

|  |
| --- |
| 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](#_Toc479075555)

[Table of Figures iii](#_Toc479075556)

[Acknowledgements v](#_Toc479075557)

[University of Abertay Dundee Permission To Copy vi](#_Toc479075558)

[Abbreviations, Symbols, Notation and Glossary of Terms vii](#_Toc479075559)

[1. Introduction 1](#_Toc479075560)

[1.1. Introduction to IoT 1](#_Toc479075561)

[1.2. History of IoT 2](#_Toc479075562)

[1.3. The Modern Smart Home 3](#_Toc479075563)

[1.4. Penetration Testing and IoT 4](#_Toc479075564)

[1.5. Devices Tested in this project 5](#_Toc479075565)

[1.6. Research Questions 5](#_Toc479075566)

[1.7. Research Aims 5](#_Toc479075567)

[1.8. Research Objectives 5](#_Toc479075568)

[1.9. Statement of Structure 6](#_Toc479075569)

[2. Background 7](#_Toc479075570)

[2.1. Business Implications 7](#_Toc479075571)

[2.2. Future Projections 7](#_Toc479075572)

[Appendices 8](#_Toc479075573)

[List of References 9](#_Toc479075574)

[Bibliography 10](#_Toc479075575)

# Table of Figures

**No table of figures entries found.**Table of Tables

[Table 1 – Fourth Industrial Revolution 1](#_Toc479023569)

# 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, FK219XE

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

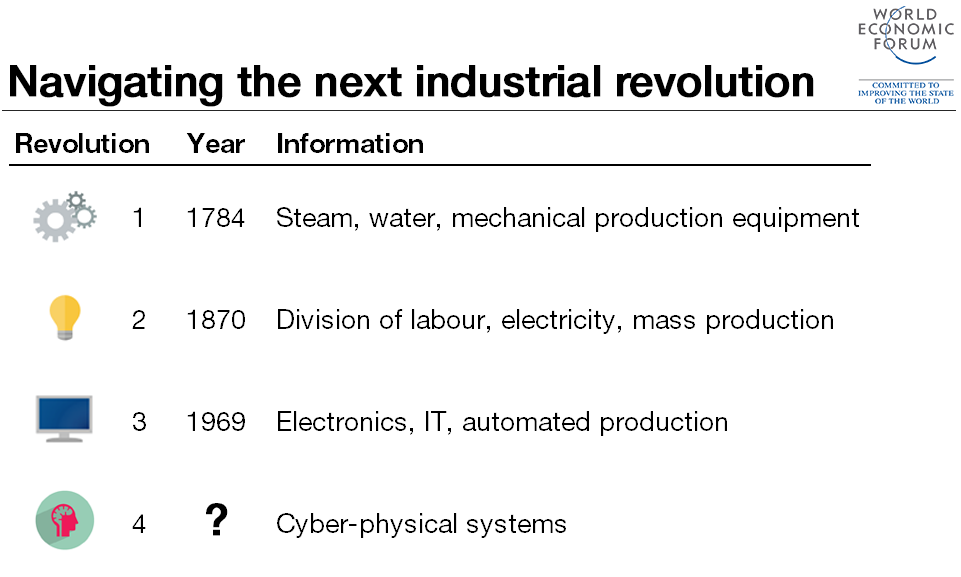
Since its invention in the late 1960s as a part of the third industrial revolution, the internet as we know it has underwent many transformations most notably the invention of the World Wide Web by Sir Tim Berners-Lee in 1990 which introduces the world to the concepts and advantages of interconnectivity. 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.
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

### Business Implications

### Future Projections

# 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].

# Bibliography

If required