

Netbouncer¹

¹“NetBouncer: Client-legitimacy-based High-performance DDoS Filtering,”
Thomas, Mark, Johnson, Croall, DISCEX 2003

- Goal: detect legitimate clients and only serve their packets
- Victim-end, inline defense system deployed in front of the choke point
- Keeps a list of legitimate clients:
 - Only packets from these clients are served
 - Unknown clients receive a challenge to prove their legitimacy, several levels of legitimacy tests
 - Various QoS techniques are applied to assure fair sharing of resources by legitimate client traffic
 - Legitimacy of a client expires after a certain interval

1

Can it work?

- Successfully defeats spoofed attacks
- Ensures fair sharing of resources among clients that have proved to be legitimate
- All legitimacy tests are stateless – defense system cannot be target of state-consumption attacks
- Some legitimate clients do not support certain legitimacy tests (i.e. ping test)
- Legitimate client identity can be misused for attacks
- Large number of agents can still degrade service to legitimate clients, creating “flash crowd” effect

2

Advantages and Limitations

- + Ensures good service to legitimate clients in the majority of cases
- + Does not require modifications of clients or servers
- + Stateless legitimacy tests ensure resiliency to DoS attacks on Netbouncer
- + Realistic deployment model: Autonomous solution, close to the victim
- Attackers can perform successful attacks by:
 - Misusing identities of legitimate clients
 - Recruiting a large number of agents
- Some legitimate clients will not be validated
- Challenge generation may exhaust defense

3

SOS¹

¹“SOS: Secure Overlay Services,” Keromytis, Misra, Rubenstein, ACM SIGCOMM 2002

- Goal: route only “confirmed” user’s traffic to the server, drop everything else
- Clients use overlay network to reach the server
- Clients are authenticated at the overlay entrance
- Small set of source addresses are “approved” to reach the server, all other traffic is heavily filtered out

4

SOS

- User first contacts nodes that can check its legitimacy and let him access the overlay – *access points*
- Approved nodes whose traffic can pass through the firewall– *secret servlets*
 - Their identity has to be hidden, because their source address is a passport for the realm beyond the firewall
- Nodes that know identity of secret servlets – *beacons*
 - Any node that receives a packet to the target uses Chord to reach a beacon
 - Chord is overlay routing algorithm hashes nodeIDs into the routing table and then routes to those hashed identifiers
 - It is guaranteed to reach node with a given nodeID within $O(\log N)$ hops
 - We use target IP address as nodeID for beacon nodes

5

SOS

- User sends packets to access point
- Access point hashes target IP address and uses this and Chord to route packets to beacons
- Beacons route packets to secret servlets
- Secret servlets *tunnel* packets to firewall
- Firewall lets in only packets with source IP of a secret servlet
- If any node fails, other nodes can take over its role

6

Can it work?

- SOS should successfully protect communication with a private server:
 - Access points can distinguish legitimate from attack communications
 - Overlay protects traffic flow
 - Firewall drops attack packets
- Redundancy in the overlay and secrecy of the path to the target provide security against DoS attacks on SOS

7

Advantages and Limitations

- + Ensures communication of “confirmed” user with the victim
- + Resilient to overlay node failure
- + Resilient to DoS
- Does not work for public service
 - Clients must be aware of overlay and use it to access the victim
- Traffic routed through the overlay travels on suboptimal path
- Still allows brute force attack on links entering the filtering router in front of client
 - If the attacker can find it ⁸

Client Puzzles¹

¹“Client puzzles: A cryptographic countermeasure against connection depletion attacks,” Juels, Brainard, NDSS 1999

- Goal: preserve resources during connection depletion attack
- When under attack:
 - Server distributes small cryptographic puzzle to clients requesting service
 - Clients spend resources to solve the puzzle
 - Correct solution, submitted on time, leads to state allocation and connection establishment
 - Non-validated connection packets are dropped
- Puzzle generation is stateless
- Client cannot reuse puzzle solutions
- Attacker cannot make use of intercepted packets

10

Can it work?

- Client puzzles guarantee that each client has spent a certain amount of resources
- Server determines the difficulty of the puzzle according to its resource consumption
 - Effectively server controls its resource consumption
- Protocol is safe against replay or interception attacks
- Other flooding attacks will still work

Advantages and Limitations

- + Forces the attacker to spend resources, protects server resources from depletion
- + Attacker can only generate a certain number of successful connections from one agent machine
- + Low overhead on server
- Requires client modification
- Will not work against highly distributed attacks
- Will not work against bandwidth consumption attacks
- Puzzle verification consumes server resources

11

COSSACK¹

¹“COSSACK: Coordinated Suppression of Simultaneous Attacks,” Papadopoulos, Lindell, Mehlinger, Hussain, Govindan, DISCEX 2003

- Goal: detect the attack, place response near the sources
- COSSACK watchdogs are located at edge networks and organized into a multicast tree
- Client watchdog detects the attack, notifies all involved sources via multicast tree
- Sources join victim-specific group and exchange information
- Involved sources perform smart filtering to control attack traffic

12

Can it work?

- Victim-end detection is very accurate
- Source-end response effectively stops attack, minimizes collateral damage
- COSSACK should successfully detect and stop flooding attacks from protected networks
- May inflict collateral damage if attack is similar to legitimate traffic

13

Advantages and Limitations

- + Accurate detection at the victim, effective response at the source
- + No changes are required at client machines
- Multicast communication is not scalable
- Attacks from unprotected networks cannot be stopped
- Collateral damage will be inflicted if attack is similar to legitimate traffic

14

DefCOM¹

¹Forming alliance for DDoS defense, Mirkovic, Robinson, Reiher, Kuenning, NSPW 2003

- Goal: detect the attack, rate-limit the attack traffic, forward legitimate traffic
- DefCOM nodes build an overlay network
- Three types of nodes:
 - *Alert generator* – detect the attack, inform other nodes
 - *Classifier* – distinguish legitimate from suspicious traffic, forward legitimate packets marked with *legitimate* mark, rate-limit suspicious packets, mark them with *monitored* mark
 - *Rate-limiter* – rate limit all traffic to the victim, give the highest priority to legitimate, then to marked traffic
- Alert generators and classifiers deployed at the edge, rate-limiters deployed at the core

16

Can it work?

- Victim-end detection is very accurate
- Source-end response effectively stops attack
- Rate-limiters in the core handle attacks from networks that do not have classifier nodes
- Classifiers minimize collateral damage
- DefCOM should successfully stop flooding attacks, while guaranteeing good service to legitimate traffic

Advantages and Limitations

- + All actions are performed where they are most successful:
 - + Accurate detection at the victim
 - + Rate-limiting in the core
 - + Traffic differentiation at the source
- + Selective response provides low collateral damage
- + Core nodes handle attacks from legacy networks
- + Overlay architecture provides scalability
- + Only a few deployment points are needed
- Only effective with some core router deployment
- Compromised overlay nodes can damage operation

17