Literature Review

"Securing Home Networks"

P15209971

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. This review will focus on three major themes: Network security, explaining why it is so important and what do to be secure; Smart devices' impact on network security and finally network scanning tools.

I -Network security:

With the everyday use of the Internet, threats and online attacks have now become very common, therefore it is important to secure ourselves in order to prevent such attacks. The idea behind network security is to take precautions to protect the system from intruders (Sans.org, n.d.). In fact, according to the handbook from Cisco Systems about networking technologies (Cisco Systems, Inc, 2004), the main threats to a network are:

- **Unauthorized access**: accessing and using a system without the owner or administrator's permission
- **Weak authentication**: system's that do not need the credentials of the administrator to change settings or install programs.
- **Passwords:** the use of weak passwords or the same one on multiple systems.
- **Packet sniffers:** using tools that capture network packets to analyse the ones with sensitive information.
- **Application layer:** attacking the weaknesses in an application software, most common application layer attacks are: memory corruption and buffer overflows (Kumar and Kumar, 2014).
- **Viruses, worms and Trojan horses:** a virus is a piece of malicious software that spreads by infecting other programs. A virus can be embedded in email

attachments, pictures, documents, etc. and can only infect the system after user interaction. A worm is a program runs on its own and that can spread through networks. It attacks a victim machine by consuming all of its resources. A Trojan horse is a program that seems to have a useful function but also has a hidden malicious function.

- **IP Spoofing:** when the attacker's machine pretends to be a trusted IP address, giving him access to restricted resources available on the network
- **Denial of Service:** the aim of this attack is to disrupt access for legitimate users to a service.

It is important to know these types of attacks as it will help you protect your network against intruders (Scitechconnect.elsevier.com, 2013). Whether you are the network administrator for a business or your own personal network, it is essential to set up your network to avoid any device compromise. The paper from Kumar and Kumar explains the importance of setting up an Intrusion Detection Service and Intrusion Prevision Service (IDS/IPS) as they monitor network traffic and scan for suspicious data in packets (Pandasecurity.com, 2017). Furthermore, setting up firewalls and content filtering services such as spam filtering, antivirus (Feamster, 2010) (Kumar and Kumar, 2014) will protect the network from viruses and many other types malware that attackers may use to infect devices or networks. Additionally, the "Internetworking Technologies handbook" from Cisco systems advise network admins in using the 'Password Aging' technique to defend against bad passwords and therefore, mitigate against password attacks. Although a downfall of using this technique is that because it forces users to change their passwords after a certain time, the chances of them writing that password down are higher (Access.redhat.com. (n.d.), opening up to new physical threats. The handbook also suggests setting up ingress and egress filtering to protect against IP spoofing (Cisco Systems, Inc, 2004).

For companies, the importance of setting up security policies is mentioned in all papers relevant to this topic, as they cover the basics of security in a workplace. Security policies allow businesses to **Prevent**, **Detect, Mitigate** and **Recover** from any type of attack. Another form of defence multilayer security, which consists of having multiple zones of defence to protect a network (Cisco Systems, Inc, 2004), therefore, it will identify and isolate attacks in zones to stop it from spreading and infecting other zones of the network (Kumar and Kumar, 2014).

II -Impact of home network security with smart devices:

When we think of network security, we immediately think of our laptops, desktops and smartphones, but one element we always forget to list is our smart devices. In today's homes, many household objects, such as refrigerators, lights and thermostats are now connected to your network in order to help the user in doing a certain task. *"The Internet of*

Things (IoT) can be defined as "a pervasive and ubiquitous network which enables monitoring and control of the physical environment by collecting, processing, and analysing the data generated by sensors or smart objects."" (Cisco, n.d.). These embedded systems do have a lot of great advantages, helping household owners in controlling their homes, but from a security standpoint, these devices put your privacy at risk. Due to the poor implementation of security features, hackers can get access to your home network through these IoT devices. Furthermore, having poorly set up smart devices by leaving the default settings (Cyril Jose and Malekian, 2015), will allow attackers to see certain devices without the need of connecting to your private network (Denning, Kohno and Levy, 2013). Additionally, 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 (Cyril Jose and Malekian, 2015).

Costin et al. (2014) performed a case study where they analysed over thirty-two thousand firmware images of smart devices in order to get a better understanding their security system. The study uncovered more vulnerabilities that could affect multiple devices. Approximately 140 thousand devices that are currently available and connected to a network were concerned by of the security flaws discovered in this study (Costin et al., 2014). Due to a large number of vulnerabilities, IoT devices can be the entry point in accessing personal information for attackers (Yu et al., 2015). According to Kim and Robles (2010) and Lee et al. (2014), the most common attack techniques against networks with smart devices are:

- **Network packet sniffers**: capturing network packets transmitted from smart devices, may reveal unencrypted information such as usernames and passwords
- **Password attacks**: many devices are set to their default passwords, allowing attackers to guess or find the passwords online through the manufacturer's website.
- **IP spoofing**: attackers may configure their IP as one of the smart devices in order to become a trusted device on the network.
- **MITM attacks**: attacker will use one the devices and make all the traffic pass through it to get any personal information that passes through the network.
- **Distribution of sensitive internal information to external sources:** As many IoT devices communicate with servers that are outside the home network, attackers may use this communication to transmit any personal information to other devices or networks
- **DDoS attack**

There are other forms of attacks that fall under these branches: **Data Link layer attack, Network Link layer attack, Transport layer attack** and **Application layer attack.**

Lee et al. (2014) mention the main security challenges to why these devices are not secure:

- **"Resource Constraints":** Since 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":** Because 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 attack mentioned in this paper is "Jamming" which involves transmitting signals in order to disrupt the device.
Although this paper, contrary to the other journals chosen, does, in fact, list out recommended security requirements for homes with smart devices (Lee et al., 2014):

- **"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.

Three papers focus on specific smart home devices, the first one from Denning, Kohno and Levy (2013) analyse and compare three devices: a wireless webcam toy, a wireless scale and a home automation siren. The authors made a risk assessment table of the three devices in order to compare the exposure to attack and their attractiveness of being a target of an attack. They concluded the paper by talking about the importance of understanding the risks with embedded systems and that it is essential to have a strategy for securing smart homes.

Copos et al. (2016) paper are similar to the previous one, as they test the security of two common smart devices; the Nest Thermostat and the Nest Protect. They were able to prove that if attackers analysed the traffic between the smart devices and the home network, they could determine whether the homeowners are in or out the house as the thermostat sets itself to either "home mode" or "Auto-Away" giving attackers a clear timeline.

The case study produced by Oluwafemi et al. (2013) demonstrated that with certain smart devices, attackers could do more than just steal sensitive information, they could cause physical harm to home users. 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. By accessing the system, 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 that is connected, then it can be exploited.

Another way to exploit smart homes was through an application that was able to control these devices. For instance, the authors of "Security Analysis of Emerging Smart Home Application" analysed a popular app capable of controlling IoT devices: Samsung's SmartThings. They analysed the source code of the application, which revealed many hidden features, also, they discovered that the application had full privilege access to the owner's devices. The tests revealed that the event subsystem of SmartThings was not protected enough, making sensitive information being stored in plain text and accessible. Fernandes, Jung and Prakash (2016) proceeded to exploit the flaws in the structure of the app allowing them to plant door lock codes, steal the already existing ones, disable vacation mode and induce a fake fire alarm.

III - Vulnerability scans on Networks

There are many open source tools available to use to help a network admin or a homeowner help gather information about their own network, from allowing them to know what available ports are open on a network that should not be (Vu, Khaw and Chen, 2014), to seeing what devices are currently connected on the network, making sure there's no intruder. If a scanning tool finds a vulnerability on the network, it would produce a report indicating the severity of each flaw detected and would also give you solutions on how to either rectify it or mitigate it (Wang and Yang, 2017).

The top vulnerability scanning tools are Nessus, Nmap, OpenVAS, Retina CS, MBSA and Nexpose. These tools are very similar to one another and allow network administrators to have a clearer view of what is happening on their network. For this report, we shall focus on Nessus, which scans for network devices, virtual hosts, OS, web application and IPv4/IPv6 networks (Wang and Yang, 2017) (Deraison, 2004) and alerts you if any vulnerability is found. It performs over 1200 tests making sure that none of these attacks could be used against your network or laptop (Wendlandt, n.d.).

This review was mainly focused on network security, how smart devices affect the security in home networks regardless of their benefits and how vulnerability scanning tools are used to detect any flaws on the network or on any devices connected to it. Many would agree that Internet of Things devices helps the average homeowner, but manufacturers do

not seem to focus on the security side of these devices. Therefore, putting user's personal information at risk from attackers. Many papers would agree that for business, it is essential that they put in place security policies to lower the possibility of any kind of attack. Also, using vulnerability scanning tools are very useful for network admins to find vulnerabilities, but as these tools are open source, attackers may use these programs against companies or homes and exploit any vulnerabilities that they uncover.

References:

Access.redhat.com. (n.d.). *4.3.2.2. Password Aging*. [online] Available at: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/s3-wstation-pass-org-age.html [Accessed 16 Nov. 2017].

Pandasecurity.com. (2017). *What is the difference between an IDS and an IPS? - Technical Support - Panda Security*. [online] Available at: https://www.pandasecurity.com/usa/support/card?Id=31463 [Accessed 16 Nov. 2017].

Scitechconnect.elsevier.com. (2013). *Network Security Basics*. [online] Available at: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Network-Security-Basics.pdf [Accessed 13 Nov. 2017].

Sans.org. (2017). *SANS Institute: Network Security Resources*. [online] Available at: https://www.sans.org/network-security/ [Accessed 15 Nov. 2017].

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

Cisco Systems, Inc (2004). *Internetworking technologies handbook*. Indianapolis, IN: Cisco Press, pp.793-804., pp.793-804.

Kumar, G. and Kumar, K. (2014). Network security – an updated perspective. *Systems Science & Control Engineering*, [online] 2(1), pp.325-334. Available at: http://www.tandfonline.com/doi/full/10.1080/21642583.2014.895969?scroll=top&needAccess=true [Accessed 15 Nov. 2017].

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

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*.

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].

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

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].

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

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].

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].

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].

Deraison, R. (2004). *Nessus network auditing*. Rockland, MA: Syngress Media.

Vu, H., Khaw, K. and Chen, T. (2014). A New Approach for Network Vulnerability Analysis. *The Computer Journal*, [online] 58(4), pp.878-891. Available at: https://academic.oup.com/comjnl/article-abstract/58/4/878/336010 [Accessed 12 Nov. 2017].

Wang, Y. and Yang, J. (2017). Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool. *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. [online] Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7929663 [Accessed 14 Nov. 2017].

Wendlandt, D. (n.d.). *Nessus*. [online] Cs.cmu.edu. Available at: https://www.cs.cmu.edu/~dwendlan/personal/nessus.html [Accessed 14 Nov. 2017].

IMAT3451 Project Contract Template

Student Name	Naïm Maoun
P-number	P15209971
Programme	Computer Security BSc (Hons)
Email address	naimmaoun@gmail.com
Project Title	**"**Securing Home Networks**" / "**Secure Home**"**
Project Proposer / Supervisor	Helge Janicke, Professor in Computer Science, Head of School of Computer Science and Informatics, Head of the Cyber Technology Institute (CTI), 01162577617, heljanic@dmu.ac.uk

Introduction

The aim of this project is to develop a mobile app that ordinary and non-technical home network user can use to help them set up and configure their home networks. Making sure that all security measures have been taken under consideration.

Project Background

Nowadays, with the increasing number of devices that connect to your home network puts your personal data at risk. Many home networks are improperly set up due to the lack of information and know-how on how to secure their home network, making them vulnerable to attacks from hackers. This is why it is very important to assist and guide home owners in securing their network.
As many home internet consumers, especially those who do not have an IT background, would generally leave all the default settings in place including the default password of their WIFI. Therefore, it is important to make sure they understand every security option made available to them.

Aim/Objectives/Deliverables

This is the heart of the Contract, and will require discussion with your supervisor and possibly several iterations to get it right. It is against the objectives and proposed deliverables that the final product will be assessed. So, it is important to ensure that all aspects of the assessment criteria (see Blackboard) are included in the list of objectives/deliverables.

Aims: The aim of this project is to develop a user-friendly android application to help non-technically minded home users set up securely their home network. Therefore, making sure that no device connected to the network is at risk.

Objectives:

- To understand and be comfortable at programming in java and using Android Studio
- To investigate all types of home networks security
- To investigate the implementation of Nessus in an app
- Add a glossary of all network security related terms
- Design the app in a user-friendly way

Deliverables: a list of your Project's deliverables with some general description.

	Research Projects	Development Projects	Hybrid Projects
First Submission (first deliverable) Week 7	• Project contract • Ethics form • Project Plan (e.g., Gantt Chart) • Global Checklist • Scoping Review	• Project contract • Ethics form • Project Plan (e.g., Gantt Chart) • Global Checklist • Literature Review	• Project contract • Ethics form • Project Plan (e.g., Gantt Chart) • Global Checklist • Literature Review

	(mapping out the key concepts and work in the field) • Research Questions	• Requirements • BCS checklist (if pertinent)	• Requirements • BCS checklist (if pertinent)
Final Submission (final deliverable) These are some examples: each project will need a complete set of objectives/deliverables Week 29	• Full literature Review • Updated (if needed) Research Questions • Report on the field study • Findings and analysis • Conclusions etc. • Reference list • Appendices (surveys, interviews evidence etc) • Maximum word count (main body): 15.000	• Use Case Diagrams/Use Case Descriptions/Class diagrams/ER model/State transition diagrams • Story boards/Interface Designs • Design Documentation • Test Plan • Prototype • Final report, including critical evaluation • Software • Appendices (e.g. further design documentation, test logs) • Maximum word count (main body): 15.000	• Use Case Diagrams/Use Case Descriptions/Class diagrams/ER model/State transition diagrams • Story boards/Interface Designs • Design Documentation • Test Plan • Prototype • Final report, including critical evaluation • Software • Appendices (e.g. further design documentation, test logs, surveys, interviews evidence) • Maximum word count (main body): 15.000
Viva examination: attended by the supervisor and the 2nd marker Weeks 30-32	• Oral examination (presentation of your work) During week 28 supervisors and students will need to start communication for setting up the Viva	• Oral examination (demo of your work) During week 28 supervisors and students will need to start communication for setting up the Viva	• Oral examination (presentation and demo of your work) During week 28 supervisors and students will need to start communication for setting up the Viva

Resources and Constraints

Resources: Android Studio, my smartphone for testing the app, papers on 'Home Network Security', Nessus vulnerability scanner, Wikipedia.com
Constraints: Home network with IoT devices connected to test the scanner

Sources of Information

- DMU Library
- The internet
- Android

Risk Analysis

- Compatibility issues between my phone and android studio. If this issue happens, I shall either get another android device or install an android emulator on my computer
- Not being able to implement Nessus scanner in the app. If this happens, I shall look for a similar scanner and try to integrate it to my app instead

Schedule of Activities

Week 5 -6: Research and learn all the different ways to secure a home network from different types of attacks and write literature review
Week 7: Make sure everything is in order for initial submission
Week 8: Draw up the design of the app: how the app will look like: main page, menu tab, splash screen, logo of the app
Week 9-11: Build the main structure of the app, without any feature: bare bones of the app, home screen, menu
Week 12: Add glossary page to the app with general network security terms
Week 14 -19: Build the main part of the app: Adding checklist component to the app, different configuration procedures depending on default routers from ISPs.
Week 20: Linking technical terms from the 'checklist' and router setup guide to the glossary
Week 21-22: Implement Nessus to the app
Week 23: Fully test the app
Week 24: Add graphics and improve the 'Front End' of the app
Week 25-28: Write the report: convert all the notes and drafts taken during these week to a well written paper.

Student_____**Naïm Maoun**_____ **Date**____**24/10/2017**__

Proposer _____ **Date**_____

Supervisor_____ **Date**_____

Keep the signed copy somewhere safe: include it with your initial submission. Your supervisor will require a copy as well.