MedIAM - Open source pilot implementation of secure medical IoT devices

Summary

According to cybercrime magazine, "healthcare suffers 2-3X more cyberattacks than the average amount for other industries", because the data has more value for hackers. Cyber regulations such as the EU cybersecurity act provide mandatory requirements to protect sensitive information and systems. Beyond traditional clinical systems of electronic health records (EHR), it remains really difficult to extend that line of requirements to connected devices people carry around as part of their treatments. If those medical devices aren't properly secured, people may unknowingly be broadcasting their health status, as well as many other personal sensitive data, everywhere they go. Or even be directly harmed by hacked devices. Existing protocols available for IoT are unable to meet the complete requirements from regulators.

In the current proposal, we provide an open source pilot implementation on how an equipment vendor should protect the functions and data of their medical IoT devices.

Keywords

Digital identity; IoT; healthcare; secure medical devices

Actors involved in the project

Fabien Imbault (lead), entrepreneur and founder of acert.io

The NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

The project

As a serial entrepreneur, working on the next opportunity is a peculiar moment. It's the time when you can reflect on past experiences, when you get to figure out where you might make a difference, and where your efforts will be focused on for the next 10 years. That preliminary research is a lot of hard work, from new ideas to technical prototyping. Our open source project being sponsored by NGI Trust was a fantastic possibility to discuss with our peers and disseminate those findings.

During the COVID-19 pandemic, digital platforms have helped keep the population safer, for instance via the remote tracking of chronic respiratory diseases or other comorbidities. This has led to an increase in the number of telehealth solutions and of medical devices being deployed in the field.

We started our project by analysing past security breaches. The results show that healthcare boasts one of the highest average rates of severe security findings. Not all types of healthcare organizations share the same struggles. Because they're still operating in closed legacy environments, hospitals are able to maintain their level of cyber hygiene, compared to ambulatory or nursing care facilities. In the current state of affairs, integrating with SaaS vendors or third-party connected medical equipment increases the risks, because most of them exhibit an inverted ratio for exposure relative to their internet surface area.

The industry should therefore put more emphasis on privacy-and-security-by-design as an integral part of their duty of care. And it will. Because public regulators, both in Europe and overseas, have acknowledged the vulnerability of those sensitive information systems and data, with new requirements taking the force of law.

Despite those well-established challenges, finding the right product-market fit has proven difficult. Our interviews with industry participants including CISOs, IT professionals, biomedical engineers, third-party vendors, healthcare professionals and patients, exposed a silo-ed approach to innovation. Most of the participants took improvement actions but had the feeling of institutional resistance from their other counterparts.

A way to reconcile those initiatives was to put medical efficiency at the centre. People didn't care much about network segmentation or machine identity, but were asking very pragmatic questions: what's our inventory of medical equipment? Are they well used and maintained? How can a remote maintenance process be integrated into the medical lifecycle and how would the various stakeholders - and the end-users in particular - be involved and benefit from it? How do you handle the large majority of devices that can't be updated?

The solution and the results

We designed various experiments to test our hypotheses.

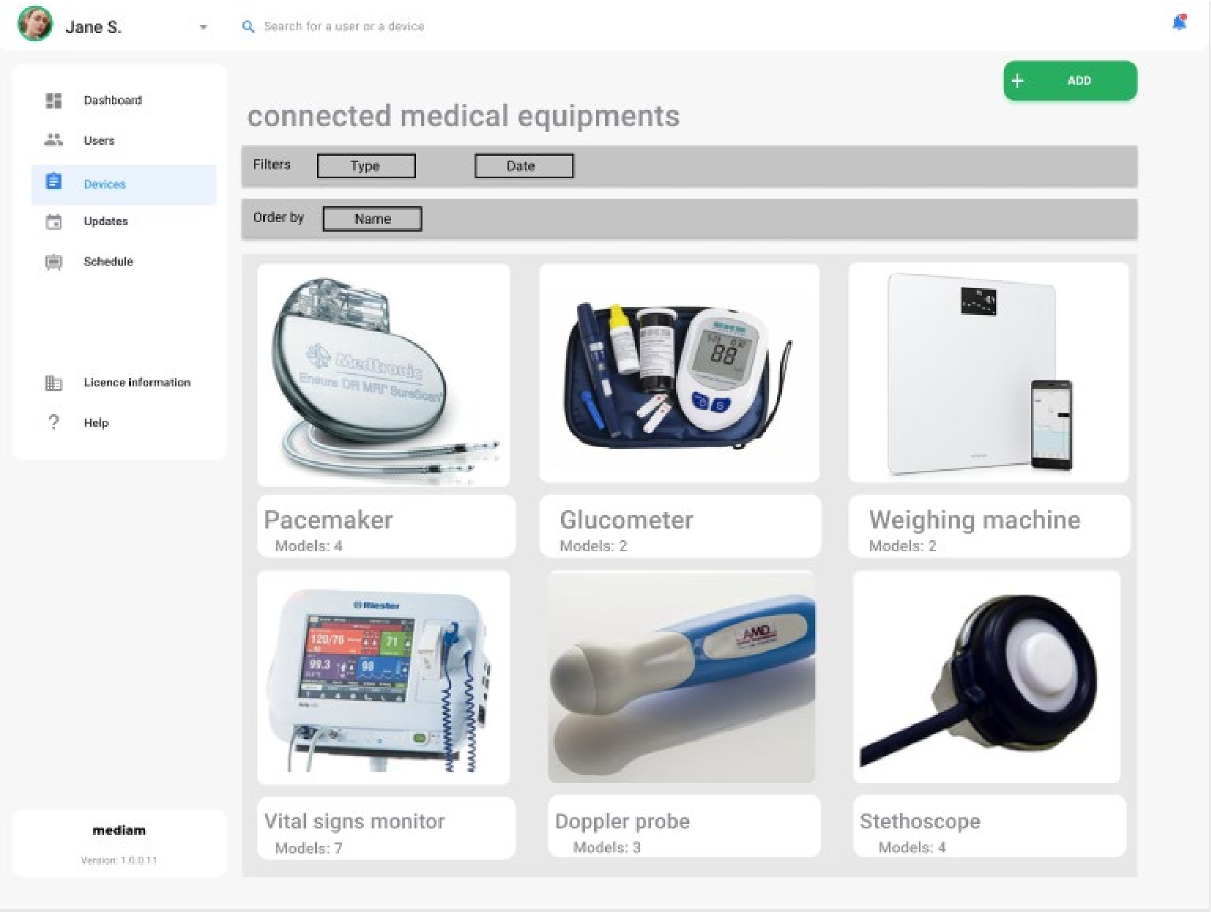

Figure 1. MedIAM prototypes

This had a profound impact on our technological choices. In particular, when implementing the security protocols, this helped us focus on a human-centric approach.

Apart from those field discoveries, the project followed its course as planned. We implemented minimum viable product experiments, got accepted two peer reviewed research articles, published some dissemination blog articles, updated an upcoming IETF standard and will be publishing a patent. We now plan to support those developments and broaden their scope into a new start-up that will focus on digital identity for privacy sensitive environments.

Testimonial

NGI Trust helped us a lot in our journey, as it offered great mentorship and advice from recognized experts, both on the technical and business perspectives. We also really appreciated the focus on how to build a business that builds upon an open source strategy.

Our project started in a less developed area, with the main objective of protecting children and young people using the Internet.