Arxan Protects Pacemaker Medical Device

The advancement of cloud and mobile technologies have transformed the way medical devices are accessed and data is shared with patients and medical practitioners. As a pioneer in the medical device market and one of the largest, global medical device manufacturers, this organization was leading the charge producing new medical device applications. They realized, however, that there were new risks that were unique to mobile applications; particularly given the significant increase in the volume of patient data for physicians and patients that applications were sending to apps on mobile devices. For this reason, they embarked on a strategy to harden their high-risk medical applications – starting first with all of their Class III medical devices that connect to mobile apps. Arxan was selected as their app protection partner, and now protects key applications, including those that monitor and control pacemakers.

Challenge: The physicians needed to be able to: Securely read and monitor patient data provided by medical devices and control and monitor the medical devices using a mobile application. The medical device company, however, faced a security challenge from potential tampering by hackers — including the injection or hooking of malicious code and/or attacks on memory — which could compromise the run-time operation of the application, and thereby cause unsafe or improper operation and a potential danger to patient safety.

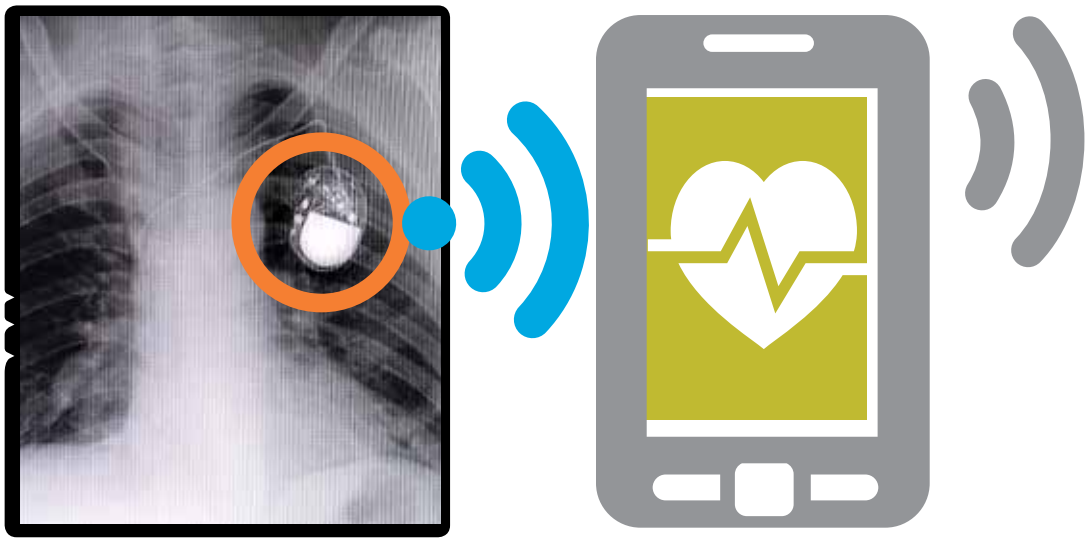
Solution: The company's application was created using Xamarin, and is now protected with Arxan Application Protection. They followed Arxan's patented and proven approach to protecting applications for healthcare and medical device providers that minimizes threats to patient health and safety by protecting binary code and cryptographic keys, and thereby also ensures the privacy and confidentiality of medical health records used in the application. Arxan "Guards" were inserted into the application binary to harden and tamper-proof the code, detect attacks at runtime, and defend the app.

The protection solution is both reactive and proactive. It is able to: repair tampered elements of the software application by replacing them with the original code, provide alerts and "phone home" protocols to monitoring consoles, and react to attacks with exit, fail, and notify functionality. These techniques prevent the disassembly or decompilation of the application or application logic that can expose code and IP. Arxan protection was applied at the post-compile stage by injecting guards into the binary. Once protected, a hacker would only be able to see obfuscated code, or "scrambled junk." With this approach, the security is "built-In" to the application so it is protected everywhere it resides – on desktops, tablets and/or mobile phones.

The company deemed it essential that all Class III / high risk Medical Devices that connect to mobile devices be hardened.

Results: The pacemaker solution and related mobile app have been successfully protected from attacks. Patient data has remained confidential, and the application has not been tampered with in a manner that jeopardizes patient safety.

The pacemaker app was built to run in Android and iOS environments – but the medical device manufacturer understood they could leverage the same protection approach for their embedded applications running on Windows and Linux, and for all of the other major mobile platforms they were using. They are in the process of rolling out Arxan Application Protection to their other applications.



About Arxan Technologies

Arxan is the trusted global leader of Application Attack Prevention and Self-Protection products for Internet of Things (IoT), Mobile, Desktop, and other applications. We help protect our customers against financial loss, brand damage, fraud, IP theft, stolen credentials, fraudulent transactions, unauthorized access, non-compliance with regulatory and industry standards, and more. Our unique patented guarding technology **1. Defends** applications against attacks, **2. Detects** at run-time when an attack is being attempted, and **3. Deters** attacks to stop hackers, send alerts, or repair making customers' applications truly resilient. We are currently protecting applications running on more than 500 million devices across a range of industries, including: financial services, automotive (connected automobiles), healthcare (connected medical devices), digital media, gaming, high tech/independent software vendors (ISVs), and others. The company's headquarters and engineering operations are based in the United States with global offices in EMEA and APAC. **Learn more at www.arxan.com.**