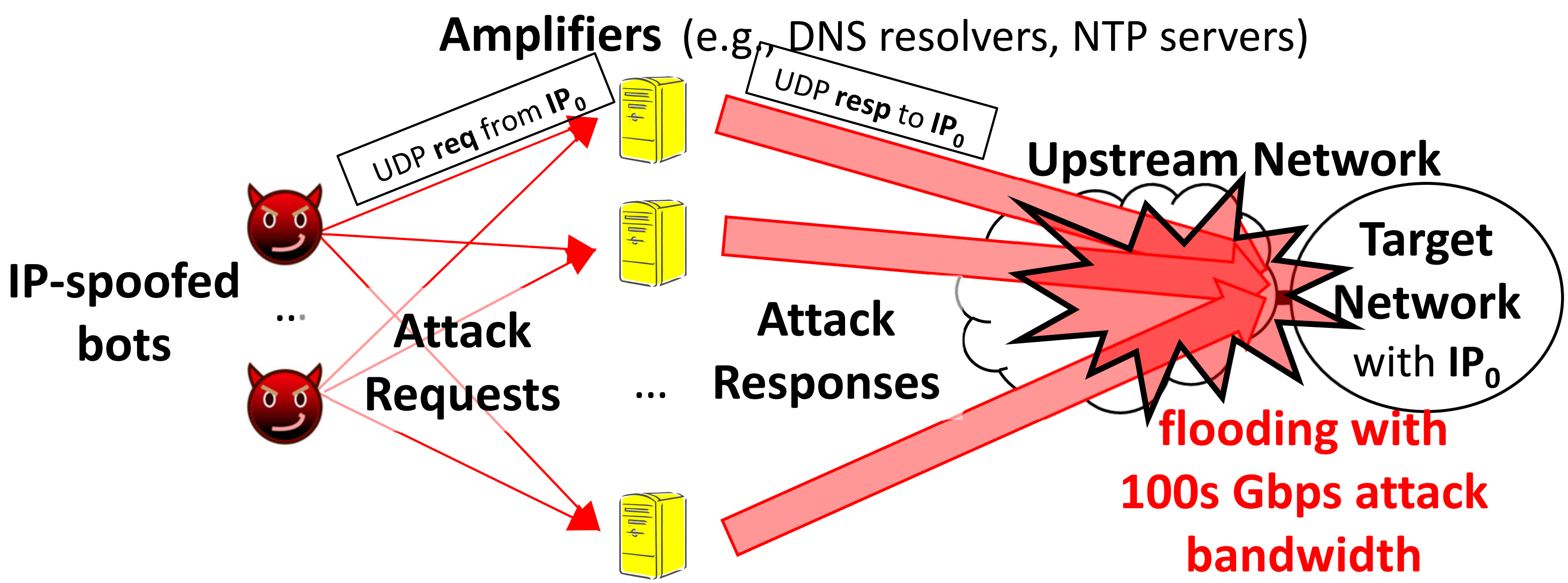
Economi
against F
after talk
end with

DoS attacks in the Internet



Amplification Attacks

- Amplification DDoS attacks



So popular!

- UDP-based DDoS accounts for 83% of all DDoS attacks.

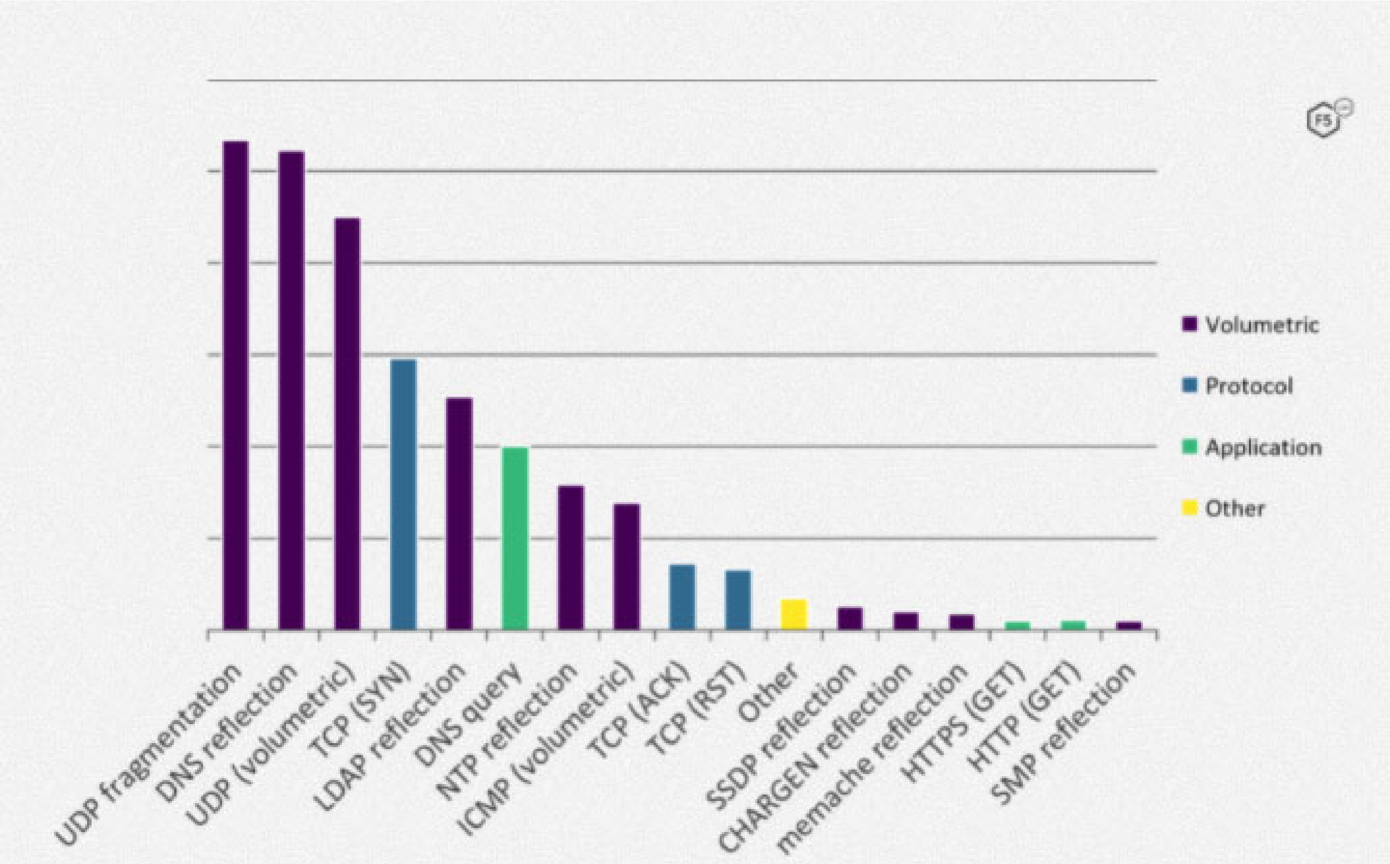
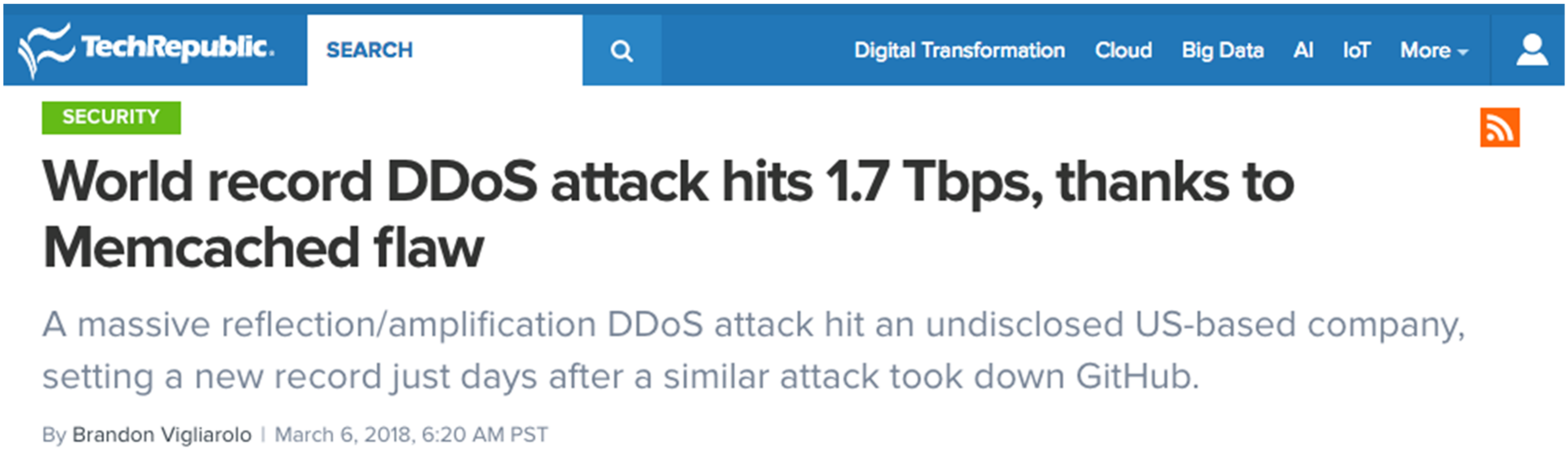


Figure 3. Frequency of different DDoS attack tactics, January 2020 through March 2021.

https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

Recent Amplification Attacks



TechRepublic. SEARCH Digital Transformation Cloud Big Data AI IoT More

SECURITY

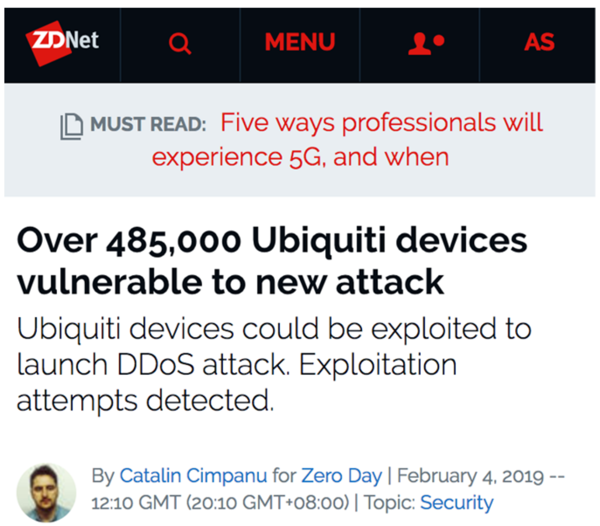
World record DDoS attack hits 1.7 Tbps, thanks to Memcached flaw

A massive reflection/amplification DDoS attack hit an undisclosed US-based company, setting a new record just days after a similar attack took down GitHub.

By Brandon Vigliarolo | March 6, 2018, 6:20 AM PST

How to mitigate amplification attacks?

- Prevent IP spoofing?
  - Not effective unless achieving 100% prevention
- Fixing (or removing) vulnerable amplifiers?
  - Distributed, owned by third parties, lack of incentives
- Blocking target protocol at destinations?
  - Potential collateral damage



ZDNet MENU AS

MUST READ: Five ways professionals will experience 5G, and when

Over 485,000 Ubiquiti devices vulnerable to new attack

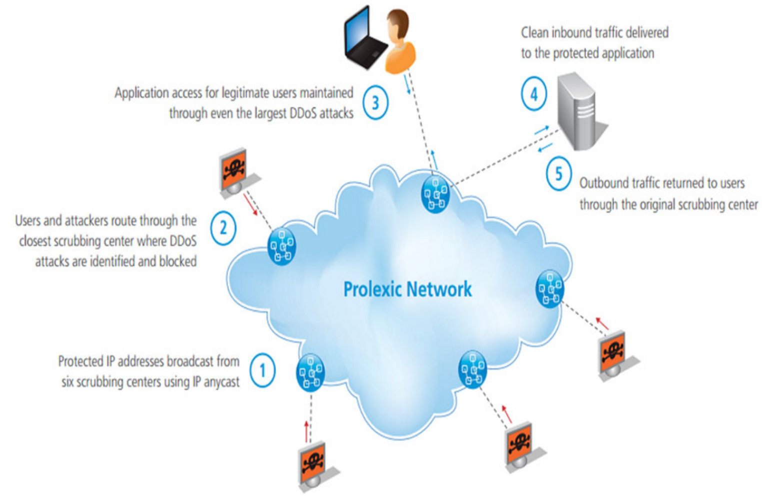
Ubiquiti devices could be exploited to launch DDoS attack. Exploitation attempts detected.

By Catalin Cimpanu for Zero Day | February 4, 2019 -- 12:10 GMT (20:10 GMT+08:00) | Topic: Security

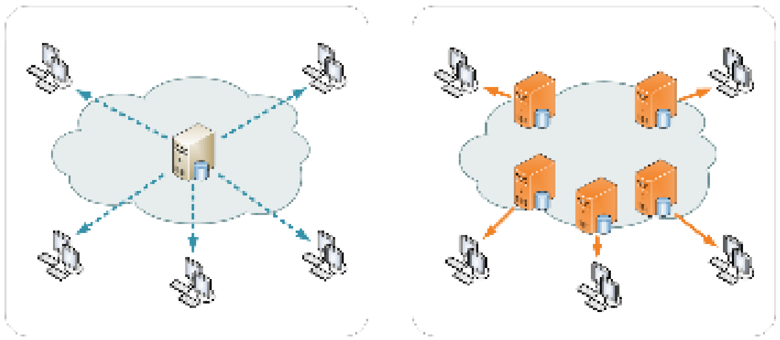
(Feb 2019)

DDoS defense

- **Two practical commercial solutions**:
  1. Cloud-based traffic scrubbing
  2. Content-distribution network (CDN)
  - Good enough?
    - Significant cost (market monopoly)
    - Cannot handle Crossfire-like attacks
    - Security issues (e.g., TLS keys, sensitive data distributed on replicas)
- **Collaborative defenses**
  - Size of an attack is often beyond the capacity of single ISP
  - IETF standard to construct a standard channel between ISPs
  - Challenge: ISPs are competitors



Traffic scrabbing example (by Akamai)



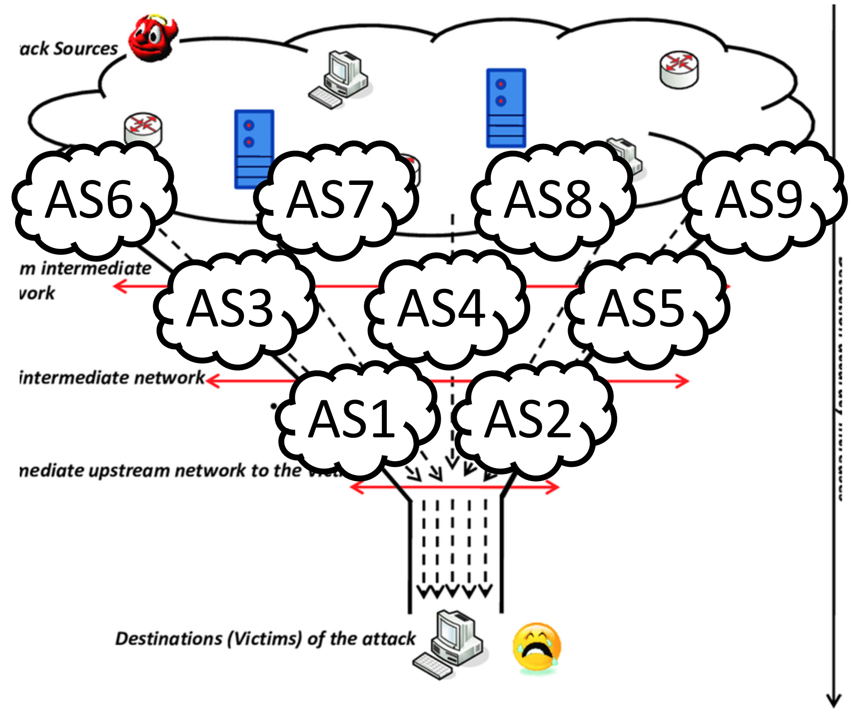
CDN Concept

A DDoS solution: ***empowering receivers to authorize flows***

SIFF (IEEE S&P 2004)

SIFF: Stateless Internet Flow Filter

- Fundamental problem: receiver has no control over who can send traffic to it
- We want to enable receiver to stop misbehaving senders
- Challenges:
  - Need per-flow state in network?
  - Where to filter?
  - Need trust relationship between ISPs?
  - Routers need to authenticate receiver requests to stop flows?



Overview of SIFF

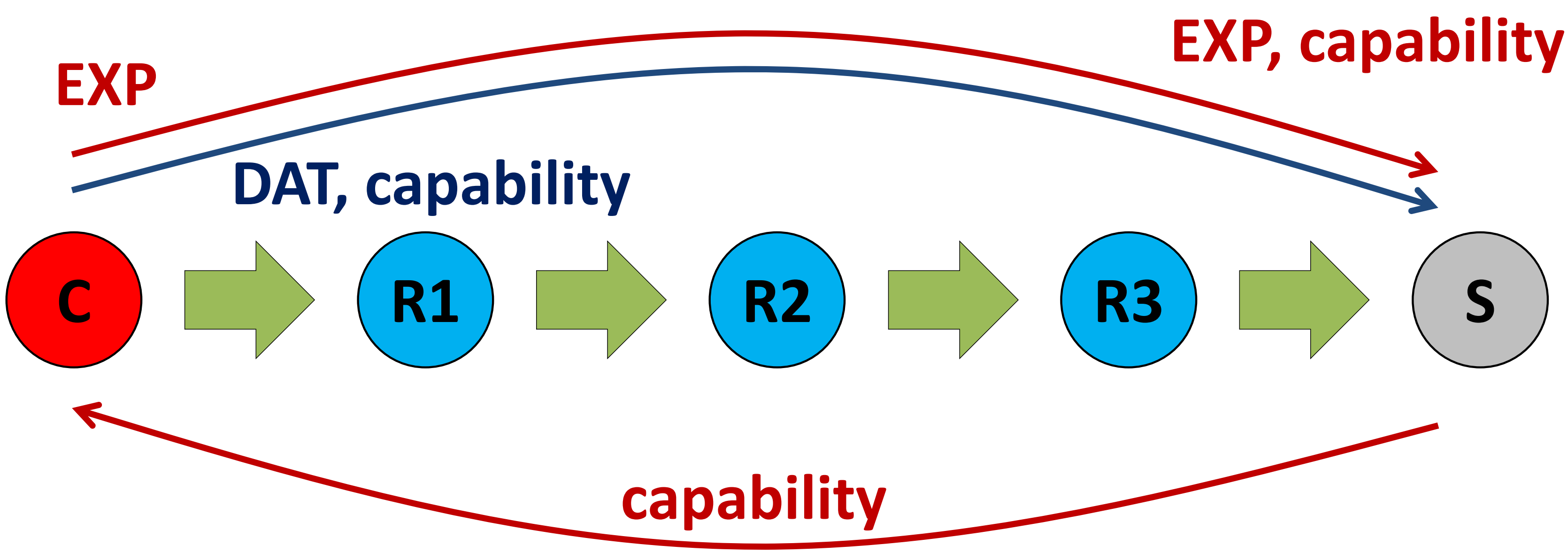
- Goal: enable ***receiver*** to ***control*** its incoming traffic
- Key ideas
  - ***Path fingerprints*** for traffic authorization
    - path fingerprint is used as a ***capability***
    - Only clients who know their path fingerprint get authorization
  - Authorized or "***privileged***" packets get priority over non-privileged packets
    - in bandwidth DoS, privileged packets are undisturbed by non-privileged packets

Overview of SIFF (cont'd)

- Create two Internet packet classes
  - ***Unprivileged*** (*best-effort*): Signaling and legacy traffic
  - ***Privileged***: Receiver controlled traffic flows
- Privileged packets given priority at routers
  - Privileged packets never dropped by unprivileged packet flooding
- Privileged packet flooding is impossible (with high probability)

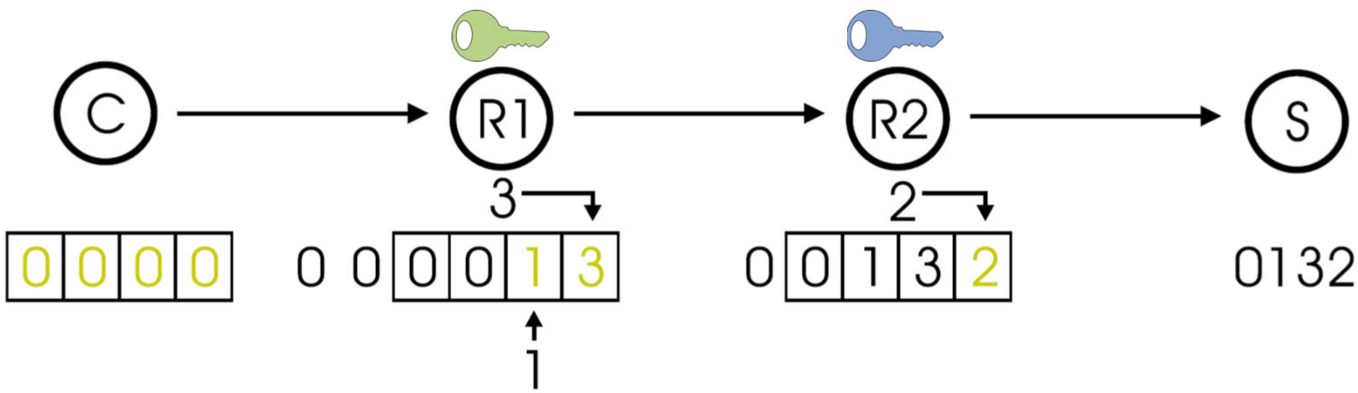
SIFF Handshake

1. Client C sends ***best-effort (i.e., unprivileged)*** packet to server S, arriving packet accumulates **capability**
2. If S wants to allow C to send privileged traffic, S sends capability back to C
3. C includes capability in packets to send at ***privileged*** level



SIFF Marking: ***Unprivileged*** Packets

EXP

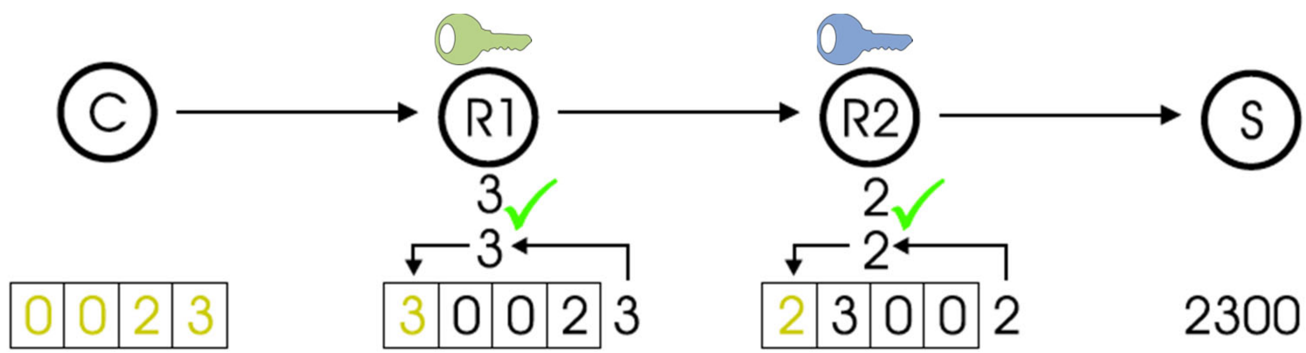


- SIFF routers ***mark*** unprivileged packets
- Marking should be ***unpredictable***
  - Hash with ***key*** known only to each router
- Markings unique to Sender/Receiver pair
  - Add source IP and destination IP to hash
- Hash calculation must be done in hardware for performance
- Server sends the ***capability*** back to client if it ***allows*** this flow

SIFF Marking: ***Privileged*** Packets

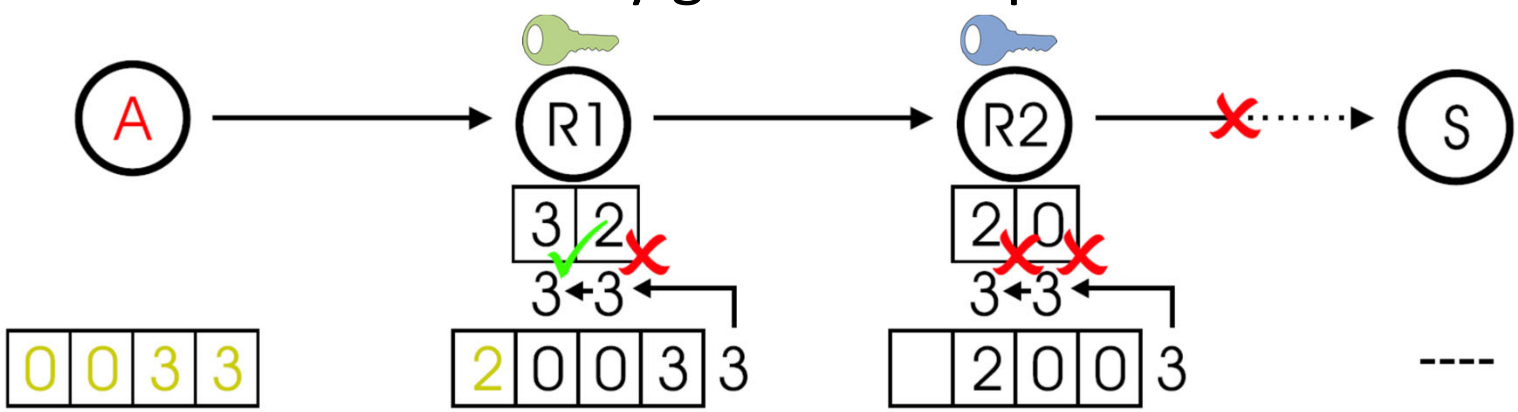
- SIFF routers ***verify*** marking in the header
  - Correct marking: router rotates it into the MSB
  - Incorrect marking: router drops packet
- Without receiver help, sender does not learn capability, cannot send privileged traffic
- IP Spoofing: capability does not reach attacker

DAT, capability



Problem: Static Privilege

- Once received, Sender can abuse capability
- Goal: Dynamic Privilege
  - Expire capabilities over time
- Solution: **Key switching**
  - Routers change keys periodically, but maintain x > 1 valid keys foreach time window
  - Receiver automatically gets new capabilities



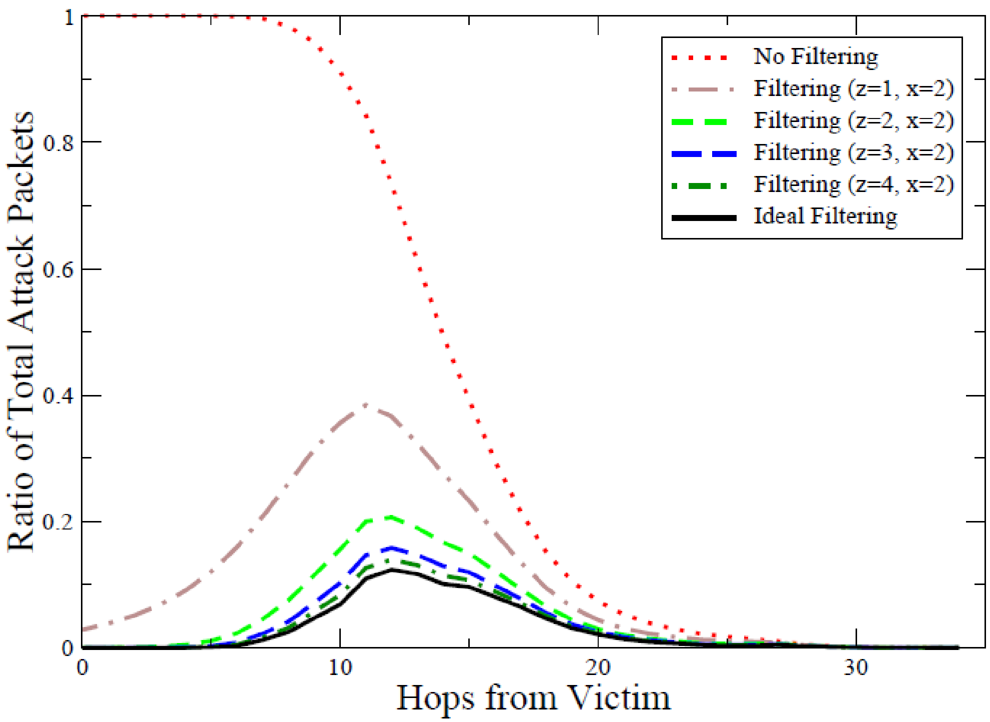
Receiver-controlled Flows

- As packet flow caries on, receiver receives updated markings
- If receiver wants to continue to enable sender to send privileged traffic, receiver sends updated marking as capability to sender
- If receiver wants to terminate malicious flow, receiver simply stops updating sender with new capability, and routers will soon stop the flow early in network

SIFF Performance

- DDoS: Attackers flood "***forged (guessed)***" privileged traffic
  - Probability of fooling a SIFF router:

    $P(x,z) = 1 - (1 - 1/2^z)^x$
  - Probability of fooling d SIFF routers: $P(x,z)^d$



- z = number of bits per router mark
- x = number of marks in router's window
- T_k = time between router key changes

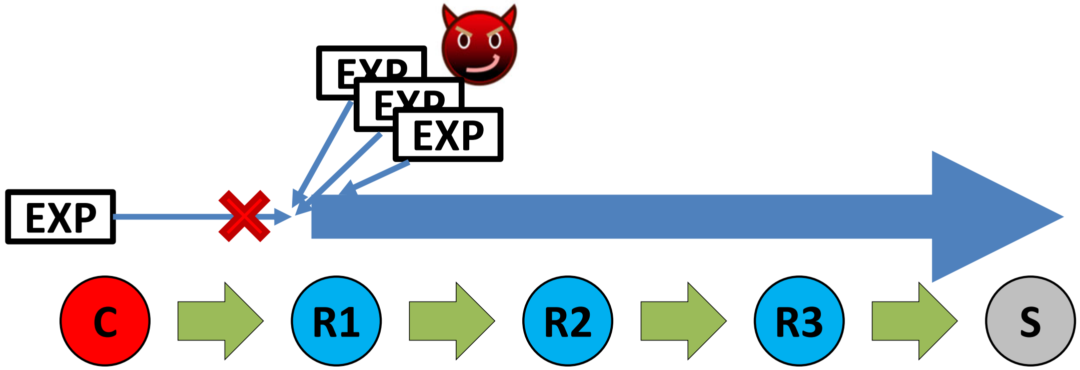
SIFF Summary

- DoS-less sender/receiver communication
  - ***Receivers*** can ***stop malicious flows***
  - ***1 unprivileged packet*** establishes ***privileged connection***
- Lightweight at routers (***stateless***)
  - Small constant state/processing per packet
- Incremental deployment/backward compatible
- ***No trust*** required between ISPs
- ***No authentication*** required at routers

Limitations of SIFF

- Not distinguish bad/good senders
  - E.g., An attacker could rotate machines for persistent attack
- Router upgrade is required.
  - Path that does not have SIFF router may become congested by attack.
- Collusion attack is still a risk.
  - If a malicious sender colludes with some intermediate router en route, the router could (partly) help the sender forge capability.
- Only granularity of host, not service
- Flooding the EXP packets? (a.k.a. ***Denial-of-Capability attack***)

Solutions to Denial-of-Capability attacks?

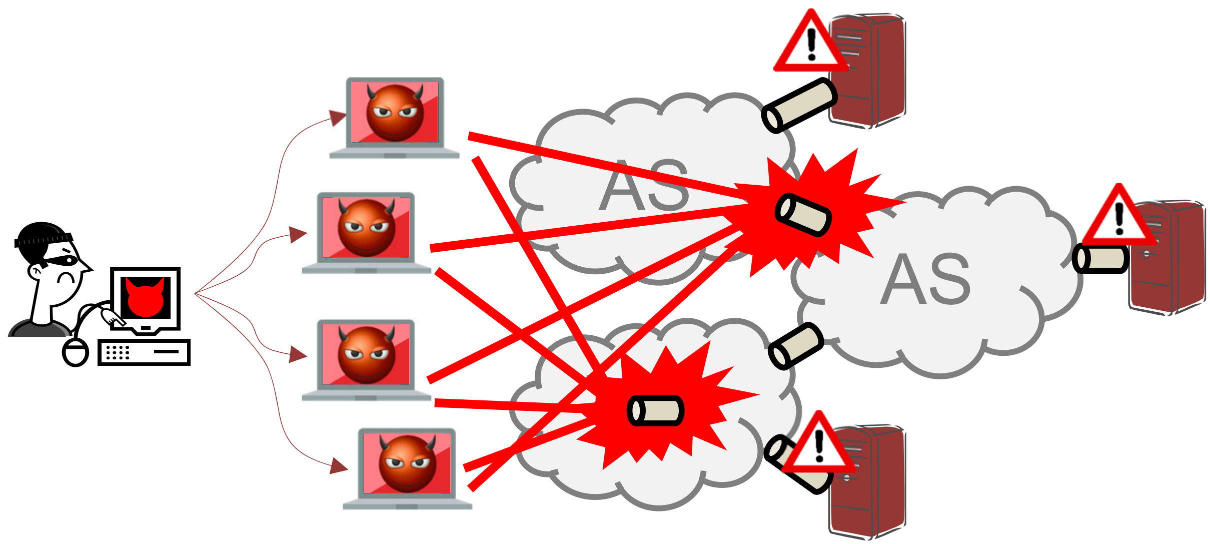


- Desired property: ***fairness*** among senders
  - Each client has similar chance to send EXP packets to servers
  - But how to achieve fairness?
    - Source IP address?

- Portcullis (2007): ***Proof-of-work*** scheme for fairness of EXPs
  - Introduce **"puzzle"** to solve before sender sends packets

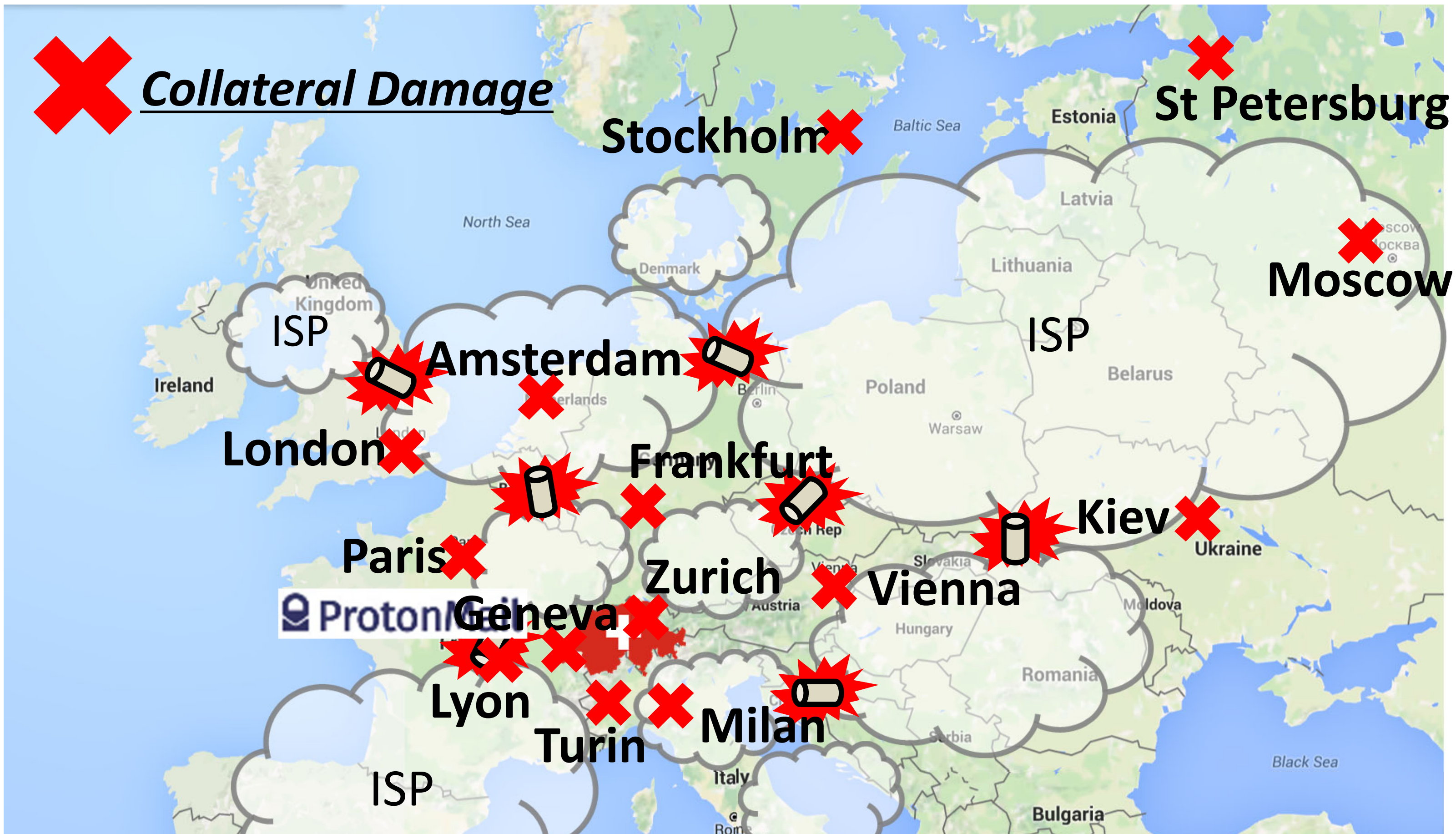
Non-traditional DDoS attacks

Non-traditional attacks:



- ***Link-flooding***: flood ***network links*** in the ***core*** of the Internet (e.g., Tier-1 or Tier-2 ISPs) to degrade the communication of end-point servers
- ***Indirect***: the ***locus*** of the attack (i.e., flooded links) is ***different*** from the ***ultimate targets***; e.g., end-point servers
- ***Academic studies***: link cuts [Bellovin’03], link-flooding [Studer’09]
- ***Real-world* instances:** Spamhaus (2013), ProtonMail (2015)

ProtonMail DDoS attack (Nov. 3 - 10, 2015)



Extremely long recovery process (1 week)

- ✓ ***Indirect*** attack => ISP ***collaboration, manual*** operations
- ✓ ***Adaptive*** adversary – in real-time

The *Crossfire* Attack

*A **link-flooding attack** that degrades/cuts off network connections of **scalable N-server** area **persistently***

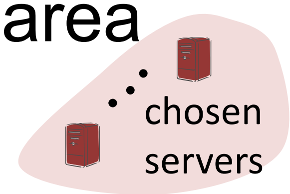
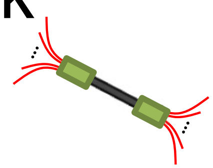
- **Scalable N-Server areas**

  - **N** = small (e.g., 1 -1000 servers), medium (e.g., all servers in a US state), large (e.g., the West Coast of the US)

- **Persistent**:

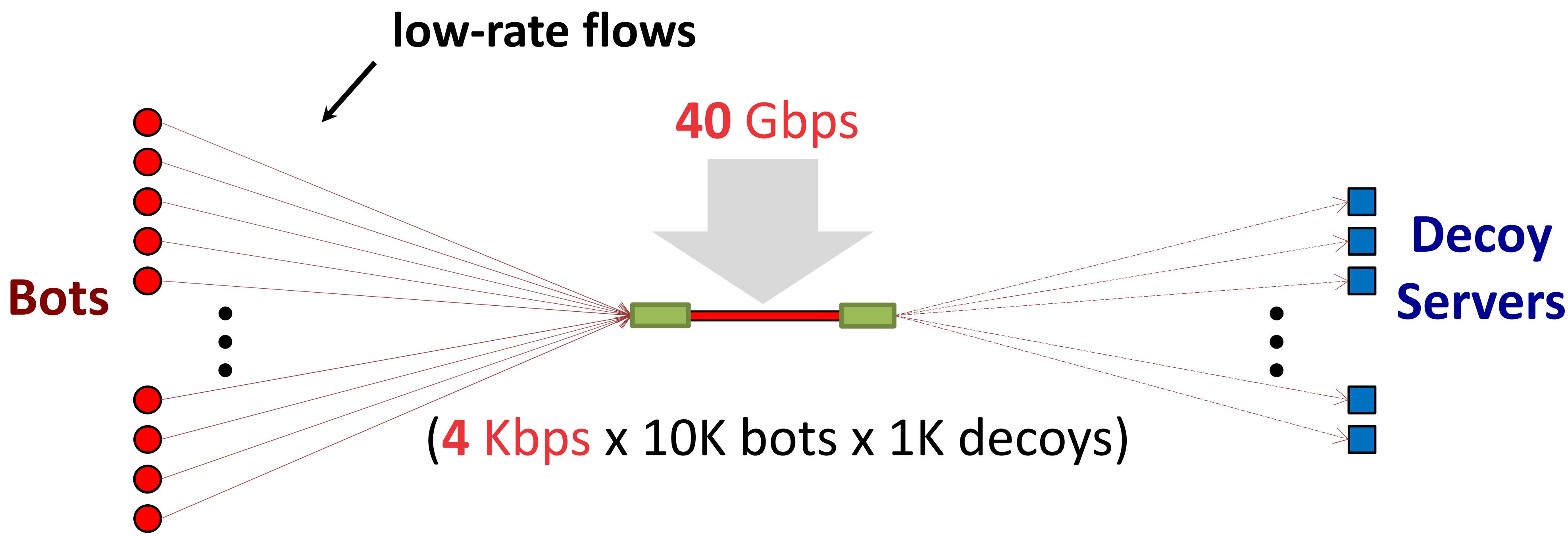
  - attack traffic is **indistinguishable from legitimate**
    - low-rate, changing sets of flows
  - attack is "**moving target" for same N-server area**
    - changes target links before triggering alarms

Definitions

• Target area 	Area containing chosen target servers e.g., an organization, a city, a state, or a country
• Target link 	Network link selected for flooding
• Decoy server 	Publicly accessible servers surrounding the target area

1-Link Crossfire

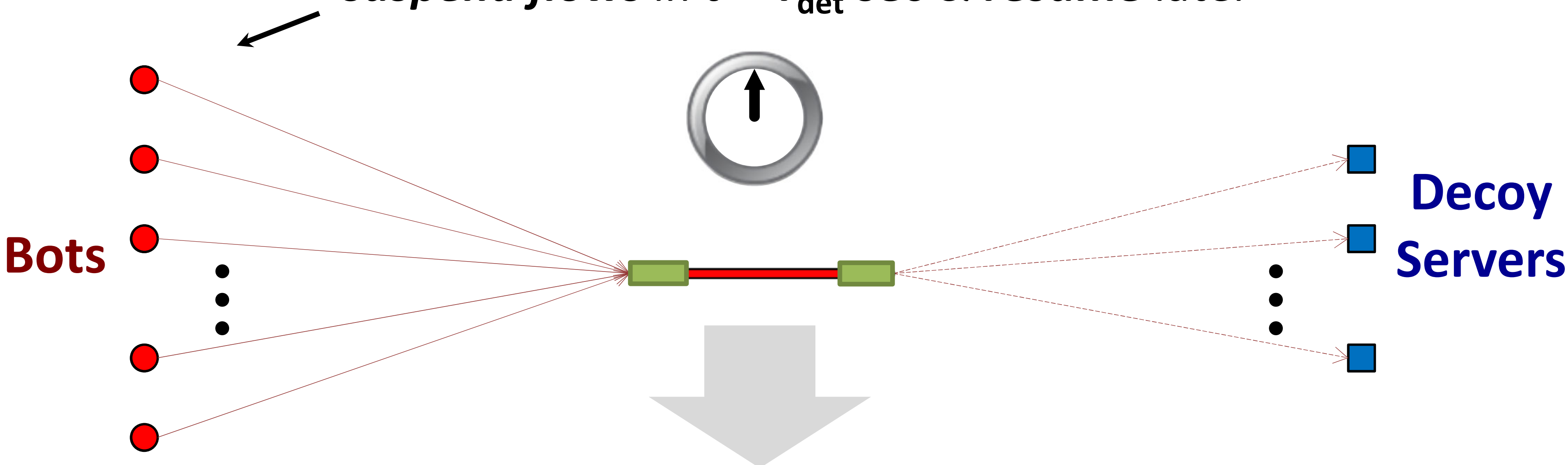
Attack Flows => Indistinguishable from Legitimate



1-Link Crossfire

Attack Flows => Alarms Not Triggered

suspend flows *in* ***t*** **< T$_{det}$ sec** & **resume** later



link-failure detection latency, T$_{det}$

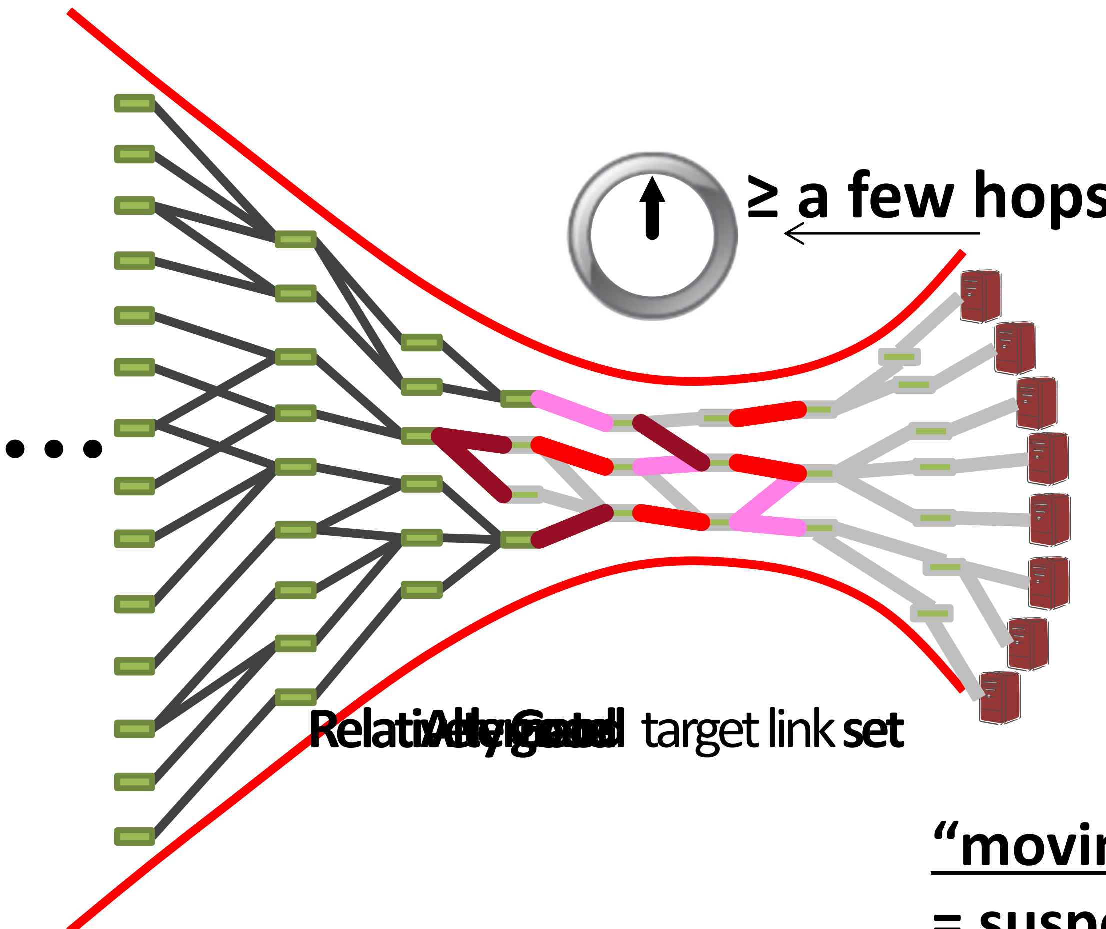
IGP routers: **217 sec**/80 Gbps – **608 sec**/60 Gbps

BGP routers: **1,076 sec**/80Gbps – **11,119 sec**/60 Gbps

t **= 40 – 180 sec => Alarms are Not Triggered**

n-Link Crossfire

- ***n* links traversed by a large number of persistent paths to a target area.**



<u>small *n*</u>; e.g., 5 - 15
"Narrow Path Waist"
(observed power law
for Internet route paths)

N servers

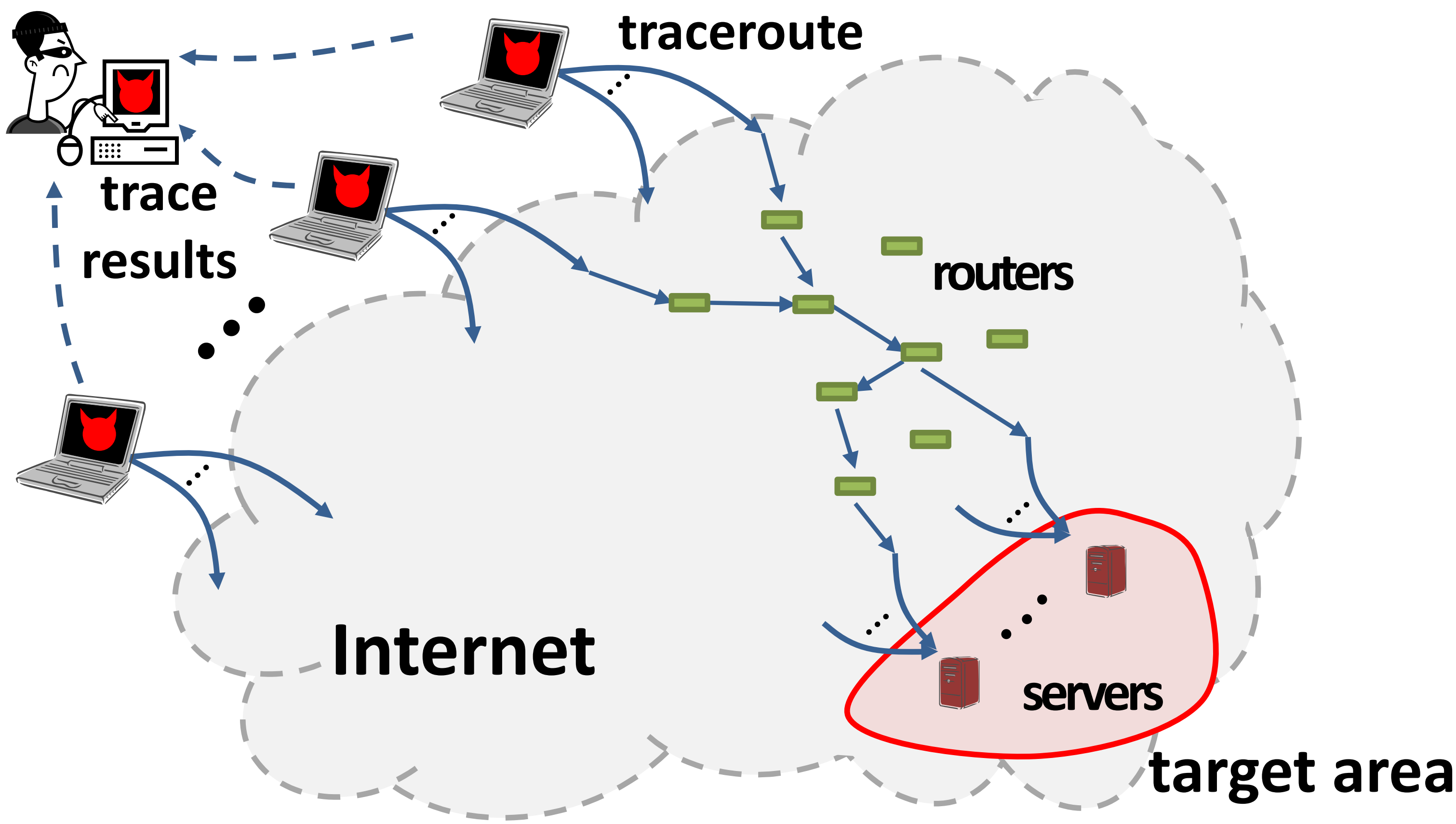
<u>"moving targets,"</u> same N servers
= suspend-resume *flooding of*
***different* link sets**

Experiments
Geographical Distribution of Traceroute Nodes

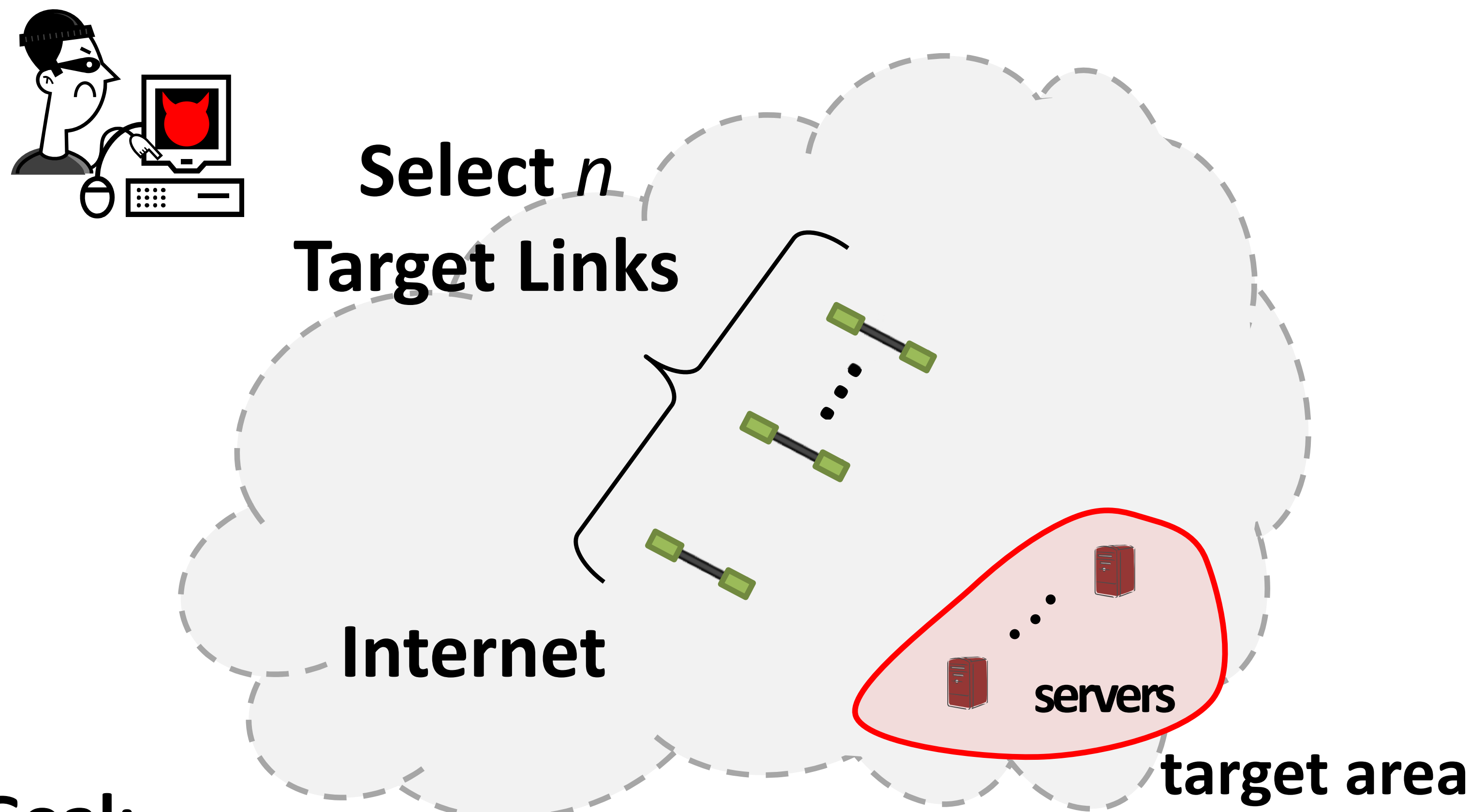
- 1,072 traceroute nodes
  - 620 PlanetLab nodes + 452 Looking Glass servers

PlanetLab node   Looking Glass server

ATTACK STEP 1: RECONNAISSANCE



ATTACK STEP 2: TARGET-LINK SELECTION

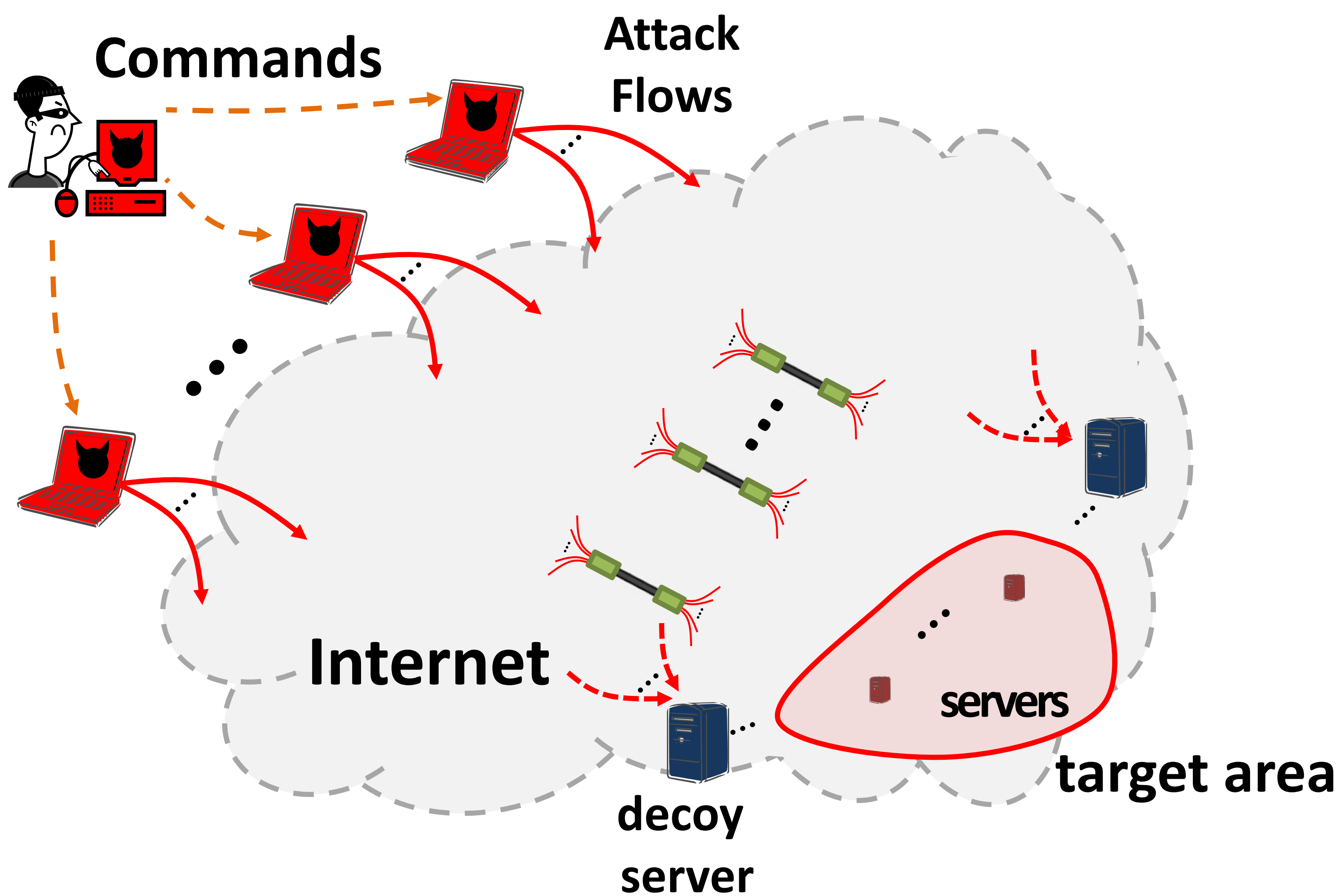


Goal:

Find *n* links whose congestion maximizes connectivity *damage*

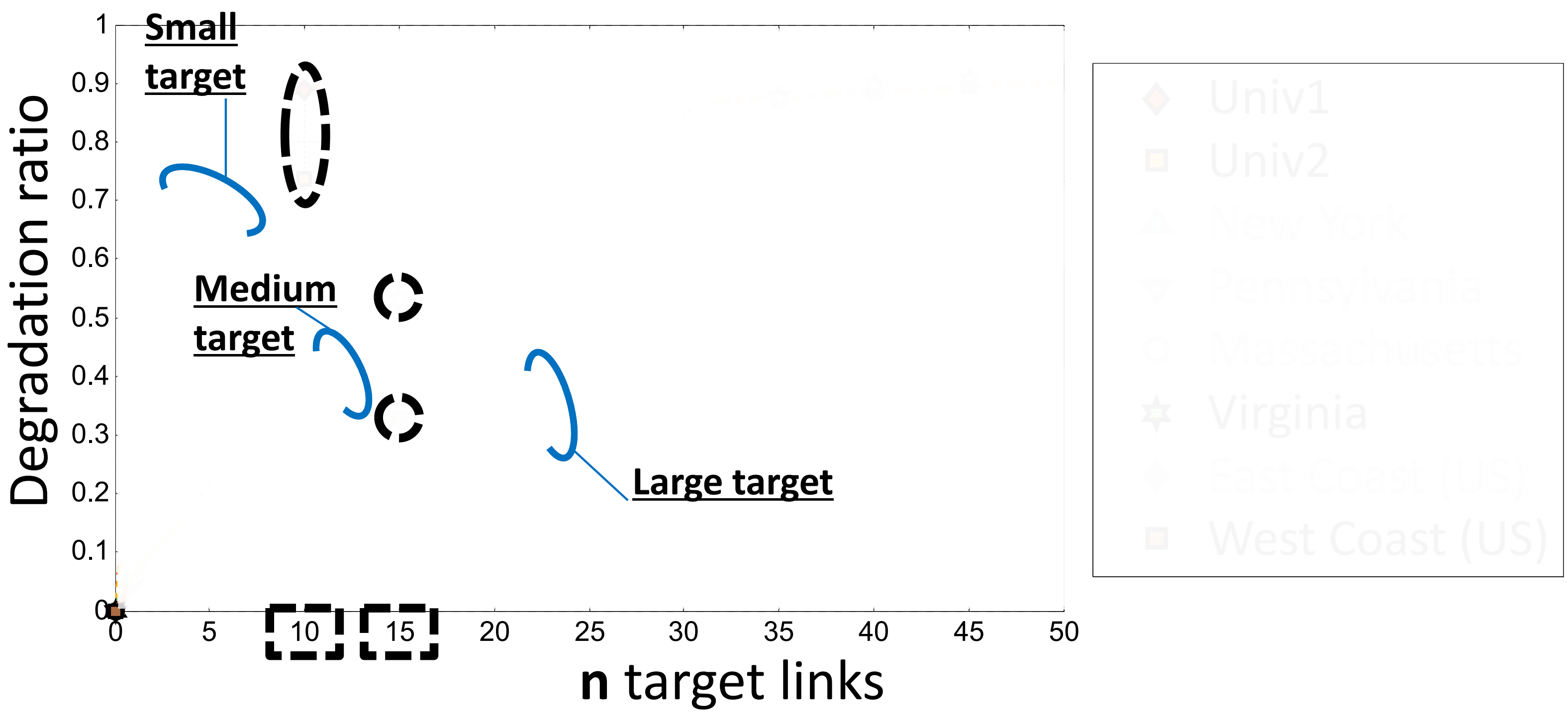
=> maximum coverage problem

ATTACK STEP 3: FLOODING



Degraded Connectivity

* **Degradation Ratio (target link set) =** $\frac{\text{\# \textit{degraded} bot-to-target area \textbf{paths}}}{\text{\# \textit{all} bot-to-target area \textbf{paths}}}$

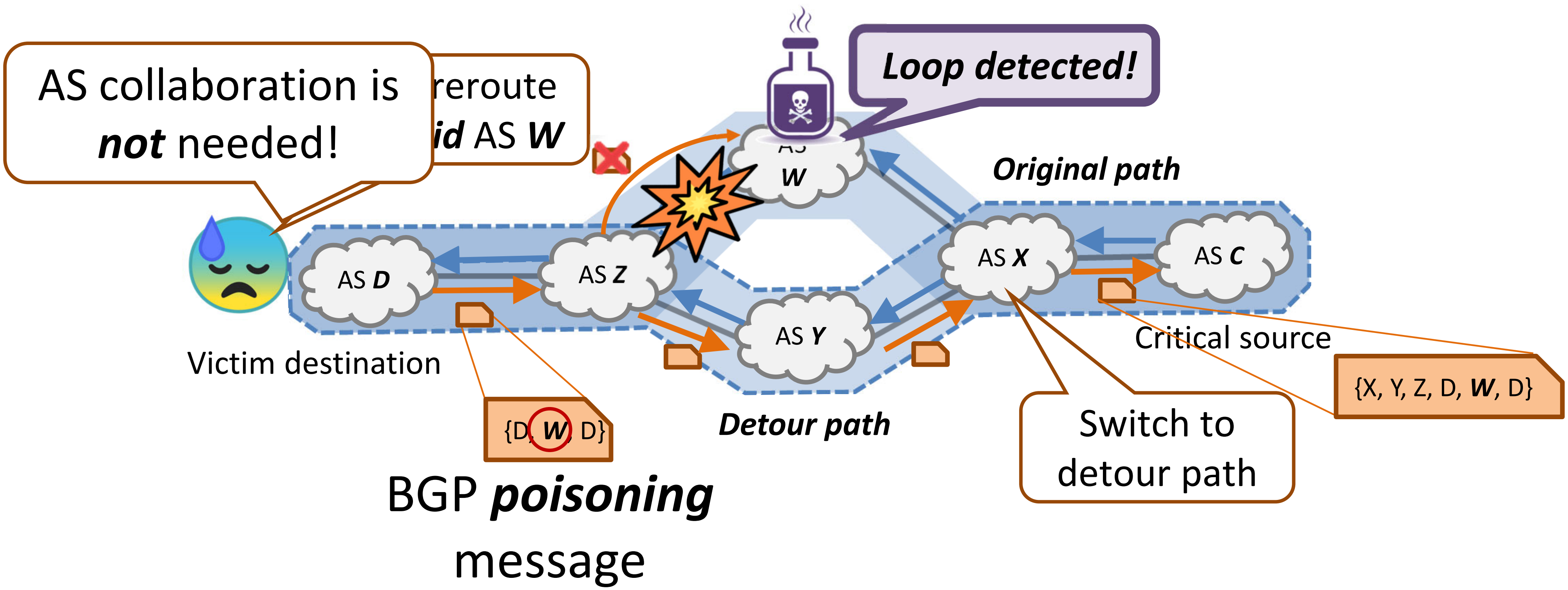


- Flooding *a few* target links causes *high* degradation (DR*)
  - 10 links => DR: 74 – 90% for Univ1 and Univ2
  - 15 links => DR: 53% (33%) for Virginia (West Coast)

How to mitigate Crossfire?

- Remove chock points?
  – Known to be the inherent problem of Internet routing
- Rerouting?
  – e.g., Can a destination network create on-demand detours to avoid the congested links?
  – Routing Around Congestion (RAC) [IEEE S&P 2018]

Routing Around Congestion (RAC): Rerouting using BGP poisoning [Smith *et al.*, S&P '18]



Not sufficient against adaptive attackers, who detects a detour and adjust attacks

Summary

- **DoS problem**
  - Attacks are so prevalent; they don't make news anymore (unless record breaking new attacks!)
- **Amplification attack**
  - Plenty of vulnerable services that amplify attack traffic

- **SIFF**
  - Receiver has no control over who can send traffic to it
- **Crossfire: DDoS attack against Internet core**
  - It is possible to flood network links in the Internet core
  - Significant damage by careful selection of link targets
  - Still largely an open problem!

Questions?

Next week:
Anonymous Communication

Paper to read

- “**Tor: The Second-Generation Onion Router.**” (USENIX Security 2004)