Dr Cecilia Loureiro-Koechlin
Lancaster University,

with Jose-Rodriguo Cordoba-Pachon
Lynne Coventry, Soteris Demetriou, Charles Weir

Project Aim

In the fast-moving field of 'Biological Internet of Things' (Bio-IOT), it becomes challenging to identify information security and privacy problems a new product might encounter.

The FiVu project explores Design Fiction and Science Fiction as potential tools to help software developers improve their security practices in Bio-IOT.

Design Fiction

Sterling (2012) defines Design Fiction as "the deliberate use of diegetic prototypes to suspend disbelief about change". The term 'diegetic' means that the characters in a story relate to the 'prototypes' to persuade readers of their feasibility (Lindley, 2015) or to explore implications of their use. In the words of Blythe (2014) "Design Fictions present 'fantasy prototypes' in plausible near futures".

Thus, Design Fiction permits "thinking through details and ramifications of a technology without actually figuring out [its] implementation" (Baumer et al., 2018), and therefore it is a valuable tool to study the 'potential future adoptions' of emerging technologies (Lindley et al., 2017).

Science Fiction

Design Fiction is "a conflation of design, science fact, and science fiction" practices (Bleecker, 2009).

Dourish and Bell (2013) believe that Science Fiction "does not merely anticipate but actively shapes technological futures through its effect on the collective imagination...[providing designers with] prototypes for future technological environments" (2013).

Approach

Analysing fictional stories can help designers identify the cultural, social and political contexts present. We believed it could therefore help software designers identify security and privacy problems that might not be easy to identify any other way (Merrill 2020).

In the FiVu project, therefore, we created Design Fictions by combining both Science Fiction and Expert Security knowledge in a new and innovative way, as follows.

Stage One: Create design fiction narratives

a) We created a Use Case about a Bio-IOT fictional App called *GeneVault*.
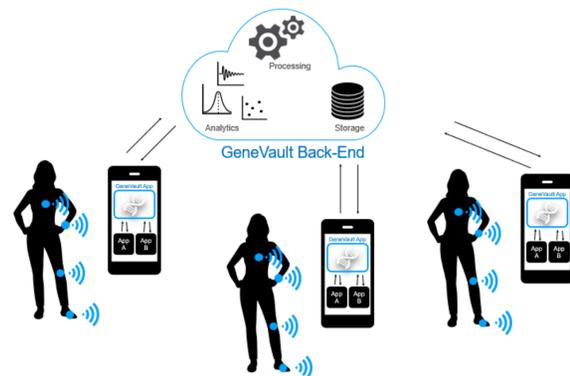
b) We presented *GeneVault* to several Security Experts and ask them to identify security threats.

c) We then presented *GeneVault* and those identified threats to several SciFi enthusiasts and asked them to suggest science fiction pieces that come to mind

d) We selected 3 of the suggested pieces, and created a one-page fictional narrative from each. Two of the narratives involved *GeneVault* explicitly and one of them suggested it by the data it gathered and stored.

Stage Two: Trial fictional narratives in a workshop

To test whether Design Fiction narratives created in this way could facilitate developers' thinking of security issues, we organized an online workshop with 7 Masters and PhD students, all with experience in software development.

Generic Threats for BIO-IoT.
Feedback on the Usefulness of Fiction
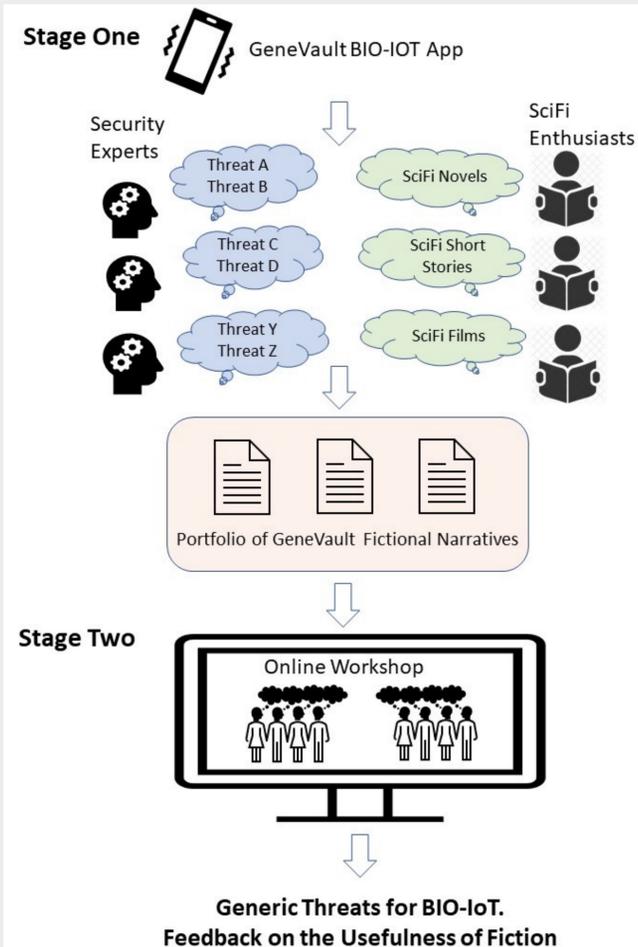
The workshop participants received the *GeneVault* Use Case by email one day before the event.

During the workshop they completed four 20-minute sessions, devising, in each, possible security problems for an App like *GeneVault*:

- First, a session based only on the *GeneVault* use case,

- Then three sessions, each after reading one of the fictional narratives.

They used a shared online whiteboard as a focus for discussion and to capture the results.

Finally, the participants completed a short online questionnaire about the workshop and the use of fictions for software development and discussed their answers.

Results and Conclusions

The innovative method was successful in producing fictional narratives for the *GeneVault* prototype. It proved easier to generate short fiction pieces based on existing Science Fiction than to generate such pieces from scratch.

However, we found that the four-step method may be too laborious for practical use. Step (b), the Security Experts, contributed least to the process and we might experiment with omitting it.

Feedback from the workshop participants was positive. They felt that this kind of workshop would be a good workshop for a real project; that the fictional narratives inspired new ideas; and that it was fun!

The narratives did inspire the participants to generate many new and different security issues for *GeneVault*. These were broadly in two categories: Technological Threats and Socio-political issues or Safeguarding.

Many of the threat ideas inspired by the design fiction, however, were in the second category, and of questionable value in the practical design of a new product. Yet, they did include examples of a wide range of threat types. We conclude that with suitable facilitation, a second 'focusing' step for the workshop would be effective in identifying practical threats for software designers to mitigate.

The fictional narratives are publicly available for further research or commercial use at: https://bit.ly/ThreatFictionBank

References

Baumer, E., Blythe, M., & Tanenbaum, T. (2020). Evaluating Design Fiction. Proceedings of the 2020 ACM Designing Interactive Systems Conference, 1901-1913.

Bleecker, J. (2009) Design Fiction: A Short Essay on Design, Science, Fact and Fiction. Near Future Laboratory, Venice Beach, CA.

Blythe, M. (2014). Research through design fiction: narrative in real and imaginary abstracts.. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 703-712.

Dourish, P., & Bell, G. (2013). "Resistance is futile": Reading science fiction alongside ubiquitous computing. Personal and Ubiquitous Computing, 18(4), 769-778.

Lindley, J 2015, A pragmatics framework for design fiction. in Proceedings of the 11th European Academy of Design Conference.

Sterling, B. (2012) Sci-Fi Writer Bruce Sterling Explains the Intriguing New Concept of Design Fiction. Slate. https://slate.com/technology/2012/03/bruce-sterling-on-design-fictions.html

Merrill N (2020) Security Fictions: Bridging Speculative Design and Computer Security. In: DIS 2020 - Proceedings of the 2020 ACM Designing Interactive Systems Conference. ACM, Eindhoven, pp 1727–1733