Vulnerabilities, Attacks and their Mitigation: An Implementation on Internet of Things (IoT)

Shamneesh Sharma, Manoj Manuja, Keshav Kishore

Abstract: ***IoT is much-hyped technology in today's world still it helps us to achieve the goals of ubiquitous computing. Although, there are many challenges in adoption and implementation of IoT based solutions. One of the major challenges is security of IoT products and services. Day after day exposures like Insecure Firmware, Data Protection, Identity Thefts and DoS/DDoS Attack in the field of IoT are being oppressed with malicious objectives so we need to focus on these security issues. A framework of IoT may use many services on a single platform to give a specific applicability to the applications. These services can be sensor fields, cloud computing and data analytics so the security architecture should ensure its measures on each level such as physical access, remote access and secured data access. This paper presents the study on existing attacks and mitigation in IoT Services which enables for finding and patching security vulnerabilities. With the help of machine learning and data analytics, IoT services and security can be made proactive rather than reactive.***

Index Terms: Internet of Things (IoT), Security in IoT, Attacks in IoT, Data Protection in IoT, IoT Services

I. INTRODUCTION

According to research studies, there will be a global network of 21 billion of IoT devices by the end of year 2020 so there is an alarming concern of security in this field [1]. The number of attacks and threats on Internet of Things (IoT) are increasing rapidly in terms of both numbers and complexity of attacks. Some of the major attacks [2] on IoT Infrastructure in recent years are Stuxnet, Mirai botnet, Botnet barrage and Brickerbot. The Major Challenges to Internet of Things (IoT) security are as follows:

1. Since IoT is designed for automation support, most of the devices do not need human attention. Attackers take the advantage of this and harness the IoT services for their malicious intent.
2. Most IoT Infrastructure runs on wireless networks which is prone to various air attacks.
3. Most of the security solutions and implementations are very complex in nature which is difficult to implement in IoT due to battery power and low computation resources.

The Internet of Things (IoT) has been using multiple technologies integrated on a single platform [3] so the possibilities of attacks can be increased at each level. On the other hand data dissemination [4] in these networks is a major concern itself. The real work on the technology of Internet of Things (IoT) has been started in the year of 1999 when Kevin Ashton coined this term. From 1999 to 2004, different research groups like Cisco, MIT Multimedia Labs, Auto-ID Center and many more have started their research on it [5].

Revised Manuscript Received on August 05, 2019.

Shamneesh Sharma, Head, Division of Information Technology, Alakh Prakash Goya Shimla University, Shimla (H.P.) India
Dr. Manoj Manuja, Vertical Head (IT) iNurture Education Solutions, Banglore, India
Kshav Kishore, Associate Professor, Department of Computer Science & Engineering, Alakh Prakash Goyal Shimla University, Shimla (H.P.) India

II. LITERATURE SURVEY

There are certain security requirements [6] in order to consider IoT environment secure. There requirements include secure authentication and authorization mechanism, security of IoT Data, secure bootstrapping and transmission of data. Author of [7] has also suggested the security requirements for Internet of Things (IoT) which includes Attack resiliency, Data Authentication, Access Control Mechanism and Client's Privacy.

A. Vulnerabilities in Internet of Things (IoT)

It has been proved and demonstrated thorough the analysis that current IoT devices, designs and methodologies are vulnerable to cyber attacks at all levels hardware, software and network [8]. Author of [9] has explained the vulnerabilities in IoT plug & play systems.

Sr. No.	Vulnerability
1	Insecure methods of Authorization & Authentication
2	Insecure Network Design & Services
3	Insecure Storage Platforms
4	Lack of Integrity Verification
5	Insecure Device Interface
6	Insecure Infrastructure
7	Insecure Software Platforms

Table 1. Vulnerabilities in IoT

B. Attacks in Internet of Things (IoT)

In most of the Commercial IoT Devices there are hardware vulnerabilities which can lead to the remote access over the whole system of IoT using low level access mechanism which therefore leading to password hashes of the devices.

IoT Layer	Attack Vectors
Application Layer	Scripting vulnerabilities [10]
	Buffer overflows [11]
	Cookie poisoning [12]
	Hidden field manipulation [13]
	Parameter tampering [14]
	Cross-site scripting [15]
	SQL injection [16]

Network Layer	Eavesdropping [17]
	Data Modification [18]
	Identity Spoofing (IP Address Spoofing) [19]
	Denial-of-Service Attack [20]
	Man-in-the-Middle Attack [21]
	Compromised-Key Attack [22]
Perception Layer	In-the-Field Attacks [23]
	Insecure Firmware [24]
	Brute Force Attack [25]
	External Flash [26]
	Unauthorized access to Data [27]

Table 2. Vulnerabilities in IoT

III. METHODOLOGY

In this paper, we have taken three vulnerabilities which lead to attack at each layer to consideration and performed attacks. Each attack vector is associated with the vulnerability of the system. The detail of the performed experiment is given below on most commonly available tools:

Vulnerability	Attack Vector	IoT Layer
Insecure methods of Authorization and Authentication	SQL injection	Application Layer
Insecure Network Design and Services	Denial-of-Service Attack	Network Layer
	Man-in-the-Middle Attack	
Insecure Storage Platforms	Unauthorized access to Data	Perception Layer

IV. EXPERIMENTAL SETUP AND RESULTS

We have performed different types of attacks in a layer wise manner according to the vulnerabilities discussed in the Table 2. We used inexpensive hardware and most popular tools for attacks available commonly on Internet.

A. SQL Injection

We have performed the experiment on the local IoT setup by using SQL Injection Tool Havij. Nowadays, most of the SoC (System on Chip) and IoT gateways have a web interface for Easy management of IoT Services. Administrator can monitor, manage and customize the services as per requirements. User credentials need to be validated via login forms on user data bases using SQL Queries. Form Data can be submitted using HTTP protocol which is very insecure. According to Wired [28], 50% of all internet traffic is using HTTP protocol for communication; however the world is rapidly adopting the HTTPS protocol standards.

In SQL injection, the attacker guesses the username and uses the unhandled SQL Query to get authorized. For example, normally in IoT web admin console, it asks for username and password. Most commonly used usernames are admin, Administrator, Default user name set by vendor and in password "1'" or "1'=1'". If SQL query is not sanitized properly for "Unsanitized-User-Input-Data". This username and password works on almost 90% SQL Injection vulnerable web pages.

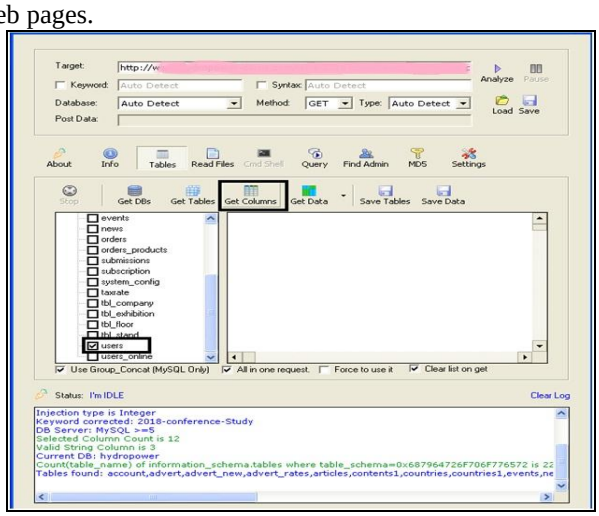


Fig.1 SQL Injection Attack using Havij Tool

B. Denial of Service Attack

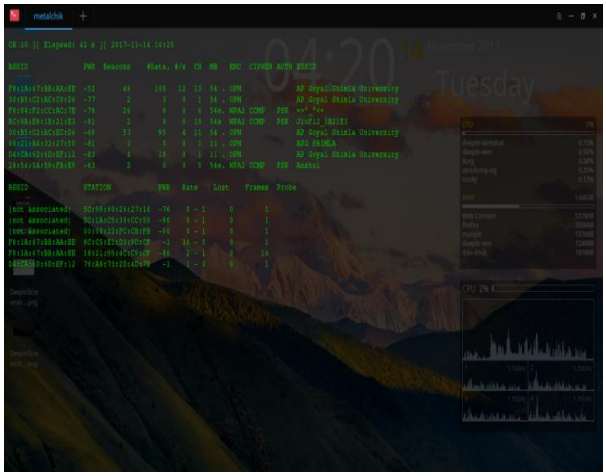
We have performed denial of service attack using Web Stresser Tool. As IoT uses internet for data communication, each node or IoT Gateway have unique IP Address which can be traced back to the devices. The public IP can be enumerated and attacked for DoS attacks. The Attacker needs only two things; IP and Port Number, on which IoT based service is running. Dos Attack yields in unavailability of IoT services. IoT Devices, these attacks are quite successful as the target consists of battery power ubiquitous devices. During the attack, the battery of these devices drains at very high rate and device becomes dead. The soft target of DoS attack is IoT gateway, which blocks a whole segment of sensor fields which further resulting in the data loss and inaccurate outputs.

Fig.2 DoS Attack on IoT using IP Stresser Tool

C. Man-in-the-Middle Attack

Since IoT uses wireless network for accessing internet and these networks are open in nature, attacker can join the wireless network using a powerful antenna and network scanner. Attacker can monitor and manipulate all the traffic in the network. We have used Aircrack-ng to

perform this attack on IoT wireless networks. Attacker can act as rouge access point which redirects control of entire network traffic.



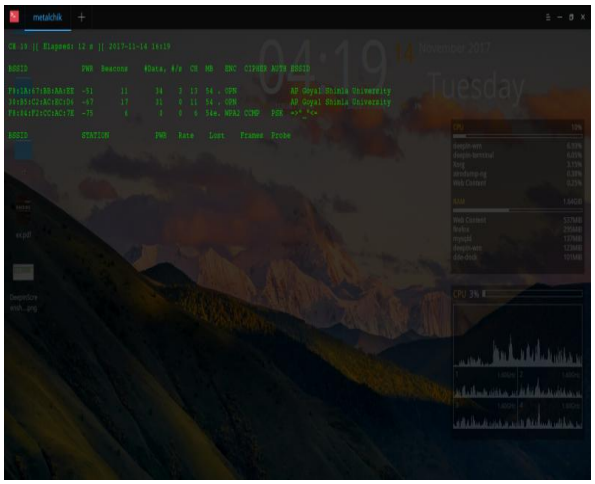


Fig.3 Man-in Middle Attack on IoT using Aircrack-ng Tool

D. Unauthorized access to Data

Network sniffing and SQL injection are most common ways to gather data from network and databases. Wireshark packet sniffer is most popular tool for sniffing any network. IoT uses wireless networks for data transmission so Wireshark can capture packets to analyze the data.

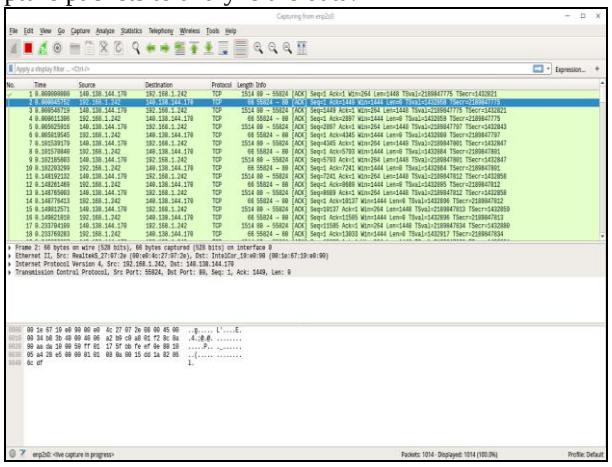


Fig.5 Unauthorized Data Access on IoT using Wireshark Tool

V. DISCUSSION AND ANALYSIS

In a very famous proverb it is said that prevention is better than cure. In case of any technologies this applies to the vulnerabilities. There must be some standard practices and countermeasures that must be applied to make IoT Ecosystem secure and reliable. Some of the mitigations for the performed attacks have been discussed below:

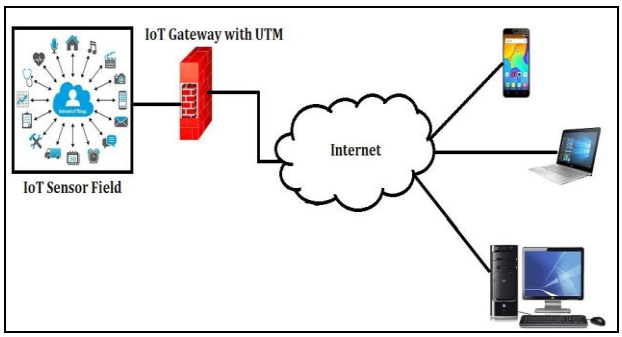


Fig.5 Proposed Secure IoT Ecosystem

A. Mitigations for SQL injection

The application programmer should take care of following precautions while implementing the services:

- Continuously monitor SQL statements from database-connected applications.
- Employ comprehensive data sanitization.
- Avoid constructing SQL queries using user input.
- Limit database privileges by context and roles.

B. Mitigations for Denial of Service Attack

The prevention of DoS attacks is by implementing a dedicated node which performs the following tasks:

- Monitoring of network traffic using firewall or UTM
- Using Access Control Lists (ACL)
- Using Rate limiting

C. Mitigations for Man-in-the-Middle Attack

The prevention of Man-in-Middle attack is by implementing a firewall system with following policies and protocols:

- MAC ID binding
- DNS SEC
- HTTPS

D. Mitigations for Unauthorized access to Data

To secure the IoT Ecosystem from the unauthorized data access, there is a need of implementation of a system that can present the unauthorized access in any system. In the IoT Ecosystem, the data can be accessed from the gateway which is connected to the internet as shown in Fig. 1. To secure the unauthorized data access, we need to secure the IoT Gateway with a firewall system.

VI. CONCLUSION AND FUTURE SCOPE

Internet of Things (IoT) has transformed the entire community by creating incredible benefits. This has attracted many researchers to it alongwith hackers and attackers hence proper authentication and authorization methods should be implemented to secure the IoT Environment. Networking appliances and other objects are comparatively new in the domain of IoT hence the security is not always

considered in product design. IoT is relatively new domain, surprisingly all the traditional cyber attacks can be performed on it. To prove this, we have performed the three attacks in this paper and suggested the mitigations and countermeasures. In this paper researchers have discussed the SQL Injection, Denial of Service, Man-in-Middle and Unauthorized data access attacks on a local IoT system setup in a house using the commonly available popular tools for attacks. In future the suggested mitigations can be implemented and experiments can be performed to check the integrity of implementations of suggested mitigations and counter measures.

REFERENCES

1. Gartner. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. [online] Available at: https://www.gartner.com/newsroom/id/3598917 [Accessed 11 Oct. 2017].
2. Roman, R., Zhou, J. and Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), pp.2266-2279.
3. Sharma, S. and Kishore, K. (2017). Data Dissemination Algorithm using Cloud Services: A Proposed Integrated Architecture Using IoT. In: 2nd International Conference on Innovative Research in Engineering Science and Technology (IREST-2017). Eternal University, Baru Sahib, pp.67-70.
4. Kishore, K. and Sharma, S. (2016). Evolution of Wireless Sensor Networks as the framework of Internet of Things- A Review. International Journal of Emerging Research in Management and Technology, Volume 5, Issue 12.
5. Sharma, S. and Kishore, K. (2017). Internet of Things (IoT): A Review of Integration of Precedent, Existing & Inevitable Technologies. AGU International Journal of Engineering and Technology, Volume 4, Jan-Jun 2017, e-ISSN: 2455-0442, p-ISSN: 2455-6734.
6. E. Borgia, "The Internet of Things vision: Key Features, Applications and Open Issues", Computer Communications (2014), doi: http://dx.doi.org/10.1016/j.comcom.2014.09.008
7. Rolf H. Weber, "Internet of Things- New security and privacy challenges", Computer Law and Security Review, Elsevier, 23-30, 2010.
8. McKnight, M. (2017). IOT, Industry 4.0, Industrial IOT… Why connected devices are the future of design. KnE Engineering, 2(2), p.197.
9. Zhen Ling, Junzhou Luo, Yiling Xu, Chao Gao, Kui Wu and Xinwen Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System", IEEE Internet of Things Journal, 2327-4662, 2016, DOI 10.1109/JIOT.2017.2707465
10. Whitelegg, D. (2016). Combating IoT cyber threats. [online] IBM Developer. Available at:
11. https://www.ibm.com/developerworks/library/iot-security-best-practices-iot-apps/ [Accessed 24 Oct. 2017].
12. Eslam Medhat. (2017). Millions of IoT devices are vulnerable to buffer overflow attack - Latest Hacking News. [online] Available at:
13. https://latesthackingnews.com/2017/07/18/millions-of-iot-devices-are-vulnerable-to-buffer-overflow-attack/ [Accessed 8 Nov. 2017].
14. 12. Osborne, C. (2017). A SSHowDowN in security: IoT devices enslaved through 12 year old flaw | ZDNet. [online] ZDNet. Available at:
15. http://www.zdnet.com/article/a-sshowdown-in-security-iot-devices-attack-devices-through-12-year-old-flaw/ [Accessed 8 Nov. 2017].
16. 13. Hussain, I., Djahel, S., Zhang, Z. and Naït-Abdesselam, F. (2015). A comprehensive study of flooding attack consequences and countermeasures in Session Initiation Protocol (SIP). Security and Communication Networks, 8(18), pp.4436-4451.
17. 14. Akram, H., Konstantas, D. and Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. International Journal of Advanced Computer Science and Applications, 9(3).
18. 15. Gupta, S. and Gupta, B. (2015). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of System Assurance Engineering and Management, 8(S1), pp.512-530.
19. 16. Loeb, L. (2016). A Security Protocol for the Internet of Things. [online] Security Intelligence. Available at:
20. https://securityintelligence.com/a-security-protocol-for-the-internet-of-things/ [Accessed 15 Oct. 2017].
21. 17. Li, X., Wang, H., Dai, H., Wang, Y. and Zhao, Q. (2016). An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things. Mobile Information Systems, 2016, pp.1-10.
22. 18. Sollins, K. (2019). IoT Big Data Security and Privacy vs. Innovation. IEEE Internet of Things Journal, pp.1-1.
23. 19. Gera, J. and Battula, B. (2018). Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds. EURASIP Journal on Information Security, 2018(1).
24. 20. Alim, M., Riadi, I. and Prayudi, Y. (2018). Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard. International Journal of Computer Applications, 180(35), pp.23-30.
25. 21. Čekerevac, Z., Dvorak, Z., Prigoda, L. and Čekerevac, P. (2017). INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS. MEST Journal, 5(2), pp.15-5.
26. 22. Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal, pp.1-1.
27. 23. Riahi Sfar, A., Natalizio, E., Challal, Y. and Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), pp.118-137.
28. 24. Crawley, K. (2017). Internet of Things: Convenient But Insecure. [online] Cylance.com. Available at:
29. https://www.cylance.com/en_us/blog/internet-of-things-convenient-but-insecure.html?aliId=23334118 [Accessed 8 Nov. 2017].
30. 25. Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., Nespoli, P. and Gómez Mármol, F. (2018). Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. Wireless Communications and Mobile Computing, 2018, pp.1-18.
31. 26. Tay, C. (2018). The impact of information and communication technologies on bilateral trade in services. International Journal of Services Operations and Informatics, 9(1), p.40.
32. 27. Ashwin Pal (2017). The Internet of Things (IoT) – Threats and Countermeasures. [online] Cso.com.au. Available at:
33. https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/ [Accessed 12 Nov. 2017].
34. 28. Finley, K., Davis, M., Baker-Whitcomb, A., Newman, L., Greenberg, A. and Eveleth, R. (2019). Half the Web Is Now Encrypted. That Makes Everyone Safer. [online] WIRED. Available at:
35. https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/ [Accessed 22 Mar. 2019].

AUTHORS PROFILE

Shamneesh Sharma is currently serving as IT-Head at Alakh Prakash Goyal Shimla University, Shimla (H.P.). India. He has played vital role in the implementation of New IT-Infrastructure, ERP System and Website Development along with its maintenance in the University. He is having more than 8 Years of academic and administrative experience in the field of Computer Science & Information Technology. He is B. Tech & M. Tech and presently pursuing Doctorate in the fineld of Computer Sciecne and Engineering. He has published more than 15 research manuscripts in various International & National journals & conferences. He has also presented papers in International and National conferences.

He is the member of various International & National professional & academic bodies. In addition to this, he is the member of Editorial Board of various International Journals related to the field of Computer Science & Information Technology. He is the part of more than 10 international Journals of repute as Reviewer. He has guided the students in their M. Tech dissertations. He is also the part of Indira Gandhi National Open University, Delhi as Project Guide in the region of Shimla (H. P.). He is an active participant of various Seminars, Induction and faculty development programmes.

His main areas of expertise are Energy Efficiency in Wireless Sensor Networks, Efficient use of IT Resources in the Organizations and Security in Wireless Networks. He has also been invited for guest lecturers in the Short Term Courses at National Institute of Technical Teacher Training & Research, Chandigarh.

Dr. Manoj Manuja is currently associated with Vertical Head – I.T. at iNurture Education Solutions, Bangalore and responsible for the design, development, deployment and smooth operations of 59 I.T. programs on niche technologies across 26 campuses with 246+ faculty members on board. In the previous assignment, he has worked as Principal – Education & Research and Head – Data Science and Big Data Competency Development Team at Infosys Limited, India. He has published more than 19 research papers in SCI Indexed / IEEE / Journals of repute / International Conferences. His primary expertise is in Data Science, Big Data Technologies and Cloud Computing, with globally recognized certifications from Amazon Web Services (AWS), IBM and Microsoft. Dr. Manuja has more than 24 years of diverse experience in the field of Technical Competency Development and Information Technology. He has been an active member of many professional societies.

Keshav Kishore is currently working as Faculty of Computer Science & Engineering at Alakh Prakash Goyal Shimla University, Shimla. He is having more than 9 years of Industry and Academics in the fiend of Computer Science and Information Technologies. He also worked as LAMP Developer in Computer Ware India Pvt. Ltd- New Delhi, India. He is pursuing Ph. D (Computer Sciecne & Applications) from Magadh University, Bihar, India. He is an MCA and alumnus of SRM University, Chennai, India under the program of M. Tech (Computer Science & Engineering). He has published more than 15 papers in national and International Journals of repute.