

|  |
| --- |
| Investigating Vulnerabilities In IoT devices in the context of a smart home  Michael W Crow  BSc Ethical Hacking and Countermeasures, 2017 |

|  |
| --- |
| School of Arts, Media and Computer Games  Abertay University |

# Abstract

Jfjfgjgjg gobbledegook

Table of Contents

[Abstract i](#_Toc480502249)

[Table of Figures iv](#_Toc480502250)

[Table of Tables v](#_Toc480502251)

[Acknowledgements vi](#_Toc480502252)

[University of Abertay Dundee Permission to Copy vii](#_Toc480502253)

[Abbreviations, Symbols, Notation and Glossary of Terms viii](#_Toc480502254)

[1. Introduction 1](#_Toc480502255)

[1.1. Introduction to IoT 1](#_Toc480502256)

[1.2. History of IoT 2](#_Toc480502257)

[1.3. The Modern Smart Home 3](#_Toc480502258)

[1.4. Penetration Testing and IoT 4](#_Toc480502259)

[1.5. Devices Tested in this project 5](#_Toc480502260)

[1.6. Research Questions 5](#_Toc480502261)

[1.7. Research Aims 5](#_Toc480502262)

[1.8. Research Objectives 5](#_Toc480502263)

[1.9. Statement of Structure 6](#_Toc480502264)

[2. Background 7](#_Toc480502265)

[2.1. IoT Market Projections 7](#_Toc480502266)

[2.2. Cyber Security Implications 10](#_Toc480502267)

[2.3. IoT in Industry 11](#_Toc480502268)

[2.4. IoT Architecture 12](#_Toc480502269)

[2.5. IoT Attack Vectors 14](#_Toc480502270)

[2.6. IoT and Botnets 15](#_Toc480502271)

[2.7. OWASP IoT top Ten 16](#_Toc480502272)

[3. Methodology 18](#_Toc480502273)

[3.1. IP Security Camera 1 18](#_Toc480502274)

[3.2. IP Security Camera 2 18](#_Toc480502275)

[3.3. Baby Monitor 18](#_Toc480502276)

[3.4. Bluetooth Heart Rate and Blood Pressure Monitor 18](#_Toc480502277)

[3.5. Smart Power Plug 18](#_Toc480502278)

[3.6. Bluetooth weight scales 18](#_Toc480502279)

[3.7. Bluetooth Lightbulb 18](#_Toc480502280)

[4. Results 19](#_Toc480502284)

[5. Discussion 21](#_Toc480502285)

[5.1. Case Studies 21](#_Toc480502286)

[5.2. Real World Implications 21](#_Toc480502287)

[5.3. Countermeasures 21](#_Toc480502288)

[6. Conclusion 22](#_Toc480502289)

[6.1. Future work 22](#_Toc480502290)

[Appendices 23](#_Toc480502291)

[List of References 24](#_Toc480502292)

[Bibliography 28](#_Toc480502293)

# Table of Figures

[Figure 1 – Aspects of life effected by IoT 7](#_Toc480480790)

[Figure 2 – IoT Market trends by Sector 8](#_Toc480480791)

[Figure 3 – Home Internet Enabled devices by category 9](#_Toc480480792)

[Figure 4 – Preparing for IoT in the workplace 12](#_Toc480480793)

[Figure 5 – Three Layer IoT architecture 13](#_Toc480480794)

[Figure 5 – IoT architecture 13](#_Toc480480795)

# Table of Tables

[Table 1 – Fourth Industrial Revolution 1](#_Toc480415041)

[Table 2 – IoT Units Installed by Category 9](#_Toc480415042)

[Table 3 – IoT Vulnerability Results Table 12](#_Toc480415043)

# Acknowledgements

I would like to thank my supervisor, Xavier Bellekens and head of course Colin Mclean for their advice and support throughout this project and years of study.

I would also like to thank my friends, family and peers who also supported me through my years of study at Abertay University.

# University of Abertay Dundee Permission to Copy

Author: Michael W Crow

Title: Investigating Vulnerabilities In IoT devices in the context of a smart home

Qualification: Ethical Hacking and Countermeasures

Date of Submission: 26/04/2017

~~\* I agree that a copy may be made of the whole or any part of the above-mentioned project report without further reference to the undersigned~~

or

\* A copy shall not be made of the whole or any part of the above-mentioned project report without the written consent of the undersigned.

(\* Please strike out whichever does not apply)

Signature: Michael Crow

Address: Riverview, Main Street, Killin, Perthshire, Scotland, FK218XE

Date: 4/04/2017

# Abbreviations, Symbols, Notation and Glossary of Terms

IoT

P&G – proctor and gamble

Smart Device

Smart Home

Penetration or Pen Test

Penetration tester

White Hat hacking

Black Hat hacking

## Introduction

In the modern age in which we live very few aspects of life are hidden from the ever advancing wave of modern technology, According to the office for national statistics in 2016, 89% of households in the UK had access to the internet [1] this compared to just ten years before in 2006 when only 57% of UK households had access to the internet highlights the extraordinary popularisation and advancement of the industry in the last decade alone.

With the benefits of technology now firmly cemented into the daily routine of the everyday person, developers of the industry are constantly producing new and intriguing ways in which technology can benefit people in making their lives easier and more productive.

At the forefront of this exciting time in technological advancement lies the subject of the Internet of Things or IoT.

### Introduction to IoT

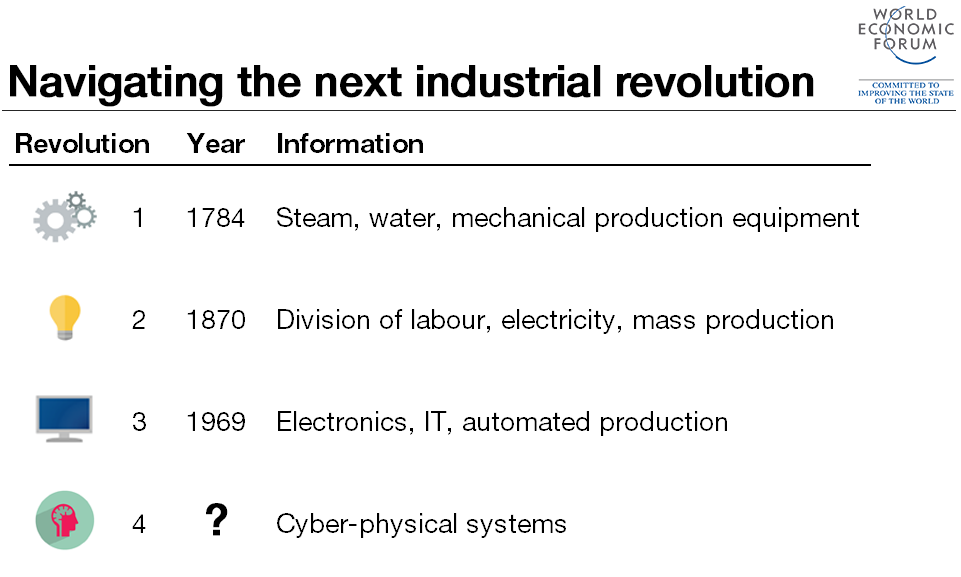
Since its invention in the late 1960s as a part of the third industrial revolution, the internet as we know it has underwent many transformations most notably the invention of the World Wide Web by Sir Tim Berners-Lee in 1990 which introduces the world to the concepts and advantages of interconnectivity. The most modern development in the internet is represented by the concept of the Internet of Things (IoT) is considered by many industry and economic experts as the possible fourth industrial revolution combined with artificial intelligence[2].

Table 1 – Fourth Industrial Revolution – World Economic forum (Klaus, 2016) [2]

The role of the internet of things in the progression of technology appears to be a substantial one in both the near and distant future and therefore it is a very hot topic in the technological world however, many main stream media outlets through using Internet of Things as a “buzz phrase” tends to confuse the general population as to what IoT actually is. As simply defined by the oxford dictionary the internet of Things is; “The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data” (Oxford Dictionary, 2016) [3]. These interconnected devices and everyday objects are often referred to as “smart devices” and form what can be described as the “building blocks” of which the Internet of Things is formed upon.

### History of IoT

The topic of interconnected devices is not by any means a new concept as the idea itself can be traced back to the year 1926 when Nikola Tesla stated;

*"When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole.........and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."* (Tesla, 1926).

The concept of interconnectivity continues through the decades until the creation of what many consider the first ever interconnected device in 1990 when John Romkey invented “The Internet Toaster” which used TCP/IP networking to allow itself to be turned off and on over the internet [4].

The term “Internet of things” Is claimed to be coined even as far back as 1999 by Kevin Ashton when he used it as a title of a presentation he was making to Procter & Gamble (P&G) about RFID chip connectivity. [5]

Fast forward to 2011 when the public launch Internet Protocol version 6 (IPv6) produced the scope in which current and future developments of the internet of things can occur as IPv6 allows for 2128 unique internet IP addresses compared to only 232 (4.29Billion) Which IPv4 had almost completely been allocated by the year 2011. The almost limitless amount of IP addresses that IPv6 can assign therefore increasing the rate at which IoT devices can be produced.

### The Modern Smart Home

In 2016 the internet was accessed daily by 82% of adults over the age of 16 in the UK [6], That Amounts to 41.8 Million individuals across the country this compared to 35% (16.2 million) of adults that access the internet daily in 2006 demonstrates that in the last ten years alone internet access has become an integral part of our society, however it is not only the percentage of the population that access the internet that has changed the way in which they access the internet has also seen a dramatic change.

In 2016 70% of adults used a mobile phone or “smart phone” to connect to the internet “on the go” which is a rise of 4% from 2015 [7]. Another device which was not traditionally connected to the internet was televisions, in 2016 28% of adults in the UK used televisions or “smart TVs” to connect to the internet which has also seen a rise of 4% since 2015 [8].

As such devices become more and more popular amongst the general population the concept of the “smart home” is becoming of increasing interest to business and consumer alike.

A “smart home” is a household in which many “smart devices” are used to aid and entertain in everyday life, these devices are often interconnected to a main controller system which can be accessed from a smart phone or remote device which can be used to control devices such as smart lighting, washing machines fridges etc. with the concepts of the internet of things any device can be accessed and controlled remotely over internet connection.

### Penetration Testing and IoT

With the Internet of things quickly becoming an exciting revolution in technological innovation organisations are keen to produce and develop as many devices as the can as quickly as they can, thus many devices are being produced without the proper security testing being carried out. The internet of things at this point has no worldwide standards agency setting a benchmark for security, as a result many smart devices are being purchased by businesses and consumers alike which contain multiple security flaws and therefore may pose risks to personal and private data.

In other sectors of information technology one technique which can be used to assess the security levels of devices and systems is penetration testing. Penetration testing involves the active gathering of information about the device or system in question in an attempt to identify the security weaknesses and entry points in which an attacker or “hacker” may use to compromise the device or system. The person or persons performing the penetration test are often referred to as “white hat” hackers as opposed to “black hat” hackers who aim to exploit security vulnerabilities for unauthorised purposes [9].

In this investigation, existing penetration techniques will be used against multiple “smart devices” in order to assess their current state of security. The penetration testing methodology that will be used in this investigation is the OWASP IoT Methodology.

### Devices Tested in this project

The “smart devices” tested in this project are listed below, all names make and models of the devices are withheld for security purposes:

1. IP Security Camera 1 – Internet based security camera.
2. IP Security Camera 2 – Internet based security camera with audio capabilities.
3. Baby Monitor – Internet based baby monitor with audio capabilities.
4. Bluetooth Heart Rate and Blood Pressure Monitor.
5. Smart Power Plug – Internet based power socket controller.
6. Bluetooth weight scales.
7. Bluetooth Lightbulb

### Research Questions

How can IoT devices adversely affect the security of a “smart home” and its users. What techniques can be deployed against IoT devices to expose their vulnerabilities? Are IoT devices vulnerable? If so what countermeasures can be implemented in order to protect them and their users?

### Research Aims

The overall aim of this investigation is to analyse the possible vulnerabilities of various internet of things devices which could be present in a smart home and were applicable provide suggested suitable countermeasures which could be put in place in order to protect the internet of things devices and their users.

### Research Objectives

This investigation aims to achieve the following objectives:

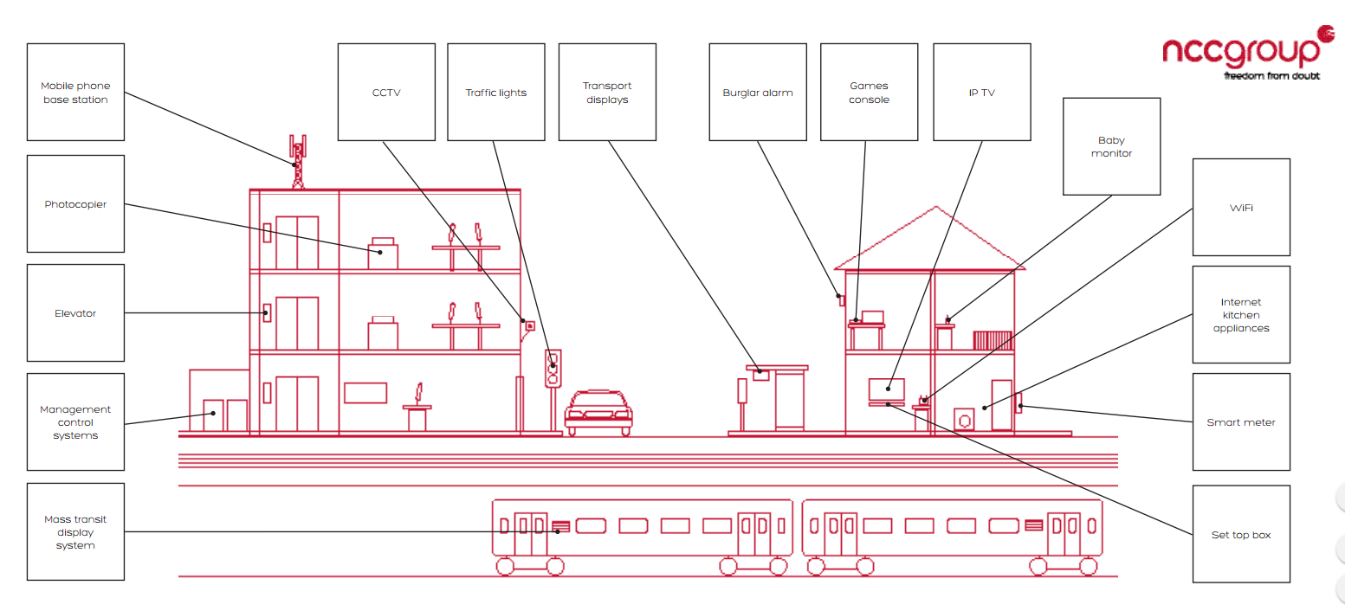
* Analyse the various techniques used to compromise IoT devices.
* Identify Vulnerabilities in all IoT devices Tested.
* Review the level of security present in all IoT devices tested and recommend possible countermeasures to prevent future attacks.

### Statement of Structure

This investigation was based mainly on practical penetration testing of IoT devices with research fundamental to the learning and developing attacks which could be deployed against popular IoT devices thus backing up the practical work carried out. The results of the practical aspects of this investigation were used in conjunction with research to highlight the current state of security in IoT devices and the possible repercussions which users may face as a result. This section of the investigation has been an introduction to the concepts of IoT, Smart Homes and penetration testing. The following section of this investigation is the background and review of current literature which will provide evidence of the current state of play of IoT in the business and consumer markets and will highlight the current academic efforts which aim to assess IoT security. Following the investigation background will be the methodology section documenting the practical steps which were taken to produce the results which will then be discussed with reference to the aims and objectives of this investigation before any conclusions are drawn.

## Background

### IoT Market Projections

The connection of everyday objects to the internet is one of the most discussed about and exciting revelations in modern day technology, this excitement is shared by developers and consumers alike. The main reason for the recent interest in the Internet of Things is its ability to impact on every aspect of modern life.

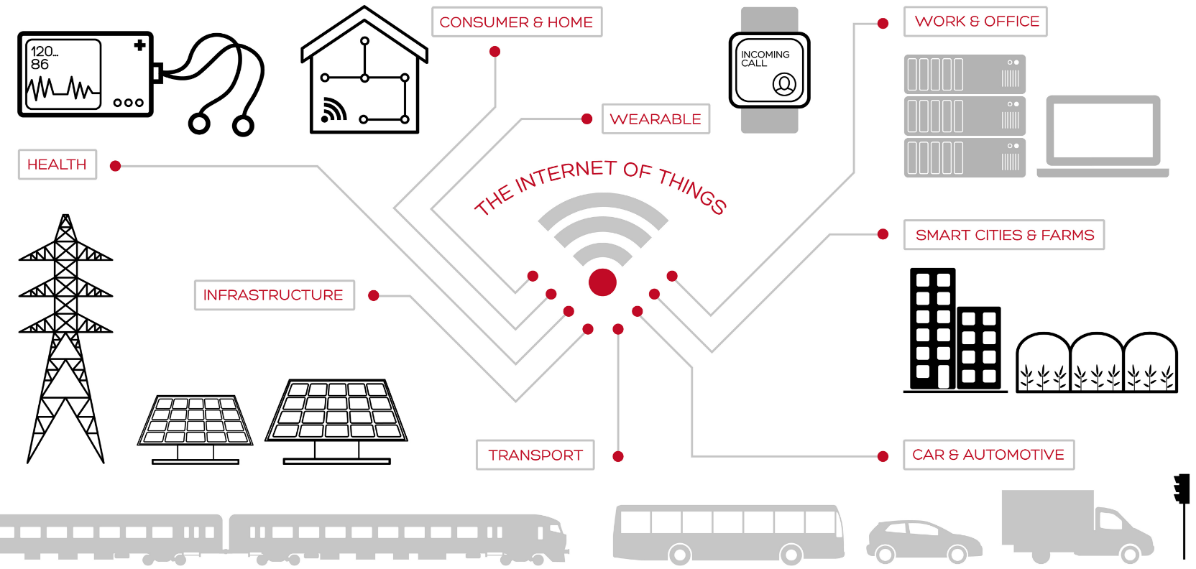


Figure 1 – Aspects of life effected by IoT (NCC Group, 2016) [10]

Which figure is better?

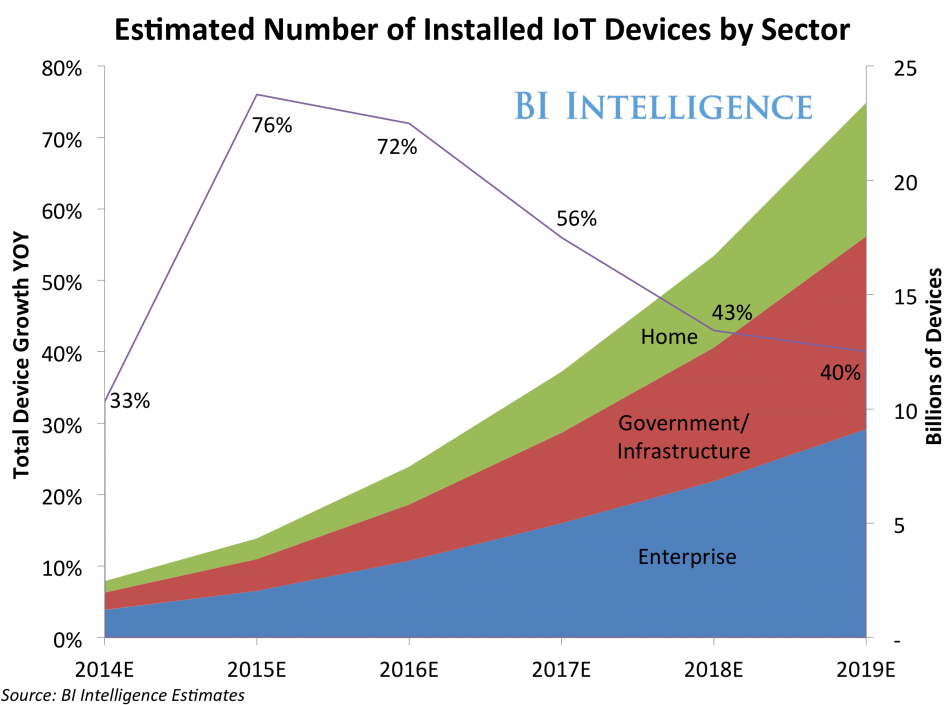
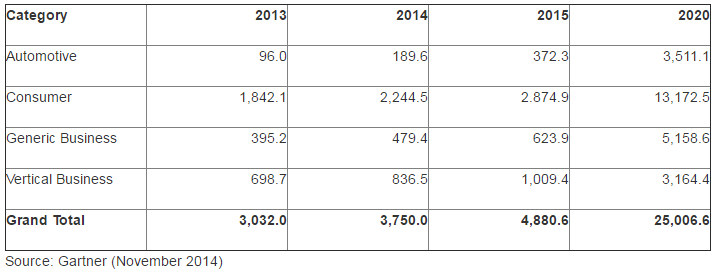
As depicted in figure 1 the Internet of Things is set to influence every sector of industry from home users to enterprise and even government and infrastructure and the rapid developments seem to show no sign of slowing down.

Figure 2 – IoT Market trends by Sector (Business Insider UK, 2014) [11]

Figure 2 above from a report produced by Business Insider UK depicts the current and future market trends of IoT, it estimates that by 2019 the internet of things will have become the “largest device market in the world” [11] more than twice that of the smart phone, PC, tablet, connected car and wearable markets combined [11] this will result in IoT adding $1.7 trillion in value to the global economy in 2019 thus highlighting the huge interest from business in relation to IoT.

Currently the enterprise sector has the largest market share of IoT technologies, however future trends dictate that this share will decline with government and home sectors set to expand rapidly in the near future [11].

According to Gartnerthere will be 25 Billion devices connected to the internet of things in 2020 [12].The vast majority of these devices will be in the consumer sector with over 13 Billion devices.

 Table 2 – IoT Units Installed by Category in Million (Gartner, 2014) [12]

The future growth of the home sector which is set to drive global IoT investments provides the scope for this investigation which will focus on the domestic consumer sector “smart devices” and their users.

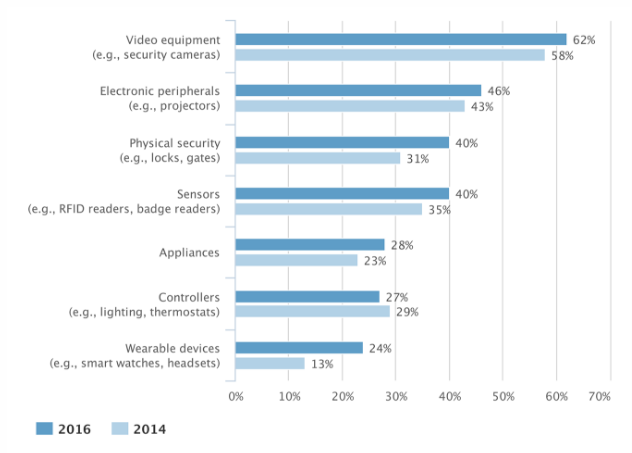
The domestic consumer market consists of a wide verity of technologies from wearable technologies to security cameras, this verity of consumer IoT devices is evidenced in a report by the marketing research organisation “Spiceworks” who surveyed 440 IT professionals across the globe [13].

Figure 3 – Home Internet Enabled devices by category (Spiceworks, 2016) [13]

This report by SpiceWorks shows that currently the most popular IoT devices in the consumer sector are video related devices, it is for this reason that a larger focus on video based IoT devices was adopted with three video based devices being selected to test.

### Cyber Security Implications

#### 2.2.1 Current Landscape

The topic of cybersecurity as a whole, has become a valid and excepted expense in the most modern business models, this has come to be after years of high profile breaches which has opened the eyes of big business to the losses which can be incurred both in relation to financial loss and logical data loss. Recent research conducted by the UK government

Government research found that in the last year 46% of UK businesses experienced a cyber security breach of some kind [14], the study also revealed that 67% of the surveyed businesses have a budget for cyber security but only 11% have a cyber security incident plan [14]. As a direct result of this research governmental bodies are urging businesses to take a more no nonsense approach to the threats of cybersecurity as government themselves has as they recently announced a further £1.9 Billion investment in cybersecurity [14], this large investment highlights the fact that cybersecurity reaches every department of modern life.

This current cybersecurity landscape imposed on government and business is a result of the various legislative and compliance frameworks that now exist within the industry such as PCI DSS compliance for example, which focuses on securing the IT infrastructure and software of businesses which handle card payment transactions, if businesses don’t comply they face large fines. This is just one example of how international legislature can act as an incentive to organisations in relation to increasing their levels of cybersecurity.

#### 2.2.2 Introduction of IoT

As internet of Things devices become more and more prevalent in business and government as they are forecast to, it will only become harder for these sectors to defend against cyber-attacks. This is due to the diverse range of IoT devices which will be used in various areas of business performing a range of tasks from physical security such as IP cameras to sensor based systems at the customer facing front end. The increased usage of these devices will therefore increase the number of potential entry points which attackers could exploit. Currently at the time of writing there is no standards authority regulating the security level of existing or newly developed internet of things devices, the prospect of this wave of technology being introduced to every sector of life without proper scrutiny is a daunting prospect for business, government and consumers alike.

Recent research conducted by Sadeghi, Wachsmann and Waidner (2015)[15] details the security and privacy challenges facing the industrial internet of things, supporting the argument that industry’s current urge to “connect the unconnected” is leaving itself open to further potential entry points for attackers. Sadeghi, Wachsmann and Waidner (2015) [15] state that industry cannot afford to adapt to the threats posed by IoT as slowly as it did to the now accepted threats and common practices of cyber security. Although this statement is agreeable the concepts of IoT security must be viewed upon holistically and organisations must be educated on the threats which may put their systems at risk. This may not be as easy as some may think due to industry’s resilience to inherent further costs and procedures without substantial proof.

### IoT in Industry

In a recent report by SpiceWorks [16], which surveyed 440 industry professionals worldwide, 84% of professionals agreed that the most concerning aspect of Internet of Things integration into industry is that the devices themselves “create more entry points into the network”. The study also details that three quarters of IT pros are also extremely worried that the manufactures of IoT “aren’t implementing sufficient security measures” [16]. Further research conducted by Borgohain, Kumar and Sanyal, (2015) [17] goes as far as to state that based on its survey of vulnerabilities in internet of things devices and systems industry must first focus on securing the IoT infrastructure and devices that currently exist and halt the rapid development of new devices until a point which it can be assured that they can be secured in order to protect consumer and industrial privacy. This strong opinion highlights the severity of the situation according to industry experts.

However this warning to industry seems to have been ignored, again referring to the recent survey carried out by SpiceWorks (2016) [16] in which they asked if organisations are preparing for IoT in the workplace:

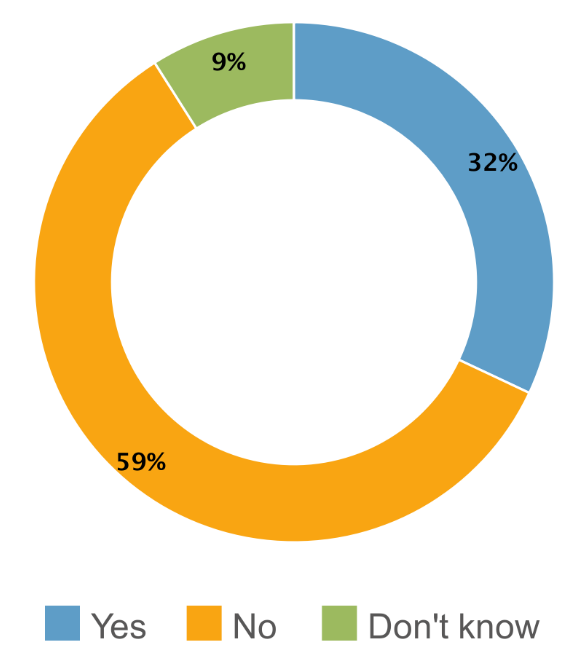


Figure 4 – Preparing for IoT in the workplace (SpiceWorks 2016) [16]

As depicted in figure 4 above, 59% of professionals confessed that they were not in fact preparing for the introduction of IoT in the workplace.

### IoT Architecture

In order to fully understand the vulnerabilities facing the Internet of Things and whether or not they are vulnerable, a large focus on the architecture of IoT, According to research conducted by Yousuf, Mahmoud and Imran Zualkernan, (2015) [18] IoT operates on three layers; The Perception layer, The Network Layer, and the Application layer. The Perception or “Sensors” layer is the layer in which data is acquired, the data is collected and processed in this layer, this data is then sent to the network layer. The network layer of the architecture is responsible for data transmission and routing, it achieves this through making use of wireless technologies such as Wifi, Bluetooth or 3G/4G. These technologies filter and transmit the data to and from the IoT device.

The final layer of architecture proposed by Yousuf, Mahmoud and Imran Zualkernan, (2015) [18] is the application layer, this layer validates the sending and receiving of data to and from the network layer, it achieves this through various authenticity and confidentiality techniques. This research by Yousuf, Mahmoud and Imran Zualkernan, (2015) [18] defines IoT architecture in its simplest form as demonstrated by figure 5 below;

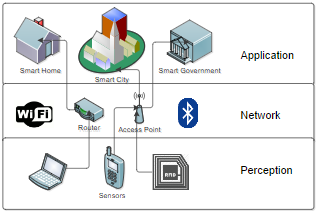


Figure 5 – Three Layer IoT architecture (Yousuf, Mahmoud and Imran Zualkernan, 2015) [18]

However further research conducted by Farooq et al, (2015) [19] proposes a slightly more detailed architecture for the Internet of things with a “Middle-Ware Layer” being added as a fourth layer in between the network layer and the application layer as depicted in figure 5 below;

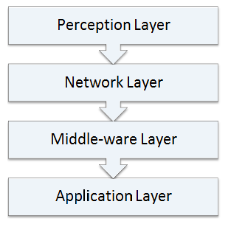


Figure 5 – Four Layer IoT architecture (Farooq et al,2015) [19]

This Middle ware layer acts as a further information processing system automating the delivery of data to relevant databases providing storage capabilities, this then allows the application layer to process the more practical aspects of the architecture with extra resource such as user interaction and the implementation of smart environments and transportation.

### IoT Attack Vectors

Understanding the way in which Internet of Things devices are constructed and operate is vital to identifying the possible techniques which attackers could employ in order to exploit their vulnerabilities.

Research conducted by Abomhara and Køien (2015) [20] details an extensive list of attacks which can exploit vulnerabilities existing in modern IoT devices face. Abomhara and Køien (2015) [20] group the attacks as follows;

* Physical Attacks – Attacks in which the tampering of hardware and connection ports is performed.
* Reconnaissance Attacks – The mapping and discovery of open ports and services as well as gathering IP address information by an attacker.
* Denial of service (DoS) Attacks – An attack which can disable the functionality of the device or the system in which it is a part of.
* Access Attacks – These types of attacks can be grouped into physical access attacks and remote access to attacks. An access attack involves unauthorised access to the device or its network.
* Privacy Attacks – Attacks which aim to steal private user data, privacy attacks can entail data mining, espionage, sniffing and password cracking attacks.

This grouped list off attacks facing IoT devices is testament to the diverse nature of IoT technologies as any number of these attacks can be performed on an IoT device or network. Research carried out by Nawir et al, (2017) [21] mirrors much of this opinion, that the Internet of Things faces substantial amounts of security related issues, this research places an interesting blame on a recent inactivate in china called “Sensing China” an attempt to “rapidly accelerate the development of IoT across the country” (Nawir et al, 2017) [21] , a keen interested is also taken in this research to the usage of IoT devices in denial of service attacks of which several high-profile cases have been documented recently.

### IoT and Botnets

In recent years Distributed Denial of Service (DDoS) attacks have grown in popularity amongst attackers, the attack itself aims to make an online service unavailable to its users, this is achieved through flooding the services servers with extremely large amounts of information or “traffic” (Mirkovic, Prier and Reiher, 2003) [22], this traffic is sent to the services servers from multiple sources often making use of a “botnet”. A “botnet” is a “large collection of well-connected compromised machines that can be co-ordinated to partake in malicious activities” (Rajab et al., 2007) [23]. As conventional DDoS attacks have grown in popularity over recent years as to has the defence against them, organisations are monitoring their traffic and communications with the outside world with a lot more scrutiny this has resulted in attackers resorting to think outside the box in terms of approach and scale of DDoS attacks, especially the size and scale of the botnets used.

In September 2016 the Mirai botnet announced its presence as the key behind the largest DDoS attack in history (Newman, 2016) [24]. Mirai operated by implanting malware onto vulnerable IoT devices such as IP Cameras, smart DVRs and routers, in doing so Mirai managed to compromise as many as “half a million devices” in 164 countries according to research conducted by Angrishi (2017) [25]. This huge number of compromised devices allowed the Mirai botnet to produce a record braking 1.1Tbps DDoS attack (Angrishi 2017) [25] and through doing so managed to take out a number of high profile internet based services such as Amazon, Spotify, Twitter and many, many more (Cox, 2016) [26].

Figure 6 below depicts the distribution of the Mirai Botnet as of 26th October 2016;



Figure 6 – Distribution of Mirai Botnet (Angrishi 2017) [25]

The current academic climate clearly dictates a feeling of unrest in relation the IoT security amongst security professionals and researchers alike as evidenced through numerous sources, through the latest research of the Mirai botnet it appears as though these feelings of unrest are well warranted as many feel as though this is just the beginning. However the academic climate seems to be overwhelmingly focused on the big picture of IoT security and therefore much of the current research fails to detail exactly how vulnerable the internet of things is through practical methods. The following sections of this investigation aims to build upon the evidenced current research that documents the possible security vulnerabilities and architecture structures with the overall aim of creating a step to step guide to exploit some of these vulnerabilities to judge if IoT devices are on an individual level as vulnerable as security experts dictate.

### OWASP IoT top Ten

In order to assess the level of security present on the internet of things devices tested in this investigation the Open Web Application Security Project (OWASP) Internet of Things testing methodology was adopted [27]. OWASP is a non-profit organisation operated by security professionals all over the world. The main reason for choosing this methodology is its open source nature and therefore its free to use and distribute. The OWASP IoT methodology itself replicates the original OWASP penetration testing methodology which is based on the OWASP top ten which is a list of vulnerabilities which OWASP deem to be the most crucial to systems.

The OWASP IoT top Ten vulnerabilities are as follows;

1. Insecure Web Interface

The assessment of insecure web interfaces will not be explored in this investigation as explicit consent has not been granted, this will form part of the future work section of this document.

1. Insufficient Authentication

To test for insufficient authentication analysis of default system passwords will be performed. Network traffic analysis will lso be performed with Wireshark.

1. Insecure Network Services

The NMAP tool will be used to assess the IoT devices their open ports and services which are running on those ports.

1. Lack of Transport Encryption

The lack of transport encryption will be assessed using Wireshark to determine whether data is being properly encrypted when transported or if data is transported in plain text.

1. Privacy Concerns

Privacy concerns will be explored with the use of sniffing and file exploration depending on the existing vulnerabilities of the IoT device

1. Insecure Cloud Interface

Devices using a cloud interface will be assessed through account enumeration. Traffic analysis will be performed with Wireshark to determine any exposed credentials or account vulnerabilities.

1. Insecure Mobile Interface

Mobile interface vulnerabilities will be explored using packet sniffing techniques with Wireshark and account enumeration.

1. Insufficient Security Configurability

The configurability of all devices will be investigated focusing on the extent which permissions can be configured and configurability options available.

1. Insecure Software/Firmware

Insecure software present on the devices will be investigated to determine file encryption levels, verification methods and update functionality as well as a further focus on firmware containing sensitive information.

1. Poor Physical Security

The devices will be analysed in relation to the accessing of software via physical ports such as USB and the possible presence or use of removable storage media.

The following section of this investigation documents the practical steps which were taken to assess the level of security of each individual Internet of Things Device tested in the scope of this investigation.

## Methodology

### IP Security Camera 1

### IP Security Camera 2

### Baby Monitor

### Bluetooth Heart Rate and Blood Pressure Monitor

### Smart Power Plug

### Bluetooth weight scales

### Bluetooth Lightbulb



## Results

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IOT Device Vulnerability table | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | Vulnerabilities --> | Insufficient Authentication / Authorization | Insecure Network Services | Lack of Transport Encryption | Privacy Concerns | Insecure Mobile Interface | Insufficient security configurability | Insecure software/firmware | Poor Physical Security |
|  |  |
| ID No. | Device |  |  |  |  |  |  |  |  |
| 1 | IP Camera 1 |  |  |  |  |  |  |  |  |
| 2 | IP Camera 2 (With Sound) |  |  |  |  |  |  |  |  |
| 3 | Blood pressure Monitor |  |  |  |  |  |  |  |  |
| 4 | Smart Power Plug |  |  |  |  |  |  |  |  |
| 5 | IP Camera 3 (Baby Monitor) |  |  |  |  |  |  |  |  |
| 6 | Bluetooth Scales |  |  |  |  |  |  |  |  |
| 7 | Bluetooth Lightbulb |  |  |  |  |  |  |  |  |

Table 3 – IoT Vulnerability Results Table

## Discussion

### Case Studies

### Real World Implications

### Countermeasures

## Conclusion

### Future work

# Appendices

# List of References

[1] [6] [7] Office for National Statistics, “Internet access – households and individuals: 2016” (4/8/2016) [Online] Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016> [Accessed March 2017].

[2] Klaus, Schwab, “The Fourth Industrial Revolution: what it means, how to respond” (14/1/2016) [Online] Available at: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> [Accessed October 2016].

[3] Oxford Dictionary, “Internet of Things” [Online] Available at:

<https://en.oxforddictionaries.com/definition/internet\_of\_things>

[Accessed September 2016].

[4] Deoras, Srishti, “First ever IoT device- “The Internet Toaster”” (5/8/2016) [Online] Available at: <http://iotindiamag.com/2016/08/first-ever-iot-device-the-internet-toaster/> [Accessed February 2017].

[5] Ashton, Kevin, “That 'Internet of Things' Thing”” (22/6/2009) [Online] Available at: <http://www.rfidjournal.com/articles/view?4986 > [Accessed March 2017].

[8] Deloitte Statistics, “The Internet of Things (IoT): most entertaining” (2016) [Online] Available at: <https://www.deloitte.co.uk/mobileuk/internet-of-things/> [Accessed March 2017].

[9] Rouse, Margaret, “Whatis.com - pen test (penetration testing)” [Online] Available at: <https://www.deloitte.co.uk/mobileuk/internet-of-things/> [Accessed March 2017].

[10] NCC Group, “Internet of Things (IoT)” (2016) [Online] Available at: <https://www.nccgroup.trust/uk/our-solutions/your-sectors/internet-of-things/> [Accessed November 2016].

[11] Greenough, John, “The 'Internet of Things' Will Be the World's Most Massive Device Market and Save Companies Billions of Dollars” (18/11/2014) [Online] Available at:

<http://uk.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?r=US&IR=T>[Accessed October 2016].

[12] Gartner Inc., “Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015” (11/11/2014) [Online] Available at:

<https://www.gartner.com/newsroom/id/2905717>

[Accessed September 2016].

[13][16] SpiceWorks IT, “2016 IoT Tends: The Devices have Landed, How IT and IoT are learning to peacefully coexist” (2016) [Online] Available at:

<https://www.spiceworks.com/marketing/reports/iot-trends/#section-0>

[Accessed October 2016].

[14] Klahr, R., Shah, J., Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V. Cyber security breaches survey 2017 Main report (2017). [Online] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/609186/Cyber\_Security\_Breaches\_Survey\_2017\_main\_report\_PUBLIC.pdf> [Accessed 15 Apr. 2017].

[15] Sadeghi, A., Wachsmann, C. and Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. [Online] Available at: <http://ieeexplore.ieee.org/document/7167238/> [Accessed 20 February 2017].

[17] Borgohain, T., Kumar, U. and Sanyal, S. (2015). Survey of Security and Privacy Issues of Internet of Things. [Online] Available at: <https://www.researchgate.net/publication/270763270\_Survey\_of\_Security\_and\_Privacy\_Issues\_of\_Internet\_of\_Things> [Accessed 10 Feb. 2017].

[18] Yousuf, T., Mahmoud, R. and Imran Zualkernan, F. (2015). nternet of Things (IoT) Security: Current Status, Challenges and Countermeasures. [Online] Available at: <https://www.researchgate.net/publication/300413927\_Internet\_of\_things\_IoT\_security\_Current\_status\_challenges\_and\_prospective\_measures> [Accessed 10 Feb. 2017].

[19] Farooq, M., Waseem, M., Khairi, A. and Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). [Online] Available at: <https://www.researchgate.net/publication/272488555\_A\_Critical\_Analysis\_on\_the\_Security\_Concerns\_of\_Internet\_of\_Things\_IoT> [Accessed 10 Feb. 2017].

[20] Abomhara, M. and Køien, G. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. [Online] Available at: <https://s3.amazonaws.com/academia.edu.documents/39628024/Cyber\_Security\_and\_the\_Internet\_of\_Thing20151102-5470-rumluk.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1492727999&Signature=08kKMpmV6nyHIlyIfyWikevYyqQ%3D&response-content-disposition=inline%3B%20filename%3DCyber\_Security\_and\_the\_Internet\_of\_Thing.pdf> [Accessed 10 Feb. 2017].

[21] Nawir, M., Amir, A., Yaakob, N. and Lynn, O. (2017). Internet of Things (IoT): Taxonomy of security attacks - IEEE Xplore Document. [online] Available at: <http://ieeexplore.ieee.org/document/7804660/> [Accessed 20 Feb. 2017].

[22] Mirkovic, J., Prier, G. and Reiher, P. (2003). Attacking DDoS at the source - IEEE Xplore Document. [Online] Available at: <http://ieeexplore.ieee.org/abstract/document/1181418/> [Accessed 10 Feb. 2017].

[23] Rajab, M., Zarfoss, J., Monrose, F. and Terzis, A. (2007). My Botnet is Bigger than Yours (Maybe, Better than Yours. [Online] Available at: <https://www.usenix.org/legacy/event/hotbots07/tech/full\_papers/rajab/rajab.pdf> [Accessed 10 Nov. 2016].

[24] Newman, L. (2016). The Botnet That Broke The Internet. [Online] Wired.com. Available at: <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/> [Accessed 3 Nov. 2016].

[25] Angrishi, K. (2017). Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. [Online] Available at: <https://arxiv.org/pdf/1702.03681.pdf> [Accessed 20 Mar. 2017].

[26] Cox, E. (2016). Mirai IoT Botnet: 5 Fast Facts You Need to Know. [Online] Available at: <http://heavy.com/tech/2016/10/mirai-iot-botnet-internet-of-things-ddos-attacks-internet-outage-blackout-why-is-internet-down/> [Accessed 3 Nov. 2016].

[27] OWASP Internet of Things Project Top Ten (10/9/2016) [Online], Available at:

<https://www.owasp.org/index.php/OWASP\_Internet\_of\_Things\_Top\_Ten\_Project>

[Accessed September 2016].

# Bibliography

If required