Talking Cybersecurity with Health IoT Developers

Charles Weir
Anna Dyson
Dan Prince
Security Lancaster

Introduction

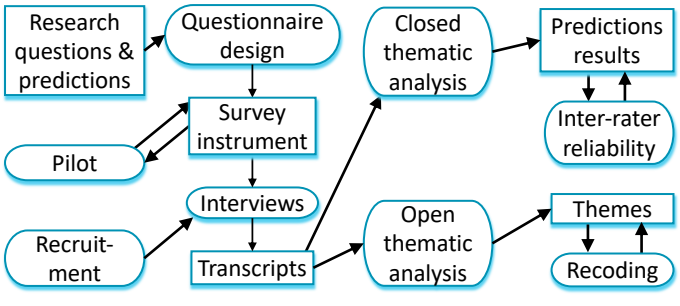
Health Internet of Things (HIoT) innovation offers vast potential benefits, providing both health monitoring and intelligent treatments. But there are huge potential cybersecurity, and privacy dangers with the resulting devices and systems. The teams producing HIoT innovations tend to be in small companies and often lack access to professional security expertise. To support such teams, our HIPSTER project aims to help them with cybersecurity risk assessment.

Yet for development teams, security and privacy are just two aspects amongst many for the products they develop, and developers have correspondingly limited time available to devote to learning about them. So, any guidance or advice must use developers' language and mesh with their existing procedures and operations, otherwise such advice risks being ignored or misunderstood.

Aim

To support such development teams, our project is developing a support package that draws on HIoT industry-specific knowledge. But to create usable developer security guidance and support, we want first to know the language developers use to discuss cybersecurity, and to understand how their cybersecurity decisions are made.

Method



Supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, under UK EPSRC grant EP/S035362/1

Results

The survey of 20 senior professionals found that very few developers used many of the cybersecurity terms used by specialists. Participants understood the concept of software security, and many conducted risk assessments around security concepts, though 'privacy' was not always a term they used. 17 of the 20 participants used stories—representing cybersecurity knowledge with ad hominem examples—to discuss issues. All identified ways in which cybersecurity issues were important to their customers, and industry standards were a major driver for many. Their decision-making, however, was complex, with many factors affecting the process.

For example, the word cloud below shows that developers' words for vulnerabilities (brown) are different from cybersecurity experts' (black):

Conclusions

We conclude that any support package for use by HIoT developers should:

- Assume that developers understand the concepts of cybersecurity and privacy;
- Expect them probably to know risk-based threat assessment; Expect a need for security or privacy from their customers—often for compliance with existing safety and privacy standards;
- Avoid terms such as 'threat', 'risk', 'threat actor' and 'victim';
- Use stories to express cybersecurity issues effectively; and
- Work with teams' existing decision-making processes.

Project Partners

chiptech · WEATHER FLARE · FUJITSU · rinicom secure communications · PETRAS · UK Research and Innovation · Lancaster University