CSE 406
ICMP Blind Connection Reset Attack

Nirob Arefin
Student ID:1505050
Group 3 (Section A)

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology
(BUET)
Dhaka 1000

July 30, 2019

Contents

1 Definition 2

2 Topology Diagram 2

3 Timing Diagrams 3

3.1 Timing Diagram of ICMP 3

3.2 Attack Strategies and Timing Diagram 4

4 Packet Details 6

5 Justification 6

1 Definition

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).So basically ICMP is an error detecting protocol which sends an error message to the hosts in case of some communication disturbance between them.

When hosts who are communicating over TCP protocol is handed an ICMP error message, it will perform its fault recovery function, as follows:

- If the network problem being reported is a "hard error", TCP will abort the corresponding connection.
- If the network problem being reported is a "soft error", TCP will just record this information, and repeatedly retransmit its data until they either get acknowledged, or the connection times out.

Generally a host should abort the corresponding connection when receiving an ICMPv4 error message that indicates a "hard error". One could extrapolate the concept of "hard errors" to ICMPv6 error messages of type 1 (Destination Unreachable), codes 1 (communication with destination administratively prohibited), and 4 (port unreachable).

Thus, an attacker could use ICMP to perform a blind connection-reset attack by sending any ICMP error message that indicates a "hard error" to either of the two TCP endpoints of the connection. Because of TCP's fault recovery policy, the connection would be immediately aborted.

2 Topology Diagram

' In the topology of ICMP blind-connection reset attack, the victim or client are connected to the same router, so they are in the same network. So the attacker can sniff the server ip to which the client is connected.

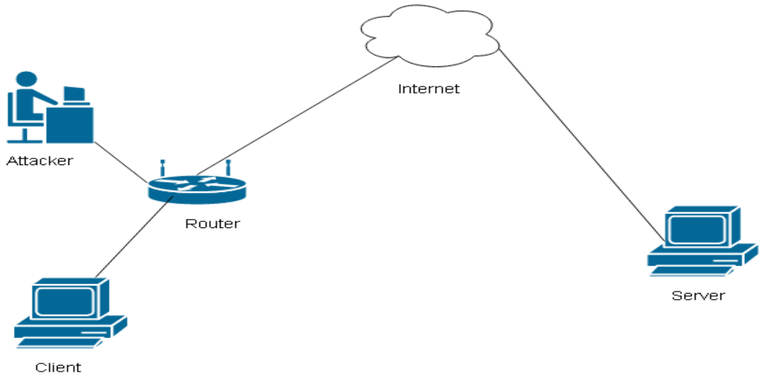

Figure 1: Topology Diagram for ICMP Blind-Connection Reset Attck .

3 Timing Diagrams

3.1 Timing Diagram of ICMP

The Ping utility is essentially a system administrator's tool that is used to see if a computer is operating and also to see if network connections are intact. Ping uses the Internet Control Message Protocol (ICMP) Echo function.This program works much like a sonar echo-location. It sends a small packet of information containing an ICMP ECHO_REUEST to a specified computer, which then sends a ECHO_REPLY packet in return.

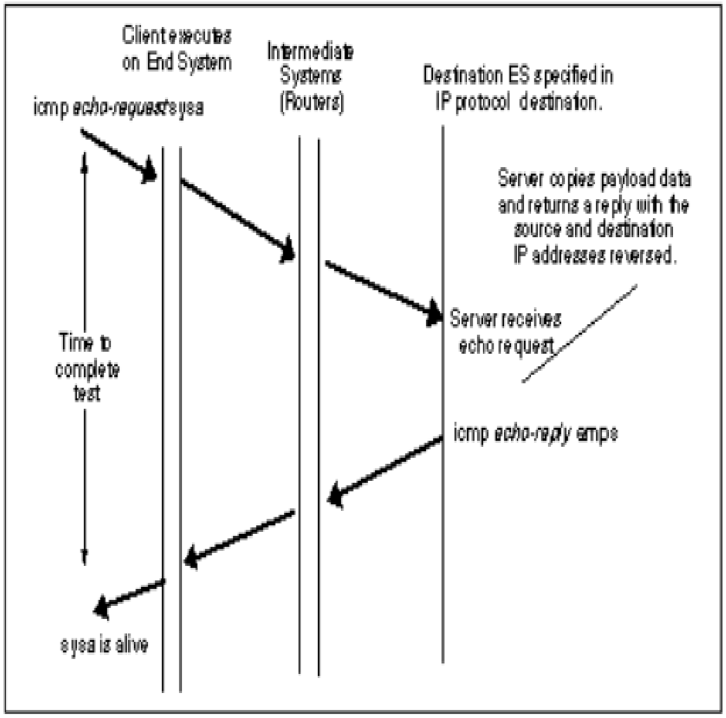

Figure 2: Use of the ping program to test whether a particular computer (”sysa”) is operational.

3.2 Attack Strategies and Timing Diagram

1. First, the client establishes a TCP connection with the server by 3-way handshaking.

2. The attacker then acquires the IP address of the server by sniffing using WireShark . So the client resets its connection and tries to connect to the server again.

3. The attacker then creates an ICMP packet using raw socket with appropriate type and code for resetting connection and with the IP address of the server as source ip in header portion of the packet.This packet will convey the message to reset the connection of the client. After receiving this message the client will reset its connection and try to connect with the server again.

4. The attacker repeats the attack and this way the connection of the client is being reset.

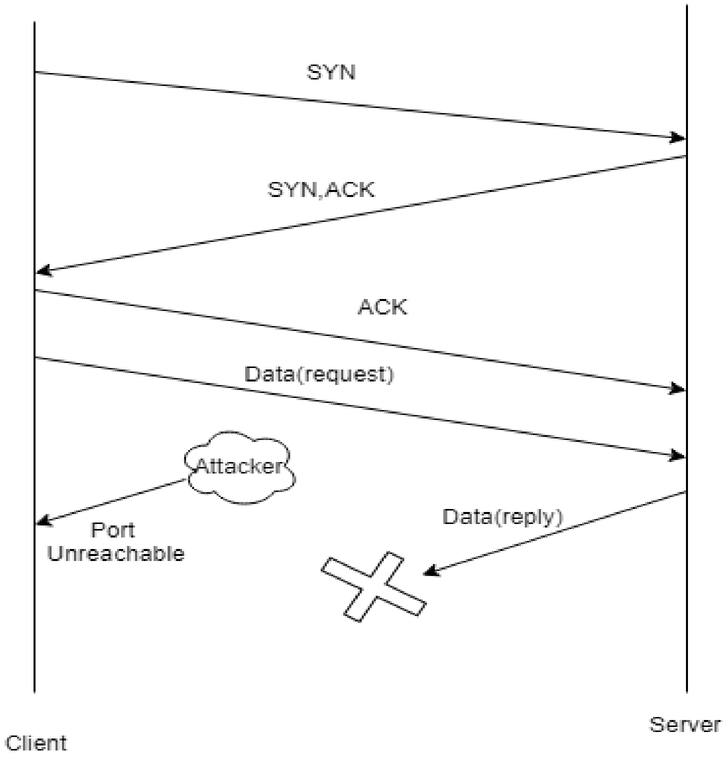

Figure 3: Attack Timing Diagram

4 Packet Details

ICMP error messages of Type: 3 represent a ”destination unreachable” situation, where code values clarify the type of unreachable. So, in ICMP message Type is set as 3. Source address and destination address are set as server address and client address respectively. These are included in the packet so that the client can not identify whether this message is from real server or not.

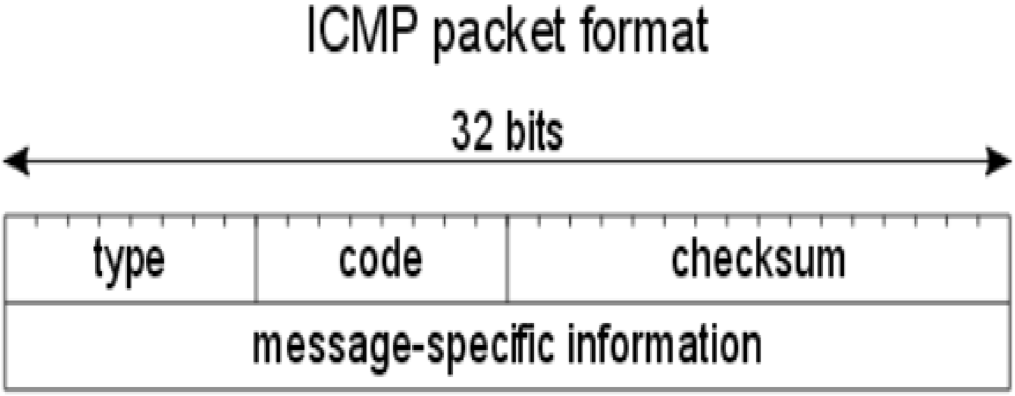

Figure 4: ICMP message format

5 Justification

Some OS, when receiving hard errors, does not disconnect the connection. In that case, it is difficult to attack. In all other cases, our design should work.