Investigating Vulnerabilities in IoT devices in the context of a smart home

Michael W Crow - 1202317

BSc Ethical Hacking and Countermeasures,
2017

School of Arts, Media and Computer Games
Abertay University

Abstract

The Internet of Things, albeit not a new concept, is one of the most exciting and talked about technologies of the decade. The Internet of Things promises to impact upon many, if not all aspects of modern society and so developments should be met with great ambition and enthusiasm as the Internet of Things in the very near future promises to revolutionise the way we live, work and play. However, not everyone is that excited for the rapid technological developments and forecast business growth, IT security professionals across the globe are ringing alarm bells amongst all sectors of society; home, business and even at governmental level about the potential vulnerabilities which could be present on these Internet of Things devices and the multiple ways in which they can harm each sector both together and separately, but is it as insecure as everyone is claiming?

This investigation through research aims to collect the current views and opinions of the current IT security professionals and the current and future trends of the Internet of Things. Practical analysis of a set of Internet of Things devices will then be analysed to determine if in fact they are vulnerable and if so how vulnerable are they? And what are the most and least common vulnerabilities in the current state of Internet of Things climate.

The practical stages of this investigation are documented in such a way that the techniques used and attacks carried out in this investigation could be repeated in order to raise awareness of the types of ways an attacker could attempt to compromise a “smart device”.

Finally, as conclusions are drawn about the overall level of security present on Internet of Things devices, possible countermeasures will be provided in order to aid in making the internet of things, specifically domestic “smart homes” safer for users and their personal data.

Table of Contents

Table of Figures

Table of Tables

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 - Internet of Things.

P&G - Proctor and Gamble.

Smart Device – An interconnected IoT device.

Smart Home – An Interconnected home of multiple IoT devices.

Penetration or Pen Test – The performing of security testing from an offensive point of view in order to gain an overall level of security present in hope of further securing the system or device as a result.

Penetration tester – the person or persons who conduct the penetration test.

White Hat hacking – The testing or hacking of a system or device with the explicit permission of the intellectual property owner.

Black Hat hacking – The testing or hacking of a system or device with no permission of the intellectual property owner.

1. Introduction

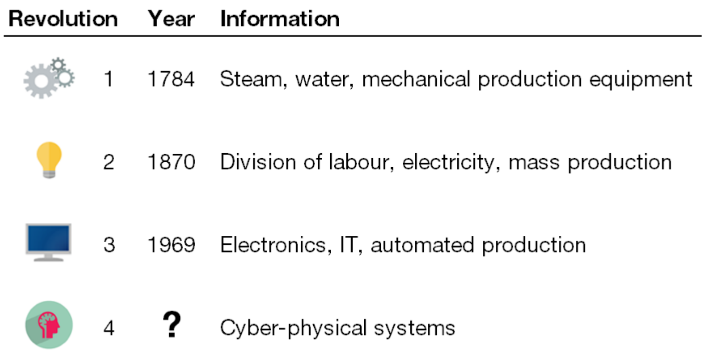
In the modern age in which we live very few aspects of life are hidden from the ever-advancing wave of modern technology, according to the office for national statistics in 2016, 89% of households in the UK had access to the internet [1] this compared to just ten years before in 2006 when only 57% of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

1.1. 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 introduced 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].



Revolution	Year	Information
1	1784	Steam, water, mechanical production equipment
2	1870	Division of labour, electricity, mass production
3	1969	Electronics, IT, automated production
4	?	Cyber-physical systems

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.

1.2. 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 2^{128} unique internet IP addresses compared to only 2^{32} (4.29 Billion) 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.

1.3. 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.

1.4. 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.

1.5. 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.

1.6. 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?

1.7. 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.

1.8. 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.

1.9. 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.

2. Background

2.1. 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.

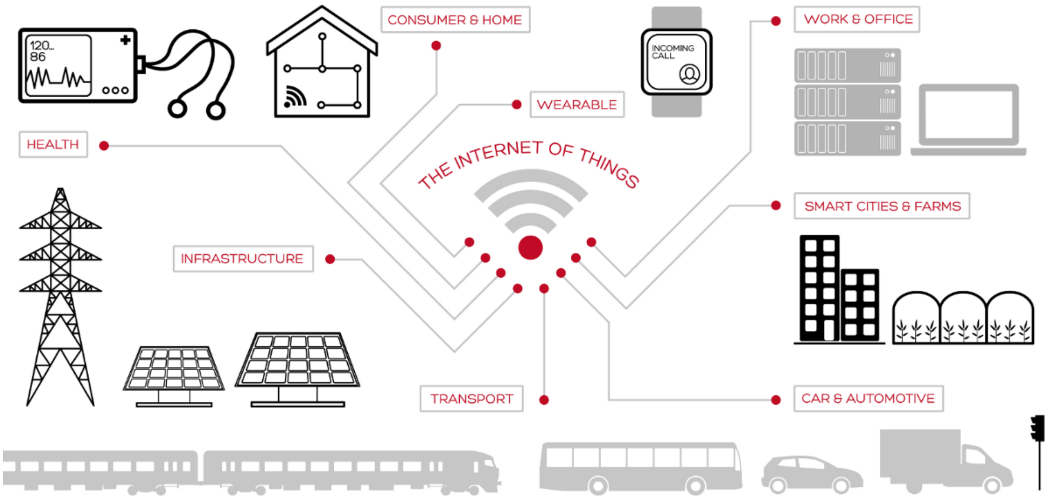


Figure 1 – Aspects of life effected by IoT (NCC Group, 2016) [10]

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.

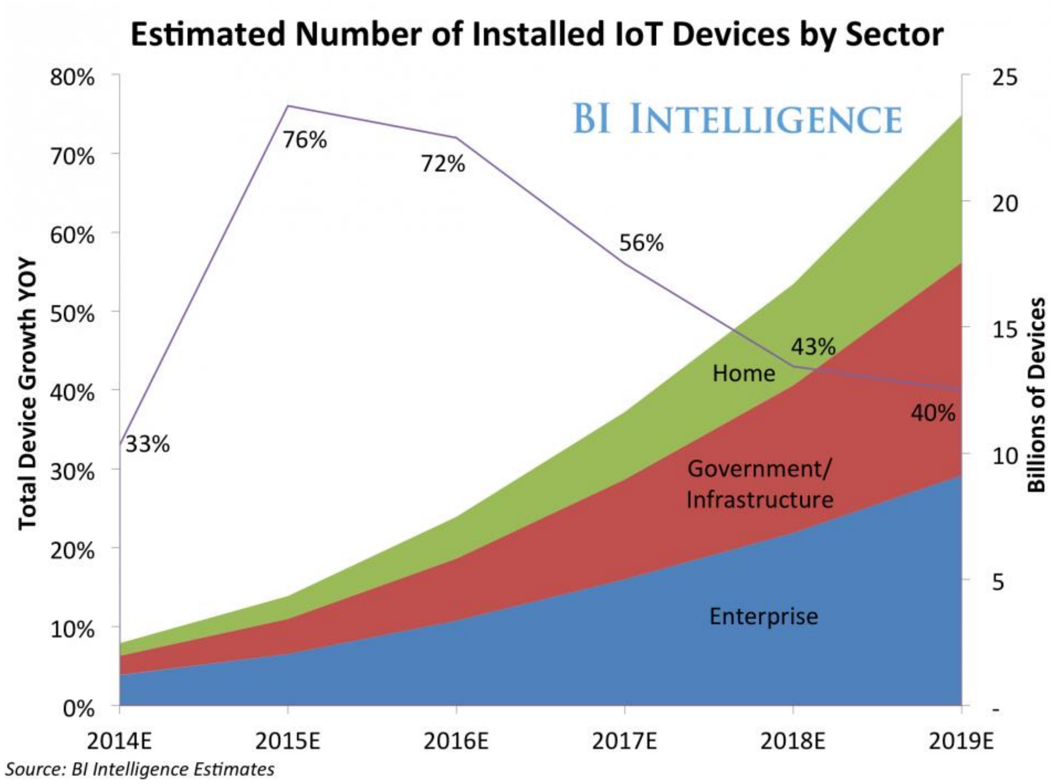
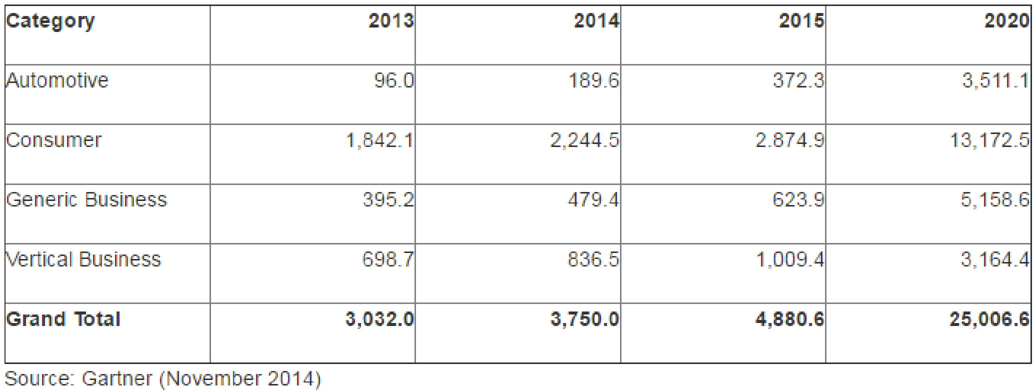


Figure 2 – IoT Market trends by Sector (Business Insider UK, 2014) [11]

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 Gartner there 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.



Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Source: Gartner (November 2014)

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].

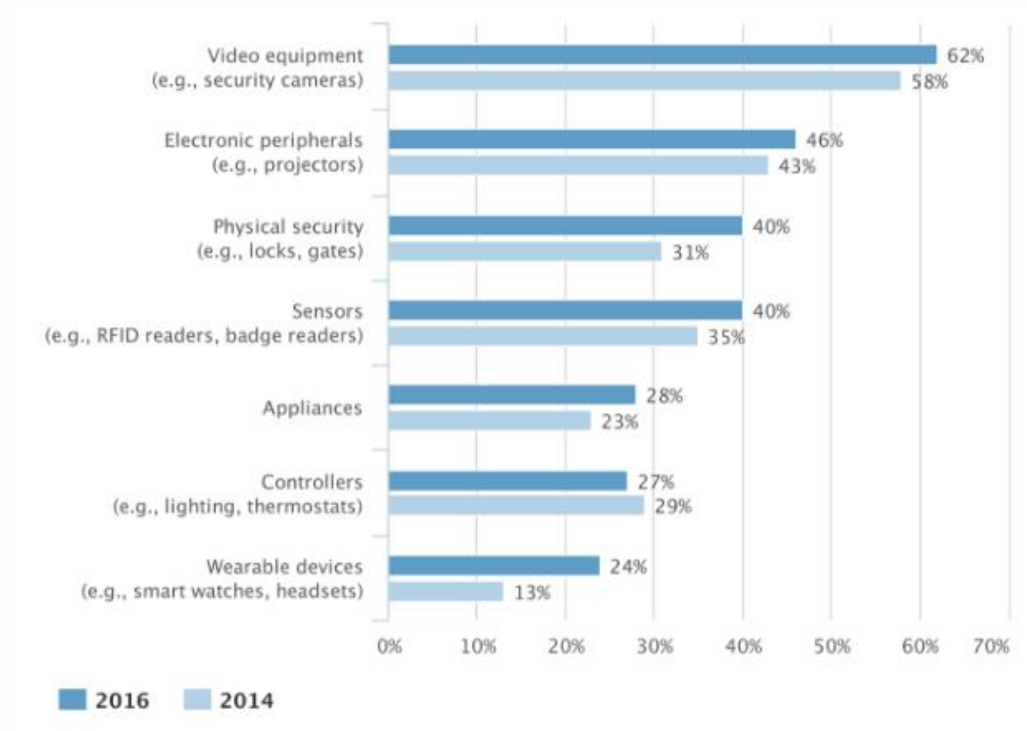


Figure 3 – Home Internet Enabled devices by category (Spiceworks, 2016) [13]

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.

2.2. 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 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.

2.3. 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:

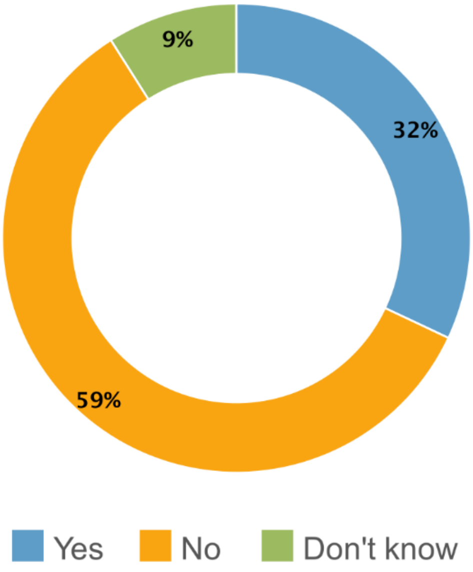


Figure 4 – Preparing for IoT in the workplace (SpiceWorks 2016) [16]

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.

2.4. 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 must be adopted. 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 Wi-Fi, 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. The application 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;

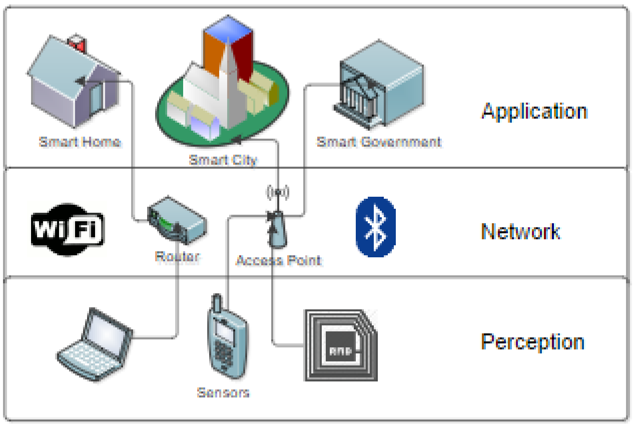


Figure 5 – Three Layer IoT architecture (Yousuf, Mahmoud and Imran Zualkernan, 2015) [18]

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 6 below;

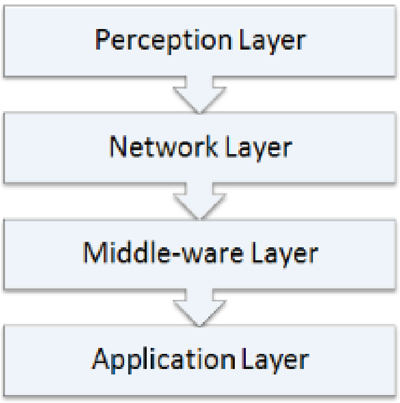


Figure 6 – Four Layer IoT architecture (Farooq et al,2015) [19]

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.

2.5. 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 initiative 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.

2.6. 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 servers of the service with extremely large amounts of information or "traffic" (Mirkovic, Prier and Reiher, 2003) [22], this traffic is sent to the 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 7 below depicts the distribution of the Mirai Botnet as of 26th October 2016;

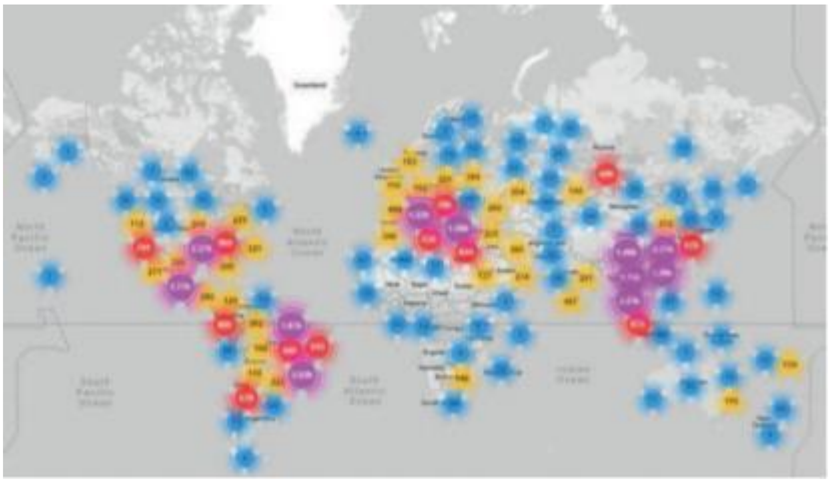


Figure 7 – Distribution of Mirai Botnet (Angrishi 2017) [25]

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.

2.7. 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**
2. **Insufficient Authentication**
3. **Insecure Network Services**
4. **Lack of Transport Encryption**
5. **Privacy Concerns**
6. **Insecure Cloud Interface**
7. **Insecure Mobile Interface**
8. **Insufficient Security Configurability**
9. **Insecure Software/Firmware**
10. **Poor Physical Security**

3. Methodology

This section of the 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.

As previously discussed the practical aspects of this investigation were carried out referencing the OWASP IoT Top ten testing project and methodology.

3.1. Data Collection Methods

A total of six IoT devices were tested in this investigation, the devices were all tested in a lab and home environments using multiple PC computers running Kali Linux, Windows 7 and Windows 10 combined with an iPhone 6s for the mobile interface applications. All results have been kept strictly confidential with the investigator and project supervisor.

3.1. Ethical Considerations

Only proof of concept data was using the testing of all applications therefore no personal user information was obtained or distributed. Any testing which could impact negatively on the devices services was not performed, therefore some areas of the OWASP IoT methodology testing was not performed such as web application testing due to ethical and legal reasons.

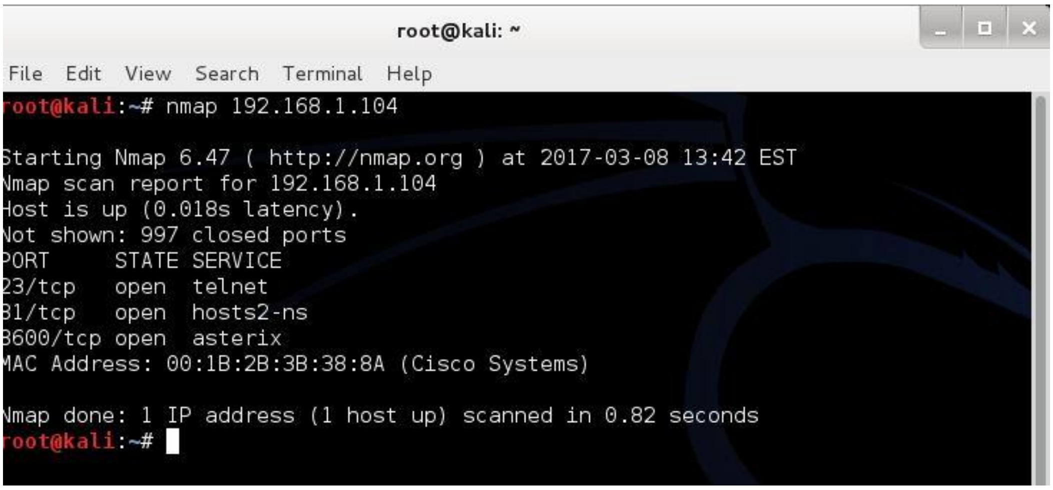
3.2. IP Security Camera 1

The first device which was tested in this investigation was IP Security Camera 1, this generic IP camera operated over Wi-Fi and through Ethernet connection. It operates as a live CCTV network camera which has the capability of mobile, browser and desktop application viewing. Mobile viewing can also be done remotely via a mobile application. The camera allows for the user so store images and video at set intervals or constantly.

IP Security camera was set up in a lab testing environment connected via Ethernet to begin with for calibration until Wi-Fi capability was set up.

The first stage of testing this camera involved performing an Nmap [28] scan against the IP address of the camera. Nmap [28] is a free to use tool which is used for port scanning and network exploration including what services are running on the open ports of the device [28]. The IP address of the camera in this case was found to be 192.168.1.104.

The Nmap [28] scan results for IP Camera 1 can be evidenced in figure 8 below;



```
oot@kali:~# nmap 192.168.1.104

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-08 13:42 EST
Nmap scan report for 192.168.1.104
Host is up (0.018s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
81/tcp   open  hosts2-ns
8600/tcp open  asterix
MAC Address: 00:1B:2B:3B:38:8A (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
oot@kali:~# █
```

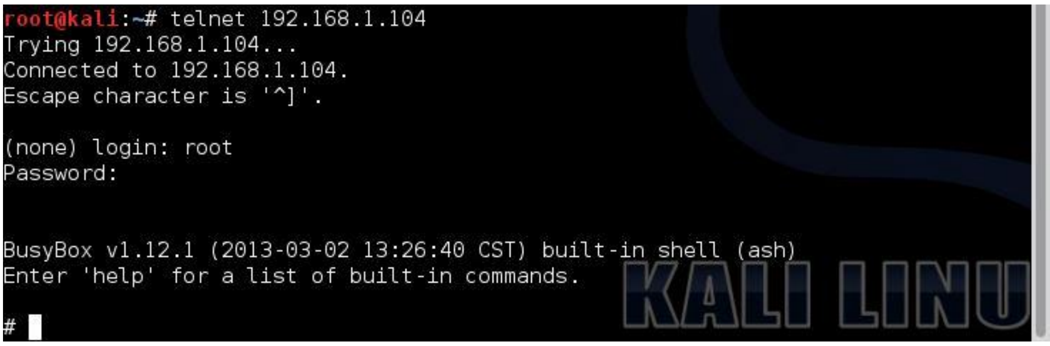
Figure 8 – Nmap Scan IP Camera 1

The Nmap [28] scan clearly shows three open ports on the device;

- TCP Port 23- Telnet
- TCP Port 81 – hosts2-ns
- TCP Port 8600 – asterix

The presence of an open telnet service running on its default port was of much interest as telnet is a service which allows for the remote connection to network devices.

The next stage of the test was to attempt to remotely connect to the camera via its telnet service.



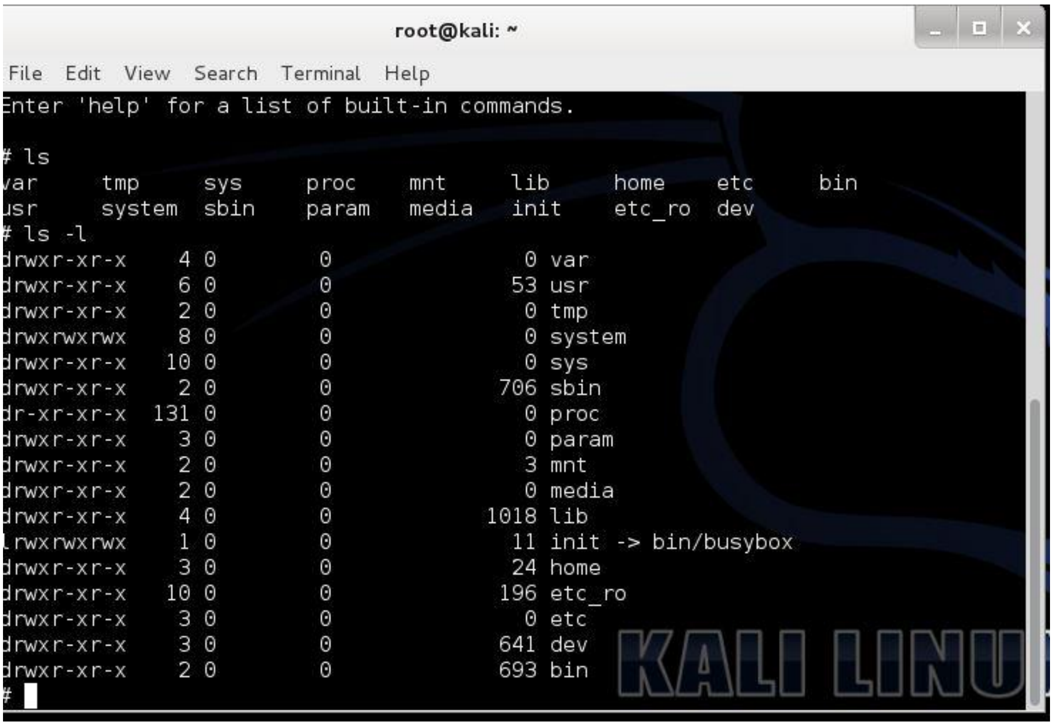
```
root@kali:~# telnet 192.168.1.104
Trying 192.168.1.104...
Connected to 192.168.1.104.
Escape character is '^]'.

(none) login: root
Password:


BusyBox v1.12.1 (2013-03-02 13:26:40 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# █
```

Figure 9 – Telnet IP Camera 1

As evidenced in figure 9 above access to the IP Camera was granted, this was achieved by simply guessing the root password of the device, the following credentials were used to connect via telnet to the camera;

- Login – **root**
- Password – **123456**

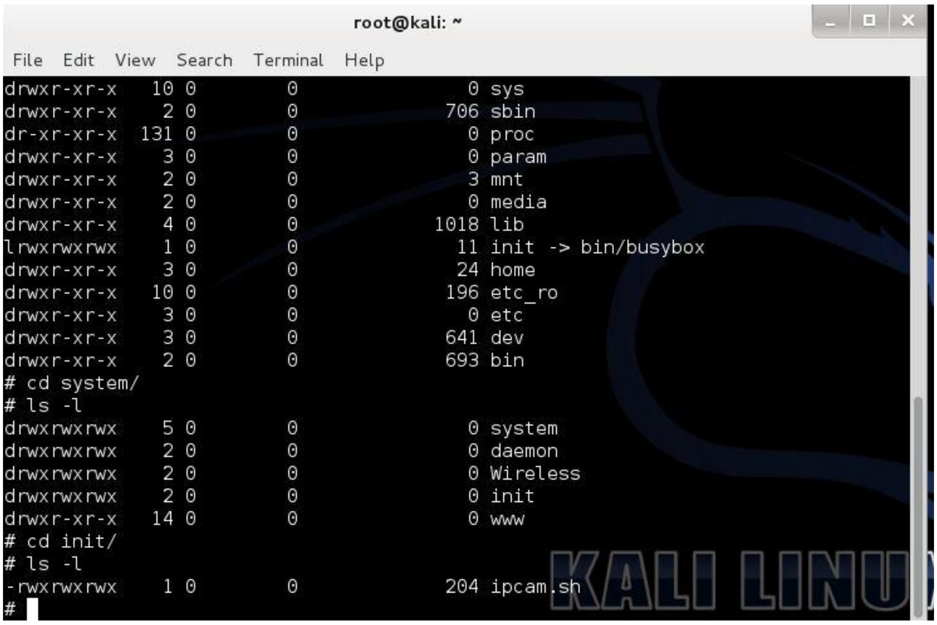
Once connected to the camera exploration of the files present on the IP Camera could be carried out. Files present on the device are presented in in figure 10 below;



```
Enter 'help' for a list of built-in commands.

# ls
var     tmp     sys     proc    mnt     lib     home    etc     bin
usr     system  sbin    param   media   init    etc_ro  dev
# ls -l
drwxr-xr-x    4 0        0               0 var
drwxr-xr-x    6 0        0              53 usr
drwxr-xr-x    2 0        0               0 tmp
drwxrwxrwx    8 0        0               0 system
drwxr-xr-x   10 0        0               0 sys
drwxr-xr-x    2 0        0             706 sbin
dr-xr-xr-x  131 0        0               0 proc
drwxr-xr-x    3 0        0               0 param
drwxr-xr-x    2 0        0               3 mnt
drwxr-xr-x    2 0        0               0 media
drwxr-xr-x    4 0        0            1018 lib
lrwxrwxrwx    1 0        0              11 init -> bin/busybox
drwxr-xr-x    3 0        0              24 home
drwxr-xr-x   10 0        0             196 etc_ro
drwxr-xr-x    3 0        0               0 etc
drwxr-xr-x    3 0        0             641 dev
drwxr-xr-x    2 0        0             693 bin
#
```

Figure 10 – IP Camera 1 file system

After further exploring the files within the IP Cameras system an interesting file called “ipcam.sh” was discovered, the location of this file within the system was “/system/init/ipcam.sh” which can be seen in figure 11 below;

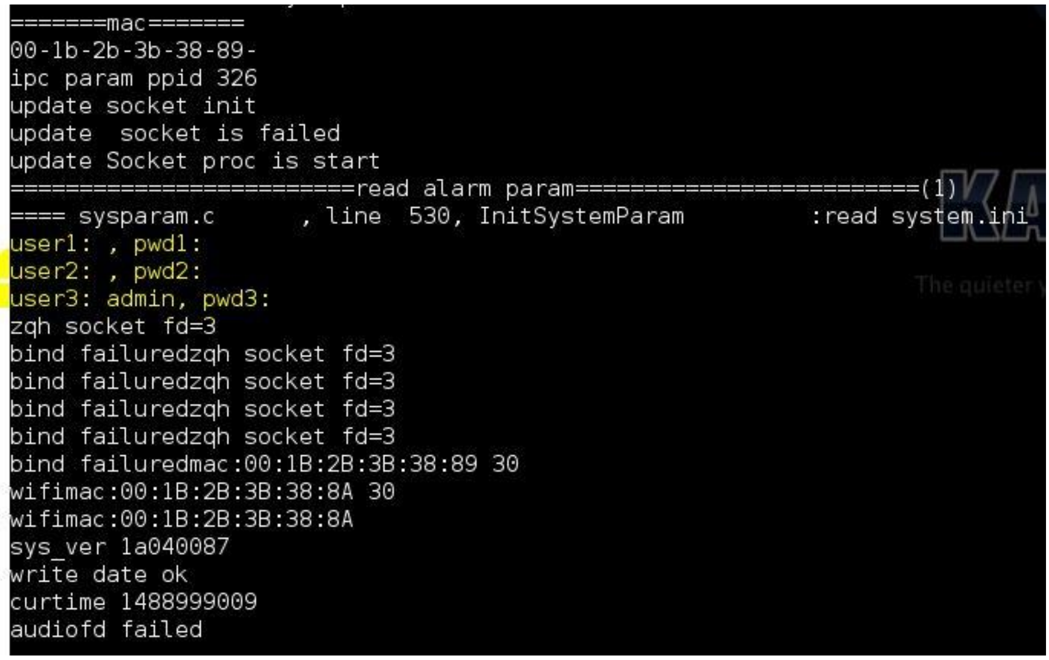


```
drwxr-xr-x   10 0        0               0 sys
drwxr-xr-x    2 0        0             706 sbin
dr-xr-xr-x  131 0        0               0 proc
drwxr-xr-x    3 0        0               0 param
drwxr-xr-x    2 0        0               3 mnt
drwxr-xr-x    2 0        0               0 media
drwxr-xr-x    4 0        0            1018 lib
lrwxrwxrwx    1 0        0              11 init -> bin/busybox
drwxr-xr-x    3 0        0              24 home
drwxr-xr-x   10 0        0             196 etc_ro
drwxr-xr-x    3 0        0               0 etc
drwxr-xr-x    3 0        0             641 dev
drwxr-xr-x    2 0        0             693 bin
# cd system/
# ls -l
drwxrwxrwx    5 0        0               0 system
drwxrwxrwx    2 0        0               0 daemon
drwxrwxrwx    2 0        0               0 Wireless
drwxrwxrwx    2 0        0               0 init
drwxr-xr-x   14 0        0               0 www
# cd init/
# ls -l
-rwxrwxrwx    1 0        0             204 ipcam.sh
#
```

Figure 11- ipcam.sh file location

When the file “ipcam.sh” was run it returned interesting results as the complete system setup and configuration of the IP Camera was dumped to the screen. A full export of the system configuration dump can be referenced in **Appendices 7.1**.

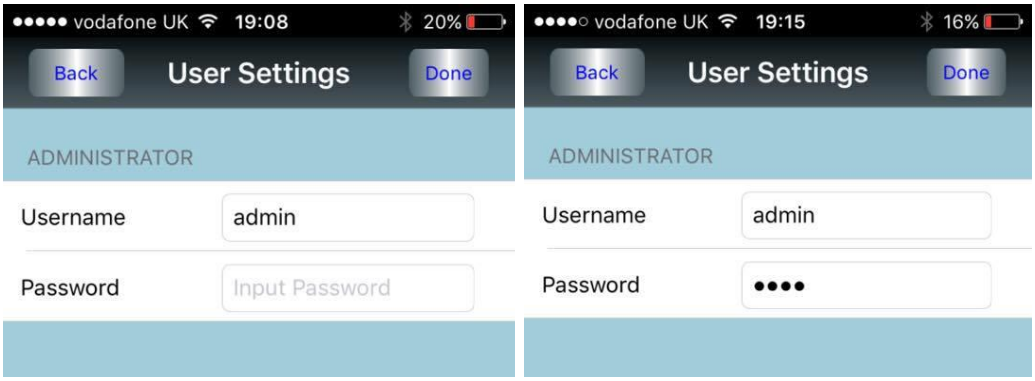
Upon close inspection of the system configuration dump it was discovered that all username and password information was displayed as shown in figure 12 below;



```
=======mac=======
00-1b-2b-3b-38-89-
ipc param ppid 326
update socket init
update  socket is failed
update Socket proc is start
=========================read alarm param=========================(1)
==== sysparam.c      , line  530, InitSystemParam        :read system.ini
user1: , pwd1:
user2: , pwd2:
user3: admin, pwd3:
zqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredmac:00:1B:2B:3B:38:89 30
wifimac:00:1B:2B:3B:38:8A 30
wifimac:00:1B:2B:3B:38:8A
sys_ver 1a040087
write date ok
curtime 1488999009
audiofd failed
```

Figure 12 – Username and password dump

In order to confirm that this was in fact the usernames and passwords of the user accounts the password was changed using the mobile application evidenced in figure 13 below;

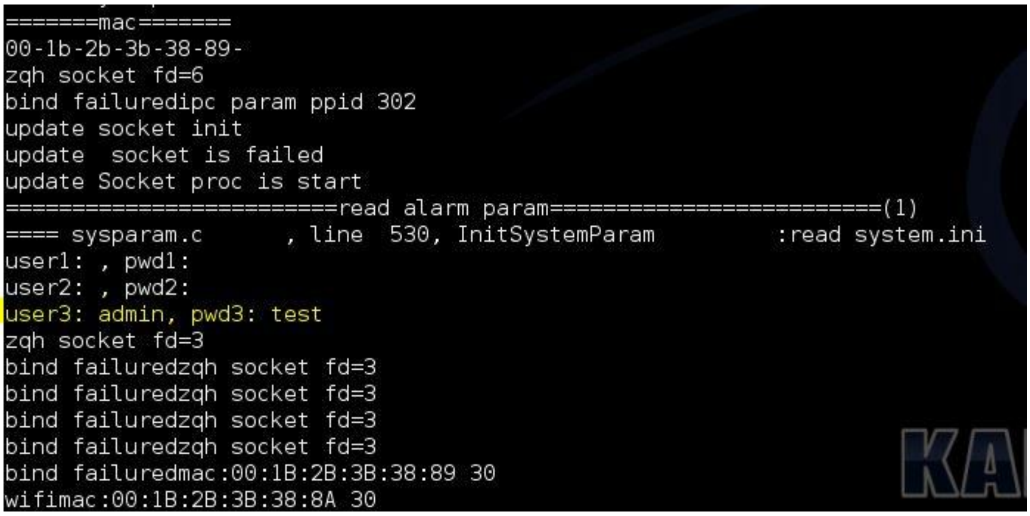


Username admin
Password Input Password

Username admin
Password ••••

Figure 13 – Password change test

The password was changed to “test” using the mobile application. Once the password was changed the “ipcam.sh” file was executed once again which confirmed suspicions that the dumped usernames and password in question were in fact accurate. Evidence of the dumped usernames and passwords after the changing of the user’s passwords is demonstrated in figure 14 below;



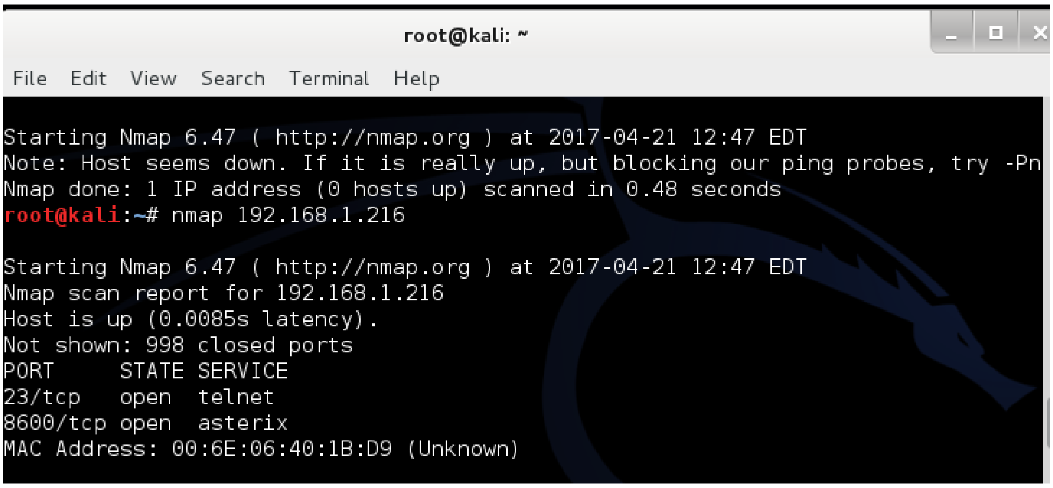
```
=======mac=======
00-1b-2b-3b-38-89-
zqh socket fd=6
bind failuredipc param ppid 302
update socket init
update  socket is failed
update Socket proc is start
=========================read alarm param========================(1)
==== sysparam.c       , line  530, InitSystemParam         :read system.ini
user1: , pwd1:
user2: , pwd2:
user3: admin, pwd3: test
zqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredmac:00:1B:2B:3B:38:89 30
wifimac:00:1B:2B:3B:38:8A 30
```

Figure 14 – User Information dump after password change

3.3. IP Security Camera 2

The second device to be tested was a secondary IP Security Camera, it must be noted that this camera was of an entirely separate brand to IP Security camera 1. This IP Camera operated in much the same was as IP Security Camera 1 in that it produced a live video feed which can be sent to a mobile application to allow the user to view it. This camera also allowed for rotation on two axis as well as the ability to both listen to and send live audio to and from the camera. The camera was connected to the network via Ethernet connection until Wi-Fi settings could be configured. The mobile application was also install and set up allowing connection to the camera via Wi-Fi.

The first stage in testing IP Security Camera 2 was to perform a Nmap [28] port and service scan against its IP Address. The IP address of IP Camera 2 was “192.168.1.216”.



```
Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-21 12:47 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.48 seconds
root@kali:~# nmap 192.168.1.216

Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-21 12:47 EDT
Nmap scan report for 192.168.1.216
Host is up (0.0085s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
8600/tcp open  asterix
MAC Address: 00:6E:06:40:1B:D9 (Unknown)
```

Figure 15 – Nmap Scan IP Camera 2

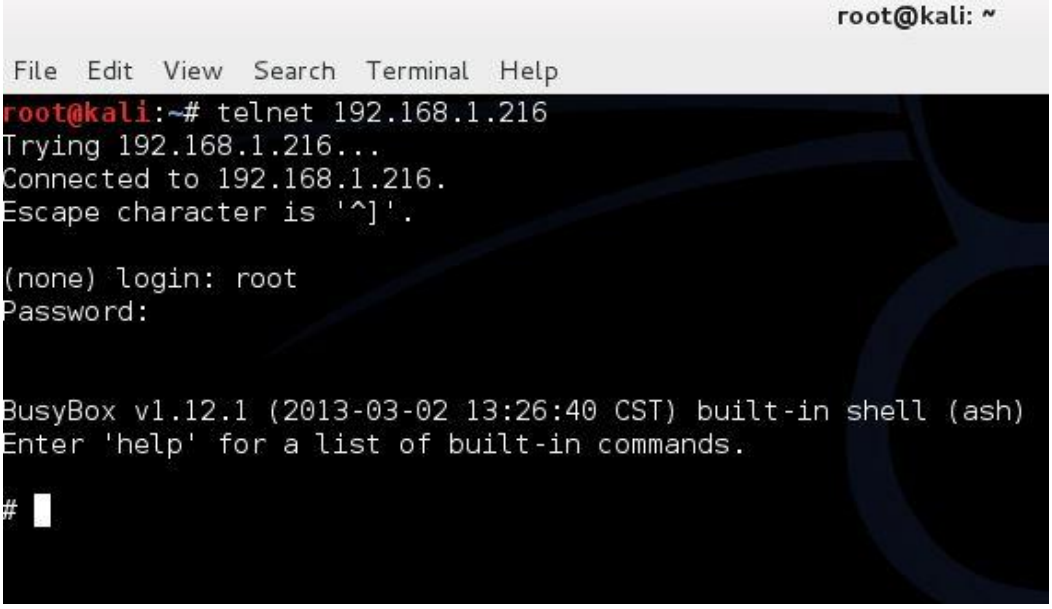
Figure 15 above displays the Nmap [28] port and service scan results for IP Security Camera 2. The two ports open are;

- TCP Port 23 - telnet
- TCP Port 8600 – asterix

An attempt to connect to the IP camera through telnet was then carried out. With the use of password guessing, the telnet login and password were found to be;

- Login – **root**
- Password – **123456**

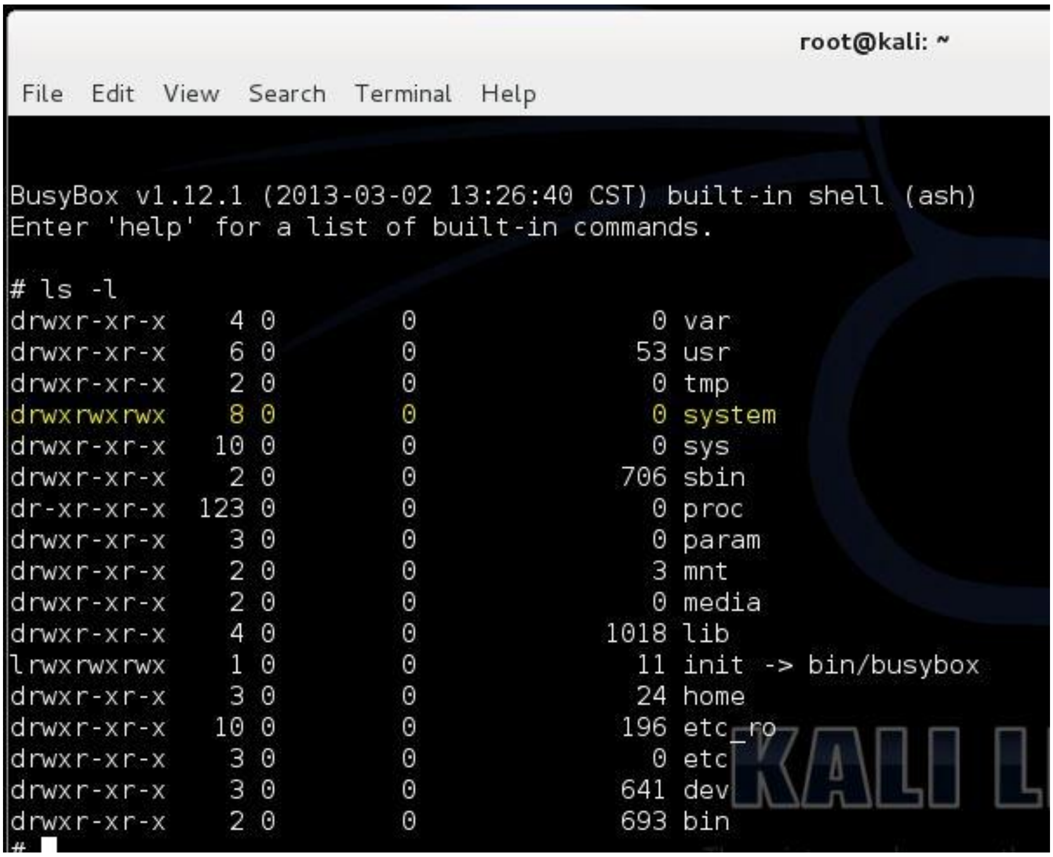
The process of the connection to IP Security Camera 2 is demonstrated in figure 15 below;



```
root@kali:~# telnet 192.168.1.216
Trying 192.168.1.216...
Connected to 192.168.1.216.
Escape character is '^]'.

(none) login: root
Password:


BusyBox v1.12.1 (2013-03-02 13:26:40 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# 
```

Figure 15 – Telnet login to IP Security Camera 2

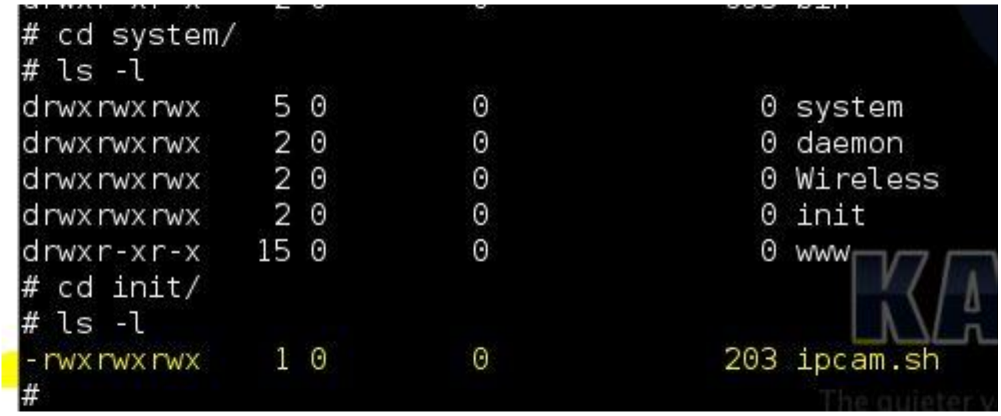
Once connection to the IP Camera was established its file system was explored, the files present on IP Security Camera 2 are shown in figure 16 below;



```
BusyBox v1.12.1 (2013-03-02 13:26:40 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ls -l
drwxr-xr-x    4 0        0               0 var
drwxr-xr-x    6 0        0              53 usr
drwxr-xr-x    2 0        0               0 tmp
drwxrwxrwx    8 0        0               0 system
drwxr-xr-x   10 0        0               0 sys
drwxr-xr-x    2 0        0             706 sbin
dr-xr-xr-x  123 0        0               0 proc
drwxr-xr-x    3 0        0               0 param
drwxr-xr-x    2 0        0               3 mnt
drwxr-xr-x    2 0        0               0 media
drwxr-xr-x    4 0        0            1018 lib
lrwxrwxrwx    1 0        0              11 init -> bin/busybox
drwxr-xr-x    3 0        0              24 home
drwxr-xr-x   10 0        0             196 etc_ro
drwxr-xr-x    3 0        0               0 etc
drwxr-xr-x    3 0        0             641 dev
drwxr-xr-x    2 0        0             693 bin
# 
```

Figure 15 – IP Security Camera 2 file system

As the file system appeared to be very similar to that of IP Security Camera 1 the “/system/init” directory was explored for similar files as “ipcam.sh” which was discovered in IP Camera 1.

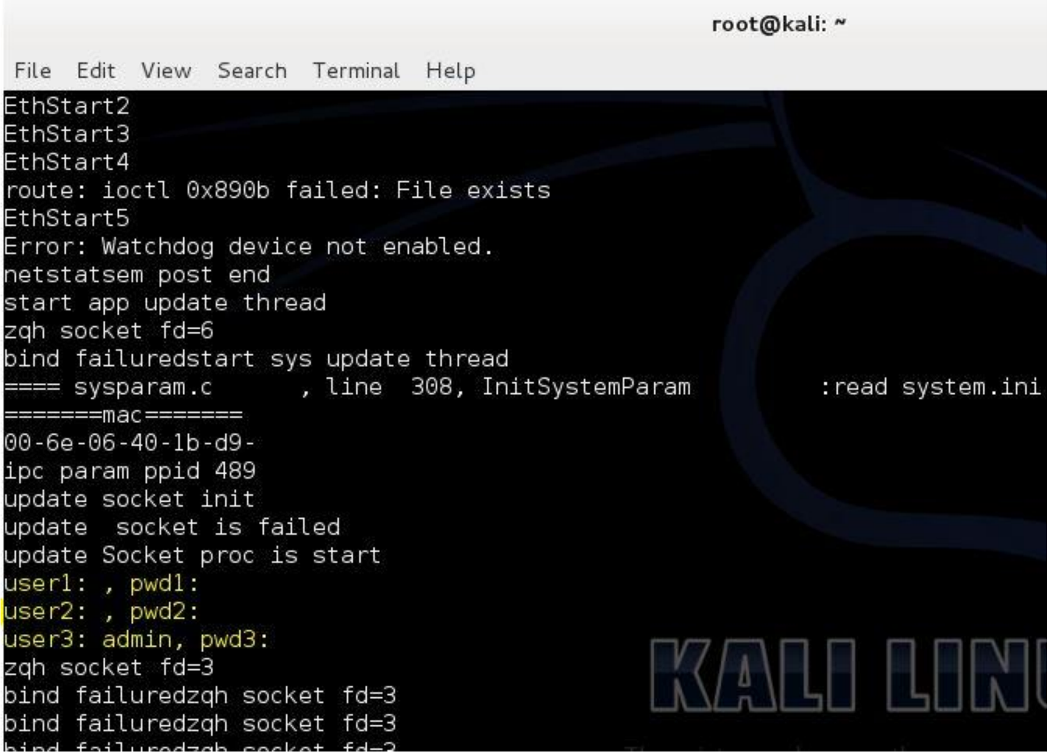


```
# cd system/
# ls -l
drwxrwxrwx    5 0        0            0 system
drwxrwxrwx    2 0        0            0 daemon
drwxrwxrwx    2 0        0            0 Wireless
drwxrwxrwx    2 0        0            0 init
drwxr-xr-x   15 0        0            0 www
# cd init/
# ls -l
-rwxrwxrwx    1 0        0          203 ipcam.sh
#
```

Figure 16 – ipcam.sh file position IP Camera 2

The Linux executable file “ipcam.sh” was located in the “system/init” file directory as evidenced by figure 16 above. When executed this file dumped all system configuration to the screen similar to IP Security Camera 1, the full output of the “ipcam.sh” for IP Security Camera 2 can be reference in **Appendices 7.2**.

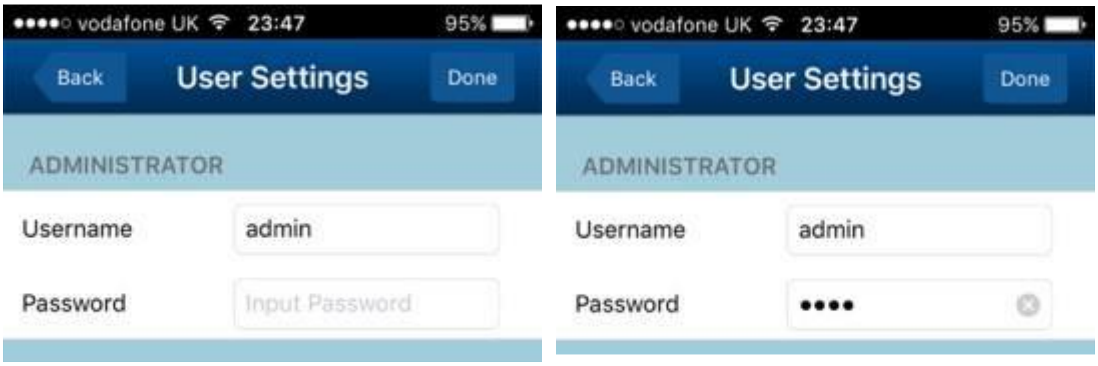
Within the output of “ipcam.sh” was a list of usernames and passwords as shown in figure 17 below;



```
EthStart2
EthStart3
EthStart4
route: ioctl 0x890b failed: File exists
EthStart5
Error: Watchdog device not enabled.
netstatsem post end
start app update thread
zqh socket fd=6
bind failuredstart sys update thread
==== sysparam.c      , line  308, InitSystemParam        :read system.ini
=======mac=======
00-6e-06-40-1b-d9-
ipc param ppid 489
update socket init
update  socket is failed
update Socket proc is start
user1: , pwd1:
user2: , pwd2:
user3: admin, pwd3:
zqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
```

Figure 17 – Logins and password dump IP Camera 2

As with IP Camera 1 the password of the user account was changed in order to confirm that the accounts displayed when executing the “ipcam.sh” file were in fact the correct user account details.



●●●●○ vodafone UK 23:47 95%

Back | User Settings | Done

ADMINISTRATOR

Username: admin

Password: Input Password

●●●●○ vodafone UK 23:47 95%

Back | User Settings | Done

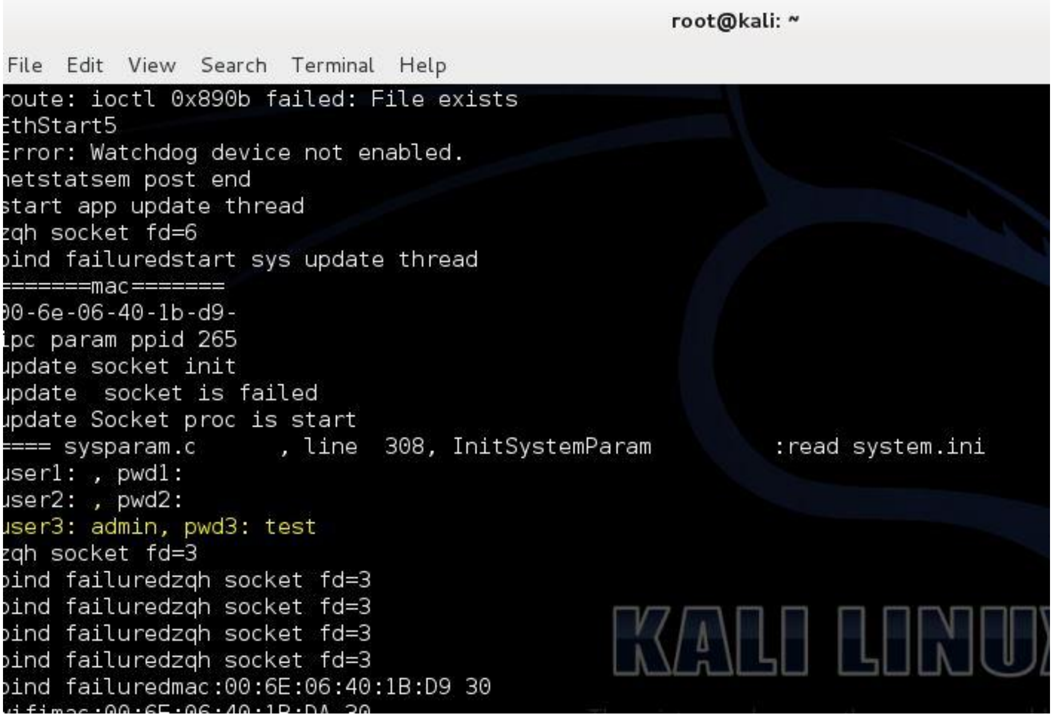
ADMINISTRATOR

Username: admin

Password: ●●●●

Figure 18 – Password change test IP Camera 2

Figure 18 above evidences the change in password to “test”. Following this change the “system/init/ipcam.sh” file was re executed and the user information had in fact changed to “test” as evidenced in figure 19 below;



root@kali: ~

```
oute: ioctl 0x890b failed: File exists
thStart5
rror: Watchdog device not enabled.
etstatsem post end
tart app update thread
qh socket fd=6
ind failuredstart sys update thread
======mac=======
0-6e-06-40-1b-d9-
pc param ppid 265
pdate socket init
pdate  socket is failed
pdate Socket proc is start
=== sysparam.c      , line  308, InitSystemParam          :read system.ini
ser1: , pwd1:
ser2: , pwd2:
ser3: admin, pwd3: test
qh socket fd=3
ind failuredzqh socket fd=3
ind failuredzqh socket fd=3
ind failuredzqh socket fd=3
ind failuredzqh socket fd=3
ind failuredmac:00:6E:06:40:1B:D9 30
```

Figure 19 – information dump after password change IP Camera 2

3.4. Baby Monitor

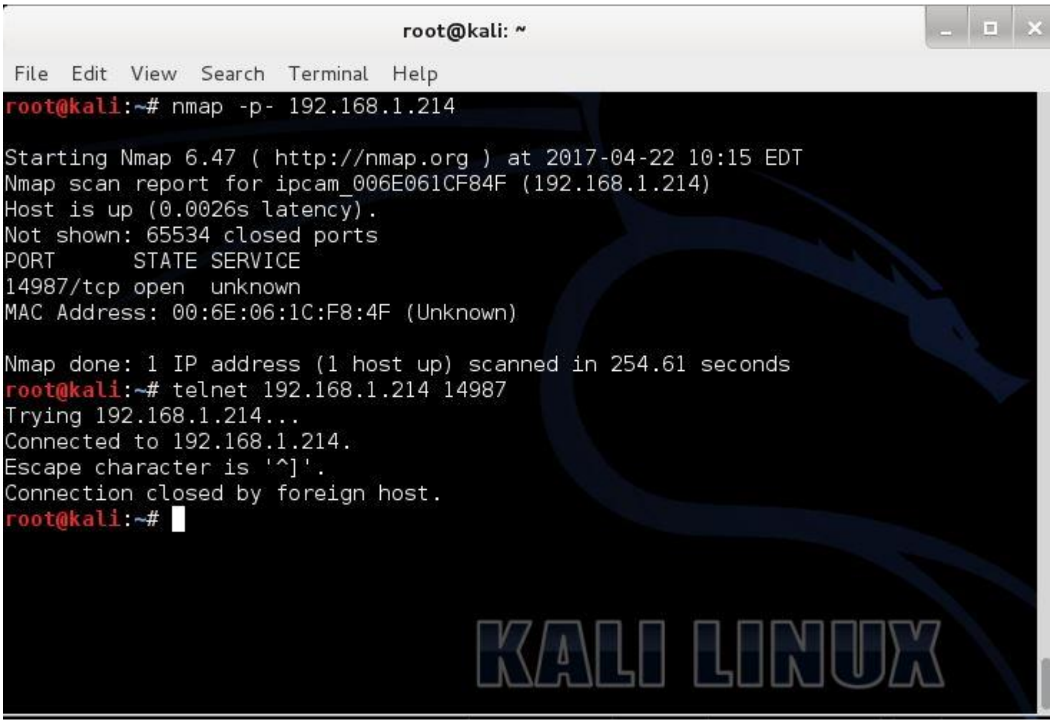
The third device tested was an IP security camera which was marketed as a home baby monitor which has been “secured” for the user’s protection. The device worked in much of the same way as the other IP Security Camera devices tested in this investigation. The camera allows for live streaming of images to a dedicated mobile and browser applications.

The first stage in testing the baby monitor was to perform a Nmap [28] ports and services scan against its IP address, the IP address of the baby monitor in this case was 192.168.1.214. The baby monitor was found to have only one port open;

- TCP Port 14987 – Unknown Service

After further investigation port 14987 was found to be running a telnet service.

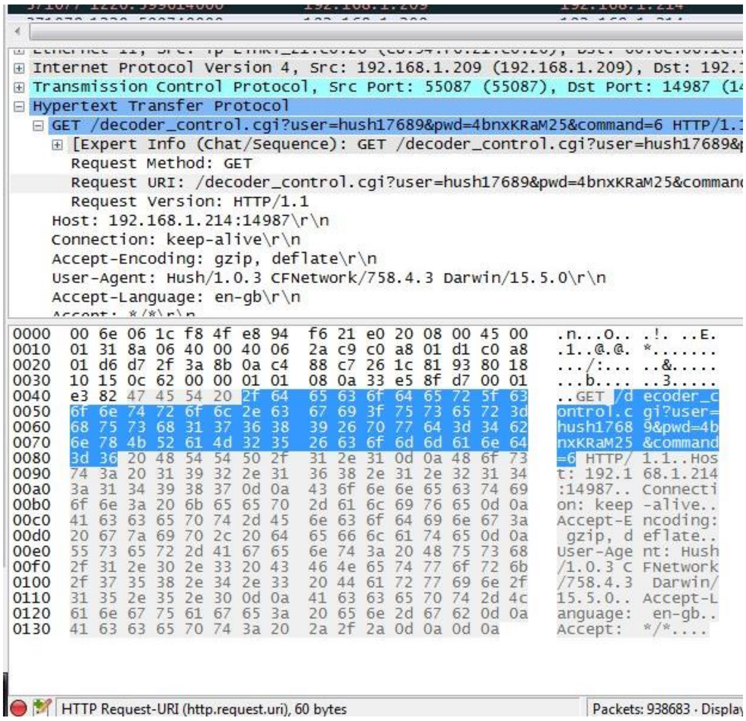
Figure 20 below demonstrates the output of the Nmap [28] scan performed against the baby monitor and the attempt to connect to the telnet service;



```
root@kali:~# nmap -p- 192.168.1.214

Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-22 10:15 EDT
Nmap scan report for ipcam_006E061CF84F (192.168.1.214)
Host is up (0.0026s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
14987/tcp open  unknown
MAC Address: 00:6E:06:1C:F8:4F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 254.61 seconds
root@kali:~# telnet 192.168.1.214 14987
Trying 192.168.1.214...
Connected to 192.168.1.214.
Escape character is '^]'.
Connection closed by foreign host.
root@kali:~# 
```

Figure 20 – Baby Monitor Nmap Scan Results and telnet connection

The baby monitor device has disabled remote connection to its systems over telnet however the next stage of the testing, packet sniffing, revealed that the telnet service running on port 14987 was unencrypted.



```
⊞ Internet Protocol Version 4, Src: 192.168.1.209 (192.168.1.209), Dst: 192.1
⊞ Transmission Control Protocol, Src Port: 55087 (55087), Dst Port: 14987 (14
⊟ Hypertext Transfer Protocol
  ⊟ GET /decoder_control.cgi?user=hush17689&pwd=4bnxKRaM25&command=6 HTTP/1.1
    ⊞ [Expert Info (Chat/Sequence): GET /decoder_control.cgi?user=hush17689&p
      Request Method: GET
      Request URI: /decoder_control.cgi?user=hush17689&pwd=4bnxKRaM25&comman
      Request Version: HTTP/1.1
    Host: 192.168.1.214:14987\r\n
    Connection: keep-alive\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Hush/1.0.3 CFNetwork/758.4.3 Darwin/15.5.0\r\n
    Accept-Language: en-gb\r\n
    Accept: */*\r\n
```

```
0000   00 6e 06 1c f8 4f e8 94  f6 21 e0 20 08 00 45 00   .n...O.. .!. ..E.
0010   01 31 8a 06 40 00 40 06  2a c9 c0 a8 01 d1 c0 a8   .1..@.@. *.......
0020   01 d6 d7 2f 3a 8b 0a c4  88 c7 26 1c 81 93 80 18   .../:... ..&.....
0030   10 15 0c 62 00 00 01 01  08 0a 33 e5 8f d7 00 01   ...b.... ..3.....
0040   e3 82 47 45 54 20 2f 64  65 63 6f 64 65 72 5f 63   ..GET /d ecoder_c
0050   6f 6e 74 72 6f 6c 2e 63  67 69 3f 75 73 65 72 3d   ontrol.c gi?user=
0060   68 75 73 68 31 37 36 38  39 26 70 77 64 3d 34 62   hush1768 9&pwd=4b
0070   6e 78 4b 52 61 4d 32 35  26 63 6f 6d 6d 61 6e 64   nxKRaM25 &command
0080   3d 36 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   =6 HTTP/ 1.1..Hos
0090   74 3a 20 31 39 32 2e 31  36 38 2e 31 2e 32 31 34   t: 192.1 68.1.214
00a0   3a 31 34 39 38 37 0d 0a  43 6f 6e 6e 65 63 74 69   :14987.. Connecti
00b0   6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive..
00c0   41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
00d0   20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate..
00e0   55 73 65 72 2d 41 67 65  6e 74 3a 20 48 75 73 68   User-Age nt: Hush
00f0   2f 31 2e 30 2e 33 20 43  46 4e 65 74 77 6f 72 6b   /1.0.3 C FNetwork
0100   2f 37 35 38 2e 34 2e 33  20 44 61 72 77 69 6e 2f   /758.4.3  Darwin/
0110   31 35 2e 35 2e 30 0d 0a  41 63 63 65 70 74 2d 4c   15.5.0.. Accept-L
0120   61 6e 67 75 61 67 65 3a  20 65 6e 2d 67 62 0d 0a   anguage:  en-gb..
0130   41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 0d 0a      Accept:  */*....
```

HTTP Request-URI (http.request.uri), 60 bytes

Packets: 938683 · Display

Figure 21 – Packet sniffing of Baby Monitor

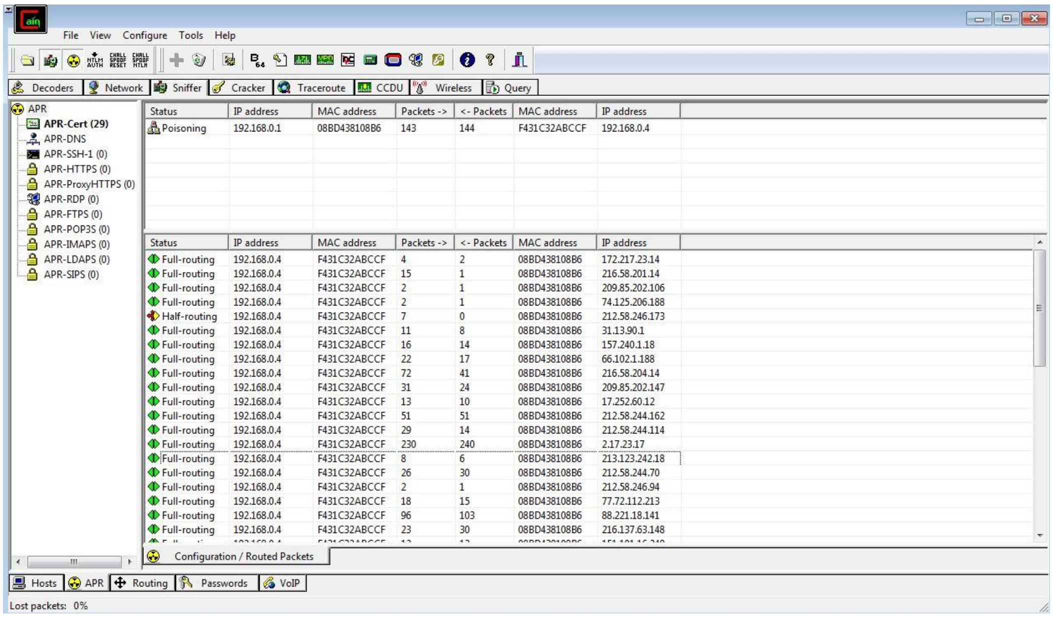
Figure 21 above shows the Wireshark [29] analysis of the data packets transferred to and from the baby monitor, within one of the data packets is the user credentials used to connect to “192.168.1.214” port “14987”. The credentials discovered are as follows;

- User – **hush17689**
- Password – **4bnxKRaM25**

3.5. Bluetooth Heart Rate and Blood Pressure Monitor

The fourth device tested was a wireless blood pressure and heart rate monitor, this device used Bluetooth to communicate to and from a dedicated mobile application. The mobile application itself allowed the user to capture and store blood pressure and heart rate information within the mobile device itself. The user is provided with the option to export all data to a healthcare professional or friend/family member, this functionality of the application makes use of email to export the data.

The first stage of testing the Bluetooth blood pressure monitor was to perform a man in the middle attack between the mobile application and cloud interface. The process was completed using the Cain and Able penetration testing tool [30] and Wireshark [29]. Figure 22 below evidences the process of the man in the middle attack on the device;

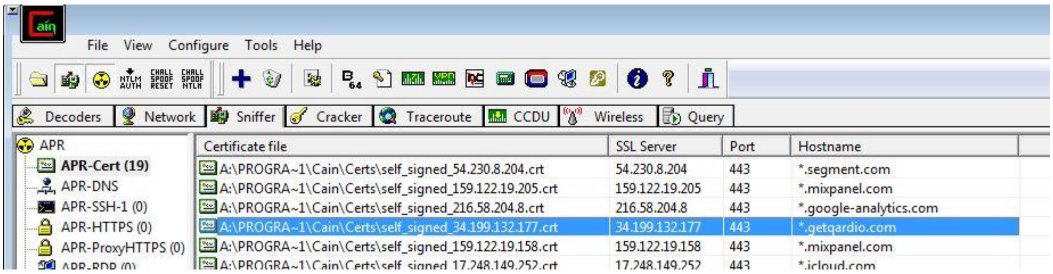


Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.0.1	08BD438108B6	143	144	F431C32ABCCF	192.168.0.4

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.0.4	F431C32ABCCF	4	2	08BD438108B6	172.217.23.14
Full-routing	192.168.0.4	F431C32ABCCF	15	1	08BD438108B6	216.58.201.14
Full-routing	192.168.0.4	F431C32ABCCF	2	1	08BD438108B6	209.85.202.106
Full-routing	192.168.0.4	F431C32ABCCF	2	1	08BD438108B6	74.125.206.188
Half-routing	192.168.0.4	F431C32ABCCF	7	0	08BD438108B6	212.58.246.173
Full-routing	192.168.0.4	F431C32ABCCF	11	8	08BD438108B6	31.13.90.1
Full-routing	192.168.0.4	F431C32ABCCF	16	14	08BD438108B6	157.240.1.18
Full-routing	192.168.0.4	F431C32ABCCF	22	17	08BD438108B6	66.102.1.188
Full-routing	192.168.0.4	F431C32ABCCF	72	41	08BD438108B6	216.58.204.14
Full-routing	192.168.0.4	F431C32ABCCF	31	24	08BD438108B6	209.85.202.147
Full-routing	192.168.0.4	F431C32ABCCF	13	10	08BD438108B6	17.252.60.12
Full-routing	192.168.0.4	F431C32ABCCF	51	51	08BD438108B6	212.58.244.162
Full-routing	192.168.0.4	F431C32ABCCF	29	14	08BD438108B6	212.58.244.114
Full-routing	192.168.0.4	F431C32ABCCF	230	240	08BD438108B6	2.17.23.17
Full-routing	192.168.0.4	F431C32ABCCF	8	6	08BD438108B6	213.123.242.18
Full-routing	192.168.0.4	F431C32ABCCF	26	30	08BD438108B6	212.58.244.70
Full-routing	192.168.0.4	F431C32ABCCF	2	1	08BD438108B6	212.58.246.94
Full-routing	192.168.0.4	F431C32ABCCF	18	15	08BD438108B6	77.72.112.213
Full-routing	192.168.0.4	F431C32ABCCF	96	103	08BD438108B6	88.221.18.141
Full-routing	192.168.0.4	F431C32ABCCF	23	30	08BD438108B6	216.137.63.148

Figure 22 – Man in the middle Cain

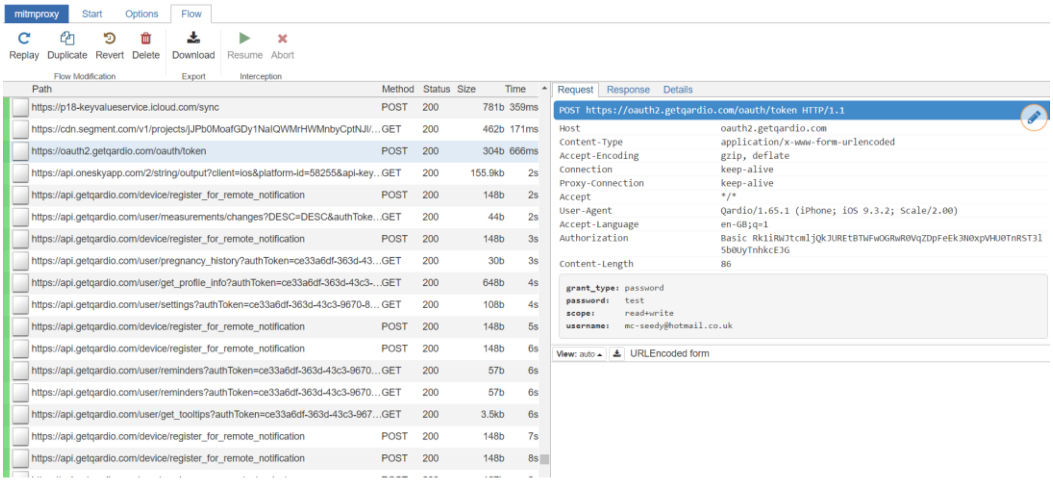
Analysis of the certificates generated when performing the man in the middle attack showed a connection to the devices cloud interface as shown in figure 23 below;



Certificate file	SSL Server	Port	Hostname
A:\PROGRA~1\Cain\Certs\self_signed_54.230.8.204.crt	54.230.8.204	443	*.segment.com
A:\PROGRA~1\Cain\Certs\self_signed_159.122.19.205.crt	159.122.19.205	443	*.mixpanel.com
A:\PROGRA~1\Cain\Certs\self_signed_216.58.204.8.crt	216.58.204.8	443	*.google-analytics.com
A:\PROGRA~1\Cain\Certs\self_signed_34.199.132.177.crt	34.199.132.177	443	*.getqardio.com
A:\PROGRA~1\Cain\Certs\self_signed_159.122.19.158.crt	159.122.19.158	443	*.mixpanel.com
A:\PROGRA~1\Cain\Certs\self_signed_17.248.149.252.crt	17.248.149.252	443	*.icloud.com

Figure 23 – Cloud interface connection

Analysis of the data packet transfer to this cloud interface via Wireshark [29] showed that all traffic was in fact encrypted using SSL (TLS v1.2). In order to circumnavigate this encryption a tool called man in the middle proxy (mitmproxy [31]) was used in order to receive the data unencrypted. Figure 24 below evidences the unencrypted traffic using mitmproxy [31];

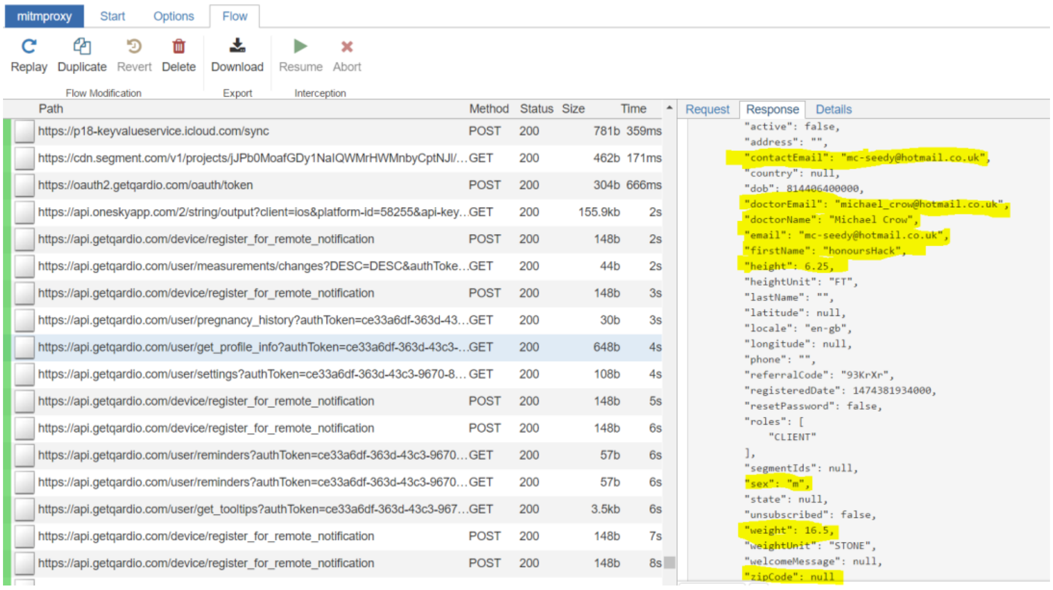


Path	Method	Status	Size	Time
https://p18-keyvalueservice.icloud.com/sync	POST	200	781b	359ms
https://cdn.segment.com/v1/projects/jJPb0MoafGDy1NaIQWMrHWMnbyCptNJI/…	GET	200	462b	171ms
https://oauth2.getqardio.com/oauth/token	POST	200	304b	666ms
https://api.oneskyapp.com/2/string/output?client=ios&platform-id=58255&api-key…	GET	200	155.9kb	2s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	2s
https://api.getqardio.com/user/measurements/changes?DESC=DESC&authToke…	GET	200	44b	2s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	3s
https://api.getqardio.com/user/pregnancy_history?authToken=ce33a6df-363d-43…	GET	200	30b	3s
https://api.getqardio.com/user/get_profile_info?authToken=ce33a6df-363d-43c3-…	GET	200	648b	4s
https://api.getqardio.com/user/settings?authToken=ce33a6df-363d-43c3-9670-8…	GET	200	108b	4s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	5s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	6s
https://api.getqardio.com/user/reminders?authToken=ce33a6df-363d-43c3-9670…	GET	200	57b	6s
https://api.getqardio.com/user/reminders?authToken=ce33a6df-363d-43c3-9670…	GET	200	57b	6s
https://api.getqardio.com/user/get_tooltips?authToken=ce33a6df-363d-43c3-967…	GET	200	3.5kb	6s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	7s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	8s

```
POST https://oauth2.getqardio.com/oauth/token HTTP/1.1
Host              oauth2.getqardio.com
Content-Type      application/x-www-form-urlencoded
Accept-Encoding   gzip, deflate
Connection        keep-alive
Proxy-Connection  keep-alive
Accept            */*
User-Agent        Qardio/1.65.1 (iPhone; iOS 9.3.2; Scale/2.00)
Accept-Language   en-GB;q=1
Authorization     Basic Rk1iRWJtcmljQkJUREtBTWFwOGRwR0VqZDpFeEk3N0xpVHU0TnRST3l
                  5b0UyTnhkcEJG
Content-Length    86

grant_type: password
password:   test
scope:      read+write
username:   mc-seedy@hotmail.co.uk
```

Figure 24 – mitmproxy blood pressure monitor

Within the viewable unencrypted connections/data was the username and password of the user as shown in figure 24 above. Upon further inspection of the data transfers was the complete user profile and information being transferred to the cloud interface of the device as detailed in figure 25 below;



Path	Method	Status	Size	Time
https://p18-keyvalueservice.icloud.com/sync	POST	200	781b	359ms
https://cdn.segment.com/v1/projects/jJPb0MoafGDy1NaIQWMrHWMnbyCptNJI/…	GET	200	462b	171ms
https://oauth2.getqardio.com/oauth/token	POST	200	304b	666ms
https://api.oneskyapp.com/2/string/output?client=ios&platform-id=58255&api-key…	GET	200	155.9kb	2s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	2s
https://api.getqardio.com/user/measurements/changes?DESC=DESC&authToke…	GET	200	44b	2s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	3s
https://api.getqardio.com/user/pregnancy_history?authToken=ce33a6df-363d-43…	GET	200	30b	3s
https://api.getqardio.com/user/get_profile_info?authToken=ce33a6df-363d-43c3-…	GET	200	648b	4s
https://api.getqardio.com/user/settings?authToken=ce33a6df-363d-43c3-9670-8…	GET	200	108b	4s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	5s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	6s
https://api.getqardio.com/user/reminders?authToken=ce33a6df-363d-43c3-9670…	GET	200	57b	6s
https://api.getqardio.com/user/reminders?authToken=ce33a6df-363d-43c3-9670…	GET	200	57b	6s
https://api.getqardio.com/user/get_tooltips?authToken=ce33a6df-363d-43c3-967…	GET	200	3.5kb	6s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	7s
https://api.getqardio.com/device/register_for_remote_notification	POST	200	148b	8s

```
"active": false,
"address": "",
"contactEmail": "mc-seedy@hotmail.co.uk",
"country": null,
"dob": 814406400000,
"doctorEmail": "michael_crow@hotmail.co.uk",
"doctorName": "Michael Crow",
"email": "mc-seedy@hotmail.co.uk",
"firstName": "honoursHack",
"height": 6.25,
"heightUnit": "FT",
"lastName": "",
"latitude": null,
"locale": "en-gb",
"longitude": null,
"phone": "",
"referralCode": "93KrXr",
"registeredDate": 1474381934000,
"resetPassword": false,
"roles": [
    "CLIENT"
],
"segmentIds": null,
"sex": "m",
"state": null,
"unsubscribed": false,
"weight": 16.5,
"weightUnit": "STONE",
"welcomeMessage": null,
"zipCode": null
```

Figure 25 – Personal information Blood pressure monitor

This information included the doctor information and user information such as height, geographical location, phone number, sex, weight and postal code. When the user exported the data within the email functionality of the mobile app the complete contents of the email could be captured including any notes. It should also be noted that using mitmproxy [31] allows for the editing of this data for example email address and then by replaying the connection the data could be sent to another email address chosen by the attacker.

3.6. Smart Power Plug

The next device tested was a generic smart power socket device. This device allows a user to control the turning on and off any electrical device connected via mains plug socket, the device advertises that connection and control of the smart plug is only available through its dedicated mobile application. The device also provides the user with a time setting functionality, which allows the user to a specific time to allow or disallow power to the electrical item connected via the smart power plug.
The first stage in testing was to attempt to Nmap [28] scan the device in search for open ports and services present on the device however, all communication ports were closed on the device. The next stage of testing was to assess the level of security present on the mobile application, upon inspection it was discovered that there was numerous applications present on the apple app store which would allow any mobile user in the vicinity of the smart plug to add it as a device without a specific password, the user could also access the plug out with the network in which it is set up, in the case of this investigation the smart plug could be controlled using a second mobile device using 4G as shown in figure 26 below;

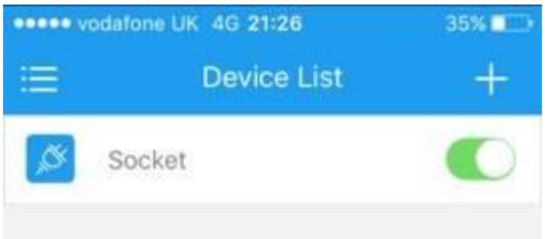


Figure 26 – smart plug remote network

After further research into the smart plug itself, it was discovered that a desktop application had been created by a previous user that when run would allow for the connection to the plug connected to the same network as the desktop itself. The application created by Andrius Štikonas is freely available on GitHub [33]. Figure 27 below is a combination of screenshots evidencing the applications functionality in relation to the turning off and on of the smart plug;

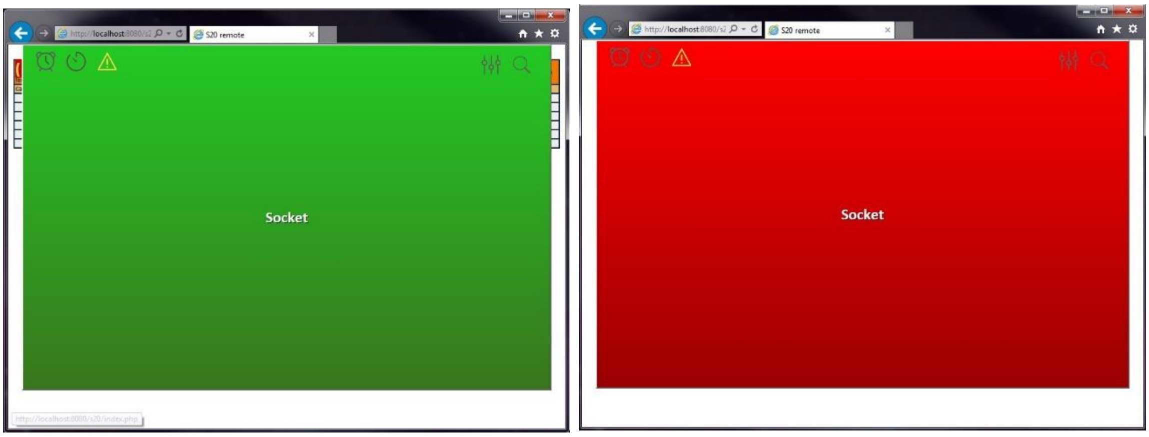
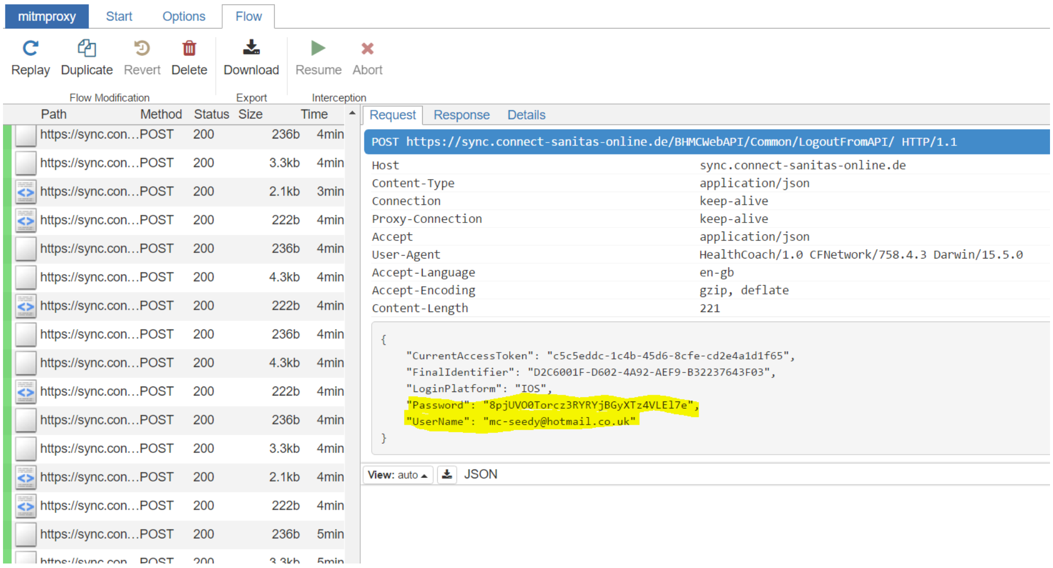


Figure 27 – Smart Plug Desktop Application

3.7. Bluetooth Weight scales

The sixth device tested was a smart weight scale, the scale makes the use of Bluetooth technology to connect to a mobile device which has been pre-installed with a dedicated mobile application. The mobile application acts as a general health tool which contains information on the user’s weight history, height and other personal details. The application also provides an email functionality which can export all health data to a specified email address.

The testing of this device was conducted using mitmproxy [31] in order to capture the communication of the smart scale mobile application. The first interesting communication captured was the immediate connection to the applications cloud interface, this connection displayed the username and password in the request packet, however the user’s password was in fact encrypted. Figure 28 below is details the capture of the cloud connection with username and encrypted password;



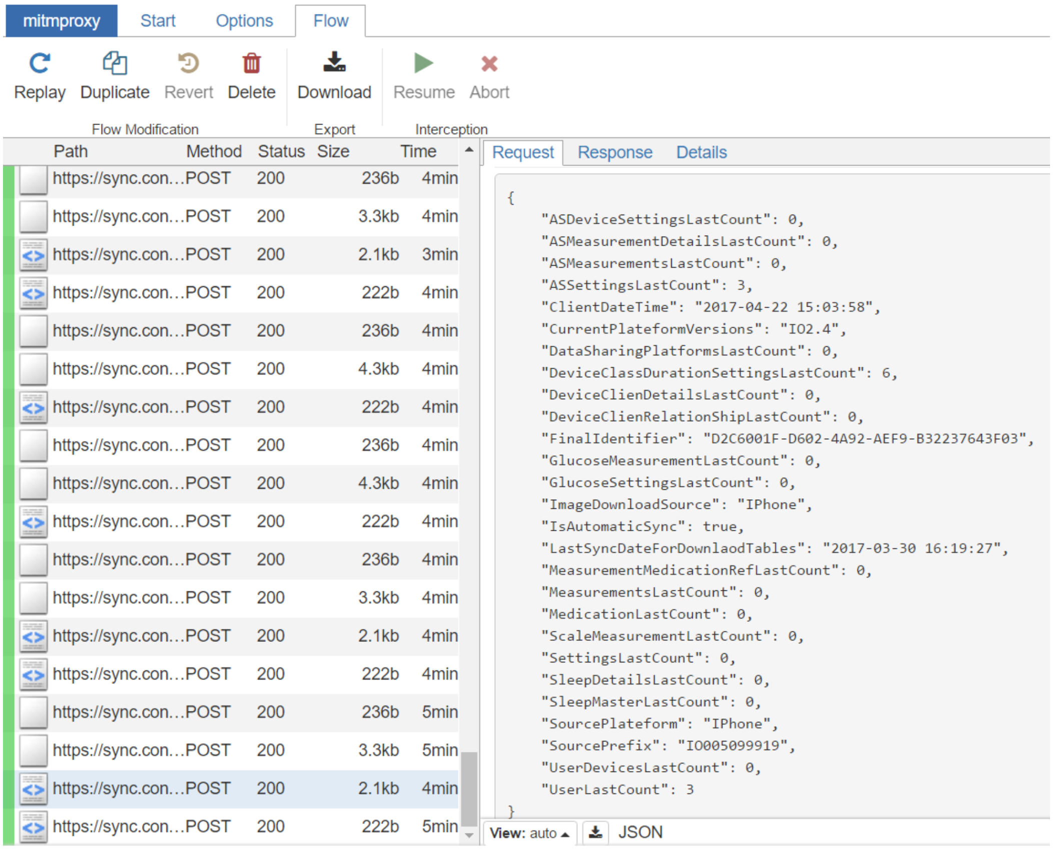
Path	Method	Status	Size	Time
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	3.3kb	4min
https://sync.con…	POST	200	2.1kb	3min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	4.3kb	4min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	4.3kb	4min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	3.3kb	4min
https://sync.con…	POST	200	2.1kb	4min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	5min
https://sync.con…	POST	200	3.3kb	5min

```
POST https://sync.connect-sanitas-online.de/BHMCWebAPI/Common/LogoutFromAPI/ HTTP/1.1
Host                   sync.connect-sanitas-online.de
Content-Type           application/json
Connection             keep-alive
Proxy-Connection       keep-alive
Accept                 application/json
User-Agent             HealthCoach/1.0 CFNetwork/758.4.3 Darwin/15.5.0
Accept-Language        en-gb
Accept-Encoding        gzip, deflate
Content-Length         221
```

```
{
    "CurrentAccessToken": "c5c5eddc-1c4b-45d6-8cfe-cd2e4a1d1f65",
    "FinalIdentifier": "D2C6001F-D602-4A92-AEF9-B32237643F03",
    "LoginPlatform": "IOS",
    "Password": "8pjUVO0Torcz3RYRYjBGyXTz4VLEl7e",
    "UserName": "mc-seedy@hotmail.co.uk"
}
```

Figure 28 – Smart Scales Cloud Connection

The next stage of the testing involved the analysis of further connection to the cloud interface from the mobile interface, one connection to the cloud interface returned the entire personal profile of the user, information such as medication counters and sleep counters were displayed, furthermore a full database upload was captured which included multiple counts of private information, a full dump of the database upload can be referenced in **Appendices 7.3**. A summary of the private user information counts can be evidenced in figure 29 below;



Path	Method	Status	Size	Time
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	3.3kb	4min
https://sync.con…	POST	200	2.1kb	3min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	4.3kb	4min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	4.3kb	4min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	4min
https://sync.con…	POST	200	3.3kb	4min
https://sync.con…	POST	200	2.1kb	4min
https://sync.con…	POST	200	222b	4min
https://sync.con…	POST	200	236b	5min
https://sync.con…	POST	200	3.3kb	5min
https://sync.con…	POST	200	2.1kb	4min
https://sync.con…	POST	200	222b	5min

```
{
    "ASDeviceSettingsLastCount": 0,
    "ASMeasurementDetailsLastCount": 0,
    "ASMeasurementsLastCount": 0,
    "ASSettingsLastCount": 3,
    "ClientDateTime": "2017-04-22 15:03:58",
    "CurrentPlateformVersions": "IO2.4",
    "DataSharingPlatformsLastCount": 0,
    "DeviceClassDurationSettingsLastCount": 6,
    "DeviceClienDetailsLastCount": 0,
    "DeviceClienRelationShipLastCount": 0,
    "FinalIdentifier": "D2C6001F-D602-4A92-AEF9-B32237643F03",
    "GlucoseMeasurementLastCount": 0,
    "GlucoseSettingsLastCount": 0,
    "ImageDownloadSource": "IPhone",
    "IsAutomaticSync": true,
    "LastSyncDateForDownlaodTables": "2017-03-30 16:19:27",
    "MeasurementMedicationRefLastCount": 0,
    "MeasurementsLastCount": 0,
    "MedicationLastCount": 0,
    "ScaleMeasurementLastCount": 0,
    "SettingsLastCount": 0,
    "SleepDetailsLastCount": 0,
    "SleepMasterLastCount": 0,
    "SourcePlateform": "IPhone",
    "SourcePrefix": "IO005099919",
    "UserDevicesLastCount": 0,
    "UserLastCount": 3
}
```

Figure 29 – Smart scales user information count

4. Results

Table three bellows depicts the number of vulnerabilities found in each device which was tested in this investigation;

IOT Device Vulnerability table										
	Vulnerabilities -->	Insufficient Authentication / Authorization	Insecure Network Services	Lack of Transport Encryption	Privacy Concerns	Insecure Cloud Interface	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			✓	✓	✓		✓		

Table 3 – IoT Vulnerability Results Table

Figure 30 below details the number of vulnerabilities grouped by device;

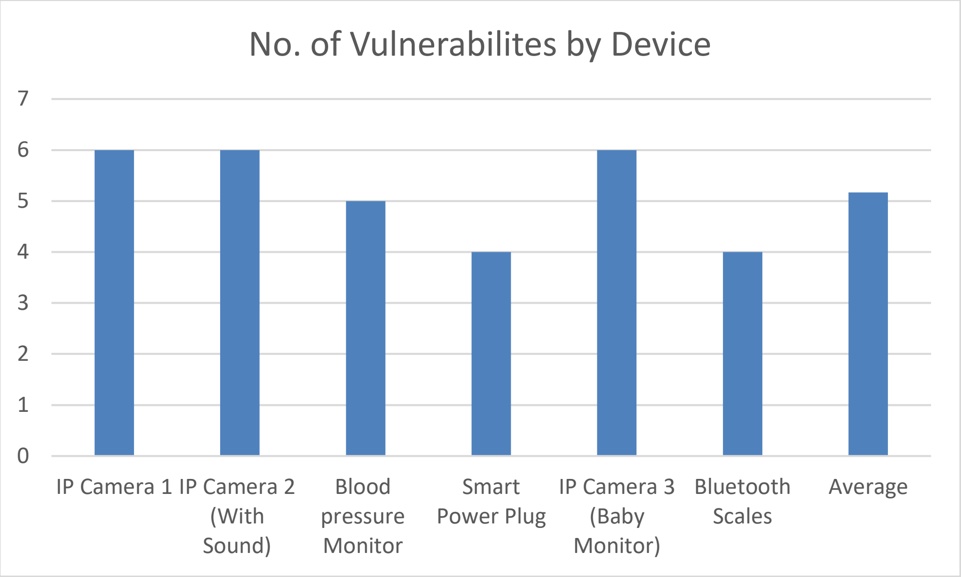


Figure 30 – No. of Vulnerabilities by Device

4.1. IP Security Camera 1

The first IP Security Camera that was tested in this investigation was found to have a total of six vulnerabilities. The vulnerabilities found were;

- Insufficient Authentication / Authorization
- Insecure Network Services
- Privacy Concerns
- Insufficient security configurability
- Insecure software/firmware
- Poor Physical Security

4.2. IP Security Camera 2

The second IP Security Camera that was tested in this investigation was found to have a total of six vulnerabilities. The vulnerabilities found were;

- Insufficient Authentication / Authorization
- Insecure Network Services
- Privacy Concerns
- Insufficient security configurability
- Insecure software/firmware
- Poor Physical Security

4.3. Baby Monitor

The third IP Security camera tested in this investigation which was marketed as a baby monitor contained a total of six vulnerabilities. The vulnerabilities found consisted of;

- Insufficient Authentication / Authorization
- Insecure Network Services
- Lack of Transport Encryption
- Privacy Concerns
- Insufficient security configurability
- Poor Physical Security

4.4. Bluetooth Blood Pressure and Heart Rate Monitor

The Bluetooth Blood pressure and heart rate monitor tested in this investigation was found to have a total of five security vulnerabilities. The vulnerabilities found consisted of;

- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient security configurability

4.5. Smart Power Plug

The smart power socket testing in this investigation was found to have a total of four existing vulnerabilities. The vulnerabilities found consisted of;

- Insufficient Authentication / Authorization
- Insecure Mobile Interface
- Insufficient security configurability
- Insecure software/firmware

4.6. Bluetooth Weight Scales

The Bluetooth weight scales tested in this investigation had a total of four security related vulnerabilities. The vulnerabilities found consisted of;

- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insufficient security configurability

4.7. Security Concerns Grouped by Vulnerability

Overall there was a total of thirty-one vulnerabilities found when testing all devices in this investigation. Figure 31 below details the number of vulnerabilities found during testing grouped by the type of vulnerability present on devices;

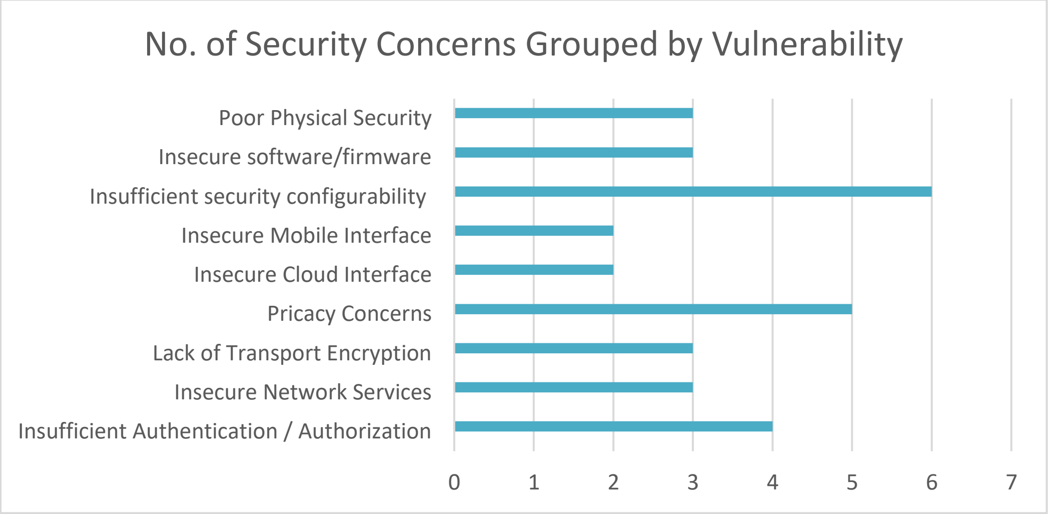


Figure 31 – No. of Security Concerns Grouped by vulnerability

5. Discussion

This section of this investigation will interpret the results gathered from the performing of the methodology section. This section will discuss the overall level of security present on each of the devices tested in the methodology and then reference the real-world implications of the results which could be implemented in order to counteract the vulnerabilities found.

5.1. IP Security Camera 1

The first device which was tested in this investigation, IP Security Camera 1 was found to have a total of six vulnerabilities. It was clear when testing that the level of security present on the device was not considered when the device was being developed and its software/firmware implemented. Considering that a user, be it business or personal, will use a device of this nature to further secure their home or business various amounts of personal images and details would be put at risk by this device. It can be said that not a single aspect of this device is secure in any way, the use of an unencrypted telnet service puts this device at risk from remote connection, furthermore as the root password on the telnet connection is set to “123456” any attacker of even the lowest skill level would be able to gain remote access to the device with ease. If an attacker was to gain remote connection to this device, they would have access to all privately stored images and videos taken by the camera thus the device is a massive concern in relation to privacy. Although the mobile application and desktop application associated with this device provides the user with the ability to change their username and password of the camera connection, the backend vulnerability via telnet and passwords printed in plain text mean that this configurability can be deemed pointless. The applications also do not ask for an initial password to provide initial access to the application therefore if access to the mobile or desktop device was gained by an unauthorised person instant access to the camera stream and saved data would be granted. Furthermore, as the camera firmware priorities Ethernet connection via the open Ethernet port on the device an attacker could gain access to the camera via Ethernet connection and thus command control over the device.

5.2. IP Security Camera 2

The second device tested in this investigation, IP Security Camera 2, was found to have a total of six vulnerabilities. It was clear when testing that the firmware present on this security camera was almost identical to that of IP Security Camera 1 even though the camera was a completely separate brand, make and model. The physical nature of the camera was also inherently different from IP Security Camera 1 as it allowed for the movement of the camera on two axis, the camera also had sound input and output capabilities which were not present on IP Security Camera 1. As the firmware and setup of IP Security Camera 2 was almost completely identical to IP Security Camera 1 the same vulnerabilities were also present on the device this indicates that when developing the camera no further effort was made on the part of the developers to secure the software and firmware. The presence of an unsecured telnet service on the device would allow an attacker of a basic skill level to access the device remotely with a root password of “123456”. As remote access was available the private data available such as screenshots and live recordings with sound would be available to the attacker which is cause for some major concern. The dedicated mobile application of the device had very little user configurability which again would allow unauthorised access to the camera due to no ability for the user to set up initial authentication to access the device. An open Ethernet port is also present on the device which would allow an attacker to take control of the device via Ethernet Connection similarly to IP Security Camera 1, as Ethernet connection are prioritised over previously configured Wi-Fi connections. As a device, such as this would be purchased by a user or organisation to further secure an aspect of their livelihood such as a home or office, the overall level of security present on the device is not to a moral standard by any means.

5.3. Baby Monitor

The third device tested in this investigation was a Baby Monitor with interconnectivity. The smart baby monitor was found to have a total of six vulnerabilities. It should be noted for the purposes of this investigation that the smart baby monitor possessed the exact same physical attributes as IP Security Camera 2 which suggest that the camera had been previously purchased as a standard IP Security Camera and re-marketed as a smart baby monitor. This assumption can be made as both the smart baby monitor and IP Security Camera 2 were of two different brands however the make and models of the cameras were identical as detailed by the manufacturers specification sticker present on the underside of both cameras. Similarly to IP Security Camera 1 and IP Security Camera 2, the smart baby monitor had telnet connectivity available, however the developers of this particular brand had made some efforts to secure the device further as the telnet service was not running on its default port (TCP port 23) and instead was running on TCP Port 14987. Not only was the telnet service running on an alternative port, the service was also configured in such a way that disallowed unauthorised connection to the device itself. This configurability showed a further attempt to secure the camera from unauthorised remote connections unlike IP Security Camera 1 and IP Security Camera 2. However, the overall level of security present on the smart baby monitor was undermined by its lack of transport encryption. The lack of transport encryption on the devices communications would allow for an attacker of a low skill level to obtain the default username and password credentials used to connect to the camera, this could then be used to access the cameras live feed and previous saved images and video (with audio) files via both the dedicated smartphone and browser applications. As the device is branded as a “secure” smart baby monitor the type of user data which could be obtained by an attacker would be severely private to users and parents alike. The applications themselves also had to options to configure access authorisation much like IP Security Camera 1 and IP Security Camera 2. The smart baby monitor also had an open Ethernet port present and as the camera was configured to prioritise Ethernet connections over Wi-Fi connections an attacker would be able to gain control over the smart baby monitor via connecting physically via Ethernet cable.

5.4. Bluetooth Blood Pressure and Heart Rate Monitor

The fourth device which was tested in this investigation was the Bluetooth blood pressure and heart rate monitor. The smart blood pressure monitor was found to have a total of five security vulnerabilities. As Bluetooth itself is a relatively secure service due to encryption and authorisation methods the vulnerabilities found with this device were found within the dedicated blood pressure application itself and its connection to the devices cloud interface. With the connectivity to the devices cloud interface being monitored, it was clear that the SSL (TLS v1.2) level of transport encryption was configured was easily bypassed using a tool such as mitmproxy [31] or SSL strip [32], this would allow an attacker access to the users personal account information as well as private health data therefore data privacy is a major issue with this device. The email functionality of the application could also be intercepted which would disclose all email information of the user and their health care professional whom is receiving the data, with the aid of a proxy software such as mitmproxy [31] used in this investigation an attacker would be able to perform a replay attack of the data packets sent in this communication, the editing of the email address could also be performed which would allow an attacker to send the exported health data from the app to an email address of the attackers choosing. These types of attacks could be performed by a low to mid-range skilled attacker. The dedicated mobile interface of this device was also found to be insecure to a certain extent, although the mobile application does allow for the user to set up and initial access password this is not set as default therefore any unauthorised person with access to the mobile phone could view and export the private health data of the user to any defined email address.

5.5. Smart Power Plug

The fifth device tested in this investigation was the smart power plug. The smart power plug was found to have four vulnerabilities this is the joint lowest number of vulnerabilities found in all six devices tested. However, this is not due to the devices level of security but rather its limited usability and practical purpose. When setting up the smart power plug there was no authentication or authorization required, this was partly due to the setup configuration process which involves connecting to the smart power plugs dedicated Wi-Fi network and then pointing it towards the user’s home network or office network. However, this would then allow an attacker to reconfigure the device to a separate network even after it has been set to the user’s home network, this is due to the lack of authorisation and authentication present on the device. The authorisation is evidently non-existent as any secondary user which has the dedicated application installed on their mobile device can also control the device not only over the network but remotely once the device has been setup which again requires not authentication or authorisation. Not only does the dedicated application allow for this functionality but also generic Chinese based applications created for other brands of the same type of device highlighting the negligence in the development stages of this device, especially in relation to the devices mobile interface. Not only is the device insecure in relation to mobile interfaces but control over the device can also be gained through a desktop application which the devices documentation specifically details is not possible. The security vulnerabilities relating to this device may seem elementary as no user information is stored or transferred using the device. Taking this into consideration, the consequences are rather small in scale. However, as the device can be used in conjunction with any UK mains powered device, there is no limit to the damage which could be caused by an attacker remotely turning the device off. This could be considered a denial of service attack of sorts, as loss of power could contribute to a range of inconvenient outcomes, from loss of work on a desktop PC to the powering down of a freezer causing food wastage to even home medical equipment which could be detrimental to the user in a number of ways.

5.6. Bluetooth Weight Scales

The last device tested within the scope of this investigation is the Bluetooth weight scales. The Bluetooth weight scales were found to have four vulnerabilities in total. Like the Bluetooth blood pressure monitor tested in this investigation, the vulnerabilities found in the Bluetooth weight scales relate in most to the devices back end implantation, its mobile application and the devices cloud interface. When the connections between the mobile application and the devices cloud interface were monitored in the case of this experiment using mitmproxy [31] it was evident that the level of transport encryption present on the devices communication was not the best as SSL (TLS1.2) encryption is easily bypassed with the use of mitmproxy [31] or SSL strip [32]. When the user is connected to the mobile application, an update is sent to the cloud interface every minute or so. Within this update the mobile application sends the username (which consists of the users email address) and the password which is in the form of a salt encrypted hash which is evidence of further attempt to encrypt the user's password has been implemented. However, the password is the only encrypted aspect of data as the mobile application send a database update to the cloud interface with all user information. Within the captured database update is numerous amounts of personal user information, this is due to the fact that the mobile application acts as an overall health application. Information such as the user's medication data would be available to the attacker which is obviously a major security concern. The mobile application itself does not have initial access authorisation configured, as is the case with every other mobile application tested in this investigation. Any unauthorised person with access to the mobile application could gain access to the user's personal heath data and through the email functionality of the application, export this data via email to any specified email address without the users knowledge. This email data can also be intercepted by an attacker via mitmproxy [31] and replayed with altered email credentials, similar to that of the Bluetooth blood pressure monitor without the knowledge of the user. The overall level of security present on the Bluetooth smart scales is a major concern for users especially with respect to their private health information.

5.7. Real World Implications

All the devices that were tested in this investigation were found to have at least four security vulnerabilities, this clearly indicates that the previous research conducted by the multiple sources referenced in this investigation appears to be correct. The main vulnerability; insufficient security configurability is evident in every smart device tested in this investigation therefore highlighting it as the most common in the scope of this project.

As per the devices tested, this investigation has a strong focus on the domestic sector of the internet of things with a further focus on IP Security Cameras including the Smart Baby Monitor. With recent high-profile examples of IoT devices being used in calculated world-wide distributed denial of service attacks in the form of the Mirai botnet, it is evident that the majority of devices are susceptible to such malware through the telnet remote access service, as two out of the three IP security cameras tested had root telnet passwords of “123456” which would be easily susceptible to Mirai, it is obvious that this is no small problem.

However, the attempted implementation of extra security measures on the Smart Baby monitor, compared to that of IP Security Camera 1 and IP Security Camera 2 acts as evidence that some organisations are taking security into consideration to a certain extent. This information is interesting given the fact that the Smart Baby monitor has exactly the same hardware as IP Security Camera 2, this demonstrates that hardening security even at a basic level is somewhat possible.

It is evident from the result gathered in this investigation that in relation to the domestic IoT market, user's private data integrity is at a major risk as all devices which handled users private data contained privacy vulnerability, this result highlights the extent at which the current level of IoT security is unquestionably low and much more has to be done in order to counteract these vulnerabilities.
Another observation made in this investigation is that when traced the origins of IP Security Camera 1, IP Security Camera 2, the Smart Baby Monitor and the Smart Power Plug can be traced to Chinese manufacturers, this indicates that the proposed theory of (Nawir et al, 2017) [21] appears to be somewhat true in that little effort or consideration of security is present on these devices, especially in considering the multiple cases of dedicated mobile application failures.

The following section of this investigation concludes the main points discussed in this investigation and offers possible countermeasures which could be implemented to secure the Internet of Things devices tested in this investigation as well as the internet of things as a whole. The next section also suggests what future work could be performed in order to further the research conducted in this investigation.

6. Conclusion

6.1. Countermeasures / Recommendations

As evidenced by the first two IP Security Cameras tested (IP Security Camera 1 and 2) were compromised mainly by the presence of a remote connection service (telnet) and the fact that this service was not encrypted combined with extremely weak root passwords. This vulnerability could be counteracted in IoT devices according to the OWASP IoT penetration testing guide by configuring the Secure Shell (SSH) protocol as a replacement. However, as evidence by the Smart Baby Monitor, IoT devices must also consider transport encryption in order to secure the connection made on the network by devices, additional security could be implemented in this case by the configuration of an application firewall on all devices as suggested by OWASP. Both the Bluetooth heart rate and blood pressure monitor and the Bluetooth weight scales were found to have insecure cloud interfaces, this vulnerability could be countered by the implementation of more password controls such as a minimum level of password security, password lockout and expiration controls and the application of two factor authentication.
The most populous vulnerability discovered in this investigation was the lack of security configurability, in particular on the mobile application interfaces of the Internet of Things devices, this vulnerability could be countered by a complete overhaul of the mobile applications design in such a way that would allow for initial access authorisation to be set as default also in the case of dedicated applications the implementation of device authorisation for the use only by that specific mobile application. This configuration would further increase the security levels present of the smart power plug tested in this investigation.
The implementation of these countermeasures would therefore increase the privacy and integrity of the user's data.

One further consideration which could benefit the internet of things as a whole, would be the creation of an "Internet of Things global standards agency" this would counter the rapid development of these types of devices in China which are clearly being released with little or no level of security present.

In conclusion, the diverse world of the Internet of Things has throughout this investigation been proven to be inherently insecure. This investigation has proven that Internet of Things devices pose multiple threats to society as a whole, this has confirmed the suspicions of the research referenced in the background section of this investigation and evidenced throughout the methodology section as well as the results gathered.

Until substantial further steps are taken by the international community and the developers of the devices, the current and projected rapid growth of the internet of things will cause more harm than good especially in relation to the domestic user their “smart homes” and their private data.

6.2. Future work

The research conducted in this investigation could be furthered in multiple ways;

Firstly, the accuracy of the results gathered in this investigation could be made more accurate by the testing of more devices as well as a more diverse range of devices, this would aid in receiving a more accurate overall view of the level of IoT security and may also help to identify further vulnerabilities that may exist.

Secondly, as the explicit permission of the developers of the devices tested in this investigation was not obtained, a number of tests could not be conducted in relation to the website applications of IoT devices. As the OWASP IoT testing project rates web application vulnerabilities as the number one most common IoT security vulnerability the permission to test such platforms would benefit this research in its accuracy and scope.

Thirdly, as this research attempts to give a step by step guide to the performing of some of these tests it would be beneficial for other academic security researchers to publish similarly formatted research which could aid in both the awareness and education of penetration testers to the ways in which IoT devices can be compromised in order to protect them for the future.

7. Appendices

7.1. IP Security Camera 1 – ipcam.sh output

```
# ./ipcam.sh
# Watchdog device not enabled.
zqh socket fd=3
 InitSystemParam 0
========================read system param from
file==================================
mac:00:1B:2B:3B:38:89 30
wifimac:00:1B:2B:3B:38:8A 30
wifimac:00:1B:2B:3B:38:8A
bind failuredie param ppid 329
zqh socket fd=3
daemon:===== wifi.c, line 71, WifiConfig():     SSID=Flat 5
daemon:===== wifi.c, line 347, WifiDriversInit():       insmod From kernal
bind failuredie param ppid 336
insmod: cannot insert
'/lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2_sta/rt2860v2_sta
.ko': Success
daemon:===== wifi.c, line 355, WifiDriversInit():       [insmod
/lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2_sta/rt2860v2_sta.
ko mac=00:1B:2B:3B:38:8A] OK
EthMacInit2
ifconfig: SIOCSIFHWADDR: Device or resource busy
EthMacInit3
EthMacInit4
brctl: bridge br0: File exists
switch reg write offset=14, value=5555
switch reg write offset=40, value=1001
switch reg write offset=44, value=1001
switch reg write offset=48, value=1001
switch reg write offset=4c, value=1
switch reg write offset=50, value=2001
switch reg write offset=70, value=ffffffff
switch reg write offset=98, value=7f7f
switch reg write offset=e4, value=7f
done.
EthMacInit5
EthMacInit5
switch reg write offset=14, value=5555
switch reg write offset=40, value=1001
switch reg write offset=44, value=1001
switch reg write offset=48, value=1001
switch reg write offset=4c, value=1
switch reg write offset=50, value=2001
switch reg write offset=70, value=ffffffff
switch reg write offset=98, value=7f7f
switch reg write offset=e4, value=7f
done.
eth is start
=====InitNetDrivers=======
======dns failed===========:
pid 323
NetThreadProc
Error: Watchdog device not enabled.
netstatsem post
Daemon...=======network change=======
Daemon...netok -1 link 2
net is work on eth
enter ethernet  dhcp mode
EthStart1
route: ioctl 0x890c failed: No such process
EthStart2
EthStart3
EthStart4
EthStart5
Error: Watchdog device not enabled.
```

```
netstatsem post end
start app update thread
start sys update thread
zqh socket fd=6
bind failured=======mac=======
00-1b-2b-3b-38-89-
ipc param ppid 326
update socket init
update  socket is failed
update Socket proc is start
=========================read alarm
param=========================(1)
==== sysparam.c      , line  530, InitSystemParam         :read system.ini
user1: , pwd1:
user2: , pwd2:
user3: admin, pwd3: test
zqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredmac:00:1B:2B:3B:38:89 30
wifimac:00:1B:2B:3B:38:8A 30
wifimac:00:1B:2B:3B:38:8A
sys_ver 1a040087
write date ok
curtime 1492789427
audiofd failed
ie param ppid 415
ie param ppid 415
==== encrypt.c       , line  809, CheckAudioChip          :iRet=0, rdat=0xfd
==== encrypt.c       , line  839, CheckAudioChip
:=============Audio Chip Check FAILED!!!!!!!
=======mac=======
00-1b-2b-3b-38-89-
============autio init=========
Ethnet Dhcp
udhcpc (v1.12.1) started
audio capture:421
==== stream.c        , line  564, VideoEnable             :---
VideoEnable(bysize=0)---Initing...
Sending select for 192.168.1.103...
Lease of 192.168.1.103 obtained, lease time 86400
deleting routers
route: ioctl 0x890c failed: No such process
adding dns 192.168.1.254
Unable to set format: Device or resource busy.
init thread ok
capture video:452
Socket proc is start pid=456
send live jpeg:457
send live jpeg:458
send live jpeg:459
send live jpeg:460
send video jpeg:461
send video jpeg:462
send video jpeg:465
send live audio:466
send live audio:467
send live audio:468
send live audio:469
AudioPlayProc:470
send video jpeg:463
send record file:471
============Error grabbing=-3, nCount = 1
send record file:472
send record file:473
send record file:474
```

```
iRet 0 upnp:/system/system/bin/upnpc-static -a 192.168.1.103 81 81 TCP
iRet 0
start gpio check
start motion check
start alarm proc
==== dns.c          , line  179, DnsSendAlarmProc        :start alarm to DNS
server...

web pid:489
init thread ok
========ipaddr 192.168.1.103===========
========port 81===========
FrameRate proc:490
p2p init proc
P2P cmd thread is start...
P2P media thread is start...
P2P play thread is start...
==== moto-new.c      , line 5381, InitMoto               :Init, alarminhappen =
1
==== moto-new.c      , line 1945, ReadVertSteps           :Read
maxverttime = 160
==== moto-new.c      , line 1999, GetVertTime            :get vertime 144

==== moto-new.c      , line 5604, MotoThreadStart         :=========Start,
verttime = 144, maxverttime=160======
==== moto-new.c      , line 1636, ReadLevelSteps          :Read
maxleveltime = 516
==== moto-new.c      , line 1663, GetLevelTime           :get levelime 0

P2P media thread is start...
P2P cmd thread is start...
[ error: /mnt/hgfs/vm_share-2/svn-down/app-jpg_V2.0/func/lens_moto.c,
1468]=>   !!! ERROR : GetLensMotoSitStoreInfo !!!
```

```
dhcp is start...=0
daemon:===== network.c, line 601, DhcpStart():  Set DNS 1 and 2 to
NULL
daemon:===== network.c, line 627, DhcpStart():  2 = []
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[0] = 1
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[1] = 9
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[2] = 2
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[3] = .
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[4] = 1
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[5] = 6
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[6] = 8
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[7] = .
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[8] = 1
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[9] = .
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[10] = 2
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[11] = 5
daemon:===== network.c, line 632, DhcpStart():  Change DNS2[12] = 4
daemon:===== network.c, line 660, DhcpStart():  1 = []
daemon:===== network.c, line 661, DhcpStart():  2 = [192.168.1.254]
run route by zqh
==== network.c      , line 3436, Networkhread          :Create Thread
WfiCheckProc
==== network.c      , line 3342, WfiCheckProc          :===wifi check
status===
==== capture.c      , line  370, SetBrightness         :size iRet=0, value=1
==== capture.c      , line  393, SetContrast           :size iRet=0 value=16
sat1
sat2
==== video.c        , line  994, VideoParamInit        :--------------
VideoParamInit----------
set mirr flip=5
==== video.c        , line 1122, VideoParamInit        :set mirr flip, Param =
5, Saturation = 5
```

```
=============Error grabbing=-3, nCount = 2
[Biz_API.cpp �� 2728 �� ]; pkt_recvTh start!!
[Biz_API.cpp �� 2741 �� ]; pkt_recvTh start sucessfully!!
[Biz_API.cpp �� 2751 �� ]; sendThread start!!!
[Biz_API.cpp �� 2764 �� ]; sendThread create success!!!
[Biz_API.cpp �� 2774 �� ]; timerThread start!!!
[Biz_API.cpp �� 2787 �� ]; timerThread create success!!!
sat1
sat2
write -1
==== main.c        , line  300, main
:SystemVerion==================[ 26.4.0.135 ]==============
write -1
==== encrypt.c     , line 1188, CheckEncryptProc       :start
CheckEncryptProc !!!
==== encrypt.c     , line 1192, CheckEncryptProc       :CheckEncrypt
now
==== encrypt.c     , line 1197, CheckEncryptProc       :CheckEncrypt ok
=============Error grabbing=-3, nCount = 3
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 4
gate way:0.0.0.0        192.168.1.254   0.0.0.0        UG    0      0        0
eth2

======dns failed===========:
--------------SaveSystemParam----------
bparam.stNetParam.szIpAddr = 192.168.1.103
link:2 status:2
=============Error grabbing=-3, nCount = 5
==== dns.c         , line 1203, FactoryRegisterProc     :Start
FactoryRegisterProc
========version:1010907===========
========DeviceID:MEYE-158538-EEBCB=========
=============Error grabbing=-3, nCount = 6
==== moto-new.c      , line 5498, MotoCentProc          :=====moto is
start=====

==== moto-new.c      , line 5499, MotoCentProc          :moto start, read
moto sit
==== moto-new.c      , line 5500, MotoCentProc          :presend = 0,
speed = 5
==== moto-new.c      , line 5507, MotoCentProc          :Set Moto to
Center-----
==== moto-new.c      , line 4557, SendMotoCmd            :Motocmd=0
start run ddns
write date ok
=============Error grabbing=-3, nCount = 7
=============Error grabbing=-3, nCount = 8
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 9
=============Error grabbing=-3, nCount = 10
def key proc
=============Error grabbing=-3, nCount = 11
externwifistatus=0
=============Error grabbing=-3, nCount = 12
=============Error grabbing=-3, nCount = 13
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 14
iRet 0
bFlagInternet 1
bFlagHostResolved 1
bFlagServerHello 1
NAT_Type 2
PPPP_Share_Bandwidth(1) iRet 0
P2P init =1
=============Error grabbing=-3, nCount = 15
=============Error grabbing=-3, nCount = 16
```

```
=============Error grabbing=-3, nCount = 17
=============Error grabbing=-3, nCount = 18
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 19
=============Error grabbing=-3, nCount = 20
==== moto-new.c      , line 3633, MotoCenter              :------verttime = 0
=============Error grabbing=-3, nCount = 21
=============Error grabbing=-3, nCount = 22
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 23
=============Error grabbing=-3, nCount = 24
==== moto-new.c      , line 3669, MotoCenter              :==========Will
Center, verttime = 160
dircnt 64 verttime 160
=============Error grabbing=-3, nCount = 25
=============Error grabbing=-3, nCount = 26
===onstart===1
=============Error grabbing=-3, nCount = 27
on start = 0
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 28
=============Error grabbing=-3, nCount = 29
=============Error grabbing=-3, nCount = 30
=============Error grabbing=-3, nCount = 31
=============Error grabbing=-3, nCount = 32
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 33
=============Error grabbing=-3, nCount = 34
=============Error grabbing=-3, nCount = 35
=============Error grabbing=-3, nCount = 36
=============Error grabbing=-3, nCount = 37
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 38
=============Error grabbing=-3, nCount = 39
```

```
=============Error grabbing=-3, nCount = 40
=============Error grabbing=-3, nCount = 41
=============Error grabbing=-3, nCount = 42
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 43
=============Error grabbing=-3, nCount = 44
=============Error grabbing=-3, nCount = 45
=============Error grabbing=-3, nCount = 46
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 47
=============Error grabbing=-3, nCount = 48
=============Error grabbing=-3, nCount = 49
=============Error grabbing=-3, nCount = 50
=============Error grabbing=-3, nCount = 51
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 52
=============Error grabbing=-3, nCount = 53
=============Error grabbing=-3, nCount = 54
=============Error grabbing=-3, nCount = 55
=============Error grabbing=-3, nCount = 56
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 57
Connection closed by foreign host.
root@kali:~#
```

7.2. IP Security Camera 2 - ipcam.sh output

```
# ./ipcam.sh
# Watchdog device not enabled.
 InitSystemParam 0
========================read system param from
file=================================
mac:00:6E:06:40:1B:D9 30
wifimac:00:6E:06:40:1B:DA 30
```

```
wifimac:00:6E:06:40:1B:DA
zqh socket fd=3
zqh socket fd=3
bind failuredie param ppid 302
bind failuredie param ppid 300
daemon:===== wifi.c, line 311, WifiDriversInit():       insmod From kernal
insmod: cannot insert
'/lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2_sta/rt2860v2_sta
.ko': Success
daemon:===== wifi.c, line 316, WifiDriversInit():       [insmod
/lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2_sta/rt2860v2_sta.
ko mac=00:6E:06:40:1B:DA] OK
EthMacInit2
ifconfig: SIOCSIFHWADDR: Device or resource busy
EthMacInit3
EthMacInit4
brctl: bridge br0: File exists
switch reg write offset=14, value=5555
switch reg write offset=40, value=1001
switch reg write offset=44, value=1001
switch reg write offset=48, value=1001
switch reg write offset=4c, value=1
switch reg write offset=50, value=2001
switch reg write offset=70, value=ffffffff
switch reg write offset=98, value=7f7f
switch reg write offset=e4, value=7f
done.
EthMacInit5
EthMacInit5
switch reg write offset=14, value=5555
switch reg write offset=40, value=1001
switch reg write offset=44, value=1001
switch reg write offset=48, value=1001
switch reg write offset=4c, value=1
switch reg write offset=50, value=2001
switch reg write offset=70, value=ffffffff
switch reg write offset=98, value=7f7f
switch reg write offset=e4, value=7f
done.
eth is start
=====InitNetDrivers=======
daemon:===== network.c, line 383, DnsConfig():  Save to File, 1 = [8.8.8.8]
daemon:===== network.c, line 384, DnsConfig():  Save to File, 2 = [192.168.1.254]
pid 289
NetThreadProc
Error: Watchdog device not enabled.
netstatsem post
=======network change=======
netok -1 link 2
net is work on eth
enter ethernet  dhcp mode
EthStart1
route: ioctl 0x890c failed: No such process
EthStart2
EthStart3
EthStart4
route: ioctl 0x890b failed: File exists
EthStart5
Error: Watchdog device not enabled.
netstatsem post end
start app update thread
zqh socket fd=6
bind failuredstart sys update thread
=======mac=======
00-6e-06-40-1b-d9-
ipc param ppid 295
```

```
update socket init
update  socket is failed
update Socket proc is start
==== sysparam.c      , line  308, InitSystemParam        :read system.ini
user1: , pwd1:
user2: , pwd2:
user3: admin, pwd3: test
zqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredzqh socket fd=3
bind failuredmac:00:6E:06:40:1B:D9 30
wifimac:00:6E:06:40:1B:DA 30
wifimac:00:6E:06:40:1B:DA
sys_ver 5102008c
write date ok
curtime 1492793149
audiofd failed
ie param ppid 379
ie param ppid 379

WRITE I2C : Write Error - TX Data==== encrypt.c      , line  472,
CheckEncrypt          :==========encrypt is error===========

fp == null

WRITE I2C : Write Error - Sub Addrwrite i2c not ack
==== encrypt.c      , line 1122, CheckChipOk          :es8388 isn't exist...

audio capture:383
=======mac=======
00-6e-06-40-1b-d9-
===========autio init========
audio play:384
==== stream.c        , line  368, VideoEnable            :---
VideoEnable(bysize=0)---Initing...
Ethnet Dhcp
udhcpc (v1.12.1) started
Unable to set format: Device or resource busy.
init thread ok
capture video:397
Socket proc is start pid=401
============Error grabbing=-3, nCount = 1
send live jpeg:406
send live jpeg:407
send live jpeg:408
send live jpeg:409
send video jpeg:410
send video jpeg:411
send video jpeg:412
send video jpeg:413
send live audio:414
send live audio:415
send live audio:416
send live audio:417
AudioPlayProc:418
send record file:419
send record file:420
send record file:421
send record file:422
Sending select for 192.168.1.216...
Lease of 192.168.1.216 obtained, lease time 86400
iRet 0 upnp:/system/system/bin/upnpc-static -a 192.168.1.216 14987
14987 TCP
iRet 0
start gpio check
start motion check
start alarm proc
==== dns.c           , line  107, DnsSendAlarmProc        :start alarm to DNS
server...

init thread ok
web pid:442
========ipaddr 192.168.1.216===========
========port 14987===========
FrameRate proc:443
p2p init proc
P2P cmd thread is start...
P2P media thread is start...
==== moto-new.c      , line 4418, InitMoto                :Init, alarminhappen =
0
==== moto-new.c      , line 1318, ReadVertSteps           :Read
maxverttime = 140
==== moto-new.c      , line 1372, GetVertTime             :get vertime 56

==== moto-new.c      , line 1026, ReadLevelSteps          :Read
maxleveltime = 510
==== moto-new.c      , line 1053, GetLevelTime            :get levelime 268

P2P play thread is start...
P2P media thread is start...
P2P cmd thread is start...
deleting routers
route: ioctl 0x890c failed: No such process
==== network.c       , line 2897, Networkhread            :Create Thread
WfiCheckProc
==== capture.c       , line  366, SetBrightness           :size iRet=0, value=1
==== video.c         , line  664, VideoParamInit          :--------------
VideoParamInit----------
set mirr flip=5
```

```
==== video.c         , line  717, VideoParamInit          :set mirr flip, Param =
5, Saturation = 5

============Error grabbing=-3, nCount = 2
==== network.c       , line 2832, WfiCheckProc            :===wifi check
status===
adding dns 192.168.1.254
write -1
============Error grabbing=-3, nCount = 3
dhcp is start...=0
daemon:===== network.c, line 488, DhcpStart():  Set DNS 1 and 2 to
NULL
daemon:===== network.c, line 514, DhcpStart():  2 = []
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[0] = 1
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[1] = 9
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[2] = 2
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[3] = .
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[4] = 1
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[5] = 6
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[6] = 8
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[7] = .
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[8] = 1
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[9] = .
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[10] = 2
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[11] = 5
daemon:===== network.c, line 519, DhcpStart():  Change DNS2[12] = 4
daemon:===== network.c, line 547, DhcpStart():  1 = []
daemon:===== network.c, line 548, DhcpStart():  2 = [192.168.1.254]
run route by zqh
==== main.c          , line  441, main
:SystemVerion=================[ 81.2.0.140 ]=============
Error: Watchdog device not enabled.
============Error grabbing=-3, nCount = 4
============Error grabbing=-3, nCount = 5
```

```
=============Error grabbing=-3, nCount = 6
gate way:0.0.0.0        192.168.1.254   0.0.0.0         UG    0      0        0
eth2

daemon:===== network.c, line 383, DnsConfig():  Save to File, 1 =
[8.8.8.8]
daemon:===== network.c, line 384, DnsConfig():  Save to File, 2 =
[192.168.1.254]
--------------SaveSystemParam----------
bparam.stNetParam.szIpAddr = 192.168.1.216
link:2 status:2
==== dns.c           , line  694, FactoryRegisterProc
:FactoryRegisterProc

========version:20804===========
==== moto-new.c      , line 4438, MotoCentProc           :=====moto is
start=====

==== moto-new.c      , line 4439, MotoCentProc           :moto start, read
moto sit
==== moto-new.c      , line 4440, MotoCentProc           :presend = 0,
speed = 5
==== moto-new.c      , line 4447, MotoCentProc           :Set Moto to
Center-----
==== moto-new.c      , line 3611, SendMotoCmd            :Motocmd=0
=============Error grabbing=-3, nCount = 7
start run ddns
iRet 0
bFlagInternet 1
bFlagHostResolved 1
bFlagServerHello 1
NAT_Type 0
PPPP_Share_Bandwidth(1) iRet 0
P2P init =1
```

```
=============Error grabbing=-3, nCount = 8
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 9
=============Error grabbing=-3, nCount = 10
=============Error grabbing=-3, nCount = 11
def key proc
check wifi
=============Error grabbing=-3, nCount = 12
=============Error grabbing=-3, nCount = 13
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 14
=============Error grabbing=-3, nCount = 15
=============Error grabbing=-3, nCount = 16
=============Error grabbing=-3, nCount = 17
=============Error grabbing=-3, nCount = 18
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 19
=============Error grabbing=-3, nCount = 20
=============Error grabbing=-3, nCount = 21
=============Error grabbing=-3, nCount = 22
=============Error grabbing=-3, nCount = 23
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 24
=============Error grabbing=-3, nCount = 25
=============Error grabbing=-3, nCount = 26
=============Error grabbing=-3, nCount = 27
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 28
=============Error grabbing=-3, nCount = 29
==== date.c          , line  141, NtpThreadProc          :Call GetNtpTime
==== date.c          , line   90, GetNtpTime
:bparam.stDTimeParam.byIsNTPServer = 1
==== date.c          , line   91, GetNtpTime
:bparam.stDTimeParam.szNtpSvr = time.nist.gov
```

```
==== date.c          , line   96, GetNtpTime              :start connect timer
server...=time.nist.gov
=============Error grabbing=-3, nCount = 30
=============Error grabbing=-3, nCount = 31
=============Error grabbing=-3, nCount = 32
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 33
=============Error grabbing=-3, nCount = 34
=============Error grabbing=-3, nCount = 35
=============Error grabbing=-3, nCount = 36
=============Error grabbing=-3, nCount = 37
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 38
dircnt 56 verttime 140
=============Error grabbing=-3, nCount = 39
=============Error grabbing=-3, nCount = 40
===onstart===1
=============Error grabbing=-3, nCount = 41
on start = 0
=============Error grabbing=-3, nCount = 42
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 43
=============Error grabbing=-3, nCount = 44
=============Error grabbing=-3, nCount = 45
=============Error grabbing=-3, nCount = 46
=============Error grabbing=-3, nCount = 47
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 48
=============Error grabbing=-3, nCount = 49
=============Error grabbing=-3, nCount = 50
=============Error grabbing=-3, nCount = 51
=============Error grabbing=-3, nCount = 52
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 53
```

```
=============Error grabbing=-3, nCount = 54
=============Error grabbing=-3, nCount = 55
=============Error grabbing=-3, nCount = 56
Error: Watchdog device not enabled.
=============Error grabbing=-3, nCount = 57
Connection closed by foreign host.
root@kali:~#
```

7.3. Smart Scale Database Dump

```
"ClientDateTime": "2017-04-22 15:10:20",
   "DestinationPlateform": "Cloud",
   "FinalIdentifier": "D2C6001F-D602-4A92-AEF9-B32237643F03",
   "IsAutomaticSync": 0,
   "SourcePlateform": "IPhone",
   "SourcePrefix": "IO005099919",
   "jsonDataRecordsList": [
      {
         "RecordData":
"{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserI
d\":1,\"Revision\":0,\"CreatedDate\":\"2017-03-30
17:27:08\",\"lastRecordOfHistoryTable\":0,\"GlobalTime\":\"2017-03-30
16:27:08\",\"SharingPlatform\":\"HealthKit\",\"PermissionType\":\"Write\",\"I
sAgreedToConnect\":false,\"IsDeleted\":false}",
         "TableName": "DataSharingPlatforms"
      },
      {
         "RecordData":
"{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserI
d\":1,\"Revision\":1,\"CreatedDate\":\"2017-03-30
17:27:08\",\"UpdatedDate\":\"2017-04-15
21:49:18\",\"GlobalTime\":\"2017-04-15
20:49:18\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0
```

```
,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Wri
te\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",
            "TableName": "DataSharingPlatforms"
        },
        {
            "RecordData":
"{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserI
d\":1,\"Revision\":2,\"CreatedDate\":\"2017-03-30
17:27:08\",\"UpdatedDate\":\"2017-04-22
15:55:10\",\"GlobalTime\":\"2017-04-22
14:55:10\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0
,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Wri
te\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",
            "TableName": "DataSharingPlatforms"
        },
        {
            "RecordData":
"{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserI
d\":1,\"Revision\":3,\"CreatedDate\":\"2017-03-30
17:27:08\",\"UpdatedDate\":\"2017-04-22
15:59:23\",\"GlobalTime\":\"2017-04-22
14:59:23\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0
,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Wri
te\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",
            "TableName": "DataSharingPlatforms"
        },
        {
            "RecordData":
"{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserI
d\":1,\"Revision\":4,\"CreatedDate\":\"2017-03-30
17:27:08\",\"UpdatedDate\":\"2017-04-22
15:59:29\",\"GlobalTime\":\"2017-04-22
14:59:29\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0
```

```
,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Wri
te\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",
            "TableName": "DataSharingPlatforms"
        },
        {
            "RecordData": "{\"globalTime\":\"2017-04-22
14:59:58\",\"Revision\":1,\"Source\":\"WE149106703GSS000002\",\"Updat
edDate\":\"2017-04-22
15:59:58\",\"UserId\":1,\"TargetEndValue_mgdl\":160,\"CreatedDate\":\"20
17-03-30
18:18:49\",\"GlucoseSettingId\":1,\"UpdatedSource\":\"IO005099919GSS0
00002\",\"TargetStartValue_mgdl\":110,\"TargetEndValue_mmol\":8.8,\"T
argetStartValue_mmol\":6,\"RevisionCount\":0,\"IsDeleted\":false,\"IsNew
Record\":false,\"DisplayUnit\":\"mg_dL\"}",
            "TableName": "GlucoseSettings"
        },
        {
            "RecordData": "{\"globalTime\":\"2017-04-22
15:00:21\",\"Revision\":2,\"Source\":\"WE149106703GSS000002\",\"Updat
edDate\":\"2017-04-22
16:00:21\",\"UserId\":1,\"TargetEndValue_mgdl\":160,\"CreatedDate\":\"20
17-03-30
18:18:49\",\"GlucoseSettingId\":1,\"UpdatedSource\":\"IO005099919GSS0
00002\",\"TargetStartValue_mgdl\":110,\"TargetEndValue_mmol\":8.8,\"T
argetStartValue_mmol\":6,\"RevisionCount\":0,\"IsDeleted\":false,\"IsNew
Record\":false,\"DisplayUnit\":\"mg_dL\"}",
            "TableName": "GlucoseSettings"
        },
        {
            "RecordData":
"{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserI
d\":1,\"Revision\":5,\"CreatedDate\":\"2017-03-30
17:27:08\",\"UpdatedDate\":\"2017-04-22
16:08:33\",\"GlobalTime\":\"2017-04-22
```

```
15:08:33\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0
,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Wri
te\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",
          "TableName": "DataSharingPlatforms"
      },
      {
          "RecordData":
"{\"AdvPackagesTimeInterval\":0,\"ActivityGrade\":0,\"pairingBit\":false,\"cr
eateUserStatus\":0,\"batteryLevel\":100,\"TXPower\":0,\"UserDetactionLim
its\":2,\"UDID\":\"8633A31A-CDCB-E750-FB1B-
36FE400F426F\",\"GlobalTime\":\"2017-04-22
15:10:19\",\"UserOnDevice\":0,\"pairingCompleted\":false,\"optionalDevice
Name\":\"test
\",\"Source\":\"IO005099919DCR000001\",\"firmwareVersion\":5,\"IsNewR
ecord\":true,\"RSSI\":-56,\"CreatedDate\":\"2017-03-30
17:20:40\",\"isTrusted\":true,\"UpdatedSource\":\"IO005099919DCR00000
1\",\"DeviceUnit\":1,\"PowerSavingMode\":false,\"ID\":1,\"DeviceId\":4,\"in
Range\":false,\"IsDeleted\":false,\"scaleVersion\":5,\"deviceName\":\"SANI
TAS
SBF70\",\"NoOfUsers\":1,\"UserId\":1,\"userExists\":false,\"measurementE
xists\":false,\"UpdatedDate\":\"2017-04-22
16:10:19\",\"unknownMeasurementsCount\":0,\"Revision\":29}",
          "TableName": "DeviceClientRelationship"
      }
   ]
}
```

View: auto   JSON

8. 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].

[28] Nmap Tool [Online] Available at:
<https://nmap.org/> [Accessed September 2016]

[29] Wireshark Tool [Online] Available at:
<https://www.wireshark.org/> [Accessed September 2016]

[30] Cain and Abel Tool [Online] Available at:
<http://www.oxid.it/cain.html> [Accessed September 2016]

[31] mitmproxy Tool [Online] Available at:
<https://mitmproxy.org/> [Accessed April 2017]

[32] SSL strip Tool [Online] Available at:
<http://tools.kali.org/information-gathering/sslstrip> [Accessed March 2017]

[33] Štikonas, Andrius, Reverse engineering Orvibo S20 socket (24/2/2015) [Online] Available at:
<https://stikonas.eu/wordpress/2015/02/24/reverse-engineering-orvibo-s20-socket/comment-page-1/> [Accessed February 2017]

Bibliography

Anon, (2013). “An Introduction to the Internet of Things (IoT)”. [online] Available at: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf [Accessed 26 Nov. 2016].

Anicas, M. (n.d.). OpenSSL Essentials: Working with SSL Certificates, Private Keys and CSRs | DigitalOcean. [online] Digitalocean.com. Available at: https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs [Accessed 26 Mar. 2017].

m00nie.com. (2015). Decrypt HTTPS (SSL/TLS) with Wireshark. [online] Available at: https://www.m00nie.com/2015/05/decrypt-https-ssltls-with-wireshark/ [Accessed 26 Apr. 2017].

Hacking SRICam Password PRINT PASSWORD TO SCREEN. (2015). [Blog] Available at: http://www.openipcam.com/forum/index.php?topic=1155.0 [Accessed 10 Feb. 2017].

Meola, A. (2016). What is the Internet of Things (IoT)?. [online] Business Insider. Available at: http://uk.businessinsider.com/what-is-the-internet-of-things-definition-2016-8 [Accessed 14 Jan. 2017].

Mitchell, B. (2016). Introduction to the Internet of Things (IoT). [online] Lifewire. Available at: https://www.lifewire.com/introduction-to-the-internet-of-things-817766 [Accessed 23 Jan. 2017].

Parr, B. (2017). IPv4 & IPv6: A Short Guide. [online] Mashable. Available at: http://mashable.com/2011/02/03/ipv4-ipv6-guide/#A8fIa8uLmOq6 [Accessed 26 Feb. 2017].

Server, W. (2009). Introducing TLS v1.2. [online] Technet.microsoft.com. Available at: https://technet.microsoft.com/en-us/library/dd560644(v=ws.10).aspx [Accessed 26 Mar. 2017].

Townsend, K. (n.d.). Introduction | Introducing the Adafruit Bluefruit LE Sniffer | Adafruit Learning System. [online] Learn.adafruit.com. Available at: https://learn.adafruit.com/introducing-the-adafruit-bluefruit-le-sniffer [Accessed 21 Feb. 2017].

Anon, (2016). TRENDS 2016 (IN) SECURITY EVERYWHERE. [online] Available at: https://www.welivesecurity.com/wp-content/uploads/2016/02/eset-trends-2016-insecurity-everywhere.pdf [Accessed 19 Jan. 2017].