International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 9 Sep 2021, pp: 1229-1233 www.ijaem.net ISSN: 2395-5252

Threats and Security Issues onIoT Devices securing through API

Dr. Divya Premchandran, Dr. Thupalkula Bhaskar,
Asst. Professor, Keraleeya Samjam (Regd.) Dombivli's Model college
Associate Professor, Sanjivani College of Engineering Kopargoan

Submitted: 10-09-2021 Revised: 19-09-2021 Accepted: 23-09-2021

ABSTRACT
In Today' World in every pace of our daily lives there is widespread use of IoT Technologies for smart living. But these devices are never without security risks. This paper gives a brief overview of security issues in these smart devices. Here we are comparing few devices and their possible security assaults in these devices and to manage with current open software and their limitations.

Keywords: IoT, IoT devices, Botnet, API, Mirai Malware

I. INTRODUCTION

The internet of things is a diversity in IoT devices makes the IoT's scope so broad and its security challenging. The main features of an IoT device is that these devices are able to connect to the internet and interact with its environment through the collection and exchange of information. Devices commonly have minimum computing capacity and only a few specific functions. Because devices are so variant, that they are countless ways IoT can be used and applied to different situations.

Smart homes demonstrate just how accessible IoT devices are. Users can update home security system through smart locks, IP cameras and motion sensors or to improve through a smart TV, smart speakers and connect with game consoles. IoT devices are flexible and portable and can be connected to any network hence the fragmentation of the IoT and carries many security concerns. The lack of Industry standardization and foresight given rise to compatibility issues that also complicate the matter of security in these devices. The portability of these devices arises maximum threats as it can connect in different networks and these devices can easily compromised.

Many Threat and Risks can be foreseen in these interconnecting devices. IoT Security is critical because of the expanded attack of threats that have already in existing internet.

Vulnerabilities are a large problem that constantly poisoning users and organizations. Main reason behind it is the lack of computational capacity for built in security. Malware attacks are most frequent seen variants as they are versatile and profitable for cybercriminals.

Distributed -Denial -Of- Service (DDOS) attacks are easily infected to IoT devices. As these wireless devices are exposed to internet hence these objects are easily targetedand compromised with personal information.Security oversights, poor password hygiene and overall device mismanagement can assist in the success of these threats.

II. LITERATURE SURVEY

A Botnet is network that combines various system together and takes control on victim device and comprise them. Hackers can control botnet by executing DDoS and Phishing. This study is the first published in IoT bot malware-mirai in IoT Botnet Forensics [1] fully functioning Mirai botnet network architecture and conduct a comprehensive forensic analysis on the Mirai botnet server was discussed.

A denial-of-service (DoS) attack deliberately tries to cause a capacity overload in the target system by sending multiple requests. Unlike phishing and brute-force attacks, attackers who implement denial-of-service not aim to steal critical data.

The main reason of that system becomes unavailable because the victim device is overwhelmed with thousands of requests making the resources and capacity overload. The Distributed Denial of Services (DDoS) attack is carried out from a large number of systems which attack one target maliciously. For this purpose, machines called botnets or zombies are used to request a service at exactly the same time. Author [2] had proposed Intrusion discovery framework in view of human insusceptible framework utilizes signature based and inconsistency-based location methods.

The Author [3] work reviews the existing techniques, their drawbacks and claimed advantages of the upcoming password techniques. It also surveys some of the supportive methods for the naive users of password techniques.

There are various studies as well as services that have been conducted on the current trends in IoT security [4] The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Traffic interceptors and analysers help identify and investigate various cyber threats. IoT enabled devices have been used in industrial applications and for multiple business purposes [5]. The apps help these businesses to attain a competitive edge over their competitors. However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services. It is essential to have professionals to overcome these threat concerns and develop comprehensive security measures and policies to protect their business assets and ensure services continuity and stability. For example, smart kitchen home IoT enabled appliances connected to the local network can be a source of the breach for hackers to get access to the business and/or personally sensitive data or to manipulate and interrupt the business workflow.

III. IOT DEVICES

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. The Arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything, from something as small as a pillto something as big as an aeroplane, into a part of the IoT. Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The Internet of Things is making the fabric of the world around us smarter and more responsive, merging the digital and physical universes.

Pretty much any physical object can be transformed into an IoT device if it can be connected to the internet to be controlled or communicate information.

A lightbulb that can be switched on using a smartphone app is an IoT device, as is a motion sensor or a smart thermostat in your office or a connected streetlight. An IoT device could be as fluffy as a child's toy or as serious as a driverless truck. Some larger objects may themselves be filled with many smaller IoT components, such as a jet engine that's now filled with thousands of sensors collecting and transmitting data back to make sure it is operating efficiently. At an even bigger scale, smart cities projects are filling entire regions with sensors to help us understand and control the environment.

The term IoT is mainly used for devices that wouldn't usually be generally expected to have an internet connection, and that can communicate with the network independently of human action. For this reason, a PC isn't generally considered an IoT device and neither is a smartphone even though the latter is crammed with sensors. A smartwatch or a fitness band or other wearable device might be counted as an IoT device.

The Internet of Things is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

The definition of the Internet of Things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers.

3.1 Different types of IoT devices are:

3.1.1. Smart watch

Wearable IoT devices are used like smart watch and fitness trackers, are the among the most conspicuous examples of Internet of Things technology.

Accordingrecent Interconnected technology survey from Clutch, wearables are used primarily for singular functions such as checking the time and tracking exercise.

Wearable IoT devices reflects a broader trend of people using IoT devices as standalone technologies, rather a broader trend of people using IoT devices as standalone technologies, rather than within an ecosystem of connected devices. As a result, IoT technology has not fully penetrated consumer's daily lives but these devices are not from risk free. These devices are easily hacked and could create threats in private networks. It is links to a mobile which can provide a hacker window of opportunities. Many API are available like Norton 360 with LifeLock or google security can provide quite safeguard to a limit but its not enough for cybercriminals to a greater extends. The most common issue is user authentication. Two factor authentication limits the authorization after multiple failed passwords attempts.

3.1.2. Smart Homes

Smart home technology, also often referred to as home automation provides homeowners security, comfort, convenience and energy efficiency by allowing them to control smart devices, often by a smart home app on their smartphone or other networked device. A part of the IoT, smart home systems and devices often operate together, sharing consumer usage data among themselves and automating actions based on the userspreferences.

Smart home systems achieved great popularity in the last decades as they increase the comfort and quality of life. Most smart home systems are controlled by smartphones and microcontrollers. A smartphone application is used to control and monitor home functions using wireless communication techniques. But these devices are also vulnerable to wide range of attacks. Man- in the -middle an attacker breaches, interrupts or spoofs communications between two systems. Information generated by unprotected these interconnecting devices provide cyber attackers with an ample amount of targeted personal information that can be exploited for fraudulent transaction and identity theft. Nest API is good solution for home automation with is product from google store.

Farm.Bot API is open source solution for smart homes with better security features.

1.3.1.3 Smart Thermostat

Smart thermostats are thermostats that can be used with home automation and are responsible for controlling a home's heating andor air conditioning. Devices perform similar functions as a Programmable thermostat as they allow the user to control the temperature of their home throughout the day using a schedule, but also contain additional features, such as sensors and WIFI connectivity that improve upon the issues with programmable thermostats.

Like a connected thermostat, they are connected to the Internet. These IoT devices allows users to adjust heating settings from other internet-connected devices, such as a laptop or smartphones. Thispermits users to control the thermostat remotely. This ease of use is essential for ensuring energy savings: studies have shown that households with programmable thermostats actually have higher energy consumption than those with simple thermostats because residents' program them incorrectly or disable them completely.

Smart thermostats also record internal or external temperatures, time the HVAC system has been running and can even notify you if your air filter needs to be replaced. This information is typically displayed later on an internet-connected device. Device hijacking can control the device to a certain level and re-infect all smart devices in the home. For eg:- thermostat can be compromised and gain access to an entire network and remotely give access of a door or can change authorization. BrickerBot coded to exploit password in IoT devices and cause permanent denial of services. For eg;- Fake data fed to thermostats in an attempt to cause damage via overheating. Rambus Security solution for smart homes which can secure homes by secure boot feature by hardcoded cryptographic code signing techniques. Mutual authentication by using One-way hashing ensures that data originates from legitimate device not from hacker source.

3.1.4. Automated Cars

One of the most futuristic applications of IoT is the autonomous car. These cars that seem like a product from the near future actually exist today and are mostly under development or prototype stages. The cars will not have drivers and are sensible enough to take you to your destination on their own. Equipped with tons of devices like sensors, gyroscopes, cloud architecture, internet and more, these cars sense huge chunks of data on traffic, pedestrians, conditions of the road such speed breakers, potholes, corners and sharp turns and immediately process them at rapid speeds. This information is passed to the controller which takes corresponding driving decisions. Artificial Intelligence and Machine Learning are crucial aspects of driverless cars as well.

One of the central challenges in vehicle is that various electrical components in a car are connected via internet. Thus, if hacker manage to gain access to a vulnerable peripheral ECU for instance car's Bluetooth from there system may not be able to control of safety critical ECU like its brakes or engine and wreak havoc. Auto ISAC an industry group of major auto manufacturers and suppliers released a brief best practice for automotive cybersecurity. Another recommendation is continuing risk assessments processed support by threat Intelligence to identify all possible AI danger and emerging threats in autonomous driving.

3.1.5. Help assist devices

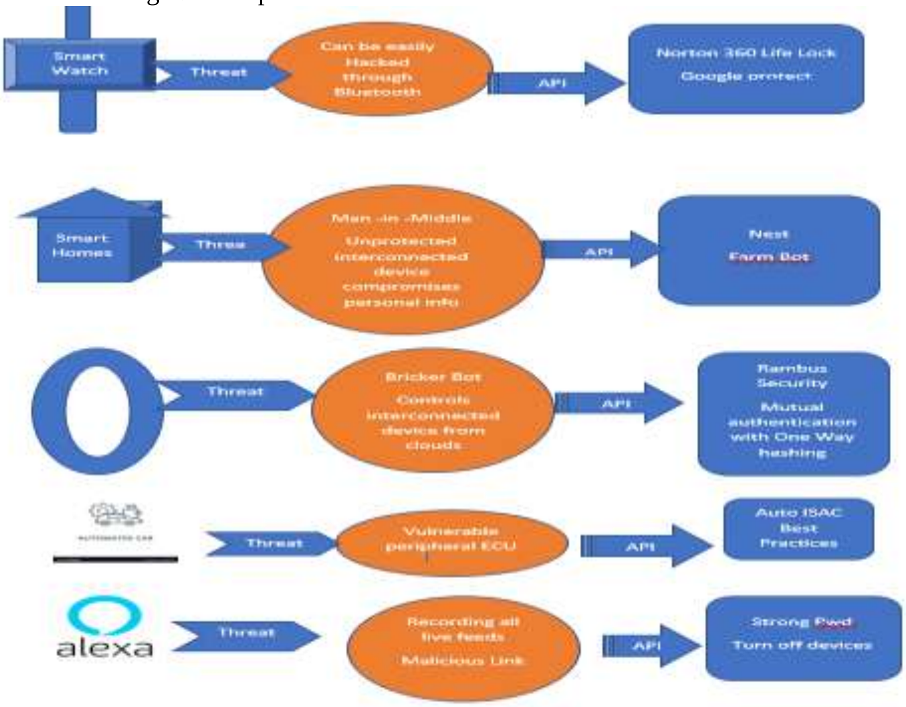
Now a days in every home these advance IoT devices are becoming daily part of human routines. These devices are never risk free as it is listening to all and even recording continuously. Hackers can create malicious link which can sent to an unsuspecting user.

Even users' personal details are also on stake as these devices are not off and all conversations can be listened by cybercriminals. Choosing strong passcode can solve the problems to a limit. Now a days build security apps in Alexa, Echo and Dot devices can solve the problems to an extent.

IV. SECURING VARIOUS IOT DEVICES

As in this paper we had underwent with various types of Interconnecting devices and their issues in relation with security and threats. Shoring up the security of active APIs is one of the best ways to protect inbound and outbound IoT data. Generally, web API security concerns the transmission of data through interfaces that are connected to the internet and exposed. Authentication is the key, especially when third parties are involved. Device connected through API call for tokens to verify authentications. By using Hashing algorithm user authenticity can be protected and unauthorized connections will be denied. Every API should have a hard quota by using triggers to prevent Denial of Service attacks. More leverage API gateway as point of enforcements. Continues Audit to discover the threats and new attacks. Figure 4.1 shows the comparison of IoT devices with possible threats and API solutions.

Fig 4.1 Comparison of IoT devices with threats and API



V. CONCLUSION

Web API security will strengthen Iot connections to better protect collected, processed and communication of Information. As Internet is never completely secure as of open connections and there are other hackers gets the leverage. When

API focus on developing secure, effective and trustworthy systems, it hampers potential attackers and also secure all data in these IoT devices. Better token security using Swarms SRC20 can limits tampering IoT devices. Even REST API technologies helps to secure interfaces between connecting devices and sensors and storage features. Even it can make devices light provide more security and reduce power consumptions. More Web API security should be developed secure the IoT devices.

REFERENCES

[1]. IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers by XiaoluZhang, Oren UptonNicole, Lang Beebe ,Kim-Kwang, Raymond ChooDepartment of Information Systems & Cyber Security, University of Texas at San Antonio, San Antonio, TX, 78249, USA

[2]. IoT Security against DDoS Attacks Using Machine Learning Algorithms,Tayyaba Khalil MPhil. Computer Science, Kinnaird College for Women, Lahore.

[3]. TCpC: a graphical password scheme ensuring authentication for IoT resources,Priya Matta, Bhaskar Pant.

[4]. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. ComputerNetw. 2019, 148, 283–294.

[5]. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. IEEE Commun. Surv. Tutor. 2018, 21, 1636–1675.