IOT Security

M.Snehalatha

M.C.A Department

AV College of Arts,Science and Commerce.

ABSTRACT

The Internet of things encompasses many numbers of devices connected using variety of monitoring and controlling functions. These devices will be used for collecting different types of data, tracking the data, analyzing the data and then controlling various manual things. These operations can be performed remotely which initiates the security issues. The expansion of digital devices controlling the non digital devices leads to vulnerabilities and exploit the infrastructures.

Generally the product life cycle begins with analyzing the problem or considering the existing system and then developing the product, testing and deploying the product. All the issues related to the security, risks, attacks will be majorly exposed in implementation phase. Which may be viable in non IOT products? But in the case IOT where the Things are real time entities, the developer should consider the security, risks, attacks etc at design phase.

During the Design phase, in addition to software based security, hardware based security, proving the alarms in case of emergencies should be considered. At the lowest level, the infrastructure should not be complicated to the end user.

The API developed should be user friendly, should be able to support various devices (things) using minimal port which can achieved through Agile methodologies incorporating the secure application development.

Finally security should be intrinsic in the initial phase of IOT product development rather than considering at the end. As the IOT products are developed to serve the mankind, serve the society for better cause, the effort should be taken to avoid the Risks, threats and cyber attacks.

Keywords-Security,Device Security,risk analysis

Introduction

The product life cycle begins with analyzing the problem or considering the existing system and then developing the product, testing and deploying the product. All the issues related to the security, risks, attacks will be majorly exposed in implementation phase. Which may be viable in non IOT products? But in the case IOT where the Things are real time entities, the developer should consider the security, risks, attacks etc at design phase.

IOT applications are introduced in all the sectors beginning from home, cities, hospitals, industries, enter prises, agiculture etc and within five years, it is estimated that each and every device will be connected and tracked. The block chain, biometric and facial recognition system, drones interface system may prone to attack and threat which will impact personal safety and disturb the physical world.

The use of cloud which is open source memory making IOT application cost effective attracting numerous startups to major enterprises. Developing the quick software postponing or not considering the risks and security issues until implementation and the due to feasibility of cost, end customer are increasing exponentially, so malicious attack may become a serious crisis on digitization of devices. Most disgusting thing is that victims don't even aware that their devices are hijacked and used as weapons on the Internet. One solution is that end users and companies should constantly monitor the devices and check for intruders and malicious attacks, which proves to be more efficient.

As there are no rules and regulatory system for the Internet, then IOT standards and Regulations are far away so it is the responsibility of the developers, consumers and organizations to protect the devices connected to the Internet. Global IOT security standards should be made to harden the devices.

Unfortunately IOT vendors put the risk, security and attack at the end of development may create a significant loss of operation. The most alarming scenario is, due to massive growth of the devices on IOT applications, the vendors are giving third party access for the devices, which is helpful for the vendors to come up with upgraded software but consumer devices are under high rate of risk.

Assessing of the IOT devices security should be made mandatory by IOT vendors. These vendors should be able to identify the unauthorized devices or non certified devices should be monitored. Organizations need to conduct audit on security and risk on regular basis and even when situation demands. Even the device management is implemented by the third party, check the permissions of the third party, and update the permission on regular basis. Implement the compliance standards for the vendors also. The mistakes done by third party will have the cascading effect and may cost in-house organization also.

Every IOT vendor should regularly update the software as obsolete software may be ulnerable.Regularly replacing the old hardware makes the process working without any errors. It should be the responsibility of the vendor to keep informed to the consumers of all the threats and warning the consumers to keep upgrading the software in order to avoid the risks of not accessing the deceives or losing the device connection.

IOT vendors should be able to track the traffic congestion and protect the IOT device communication which also protects the devices from attacking. Before connecting the devices to the Internet, the internal device security should be checked to avoid further complications in the IOT Applications. Basically the IOT devices should have the high security features as they will be populated with the smart tools like smartphones, tabs and laptops. Iota security requires company-wide collaboration with the device manufactures and synchronization with them to make sure all endpoints are secured properly. Regularly monitoring of virus and malware should be there to protect the devices form hijacking and may be shutting down the device.

Device segregation also plays a major role, device access list should be designed, and all the devices should not give access to entire system.

The security challenges in IOT system are the privacy of data and information regarding the devices, integration of security and IOT protocols. Integration of security and architectures. Mobility of devices, data management and routing protocols.

IoT devices require hardening after installation to mitigate the threat of compromise. Security solutions can help lock down these devices before cybercriminals attack. Some of the solutions can be

- Carefully read the device’s instructions or contact the manufacturer for support
- Secure home networks and locate IoT devices on the secured networks
- Change all default passwords and user IDs
- Audit devices to determine which ones have default accounts
- Opt for devices made by manufacturers with a track record of security awareness

• Utilize firmware/software updates made available by IoT device providers

• Disable the universal plug-and-play protocol on any routers

• Isolate IoT devices on protected networks

• Perform security testing of IoT devices

• Create an asset inventory that includes mapping the network to discover all paths of ingress and egress; this could allow you to discover that the IoT network has its own internet gateway that is not enterprise-class and does not conform to security policies or applicable laws, regulations and contracts.

• Monitor network access to determine normal behavior and detect anomalies

• Apply access controls between IoT devices and IT resources using enterprise firewalls, intrusion prevention systems, and integration with identity and access management, to the extent that it is supported

• Collaborate with the Internet of Things Security Foundation (IoTSF) to help secure IoT technologies

A cloud content management platform can address these needs, by securing access for everyone in the extended enterprise. With the confidence that corporate information is secure, employees can use digital business processes to work more flexibly and creatively with partners and customers to deliver more-innovative products and services. Storing content in the cloud also supports the Protection for sensitive information, Central storage that simplifies access to all content Visibility and control over who is sharing what a seamless user experience How to integrate security into automated business processes and digital services.

Storing content in the cloud also supports the “single source of truth” model: Everyone is always working with the latest version of information. This means that automated workflows are easier to implement and can operate more smoothly, as content is no longer scattered across multiple systems with their own structure and interfaces. The cloud also reduces the management burden for technical teams, instead enabling them to focus on business activity and shorten time-to-market for new digital services. Having all content centralized in one system—versus storing content across multiple disconnected systems—can make it easier to detect real threats. The cloud also enables security professionals to collect data to track patterns of user/content interactions and behavior. New approaches to the problem, such as machine learning, can help address alert fatigue, by first establishing what "normal" user behavior is and then detecting anomalies. Today's technologies can process logs quickly to detect irregular activity such as malicious data infiltration attempts or inadvertent data loss caused by an inattentive user.

A robust cloud content management platform centralizes and protects your content and extends security controls across your business environment. This approach empowers IT to securely improve content management and collaboration, reduce data loss, maintain compliance, and simplify governance—all while taking advantage of innovations in cloud security.

The Internet of Things provides both businesses and individuals with unparalleled amounts of meaningful data. Yet with this access comes the potential for security compromises, IBM provides a comprehensive solution to address the complexity of IoT security, has security by design engineered into the platform and the infrastructure upon which the platform is based.

The good news for IoT device and solution providers is that there are several industry consortia and groups worldwide, including the Industrial Internet Consortium (IIC), IoT Security Foundation, National Institute of Standards and Technology (NIST)39, and the Alliance for Internet of Things Innovation (AIOTI)40, that are developing IoT frameworks, guidelines and recommendations.

Conclusion

The main objective of IoT security is to preserve privacy, confidentiality, ensure the security of the users, infrastructures, data, and devices of the IoT, and guarantee the availability of the services offered by an IoT ecosystem.

Acknowledgements

Thanks to the Bhavan’s College management and staff for giving this opurtunity

REFERENCES Techrepublic.com