International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Internet of Things, Security A Bigger Task than Development?

Sheetal Kasale[1], Pingale Murali Manish[2]

[1](BCA II Year), [2](B.Com(Hons) III Year), Bhavan's Vivekananda College, Sainikpuri, Secunderbad ,Telangana (India)

ABSTRACT: *Ubiquitous sensing along with Radio Frequency Identification (RFID) enabled by Wireless Sensing Network (WSN) transforms the normal internet into The Internet Of Things (IOT) , where every gadget around you is smart and enables machine to machine communication with sensors and acuatators becoming a part of our environment ,where this information is shared across various platforms transforming IOT from a single technology to a global concept . A world where digital , real and virtual create smart environment .In this era where SMART is the new GREEN , the transition from closed public enterprise networks to public internet is justly raising alarms about security . As we become increasingly reliant on this smart devices , their intrusions and interferences threaten public safety. Be it cyber attacks like Mirai Botnet Attack , Sybil Attacks or Hello Flood Attacks , the number of attacks are increasing with the inventions . These attacks are due to various challenges in Internet Of Things (IOT) architecture from the microcontrollers to challenges faced by Big Data , Data security , Cryptography and Authorization Issues . This paper discusses most of the issues faced by Internet Of Things (IOT) architecture and privacy - breach challenges due to various attacks and the solutions for these challenges .*

Keywords : **Wireless Sensor Network , Cyber Attack , Privacy Breach , Data Security , Internet Of Things Architecture .**

OBJECTIVES

1. To examine and analyse the IOT Architecture following the OSI Model .
2. To classify the security issues on the basis of OSI Model .
3. To study the scope of IOT in terms of security .
4. To find better security solutions .

INTRODUCTION

'Internet Of Things' is a rapidly changing paradigm which is self analysing based on standardised communicable protocols where non living things use embedded technology , gateways and clouds to stay connected to the internet , which distinguishes it from the traditional internet. IOT is growing at a perilously quick pace and researches estimate that by 2020 , the quantity of active wireless devices can exceed fifty billion .For this technology and its services to stay synchronised , it needs to coordinate in the form of network with standard protocols .

IOT AND NETWORKING

Networking technologies enable intercommunication among IOT Components . Standard protocols specify the rules and formats that devices use for establishing and managing networks as well as for transmission of data across those networks . The most widely accepted model of how these protocols and components should be designed in a network architecture is given by the OSI model . [1]

Open System Interconnect Model

It is not a protocol but is a model to organize protocols for making the network architecture most flexible and robust . OSI is taken as a reference to explain IOT Architecture .It delegates the task to seven layers , from below :

1. Physical - Defines the topology and transmission mode
2. Data Link - It Consists of two layers namely Media Access Control - (Checks for transmission errors and converts bits into data frames) and Logical Link Control - (Identifies devices by MAC Address)
3. Network - It delivers data packets to logical addresses (IP) using Routing Algorithms.
4. Transport - It segments, numbers, reassembles the packets without errors .
5. Session - It communicates and synchronizes connections between networks.

6. Presentation - It Compresses, Encrypts, Decrypts the data.
7. Application - Deals with user interface and services.

The weak points in each layer are exploited by unethical hackers, so this Classification helps in better identification of the drawbacks at each layer . The issues regarding each layer can be discussed . [3] [10]

ISSUES AND CHALLENGES

Physical Layer

The main Challenges faced by the tangible components are

1. Device Duplication
2. Sleep Mode
3. Node Impersonation
4. Node Encryption
5. Faulty Hubs and Repeaters
6. Cipher Block Chaining
7. Bandwidth Problems

Solution -
Regular Updation of Network and Authentication algorithms and Node Identity checks and control laid down by Administrator .

Data Link Layer - The issues are

1. Sink Hole Attack
2. Boot Strapping issues
3. Physical Address Authentication
4. Traffic Control and Over- Loading issues

Solution -
Checking Virtual Local Area Network (VLAN) and MAC Addressing and check Spanning Tree Protocol (Manages Network loops) . Maintaining unique keys and identifying Traffic while boot strapping into the network, double securing the boot strap algorithms to prevent intrusion.

Network Layer - The issues are

1. Worm Hole Attack
2. Sybil Attack
3. Hello Flood Attack
4. Faulty Routing Algorithms

Solution -
Mapping routes and having alternate multipath to prevent malicious routes , Checking for Incorrect device configurations to prevent identity spoofing , usage of few troubleshooting commands (ping , trace) which will let us know whether the network connection is working properly .

Transport Layer - The issues are

1. Black Hole Attack
2. Selective Forwarding
3. Over claiming or misclaiming
4. Unauthorised Filtering of packets

Solution -
Data Security Lifecycle Management , Identifier and Authenticator , Proper numbering and Service Point Address checks to ensure packet delivery . Verification of Firewalls , and disabling of Quality of Services (QoS) as it is the reason for many network issues .

Session Layer - The issues are

1. Eavesdropping into Interprocess communication to disrupt working
2. Failure to Identify missing data or Data Falsification

Solution -
Double check the order and originality of the packets .

Presentation Layer - As this layer deals with data and it's encryption , the issues are

1. Big Data issues like Data or Identity theft\Falsification
2. IP Server \ Network Manipulation
3. Cryptography \ Encryption Issues

Solution
Checking for Faulty Description Algorithms .
Checking for Failure of Complete Encryption.

Application Layer -

1. It comprises of all the Back-End Issues faced by Administrators
2. Securing App Platforms and Clouds
3. Denial of Service(DOS) and Distributed Denial of Service (DDOS)
4. Mirai Botnet
5. Bricker Bot
6. Data Manipulation
7. Threat of Exposure of routing information
8. Draining of resources
9. Filling of Memory
10. Network taken down

Solution -
Restricted access to working related information.
Double check of access permission and credibility of data.
Acknowledging memory allocation level .
Acknowledging before changing of key algorithms .
Access request to main administrator .
Regular check of functioning of the back-bone algorithms .

VIOLATIONS AND CRITICISMS

There are several critics and sceptics concerning security and regulation within the net of Things. In 2013, the FTC used an organization known as trendnet inc, that produces wireless webcams. The FTC believed that trendnet did not provide enough security for end-users. In

the end, In the top, over 700 webcams were compromised and even some geographical info was compromised [Dimov13]. Despite these actions, several sceptics believe the Federal Trade Commission won't be able to regulate privacy within the IoT. One reason is attributable to the big selection and amount of makers. Regulation for each manufacturer, which builds very specific devices, is inconceivable. Other critics and experts believe software patching and updating will not be feasible for many applications of the IoT [Schneier14]. At the same time, with such growth in the industry, the FTC is slow and ineffective as a deterrent [Clearfield13]. As the IoT develop towards medical fields and conveyance automation, security and privacy is come back physical threats to users. [Chris Lu4]

SUGGESTIONS :

1. Checking plugging and working of cables, devices and transmission media .
2. Hub information should be properly encrypted and repeaters should be placed to prevent data loss.
3. Signal attenuation and disturbance should be taken care of.
4. Usage of commands like 'netstat' displays the network connections, routing tables and network protocol statistics for a regular check .
5. MQ telemetry transport protocol developed by IBM ,taken up by OASIS can be used for communication with low-bandwidth devices .
6. Application Package Interface governs data flow and protects sensitive information should be double-secured .
7. Protocols like User Datagram Protocol, transmission control protocol , stream control protocol ,see the error in data or length and sequence the stream of data should be used in transport layer to protect the network from DoS attack .
8. Login and authentication locks should be activated at all times.
9. One time infiltration of permitted users should be done.
10. Bit locker encryption introduced by Microsoft should be used for secure booting technology.
11. Introduction of software upgrades to prevent bugs and theft of safety algorithms.
12. Hardware secure modules should be used for for key generation, an example of it is system on chip embedding hardware support
13. Commands like 'TCPdump' and 'NSlookup' should be used to analyze packets and for IP address mapping respectively .
14. Gemalto software solutions could be used for securing devices, clouds and lifecycle management and also using 'software information and event management' process .
15. Usage of transport layer security and datagram transport layer security in transport and application layer .
16. Security key exchange algorithms should be treated as sensitive information and must be given limited access .
17. Pure VPN encryption of online communication .
18. Analyse the traffic flow and network flow pattern in personal networks .
19. Encouragement of usage of peer to peer communication incase of breakdown of network .
20. Network and transport layer should use extensible authentication(EAP), internet key exchange version 2(IKEv2) and host identity protocol (HIP) and also data security lifecycle management identifier and authenticator .
21. Regular updation and changing of algorithms to prevent data theft or falsification.

CONCLUSION :

Indeed security of the internet of things is a tougher task than it's development. Security should be focused more because large attacks like Mirai Botnet attacks flooded 150000 devices with more than 1tb per second and bought down large sites like Reddit, Airnbnb and so on. Companies like Microsoft acquiring Azure, Soltair and now Cloud flare is a huge plus point as it paves way for collaborations in striving to make one global technological community , it is also the user's individual responsibility to administer the safety and security of the device and their personal network and also the security must be administered since day 1 and should at any cost be not neglected. Also regular updation of software should be done. Thus these things help in making the internet of secure things .[1]

REFERENCES

1. Data Communications and Networking By Behrouz A Forouzan.
2. https://www.purevpn.com/blog/iot-the-biggest-security-nightmare/

3. https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017
4. https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/
5. https://techcrunch.com/2016/05/03/microsoft-acquires-italian-iot-company-solair/
6. https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devices-from-being-forced-into-botnet-slavery/
7. https://techcrunch.com/2017/04/20/microsoft-launches-new-iot-services-for-the-enterprise/
8. https://techcrunch.com/2017/04/27/cloudflare-debuts-a-security-solution-for-iot/
9. http://www.computernetworkingnotes.com/ccna-study-guide/osi-model-advantages-and-basic-purpose-explained.html
10. https://www.ibm.com/developerworks/library/iot-lp101-connectivity-network-protocols/index.html
11. http://platinumcctv.com/securing-your-ip-cameras-iot
12. https://techcrunch.com/2017/04/25/brickerbot-is-a-vigilante-worm-that-destroys-insecure-iot-devices/