NDN IP DDOS

From ECCAWiki

Contents

Possible attack vectors on NDN

- Paper: Y. Chung, "Distributed Denial of Service is a Scalability Problem" in CCR, 2012.

```
"push-pull" attack, where "bots" generate interests for data that is generated by another bots

No evaluation
```

- Tobias Lauinger, "Security & Scalability of Content-Centric Networking", Master Thesis, 2010

```
Interesting thesis,
listing several potential attacks on NDN, including threat of cache enumeration (list, probe, clone)

Evaluation: DLAM (Digital subscriber line multiplexer) service for youtube-like service.
1000 users, with 10% of simultaneous watching. Realistic traffic (actual videos, videos popularity
based on Youtube report)
```

IP

Security reports

- ARBOR networks, "Worldwide Infrastructure Security Report", Volume VII, 2011

```
Partial rank of tools to mitigate attacks:
  1. ACLs, 2. Dst-based blackholing, ... 5. Src-based blackholing ... ... CDNs
  !! no QoS solutions !! Concerns that rate-limiting will have unintended side effect on legitimate users
In general, up to 30 minutes to mitigate attack. Some longer.
```

Botnets

- Thorsten Holz, Moritz Steiner, Frederic Dahl, Ernst Biersack, Felix Freiling, "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm", in LEET, 2008

```
 The lower bound being around 5,000 – 6,000 and the upper bound being around 45,000 – 80,000 distinct bots
```

```
5,000 and 40,000 peers concurrently online.
```

- Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, Andreas Terzis, "My Botnet is Bigger than Yours (Maybe, Better than Yours) : why size estimates remain challenging", in Hotbots, 2007

```
footprint = 48,500 bots over the entire tracking period
live population = does not exceed 3,000
```

Surveys

- T. Peng et al. "Survey of network-based defense mechanisms countering the DoS and DDoS problems" in ACM Computing Surveys (CSUR), 2007
- J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", in CCR, 2004.
- A. Ashfaq et al. "A Comparative Evaluation of Anomaly Detectors under Portscan Attacks", in RAID, 2008
- K. Nyalkalkar et al. "A Comparative Study of Two Network-based Anomaly Detection Methods", in INFOCOM, 2011.
- J. Mirkovic et al. "How to test DoS Defenses", in CATCH 2009.

Proposals

Network level (Flooding)

Name	Year	Publication	Key features	Evaluation		
				Method	Topology	Traffic
Pushback	2001, 2002	Mahajan et al. "Controlling High Bandwidth Aggregates in the Network", TR Ioannidis et al. "Implementing Pushback: Router-Based Defense Against DDoS Attacks", in NDSS	(hop-by-hop push back) aggregate-based congestion control/congestion signatures (e.g., per-destination), rate-limiting, explicit notification	ns2	simple 3-level, 1-1-2-4(client)-node; 4-level 1-1-4-16-64(client) node topology	(good) WEB traffic using ns2 generator, (bad) 1Mbps CBR
SIFF	2004	A. Yaar et al. "SIFF: A stateless Internet flow filter to mitigate DDoS flooding attacks", in Symposium	(time-based tickets, capabilities)	something uses CAIDA Skitter	?	?

		on Security and Privacy				
AITF	2005	K. Argyraki et al. "Active Internet Traffic Filtering: Real-Time Response to Denial-of-Service Attacks", in USENIX	path recording, last-point of trust detecting,	DaSSF	AS-mapped, OC-192, OC-48, 100Mbps, 10Mbps; ~200ms/~20ms	10k, 100k, 1M attack sources, various attack scenarios
PacketSymmetry	2005	Christian Kreibich, "Using Packet Symmetry to Curtail Malicious Traffic", in Hotnets	(? leverages packet symmetry to detect and remove bad traffic) packet asymmetry - number of transmitted packets (tx) to received packets (rx) negative values when rx outweighs tx, positive values when tx outweighs rx, and zero in the case of perfectly balanced traffic	Packet trace analysis	170,000 IP addresses	-
TVA	2005	X. Yang. "A DoS-limiting Network Architecture", in SIGCOMM	like SIFF, traffic-based tickets, hierarchical per-AS, per-source fair queuing	ns2, 1-machine emulation	Dumbbell topology	(good) FTP transfers with abort function, (bad) bandwidth flood, colluding attacker, capability req flood, other
FastPass	2006	Dan Wendlandt, "FastPass: Providing First-Packet Delivery", TR	(tokens: various puzzles, other methods) traffic authorization, routers verify and filter.	Emulab	small (bottleneck, 20 nodes), dual domain topology	(req channel) 5Mbps/1Mpbs, (links) 100Mbps/20Mbps, (bad) 240Kbps
		M. Natu and J. Mirkovic, "Fine-Grained Capabilities for Flooding	based on TVA/SIFF: specifies previously unspecified mechanisms to grant "tickets" for requesters,		simple 15-node topology with 1 victim, 2 legitimate users, 7	simple traffic

	2006	DDoS Defense Using Client Reputations", in SIGCOMM LSAD workshop	extends capabilities to include priorities, changing tickets to be only destination-dependent, not path dependent	Emulab	attackers, and 3 routers. Bottleneck 100Kbps, 100Mbps other links,	pattern (SSH/telnet sessions)
DefCOM	2006	G. Oikonomou et al. "A Framework for Collaborative DDoS Defense", in USENIX ACSAC	Communication between src, core, and dst to provide collaborative defense. Dst raises alerts, src differentiate bad/good, packet tagging. Core rate-limit, congestion-aware re-tag. Traffic prioritization.	DETER	Tree topology	Telnet sessions
dFence	2007	Ajay Mahimkar et. al "dFence: Transparent Network-based Denial of Service Mitigation", in NSDI	(middleboxes) TCP connection proxying, rate estimation and TCP/ACK modification	real implementation	straight line, 20 copper ports and two fiber ports	1.5Mpps/64-byte packet; max TCP throughput 100Mbps
LazySusan	2007	J. Crowcroft et al. "Lazy Susan: dumb waiting as proof of work", TR	(latency-based proof of work--- computational puzzles)	Theory	-	-
Portcullis	2007	Parno et al. "Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks", in SIGCOMM,	Protecting connection setup with computational proof of work, tickets and traffic prioritization for the rest, per-computational fairness; DNS to disseminate puzzles There are many other puzzle-based schemes, on which Portcullis is based or which	Theory, sim?	single bottleneck (theory, fairness proof), derived from CAIDA Skitter (sim, "realistic," large-scale, tree-like), sender 20Mbps, victim 200Mbps, core 2Gbps, 1000bit req, 5% reserved for reqs 1k (good), 1k-	Protecting connection setup with computational proof of work, tickets and traffic prioritization for the rest

			problems it solves		20k (bad),	
PSP	2008	J. Chou et al. "Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks", in USENIX security symposium	topology as origin-destination pairs, packet tagging, OD traffic isolation, sharing based on historic bandwidth demand	ns2	two large ISP networks (US, EU)	Traffic matrices from measurements, UDP simulated
StopIt	2008	X. Liu et al. "To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets" in SIGCOMM	(filtering) tagging with passports, tagged prioritization, dst-invoked filter instantiation	DETER, ns2	line topology (DETER), random portion of AS map (ns2)	FTP transfers with abort function
NetFence	2010	Liu et al. "NetFence: Preventing Internet Denial of Service from Inside Out", in SIGCOMM	congestion policing: fair queuing (one leaky bucket per {src,L}, L-bottleneck), secure "ticketing" with signals for AIMD to increase/decrease bandwidth allowance	DETER, ns2	Simplistic scenario, modeling 25k-200k nodes (2 routers modeling core, with attached AS networks with good/bad users)	Good user: 20kbytes/TCP, Bad user 1Mbps/UDP, channel between routers 10Gbps
Shield	2011	Kline et al. "Shield: DoS Filtering Using Traffic Deflecting", in ICNP	(middleboxes) on-demand filtering, BGP-based redirection	-	-	-

Overlay-based solutions

Name	Year	Publication	Key features	Evaluation		
				Method	Topology	Traffic
Mayday			(overlay)			
OverDoSe			(overlay)			
Phlanx			(overlay)			

(FONet)			(overlay)			
CenterTrack	2000	Robert Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods", in USENIX	(overlay) reroute suspicious traffic to a special routers with diagnostic capabilities using an overlay	real implementation	-	-
SOS	2003	D. Angelos et al. "SOS: An Architecture for Mitigating DDoS Attacks", Journal on Selected Areas in Communications	(overlay)	Theory, PlantLab	Varied number of overlay hops	Contacted 3 SSL servers

Application level (resource exhaustion)

Name	Year	Publication	Key features	Evaluation		
				Method	Topology	Traffic
Speak-Up	2006	M. Walfish et al. "DDoS Defense by Offense"	(speed up good clients) "payment" traffic on a separate channel for bids in an auction for access to the destination, encourage good guys to increase bw during app-layer attacks; the front-end selects the client that has sent the most bytes	Theory, Emulab	one shared LAN, multiple shared LANs with different bandwidths (50 clients, each with 2 Mbits/s of access bandwidth)	HTTP requests as Poisson process, limit outstanding requests, limited backlog of requests.
	2010	S. Yadav et al., "Detecting Algorithmically Generated Malicious Domain Names", in IMC	compute metrics that characterize the distribution of the alphanumeric characters or bigrams (two consecutive alphanumeric characters) within the set of domain names. Specifically, we propose the following metrics to quickly differentiate a set of legitimate domain names from malicious ones	implementation	DNS PTR records corresponding to all IPv4 addresses. The database contains 659 secondlevel domains with at least 50 third-level sub-domains, while there are 103 second-level domains with at least 500 thirdlevel sub-domains.	-

Source spoofing protection

Name	Year	Publication	Key features	Evaluation		
				Method	Topology	Traffic
Flow-Cookies	2006	Casado, M., "Flow-Cookies: Using Bandwidth Amplification to Defend Against DDoS Flooding	(middleboxes) cookie = MAC source authenticator. TCP only	-	-	-

		Attacks", in IWQoS				
Clouseau	2006	J. Mirkovic et al. "A Practical IP Spoofing Defense Through Route-Based Filtering", TR	connection fiddling, reaction observing, filtering	Emulab	Simple 5-node	telnet-like connections
AIP	2008	D. Andersen et al. "Accountable Internet Protocol (AIP)", in SIGCOMM	self-certifying names/addresses (trusted host software to block unwanted traffic)	-	-	-
RAD	2009	Kline et al. "RAD: Reflector Attack Defense Using Message Authentication Codes", USENIX ACSAC	Source/network-based packet marking with cryptographic authentication codes that effectively prevents traffic reflecting	DETER	small topology ~50 nodes	Use of real core traces for traffic reply (from MAWI, 15 min per trace). SEER tool replays traffic in congestion-responsive manner. Measuring successful transactions. Traffic processing with CAIDA CoralReef package.
Kill-a-Bot			(for app-layer attacks)			

General methods

- network capabilities (aka tickets) with traffic prioritization
- fair queuing (various granularity: source, path, destination; proof-of-work: bandwidth, computation)
- source spoofing protection
  - direct flooding
  - reflector flooding