Dylan Use Case

**Persona**:

Alice is the owner of the coffee shop *C@ff1n3 Dr3@ms,* and she uses Home Assistant (HA) to control her businesses IoT devices. The IoT devices she uses at the coffee shop are a smart thermostat, and a smart utility meter to help regulate the climate control system and monitor her business’ power consumption. The power meter will adjust the climate control systems heating and cooling program to stop it from using to much power during peak times.

**Attacker**:

Bob is a disgruntled barista that is upset with how busy the coffee shop is, and that he does not get the days off that he wants. To help solve his issue of being too busy without enough help, Bob decides to buy the same smart thermostat and utility meter. Since Alice puts all her IoT devices on the same wi-fi network that she lets the guests use, Bob is easily aware of the password to the network. As he adds the devices to the network, Home Assistant notices them on the network and adds them to its list of devices. Since HA communicates to the devices via mDNS (a UDP based protocol) HA does not get back an acknowledgement that the message went to the correct device.

Bob switches the hostname on the original smart thermostat (Thermostat A) with the one he bought (Thermostat B) but does not attach Thermostat B to the climate control system. The result is that when HA changes the temperature to match the heating or cooling program the climate system does not respond to the message, as Thermostat B receives the mDNS packet for this. This causes guests to leave the coffee shop due to the climate being uncomfortable. Bob hides Thermostat B inside the coffee shop so that HA will still notice it on the network, but in a place that Alice is unlikely to find it.

Bob does a similar malicious action with the smart utility meter. Switching the hostnames with the one he bought and hides the one he bought within the coffee shop so that HA does not notice it is gone. The result is that the original utility meter will continue to receive messages to lower the power consumption from the smart thermostat. Since the original meter is not connected to the utility lines it will not be able to shutdown the higher than ordered power consumption.

**Security Requirement to mitigate risk:**

1. To mitigate this risk MFA for adding any new device to the HA system needs to be implemented. This will stop rogue IoT devices from being added without the system owner’s knowledge.
2. To mitigate the risk of this mDNS attack, change the method that HA communicates to the IoT devices to TCP. Changing to TCP would allow HA to receive back an acknowledgement that the message was received by the correct hostname. This will require changing from mDNS to DNS as a means of sending out packets from HA to the IoT devices.
   1. HA could also verify the DNS packets via MAC addresses instead of hostnames.