Proceeding of International Conference on Systems Computation Automation and Networking 2019

A Review of Security Challenges in Home Automation Systems

Aditya Chakraborti
B. Tech. Computer Engineering
Mukesh Patel School of Technology Management and Engineering
Mumbai, India
adityachakraborti13@hotmail.com

Aastha Jain
B. Tech. Computer Engineering
Mukesh Patel School of Technology Management and Engineering
Mumbai, India
aasthajain1399@gmail.com

Siddarth Menon
B. Tech. Computer Engineering
Mukesh Patel School of Technology Management and Engineering
Mumbai, India
siddarthmenon28@gmail.com

Prof. Krishna Samdani
Department of Computer Science Engineering
Mukesh Patel School of Technology Management and Engineering
Mumbai, India
krishna.samdani@nmims.edu

***Abstract*—Home Automation is one of the up-and-coming domains of technology that has immense scope in the near future. In the past, home automation has been associated with science-fiction, but now, with advancement in technology, home automation is now a reality. With this reality, also comes problems associated with it. Vulnerabilities in a home automation system when exploited, can compromise the safety of the people living in that house. In this paper, we look at the existing solutions available to improve the security of a home automation system and compare them to decide which solution is better in what context.**

***Keywords*—Home Automation, Security, Network Security, Review**

I. Introduction

A home automation system refers to the electronic control of household features and interfaces. It consists of various sub-systems of devices, sensors, actuators, that can be controlled and communicated with remotely [1]. Some examples would include sensors like wireless sensor networks (WSNs), channel modulators, temperature sensors and devices like lights, fans, televisions, to name a few [3]. Each device communicated with another device within the home automation system through a network connection.

Home automation systems have evolved with progress in technology. From being a central, cohesive model, where all the devices and sensors are coordinated by a single, central controller, smart home systems have moved on to become individual devices and sensors that are connected in an ad-hoc manner [1].

As with any device on a network, a home automation system also faces many susceptibilities which other common devices face, like routing attacks, replay attacks, wormhole attacks to name a few [2]. A secure home automation system would be one that is free from all vulnerabilities, and in turn, this would mean that all the devices used in the system must be protected. Achieving this is an arduous task because nowadays, a home automation system is likely to have devices, sensors supplied from various manufacturers it is likely that most devices use different protocols.

It is obvious that securing home automation networks is vital, and thus in this paper, we look at different solutions proposed by authors to improve the security of the system, and then analyze and compare the suggested solutions to decide which solution works best and the context around these solutions.

In the following sections we have reviewed solutions for security modules in home automation system networks that aim to curb some of the challenges to home automation systems. In section II, we go through the literature review by first looking at how we shall classify the solutions that we came across, followed by the challenges or threats to the home automation security systems and their networks. Then we explore some existing systems, that aim to enhance or solve the network security challenges to home automation systems. Further, in section III, we note our inferences from the systems mentioned and explored in section II, and finally in section IV, we conclude our paper with a jest of what we have learned and how these system would help curb the security challenges to home automation system.

II. Literature Review

In this review paper, we're looking at the already available technologies, or solutions presented to improve the security of home automation systems. Looking at the plethora and variance of the proposed systems, we classified the proposed solutions into two broad categories:

- Software Solutions
- Embedded Solutions

The software solutions refer to those system proposals that only take network security algorithms or any networking protocols in consideration.

@IEEE 978-1-7281-1524-5

On the other hand, embedded solutions envelop those proposed systems that depend on both software and hardware to work. These are full-fledged systems where the authors designed the system architecture, and not only the software that the system would run on.

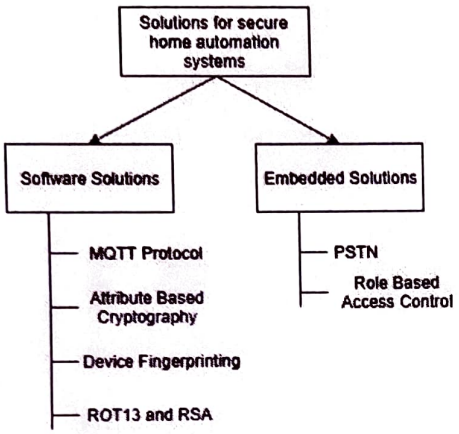

Fig. 1. Classification of solutions for secure home automation systems.

While looking for existing solutions, we identified a paper on the taxonomy of threats to a home automation system [1]. The authors' classified threats into 3 major groups:

- Intentional Threats
- Unintentional Threats
- Malfunctions

In intentional threats, they talk about Identity fraud, denial of service attacks, hijacking of the network and manipulation of information. These are those threats that abuse the use of a system. Here the attacker, might impersonate as a genuine user and gain access to the house, might disrupt the services, or might feed wrong information to the system [1]. All of these conditions may be harmful to the users of the system, and thus, intentional threats must be suppressed by the system.

Unintentional threats and malfunctions, as described by the authors, consists of accidental change or manipulation of data, Information leakage, information from unreliable sources and lack of planning, internet malfunction, communication channel failure, failure of devices or services, power failure, or damage to sensors [1]. These threats are the result of poorly designed security protocols, controls, and algorithms, along with poorly designed or incompatible system architectures.

This paper gave an idea of the threats and risks related to home automation and helped us understand the aim of some proposed solutions for security in home automation systems.

Another system that we came across was a Home Automation system using the MQTT protocol [3]. This system looks to use a popular communications protocol called MQTT. MQTT stands for message queuing telemetry transport. It works in a star topological fashion. There is a central server that is called a broker, and multiple clients. Clients may be subscribed, or may not be subscribed. If any client gets a new piece of information, they send it to the broker, from where the broker sends the information to only those clients that have subscribed to this particular type of information. MQTT is very lightweight and sends plain text. Encryption is done using the TCP/IP protocol [5].

The proposed system employs a couple of NodeMCUs to serve as brokers in the system, and all of the services and sensors serve as clients. They divided the system into 3 modules.

- The data collection unit
- The central processing unit
- The interface unit

The data collection unit would contain all of the sensors to monitor the status of the environment of the house. The data collected by them is sent to the central processing unit using the MQTT protocol. Here, two NodeMCUs do the processing and thus carry out different operations. The interface unit is where the user can look at the readings given by the data collection unit, as well as give commands based on their requirements [3].

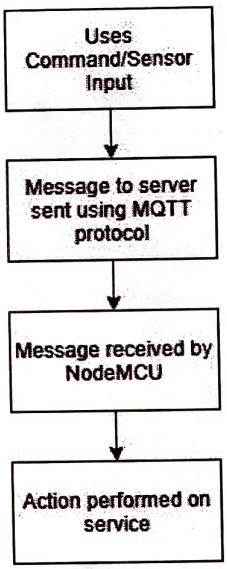

Fig. 2. Block diagram of MQTT based home system.

The MQTT protocol used in the system is likely to reduce errors produced by unintentional threats and malfunctions as the data being sent is very small and would thus rely on external factors for a very short amount of time.

In conclusion, we would like to focus on the MQTT protocol used by the system rather than the system itself, as the protocol can be used independent of the system, and hence we have decided to classify this system as a software solution.

After looking at a protocol used for automation, which did not provide a solution to intentional threats, we looked at a technique that would help secure the system against those.

The paper "ZigBee Security for Home Automation Using Attribute-Based Cryptography" provides us just that [6].

The proposed system uses cryptography to enhance the security of the home automation system against intentional threats. ZigBee in itself is home automation enabling technology with its own security layers. But the security features in ZigBee provide us with a disadvantage that it requires too many keys. The disadvantage of using too many keys is that it results in an increase in the overhead of the system. Thus the memory requirement of the system increases which gradually increases the cost. Also, security in ZigBee is not flexible and does not offer any service that depends on the users i.e. it is very restricted [6].

To overcome these challenges, the authors proposed a new cryptography solution, ABE, over the AES algorithm used in ZigBee. The ABE makes use of a symmetric cryptography module with a 128-bit Advanced Encryption Standard algorithm. The ciphertext policy for encryption consists of five algorithms or steps, as mentioned by the authors [6].

- Setup
- Encryption
- Key Generation
- Decryption
- Delegation

The setup phase would take no explicit input. The only input given to the system would be the security parameter. Using this, the algorithm outputs a public parameter and the master key.

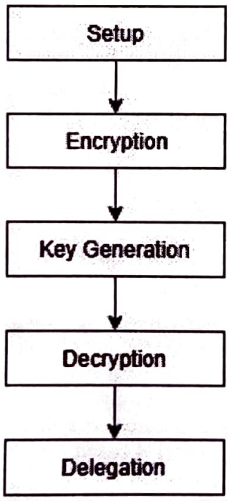

Fig. 3. Block diagram of the attribute-based cryptography algorithm [6].

Now, at the encryption phase, the public parameter, message to be transmitted and the access structure are put in as input to the system. These produce the ciphertext. The ciphertext produces attributes that only the access structure can decrypt. Now that the ciphertext is generated, a key has to be generated. To do this, the master key and the set of attributes is taken to generate the private key. This is how the proposed algorithm encrypts data. To decrypt data, the ciphertext is subject to the public key, and the private key [6].

When the entire process is completed the user gets the decrypted message. But if there is an erroneous transmission of information then the set of attributes and the keys are formulated in a different way thus decryption does not take place and the message is discarded. This is helpful in cases when malicious information tries to pass from one node to the other. The main module in ABE is the access structure. It controls all the attributes of the system and enables efficient encryption and decryption of information [6].

In conclusion, the ABE cryptography algorithm not only increases the efficiency of the system but also reduces the overhead of the usage of a large number of keys. The above system is better than the current cryptography modules being currently used, like public key cryptography and identity cryptography. The ABE technique is better than these two modules in aspects like the number of keys, key escrow. It doesn't have a key directory hence has efficient memory utilization. We shall classify this algorithm under software solutions as the entire proposed solution focusses on an algorithm.

In addition to this, we came across another proposal that focused on device fingerprinting to identify unique, genuine devices that try to access the system [2].

The authors' work utilizes device fingerprinting and legitimate login credentials as a part of a double verification process for the authorized user and their device identification. When a user wants to access the system, they enter their login credentials. The system also takes as input the parameters for device fingerprinting. If the login credentials match, then the device identification algorithm verifies the device. If the device after verification is found to be in the "whitelist", then the client device is allowed access to the system. Otherwise, if the device is found to be in the "blacklist", then the device is blocked from accessing the system. And, if a device is not in both, the "whitelist" or the "blacklist", then the client device will have to be verified by some other means, like sending an OTP to the user via SMS. If the user is verified, then the client device will be added to the "whitelist", otherwise, it will be added to the "blacklist" [2].

The authors considered various approaches for Remote Physical Device Fingerprinting before settling for fingerprinting using JavaScript, Flash, and Geo-Location. They listed out all of the browser and device specific parameters which their algorithm uses to identify unique devices. All of the listed device parameters add to the uniqueness of a device and thus are used as parameters to formulate that device's fingerprint. The parameters used by them are:

- User Agent Parameters
- Screen Parameters

- Lesser Bit Parameters
- MIME Parameters
- Plugin Parameters
- Date Object Parameters
- Geo-Location Parameters
- Flash Parameters
- System Fonts

The whole idea of using these parameters is that a client's device specific screen parameters will remain constant over time [2].

These parameters and validations would protect the system against intentional threats. The authors even suggested using a hash function to encrypt the device parameters for added security [2].

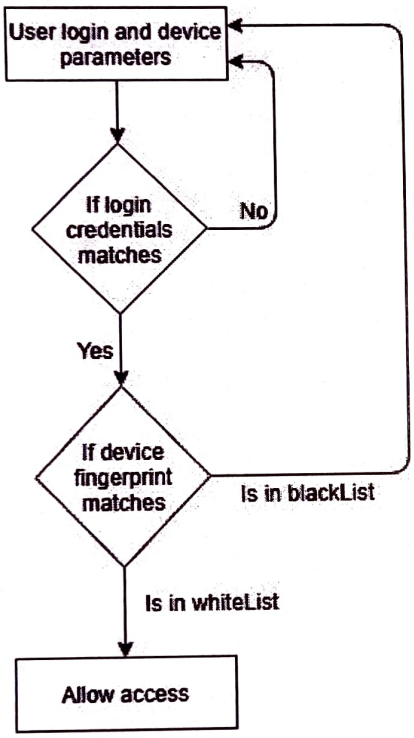

Fig. 4. Diagram of device fingerprinting algorithm [2].

In conclusion, this fingerprinting algorithm seems very secure and efficient. Since the focus of this solution is an algorithm, and which can be implemented independent of system architecture, we shall classify this solution under the software solutions tab.

Next up, we came across a paper that suggested an encryption method, which would be used to encrypt SMS messages that would contain the commands that are to be processed by the system [8].

The proposed model given by the authors suggests that SMS be used for control of home automation systems. But, SMS transmission is very insecure. To counter this problem, the authors suggested a new encryption solution, which was a combination of two existing encryption algorithms [8].

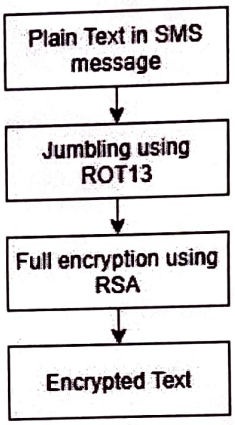

Fig. 5. Block Diagram of the encryption process [8].

The system works by taking in input by SMS from the user, encrypting the message or command using the encryption algorithm, and then sending the SMS to the system to carry out the intended function, where the message will first be decrypted and then processed [8].

The encryption algorithm works by taking the plain text as input and then passing it through a couple of encryption algorithms. The algorithms are the ROT13 algorithm, which is first used to jumble up the contents of the plain text, and then the RSA algorithm, which using its public and private key concepts makes the already jumbled data more secure. This combination, in this particular order, is used to encrypt the data [8].

While decrypting, the encrypted data is first taken through the RSA decryption algorithm that makes use of the public and private keys used in encryption, and then goes through a round of ROT13 again, which produces the plain text again [8].

In conclusion, this algorithm, which combines two widely used cryptographic algorithms, makes it more difficult for an intruder to intercept the messages by providing two layers of security. Even if the attacker breaks through the first layer, it might be too late for the attacker to have any use of the message by the time they crack the second layer. The proposed solution, being purely an algorithm based solution, we have classified it under the software solution category.

The first system that we came across in the embedded solutions category was a Public Switched Telephone Network (PSTN) based Home Automation and Security System [4]. In this paper, the authors suggested using nationwide telephone lines to communicate with the home automation system. The system is divided into three parts. The PSTN based call handling system, the dual tone multiple frequencies (DTMF) based decoder circuit, and micro-controller based system to control the services [4].

The call handling system consists of PSTN, the ring detection circuit and the call pickup circuit. The user calls the system using

the PSTN, and the call is picked up by the ring detection circuit. But it does not pick up the call. Picking up the call is done by the call pick-up circuit using a timer. After the call is connected, the system uses a dual tone multiple frequency (DTMF) decoder to first authenticate the user. The system requires the user to enter a 4-digit user access code. Using the DTMF decoder, the code is compared with the authentication data. If the code is correct, the user is allowed access, otherwise, the user is prompted to enter the correct code. For security purposes, the user can only enter the code 4 times before the system is reinitialized. Upon granting access, the DTMF decoder is then used to decode the command that the user shall enter. Then, the micro-controller steps in, and first receives the decoded DTMF code and then processes this code to determine the command and then performs the appropriate function [4].

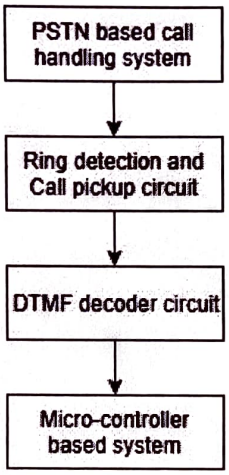

Fig6. Block diagram of the PSTN based home system [4].

In conclusion, this proposed solution suggests using a DTMF code to authenticate users. With the whole system have different layers of abstraction and only one entry point, it might possibly protect the system against some threats mentioned above. Since the entire suggested solution is a whole system, we are classifying this under embedded solutions.

The next solution we looked at is Role-based Access Control [7].

The RBAC (Role Based Access Control) model is a security model which was proposed by the authors to enhance the security of an existing home automation system. To do so, three layers of sub-modules have to be verified [7]. These are:

- Authentication
- Access Control
- Security Policy Management

The proposed security model works at the home gateway section of the system. The home network is divided into three components:

- Home user
- Home Gateway (Where RBAC functions)
- Service Provider

The first module in RBAC is the integration module and is accessed by the authentication server. If the authentication is successful then the authentication stage terminates [7].

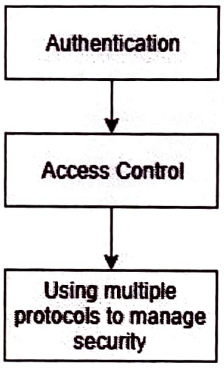

Fig. 7. Block Diagram of the RBAC system [7].

The second module in RBAC is access control. The access control block consists of databases, the definition module, and the enforcement module. When a request is received from the user it is transmitted to the definition module. The module, in turn, uses the database and retrieves logical and relevant information. The status is then sent to the enforcement module which passes the decision of granting or not granting access. The access control module then accesses user information from the authentication module and surveys the database using the information accessed as a key. With the help of this, the access control block is able to discard or grant access to service requests [7].

The third module in RBAC is the security management policy. This module sets and manages the security protocols of the home gateways. The security protocol manager consists of the admin interface, manager protocol, log manager and a network protocol. The policies are accessed and used here [7].

The three modules after execution help in increasing the security of the home network and protects it from attacks and malicious information. It creates a secure home network in which the modules efficiently function [7].

In conclusion, we classify the RBAC method under embedded solutions as it features a whole environment packed in one and is more of a system solution than an algorithmic one.

III. Result/Inferences

From the entire literature review, we have summarized the following.

First, we divided the proposed solutions into two categories- software solutions and embedded solutions that would help us compare the solutions to the security challenges in a fair manner, on a level field.

This classification simplifies our method of comparison among the solutions while also making the comparisons compatible.

TABLE I. SOFTWARE SOLUTIONS VS EMBEDDED SOLUTIONS.

Type	Implementation	Dependency
Software	Easy to implement and implementation cost is low.	Low dependency on other modules of the system.
Embedded	Ease of implementation depends on the level of complexity. Usually high.	Heavily dependent on subsequent modules

Since it is not justified to compare software solutions and embedded solutions with each other, we compare them separately, with the factors of ease of use and type of threat, in mind.

Here, we first compare the five software solutions mentioned in our literature review. We shall compare them on two aspects, the type of threat that they work best against, and the complexity of the solution. High complexity equals a higher level of protection against the specified type of threat.

We define the scale of complexity on the basis of the following:

- Number of parameters to be tested
- Complexity of the parameters to be tested

TABLE II. COMPARISONS OF SOFTWARE SOLUTIONS

Solution	Type of Threat	Complexity
MQTT	Unintentional threats and malfunctions	Low
Attribute-based Cryptography	Intentional threats	High
Device Fingerprinting	Intentional and unintentional threats	High
ROT13 + RSA	Intentional threats	Moderate

Now, we shall compare the embedded solutions based on the same metrics.

TABLE III. COMPARISONS OF EMBEDDED SOLUTIONS

Solution	Type of Threat	Complexity
PSTN	Intentional and unintentional threats	High
RBAC	Intentional threats	High

IV. CONCLUSION

Not all solutions give us the same level of security against all types of threats, rather every solution is fine-tuned for a particular type of threat or problem and aims to solve that. Also, those solutions that have a narrow scope tend to do better within that scope. However, according to our review, we can conclude that Attribute based cryptography and Device fingerprinting gives us the best system performance in the software solutions class and PSTN provides the same in the embedded solutions class.

REFERENCES

[1] Malik Nadeem Anwar, Mohammad Nazir, and Khurram Mustafa, "Security threats taxonomy: Smart-home perspective", in the 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA), 15-16 Sept. 2017.

[2] Arun Cyril Jose, Reza Malekian, and Ning Ye, "Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home", in IEEE Access, Vol. 4, Sept. 2016.

[3] J Prabaharan, Ashvith Swamy, Aditya Sharma, Kumar N. Bharath, Palak R. Mundra, and Khurram J Mohammed, "Wireless home automation and security system using MQTT protocol", 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 19-20 May 2017.

[4] Faizan Farid, Muhammad Rehan, Faiza Faizan, and M Tahir Qadri, "Home automation and security system via PSTN", 2010 2nd International Conference on Education Technology and Computer, 22-24 June 2010.

[5] Margaret Rouse and Peter Waher, "MQTT (MQ Telemetry Transport)", www.internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport, 14-10-2018.

[6] Hwajeong Seo, CheolSoo Kim and Howon KimZigBee, "Security For Home Automation Using Attribute-Based Cryptography", 2011 IEEE International Conference on Consumer Electronics (ICCE), 9-12 Jan. 2011.

[7] Geon-Woo Kim, Do-Woo Kim, Jun-Ho Lee, Jin-Beon Hwang, and Jong-Wook Han, "Considerations on Security Model of Home Network", 8th International Conference Advanced Communication Technology, 20-22 Feb. 2006.

[8] Teddy Mantoro; Yosep Lazuardi, "SMS based home appliance security approach using ROT 13, RC4 and RSA algorithm", International Conference on Computing, Engineering, and Design (ICCED), 23-25 Nov. 2017.