VIEW POINT

IoT Security Assurance

Abstract

IoT is one of the rapidly growing emerging technologies. It is entering in all walks of our life with connected cars, connected smart homes, connected healthcare, wearables, etc. and exchanging large amount of sensitive/PII information over internet. This increases the security risk of IoT devices. In this document we are proposing an approach for security assessment of various IoT components.

Infosys
be more

Introduction

New testing processes and tools are developed continuously to improve the quality of software. Today, the IT industry is gaining momentum in agile deliveries and development and operations (DevOps), which is creating new possibilities by integrating development, test, and operations teams. To keep pace with these changes, testing processes and tools need transformation such that testing platforms can be accessible to all stakeholders and made simple.

IoT Applications

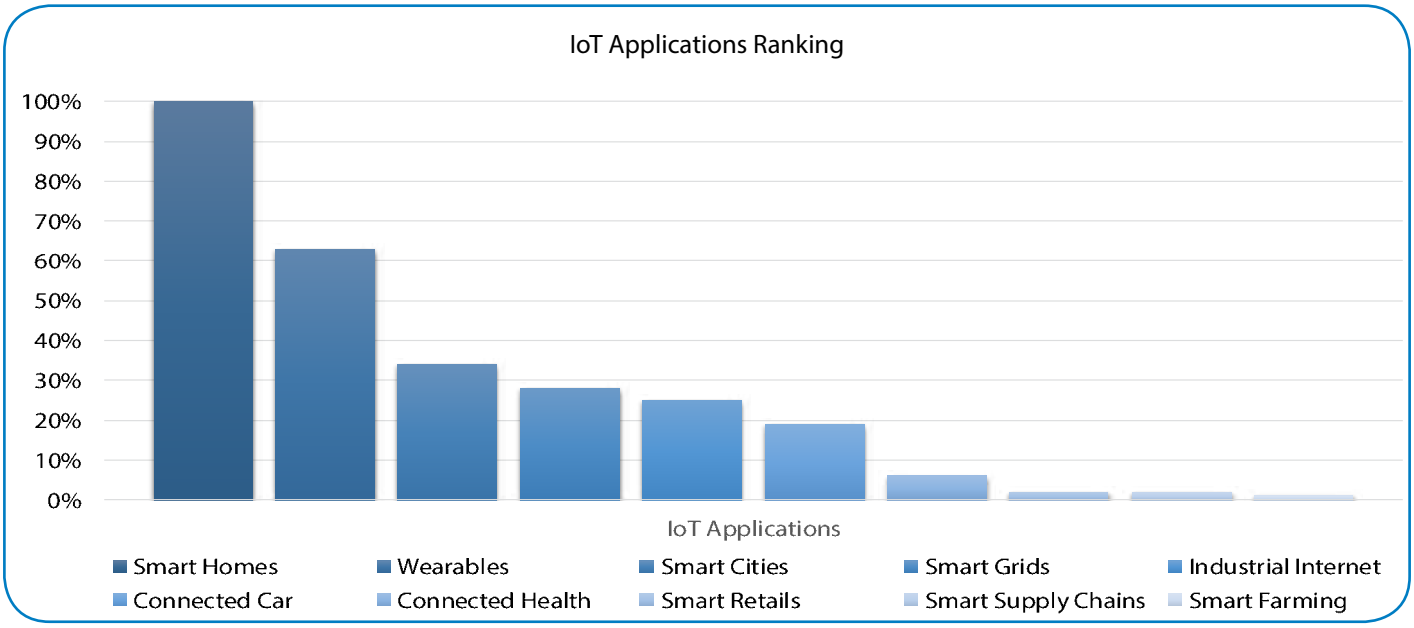

Figure 1. Ranking of the IoT applications

It's evident from the above figure that IoT devices have multi-dimensional usage and are omnipresent. Well, this wide variety of IoT applications poses some interesting use cases with respect to security of data. Suppose you're using a mobile app for unlocking and controlling peripherals like air conditioning, music system etc., of a vehicle. If someone is able to intercept into the communication channel, say Wi-Fi, used between app and peripheral receiver. The attacker would be able to pose threat to the owner as well as the vehicle.

IoT Systems Architecture

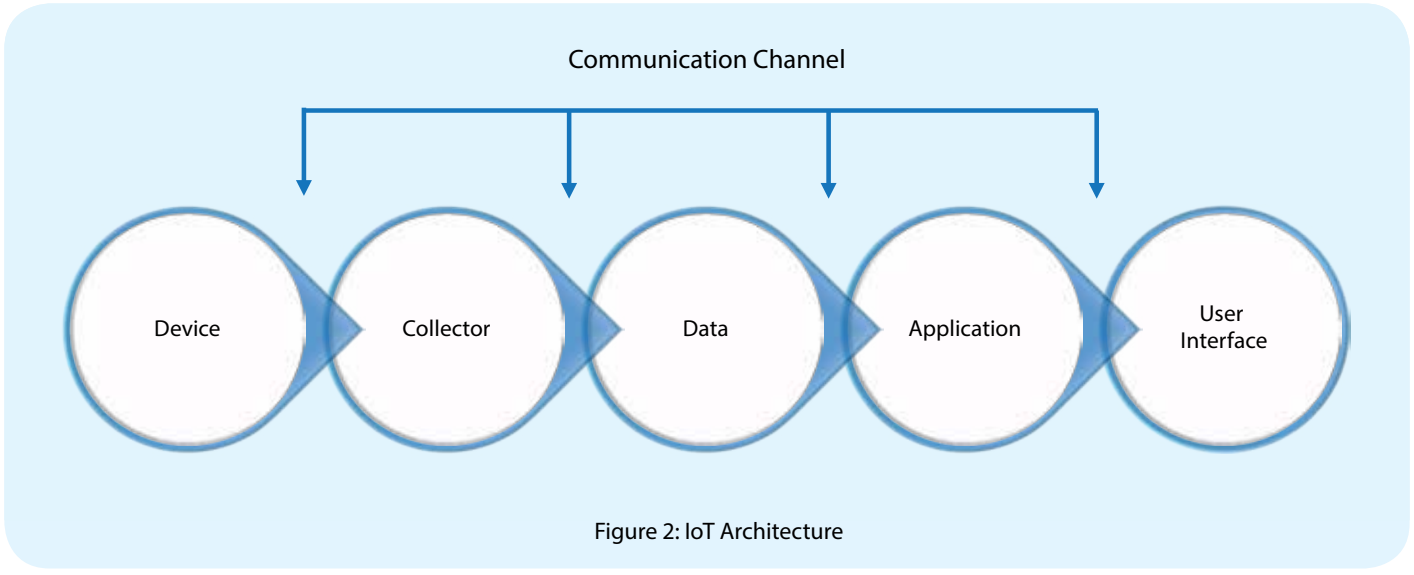

Figure 2: IoT Architecture

I. Device - Sensors, actuators for monitoring and notifying the events.

II. Collector – systems to collect and pre-process the data sent by sensors

III. Data – repository of data accumulated after pre-processing, it can be local or cloud as well

IV. Application – processes the data according to the required usage

V. User Interface – Web or mobile app interface which provides relevant information to the user

VI. Communication Channel – wired or wireless communication link between two layers, it may be entirely absent for a locally connected layer, say when collector and data layers reside on same system.

Attack Surfaces

The Internet of Things infrastructure can be divided mainly into four components,

1. Devices (Gateways, Sensors, Actuators)
2. Communication Channel (Wi-Fi, Bluetooth)
3. Cloud Interface
4. Application Interface (mobile and/or web)

Components	Attack Surface
Devices (Sensors, Gateways)	Device memory, firmware, physical interfaces like USB ports, web interfaces, admin interfaces, Update Mechanism
Communication Channel	Device Network traffic using LAN, Wireless (Wi-Fi, ZigBee, Bluetooth)
Cloud Interface	Getting access to sensitive data/PII stored on cloud by Injection attacks, weak passwords or default credentials, Insecure Transport encryption.
Application Interface (Web and mobile)	Getting access to sensitive data or PII by exploiting vulnerabilities like OWASP web and mobile Top 10, in application interfaces.

Table – IoT components are their attack surfaces

Latest attacks

The insecure implementation of IoT devices are routinely being hacked and even used as accessories in cyber-attacks.

1. Hotel Room Locks prone to Hacking Device: -

   Onity United Technologies are leading supplier of electronic locking system. A Mozilla developer Cody found vulnerabilities in the locks in 2012. The device created by Cody reads the lock's memory and gets the cryptographic key information. It sends that information to the door lock which allows the hacker to gain access to the room.

2. Massive DDoS attacks zombies 25,513 CCTV cameras: -

   Researchers from Sucuri have claimed that CCTV cameras can and are being used for DoS attacks. The attackers use these cameras as botnets. The attack may last for days and could surge to a several thousand HTTP requests per second. Following pie chart depicts the distribution of CCTV Botnets.

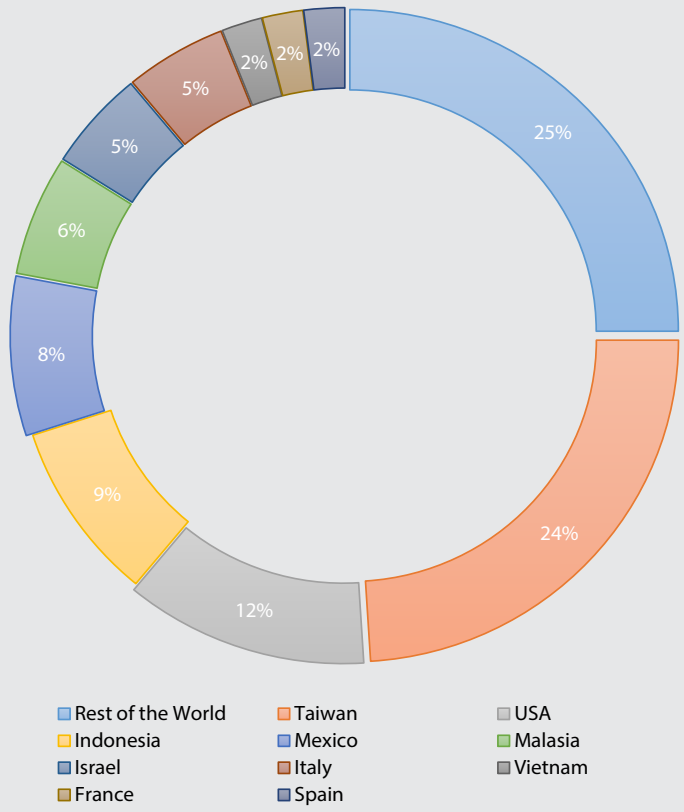

Figure 3. CCTV DDoS Botnet Geographic Distribution

(Data Courtesy: https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html)

3. Nissan Leaf electric cars hack vulnerability disclosed: -

2016 has proved out to be a bad year for IoT security after all. In early 2016 Troy Hunt, and Australian web security expert demonstrated how Nissan Leaf's companion app can be used to hack the vehicle. Even the app was optional, as a simple web request via a browser was able to control vehicle AC, Heating system and may also reveal the owner's identity, if its VIN was known. This was proved by the researcher while sitting on a computer in Australia, controlling systems of a vehicle that belonged to an acquaintance of his in United Kingdom! Though, the criticality of the issue may not be life threatening but could still be used to drain car battery for least to say, which in turn can leave the owner in perilous situations.

Thus, the security incidents discussed are examples of how lack of security measures in IoT devices can not only compromise personal security but also can be leveraged to impact security of other internet services as well.

Figure 4. Extent of attack on Nissan Leaf

Infosys security assessment approach for IoT

Following practices should be followed while designing an IoT system, to ensure security: -

If any other protocols like ZigBee is used, then following methods can be implemented to mitigate any possible security issues:

1. Implement AES Encryption. It provides confidentiality as well as integrity.
2. Implement Master Keys to secure Key Establishment Procedure.
3. Implement Link Keys to encrypt the information sent across nodes.
4. Implement Network Keys to authenticate and validate each device which attempts to join the network.

If MQTT protocol is being used, then follow following methods.

1. A firewall with sophisticated ruleset should be implemented for every connection to a MQTT broker.
2. Block all the UDP packets as MQTT uses TCP.
3. All the ICMP packets should not be blocked as response to PING and TRACEROUTE will be hampered. Instead, investigation of ICMP packets is good approach.
4. Traffic to any ports which are not needed for the MQTT system should be blocked. Following are MQTT ports
   - 1883: This is the default port for MQTT over TCP.
   - 8883: This is the default port for MQTT over TLS.
   - Use MQTT over TLS for all communications.
   - Use updated software for all the component as they will be fixed for older security vulnerabilities.]
   - Apart from above guidelines implementation of Demilitarized Zones and Load Balancers will further strengthen the security of the system.

Recommended security testing approach for each layer of IOT stack is as follows

Sensor : Hardware	
Security threats	Security assessment test case
L2: Insufficient Authentication/ Authorization	Check for Password Complexity and Password Recovery mechanism for device Check for poorly Protected Credentials and inefficient two Factor Authentication
L3: Insecure Network Services	Check for Role Based Access Control Check for open ports, check if there are any unnecessary ports utilized.
L5: Privacy Concerns	Check if getting access to device memory to get sensitive/personal data stored, encryption keys, certificates is allowed
L8: Insufficient Security Configurability	Check if Firmware extraction and modification is possible Check for User or Admin Command Line Interface issues
L10:Poor Physical Security	Privilege escalation Check if device can be reset to insecure state or default state Check if device or internal memory can be accessed via USB ports and SD cards

Sensor : Software	
Security threats	Security assessment test case
L3: Insecure Network Services	Radio communication analysis between device and the gateway by attacking ZigBee, zWave, 6LoWPAN
L9:Insecure Firmware/ Software	Attacking Bluetooth Low Energy (BLE) Checking if device has direct connection - connecting to mobile app which is in same network Check for firmware Update Functionality Check if firmware Contains Sensitive Information Check if firmware update functionality is using encryption and secure communication and update file encrypted Check for insecure or misconfigured services like FTP, Telnet , TFTP, Finger, SMB, e.g. misconfigured NAT-PMP services, hard-coded Telnet logins

Gateway (Raspberry Pi: USB)	
Security threats	Security assessment test case
L2: Insufficient Authentication/ Authorization	Check for Password Complexity and Password Recovery mechanism for device Check for poorly Protected Credentials and inefficient two Factor Authentication
L3: Insecure Network Services	Check for Role Based Access Control Check for open ports, check if there are any unnecessary ports utilized.
L5: Privacy Concerns	Check if getting access to device memory to get sensitive/personal data stored, encryptio keys, certificates is allowed
L8: Insufficient Security Configurability	Check if Firmware extraction and modification is possible Check for User or Admin Command Line Interface issues
L10:Poor Physical Security	Privilege escalation Check if device can be reset to insecure state or default state Check if device or internal memory can be accessed via USB ports and SD cards

Message broker	
Security threats	Security assessment test case
L4: Lack Of Transport Encryption **Insecure Data Storage**	Check for sensitive data stored on Kafka as it does not support encryption of data at rest Check if configuration files can be accessed and modified

Cloud Interface	
Security threats	Security assessment test case
I6: Insecure Cloud Interface **OWASP Cloud Top 10 vulnerabilities** **Arbitrary Code Execution**	Check for Insufficient authentication, lack of transport encryption and account enumeration to access data or controls via the cloud website. Check if firewall is configured (if the master of the cluster is exposed to the internet without having any firewall in between then anyone with access to the master URI can submit jobs to the cluster remotely) Check for arbitrary code execution Check for OWASP Cloud Top 10 risks R1: Accountability & Data Risk R2: User Identity Federation R3: Regulatory Compliance R4: Business Continuity & Resiliency R5: User Privacy & Secondary Usage of Data R6: Service & Data Integration R7: Multi-tenancy & Physical Security R8: Incidence Analysis & Forensics R9: Infrastructure Security R10: Non-production Environment Exposure

Application-Web Interface	
Security threats	Security assessment test case
I1: Insecure Web Interface **OWASP Web Top 10 vulnerabilities**	Check for OWASP web Top 10 issues A1:Injection A2:Broken Authentication and Session Management A3:Cross-Site Scripting (XSS) A4:Insecure Direct Object References A5:Security Misconfiguration A6:Sensitive Data Exposure A7:Missing function level control A8:CSRF A9:Using vulnerabilities from known unknown components A10Unvalidated Redirects and Forwards

Application-Web Interface	
Security threats	Security assessment test case
I7: Insecure Mobile Interface **OWASP Mobile Top 10 vulnerabilities**	Check for OWASP Mobile Top 10 issues M1: Weak Server Side Controls M2: Insecure Data Storage M3: Insufficient Transport Layer Protection M4: Unintended Data Leakage M5: Poor Authorization and Authentication M6: Broken Cryptography M7: Client Side Injection M8: Security Decisions Via Untrusted Inputs M9: Improper Session Handling M10: Lack of Binary Protections

Conclusion

IoT is no doubt a fascinating, yet emerging technology. The prioritization of rapid development over security by the developers has caused rise of new IoT vulnerabilities. A large number of IoT devices have already become victims of hacks, botnets and other attacks constantly. Proper security frameworks for IoT, like .NET, Java, Android and iOS, should be made available. IoT solution developers must have security know how. IoT application development should follow secure development life cycle, security tests have to be mandatory. In addition to these, advance approaches like machine learning can also be applied to ensure the IoT security.

About the authors

- Amitesh Gaurav is the Systems Engineer working with Infosys Center for Emerging Technology Solutions group. He works as Security analyst. His focus areas are Web, Mobile and IOT Application security assurance.
- Jayaprakash Govindaraj is the Senior Technology Architect, and leads Security CoE at Infosys Center for Emerging Technology Solutions group. His focus areas are Web, Mobile and IOT Applications Security Assurance, Secure Development and Managed Security Services.

References:

1. http://www.forbes.com/sites/thomasbrewster/2014/11/07/car-safety-tool-could-have-given-hackers-control-of-your-vehicle/#2b98d1ef21b0
2. http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html
3. http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf
4. http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc
5. http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf
6. http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-Iotecosystem.pdf
7. http://internetofthingsagenda.techtarget.com/info/getstarted/Internet-of-Things-IoT-Security-Threats
8. http://internetofthingswiki.com/iot-trends-in-2016/300/
9. http://internetofthingswiki.com/iot-trends-in-2016/300/
10. https://iotsecuritywiki.com/

For more information, contact askus@infosys.com

Infosys be more