# Introduction

Advancements within modern technology has led to the introduction of a new type of device: interconnected. These types of devices have been coined with the name Internet of Things (IoT). Such devices are establishing a new way of life for consumers by providing them with the ability to gain more control over certain aspects of their lives and automate tasks. It cannot be argued that implementing numerous IoT devices within a home to create a smart home environment entails numerous benefits for the owner. Advantages include greater control over bills with smart thermometers and meters, the automation of mundane everyday tasks provided by smart kettles and fridges, to the ability to monitor your home without being in the same country with security systems that can be controlled remotely. However, among each advantage implementing an IoT device can bring, it is countered by a disadvantage in the form of an exploitation that can cause a detrimental effect on the owner’s safety and personal information. For example, the smart lock that enables you with the ability to provide a friend access to your home when you are out of town, or check that the door is definitely locked, can easily be abused by malicious attackers. Before smart locks, a burglar would have to be directly in front of your door in order to attempt to gain access and thus risk the possibility of being noticed by a neighbour or passer-by. However, with a smart lock, they can now attack your lock from the safety of their car parked on the street. When smart locks become the norm, no one is going to think twice if they see an unfazed stranger march directly into your home, as it shall be presumed that it was you that provided them access. It is becoming apparent that manufacturers of IoT devices are prioritising the pressure to meet consumer demand over implementing security, and as a result are putting their consumers at risk. As the IoT industry begins to grow, so shall the cyber attacks that are used either against them or utilising them.

## Introduction to IoT

The term Internet of Things (IoT) refers to ordinary devices that have been upgraded with the implementation of an embedded computer system. The introduction of the embedded computer system provides the devices with additional functionality, namely the ability to send and receive data wirelessly.

NEED TO BE MORE IN DEPTH – ADD A FIGURE

These upgraded devices then utilise their built-in hardware and software to communicate with servers and/or other interconnected devices via various communication protocols. *They often send data to cloud-computing servers where it’s then aggregated and analysed. We can usually access the results via web apps or browsers on our mobile devices or home computers.*

### They are typically small devices with little power and storage space, hence data is often stored in the cloud or accessed through the applications database on your smart phone.

Another thing done by them because of the specifications is smaller OS’s such as BusyBox. These OS’s are typically less resource hungry and

For example, BusyBox, an operating system developed specifically for embedded devices is used by a lot of IoT devices. Developers use the OS’s as they are able to operate with limited resources, less processing power necessary etc. Maybe also mention httpd?? Another compact version of something for embedded devices.

They are small devices with little power and storage space… hence BusyBox OS, cloud storage etc..

Reinforce that even though they have less storage/power etc all the tools they use etc are all well established and therefore there is no excuse for the vulnerabilities commonly found in IoT devices as they are trivial like shit password policies and the like.

## Current Situation

Recently, a children’s doll “My Friend Cayla” was hacked by Pen Test Partners where it was discovered that an attacker was able to eavesdrop on conversations the child is encourage to have with the doll. It was also found that the application’s database could be accessed and modified, giving an attacker access to personal information such as the child’s name and their parents names, and also allowing them to communicate directly with the child *ref*. This caused outrage, as it posed such a threat to the children in that anyone with the ability to exploit the toy would be able to interact with the child. This has led to *organisation* enforcing legal action against the manufacturer *ref* as they have violated *what*. Also, as of February 2017, Germany’s Federal Network Agency has prohibited the sale of the doll, branding it an “illegal espionage apparatus” and therefore illegal to sell as within Germany it is against the law to sell surveillance devices that are disguised as something else, which at its core is what My Friend Cayla is.

A more widespread issue caused by trivial vulnerabilities found within a magnitude of IoT devices was the execution of the Mirai Botnet. The Mirai Botnet *did what* and thus is predicted to be seen as a historic attack.

Involved 10s of millions of IoT devices (has this scale ever been witnessed before?)

The fact that an attack of this scale was possibly merely by exploiting manufacturers shit default passwords that do not need to be changed highlights the issue that security is an afterthought.

Dyn – who does it provide services too – they were all down – that’s a big thing.

2015 saw the first *conference* dedicated to the security of IoT devices at Defcon, a world-renowned conference for computer security attended by many high profile security researchers and enthusiasts. The *conference,* called IoT village, entails Capture the Flags, talks, workshops and a multitude of contests for attendants to participate in in an effort to find zero day vulnerabilities and propose best practices for implementing security in the world of IoT*.* This new-found interest in the Internet of Things discussed throughout security conferences the world over indicates that the IoT industry is fast becoming a keen area of interest for hackers, mainly due to their notorious lack of security.

## Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) group was established in September of 2001. Disheartened by a lack of resources on the Internet pertaining to *application* security, founders Mark Curphey and Dennis Groves created OWASP in the hope of introducing *trustworthy computing*. To this day, it is a not-for-profit organisation, fuelled by the thousands of contributors desire to improve the security of software. Its belief is that this can be obtained by developing a transparent system for consumers, businesses and developers.

The organisation blossomed from *statistic* due to its value of honesty. It stays honest as it is open source. All content found within the website comes from the contributors experience and knowledge rather than organisations marketing their newest cyber security tool. Due to this, OWASP became a highly regarded resource due to its unbiased publishing which ultimately makes it a trustworthy resource. *As part of its mission* to provide open source content, *OWASP sponsor multiple security related projects, one of the most popular being the Top 10 Project*.

**Top Ten Project**

The first Top Ten project was published in 2003. OWASP describes the goal of the Top Ten project as “raise awareness about application security by identifying some of the most critical risks facing organisations”. [2]

The ten items contained within each Top Ten Project are selected and then rated according to data provided to the organisation from a variety of firms that specialise in application security. This data can contain in excess of 500,000 vulnerabilities, spanning hundreds of organisations and thousands of applications. In order to determine the rating of each vulnerability, multiple factors are considered including the exploitability, detectability and impact of each. Each factor is determined by a consensus estimation and paired with the number of occurrences of the vulnerability within the aforementioned data set.

Over each and every top ten project, their template for displaying information remains the same. Each issue contains a table as seen below:

FIGURE

This is then followed by four separate sections detailing the best practices that can be utilised to detect and exploit each vulnerability, example attacks scenarios, mitigation techniques that can be implemented to eliminate the vulnerability and references for further reading.

As seen in each Top Ten Project so far, the same information is provided in relation to the risk. The information is made up of:

* A description of the risk – *more*
* Example attack scenarios - *more*
* Testing guidelines – tools and techniques that can be utilised to detect and exploit each *risk/vulnerability*
* Mitigation techniques that can be implemented to eliminate the vulnerability; and
* References for further reading

**OWASP Internet of Things Project**

The first IoT Top Ten was published in 2014. The Internet of Things Top Ten Project differs from previous Top Ten Projects as rather than listing the top vulnerabilities it lists the most vulnerable attack surfaces for IoT, and thus the vulnerabilities typically found within them. The ten attack surfaces within the top ten are described below:

I1 | Insecure Web Interface

Need to decide whether to give a brief explanation of each attack surface within the introduction, or just name them and describe each within the procedure.

I2 | Insufficient Authentication/Authorization

I3 | Insecure Network Services

I4 | Lack of Transport Encryption

I5 | Privacy Concerns

I6 | Insecure Cloud Interface

I7 | Insecure Mobile Interface

I8 | Insufficient Security Configurability

I9 | Insecure Software/Firmware

I10 | Poor Physical Security

## Project Aims and Objectives

The aim of the project is to create a smart home with the implementation of numerous IoT devices that offer a range of features to the consumer. In order to achieve this aim, the devices within this created `Smart Home Environment’ shall be subjected to rigorous penetration testing in an attempt to provide evidence that insecure devices are being released prematurely by manufacturers in an attempt to cope with consumer demands. Thus, introducing a discussion of the need for a security standard to be developed to enable both consumers and organisations to make an informed decision on the devices they purchase.