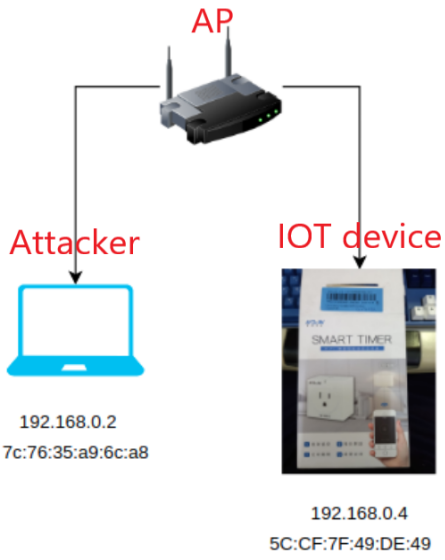
Term Project: Exploring Vulnerabilities in IoT Devices

student id: 0711282-0716077

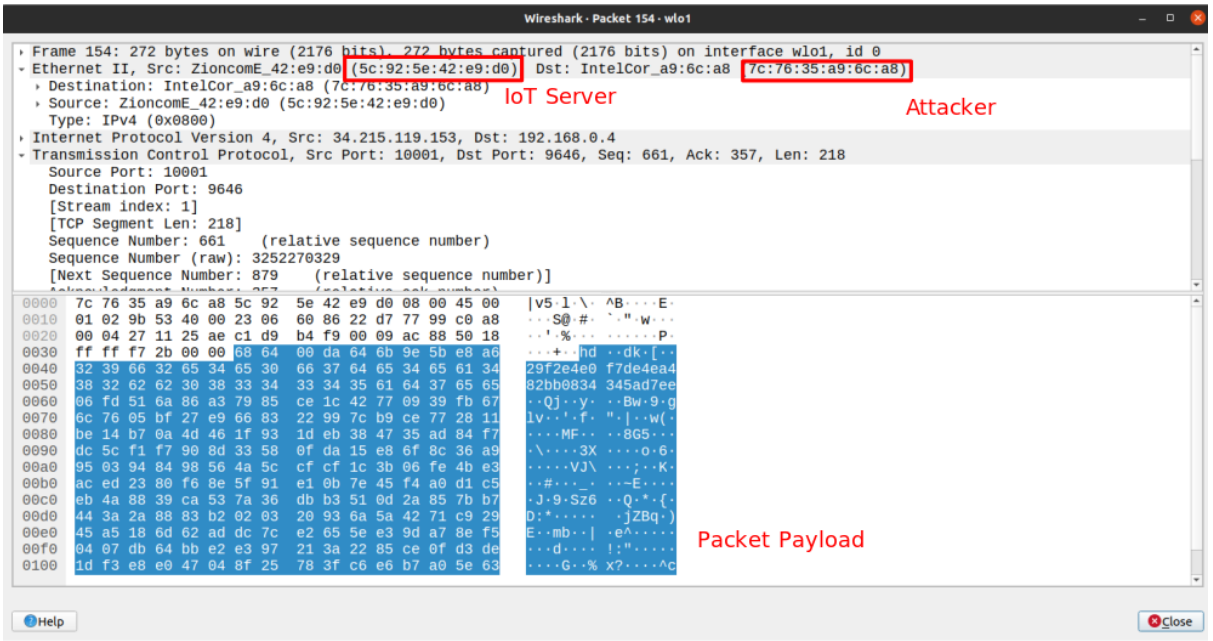
Task 1: Show how IoT communication is protected

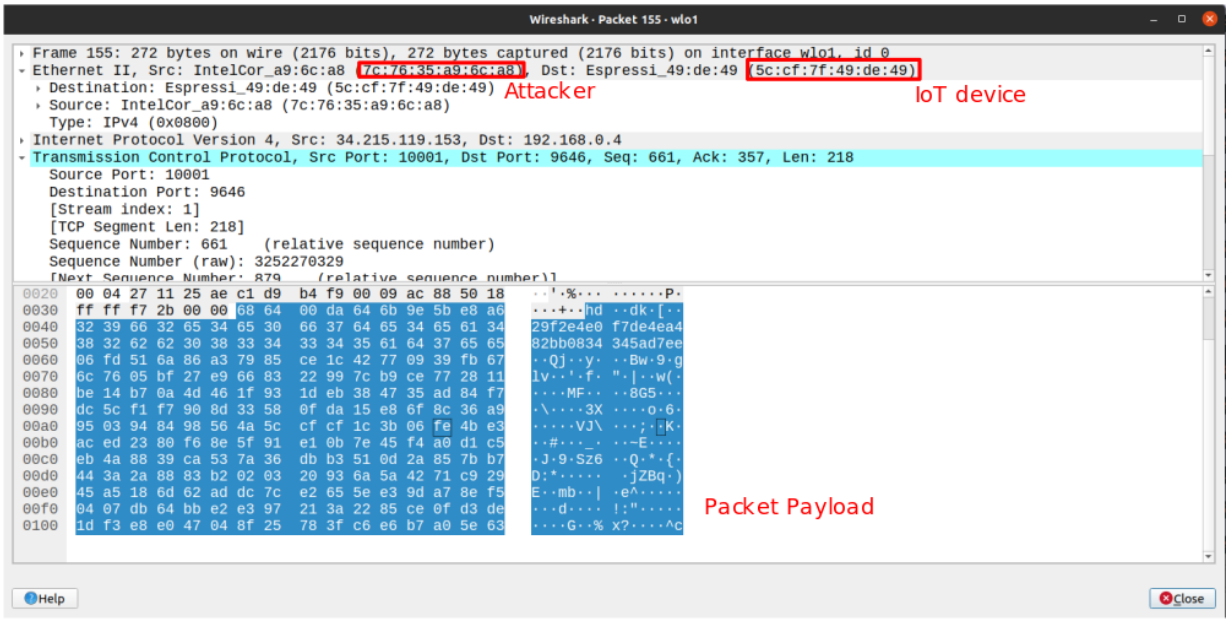
Our IoT device is smart timer call ”TE-686i 無限智能插座定時器”. First, our network scenario is:



Because we want to see the packet between an IoT device and an IoT server, we use MITM and just forward the packet to see the content of the packet. After we checking the packet payload received during MITM, we can see that it’s message is protected, so our scenario is case II.

message:





Task 2: Launch an MITM attack and examine whether it can work for the IoT device. Why yes or why no?

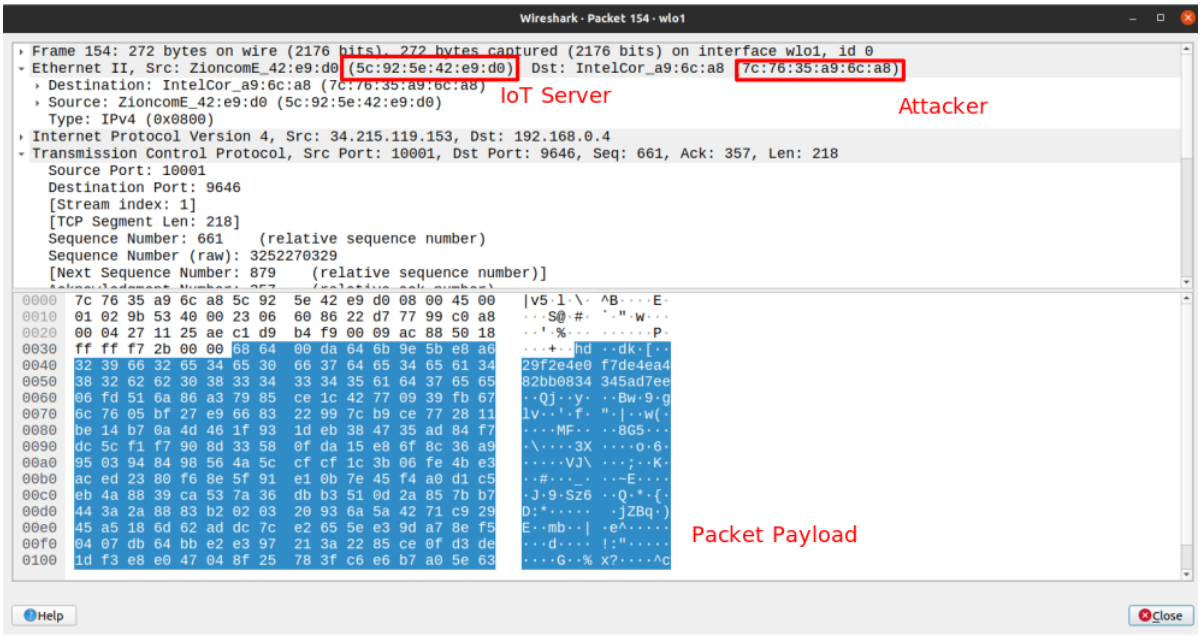
Because the definition of MITM in the spec is not specific, so if MITM is only used to monitor the packet between the IoT server and the IoT device, the answer is yes. If MITM is used to control the IoT device, the answer is no because the message is protected, we don't know what the ciphertext means.

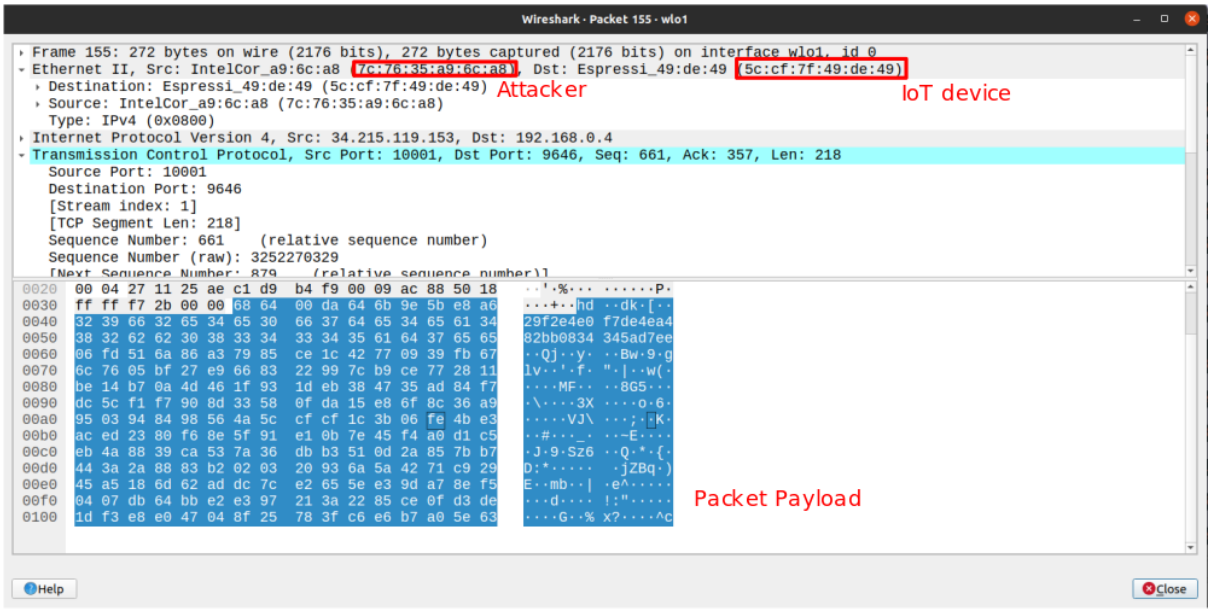
For only to monitor the packet between IoT server and IoT device, our MITM attack can launch successfully, because this IOT device works as following:

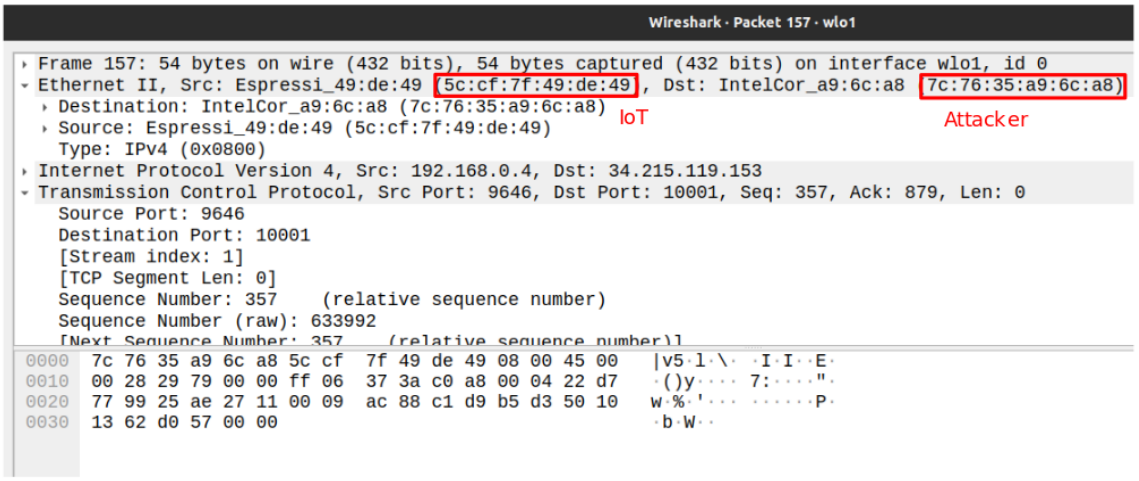
1. mobile device such as cell phone use app(YD home 2) to send signal to IOT device
2. the signal first send to it's server through Internet, then the server send it to the router
3. the router receive the packet and transmit it to IOT device

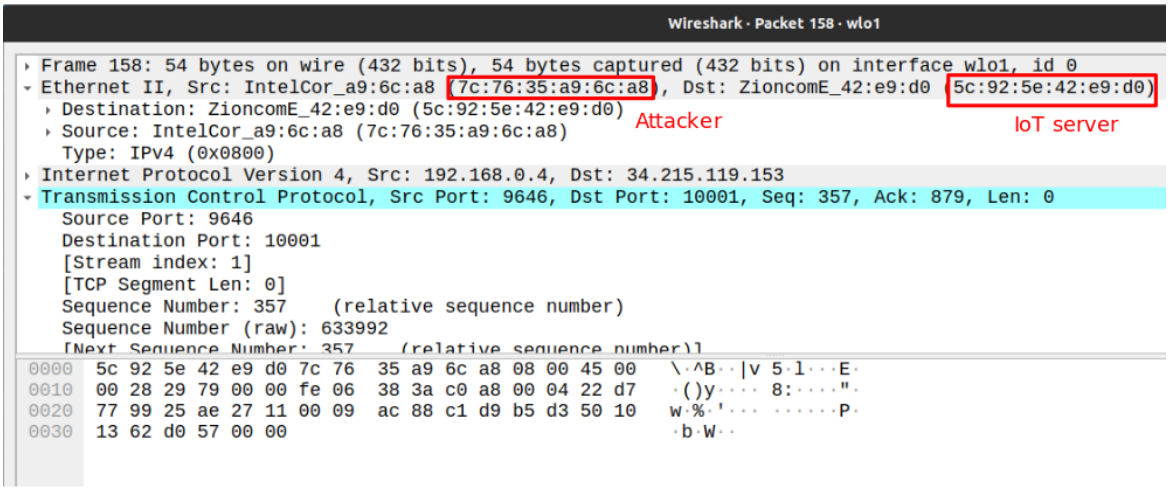
Use arp spoofing to disguise our attacker as the IOT device's mac address, so the message will first be sent to the attacker, then transmitted to the IOT device. So whether the message is protected makes no difference because we just simply forward it.

the following images is the process of monitoring the packet between the IoT device and IoT server:


Wireshark · Packet 154 · wlo1
Frame 154: 272 bytes on wire (2176 bits), 272 bytes captured (2176 bits) on interface wlo1, id 0
Ethernet II, Src: ZioncomE_42:e9:d0 (5c:92:5e:42:e9:d0), Dst: IntelCor_a9:6c:a8 (7c:76:35:a9:6c:a8)
Destination: IntelCor_a9:6c:a8 (7c:76:35:a9:6c:a8)
Source: ZioncomE_42:e9:d0 (5c:92:5e:42:e9:d0)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 34.215.119.153, Dst: 192.168.0.4
Transmission Control Protocol, Src Port: 10001, Dst Port: 9646, Seq: 661, Ack: 357, Len: 218
Source Port: 10001
Destination Port: 9646
[Stream index: 1]
[TCP Segment Len: 218]
Sequence Number: 661 (relative sequence number)
Sequence Number (raw): 3252270329
[Next Sequence Number: 879 (relative sequence number)]
IoT Server
Attacker
Packet Payload
Help
Close


Wireshark · Packet 155 · wlo1
Frame 155: 272 bytes on wire (2176 bits), 272 bytes captured (2176 bits) on interface wlo1, id 0
Ethernet II, Src: IntelCor_a9:6c:a8 (7c:76:35:a9:6c:a8), Dst: Espressi_49:de:49 (5c:cf:7f:49:de:49)
Destination: Espressi_49:de:49 (5c:cf:7f:49:de:49)
Source: IntelCor_a9:6c:a8 (7c:76:35:a9:6c:a8)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 34.215.119.153, Dst: 192.168.0.4
Transmission Control Protocol, Src Port: 10001, Dst Port: 9646, Seq: 661, Ack: 357, Len: 218
Source Port: 10001
Destination Port: 9646
[Stream index: 1]
[TCP Segment Len: 218]
Sequence Number: 661 (relative sequence number)
Sequence Number (raw): 3252270329
Attacker
IoT device
Packet Payload
Help
Close


Wireshark · Packet 157 · wlo1
Frame 157: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlo1, id 0
Ethernet II, Src: Espressi_49:de:49 (5c:cf:7f:49:de:49), Dst: IntelCor_a9:6c:a8 (7c:76:35:a9:6c:a8)
Destination: IntelCor_a9:6c:a8 (7c:76:35:a9:6c:a8)
Source: Espressi_49:de:49 (5c:cf:7f:49:de:49)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 34.215.119.153
Transmission Control Protocol, Src Port: 9646, Dst Port: 10001, Seq: 357, Ack: 879, Len: 0
Source Port: 9646
Destination Port: 10001
[Stream index: 1]
[TCP Segment Len: 0]
Sequence Number: 357 (relative sequence number)
Sequence Number (raw): 633992
IoT
Attacker



Moreover, What happens if we do not forward the packet? The packet would stop at the attacker's device and the IoT device would not receive the command. We recorded the video so you can understand it ! 😀

👇👇👇

[CSC term project video]