

MITIGATE VUNERABILITIES IN SELECTIVE SMART HOME DEVICES AND PROPOSE RECOMMENDATIONS TO ACHIEVE SECURITY

Introduction 1

Cyber security is important in every day life but even more import with smart home devices. This includes devices such as google chrome and amazon echo dot. Security for these devices are important as they are based in your home. These devices can make ease of life with everyday tasks but can hold important data and linked to other important data such as credit card information or linked to other accounts such as Facebook.

Aims 2

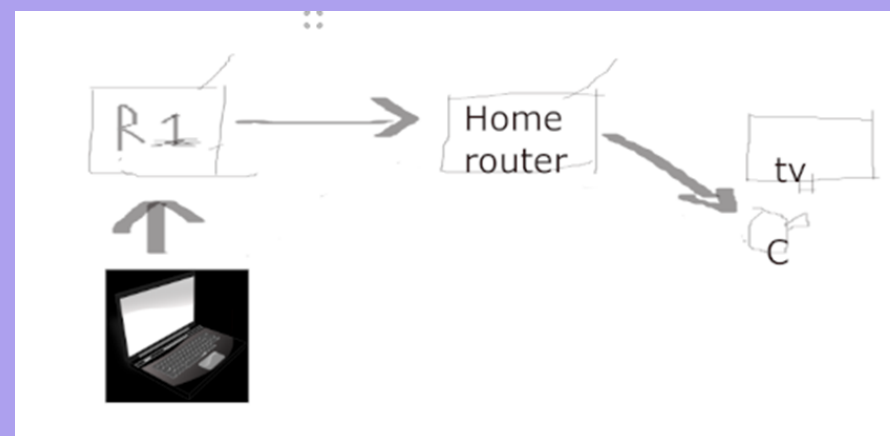
- To see how secure smart home devices are
- To actually see how secure smart home devices are
- What smart devices are commonly used

Objectives 3

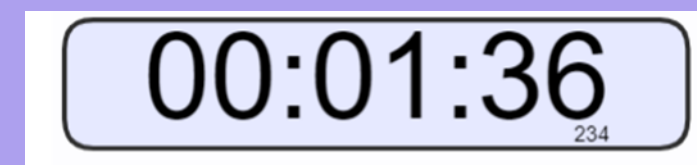
- Researching the advancement of smart homes with how the security is improved over the years.
- The main features of smart home devices
- What is the main security of smart devices that are built in from out of the box

Design-4

the main designs for the experiment was to a casting device using a separate network to play a video. This was done by first seeing id the device could be reached from the same network and separate network. After this the actual attack was done to see if they work using cURL commands. After this brute force was used to gain access to the device.



Result 5— it took 1:30 seconds to gain access to the device using the out of the box password. The device could only be pinged from the same network and was unreachable on a separate network. The same results were found from using cURL commands where the attack only worked using the same network.



Conclusion 6— overall, the security of smart home devices are mostly secure. Where some basic security would be needed to be added. This means that everyday security for the devices are mostly secure and need minimal alteration to make them secure. The biggest factor is to make sure security on the devices are two-factor if allowed.

Connor Osborne

1800742@student.uwtsd.ac.uk

Computer networking and cyber security