Current Trends in Technology and Science
ISSN: 2279-0535, May-2020, Volume: XI, Issue: IV

Cyber Security Threats to IOT Application and Service Domain

Mohd. Arif Khan
M. Tech Research Scholar
SORT Peoples University
mohdarifkhan8@gmail.com

Prof. Pankaj Savita
A. P. in CSE Department
SORT Peoples University
er.pankajsavita@gmail.com

Abstract: We are currently living in the post-PC era where smart phones and other wireless handheld devices are changing our environment, making it more interactive, adaptive and informative. Termed as Internet of Things (IoT) evolving into Internet of Everything, the new ecosystem combines wireless sensor networks, cloud computing, analytical data, interactive technologies, as well as smart devices, to provision solutions in which the objects are embedded with network connectivity and an identifier to enhance object-to-object interactions. IoT innovation is advancing and provides diverse smart solutions or applications. From e-transport to e-health; smart living to e-manufacturing and many other e-solutions. In this environment, the rising trend of cyber-attacks on systems infrastructure coupled with the system inherent vulnerabilities presents a source of concern not only to the vendors, but also to the consumer. These security concerns need to be addressed in order to ensure user confidence so as to promote wide acceptance and reap the potentials of IoT. From the perspectives of firmware, hardware and software infrastructure setups, this paper looks at some of the major IoT application and service domains, and analyze the cyber security challenges which are likely to drive IoT research in the near future..

Keywords

Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.

1. INTRODUCTION

Nowadays, a secure and comfort house are hard to get. Another problem is the energy. Inside the house, there is often a waste of energy by letting the appliances turned on without being used. By using smart home systems, users can easily monitor and control the device inside the home, improve home security by enabling home locking systems based on user location, and monitor the energy usage of each device.

The smart home system uses Internet of Things (IoT) technology. IoT technology utilizes the internet to be able to exchange data and communicate [1]. The use of IoT on smart house systems is based on the ease of every user in accessing the internet. By using IoT technology, users can access all devices in the home anytime and anywhere through mobile devices as long as the mobile device is connected to the internet. Therefore, by using a smart home system, users can enjoy the ease in monitoring and controlling the house in real time [2]

In general, smart home system can be configured as shown in Figure 1. As shown in Figure 1, smart home system consists of largely three components, home server, home gateway, and smart home devices. First, the home server provides storage, integration and distribution function of the information collected from various media in the home as a kind of computer device.

Fig1. Smart Home System

Next, the home gateway performs a relay function, or inter connect function between the subscriber access network and a wired/wireless home network. Finally, smart home devices can intelligently provide the information exchange function between the devices, and external internet access function [7].

2. Required Security Function for Smart home

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as

A, Confidently In case of data communication between devices as well ascending data to the outside, the transferring data should be converted into cipher text form. That is, the data confidentiality should be provided. And, we recommend using hardware security module to enhance security of device which has a specification capable of providing a security feature by mounting a hardware security module. For example, device identification information can be managed securely by using the hardware security module.

B. Integrity

Low ƒh capacity smart home devices (e.g., tiny sensors and actuators, etc.) and a home server can use the access control function and mutual authentication function provided by the home gateway. In consideration of the device specification, the critical data (user's privacy data, key information, and access control/authentication data, etc.) should be stored securely using hardware security module. Besides, data integrity should be provided to prevent data from being changed.

C. Availability

Low ƒh capacity smart home devices (e.g., tiny sensors and actuators, etc.) and a home server can use the access control function and mutual authentication function provided by the home gateway. In consideration of the device specification, the critical data (user's privacy data, key information, and access control/authentication data, etc.) should be stored securely using hardware security module. Besides, data integrity should be provided to prevent data from being changed.

3. Cyber Security Threats to Smart home

A. Attack surface areas

Devices have many vulnerable attacking surfaces and it may vary as each device works with different technology and have used different approach to design the product [3]. OWASP testing on IoT have developed many attack surfaces which can be related to the smart appliances available. Consumer/user must be also aware what are the vulnerabilities associated with attacking the surfaces of devices [4]. The following are the summary of attack surface areas [5, 6, 7] based on our literature survey.

i. Ecosystem Access Control: - how devices communicate with each and other and also how they follow user instruction- for example: Turn on the Kettle - request, send through mobile and how kettle automatically get turned on and heat the water. In analysing how the network traffic moves between the devices and how to send and receive device build a trust with another component.

ii. Device Memory: In device memory user details are stored such as usernames, passwords, ID's, keys and all information that user and have shared with the device.

iii. Device web interface: The mobile application can not only control the device; it can also access web interface. Website and web application have many vulnerabilities - such as SQL Injection, Phishing, Cross- site scripting.

iv. Device firmware: Device firmware is added to the device at the time of manufacturing, and it is also capable of storing information in it, and if it gets exposed, it can leak sensitive information like keys, credentials, API and whole device history.

v. Device network service: Every device has some open network ports through which they can be highly vulnerable to different attacks such Denial of Service, Injections, Replay attacks, creating blocking.

vi. Administrative interface: Every device has some admin functionality at the backend, and it is similar to the web

Interface, but in this, it is using more functionality as its admin and has a different interface. It is highly vulnerable to SQL Injection, Cross- Site Scripting, Weak Passwords, two-factor authentication.

vii. Local data storage: Data can be stored in the device should be encrypted and must use encrypted keys to save the data and the key used is similar or different in saving.

viii. Cloud web interface: There are millions of IoT devices already in the market, and if all IoT are using the same cloud to access the device and save the data. Then it becomes a superior problem and causes significant problems through vulnerabilities such as SQL Injections, Cross- Site Scripting, Weak Password, Account lockout.

ix. Third-party backend API’s: Personal data in the device can be shared in multiple places because the device is not designed to handle the data to be stored in a secure or encrypted way.

x. Update mechanism: Often the devices are patched using plain protocol rather than the encrypted channel. This might leads to vulnerabilities like leak credentials and could be transmitted by hacker and can lose of PII

xi. Mobile application: Mobile application comes with the IoT device purchased and is used to control the device, but it can increase the vulnerability such as pre-installed injection in user device can lead to much severe conciseness and can manage many different storages of cloud and other data storages.

xii. Ecosystem communication: List of the device which is part of communication and how they are communicating through checks, using ecosystem command and pushing updates to devices.

xiii. Network Traffic: How the network is designed and reaches the devices, which type of network used, could be LAN/WAN, what is the range of the network – shorter long.

xiv. Authentication or authorisation: Various devices lack the feature of 2-factor authentication. In two-factor authentication device can be connected through mobile by two security step or verification instead of one and now mostly device only use a weak password to gain access. Lack of Session Key, NFC, token and Cookie in available IoT Devices.

4. Vulnerabilities

A. **Username enumeration:** Is when user enters account name and ID and if it is wrong the backend system software responds to the request as 'the registered email /account name do not exist in the system, please try again'.

B. **Weak password:** Weak password is set such as '0000', '000000', '1234', '123456', etc. Also when password does not have an uppercase letter, numbers, minimum eight lengths, symbols.

C. **Account lockout:** Account Lockout is the number of failed attempt which user has inputted, and then automatically account ID gets locked out for a certain period. The example- can be noticed in smart phones when user enters 3 or 5 wrong passwords then consider automatically lockout for 30 seconds to one minute.

D. **Unencrypted Services:** Data sent between the devices and connectivity between the devices is Not encrypted. Hence it can be easily intercepted by the hacker, and it becomes vulnerable and easy to hack

E. **Two-Factor Authentication:** Devices lack two-factor authentication while connecting to the devices, such as a use of tokens, fingerprint scanners, encrypted code, etc. For connectivity with devices or even in an email two factor are now available.

F. **Encryption:** Encryption applied on some devices, but they are not correctly configured and installed in the system and could be out of lacking new updates, which can expose the device and make it vulnerable to hackers.

G. **Patches on plain text:** Updates which are sent to devices are not secure and encrypted, and some tools allow automatic updates.

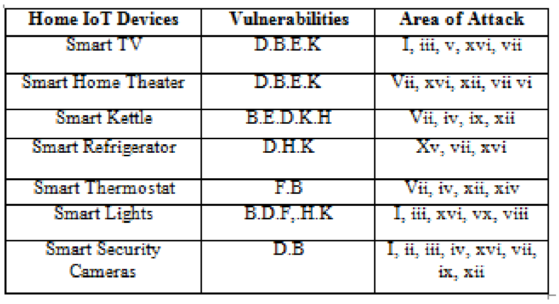
H. **Denial of Service (DoS):** Many different machines can attack the device at the same time at the network layer of the device. As a result, it can device can stop respond because of too much overloading.

I. **Storage Media Access:** When storage media can be removed by in person from a device by hacker and can retrieve all the PII for storage media.

J. **Firmware version:** Currently installed firmware Versions in the device are present in the system information and also last and new updates information is missing/not displayed and mentioned

Analysis

Analysis of the threats was done with different IoT devices individually. The following table (Table I) explains the links between those devices along with the vulnerabilities and the attack surface. Researchers proved that they were able to hack TV interfaces the SSL in not encrypted and which makes it very easy for hacker to attack with Man in the Middle attack. In RSA showcased a security test on TV. They demonstrated lack of security in TV App store as TV system ask for very weak password which is only 4 digit and the card detail for application purchase. Indecent 2014 some group of hackers hack the TV with these of Raspberry Pi and USB attached to the device and factory setting firmware was very weakly designed). But Apple TV is the only option in Home Entertainment device which has the option of 2 factor authentication and ask for strong password (Apple 2016). However, there are some basic measures such as keeping the device updated and firmware up to date, read manual, if TV has camera cover it with a tape and refer to the manufacturer regarding the security of the device.



Home IoT Devices	Vulnerabilities	Area of Attack
Smart TV	D.B.E.K	I, iii, v, xvi, vii
Smart Home Theater	D.B.E.K	Vii, xvi, xii, vii vi
Smart Kettle	B.E.D.K.H	Vii, iv, ix, xii
Smart Refrigerator	D.H.K	Xv, vii, xvi
Smart Thermostat	F.B	Vii, iv, xii, xiv
Smart Lights	B.D.F,.H.K	I, iii, xvi, vx, viii
Smart Security Cameras	D.B	I, ii, iii, iv, xvi, vii, ix, xii

5. Result

Unencrypted services, weak password, firmware version, denial of service and two-factor authentication are common vulnerabilities are mostly common in all smart home appliances and as a result they have familiar attacking surfaces. It is very unsafe situation for user so before purchasing they can look into the following threat vector and the number of threats and attacks which have occurred on these devices could be helpful. Even developer of IoT devices should look back first to the attacks that have been happened on devices and first aim is try to fix that patches permanently and then develop new device. By this they will ensure quality and safety assurance to user.

6. REFERENCES

[1]. J.C. Talwana and H.J. Hua, “Smart World of Internet of Things (IoT) and It’s Security Concerns,” in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, 2016, pp. 240-245.

[2]. Trio Adiono, Billy Austen Manangkalangi, Rahmat Muttaqin, Suksmandhira Harimurti, Waskita Adijarto ,” Intelligent and Secured

Software Application for IoT Based Smart Home, IEEE conference

[3]. Shivraj, VL, Rajan, MA, Singh, M & Balamuralidhar “One time password authentication scheme based on elliptic curves for Internet of Things (IoT)', in Information Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on, pp. 1-6. (2015)

[4]. OWASP 2016, IoT Security Guidance, https://www.owasp.org/index.php/IoT_Security_Guidance

[5]. Weber, M & Boban, M 'Security challenges of the internet of things', in 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 638-643. (2016)

[6]. Jing, Q, Vasilakos, AV, Wan, J, Lu, J &Qiu, D, 'Security of the Internet of Things: perspectives and challenges', Wireless Networks, vol. 20, no. 8, pp. 2481-2501 (2014)

[7]. Meddeb, A, 'Internet of things standards: who stands out from the crowd?’ IEEE Communications Magazine, vol. 54, no.7, pp. 40-47. (2016)