Cyber Security of Smart Homes: Development of a Reference Architecture for Attack Surface Analysis

K. Ghirardello*, C. Maple*, D. Ng†, P. Kearney§

**CSC, WMG, University of Warwick, UK. {K.ghirardello.1, cm}@warwick.ac.uk; †Cyberowl, UK. daniel.ng@cyberowl.io; §Birmingham City University, UK. Paul.Kearney@bcu.ac.uk*

Keywords: Smart Home, Reference Architecture, Internet of Things, Attack Surface.

Abstract

Recent advances in pervasive computing have caused a rapid growth of the Smart Home market, where a number of otherwise mundane pieces of technology are capable of connecting to the Internet and interacting with other similar devices. However, with the lack of a commonly adopted set of guidelines, several IT companies are producing smart devices with their own proprietary standards, leading to highly heterogeneous Smart Home systems in which the interoperability of the present elements is not always implemented in the most straightforward manner. As such, understanding the cyber risk of these cyber-physical systems beyond the individual devices has become an almost intractable problem. This paper tackles this issue by introducing a Smart Home reference architecture which facilitates security analysis. Being composed by three viewpoints, it gives a high-level description of the various functions and components needed in a domestic IoT device and network. Furthermore, this document demonstrates how the architecture can be used to determine the various attack surfaces of a home automation system from which its key vulnerabilities can be determined.

1 Introduction

The Internet of Things (IoT) is rapidly gaining momentum in a variety of different industries, promising to change the manners with which people work, live and interact with technology. With both ubiquitous and cloud computing becoming increasingly widespread and relevant, it is no surprise that many multinational technology companies have entered the Smart Home market by releasing Smart Home control points (i.e. Google Home, Amazon Echo, and so on) and cloud platform services (such as Amazon Web Services). In fact, it is estimated that by 2020 the total number of employed Smart Home devices will reach approximately 12.8 billion units [1], while, according to Jupiter Research, the global revenue generated from Smart Home services will amount to $71 billion by the end of 2018 [2]. As such, future home environments are set to accommodate a sundry of new internet connected devices which perpetually collect data on their surroundings and take action accordingly through the use of remote servers, where the information is processed, stored and interpreted.

While there are clear benefits to Smart Homes, such as remote control of home functions and efficient energy consumption, there are also major concerns regarding their security that must be addressed [3]. The introduction of a variety of IoT devices into a Personal Area Network (PAN), in fact, necessarily leads to an increase of the attack surfaces that may be exploited by malicious hackers [4], which is especially worrisome considering the high number of average vulnerabilities associated with the most popular IoT products [5]. Moreover, the absence of widely adopted guidelines related to how Smart Home devices are to be designed and assembled has created a myriad of products that follow proprietary standards. This commonly leads to the creation of heterogeneous residential networks in which it is difficult to assure the security and privacy of consumers [6], particularly when different cloud services are interacting with each other [7, 8]. On the other hand, as businesses have a priority of minimizing costs and releasing their product to the public as quickly as possible [9], an insufficient amount of resources is being devoted to ensuring that products and services are secure by design. There is, therefore, a critical need to understand the cyber risk of Smart Home networks beyond the individual devices and in the context of the entire system.

This paper proposes a high level reference architecture which maps Smart Home products and services to facilitate security analysis on residential IoT systems. It comprises multiple viewpoints through which a home automation network can be defined, each of which was chosen to detail the processes that enable IoT cloud platforms, the elements that compose Smart Home devices and networks and the methods through which device communication and interaction are possible. This architecture enables the creation of a detailed account of the crucial vulnerabilities associated with the different Smart Home attack vectors, thus allowing IoT developers and manufacturers to recognize the ecosystem in which their product or service will operate and identify its attack surface.
The remainder of this paper is organised as follows. Section 2 summarises other IoT reference architectures that were considered in the development of the one presented in this paper. In Section 3 the derived Smart Home reference architecture is presented, divided in its three viewpoints and components. Section 4, then, explains the way with which the architecture may be used in determining a residential IoT

network's attack surfaces. Finally, a summary and conclusion round up the paper in Section 5.

2 Related Work

A number of different reference architectures have been developed in the IoT domain, either to generalize its various applications or to specify a particular type of implementation. The IoT-A reference model [10] and the ISO/IEC IoT reference architecture (IoT RA) [11] represent high level, multi-dimensional architectural frameworks which are decomposed into various architecture views to give an all-encompassing understanding of IoT systems. Both documents aim to provide a starting point for the development and deployment of system specific architectures and thus represent very general descriptions with little detail on the actual interactions between certain components within specific Views. The Industrial Internet Consortium has likewise produced a reference architecture [12] which takes on a similar approach as the previously mentioned examples, delineating five separate viewpoints concerned with distinct topics of interest, and while it does present a more granular portrayal of IoT systems, it was conceived exclusively as an architecture for Industry 4.0.

Numerous IT companies have also produced reference architectures for their own IoT platforms. Indeed, Intel IoT [13], Microsoft Azure IoT Hub [14], Amazon Web Services [15] and IBM Watson IoT Platform [16] are accompanied with documentation of the inner workings of their services. Compared to the more general IoT-A model and IoT RA, these reference architectures offer a vastly more detailed explanation of the back-end components of the cloud with their relative connections and interactions, furthermore allowing different cloud services to interact with one another. While these characteristics are of great importance for a Smart Home reference architecture which facilitates security analysis, the diversity in technologies and applications adopted by these IoT solutions has resulted in dissimilar architectures which are dependent on each service's specifications. Moreover, these architectures do not offer multiple viewpoints, as they present a combination of different concepts which would be described separately in models more similar to the ISO/IEC IoT RA.

Exclusively for domestic environments, the SmartThings reference architecture [17] depicts the structure behind the open platform developed by SmartThings Inc., which connects Smart Home devices to the cloud and provides communication among all connected devices. Unfortunately, this architecture presents many of the problems of the precedent models, since it is unable to clearly specify the way with which the cloud functions and it lacks the multiple viewpoints that describe the entire system.

3 Smart Home Reference Architecture

This Smart Home reference architecture aims to give a layered description of domestic IoT systems, providing a comprehensive understanding of smart device behaviour and interactions through multiple viewpoints. Each viewpoint is furthermore deconstructed into components, which serve a specific purpose and interact with other components in its viewpoint. The viewpoints were chosen by dividing the smart home ecosystem in three essential components: Services, Devices and Connections. As such, the following were delineated:

The **Functional Viewpoint**, concerned with the functions that enable IoT devices, their structure and interactions.

The **Physical Viewpoint**, concerned with the physical components of the of the Smart Home ecosystem.

The **Communication Viewpoint**, concerned with the technologies that enable devices and cloud platforms to interact.

These viewpoints should not be considered separate and independent from one another, but specific perspectives that work together in conjunction. Having scrutinized a multitude of cloud platforms and IoT devices, the resulting architecture is vendor-neutral and not dependent on specific types of technologies or information. Furthermore, its high level of abstraction and modular nature, given how not every viewpoint component must be present in a specific implementation of a domestic IoT system, allows it to be applicable to a wide variety of Smart Home systems.

3.1 Functional Viewpoint

The Functional Viewpoint highlights the necessary functions needed for a Smart Home ecosystem to operate correctly. The IoT network is divided into six functional layers, each with a generic range of capabilities, which can be further divided into functional modules that serve more specific purposes critical for the layer they reside in.

3.1.1 Edge Layer

The Edge layer presents the functions that allow smart devices to interact with their surroundings. It is responsible for the observation of an environment, the creation of data relative to such environment and its manipulation according to the information extracted from the data. Because it deals with the physical world, this layer is necessarily implemented through tangible devices to be located in a consumer's household.

Sensor. Sensing is the function with which a piece of hardware can determine the parameters of its environment and convert it into a digital signal, which is then processed in order for the system to understand the state of said environment.

Actuator. Actuators are components of the IoT system which can control and manipulate the real world. It receives a control signal which is then converted into an action, such as

switching a light off, turning a boiler on or activating a speaker.

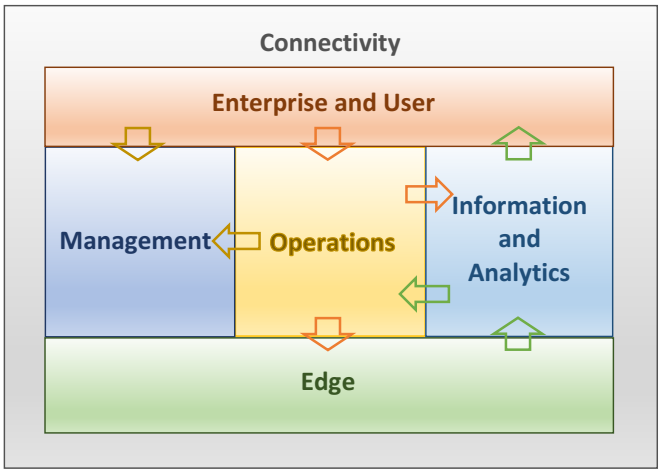

Figure 1: Functional Layers of the Smart Home System. Green arrows represent data flow, orange control flow and yellow management flow.

3.1.2 Connectivity Layer

The Connectivity layer is tasked with the integration of cloud services in smart devices. With many smart devices not holding the capability to process, store and analyse collected data locally, this section of the system connects a local network of devices to the Internet, where the IoT cloud services can be accessed.

Residential Gateway. This component allows a local area network (LAN) to connect to a wide area network (WAN). A residential gateway manages information flow by receiving data from various sources and standardizing it to a form which can be handled by the Internet. Also, to ease the workload of cloud providers, these components may also be provided with certain capabilities such as data aggregation, filtering and transformation.

Cloud Gateway. Comparable to how a Residential Gateway enables smart devices to connect over the internet, the Cloud Gateway is responsible for the safe flow of data from the Wide Area Network to a cloud provider and vice versa. It therefore enables the connection of multiple devices, normalizing their data flow and permits the back end to further process the information it receives, while also allowing to receive and send information to third party cloud providers, which is the primary method through which heterogeneous IoT devices can communicate. In order to enable a secure form of communication to and from the system, Cloud Gateways are provided with a firewall which blocks any form of data that does not meet distinct predetermined policies. Furthermore, a Cloud Gateway will enact both device authorization and authentication through the help of the Device Identity module.

3.1.3 Information and Analytics Layer

The Information and Analytics layer is composed of the set of functions necessary for the correct and secure handling of gathered data. This layer also interacts with the Operations and Management layer by supplying it with the necessary information for the system to make decisions in a timely fashion, and with the Enterprise and User layer by presenting data on connected smart devices to end-users, application developers or internal departments of the same enterprise.

Data Flow and Transmission. This module is tasked with the rapid and efficient transfer of data within the cloud to its individual components. As the cloud gateway identifies and authenticates data into the system, data streams are then channelled in order to facilitate the transportation of such information to either be stored, analysed or processed to start a chain of actions. As cloud platforms are typically required to connect to a vast number of geographically dispersed devices, this module may employ load balancers to distribute traffic into multiple data streams across many processors, storage units, etc. By segregating data according to information contained in the application protocol header, the cloud provider can increase its reliability of service and minimize its downtime. The type of data it may handle include *telemetry*, generated by a device's sensor, *device metadata*, which is information relative to a specific IoT device, and *alerts and actions*, which may be incurred when Smart Home devices present the capability of pre-processing data at the Edge.

Data Analytics. The Analytics module utilizes Machine Learning and Big Data analytics to extract vital information from raw, unstructured data. Therefore, the cloud utilizes the entirety of a device's telemetry data, often supported by data from secondary sources, to uncover particular patterns that may be instrumental in the service provided by the back end. The Analytics module can process data either in bulk, when real-time analysis is not required, or streaming, when an associated cloud service will continuously receive and immediately process high volumes of time constrained data, applying decision making to the transient data flows. As the Analytics module receives and processes data from the Storage module or Data Flow and Transmission module, it then interacts with the Logic and Rules module, where further actions are taken depending on the resulting intelligence received.

Storage. Once data is received by the cloud service, the Storage module is tasked with its safe and persistent storage within the system to facilitate cloud analytics and service orchestration. This data can either originate from the devices themselves, from third-party cloud services or, in the case of processed data, from the Analytics module. Device originated data that is not telemetry, such as device identity and metadata, will generally not be handled by this module, rather by the Device Management and Device Identity and Registry modules.

3.1.4 Operations Layer

The Operations Layer represents the set of functions which apply domain logic, rules and models. It receives processed data from the Information and Analytics layer and, depending on its value, takes the required actions. Alternatively, it receives direct commands which must be executed from the Edge or Enterprise and User layer.

Logic and Rules. The Logic and Rules module represents the collection of domain logic functions which aim to enforce specific business functionalities of the IoT cloud service. It receives the normalized or analysed telemetry data and generates actions based on predefined rules. Additionally, the Logic and Rules module will include the set of functions which determine what commands are given to devices in order to operate their actuators, and application logic, which enables the use of User Interfaces and API.

3.1.5 Management Layer

The Management layer is responsible for the continued operation of IoT services associated with smart devices, representing the set of functions devoted to device provisioning, monitoring and control.

Device Management. Device Management includes the set of functions which assure that IoT devices safely and properly make use of a cloud's services. These includes device provisioning, which refers to the process of registering new devices into the IoT system, device configuration, which allows users to set up their device with specific attributes, device monitoring and software/firmware updating.

Device Identity and Registry. This module stores the information needed for each connected device to be fully functional and able to utilize cloud-based services. Device Identity contains cryptographic material and attributes used by the Cloud Gateway module to authenticate incoming flows of data, while the Device Registry stores information, different from the records present in the Device Identity, about devices that the cloud provider may access, control and manage. Ordinarily, these two components are kept separate in order to ensure low latency the device-cloud communication by limiting the amount of information associated with the Device Identity and to prevent the Device Registry to contain critical key or cryptographic material

3.1.6 Enterprise and User Layer

The Enterprise and User layer represents the set of functions managed by a business that enable smart device consumers and third party services to gain access to cloud applications, functionalities and collected/analysed data through a common interface. Furthermore, through this layer businesses are able to implement their own domain logic in the Cloud layer.

APIs. An Application Programming Interface (API) is a set of methods and functions which promote communication between various software programs. In the context of a Smart Home network, APIs expose a cloud's information and services for the public to utilize, enabling third party developers and business partners to produce pieces of software dependent on key elements of the IoT cloud. This module represents the primary manner with which smart devices communicate with different cloud services or devices. Furthermore, it connects to the Storage or Data Analytics module through Data Flow and Transformation, since information must first be standardized before leaving the cloud platform, and to the Logic and Rules module when commands to be executed are received.

User Interface. While APIs are generally created for application developers, the User Interface (UI) represents the main point of access to IoT services and information for the end user. As ordinary consumers are not assumed to be technically proficient, a focal point of these interfaces is to ensure that they are intuitive and easy to use. Through this component, end users are able to register new devices by sending the necessary information to the Device Management module (which subsequently will update the Device Identity and Registry), control their device by directing commands to the Logic and Rules module and monitor it by receiving either real-time data (live streaming from smart security camera) or processed and analysed information. While UIs predominantly employ APIs to operate, there are some which communicate directly with the cloud service. Whether smart devices are devoid of a built in interface or are large enough to accommodate one, the main method of implementing UIs is through mobile and web applications. In other cases, such as with the Amazon Echo and Google Home, smart devices may exist solely to provide a centralized user interface for many other smart devices and cloud services.

Business Domain. The Business Domain module represents the gateway through which business decisions can affect the normal functioning of the cloud services and associated products. Being connected to the Logic and Rules component, it is able to alter the network's domain logic, reshaping its existing characteristics or adding new features to the cloud. Also, it is responsible for the release of new software and firmware updates to each connected device, thus triggering specific functionalities in the Device Management module.

3.2 Physical Viewpoint

The Physical Viewpoint of the Smart Home reference architecture aims to delineate a residential IoT system through the technological components necessary for the implementation of the functions described in the previous viewpoint. It therefore presents the required pieces of hardware and software to be used for the collection, transportation and processing of data, with subsequent commands being created and directed to specific components. Other than the functions delineated in the previous viewpoint, there are a multitude of system requirements that the Physical Viewpoint must also take into account, such as computational constraints, low latency data transmission, low energy consumption, interoperability of dissimilar technologies, etc.

Since the detailed presentation of each variation of IoT technology is a time consuming process outside of the scope of this document, this Physical Viewpoint rather describes the general tools that either interact with an environment and transmit data or that enable other devices to interact and communicate in an environment.

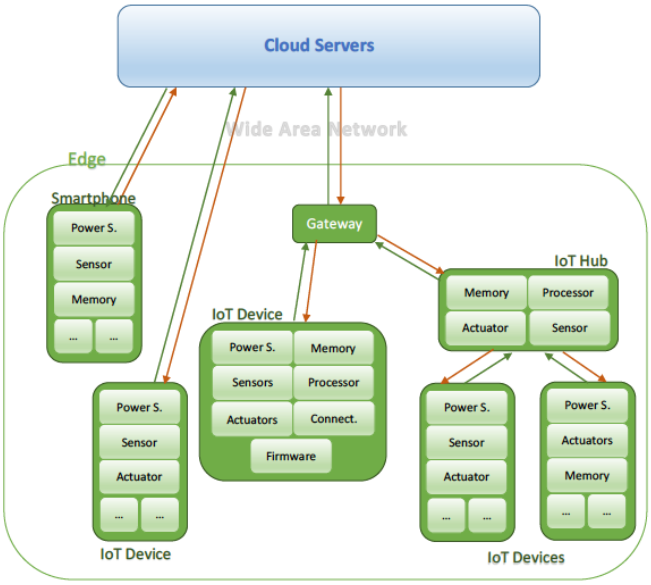

Figure 2: Physical viewpoint of a Smart Home System.

3.2.1 Components

In this viewpoint, a device can be broken down in the following components: sensors, actuators, processors, memory, power sources and firmware. These components don't all necessarily have to be present for the piece of technology to be considered an edge device.

Sensors. Being the component which implements the sensing function from the Functional Viewpoint, a sensor detects changes or events in its environment, converting analogue signals to electric ones and sending them to other electronic components. Other than ensuring that a sensor does not actively interact with the entity it is observing, it is typically important that the generated readings are as accurate as possible.

Actuators. As with sensors, actuators are the physical implementation of the actuation function from the Edge Layer, thus taking action or controlling a specific entity of interest. They receive commands directly from a user interface or indirectly through sensor data processed either locally or, more commonly, through the cloud. A single actuator can either operate independently or in conjunction with other actuators to provide a more complex set of state changes to a physical entity. Common examples of actuators are loudspeakers and power switches.

Processors. These components are responsible for the interpretation of data produced by sensors and third parties and the consequent enactment of control logic. This process ranges from very simplistic, such as perceiving and altering a room's temperature, or extremely complex, in which case Machine Learning and Artificial Intelligence techniques may be involved. Although certain IoT technologies do present edge computing (i.e. local processors) to decrease the processing load of remote systems, most devices rely on cloud processing almost exclusively.

Memory. Memory can either be volatile or non-volatile. Volatile memory is generally used in aiding the normal activity of a processor, retaining data and information that is currently being used. Non-volatile memory permanently stores information, even after its power source is removed. This kind of memory is often used in smart devices that seek to store sensor data locally, either as back-up or to be uploaded to the cloud in bulk at a later time.

Power Source. This component is responsible for providing electrical devices and appliances with enough power to ensure their ordinary operability. A Power Source may be included in a piece of technology either through portable batteries or direct mains electrical power supply. This component is particularly important in determining the mobility of the considered device.

Firmware. This component is comprised by the class of software used to control and monitor hardware components while being able to receive, read and transform data signals. It bridges the digital world with the material one by abstracting common computing resources and allowing digital signals to be converted into motion. For any IoT device able to connect to a cloud platform, it is of central importance that the Smart Home system can frequently update device software to patch bugs, fix vulnerabilities and add new functionalities.

3.2.2 Devices

The following represent the types of devices present at the end user's residence that compose the Smart Home Local Area Network.

IoT Smart Devices. Known as the "*things*" of the Internet of Things, IoT devices are the physical objects with non-computing primary functions, that is they are able to sense and/or interact with an environment and can connect to a network over which they transfer data and receive commands. These may range from security cameras, lightbulbs and door locks to fridges, dishwashers and kettles.

IoT Hubs. IoT hubs are designed to provide a central controller that can connect a multitude of smart devices. These can be homogenous or heterogeneous hubs. The first kind is generally produced by the same company that produces the IoT devices it is able to connect to and, therefore, are generally required for the normal functioning of the connected devices. This is common for especially small IoT devices which alone are not able to connect to the WAN or cannot process the data it produces. Heterogeneous hubs

connect a multitude of different devices and enable them to communicate with each other. They usually come with their own application which allows the consumer to control all connected technology through a single portal.

Residential Gateway. Residential Gateways are customer-premises equipment that connects IoT devices with the Internet. They are the physical implementation of the Residential Gateway functional module, thus they receive data from connected devices and translate it into the suitable communication protocol. In certain cases, Residential Gateways may integrate some of the functionalities of IoT hubs, providing local data pre-processing and analytics or two-way device communication without the need to connect to a cloud server.

Smartphones/Tablets/Computers. These are devices whose primary functions are computing related, which, in the context of the Smart Home system, include providing to an end user a way through which IoT devices can be monitored and controlled. While not generally considered IoT smart devices, smartphones occupy a particular position in these networks, since they also include sensors, such as microphones and accelerometers.

3.3 Communication Viewpoint

The Communication Viewpoint describes the communication protocols employed to enable IoT devices to receive and transmit information to other devices and cloud services. Being a crucial element of any Machine-to-Machine network, these protocols determine the manner with which data is encoded, formatted, and transported from host to host. This viewpoint draws from the Internet Protocol Suite (TCP/IP) to categorize the various used protocols in four abstraction layers, each of which provides a number of functions needed for device networking, making use of layers below and providing services to the ones above. Therefore, a Smart Home system will employ a stack of protocols in which lower layers are logically closer to the physical transmission of data, while higher layers deal with more abstract data, being logically closer to application programs.

3.3.1 Link Layer

The lowest layer of the TCP/IP model, it defines the technology through which data is physically transmitted through the system. This layer connects sensors, actuators, devices and other edge nodes, regulating how information is transformed in electrical or radio signals, depending on the kind of network connection capabilities of the device. Furthermore, the link layer is responsible for receiving data from the Internet Layer and encoding IP packets/data into frames, which include source and destination MAC addresses, a Frame Check Sequence which checks for transmission errors for the frame and a Preamble that synchronizes the receiving of frames.

Wi-Fi. Being present in all homes with a wireless router, a vast number of smart device manufacturers currently create devices which utilize this protocol. It supports high bandwidth frequencies, around 2.4 and 5 GHz, and high data rates of hundreds of bits per second. While these specifications are optimal for video streaming and file transfers, they imply higher power consumptions, thus smaller, battery-provisioned IoT devices may not be best suited for Wi-Fi connections. Also, being a fairly well supported protocol, it is not uncommon for domestic Wi-Fi networks to include a number of different devices (IoT and not) competing for bandwidth, which results in their slower response times and higher latency.

Ethernet. As with Wi-Fi, Ethernet is similarly a protocol implemented or supported by many residential LANs. It sports some of the highest data rates possible, with extreme cases going up to 10 Gbps, and without the problem of bandwidth interference, it represents one of the most reliable communication protocols at this layer. On the other hand, being a wired solution implies that its connected devices must be stationary and connected to an Ethernet port.

IEEE 802.15.4. Defined in 2003 by the IEEE 802 working group, 802.15.4 represents a communication standard for low data rate wireless personal area networks (LR-WPAN) for devices using low-complexity, short-range radio frequency transmissions [18]. Compared to the more power intensive WI-FI, it operates on bandwidths that generally span from 868/915 MHz to 2.4 GHz, with transfer rates between 20 and 250 Kbps. This standard is targeted for devices with very low manufacturing costs and simplistic architectures, therefore needing a form of communication with low power consumption.

Cellular. Cellular communication protocols are the set standards which enable certain devices to communicate over a long distance. Though dependent on the specific protocol used, cellular communications generally support high data rates (around 600kbps to 10Mbps for 3G, 3 to 10Mbps for 4G) and frequencies that go from 800 to 2600MHz.

3.3.2 Internet Layer

The Internet Layer is tasked with the routing of data to the correct destination which is specified through an identification, such as the IP address for the Internet Protocol. It determines the fastest route through which a message can be received and, in case the selected route presents any sort of issue, it selects alternative routes. The Internet Layer receives data from the Transport Layer and sends data to the Link Layer.

IPv6. The Internet Protocol version 6 (IPv6) is the latest form of the Internet Protocol, which is the principal protocol used in the Internet Layer. It is responsible for delivering data packets by the IP address present in the header of the datagram. This protocol was created to address a core

problem present in the previous version (IPv4), that is the limited amount of addresses that it is able to provide. In order to bridge the IPv6 technology to unsupported wireless networks of devices with low power consumption and processing abilities, such as BLE, the *IPv6 Low Power Wireless Personal Area Network (6LoWPAN)* is commonly used. Moreover, these low-power networks often present frequent topology changes and lossy radio links, resulting in an environment in which routing packets becomes challenging. To that end, the *IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL)* is used to reactively create a graph of nodes which determines the optimal path through which data can be transferred.

3.3.3 Transport Layer

The Transport Layer provides host-to-host communication, delivering information to the target application program. As the Application Layer normally processes data streams rather than datagrams, this layer ensures that data is received by the host in the appropriate order and, through an error detection code, that it has not been corrupted or lost. The Transport Layer is also responsible for the control of data flow: it, in fact, determines if a host's data buffer is able to handle the amount of data it needs to receive.

TCP. The Transmission Control Protocol (TCP) is a connection-oriented protocol, meaning that it creates a connection between a sender and receiver which is maintained active until all required messages have been sent. Even if any problem is incurred in the Link or Internet Layers while transferring data, TCP enacts a series of procedures that guarantee that the information is received intact: a sender keeps track of all packets sent with a timer and waits for the receiver to respond with an acknowledgment message. If the timer stops and no such message is received, the sender then re-transfers the "lost" packet. It is one of the central protocols of the Internet Protocol Suite, being used by applications such as the World Wide Web, email correspondence and video streaming.

UDP. Compared to TCP, the User Datagram Protocol (UDP) uses a much simpler method to transmit data, which does not check whether packets have been received by an end host, or whether they arrived in the correct order. Thus, UDP represents a less reliable Transport Protocol than TCP, possessing only data integrity capabilities through checksum algorithms. On the other hand, the simplified datagram-transfer process results in a faster connection with lower latency and protocol overhead, which makes UDP a more appropriate protocol for applications that can tolerate some data loss without affecting their service.

3.3.4 Application Layer

The Application Layer represents the highest layer of the TCP/IP stack, where communication is standardized for network processes. Here protocols directly interact with applications, allowing them to make use of the functionalities provided by the lower layers. Since there are numerous Application Layer protocols depending on the application they interact with, this document presents some of the more relevant for their implementation in Smart Home environments.

MQTT. The Messaging Queuing Telemetry Transport (MQTT) protocol is a lightweight communication standard designed for resource constrained, low bandwidth networks. It employs a publish/subscribe in which edge nodes publish information to a broker that, in turn, conveys such information to selected clients according to the topics to which they are subscribed. Also, the broker is capable of buffering information in case a device disconnects from the network, allowing it to receive it the moment it reconnects. As a lightweight protocol, it is suitable for monitoring a large number of devices without having severe performance implications to a network's bandwidth.

AMQP. The Advanced Message Queueing Protocol (AMQP) is an open-source standard that supports various middleware messaging applications, allowing different systems to communicate independently of their internal specification.

CoAP. The Constrained Application Protocol (CoAP) allows resource-constrained devices to interact with the Internet, enabling IoT and Machine-to-Machine applications. As with MQTT, CoAP is applied in lossy networks with low-powered devices where the network requirements are low message overhead and contained data size transfers, while it differs from MQTT in the fact that it does not require an underlying reliable Transport Layer protocol, as it runs over UDP. Also, CoAP is a one to one protocol that supports one-to-many or many-to-many multicast message delivery.

XMPP. Initially created for instant messaging and presence information, the Extensible Messaging and Presence Protocol (XMPP) is a decentralized messaging protocol with near real time exchange of data between network nodes. It presents a set of core protocol standards to specify its client-server messaging, while a set of XMPP extensions can broaden its implementation. For IoT specifically, XMPP can define the structure of the retrieved device data, provides a relatively lightweight middleware (although not to the extent of MQTT and CoAP) and is federated, thus allowing device interoperability.

DDS. The Data Distribution Service (DDS) is a publish/subscribe communication standard which presents distributed processing – directly connecting sensors, devices and applications to each other without any dependence on centralized IT infrastructure.

HTTP/HTTPS. The most widely deployed protocols on the internet, the Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) are less suited for IoT applications because of the length of messages transmitted and short-lived device connections it would create.

3.3.5 Other protocols

Although the previously defined list provides a solid basis to outline a Smart Home communication network, there are a number of widespread standards that either are based on a group of the described protocols (ZigBee, Thread), employ their own proprietary protocols (BLE, Z-Wave) or operate through different pieces of technology (X10, UPB, Insteon).

BLE. Bluetooth Low Energy (BLE) supports frequencies (2.4GHz) and connection ranges (50-150 meters) similar to previous Bluetooth versions. What it improves on its predecessor is the fact that it consumes a very contained amount of power. Hence, this protocol is better suited for devices that do not require a constant connection to back-end servers, but rather that transmit low amounts of data at specific points in time, disabling the connection as soon it is not required to conserve power.

ZigBee. Based on the 802.15.4 wireless standard, ZigBee is a communication protocol with a 2.4 GHz radio frequency, 100-meter range and supported data rate of 250 Kbps. If configured correctly, it has the potential to be one of the most secure residential communication protocols, since it uses the same encryption technology used by international banks and financial institutions. Being a mesh network protocol, ZigBee counts 3 types of devices in its network: a controller which coordinates the network composition, a router that extends the network's range and end-devices. As each device can be used as a router, end devices here do not need to communicate directly with a central hub.

Z-Wave. Closely related to ZigBee, Z-Wave is a protocol specifically created for home automation purposes. It is likewise based on mesh network technology with a central control hub, which can configure and manage the network. With low data rates that reach at most 100 Kbit/s, Z-Wave offers low-latency communication among a long list of supported devices, all of which can communicate and interact with each other. This protocol runs on a lower than usual 908.42MHz frequency, which ensures that the network does not experience interference from technologies which use higher bands and that there are fewer devices on that frequency.

Thread. Specifically designed for home automation, Thread is a low power open source protocol based on IEEE802.15.4, IPv6-6LoWPAN and UDP. As such, it is able to interact with other IP-based standards (unlike ZigBee and Z-Wave) and handle up to 250 power-constrained devices, making it a complementary protocol to WI-FI for home automation.

X10/UPB. The oldest protocol created for Smart Home devices still in use, X10 employs a house's electrical wires to transmit signals representing digital information to any of the millions of supported devices. However, it suffers from very slow command/information transmission and is quite limited in terms of the amount of data transmitted at a time. The Universal Powerline Bus (UPB) can be considered the next version of the X10, being a peer-to-peer powerline communication protocol with greater reliability and faster data transmission rates. Its main downside is the fact that, while it supports a considerably higher number of connected devices at a time compared to the X10, it has far fewer compatible devices. Both protocols offer relatively low bandwidth, no encryption capabilities and must be implemented into a house by technicians. Lastly, these protocols are not designed to grant the connected devices Internet access.

Insteon. Insteon uses both wireless and wired technology to provide a dual-mesh network of various devices that each independently transmit and repeat data signals, allowing it to support a large number of nodes at a time. Furthermore, by being able to send signals over both wired and wireless options, it represents one of the best options for reliable connectivity.

4 Smart Home Attack Surface

The multiple viewpoints presented in this Smart Home reference architecture offer a comprehensive, high-level overview of a domestic IoT network. With the actual realization of such systems frequently resulting in notably idiosyncratic and heterogeneous structures, the modular nature of the presented architecture allows it to be applied to Smart Home ecosystems which may vastly differ on an ad hoc basis, being heavily influenced by such factors as available technology and device compatibility with previously installed technology. As a result, both small and large scale home automation networks can be outlined, given the absence of implicit structural restrictions on the number of devices and back-end services that may be represented. Figure 3 depicts a particular Smart Home implementation, where Functional, Physical and Communication Viewpoints are presented together.

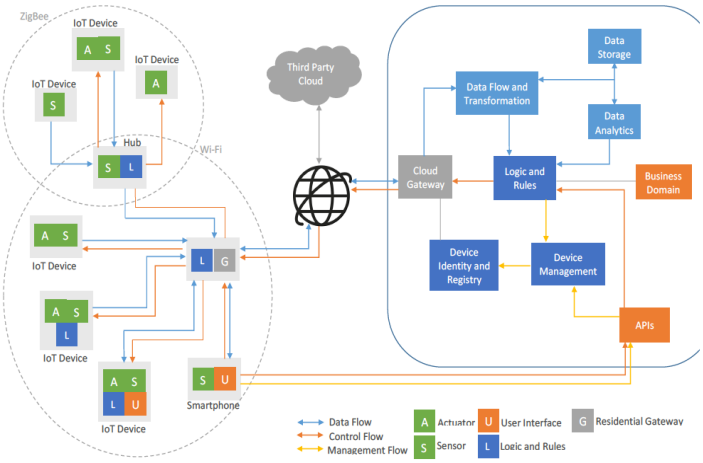

Figure 3: Smart Home architecture example with the three viewpoints merged

In this structure the Edge presents a series of different IoT Devices connected to a router directly through Wi-Fi or indirectly through an IoT hub. Each device with a sensor produces data as it observes its environment and uses its connection to a router to send it to the remote Cloud servers. As data reaches the cloud through the Cloud Gateway, it is further transferred to the Storage, Analytics or Logic and Rules component. If this last module creates a device actuation command, it is forwarded to the Cloud Gateway, which then connects to the Residential Gateway and sends the command to an Actuator. In case the created command involves a device or service not managed by the same cloud platform, which is often the case in Smart Home environments, then APIs may be used to connect to the appropriate Third-Party Cloud. Alternatively, devices with the Logic and Rules module may make certain control decisions locally, without the need to connect to remote servers.

By clearly illustrating the various processes, devices and data/control flows pertaining to a Smart Home network, a straightforward assessment can be made of the particular elements or areas critical to the overall functioning of the system and of the many pathways and entry points malicious attackers may exploit to compromise said system. As such, a stakeholder may employ the proposed reference architecture to determine the attack surface of Smart Home products and services, which is crucial to systematically identifying relevant threats for each component and interaction, generally achieved by adopting a threat categorization such as STRIDE. Not only would this assist engineers and system designers to implement security by design in their products, but furthermore allows them to determine how secure a certain piece of technology is in the context of the network it resides in.

To clarify the preceding paragraph, the following example is proposed. Utilizing the architecture present in Figure 3, a security analysis on the represented system might start with the residential gateway, as it is the main entry point to the considered Home Area Network. While these are provisioned with firewall filtering capabilities, a possible way of compromising it would be to physically tamper it (T in the STRIDE classification): attackers with physical access to the network, in fact, may be able to alter its settings, creating new device pairing requests and installing custom SSL certificates. This would allow the network's traffic to be redirected to alternative servers owned by the attackers [19]. As residential gateways are responsible for connecting IoT devices to the cloud, telemetry data may be read and specific control commands may be redirected. Furthermore, a compromised residential gateway would have several other implications to the security of the system. Figure 3, in fact, shows that a ZigBee network is connected to the residential gateway through a IoT hub. As many of these devices continuously generate network traffic to check for firmware updates without any form of encryption or authentication, an attacker may be able to carry out a man-in-the-middle attack and compromise the hub's firmware [19].

Additionally, the reference architecture is able to briefly approach security analysis through the supply chain of consumer IoT devices and services. For products, in fact, Section 3.2.1 details the necessary components that make up the devices at the Edge, while Section 3.3.1 lists the possible communication protocols that said devices may employ. In such manner the complete Smart Home attack surface will consider possible vulnerabilities present in the core elements of consumer products. On the other hand, the supply chain for services can be examined through the Functional Viewpoint, which details the inner processes through which cloud platforms collect data and implement application and domain logic.

5 Conclusion

With the Internet of Things recently surfacing into the public view, a variety of novel devices have emerged to compose ever-more complex and heterogeneous Smart Home networks, for which understanding their inherent cyber risk has become a challenge. This paper seeks to represent such systems through a high-level reference architecture that maps IoT products and services. It is comprised of three viewpoints, namely the functional viewpoint, which introduces the functions that enable Smart Home technology, the physical viewpoint, which presents the different elements that compose domestic IoT devices and networks, and the communication viewpoint concerned with the communication protocols associated with these cyber-physical systems. Each viewpoint is further decomposed into modular components which allow the reference architecture to be applied to a range of different Smart Home implementations. The paper then illustrates that the combination of the three viewpoints gives a detailed enough understanding of these systems, outlining its most important components and connections, to be used to determine its attack surfaces, through which the system's vulnerabilities may be categorised.

Acknowledgements

This paper is produced as part of the PETRAS project "Security and Performance in the IoT Smart Home" (SPIoTSH), which is in collaboration with the IoT Security Foundation (IoTSF), the Building Research Establishment (BRE) and CyberOwl.

References

[1] Gartner, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016" (2017). Available at: https://www.gartner.com/newsroom/id/3598917

[2] Juniper Research, "Smart Home Revenues to Reach $71 Billion by 2018, Juniper Research Finds" (2014). Available at: https://www.juniperresearch.com/press-release/smart-home-pr1

[3] C. Maple, “Security and privacy in the internet of things.”, *Journal of Cyber Policy,* **2(2)**, pp. 155–184 (2017).

[4] I. Lee, K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises.” *Bus. Horiz.* **58**, pp. 431–440 (2015).

[5] Hewlett Packard, “HP study reveals 70 percent of Internet of Things devices vulnerable to attack.” (2014) Available at: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VOTykPnF-ok

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, 2002a. “A survey on sensor networks.” *IEEE Commun. Mag*. **40 (8)**, pp. 102–114 (2002).

[7] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of things (IoT): A vision architectural elements and future directions", *Future Gen. Comput. Syst*., **29 (7)**, pp. 1645-1660, (2013).

[8] L.M. Kaufman, “Data security in the world of cloud computing”, *IEEE Security and Privacy Magazine,* **7**, pp. 61–64 (2009).

[9] Accenture, “Igniting Growth in Consumer Technology.” (2016) Available at: https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf

[10] M. Bauer et al., “Iot reference architecture.” In *Enabling Things to Talk*, pages 163–211. Springer, 2013

[11] F. Carrez et al., “IoT-A Deliverable D1.5 – Final Architectural Reference Model for the IoT v3.0”, *ISO/IEC CD* 30141:20160910(E) (2013). Available at:https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf

[12] S.-W. Lin et al., “Industrial Internet reference architecture,” Industrial Internet Consortium *(IIC)Tech. Rep.*, (2015). Available at: https://www.iiconsortium.org/IIRA-1-7-ajs.pdf

[13] Intel, “The Intel IoT Platform”. Available at: https://www.intel.co.uk/content/www/uk/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html

[14] Microsoft, “Microsoft Azure IoT Reference Architecture” (2016). Available at: https://azure.microsoft.com/en-gb/updates/microsoft-azure-iot-reference-architecture-available/

[15] Amazon Web Services, “AWS IoT Documentation,” (2016). Available at: https://aws.amazon.com/de/documentation/iot/

[16] BM, “IBM Edge Delivery Services” (2017). Available at: https://www.ibm.com/msen/marketplace/global-network-for-online-workloads.

[17] SmartThings Inc., “SmartThings API Documentation.” (2015) http://docs.smartthings.com/en/latest/ref-docs/reference.html.

[18] “IEEE Standard for Low-Rate Wireless Networks", (2016).

[19] M.B. Barcena, C. Wueest, “Insecurity in the Internet of Things” (2015). Available at: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf