Security Presentation

For CSCI 301 – Spring 2021

By Micah Stargel

Overview

- What was the Issue?
- Successful Strategies for How to Prevent Something Like This in the Future
- What I as a Programmer Can Do to Ensure This is Not as Easy to Do on My Code
- Sources

What was the Issue?

- When?
  - Happened before 2017
- What?
  - Many medical devices (many from St. Jude Medical) with embedded computer systems that can be vulnerable to cybersecurity intrusions and exploits (as many as 465,000 in the US).
- What are the medical devices?
  - Pacemakers and defibrillators.
- What do they do?
  - Used to monitor and control patients' heart functions and prevent heart attacks.
- Why is it possible?
  - The cardiac devices are connected to the internet.
- Why is this a problem?
  - Modify programming commands remotely (software issue).
  - Ex. - Rapid battery depletion or administration of inappropriate pacing.

Successful Strategies for How to Prevent Something Like This in the Future

- What has already been done?
  - Software update (August 2017)
  - "Cybersecurity, including device security, is an industry-wide challenge and all implanted devices with remote monitoring have potential vulnerabilities. As we've been doing for years, we will continue to actively address cybersecurity risks and potential vulnerabilities and enhance our systems.“

    - Candace Steele Flippin (spokeswoman for St Jude)
- What can continue to be done?
  - Frequent updates to combat new and ever changing/improving technology and therefore new and improved hacking.
  - “Normal” security measures:
    - Passwords/authorization/authentication
    - Debugging
    - Monitoring
    - Self-defending code

What I as a Programmer Can Do to Ensure This is Not as Easy to Do on My Code

- Know the language I’m using
- Know the environment the code will be used in
- Stay current on threats
- Use most recent versions of programming languages
- Passwords/authorization/authentication
- Use higher level languages
- Self-defensive code

Sources

- https://www.biospace.com/article/releases/fda-recalls-465-000-st-jude-medical-pacemakers-over-hacking-fears-/#:~:text=Jude%20Medical's%20RF%2Denabled%20implantable,device%20using%20commercially%20available%20equipment.
- https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/
- https://www.healthcareitnews.com/news/fda-patients-st-jude-pacemakers-update-needed-keep-hackers-out-devices
- https://www.csoonline.com/article/3222068/465000-abbott-pacemakers-vulnerable-to-hacking-need-a-firmware-fix.html

Summary

- What was the Issue?
- Successful Strategies for How to Prevent Something Like This in the Future
- What I as a Programmer Can Do to Ensure This is Not as Easy to Do on My Code
- Sources