To Know the Road Ahead: A Forward-Looking Analysis of Lessons to Learn from IP DDoS

Joint work:

Zhiyi Zhang (UCLA); R. Can Aygun (UCLA); Guorui Xiao (UCLA); Sichen Song (UCLA); Eric Osterweil (George Mason University); Angelos Stavrou (Virginia Tech); Lixia Zhang (UCLA)

Distributed Denial of Service (DDoS) attacks are perennial, but are they inevitable?

- DDoS is, perhaps, one of the oldest sicknesses that still plagues the Internet today
- First widely recorded DDoS over 21 years ago
  - Trin00
- 2015: new programs prepared for 1TB attacks *one day* (e.g., DHS' 2015 DDoSD program)…
- In 2016, krebsonsecurity.com gets slammed with over >665Gbps attack
- Later in 2016, IoT CCT cameras leveraged to slam OVH with 1.1Tbps attack
- Then in 2016, Dyn gets knocked over by 1.2Tbps attack from Mirai botnet (IoT devices)
- And the volumes and availability of attack-tools have only grown

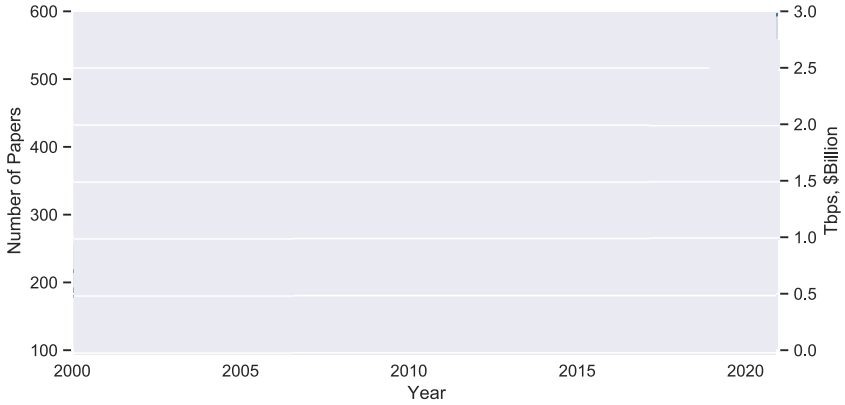
https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

https://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/1476220

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Community/researchers have been fighting

- As attacks have grown, so too has our work to address them!
- More and more research has poured in
- More and more billions of dollars
- But, attack volumes have kept up with (and often outpaced) all proposed mitigations



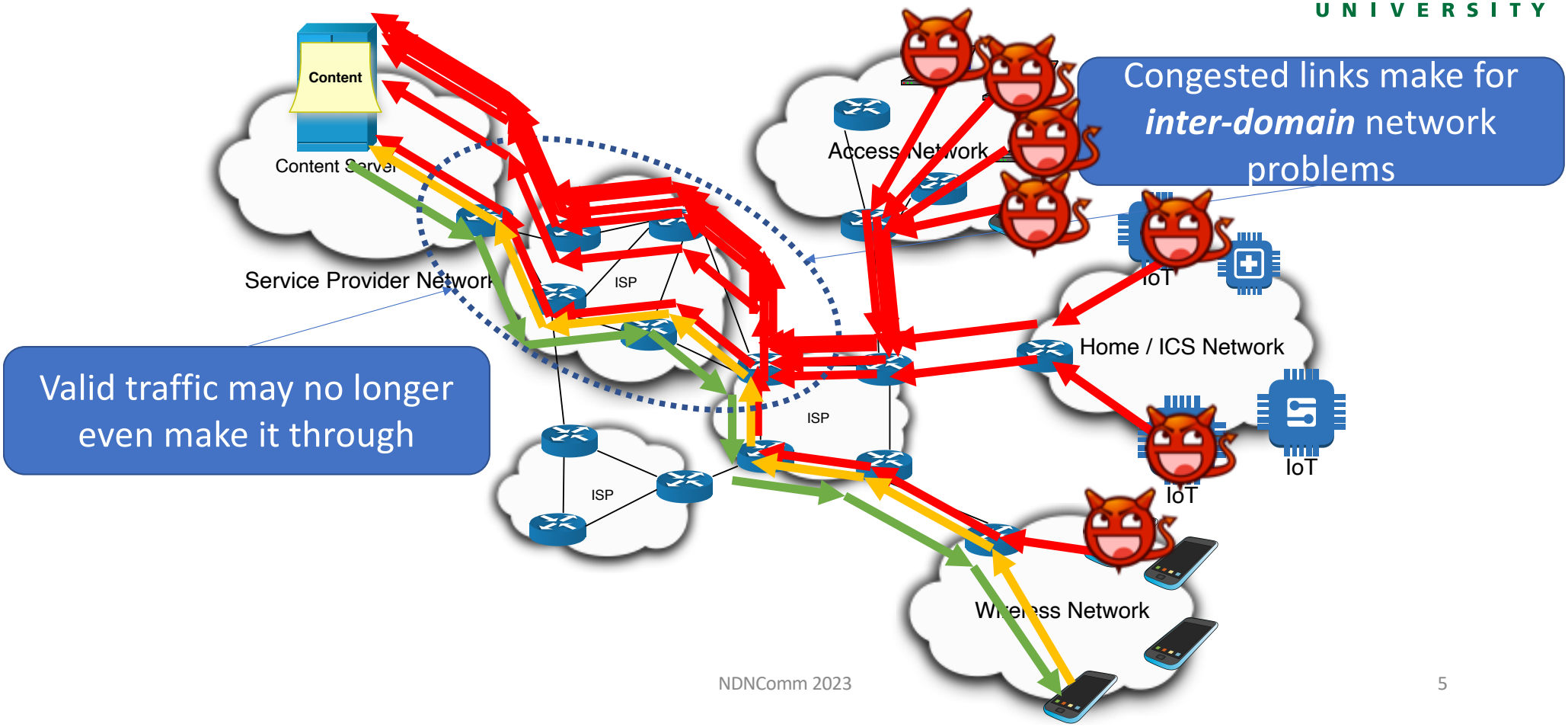
- We conducted a large-scale ***architectural*** analysis of the literature* to determine how we can break this cycle… <u>And this has laid a path forward!</u>

* *Under submission*

Outline

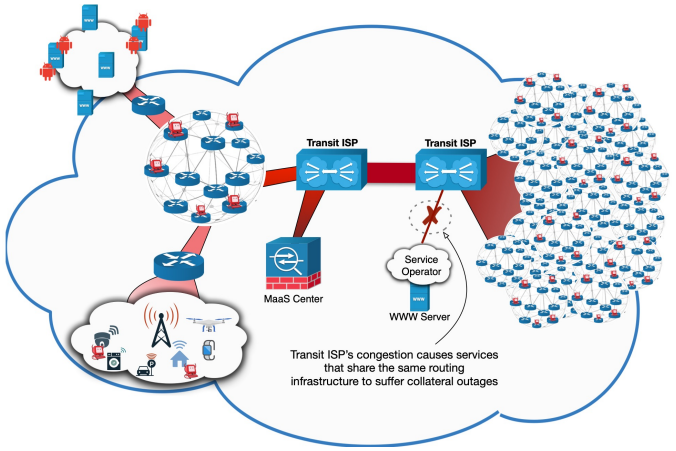
- Our evaluation of ~25,000 DDoS proposals and literature produced over 30+ years
- Our observations of DDoS and the basic attack surface it exploits
- Basic architectural advantages of NDN in this cybersecurity setting

Basic illustration of volumetric DDoS



Problem is the aggregate/inter-domain

- Lots of packet love aggregates through the network
  - Smaller networks and traffic volumes from the edge form attacks
  - Like tributaries
- As they join together on their way to the victim, they become more unbearable
  - As tributaries form torrents and rivers



[1]

- The actual sizes of large DDoS attacks are often unknown/unknowable
  - Can only be measured and evaluate at discrete network vantages
  - When links saturate, they do not pass on traffic (i.e., underreporting)

[1] Osterweil, Eric, Angelos Stavrou, and Lixia Zhang. "21 Years of Distributed Denial-of Service: Current State of Affairs." *Computer* 53, no. 7 (2020): 88-92.

“To know the road ahead…”

- “… ask those coming back” – Chinese proverb
- If DDoS is a plague for today’s IP Internet, can its symptoms illustrate how to prevent it for tomorrow’s architecture?
- We conducted a ***architectural*** study over roughly 25,000 papers, RFCs, and patents from the past 30+ years; with close inspection of over 260 of these works
- What has been [re]discovered, and what has met with deployment success, i.e., a form of requirements analysis

What we found

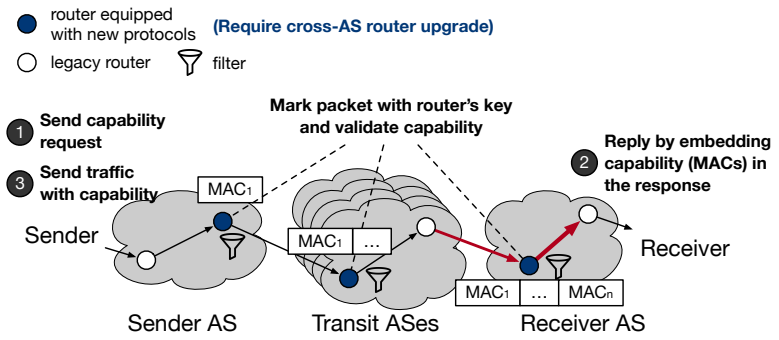
- The DDoS space embodies a great deal of variability
- But, there are a few basic vulnerabilities in the IP network layer that primarily enable it
- Moreover, there are relatively few basic remediation ***design patterns repeated*** throughout the literature
- Further, our aggregate/architectural analysis showed basic ***misalignments*** between costs/benefits

Categorization of DDoS defenses

- Preventative
  - Network-level preventive remedies: standards-based to admission-control
  - Solutions with no active measurement for DDoS detection
- Detection-only
  - Just knowing what is/isn't DDoS traffic is not straightforward
  - Assumed a separate mitigation mechanism in place mitigate DDoS attacks
- Mitigation-only
  - Solutions that just handle/squash DDoS attack traffic
  - Rely on a separate mechanism to detect and classify traffic
- Holistic
  - Approaches that do combined detection and mitigation

Synthesizing preventative-only approaches

- Preventing address spoofing [1, BCP-38/84]
  - Ingress/egress ***filtering***
- Some work added ***state to routers*** [2]
- Some work added state to ***packets*** [3]



- Capabilities works introduced ***authorize senders*** (i.e., RTS) [4-6] and added ***state*** (some made use of ***overlays*** to assist)
- Further works continued reusing the design pattern of adding state to routers/packets…

[1] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets," *ACM SIGCOMM computer communication review*, vol. 31, no. 4, pp. 15–26, 2001.

[2] Jun Li, J. Mirkovic, Mengqiu Wang, P. Reiher, and Lixia Zhang, "Save: source address validity enforcement protocol," in *Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2002, pp. 1557–1566.

[3] X. Liu, A. Li, X. Yang, and D. Wetherall, "Passport: secure and adoptable source authentication," in USENIX Symposium on Networked Systems Design and Implementation, 2008, pp. 365–378.

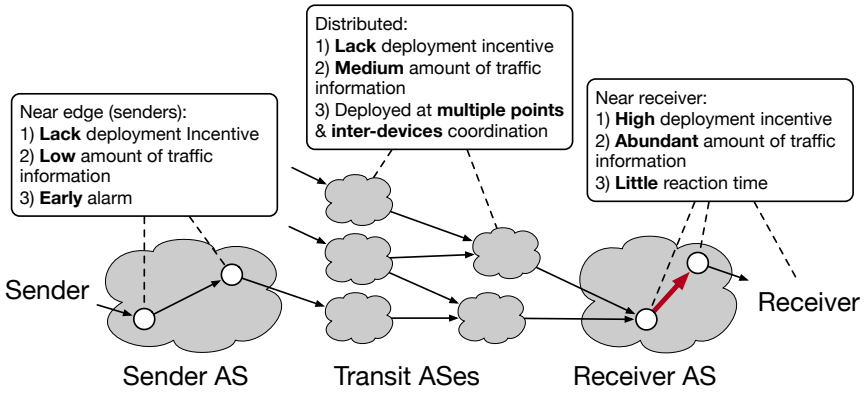
[4] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing internet denial-of-service with capabilities," *Computer Communication Review*, vol. 34, pp. 39–44, 01 2004.

[5] A. Yaar, A. Perrig, and D. Song, "Siff: a stateless internet flow filter to mitigate ddos flooding attacks," in *IEEE Symposium on Security and Privacy*, 2004, pp. 130–143.

[6] X.Yang,D.Wetherall,andT.Anderson,"Tva:Ados-limitingnetwork architecture," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1267–1280, 2008.

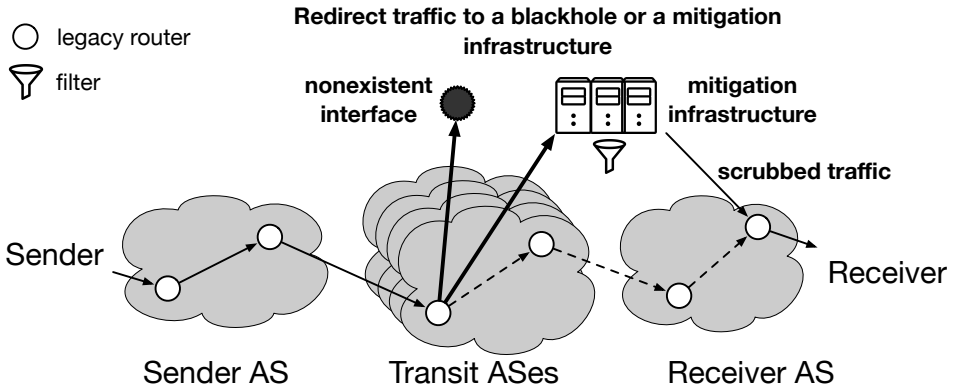
Detection and classification synthesis

- Near receiver (i.e., victim)
  - Massive traffic → better evaluation
  - ***High deployment incentive***
  - But, may already be ***too late***
- Distributed
  - Very variable amount of info
  - ***No deployment incentive***
  - Requires *inter-administrative trust*
- Near source
  - Often, not much telemetry
  - ***No deployment incentive***
  - Benefit: ***before any damage***



Mitigation only

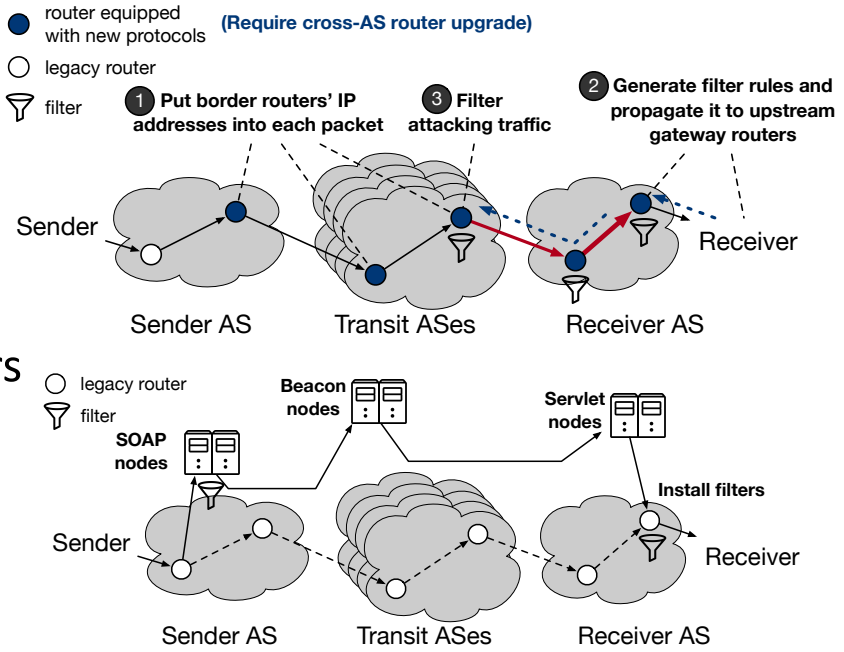
- Black holing
  - If sources known, networks can refuse to route their traffic
  - Simple/effective, but major collateral damage



- Mitigation as a Service (MaaS)
  - Pay an organization to "*scrub*" attack traffic away from legit traffic
  - MaaS provider can BGP hijack a customer's routes, and intercept all traffic
  - Use proprietary logic to scrub, and then preserve connectivity for legit traffic
  - ***No changes needed to infrastructure***
  - This is the primary defense used today

Mitigation only - distributed traffic filtering

- Receiver-controlled filtering
  - Filters pushed into the network
- Some used BGP to disseminate[1,2]
  - Additional state in packets or at routers
- Other approaches disseminate over *an **overlay network*** [3-5]



[1] K. J. Argyraki and D. R. Cheriton, "Active internet traffic filtering: Real-time response to denial-of-service attacks." in *USENIX annual technical conference, general track*, vol. 38, 2005.

[2] R. Chen, J.-M. Park, and R. Marchany, "Track: A novel approach for defending against distributed denial-of-service attacks," *Technical P˜ eport TR ECE—O6-02. Dept. of Electrical and Computer Engineering, Virginia Tech*, 2006.

[3] X. Liu, X. Yang, and Y. Lu, "To filter or to authorize: Network-layer dos defense against multimillion-node botnets," in *ACM SIGCOMM 2008 conference on Data communication*, 2008, pp. 195–206.

[4] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: Secure overlay services," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 4, pp. 61–72, 2002.

[5] D. G. Andersen *et al.*, "Mayday: Distributed filtering for internet ser- vices." in *USENIX Symposium on Internet Technologies and Systems*, vol. 4, 2003.

Lesson(s)?

- Looking at what proposals have repeatedly asked for
  - Changes to the routing infrastructure, e.g.:
    - Add state to stateless IP
    - Add filters
    - Add admission control / flow parity
- Looking at what has vs. what has *not* been deployed
  - Solutions requiring changes to the routing infrastructure:
    - ∅
  - Solutions that require deployment by non-impacted parties
    - ~ ∅
  - Solutions that align deployment costs with incentives (e.g., benefits)
    - MaaS providers
    - Anycast solutions

Today, MaaS is the primary defense

- MaaS networks provision enough capacity to withstand the throw weight of ever-growing attacks
- In the words of an operator of (arguably) *the* network to beat, “always be 10x bigger…”

- Costs/incentives aligned + no infrastructure upgrade needed
- But scalable?
  - A distributed defense would befit a distributed attack…

Going forward

- Today's butcher's bill makes for tomorrow's feast
- Previous work has observed that NDN is *inherently* resistant to DDoS attacks like those in the IP Internet [1]
- Nevertheless, some outstanding work remains
  - Interest flooding attacks [2, …] , etc.
- Lessons from the IP DDoS literature form a clear requirements list for NDN DDoS defense
  - Flow-parity
  - In-network state
  - Fine-grained / in-network control (e.g., filters)
  - Backpressure mechanisms
  - Inherent admission control
  - And more…
- A clear motivating direction for future work

[1] P. Gasti, G. Tsudik, E. Uzun and L. Zhang, "DoS and DDoS in Named Data Networking," *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, Nassau, Bahamas, 2013, pp. 1-7, doi: 10.1109/ICCCN.2013.6614127.

[2] Xin, Yonghui, Yang Li, Wei Wang, Weiyuan Li, and Xin Chen. "A novel interest flooding attacks detection and countermeasure scheme in NDN." In 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-7. IEEE, 2016.

Conclusion

- Our work shows that the DDoS problem is a clarion call for an architecture like NDN
- One of our main findings is that ***mis***aligning deployment costs with benefits is non-starter
  - Here, NDN stands out because it is a general purpose architecture
  - The benefit proposition for NDN includes its inherent DDoS resistance, but ***also*** the multitude of other service/application semantics that it better enables
  - Said simply, why deploy a DDoS-only solution when the general purpose of NDN also delivers benefits that expand beyond just DDoS?
- The dire state of DDoS is an exciting opportunity for NDN
- Our paper is under submission

Thank you

Questions?

Backup

Distributed Denial of Service (DDoS) attacks

- DDoS varies widely, in form and function
- There isn't just ***one*** type of DDoS!
- At a high-level:
  - DoS attacks are those that disrupt the function or availability of a service
  - **D**DoS attacks are DoS attacks that are effectuated by a *distributed* infrastructure
- Details include
  - The set of *distributed* sources used for attacks
  - What type of traffic is used in the attack
  - Which components of a service are targeted for the attack
  - How attack sources are enlisted/acquired
  - And more…

Attackers have an implicit advantage

- In order for providers to distribute their footprints, they pay heavily for provisioning and capacity
  - Can't keep pace with free/readily available/highly distributed attackers (i.e. bots)

- Paying for *terabits* of global *aggregate* capacity is way more expensive than *free*
  - And, DDoS is moving its TTPs from network/transport to application layers

This is an impedance mismatch!
We need a way for our DDoS countermeasures to be as *topologically* distributed as attackers

Attack sources

- Generally, robot-Networks (botnets)
- There are a variety of ways that machines can be enlisted into botnets
  - Malware infects and provide adversaries access
  - Miscreants compromise credentials and gain shells
  - …
- Malware, similarly, spreads in many many ways
  - Users inadvertently download and run (e.g., clicking on a link in email, scanning malicious QR codes, etc.)
- Once an adversary has a set of bots, she can use it or rent it to others
  - Often called a “booter” service

State of affairs

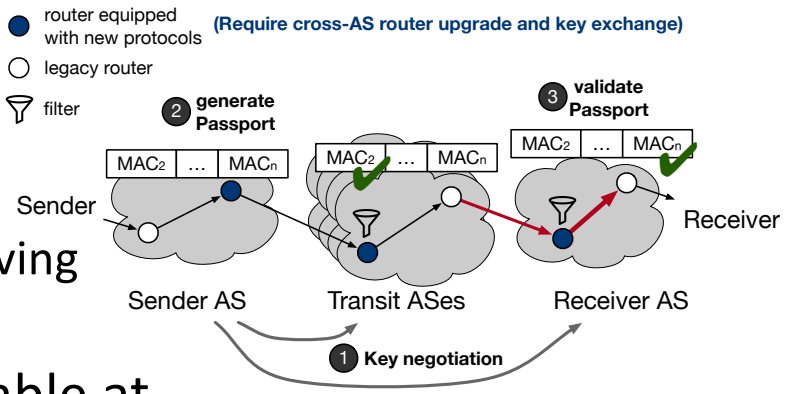
- It has always been easier to gain attack capacity than defensive capacity
- DDoS is an asymmetric threat with an impedance mismatch between attackers and defenders
  - Much easier to attack than defend
- The gap between adversaries' barriers to attack and the price to defend has always been large, but it is growing

Common types of DDoS

- Broadly
  - Volumetric
  - Low-and-slow
- Volumetric DDoS
  - A large sledgehammer of “packet love” (lots of unwanted traffic)
  - Goal is to overwhelm
- Low-and-slow
  - Generally to exploit protocol weaknesses
  - Cripple without overwhelming traffic volumes
- Different types/examples of DDoS attacks are discriminated by how they are *evaluated* (i.e., detected, on the victim side)
- The Techniques, Tactics, and Procedures (TTPs) are used to differentiate and attribute

Preventative-only approaches

- Preventing address spoofing [1,…]
  - Solutions like BCP-38/BCP-84 (ingress/egress ***filtering***)
  - Aims to eliminate DDoS traffic before leaving its source
- SAVE [2] added new incoming traffic table at each ***router***
- Passport [3] let ***packets*** carry the information needed for their source address validation



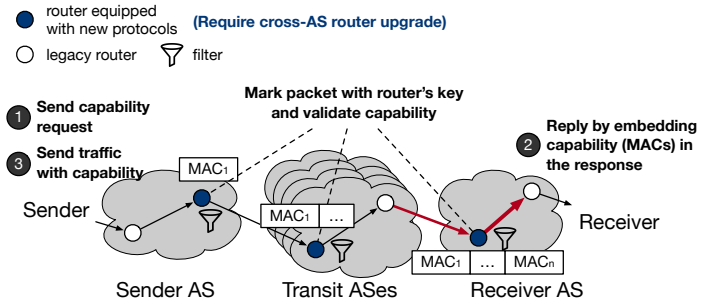
[1] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets," *ACM SIGCOMM computer communication review*, vol. 31, no. 4, pp. 15–26, 2001.

[2] Jun Li, J. Mirkovic, Mengqiu Wang, P. Reiher, and Lixia Zhang, "Save: source address validity enforcement protocol," in *Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2002, pp. 1557–1566.

[3] X. Liu, A. Li, X. Yang, and D. Wetherall, "Passport: secure and adoptable source authentication," in USENIX Symposium on Networked Systems Design and Implementation, 2008, pp. 365–378.

Preventative only approaches (continued)

- Capabilities-based approaches
  - Some approaches focus on flow parity through admission control
- [1] focused on an ***overlay/RTS***



- SIFF [2] proposed a Stateless Internet Flow Filter
  - Receivers ***authorize senders*** via a "capability" token that is carried in packets
- TVA [3] enhanced SIFF and bound it to specific network path
- All of these require ***new state in IP's stateless processing***…
  - Deployment has not begun

[1] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing internet denial-of-service with capabilities," *Computer Communication Review*, vol. 34, pp. 39–44, 01 2004.
[2] A. Yaar, A. Perrig, and D. Song, "Siff: a stateless internet flow filter to mitigate ddos flooding attacks," in *IEEE Symposium on Security and Privacy*, 2004, pp. 130–143.
[3] X.Yang,D.Wetherall,andT.Anderson,"Tva:Ados-limitingnetwork architecture," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1267–1280, 2008.

Preventative only approaches (continued)

- Traceback
  - i.e., where did attack traffic come from?
- Because IP's statelessness (rather than in spite of it), used tokens
  - [1-4] ***marked packets***, Pi [5] hashes routers' IP addresses in packet header
  - Similar to TVA, but no key-mgmt. needed
  - [2-3] let/made ***routers keep this state***
- Deployment challenge: upgrade all infrastructure?

[1] R. Stone et al., "Centertrack: An ip overlay network for tracking dos floods." in USENIX Security Symposium, vol. 21, 2000, p. 114.

[2] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network
support for ip traceback," in Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, 2000, pp. 295–306.

[3] ——, "Network support for ip traceback," IEEE/ACM transactions on networking, vol. 9, no. 3, pp. 226–237, 2001.

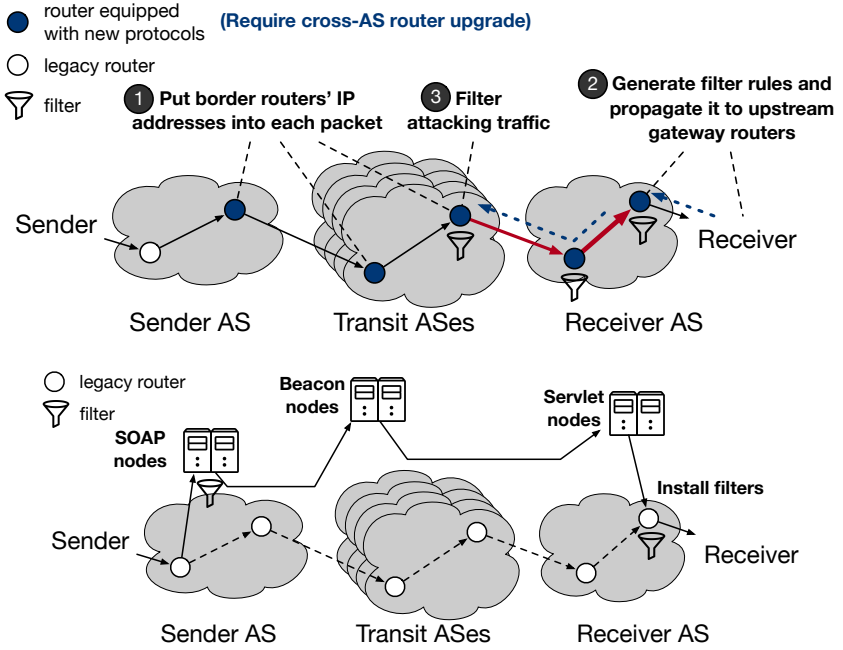
[32] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Hash-based ip traceback," ACM SIGCOMM Computer Communication Review, vol. 31, no. 4, pp. 3–14, 2001.

[4] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchak- ountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet ip traceback," IEEE/ACM Transactions on networking, vol. 10, no. 6, pp. 721–734, 2002.

[5] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against ddos attacks," in Symposium on Security and Privacy. IEEE, 2003, pp. 93–107.

Mitigation only - distributed traffic filtering

- Receiver-controlled filtering
  - If a service can create filters, can they be pushed into the network
  - A proposal called AITF [1] suggests a way for this to be done
  - Has each BGP border router put its IP in each packet, so filters can trace-back to sources (i.e., attackers)
  - Another approach, TRACK [2], takes a similar approach, but keeps state at routers
- Other approachs called StopIt [3], SOS [4] and Mayday [5] propose the same filter dissemination, but over *an **overlay network***



[1] K. J. Argyraki and D. R. Cheriton, "Active internet traffic filtering: Real-time response to denial-of-service attacks." in *USENIX annual technical conference, general track*, vol. 38, 2005.

[2] R. Chen, J.-M. Park, and R. Marchany, "Track: A novel approach for defending against distributed denial-of-service attacks," *Technical P˜ eport TR ECE—O6-02. Dept. of Electrical and Computer Engineering, Virginia Tech*, 2006.

[3] X. Liu, X. Yang, and Y. Lu, "To filter or to authorize: Network-layer dos defense against multimillion-node botnets," in *ACM SIGCOMM 2008 conference on Data communication*, 2008, pp. 195–206.

[4] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: Secure overlay services," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 4, pp. 61–72, 2002.

[5] D. G. Andersen *et al.*, "Mayday: Distributed filtering for internet ser- vices." in *USENIX Symposium on Internet Technologies and Systems*, vol. 4, 2003.

NDN's role

- Our analyses bear out that NDN offers a *principled* solution to the problem exposed by the IP DDoS threat
  - Lack of flow parity in IP foundationally enables DDoS – A central tenet of NDN
  - The vast majority of DDoS proposals attempt to add state to IP's stateless forwarding plane – A feature of NDN
  - The majority of proposals require their own specific inter-domain upgrades to parties who do not tend to derive benefits (i.e., cost/benefit misalignment)