ISSN (Online) : 2454 -7190 **ISSN (Print) 0973-8975**
Copyright reserved © J.Mech.Cont.& Math. Sci., Vol.-14, No.2, March-April (2019) pp 509-520

IoT Security: A review of vulnerabilities and security protocols

[1*]Ravi Kiran Varma P, [2]Priyanka M, [3]Vamsi Krishna BS

[4]Subba Raju KV

[1234] Department of Computer Science and Engineering, MVGR College of Engineering, Vizianagaram, Andhra Pradesh, India

[1]ravikiranvarmap, [2] priyanka.mandapati, [3] bsvamsikrishna, [4]srkakarlapudi@gmail.com

Corresponding Author: Ravi Kiran Varma P

Email: ravikiranvarmap@gmail.com

https://doi.org/10.26782/jmcms.2019.04.00037

Abstract

Internet of Things (IoT) technology is ubiquitous. In the past decade there was an exponential growth in IoT deployments, so as the potential danger of attacks and threats using IoT devices. The privacy of an individual can be breached and the sensitive information can be disclosed if proper security measures are not in place in the IoT device. A patient monitoring system using an IoT device is vulnerable to many such threats. Even centrifuges and atomic reactors were fallen victim of an industrial security breach caused by popular malware like slammer and Stuxnet. Vehicular and personal gadgets are vulnerable to IoT vulnerabilities that may lead to a leak of information to potential insurance companies and thereby increase of premiums. Our own homes including energy meters, IP cameras, and security monitoring systems may be taken control by hackers if there exist vulnerabilities in the IoT devices. This paper, discusses on IoT vulnerabilities by surveying several sectors of IoT and proposes several security measures that can be implemented to minimize those vulnerabilities.

Keywords : Internet of Things, IoT, Vulnerabilities, Security Issues, Protocols, IoT Security.

I. Introduction

The Internet of Things (IoT) and its applications are proliferating. The very fact that the IoT devices are connected to the internet, so is the threat of attackers. A mere IoT based solution does not help unless it the device is protected with appropriate security measures and protocols [IV][X][XIII]. This article discusses the vulnerabilities that are caused due to IoT in different areas. A specified architecture has been developed for IoT communication. They are many models proposed but

commonly used is the five-layer architecture. Figure 1 represents the different models or architectures proposed for IoT communication. Generally IoT deployments may consist of three-layer or a five-layer architecture[XVI]. In this paper we will also discuss the different security protocols which are used in different layers of IoT architecture.

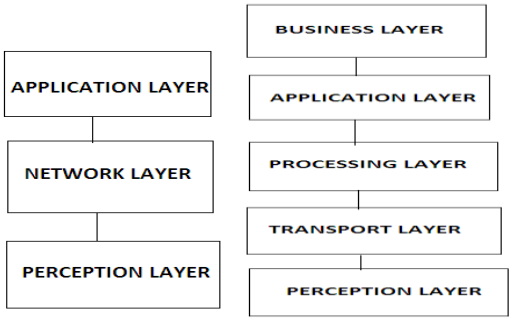

Fig 1.Three-layered and Five-layered architecture

II. IoT Vulnerabilities in different Verticals

IoT Health Care

The use of IoT devices in monitoring the health care of patients have become an attractive application in the present days. The following are the application [XIV]where IoT has been usedconcerning health care

- Sensing of the level of glucose or level of sugar in the blood, which is done by using a device which is directly connected to the main system where it being monitored through the network.
- An application or device has also been developedto monitor the heart rate of the patients over a prolonged period, measured by electrocardiography.
- Blood pressure of users is also monitored remotely.
- There are several other applications like the monitoring of pulse, Body temperature and also applications which would manage the medicines that he/she have to take according to the disease.

Generally these applications are done by either the use of mobile phone applications or the wearable devices. These applications have been playing a major role in healthcare due to its benefits. Table 1 gives us a detailed list of benefits the IoT healthcare devices are offering

Table 1. IoT devices with benefits

IoT device	Benefits
Mobile applications	• Cost reduction. • Communication has become easy between the user and the doctor. • Remote monitoring.
Wearable Devices	• These made the interaction between the users and doctor easy. • Treatment now became personalized.

Vulnerabilities

Privacy of patients: IoT devices based on Android applications are growing rapidly. The smartphones containing the health care information of patients are connected to the IoT devices. Thisis done when a person installs a particular application. This lead to a vulnerability since attackers are making use of these applications which are unprotected to extract information or sensitive data of the patients. They generally use methods such as reverse engineering. This lead to a greater effect on the privacy of the patient. Not only privacy but the intellectual property of the patients are also affected.

The greater risk is caused when the user installs the particular application and when they are asked to grant permission to access the device. The users are not aware of the risks that would be caused due to this. Mainly Android devices are more prone to such malicious events to take place than the Io's devices.

Solution: To protect the mobile applications from vulnerabilities such as reverse engineering, code Obfuscation technique proposed in [IX] can be used. This is nothing but the actual code is changed into a form that is not understood easily. It is in encrypted form. They are generally applied to the API's of the mobile phones to protect them. In general to protect a device or application from the threats three key points need to be kept in mind. They are: predict, prevent and detect (Fig. 2).

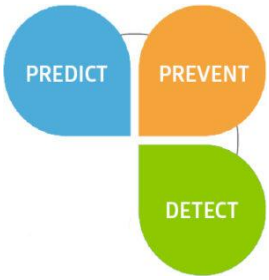

Fig. 2. Fundamental aspects of Mobile app security

Safety of Patients: This vulnerability mainly occurs by the applications which are connected to wearable devices. These applications may be destroyed by the attackers

which may cause physical harm to the users. The data which is being collected from the wearable devices may become an exploit to the hackers in gaining sensitive information. Generally attacks such as Return Oriented Programming (ROP)[IX] arise when devices are not secured. This type of attack allows the attacker to run any type of malicious code under any security defenses. Small instructions known as gadgets are used in this type of attack. To implement this code a stack data structure needs to be used. The return address of each instruction is stored in this stack. To keep track of pointers which points to the return addresses in the stack ROP chains are used in gadgets. When this type of attack has been used it becomes difficult to decode the sequence in which it is being executed.

Protocol. A proposed safe protocol is designed for wireless communication.The main aim is to provide a safe transfer of information in the communication session. This protocol in implanted devices mainly operates in the 5 step process. [XX] Let us consider a sender as x and receiver as y the algorithm takes place as follows

Step 1: Sender_x→ Reciever_y
Step 2: Reciever_y → DBS
Step 3: DBS → Reciever_y
Step 4: Receiver_y → Sender_x
Step 5: Sender_x → Receiver_y

For this protocol to run efficiently *CASPER* converts the protocol into the source code for verification.

IoT vulnerabilities in Industry

Slammer worm. Slammer worm came into existence in the year 2003. USA nuclear power plant was affected by an attack. Two important monitoring control systems in the plant have become vulnerable to this attack. Slammer code mainly comprises of 376bytes and occupies the process space of Microsoft SQL server. The financial damage caused due to this worm is $750million [VII].
Working procedure:

- Slammer initially starts by randomly choosing some IP addresses
- Now it selects a few hosts it found to be susceptible.
- Finally it transforms the malicious code into the selected host.

This worm mainly uses a popular attack known as buffer overflow. This mainly uses a great amount of CPU power and energy. Till date this worm is said to be the fastest transmitting worm [III]. This attack mainly occurs due to lack of security protection near nuclear devices. The firewalls which are used in this plant should mainly have security protection to avoid such incidents.

Stuxnet. This worm came into existence in the year 2010. It is an extremely sophisticated computer worm. It was believed that it was first developed by the intelligence agencies of the United States and Iran countries. This worm was mainly targeted to attack and disrupt the Iranian centrifuge program. Thiswas mainly targeted to a specific PCS component involved in this program. This first disrupted the system monitoring physical components and then next the logical controller. This mainly exploited many zero-day-vulnerabilities.

Table 2. Stuxnet worm geographical distribution [21]

Country	Percentage(%) of attack
India	8.32
USA	1.55
Iran	58.86
Indonesia	18.22
Pakistan	1.29
Others	9.21

Table 3. Common vulnerabilities of IoT devices

Vulnerability	Description	Solution
Cleartext local API	This is caused when local communication is not in an encrypted form.	This can be solved by simply using encrypted protocols such as HTTPS and SSH
Unencrypted Storage	This is caused when the information stored on the disk is in clear text format	This can be solved by storing all data in encrypted format, which can be accessed only by authorized users
Backdoor Accounts	This happens when the local accounts have easily guessed passwords.	By using a unique passwords and generating password by using algorithms that cannot be guessed easily this problem can be solved.
UART(Universal Asynchronous Receiver/Transmitter) access	In this type, the local attacker can alter the IoT device	The devices should be at least tamper-evident and should also inform the owner when alteration of device occurs.

Working Procedure. This worm mainly works in two phases

- Propagation phase: In this phase the worm spreads through the network and exchanges its file with the host system using peer-peer communication [XII].
- Injection phase: It is at this phase the worm starts working on the system and makes the system to work abnormally

The states having more interest in cyber-attacks should also have an interest in protecting themselves from such attacks. The people or users should be more educated about these attacks. The people responsible for protecting the nuclear facilities are less trained than their capabilities. So we need to educate more about such type of attacks which would cause great damage to their facilities to avoid them further. Table 2 represents the %of geographical distribution of the Stuxnet worm in 2010. Overall any vulnerability can be solved by using the following countermeasures:

- Prevention
- Detection and recovery
- Resilience
- Deterrence

In the industrial application of IoT, the four-layered architecture is used. For providing security in the industry vertical the following protocols are used:

Open Trust Protocol (OTP). This protocol is used to manage security configurations in a trusted network. This is also used to add or delete or install an application.

X.509. This protocol is used to manage symmetric key encryption. This is a part of the transport layer security protocol. The following are the common vulnerabilities caused in IoT devices

IoT vulnerabilities on Energy systems:

Smart homes. This is one of the important IoT applications. IoT makes homes smarter and also helps in the efficient utilization of energy. The main aim of smart homes is to make events being done automatically. The efficient working of smart homes depends upon the amount the internet is available for the devices to work. This application saves energy and provides a better life. The main usage and its further workings are explained in [VI]. The following are the reasons why vulnerabilities occur in smart homes

- They are generally caused due to limited Authentication, Authorization and Availability of resource.
- They are also caused due to limited security measures in the web interfaces.
- They are also prone to attacks when there is less effective cryptographic support.

Monitoring energy consumption in a smart city. The energy consumption can also be monitored by IoT devices. These devices help us to make a report on the energy consumption of various devices in the city. By this we can also have a clear view of what sources are consuming more energy and try to optimize them [II]. The vulnerabilities caused in smart cities are due to the following

- The privacy in the smart home is limited.
- The connectivity which is established through the cloud is also not secured.

IoT Vulnerabilities in Insurance Industry

More than the health care systems the hospitals offer the citizens of America are mostly used for acquiring insurance. [V] Almost all have insurance and nearly about half of the Americans accept auto insurance with the companies. These companies generally have IoT devices connected to their vehicles which collect the data about the users.

Privacy leak. Only 26% [XIX] of the Americans decline the offers that the auto insurance companies offer. But almost more than half of the citizens accept the monitoring done by the insurance companies such as location and driving speed, to possess the offers that these companies offer. Due to collecting, transferring and sharing these sensitive data would cause great damage to the privacy of the individual.

Solution. To protect sensitive information techniques such as encryption should be used. But still protection is provided to a little extent. The solution should involve deeper research

III. IoT security Protocols

IP-Based Security Protocols

When IoT security is based on the IP, then for an IP-based IoT security we need to look at the TCP/IP protocol stack [XVIII]. This is because the protocols are designed according to this stack. The mainly focused protocols under this category are IKEv2/IPSec which is used for key exchange and for providing valid authentication, TSL/SSL is another protocol which provides a way for secure communication to take place, DTLS is also one such protocol which provides safe communication, EAP supports duplication of messages and PANA are used for enabling multiple authentication mechanisms. Table 4 represents protocols at different layers and also the relationships which exist between these IP security protocols is represented in Fig. 3[XVII].

Table 4. Protocols used in TCP/IP Layers

TCP/IP LAYERS	Protocols Used
Application layer	SSH
Network layer	Host Identity Protocol(HIP),Internet key exchange(IKEv2)/IPSec, Protocol for caring Authentication mechanism for Network Access(PANA)
Transport Layer	Transport Layer Security(TLS),Datagram-oriented Transport Layer Security(DTLS)
DATA Link Layer	Extensible Authentication Protocol(EAP)

Protocols based on five-layer architecture

There are different protocols for different layers in the architecture. Since generally a five-layered architecture is used in the IoT communication we would discuss the protocols in each layer. Fig. 4 represents security protocols in each layer [I][VIII][XI]:

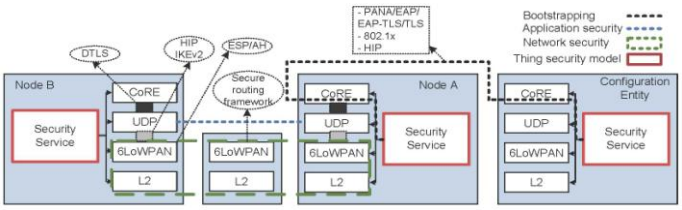

Fig3. IP-based security protocols

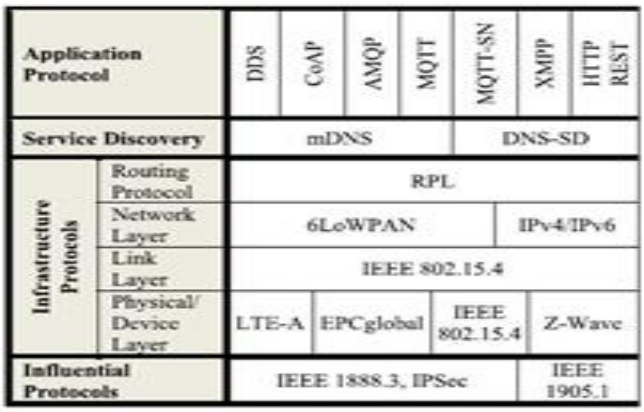

Fig 4. Security protocols in different layers

Application Protocols. The protocols used in the application layer are in Table 4.

Service Discovery Protocols.

Table 4. Protocols in application layer

Protocol	Description	Security
Constrained Application Protocol(CoAP)	The client and server exchange messages using Rest.	DTLS
Message Queue Telemetry Transfer(MQTT)	Embedded devices and networks are connected with application layer and middleware layer	TLS/SSL
Extensible Messaging and Presence Protocol (XMPP)	It was designed for chatting and message exchanging	TLS/SSL
Advanced Message Queuing Protocol (AMQP)	This protocol is used to provide reliability in message exchange. The main advantage of this protocol is that it provides reliability even after disruption.	TLS/SSL

Table 5 explains the different service discovery protocols [XV]

Table 5. Service discovery protocols

Protocol	Description
Multicast DNS(mDNS)	This protocol mainly performs the task of unicast DNS.It is an appropriate protocol for DNS services.
DNS service discovery	This is termed as a pairing function of required services by clients using mDNS. By using this kind of protocol, the clients can discover a set of desired services in a specific network DNS messages

Influential protocols: The influential protocols are listed in Table 6.

Infrastructural Protocols: This protocol wholly involves four layers. They are Network layer, link layer, Physical layer, routing protocol. Table 8 briefly represents the protocols which fall under this category.

Table 8. Infrastructural protocols

Protocol	Category/layer
Routing Protocol for Low Power and Lossy Networks (RPL)	Routing protocol
6LowPAN	Network layer
IEEE 802.15.4	Link layer
Bluetooth Low Energy	Link layer
EPCglobal	Physical layer
LTE-A (Long Term Evolution—Advanced)	Physical layer

IV. Conclusion

IoT though made the life of people easier, at the same time posed numerous vulnerabilities that would sometimes also cause damage to human life. This paper presented a comprehensive review of security vulnerabilities and countermeasures in various sectors of IoT. To avoid these vulnerabilities strong security mechanisms such as encryption, using a strong password for authentication, implementation appropriate security protocols is quite essential. Sometimes just providing security to IoT devices alone is not sufficient. The perimeter within the IoT device must also be secured by employing firewalls, integrated threat handling devices, Intrusion Detection/Prevention devices, Virtual Private Networks etc. The people responsible

for securing devices should also be given more training about the emerging day-to-day attacks along with their countermeasures. Amongst all, user awareness and training are one of the essentialcomponents.

Table 6. Influential protocols

Protocol	Description
Security	At Network Layer: IPSec provides protection at the network layer. This is an important security protocol along with 6lowPAN.
	At Link Layer: IEEE 802.15.4 offers security mechanisms at the data link layer. This protects the communication among the neighboring devices.
	At Transport Layer: Transport Layer Security (TLS) provides security a mechanism at the transport layer. It is used to provide security for TCP communication.
	CODO is a security solution at the file system level, which could improve the performance of the security operations.
Interoperability (IEEE 1905.1)	This protocol is designed for digital home networks and heterogeneous technologies. This provides a layer of abstraction which hides the diversity of media access control topologies.

References

I. Ahmad-Reza Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," San Francisco, CA, USA, 2015.

II. AndreaZanella, NicolaBui and AngeloCastellani, "Internet of Things for Smart Cities," vol. 1, no. 1, 2014.

III. D. MOORE, V. PAXSON and STEFAN SAVAGE, "Inside the Slammer Worm," 2003.

IV. D. Singh, G. Tripathi and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," Seoul, South Korea, 2014.

V. Jason Bau, Elie Bursztein, Divij Gupta and John Mitchell, "State of the Art: Automated Black-Box Web Application Vulnerability Testing," Berkeley, California, USA, 2010.

VI. Jinesh Ahamed and Amala V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," Ras Al Khaimah, United Arab Emirates, 2016.

VII. Kevin Poulsen, "Slammer worm crashed Ohio nuke plant network," 2003.
VIII. M. Muneer Bani Yassein, Mohammed Q. Shatnawi and Dua' Al-zoubi, "Application layer protocols for the Internet of Things: A survey," Agadir, Morocco, 2016.
IX. NausheenFarha and Sayyada Hajera Begum, "Healthcare IoT: Benefits, vulnerabilities and solutions," Coimbatore, India, 2018.
X. P Ravi Kiran Varma, Kotari Prudvi Raj and KV Subba Raju, "Android mobile security by detecting and classification of malware based on permissions using machine learning algorithms," in IEEE International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC), Tiruchengode, 2017.
XI. P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," 2017.
XII. Rahat Masood, Um-e-Ghazia and Dr. Zahid Anwar, "SWAM: Stuxnet Worm Analysis in Metasploit," Islamabad, Pakistan, 2011.
XIII. Ravi Kiran Varma Penmatsa and Padmaprabha Kakarlapudi, "Web phishing detection: feature selection using rough sets and ant colony optimisation," International Journal of Intelligent Systems Design and Computing, vol. 2, no. 2, pp. 102-113, 2018.
XIV. S. M. Riazul Islam, Daehan Kwak, Kabir MD. Humaun and .., "The Internet of Things for Health Care: A Comprehensive Survey," vol. 3, 2015.
XV. Simone Cirani, Luca Davoli, Gianluigi Ferrari and ..., "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," vol. 1, no. 5, 2014.
XVI. Smruti R. Sarangi and Pallavi Sethi, "Internet of Things: Architectures, Protocols, and Applications," 2017.
XVII. Tobias Heer, Oscar Garcia-Morchon and R. Hummen, "Security Challenges in the IP-based Internet of Things," 2011.
XVIII. Tobias Heer, Oscar Garcia-Morchon and Sye Loong Keoh, "Security Challenges in the IP-based Internet of Things," vol. 61, no. 3, 2011.
XIX. Wei Zhou, Y. Yan Jia, Anni Peng and Yuqing Zhang, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," 2018.
XX. Woo-Sik Bae, "Verifying a secure authentication protocol for IoT medical devices," Boryeong,Korea, 2017.