# Literature Review

## Introduction

In recent years, the Internet of Things has come under intense scrutiny from security researchers as a result of their notorious security weaknesses. As this paper aims to demonstrate the detrimental affect implementing insecure IoT devices can have on homeowners, previous research has been reviewed in order to better understand the current battles faced by developers of such devices, as well as threats that IoT causes consumers. With this foundation of knowledge, it shall then be possible to build upon the existing literature by developing a smart home case study for the purpose of penetration testing. The review shall first cover topics such as the threats they present, and the privacy concerns related. Then reasons for these present threats such as device constraints and lack of legislation.

There are a vast array of IoT device markets (health, transport, etc) . However, since the focus of this research is issues that may be faced by consumers upon installation of insecure IoT devices within their homes and how this may be combated, these aspects shall not be reviewed and/or only referenced where appropriate.

## Threat Landscape

The main issue faced by both consumers and manufacturers is the threat landscape of IoT devices. A threat landscape provides an overview of threats viable to IoT devices, based on current and emerging trends within cyber security (ENISA website). As explained by <name>, the “increased population (number of IoT devices), complexity, heterogeneity, interoperability, mobility, and distribution of entities (smart objects, controller, user, and services) expand the attack surfaces in the interconnected things’ networks.” (ref Towards an Analysis of Security Issues, Challenges,

and Open Problems in the Internet of Things)

In relation to other technologies, such as websites, the increased number of attack surfaces present on IoT devices presents a challenge to developers. This is due to the fact that they often implement multiple user interfaces such as web, mobile and cloud thus generating more vectors susceptible to attack. They also process large amounts of data, often amongst other similar devices within the smart home and third parties which could highly motivate attackers with financial motives due to the likeliness of information that can be used to commit fraud and blackmail.

At the time of writing, there are already more devices (8.4 billion) connected to the Internet than there are people in the world (Meulen, 2017). As this number undoubtedly continues to grow, with Gartner estimating 26 billion IoT devices connected by 2020 (Rivera, 2013), security cannot afford to be an afterthought. As the world of interconnected devices begins to be more frequently adopted by home owners and industries, “each entity, depending on its type, carries with it an associated set of channels, methods, and data items, each of which is subject to potential abuse.” It would be ignorant to operate under the assumption that, due to the Internet of Things ultimately being ordinary devices that have been upgraded to implement other well established technologies, that the do not pose a threat, as the “increased population has the effect of creating an explosion in the total number of potential target resources across the Internet, as well as within any specific environment.” (ref IEEE)

## Privacy Concerns

As a result of their interconnected nature, IoT devices handle a large quantity of personal information. Due to the high quantity of personal information gathered and analysed by IoT devices and their accompanied cloud servers the impact of a security breach effects not only a user’s data but also poses a direct threat to their health and safety, which in turn “changes the accepted idea that the home is usually a safe place to live in.” (ENISA, security)

Another paper published by ENISA states that implementing numerous IoT devices within the home to create a so-called “Smart Home Environment” shall generate a vast amount of personal information pertaining to everyday activities undertaken by the inhabitants. This large amount of data combined with its sharing with third parties that may be responsible for the development and/or maintenance of different aspects of the device means that the “visibility of the smart home occupant is increased” and as such “Smart home functions may have serious impacts upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of location, and privacy of association.” (ENISA, threat). The lack of respect for personal data found by the myriad of released insecure devices demonstrates that IoT devices may end up enabling security breaches rather than working to combat them. One example provided by (ref risk analysis) describes one such scenario:

“A burglar may remotely monitor routine activity patters based on when persons in the household are at home, and thus get the means to conduct the burglary when the house is empty” (ref risk analysis)

## A Lack of Legislation

An investigation into the underlying issues that are resulting in a multitude of insecure IoT devices being released revealed that there are multiple economic factors that appear to be influencing manufacturers decision to circumvent implementing basic security. According to ENISA, “security features may be limited in order to keep the costs of the devices affordable” (ref ENISA, threat).

A lack of knowledge from consumers in relation to the information that may be gathered by IoT devices appears also to be encouraging manufacturers to forgo security. As ENISA states, “it may not be immediately obvious to smart home users what information can be collected by the smart home, and how sensitive this information might be” (ref ENISA, threat). Without this knowledge, consumers may not see security as a requirement when purchasing IoT devices, thus putting no pressure on manufacturers to invest in security. However, in the case where consumers are concerned about their privacy and therefore seek secure devices, NCC states that “regulators will often stipulate requirements that can be trivially met without achieving the desired level of cyber-security”. This results in an average consumer with no real technical knowledge being easily be led to believe that they are purchasing secure devices, as they shall “look for documented security capability (e.g. encryption of a particular strength) rather than the quality of the implementation” (ref NCC). These gaps in the knowledge of the general public appear to be being exploited by manufacturers who are profiting by releasing insecure devices that require less skill and time to develop, as well as not facing any repercussions for their irresponsibility.

Additionally, another factor that may influence the implementation of security may be directly linked to the limited knowledge of the developer themselves. For instance, many IoT devices available today are ordinary devices that have been upgraded to incorporate additional functionality. This means that the smart components “may be developed by manufacturers with limited experience of security design, as they add connectivity to their existing products” (ref ENISA, threat).

Another issue that results in insecurity is the lifecycle of these devices. Even devices that are developed with security as a priority shall undoubtedly encounter vulnerabilities within a decade’s time if or when manufacturers decide to cease support for their devices if past trends in computer security are anything to go by. One example is that “assumptions are made that transport security will be guaranteed forever or at least the lifetime of the product. As we have seen with GSM, WEP and a number of other wireless protocols this assumption would have been proven incorrect.” (ref NCC)

A major contributing factor in the terms of a lack of security may be the result of limitations within the devices themselves, which shall be discussed in more detail below.

## Device Constraints

There are typically two types of IoT devices found within the home: high-capacity and constrained. High-capacity devices are generally powered from the mains and have adequate storage and processing capabilities for implementing security features. Constrained devices, on the other hand, may present issues as “security in these devices may be limited due to their comparatively low capacities (CPU, memory, battery…)” (ref ENISA, security). This results in many IoT devices lacking the dedicated security they require in order to maintain privacy and avoid vulnerabilities as they lack the resources to do so.

## Conclusion

If the implementation of IoT devices within homes continues to increase as expected, it is reasonable to assume that as with every other popular form of technology the industry shall become a prime target for malicious hackers. According to the literature reviewed, the Internet of Things faces many hurdles when it comes to applying security and combating privacy concerns due to device constraints and the increased threat landscape. However, a greater understanding of the need for security by consumers and the introduction of laws and regulations by relevant authorities shall hopefully enforce manufacturers to implement security.

There is literature available that documents the preferences and concerns of current smart home users, literature that investigates their threat landscape and thus expected vulnerabilities. However, there appears to be a lack of documentation relating to the simulation of a real world attack on domestic IoT devices, that follows a specific methodology and creates a case study on a so-called “smart home” as a whole. As such, this paper aims to build upon the existing available literature by doing so, and in the process draw conclusions based upon the different variables such as devices created by well-known brands compared to that of lesser known, as well as different types of devices that may collect different information and operate using different protocols.

Rob van der Meulen. (2017). *8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.* Available: http://www.gartner.com/newsroom/id/3598917. Last accessed 24/04/17.

Janessa Rivera. (2013). *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020.* Available: http://www.gartner.com/newsroom/id/2636073. Last accessed 24/04/17.