CASE STUDY

heartmonitor

IMPLANTABLE HEART MONITORING DEVICE WITH REMOTE UPDATE/CONFIGURATION CAPABILITY

APPLYING **AIS CYBERSECURITY EXPERTISE** TO THE WORLD OF **MEDICAL DEVICES** TO ENSURE LIFESPAN SECURITY.

The Problem

A medical device manufacturer was designing a new implantable device with over the air update capability and wanted analysis of alternatives for different technologies to ensure security over product life span (approx. 15 years)

Ecosystem included implantable device, manufacturer supplied programmer for Healthcare Delivery Organization (HDO), and bring your own device (BYOD) capability for patients.

Attack surface includes all components of ecosystem as well as communication/wireless protocols utilized (i.e. Bluetooth, BLE, 802.x, TCP/IP, etc.)

How To Test

As this was a design project we looked at public and theoretical vulnerabilities and presented a tradeoff study. Testing conducted by 3rd party after manufacture.

Regulatory Requirements Met

FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

THE AIS APPROACH

Our experience attacking common protocols and technologies allowed the customer to understand adversary mindset and not design in an "engineer vacuum." We helped them to understand adversary behavior and user operation. AIS allowed the customer to conduct the AoA/trade study in a much quicker and more accurate manner.

Security risks and weaknesses in encryption of the wireless protocol were analyzed, and additional protections were recommended to mitigate the possibility of both compromise of patient health information and compromise of patient safety. Appropriate recommendations were given. Further design assistance and pre-deployment security assessments were conducted to facilitate OTA updates. The design was evaluated and methods to prevent compromise were provided including full-disk encryption, user and management role-based authentication, and hardening of the OS kernel. Finally, the encryption and key management of server infrastructure were examined and additional risk controls were recommended.

Contact AIS for more information

info@ainfosec.com

WORKING IN AN EXPANDING LIST OF VERTICALS TO PROVIDE CYBERSECURITY SOLUTIONS THAT **MAKE OUR WORLD SAFER.**

A Little About AIS

AIS has conducted hundreds of embedded system design reviews, application analysis efforts, and secure code reviews in an effort to better understand trending technologies and to decrease the overall threats to the system – typically cyber-physical systems. Most recently AIS has focused on embedded systems supporting automobiles, remotely operated or autonomous aircraft, and self-driving military ground vehicles. AIS has also carried out cybersecurity testing of medical devices . All of the embedded platforms supporting the operation of these targets offer communications mechanisms, memory, processors, data storage, and most importantly, software that may be potentially vulnerable to attack.

AIS serves as the security consultants for the DARPA High Assurance Cyber Military Systems (HACMS) effort. The HACMS program is a research effort to improve the overall security of the embedded systems supporting the operation of autonomous or semi-autonomous vehicle platforms, both military and civilian. Vehicles used for experimentation in the HACMS program include small quadcopters, medium-scale wheeled robots, automobiles, a Heavy Equipment Transport vehicle from the U.S. Army, and Boeing's Unmanned Little Bird helicopter. Exemplar platforms tested by AIS under HACMS is shown below.

Key Capabilities of the A-Lab

- System and Software Security
- Cyber Capabilities Development
- Software Analysis Tools
- Penetration Testing
- Software Characterization
- Functional Testing
- Reverse Engineering

LINTHICUM, MD | CATONSVILLE, MD | ROME, NY

ais
AINFOSEC.COM