Internet Society
India Mumbai

Topic: IoT and IoT Security Issues in the healthcare and pharmaceutical sectors.

Date: 20 thNovember,2018

Venue: Hinjewadi Phase 2,Pune.

Nikola Tesla, in an interview with the Colliers magazine in 1926, had stated, "*When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole.....and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."* Though he did not coin the term "Internet of Things", he is considered to be one of critical members working on the IoT concept. Kevin Ashton is credited for the term "The Internet of Things" in 1999 during his work at Procter & Gamble. He was able to create ripples with his work but IoT actually blew up in 2013 and is continuing to grow exponentially. According to NASSCOM, the global market size of IoT is expected to touch USD 3 trillion by 2020 with nearly 20.4 billion IoT devices being deployed.

Although IoT in the healthcare industry is not yet in widespread use, experts predict a massive growth, on the clinical side as well as on the back end. Many multinational corporations are heavily investing in IoT to provide better services to their clients. ISOC India Mumbai volunteer, Ms. Sneha Tambe conducted a session on IoT and IoT security issues for the healthcare industry in a leading multinational corporation. This multinational corporation is a Fortune 500 company, has a net revenue of US$39.6 billion for fiscal 2018, and offices and operations in more than 200 cities in 52 countries. The session primarily focused on making people aware about the IoT applications, IoT security issues in the healthcare and pharmaceutical sectors so that they can better relate to it.

According to Sneha's research, IoT can transform the healthcare and pharmaceutical sectors by changing how the pharmaceuticals are manufactured, how they are tested, how the patients are consuming their medicines, how the healthcare professionals are keeping a track of patient's dosage, how the different healthcare services are delivered and so on. IoT can provide many benefits by improving the drug's time-to-market, eliminating waste and improving the consumer experience.

Advanced sensors can be placed on the manufacturing machinery to ensure rigid quality control. Temperature, humidity, light exposure, room pressure can be tracked and controlled according to the drug requirement. Sensors can also be used in the storage centres wherein potential contamination could be minimized by keeping the drug in a controlled environment. These sensors can then alert the required stakeholders in case of a contamination in a drug and any consequence of drug getting exposed to unfavourable conditions would not result in any human fatality.

One of the participants informed the audience that IoT can keep a track of the drug dosage for a patient. Intelligent pill bottles can track when the patients take their

medication and can send an alert when a dosage is missed. Sensors can also be embedded in certain medications in order to understand the impact of the medication on the patient and can easily alert the healthcare professionals if any adverse reaction is detected. These sensors can also collect vital data which can be compared to the clinical studies and can be used to modify the medicine and dosage for the patients.

One of the ISOC India Mumbai volunteers, Prateek, reminded the audience that the proliferation of devices collecting health data, sending them over to process them where proper processing capabilities are available (which is in most cases is the Cloud), and exploiting it with the proper tools (big data), introduces new risk components to take care of. Thus, data security and privacy are critical challenges for IoT, especially in the healthcare and pharmaceutical industries. This data must be safeguarded to protect the individuals' privacy and must be secured to prevent threat from the competitors. In the United States, the HIPAA(Health Insurance Portability and Accountability Act) law states a broad set of regulations that are concerned with the collection and usage of medical data for uniquely identifying individuals. Before IoT, this data was collected offline and secured by the organization's information systems. But with IoT, the number of devices collecting this data has astronomically increased. Any device, if not protected, can prove to be a potential gateway for hackers. There is a possibility that a zero-day exploit in a medical device can be used to injure or even kill someone without being detected. The rise in hackable medical devices has forced the FDA to issue formal guidance on how medical device makers should handle reports about cyber vulnerabilities.

It is possible for the hackers to tamper with the medical devices to harm individuals and healthcare clinics/hospitals together. The term coined for the medical device hijacking is "medjacking".One of the security engineers from the corporation narrated the findings of an important report. According to him ,TrapX released a report in 2015 which stated that most healthcare organizations are vulnerable to medjacking. The report provided details about the medjacking incidents occurred in 3 leading hospitals in the US. In a case mentioned in the report, a blood gas analyser was infected with two different types of malware. It was used to steal passwords for other hospital systems and confidential data was sent to computers in Eastern Europe. At another hospital, the radiology department's image storage system was used to gain access to the main network and highly sensitive data was sent to servers in China. Stolen medical identities are much more valuable than the price of a stolen credit card number.

One of ISOC India Mumbai volunteers narrated the incident of Johnson & Johnson(J and J). The company recently informed patients that it has learned of a security vulnerability in one of its insulin pumps that a hacker could exploit to overdose diabetic patients with insulin. This system is vulnerable because communications are not encrypted, to prevent hackers from accessing the device. Hackers can force the device to deliver unauthorized insulin injections. The chances of such a hack happening is very low. However, this is the first time a manufacturer of medical devices had issued such a warning to patients about a cyber vulnerability. This revelation has increased concerns about possible bugs in pacemakers and ICDs. J&J is warning customers and providing advice to fix the issue.

It is essential to understand the critical role of data in the healthcare and pharmaceutical sectors. IoT is definitely transforming these industries but it comes with its issues. Mostly it is noticed that when people are given timely and efficient trainings, these issues could be minimized. Though there is nothing called as a “completely secure, hack-free system”, we can increase our knowledge regarding the issues and invest into advanced systems in order to avoid their occurrence.

Apart from healthcare and pharmaceutical industries, one of the audience members asked a query about Internet Society’s work in IoT arena. They were informed that ISOC only endorses consumer IoT products that are compliant to the OTA(Online Trust Alliance) IoT Trust Framework. The IoT Trust Framework includes a set of strategic principles necessary to help secure IoT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices.

The informative session concluded with the audience appreciating the efforts of ISOC India Mumbai volunteers for increasing their awareness on IoT issues within healthcare and pharmaceutical industry. They were also happy to know about the OTA framework.