CSC7078 Secure IoT Communications 40313770 Kevin Brolly

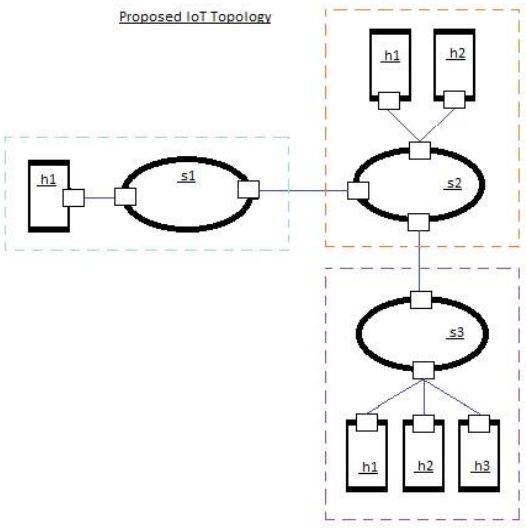
Scenario

A healthcare business would like to implement IoT devices into their infrastructure as an RFID based patient chart due to the inexpensive nature and speed of deployment, they are keen to implement. However there have been concerns deploying such devices due to issues concerning data protection and personal information such as:
Lack of device support via firmware/security updates.
Weak / default credentials.
Device specification limits security measures.
Issues of maintainability.
These issues make IoT suitable attack vectors for botnets such as Mirai and its variants that can be used as part of a DDoS attack. They have decided that the IoT devices will be configured for ethernet connection to minimise attack vectors.

Solution

To protect this IoT network and greater business network a firewall will be developed to restrict IoT communications by creating a policy to differentiate between authorised and unauthorised network communications.
To assess whether a DDoS attack originates from the IoT network and enact policy protecting the remaining network.

Design/Analysis Requirements



To enact the proposed firewall solution the IoT network I will
deny all traffic from hosts associated with S1.
Deny UDP traffic from hosts on S2.
Hosts on S3 will be prevented from cross communication.

As the firewall will prevent UDP traffic to S3 to detect a TCP SYN attack I will
Monitor TCP SYN packets.
Count them.
Enact policy based on predefined threshold.

Implement background traffic to test solution performance outside of a vacuum.

Figure 1.: Depicts s1 as part of greater business network, s2 hosts maintain the IoT devices on S3.

To demonstrate my solution I will adapt an existing topology as seen in Figure 1., create traffic via hping3, build in SDNCockpit as it provides a multiplexer with traffic generator, Mininet terminal and RYU SDN controller and supports synchronous development.

Project evaluation methods

To evaluate the firewall and SDN application I will:
Test if requirements are met and explore exception handling.
Monitor network performance to establishing latency caused by application introduction with a varying amount of background network traffic and number of connected IoT devices.