

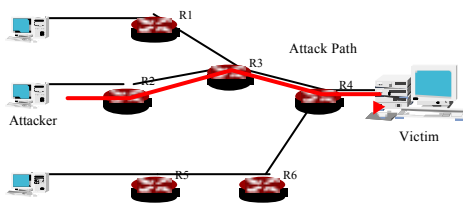
Security (2): IP Traceback

Suguru Yamaguchi
Nara Institute of Science and Technology

Background

- "Denial of Service" (DoS) are frequently observed
 - Concentration of the forged traffic to the targeted servers
 - Try to stop their services
 - Technical aspects
 - Simple traffic generation (ICMP flooding, TCP SYN flooding)
 - Source IP address spoofed
 - Simple DoS from a single source vs. Distributed DoS from multiple source
 - Over 100Mbps is not special

DoS Attack



It's so difficult to find the source

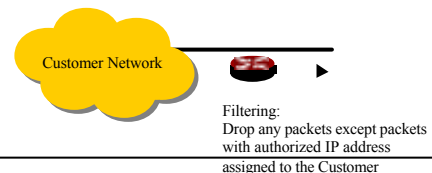
- Forged source IP address
 - IP header is not protected so that it's quite easy to forge the source IP address
 - In actual DoS attacks, even the actual traffic source is a single host, but the huge variety of source IP address can be observed.
- Advanced Attack software
 - DDoS
 - Forged source IP address, multiple target port
 - Long duration
 - About 30 min. in average
 - Few "Ping-of-death" type attack

Assumption

- Capability of Attackers
 - Any attackers can generate any kind of IP datagram
 - Multiple attackers may work cooperatively to conduct DDoS
 - Attackers can assume the all the traffic are monitored by ISP and other authorities
- Characteristics of Attacks
 - Generating large number of packets for some long duration (e.g. 30 min.)
 - Attack path is hardly changed
- Assumptions on Routers
 - Capacity of CPU processing and memory are limited
 - Router is not threatened by intrusion and other unauthorized access
 - Router never generates any kind of forged data
- Any packets may be discarded and reordered

Against DoS attacks

- Ingress filtering
 - Source IP address test and filtering
 - Effective
 - Still there are many chances to have packets with forged source IP address
 - All the ISP does not deploy Ingress filtering



IP trace back (1)

- Link testing
 - Input debugging
 - With help by ISP
 - Obtain traffic pattern and characteristics from victims
 - Trace traffic log saved at router
 - One by one from victim side
 - Trace back by manually, and some automated tools have been available
 - Huge overhead
 - It's not doable in the case of DDoS
 - Controlled flooding
 - Proposed by Burch and Cheswick
 - Topology map should be prepared
 - Observe DoS traffic change in the case insertion of burst traffic is on specific link. If the DoS traffic is changed, then we can conclude the DoS traffic is surely flowing through the link
 - Need ISP's help
 - This method can be considered of DoS
 - Cannot be apply in aftermath

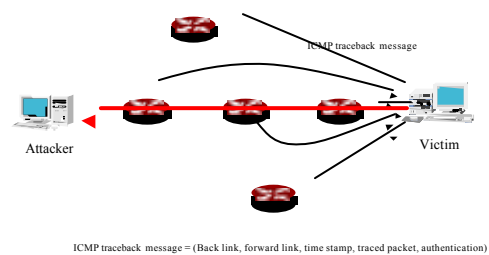
IP trace back (2)

- Logging
 - Sampling packets and record on routers
 - Save packets themselves
 - Save in/out interface data
 - Reconstruction of attack path using data mining tools applied to the packet log
 - Huge resource is required
 - Data storage
 - Processing power for data mining
 - Not effective for ultra broadband backbone such as 10G, but it becomes more popular in commercial ISP environment
 - Can be traceable even for "Ping-of-Death"
 - Sampling rate vs. attack path reconstruction overhead.

IP trace back (3)

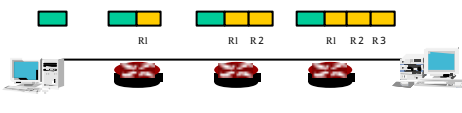
- ICMP tracebackMessage
 - Bellovin@ATT Laboratories Research
 - *ICMP Tracebackmessages, draft-bellovin-itrace-.txt*
 - Method
 - Sampling packet with quite low possibility (e.g. 1/20000)
 - Record inbound/outbound interface
 - Sampled packet and interface data are packed in to ICMP message, then send the ICMP message to the destination host
 - Normally, ICMP message is transferred in out-band channel
 - Issues
 - Adding more traffic
 - ICMP message filter is normally enabled at firewalls
 - Reconstruction of attack path takes longer duration such as 30 min.
 - Trade off: Time required for attack path reconstruction vs. the number of ICMP traceback message

ICMP traceback messages



IP trace back (4)

- Traffic Marking
 - Marking all the packet at each router
 - Theoretically possible, but practically impossible
 - High overhead at packet header processing at each router
 - No space available in IP header
 - Limited space even for IP option (IPv4)
 - High process overhead (IPv6, hop-by-hop option?)



IP trace back (5)

- Probabilistic traffic marking
 - Savage@Univ. of Washington
 - *Practical Network Support for IP traceback, ACM SIGCOMM'00.*
 - Method
 - Sampling packets with quite low possibility
 - Encode router information and write it to unused field of IP header
 - In-band approach
 - No changed on IP itself and low overhead
 - Which field can we use?
 - What algorithm can we use as encoding the mark?

Node sampling

- Write information about passed node
 - with probability p
 - $p(1-p)^d$
 - Possibility we can observe the info about router with distance d
 - The large number of packets we need to reconstruct attack path

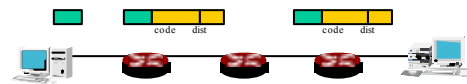
Edge Sampling

- Record Start node, end node into the IP header
 - Method
 - Record start node, end node and hop count (distance)
 - Write it to the IP header with probability p
 - Write start node field, set 0 to the distance
 - Write it to the IP header with probability $1-p$
 - Write end node field, increment distance
 - Make tree rooted by victim's host
 - Using distance field
 - Encoding method is required
 - Many info have to be recorded

Encoding Method

- XOR
- Non-overlapped fragment into IP identification field (16bit)
- IP address "hash"
- FMS (fragment Marking Scheme)
 - Integration of three method
- AMS (Advanced and authenticated Marking Scheme)
 - D. Song and A. Perrig. Advanced and authenticated marking schemes for IP traceback. Technical Report UCB/CSD-00-1107, University of California, Berkeley, June 2000.

XOR

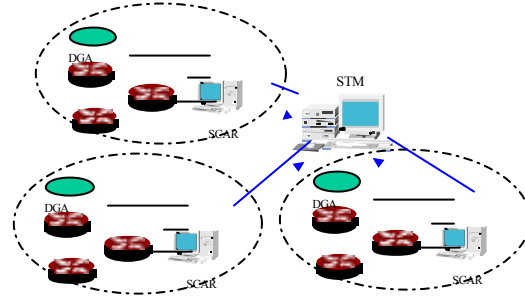


Code	Dist	Calc. at victim node
R3	0	R3
$R2 \times R3$	1	$R3 \times (R2 \times R3) = R2$
$R1 \times R2$	2	$R2 \times (R1 \times R2) = R1$

IP trace back (6)

- Hash-based marking at router
 - Snoeren@BBN
 - Hash-based IP Traceback, SIGCOMM'01
 - SPIE (Source Path Isolation Engine)
 - Implement on routers
 - Calculate hash for recently forwarded packets (packet digesting)
 - Components
 - DGA: data generation agent
 - SCAR: SPIE Collection And Reduction agent
 - STM: SPIE Traceback Manager

SPIE@ISP



More issues

- Need to work cooperatively among autonomous systems in order to make complete IP trace back
 - Each AS is managed by different operational entity
 - Differences in management policy
 - Lack of information may happen so that we need to make negotiation to exchange any kind of information for IP traceback
 - At least hierarchical IP traceback structure is required
 - 2 layer, AS internal and inter AS
 - Modifications and adding functions to the router are required
 - Financial issue
 - Multiple attackers
 - In the case multiple attackers are using the same forged source address space, it is quite hard to reconstruct attack path.
 - It is quite likely to observe this situation in the case multiple attackers are using the same attack tools
 - Making attack path tree can be a solution, but more overhead on analysis
-

Standardization at IETF

- IETF itrace BOF
 - Had meetings in 3 previous IETF meetings
 - Still in Research level
 - More work need if we step forward to standardization process
 - Forming small group to work on the IP traceback methodologies (IETF54)
-

Who need this function?

- Law enforcement for forensics works
 - DoS and DDoS are ranked in major attacks that can make serious loss in terms of business
 - Chasing back to attacker is always required
 - Military Networks
 - By their nature
 - Monitoring everything, so brute force method can be applied
-

Summary

- IP traceback
 - Research area has been activated since year 2000
 - Mainly target is to provide trace back capability against DoS attacks
 - Still research phase
 - Multiple AS environment
 - Multiple attack hosts using the same forged source address range
 - Implementation
 - A few steps in IETF
 - Implementation
 - Few on commercial router products
 - Hardware packet forwarder is a major reason why few are available on commercial router products
 - No market arise
-