Lecture 26

CS625: Advanced Computer Networks
Fall 2003

Tuesday, 21 October 2003

Bhaskaran Raman
CSE, IIT-Kanpur

http://www.cse.iitk.ac.in/users/braman/courses/cs625-fall2003/outline.html

Topic for Today

- Denial of Service Attacks: IP Traceback
-
- *No class Friday! Some other time?*
- *Scribe for today?*

Denial of Service Attacks

- DoS attacks:
  - Usually beyond crypto
  - Can be distributed (DdoS)
  - Very difficult to tackle
- Perfect solution is difficult
- Operational goal:
  - Identify machines generating the attack
  - That is, **IP Traceback**
  - Difficult due to spoofed source IP, stateless nature of Internet

Possible Solutions

- Ingress filtering
- Input debugging
- Controlled flooding
- Logging
- ICMP traceback
- Packet marking [SWK00]
- Comparison metrics: management, network, router overhead, preventive/reactive, distributed capability, post-mortem capability

IP Traceback: Some Definitions

- Victim
- Attack tree
- Attack path
- Exact traceback
- Approximate traceback
- Marking algorithm:
  - Marking procedure
  - Path reconstruction procedure
- Convergence time: in terms of number of packets to victim

Conservative Assumptions

- Regarding attacker:
  - Can generate any packet
  - Multiple attackers possible
  - May be aware that they are being traced
- Regarding network/routers:
  - Packet loss/reordering can happen
  - CPU/Memory are constrained
- Helpful assumptions:
  - Attackers send many packets
  - Stable routes
  - Not many routers compromised

Packet Marking: Node Append

- Append node at each hop
- Advantage: fast convergence
- Disadvantages:
  - High router overhead
  - Fragmentation
  - Attacker can misguide easily

Packet Marking: Node Sampling

- Static field in packet header
- Router puts its address in that field, with probability p
- Calculate router order at victim based on probability
- Advantage: difficult for attacker to insert false routers in path if $p > 0.5$
- Disadvantages:
  - Long convergence time
  - Multiple routers at same distance possible

Packet Marking: Edge Sampling

- Start, End, Distance fields in packet
  - Edge is marked and its distance from victim
- Robust to spoofing: can use any *p*
- Quick convergence
- Can handle distributed attacks
- But, cannot trust any marking beyond closest attacker
- Disadvantage: extra space in IP packet

Encoding Issues

- Edge sampling requires 72 bits: 32 + 32 + 8
- IP options: slow, may lead to fragmentation
- Out-of-band: router/network overhead
- Overloading the 16-bit IP identification field used for fragmentation

Compressed Edge Fragmentation Sampling

- Three ideas:
  - Encode *exor* of the two IP addresses making up an edge *(edge-id)*
  - Fragment edge-id into *k* parts, and include log2(k) additional bits
  - Include hash of IP address

IP Header Encoding

- Encode in IP fragmentation field
- Example: hash = 32, IP = 32, k = 8, distance field in 5 bits
- Backward compatibility issues:
  - Forced to penalize fragmented packets
  - But only 0.25% of packets are fragmented

Further Issues

- Backward compatibility, IPv6
- Distributed attacks
- Path validation
- Attack origin detection

Tomorrow...

- Domain Name System (DNS)
- Security attacks based on DNS