BY: JESSICA TAYLOR

HACKABLE MEDICAL DEVICES

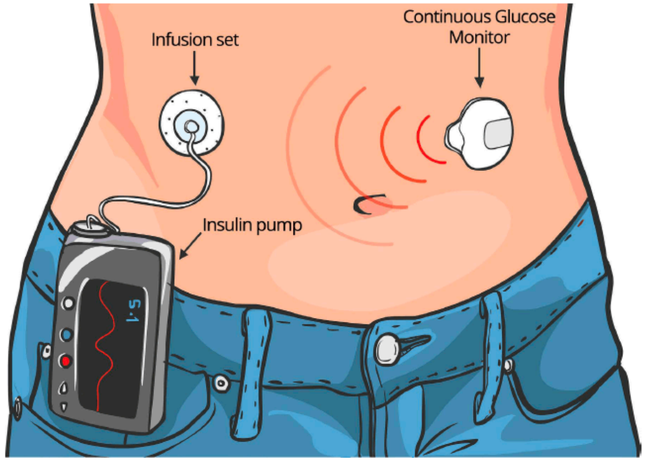
What is an Implanted Medical Device?

A man-made device surgically implanted partly or completely into the human body to replace, support, or enhance biological functions

Image Source: https://etactics.com/blog/why-hackers-exploit-implantable-medical-devices

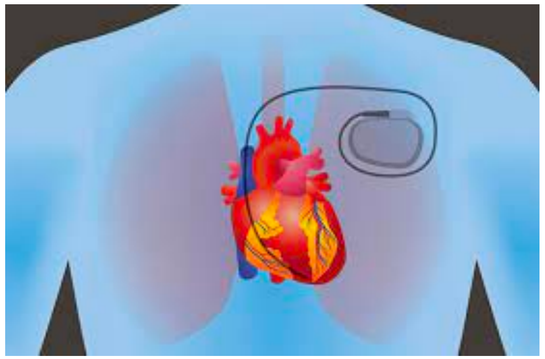
WHAT MEDICAL DEVICES ARE HACKABLE?

Diabetic Insulin Pumps



https://www.umassmed.edu/dcoe/diabetes-education/pumps_and_cgm/

Cardiac Pacemaker



https://www.pennmedicine.org/updates/blogs/heart-and-vascular-blog/2022/may/icds-and-pacemakers

Cochlear Implants

https://professionals.cid.edu/understanding-and-minimizing-the-effects-of-static-electricity-on-cochlear-implants/

Intrathecal Pain Pump

https://coloradopain.co/pain-treatments/interventional-procedures/intrathecal-pump-implants/

CONSEQUENCES OF HACKING A MEDICAL DEVICE

- Hacking a medical device can cause harm or death to the individual with the device (Clark, 2019).
- Cardiac devices can be altered to send inappropriate/lethal signals to the heart.
- Insulin pumps can be altered to administer lethal doses of insulin
- Intrathecal pain pumps can be altered to administer lethal doses of medication

https://www.techdemand.io/tag/unethical-hacking/

WHO, WHAT, WHEN , WHERE, & WHY?

- A hacker named Jay Radcliffe, who has diabetes, was curious if his insulin pump could be hacked. So, he did some experimenting and successfully discovered that the answer is: YES (Jaret, 2018).
- The method used to hack an insulin pump involves reverse engineering the device's wireless communication methods, such that the device could perform injection attacks (Radcliffe, 2011).
- At the 2011 Black Hat Conference, Radcliffe states "This combination of devices turns me into a Human SCADA system; in fact, much of the hardware used in these devices are also used in Industrial SCADA equipment".

VULNERABILITIES IDENTIFIED

- After Radcliffe determined insulin pumps can be hacked, several other hackers discovered vulnerabilities in other implantable medical devices, such as pacemakers (Clark, 2019).
- The leading vulnerabilities in implantable medical devices include:
  - Lack of software updates and patches (Williams & Woodward, 2015)
  - Lack of basic security features (Williams & Woodward, 2015)
  - Lack of encryption (Williams & Woodward, 2015)

IMPLANTABLE MEDICAL DEVICES ARE PRONE TO THREE AREAS OF ATTACK:

1. ATTACKS ON WEB SERVERS (NMAP SCAN CAN IDENTIFY POTENTIAL VULNERABILITIES IN THE NETWORK)
2. ATTACKS ON DATABASE SERVERS (SQL INJECTION ATTACK)
3. ATTACKS ON APPLICATION SOFTWARE (ANY KIND OF CODE INJECTION)

Williams & Woodward, 2015

HOW TO PREVENT ATTACKS ON MEDICAL DEVICES

- Medical device companies should work with cybersecurity professionals to ensure hardware and software components meet strict security standards.
- Medical device software should be updated frequently with potential vulnerabilities identified and patched
- Associated web and database servers should be secure and able to withstand common attacks such as SQL and code injections.
- Ensure access is only granted where access is needed
- Programmers should use proper security techniques when creating code.

REFERENCES

- Clark, M. (2019, December 2). *Why hackers exploit implantable medical devices*. Etactics. Retrieved April 13, 2023, from https://etactics.com/blog/why-hackers-exploit-implantable-medical-devices
- Jaret, P. (2018, November 12). *Exposing vulnerabilities: How hackers could target your medical devices*. AAMC. Retrieved April 13, 2023, from https://www.aamc.org/news-insights/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices
- Radcliffe, J. (n.d.). *Black Hat USA 2011 //briefings*. Black Hat ® Technical Security Conference: USA 2011 // Venue. Retrieved April 13, 2023, from https://blackhat.com/html/bh-us-11/bh-us-11-briefings.html#Radcliffe
- Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.)*, *8*, 305–316. https://doi.org/10.2147/MDER.S50048