Quiz 1 Posted on DEN

- 8 multiple-choice questions
- Open book but no Internet
- Due by Wed 3/7
- Should be taken before you start working on your Firewalls lab
- You will retake the same test as Quiz 2 after the lab (not posted yet)
- Grading: If you take both quizzes I’ll just use the higher grade. If you skip one I’ll average both grades.

Report 2 Technically Due Today

- You can take a week of a grace period
- You should receive your report 1 grade today
  - Look where you lost points and how you can improve
  - If you already submitted report 2 and want to resubmit you can do so through the system

TCP SYN Flood

- Attacker sends lots of TCP SYN packets
  - Victim sends an ack, allocates space in memory
  - Attacker never replies
  - Goal is to fill up memory before entries time out and get deleted
- Usually spoofed traffic
  - Otherwise patterns may be used for filtering
  - OS at the attacker or spoofed address may send RST and free up memory

TCP SYN Cookies

- Effective defense against TCP SYN flood
  - Victim encodes connection information and time in ACK number
  - Must be hard to craft values that get encoded into the same ACK number – use crypto for encoding
  - Memory is only reserved when final ACK comes
- Only the server must change
  - But TCP options are not supported
  - And lost SYN ACKs are not repeated

Small-Packet Floods

- Overwhelm routers
  - Create a lot of pps
  - Exhaust CPU
  - Most routers can’t handle full bandwidth’s load of small packets
- No real solution, must filter packets somehow to reduce router load

Shrew Attack

- Periodically slam the victim with short, high-volume pulses
  - Lead to congestion drops on client’s TCP traffic
  - TCP backs off
  - If loss is large back off to 1 MSS per RTT
  - Attacker slams again after a few RTTs
- Solution requires TCP protocol changes
  - Tough to implement since clients must be changed
Flash-Crowd Attack

- Generate legitimate application traffic to the victim
  - E.g., DNS requests, Web requests
  - Usually not spoofed
  - If enough bots are used no client appears too aggressive
  - Really hard to filter since both traffic and client behavior seem identical between attackers and legitimate users

Reflector Attack

- Generate service requests to public servers spoofing the victim’s IP
  - Servers reply back to the victim overwhelming it
  - Usually done for UDP and ICMP traffic (TCP SYN flood would only overwhelm CPU if huge number of packets is generated)
  - Often takes advantage of amplification effect – some service requests lead to huge replies; this lets attacker amplify his attack

Sample Research Defenses

- Pushback
- Traceback
- SOS
- Proof-of-work systems
- Human behavior modeling

Pushback:

"Controlling high bandwidth aggregates in the network."
Mahajan, Bellovin, Floyd, Paxson, Shenker, ACM CCR, July 2002

- Goal: Preferentially drop attack traffic to relieve congestion
- Local ACC: Enable core routers to respond to congestion locally by:
  - Profiling traffic dropped by RED
  - Identifying high-bandwidth aggregates
  - Preferentially dropping aggregate traffic to enforce desired bandwidth limit
- Pushback: A router identifies the upstream neighbors that forward the aggregate traffic to it, requests that they deploy rate-limit

Can it Work?

- Even a few core routers are able to control high-volume attacks
- Separation of traffic aggregates improves current situation
  - Only traffic for the victim is dropped
  - Drops affect a portion containing the attack traffic
- Likely to successfully control the attack, relieving congestion in the Internet
- Will inflict collateral damage on legitimate traffic

Advantages and Limitations

+ Routers can handle high traffic volumes
+ Deployment at a few core routers can affect many traffic flows, due to core topology
+ Simple operation, no overhead for routers
+ Pushback minimizes collateral damage by placing response close to the sources
  - Pushback only works in contiguous deployment
  - Collateral damage is inflicted by response, whenever attack is not clearly separable
  - Requires modification of existing core routers
Traceback


• Goal: locate the agent machines
• Each packet header may carry a mark, containing:
  – EdgeID (IP addresses of the routers) specifying an edge it has traversed
  – The distance from the edge
• Routers mark packets probabilistically
• If a router detects half-marked packet (containing only one IP address) it will complete the mark
• Victim under attack reconstructs the path from the marked packets

Traceback and IP Spoofing

• Traceback does nothing to stop DDoS attacks
• It only identifies attackers’ true locations
  – Comes to a vicinity of attacker
• If IP spoofing were not possible in the Internet, traceback would not be necessary
• There are other approaches to filter out spoofed traffic

Can it Work?

• Incrementally deployable, a few disjoint routers can provide beneficial information
• Moderate router overhead (packet modification)
• A few thousand packets are needed even for long path reconstruction
• Does not work well for highly distributed attacks
• Path reassembly is computationally demanding, and is not 100% accurate:
  – Path information cannot be used for legal purposes
  – Routers close to the sources can efficiently block attack traffic, minimizing collateral damage

Advantages and Limitations

+ Incrementally deployable
+ Effective for non-distributed attacks and for highly overlapping attack paths
+ Facilitates locating routers close to the sources
  – Packet marking incurs overhead at routers, must be performed at slow path
  – Path reassembly is complex and prone to errors
  – Reassembly of distributed attack paths is prohibitively expensive

SOS

11 SOS: Secure Overlay Services,” Keromytis, Misra, Rubensteain, ACM SIGCOMM 2002

• Goal: route only “verified user” traffic to the server, drop everything else
• Clients use overlay network to reach the server
• Clients are authenticated at the overlay entrance, their packets are routed to proxies
• Small set of proxies are “approved” to reach the server, all other traffic is heavily filtered out

SOS

• User first contacts nodes that can check its legitimacy and let him access the overlay – access points
• An overlay node uses Chord overlay routing protocol to send user’s packets to a beacon
• Beacon sends packets to a secret servlet
• Secret servlets tunnel packets to the firewall
• Firewall only lets through packets with an IP of a secret servlet
  – Secret servlet’s identity has to be hidden, because their source address is a passport for the realm beyond the firewall
  – Beacons are nodes that know the identity of secret servlets
• If a node fails, other nodes can take its role
Can It Work?

- SOS successfully protects 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

Advantages And Limitations

- Ensures communication of “verified user” with the victim
- Resilient to overlay node failure
- Resilient to DoS on the defense system
  - Does not work for public service
  - Traffic routed through the overlay travels on suboptimal path
  - Brute force attack on links leading to the firewall still possible

Client Puzzles

- Goal: defend against connection depletion attacks
- When under attack:
  - Server distributes small cryptographic puzzles to clients requesting service
  - Clients spend resources to solve the puzzles
  - 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

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 (Defense By Offense paper changes this)