

Attack Mapping for IoT
William Bathgate

Technical Report

RHUL-ISG-2022-1

11 April 2022



Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student Number: 160423783

William Bathgate

Attack Mapping for IoT

Supervisor: Dr. Salaheddin Darwish



*Submitted as part of the requirements for the award of the
MSc in Information Security at
Royal Holloway, University of
London.*

Acknowledgements.

I would like to sincerely thank my supervisor Dr. Salaheddin Darwish for his continued support and guidance throughout this thesis, as well as his constant encouragement.

Further thanks go to fellow students such as Christos Isaias, who have been a good friend in my final year of studies here at Royal Holloway, University of London, helping to inspire me to achieve greater things. And lastly to my wife, Claudia, and our two daughters, Sophia, and Emma, who all have greatly supported me during my studies of this MSc over the past four years.

Contents

Chapter 1 Executive Summary	8
Chapter 2 Introduction.....	9
2.1 Motivation	9
2.2 Objectives.....	10
2.3 Structure of the Report	12
Chapter 3 Literature Review	14
3.1 The IoT.....	14
3.2 Smart Home IoT Devices.....	35
Chapter 4 Smart Home Attack Map	62
4.1 Structure of the Smart Home Attack Map.....	62
4.2 Smart Home Attack Map.....	64
4.3 Counter-measures and security controls	77
Chapter 5 Conclusions	81
a. Limitations.....	81
b. Conclusion.....	82
References	85

List of Figures

1	Figure 3.1 The layering model used with the Internet protocols (TCP/IP) [36].	15
2	Figure 3.2 CoAP protocol stack for a healthcare system	20
3	Figure 3.3 Five Layer IoT Architecture Model	23
4	Figure 3.4 A simple IoT domain classification [42].	27
5	Figure 3.5 Smart Home Side-View [72].	36
6	Figure 3.6 Layers and several applications of IoT for smart environments [75]	38
7	Figure 3.7 REST-based 7 Layer Architecture for Smart Homes [76]	39
8	Figure 3.8 Cloud Computing Layer for Smart Homes [76]	42
9	Figure 3.9 Security Assurance of Smart Home Devices [80]	49
10	Figure 4.2.1 Reconnaissance/Initial Access/Exploitation Overview	66
11	Figure 4.2.2 Reconnaissance/Initial Access/Exploitation Top	67
12	Figure 4.2.3 Reconnaissance/Initial Access/Exploitation Bottom	68
13	Figure 4.2.4 Cross-Contamination Overview	72
14	Figure 4.2.5 Cross-Contamination 1.	73
15	Figure 4.2.6 Cross-Contamination 2	74
16	Figure 4.2.7 Cross-Contamination 3	75
17	Figure 4.2.8 Cross-Contamination 4	76

List of Tables

1 **Table 3.2** 6 Layer IoT Stack [62]. 19

2 **Table 3.3** IoT Architecture [14, 59] 21

3 **Table 3.4** Mrabet et al. (2020) Proposed IoT Architecture and Threats [22]
. 25

4 **Table 3.5** Smart Home Technologies [12, 22, 75, 76] 44

5 **Table 3.6** Classification of IoT Attacks [19] 46

6 **Table 3.7** Smart Home IoT Attack Layers [73] 47

7 **Table 3.8** Tactics & Techniques Matrices for Smart Home Domain54

8 **Table 4.1** Cyber Kill Chain and MITRE ATT&CK framework stages
comparison [87]62

9 **Table 4.2.1** Reconnaissance/Initial Access/Exploitation Connector
Justifications65

10 **Table 4.2.2** Cross-Contamination Connector Justification71

List of Abbreviations

2FA Two-Factor Authentication
AmI Ambient Intelligence
ARP Address Resolution Protocol
CRUD Create Read Update Delete
DCMS Department for Digital, Culture, Media and Sports
DNS Domain Name System
EPROM Erasable Programmable Read Only Memory
FI Future Internet
FTP File Transfer Protocol
GPS Global Positioning System
HTTP Hypertext Transfer Protocol
ICMP Internet Control Message Protocol
ICT Information and Communication Technology
IDT Intrusion Detection System
IGMP Internet Group Message Protocol
IoC Internet of Content
IoS Internet of Services
IoT Internet of Things
IP Internet Protocol
IPS Intrusion Prevention System
IPsec Internet Protocol Security
ISO International Organization for Standardization
L2TP Layer 2 Tunneling Protocol
LAN Local Area Network
LFI Local File Inclusion
LPWAN Low Power Wide Area Network
M2M Machine-to-Machine
MAC Media Access Control
MAS Multi-Agent Systems
MITM Man-In-The-Middle
OPEX Operating Expenses
OS Operating System
OSI Model Open Systems Interconnectivity Model
OWASP Open Web Application Security Project
PGP Pretty Good Privacy
PIN Personal Identification Number
PMD Personal Medical Devices

POP3 Post Office Protocol 3
PPTP Point-to-Point Tunneling Protocol
RAM Random Access Memory
RCE Remote Command Execution
REST Representational State Transfer
RFI Remote File Inclusion
RFID Radio Frequency Identification
ROM Read-Only Memory
SDR Software Defined Radio
SOA Service-Oriented Architecture
SoC Systems-on-a-Chip
SSH Secure Shell
SSL Secure Socket Layer
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
TCP Transmission Control Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
TfL Transport for London
TLS Transport Layer Security
UDP User Datagram Protocol
UK United Kingdom
VoIP Voice over Internet Protocol
VPN Virtual Private Network
WSN Wireless Sensor Networks
WWW World Wide Web
XXE XML External Entities
XSS Cross-site Scripting

Chapter 1 Executive Summary

This thesis examines the security issues associated with the IoT, particularly those within the smart home. In doing so, technologies and attacks are examined. This results in the purpose of this thesis, to develop an attack map which details how an attacker may gain initial access to a part of the smart home IoT infrastructure, followed by subsequent attacks and how one attack may impact or lead to other attacks and what the resulting effect may be on devices, the infrastructure or victim. Finally, the thesis examines common risks that lead to successful attacks and suggests security controls that can be put in place to minimize risk and the likelihood of threats from being realized.

Chapter 2 Introduction

2.1 Motivation

There are currently more devices connected to the Internet than people on this planet [7]. These objects which connect to the Internet are known as Internet of Things (IoT) devices. The rate of adoption across various fields in our modern society is increasing rapidly [4]. Machine-to-Machine (M2M), another term for IoT, has been adopted amongst many industries and has found many applications such as, industrial control systems, healthcare, transportation, entertainment, energy management such as smart metering and the smart grid, home appliances to name but a few. [2].

The Internet is changing and evolving ever so quickly. This trend is known as 'Future Internet (FI)'. FI is the amalgamation of three different paradigms, Internet of Things (IoT), Internet of Services (IoS) and Internet of Content (IoC). Service oriented Computing (SoC) plays a special part within the cooperation of these paradigms. FI overcomes the issues associated with the current Internet by incorporating converged services, intelligent services, and other associated smart services. [43]

Having heterogenous smart home systems with many different devices incorporating different standards, technologies and platforms makes interoperability between machines far more complex. Interoperability is defined as the capability of devices to connect with one another and transfer data (packets) efficiently, so that it may be processed and used by other entities [14]. And with greater complexity comes the introduction of a greater attack surface due to vulnerabilities creeping into the system. One vulnerability may be exploited which may lead to another vulnerability being exploited and so on. With that said, this is perhaps one reason why IoT devices are a target for cybercriminals. Interestingly, just this year (2020), an increase of 30% in IoT malware attacks was found, with a total of 32.4 million attacks globally [29].

The above suggests that now more than ever, we must identify how we can protect organisations and civilians from having their assets compromised by these malicious individuals as a community of security specialists.

Due to the Coronavirus pandemic of 2020, many people are working

remotely using their personal home networks. This poses a great opportunity for the cybercriminal. Acronis (2020) released a cyberthreats report this year stating that 2021 will be the 'Year of extortion', identifying 'Remote workers under attack' as one of the 'key cyberthreats and trends of 2020'. Furthermore, 'Nearly half of all IT managers struggled to instruct and secure remote workers' [30]. In support of this, at Black Hat Europe 2020, Sygnia [33] described how an Eastern European cybercrime organisation (referred to as "Elliptical Spider") had exploited vulnerabilities in TP-Link home routers from individuals working from home and subsequently targeted a pharmaceutical company, attempting to extort \$300,000,000.00 in Bitcoin. This thesis's motivation is to determine an attack map for smart home networks through IoT devices and suggest security controls to ensure the security goals of confidentiality, integrity, and availability are met to secure the home network.

2.2 Objectives

2.2.1 Aim and Objectives

The aim of this work is to investigate the possible attacks on the IoT Smart Home, to create a map of these attacks and their correlated impacts. This proposed map becomes a guide for the security experts to conduct an effective and efficient security assessment for such a system. To achieve this aim, the following objectives will be followed:

Objectives:

1. Find relevant references – Literature review. This is conducted throughout the entire duration of the project. Identify what IoT is, what the Smart Home is as well as other definitions.
2. Understanding the security issues with IoT - Identify the technologies (security and authentication systems) used in these IoT smarthome devices. Identify why users use the IoT devices, how and why they have been successful. Leading on to supply and demand, and therefore buggy and vulnerable (not tested very well) IoT devices being let loose into the market. Identify reasons why cyber criminals may target a home network. For each of the above reasons, identify the potential attacks and ways in to the home network and ways in which the attacker may be able to pivot to gain further control. Attack map/surface etc. Categorise different types of IoT device and associated vulnerabilities.
 - i. Understanding the security issues with IoT

- ii. Analysing devices – evaluation of attacks.
 - iii. Criteria defined for assessment.
3. Framework proposal which maps between concepts, a guide to attacking a smart home. Identify controls that could be put in place to mitigate and minimise risk – Could controls be placed within the IoT device e.g., EDAS, Event-Driven Adaptive Security, Aman (2015) or network access control devices such as the ‘Aruba ClearPass’ [56].
4. Conclusion and recommendation of tools.

2.2.2 Methodology

This project will follow a theoretical methodology, focusing on a research approach. Key points which will enable me to achieve the goal of the report which is to map possible attacks on Smart Home IoT devices:

- Investigating and analysing security technologies used in IoT devices as well as their vulnerabilities
- Researching different smart home network tools which can be used detect vulnerable devices or potential attacks. These could be embedded within the IoT device, network software, or hardware.
- Understanding consumerism and Smart Homes and the motives of cyber criminals
- Understanding how one attack or compromised device may lead to further attacks
- Literature review from a mixture of sources including but not limited to: books, journals, articles, white papers, interviews and questionnaires.

Finding relevant literature and information will be conducted using the following methods:

- Relevant literature will be found through use of the University’s online library in the first instance. Secondly, supporting research will be conducted through use of a search engine such as Google. Google Scholar may be used amongst a variety of online libraries.
- Asking experts within the field of IoT security
- IoT network security tools will be investigated by search engine queries, reading appropriate literature, asking experts in online forums, asking colleagues etc.
- Reading surveys, white papers, projects and articles related to IoT and smart home security.

- Some objectives will require PoC and thus an analysis of the source code, looking at the attacks, data sets, as well as previous research.

2.3 Structure of the Report

Before delving into the report structure, it is essential to note this project's approach and report. This report is written in such a way that assumes the reader is reading it linearly, with each chapter and section building upon existing knowledge detailed in said chapter. This is an example of scaffolded learning and will allow the reader to access this report's contents regardless of technical understanding. Therefore, this report will follow the following structure:

Chapter 3 includes background research (including the literature review) of:

- The IoT:
 - Explaining what it is
 - The different sectors and industries it has been applied to
 - Growth, Subsequent impact and Challenges
 - Standards, technologies, and frameworks
 - Legislation (United Kingdom specific)
- Smart Home IoT devices:
 - Common devices
 - Technologies, standards, and frameworks explaining how specific Smart Home IoT devices work
 - Attacks, Threats, and Vulnerabilities of a Smart Home network

In Chapter 4, we design an attack map that depicts how attackers may gain an initial foothold on a home network through exploiting a vulnerability in an IoT device, from where they may pivot between devices or escalate privileges to compromise assets on the network with regards to the CIA triad: Confidentiality, Integrity and Availability, and perhaps commit further crimes such as blackmail, install spyware or use stolen credentials to gain access to other systems, etc.

Finally, we propose a solution, suggesting how we may minimize risk in a Smart Home network environment.

This report ends with Chapter 5, our conclusion, which summarizes our findings, details limitations of said findings, and describes any future work which may be carried out. Ultimately, it concludes with an assessment against this report's original objectives, stating how they have been successfully met.

Chapter 3 Literature Review

In this chapter, we analyse and discuss relevant research, which will allow us in chapter 4 to formulate our proposed solution. In particular, we decompose the IoT into sub-sections enabling us to take a detailed look at what it is, the technologies used, and the impact it has had before identifying specific attacks and vulnerabilities in a Smart Home network. Consequently, by the end of this chapter, you, the reader, will have a good understanding of the fundamental technologies and threats to the IoT.

3.1 The IoT

3.1.1 Definition of the IoT

The IoT (also referred to as M2M, Future Internet, and Internet of Objects) refers to 'Things', which are machines, objects or devices that use the Internet's infrastructure to communicate and transfer data with one another, without the need for human interaction. That is not to say that humans do not interact with these devices, especially in the case of smart home or health related IoT devices which may require humans as an input or to be remotely controlled. These IoT devices have been adopted amongst various sectors from energy with the smart grid, health with Personal Medical Devices (PMDs) that monitor a human's health, adjust parameters and generate reports, and within our very own homes. This has resulted in the combination of physical and cyber worlds. The expression "Internet of Things" (IoT) was coined back in 1999 by Kevin Ashton, a British technology pioneer. He cofounded the Auto-ID Center at the Massachusetts Institute of Technology. [45]

Krishna (2017) defines the IoT as a 'dynamic global information network consisting of Internet – connected objects'. RFID Internet of Things devices driven by Wireless sensor networks (WSN) find themselves across multiple applications and industries such as energy, health, transportation, agriculture and entertainment. These 'Things' vary vastly in terms of sector and application in which they are used, size, capacity, energy consumption and computational power. [8]

Ammar et al. (2017) states that there has been a very rapid growth of Internet connected devices. These devices may be very basic in the nature, being simple sensors, or they may be extremely complex, for example, cloud servers. These 'Things' may be IP cameras, thermostats, smart bulbs, electronic

appliances, smart security and much more. Furthermore, these IoT devices are all similar in that they connect to the Internet and exchange data. This network connectivity allows these devices to be controlled remotely. This is achieved through making use of existing network infrastructure, be it home networks / Local Area Networks, or Wide Area Networks such as the Internet. This results in further integration with the real world, and less human interaction being needed. These everyday objects such as bulbs or cameras become ‘smart’ through the IoT, making use of its technologies. [1]

IoT devices may connect to the Internet in several ways. They may connect directly to the Internet wirelessly or wired. They may also make use of an IoT gateway. This gateway collects data from IoT devices and can transfer the data more securely.

In the next section of this thesis, we look at the infrastructure the IoT utilizes, the Internet.

3.1.2 IoT Infrastructure

Before defining what the IoT is, we will first understand a fundamental part of the IoT, the Internet. The Internet is a global infrastructure, a network of networks spanning the globe, allowing humans to communicate with one another by interacting with applications on their devices. The Internet provides human-human communication. This naturally leads onto the TCP/IP protocol stack/suite. The TCP/IP stack is an abstract 4/5 layered network communication model that defines how data is transmitted through sets of rules, known as protocols. Each layer of the TCP/IP stack has a specific purpose and has particular protocols associated with it.

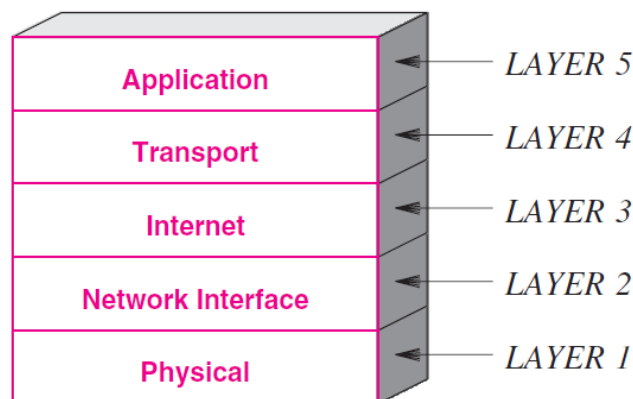


Figure 3.1 The layering model used with the Internet protocols (TCP/IP) [36].

In the above figure, Comer (2009) depicts a visual representation of the layered TCP/IP protocol stack. Each layer within the stack communicates directly with the layers above and below it, with humans interacting with Layer 5, the Application layer. Layers are sometimes combined or are referred to by other names such as Data Link replacing the Network Interface layer. The next section will briefly summarise each layer's functionality as described by Comer (2009).

Layer 1: Physical – Layer 1 is the bottom layer of the TCP/IP stack, where protocols specify details regarding the underlying transmission medium and associated hardware. The Physical Layer specifies how signals are used to transmit data, for example, different voltages representing digital values. Examples of protocols within this layer include Ethernet, Bluetooth, Digital Subscriber Line, Wi-Fi.

Layer 2: Network Interface – This layer is concerned with specifying how data is sent over the network and may include details about network requirements such as network addresses, maximum packet size, and the underlying mediums that belong in layer 2. The Network Interface layer is concerned with the communication of higher-layer protocols and the underlying network. MAC (Media Access Control) addresses are utilised on this layer.

Layer 3: Internet – This layer is responsible for the logical transmission of packets over the Internet. Considerations that Layer 3 protocols specify include the Internet addressing structure, the format of Internet packets, how packets are divided and re-assembled, routing of packets and handling errors during transmission, and fragmentation of data packets. Examples of protocols within this layer include Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Group Message Protocol (IGMP).

Layer 4: Transport – The Transport Layer creates a virtual connection between network hosts. There are two protocols which this layer deals with, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP sends data reliably; however, it is slower than UDP, which sends data quickly, but transfers are not guaranteed and are best effort. Therefore, UDP is better suited for Voice over Inter Protocol (VoIP). In contrast, TCP is better suited for Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) from the Application Layer, which requires reliable transfers.

Layer 5: Application – The Application Layer is the layer with which users interact and, therefore, the TCP/IP stack's top layer. For example, a user who wants to view a website will use a web browser, which in turn will make use of HTTP to send a GET request to the webserver. This process is done through HTTP messages, which can be one of two types, requests and responses. The aforementioned is an example of one of many protocols that can be used in the Application Layer. This layer specifies how applications on two different machines will communicate, dictating the format of messages, as well as procedures. Examples of protocols used at this layer include HTTP, FTP, SMTP, POP3, SNMP, SSH, Telnet, DNS, etc. [36]

A severe issue with TCP/IP is that it was developed for networking and communication purposes over the Internet but was not done with security in mind from the outset. With the onset of electronic commerce and online payments, privacy has become paramount. This has resulted in the subsequent obligatory addition of security technologies. Kizza (2017) lists security protocols which may be implemented at specific layers of the TCP/IP stack: Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, secure IP (IPsec), Secure HTTP (S-HTTP), secure e-mail (PGP and S/MIME), SSH, and others [37]. Whereby, SSH is implemented at the Application Layer (Content Filtering, Encryption), SSL and TLS at the Transport Layer (Port Filtering), and IPsec implemented at the Network Layer, PPTP, and L2TP at the Data Link Layer (VPN Tunneling), and scrambling and hopping at the Physical Layer, for example.

With conventional use of the Internet, the end-user interacts with the top layer of the TCP/IP protocol stack, the Application Layer. The IoT differs in that the Internet was predominantly associated with the World Wide Web (WWW). Digital or online files and resources may be shared through the infrastructure of the Internet; it is cyber based. However, a shift has occurred whereby cyber and physical realms are merging/have merged. The IoT is primarily concerned with M2M communication, allowing machines to independently communicate with one another without the need for human interjection. They use a network (two or more devices connected to share data or resources) to achieve this, with the Internet being the core technology. Before we define what the IoT is, let us delve into how people have devised different models and architectures for the IoT with a layered abstract approach, similar to the TCP/IP protocol stack.

3.1.3 IoT Architectures

In this section we examine the possible architectures of the IoT, comparing it with TCP/IP, and ISO/IEC 7498; the Open Systems Interconnectivity (OSI) Reference Model and how IoT technologies may fit within that model. Now, like the TCP/IP protocol stack, both models are abstractions of network models, displaying a layered architecture. Nevertheless, there are several significant differences. [57]

Mrabet et al. (2020) states that there is no set defined architecture that is adopted across the globe and domains for the IoT, but instead, many different architectures have been suggested. Architectures range from three-layer to five-layer and are also designed for specific purposes such as middle-ware-based or service-oriented. This only adds to the complexities of the IoT. [22]

A common five-layer model is:

1. **Application** – management of IoT device, delivery of data to user.
2. **Middleware** – provides interoperability – management of device and information.
3. **Internet** – conversion and transfer of data. Provides endpoint connectivity. Provides compatibility between different network technologies e.g. Bluetooth, LAN and LoRaWAN.
4. **Access Gateway** – centralization of communications through translation of protocols and messaging. Collection of data and manages the transportation of data between multiple devices and applications.
5. **Edge Technology** – IoT capable device such as a smartphone. It provides an endpoint and is used to connect directly to the IoT device.

The technologies and protocols for the IoT may be broken down into the following categories:

- **Wireless Communications:**
 - Short Range – Bluetooth Low Energy (BLE), Light Fidelity (Li-Fi), Near Field Communication (NFC), Radio-Frequency Identification (RFID), Wi-Fi
 - Medium Range – HaLow, LTE Advanced
 - Long Range – Low-Power Wide Area Networking (LPWAN), Very Small Aperture Terminal (VSAT), Cellular

- **Wired Communications:** Ethernet, Multimedia over Coax Alliance (Moca), Power Line Communication (PLC).
- **Operating System:** ARM Embedded OS (De facto OS for IoT devices), Ubuntu Core (Very popular), RIOT OS, RealSense OS, INTEGRITY OS. [85]

Windpassinger (2019) suggests an IoT stack which makes use of the TCP/IP protocol stack. He adds that there is a lot of discussion currently amongst different standardization organizations about an adapted IoT stack that markets could make use of. However, he then proposes that different stacks may have to be used based upon the context and nature of how the IoT device is to be used. [63]

The below is an adapted version of his proposal.

IOT STACK		
TCP/IP	IoT applications	Device Management
Data Format	Binary, JSON, CBOR	
Application Layer	CoAP, MQTT, XMPP, AMPQP	
Transport Layer	UDP, DTLS	
Internet Layer	IPv6/IP Routing	
	6LOWPAN	
Network/Link Layer	IEEE 802.15.4 MAC	
	IEEE 802.15.4 PHY / Physical Radio	

Table 3.2 6 Layered IoT Stack [62]

Furthermore, Windpassinger (2019) states that the IoT can be defined through six layers, whereby four of the layers are vertical, and two are transversal layers. The vertical layers being:

- IoT Devices & Things.
- IoT Gateways.
- IoT Platforms.
- IoT users Access and Applications.

The transversal layers being:

- IoT Networks (wired and wireless).
- IoT Security. [63]

It must be noted that although the architectures may be similar, protocols implemented within an IoT protocol stack must be different from those within the TCP/IP stack. This is for the main reason that IoT devices are low power devices which are required to operate for months or even years on a single set of batteries. [19]

Traditional Stack	CoAP Stack
Application Layer	CoAP
Transport Layer	UDP
Network Layer	IPV6/RPL
Network Adaptation Layer	6LoWPAN
Data Link Layer	802.15.4
Physical Layer	802.15.4

Figure 3.2 CoAP protocol stack for a healthcare system [18]

In Figure 3.2 we see an example of a protocol stack designed for healthcare using the Constrained Application Protocol (CoAP) healthcare framework which is an architecture for an IoT healthcare system. It has been designed for devices such as sensors which have limited resources. It is based on the Representational State Transfer (REST) paradigm.

The CoAP protocol can send reliable data transmissions through use of Con and ACK messages. Another option which makes it versatile is that it can send best effort data transmissions through use of NON messages. It is similar to HTTP in the fact that it utilizes four methods, GET, PUT, POST and Delete. These methods are used to communicate sensor data. [18]

Choudhary and Jain (2016) as well as Khan et al. (2012), Yang et al. (2011) and Wu et al. (2010) suggest a simple 3-layer overall architecture for IoT devices [14, 11/59, 12/60, 61]. Andrea, Chrysostomou and Hadjichristofi (2015) support this when writing that the IoT is quite often 3 layered structure:

- the **Application Layer**
- the **Network Layer**

- the **Physical/Perception Layer** [12, 19]

An adaptation of the popular 3-layer IoT architecture may be seen below. It is flexible in its approach as it must tackle the interoperability issues in the IoT and must be able to connect an extremely large number of devices over the Internet, and due to amount of ‘Things’ connected, it must be able to withstand large amounts of traffic.

<u>Three Layer</u>	<u>SOA (Service-Oriented Architecture)</u>	<u>Middleware Based</u>		<u>Five Layer</u>
Application Layer	Applications	Application Layer		Business Layer
	Service Composition	Middleware Layer		Application Layer
	Service Management	Coordination Layer		Service Management
Network Layer	Object Abstraction	Backbone Network Layer		Object Abstraction
Perception Layer	Objects	Existing Application System	alone	Objects
			Access Layer	
			Echo Technology	

Table 3.3 IoT Architecture [14, 59]

It is important we understand what is meant by these layers as described by Choudhary and Jain (2016) in Table 3.3. We will in particular look at their ‘Five Layer’ model (far right column highlighted in blue), whilst comparing other definitions and models they have provided.

The ‘perception layer’ a.k.a. the ‘object layer’ is similar to the bottom, physical layer of the OSI reference model. The object layer consists of hardware and collects data from the physical world. It then processes the gathered information and transfers it to upper layers. This layer includes sensors, RFID and ‘two-dimensional code equipment’ which gathers data such as the temperature, weight and movement/vibrations etc. Ultimately, the perception layer converts collected data and transfers it up to the network/object abstraction layer through secure channels.

The object abstraction layer receives the data from the object layer and transfers it to the upper layers through secure channels. Data is transferred to the ‘central information processing system’ through such technologies as 6LoWPan, Zigbee, WiFi, infrared, GSM, 3G etc. It is important to note that

6LoWPAN is an acronym for IPv6 over Low-Power Wireless Personal Area Networks [16] and it is widespread amongst a variety of popular IoT architectures.

The service management/middleware layer is a software layer/set of sub layers which allows different components of the IoT to communicate with one another, allowing new technologies to be developed and integrated within the existing infrastructure. Furthermore, it enabled efficient communication amongst software by providing a connectivity layer for the application layers and sensors to make use of. This middleware layer consists of the service oriented architecture, but also deals with the collection and filtering of data which has been received from the object layer. It also manages the storage of information related to lower layers, as well as making decisions and delivering of services over the network wire protocols.

The application layer provides a means for the user to manage the service in which they are using. This is based upon the information in the middleware layer and delivers information to the user in a format they can understand such as reports. These reports may be logistics, or perhaps retail or even health related. The application layer however, does not build upon the IoT architecture, but instead interprets the information which is requested by the user.

Finally, we have the top layer, the business/management layer which is responsible for the monitoring and management of the four layers beneath it. In turn, it manages all of the IoT applications, services and provides top level analytical reports which may include graphs etc. useful for decision making by managers and executives. [14, 59, 60, 61]



Figure 3.3 Five Layer IoT Architecture Model

Nolle (2020) corroborates the above approach when he identifies two different models for IoT, the traditional device-centric model, and the service-oriented architecture (SOA) which can be seen in Table 3.3.

The IoT device-centric model consists of many sensors which create events. These sensors are available through the network. It also consists of open controllers which can react to real-world stimuli. The applications receive the events which are created by the sensors, and then send appropriate commands to the controllers.

The IoT service-oriented architecture (SOA) focuses on software functionality. This software functionality is efficient as it is reusable and may be

applied to a variety of tasks. The two models differ in their approaches. The SOA focuses on how the IoT application interacts with the physical world, whereas the device-centric model focuses more so on the technical aspects. [65]

Ferrari (2019) in his course on 'Hacking IoT Devices' puts forth four different communication models:

- Device-to-Device Model – for example a mobile phone communicating with a wireless printer over a wireless medium e.g. Bluetooth, NFC, Wi-Fi etc.
- Device-to-Cloud Model – IoT devices are connected directly to the application server. A home with multiple security sensors (smoke sensors, fire sensors, cameras) are connected directly to the application server which is hosted in the cloud. This application server acts as an intermediary between the sensors and alarms / safety and security controls for example.
- Device-to-Gateway Model – Similar to the Device-to-Cloud model; however, it collects data from all sensors (smoke sensors etc. and alarms), and then sends it to the application server. This gateway can then filter and examine data, implement security and act as protocol and message translation.
- Back-End Data Sharing Model – Devices communication with application servers, extending the Device-to-Cloud model and making it scalable so the sensors are accessible by multiple third parties. [85]

In Table 3.4 Mrabet et al. (2020) proposes a detailed and thorough IoT architecture. This table comes from their paper, 'A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis' which appears to have some of the best guidance and information about each layer to date. A fascinating read for anyone interested in this topic. It is of great importance to note the technologies used at each layer within this table, as it really details and links together how the IoT may work and builds upon previous research and ideas of IoT architectures. [22]

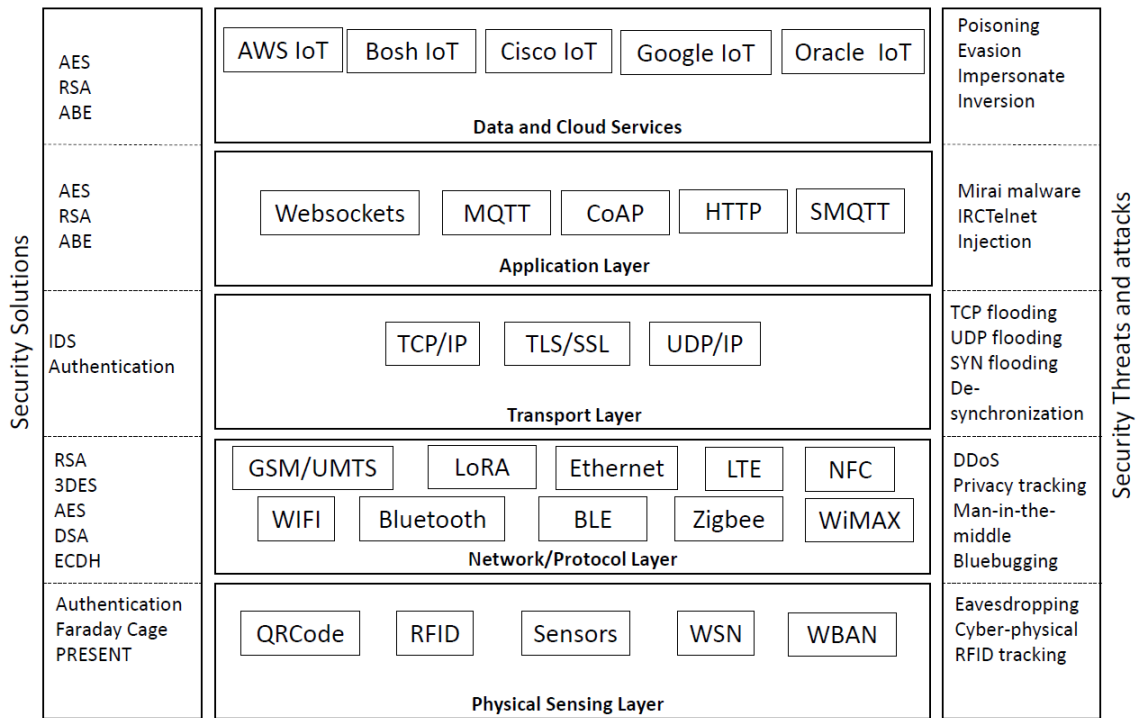


Table 3.4 Mrabet et al. (2020) Proposed IoT Architecture and Threats [22]

The development of these architectures solves many of the issues related to interoperability within IoT by examining the protocols and layers. [62]

With this fundamental understanding of the technologies and architectures which can be implemented as part of the IoT, we may now examine different IoT paradigms.

3.1.4 IoT Paradigms

Pervasive/ubiquitous computing – Pervasive computing also known as ubiquitous computing is often associated with the incorporation of microprocessors into everyday objects. This allows further features to be introduced, primarily allowing the transfer of data between devices. These devices can be found everywhere, are completely connected via networks. They are always available, hence the terms, ubiquitous and pervasive. [38]

Ambient intelligence – Ambient Intelligence (AmI) attempts to solve everyday problems by implementing information technology into day-to-day items and activities. AmI has found its way into many innovative services, for example the IoT, smart environments, and e-health for example. An AmI

environment consists of autonomous devices. These devices are not intrusive to the consumer but allow the user to reap all of the benefits of using the devices, without necessarily being aware of their presence. However, the devices are aware of the presence of humans and through sensors may react to gestures and actions etc. [39]

Everyware – Everyware is a term that is often used interchangeably with ambient computing, ubiquitous and pervasive computing, which refers to sensors which connect to the Internet. These devices take inputs from the environment whether it is a smart home or otherwise and process the input. This results in the constant monitoring and profiling of the consumer. Mutter goes on to explain the different trends that ‘Everyware’ may impact, suggesting that mobile computing, wearable devices, Internet of Things, cloud computing, hyper-personalization, and digital marketing may be some of those most effected. [40]

Physical computing – Physical computing is a term that is often associated with the connection between analog and physical worlds. This is accomplished through use of devices which connect to one another and have capabilities of sensing and computational processing. Physical computing includes many research domains, such as human-material interactions, tangible interactions, and shape-changing and organic user interfaces. [41]

Internet of Things – The IoT has brought about change in our lives in terms of the sheer amount of information and interactivity we are now processing. This change has been brought about by low-power wireless technologies, coupled with embedded microprocessors and intelligence which are Internet-enabled, meaning that they can connect to the Internet for processing and transfer of information. The IoT combines both analog and digital worlds and can be classified into personal IoT, industrial IoT and at-scale. Personal IoT includes smart homes for example. Whereas industrial IoT can be a smart factory, and at-scale IoT may be a smart city for example. [42]

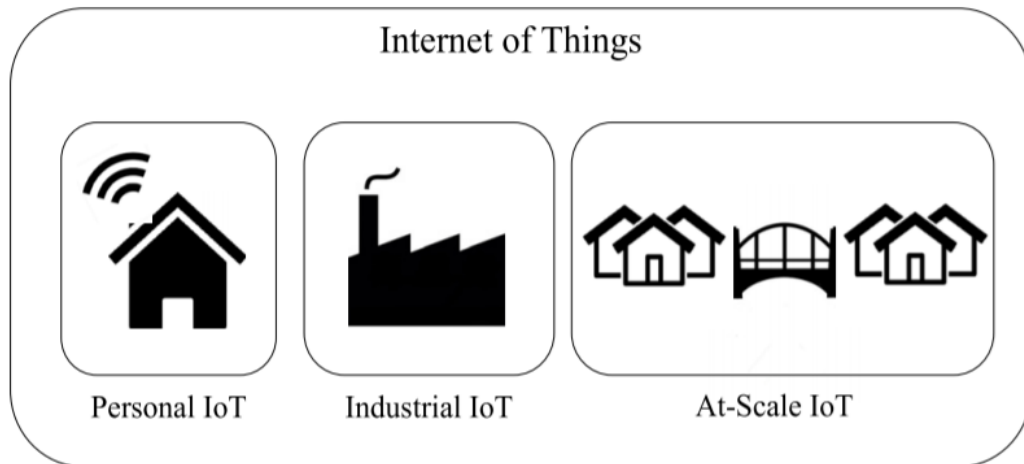


Figure 3.4 A simple IoT domain classification [42].

M2M – Machine to Machine (M2M) is a term used to describe the wireless or wired communication and exchange of data between two devices, machines, or equipment without human interaction. These autonomous devices are most often low powered and low-cost. An M2M system includes several components: sensors, a wireless network, a device which has Internet connection capabilities, and gateway which manages the connection between devices and also between the M2M network and other networks. As has been said about other paradigms we have previously discussed, M2M has been found across many different sectors such as industrial automation, transportation, healthcare, smart grid, utilities, smart cities, fleet management, consumer electronics and smart homes. [2]

3.1.5 Domains

As stated previously, there are more devices connected to the Internet than there are people in the world [7]. It is not only companies with a technological focus such as 'Ericsson, Bosch or Siemens' that are making use of the IoT, but rather a variety of markets. Instead, we are currently observing the birth of a mega-market where multiple markets such as home, logistics, energy management, information technology and telecommunications amongst others are merging [45]. As an end user, the IoT is not something which we will individually experience. However, we are seeing more and more objects connected to the Internet, making use of its connectivity to improve efficiency in comparison to unconnected devices or previously physical unsmart

artefacts.

Figure 3.2 suggests several domains in which IoT devices may be classified: 'Personal IoT', 'Industrial IoT', and lastly, 'At-Scale IoT'. I will further simplify this by categorizing IoT devices into just 2 primary domains:

1. Industrial Sector - organisations, smart grid, healthcare, corporate IoT.
2. Connected Home - smart cities, connected home, enterprise security.

Furthermore, Mrabet et al. (2020) proposes that there are several domains for IoT applications including, different utilities such as electricity and water, transportation, and logistics, environmental and agriculture, and finally, industrial and manufacturing. [22]

We will now briefly detail each of the above sectors, defining what they are and how IoT has been adopted and utilised within said sector.

The Industrial Sector

Smart grid – The Department of Energy's Office of Electricity (OE) defines the grid when writing, that the grid is an electronic grid. This electronic grid is made up of various components such as transmission lines and transformers, amongst other things such as substations for example. This electronic grid takes the electricity from the power plant and delivers it to wherever is needed, be it your home or office. The electric grid in current use was built over a century ago in the 1980s, and over time has improved with new additions [48]. However, within our society, the electric grid is being pushed to its capacity. A plausible solution is the 'Smart grid'. There are two primary benefits to the smart grid. The first, improvements to the economy and to businesses as well as all users of the grid. The second, improvements to our environment. The smart grid achieves this through improvements made in terms of reliability, availability, and efficiency. In particular the Department of Energy's Office of Electricity details how it does this:

- More efficient transmission of electricity
- Quicker restoration of electricity after power disturbances
- Reduced operations and management costs for utilities, and ultimately lower power costs for consumers
- Reduced peak demand, which will also help lower electricity rates
- Increased integration of large-scale renewable energy systems
- Better integration of customer-owner power generation systems, including renewable energy systems

- Improved security [48]

Transport/logistics – Transportation may be defined as the process of moving and delivering of goods from one location to another. Bassi et al. (2013) states that regarding transport logistics, the IoT improves several aspects. One such aspect is material flow systems, another is the positioning and tracking of shipments across the globe, and finally, automating the identification of these shipments. Furthermore, as is with the purpose of many applications of the IoT, it improves the efficiency of how energy is used. This will save organisations energy consumption costs, but also improve efficiency of their operations with ‘intelligent cargo movement’, as well as having less of an impact on the environment. This is achieved through M2M communications whereby supply chain information is automatically synchronised with real-time tracking of objects. Furthermore, due the nature of IoT devices, it enables remote communication between humans and goods [45].

Transportation may also include vehicles carrying those goods, or vehicles and movement in general. This could be private or public transportation. Smart cities can improve traffic congestion through use of IoT. Traffic lights which are connected to the IoT have sensors which detect the presence of cars and will adjust the timing of the lights in real-time which can drastically improve real-time traffic congestion. Furthermore, if we take the example of public transportation such as a bus or train, users may use RFID (Radio Frequency Identification) on a number of different devices, be it smart cards or smart phones to make payments for their fares. As can be seen, IoT can and is already greatly improving the efficiency of transportation. This can be seen with the implementation of ‘Oyster Cards’ by Transport for London, which allow a user to ‘touch’ in or out as they are travelling, removing the need for people to purchase other physical tickets or make payments etc. Furthermore, the TfL (Transport for London) Oyster card may be used in conjunction with the ‘contactless app’ which allows a user to manage payments, check journey history and more [50].

Factories/Production – Following on from transport/logistics, factories and production are incorporating the IoT to improve their operations, thus reducing their operating expenses (OPEX). Benotsmane et al. (2019) defines a Smart Factory as, a system which utilizes many elements of Industry 4.0 such as IoT and Big data. Autonomous robots, tools, sensors, controllelrs and other

devices transfer continuous data with one another to achieve goals, resulting in more efficient production. This has an impact in that it makes it possible for factories to produce more, do it more efficiently, whilst also being environmentally friendly. Furthermore, there is far less need for human interaction, and therefore fewer employees. [45, 51]

Ahuett-Garza and Kurfess (2018), and Zhong et al. (2017) both suggest that the production sector is having to adapt to a change in the market. This is due to a variety of reasons, including globalisation, whereby goods are transported worldwide. To add, short shelf-lives of products with technology advancing at an incredible rate, making new technology quickly redundant or unwanted by consumers, as well as the supply and demand and the expectations of customers. This has meant that the production sector has had to adapt significantly [52, 53].

The impact of these technologies is well-known and an often argued point in that it may cause manual and laborious roles within the workforce to be made redundant. Conversely, a large number of technicians will be needed to maintain these machines, and roles will be introduced for the programming and repair of these machines.

Retail/Consumer IoT – IoT has affected the retail sector in several ways. The first and most obvious is that of the sale of actual IoT devices such as Amazon’s Alexa, Amazon Echo, Google Echo, Google Home, Ring security, Smart TVs etc. These devices often have their own proprietary standards, which lead to heterogeneous and varied environments which adds interoperability, meaning that due to the variety of technologies, there is greater complexity in the communication between these devices, which naturally leads to more vulnerabilities being present. This has altered the consumer’s market, with customers transforming their homes with these IoT devices, resulting in a lifestyle change. Further to this, organisations from all over the globe are creating alternative devices to those mentioned above which provide the same or similar functionality.

Healthcare – The healthcare sector utilizes the IoT in a variety of ways. The IoT has had an obvious impact on patients and medical practitioners since its introduction. Mohan (2014) gives an example of how when writing, that PMDs (Personal Medical Devices) have allowed patients to be treated without the need for a doctor or nurse, sometimes remotely, even from the comfort of

their home. This enables patients to be more independent before they need assistance. PMDs are usually consist of a wireless interface which transfers data to and from a base station. This base station has many functions such as reading of medical reports generated from data collected by the PMD, checking of status, reading and updating parameters and much more. These PMDs will most likely be able to communicate and transfer data to and from the cloud and connect to the Internet from any Internet access point.

A disadvantage of using this technology is that as it is connected, the wireless interface exposes the PMD to security threats, which could amongst other things such as privacy concerns, lead to a life-threatening situation is data is manipulated, or the device becomes unavailable through nefarious means. As the device is connected to the Internet, it also means that it is vulnerable to attacks across the globe [6, 45].

The Connected Home

Smart Cities – Giffinger et al. suggests that a smart city is improved through incorporating IoT. A city may be improved with regards to its economy, governance, living, environment, mobility/transportation, and people [44]. It is an urban area which achieves a high quality of life through the promotion of sustainable development [45]. Thales Group (2021) states that Low Power Wide Area Networks (LPWAN), wireless and cellular technologies are connecting and improving infrastructure. In addition this impacts the residents of this smart city by improving their quality of life through efficiency and convenience. How is this achieved? Citizens of the smart city engage in a variety of ways using smart phones, mobile devices, connected cars and homes. Each of these devices may be paired with the city's physical infrastructure. Furthermore, energy distribution, refuse collection, traffic congestion and air quality may all be improved through incorporating the IoT within a city [49].

The Connected Home – IoT devices can be used within the home to make it a smart home. Bassi et al. (2013) [45] suggests that IoT 'mainly impacts three aspects' within the smart home: 'resource usage (water conservation and energy consumption), security and comfort'.

To elaborate, IoT devices may enhance how energy utilities are used within the home, such as electricity, heating, and water consumption for example, 'Hive' which is used within 1.9 million homes and allows the user to control everything within the home, whether it is controlling a utility such as

heating, or security related such as cameras or alarms. It does this whilst integrating with other IoT devices within the home such as Amazon Alexa, Google Assistant and Siri, making it M2M [46].

In addition, IoT devices may be used to enhance the security of the home. Devices such as Amazon's Blink home CCTV or a number of different smart home IoT devices from Ring. Ring states that it enables the user to receive notifications on their smart phones when the camera has detected motion, check a live view, and even speak to people through a built-in speaker [47]. They provide devices such as video doorbells, security cameras and security systems, all which can be operated remotely from a smart phone. These devices may improve security, detecting theft, fire or unauthorized entry [45].

3.1.6 Growth, Impact and Challenges

If there is one word that I keep seeing coming up repeatedly in my research that sums up the growth of the IoT, it is 'rapid'. Andrea, Chrysostomou and Hadjichristofi (2015) state that in the last 10 years the IoT landscape had 'rapidly' grown and developed. However, the issue here is that along with this growth, security challenges have not been identified. [19]

Choudhary and Jain (2016) briefly describe the exponential rise of the IoT, when saying that initially IoT was introduced to support RFID. This occurred in 1999. However, it continued to gain recognition and was implemented in many Internet connected objects in 2010, whereby the ratio between users and the number of devices connected to the Internet was greater than 1 device per user. It is predicted that this trend will continue to increase. [14]

This rapid growth and adoption of the IoT has led to many security issues. But why? Ko et.al (2017) identifies the risks involved with using IoT devices, suggesting that it may be down to the sheer variety of devices. There is a large amount of different wireless technologies as well as a large number of devices using operating systems which have not been secured as well as open-source software. [4]

With this in mind, perhaps one of the primary reasons for security issues in IoT devices is that the rate at which these technologies have been in demand by the consumer across the globe has meant products may not have been securely designed, whilst working with an extremely large number of potential frameworks, technologies and protocols, in different countries. To sum this up,

there is a lack of consistency and guidance which has made it extremely hard for developers to get it 'right'.

Ammar, Russello, and Crispo (2018) explain that the actual process of application development for IoT is extremely challenging. This is due to how complex it is, the lack of guidance available, the amount of programming languages needed and a large amount of communication protocols. Therefore, developers must not only develop the application, but also manage the hardware and software layers of the IoT infrastructure. [1]

Choudhary and Jain (2016) confirm these challenges when writing that there are many challenges associated with the IoT. These challenges include security/privacy, interoperability, reliability, and scalability to name but a few. They suggest that these issues must be addressed by the programmers as well as the providers of the service. [14]

3.1.7 Frameworks

Following on from the challenges identified in the previous section, frameworks have been developed which do indeed provide some sort of structure and combat the aforementioned issues. An IoT framework is defined as guidance and rules, along with protocols and standards which enable the implementation of an IoT application. [1]

There are several very popular frameworks that have been adopted. These are:

- AWS (Amazon Web Services) IoT
- ARM mbed IoT
- Azure IoT Suite
- Bosh IoT
- Brillo/Weave
- Calvin
- Cisco IoT
- Google IoT
- HomeKit
- Kura
- Oracle IoT
- SmartThings [1, 22].

This list is not a definitive list as there are many, many different frameworks out there. Each framework is part of an IoT ecosystem which allows devices within it to communicate with one another and provides several advantages such as the management of devices, protocols, information flow and the analysis of information which has been collected. However, with this, an issue arises, and that is the ability for devices of one framework to communicate with that of another, and whether companies who develop these frameworks will benefit from allowing this functionality. For example, Amazon's AWS IoT. Do they benefit from constraining developers and customers, keeping them within their IoT ecosystem? Perhaps this may be profitable for them. We will not look at these frameworks in any further detail at this point in time, but will review them in the context of the topic of thesis, smart homes, in later sections.

3.1.10 Legislation (United Kingdom specific)

In this section we will briefly look at legislative considerations within the United Kingdom. The reason for this is that Royal Holloway, University of London, and I, are both located in the United Kingdom. At the time of writing this, the U.K. government are proposing new legislation that all manufacturers and suppliers of IoT devices must abide by. This new law will aid in the protection of millions of citizens that use IoT devices within their households. The penalty for not complying to these requirements is a fine of up to 4% of their annual worldwide turnover, or the product being suspended or recalled from the UK market. There are essentially three mandatory requirements which have been drawn up by the Department for Digital, Culture, Media and Sports (DCMS):

- All consumer internet-connected device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of consumer IoT devices must provide a public point of contact so anyone can report a vulnerability and it will be acted on in a timely manner.
- Manufacturers of consumer IoT devices must explicitly state the minimum length of time for which the device will receive security updates at the point of sale, either in store or online.

It is expected that full compliance of all three measures must be met from manufacturers and suppliers/resellers in 2021 and they will be given 9 months

from the date this new legislation is introduced. Bray (2021) informs us that further laws will be introduced by the K government regarding IoT Cyber Security from 2022 onwards. [67, 68]

3.2 Smart Home IoT Devices

The smart home, what is it? To simply describe a smart home, it is a home or place of residence which utilises networked technology to enhance the lives of the inhabitants. This is accomplished through use of smart home or IoT devices such as:

- voice controllers
- indoor/outdoor cameras
- utilities/environment - smart meter, air quality, smoke detector, thermostat, thermometer etc.
- ordering of items (AWS dash button)
- smart controller
- household appliances (cooking and otherwise)
- doorbells
- security systems
- smart electronics – smart TV etc.
- alarm clock
- speaker/entertainment systems
- smart bulbs – smart lighting system
- garage door automation etc.

These objects which may usually be quite unintelligent or mundane in nature with basic functionality, can now communicate with other devices via the global network infrastructure we all know as the Internet, with or without human interaction. This unleashes countless opportunities and advantages for these devices which are now 'smart', including, remote control, analysis of data, updates, added functionality, network connectivity, automatic reactive behaviour based upon collected data from sensors, interaction with the databases and applications and users, the list goes on.

In accordance with my definitions above, Rehman and Gruhn (2018) introduce the concept of a smart home when writing that IoT and Cyber-Physical Systems (CPS) are a new technology which links physical devices across a network automatically. This is done through the use of sensors, physical devices and hardware, software, actuators and the network infrastructure. This allows these devices to be remotely controlled, as they are connected to the Internet. Home appliances that utilize the IoT are one such example of how the IoT has found its way into our homes. [25]

Bassi et al. (2013) suggests that the main purpose of integrating these IoT devices within our households to make 'smart homes' is that they are aware of the goings on within our homes. This impacts three main parts of the home, energy consumption and the use of resources, the security of the home, and finally, the comfort of the inhabitants of the smart home. [45]

Figure 3.5 shows a visual representation of a smart home.



Figure 3.5 Smart Home Side-View [72]

Chang (2019) identifies that the growth in smart home devices is very likely to increase each year at a rate of 16.9%. It is predicted that this will occur it year until 2023. [73]

3.2.1 Devices

A 'typical' smart home consists of a variety of devices, not just the IoT smart devices which we have discussed prior to this section. In this section we will identify what other devices are needed in order for a smart home to operate and function as intended. We will categorise these devices as Ghirardello et al. (2018) has done so in their paper, 'Cyber Security of Smart Homes: Development of a Reference Architecture for Attack Surface Analysis' [55]. These categories are as follows:

IoT Smart Devices – These 'things' are physical objects which are able to collect data from the environment through use of sensors and connect to a network to transfer data and receive commands which will update the operations of said device. Examples include security cameras, appliances such as smart cookers and washing machines, lightbulbs and locks.

IoT Hubs – These are a central controller which connects and manages a variety of different devices. There are two types of IoT hub, homogenous, and, heterogeneous. Homogenous IoT hubs are developed and produced by the same company which produces the IoT devices, thus creating an IoT ecosystem. These hubs are needed for the IoT devices to operate correctly. Heterogeneous IoT hubs on the other hand, connect a variety of devices, allowing them to transmit data with one another. An associated application is often required with this type of hub which allows the consumer to control all connected technologies from one, singular point of contact.

Residential Gateway – This is the equipment that is located within the user's home which provides a connection from the IoT devices to the Internet.

Smartphones/Tablets/Computers – These devices are different to the IoT devices mentioned above. Why? Their main function is not to extend the functionality of a physical object, but instead, their functions are computing related. However, they may very well still be required within the context of a smart home to control and manage IoT smart devices. Furthermore, smartphones have built in sensors which include microphones and accelerometers so may provide further assistance within the smart home. [55]

3.2.2 Technologies, standards and frameworks - how Smart Home IoT devices work

In this section we will look at the technologies that are often implemented within a smart home. Not to repeat oneself, but we recall a layered IoT architecture which has been discussed previously. The figure

below shows not only the layers, but also the technologies and purpose of each layer. This is comparable to Table 3.4 devised by Mrabet et al. (2020).

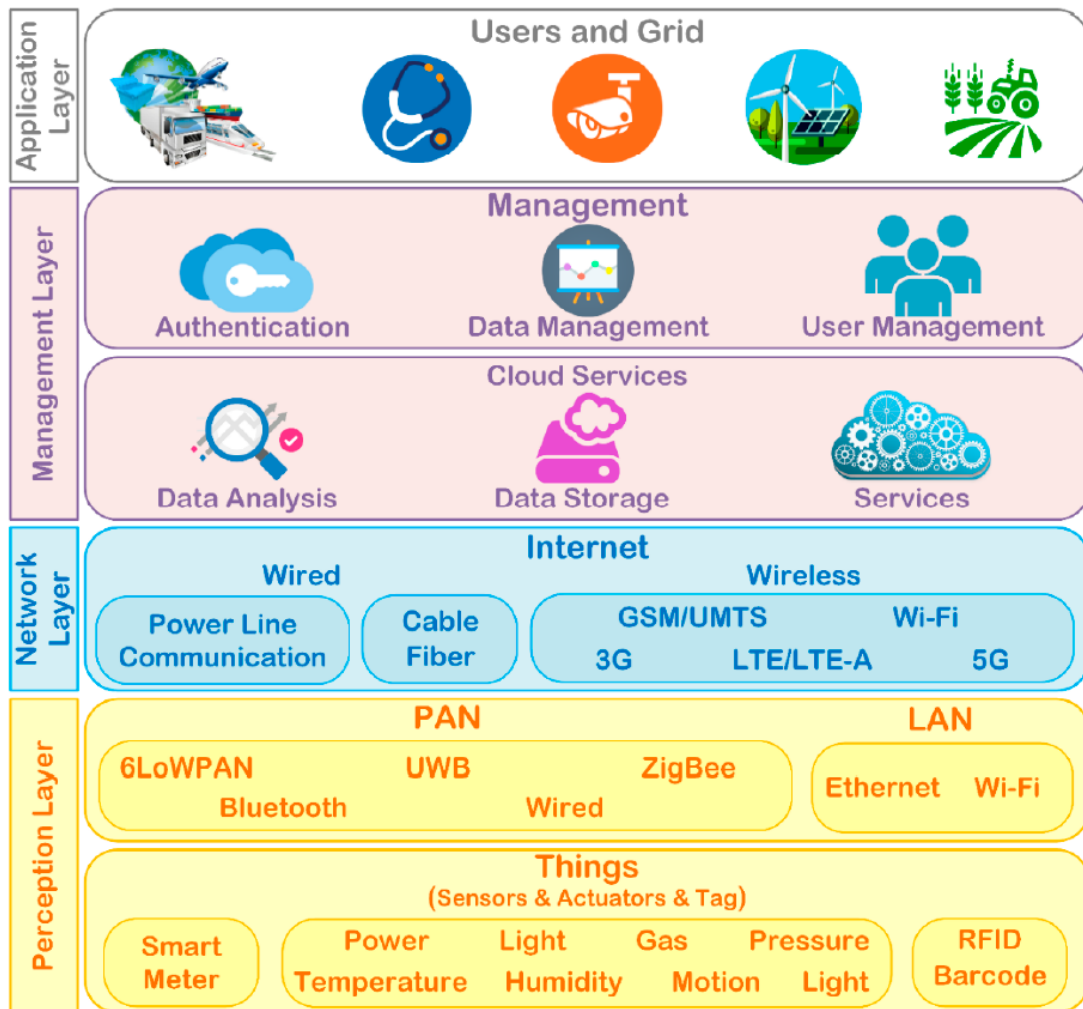


Figure 3.6 Layers and several applications of IoT for smart environments [75]

However, let us now look specifically at a proposed IoT architecture for the smart home. This will allow us to analyse the technologies we find commonly within this environment.

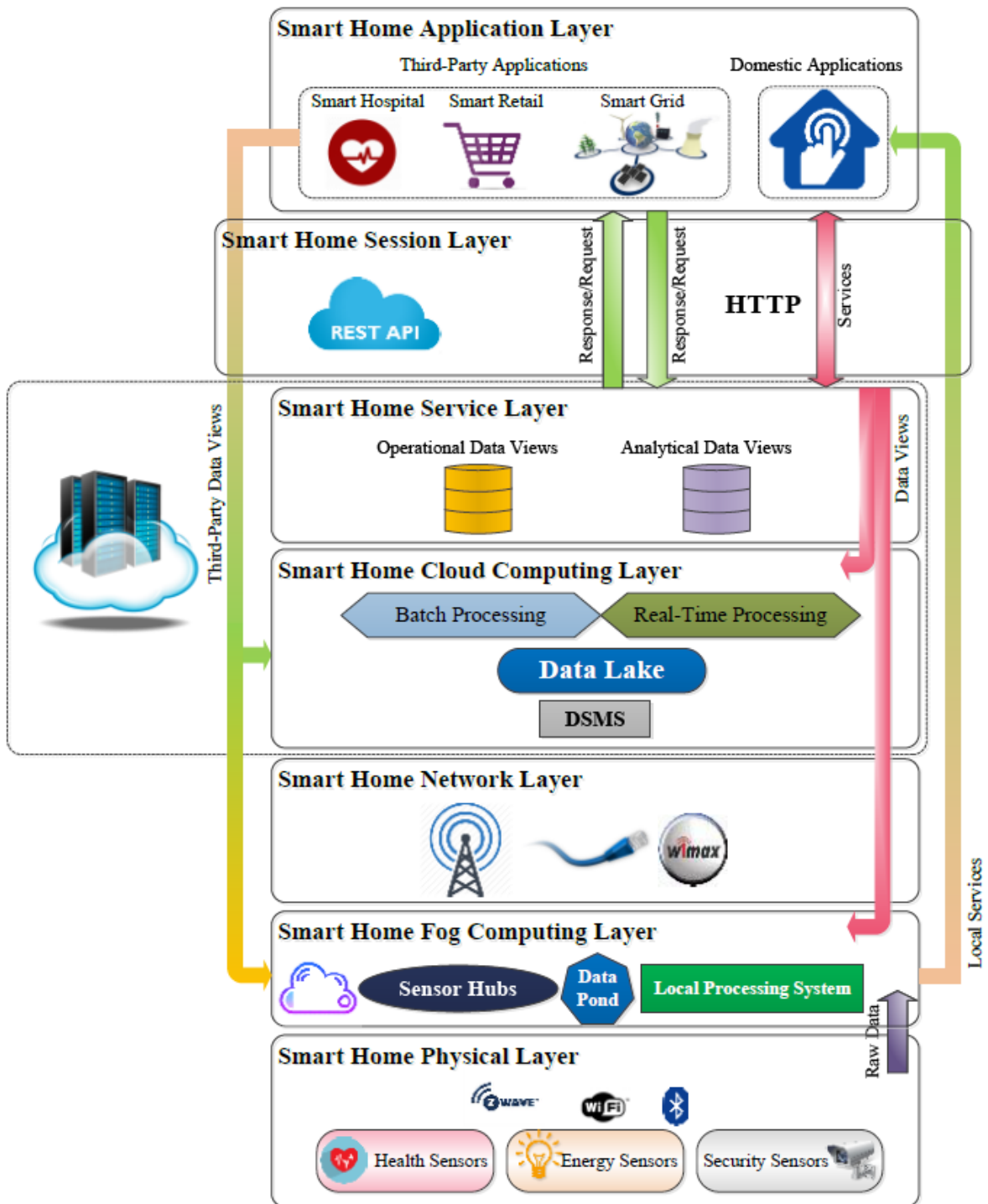


Figure 3.7 REST-based 7 Layer Architecture for Smart Homes [76]

Mokhtari et al. (2019) propose a 7-layered architecture specifically for smart homes consisting of the following layers, at the bottom is the physical

layer, above this is the fog-computing layer, then network, cloud-computing, service, and session layers, with the application layer sitting at the top. These can map across to the 3-layer model of application, network and physical/perception. However, we will use this 7-layered architecture as it is specifically designed as a solution for smart homes.

We will now identify the purpose of each layer according to Mokhtari et al. (2019). Note, we may assume that data passes between the layers in order. I mention this, so I can keep this concise and not add to the explanation of each layer about them transmitting it to the adjacent layer/layers.

- **Physical layer:** Data is collected on this layer through use of sensors.
- **Fog-computing layer:** Data storage and processing.
- **Network:** The sensor or a device sends its data to the cloud-computing layer and the data are transformed to a specific common format that are understood by all devices and application
- **Cloud-computing layer:** Scalable solution for data processing and storage. Required for extensive computing which cannot be implemented at the edge in the fog-computing layer.
- **Service layer:** The processed data from the cloud-computing layer will be provided as data-driven services to different smart home and third-party applications in this layer.
- **Session layer:** management of sessions
- **Application layer:** the applications will utilize the session layer and RESTFUL APIs to use the data-driven services of the smart home.

The above smart home architecture may provide an environment which is universal and allows all manner of IoT device to communicate and operate as intended. [76]

Before we examine the technologies at each layer, let us quickly identify the components which an IoT device within a home network typically comprises of. These components include:

- ‘Microcontroller Units (MCUs). These are essentially extremely small

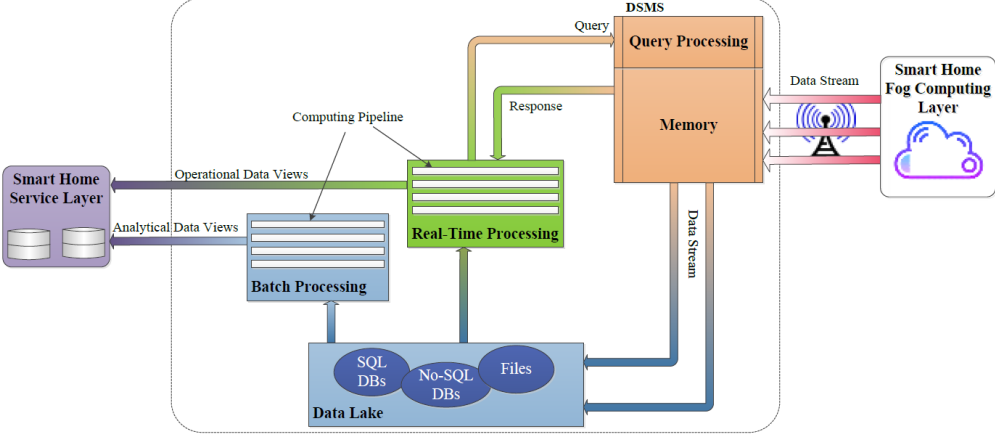
computers within a single microchip.

- Dedicated modules. These are developed for a particular purpose such as Wi-Fi communications, and are a hardware component.
- Systems-on-a-Chip (SoCs). This is a single chip which consists of a microprocessor which works alongside a variety of different integrate peripherals.
- Original Equipment Manufacturer (OEM) boards. This is a system board which may be used with products which have been developed by a different manufacturer. [31]

Understanding and identifying the technologies implemented at each layer of this architecture is extremely important in the context of this paper. Why? It will allow us to identify potential security vulnerabilities and therefore, recognize threats. This is the first stage in developing our attack map. Once this is completed, we may understand how an attacker may link together various attacks and threats, leading to a fully developed attack model for smart homes.

Without further ado, below are details and associated explanations of the technologies which may be implemented at each layer. We will omit the purpose of each layer from this discussion as it has previously been discussed.

Layer	Technologies
Physical / Perception	<p>Sensors and devices.</p> <p>Smart home energy: This is managed by the smart home Energy Management System (EMS) which senses and monitors the status of an energy device. These sensors include smart appliances (washing machines etc.), comfort system (smart lighting, temperature etc.), local energy generation (environmental data such as weather data), electric vehicles which may charge and discharge their power as part of the home energy management plan, and finally, energy meters which measure and monitor the electricity consumed within the home.</p> <p>Smart home security and safety: Fire sensors and access sensors.</p> <p>Smart home health: Health sensors may make use of the smart home and wireless sensor network (WSN) platform. Sensors to detect Activities of Daily Living (ADLs) – environmental and wearable sensors. And secondly, sensors which are part of the smart home health monitoring system which again include environmental and wearable sensors.</p>

	<p>Perception layer technologies include: Things: Sensors and actuators and tags include. For example: Smart meter, RFID, barcode, QRcodes, WSN, WBAN, and sensors for power, temperature, light, humidity, gas, motion, pressure and light.</p> <p>PAN: 6LoWPan, Bluetooth, UWB, Wired, ZigBee, Z-Wave, BLE, NFC</p> <p>LAN: Ethernet, Wi-Fi [12, 22, 75, 76]</p>
Fog-computing layer	<p>Sensor hubs which does simple data processing which occurs at the edge, such as data concentration and scheme mapping to the sensor data. It is close to the end devices to minimize latency and reduces data traffic to the cloud as it processes tasks which do not need cloud capabilities.</p> <p>Local processing system which provides local data processing tasks and services to smart home applications.</p>
Network	<p>Smart home gateway, communication protocols such as: Ethernet, cellular and WIMAX that are used to transfer the data to the cloud computing layer. Long Range (LORA) which can send sensor data directly to the cloud computing layer.</p> <p>Network layer technologies include: Wired: power line communication, cable fiber. Wireless: WiMAX, LoRA, GSM/UMTS, 3G, LTE/LTE-A, Wi-Fi, 5G [12, 22, 75, 76]</p>
Cloud-computing layer	 <p>Figure 3.8 Cloud Computing Layer for Smart Homes [76]</p> <p>Data Stream Management System (DSMS) – deals with continuous data and online analysis in real-time. It ingests the streamed data and performs real-time queries. An example of a simple SQL query might be: <i>SELECT * INTO output FROM streamedData</i></p> <p>Can store data to the Data Lake. In the smart home we may have hundreds of sensors which generate streamed data events which include payload data in JSON format. For example:</p> <pre>{ "timestamp": "20190127124357", "dsp": "tempsensor",</pre>

	<pre> "temp": "28" } </pre> <p>This data event is pushed to the cloud-computing layer by the sensor hub.</p> <p>Data Lake – Data is required to have specific, pre-defined schema. Central data storage deals with this issue by storing data in any format, and then add the schema to the raw data when it is required for data processing. This allows data to be stored in any format as it has SQL, No-SQL databases, as well as files.</p> <p>Real-time processing system (pipeline) – processes the main data. Provides capability of data processing for real-time applications such as the scheduling of appliances, management of smart home energy, as well as the detection of anomalies for example. Data views, DSMS, data lake are input and processed through the computing modules to output the operational data view in the service layer.</p> <p>Batch processing system (pipeline) – analyses complex behavioral sets of large quantities of data. For example, processes which require historical data. Data lake is processed through computing modules and then outputted the analytical data view in the service layer. No real-time data processing is needed for this.</p>
Service layer	<p>Data views are used at this layer. Processing the whole or even part of a smart home dataset with a specific query function is difficult and requires a lot of processing time. It is for this reason is that Mokhtari et al. (2019) proposed data views due to access speeds when queried. All data-driven services from the computing layer are available at the service layer through the smart home data view, which is specifically, standardized formatted metadata. There are three main types of data view, operational data views, analytical data views, and third-party data views (which have previously been discussed). Having a standardized data format provides a shared data environment. The views may exist however in different formats such as XML, JSON etc. For example, XML format for a device may be formatted as:</p> <pre> <?XML version="1.0" encoding="UTF-8"?> <DeviceView> <HomeID>5</HomeID> <HubID>1</HubID> <DeviceID>30</DeviceID> <Value>15</Value> </DeviceView> </pre> <p>Further attributes may be added, however, these attributes for each type of device within the smart home should be standardized.</p>
Session layer	<p>Provides a means for the transmission of data between the service and application layers through the use of APIs. Due to the fact that energy is limited, a continuous connection between these two layers is not possible, so Mokhtari et al. (2019) propose a REST-based architecture which uses RESTFUL APIs and URL-based communication. RESTFUL methods are all based on the hypertext transfer protocol (HTTP). This REST-based system identifies resources by a hierarchical structured uniform resource locator (URL) e.g. a collection of hubs may be /hubs, whereas, a specific device under a specific hub may have the URL</p>

	<p>/hubs/{hubid}/devices/{deviceid}. HTTP methods are used for CRUD (Create (CREATE), Read (GET), Update (PUT) and Delete (DELETE)) a resource in the server. As such, all resources should be designed with the REST architecture.</p> <p>The process: A client (application) sends a request (HTTP method) to the server (service layer), 'the session layer parses the resource information' and if it is an authenticated session, it will 'find the resource (view), encapsulate' it and then provide it to the application.</p>
Application layer	<p>There are two main classes of applications within this layer, domestic applications (device control, EMS etc.), and third-party applications (capabilities to exchange data-driven services with third-party applications from the smart city, including the smart grid, smart hospital, smart retail etc. This layer includes applications which are subscribed to use or exchange data-driven services within the smart home.</p>

Table 3.5 Smart Home Technologies [12, 22, 75, 76]

As can be seen in the above architecture and identification of IoT technologies, protocols and layers are different to that of the TCP/IP protocol stack. This is primarily due to the fact that IoT devices are low power and require battery charge for months or years at a time without any recharge. Therefore, the IoT protocols and standards which must allow for such a wide variety of different devices and technologies do not have the same level of security as the widely established TCP/IP protocol suite. [19]

This leads us onto the next section which is identifying the attacks, threats and vulnerabilities that are possible in a smart home network.

3.2.3 Attacks, Threats and Vulnerabilities of a Smart Home network

Both Andrea, Chrysostomou and Hadjichristofi (2015) [19] and Deogirikar and Vidhate (2017) [20] state that although there is considerable research conducted in a variety of fields with regards to security challenges and security mechanisms, at this point in time, research which has been conducted with regards to the IoT has not addressed the security challenges in a detailed manner [19]. Instead, the majority of IoT security related research is specific and authors have only looked at very precise elements and technologies which are used in the IoT such as the threats and potential attacks which may be carried out on RFID systems. Other researchers have explored the security issues which arise when connecting the IoT to cloud

computing, or even jamming attacks specific to Wireless Sensor Networks for example. Andrea, Chrysostomou and Hadjichristofi (2015) and Deogirikar and Vidhate (2017) attempt to address different IoT attacks which we will examine and then apply to the context of the smart home. This will allow us to then map different attacks together.

Andrea, Chrysostomou and Hadjichristofi (2015) created a table which classifies IoT attacks into four categories: physical attacks, network attacks, software attacks, and encryption attacks. Deogirikar and Vidhate (2017) refer to the same table in their research paper, 'Security Attacks in IoT: A Survey'. Below, we can see the table as developed by Chrysostomou and Hadjichristofi (2015). It is important to note that these attacks are generalized to the entire IoT landscape and not just to smart homes, therefore specific attacks such as the Sybil Attack is not applicable to this project. [19, 20]

Physical Attacks	Network Attacks	Software Attacks	Encryption Attacks
Node Tampering	Traffic Analysis Attacks	Virus and Worms	Side Chanel Attacks
RF Interference	RFID Spoofing		Cryptanalysis Attacks: a) Ciphertext Only Attack b) Known Plaintext Attack c) Chosen Plaintext or Ciphertext Attack
Node Jamming	RFID Cloning	Spyware and Adware	
Malicious Node Injection	RFID Unauthorised Access	Trojan Horse	
Physical Damage	Sinkhole Attack		
Social Engineering	Man In the Middle Attack	Malicious scripts	
Sleep Deprivation Attack	Denial of Service		
	Routing Information Attacks		Denial of Service
Malicious Code Injection on the Node	Sybil Attack	Man In the Middle Attack	

Table 3.6 Classification of IoT Attacks [19]

Chang (2021) identifies with specifics, the attacks that may occur within a smart home on a typical IoT device in the research paper, 'IoT Device Security - Locking Out Risks and Threats to Smart Homes'. These attacks are categorized by the attack layers, hardware, firmware, OS (operating systems and applications), web interface, protocol, and policy. Within each layer, security issues and threats are identified.

Attack layer	Security issues	Risks
Hardware	<ul style="list-style-type: none"> › Ease in being dismantled and further examined › Existing debug port 	<ul style="list-style-type: none"> › Hackers can connect to the JTAG UART, I2C, and SPI of the system without any security limitations.
Firmware	<ul style="list-style-type: none"> › Credential issues › Backdoor issues › Unpatched firmware › Buffer overflow issues › Privilege escalation 	<ul style="list-style-type: none"> › Hackers can use the default and hard-coded passwords in the firmware. › Hackers can easily predict these passwords and access the system easily.
Operating system and application	<ul style="list-style-type: none"> › Unpatched operating system › Buffer overflow issues › Privilege escalation › Possibility of man-in-the-middle (MitM) attacks 	<ul style="list-style-type: none"> › Buffer overflow (stack, heap, and integer) can allow hackers to gain privilege or control over the system.
Web interface	<ul style="list-style-type: none"> › SQL injection › Directory traversal › Buffer overflow issues › Cross-site scripting (XSS) › Cross-site request forgery (CSRF) › Use of default or sample pages › Privilege escalation issues › Other OWASP issues 	<ul style="list-style-type: none"> › Hackers can gain access to the system without the need for a password. › Hackers can get information that the web interface should not provide (e.g., internal IP address, system structure, directory name, and database configuration).
Protocol	<ul style="list-style-type: none"> › DoS or DDoS › Session hijacking › Authentication bypass › Media access control (MAC) spoofing attacks › PIN cracking attacks › MitM attacks › Hard-coded key attacks › Replay attacks 	<ul style="list-style-type: none"> › Hackers can disable the device function by flooding the connection bandwidth. › Hackers can initiate hijacking sessions to send forged data. › Hackers can steal data or credentials through MitM attacks. › Hackers can replay stolen data to bypass authentication.
Policy	<ul style="list-style-type: none"> › Misconfigured policies › Policy violations 	<ul style="list-style-type: none"> › Hackers can leak sensitive data, such as credentials, connection strings, IP addresses, and internal network topology. › Hackers can gain unlimited access to the system. › Unknown exposure outside the network through settings like enabled UPnP in devices.²

Table 3.7 Smart Home IoT Attack Layers [73]

As can be seen in Table 3.6 and Table 3.7, there are many attacks which have been repeated within both tables. Further to this, OWASP Foundation, Inc. (2018) released their top 10 things to avoid when building, deploying and managing IoT systems which could lead to security violations. These are:

1. Weak, Guessable, or Hardcoded Passwords - Use of easily

bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2. Insecure Network Services - Unneeded or insecure network services running on the device itself, especially those exposed to the internet that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.
3. Insecure Ecosystem Interfaces - Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
4. Lack of Secure Update Mechanism - Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
5. Use of Insecure or Outdated Components - Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
6. Insufficient Privacy Protection - User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
7. Insecure Data Transfer and Storage - Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8. Lack of Device Management - Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9. Insecure Default Settings - Devices or systems shipped with insecure default settings or lack the ability to make the system

more secure by restricting operators from modifying configurations.

10. Lack of Physical Hardening - Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device. [79]

UL LLC (2020) attempts to determine the IoT devices within a smart home which need the most protection in the below diagram. UL LLC propose this order based solely upon the Internet connectivity of the device. For example, they suggest that devices that are directly accessible from the Internet such as cameras, baby or pet monitors, routers, modems and Internet exposed hubs need the most security assurance. This is because they are exposed and may be accessed via the Internet. The Internet being a global infrastructure which therefore results in attackers being able to attack the device from any location on this planet. This is in contrast to other devices which may only be accessible once an attacker has access to the LAN (Local Area Network). [80]

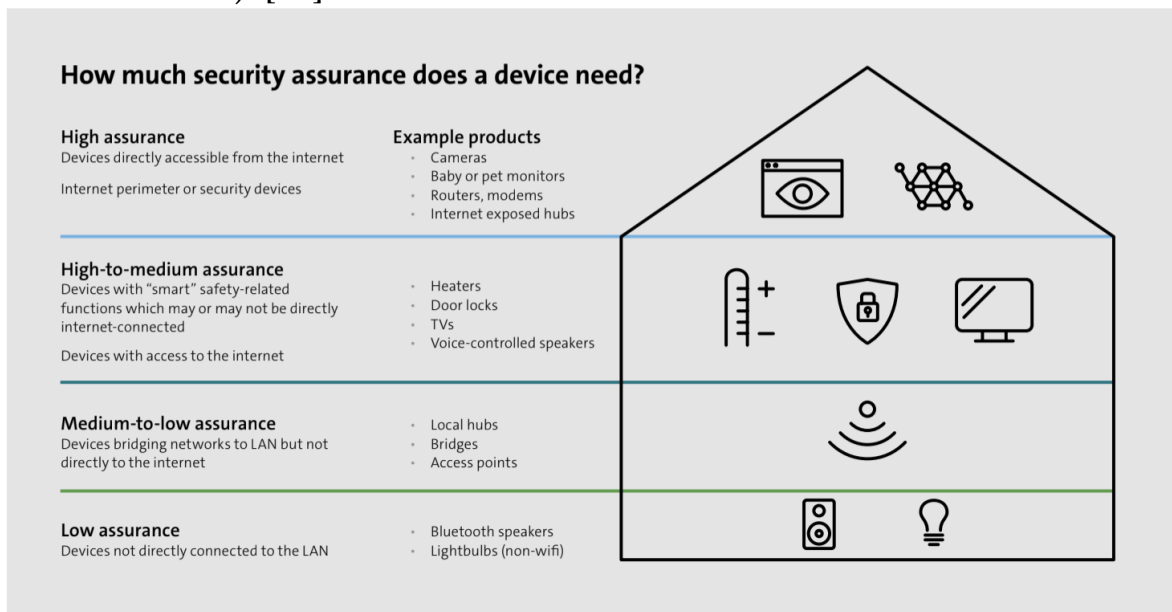


Figure 3.9 Security Assurance of Smart Home Devices [80]

Let us now look at a few specific attacks on IoT devices that may occur in a smart home and how they link with one another as examples. These attacks may be carried out for all manner of reasons depending on the type

of attacker and their purpose. If they are government funded, opposing businesses or a hacktivist, they may be hijacking devices to gather intelligence, or leverage systems to gain credentials to carry out further attacks such as ransomware or denial of service. Other attackers may be malicious partners, taking control of IoT devices as part of Cyber Stalking, which could then lead to other crimes such as manslaughter. For example, an attack may monitor the behaviours and routines via the CCTV IoT device, manage the climate control to make the victim feel uncomfortable or hot, burn or spoil food if they have smart cookers and refrigerators, or even lock the victim, disabling CCTV and starting a fire to cause physical harm to the victim. Other attackers may not be quite so malicious and may just be curious script kiddies who are attacking the system due to the challenge.

Essentially, all the positive purposes IoT devices are created for such as security, energy consumption, entertainment, stock control or home appliances for comfort, can be disrupted and have the complete opposite effect, a negative impact, causing physical and emotional discomfort, security and leaking of confidential information, denial of service, overuse of energy, expenditure of finance/financial control, and an attack on the physical security and well-being on the victim.

We will now use this information in conjunction with the MITRE ATT&CK® Navigator and the layer templates for Mobile and Enterprise layers, as a foundation to categorise different techniques which an attacker might use on a smart home network [78].

MITRE ATT&CK® is a knowledge base which suggests the Adversarial Tactics, Techniques, and Common Knowledge an attacker may use from his/her perspective for three domains: Enterprise, Mobile, and ICS. It has been developed by the MITRE Corporation who are a United States non-profit research institute, commonly known for managing the famous CVE (Common Vulnerabilities and Exposures) database.

MITRE ATT&CK® was developed with the following three concepts in mind:

1. Designed from the adversary's perspective.
2. Use of real-world examples, utilizing empirical data.

3. An appropriate level of abstraction is used to cover such a vast threat landscape, allowing connections to be made between offensive and defensive actions. [77]

It is important to note that it has been developed with a high level of abstraction. Why? It cannot contain such intricate information such as IP addresses or even information related to specific malware such as signatures, otherwise the scope of the project would be too vast, become unmanageable and grow exponentially as more and more IoT devices are developed and deployed. Furthermore, it would quickly become out of date and therefore unusable.

With the above said, it is especially important that this project too, has a level of high abstraction, so that it is not just a snapshot of a time in history, but instead, something which can be referred to for at least a few years. Therefore, information will be organized with a high degree of abstraction when developing and categorizing the attacks an attacker might use on a smart home network based upon the MITRE ATT&CK® Navigator, but also when developing the solution of this project, the attack map. This leads us to the application of the MITRE ATT&CK Navigator on Smart Home IoT devices, which can be seen below. This has been developed with similar headings from the domains, Enterprise, Mobile and ICS (Industrial Control Systems). Obviously specific attacks and headings may have been removed as they are not applicable to smart homes. For example, Sybil attacks have been removed as it is unlikely that a smart home will have more than 20-30 sensors. So yes, a Sybil attack is appropriate for a factory and ICS as it will have more M2M interactions, but this is not so for a smart home.

The reason IoT cannot fit into one specific domain is that the IoT architecture fits somewhere between them. Smart homes are now being used for enterprise services with technologies such as AWS and cloud services being used, and actual IoT devices may be built using operating systems which may be specifically designed for IoT devices, but may also be stripped down versions of mobile operating systems such as Google's 'Android Things'. Google has now stated that this IoT project will be stopped by January 2021. It is an embedded operating system which runs IoT devices on low battery to communicate with other devices using BLE and Wi-Fi using

the operating system which makes use of the protocol Weave. [81]

From the MITRE ATT&CK® Navigator Matrices [83] for the three different domains we can see the operating systems and types of device in the filters for each domain are: Linux, macOS, Windows, Office 365, Azure AD, AWS, GCP, Azure, SaaS, PRE, Network, Field Controller/RTU/PLC/IED, Safety Instrumented System/Protection Relay, Control Server, Input/Output Server, Windows, Human-Machine Interface, Engineering Workstation, Data Historian, Android, and iOS. This is in comparison to the operating systems often associated with IoT devices such as: Nucleus RTOS, Amazon FreeRTOS, TinyOS, Windows 10 IoT, Tizen, Wind River VxWorks, Apache Mynewt, Contiki, Android Things, balena OS, Micrium uC/OS, Nano-RK, Particle Device OS, RIOT OS, Siemens MindSphere, Ubuntu Core, Zephyr RTOS etc. It is important to note that RTOS stands for real-time operating system [82]. As can be seen, the number of operating systems for individual IoT devices, along with different technologies at each layer of the IoT architecture means that heterogenous smart home systems lead to complex interoperability, and therefore, it is important we analyse this from a high level.

Interestingly, Ikarus Software Security (2019) suggest that the IoT is largely incorporated in ICS. However, for this project, we are focusing on IoT within the smart home and therefore will not use the ICS layer solely from MITRE ATT&CK® navigator [83].

<u>Reconnaissance</u> (if targeting a specific individual, organisation or device - OSINT)	<u>Resource Development</u>	<u>Initial Access</u>	<u>Execution</u>	<u>Persistence</u>	<u>Privilege Escalation</u>	<u>Defense Evasion</u>	<u>Credential Access</u>	<u>Discovery</u>	<u>Lateral Movement</u>	<u>Collection</u>	<u>Command & Control</u>	<u>Exfiltration</u>	<u>Impact</u>
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Execution through IoT API	IoT API Hooking	Code Injection	Exploitation for Evasion	Brute Force	Control Device Identification	Attack PC via USB/wireless Connection from IoT device	Archive Collected Data	Commonly Used Port	Exfiltration Over Physical Medium	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Scheduled Task/Job	Account Manipulation	Exploit IoT OS Vulnerability	Indicator Removal on Host	Credentials from Password Stores	I/O Module Discovery	Exploitation of Enterprise Services	Audio Capture	Connection Proxy/ Proxy	Exfiltration Over Web Service	Data Destruction
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Inter-Process Communication	Valid Accounts	Exploit Trusted Execution Environment	Rootkit	Exploitation for Credential Access	Network Connection Enumeration	Exploitation of Remote Services	Automated Collection	Standard Application Layer Protocol	Exfiltration Over Other Network Medium	Data Encrypted for Impact
Gather Victim Organisation Information	Develop Capabilities	Phishing	User Execution	Broadcast Receivers	Boot or Logon Scripts	Rogue Master Device	Man In The Middle	Network Service Scanning	Internal Spearphishing	Data from Cloud Storage Object	Uncommonly Used Port	Automated Exfiltration	Data Manipulation
Phishing for Information	Establish Accounts	Supply Chain Compromise	Software Deployment Tools	Code Injection	Scheduled Task/Job	Masquerading	Modify Authentication Process	Network Sniffing	Lateral Tool Transfer	Data from Configuration Repositories	Web Service	Scheduled Transfer	Defacement/ Adware
Search Closed Sources	Obtain Capabilities	Trusted Relationship	Command & Scripting Interpreter	Compromise IoT Application Executable on mobile	Valid Accounts	Code Injection	Network Sniffing / Traffic Analysis Attacks	Remote System Discovery	Remote Service Session Hijacking	Data from Local System	Remote File Copy	Transfer Data to Cloud Account	Disk Wipe/ Delete Device Data
Search Open Technical Databases		Valid Accounts	Exploitation for Client Execution	Modify partition		Geofencing	IoT OS Credential Dumping	Serial Connection Enumeration	Software Deployment Tools	Data from Network Shared Drive	Alternate Network Mediums	Exfiltration Over Alternative Protocol	Endpoint Denial of Service / DOS
Search Open Websites/ Domains		Hardware Additions	Native Code	Prevent removal of malicious account		Modify Partition	Steal Web Session Cookie	Application Discovery	Taint Shared Content	Data from Removable Media	Standard Cryptographic Protocol	Commonly Used Port	Firmware Corruption
Search Victim-Owned Websites		Internet Accessible Device	Broadcast Receivers	System firmware		Device lockout	2FA Interception	Evade Analysis Environment	Use Alternate Authentication Material	Email Collection	Communication Through Removable Media	Data Encrypted	Inhibit System Recovery
Social Engineering (Specific attacks listed above)		Wireless Compromise	Man in the Middle / Man In The Middle	Project File Infection		Application Discovery	Unsecured Credentials	File and Directory Discovery	Default Credentials	Input Capture	Remote Access Software	Standard Application Layer	Network Denial of Service / DOS
		Replication through Removable Media	Scripting	Boot or logon scripts		Delete Device Data	Access Sensitive Data in Device Logs	Location Tracking	External Remote Services	Man In The Middle	Protocol Tunneling		Resource Hijacking
		Spearphishing Attachment	Command-Line Interface			Evade Analysis Environment	Access Stored Application Data	Process Discovery	Remote File Copy	Video/Camera Capture	Encrypted Channel		Service Stop
		Deliver Malicious App to	Project File Infection			Modify Trusted Execution	Capture SMS Messages	System Information	Valid Accounts	Screen Capture	Dynamic Resolution		System Shutdown/Reb

		Mobile Phone which manages IoT device via Authorized App Store/ or other means				Environment		Discovery					oot
		Exploit via Charging Station or PC				Native Code	Exploit TEE Vulnerability	System Network Configuration Discovery	Sinkhole Attack	Capture Clipboard Data	Data Encoding		Clipboard Modification
		Exploit via Radio Interfaces / RF Interference / RFID Spoofing / RFID Cloning / RFID Unauthorised Access				Obfuscated Files or Information	Input Capture	System Network Connections Discovery	Selective Forwarding Attack – from Sinkhole Attack	Location Tracking	Data Obfuscation		Device Lockout
		Install Insecure or Malicious Configuration for IoT device / Malicious Node Injection				Uninstall Malicious Application	Keychain	Account Discovery	Acknowledge Spoofing Attack – from Sinkhole Attack	Network Information Discovery	Multi Stage Channels		Input Injection
		Authorization bypass				File/Directory Permission Modification	Network Traffic Capture or Redirection	Cloud Infrastructure Discovery		Network Traffic Capture or Redirection			Damage to Property
		Masquerade attack				Masquerading	URI Hijacking	Cloud Service Dashboard		Access Stored Application Data			Denial of Control
		Node Tampering				Modify Authentication Process	Spyware	Cloud Service Discovery		Access Notifications			Denial of View
		Node Jamming				Valid Accounts		Network Share Discovery		Access Sensitive Data and Device Logs			Loss of Availability
		Physical Damage				Unused/Unsupported Cloud Regions		Password Policy Discovery		Access Calendar Entries			Loss of Control
		Sleep Deprivation Attack				Process Injection		Peripheral Device Discovery		Foreground Persistence			Manipulation of Control
		Malicious Scripts/ Virus & Worms				Impair Defenses		Remote System Discovery		Spyware			Manipulation of View
		Side Channel Attack				Hide Artifacts, deobfuscate/decode files or information							Theft of Operational Information
		Cryptanalysis Attacks (Ciphertext Only, Known Plaintext, Chosen Plaintext or Ciphertext)											

Table 3.8 Tactics & Techniques Matrices for Smart Home Domain

Table 3.8 includes 2 categories of tactics and techniques which cover the preparatory techniques an attacker may use before engaging in the attack phase. These are reconnaissance and resource development. It is important to note that most tactics and techniques have been taken from the three domains as listed by MITRE, however, also include physical, network, software, and encryption attacks from Chrysostomou and Hadjichristofi (2015) which are emphasized with bold text and light blue background cell formatting. [83, 19]

As can be seen from the above table I have created based upon the different domains identified by MITRE, the attack surface for IoT is extremely large and due to the way in which it is implemented, there are more technologies and tools which can be used to attack than the other three domains. This is partly because it is not just the device or the physical layer that is vulnerable, but also other layers within the IoT architecture.

In this next section we will now look at a couple of these attacks which are particularly common in smart homes in more detail, explaining how an attacker may carry out such an attack, then leverage it to laterally move across a home network to compromise further devices, collect further information and commit subsequent attacks. We will focus on attacks which utilize specific and common technologies within smart home IoT devices such as sensors, nodes, RFID etc. rather than more commonplace attacks which may be used to gain access to a network such as viruses and social engineering. However, these will obviously be included within the Attack Map.

Smart Home Attack Surfaces

Let us further explore the attack surfaces that may be used by an attacker when compromising a smart home as identified by Ferrari (2019).

Stored Credentials – Devices may store sensitive information that an attacker can access. For example, data may be stored in the hub before it is transmitted to the server. Data may be stored in a various ways, whether it is volatile such as RAM (Random Access Memory), non-volatile such as ROM (Read Only Memory), EPROM (Erasable Programmable Read Only Memory), it does not matter, as an attacker may gain access to these

credentials. This also leads onto another area with unencrypted local data storage. If this data is not encrypted, it is in plaintext and therefore readable to the attacker, which compromises the security goals of confidentiality and integrity.

Access Control – Controls need to be in place to prevent attackers from accessing the system.

Firmware Extraction – Firmware extraction and firmware extraction can be carried out by an attacker if they have physical access to the device. This allows the attacker to identify vulnerabilities in the system which may be exploited.

Firmware Attacks – The firmware can be changed or even replaced by the attacker when there are no security controls or validation in place. This could lead to another area which is Malicious Updates.

Malicious Updates – This can allow the attacker to update the device at will. This is potentially very dangerous as it could be updated with malicious updates that prevent legitimate updates or security vulnerabilities from being patched, or even, it could be updated to have backdoors. The update is redirected and updated from a malicious source rather than the legitimate source.

Privilege Escalation – When gaining access as a standard user, an attacker may be able to find a way to escalate their privileges to become a root user or administrator, or at least run commands as a root user.

Misconfigurations or Resetting the Device to an insecure state – this may be done accidentally by the user or perhaps by a maintenance engineer. However, it may also be done purposefully by an attacker, for example, disabling 2FA (Two-Factor Authentication). Glitch attacks and specific command sequences may be used to reset the device to an insecure state.

Web Attacks – If the IoT device uses a web application in part of its framework, then web attacks may be common. This means the OWASP Top 10 may be applied to this situation as well.

Network Services – Attacks may be against services running on the network such as FTP, SSH, SNMP, Telnet etc. can allow an attacker to remotely connect, access and tamper with files, and take control of the vulnerable IoT device.

Cloud Computing – If the IoT device makes use of a cloud service, a vulnerable cloud application may be exploited by an attacker.

Insecure APIs – API traffic may not be encrypted, and if this is connected to the Internet, this is particularly concerning as an attacker will be able to see all processes taking place on the victim's device.

Mobile Applications – Even if the hardware and device is secure, a vulnerability in the mobile application may be exploited. It only takes one weakness in the entire system for an attacker to gain an initial foothold. [85]

Common IoT Attacks as identified by Ferrari (2019)

DDoS Attack – A Distributed Denial of Service attack can target IoT devices, gateways, as well as application and cloud servers. A network of compromised devices also known as bots or zombies make up a botnet. The bot master will then send commands to each of the bots which are distributed. These bots will then send many requests and flood the IoT device, gateway or application and cloud servers with packets. Whilst these requests are attempting to be processed, it prevents legitimate users and processes from running, compromising the security goal, availability. Hence the name, 'Denial of Service'.

Radio Attack – An example of a radio attack is the Rolling Code Attack – Rolling code is often found in doors which are within the smart home such as car doors or garage doors. The way these systems work is that the user triggers a command by selecting a button on a remote. This then generate a random code which may not be predicted. However, an attacker may intercept this signal and also jam it. This results in the receiver not ever getting the code. Furthermore, the attacker may use this intercepted code to unlock the garage door giving them physical access to the smart house, or

physical access to the car. Radio attacks may be carried out using tools such as HackRF One.

Jamming Attack – This type of attack jams a signal (Wi-Fi, GPS etc.) and therefore prevents two devices from communicating with one another. This type of attack is both cheap and easy to carry out.

BlueBorne Attack – This type of attack exploits IoT devices which utilize Bluetooth wireless communications technology. This type of attack results in the attacker gaining unauthorized access to the vulnerable IoT device. It is important to note that the attacker need not be paired or in discoverable mode to execute such an attack.

Backdoor – This provides the attacker with persistence and makes it possible for an attacker to gain remote access to the vulnerable IoT device.

Other attacks that are common to smart home IoT devices may be eavesdropping, man-in-the-middle attacks, forged malicious devices, side-channel attacks and ransomware attacks to name but a few. [85]

Cross-Contamination – When there are multiple components working alongside one another as part of an IoT infrastructure, if one is vulnerable it may impact and affect another device or component. For example, if the router is tampered with, then this will affect the IoT hub. Or perhaps if a ransomware attack is carried out on a specific component, this will impact other devices and services on the network. Now, cross-contamination is a big issue as it shows how one flaw, weakness, or vulnerability in the entire IoT framework can lead to further attacks that may impact the smart home in worse ways.

3.2.4 – Case Studies / Scenarios

From the matrices I created in the previous section, it is clear to see what a vast attack surface we are dealing with when it comes to IoT devices within the smart home. In this section we will take a look at actual events where an attacker has gained initial access and exploited a vulnerability

within the smart home to laterally move across the LAN and gain further information and compromise the network further.

Pentest Partners (2021) found that they were able to hack into a home network and car by exploiting a deauthentication bug in Google Chromecast which was first discovered in 2014, which then allowed them to get the TV running the Chromecast to talk to and hack Amazon Alexa. They firstly identified the vulnerable smart home by using an online Wardriving database (https://wagle.net/search?ssidlike=Chromecast___) which detailed that the home network was using Google Chromecast. Wardriving is when an attacker locates a Wi-Fi network that may be vulnerable by 'driving' around in a moving vehicle. From outside the physical premises of the smart home an attacker can deauthenticate the Google Chromecast with a high-gain antenna on a wireless adapter. By deauthenticating the Chromecast, it puts it into setup mode. This ties in with the above attack surface we previously mentioned of 'Resetting the Device to an insecure state'. Once this stage is completed, the attacker can make the Chromecast connect to the attacker rather than the home network. This is the initial foothold completed. This is where the attacker can carry out the attack. Now a connection is established, the attacker can upload a YouTube video with verbal commands stated which will get sent to the Chromecast and consequently played through the television, which will then be picked up by the Alexa.

Pentest Partners (2021) then go on to show how they may use this initial attack to conduct further attacks on other IoT devices. Through the television, they send the command 'Alexa, turn on the kettle'. This results in the smart kettle heating up. Other attacks which could be triggered are more malicious such as, 'Alexa, set the thermostat to off mode', this could lead to the pipes in your home being frozen. Some security and unlocking devices such as a front door lock or a house alarm which are connected to the smart home such as locks etc. might require a PIN (personal identification number). If a PIN is simple such as 0000 or 1234, this is easily guessable by the attacker. Therefore, an attacker may be able to gain physical entry to the actual home. Furthermore, as previously stated, some credentials are stored. Pentest Partners (2021) demonstrate that using the mobile application for Alexa, you could retrieve a PIN.

There are also many other unofficial Alexa integrations which can allow you to open a garage door for example using the command, 'Alexa, open the garage door'. If the car within the garage is connected you may even be able to get the car to automatically drive itself out of the garage using 'Alexa, summon the Tesla'. However, this is a bit of a stretch as it is unofficial, but it does display what is possible by an attacker.

Other more mischievous attacks that might cause psychological harm to an inhabitant of the smart home might be for example, setting an alarm which reoccurs everyday at 3AM. They then suggest that this is resolved by setting the microphone to 'off' when voice control on the Amazon Alexa is not needed. [86]

Neagle (2015) comments on an attack discovered by PenTest Partners who are security researchers, which allowed them to obtain Gmail user's credentials from a Samsung smart fridge (model RF28HMELBSR). This is obviously extremely dangerous as email is one of the main forms of communication users use to sign up to all sorts of services, be it e-commerce, social networking, business related etc. If an attacker gains those details it could lead to further attacks such as blackmail and financial extortion, denial of services by changing passwords on accounts, gathering further information and banking information from users and taking control of any online accounts which as I have stated above could be online banking (if 2FA is weak, or perhaps ringing up support and social engineering the bank support line to reset the login details and gain full control of the bank), e-commerce (theft), social networking (cyber stalking and harassment) etc.

The attack the team performed was a man-in-the-middle (MITM) attack. They located the smart fridge from wardriving and outside the physical location of the fridge. They were able to exploit the fridge as it did not validate SSL certificates, even though it did incorporate SSL as part of its security. This consequently allowed the team to perform MITM attacks against most connections. As the fridge integrates with Gmail calendar, this provided the attackers with an opportunity to monitor the network to identify usernames and passwords when the fridge is linked to Gmail. This occurred at 'Defcon 23', however, an attack very similar in nature did occur in the wild. One hundred thousand devices were hijacked as part of a spam

attack which exploited a vulnerability in a smart refrigerator. It is unknown if attackers in the real-world have been exploiting these vulnerabilities, but it is suspected that they might. [84]

Chapter 4 Smart Home Attack Map

4.1 Structure of the Smart Home Attack Map

When approaching a method for solving the problem of designing an attack map for Smart Homes, the attack map could be designed and sorted in a variety of ways. For example, it could be designed by device, by layer of IoT infrastructure, by type of vulnerability, by impact and the list goes on. However, I will approach this attack map via stages similar to that of the ‘Cyber Kill Chain’ and ‘MITRE ATT&CK’ frameworks. Below we can see a comparison of the stages a penetration tester or attacker might use.

Cyber Kill Chain	MITRE ATT&CK
Reconnaissance	Initial Access
Intrusion	Execution
Exploitation	Persistence
Privilege Escalation	Privilege Escalation
Lateral Movement	Defense Evasion
Obfuscation/Anti-forensics	Credential Access
Denial of Service	Discovery
Exfiltration	Lateral Movement
	Collection
	Exfiltration
	Command and Control

Table 4.1 Cyber Kill Chain and MITRE ATT&CK framework stages comparison [87]

If we continue with all these stages, technologies and vulnerabilities within a smart home, the attack map will be extremely vast. For the sake of this project, this is not viable due to deadlines in which this report must be completed. Furthermore, the threat landscape is ever evolving with new technologies being introduced and adapted. Therefore, it should be a project which is constantly being updated. However, this is not viable.

In conclusion, the best way forward is to simplify the attack map by decomposing it into different attack stages as suggested in Table 4.1. This way we can analyse that thoroughly. Then we can look at specific approaches and tools used during that stage. These tools will be the most common and widely documented so that we have a good overview of the attacks. From here, we can link the attacks together. Each link will be labelled with a number so that an explanation and justification may be included in a table below the attack

map. Ultimately, we will end up with several sub sections of the attack map which are analysed at a deeper level, and then we may consolidate this work by producing a higher-level attack map.

The stages of the penetration test/attack will be decomposed into the stages in which an attacker may carry them out. For example, before carrying out an attack, it is important that an attacker identifies a vulnerability. Therefore, the first stage will be 'reconnaissance/initial access'. This is then followed by 'execution/exploitation' which will be combined as part of the same stage, and then 'stage 2' shows several things an attacker may do once they have carried out their initial attack in order to gain unauthorized access:

1. **Reconnaissance/Initial Access** (bug/vulnerability which allows a connection to be made. How does an attacker identify the bug and establish the initial access? E.g., wardriving allows them to identify a smart home network which has a vulnerable Chromecast. Furthermore, how does the attacker gain the initial access? E.g., exploiting the vulnerability in the Chromecast to reset it to a vulnerable state)

Execution/Exploitation (the attack that is carried out. These attacks will be categorized under headings such as credential access, whereby a man-in-the-middle attack might be used. This may also cover discovery on the smart home network where other devices are discovered on the network or particular services etc. in order to launch other attacks.)

2. **Cross-Contamination** (how might an attacker use one compromised device to impact or attack another device? E.g., using a Chromecast to voice control an Alexa to unlock the front door. Or perhaps as part of a DDoS attack, a device may be hijacked and become a bot within a botnet, remotely controlled and commanded to carry out attacks.)

Privilege Escalation (how an attacker might be able to escalate their privileges to become a user with more control and access rights)

Persistence (backdoor – how might an attacker ensure that remote access and control is persistent and sustained?)

Each of the above headings will have its own separate attack map. However, they as previously mentioned, they will all be combined into the final solution at a higher level. Other headings from MITRE ATT&CK and the Cyber Kill Chain have been purposefully removed to keep the scope of this project smaller and simple.

4.2 Smart Home Attack Map

4.2.1 Reconnaissance / Initial Access / Exploitation

On the following page is the first stage of the attack, ‘Reconnaissance / Initial Access’. This stage sets out how an attacker may gather intelligence and information about a victim or vulnerable device or technology. Then how they may use that information to gain initial access to the device, IoT framework or smart home network. This is depicted as an attack map.

Connectors between different phases or parts of the attack map are labelled with a number. This number is included in the table below with a justification as to how one technique may lead to another phase, technique, or tool. This stage of the attack will stop once the attacker has gained unauthorized access in one way or another. The following map will start with various attacks that can be used and then link different attacks and devices to one another.

Connector Label No.	Connection	Justification
1	Social engineering to searching of technical databases	Any social engineering activity may lead to the discovery of device information, such as device name, model, and version. This can give the attacker information which can be queried in a technical database to search for vulnerabilities and exploits. Thus, allowing them to target the victim.
2	OSINT to social engineering	An attacker may find information such as leaked credentials or personally identifiable information (PII) which allows them to perform an enhanced social engineering attack.
3	OSINT to searching of technical databases	An attacker may find out that a victim is using a specific device, for example, this could be found through an image on a social network of their home where their account is public e.g., Facebook. Alternatively, a victim may have posted on a public support form for a particular IoT device. The attacker can then search the technical database to identify vulnerabilities and exploits in order to plan an attack.
4	Various forms of social engineering attack connect to information disclosure.	All types of different social engineering techniques may lead to the victim disclosing confidential information to the attacker. Details such as usernames, passwords, emails, PINs and PII etc. may be disclosed. This information could be used in further attacks to overcome 2FA and multi-factor authentication, as well as access to other services and applications.
5	Information disclosure from social engineering to credential access	Once a successful social engineering attack has been carried out and an attacker has gained credentials. These credentials may be used to access associated accounts, or access public facing IoT applications which are part of the vulnerable IoT framework, whether they are on cloud, mobile, desktop or otherwise.
6	Physical access of IoT device links to physical or remote access to device	Whether an attacker has physical access or remote access is irrelevant with regards to this connection. An attacker may exploit a misconfigured or reset a device so that it connects to the attacker from within the home, allowing remote command execution (RCE).
7	Haveibeenpwned.com, namechk.com link to leaked credentials	Various sites may be used by an attacker to determine if an account or username has been compromised. If it has, the attacker can search for these leaked details on the dark web or in forums for example.

8	Vulnerable web application links to file inclusions	If there is a vulnerable web application as part of the IoT framework which may be exploited via the OWASP top 10 or other means, it could lead to a file inclusion exploit, whereby an attacker runs a file by uploading it to the web application or submits input into local files in a nefarious manner in order to perform another attack such as remote command execution, directory traversal or information disclosure of sorts.
9	Access to stored credentials connects to access associated accounts	If an attacker obtains hashed passwords and is able to crack them to find the plaintext / undigested passwords, these details may be used to access associated accounts and services. These may be other social media account, or network services such as Telnet, SSH or FTP for example.
10	RFI connects to RCE	If an attacker can get the vulnerable web application to execute or run a remote file they are hosting, this can lead to remote command execution. A technique I personally like to do is to use 'SimpleHTTPServer' in python on port 80: <i>python -m SimpleHTTPServer80</i> If the attacker then sets up a netcat listener on port 443 for example with <i>nc -nvlp 443</i> , their machine will listen for incoming connections. The attacker may have managed to upload a malicious file such as ' <i>evil.txt</i> ' with the following code inside: <i><?php echo shell_exec("bash -i>& /dev/tcp/attackers.ip/443 0>&1");?></i> Now when the attacker navigates to the file on the vulnerable web application e.g., <i>http://target.ip/index.php?ACS_path=http://attackers.ip:80/evil.txt?</i> The attacker will get a reverse shell, giving them remote command execution.
11	RCE to other vulnerable network services	If an attacker has RCE then they may be able to gather further information once on the system, escalate privileges to use other services, upload/replace/delete and download files, traverse directories etc.
12	Device information from receipts/product manuals obtained by dumpster diving to searching of technical databases	Device and IoT produce information may have been obtained via the collection of dumpster diving by means of receipts, product manuals etc. This information can consequently be used as part of a query to gather vulnerability and exploit information by the attacker.
13	Stalking to searching of technical databases and further attacks	An attacker may observe a victim. From this they may gather information such as place of residence, as well as purchased IoT devices, as well as daily schedule. Device details can be used to search for exploits and plan an attack. Furthermore, knowing a schedule may allow the attacker to gain physical access to the property whilst the victim is not on the premises, or perhaps cause distress to the victim by setting an alarm at 3AM each day etc. to name but a few potential attacks.
14	Social engineering techniques to downloading of malware onto victim machine	A variety of social engineering techniques may be employed by an attacker in order to get the victim to download malware onto their system. It may be a link an email, an attachment, "technical support" instructions over the phone, by email, by letter, by text or another tactic.
15 & 16	Website analysis to credentials	An attacker may scrape a website for usernames, email addresses, topics of interest which could all indicate possible credentials. For example, a wordlist that could be used as part of a dictionary attack with Hydra may be generated from text found on a website with the following command: <i>cewl -w xxxxwords.txt -d 10 -m 1 http://target.ip/</i> Using Hydra, an attacker may then gain access to network services such as FTP or SSH or IoT applications.

Table 4.2.1 Reconnaissance/Initial Access/Exploitation Connector Justifications

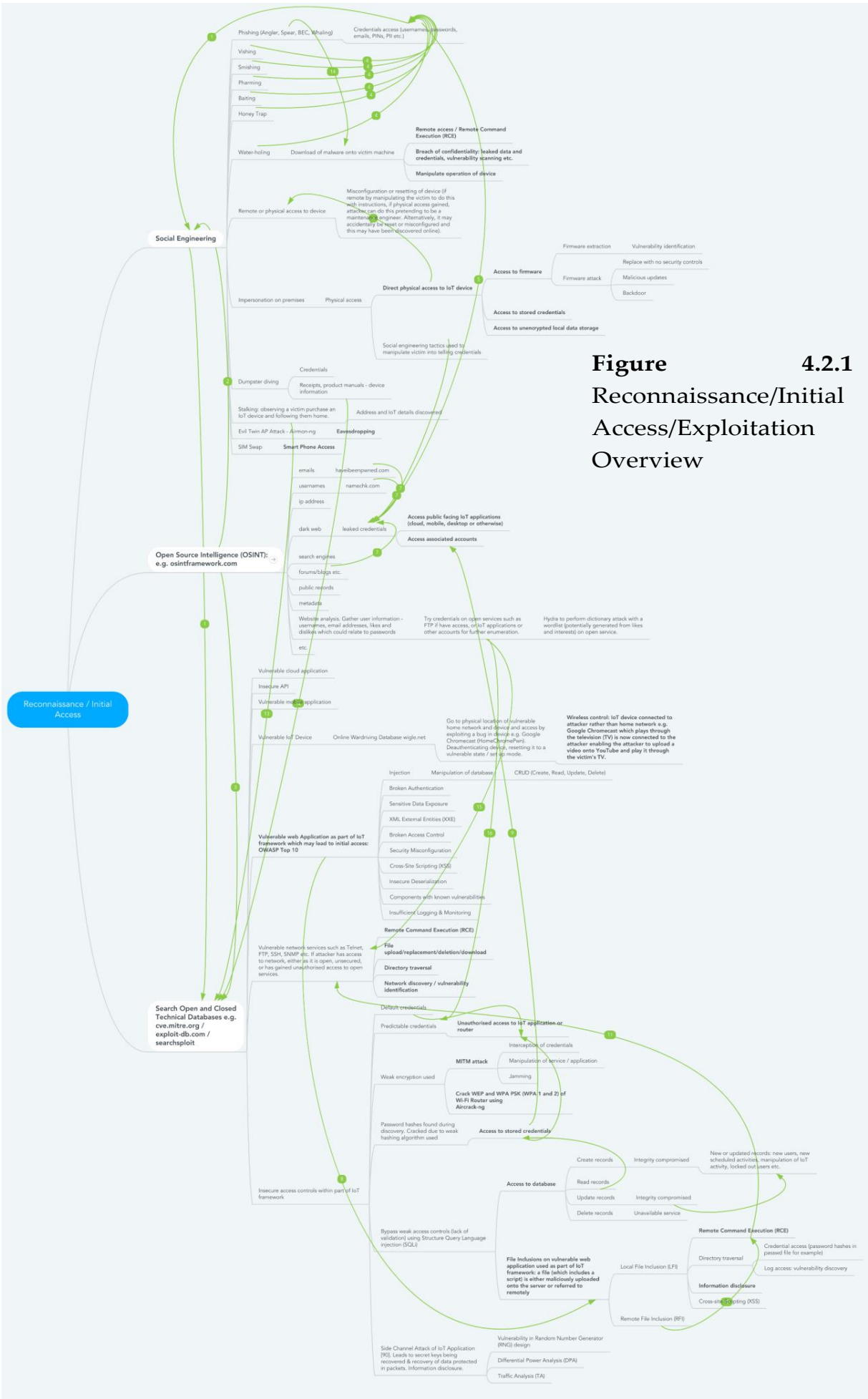
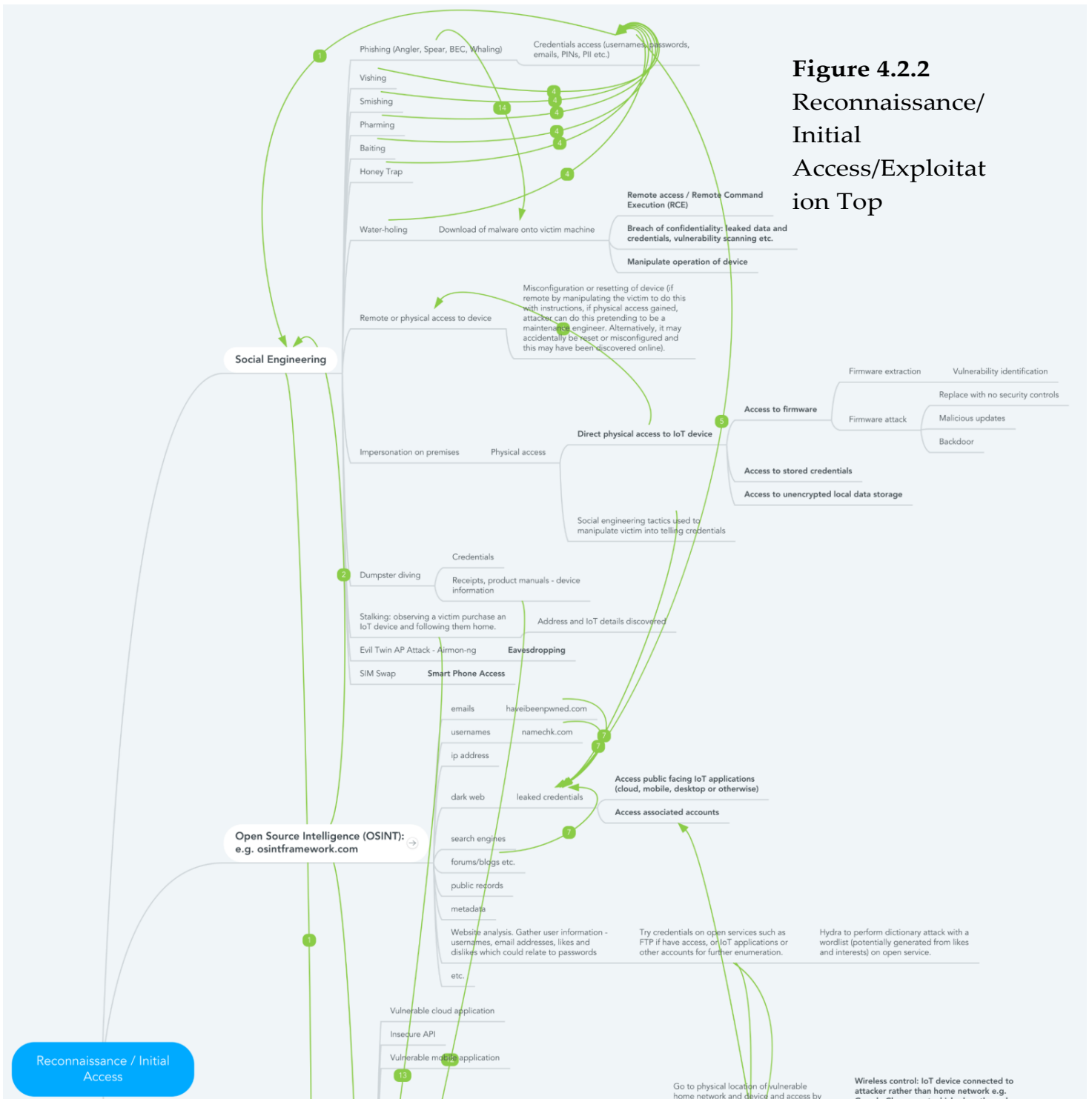
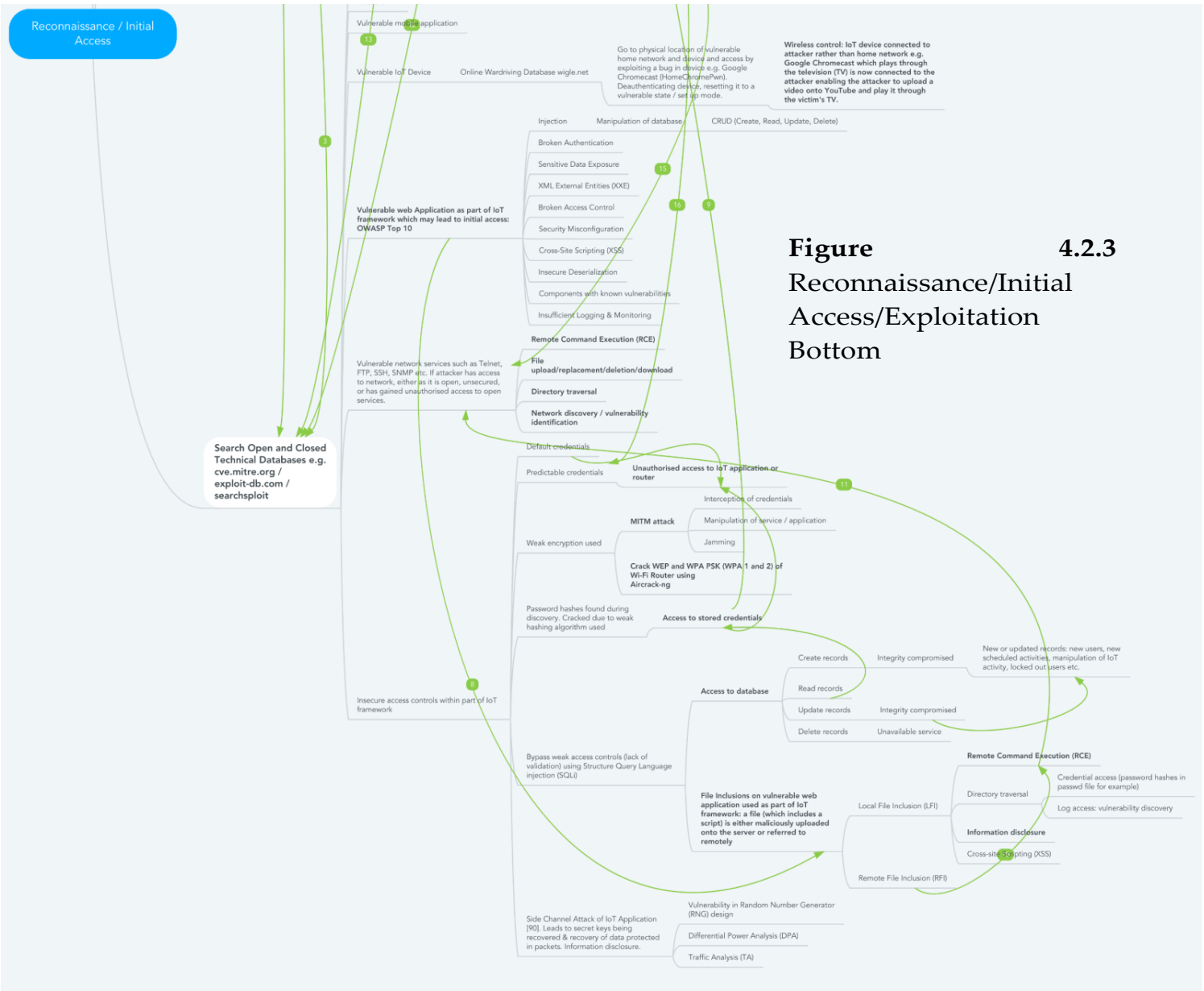


Figure 4.2.1
Reconnaissance/Initial
Access/Exploitation
Overview

The Reconnaissance/Initial Access/Exploitation map on the previous page is obviously quite hard to see, so over the next couple of pages it will be split. The previous image displays an overview, whereas these cross-sections of the image will allow the reader of this report to see it in more detail.





4.2.2 Cross-Contamination

This map will begin with an attacker who has gained an initial foothold on the network. This may either be a compromised service, device, or technology. The map will then visually represent how an attacker may attack or impact other parts of the home network from this initial point of attack.

Devices will be unnamed, and instead categorized by type of device to keep it purposefully generic. Explanations and justifications of how attacks connect with one another will, like above, be listed in a table.

Connector Label No.	Connection	Justification
1	Compromised smart TV links to voice controller	Compromised smart TV can play videos with voice commands to take control of the voice controller. For example, exploiting a bug in Chromecast which allows an attacker to reset the device to connect to their network, allows them to stream arbitrary content (videos with embedded voice commands such as 'Alexa, open garage door'), which can then be used to take control over Amazon Alexa for example which can then command any connected device. Furthermore, the videos could have SQLi commands which could access databases for information disclosure which could be used for passwords to be used against other accounts or OSINT, or even be used as part of a ransom, or for resale.
2	Compromised voice controller links to all other devices connected e.g. smart TV	If an attacker has gained control over a voice controller, any IoT device which is controlled and connected to the voice controller may be controlled. This could be security locks, home appliances, environmental control, home surveillance, smart TVs and entertainment equipment etc.
3	Physical access to devices within home links to cyberstalking	Once an attacker has gained physical access to the premises, they may be able to install surveillance hardware within the home. For example, they could then plant spyware or other actual listening or remote viewing devices and use these devices for cyber stalking or to gather further details. Below this is 'Analysis/tampering of existing technology within home', this could obviously lead to reconnaissance and gathering of information which could be searched for in a database of exploits, or it could be used to plant a backdoor, rootkit, spyware etc. which could lead to MITM attack, persistence etc. Furthermore, gaining physical access could lead to duplication of devices, forgery of documents such as passports, or replicas/cloned RFID badges etc. which could then be used to target the victim's place of work and gain access to their organisation's building. Having forgeries could also lead to identity theft and sale of identity, psychological harm and anxiety caused and denial of availability to services such as banks due to having compromised details.
4	Cryptanalysis attack allows attack on devices of the same type	A cryptanalysis attack on a radio communications IoT device allows an attacker to capture, analyse and reverse engineer the original transmission and command sequence. Once this is done, an attacker may craft their own messages and use these against devices of the same type.
5	DDoS attack on a	A DDoS attack on a router means that all devices that require an Internet

	router links to denial of availability	connection through the router will not be able to connect. Therefore, data cannot be transmitted to and from the cloud and updated in real-time. This results in data potentially not being up to date (integrity compromised), availability of services not available to victim when required, and could lead to physical harm e.g. a smart health monitoring system will not be updated and could affect the victim's health negatively.
6	A compromised security lock links to physical access to smart home	If an attacker has compromised a security lock, this leads them to gain physical access to the premises. This could then lead to theft of items, installation of surveillance hardware, information gathering, and analysis/tampering of existing technology within the home. Which could then lead to as previously stated, reconnaissance and gathering of information which could be searched for in a database of exploits, or it could be used to plant a backdoor, rootkit, spyware etc. which could lead to MITM attack, persistence etc.
7	Disabling of alarms links to physical access to smart home	If an alarm or sensor which is triggered by movement is disabled, when an attacker forces open a physical lock or gains physical access to the premises, the victim will not be notified.
8	Botnet links to DDoS Attack	A variety of compromised devices on the attack map share this connector label. This is because many of the IoT devices within a smart home may be used as a zombie within a botnet. It can be used to perform a DDoS attack to target another device such as a web server, which would bring down any services related to it such as a government website, or perhaps a video game server, so that players may not access this service and have online functionality or perhaps even make online purchases, costing the organisation money in terms of lack of sales, repair and maintenance, incident response, damage to reputation etc.
9	Compromised security links to compromised radio communications	A compromised radio communications IoT device, for example a garage door, could be opened through use of a replay attack. This means the garage door lock has been compromised, hence the connection between these two attacks.
10		
11	Information disclosure from eavesdropping using a smart TV's remote control microphone links to account compromised	If an attacker can gain information from eavesdropping on a household e.g. gaining information about their likes or even passwords, they can attempt associated accounts for the victim to gain unauthorized access. From this, they may launch a variety of attacks such as disabling 2FA, reconnaissance, harassment, blackmail, sale of information and account access, public leakage of credentials and psychological damage to victim.
12	Credentials gained from cyber stalking links to compromising of victim's other accounts	Credentials gained from analysis of captured video or audio, or password lists generated from the likes/dislikes and PII which have been gathered for a targeted victim may be used to gain unauthorized access to the victim's other accounts, which could then be used to launch a variety of other attacks.
13&14	SIM swap access to overcome 2FA links to access to other accounts.	An attacker who has performed a SIM swap can overcome 2FA when an SMS message is sent to the phone number associated with an account to log in. Likewise, this works the other way, if an attacker has accessed an account, they may update the 2FA to point to a different mobile phone number they have access to, and overcome 2FA that way.
15&16	Access to stored account information on system/web browser/software accounts links to access to other accounts	If an attacker obtains credentials and passwords from stored locations e.g. browser's saved passwords, these can then be used and attempted on other accounts held by the victim which then allows them to gain unauthorized access to accounts with the compromised password.
17		
18	Blueborne Attack links to Blueborne Attack	A compromised smart phone/computer or laptop which has Bluetooth technology enabled links may be susceptible to a Blueborne attack whereby an attacker gains unauthorized access and may then be able to

		remotely control the device, carry out a MITM attack or listen to audio for example.
19	MITM attack links to MITM attack (further info explained)	A compromised Windows machine via Bluetooth may be susceptible to a MITM attack which could be used to either capture data (Eavesdropping, packet sniffing etc.) or to craft and inject malicious packets into communications.
20	Compromised generic IoT device/accounts etc. can lead to a ransom	After a device or account has been compromised and the victim identified. A ransom may be demanded so that normal services are restored when the payment is completed. This may not be ransomware, but instead ransom. This could also result in the victim being told as part of the ransom to disclose confidential or sensitive information, which could be used to launch other attacks, such as blackmail, compromise of other accounts, sale of information, damage to reputation humiliation and psychological harm.
21	Ransom links to Ransom (see above number)	This link was made to tidy up the map, otherwise every device would be linking to the same ransom point and it would make it harder to read.
22	Privilege escalation links to compromised smart phone/computer or laptop connected to home network	If a user has gained access as a local user to a system, then escalated their privileges to become system or root, they may then laterally move to another device that is connected or alternatively be on that device with higher privileges and launch further attacks.

Table 4.2.2 Cross-Contamination Connector Justifications

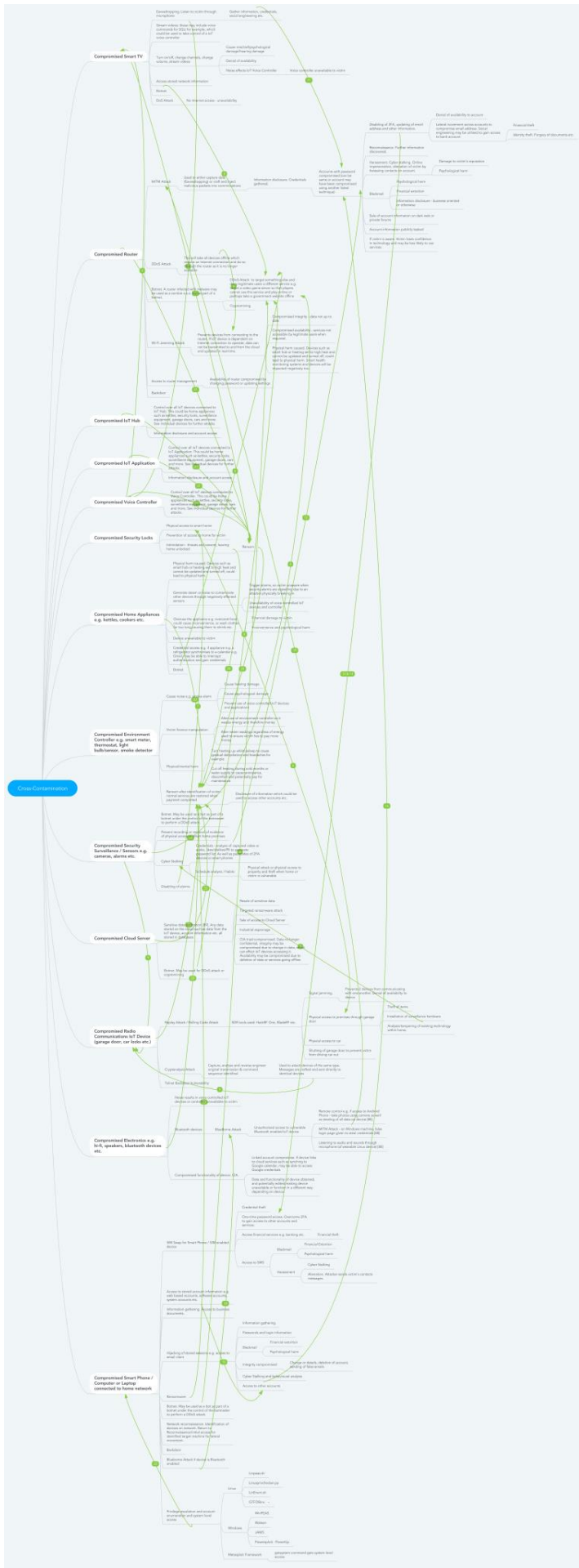
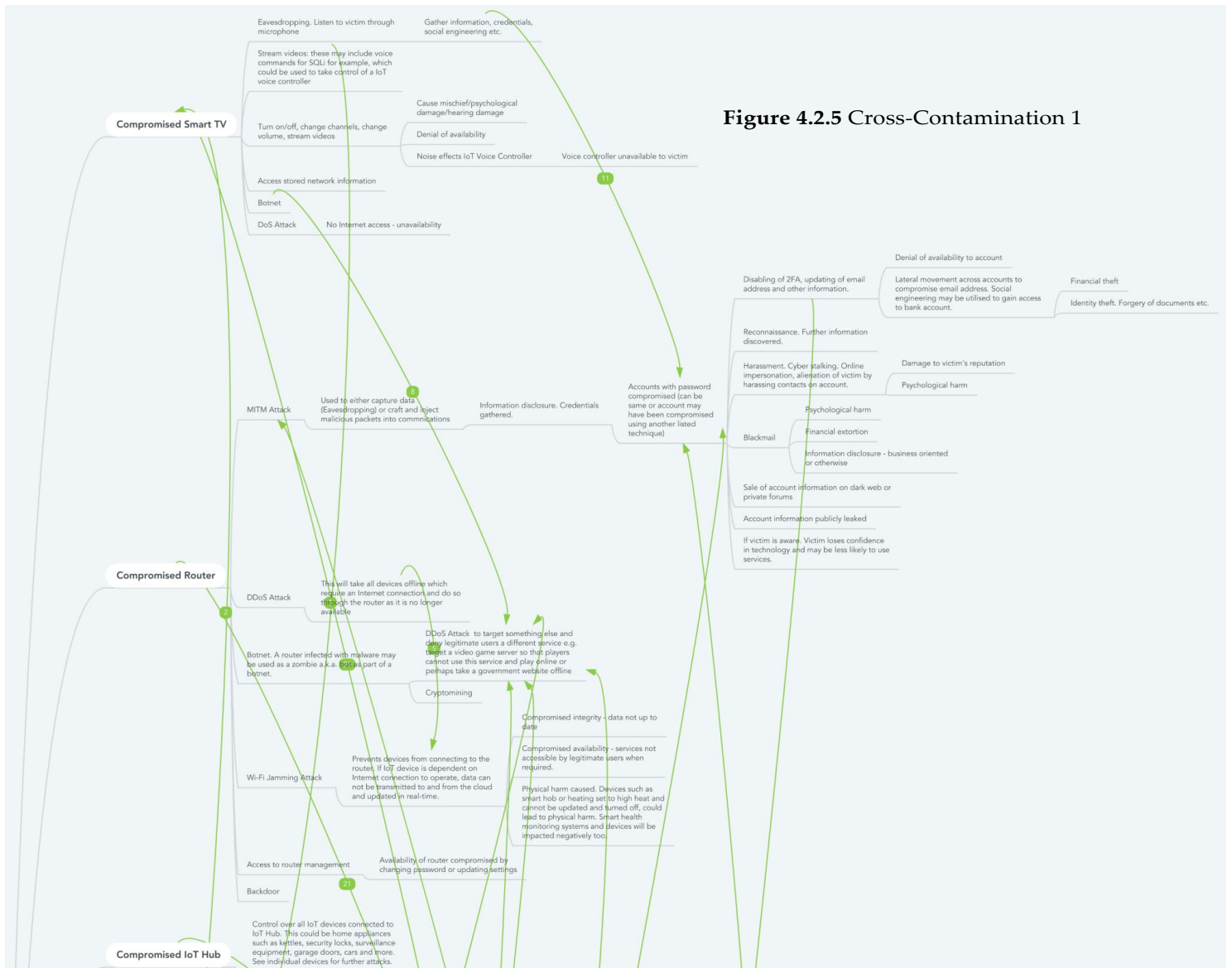


Figure 4.2.4 Cross-Contamination Overview



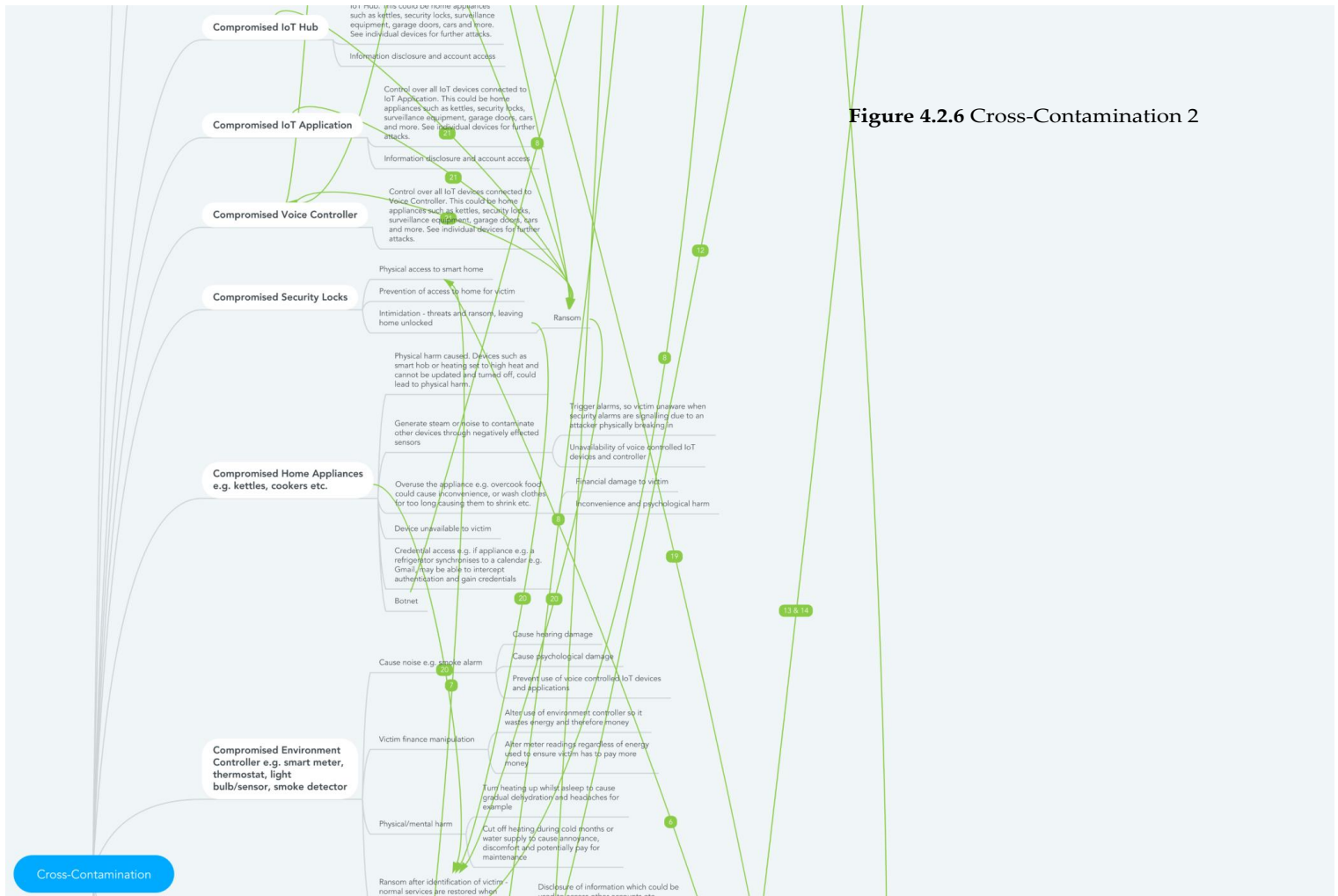


Figure 4.2.6 Cross-Contamination 2

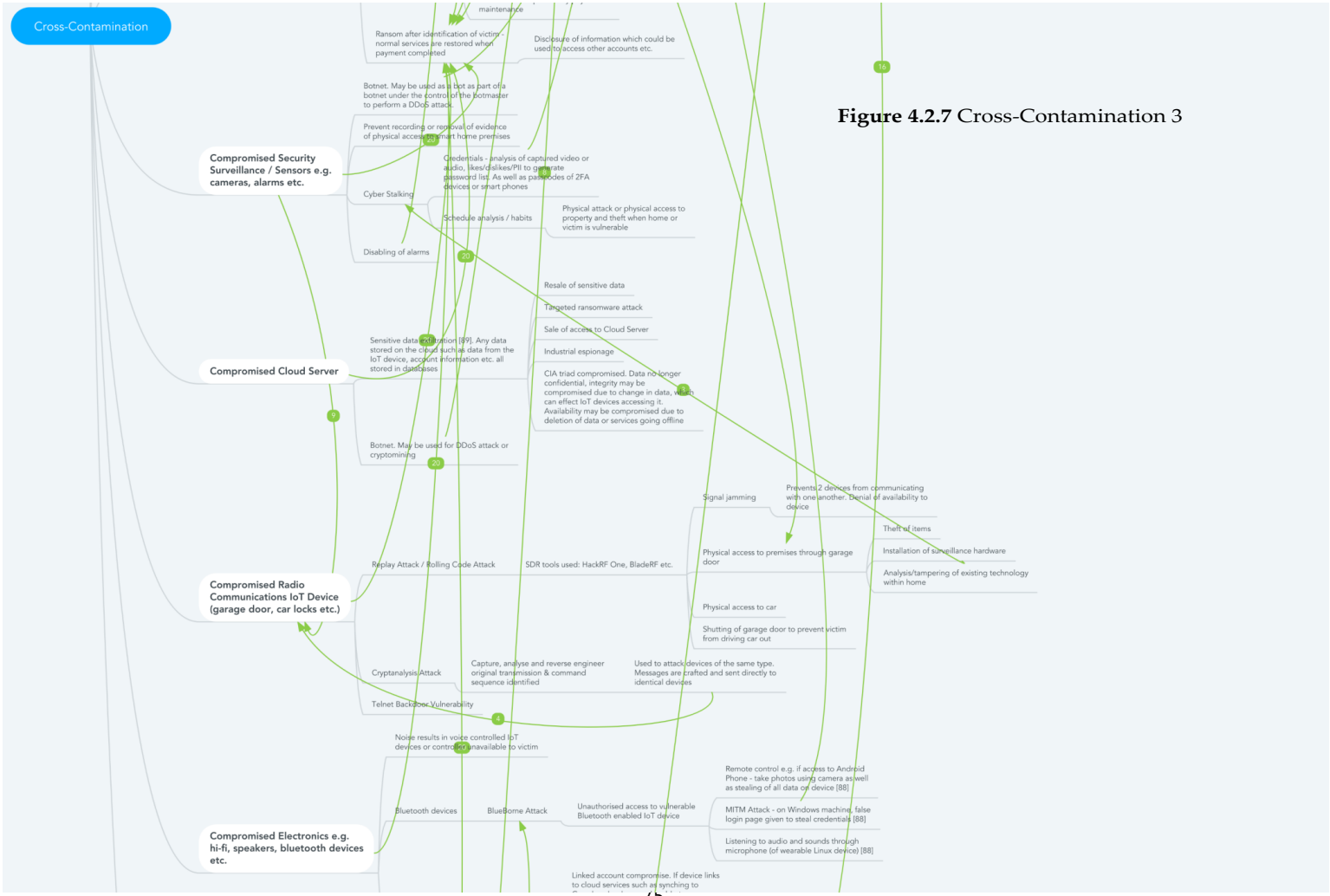


Figure 4.2.7 Cross-Contamination 3

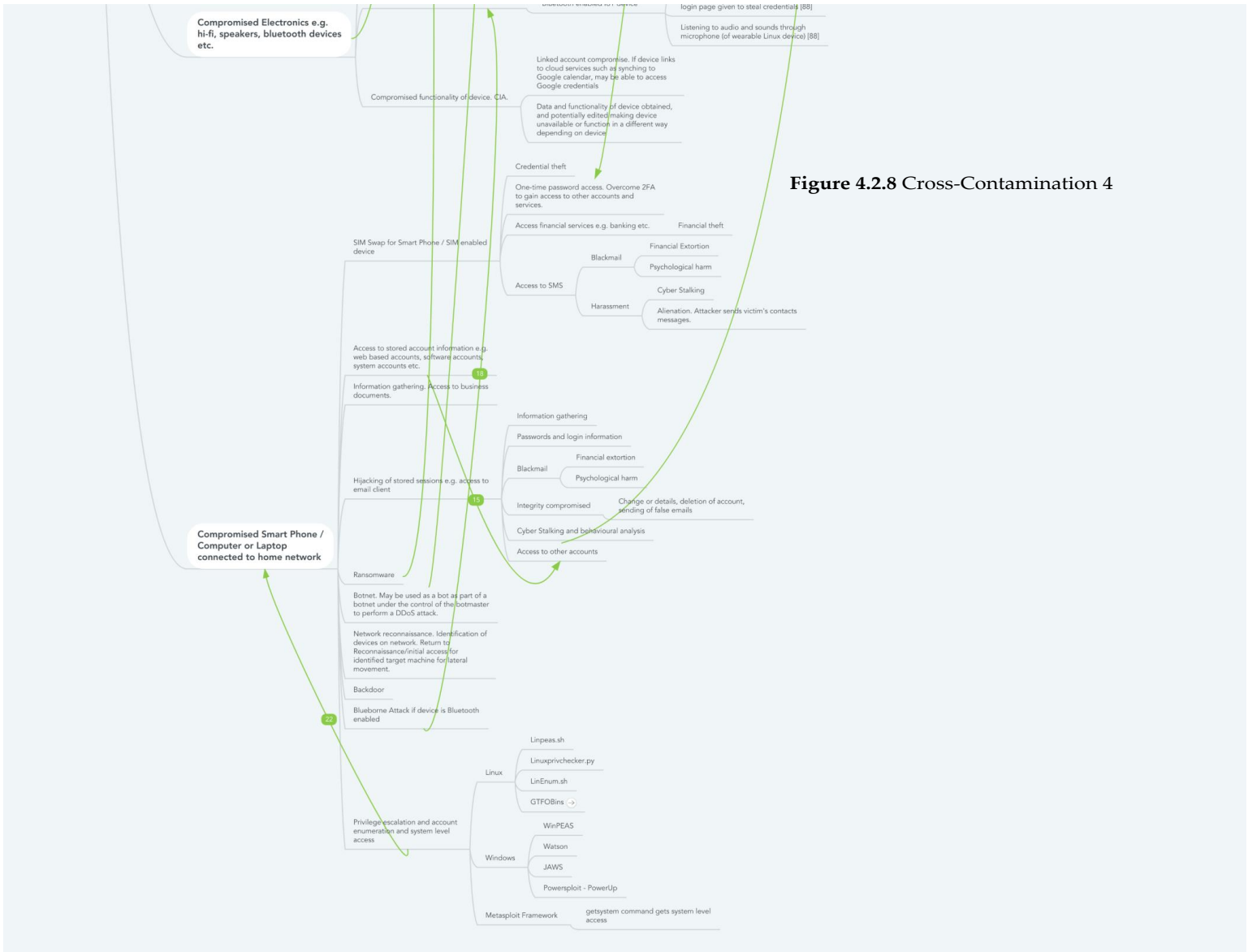


Figure 4.2.8 Cross-Contamination 4

4.3 Counter-measures and security controls

According to Tuna, G. et al. (2017) there are several security goals that should be considered within an IoT infrastructure. These include the established 'CIA triad', however, are not limited to these three:

- Confidentiality, this ensures that data whilst in transmission or even in storage is kept private and is not readable by unauthorized users. This prevents information disclosure.
- Integrity, this ensures that the data has not been tampered with, either during transmission, or when stored. The integrity of the data is retained. Unauthorized alteration of data can have catastrophic results. For example, data stored about a user's health in the cloud is altered in an unauthorized manner, and when the device attached to the victim is updated with data stored in the cloud, it could result in a negative and harmful effect as stated in the attack map.
- Availability, this ensures that services are available to authorized users when needed and required.
- Access Control, this ensures that different users, machines or requests can only access content and services which are strictly needed for the process.
- Authentication, this ensures that the data being received is from an authentic, trusted sender. This supports data integrity.
- Non-repudiation, this ensures that if a device or part of the IoT framework has transmitted data, it cannot deny this at a later date. This supports authentication and therefore, data integrity.
- Freshness secrecy, this ensures that data cannot be replayed. This supports data integrity. [2]

Now that we have identified the core security goals of an IoT framework within a smart home, what can we do to ensure that these objectives are met? This is what we will look at in this section. We will examine these controls from the perspective of the end user, as well as developers, as everyone involved in the IoT framework and system is responsible for security and the prevention of attacks.

There are some common ways in which we can minimize risk to prevent threats from being realized, as well as meeting the above security goals. From our attack map, previous research, OWASP IoT Project (2017) and Ferrari (2019) we have identified key vulnerable areas and security controls which may be implemented to improve security.

Convenience vs security, the disabling of unused technologies. If network services, ports, access rights from users and devices, and sensors are not explicitly needed, make sure that they are disabled. For example, ensure that there are no open ports which do not need to be open, or network services available which do not need to be available as this may allow an attacker to gain an initial foothold, especially if it not maintained or tested regularly by security experts. Also, ensure that access rights are restricted for both users and devices, so only data or processes may be accessed that are needed for the minimum amount of functionality. This leads on to disabling insecure Universal Plug and Play services (UPnP). Further to this, sensors that are not needed should be disabled. What do I mean by this? Let us examine a scenario. Within a voice controller which is connected as part of an IoT ecosystem, the microphones (sensors) should be turned off when not needed. This is for the reason that if another device is compromised, it cannot use the voice controller as part of the attack map. In addition, to the above, if debugging ports are not needed, they should be disabled too. Ports such as UART, JTAG and GPIO should be disabled after shipping. Insecure or outdated components must be not used or disabled, this includes vulnerable libraries. Ultimately, it is extremely important to weigh up security and convenience, and find a balance that fits the risks and value of assets the inhabitants of the smart home have.

Updates, securing hardware and secure technologies. Risk may also be minimized by keeping things up to date and maintaining hardware and ensuring the hardware is secured. This may be reactive and achieved once a bug has been discovered. For example, firmware updates must be enabled and updated regularly. These updates or patches may be applied within the hardware. These updates must be done so in a controlled and secure manner. Regular and periodic penetration tests must therefore be conducted on these devices and on the IoT infrastructure to ensure that no bugs are left unaddressed, as this will be a vulnerability that an attacker may exploit. Securing of hardware may be achieved by implementing secure boot and keeping digital certificates protected. In addition strong encryption should be used as an attacker may often begin their infiltration by extracting the firmware from the device itself. Storage, drivers, firmware and data addresses should all be encrypted. Continuing with encryption, data during transmission and in storage must be encrypted or hashed. It is recommended to use encryption technology in HTTP by implementing security technologies such as SSL/TSL/DTSL.

Passwords and authentication. We can see that from the attack map that if an attacker gains access to an account or user credentials such as username and password, this can lead to further attacks or the compromising of other accounts. By having strong, unique passwords and updating them regularly, it means that if there is a data breach, these credentials may not be used on associated accounts. From a developer's perspective, it is important to never hardcode passwords in the program or firmware. Default or built in passwords must be changed. Moreover, 2FA or MFA should be implemented as a minimum security requirement during the authentication process, whereby the proposed identity of a user logging in is verified. This authentication must be done with two of a three possible types of authentication, something known (a shared secret such as a password), something owned (an ID badge or cryptographic key for example), or something the user is (biometrics such as data stored about the user's retina). By combining two or more of the above, it is a lot more difficult for an attacker to gain unauthorized access. Whereas, individually, each may be weak e.g. something owned may be cloned or forged, or a password may be cracked using a dictionary attack. In addition, password recovery must be done so in a secure manner and may require a different form of communication to recover it e.g. for email recovery, send a recovery PIN to an associated mobile phone (something owned). This relates back to OWASP's IoT Project (2017) whereby lack of authentication and authorization, or weak encryption, as well as lack of sanitization of inputs and output filtering can lead to insecure ecosystem interfaces, such as a vulnerable backend API or insecure web, mobile or cloud interface.

In relation to the above, login attempts must be monitored, blocking accounts and blacklisting IP addresses who reach a specific number of login failures. This leads onto the last point which is the detection of vulnerabilities or threats through use of an IDS (Intrusion Detection System) or IPS (Intrusion Prevention System). [79, 85]

How does one ensure that all of these security controls are implemented from design through to shipment and integration within a smart home? Policies, regulations and standards may pave some sort of way forward and progression in terms of security. However, this is only part of the solution, as when the responsibility of security is left up to the purchaser of the IoT device, they have free will to choose poor passwords which is a potential attack vector as discovered credentials may consequently be used in the common attack, credential stuffing. In which case, education of security to end users and

inhabitants of smart homes, coupled with forced security actions such as updating a password. Ultimately, there is no perfect solution that will completely minimize all risk, just controls which may be implemented to help reduce the likelihood of a threat being realized.

Chapter 5 Conclusions

In the following section we will review any limitations associated with the attack map as well as limitations to the suggested security controls, as well as conclusions which can be drawn from this thesis.

a. Limitations

The solution being proposed has the following limitations:

- i. **Attack map – too simple, not all possible attacks covered.** A limitation of the attack map is that it is too simple and does not cover every eventuality. The reason for this is simple, technology is progressing, and with that, new attacks are developed and the threat landscape is ever changing. Therefore, this attack map, is to some degree a snapshot of common attacks. Not all possible attacks and technologies are covered, as this would over complicate the map. Furthermore, it would be an expansive project and not viable for a thesis, due to the quantity of work involved and amount of time needed. It would have to be in a constant state of transition, updating on a daily basis. This was not a reasonable proposal for a thesis, and therefore, I believe that the level of complexity if appropriate, examining the most common attacks and how they may connect to further attacks.
- ii. **Attack map – too complex.** Some readers of this thesis may find that the links between the attacks are difficult to follow. However, the attack map has been broken down into 2 phases, and each has been broken down into further images that are viewable. If one studies the links between attacks, they will see that they are numbered. These numbers link to the justifications table which can be used for further information to help explain how one attack may cause cross-contamination, or lead to another attack. Furthermore, if the attack map was made any simpler then it would not be as effective. The way it is, it shows an overview of common attacks and how they can link to one another. It could be argued, that this map could include even more detailed analysis with even deeper detail of technologies. However, as stated in the previous point, this could make the

project considerably vaster.

iii. **Security controls. No perfect way to completely reduce all risk. Playing catch up.** Unfortunately, there is no way to completely remove all risk. This is one of the first things we learn when we study risk management. We can only but mitigate risk. We may accomplish this by incorporating the following strategies:

1. Risk Avoidance – develop an alternative strategy with avoids the risk.
2. Risk Acceptance – accepting the risk and the impact that it may have on the assets of the organisation. Taking no action.
3. Risk Limitation – reducing the risk by implementing security controls. This helps the organisation to prepare for and act against potential threats to minimize the impact
4. Risk Transference – passing the responsibility of the risk onto a third party.

With this in mind, coupled with the fact that the threat landscape as previously stated is constantly evolving, as the defenders we must be, it is a game of cat and mouse whereby the attackers find a new attack and a new threat is developed, and then we must react. This is even the case when preventative measures are in place. We may think we have an expensive IPS or IDS or security mechanisms that are implemented within the IoT hardware within our smart home, or even elsewhere in the IoT framework, but it takes just one vulnerability, bug or flaw that is discovered by an attacker to circumvent these security controls. Therefore, regrettably, there is no possible way to ensure that the smart home is perfectly secure, but instead only advice that may be given to reduce risk as much as possible, and then, only if it is followed and correctly, and consistently implemented throughout the entire IoT framework will it be effective.

b. Conclusion

Finally, we will address the initial objectives of this thesis to decide whether they have

or have not been met, and to what extent.

- i. **Objective 1: Find relevant references – Literature review.** Relevant references were discovered for each part of this project with nearly one hundred sources used in support of statements or to extract information and research which was used in this thesis. These sources allowed us to identify what the IoT is, smart homes, examine a relevant IoT framework for smart homes, as well the attack phases and attacks which may be conducted on a smart home. This research during the literature review was consequently used to aid in the development of the smart home attack map in Chapter 4.
- ii. **Objective 2: Understanding the security issues with IoT.** Security issues were thoroughly examined, both in terms of the most common attacks, as well as the most common vulnerabilities and causes for threats to be realized. To summarise, some of the most common security issues associated with smart home IoT infrastructure are: passwords, insecure network services, insecure ecosystem interfaces (vulnerable cloud, web and mobile applications, insecure APIs), lack of updates and insecure components, insecure data storage and transmission (stored credentials), lack of physical hardening, lack of device management (misconfigurations etc.), and insecure default settings. These occur for all matter of reason, but one common issue is the interoperability of heterogeneous devices, meaning that there are a vast amount of diverse devices that must communicate with one another.
- iii. **Objective 3: Smart home attack map and recommended security controls.** Smart home attack maps were developed along with justifications between different techniques and attacks. The attack map for decomposed into two phases following MITRE ATT&CK and the cyber kill chain, resulting in the first attack map, reconnaissance and initial foothold, whereby an attacker gathers information, enumerates and gains initial access to the IoT infrastructure or device within the smart home. The second phase of the attack was cross-contamination, whereby an attacker carries out an attack, and it impacts other parts of the IoT infrastructure, or may be used to carry out

further attacks.

- iv. **Objective 4: Conclusion.** This section, Chapter 5, has been the conclusion where I have looked at the limitations of this project, making justifications as to why specific decisions were made during the development of the attack map. The initial objectives were also examined and assessed to see whether they had been met and to what extent.

In my opinion, the objectives that were initially set out at the beginning of this thesis have been successfully met. The purpose of this project, to develop an attack map for a smart home, was successful, and in order to accomplish this, relevant information and an understanding of the security issues, attacks and technologies related to smart homes were identified and explained in a manner that helped the reader to gain an understanding, even with little or no technological background and experience. This was achieved in the following chapters:

1. Chapter 1: Executive Summary – this chapter was brief, summarizing the thesis.
2. Chapter 2: Introduction – this chapter introduced the project, identifying the initial objectives, methodology, structure of the report and motivation. This allowed the reader to gain a deeper understanding of what this project is about, building upon the executive summary outlined in Chapter 1.
3. Chapter 3: Literature Review – this chapter examined existing literature related to the topic of study, the IoT, with a focus on smart homes. This was written in such a way that it started with simple explanations and an overview of the IoT, before examining technologies and the smart home in further detail.
4. Chapter 4: The Attack Map – this chapter detailed and justified the approach to the attack map, before developing the solution.
5. Chapter 5: Conclusion (This chapter).

Ultimately, I hope whoever has read this has taken something away from this, and found something of interest or enjoyment within these pages. Thank you.

References

1. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27. <https://doi.org/10.1016/j.jisa.2017.11.002>
2. Tuna, G. et al. (2017). A survey on information security threats and solutions for Machine to Machine (M2M) communications. (2017). *Journal of Parallel and Distributed Computing*, 109, 142–154. <https://doi.org/10.1016/j.jpdc.2017.05.021>
3. Aman, W., & Snekenes, E. (2015). Managing security trade-offs in the Internet of Things using adaptive security. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 362–368. <https://doi.org/10.1109/ICITST.2015.7412122>
4. Ko, E., Kim, T., & Kim, H. (2017). Management platform of threats information in IoT environment. *Journal of Ambient Intelligence and Humanized Computing*, 1–10. <https://doi.org/10.1007/s12652-017-0581-6>
5. Kotenko, I., Saenko, I., & Ageev, S. (2015). Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference. 2015 IEEE Trustcom/BigDataSE/ISPA, 654–659. <https://doi.org/10.1109/Trustcom.2015.431>
6. Mohan, A. (2014). Cyber Security for Personal Medical Devices Internet of Things. 2014 IEEE International Conference on Distributed Computing in Sensor Systems, 372–374. <https://doi.org/10.1109/DCOSS.2014.49>
7. Covington, M. J., & Carskadden, R. (2013). Threat Implications of the Internet of Things. *Cyber Conflict (CyCon)*, 2013 5th International Conference On, 1–12. Retrieved from https://ccdcoe.org/cycon/2013/proceedings/d1r1s6_covington.pdf
8. Krishna, B.V.S. and Gnanasekaran, T. "A Systematic Study of Security Issues in Internet-of-Things (IoT)," in International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.
9. Bhabad, M.A. and Bagade, S.T. "Internet of Things: Architecture, Security Issues and Countermeasures," *International Journal of Computer Applications* (0975 - 8887), vol. 125, no. 14, p. 1, September 2015.
10. Bauer M. et al. (2013) IoT Reference Model. In: Bassi A. et al. (eds) *Enabling Things to Talk*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40403-0_7

11. Khan, R., Khan, S.U., Zaheer, R., and Khan, S. "Future Internet: The Internet of Things architecture, possible applications and key challenges," in 2012 10th International Conference on Frontiers of Information Technology, Islamabad, Dec 2012.
12. Yang, Z. et al., "Study and application on the architecture and key technologies for IOT," in 2011 International Conference on Multimedia Technology, Hangzhou, 2011.
13. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari M., and Ayyash, M. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE COMMUNICATION SURVEYS & TUTORIALS, vol. 17, no. 4, pp. 2349-2350, 2015.
14. Choudhary, G., and Jain, Dr. A.K. "Internet of Things: A Survey on Architecture, Technologies, Protocols and Challenges," in IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), Jaipur, India, 2016.
15. Koshizuka, N., Sakamura, K. "Ubiquitous ID: Standards for Ubiquitous computing and the Internet of Things," IEEE Pervasive Computing, vol. 9, no. 4, pp. 98-101, October-December 2010.
16. Kushalnagar, N., Montenegro, G., and Schumacher, C. "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," Internet Eng. Task Force(IETF), Fremont, CA, USA, Aug 2007.
17. Ko, J. et al., "Connecting low-power and lossy networks to the internet," IEEE Communications Magazine, pp. 96-101, 05 April 2011.
18. Kumar, N. "IoT architecture and system design for healthcare systems," in 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), Bangalore, India, 2017.
19. Andrea, I., Chrysostomou, C., and Hadjichristofi, G. "Internet of Things: Security Vulnerabilities and Challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 2015.
20. Deogirikar, J., Vidhate, A. "Security Attacks in IoT: A Survey," in International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.
21. Derhamy H , Eliasson J , Delsing J , Priller P . A survey of commercial frame- works for the Internet of things. In: 2015 IEEE 20th conference on emerging technologies & factory automation (ETFA). IEEE; 2015. p. 1-8.
22. Mrabet, Hichem (28/06/2020). "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis". Sensors (Basel, Switzerland) (1424-8220), 20 (13), p. 3625.

23. Heubl, B. "How to hack into the IOT: An E&T investigation carried out with leading cyber-threat experts reveals how simple it is to hack web-connected Internet of Things (IoT) devices and explores the implications for consumers and critical infrastructure in the UK," in *Engineering & Technology*, vol. 14, no. 7/8, pp. 18-23, Aug.-Sept. 2019, doi: 10.1049/et.2019.0700.
24. Sarmah, R., Bhuyan, M., and Bhuyan, M.H. "SURE-H: A Secure IoT Enabled Smart Home System," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 59-63, doi: 10.1109/WF-IoT.2019.8767229.
25. Ur Rehman, S., and Gruhn, V. "An approach to secure smart homes in cyber-physical systems/Internet-of-Things," 2018 Fifth International Conference on Software Defined Systems (SDS), Barcelona, 2018, pp. 126-129, doi: 10.1109/SDS.2018.8370433.
26. Alrawi, O., Lever, C., Antonakakis M., and Monroe, F. "SoK: Security Evaluation of Home-Based IoT Deployments," 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 1362-1380, doi: 10.1109/SP.2019.00013.
27. Yang, A., Zhang, C., Chen, Y., Zhuansun Y., and Liu, H. "Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2521-2530, April 2020, doi: 10.1109/JIOT.2019.2946214.
28. Meneghello, F., Calore, M., Zucchetto, D., Polese M., and Zanella, A. "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.
29. Help Net Security. (2020). Ryuk ransomware behind one third of all ransomware attacks in 2020. [online] Available at: <https://www.helpnetsecurity.com/2020/11/03/ryuk-ransomware-2020/> [Accessed 26 Dec. 2020].
30. Ivanyuk, A. and Wuest, C. (2020). Acronis Cyberthreats Report 2020 Cybersecurity trends of 2021, the year of extortion. [online] Available at: https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Threats_Report_2020_EN-US_201201.pdf [Accessed 3 Dec. 2020].
31. Forescout Research Labs, 2020. AMNESIA:33 - How TCP/IP Stacks Breed Critical Vulnerabilities In Iot, OT And IT Devices. [online] Available at: <https://www.forescout.com/company/resources/project-memoria-and-amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices-report/> [Accessed 3 Dec 2020]. - <https://www.forescout.com/company/blog/amnesia33-forescout-research-labs-finds-33-new-vulnerabilities-in-open-source-tcp-ip-stacks/>
32. BSIMM, 2020. BSIMM11. [online] Available at: <https://www.bsimm.com/download.html>

[Accessed 9 Dec 2020].

33. Finkelstein, A., Warshavski, D. and Wasserman, B. 2020. Extortion Attack: A View From the Frontlines of Cyber. Black Hat Europe 2020, 9 Dec., Online (Sygnia Virtual Booth).
[REMOVE]Black Hat Talk – showing how vulnerability in TP Link home router, was used as part of a ransomware for a pharmaceutical company for \$300,000,000. #
34. Zarandy, A., Shumanilov, I. and Anderson, R. 2020. "Hey Alexa what did I just type? Decoding smartphone sounds with a voice assistant." arXiv:2012.00687 [cs.CR]
35. FireEye, Inc, 2020. A Global Reset – Cyber Security Predictions 2021. [online] Available at: <<https://content.fireeye.com/predictions/rpt-security-predictions-2021>> [Accessed 14 Dec 2020].
36. Comer, D., 2009. Computer Networks And Internets. 5th ed. Upper Saddle River, NJ, USA: Pearson Education.
37. Kizza, JM. (2017) Computer Network Security Protocols. In: Guide to Computer Network Security. Computer Communications and Networks. Springer, Cham. https://doi.org/10.1007/978-3-319-55606-2_17
38. Techopedia.com. 2020. What Is Pervasive Computing? - Definition From Techopedia. [online] Available at: <<https://www.techopedia.com/definition/667/pervasive-computing>> [Accessed 30 December 2020].
39. Ramos, C., Augusto, JC., Shapiro, D. Ambient Intelligence-the Next Step for Artificial Intelligence. IEEE intelligent systems. 2008;23:15-18.
40. Mutter, AD. Welcome to 'Everyware' Computing. Editor & Publisher [serial online]. 2015;148:22.
41. Patterson HM. Physical Computing's Connected and Shape-Changing Future. IEEE pervasive computing. 2017;16:7-11.
42. Khaled AE, Helal A, Lindquist W, Lee C. IoT-DDL–Device Description Language for the “T” in IoT. IEEE access. 2018;6:24048-24063.
43. Balakrishnan SM, Sangaiah AK. MIFIM—Middleware solution for service centric anomaly in future internet models. Future generation computer systems. 2017;74:349-365.
44. Giffinger R. et al. Smart Cities – Ranking Of European Medium-Sized Cities. Vienna: Centre of Regional Science (SRF), Vienna University of Technology; 2007. http://www.smart-cities.eu/download/smart_cities_final_report.pdf. Accessed January 4, 2021.

45. Bassi A. et al. (eds) *Enabling Things to Talk*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40403-0_7
46. Hive | Start Your Smart Home. Hivehome.com. <https://www.hivehome.com/>. Published 2021. Accessed January 4, 2021.
47. Security Cameras. Ring. <https://en-uk.ring.com/pages/security-cameras>. Published 2021. Accessed January 4, 2021.
48. Smart Grid: The Smart Grid | SmartGrid.gov. Smartgrid.gov. https://www.smartgrid.gov/the_smart_grid/smart_grid.html. Published 2021. Accessed January 4, 2021.
49. What is a smart city? Technology and examples. Thalesgroup.com. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/smart-cities>. Published 2021. Accessed January 4, 2021.
50. Oyster online - Transport for London - Oyster cards. Oyster.tfl.gov.uk. <https://oyster.tfl.gov.uk/oyster/entry.do>. Published 2021. Accessed January 7, 2021.
51. MDPI. Economic, Social Impacts And Operation Of Smart Factories In Industry 4.0 Focusing On Simulation And Artificial Intelligence Of Collaborating Robots.; 2019. <https://www.mdpi.com/2076-0760/8/5/143/pdf-vor>. Accessed January 8, 2021.
52. Ahuett-Garza, Horacio, and Thomas-R. Kurfess. 2018. A brief discussion on the trends of habilitating technologies for Industry 4.0 and Smart Manufacturing. *Manufacturing Letters* 15: 60–63.
53. Zhong, Ray-Y., Xun Xu, Eberhard Klotz, and Stephen Thomas Newman. 2017. Intelligent manufacturing in the context of Industry 4.0. *A Review Engineering* 3: 616–30.
54. Ilascu I. Hacker used ransomware to lock victims in their IoT chastity belt. *Www-bleepingcomputer-com.cdn.ampproject.org*. <https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/hacker-used-ransomware-to-lock-victims-in-their-iot-chastity-belt/amp/>. Published 2021. Accessed January 10, 2021.
55. Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: development of a reference architecture for attack surface analysis. *IoT* 2018. https://pdfs.semanticscholar.org/21a5/567edfde6f0af996744d50b9622953656787.pdf?_ga=2.60842283.622847652.1610526118-898579358.1610526118. Accessed January 13, 2021.

56. Arubanetworks.com. <https://www.arubanetworks.com/products/security/network-access-control/>. Published 2021. Accessed January 14, 2021.
57. BS 6568-1:1988, EN 27498:1989,ISO 7498-1984,ISO 7498:1984/Add. 1:1987: Reference model of open systems interconnection. Basic reference model (incorporating connectionless-mode transmission). British Standards Institute; 1988.
58. What is OSI Model | 7 Layers Explained | Imperva. Learning Center. <https://www.imperva.com/learn/application-security/osi-model/>. Published 2021. Accessed January 14, 2021.
59. Khan, R., Khan, S. U., Zaheer, R., and Khan, S. "Future Internet: The In-ternet of Things architecture, possible applications and key challenges," in Proc. 10th Int. Conf. FIT, 2012, pp. 257–260.
60. Yang, Z. et al., "Study and application on the architecture and key technologies for IOT," in Proc. ICMT, 2011, pp. 747–751.
61. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., and Du, H. Y. "Research on the architecture of Internet of Things," in Proc. 3rd ICACTE, 2010, pp. V5-484–V5-487.
62. Windpassinger N. The layered OSI reference model in an ocean of IoT protocols. Internet Of Things (IoT). <https://nicolaswindpassinger.com/osi-reference-model>. Published 2021. Accessed January 15, 2021.
63. Windpassinger N. IoT will be defined through these six layers... Internet Of Things (IoT). <https://nicolaswindpassinger.com/iot-stack-heading>. Published 2021. Accessed January 15, 2021.
64. Vermesan O, Friess P. Digitising The Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds. Denmark: River Publishers; 2016.
65. Nolle T. Understand how to apply SOA for IoT. IoT Agenda. <https://internetofthingsagenda.techtarget.com/feature/Understand-how-to-apply-SOA-for-IoT>. Published 2021. Accessed January 15, 2021.
66. Ray P.P. A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences. 2018;30(3):291-319.
67. Government to strengthen security of internet-connected products. GOV.UK. <https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products>. Published 2020. Accessed January 19, 2021.

68. Bray O. UK Government eyes up new legislation for “smart” products | Lexology. Lexology.com. <https://www.lexology.com/library/detail.aspx?g=13aa751f-cf55-4e29-8557-2a3d15ff40d2>. Published 2021. Accessed January 19, 2021.
69. Hashim A. Ring Neighbors App Vulnerability Exposed Users’ Precise Location Data. Latest Hacking News. <https://latesthackingnews.com/2021/01/19/ring-neighbors-app-vulnerability-exposed-users-precise-location-data/>. Published 2021. Accessed January 20, 2021.
70. How to Hack Your Alexa using a Voice Command-SQL Injection | Hacker Noon. Hackernoon.com. <https://hackernoon.com/voice-command-sql-injection-hack-uncovered-for-alexa-9914x3zwp>. Published 2019. Accessed January 20, 2021.
71. Protego Labs. Alexa SQL Injection Hack Into Unsecured App.; 2021. <https://www.youtube.com/watch?v=KwzxojpgPqI>. Accessed January 20, 2021.
72. Sharpened Productions. Smart Home Side-View.; 2021. https://cdn.techterms.com/img/lg/smart_home_1162.jpg. Accessed January 20, 2021.
73. Chang Z. Iot Device Security Locking Out Risks And Threats To Smart Homes. Trend Micro Research; 2019. https://documents.trendmicro.com/assets/white_papers/IoT-Device-Security.pdf. Accessed January 20, 2021.
74. Winder D. Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach. Forbes. <https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/?sh=7387fc74411c>. Published 2019. Accessed January 20, 2021.
75. Kabalci Y, Kabalci E, Padmanaban S, Holm-Nielsen JB, Blaabjerg F. Internet of Things Applications as Energy Internet in Smart Grids and Smart Environments. Electronics (Basel). 2019;8:972.
76. Mokhtari, Ghassem & Anvari-Moghaddam, Amjad & Zhang, Qing. (2019). A New Layered Architecture for Future Big Data-Driven Smart Homes. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2896403.
77. Guidelines Related to Security in Smart Factories (Part 6) MITRE ATT&CK. Trend Micro. <https://www.trendmicro.com/us/iot-security/news/6036>. Published 2020. Accessed January 27, 2021.
78. MITRE ATT&CK® Navigator. Mitre-attack.github.io. <https://mitre-attack.github.io/attack-navigator>. Published 2021. Accessed January 28, 2021.
79. OWASP Internet of Things. Owasp.org. <https://owasp.org/www-project-internet-of-things/>.

Published 2018. Accessed January 30, 2021.

80. UL's IoT Security Rating Helps Demonstrate Product Security to the Marketplace. UL. <https://www.ul.com/news/ul%27s-iot-security-rating-helps-demonstrate-product-security-marketplace>. Published 2020. Accessed January 30, 2021.
81. Bradbury D. Google announces switch-off date for Android Things. Itpro.co.uk. <https://www.itpro.co.uk/mobile/google-android/358210/google-announces-switch-off-date-for-android-things>. Published 2020. Accessed January 30, 2021.
82. Best IoT Operating Systems. G2.com. <https://www.g2.com/categories/iot-operating-systems>. Published 2020. Accessed January 30, 2021.
83. IoT, IIoT, ICS: definitions, similarities and differences – IKARUS Security Software. Ikarussecurity.com. <https://www.ikarussecurity.com/en/security-news-en/iot-iiot-ics-definitions-similarities-and-differences/>. Published 2019. Accessed February 1, 2021.
84. Neagle C. Smart refrigerator hack exposes Gmail account credentials. Network World. <https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html>. Published 2015. Accessed February 1, 2021.
85. LinkedIn Learning. Ethical Hacking: Hacking Iot Devices.; 2019. <https://www.linkedin.com/learning/ethical-hacking-hacking-iot-devices>. Accessed February 12, 2021.
86. Pentest Partners LLP. Hacking with Chromecast and Alexa | Pen Test Partners. Pentestpartners.com. <https://www.pentestpartners.com/security-blog/hack-demo-video/hacking-a-home-and-a-car-with-chromecast-and-alexa/>. Published 2021. Accessed February 24, 2021.
87. Peters J. MITRE ATT&CK Framework: Everything You Need to Know. Inside Out Security. <https://www.varonis.com/blog/mitre-attck-framework-complete-guide/>. Published 2020. Accessed February 25, 2021.
88. BlueBorne Attack - GeeksforGeeks. GeeksforGeeks. <https://www.geeksforgeeks.org/blueborne-attack/>. Published 2018. Accessed March 8, 2021.
89. McArdle B. The Life Cycle of a Compromised (Cloud) Server. Trend Micro. <https://blog.trendmicro.com/the-lifecycle-of-a-compromised-cloud-server/>. Published 2020. Accessed March 8, 2021.
90. Yan Y. Side Channel Attacks on IoT Applications. https://research-information.bris.ac.uk/ws/portalfiles/portal/210500367/Final_Copy_2019_03_19_Yan_Y_PhD.pdf

Published 2019. Accessed 09, 2021.