Packet Sniffing and Sniffing HTTP Passwords

1. Definition

1.1 Packet Receiving and Processing

All the machines connected to a network interact with it through their Network Interface Cards (NIC). Each NIC has a hardware address called MAC address used to uniquely identify it. Common LANs like Ethernet and WiFi are broadcast medium by nature, which means all the machines are connected to a single shared medium. Each NIC on the network can detect all the frames flowing across the medium. When a NIC receives a frame through the medium, the frame is processed through the following steps:

1. NIC receives a frame and stores it in its internal memory.
2. The destination address in the frame is matched with the MAC address of the NIC. If they don't match, the frame is not intended for this machine and hence it is discarded.
3. If they do match, the frame is further copied into a buffer in the kernel called Ring buffer.
4. The NIC invokes an interrupt to inform the CPU about the arrival of this packet.
5. The CPU copies all the packets from the buffer into a queue, clearing the buffer.
6. Kernel invokes different callback handler functions to process different packets.
7. Handler functions dispatches the packets to appropriate user-space programs.

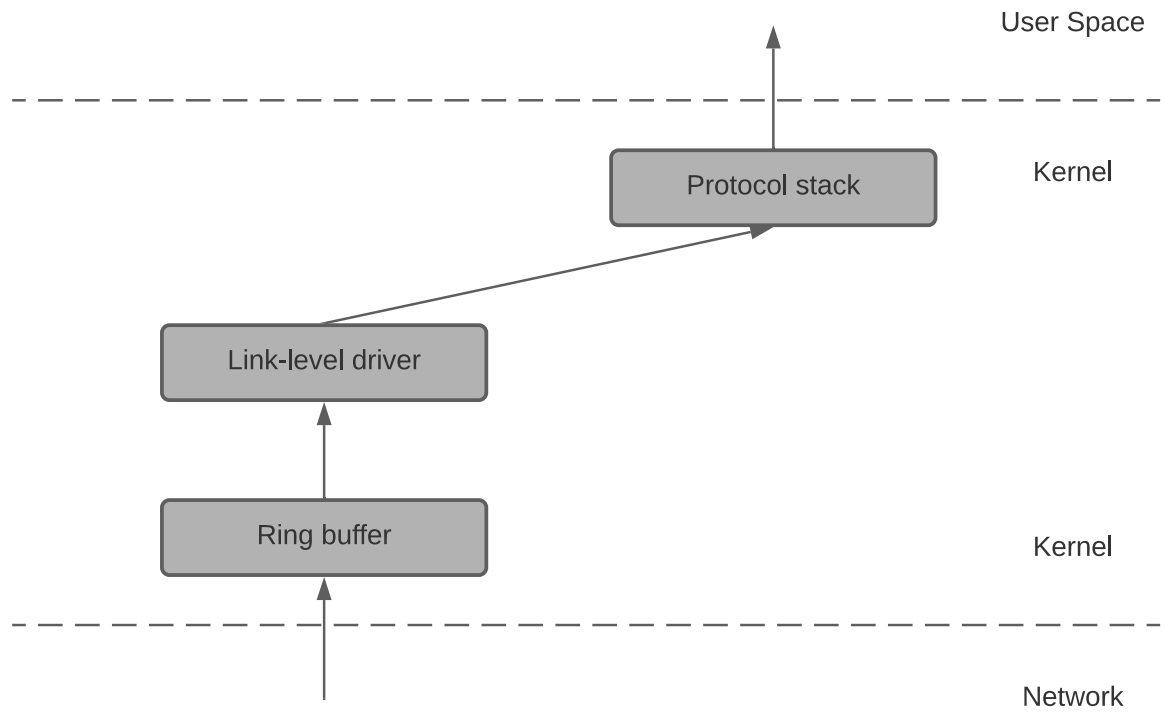

Figure 1.1: Packet flow

As mentioned above, packets whose destination address don't match with the MAC address of the NIC are discarded by default. But most of the network interface cards support a special mode called *promiscuous mode*. When this mode is activated in a wired network, NIC forwards all received frames to the kernel. A user program can be registered with the kernel to receive all these frames.

In a wireless network,. this is slightly different . Wireless devices face interference from nearby devices which can harm network performance. To avoid this, they transmit data on different channels. An NIC listens to data flowing across only one channel set up in its configuration. To get all the packets flowing across a channel, an NIC can activate a special mode called *monitor mode* (similar to promiscuous mode in wired networks). Unfortunately, most wireless NICs don't support monitor mode.

1.2 Packet Sniffing

Packet sniffing is the process of capturing live data packets as they flow across a network. Usually network administrators use it to analyze network characteristics and troubleshoot network problems. But an attacker can also use it to eavesdrop on confidential data and gain sensitive information. When packet sniffing is used for exploitation purposes, it is called packet sniffing attack.

Packet sniffing can be executed by putting the NIC of a machine into promiscuous mode and writing a user program to get all the packets flowing across a network (explained in section 1.1)

By nature, http requests and responses are not encrypted. So if confidential information like username/password is transmitted using http, an attacker machine on the same network can capture the corresponding packet and gain access to the data. In this way, hackers can employ packet sniffing attack to hack http passwords.

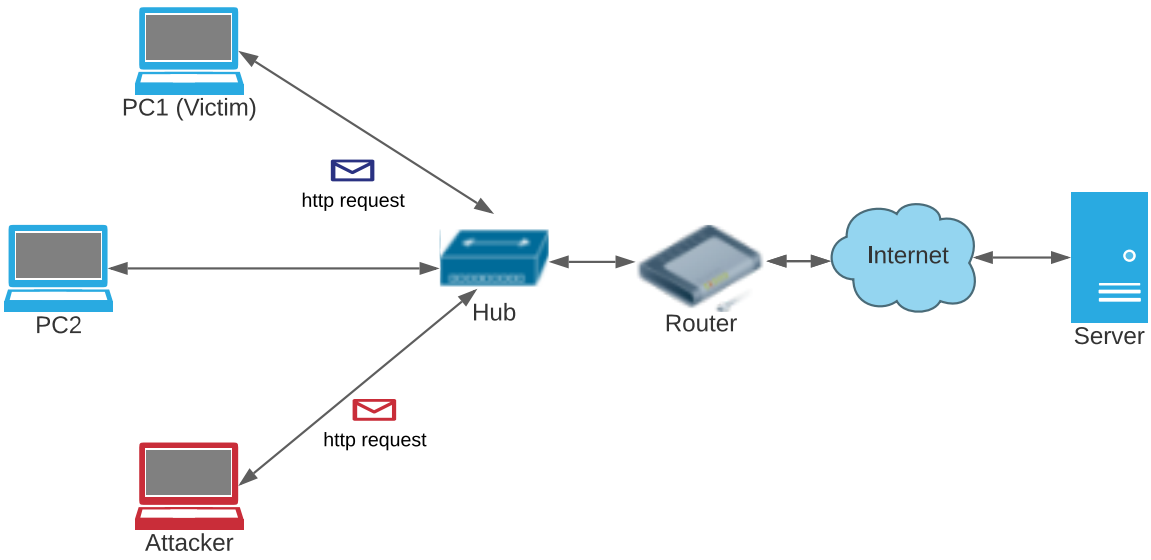

Figure 1.2: Topology Diagram of Packet Sniffing Attack

2. Timing Diagram

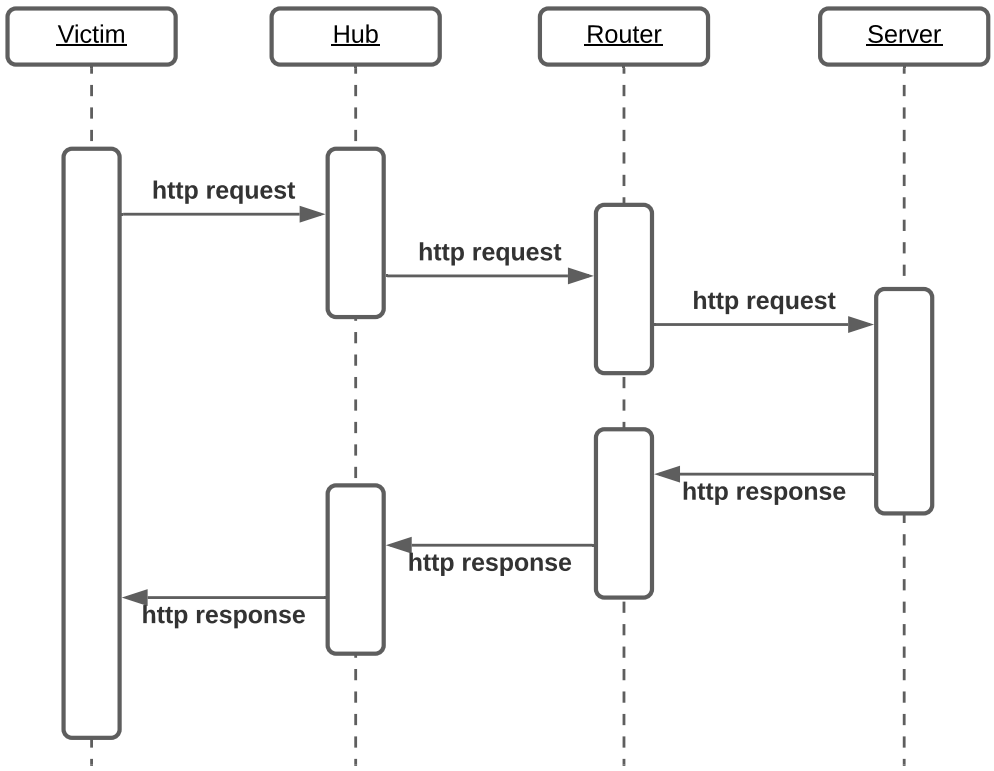

Figure 2.1: Timing Diagram of Original Protocol

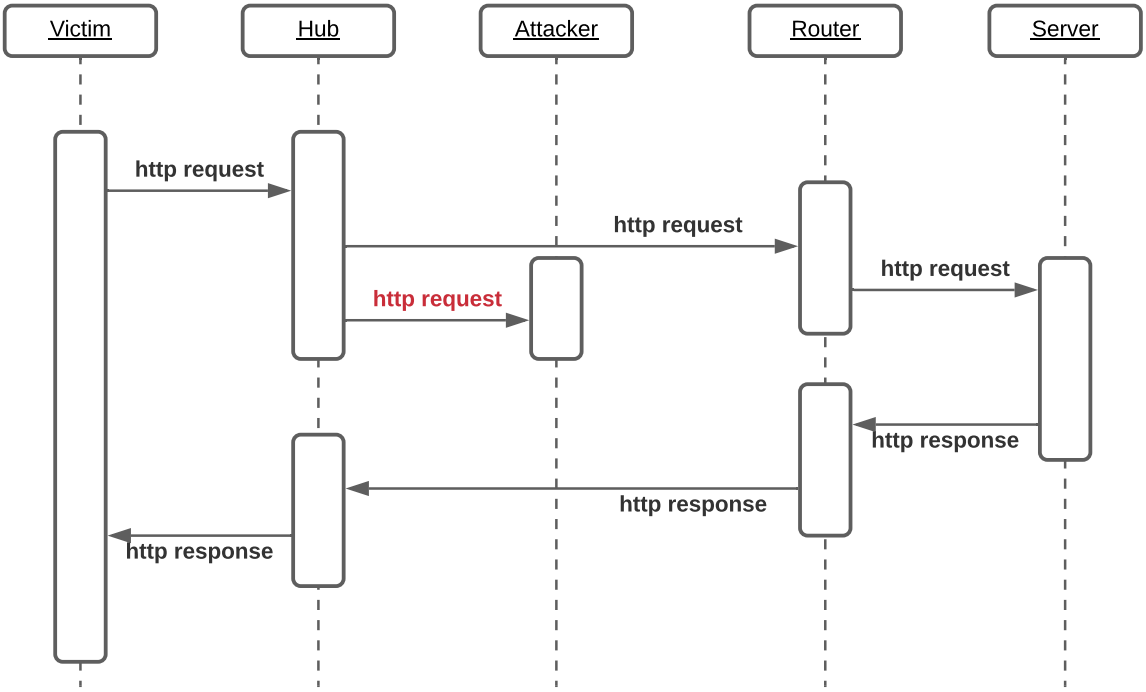

Figure 2.2: Timing Diagram of Attack

3. Frame Details

My attacking program will receive an ethernet frame from the NIC via kernel. Then I will remove the ethernet header, IP header, TCP header and finally the HTTP header. After that, I can check if the remaining http message contains my desired information. As I don't need to spoof any packet, no modification in any header is required.

Figure 3: Frame Format

4. Justification

In my program, I will first first activate the promiscuous mode in the NIC. Hence it will forward all packets flowing across the network to the kernel. Then I will create a raw socket configured to get all the packets containing http data. Next I will remove the lower-level protocol headers and get the http message. If the victim is not using https, my program will get the data unencrypted and it will be able to print the (confidential) information in the message. Thus the attack will be successful.