Distributed Denial of Service (DDoS): Attacks and Defenses

I. Pustogarov

DDoS – Papers to discuss

- One survey paper:
  - "Survey of network-based defense mechanisms countering the DoS and DDoS problems", Peng et al., ACM Computing Surveys, 2007
  - Mandatory: Sections (1, 2, 3, 4)

- One solution paper:
  - "Botz-4-Sale: Surviving organized DDoS at- tacks that mimic flash crowds", Kandula et al., NSDI, 2005
  - Mandatory: Sections (1, 2, 3.1, 4)

- PVO Book (Chap 11)
- Several other papers

DDoS – definition

- A DDoS
  - Degrades a resource used by a victim (legitimate user) or
  - Denies use of a resource by a victim
  - Clog/crash a resource

  through:
  - A coordinated group of resources controlled by an attacker
  - A group of individuals requesting resources provided by a victim
  - These resources together send traffic which is collectively malicious

- Target resources: network bandwidth, CPU, database/disk bandwidth

DDoS – definition (cont.)

- Collectively malicious traffic includes attempting to send:
  1. more data than a victim can handle,
  2. data which is malformed according to specifications,
  3. data exploiting weaknesses in a protocol implementation

- Victims (examples)
  1. Online businesses
  2. Political groups
  3. Competing parties
  4. Infrastructure providers

Attackers' motives and impacts of DDoS

- Motives
  - Money
  - Political agenda
  - Civil disobedience
    - See the Master's thesis: "Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet"
      - http://archive.org/details/2013SauterDDOSAndChallengeOfInternetCivilDisobedience
    - Hacktivism: On the Use of Botnets in Cyberattacks
      - https://journals.sagepub.com/doi/pdf/10.1177/0263276416667198
  - Power / fame

- Impacts
  - Financial
  - Reputation
    - Long term impacts
  - Critical infrastructures

Flash crowd vs. DDoS

Table II. Comparison Between Bandwidth Attacks and Flash Crowds

	Bandwidth Attack	Flash Crowd
Network impact	Congested	Congested
Server impact	Overloaded	Overloaded
Traffic	Malicious	Genuine
Response to traffic control	Unresponsive	Responsive
Traffic type	Any	Mostly Web
Number of flows	Any	Large number of flows
Predictability	Unpredictable	Mostly predictable

DDoS – a simple view

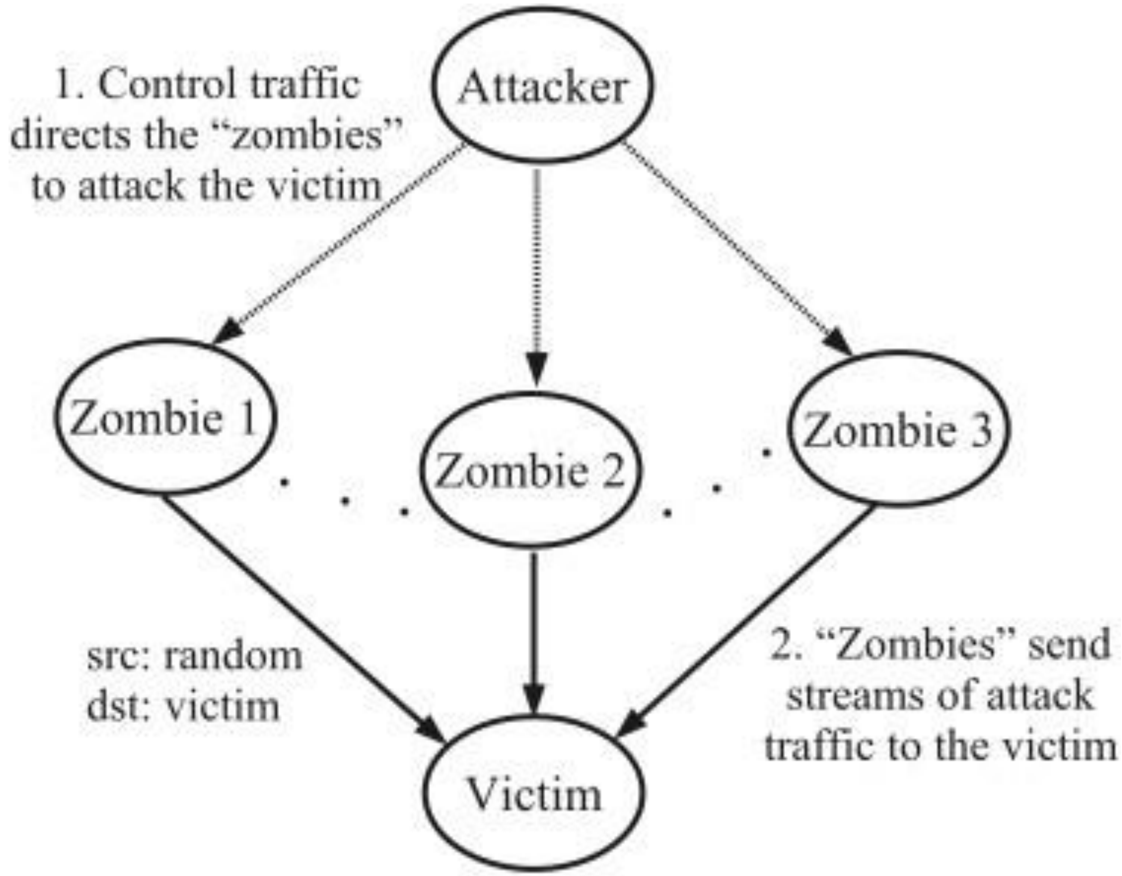


Fig. 2. Structure of a typical DDoS attack (based on Paxson [2001]).

Why DDoS is possible?

- Inherent features of Internet – including the following:
  1. End-to-end connectivity
     - Any host can attack any other hosts
     - Multi-path routing
  2. Either end may misbehave
     - Attack traffic can be "shaped" like legitimate sources
  3. Shared, limited resources
  4. Intermediate networks only attempt to forward traffic
     - No policing; decentralized by design

Defense challenges

- Target must deal with very high volumes of traffic (10Gbps or more)
- Attacks sources are geographically distributed
- An attack may mimic flash crowd

- Benchmark for mitigation tools
  - How to define "success"
- Testing in realistic environment
  - Good dataset/realistic setting is a big challenge
  - But essential for evaluating proposed solutions

Survey of attack methods

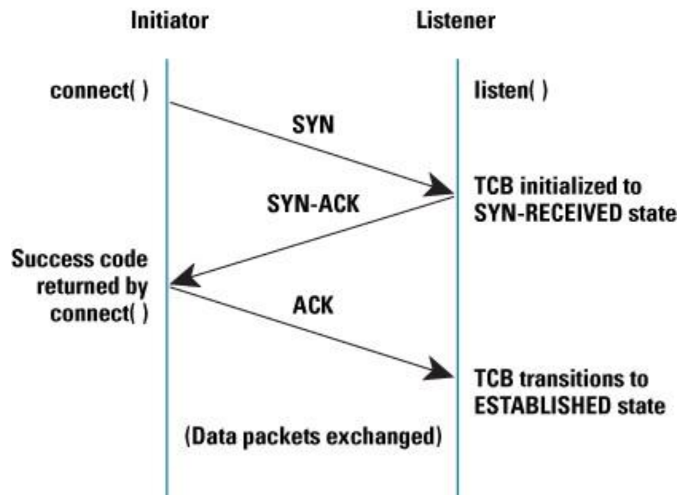
Broad categories of attacks

- Protocol based attacks
- Application based attacks
- Amplification attacks

Protocol based attacks

1. SYN floods
2. ICMP (Internet Control Message Protocol) floods
3. Ping of death (POD)

SYN flood



- Known since 1996
- TCP three-way handshake (SYN, SYN-ACK, ACK)
- Half-open connections: SYN, SYN-ACK
- Each SYN packet mandates the server to allocate resources
- Fake/genuine IP addresses can be used to send tons of SYN packets

SYN flood

- The *Transmission Control Block* (TCB) is a transport protocol data structure that holds all the information about a connection.

- The memory footprint of a single TCB depends on what TCP options and other features an implementation provides and has enabled for a connection.

- Usually, each TCB exceeds at least 280 bytes, and in some operating systems currently takes more than 1300 bytes.

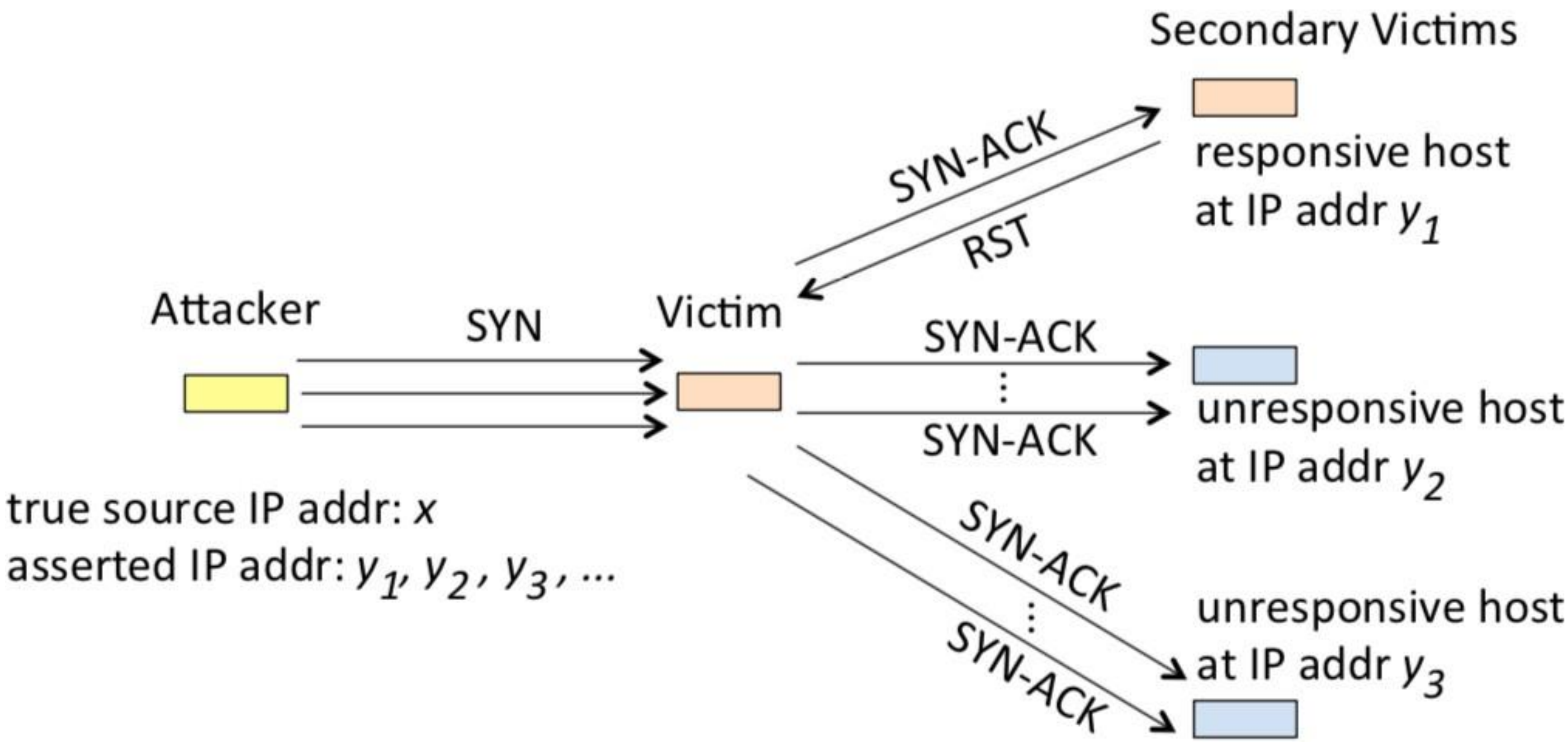


Figure 11.3: SYN flooding with spoofed IP address.

Protocol flaw

- The protocol flaw in TCP that makes SYN flooding effective is that for
  - the small cost of sending a packet, an initiator causes a relatively greater expense to the listener by forcing the listener to reserve state in a TCB.

- An excellent technique for designing protocols that are robust to this type of attack is to make the listener side operate statelessly until the initiator can demonstrate its legitimacy.

Defense: SYN Cache

- *SYN Caches*: reduce the amount of state allocated initially for a TCB generated by a received SYN, and putting off instantiating the full state.

- A hash table with a limited amount of space in each hash bucket is used to store a subset of the data that would normally go into an allocated TCB.

- If and when a handshake completing ACK is received, this data can be moved into a full TCB; otherwise the oldest bucket at a particular hash value can be reaped when needed.

- In FreeBSD, the SYN cache entry for a half connection is 160 bytes, versus 736 bytes for a full TCB

Defense: SYN Cookies

- *SYN Cookies*: zero state to be generated by a received SYN
- The most basic data comprising the connection state is compressed into the bits of the sequence number used in the SYN-ACK.
- Since for a legitimate connection, an ACK segment will be received that echoes this sequence number (+1), the basic TCB data can be regenerated and a full TCB can safely be instantiated by decompressing the ACK field.
- No storage load whatsoever on the listener, only a computational load to encode data into the SYN-ACK sequence numbers.
- The downside is that not all TCB data can fit into the 32-bit Sequence Number field, so some TCP options required for high performance might be disabled.

ICMP floods

- ICMP is used to test network status
  - Ping, traceroute tools use ICMP
  - ICMP is like UDP – no handshake necessary

- These attacks “can be” easily prevented now-a-days
  - Disable the IP-directed broadcast service at the intermediary network
  - Ingress filtering

- See also (more on DNS amplification):
  - http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack

ICMP floods / SMURF attack

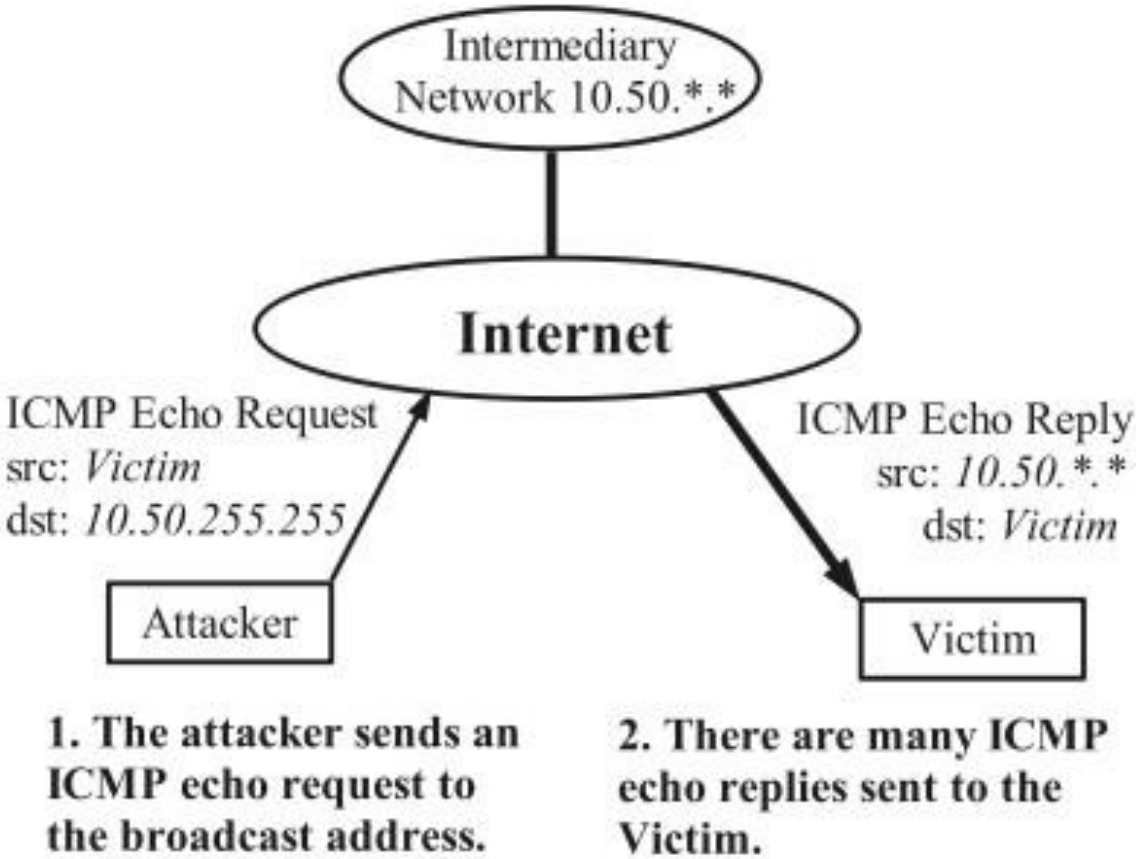
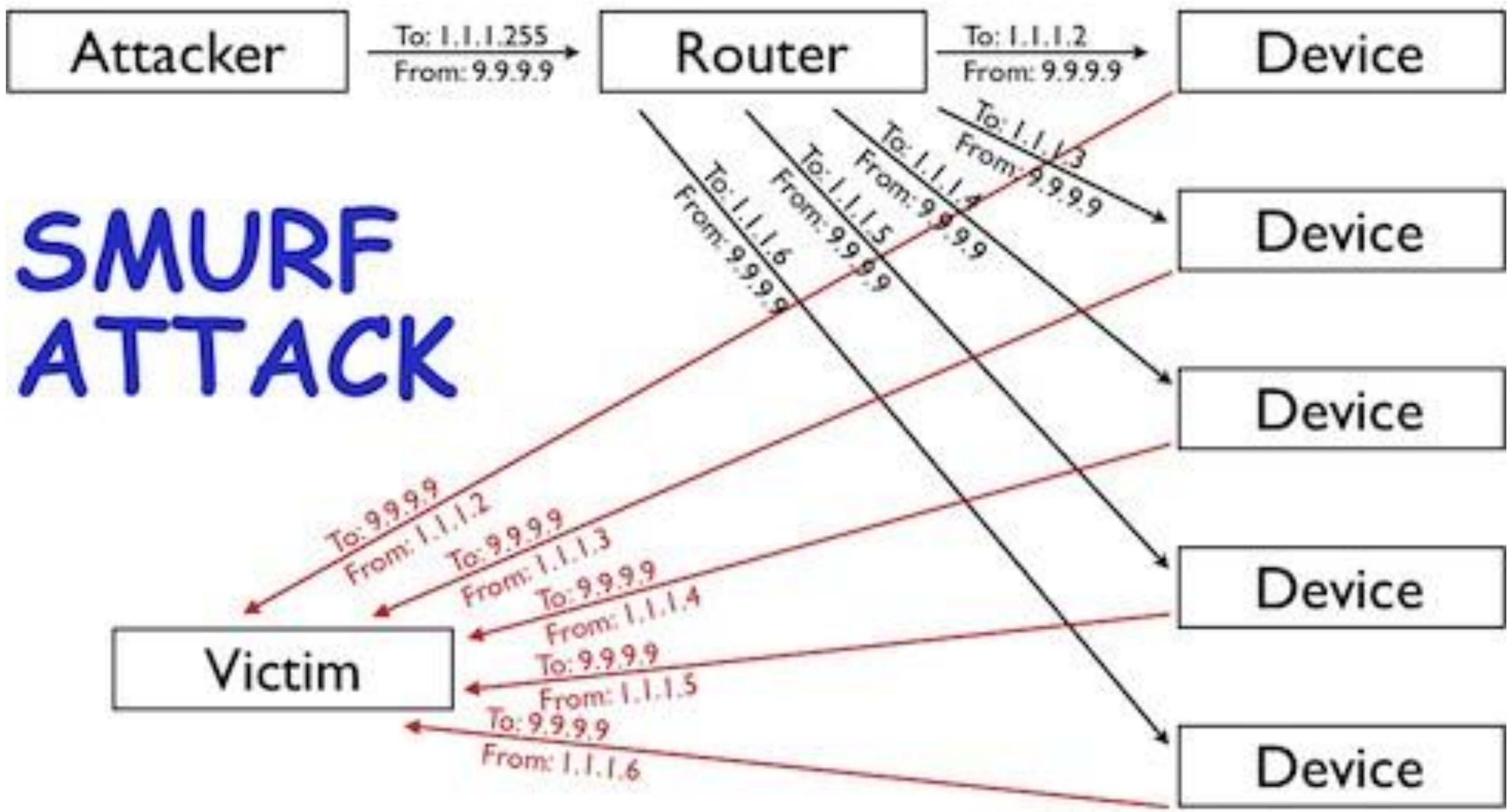


Fig. 4. A smurf attack, using an intermediary network to amplify ICMP echo requests.

Another illustration



Ping of death

- Mostly a historical attack – fixed since 1998
- Malicious ping packet to crash an OS
- Normal ping size: 84 bytes including the IP header

- Most systems could not handle ping packets larger than 65535 bytes
  - Would cause a buffer overflow
  - An early bug in most TCP/IP implementations
  - TCP/IP specification disallows packets larger than 65535 bytes
    - How to send such a packet then?

More attacks

- Teardrop
  - send a packet in fragments with fragment offset fields set such that reassembly resulted in overlapping pieces—crashing TCP/IP reassembly code in some implementations
- LAND
  - send a SYN packet with source address and port duplicating the destination values, crashing some implementations that send responses to themselves repeatedly

More attacks

- SYK-ACK flood
  - Send SYN packets to a large number of servers with the victim’s IP address (spoofed)
  - Servers respond with SYN-ACK to the victim

- UDP fragmentation
  - Send large UDP packets (>1500 bytes)
  - The victim’s bandwidth and CPU will be consumed in the process of useless reassembly