Challenges in IoT Security

Sreelatha Malempati
Prof.& Head, Department of Computer Science & Engineering, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India
lathamoturicse@gmail.com

S J R K Padminivalli V
Assistant Professor, Department of Computer Science & Engineering, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India
srivallivasantham@gmail.com

Abstract— Many IoT devices lack basic security requirements. The small size and limited processing power of many connected devices could inhibit encryption and other robust security measures, People need understanding of limitations of devices due to their size and the approaches for providing security. The challenges for implementing the security of embedded devices and providing end-to –end security are the outcomes of this study.

Keywords— Internet of Things, IoT Security, Embedded devices, Hardware security

1 Introduction

1.1 Internet of Things

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data. The number of IoT devices increased 31% year-over-year to 8.4 billion in the year 2017 and it is estimated that there will be 30 billion devices by 2020. Security is essential for the safe and reliable operation of IoT connected devices.

1.2 Applications

Today, Internet of Things is used in many applications like Home automation: Personal Health Monitoring, Building automation, Industrial automation and Smart cities. The first and most obvious advantage of Smart Homes is comfort and convenience, as more gadgets can deal with more operations which in turn frees up the resident to perform other tasks. In Personal health monitoring, it increase the relationship between consumer/ patient and healthcare providers and payers. Patient engagement and consumer consciousness play an important role here and in the relationship with healthcare payers. Building Automation processes related to energy efficiency, temperature control, security, and even sanitation can improve operations in ways that directly impact the production cost and maintenance cost. In Industrial

automation the The Internet of Things (IoT) helps to create new technologies to solve problems and increase productivity. Lastly in smart cities it helps in managing of city wastes, energy efficient lightening system, environment monitoring.

1.3 Working of an IoT end device

Consider the following IoT device. This is a small micro controller which is connected with a sensor , power supply, actuator and RF transceiver. All these micro controllers will form a network and will be connected to the internet with the help of a gateway as shown in the following figure.

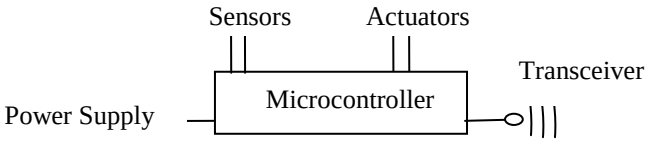

Fig. 1. IoT device

1.4 Iot Elements

IoT devices can communicate with the Internet. The End device send information to the gateway with the help of communication protocol. The information then send to a cloud where the information will be processed and the respective actions will be sent to the receiver device. The following figure illustrates the how Iot devices connect to the internet.

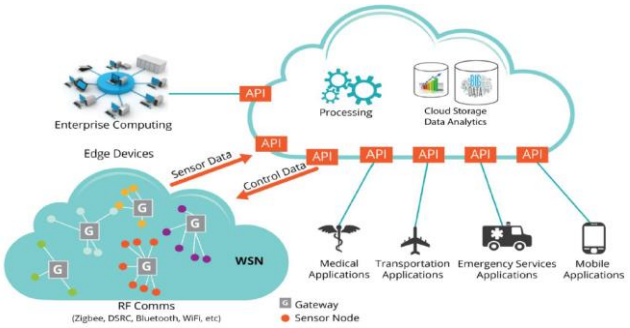

Fig. 2. IoT connecting different platforms

1.5 Communication Models

There are four models to provide communication between devices and the Internet. One of htem is Device-to-Device Communications. In this the devices will communicate autonomously without centralized control and collaborate to gather ,share and forward information. The information will be transformed into intelligence and create a intelligent environment. The quality of information gathered is depend upon the protocol we are using in getting the information. Example is the home automation system. In this small data packets flow in low data rate. Secondly, Device-to-Cloud Communications. Here IoT device connect to application service provider for exchanging data and other control information. The service provider offer cloud services which makes the data storage not a big problem. The application in IoT device has a remote access to the cloud service provider and also can be updated easily. This is useful applications which require remote monitoring. The main limitation is the interoperability between vendor of the device and cloud service provider. Device-to-Gateway Model is another in which the IoT device connect to the application service provider with intermediary device. This gateway provide security, data or protocol translation. It also pairs IoT device and communicates with a cloud service. For example health monitoring app in the smart mobiles will come under this model. The app continuously monitors the respective health parameter and send to the service provider. From there the analysis will be performed and an health alert will be send to the end-user. Lastly, Back-End Data-Sharing Model. Here, the data obtained from the devices are shared between different application service providers. This help in extending the services to the end-users. For example a corporate company easily analyze the data in the cloud produced by the devices. This an extension to Device-cloud communication. Here also interoperability is a major concern.

2 Methodology

IPv6 with 2 to the 128th power addresses, is for all practical purposes inexhaustible. This represents about 340 trillion, trillion, trillion addresses, which is more than the demand of the estimated 100 billion IoT devices going into service in the coming decades. Enables direct connection of physical objects to the Internet using microcontrollers which are constrained in computational power, memory and in power consumption. The main goals are Confidentiality, Integrity and availability. The main threats are Snooping, Traffic Analysis, Spoofing, Replaying, Repudiation, modification, Denial of service.

IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smart phones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded devices are designed for low power consumption, and have limited connectivity. They typically have only as much processing capacity and memory as needed for their tasks. Generally people overlook the risks of internet connected devices without taking proper security measures. The level of security required for an embedded device

varies depending upon the function of the device and the vulnerabilities of the device. Security requirements must take into consideration the cost of a security failure, the risk of attack, available attack vectors, and the cost of implementing a security solution.

IoT security requires an end-to-end approach. Developing secure end-to-end IoT solutions involves multiple levels of security across devices, communications and Cloud. Smart devices is about giving your device the power to evolve, making it more powerful/useful/helpful over time. This work deals with securing IoT devices using proper filters, firewalls, configurations, software updates, OS patches, IoT authentication, encryption and hardware security.

2.1 Addressing of IoT devices

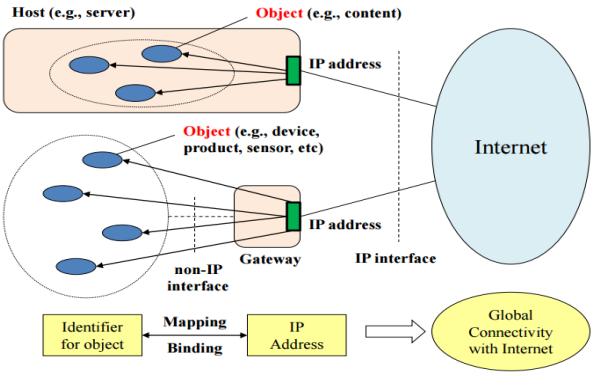

Fig. 3. Addressing scheme

There are many Issues in addressing. They are Compound Object in which an object consists of many objects. The Object Lifetime might range from years or decades down to days or minutes. The ownership & identity relationship between objects. The authentication & authorization procedure in use. The support for mobility in which dynamic objects connect from one network to another. There are many security issues will be there. The main concern is on Protection of Devices, Protection of Data, Secure communication, Secure applications. The Secure communication require use of confidentiality and data integrity mechanisms. To protect the devices against various attacks we have to use a secure operating system environment. We have to choose only those applications where security is a major concern. If we use all of them then the Internet of Things will a good solution for many problems. For addressing we may use IPv6 as it can connect up to 26 billion devices. The non IP interfaces can also be connected to the Internet with the help of the gateways.

2.2 Lifecycle of IoT Security

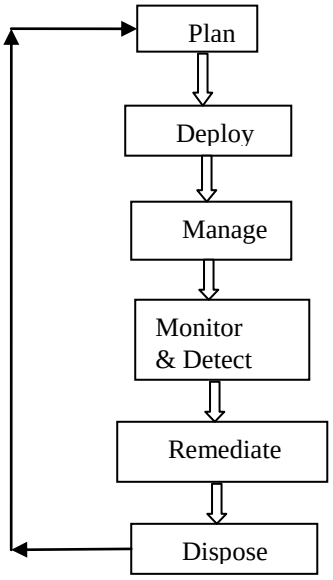

Fig. 4. Lifecycle of IoT security

To protect the devices we can use Code signing and run-time protection. Cryptographically ensure code hasn't been tampered after being "signed" as safe for the device, it can be done at "application" and "firmware" levels. All critical devices should be configured to only run signed code and never run unsigned code. Be sure malicious attacks don't overwrite code after it is loaded. OS hardening, lockdown, white listing, sandboxing, network facing intrusion prevention, behavioral and reputation based security, including blocking, logging, and alerting .Many chipmakers already build "secure boot" capabilities into their chips. Open-source, and client-side libraries like OpenSSL can be used to check signatures of code. Challenge is "managing the keys," and "controlling access to the keys" for code signing and protection of embedded software. Some Cas offer hosted services that make it easy to safely and securely administer code-signing. Sign and update individual blocks or chunks of updates and not force anyone to sign entire monolithic images, or even an entire binary file. Software signed at the block or chunk levels can enable updates to be done with much finer granularity without sacrificing security and without having to sacrifice the battery for security. When the devices are reverse engineered, vulnerabilities are discovered and exploited, they need to be patched as quickly as

possible. Code obfuscation and code encryption can considerably slow down the reverse engineering process, but not entirely prevent reverse engineering. Over-the air (OTA) manageability must be built into devices before they ship for software / firmware security patches and functionality updates. Threats can defeat all of those countermeasures, best understand your system, identify anomalies that might be suspicious or dangerous, malicious or not, diagnostics and remediation.

For Data at Rest Encryption, protect information in case of device theft/loss. For Data in Transit Confidentiality, Integrity, Authentication is required. For Data in Use Trusted execution environment, Trust Zone- ARM is used. For Data Loss Prevention Sensitive data not to be distributed outside of the user base or network.

2.3 Secure Communications

The IoT devices are having very less memory requirements. Using of encryption algorithms such as DES, AES etc makes impossible. So better algorithm is elliptic curve cryptography for providing confidentiality for the messages. But this requires key certificates to be securely exchange between the devices. A number of certificate authorities are there to provide the embedded "device certificates". By using this certificates we can exchange the securely between the devices. Certificates are transferred with the help of the protocols such as Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST), and Online Certificate Status Protocol (OCSP). With a strong CA helping to handle certificates, keys and credentials, authentication can easily be done by standards like Transport Layer Security (TLS) and Datagram TLS (DTLS). Each browser has a few "roots" of trust against which all certificates are evaluated. Embedding these roots into browsers enabled security to scale to millions of servers on the web.

3 Other Security Considerations

3.1 Application Level Considerations

Applications (could be web, mobile, cloud, etc.) must be developed with industry standard secure coding practices such as OWASP, SAFECode, SANS/CWE, etc. to minimize the risk of application related attacks. E.g. preventing SQLi, XSS, data leakage, session replay, buffer overflow attacks, etc. Leveraging best practices such as file restrictions (e.g. type, size),input validation, etc. Scanning/ testing the applications (dynamic, static, hybrid) for vulnerabilities and taking corrective measures.

3.2 Device and Gateway Security

The device security is also major concern as they are also vulnerable to do the attacks. So mechanisms such as disabling external device connectivity e.g. USB

drives, disabling direct internet access from sensitive devices/endpoints if not required, disabling or blocking of unused services such as open ports, insecure protocols, Secure booting (using keys) and Secure firmware, authentication of devices during connection, applying regular patches on device OS, etc, Secure and authenticated firmware upgrades, establishing connections with white listing instead of blacklisting devices, using of secure key exchange protocols can be implemented in the IoT devices to enhance the device security. Another important place where security can be considered is gateway security. Intruders can enter into the network wit the help of gateway. So ensure that the IoT/M2M gateway is secured from intrusions and malware by using appropriate mechanisms such as ACLs, IPS, filtering, etc.

3.3 Device constraints

Facilities should have adequate physical security such as security guards, access cards, visitor logs, CCTV cameras, secure zones, etc. for preventing unauthorized access. Appropriate security mechanisms should be leveraged for isolating sensitive information bearing segments such as IDS/IPS, firewalls, network ACLs, etc. Service provider should obtain and produce assurance certifications such as ISO 27001 SSAE/ISAE SOC reports, privacy seals, etc. Allow only strong authentication (e.g. MFA) for remote access to privileged users like administrators, clinicians, maintenance personnel for logging in securely from outside the company network. Usage of secure communication channels such as VPNs-S2S, C2S for regular employees accessing the company network from branch offices or outside locations and disabling that access when no longer needed .

3.4 Challenges to be considered

The cryptographic algorithms should work on tiny, low-power devices. Lightweight, fast and secure communication protocols are to be used in IoT devices. Hardened operating systems and secure applications are to be used across all devices. Usability concerns and privacy issues are to be

4 Conclusion and Future work

IoT security is complicated by the fact that many ‘things’ use simple processors and operating systems that may not support sophisticated security approaches. Awareness is required in the public about IoT security challenges and the proposed solutions. We are thinking to enhance the security policies for the IoT communication so that an attacker may not have a chance to do attacks.

5 References

1. Oladayo Bello,Sherali Zeadally(2016).Intelligent Device-to-device communication in the Internet-of-things.IEEE Journal .pp 1172-1182.
2. Santosh Kulkarni, Prof.Sanjeev Kulkarni(2017).Communication Models in Internet of Things:A survey .International Journal of Science Technology and Engineering.pp 88-91. Vol.3,Issue 11.
3. Abdur Rahmin Biswas, Raffaele Giaffrede (2014).IoT and Cloud Convergence.IEEE World Forum on Internet of Things.
4. Ahmed B. Altamimi and Rabie A. Ramadan (2016).Towards Internet Of Things Modelling:a gateway approach.Complex Adaptive systems modeling.
5. Eli De Poorter, Ingrid Moerman,Piet demeester(2011). Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented architecture.EURASIP journal of wireless communications and networking.
6. S.Yoon,J.Kim(2017).Remote security management server for IoT devices.International conference on information communication technology convergence,Jeju,South Korea.
7. S.oh,Y.Kim(2017).Development of IoT security component for interoperability. 13th International computer engineering conference,Ciaro Egypt.
8. Dr.G.N.K.Suresh Babu,Dr.M.Kumaraswamy (2018). Security considerations for IoT technologies. International Journal of Advance Engineering and research development.pp.1592-1599.Vol.5.Issue.4.
9. E.Ezema,A.Abdullah,NFM Sani(2018).A Comprehensive Survey of Security Related Challenges in Internet of Things.International journal of new computer architectures and their applications.pp.160-167.vol.8,No.3.
10. R.T.Tiburski,L.A.Amaral,Everton deMatos,Dario F.G de Azevedo,Fabiano Hessel(2016).The Role of Lightweight Approaches Towards the standardization of a Security Architecture for IoT Middleware Systems.IEEE Communications Magazine.pp.56-62,vol.54,Issue.34.