**SIT209 – Developing IoT applications**

Topic 9 - Above and Beyond

# Incidences of security failures in IoT:

Ever since the last decade, there has been an exponential rise in the development and users of Internet of Things. This sudden upsurge in IoT brought a lot of changes in the lives of both professional and unprofessional audience as user interfaces for these IoT devices were especially targeted for non-technical audiences. The reliability, efficiency, privacy and responsiveness provided by these applications increased the trust of people on them, to the point, critical information such as commercial cards, personal and professional information is provided to them in hope that the data would not be leaked or hacked. This led to cyber attacks being common on these applications. Personal lives, financial information being leaked allowed these attackers to hack their way to the lives of the common people through various means such as IP tracking, phishing attacks, fake links etc. and hence this is known to be as security failures in IoT.

These cyber-attacks became common after 2015, which marked the beginning of IoT era. For instance, there have been numerous incidents due to IoT security failure in recent years, including: Mirai Botnet: In 2016, the Mirai botnet was used to launch a massive Distributed Denial of Service (DDoS) attack against the DNS provider Dyn, which caused widespread internet outages. Mirai exploited the security vulnerabilities of IoT devices such as cameras, routers, and other internet-connected devices that had weak default usernames and passwords. Jeep Cherokee Hack, in 2015, security researchers were able to remotely take control of a Jeep Cherokee's steering, brakes, and other critical systems by exploiting vulnerabilities in the vehicle's infotainment system, which was connected to the internet. St. Jude Medical Pacemakers, in 2017, security researchers found vulnerabilities in St. Jude Medical's pacemaker devices that could allow hackers to take control of the devices and deliver electric shocks to patients. The vulnerabilities were patched by the manufacturer. Russian Cyberattacks on Ukrainian Power Grid, in 2015 and 2016, hackers believed to be working for the Russian government launched cyberattacks on Ukraine's power grid, causing widespread power outages. The attacks were facilitated by the use of malware that exploited vulnerabilities in industrial control systems that were connected to the internet. Ring Doorbell Security Issues, in 2019, it was discovered that Ring, a popular brand of smart doorbells, had a security vulnerability that allowed hackers to access live camera feeds and other sensitive data from users' devices. The vulnerability was patched by the manufacturer. These incidents illustrate the importance of addressing security vulnerabilities in IoT devices to prevent potential harm to individuals and critical infrastructure.

These instances happened due to various reasons, such as lack of proper security measures, inadequate implementation of security protocols, use of weak passwords, and unpatched software vulnerabilities, among others. In most cases, the area in IoT security that was lacking was proper authentication and encryption protocols. Many IoT devices are designed to be easy to use, and manufacturers often prioritize convenience over security, leading to weak or non-existent security measures. Additionally, many IoT devices are not designed to receive software updates, making it difficult to address security vulnerabilities after the device has been released. Another area that is often lacking in IoT security is privacy. IoT devices collect vast amounts of data about users, and if this data is not adequately protected, it can be easily accessed by hackers, putting users' personal information at risk.

Companies are taking various steps to improve their security from cyber-attacks on their IoT devices. They are increasingly implementing multi-factor authentication for their IoT devices to prevent unauthorized access. This involves requiring users to provide additional information beyond a password, such as a fingerprint or a code sent to their phone, to verify their identity. Encrypting the data that is transmitted between IoT devices and other systems to prevent unauthorized access. This ensures that even if a hacker intercepts the data, they will not be able to read it. Regular security checks of their IoT devices to identify vulnerabilities and address them before they can be exploited by hackers. This involves testing the devices for vulnerabilities and updating the software to address any issues. These companies are also providing security patches and updates for their IoT devices to address any newly discovered vulnerabilities. These updates are crucial because IoT devices often lack the ability to update themselves automatically, leaving them vulnerable to new security threats and also are improving user education to help users understand the importance of security and how to use their IoT devices safely. This involves providing clear instructions on how to set up and use the devices securely, as well as warning users about common security threats and how to avoid them. This creates an understanding and awareness among users, choosing IoT products based on the encryption, privacy and responsiveness.

User guidelines include, changing these defaults to unique and strong usernames and passwords, regularly check for software updates for their IoT devices and apply them promptly and updating them as they often contain security patches that address known vulnerabilities, avoiding to use public Wi-Fi or other unsecured networks to connect to their IoT devices, as these networks are vulnerable to eavesdropping and man-in-the-middle attacks, disabling any features or services on their IoT devices that are not needed as each service or feature represents a potential entry point for hackers, using antivirus software and firewalls to protect their IoT devices from malware and other security threats. These security measures can help prevent unauthorized access and data breaches.

Hence, IoT security is an increasingly important issue as more devices become connected to the internet. Instances of cyber-attacks on IoT devices, such as the Mirai botnet and the St. Jude Medical pacemaker hack, have demonstrated the potential harm that can be caused by vulnerabilities in these devices. The areas of IoT security that are lacking include proper authentication and encryption protocols and privacy protections. Companies are taking steps to improve their IoT security by implementing multi-factor authentication, encrypting data, conducting regular security audits, providing security updates, and improving user education. Users can also take steps to protect themselves from cyber-attacks by changing default usernames and passwords, keeping software up to date, using secure networks, disabling unnecessary features, using encryption, regularly checking device activity, and using strong security software. Overall, a combination of manufacturer responsibility and user awareness and action is necessary to prevent cyber-attacks on IoT devices and protect users' personal information and critical infrastructure from harm