Literature Review  
FYP: “Securing home networks”

**Intro:** The first thing that many new house owners do once they buy their house is set up an internet connection and most of the time, they will leave the default settings for multiple parameters on. Due to the number of devices that connect to our home network, they put their personal information at risk by not setting up security measures to protect themselves and their devices. There is a multitude of ways to make sure your home network is secure, this literature review will cover the main steps in assuring you have a secure network against the most common threats.

**SEARCH TERMS:** “Home network security”, “Securing home networks”, “Smart home security”

* Feamster, N. (2010). Outsourcing home network security. *HomeNets '10 Proceedings of the 2010 ACM SIGCOMM workshop on Home networks*, pp.37-42.

Relevancy: average

This paper talks about how home networks and small enterprise networks pose a challenge when it comes to network security due to the fact that they are either very poorly managed or not at all, which can lead to the breach of devices connected to the network. Although this paper talks mainly about outsourcing the security to an experienced third party, it does give out security aspects to protect home networks: spam filtering and detection of botnets and malware. Which are very common issues and necessary to protect ourselves against them.

* Denning, T., Kohno, T. and Levy, H. (2013). Computer security and the modern home. *Communications of the ACM*, 56(1), p.94.

Relevancy: high

This paper talks about the impact of consumer good on home security. It examined the different types of technological attacks on homes and identifying what makes devices attractive to attackers whilst giving out possible solutions to secure ourselves. This paper focused on 3 particular devices: wireless webcam toy, a wireless scale, and a home automation siren. The authors present a framework to determine the risk factor of each device.

* Lee, C., Zappaterra, L., Kwanghee Choi and Hyeong-Ah Choi (2014). Securing smart home: Technologies, security challenges, and security requirements. *2014 IEEE Conference on Communications and Network Security*.

Relevancy: high

This paper delves into the main issues and security threats existent in smart home networks then gives out fundamental requirements in order to assure the security and confidentiality in smart homes. The authors first talk and describe the most common smart devices found in homes, explaining how they work from the operating system they use and their specifications to their communication protocols in a network. The last section of the paper before the conclusion, the paper talks about the security side of these smart devices, mentioning the security challenges and analysing the already existing security threats. *“Smart homes require very stringent security requirements, due to the importance of the private information a home environment contains.”*

The main security challenges on smart devices are:

* + “Resource Constraints”: Due to the fact that these devices are meant to work with low power and reduced hardware, most security mechanisms are not possible to implement as they do not have enough power or memory.
  + “Unreliable communications”: there is no guarantee of a 100% packet delivery with the implemented communications protocols but also retransmissions are not possible in these type of network devices.
  + “Energy Constraints”: Due to the fact that smart devices have limited energy as they are battery powered, implementing security protocols demand a lot of energy, therefore, it limits the energy to other functions of the device.
  + “Physical Access”: unattended devices become targets to tampering therefor allowing the possibility of an attacker to extract data from the device.

Another type of physical attacked mentioned in this paper is “Jamming” which involves transmitting signals in order to disrupt the device

The paper lists out different types of possible attacks against smart devices: Data Link Layer attack, Network Layer attack, Transport Layer attack, and Application Layer attack.

At the end of the paper, the authors list out recommended security requirements for homes with smart devices:

* + “User Authentication”: Only authorized user can update smart devices.
  + “Device Authentication”: be able to differentiate between legitimate and unauthorized devices on the network
  + “Network Monitoring”: Have intrusion detection system (IDS) and monitoring tools in order to “detect network intrusions and report anomalies”.
  + “Secure Key Management”: secure pre-installed network keys to protect the network in case attackers have breached a device.
  + “Physical Protection”: Put in place anti-tampering and anti-reverse engineering solutions to avoid all sorts of physical attacks.
* Kim, T. and Robles, R. (2010). A Review on Security in Smart Home Development. *International Journal of Advanced Science and Technology*, [online] 15. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.178.1685 [Accessed 10 Nov. 2017].

Relevancy: a bit

This paper focuses on the benefits of smart home technology for home automation but also in regards to home security. The paper talks about the threat of network security to smart devices companies due to the availability of tools allowing attackers to find out weaknesses in the network. The authors listed out five of the most common attack techniques against networks:

* + - “Network packet sniffers”
    - “Password attacks”
    - “IP Spoofing”
    - “Man in the middle attacks”
    - “Distribution of sensitive internal information to external sources”

But the paper also mentions about DDoS attacks, where a denial of service attack by spam mail is the newest form of attack against smart homes. The intruder gets access to the network through a file attached to a spam email, once the file is executed, “the mail server resources will be eaten up by mass emails from other machines in the domain results denial of services.”

* Internetworking technologies handbook. (2004). 4th ed. Indianapolis, IN Cisco Press, pp.793-804.

Relevancy: high

This handbook talks about everything revolving around network and devices connected to the internet. We are focusing on the security part of this handbook, where it explains network security and talk about the threats posed to a network. Furthermore, this handbook describes ways to mitigate network threat and what tools can be utilised to improve the security. The threats against networks mentioned here are:

* + - Unauthorised access
    - Weak authentication
    - Passwords
    - Packet sniffers
    - Application layer attacks
    - Viruses, worms, trojan horses
    - IP spoofing
    - DoS

This guide mentions the importance of security policies to implement in order to reduce the chances of an attack against a company. This book also talks about Defence-in-depth security solution which consists of having multiple zones of defence to protect a network. If one zone fails, the other zones can stop the attack.

Password ageing is used to mitigate against password attacks and ingress/egress filtering to protect against IP spoofing.

* Cyril Jose, A. and Malekian, R. (2015). Smart Home Automation Security: A Literature Review. *The Smart Computing Review*, 5(4).

Relevance: a bit

This paper mainly focuses on smart home automation security, mentioning the security flaws in already available systems. We’ll focus on the security challenges mentioned by this paper.  
Attackers find smart homes good targets as not only they can detect what device is available in the house through the network but because there is no network administrator, so attackers can scan networks with a very low probability of getting caught. As home automation systems devices come from multiple manufacturers, each of these devices has a different set of vulnerabilities for an attacker to choose from. Furthermore, many home automation device, if left configured in its default setting, can be found available as its own network, so the attacker does not necessarily have to connect to the home network to determine what devices are available in the household.

* Oluwafemi, T., Gupta, S., Patel, S. and Kohno, T. (2013). Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of home automation Security. *Workshop on Learning from Authoritative Security Experiment Results*. [online] Available at: https://www.usenix.org/laser2013/program/oluwafemi [Accessed 12 Nov. 2017].

Relevancy: a bit

This paper proves that certain IoT devices can cause physical harm if exploited by an attacker. In this case study, the authors used a “connected Z-Wave enabled light dimmer” where they sent four different electrical signals in the aim to break them. In order for the attackers to exploit the light bulbs, they had to remotely access the network to be able to exploit the devices. By accessing the network, they were also able to compromise a smart home controller. This study also showed that, even if a device was not connected directly to the internet, but connects to another device who is connected, then it can still be exploited.

* Fernandes, E., Jung, J. and Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. *2016 IEEE Symposium on Security and Privacy (SP)*.

Relevancy: high

The authors of this paper analysed a popular app that controls smart homes' devices, Samsung's SmartThings, in order to identify the benefits but mainly test the security of the app. The study revealed that the app had many features that were not mentioned. Also, the app had full privilege access to the owner's devices, allowing the app. Furthermore, the tests revealed that the event subsystem isn't protected enough, allowing sensitive information stored to be revealed. The authors exploited the flaws in the structure of the app allowing them to:

(1) secretly planted door lock codes;

(2) stole existing door lock codes;

(3) disabled vacation mode of the home;

(4) induced a fake fire alarm.

* Copos, B., Levitt, K., Bishop, M. and Rowe, J. (2016). Is Anybody Home? Inferring Activity From Smart Home Network Traffic. *2016 IEEE Security and Privacy Workshops (SPW)*. [online] Available at: http://ieeexplore.ieee.org/abstract/document/7527776/ [Accessed 13 Nov. 2017].

Relevancy: a bit

This paper uses two Nest smart devices (Nest Thermostat and Nest Protect) to prove that analysing the traffic between the device and the home network, attackers can determine whether the home owners are in or out of the house. Looking at the network data traffic, attackers can clearly see when the thermostat is set on "home mode" and "Auto Away" giving attackers a clear timeline.

* Yu, T., Sekar, V., Seshan, S., Agarwal, Y. and Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices. *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV*. [online] Available at: https://dl.acm.org/citation.cfm?id=2834095 [Accessed 13 Nov. 2017].

Relevancy: a bit

This paper talks about how IoT devices can be the entry points in accessing personal information. Due to the large amount of vulnerabilities and "unfixable flaws" in IoT devices, this journal suggested a roadmap as a solution to tackle this major security issue in our homes.

* Costin, A., Zaddach, J., Francillon, A., Balzarotti, D. and Antipolis, S. (2014). A large-scale analysis of the security of embedded firmwares. *USENIX Security Symposium*, [online] 23. Available at: https://dl.acm.org/citation.cfm?id=2671232 [Accessed 13 Nov. 2017].