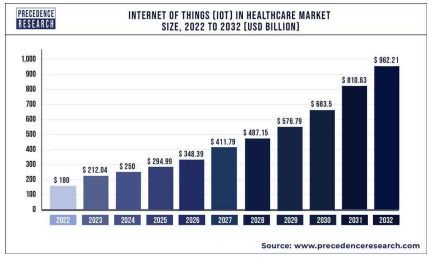
Reverse Engineering of Medical Devices for Innovation and Advancement in Healthcare

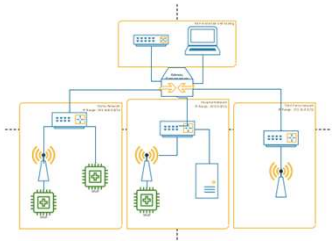
David Baldwin, Michael Nowatkowski, Jeffrey Morris, Scott Jordan

Introduction

Medical cybersecurity research addresses the critical intersection of healthcare and digital security. As medical devices expand and become increasingly interconnected, the healthcare sector is poised to become a primary target for cyber warfare. This project aims to mitigate the risks associated with a field that often underestimates the importance of cybersecurity.

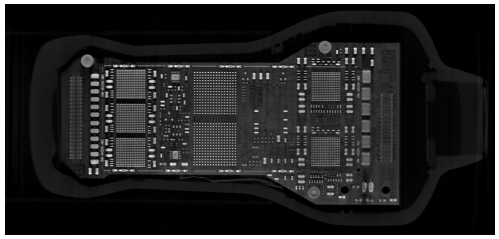


Methods



- Develop testbed environments
- Analyze hardware and methods of communication
- Rigorous reverse engineering and analysis
- Manipulate threat vectors to prove and prevent future exploitation

Medical Internet of Things(MIoT), wireless, and the privacy implications of authentication

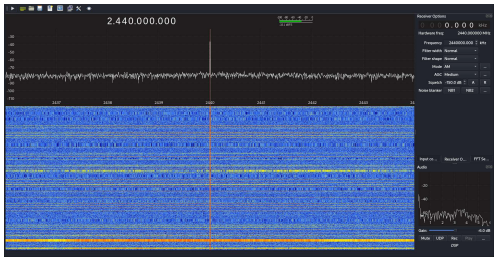


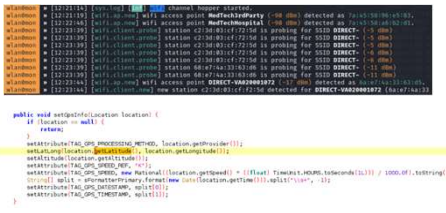
Hardware Analysis:

- Non-destructive analysis utilizing CT scans showed no signs subterfuge or other forms of supply chain attacks

Radio Frequency Analysis

- The frequencies emitted from this device aligned specifically with Bluetooth(2.4Ghz) and Wi-Fi(2.4Ghz/5Ghz)





Reverse engineering and implementation:

- Reverse engineering software shows dependent library requires GPS for authentication
- Network traffic is not fully obfuscated and can be interacted with

Results

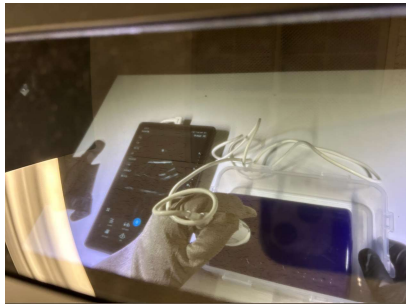
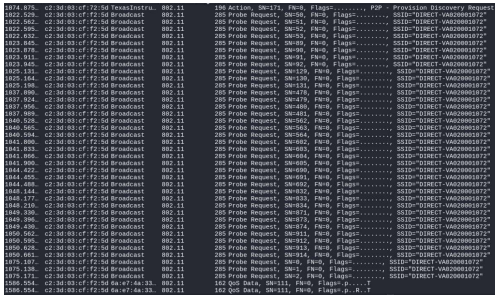


Image shows utilization of ultrasound devices during radiofrequency analysis inside of faraday cage



Network traffic shows the Wi-Fi-direct authentication handshake and successful deauth attack on device

Acknowledgement

The team would like to extend gratitude to the Augusta University for collaboration and lab space as well as the Medical College of Georgia for lending equipment and insight into unresearched projects