



International Journal Of
**Recent Scientific
Research**

ISSN: 0976-3031
Volume: 7(5) May -2016

INTERNET OF THINGS: SECURITY & PRIVACY THREATS

Shalini Vermani



THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
<http://www.recentscientific.com/> recentscientific@gmail.com



ISSN: 0976-3031

Available Online at <http://www.recentscientific.com>

International Journal of Recent Scientific Research
Vol. 7, Issue, 5, pp. 11403-11406, May, 2016

**International Journal of
Recent Scientific
Research**

Research Article

INTERNET OF THINGS: SECURITY & PRIVACY THREATS

Shalini Vermani

Apeejay School of Management, New Delhi, India

ARTICLE INFO

Article History:

Received 29th February, 2016
Received in revised form 19th March, 2016
Accepted 25th April, 2016
Published online 28th May, 2016

Key Words:

Sensors, RFID, WSN, Security,
Privacy, Internet

ABSTRACT

With IoT all the objects in the world are becoming smart. As more businesses and homeowners use smart devices to enhance company efficiency and lifestyle convenience, they are also increasing the target space for malicious cyber attacks. This paper discusses various applications of IoT and also the possible security threats that could have a huge impact on businesses and individuals.

Copyright © Shalini Vermani., 2016, this is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

Internet of Things (IoT) is a computing concept where each physical object is connected to Internet and is able to identify itself and also other devices present in the network. These devices include everything from cell phones, coffee makers, headphones, washing machines, lamps and almost all the devices one can think of. In other words, IoT is a giant network of connected "things".

In IoT, each device has inter-connected microchip inside it. These inserted microchips help not only to keep track of the devices but also sense their surrounding and report it to other machines as well as to humans. In IoT, every physical and virtual entity is communicable, addressable and accessible through the Internet. Now days, technology cost is going down, broadband Internet is becoming more widely available, cost of connecting is decreasing, most devices are created with wifi and have built in sensors. All these things are creating a "perfect storm" for IoT. According to Gartner, Inc. (NYSE: IT), the world's leading information technology research and advisory company, there were 4.48 billion connected IoT devices in 2015 and the number is expected to grow 30% in 2016. These connected devices could provide a much larger surface for attackers to target home or office networks.

APPLICATIONS OF IOT

Internet of Things touches every facet of our lives. Some applications of IoT are:

Healthcare: Health and wellness is one of the most promising application areas of IoT technology. IoT in healthcare provides

an environment where a patient's vital parameters get transmitted by medical devices onto secure cloud based platforms where it is stored, aggregated and analyzed. The major use of IoT technology in this domain includes care for the pediatric, aged and chronic disease patients.

Smart Home: Data related to home power, gas and water supply usage can be sent automatically to the corresponding utility company to enhance efficiency of the resources. In a smart home, windows, home ventilations, doors, lightings, air conditioning, refrigerators, washing machine, oven etc. can be manipulated by remote platforms or programs.

Connected Cars: Cars and vehicles act as nodes and can communicate with each other and also with the road side infrastructure. Sensors in a car can be used for safety, collision avoidance, traffic management and to provide accurate information about parking spaces.

Environmental Monitoring: Environmental monitoring applications of IoT use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions and can even include areas like monitoring movements of wildlife and their habitats.

Infrastructure Management: One of the key applications of IoT is to monitor and control operations of urban and rural infrastructures like bridges, railway tracks, on and off shore wind farms etc. IoT infrastructure can be used to monitor any event or change in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities. IoT devices for monitoring

*Corresponding author: **Shalini Vermani**
Apeejay School of Management, New Delhi, India

and operating infrastructure are likely to improve quality of service, emergency alerts and reduce cost of operations.

Manufacturing: IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands and real time optimization of manufacturing, production and supply chain management by networking machinery, sensors and control systems together.

NEED FOR SECURITY

According to the leading market research and consulting firm 'International Data Corporation (IDC)', 32 billion objects will be connected to the Internet by 2020. In future, machine to machine communication and data processing will reach all time high. Any attack on a single connected node can break an infrastructure. For example, if a hacker controls a connected car, he has access to its private data like location and potentially could also jam its braking system. Major security concerns of IoT are:

Data Confidentiality: It means that information transmitted between two nodes will remain confidential and no one else can read that information. For example, in healthcare applications of IoT, health parameters of a patient should only be transmitted to the medical practitioner and no one else could read that information.

Data Integrity: It refers to maintaining and assuring the accuracy of the data transmitted between two nodes. For example, in smart home, if the owner of the house gives instruction from his mobile to 'lock the front door of the house', then the adversary should not be able to change it to 'open the front door of the house'.

Data Authenticity: In authentication process, the receiver is assured that the data received is originated from trusted source only. For example, in infrastructure management application of IoT, sensors in a bridge transmit condition of the bridge. Based on that information, decisions like scheduling repair or maintenance of the bridge are made. To take such decisions, the receiver must be sure that the information received is from the bridge's sensors and not from any adversary.

Data Availability: One of the major concerns of IoT security is to make data available to its users, whenever needed. Data should be available not only in the normal conditions but in disastrous conditions also.

IOT TECHNOLOGIES AND SECURITY THREATS

Wireless Sensor Network

Wireless Sensor Networks (WSNs) are heterogeneous systems containing many small devices called sensor nodes and actuators with general purpose computing elements. These sensor nodes have three main components sensing, data processing and communication. There are various applications of WSNs in IoT like habitat monitoring, logistics, environment observation and forecasting, military applications and healthcare etc. WSNs are vulnerable to security attacks due to the broadcast nature of the transmission medium. Major security threats of WSNs are:

Selective Forwarding: In WSN, it is assumed that all nodes faithfully forward received messages. But in this attack,

malicious node selectively forwards packets. It may refuse to forward certain messages and simply drop them. In this attack, an adversary is interested in suppressing or modifying packets originating from few specific nodes and reliably forwards the remaining traffic from other nodes. In this way, the malicious node limits the suspicion of its wrong doing.

Wormhole Attack: Wormhole attack is a critical attack in which the attacker records the packets at one location in the network and replays it to different location. The replaying of bits could be done selectively.

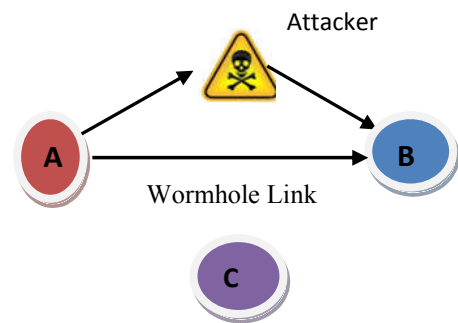


Fig. 1

For example, in fig.1, wormhole attack is carried out by attacker's node located within transmission range of legitimate nodes A and B, where A and B are not within transmission range. When a node A (for example, the base station or any other sensor) broadcasts routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of node A, and will mark this node as its parent. Attacker's node is just transmitting packets between A and B and so is virtually invisible. Now all the transmission between A and B is controlled by attacker's node, which can drop packets or can even break the link.

Wormhole attack is one of the Denial-of-Service (DoS) attacks that can affect the network even without the knowledge of cryptographic techniques implemented. It may be launched by one, two or more number of nodes.

Sybil Attack: Sybil attack happens when an insecure computer is hijacked to claim multiple identities. Using Sybil attack, an adversary can be at more than one place at one time. In this attack, a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, disparity and multipath.

Sinkhole Attack: In Sinkhole attack, an intruder compromises a node inside the network and tries to attract all the traffic from neighbor nodes. This attack can be done by making compromised node attractive to surrounding nodes with respect to the routing algorithm. So, by taking part in the routing process, the adversary can then launch more severe attacks, like selectively forwarding, modifying or even dropping packets.

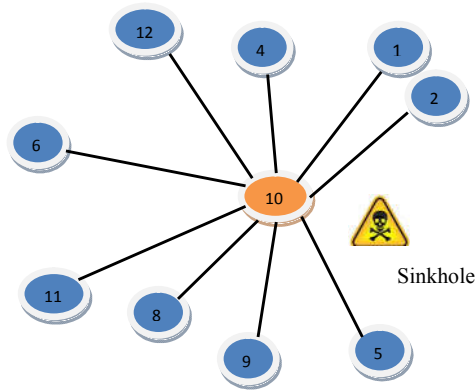


Fig. 2

Denial of Service Attack: DoS attack is to make services unavailable to legitimate users. In this attack, the victim's links are destroyed by flooding them with legitimate-like requests from attacker.

Physical Attacks: IoT to achieve its full capability, sensor devices to be implemented in each and every object. But we cannot physically protect the devices from unauthorized physical access. An attacker can substitute a node/sensor with illegal and detrimental one, thus can negotiate the functioning of the whole sensor network.

Node Replication: In this attack, an attacker simply adds a node to a sensor network by copying node- id of an existing sensor node in it. This results in false sensor readings, mis-routing of packets or even a network disconnection. In this way, the attacker disrupts a sensor network's performance.

Eavesdropping: In eavesdropping, intruder listens the information while it is transmitted between the two nodes over the network. In this attack, information remains the same but its privacy compromises.

Radio Frequency Identification Technology

Radio-frequency identification (RFID) is composed of several RFID tags and one or more RFID readers. These tags have specified address and are attached to objects. A RFID tag attached to an object provides a unique identifier for that object. RFID tags are used in various applications of IoT like patient's health parameters monitoring, track progress of production of an automobile in an assembly line, monitor temperature and humidity of perishable food item to ensure that the food is kept in proper climatic conditions, animal tracking, access control, shopping and much more. But there are various attacks against RFID technology. Some of the attacks are:

Physical Data Modification: In this, an attacker physically obtains tags and alters its information. Physical data modification can be achieved by either fault induction or by memory writing. Fault induction involves modifying data when it is written or processed whereas memory writing can be performed by using special equipments like laser cutting microscopes or small charged needle probes. Such attacks lead to inconsistency between the data stored on the tags and the objects to which these tags are attached. For example, a RFID tag attached to a food item gives incorrect information about

the contents of the food item. Secondly, this attack can reduce the traceability of a tag.

Tag Cloning: RFID tag cloning is to replace the original tag with the new one and to copy the original tag identifier (id) in it. These tags and software are easily available. So if no physical access protection is used for RFID tags, attacker can easily replace the original tag with the new one.

Tag Swapping: Tag swapping attack is a popular impersonation attack. It is a quite simple attack in which tags attached to two products are replaced with each other. Such kind of attacks usually occur in retail stores where a high priced tag is replaced with a low price tag to buy high priced product at lesser rate.

Denial of Service Attack: When a RFID reader requests information from a tag, it receives the identification id of the tag and compares it with the id stored in its database. Both RFID reader and server database are vulnerable to DoS attack and when this attack takes place, the tag fails to send its identity to the reader. So the connection between the tag and the reader will not accomplish and will interrupt the service.

CONCLUSION

IoT has significant benefits for businesses and individuals. In IoT, data transmitted from sensors or RFID tags may carry sensitive information that must be protected from unauthorized access as security is an important matter to everyone. But current IoT communication is not secure and also physical security of IoT devices is not tamper proof. For secure communication, IoT must include services such as access control for real-time end-to-end-environments, encryption and critical infrastructure protection. Learning how to stay ahead of cybercrime is challenging and will take time. We hope that security of smart devices & privacy of IoT communication will increase in the near future allowing anyone to conveniently use this technology to automate tasks. Without a doubt, IoT with privacy, data protection and ethical practices will win everyone's trust and gain competitive advantage in the connected world.

References

1. Bahekmat, M., Yaghmaee, M. H., Yazdi, A. S., & Sadeghi, S. (2012). A Novel Algorithm for Detecting Sinkhole Attacks in WSNs. *IJCTE*, 4(3), 418-421.
2. Balte, A., Kashid, A., & Patil, B. (2015). Security Issues in Internet of Things (IoT): A Survey. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(4), 450-455. ISSN: 2277 128X.
3. Chowdhury, M., Kader, M. F., & Asaduzzaman. (2013). Security Issues in Wireless Sensor Networks: A Survey. *International Journal of Future Generation Communication and Networking*, 6(5), 97-116.
4. Dlodlo, N., Foko, T., Mvelase, P., & Mathaba, S. (2012). The State of Affairs in Internet of Things Research Volume Issue. *The Electronic Journal Information Systems Evaluation*, 15(3), (244- 258).
5. Douceur, J. R. (2002). The Sybil Attack. *Peer-to-Peer Systems*, 251-260.

6. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.
7. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services*.
8. Juels, A. (2006). RFID security and privacy: a research survey. *IEEE J. Select. Areas Commun*, 24(2), 381-394.
9. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility*, 1(4), 309-348.
10. Maidamwar, P., & Chavhan, N. (2012). A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network. *IJANS*, 2(4), 37-50.
11. Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. *Lecture Notes in Computer Science*, 242-259.
12. Sathish Kumar, J., & R. Patel, D. (2014). A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications*, 90(11), 20-26.
13. Singla, A., & Sachdeva, R. (2013). Review on Security Issues and Attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4), 529-534.
14. Sklavos, N., & Agarwal, V. (2008). RFID Security. *From RFID to the Next-Generation Pervasive Networked Systems*, 107-125.
15. Soni, V., Modi, P., & Chaudhari, V. (2013). Detecting Sinkhole Attack in Wireless Sensor Network. *International Journal of Application or Innovation in Engineering & Management (IJAIEEM)*, 2(2), 29-32.
16. Sushma, Nandal, D., & Nandal, V. (2011). Security Threats in Wireless Sensor Networks. *IJCSMS International Journal of Computer Science & Management Studies*, 1(11).
17. Tsai, C., Lai, C., & Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. *Wireless Netw*, 20(8), 2201-2217.
18. U.Farooq, M., Waseem, M., Khairi, A., & Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 111(7), 1-6.
19. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). On the Security and Privacy of Internet of Things Architectures and Systems. *2015 International Workshop on Secure Internet of Things (SIoT)*.
20. Z L., & T X. (2013). Threat Modeling and Countermeasures Study for the Internet of Things. *JCIT*, 8(5), 1163-1171.

How to cite this article:

Shalini Vermani.2016, Internet of Things: Security & Privacy Threats. *Int J Recent Sci Res*. 7(5), pp. 11403-11406.

T.SSN 0976-3031



9 770976 303009 >