Bridging Missing Gaps in Evaluating DDoS Research

Lumin Shi, Samuel Mergendahl, Devkishen Sisodia, Jun Li

{luminshi, smergend, dsisodia, lijun}@cs.uoregon.edu

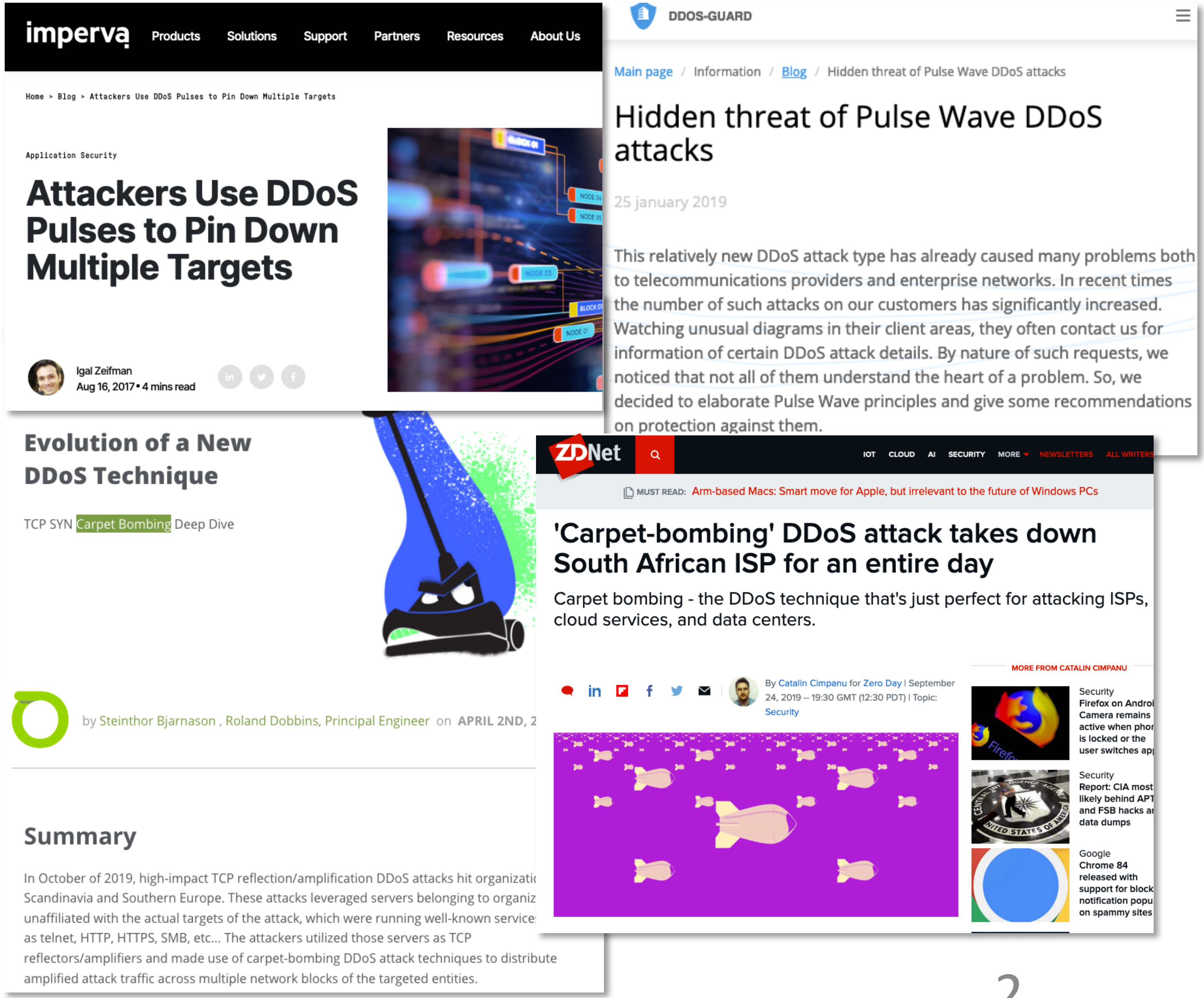
University of Oregon

Preliminary Work Paper
(Short Paper)

DDoS Attacks Today

Real-World Attacks Are Advancing

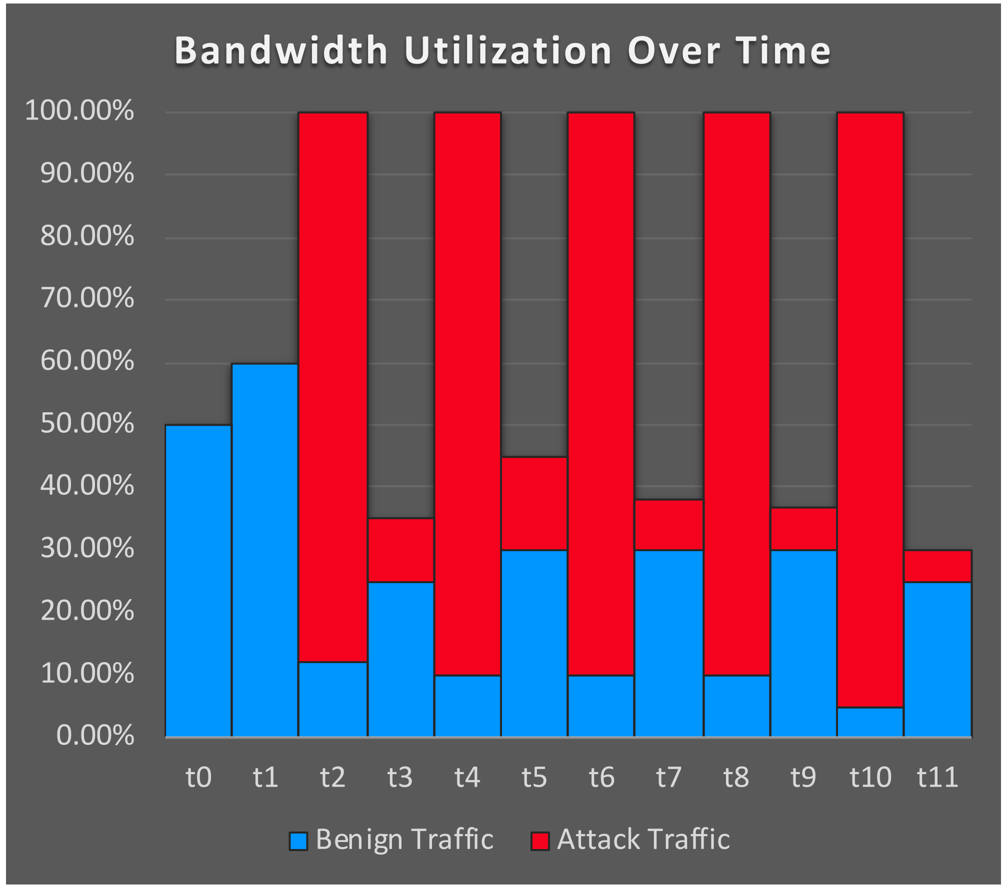
- Most DDoS attacks have common patterns of the attack traffic [1]
  - E.g., NTP amplification
  - Detection and mitigation are relatively easy
- Attacks have started to employ advanced attack techniques:
  - Pulsing-based attacks [2,3]
  - Carpet-bombing attacks [4,5]



1. https://www.netscout.com/report/
2. https://www.imperva.com/blog/pulse-wave-ddos-pins-down-multiple-targets/
3. https://ddos-guard.net/en/info/blog-detail/hidden-threat-of-pulse-wave-ddos-attacks
4. https://www.netscout.com/blog/asert/evolution-new-ddos-technique
5. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

Background: Pulsing-Based Attack

- **Pulsing-based** attacks inundate network links with short and periodic traffic bursts
  - **Detection difficulty**:
    - Requires fine-grained time-series network information
    - Difficult if not impossible otherwise
      - E.g., NetFlow
  - **Possible consequences**:
    - Reduced quality of real-time applications, e.g., online gaming
    - Reduced network throughput of benign congestion-responsive flows [1]
    - Theoretically possible to attack more networks with a limited number of bots

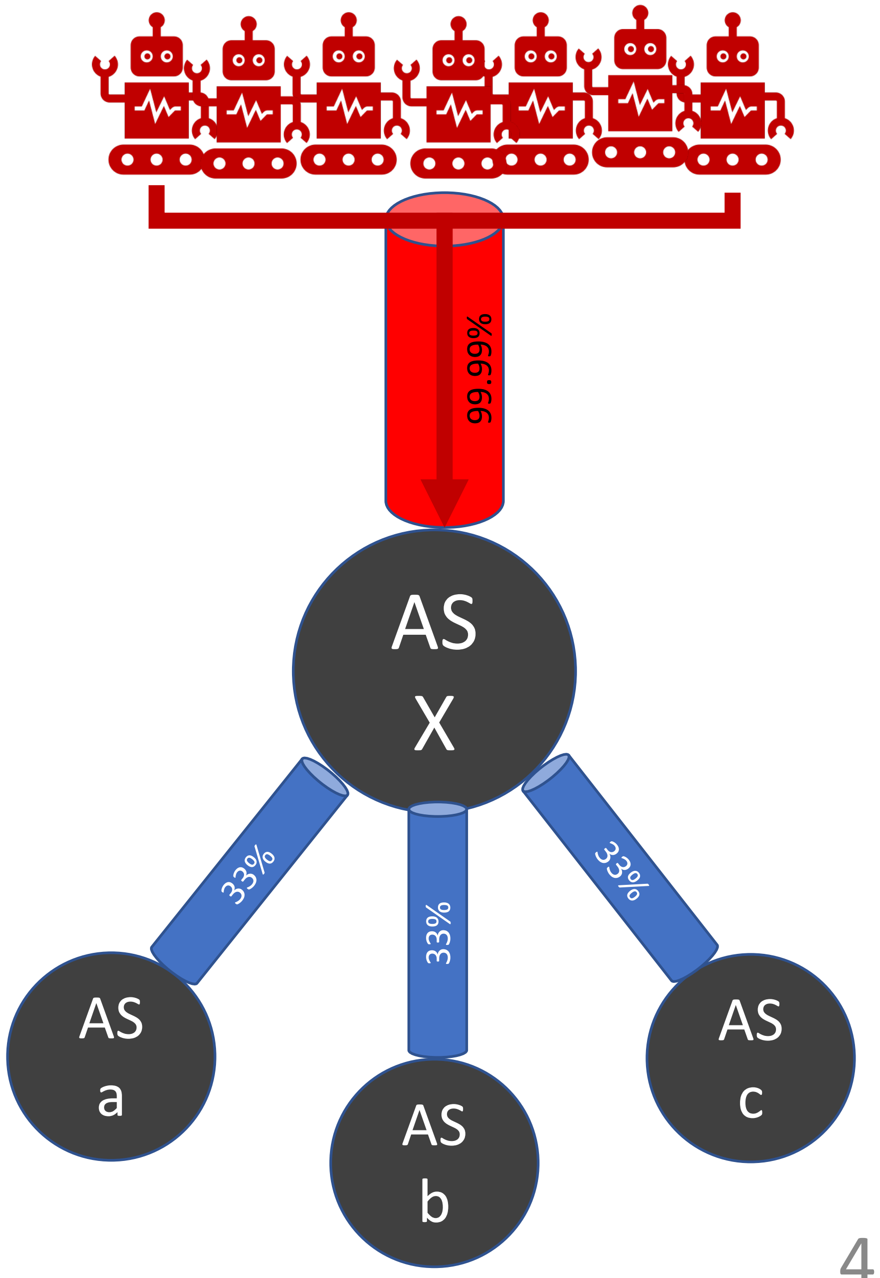


Possible link bandwidth utilization of a pulsing-based attack

1. CICADAS, AsiaCCS, 2016

Background: Carpet-Bombing Attack

- **Carpet-bombing** attacks address multiple networks/hosts of a network.
  - **Detection difficulty**:
    - **Traffic payload**: TCP SYN attacks or the CrossFire scheme [1]
    - **Point of view**: at transit networks or edge networks
  - **Possible consequences**:
    - Edge networks not knowing (why) the bandwidth degradation.
    - Blind attack mitigation performed by upstream networks (e.g., AS X).

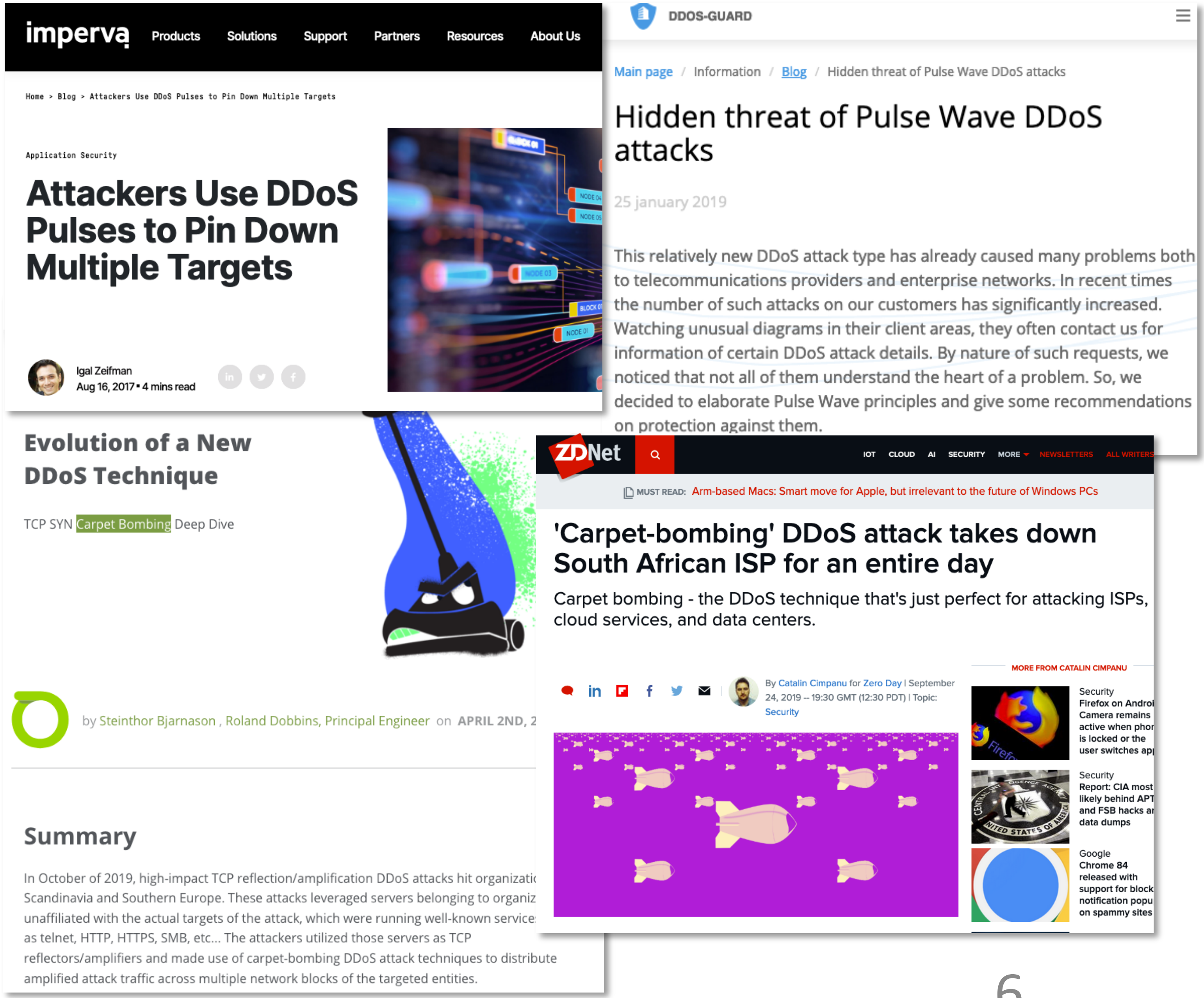


1. The CrossFire Attack, IEEE Symposium on Security and Privacy, 2013

Missing Gaps

We Know Little About Advanced Attacks

- Only a matter of time before more attacks with advanced attack techniques
- We need to know more about these advanced attacks in action
- Study them in a network with realistic background traffic



Better DDoS Detection Evaluation

- A DDoS detection system facilitates better attack mitigation
- To better evaluate the efficacy of a detection system
  - Should not only evaluate it using passive network traces
  - It must handle abrupt network changes caused by the mitigation effort
    - E.g., will it label a benign flow that is occupying more bandwidth as an attack flow?
- Must evaluate detection systems with realistic background traffic and mitigation systems

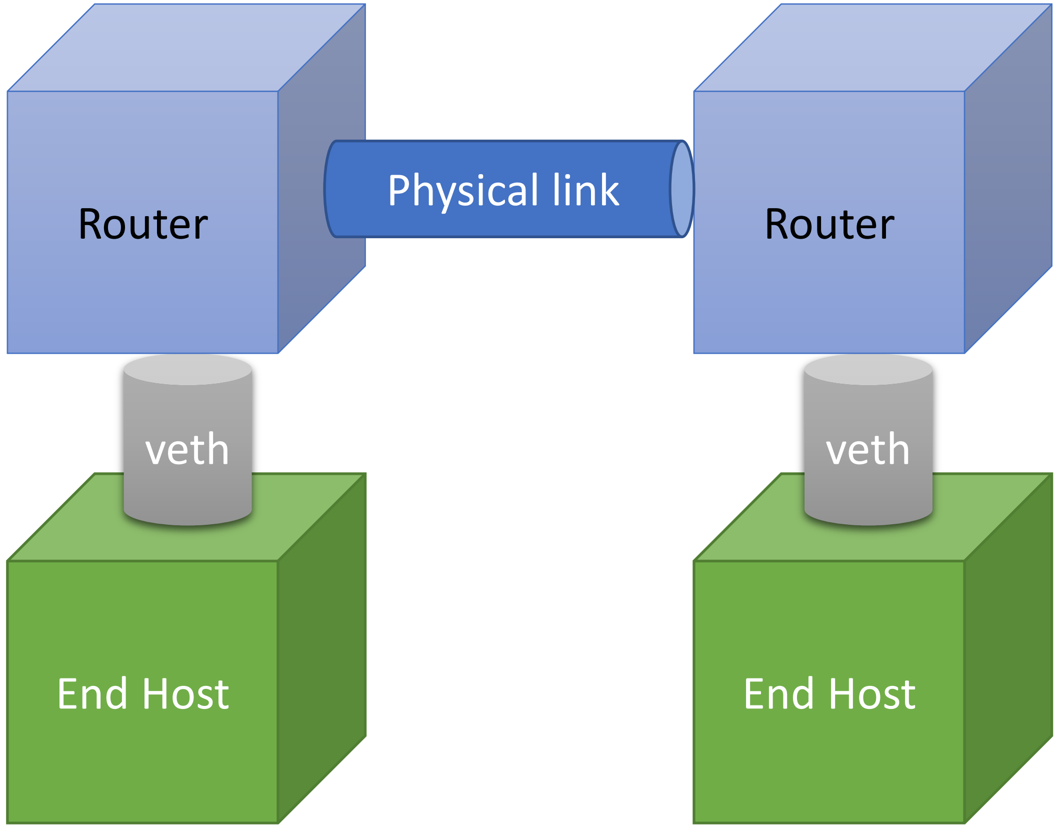
Collateral Damage in Mitigation

- DDoS victims (un)knowingly disconnect benign connections during attack mitigation
  - E.g., remotely triggered block hole (RTBH)
  - Destination-prefix-based traffic filtering
- Networks starting to adapt fine-grained mitigation solutions
  - E.g., BGP Flowspec can match/filter traffic using 5-tuple packet fields
- Limited traffic filtering capacity
  - Broad matching criteria to mitigate the attack at the cost of filtering some benign hosts
    - E.g., a Flowspec filter that blocks traffic from one /24 network to another network
- We need realistic IP assignment in DDoS mitigation evaluation

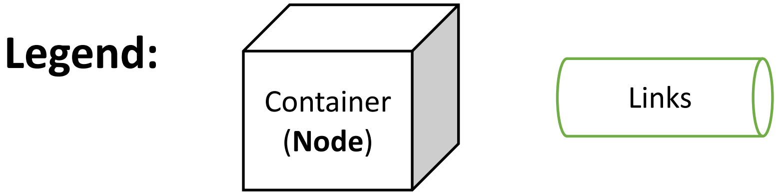
DDoS SandBox

DDoS SandBox -- Overview

- A container-based system
  - Low experiment deployment friction
    - Portable experiment node images
  - Elastic emulation fidelity
    - Distribute containers across multiple machines
  - Nodes are realized by containers
  - Physical/virtual links management

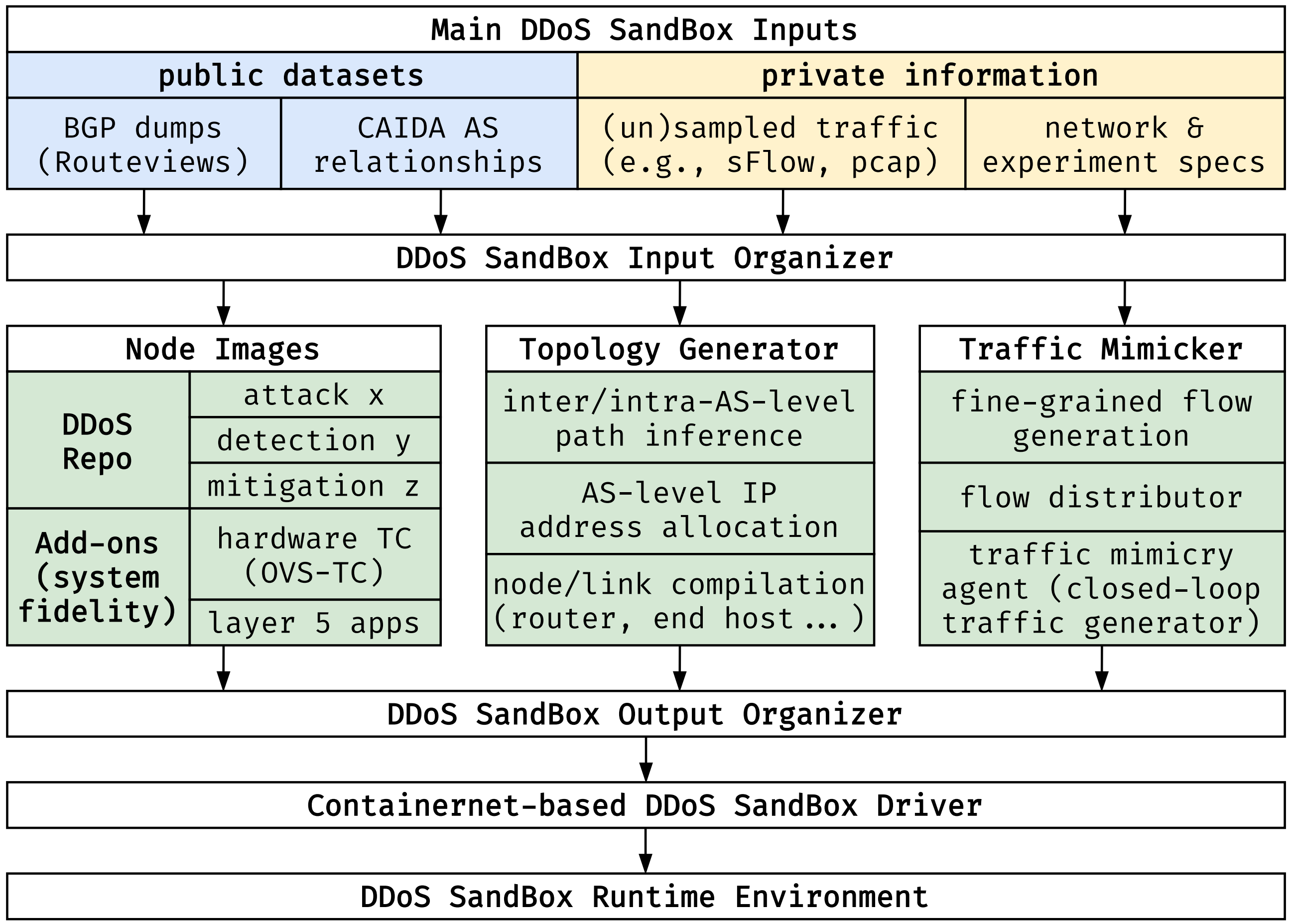


An example topology in DDoS SandBox

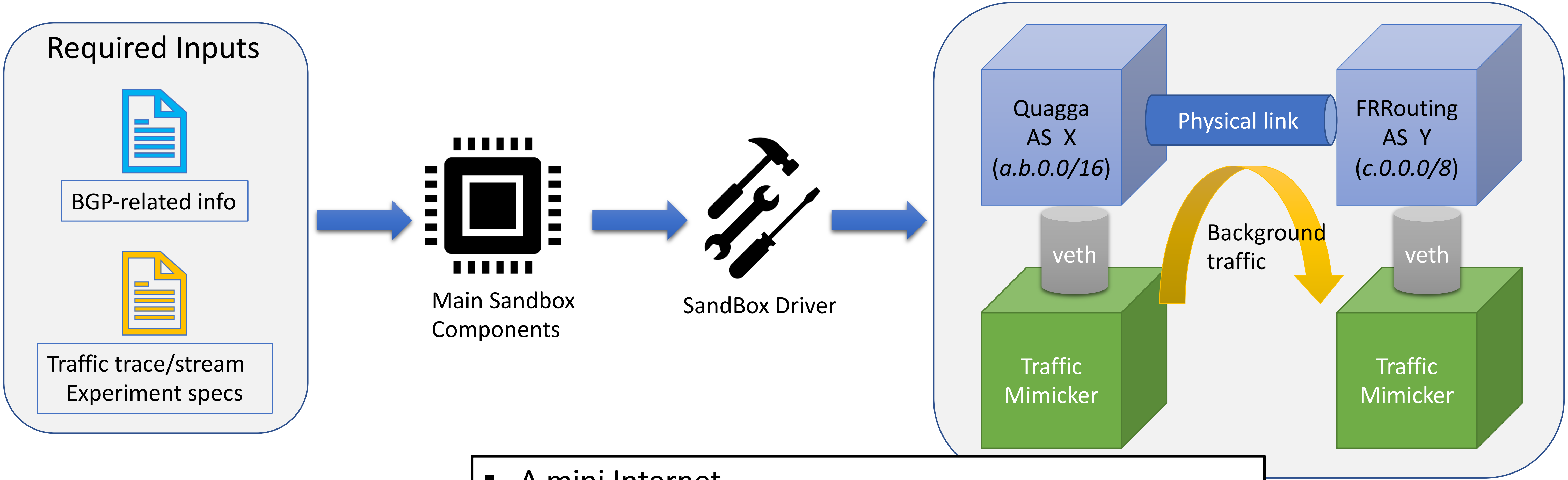


DDoS SandBox -- System Components

- **Inputs**:
  - Usage model is simple/flexible
  - Public and private datasets to create network topology
- **Topology generator**
  - Inter/intra-AS topology
  - IP allocation
- **Traffic mimicker**
  - Reads traffic trace/stream and generates fine-grained time-series flows
  - Create flows using system sockets
- **Node images**
  - E.g., routers, end hosts
- **SandBox Driver**
  - Implement nodes and links.



DDoS SandBox -- An Example Workflow



- A mini Internet
  - Arbitrary node implementation (flexibility)
    - E.g., Quagga, FRRouting
  - Realistic AS-level IP assignment
  - Congestion-aware (closed-loop) background traffic

Preliminary Evaluation -- Setup

- We evaluate our proof-of-concept (PoC) from two aspects:
  - The correctness of topology generation
  - The scalability of network instantiation time
- Two machines:
  - 3-core virtual machine, 24 GB of main memory
  - 96-core machine, 192 GB of main memory (AWS EC2 C5d)
- Software environment:
  - Ubuntu 18.04 with Docker 19.03 and Containernet

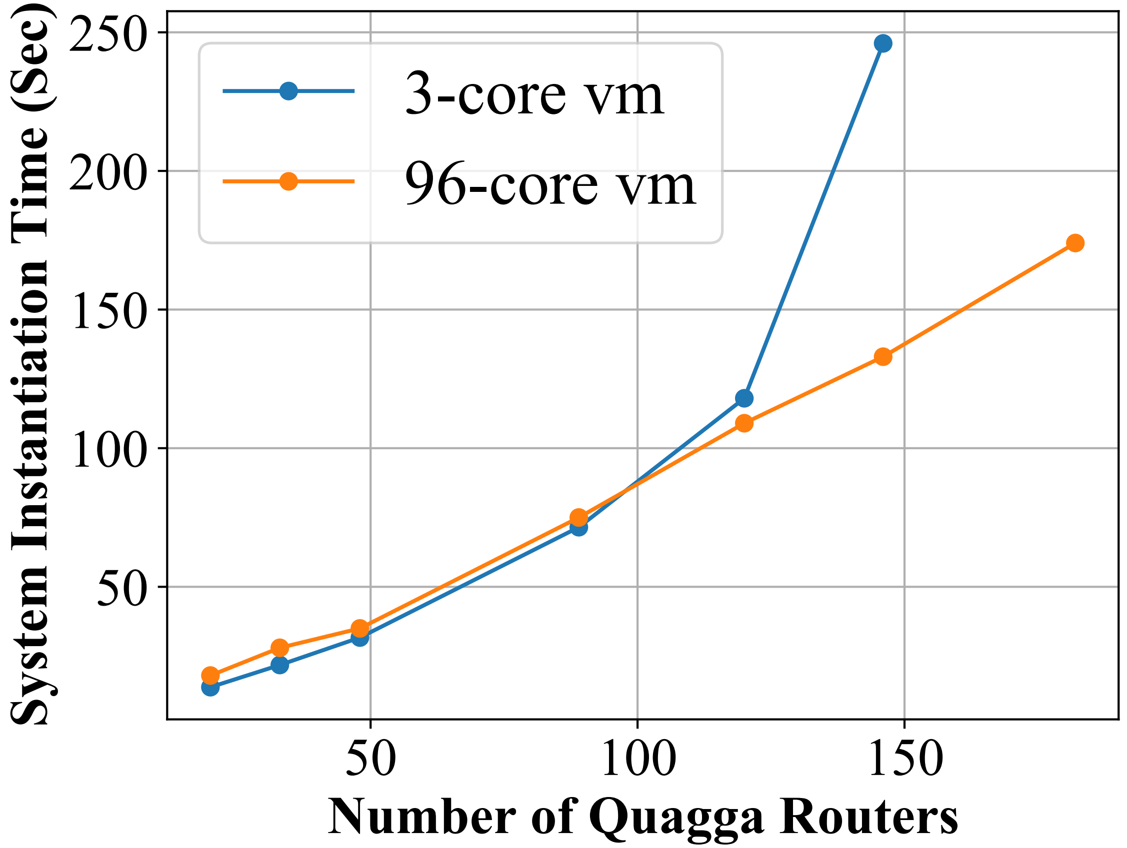
Preliminary Evaluation -- Correctness

```
root@a12145h0:/# traceroute 3.13.0.2
traceroute to 3.13.0.2 (3.13.0.2), 30 hops max, 60 byte packets
 1  129.82.0.1 (129.82.0.1)  0.457 ms  0.426 ms  0.417 ms
 2  129.82.255.255 (129.82.255.255)  0.416 ms  0.410 ms  0.406 ms
 3  129.19.255.251 (129.19.255.251)  0.489 ms  0.357 ms  0.371 ms
 4  64.57.31.245 (64.57.31.245)  0.377 ms  0.379 ms  0.381 ms
 5  3.13.0.2 (3.13.0.2)  0.570 ms  0.568 ms  0.565 ms
```

- An example traceroute result from an educational network to a cloud provider
- We can find a corresponding AS-level path on *bgpview.io*

Preliminary Evaluation -- Scalability

- The relationship of ***system instantiation time*** and ***number of Quagga routers***
- The 3-core machine w/ 24GB memory can support about 100 routers



Current and Future Work

- Integrating Traffic Mimicker into the SandBox
  - Many challenges that we did not cover in the short paper
- Implementing a set of well-received DDoS attack and defense projects
- Allow the SandBox to distribute container nodes across a cluster of machines for higher scalability
- Consider solutions with better support and compatibility as the SandBox driver
  - E.g., Container Network Interface (CNI) projects are quite promising for managing network interfaces

Conclusion

- A list of evaluation missing gaps in DDoS research
- A container-based emulation system that creates a mini Internet
- A repository of DDoS attack and defense implementations
- Much work ahead ☺

Thank You!

- We appreciate the useful comments from our paper reviewers
- We would love to hear your feedback
- You can reach us via any of the email addresses below:
  - *{luminshi, smergend, dsisodia, lijun}@cs.uoregon.edu*