Security challenges for medical devices

Name: Rama Krishna Kamma

CWID: 50321021

Medical devices have revolutionized healthcare by providing patients with better medical care and faster recovery times. However, as medical devices become more connected to networks and the internet, they also become more vulnerable to cyber-attacks. Modification of such information, whether malicious or unintentional, may result in dangerous circumstances. The security challenges faced by medical devices include the following:

Device Safety:

This class includes implants that may be required to maintain life, including artificial hearts or automated external heart rate monitors, and are placed permanently inside human bodies. A device is classed according to the danger it presents to a user or patient (class I indicate low; class III indicate high).

Device Security:

When hackers have been able to install malicious hardware or software before the device is deployed, non-communicating yet processing devices might be crucial to security. Examples include Trojans that might be installed in heart pacemakers and then activated in response to a certain incident.

Risk assessment:

Categorize several hazards based on the CIA triad. First, confidentiality; it is possible to reveal private information about the patient and her pacemaker. Integrity: Data on a device may be changed, having a range of mild to quite severe effects on the patient. The third factor, availability, may render a device useless.

Software Security:

Software designers for medical devices must take precautions to guarantee both the safety and the security of their code in addition to functionality. Secure development and update mechanisms are both required. The patient could be put in risk if the device uploads false results to the server and the cardiologist uses those values to draw the wrong conclusions and unintentionally set the device.

Hardware Security:

Hardware safety issues are more common than security issues. Back doors in military chips have already been revealed, allowing attackers to retrieve configuration information from the chip, rewrite access and cryptographic keys, change low-level silicon features, and irreparably harm the device.

IT Infrastructure:

The IT infrastructure surrounding medical equipment must be secured as well to protect them. These are appropriate for medical device security or health care security, such as wiping hard drives clean before throwing them away, backing up data, or BYOD (bring your own device) policies.

Challenges: In Medical data if a security flaw compromises the safety of non-medical devices like automobiles, it could endanger human life as well. One can picture a situation where malicious software is added to a dynamic stability control system with the goal of causing an accident and having an impact on patients' physiology and pose a long-term risk.