International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Security Fundamentals in Internet of Things

A. M. Chandrashekhar
Asst. Professor, Department of Computer Science and Engineering, SJCE, Mysuru , Karnataka,India
Chaitra K. V.
M Tech Student, Department of Computer Science and Engineering, SJCE, Mysuru , Karnataka,India
Sandhya Koti
M Tech Student, Department of Computer Science and Engineering, SJCE, Mysuru , Karnataka,India

Abstract:

With growing number of smart devices per person and at each individual's homes, it is estimated that the number of objects connected to the Internet is higher than the number of people connected to it. This trend is only gaining popularity with more and more objects now interfacing with the Internet. This in-turn creates a network of smart devices that are closely integrated with the physical world, thereby providing increased efficiency and economic benefit. This is collectively termed as Internet of Things - IoT. Just like all other technology enhancements, IoT also brings up threats and security issues that need to be considered before application of the technology in various fields.

This document provides a framework that describes the threats that will be seen at each level of IoT and the major issues needed to be addressed before implementing a secure system.

Keywords – Internet of Things (IoT); Security threats; Security vulnerabilities; Cyber attacks; Sensors; Intelligent computing

I. INTRODUCTION

In the past decade, there has been tremendous growth in the use of electronics and smart devices that are in use, leading to huge voluminous production and consumption of network data [1]. It is estimated that a staggering 75 billion devices will be connected to the internet by 2020.

Internet of Things (IoT) is the technology wherein more and more small and embedded devices get linked to the Internet. IoT describes the present and a future where several physical objects in our day to day lives will get connected with the internet and thereby get identified by surrounding objects and work in unison with them. This change in paradigm which brings in a network of several smart decentralized devices also brings up a new angle to security. Increased number of connected devices opens up more doorways for cyber-crime. With variety of devices and sensors in place, there are different kinds of vulnerabilities that exist and each of these needs to be looked into, to enable a solid foundation for IoT.

This paper provides a comprehensive study of various facets of security related to IoT. This paper is structured as follows: Section II describes the vulnerabilities, threats and attacks to which IoT is susceptible. Section III provides an overview of the domains of IoT system in which security needs to be implemented. Section IV describes the security architecture of the IoT system. Section V highlights the challenges in developing a secure architecture for IoT systems. Section VI concludes the paper summarising the different aspects of a secure IoT system.

II. ATTACKS ON IOT SYSTEM

The IoT devices may become vulnerable to cyber-attacks for the below reasons:

i. Many of the IoT devices are small or embedded devices operating without any human supervision and hence an attacker can easily gain access to them.
ii. Communication of most of the IoT devices happens over wireless networks where eavesdropping or man-in-the-middle attacks could be possible.
iii. Due to low power and low resource constraints, implementing complex security algorithms on IoT systems is not always feasible.

The different kinds of attacks [2] [3] possible are summarised in figure 1.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

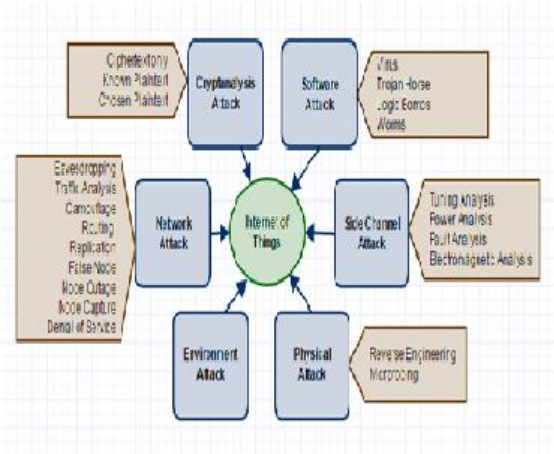

Figure 1: Attacks on IoT System

A. Physical Attacks

These attacks include reverse engineering and microprobing attacks. In case of reverse engineering, the attacker may have gained access to the technology used in the device, apply this knowledge it to understand the internal architecture and functionality of the device and thereby become capable of breaching the device security. In case of microprobing attacks, the attacker may tamper the device by accessing the chip surface directly.

B. Side Channel Attacks

These attacks include timing attacks and power analysis attacks. Based on the size of the input data and the cryptographic algorithms used, attackers are now able to compromise the IoT systems by timing analysis. Studying the power consumed by the various cryptographic devices [4], attackers are now able to extract keys and other secret information from the IoT devices.

C. Environment Attacks

Heterogeneity and the distributed nature of the IoT devices and most of them operating in an outdoor insecure environment make them vulnerable to these attacks [5].

D. Network Attacks

With most of the recent devices working in a wireless environment, the broadcast messages sent through the devices are susceptible to attacks. Routing attacks are the most common kid of these attacks. Others include node capture, eavesdropping, message corruption, traffic analysis etc.

E. Cryptanalysis attacks

Brute force attacks, dictionary attacks and replay attacks to gain access to passwords or misuse the acquired passwords fall into this category. Decryption of the encryption algorithms used by securing passwords or secure keys through various cyber-attacks is also carried out.

F. Software Attacks

These include manipulation of the controller software to change configurations with intentions of harming the system and its users. These also include Denial of Service (DoS) attacks whereby the system or resource is made unavailable to its intended users.

III. SECURITY DOMAINS OF IOT

The security implementation in any IoT system needs to encompass the domains as shown in figure 2:

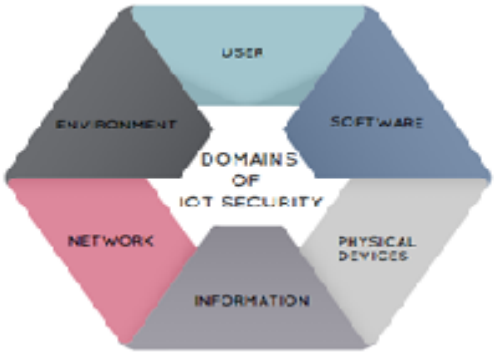

Figure 2: IoT Security Domains

A. User

There must be appropriate user authentication and authorisation mechanisms in place to secure the IoT system. The whole system becomes susceptible to attacks when the user identification is illegitimate. Every user must be associated with a set of access rights and permission to use the resources in the system.

B. Software

Software is the crucial fount of most of the security threats. The deployed software must be free from all the implementation vulnerabilities which can be exploited by an attacker. It should not be

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

prone to deliberate software attacks such as viruses, worms, Trojan horses.

C. Physical Devices

The physical components of the IoT system have to be protected from any type of physical tampering or logical probing. The security requirements of the system must not be compromised even when these devices are nabbed.

D. Information

The confidentiality and integrity of the information stored in the IoT system must be preserved. The accesses to the information must be monitored to ensure that no privacy policies are violated.

E. Network

Since most of the communications between IoT devices are through broadcasting over wireless transmission medium, maintenance of security and reliability of the network is a major concern.

F. Environment

The environment to run the IoT applications must be secure. Attacks on the environment of the IoT system are easier than the device itself. In order to prevent misuse at the application level there must be security measures implemented in the runtime environment.

IV. ARCHITECTURE OF IOT

The IoT systems are used in critical applications such as military surveillance, healthcare, medical services, intelligent transportation, intelligent home etc. The security architecture [6] of such crucial system has to be robust enough to counter attacks at various levels and provide reliable and sustainable environment. The security architecture of IoT system consists of four generic layers as shown in figure 3.

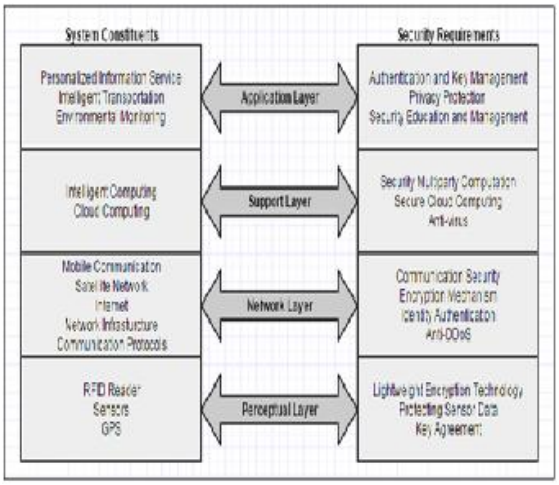

Figure 3: Security Architecture for IoT System

A. Perceptual Layer

The most basic layer is the perceptual layer which consists of all the physical devices used to collect data from the real world entities. The devices are heterogeneous in nature – different types of sensors, RFID readers, and global positioning system devices. All the data collected from different types of sensors are consolidated and stored. These data need to be protected using various encryption algorithms. Since the sensors are resource constrained with respect to computation and power, complex cryptographic algorithms cannot be used. Specialized lightweight algorithms are to be employed to provide integrity and authenticity to the data.

B. Network Layer

The network layer ensures reliable transmission of information from the perceptual layer. This layer lays the infrastructural framework for all the networking protocols needed for effective communication between the components of the IoT system. The existing communication mechanisms cannot be directly employed in case of the IoT system. This layer requires confidentiality, reliability and integrity mechanisms to provide a resilient environment countering the network attacks and also provide security during communication between devices.

C. Support Layer

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

The support layer furnishes the architecture with a suitable platform to support the applications of the system. This layer acts as the bridge between the hardware based network layer and the software based application layer. The platform must support all types of intelligent computing [7] to boost the capabilities of the underlying technologies such as cloud computing, grid computing. The support layer must embed strong security mechanisms for the pertinent technology in order to ensure smooth functioning of the system.

D. Application Layer

The application layer is the topmost and terminal layer of the security architecture of IoT system. This layer provides personalized services to the end users. The application built upon this layer may be a surveillance system, environmental monitor, intelligent transportation etc. The diverse security needs of the individual applications include authentication, privacy protection [8], access control, password and key management.

V. CHALLENGES

The challenges [9][10] that arise while developing a secure architecture for IoT systems mainly consist of:

1. The sensors embedded in the IoT system are battery powered –low energy devices. These sensors have to be exploited judiciously during enforcement of secure transmissions to minimize the energy consumption and hence make the system energy efficient.[11][12]

2. IoT devices employ broadcast mechanism for communication. This is a power draining process and also vulnerable to many attacks. Developing specialized routing algorithms for communication is laborious and may not be feasible all the time.[13][14]

3. The nodes of IoT system have limited computing power and hence complex cryptographic algorithms requiring considerable computations are not feasible for IoT system. Developing lightweight cryptographic algorithms optimised for these devices are both expensive and time consuming.[15][16]

4. IoT system aims at interconnecting heterogeneous devices to achieve communication among them. The challenging task here is to achieve interoperability among these devices in its network by providing a common platform for communication. With such diverse platforms adopted, implementation of security needs to be standardised. [17][18]

5. Ensuring the integrity of the data sent and the confidentiality of the data collected to/from IoT devices or sensors has become mandatory. Sensitive data collected by IoT devices is one of the potential vulnerabilities of the system.[19][20]

6. Considering the ubiquity of IoT systems in the current generations, the toughest task is to fulfil the information privacy requirements. Poor encryption mechanisms, backdoors or weak links could make the system more susceptible to serious issues like information leakage or misuse.[21][22]

7. Considering the huge volume of data and heterogeneity of devices, the current network security approaches may not be directly applicable to IoT domain. Proper measures suitable to the applications need to be devised to ensure security.[23][24]

8. Every IoT device is slightly different. Every configuration of IoT system thus needs to implement pertinent security mechanisms. Abstraction of security parameters is not possible.[25][26]

9. Appropriate care need to be taken to upgrade or patch the security vulnerabilities during the maintenance phase to make the system sustainable with evolving technologies.[27][28]

10. Current technological advancements compel companies to have tight deadlines to get their IoT devices into the market. With all

efforts centred on quick deployment security becomes an afterthought[29][30].

VI. CONCLUSION

The study of threats and attacks on IoT systems is an exhaustive area if we dwell into the application specifics. In this paper, we have surveyed the security challenges and attacks that are almost basic for most of the deployments of IoT systems[31][32]. Keeping in mind the various vulnerability and threat factors discussed in this paper and implementing the counter measures in every phase of development lifecycle of IoT systems, will be crucial for the future maintenance and manageability of the systems[33]. This will also ensure reduction in cost, and sustainability of the product.

In summary, rapid development of IoT for various environments and applications, need to be supplemented with appropriate security measures so as to ensure its steady growth in the future as well as to satisfy consumer and business requirements.

REFERENCES:

[1] Michael J. Covington, Rush Carskadden, "Threat Implications of the Internet of Things"; 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum, 2013

[2] Sachin Babar, Antonietta Stango, Neeli Prasad, Jaydip sen, Ramjee Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)" ; IEEE Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011

[3] Srivats Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady, "Security in Embedded System: Design challenges" ; Transactions on Embedded Computing systems, Vol. 3, Issue 3, 2004

[4] Colin O'Flynn, Zhizhang Chen, "Power Analysis Attacks against IEEE 802.15.4 Nodes"; International Association for Cryptologic Research, 2015

[5] Hagai Bar-El, "An Introduction to side Channel Attacks"; White paper, Discretix Technologies Limited.

[6] Mainetti L, Mighali V, Patrono L, "A Software Architecture Enabling the Web of Things" ; Internet of Things Journal, IEEE, Vol. 2 , Issue: 6 , Page: 445- 454, 2015

[7] Chen Qiang , Guang-ri Quan , Bai Yu, Liu Yang, "Research on Security Issues of the Internet of Things"; International Journal of Future Generation Communication and Networking, Vol.6, No.6, Page: 1-10,2013

[8] Tuhin Borgohain , Uday Kumar , Sugata Sanyal , "Survey of Security and Privacy Issues of Internet of Things"Ebraheim Alsaadi, Abdallah Tubaishat, "Internet of Things: Features, Challenges, and Vulnerabilities"; International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol. 4, No. 1, Page: 1-13, 2015

[9] Hua-Dong Ma, "Internet of Things: Objectives and Scientific Challenges"; Journal Of Computer Science And Technology, Vol. 26(6), Page: 919–924, 2011

[10] A. M. Chandrashekhar and K. Raghuveer, "*Fusion of Multiple Data Mining Techniques for Effective Network Intrusion Detection – A Contemporary Approach*", Proceedings of The 5th International Conference on Security of Information and Networks (SIN 2012), 2012, pp 33-37.

[11] A. M. Chandrashekhar and K. Raghuveer, "*An Effective Technique for Intrusion Detection using Neuro-Fuzzy and Radial SVM Classifier*", The Fourth International Conference on Networks & Communications (NetCom-2012), 22~24, Dec-2012.

[12] A. M. Chandrashekhar and K. Raghuveer , "*Intrusion Detection Technique by using K-means, Fuzzy Neural Network and SVM classifiers*", 2013 IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), 4~06,Jan2013, IEEE Catalog Number: CFP1308R-ART, ISBN Number: 978-1-4673-2907-1.

[13] A. M. Chandrashekhar and K. Raghuveer, "*Confederation of FCM Clustering, ANN and SVM Techniques of Data mining to Implement Hybrid NIDS Using Corrected KDD Cup Dataset*", IEEE

International Conference on Communication and Signal Processing (ICCSP),2014, pp 672-676.

[14] A. M Chandrashekhar A M and K. Raghuveer, "*Hard Clustering Vs. Soft Clustering: A Close Contest for Attaining Supremacy in Hybrid NIDS Development*", Proceedings of International Conference on Communication and Computing (ICC - 2014), Elsevier science and Technology Publications.

[15] A. M. Chandrashekhar and K. Raghuveer, "*Amalgamation of K-means clustering algorithem with standard MLP and SVM based neural networks to implement network intrusion detection system*", Advanced Computing, Networking, and Informatics –Volume 2(June 2014), Volume 28 of the series Smart Inovation, Systems and Technologies pp 273-283.

[16] A. M Chandrashekhar A M and K. Raghuveer, "*Diverse and Conglomerate Modi-operandi for Anomaly Intrusion Detection Systems*", International Journal of Computer Application (IJCA**)** Special Issue on "Network Security and Cryptography (NSC)", 2011.

[17] A. M. Chandrashekhar and K. Raghuveer, "*Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set*", International Journal of Information and Network Security (IJINS), ISSN: 2089-3299, Vol-1, No.4, October 2012, pp. 294~305.

[18] A. M. Chandrashekhar and K. Raghuveer, "*Fortification of hybrid intrusion detection system using variants of neural networks and support vector machines*", International Journal of Network Security & Its Applications (IJNSA) ISSN: 0974-9330[online]& 0975-2307[print].Vol.5, Number 1, January 2013.

[19] A. M. Chandrashekhar and K. Raghuveer , "*Improvising Intrusion detection precision of ANN based NIDS by incorporating various data Normalization Technique – A Performance Appraisal*", International Journal of Research in Engineering & Advanced Technology(IJREAT), Volume 2, Issue 2, Apr-May, 2014.

[20] Puneeth L Sankadal ,A. M Chandrashekhar, "*Network Security situation awareness system*" International Journal of Advanced Research in Information and Communication Engineering(IJARICE), Volume 3, Issue 5, May 2015.

[21] Prashanth G M, A.M.Chandrashekhar, "*Secured infrastructure for multiple group communication*" International Journal of Advanced Research in Information and Communication Engineering (IJARICE), Volume 3, Issue 5, May 2015.

[22] Sowmyashree K.K, A.M.Chandrashekhar, "*Pyramidal aggregation on Communication security*" International Journal of Advanced Research in Computer Science and Applications (IJARCSA), Volume 3, Issue 5, May 2015.

[23] Huda Mirza Saifuddin, A.M.Chandrashekhar, "*Exploration of the ingredients of original security*" International Journal of Advanced Research in Computer Science and Applications(IJARCSA), Volume 3, Issue 5, May 2015.

[24] Syed Tahseen Ahmed,A.M.Chandrashekhar, "*Analysis of Security Threats to Database Storage Systems*" International Journal of Advanced Research in data mining and Cloud computing(IJARDC), Volume 3, Issue 5, May 2015.

[25] Yadunandan Huded, A.M.Chandrashekhar, "*Advances in Information security risk practices*" International Journal of Advanced Research in data mining and Cloud computing (IJARDC), Volume 3, Issue 5 May 2015.

[26] Madhura S Hegde, A.M.Chandrashekhar, "*A Survey:Combined impact of cryptography and steganography*" International Journal of Engineering Research (IJOER), Volume 3, Issue 5, May 2015.

[27] Koushik P, A.M.Chandrashekhar, "*Information security threats, awareness and coginizance*" International Journal for Technicle research in Engineering(IJTRE), Volume 2, Issue 9, May 2015.

[28] Rahil kumar Gupta and A.M.Chandrashekhar, "*Role of information security awareness in success of an organization*"

International Journal of Research (IJR) Volume 2, Issue 6, May 2015.

[29] A. M. Chandrashekhar, Hariprasad M, Manjunath A, "The Importance of Big Data Analytics in the Field of Cyber Security", Volume 3, Issue 11, JAN-2016.

[30] A. M. Chandrashekhar, Arpitha, Nidhishree G, "Efficient data accessibility in cloud with privacy and authenticity using key aggregation cryptosystem", International Journal for Technological research in Engineering (IJTRE), Volume 3, Issue 5, JAN-2016.

[31] A. M. Chandrasekhar, Jagadish Revapgol, Vinayaka Pattanashetti, "Security Issues of Big Data in Networking", International Journal of Scientific Research in Science, Engineering and Technology (*IJSRSET)*, Volume 2, Issue 1, JAN-2016.

[32] A. M. Chandrashekhar, Anjana D, Muktha G, "Cyberstalking and Cyberbullying: Effects and prevention measures", Imperial Journal of Interdisciplinary Research (IJIR) ,Volume 2, Issue 2, JAN-2016.