SIT 209

SIT 209 : DEVELOPING IOT APPLICATION

TOPIC 9

IOT APPLICATION

ABOVE AND BEYOND

NAME - YOHJIT CHOPRA

ROLL NO. - 2110994798

TOPIC 9, ABOVE AND BEYOND

INCIDENCES OF SECURITY FAILURES IN IOT.

Introduction

A cutting-edge technology called the Internet of Things (IoT) connects various gadgets and allows them to speak with one another. IoT device use is expanding, which has led to an increase in security worries. IoT security flaws have grown to be a major problem, which is of grave concern to governments, organisations, and end users. Failures in IoT security can have serious repercussions, including monetary loss, reputational damage, and even fatalities. A few of the security failures or security breaches are mentioned below

Year 2016

The Mirai botnet assault that took place in 2016 was one of the biggest security lapses in IoT. The Dyn DNS infrastructure, a business that offers DNS services to many well-known websites, was subjected to a significant distributed denial of service (DDoS) attack as a result of the Mirai botnet attack. A botnet of Internet of Things (IoT) devices that had been infected by the Mirai software was used to carry out the attack. The malware targeted IoT devices with weak default passwords, including routers, cameras, and DVRs. These devices were in the hands of the attackers when they launched a significant DDoS assault on Dyn's servers. Widespread internet outages were caused by the attack in the US and other countries.

Year 2017

The 2017 WannaCry ransomware assault was another big security lapse in IoT. Around 200,000 computers in 150 countries were impacted by the WannaCry attack, which also severely disrupted essential infrastructure like hospitals, banks, and government offices. The Windows operating system's weakness was exploited by the WannaCry ransomware, allowing it to spread quickly over networks. The attacked PCs' files were encrypted by the ransomware, which then demanded money in return for the decryption key. The WannaCry incident brought to light the IoT devices' susceptibility to malware and the requirement for strong security measures to thwart such attacks.

Year 2018

The 2018 Facebook data breach, which affected millions of users globally, was another huge security blunder in IoT. In this instance, hackers were successful in accessing user data by taking advantage of a flaw in Facebook's software. This hack served as a reminder of the value of protecting IoT device data and the requirement for strong security controls to prevent data breaches.

Researchers found a flaw in smart home gadgets in 2018 that let attackers take remote control of them. The flaw affected thermostats, lights, and door locks among other smart home appliances. The Zigbee wireless protocol, which is frequently used in smart home gadgets, was vulnerable and gave attackers access to the devices. Once the attackers had access to the devices, they could remotely manipulate them and maybe breach into residences or steal private information.

Year 2019

Amazon-owned Ring, a well-known maker of smart doorbells and security cameras, has also had security issues with some of its products. In 2019, it was discovered that Ring cameras had been compromised, giving hackers access to the cameras' live video feeds and enabling them to eavesdrop on homeowners. The incident was linked to a flaw in Ring's software that let attackers access the cameras without being authenticated. Since then, Ring has improved the security of its products by introducing new security mechanisms including two-factor authentication.

Researchers found a flaw in a well-known IoT platform used in industrial control systems in 2019. Due to this flaw, attackers were able to remotely take over and operate the systems. Systems used in vital infrastructure, such power plants and water treatment facilities, were among those that were impacted. The severity of the implications if these IoT devices are compromised was underscored by this incident, which also highlighted how crucial it is to secure these devices when they are utilised in vital infrastructure.

Tesla, the producer of electric vehicles, has also encountered security issues with its IoT gadgets. Researchers showed off their ability to remotely operate a Tesla Model S car in 2019 and perform operations including unlocking the doors, turning on the headlights, and halting the vehicle. The infotainment system bug that created the vulnerability gave the researchers access to the car's network and the ability to manipulate its functions. To immediately address the issue and increase the security of its vehicles, Tesla released a patch.

The Nest Cam IQ indoor security camera has a vulnerability that allowed attackers to take over the device and eavesdrop on users, according to a 2019 Google announcement. A bug in the firmware of the camera led to the vulnerability by enabling attackers to run arbitrary code on the system. To close the hole in its devices' security and remedy the vulnerability, Google provided a patch right away.

Security researchers found a flaw in millions of IoT devices in 2019 that allowed remote attackers to take control of them. The IoT device vulnerability affected routers, cameras, and DVRs. The flaw made it possible for attackers to manage the devices with a single command while avoiding the authentication process.

Attackers may exploit the devices to launch DDoS assaults or steal personal information once they had access to them.

Year 2020

Researchers found a flaw in Amazon's virtual assistant Alexa in 2020 that made it possible for attackers to listen in on user interactions. The flaw made it possible for attackers to develop a malicious Alexa skill that could be used to secretly listen in on user conversations. The flaw made clear the necessity for strong security measures to defend against attacks on virtual assistants and other Internet of Things (IoT) devices.

The COVID-19 pandemic in 2020 significantly increased the use of IoT gadgets such smart home gadgets, remote work tools, and healthcare gadgets. IoT security vulnerabilities increased in tandem with this rise in IoT adoption. For instance, when more people began working remotely, the number of cyberattacks aimed at home networks and remote work technologies increased. Parallel to this, there was an upsurge in attacks on remote medical equipment, which can endanger the lives of patients.

Year 2022

Similar to the year 2019, 2022 also faced multiple data breaches.

Revolut

On September 11, 2022, a data breach occurred that allowed unauthorised access to the personal data of more than 50,000 customers of the finance startup Revolut.

Zoetop Business Company

The state of New York fined Zoetop Business Corporation, the company that owns the fast fashion brands SHEIN and ROMWE, US$1.9 million in October for failing to report a data breach that affected 39 million customers.

Twitter

In July 2022, a hacker that went by the alias ‘devil’ posted on hacking forum BreachForums that they had the data of 5.4 million Twitter accounts for sale.

Challenges and Solutions for a Multi-Layered Approach

The sheer quantity and variety of IoT devices present one security concern. Applications for IoT devices vary from wearables and smart homes to industrial control systems and vital infrastructure. Every application has different security needs, thus securing them calls for a multi-layered strategy.

The necessity to strike a balance between security and usability is another difficulty with IoT device security. Many IoT devices include straightforward user interfaces and few configuration choices in order to make them simple to operate. Yet, these design decisions may also increase their susceptibility to attack.

A thorough IoT security architecture that addresses all facets of IoT security, such as device design, software development, network security, and user education, is required to handle these difficulties. For manufacturers, developers, and end users as well as for governments, this framework should include recommendations and best practises.

Strong security measures are required at every level of the IoT ecosystem in order to overcome the security flaws in IoT. This encompasses manufacturers, developers, and end-users. IoT device makers must make sure their products are built with security in mind and include strong security features like encryption, authentication, and access control. Developers are responsible for making sure their software is safe and free of flaws that could be used by attackers.
Also, end users are essential in assuring the security of their IoT devices. People must take precautions to secure their devices, such as updating their software and changing the default passwords. They should also be cautious when connecting their IoT devices to public Wi-Fi networks, as these networks may not be secure.

The failings in IoT security are a problem that must be addressed by governments as well. They must create laws and rules requiring manufacturers to follow specific security requirements. To encourage innovation in the sector, governments might also support IoT security research and development.

Conclusion

In conclusion, security failures in IoT have become a significant challenge for end-users, businesses, and governments. The incidences of security failures in IoT, such as the Mirai botnet attack, the WannaCry ransomware attack, and the vulnerabilities in smart home devices, have had severe impacts on the ecosystem. To address these challenges, manufacturers, developers, end-users, and governments must work together to implement robust security measures at every level of the IoT ecosystem. Only then can we ensure that IoT devices are secure and free from vulnerabilities that can be exploited by attackers.