ICMP Blind Connection-Reset + Blind throughput reduction attack against TCP

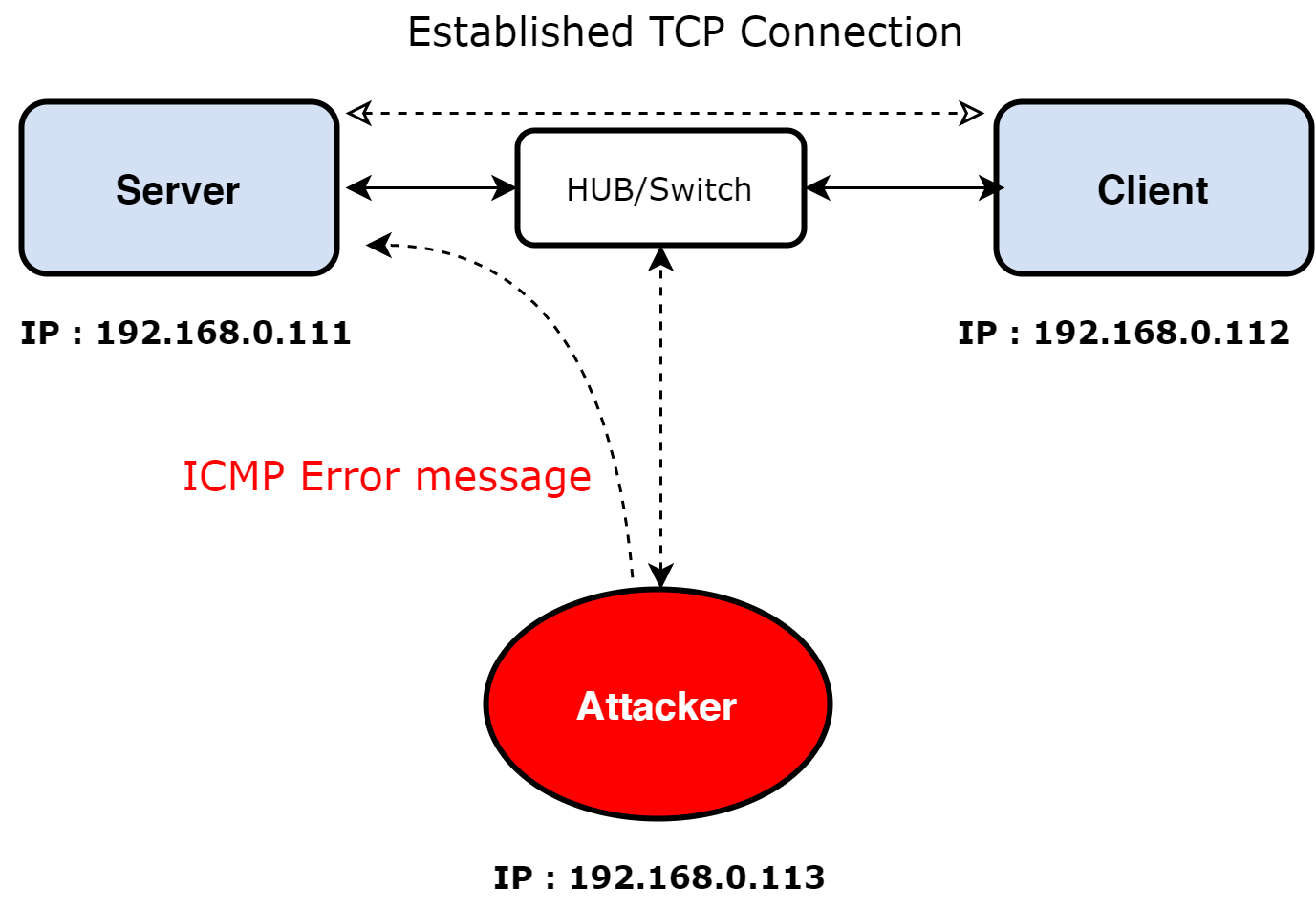
Md. Tahmidur Rafid

Student ID: 1605046

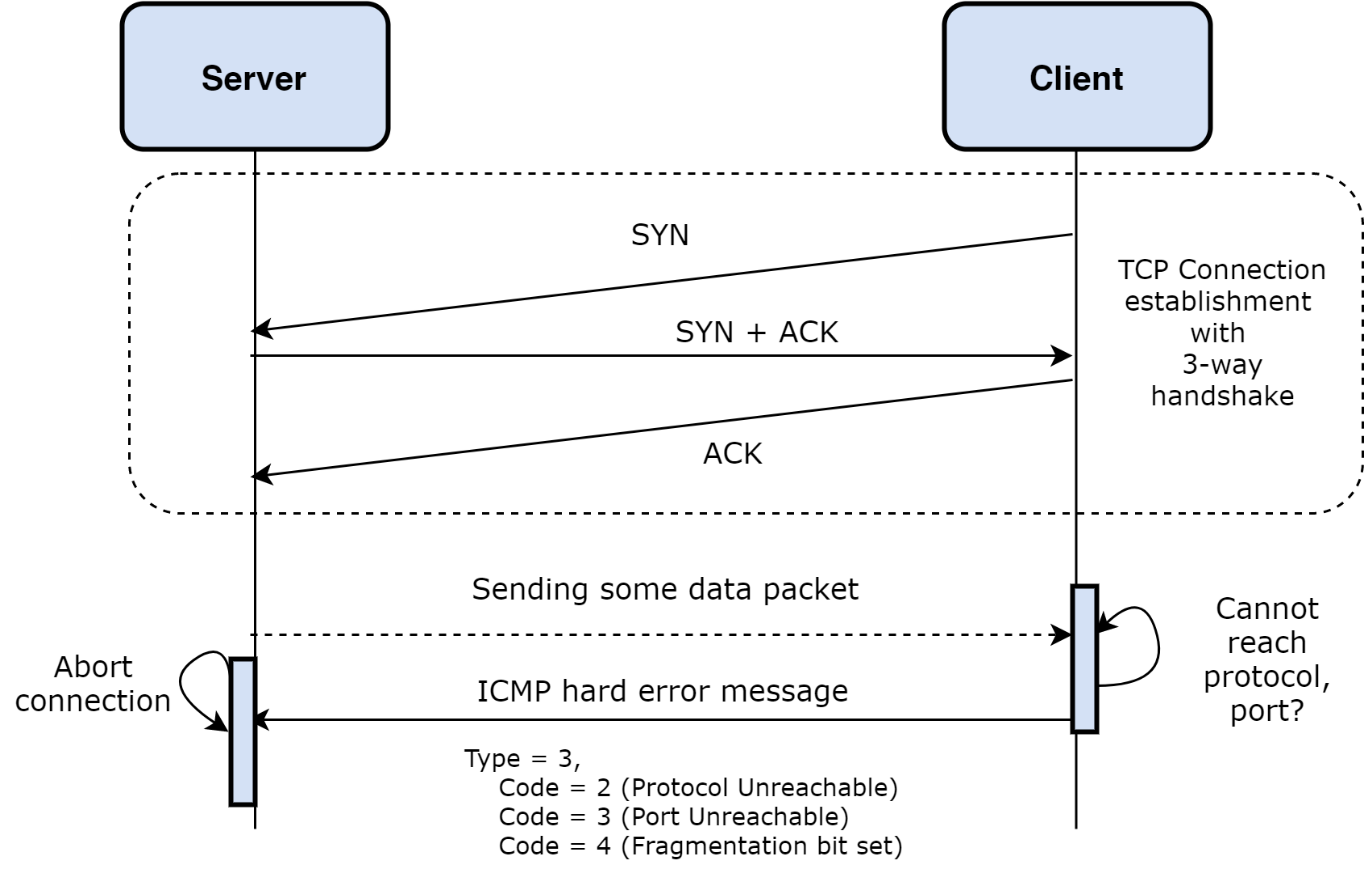
**Definition:**

ICMP Blind connection-reset attack is an attack against TCP. Using ICMP (Internet Control Messaging Protocol), communication between two hosts are performed regarding queries or informing about errors. ICMP error messages are of two types: one is hard error and another is soft error. Hard error should abort a connection. So, in ICMP Blind connection-reset attack, an attacker will send a fake ICMP hard error message to close a connection. ICMP error type 3 (Destination unreachable) with code 2 (Protocol Unreachable), 3 (Port Unreachable), 4 (Fragmentation needed) are considered as hard error. ICMP error type 4 (Source Quench) is used for congestion control mechanism. So when a sender receives a Source quench message, it will reduce the packet transmission rate, thus the throughput will be reduced.

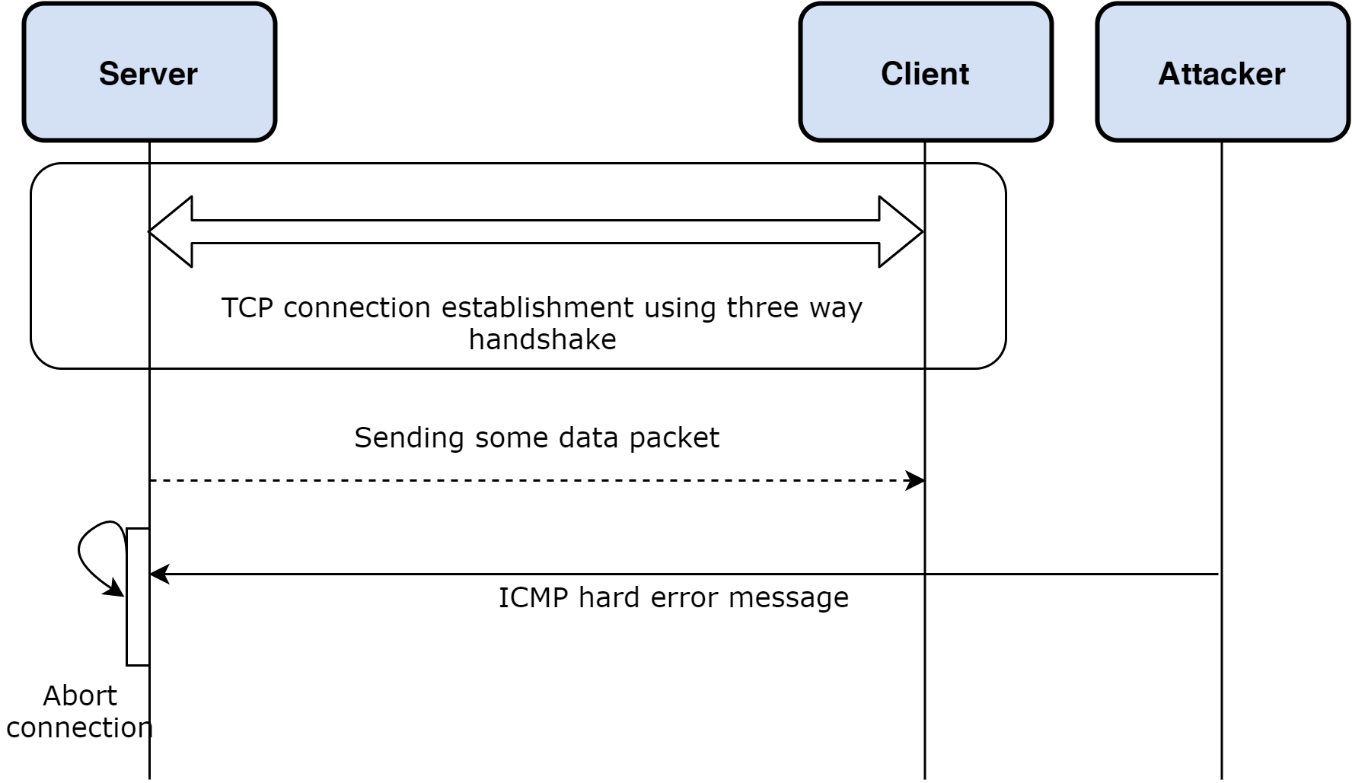
**Topology Diagram:**



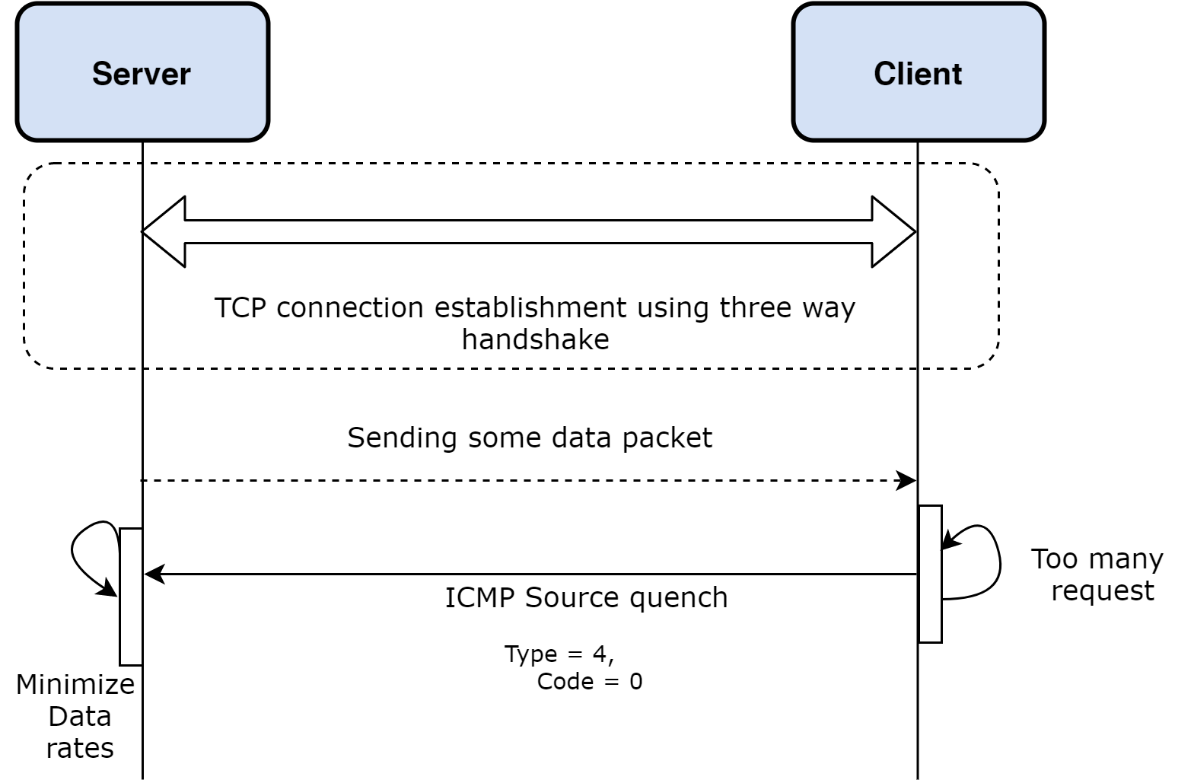
**Timing Diagram:**

****

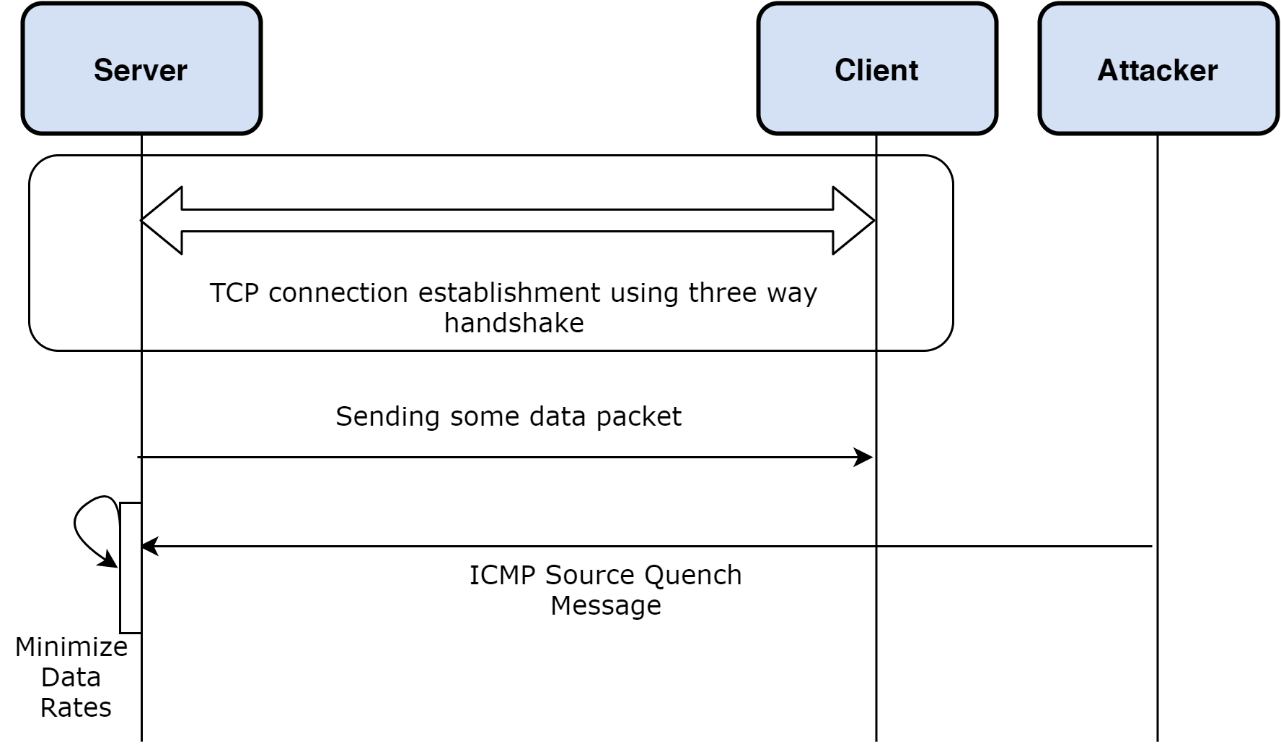
**ICMP Original Connection-reset**



**ICMP Blind Connection reset attack**

****

**ICMP Original Source Quench Message**

****

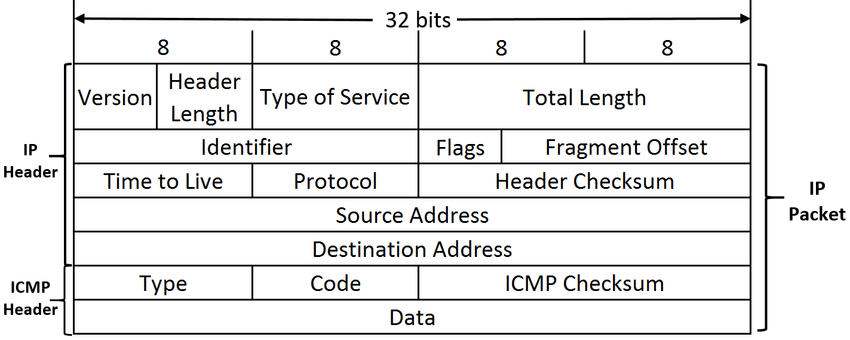
**ICMP Source Quench Attack**

**ICMP Protocol:**

ICMP (Internet Control Message Protocol) is a query and error sending protocol which is generally used to report errors regarding failure to process/send data packets to the specific hosts. The ICMP messages are divided into two types: one is for query and another is for reporting errors. The error reporting is again divided into two types: one is hard error and another is soft error. A host should abort its TCP connection in case of a hard error. Some common ICMP message types are given below:

|  |  |  |
| --- | --- | --- |
| **Type** | **Code** | **Description** |
| 3 | 0 | Destination unreachable |
| 1 | Destination host unreachable |
| 2 | Destination protocol unreachable |
| 3 | Destination port unreachable |
| 4 | Fragmentation required |
| 4 | 0 | Source Quench |
| 8 | 0 | Echo Request |

ICMP message of type 3 with error code 2, 3 and 4 are considered as hard errors. Again type 4 with code 0 is used for congestion control mechanism. When the rate of data is higher than its capacity of the corresponding router/host, source quench message is sent to reduce data rate. An ICMP packet diagram is given below:



For our attack, we will have to manually set the type and the code field with what sort of error message we want to send. We also have to manually set Source and destination IP address.

**Attacking Strategies:**

1. First we will need to know the source and the destination IP address we are targeting to attack which are usually known.
2. We will create a raw ICMP packet in our CPP code.
3. Then we will set the source and destination IP as per the system and set the type and code fields in the ICMP packet depending on which type of attack we are trying to perform.
4. For ICMP blind connection reset, we will use type 3 and code 2, 3 or 4. In case of Source Quench attack, we will use type 4 and code 0.
5. Then we will send the packet multiple times with different codes and monitor the packets on Wireshark.

**Justification:** The attacking mechanism will successfully send ICMP error packet to the desired host. But only hard errors can abort an established TCP connection. Currently ICMP hard errors are considered as soft errors in different OS and programs. So, the attack might not be successful for some systems.