Securing Our Future Homes:

Smart Home Security Issues and Solutions

Nicholas Romano

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2019

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial fulfillment of the requirements for graduation from the Honors Program of Liberty University.

____
Robert Tucker, Ph.D.
Thesis Chair

____
Wade Schofield, M.S.
Committee Member

____
Jillian Ross, Ph.D.
Committee Member

____
David Schweitzer, Ph.D.
Assistant Honors Director

____
Date

Abstract

The Internet of Things, commonly known as IoT, is a new technology transforming businesses, individuals' daily lives and the operation of entire countries. With more and more devices becoming equipped with IoT technology, smart homes are becoming increasingly popular. The components that make up a smart home are at risk for different types of attacks; therefore, security engineers are developing solutions to current problems and are predicting future types of attacks. This paper will analyze IoT smart home components, explain current security risks, and suggest possible solutions. According to "What is a Smart Home" (n.d.), a smart home is a home that always operates in consideration of security, energy, efficiency and convenience, whether anyone is home or not.

Securing Our Future Homes:

Smart Home Security Issues and Solutions

Introduction

The Internet of Things (IoT) is the interconnection between two or more devices that can interact on some sort of network. In the past decade, the development of IoT has drastically changed how millions of people live their lives, how companies conduct business and even how militaries defend countries. People no longer need to go outside to start their car, get out of bed to turn the AC or heat up or even drive their own car. Along with improvements in technology, come the challenges posed by security threats, from which the field of IoT finds no cover. More specifically, the Internet of Things is facing huge security threats in the area of smart homes. Smart homes will be analyzed, security issues will be explained and possible solutions for the future will be discussed. According to Ali, Dustgeer, Awais and Shah (2017), "The smart home is the fastest growing field of IoT technology, and it provided innovative, intelligent, ubiquitous and interactive services to users using different operations. Due to internet connected, dynamic and heterogeneous nature, smart homes create new security issues and challenges" (p. 2).

Smart Homes Background

Fifty years ago, a smart home was nothing but the mere imagination of what the distant future held. Rapidly growing technology has changed that cloudiness of a dream into a clear reality that is evolving every day. In the near future, modern homes will be buttonless, switchless and wireless. User input via voice commands and hand gestures will be the new way of controlling all types of devices throughout the house. Smart technology is not only a reality, but becoming very common amongst all types of households, even in forms one would not expect. IoT first began in the 1980s at Carnegie Mellon University where students developed an internet connected Coke vending machine that would tell the developers if enough soda was cold enough for them to quench their thirst (NortonOnline, n.d.). Since that invention, IoT has expanded beyond imagination, landing right into the very place people spend the most time, their home. Before diving into security issues and solutions, it is important to define what exactly is a smart home. Schiefer (2015), of the *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, defines a smart home as “a thing, whose main functionality is extended with networking abilities to create a new one. The additional infrastructure for those devices, like a base or control station, falls also in Smart Home” (p. 115).

Along with smart home technology, comes the task of securing these new technologies. With further advancement in the smart home field, there will be more problems to face. The ultimate goal is to use smart home applications and devices without worry; however, in today’s age this is a bothersome problem. From privacy concerns to malfunction and security breaches, users are forced to secure their devices themselves to a certain extent. For security analysts and engineers to solve current and future security issues, they must ask themselves what motivations an attacker might have. One should note that attackers who choose to attack IoT devices would most likely be extremely knowledgeable and experienced in the technology. According to “Securing Smart Homes” (2016),

> Unlike PCs and smart homes, IoT devices – at least those available in the market right now – don’t all run on a single operating system. This difference makes it more challenging for interested people to launch attacks on a wide scale. Compromising the security of such devices would also require a bit of knowhow and the right tools. (para. 2)

Although the focus of this paper is smart home security, comparing business IoT device security gives additional perspective to home security. According to “Almost Half of Companies Still Can’t Detect IoT Device Breaches” (2019), only forty eight percent of businesses are able to detect if their IoT devices have been breached. If almost half of companies using IoT devices cannot detect breaches, it is plausible to imagine a much higher percentage for smart home owners unable to detect breaches.

Smart Home Architecture

In order to analyze aspects of smart home security, one must understand smart home architecture. Abdur, Habib, Ali and Ullah (2017) say, “A smart home consists of four parts: service platform, smart devices, home gateway, and home networks” (p. 384). A service platform is simply the service provider that delivers internet bandwidth to the home; examples include Comcast, Verizon and Lumos. Smart devices are any device in the home that can connect to the internet via an IP and MAC address. These devices connect on the home network, which is usually created with a wireless router and access points throughout the house. The wireless router connects to a modem, which serves as the home gateway, or a bridge between the home network and service platform.

According to Kang, Moon and Park (2017), every smart device has its own architecture as well, including an application layer, framework layer, module core library and Linux kernel layer, which can be modified based off of the operating system being used. The application layer includes applications that can be run on multiple smart devices. For example, Netflix runs on the application layer since it is available on tablets, smart TVs, etc. The application framework includes libraries and managers to monitor activity, package managers and install managers. The module core library stores the individual functions unique to the smart device. This includes middleware, I/O configuration and display. Lastly, the Linux kernel layer is responsible for executing the most basic functions, including the file system, network settings and drivers for the device. Kang et al. (2017) also explain current techniques for smart home security, before proposing a new architecture:

> firmware validation and update scheme […] performs ID-based authentication between devices in a smart home environment and uses the key derivation algorithm for firmware image distribution. To verify the integrity of firmware image, it uses a hash chain. Firmware image is used as an input of the hash chain and is fragmented. The scheme transmits the pieces fragmented by firmware fragmentation, and put the transmitted pieces to the hash chain for verification. (p. 4)

Firmware is simply the software programmed in the IoT device that is in read only mode and cannot be changed unless the manufacturer pushes an update. The hash chain is the method in which keys are produced to uniquely identify the IoT device. This is an important aspect of device security because this enables manufacturers to push out the latest updates and patches to device firmware. Other architectures focus on different aspects, for example, privacy. These architectures focus on defense at the network level so that messaging remains secure and encrypted. Another important architecture focuses on smart home communication. Kang et al. (2017) explain an example of this: an encryption algorithm that applies AES256, which is an ephemeral Diffie-Hellman key exchange and hash function. There is a central hub where all messages being transmitted are monitored and each message is encrypted by three separate algorithms, generating a hash key. This ensures that each message remains secure and private. With unencrypted messages, an attacker can view text in plain sight with tools such as Wireshark that can view TCP/IP packet information, the protocols used to send information over the network from device to device.

Lack of Security

Unfortunately, most IoT devices connected in a smart home are not equipped with sufficient security software. The lack of security on each device poses many threats, including threats to the CIA triad: confidentiality, integrity and authenticity. Attacks on a smart home can be categorized as passive or active attacks. In a passive attack, the attacker attempts to obtain information from the home, but not modify the smart device. Attackers can monitor smart home traffic using traffic analysis and sniffing tools such as Wireshark. These types of attacks are more difficult for engineers to detect simply because system data is not altered. In contrast, active attacks attempt to modify data or operation of one or more devices in the smart home. Common types of attacks include denial of service, malicious software and message modification. According to Komninos, Philippou and Pitsillides (2014), “A message modification attack, involves the alteration of the contents of a legitimate message or the delaying or reordering of a stream of messages, aiming to produce an unauthorized effect” (p. 1937).

To categorize security attacks, the United States Federal Government uses a standard called FIPS 199 (Komninos et al., 2014). A low-level attack has a limited adverse effect on the system, moderate level attacks have a significant affect, and high-level attacks have a severe or catastrophic adverse effect on the smart home. Table 1 depicts common possible threats and categorizes them based on level of impact.

Energy consumption reporting in smart homes is important for smart grids to provide the proper data and information to the smart home system. According to Komninos et al. (2014), a system is vulnerable to eavesdropping attacks during data transmission to the EMS, a smart grid component, allowing the attacker to learn about the homeowner’s lifestyle. Different devices in a smart home leave different signatures in data loads. For example, a smart refrigerator leaves a different signature than a smart lighting system in the home. With this information, an attacker can infer which devices are on and when they are turned on. This information becomes valuable to the attacker over time, as they can plan to physically attack the house through robbery by learning tendencies of the homeowner and deciphering when they are home or not from IoT device footprints. Komninos et al. (2014) explain that attackers also can modify messages that falsify energy consumption, making the homeowner pay for energy usage they never really used.

Table 1.

Impact Levels by Threat

Possible Threats	**Security Compromised**	**Degree of Impact**
Eavesdropping	Confidentiality	L-M
Traffic Analysis	Integrity	
Message Modification	Authenticity	
Replay Attack		
EMS Impersonation		
Repudiation	Non-repudiation	M
Message Modification	Integrity	
Replay Attack	Authentication	
Tampering	Authentication	L
Illegal Software Modification/Update	Integrity	
Customer Impersonation	Integrity	L-H
Device Impersonation	Non-repudiation	
	Authentication	

Note. Adapted from "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," by N. Komninos, E. Philippou & A. Pitsillides, 2014, *IEEE Communications Surveys & Tutorials*,*16*(4)

Hardware limitations present a major problem for IoT smart home device security. Most IoT devices are limited in terms of CPU, memory and energy output. This directly relates to security at the confidentiality level. According to Maple (2017), "The largest physical layer packet in IEEE 802.15.4 is 127 bytes. Given that the frame overhead could be 25 bytes, the maximum frame size in the media access control level is 102 bytes" (p. 166). Encryption can be applied, but link-layer security would reduce the maximum frame size even more. If the encryption standard, AES-CCM-128 were used, 21 bytes would be filled, leaving only 81. Using AES-CCM-32 would fill 9 bytes, leaving only 93. It is evident that choosing an encryption standard to ensure confidentiality is challenging, given the limits associated with each standard, specifically with a public key. All IoT devices leave a digital signature when communicating on a network, which requires a public key. Using a public key requires CPU and memory power, which is beyond many systems' capability, especially those sending and receiving data frequently.

Authentication is one of the most important aspects of IoT device security; however, this area is also at risk. If an attacker is erroneously authenticated as a legitimate user, he or she can access private data that compromises either the confidentiality, integrity or availability of the device or entire smart home system. Usernames and passwords are the most common forms of authentication; however shared keys, digital signatures and biometrics are becoming more common. The goal of authentication is to eventually eliminate the need for usernames and passwords since these are easy for attackers to crack. Single sign on (SSO) is being looked at as a viable option, but the systems needed for SSO are not fully adaptable for IoT devices; nevertheless, OAuth2 may eventually allow SSO once it is adapted (Maple, 2017). The reason SSO is so difficult to implement is because IoT devices are so diverse in their authentication methods and login requirements. This is due to manufacturers conflicting policies and implementation of login requirements for devices. On the other hand, OAuth2 is an industry standard that enables third party applications access to user accounts and controls permissions based on the account. This allows manufacturer customization since OAuth2 is an open standard.

Hardware issues are also linked to authentication problems. Sometimes updating firmware on an IoT device is simply not possible, due to system architecture and patching methods. IoT system architecture is still new in the realm of computing, so sometimes developers are not able to release patches. They are forced to simply create another version of the product or implement security at another level, such as the network level. For devices that can receive patches and updates, many users have no information on when to update, how to update, and where to check for updates. This has been a major concern for manufacturers shipping products such as smart refrigerators, something many owners would never think of as needing an update.

DDoS Botnets

One reason attackers are attracted to IoT devices is for their use in botnet armies. Botnets are a collection of potentially thousands of Internet connected computing devices controlled by a botherder or botmaster often used for Distributed Denial of Service (DDoS) attacks. Due to the ever-growing presence of IoT devices, attackers can assemble large armies. PC owners usually have antivirus or malware software installed on their computer that can prevent their takeover by the botmasters. Most IoT devices simply do not have such protection. Without the owner’s knowledge, a smart refrigerator, toaster, lighting system or speaker may be part of a botnet army being used in a DDoS attack on another person or company. Many home internet users never change the default router username, “admin”, and password, “password”, on their router, virtually allowing anybody to enter their network. At the end of 2014, a botnet of home routers was used to interrupt and temporarily disable Sony and Microsoft gaming networks on Christmas day, where millions of users experienced outages, so attacking smaller businesses with less security proves to be easier (Schiefer, 2015).

Developer Issues

One of the largest reasons for IoT device security issues traces back to development. IoT Security Foundation explains how manufacturers of these smart devices are more concerned about shipping out vast numbers of devices to buyers, to avoid losing competition, than with security. The security firm Auth0 carried out a survey in which eighty-five percent of developers admitted to being rushed in application development to get their product on the market (Dickson, n.d.). Another study, led by the firm SEC, showed that millions of IoT devices were using shared SSH and HTTPS keys, practically giving attackers a way in (Dickson, n.d.).

Another issue with development is the fact that different manufacturers use different security standards for IoT devices, especially when it comes to encryption techniques, network protocols and data field types. When different standards are used on various IoT devices in a home, there is room for error in data movement and validation, network packet sending and receiving and a myriad of other conflicting issues that can compromise security. IoT-based standards and societies have yet to regulate security standards at every OSI model layer to provider more efficient security to the end user. According to Bauer, Burkacky and Knochenhauer (2017), “The IoT lacks well-established overarching standards that describe how these different parts of the technology stack should interact. Instead, large players and industry organization use their own solutions” (para. 9). Another developer issue links back directly to manufacturing requirements. In the United States there are no minimum requirements for smart devices in terms of cyber security. Due to this, many manufacturers are faced with a dilemma. Jabil (2018) explains, “If the cost of adding a data security chip outweighs the value the company will gain for the added feature, the designer will not add it to the product. Similarly, if the end user is not willing to pay more for a high-security device, the manufacturer [will most likely not implement such security]” (para. 11).

A prominent issue in the IoT community lies within the question of who is responsible for security: the manufacturer or the consumer. Currently, there is a lack of balance. In some cases, the manufacturer sells a product well suited for the smart home environment, leaving the consumer too little or no configuration options. In other cases, the manufacturer makes a great product with endless capabilities, but lacks security, and the consumer is responsible for implementing other security systems to protect their investment in their newly purchased product. Zurkus (2019) explains, “[Consumers] will increasingly hold device manufacturers accountable for security practices in their development and production processes as threat actors continue to target connected devices” (para. 12). This imposes pressure on manufacturers to meet the consumer’s needs without having overarching standards to follow.

Common Issues and Attacks

Passive and active attacks come in many forms. A very common one among smart homes is eavesdropping. In this type of attack, an attacker monitors the traffic coming in and out of a network by using tools such as Wireshark. To protect against this attack, private data and communication must be encrypted so that the traffic cannot be viewed in plain text. In masquerading attacks, “an attacker can pick up certain unauthorized benefits professing to be an alternate legal user. The attacker may imitate an unauthorized home user and thereby gain access to the smart home internal network system remotely…” (Rehman & Manickam, 2016, p. 4).

In replay attacks, the attacker essentially captures messages between two legal entities, but then later sends the same message, in an effort to mimic one of the legal entities (Rehman & Manickam, 2016). This is used to obtain access to whichever service the messages were coming from.

Probably the most well-known type of attack is malicious code. Attackers enforce harmful code on the internal network or system of a smart home and exploit any known vulnerabilities. This can include controlling devices remotely, accessing user data, viewing what the user sees and falsifying information (Rehman & Manickam, 2016). In this type of attack, the user is usually not aware, making it very effective.

To protect against these types of attacks, firewalls, intrusion detection systems and intrusion prevention systems are implemented to control network traffic and authentication before packets can enter the smart home gateway. Firewalls, IDSs and IPSs are critical because they control network traffic before packets are authorized to reach their destination. Network and security administrators can create custom rules and filters that capture traffic based on packet headers and can detect different types of attacks such as DDoS.

Another common attack on smart home devices is a sleep deprivation attack, which is where energy constrained devices are forced to keep their nodes awake, resulting in battery loss, which is executed by forcing many tasks in a 6LoWPAN environment (Khan & Salah, 2018). This allows for the attacker to slowly drain the power of IoT devices and falsify energy usage, as previously stated. The solutions implemented to stop these types of attacks are securing the network layer and control station of these devices. There are various ways manufacturers are doing this, starting with encryption techniques such as those previously discussed.

It is important to note that security issues are not always related to an attack, but can be directly related to the manufacturer itself. In a study where various smart home devices were tested, a smart television was turned on and used for fifteen minutes, and in that time a traffic analyzer showed seven-hundred different connected IP addresses (“Smart Homes,” 2018). Another tested product was a Philips Bluetooth electric toothbrush, very suspiciously requiring location access and records audio, where further investigation yielded that the toothbrush data was being sent to over twenty sources including marketing companies (“Smart Homes,” 2018). These are just two small examples; larger scale items like the Amazon Echo already leave many consumers concerned. This is a huge grey area that has no current solution. Security and privacy standards must be set in place to ensure what is considered ethical data collection.

A surprising, yet common issue in smart home device security can be tied to domestic abuse. Research at the University College London was conducted to explain how domestic abuse relates to these smart devices. Common devices in a smart home include cameras, motion and audio detection, which are usually as accessible as just downloading an app on any phone. The study showed that men were more statistically prone both to purchase the smart home devices and to be the perpetrators in domestic violence cases (“Smart Homes,” 2018). IoT devices can even aid in domestic violence because some devices allow for harassment and stalking. A man or woman can monitor their partner’s every move, force home system settings to their own liking and even change home entry permissions so that the other person cannot enter the home. While smart home devices do not cause domestic violence, in many ways they can be used to facilitate domestic violence in terms of monitoring partner activity at many levels. A solution to this type of “attack” is education. Users of IoT devices must know all risks associated before blindly purchasing or using these devices. It is important to note that domestic abuse and smart home IoT device use are not always related, yet they can be.

In 2014, there was a reported case where family members were harassed through a baby monitor; the monitor had a camera with its own IP address feeding the video to special software equipped with two-way audio (Schiefer, 2015). Unfortunately, the camera had a firmware vulnerability and an attacker took control of the baby monitor. Schiefer (2015) explains that an analysis was presented at a 2013 Black Hat convention on smart home cameras. Many of the cameras were so insecure that the attacker was able to modify the image presented on the connected software. Other analyses completed at this convention showed cloud-based solutions that had not implemented any standards or had very poor encryption for communication. This means data could be read or manipulated in plain sight on traffic analyzing software (Schiefer, 2015). These are but a few examples of how far attackers can go.

Many researchers have warned of a potentially more dangerous threat in the future of smart homes. Many people know of the attacks on Iranian and Ukrainian power grids, but these types of attacks are moving towards smart buildings, including homes.

The attacks carried out on Ukrainian power grids in 2015 used malware to attack the Industrial Control Systems (ICS) (Winder, 2019). Smart homes utilize Building Automation Systems, which can be prone to the same types of attacks. The researchers found vulnerabilities in authentication, cross-site scripting and file deletion. This study focused on smart buildings that businesses use, but smart homes are adopting the same technology.

In order to solve these problems that are clearly resulting in "real-life" attacks, experts should give input on what needs to be improved. One of the security experts said:

> In a previous job, I definitely had security officers that were all asking me about quantum computers and insisting on AES-256 because they were going to get hacked imminently. And while that may well be an issue in the future, it's really not an issue now. The issues now are really very basic: don't have a default password, don't let a device respond when it's directly connected to the internet; make sure that you can upgrade with security patches when critical flaws are found. (Mutschler, 2009, para. 4)

Mutschler (2019) continued to explain that some of the other basic areas that need to be covered are secure boot, memory protection and encrypted firmware. When another expert was asked about what should be done that is not being done yet, he explained that there is still a lot of software exposure; the software written to exchange data between devices in a smart home simply is not being written securely enough for the future. An important noted point was that attackers can easily buy inexpensive devices, open them up and explore the physical components to get a better idea of how to attack the weaknesses.

Current Solutions

Although IoT devices need to make vast improvement in terms of security, there are still many effective methods that manufacturers use. The most common type of symmetric encryption is AES128, specifically used for communication of data between devices. Sharing keys requires asymmetric encryption which is helpful; asymmetric keys are pairs of public or private keys that decrypt or verify each other (“Security for IoT Devices and Communication,” 2019). This technique uses ECDH, Elliptic CurveDiffie-Hellman, to generate the shared keys, which is very efficient in terms of CPU processing power (“Security for IoT Devices and Communication,” 2019). This is a great technique at the IoT device level. This is because the device’s size only allows for limited processing power capabilities, which limits motherboard and hardware component usage. However, between symmetric and asymmetric encryption, symmetric is much faster for authentication purposes, making it a difficult choice for developers to choose which one to use (“Security for IoT Devices and Communication,” 2019).

Hash algorithms are used in data integrity, a key component of data collection in IoT devices. Algorithms such as SHA256 produce hash values that are encrypted by a private key (“Security for IoT Devices and Communication,” 2019). Anybody with the public key, which is digitally signed by a Certificate Authority, can check if the data has been tampered with; this is commonly known as a digital signature (“Security for IoT Devices and Communication,” 2019).

Blockchain Solutions

Blockchain technology has been extensively adopted in finance and banking, where it is used in all types of cryptocurrency. In simplest terms, blockchain can be thought of as a giant spreadsheet shared over the internet that is continually updated based off of transactions all over the world, or a shared database that has no complete ownership. Moreover, blockchain is a great technology to be used in security as well. The first use of blockchain technology is allocation of address space. Currently, IPv6 address space is 128 bits, however, blockchain has a 160-bit address space (Khan & Salah, 2018). This could be used in public key hashing, generated by an algorithm known as ECDSA (Elliptic Curve Digital Signature Algorithm) (Khan & Salah, 2018). With a 160-bit address, there is space for 1.46 * 10^{48} IoT devices, which could help solve the problem of companies redundantly using public keys for digital signatures; in perspective, that would be 4.3 billion more addresses than IPv6 currently allows (Khan & Salah, 2018).

All IoT devices need to be tracked whether it be personal ownership details, make, mode, serial number or location of the device. Currently, the manufacturing company is responsible for keeping this data and maintaining all aspects of the CIA triad. Implementing blockchain technology would essentially eliminate this responsibility. Since blockchain is able to track e-commerce transactions, it would serve just as an important role in IoT registration and monitoring. According to Khan and Salah (2018) “Blockchain can be used to register and give identity to connected IoT devices, with a set of attributes and complex relationships that can be uploaded and stored on the blockchain distributed ledger” (p. 406). This is sufficient for all stages of the IoT device’s lifecycle.

Attributes include information such as the vendor, supplier and distributor (Khan & Salah, 2018).

As previously mentioned, authorization and authentication of smart home IoT devices is most often used by protocols such as OAuth2, OpenID, OMA DM and LWM2M. The problem with using these protocols is once again, that there is no industry standard. Blockchain can serve as a solution in this area as well. Khan and Salah (2018) explain how blockchain can implement smart contracts that are able to provide authentication to multiple parties for IoT devices. Blockchain logic ensures privacy by setting access rules and conditions. These smart contracts specify which users have the rights to access the device and its data, update and patch the software and hardware and change ownership of the device (Khan & Salah, 2018). Blockchain smart contracts could essentially combine the multiple protocols into one central method.

Protocols related to communication between IoT devices and the smart home's network are at risk too; however, blockchain can also aid in this area. Protocols such as HTTP, MQTT, and XMPP and asymmetric key pair, which all are connected on the blockchain network, would not be needed since blockchain would handle all protocol needs (Khan & Salah, 2018). Blockchain is much more lightweight and consequently less CPU and memory intensive. According to McLean (2019), a survey of businesses that use IoT devices showed that only three percent of respondents did not want to use blockchain security. Although this survey was conducted using IT businesses, it is plausible that smart home device manufactures share the same or a similar mindset regarding how useful and efficient blockchain technology is.

IoT Kaa Solution

A well-developed possible solution for smart home IoT devices is IoT Kaa. Chifor, Bica, Patriciu and Pop (2018) explain this system: it is a cloud platform with a web interface where users can generate code for multiple programming languages, making implementation scalable depending on the device. Kaa provides messaging systems between devices on the IoT network within a home, so authentication takes place on the cloud in Kaa's system (Chifor et al., 2018). Behind the scenes, a JSON formatted command is sent to the IoT device from the cloud. Once the device receives the message, it replies back with a FIDO authentication request that includes a header, challenge, transaction and policy (Chifor et al., 2018). FIDO, or Fast ID Online, is a standard that uses multifactor authentication and public keys to authorize clients; however, unlike other standards, the key is stored locally on the host. Each field is responsible for a different action, but in this case, the transaction field is responsible for authentication. Once the response is validated by FIDO, the device executes the command issued by the user. During the FIDO authentication process, an internal database is searched for the associated FIDO public key (Chifor et al., 2018). In this type of system, the device authenticates the user. Message integrity is guaranteed in this type of solution during transmission. Still, since the cloud logs all messages to a database, that information must be protected. This architecture proposes the following:

> [A] pair of ECC keys are generated and the public key can be retrieved via a CoAP URL. The same process is executed at the controller side and the public keys are exchanged during the device imprinting stage. Every message exchanged

> between the controller and the device is encapsulated in a cryptographic datagram which has a lightweight structure with a series of fields encoded using a type-length-value method. The message payload is encrypted with a symmetric algorithm and a new key is generated for each message. The symmetric encryption key is then encrypted with the ECC public key and all the data is encapsulated in a datagram which contains the following fields: Protocol version, Asymmetric cryptographic algorithm identifier, Symmetric cryptographic algorithm identifier, Encrypted symmetric key [and] Encrypted payload. (Chifor et al., 2018, p. 745)

ECC keys are essentially public keys developed through algebraic modeling of elliptic curves, while CoAP is a protocol that allows IoT devices to connect to a network and communicate with each other. This experimental protocol was simulated and tested under multiple conditions, with results showing a delay in message receipt; however, there is little impact on smart home applications (Chifor et al., 2018). Architectures similar to this will be vastly important to IoT smart home device security.

Access Control System Solution

Chitnis, Deshpande and Shaligram (2016) propose a system solution in an article outlining background data on system monitoring. This specific solution is for smart home entry, IoT device usage and access control. Chitnis et al. (2016) explain how the proposed system contains a database in which all individual user biometric data is stored. At the time of entry into the house, the system accesses the database for authentication purposes and if matched, the system will allow the user access to the home or single IoT device, whichever the proposed system is connected to. Other options include a smartphone application where users can authenticate themselves with a password, security code or similar technique. In most cases, it is safer if the system authenticates the user rather than the user authenticating the system. The owner or administrator of the system has the rights to add other individuals and permit access. Chitnis et al. (2016) explain that different levels of security should be implemented as well, for example, level 0 may allow the user to enter the home, but level 1, 2 and 3 may permit access to certain devices such as the lighting, thermostat and appliances. Although this proposed solution may seem simple, viable and sufficient, there are challenges involved. Many homeowners are not willing to manage a system in such a way. One would rather pay for a service that takes care of itself. Other challenges include lack of technical knowledge to manage security levels, access control and even system installation which can stem from the unwillingness to learn.

Data and Privacy

One of the most worrisome aspects of smart home security for the average consumer is securing their data and privacy. Jabil (2018) from IoT For All says, “The total number of records breached every second, minute, day and hour nearly doubled from 2016 to 2017. [Gemalto Security’s Breach Level Index] also estimates that more than 9.7 billion records have been lost or stolen in the last five years” (para. 6). If large companies such as Facebook, CNBC and Target are prone to data breach attacks, smart home users certainly are as well. In 2018, Jabil conducted a survey in which sixty-nine participants and manufacturers said their data privacy made them rethink their plans to collect and use the data collected from the smart devices they make. Manufacturers that made consumer grade devices were even more likely to be hesitant about the data usage (Jabil, 2018). Companies are learning that by collecting user data, they are creating a risk for data breaches into their own company. If the data is never there to begin with, there is no reason for the attacker to come looking for it.

Perhaps smart home manufacturers in the United States need to take notes from how the Europeans are conducting business. In May of 2018, the European Union's General Data Protection Regulation took effect, requiring all companies that do online business to take extra precautions to protect user personal data (Jabil, 2018). They need to explain how the data will be used, users must give clear consent for data collection, users may request to have their data deleted and these companies must safeguard all data and notify users if a data breach happens (Jabil, 2018). Jabil conducted a survey following the implementation of these rules, where sixty-two percent of companies said they would be more careful about rules and regulations regarding personal data, after recent media focus on the issue (Jabil, 2018). Fifty-five percent said they would monitor the market to understand what the customer finds acceptable, while forty percent said they would scale back data collection efforts and a large forty percent said they would not implement any data collection plan (Jabil, 2018).

It is important to note that the data collected by these smart home device manufacturers is usually being collected for important reasons, whether it be to solve future device problems, create reports to understand device performance or to recognize supply and demand trends. The problem in the United States is there is not one set of regulations and standards that manufacturers must follow. There are some guidelines in place from individual security companies, but they are not enforced. Unfortunately, the data collected is not always used to directly benefit the user in the ways previously mentioned. According to Jabil (2018), “34 percent of participants plan to connect the big data to retailer databases for cross-selling and branding opportunities, 31 percent want to use the information for marketing [and] 25 percent plan to sell the data to determine supply and demand trends” (para. 15).

Conclusion

Smart home IoT devices can be useful, exciting and amazing technology. With the growing presence of smart homes, these devices will become more common among families and businesses. Unfortunately, due to the early stages of development, incomplete adoption of standards and differing views of data privacy, there are many security problems that manufacturers and consumers must face. Nevertheless, many solutions seem promising, and developers are working steadily towards other security implementations. The key for all users is to educate themselves on smart home products before buying and using them, at any level, whether the product is a baby monitor or smart lighting system. On a development level, the overarching rule of thumb for IoT smart home devices is that every device should support encryption to prevent various types of attacks. Encryption is the barebone for any level of security implementation on smart home devices.

References

Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications,8*(6). doi:10.14569/ijacsa.2017.080650

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. *2017 23rd International Conference on Automation and Computing (ICAC)*. doi:10.23919/iconac.2017.8082057

Almost Half of Companies Still Can't Detect IoT Device Breaches, Reveals Gemalto Study. (2019, January 15). Retrieved January 15, 2019, from https://www.apnews.com/3e5b5f3634f9442b84abca4281477d8b

Bauer, H., Burkacky, O., & Knochenhauer, C. (2017). Security in the Internet of Things. Retrieved January 8, 2019, from https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

Chifor, B., Bica, I., Patriciu, V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems,86*, 740-749. Retrieved January 8, 2019.

Chitnis, S., Deshpande, N., & Shaligram, A. (2016). An Investigative study for smart home security: Issues, challenges and countermeasures. *Wireless Sensor Network,08*(04), 61-68. doi:10.4236/wsn.2016.84006

Dickson, B. (n.d.). You need to worry about your smart-home's security? Retrieved January 8, 2019, from https://www.iotsecurityfoundation.org/why-you-need-to-worry-about-your-smart-homes-security/

Erfani, S., Ahmadi, M., & Chen, L. (2017). The Internet of Things for smart homes: An example. *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*. doi:10.1109/iemecon.2017.8079580

Gupta, P., & Chhabra, J. (2016). IoT based smart some design using power and security management. *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*. doi:10.1109/iciccs.2016.7542317

Jabil. (2018, August 27). Navigating Smart Home Data Security Concerns. Retrieved January 11, 2019, from https://www.iotforall.com/smart-home-data-security/

Kang, W. M., Moon, S. Y., & Park, J. H. (2017). An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences,7*(1), 1-12. Retrieved January 13, 2019.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems,82,* 395-411. doi:10.1016/j.future.2017.11.022

Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials,16*(4), 1933-1954. doi:10.1109/comst.2014.2320093

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy,2*(2), 155-184. doi:10.1080/23738871.2017.1366536

McLean, A. (2019, January 15). Gemalto reports increase in blockchain use for securing the Internet of Things. Retrieved January 15, 2019, from https://www.zdnet.com/article/gemalto-reports-increase-in-blockchain-use-for-securing-the-internet-of-things/

Mutschler, A. S. (2019, January 10). IoT Device Security Makes Slow Progress. Retrieved January 15, 2019, from https://semiengineering.com/iot-device-security-makes-slow-progress/#

NortonOnline. (n.d.). What is the Internet of Things? How the IoT works, and more. Retrieved January 11, 2019, from https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html

Rehman, S. U., & Manickam, S. (2016). A study of smart home environment and its security threats. *International Journal of Reliability, Quality and Safety Engineering,23*(03), 1640005. doi:10.1142/s0218539316400052

Santoso, F. K., & Vun, N. C. (2015). Securing IoT for smart home system. *2015 International Symposium on Consumer Electronics (ISCE)*. doi:10.1109/isce.2015.7177843

Schiefer, M. (2015). Smart home definition and security threats. *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*. doi:10.1109/imf.2015.17

Securing Smart Homes. (2016, November 3). Retrieved January 29, 2019, from https://www.trendmicro.com/vinfo/gb/security/news/internet-of-things/securing-smart-homes#TheUsualSuspects

Security for IoT Devices and Communication. (2019, January 15). Retrieved January 15, 2019, from https://www.eletimes.com/security-for-iot-devices-and-communication

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Sivaraman, V., & Vishwanath, A. (2016). Low-cost flow-based security solutions for smart-home IoT devices. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. doi:10.1109/ants.2016.7947781

Smart Homes: The Big Issues. (2018, September 21). Retrieved January 11, 2019, from https://www.futurescope.co/smart-home-big-issues/

What is a Smart Home. (n.d.). Retrieved January 11, 2019, from https://www.smarthomeusa.com/smarthome/

Winder, D. (2019, January 15). Proof-Of-Concept Malware Reveals Smart Building Vulnerabilities Your Business Needs To Deal With. Retrieved January 15, 2019, from https://www.forbes.com/sites/daveywinder/2019/01/15/proof-of-concept-malware-reveals-smart-building-vulnerabilities-your-business-needs-to-deal-with/#2e21e3951939

Zurkus, K. (2019, January 14). Can Smart Home Leaks Lead to Major Cyberattacks? Retrieved January 15, 2019, from https://securityboulevard.com/2019/01/can-smart-home-leaks-lead-to-major-cyberattacks/