International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Critical Analysis of Security Issues and Measures in IoT based Smart Home Environment

Dr. Sanjay Yede

P. G. Department of Computer Science and Technology, DCPE, Amravati, India

Abstract: ***Advancement in communication and information technologies and their seamless integration has led to the emergence of the concept of Internet of Things. A variety of electronic devices, including sensors, actuators, displays, computational elements come together to form a network things those interact and exchange information is termed as Internet of Things (IoT). The devices in IoT communicate with each other and provide the users with automated and customized services. The IoT based electronic environment creates an automatic Smart Physical World termed as "Smart Home Environment". The concept of Smart Home is there for some time now. It is designed to make life of human beings, particularly the people of old age and women, better and secure through personalized smart services through information processing and automation. These Smart Homes facilitate the devices and systems to communicate with each other and are controlled automatically in order to interact with the household members and improve the quality of their life. The SHEs are heavily dependent on Internet based services and therefore they are always required to be connected to the outside world thereby creating concerns for security. This paper discusses different security threats, issues and measures regarding SHE's.***

Keywords: Smart Devices, Internet, IoT, Smart Home, Security, Security Issues, Security Measures

1. Introduction

The spread of Internet of Things (IoT) due to advances in Communication and Information technologies, the Smart Home Environment has now become a reality. Home appliances and devices are interconnected to form a home area network, via proprietary or standard TCP/IP protocols. Nevertheless, as with any form of network, smart home is also prone to security threats and vulnerabilities. These digitally controlled automated environments turn a home environment into a smart home environment, making it a more comfortable place to live. Such smart homes provide better facilities and improve the quality of life. A Smart Home facilitates a living environment that provides comfort of living, life safety, security and efficiency to the residents through the use appropriate technology [1,2,3] A smart home can help old-age people to live an independent and better life. With the emergence of flexible wearable signs sensors and location tags it has become possible to track people's health status from remote. In a typical Smart Home Environment, Internet of Things is formed by the integration of these electronic elements that are expected to sense, process and transmit data collected from the mixture of different devices, users and computers connected in the environment with a view to responding with personalized services to users. Different sensors might be placed in different locations like offices, apartments and homes to collect users' information and medical data. The network is responsible for collecting, distributing and processing vast amounts of private data with other networks, domains or systems. The sharing of the data with outside world will eventually lead to growing concerns of security, privacy and trustworthiness of the network. Generally, security deals with cryptographic techniques used to secure communication channels by ensuring message integrity, confidentiality, authenticity, whereas privacy studies the issues involved in trust and risk associated in the collection, storage, distribution and association of personal data.

2. Smart Home Concept

It is very important to understand the architecture of Smart Home in order to know the factors those affect security. Then one can select security technologies that can be applied to reduce or avoid the risk of security attacks. The Smart Home Environment is comprised of three main components; the Internal Network, the External Network and the Residential Gateway.

The Internal Network is the main part of a Smart Home Environment. It is responsible for facilitating the Internetworking of number of devices of heterogeneous nature based on the concept of Internet of Things. The Internal Network incorporates a combination of different communication media either wired or wireless via a variety of protocols. The External Network includes the Internet and the service providers which is responsible for providing services to the Smart Home members over the Internet. Finally, the Residential Gateway (RG) is a device located inside the Smart Home that works as a bridge between the Internal and External Network. [1,2,4].

2.1 Smart Home Components

The components comprising the smart home system can be classified into four categories, namely, Home Appliances & Lighting Control system, Home Entertainment System, Home Communication System and Home Security System [2, 4, 5].

2.1.1 Home Appliances, Lighting Control System

Home Appliances Control subsystem includes smart appliances that communicate with each other and also the outside through Internet. This system monitors and controls the power outlets in Smart Home and enables the user to monitor the power consumption as well as operate the power switch on/off from anywhere with the help of the Internet. The Lighting Control subsystem monitors the activities of the members of the Smart Home and intelligently manage

lights and its intensity as per need and predefined policy. The Climate Control subsystem of Smart Home controls temperature and humidity by controlling the functions of heating, ventilating, and air-conditioning. [2, 5, 4].

a) Home Entertainment System

This system facilitates the intercommunication of audio and video appliances and allows distribution of high fidelity audio and video signals over the network [2,6,7].

b) Home Communication System

This system controls telephone services such as voice and video conferencing. Also it contains devices such as PCs, printers, scanners, mobile phones, personal digital assistants (PDAs) and enables them to communicate with each other. Thus, the residents tenants are able to chat, send emails and share data (e.g. digital photos, video) with other people in any place in the world [2,7,5].

c) Home Security System

Home Security system encompasses identification through biometric recognition, voice recognition and face recognition, RFID tokens and smart cards that provide access control. It also includes alarming systems such as burglar alarms, fire/smoke alarm that allow immediate reaction. CCTV surveillance system can also be part of Home Security system for monitoring in a Smart Home. Finally, health and well-being monitoring for disabled and elderly people as well as children can be part of this system [2,7,5,8]. All these sub-systems of a Smart Home form an environment that makes the life of residents easy, safe, secured and happy.

2.2 Residential Gateway

As explained earlier, the Residential Gateway is a network device which integrates all the different networking technologies that exist in the Smart Home internal network as well as provides access from the internal network to Internet and vice versa. The Residential Gateway enables switching, routing and inter-working of functions between the devices inside the Smart Home systems over the internal network. It makes it possible to control the Smart Home systems and appliances from anywhere via Internet.[1,2,9]

Furthermore, a residential gateway enables functionalities related to security. It provides protection from unauthorized attacks and intrusions with the help of a variety of security mechanisms such as firewalls, authentication, authorization and intrusion detection [10,9].

2.3 Security Solutions in Smart Home Environment

The Devices in a smart home are connected with the help of wired as well as wireless technologies. The wireless communication is guided by IEEE 802.11 standard and its variants. Other than 802.11 the other short length wireless technologies used in Smart Home environment for interconnection of the devices are Bluetooth, ZigBee, and HyperLan.

Security in IEEE 802.11 standards is provided using Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WEP was the first security mechanism providing confidentiality, access control and data integrity in wireless communication. WEP uses RC4 encryption algorithm to protect the transmitted data. However, WEP is the most unsecured mechanism of these three, as it has a number of vulnerabilities. Transmitted packets can be easily captured and forged by attackers. Furthermore, WEP uses static keys which are rarely changed by users. WPA is a security mechanism created in response to the known serious weak-nesses of WEP. WPA is a subset of the 802.11i standard. Similar to WEP, WPA uses RC4 as its encryption method. However, the strongest of these three security mechanisms is WPA2 which is based on the full 802.11i standard. This mechanism uses Advanced Encryption Standard (AES) as encryption method and provides better security than WEP and WAP [11,12,13].

Bluetooth

Bluetooth implements several authentication and data encryption mechanisms to provide security. The Bluetooth authentication scheme uses a challenge response method. The Bluetooth encryption scheme encrypts the payloads of the transmit-ted packets using a stream cipher E_0. Furthermore, any pair of Bluetooth enabled devices that desire to communicate with each other should generate a session key, called link key, using a combination of an initialization key, the device MAC address and the Personal Identification Number (PIN). However, Bluetooth has a number of weaknesses which can be exploited by adversaries to obtain keys and the PIN numbers, depending on how session initialization of the communication standard is performed [13,14].

Zigbee

Zigbee security is based on a centralized infrastructure providing a central control on security of the network. There is a centralized trust entity that is trusted by all nodes in the network and is responsible for distribution of keys and admission control of nodes requesting to access to the network. Each network cannot have more than a single centralized trust entity and each device can be associated to only one centralized trust entity. However, this entity can be considered as a single point of failure and can be a security vulnerability of the network which can be exploited by malicious attackers. Furthermore, Zigbee standard proposes three types of keys; link key, network key and master key. Link key is shared between any two devices and is used to secure their communication. Network key is a common key for all devices and is shared among all devices in the network. Network key is used to secure all broadcast communications in the network. Master key is pre-installed or derives from the centralized trust entity and is used to generate the link keys.

Additionally, Zigbee standard provides data freshness, data integrity, authentication and encryption. Data freshness is achieved using counters which are reset every time a new key is generated. Data integrity is provided by Message Authentication Codes. Network level authentication and device level authentication are provided using the common network key and the link keys respectively. Finally, Zigbee proposes 128-bit AES encryption using the common

network key for network encryption and the link keys for device encryption [15].

HiperLAN

HiperLAN is a wireless LAN standard published by European Telecommunications Standard Institute (ETSI). There are two versions; HiperLAN 1 and HiperLAN 2. HiperLAN 1 was published in 1996 and its maximum data rate is 23.5Mbps. HiperLAN 2 was published in 2000 and can handle up to 54Mbps data rate. The basic services that two versions can support are data, audio and video transmission [16, 17].HiperLAN uses schemas for mutual authentication of mobile devices, encryption of data and exchange of encryption keys. HiperLAN standard proposes five authentication mechanisms based on the challenge response approach providing mutual authentication between mobile devices and the access point. Furthermore, HiperLAN uses the DES and 3DES algorithms for data encryption. Finally, the exchange of encryption keys is based on the Diffie-Hellman protocol. In spite the fact that HiperLAN has several relatively strong security mechanisms, there are a lot of vulnerabilities [18].

2.4 Security issues in smart home

Internal Threats

Internal threats stem from within the trusted Smart Home internal network. However, they are not given the attention they deserve compared with external attacks. Internal threats can be derived from inappropriate network construction and configuration, incomplete security plan and software pitfalls.

A wrongly configured device can raise security risks. Any home user (young children, people lacking security skills) is allowed to use any device and access any service. Besides, any resident can change the Smart Home internal network since he\she can modify the configuration of network equipment, add or remove network devices from the internal network as well as install or uninstall software of network devices. Additionally, the security features of the Smart Home environment can be modified intentionally or unintentionally by any home user. Thus, a lot of security holes for intruders can be raised when the home user does not follow security policies properly.

External Threats

Smart Home internal network is subject to a lot of security threats derived from outside world as well.. The types of the external threats are classified based on the way the information is compromised. There are two generic types of threats: passive and active attacks.

In passive attacks, the intruder intends to gain unauthorized access to information that is being transmitted without modifying it. The detection of passive attacks in a communication is not easy, since the intruder does not change the messages that are being exchanged between the sender and the receiver. Passive attacks can be either eaves-dropping or traffic analysis. Eavesdropping allows an intruder to monitor the home user traffic (e.g. telephone conversation, email message) between the Smart Home internal network and the outside world without the consent of the communicating parties. This traffic may contain confidential information that the residents do not want to disclosure it to unauthorized third parties. Eavesdropping is the most widely identified security problem in open networks and is an attack on confidentiality of the Smart Home internal network.

In active attacks, the adversary intends to tamper the information or generate fraudulent data into the Smart Home internal network. Active attacks can result in severe losses for the home users. The main types of active attacks are masquerading, replay, message modification, denial of service and malicious codes [19].

2.5 Suggested security technologies for smart homes environments

The most essential security technologies for making a Smart Home internal network secure are authentication and authorization mechanisms. Both mechanisms are required in order to restrict any malicious entity from accessing the Smart Home internal network. Furthermore, use of firewalls is another intrusion prevention mechanism that is important to increase security in Smart Home environment. However, intrusion prevention mechanisms alone are not sufficient for the Smart Home internal network because of its complexity and heterogeneity. Therefore, the use of intrusion detection systems (IDS) is also required.

Authentication Mechanisms

Authentication process includes entity authentication and message authentication. Entity authentication ensures the authenticity of the entity and message authentication verifies that the received message derives from the right sender. There are mechanisms for entity authentication as well as message authentication.

The proof by knowledge approach takes into consideration what the user knows. This approach usually checks a secret password or an identifier (ID) of the user that request access. The authentication mechanisms based on this approach called ID-password-based authentication mechanisms. The proof by possession approach depends on what the user possesses. This approach is based on the ownership of a smart card that should be connected during the login process. The authentication mechanisms that follow this approach called smart card-based authentication mechanisms. The proof by property approach is based on what the user is. In this approach, the verifier measures certain biometrics properties (e.g. fingerprint, iris, retina) of the user. The authentication mechanisms based on this approach called biometric-based authentication mechanisms.

Authorization Mechanisms

The purpose of authorization is to control the authenticated entity's access rights on network services and resources. Additionally, authorization contributes to reduce the harmful consequences of exposure to malicious accesses. Thus, authorization mechanisms are used to determine what level of access a particular authenticated entity should have on network services and resources in a Smart Home environment. For authorization within the Smart Home internal network, the exist-ing authorization mechanisms can be used. The existing authorization mechanisms can be

classified into three categories; server-based authorization mechanisms, peer-to-peer authorization mechanisms and certificate-based authorization mechanisms [10].

Server-based authorization mechanisms are used in client-server communication model. In this mechanism, the server generates and keeps authorization rules. Server-based authorization mechanism is the simplest authorization mechanism.

Peer-to-peer authorization mechanisms are based on peer-to-peer communication service model. In this mechanism, a peer manages the authorization rules or requires help of a designated authorization server. This mechanism is more complicated than the server-based authorization mechanism because of a number of constraints such as database maintenance and hardware specifications of peer's machine.

Finally, certificate-based authorization mechanisms refer to authorization infrastructures, where Authorization Certificates (ACs) are used for authentication and access control simultaneously. AC establishes authorization access rights between a subject and a resource [10].

Intrusion Prevention: Firewalls

A firewall is a hardware device or software running on another device which inspects the information passing through it in order to prevent unauthorized Internet entities from accessing private networks connected to Internet. A firewall examines all network traffic entering or leaving the private.

The firewall techniques used in order to control the network traffic are packet filtering, proxy service and stateful inspection. In packet filtering method, firewall analyzes packets, entering or leaving the private network, against a set of filters and accepts or discards them based on user-defined rules. Firewall provides a private network with the capability to perform coarse-grain filtering on IP and TCP/UDP headers, including IP addresses, port numbers and acknowledgment bits. However, in this method it is difficult for the user to configure the firewall. Furthermore, this method is vulnerable to IP spoofing attack.

Intrusion Detection

Intrusion detection is used as a second line of defence to protect the Smart Home internal network because once an intrusion is detected, a response can then take place to minimize damages. In case that an intruder succeeds in his attack over the Smart Home internal network, intrusion detection systems (IDS) can detect this attack and stop the activities of the intruder. In the Smart Home internal network, both Network-based IDS and host-based IDS can be used. Network-based IDS are used in wired networks where traffic monitoring takes place at switches, routers and gateways. How-ever, host-based IDS are used in ad hoc networks where there are not such traffic concentration points.

3. Conclusion

Smart Home is a concept that is evolved to improve quality of life of its residents. The advancement of communication technologies make it possible to establish a network of electronic devices and appliances gave birth to the concept of Internet of Things. This paper discussed the Concept and Architecture of Smart Home Environment that is based on Internet of Things. In Smart Homes, security is of extreme importance since it affects the privacy of the household members. In this paper, a variety of important security issues concerned with Smart Home environments are discussed. Also the security threats that may affect the security requirements are examined and finally, the security mechanisms that can be suitable to provide security to Smart Home environment were suggested.

References

[1] Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Dalahoche, L., & Logé, C. (2006). The Smart Home Concept: our immediate future. In *Proceed-ings of the 1st IEEE International Conference on E-Learning in Industrial Electronics.*

[2] Pohl, K., & Sikora, E. (2005). Overview of the Example Domain: Home Automation. In Pohl, K., Böckle, G., & van der Linden, F. J. (Eds.), *Software Product Line Engineering Foundations, Principles and Techniques* (pp. 39–52). New York: Springer.

[3] Jiang, L. Liu, D., & Yang, Bo. (2004). SMART HOME RESEARCH. In *Proceedings of the Third International Conference on Machine Learning and Cybernetics* (pp. 659-663). Shanghai.

[4] .Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., & Heinonen, S. (2005). Perspectives of ambient intelligence in the home environment. *Telematics and Informatics - Elsevier*, *22*(3)

[5] Baronti, P., Pillai, P., Chook, V. W. C., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sen-sor networks: A survey on the state of the art and the 802.15.4 and ZigBee Standards. *Computer Communications*, *30*(7), 1655–1695

[6] Teger, S., & Waks, D. (2002). *System Dynamics Inc* (pp. 114–119). End-User Perspectives on Home Networking. IEEE Communications.

[7] Han, I., Park, H., Jeong, Y., & Park, K. (2006). An Integrated Home Server for Communication, Broadcast Reception, and Home Automation. *IEEE Transactions on Consumer Electronics*, *52*(1), 104–109

[8] Delphinanto, A., Huiszoon, B., Rivero, D.S., Hartog, F., Boom, H., Kwaaitaal, J., & Wijk, P. (2003). *Home Networking Technologies Overview and Analysis*. Residential Gateway Environment, Deliverable D3.1.