

Term Project

0711529 陳冠儒

Device: ASUS AI800M PRO

1. Device Information



From the app of the IoT device, we can find the mac address of it,
0c:9d:92:05:00:7e.

2. ARP Spoofing

I use my windows 10 as attacker, and the IoT and the attack use the same wi-fi. The attacker IP: 192.168.0.23, attacker mac address: d8-c4-97-c2-cf-f2. The IoT IP: 192.168.0.45 (get by the ip scanning), IoT mac address: 0c:9d:92:05:00:7e.

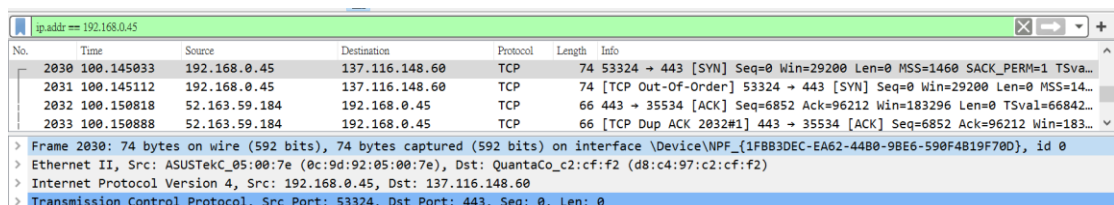


Figure 1. Victim IoT to Attacker

No.	Time	Source	Destination	Protocol	Length	Info
2030	100.145033	192.168.0.45	137.116.148.60	TCP	74	53324 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva...
2031	100.145112	192.168.0.45	137.116.148.60	TCP	74	[TCP Out-Of-Order] 53324 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=14...
2032	100.150818	52.163.59.184	192.168.0.45	TCP	66	443 → 35534 [ACK] Seq=6852 Ack=96212 Win=183296 Len=0 TSval=66842...
2033	100.150888	52.163.59.184	192.168.0.45	TCP	66	[TCP Dup ACK 2032#1] 443 → 35534 [ACK] Seq=6852 Ack=96212 Win=183...

> Frame 2031: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{1FBB3DEC-EA62-44B0-9BE6-590F4819F70D}, id 0

> Ethernet II, Src: QuantaCo_c2:cf:f2 (d8:c4:97:c2:cf:f2), Dst: ZioncomE_85:ae:b0 (f4:28:53:85:ae:b0)

> Internet Protocol Version 4, Src: 192.168.0.45, Dst: 137.116.148.60

> Transmission Control Protocol, Src Port: 53324, Dst Port: 443, Seq: 0, Len: 0

Figure 2. Attacker to AP

No.	Time	Source	Destination	Protocol	Length	Info
2030	100.145033	192.168.0.45	137.116.148.60	TCP	74	53324 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva...
2031	100.145112	192.168.0.45	137.116.148.60	TCP	74	[TCP Out-Of-Order] 53324 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=14...
2032	100.150818	52.163.59.184	192.168.0.45	TCP	66	443 → 35534 [ACK] Seq=6852 Ack=96212 Win=183296 Len=0 TSval=66842...
2033	100.150888	52.163.59.184	192.168.0.45	TCP	66	[TCP Dup ACK 2032#1] 443 → 35534 [ACK] Seq=6852 Ack=96212 Win=183...

> Frame 2032: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1FBB3DEC-EA62-44B0-9BE6-590F4819F70D}, id 0

> Ethernet II, Src: ZioncomE_85:ae:b0 (f4:28:53:85:ae:b0), Dst: QuantaCo_c2:cf:f2 (d8:c4:97:c2:cf:f2)

> Internet Protocol Version 4, Src: 52.163.59.184, Dst: 192.168.0.45

> Transmission Control Protocol, Src Port: 443, Dst Port: 35534, Seq: 6852, Ack: 96212, Len: 0

Figure 3. AP to Attacker

No.	Time	Source	Destination	Protocol	Length	Info
2030	100.145033	192.168.0.45	137.116.148.60	TCP	74	53324 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva...
2031	100.145112	192.168.0.45	137.116.148.60	TCP	74	[TCP Out-Of-Order] 53324 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=14...
2032	100.150818	52.163.59.184	192.168.0.45	TCP	66	443 → 35534 [ACK] Seq=6852 Ack=96212 Win=183296 Len=0 TSval=66842...
2033	100.150888	52.163.59.184	192.168.0.45	TCP	66	[TCP Dup ACK 2032#1] 443 → 35534 [ACK] Seq=6852 Ack=96212 Win=183...

> Frame 2033: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1FBB3DEC-EA62-44B0-9BE6-590F4819F70D}, id 0

> Ethernet II, Src: QuantaCo_c2:cf:f2 (d8:c4:97:c2:cf:f2), Dst: ASUSTek_05:00:7e (0c:9d:92:05:00:7e)

> Internet Protocol Version 4, Src: 52.163.59.184, Dst: 192.168.0.45

> Transmission Control Protocol, Src Port: 443, Dst Port: 35534, Seq: 6852, Ack: 96212, Len: 0

Figure 4. Attacker to Victim IoT

3. MITM Attack

265	28.592624	40.90.184.240	192.168.0.45	TLSv1.2	1514	Server Hello, Certificate
266	28.592624	40.90.184.240	192.168.0.45	TLSv1.2	338	Server Key Exchange, Server Hello Done
267	28.592686	40.90.184.240	192.168.0.45	TCP	1514	[TCP Out-Of-Order] 8443 → 38648 [ACK] Seq=1 Ack=518 Win=64768 Len=1448 TSval=2790...
268	28.592686	40.90.184.240	192.168.0.45	TCP	338	[TCP Retransmission] 8443 → 38648 [PSH, ACK] Seq=1449 Ack=518 Win=64768 Len=272 T...
269	28.625789	192.168.0.45	40.90.184.240	TCP	66	38648 → 8443 [ACK] Seq=518 Ack=1449 Win=32096 Len=0 TSval=2872967 TSecr=2790054047
270	28.625833	192.168.0.45	40.90.184.240	TCP	66	[TCP Dup ACK 269#1] 38648 → 8443 [ACK] Seq=518 Ack=1449 Win=32096 Len=0 TSval=287...
271	28.647267	192.168.0.45	40.90.184.240	TCP	66	38648 → 8443 [ACK] Seq=518 Ack=1721 Win=35008 Len=0 TSval=2872968 TSecr=2790054047
272	28.647267	192.168.0.45	40.90.184.240	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
273	28.647354	192.168.0.45	40.90.184.240	TCP	66	38648 → 8443 [ACK] Seq=518 Ack=1721 Win=35008 Len=0 TSval=2872968 TSecr=2790054047
274	28.647354	192.168.0.45	40.90.184.240	TCP	192	[TCP Retransmission] 38648 → 8443 [PSH, ACK] Seq=518 Ack=1721 Win=35008 Len=126 T...
275	28.723472	40.90.184.240	192.168.0.45	TCP	66	8443 → 38648 [ACK] Seq=1721 Ack=644 Win=64768 Len=0 TSval=2790054176 TSecr=2872971
276	28.723472	40.90.184.240	192.168.0.45	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
277	28.723542	40.90.184.240	192.168.0.45	TCP	66	8443 → 38648 [ACK] Seq=1721 Ack=644 Win=64768 Len=0 TSval=2790054176 TSecr=2872971
278	28.723542	40.90.184.240	192.168.0.45	TCP	308	[TCP Retransmission] 8443 → 38648 [PSH, ACK] Seq=1721 Ack=644 Win=64768 Len=242 T...
279	28.749822	192.168.0.45	40.90.184.240	TLSv1.2	1036	Application Data

Application data using the TLSv1.2 to transfer, so it's difficult to do the MITM attack.