System Security (201700086)
IoT #1 - passive protocol analysis for the lightbulb

Æde Symen Hoekstra, Luigi Coniglio (Group 24)

May 17, 2018

1 Capture

During the lab session we were able to capture multiple traces including both the packets the command from the cloud to the device that switches the light on, and the command that switches the light off. This was done by running the following command on the access point:

```
$ tcpdump -s0 -w - -i br-milight
```

We provided one trace together with this report.

2 Analysis

In order to analyze the traces we inspected the captures using wireshark. Figure 1 shows the content of the data sent from the cloud to the device. We were able determine which payload triggered which action by simply associating the timing.

3 Results

Figure 2 shows which payloads are sent by the cloud to switch on and off the lamp. After diffing the payloads we can deduce that the bytes highlighted in red are most probably meant to encode the on/off action. When those bytes are are 0x02 and 0x3f respectively the lamp will switched off, when the bytes are 0x01 and 0x3e the lamp will be switched on.

The protocol used to communicate with the lamp doesn't provide any level of security: an attacker could simply encode a similar payload and send it to the lamp in order to control it.

We also noticed the presence of what seems to be a counter (highlighted in blue): an attacker would also need to guess a correct value for this counter in order to send a valid command to the lamp. This could be done by capturing the traffic on the network in order to retrieve the current value of the counter or by simply brute-forcing it.

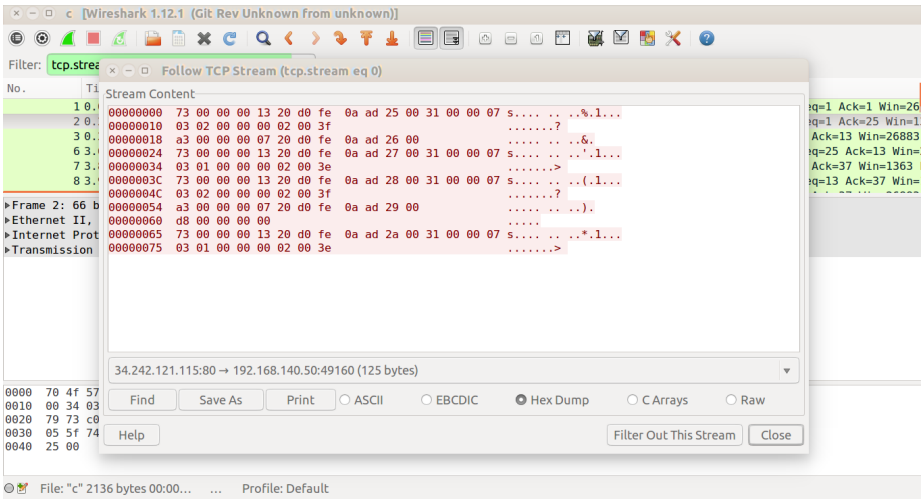

Figure 1: Commands send from the server to the lamp

1525351814.61	34.242.121.115	730000001320D0FE0AAD2500310000070302000000020003F	OFF
1525351818.29	34.242.121.115	A30000000720D0FE0AAD2600	
1525351820.90	34.242.121.115	730000001320D0FE0AAD2700310000070301000000020003E	ON
1525351826.09	34.242.121.115	730000001320D0FE0AAD2800310000070302000000020003F	OFF
1525351826.28	34.242.121.115	A30000000720D0FE0AAD2900	
1525351826.44	34.242.121.115	D800000000	
1525351830.84	34.242.121.115	730000001320D0FE0AAD2A00310000070301000000020003E	ON

Figure 2: Differential analysis of the payloads.