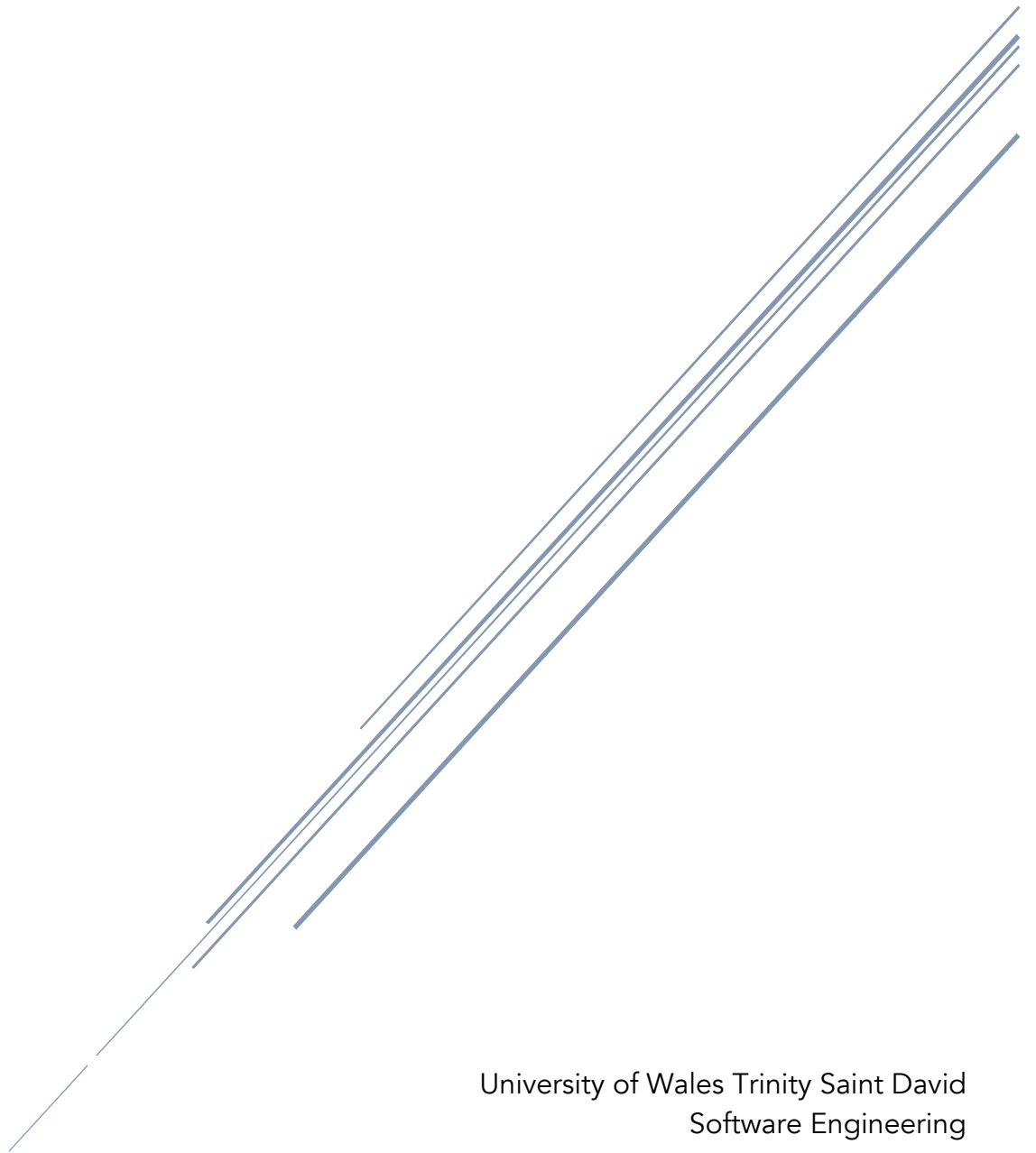


Design and Implementation of Smart Home – Implementation Report

Smart and Connected Devices I



University of Wales Trinity Saint David
Software Engineering

Siobhan Stephens - 1800709

Table of Contents

1.	Introduction	2
2.	Design.....	2
2.1.	Personal Devices.....	2
2.2.	Network Devices.....	3
2.3.	Backup Devices.....	3
2.4.	Design Diagram	3
3.	Network Security.....	5
3.1.	Router Configuration	5
3.2.	Hardware Firewall	5
3.3.	Software Firewall.....	5
3.4.	IP Address Allocation and MAC Address Filtering	5
3.5.	Encryption.....	6
3.6.	Guest Access	6
4.	Intrusion Detection and Prevention Systems	6
5.	Backup	6
6.	Scalability.....	6
7.	Physical Security.....	6
8.	IoT Device Selection	7
9.	Notes	7
10.	Conclusion	7
11.	References	7

1. Introduction

The desired outcome of this implementation is to use knowledge and understanding gained in the adjacent Smart Home report to design a smart home and protect the devices against vulnerabilities. The report outlines many of the security issues and vulnerabilities with smart home and IoT devices, and how to protect against them.

2. Design

The smart home design was created on Packet Tracer using IoT and smart devices, and consists of the following personal and IoT (smart home) devices.

2.1. Personal Devices

- 2.1.1. Humidity Sensor (IoT0 – Kitchen)
- 2.1.2. Motion Sensor (IoT1 - Hallway)
- 2.1.3. Smoke Sensor (IoT2 – Kitchen)
- 2.1.4. Air Cooler (IoT3 – Living Room)
- 2.1.5. Ceiling Sprinkler (IoT4 – Kitchen)
- 2.1.6. Heater (IoT5 – Living Room)
- 2.1.7. Heater (IoT6 – Bedroom)
- 2.1.8. Air Cooler (IoT7 – Bedroom)
- 2.1.9. Heater (IoT8 – Hallway)
- 2.1.10. Air Cooler (IoT9 – Hallway)
- 2.1.11. Smart LED (IoT10 – Living Room)
- 2.1.12. Smart LED (IoT11 – Bedroom)
- 2.1.13. Smart LED (IoT12 – Kitchen)
- 2.1.14. Smart LED (IoT13 – Garden)
- 2.1.15. Temperature Sensor (IoT14 – Living Room)
- 2.1.16. Temperature Sensor (IoT15 – Kitchen)
- 2.1.17. Temperature Sensor (IoT16 – Bedroom)

2.2. Network Devices

- 2.2.1. NAS Network Attached Storage Device
- 2.2.2. Home Router for Personal Devices (PersonalRouter)
- 2.2.3. Home Router for IoT Devices (IoTRouter)

2.3. Backup Devices

- 2.3.1. SSD Backup
- 2.3.2. Cloud Backup

2.4. Design Diagram

Figure 1 below shows the smart home design and included devices, created in Packet Tracer.

Design Diagram



Figure 1. Smart home device design in Packet Tracer

3. Network Security

Network security is a crucial aspect of keeping IoT and personal data safe, as discussed in the adjacent report. As a result, the following security measures are to be implemented.

3.1. Router Configuration

The personal router network will be named 'TropicalBrickNest5' – a unique and non-identifying string. The IoT router network will be named 'InsightTrolleyCanvas2' – another unique and non-identifying string. The passwords used for both networks shall be at least 12 characters, contain upper- and lower-case letters, numbers and special characters, must not be the same for both, and will be rotated every 6 weeks. The routers must both use WPA2 security standard. WPA2 is for wireless networks based on the Advanced Encryption Standard technology (AES) [1], providing encryption for data in transit across the network.

3.2. Hardware Firewall

A firewall will be used to offer a layer of protection to both IoT and personal routers. This will be used to block any unsolicited access to the networks and provide logs in case of an incident. If an incident was to occur, the logs would allow traceability and would help to highlight the vulnerability in the network in order to implement a fix.

3.3. Software Firewall

In addition to the hardware firewall, where possible, in-built software firewalls such as those provided by Microsoft Windows, or Apple MacOS will be used, such as on the personal computers. These software applications work similarly to a hardware firewall, by denying or permitting communications based on the firewall's configuration rules for the IP address and port information [2]. By default, Windows Firewall, allows all outbound connections, and permits only established inbound connections (those that are a direct response to an outbound connection initiated from that computer or network) [2].

3.4. IP Address Allocation and MAC Address Filtering

DHCP will be used instead of static address allocation. This is due to the complication of address allocation when new devices are added and removed from the network in a home environment. This would be a time-consuming process, and it more suited to industry settings where an individual is tasked with maintaining the IP addresses.

It was also decided that MAC address filtering was not to be used, due to the potential difficulty of accessing IoT device MAC addresses, and the time taken to maintain the MAC address list.

3.5. Encryption

All traffic for both the personal router and IoT router will be encrypted using WPA2, providing protection against packet sniffing and man-in-the-middle attacks.

3.6. Guest Access

Network access for guests will not be permitted. It would be suggested that guests use their own personal mobile data if internet access is required.

4. Intrusion Detection and Prevention Systems

IDS and IPS systems have been considered. An IDS used for IoT systems must be able to analyse packets of data and generate responses in real time, analyse packs in different layers of the network with different protocol stacks and adapt to different technologies [3]. They must be fast-response and handle high-volume data processing. As a result, there are currently a lack of IDS on the market suitable for IoT devices.

However, Snort [4], provided by Cisco, is a free, open-source intrusion detection and prevention system which is capable of adequately monitoring both the personal, and IoT device network for added protection.

5. Backup

Personal devices will have frequent backups to the Cloud and also an external SSD device. Cloud backups will occur as changes are made (as per device OS), and external backups will be taken once per week. A mirrored NAS (network attached storage) device is also to be used on the personal network, two devices mirrored in case of a device failure.

Backup is a critical aspect of the home security setup, as in the case of accidental loss, or malicious data loss through malware or a virus, personal data can be restored.

Backups to these devices will be encrypted at rest, and in transit for added security.

6. Scalability

Both the personal and IoT network are scalable, allowing for multiple devices to be added and removed. It was decided that static IP address allocation and MAC address filter would not be used so that devices could be added and removed from the network with more ease.

7. Physical Security

Along with the network security measures, it must be ensured that both personal and smart home devices are kept safe so that they cannot be tampered with. This might include not leaving personal devices out where they could be potentially stolen, such as in a car. It is also

advised that smart devices (or their main hub) be kept within the locked property, again for tampering and theft.

All devices must be kept safe with strong and unique passwords to protect against unauthorised access.

8. IoT Device Selection

As discussed in the adjacent report, many different IoT manufacturers exist, all with varying takes on security. It is important to ensure the manufacturer of the device takes adequate security precautions and implements adequate measures. It is also advised to read the full privacy-policy regarding data collection and storage. The data must be kept secure and should not be collecting any personal data that an individual is not happy with.

Therefore, it can be assumed that the devices in this design will have undergone suitable investigation regarding their security measures, data collection and storage, and privacy policy.

9. Notes

It was decided that redundant network devices would not be used in the home environment, due to cost, and the fact that a network outage would not be mission critical, or cause loss or damage to the home network.

10. Conclusion

Overall, adequate protection has been considered for the smart home design in a home setting, as it can be implemented by a 'normal' individual with some technical knowledge. If maximum security was required, some of the mentioned discarded features such as MAC address filtering could be implemented, along with the use of a VPN.

Another consideration is the implementation of extra security often requires significant technical knowledge, time, and will incur additional costs, therefore a balanced take on security has been implemented.

In order to fully demonstrate the implementation and the describe the outlined security features, packet tracer could have been used.

11. References

- [1] "WPA2 - security standard | NFON Knowledgebase UK." [Online]. Available: <https://www.nfon.com/gb/service/knowledge-base/knowledge-base-detail/wpa2>. [Accessed: 11-Jun-2020].
- [2] Miller C Lawrence, "What are Windows Firewall and Windows Defender?" [Online]. Available: <https://www.dummies.com/computers/computer-networking/network->

- security/what-are-windows-firewall-and-windows-defender/. [Accessed: 11-May-2020].
- [3] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments," *Journal of Cloud Computing*, vol. 7, no. 1. Springer Verlag, 01-Dec-2018.
- [4] "Snort - Network Intrusion Detection & Prevention System." [Online]. Available: <https://www.snort.org/>. [Accessed: 12-May-2020].