IoT and Cyber Security in Healthcare sector

In healthcare, the Internet of Things (IoT) offers many benefits, including being able to monitor patients more closely and using data for analytics. When it comes to IoT for medical device integration, the focus is shifted towards the consumer end, such as glucose meters, blood pressure cuffs, and other devices designed to record data on patient vital signs. This enables healthcare providers to automatically collect information and apply decision support rules to allow for earlier intervention in the treatment process.

Unfortunately, medical companies often do not consider the security risks of connecting these devices to the internet. 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.

Medjacking:- It is possible that hackers could tamper with medical devices to harm individuals, but we haven’t seen anything like that yet. Devices are usually hacked so attackers can get into larger medical systems and steal protected health information. In June 2015, a report was released by TrapX, a security company which revealed that most healthcare organizations are vulnerable to medical device hijacking also called "medjacking". The report provided details about incidents of medjacking in three hospitals.

- In the first case, a blood gas analyzer infected with two different types of malware was used to steal passwords for other hospital systems, and confidential data was being 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, sensitive data was retrieved and sent to a location in China.
- In the third case, hackers used the vulnerability in a drug pump to gain access to the hospital network. Stolen medical identities are much more valuable than the price of a stolen credit card number. The current state of security in many medical devices allow hackers easy access to steal massive numbers of sensitive data from healthcare provider’s systems .
- Insulin pumps are medical devices that patients attach to their bodies that injects insulin through catheters. The Animas OneTouch Ping, was launched in 2008, is sold with a wireless remote control that patients can use to order the pump to deliver a dose of insulin, which is typically worn under clothing and can be awkward to reach. Johnson & Johnson 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.

Incident timeline of Ransomware attack at AIIMS Delhi:-

Earlier on Wednesday (November 23), AIIMS had reported a malfunction in its server. Since Wednesday, the server is down, and the officials are manually managing the sample collection and OPD.

The Intelligence Fusion and Strategic Operations (IFSO) unit of Delhi Police registered a case in this regard on November 25.

AIIMS has around 40 physical and 100 virtual servers. Five have shown signs of virus infection. These servers are also being set up for scanning and new servers with updated configurations are being purchased as most servers at AIIMS were end of life/end of support. The data breach has reportedly compromised the data of nearly 3–4 crore patients, including sensitive data and medical records of the President, Prime Minister, former Prime Minister, and many other VIPs ministers.

Techniques for responding to ransomware infection:-

It is recommended to follow the following steps to recover from ransomware infection:-

- Isolate the infected system
- Turn off other computers and devices in the network
- Contact your vendor security team for better results and finding its source.
- Need to pay close attention to the ransom message itself, or perhaps ask the advice of a security/IT specialist before using decryption with free tools
- Use your backups to get recovery
- Include downloading a security product known for remediation and running a scan to remove the threat, try running a scan from a bootable CD or USB drive
- If system slowing down for seemingly no reason, shut it down and disconnect it from the Internet.
- If, once you boot up again the malware is still active, it will not be able to send or receive instructions from the command-and-control server.
- Without a key or way to extract payment, the malware may stay idle.

How to Secure IoT in Healthcare:-

- Security measures should be incorporated into the design of the IoT device, this includes conducting a risk assessment before the device is released for use in the market, authentication measures should be built into the device.
- Make sure that authentication is properly followed, device access is limited, firmware being sent to the device is verified, and device-to-device communication is monitored.
- A defense in depth strategy should be implemented, where several layers of security is in place to protect against specific risks.
- Ensure there are proper access control in place that limit unauthorized access to data, the IoT devices and the networks.
- Test the security of the IoT device before it is put into production and monitor the security of the device throughout its life cycle.
- Establish culture of security, where the employees are trained to recognize vulnerabilities.

Assignment submitted by:-

- Shweta Mahale.
- Vrushali Lobhe.
- Rudrani Angare.
- Rohit Akurdekar.