ICMP smurf attack Design Report

A. Definition of the Attack with Topology Diagram :

Definition: A smurf attack is a type of **distributed denial-of-service (DDoS)** attack that exploits **Internet Control Message Protocol (ICMP)** packets. Attackers send ICMP echo request (ping) packets to a network's broadcast address with a spoofed source IP address (the victim's IP). This causes all devices on the network to respond to the victim, overwhelming it with traffic.

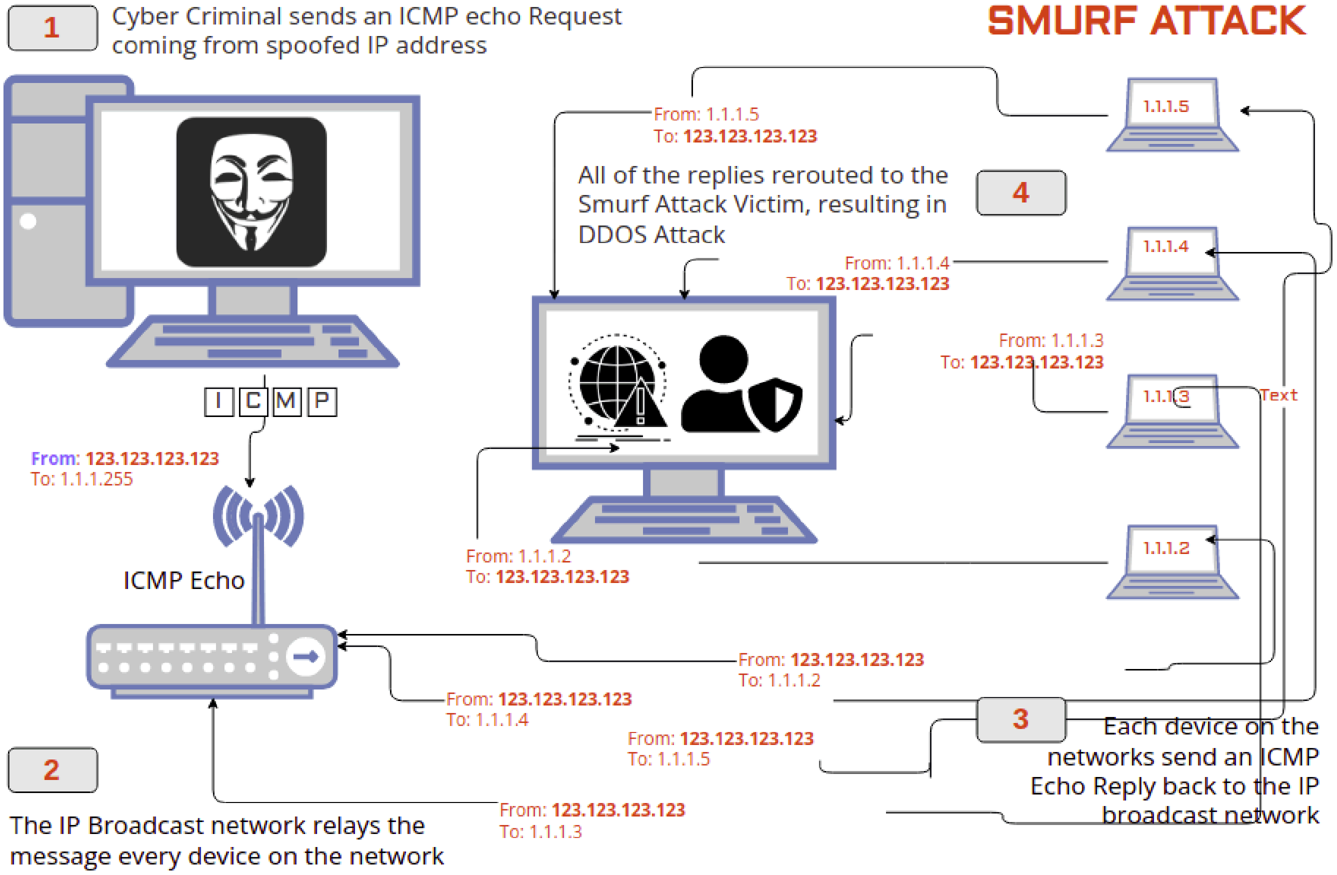


Fig: ICMP Smurf attack

How it works:

- ➢ The attacker sends ICMP Echo Request packets to a network's **broadcast address** (e.g., 192.168.1.255).
- ➢ The source IP address of these packets is **spoofed** to be the victim's IP.
- ➢ All devices on that subnet reply to the Echo Request (as per normal ICMP behavior) and send an Echo Reply to the **spoofed IP**, i.e., the **victim**.
- ➢ This **amplifies** the amount of traffic received by the victim.

Topology Diagram:

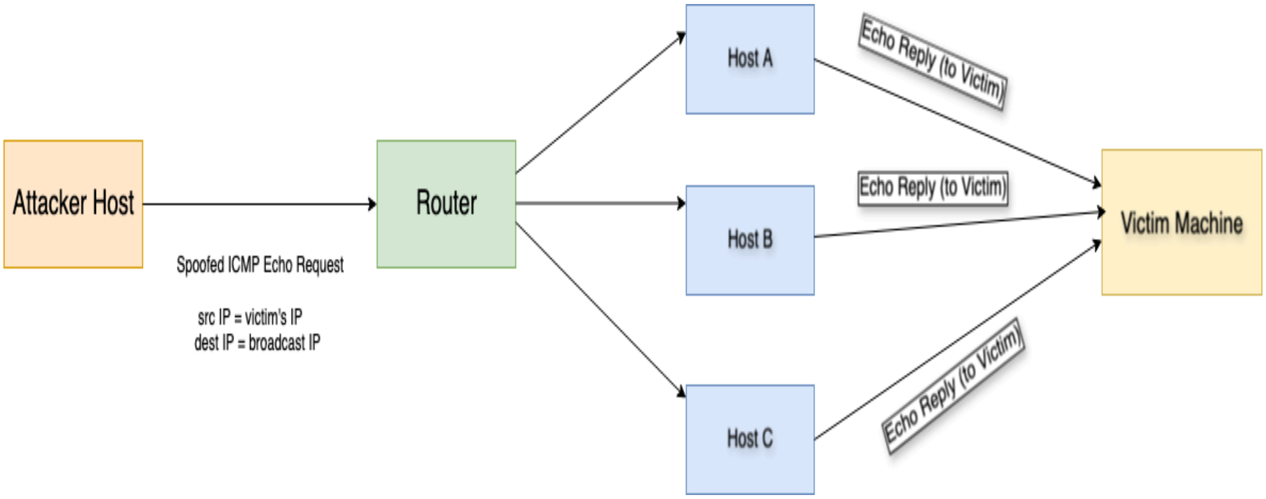


Fig : Topology diagram for ICMP smurf attack

B.Timing diagram of the original protocol and my attack timing diagram with attack strategies:

Original Timing Diagram:

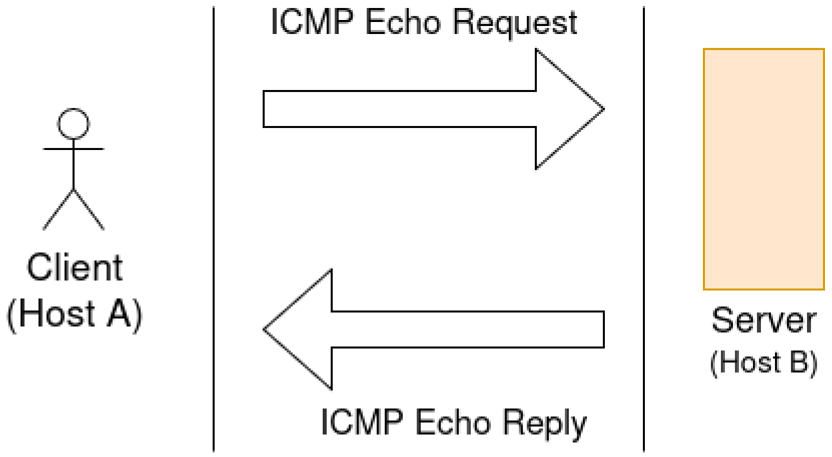


Fig:Timing diagram of the original protocol

Attack Timing Diagram:

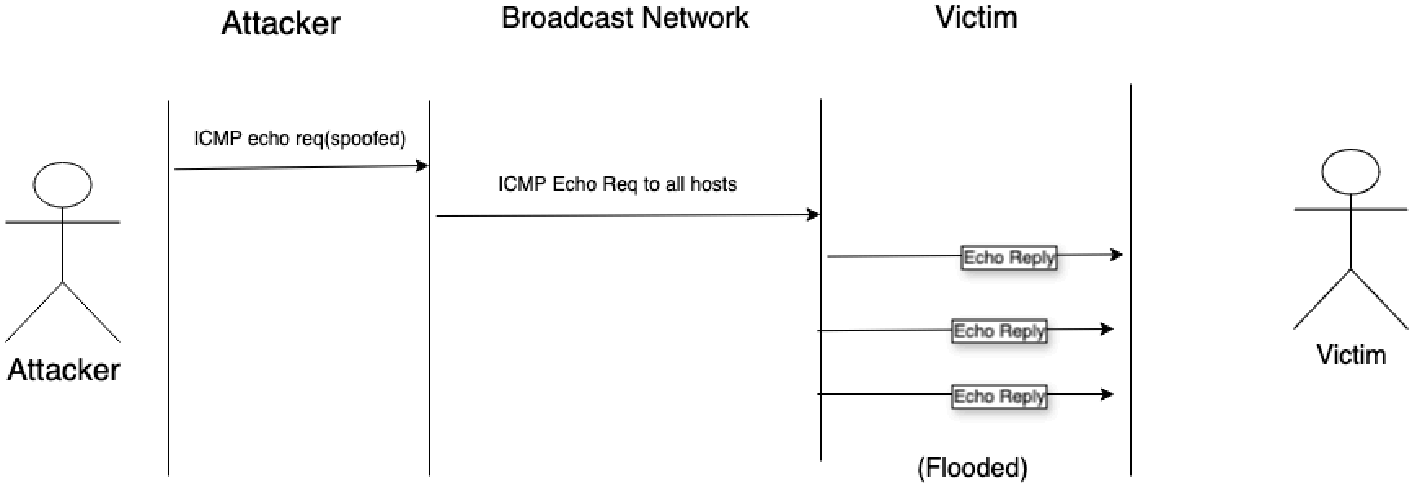


Fig:Timing diagram of the attack

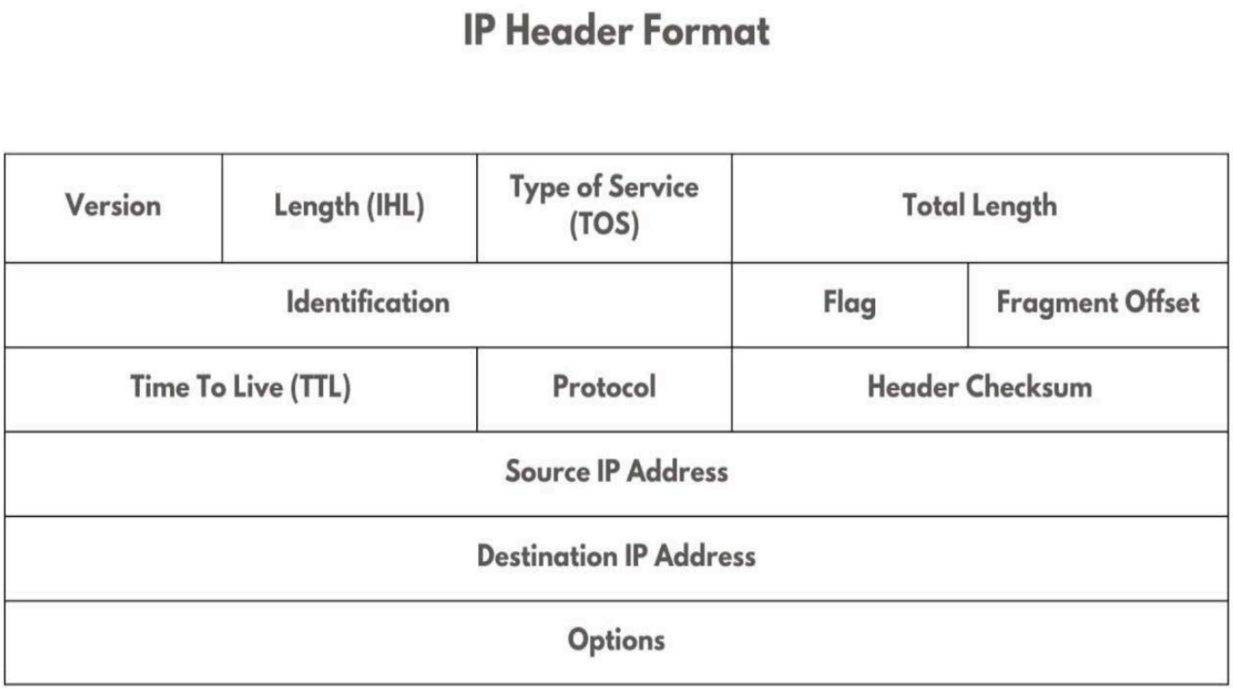
Attack Strategy:

- ➢ Spoof the victim’s IP in the Echo Request.
- ➢ Send to the broadcast address to maximize replies.
- ➢ Cause massive traffic to the victim (amplification attack).

C.Packet / Frame details for the attack and key modifications in the header:

IPv4 details:

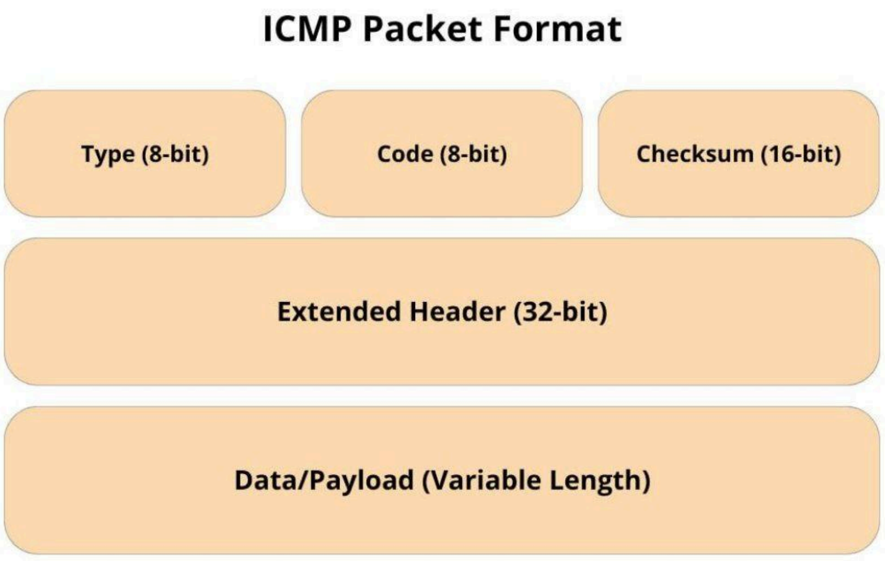
Source IP: Victim’s IP
Destination IP: Broadcast IP
Header Checksum (IP): Calculated based on the full IP header



IP Header Format

<table>
<tr><td>Version</td><td>Length (IHL)</td><td>Type of Service (TOS)</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flag</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time To Live (TTL)</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td></tr>
</table>

ICMP Echo Request Packet (Spoofed) details:
ICMP Type: 8 (Echo Request)
ICMP Code: 0
Checksum: recalculated



ICMP Echo Reply Packets (Amplification):

- Generated by **all active hosts** in the subnet.
- Sent **to Victim IP**.
- Can cause an amplification **factor** (e.g., 100x or more).

<u>Modifications / Key Points</u>

- Spoofing is key: Source IP is forged.
- Use broadcast address to trigger replies from all subnet members.

D. Justification: Why This Design Works:

- **Amplification**: A single spoofed ICMP Echo Request sent to a subnet's broadcast address reaches every host on that network. If the subnet contains N hosts, the attack traffic is amplified N times—so on a /24 network (254 hosts), one packet generates 254 replies directed at the victim.

- **IP Spoofing:** By forging the source address to be the victim's IP, all the resulting Echo Replies flood the victim rather than the attacker, concealing the attacker's identity and concentrating the traffic on the target. Since many networks lack proper ingress filtering and routers forward based solely on destination, the victim is overwhelmed without tracing back to the true source.

- **Protocol Exploitation:** ICMP Echo Requests are intended to solicit replies from every reachable device, and broadcast addresses are meant to reach all hosts on a subnet. Combining these behaviors turns ICMP into a potent DDoS mechanism, as Echo Requests to a broadcast address will trigger replies from all responding hosts.

- **Minimal Attacker Resources:** The attacker only needs to send a small volume of spoofed packets to generate a much larger flood of traffic. This efficiency makes the Smurf attack highly effective—provided the network still permits ICMP broadcasts.

Report by :

2005113 - Mohammad Ali Bhuiyan

2005119 - Sadia Afrin Sithi