International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Wearable Forensic Traces and Security Challenges

Divya Premchandran

Assistant Professor, Department of Information Technology and Computer Science, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

Abstract: ***IOT devices are used to collect various data and processed to provide better living for users in day today life. IoT devices in association with various smart devices can be utilized. It helps to simplify our daily chores and gives an opportunity for better living. Use of these devices had bought many challenges in security and data in our lives. Main problem had raised in securing and analyzing evidences for digital forensic investigation. The reason for the need for digital forensic in IoT is that these devices can provide evidences which can be a great help in criminal investigation. In this research paper I had concentrated on smart watch IoT forensic and given a foresight of challenges in collecting evidences from mentioned device.***

Keywords: Wearable device, Wearable forensic, IoT, IoT- Forensic, Smart watch, Forensic Investigation

1. Introduction

IoT like any other system need a way to analyze things that happened within a system. Performing such analysis is known as forensic. Over the last several years the use of smart wearables use has been increased significantly. Smartwatch could be a new and open frontier for cyber criminals, As smart watch are not too smart about protecting your personal information ultimately giving cyber criminals a chance to intercept that information and use it to their advantage. The information includes messages, email, contact, health information and fitness data. In recent study it has been proved that 10 smart watches they had tested is vulnerable to attack easily. Wearable devices have only just started to become a part of our lives, but they deliver a new level of functionality that could potentially open the door to new threats to sensitive information. In this paper is focusing on various smart watches preliminary forensic analysis are done as well as security challenges related with it.

Wearable devices

Wearables are electronic technology or devices incorporated into items that can be comfortably worn on a body. These wearable devices are used for tracking information on real time basis. They have motion sensors that take the snapshot of your day to day activity and sync them with mobile devices or laptop computers. After the invention of smartphones, wearable electronics are the next big innovation in the world of technology.

The efficient data processing in various devices such as smart clothes, smart wristwear and medical wearables along with consumer-oriented service of the IoT technology becomes inevitable in smart healthcare systems. The wearable market is currently dominated by health, safety, interaction, tracker, identity, fitness etc. Wearables increase the convergence of physical and digital world which automatically bring people into the IoT. The popularity of wearable devices is growing exponentially since it entirely changes the way how the consumers interact with the environment. 74% people believe that the wearable sensors assist them in interacting with the physical objects around them. Henceforth, one out of three smartphone users will wear minimum 5 wearables in 2020. Moreover, 60% believe that wearables in the next five years will be used not only to track health related information, although it can be used to control objects, unlock doors, authenticate identity and transactions. Wearables must be evolved to cope with the future to meet the expectations of consumers, where the users will wear many devices that is connected with the internet to interact with the physical surroundings and receive data in a seamless secure way. By 2021, smartwatches are estimated to be sold to nearly 81 million units which signifies 16% sales of total wearable device. According to the latest figure of Gartner report, the global shipment of wearable devices are anticipated to raise by 25.8% every year to $225 million (GBP 176.3 million) in 2019. Researchers also forecasted that the usage of wearable devices by the end users will increase to $42 billion (GBP 32.9 million) in 2019. In recent years, the IoT based Smart Healthcare system has influenced greatly on growing demand of wearable devices. In fact, the Wearable IoT (WIoT) devices are generating huge volume of personal health data. Enabling technologies such as cloud computing, Fog computing and Big Data play vital role in leveraging WIoT services. These enabling services over the voluminous health data enhance clinical process at health care system at remote or local servers. The traditional remote healthcare information system involves data transfer, signal processing mechanism and naive machine learning models deployed on remote server to process the medical data of patients. This technique has several demerits like they are not suitable for resource constrained wearable IoT devices. The resources such as processing, memory, energy, networking capability are limited in WIoT devices. Traditional mechanism lacks optimization of resource usage, prediction of medical condition, and dynamic assessment based on available information. Further, the naive machine learning techniques does not perform knowledge generation, decision making and discover hidden valuable patterns from the available medical data. The integrated platform in which cloud computing serves as backend computing systems, Fog computing as edge computing and Big data as platform for data analysis, knowledge generation promise to provide valid solution to several issues of Wearable IoT devices. Next, the health data generated through WIoT devices are personal and sensitive. Hence, the security and privacy of such delicate data at all level of WIoT ecosystem is essential. Below mentioning few wearable smart devices:

- **Smart Watches:** A watch that does more than just telling time. It provides users notifications on their calls, messages, emails, social media updates, etc.
- **Fitness Tracker:** Helps keep a track of the number of steps the user walks each day and continuously monitors the heart rate. Using this information, the devices are able to calculate and report accurate data on calorie burn and exercise done by the user.
- **Head Mounted Display:** Takes you to a different world of virtual reality. It provides virtual information directly to your eyes.
- **Sports watches:** The wearable devices are especially built for sports personnel who love running, cycling, swimming etc. These devices come with GPS tracker and records information on the user's pace, heart rate etc.
- **Smart jewellery:** Smartwatches are designed as jewelleries specially targeting women. These jewelleries' notify the users of their text messages, calls or emails when their phone is out of reach.
- **Smart Clothing:** The smart electronic devices are incorporated into the Wearable Clothing to give an interesting and fashionable look.
- **Implantable:** These wearable electronics are surgically implanted under the skin. These are usually used for medical reasons like tracking contraception's, insulin levels etc

Basic Structure of Wearable device

- **Node Communication:** Helps to pair with devices like PC or Mobile and helps application to connect with devices using Bluetooth or WIFI.
- **Data Communication:** Once node is connected then it channelizes the data communication with the wearable proprietary application. In this several systems are involved smart watch, smart phone, computer / app mobile and cloud services. There is always proprietary system available for all smart watch vendors which will be required to connect the smart watch. Hence these services help to maintain the data of smart watch in through a mobile application or system application.

There are TWO main data transfer

- From Smart Watch to proprietary system or application.
- Smart Watch to direct access without proprietary system or application

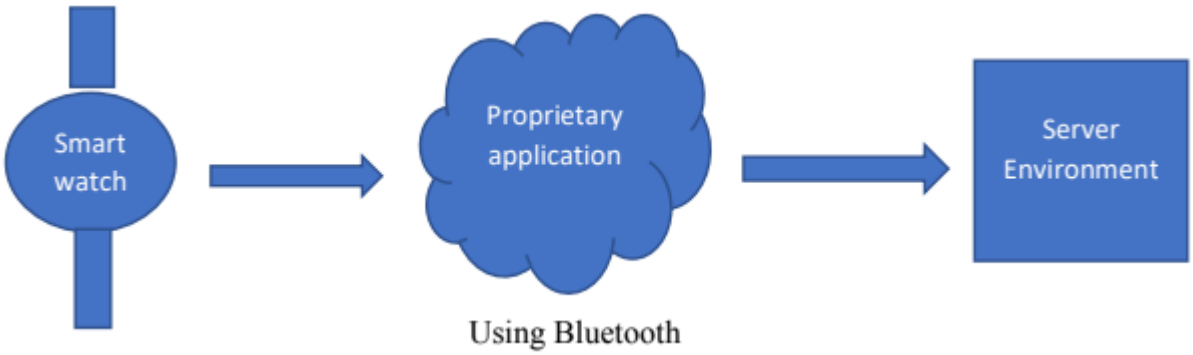

Figure 1.1: Smart Watch connection through proprietary system

In above mentioned Fig 1.1 wearable device is connected through vendors proprietary application in this connection is established using Bluetooth. The wearable send the data to its proprietary warehouse. This is performed through the proprietary transfer solution. Application running in an intermediate smart watch or Personal Computer will act as a gateway towards the server. As we are connecting with Bluetooth the energy required is very high and any time connection can be lost hence the data transfer can be affected same.

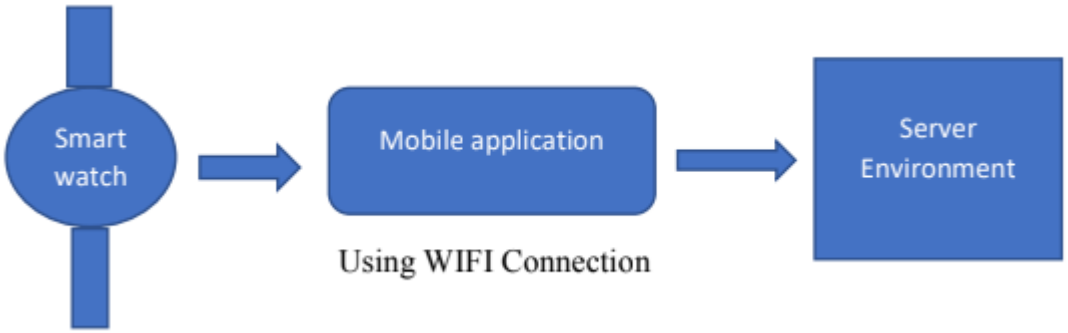

Figure 1.2: Direct access to smart watch through WIFI Connection

In above mentioned Fig 1.2 is something is not in use but very advantageous compared to the Bluetooth transmission in this direct connection can be established through WIFI access points. Here the connection between the smart watch is established for long time when compared with Bluetooth. Hence loss of data and connection risk is less when compared in considerable amount of time.

2. Conclusion

This paper analyzes the problem related to the smart watch data connection mechanism and issues related to the data communication. Here I am proposing a structure which can help to trace the data of smart watch without propitiatory tool or any vendor application intervene. Through this Bluetooth transfer hindrance can be removed in wearable devices.

References

[1] Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M., & Liljeberg, P. (2016). On the Feasibility of Attribute-Based Encryption on Internet of Things Devices. IEEE Micro, 36(6), 25–35. http://doi.org/10.1109/MM.2016.101

[2] Chifor, B.-C., Bica, I., Patriciu, V.-V., & Pop, F. (2017). A security authorization scheme for smart home Internet of Things devices. Future Generation Computer Systems. http://doi.org/10.1016/j.future.2017.05.048

[3] Mai, V., & Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. Future Generation Computer Systems, 72, 327–338. http://doi.org/10.1016/j.future.2016.06.003

[4] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37. http://doi.org/10.1016/j.jnca.2017.02.009

[5] Giaretta, A., Balasubramaniam, S., & Conti, M. (2016). Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks. IEEE Transactions on Information Forensics and Security, 11(4), 665–676. http://doi.org/10.1109/TIFS.2015.2505632

[6] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28. http://doi.org/10.1016/j.jnca.2017.04.002

[7] Rawassizadeh, R.; Price, B.A.; Petre, M. Wearables: Has the Age of Smartwatches Finally Arrived? Commun. ACM 2014, 58, 45–47. [CrossRef]

[8] Swan, M. Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2. J. Sens. Actuator Netw. 2012, 1, 217–253. [CrossRef]

[9] Richter, F. The Predicted Wearables Boom is All about the Wrist. Available online: https://www.statista.com/chart/3370/wearable-device-forecast/ (accessed on 24 May 2016).

[10] Sazonov, E.; Neuman, M. Wearable Sensors: Fundamentals, Implementation and Applications; Academic Press: Waltham, MA, USA, 2014.