Vision: Design Fiction for Cybersecurity

Using Science Fiction to Help Software Developers Anticipate Problems

Cecilia Loureiro-Koechlin
Lancaster University, UK
cecilia.loureiro@gmail.com

José-Rodrigo Córdoba-Pachón
Royal Holloway, University of London, UK
j.r.cordoba-pachon@rhul.ac.uk

Lynne Coventry
Northumbria University, UK
lynne.coventry@northumbria.ac.uk

Soteris Demetriou
Imperial College London, UK
s.demetriou@imperial.ac.uk.

Charles A. F. A. Weir
Lancaster University, UK
c.weir1@lancaster.ac.uk

ABSTRACT

Security and privacy issues are an ever-increasing problem for software systems. To address them, software developers must anticipate the problems that their developed systems may face, using a process we call 'threat assessment'. Unfortunately, given the shortage of security experts, and the need to 'think laterally', threat assessment is very difficult for many development teams. One possibility is to use stories, known as 'Design Fiction,' to help developers visualize different contexts and future use for their software. But such stories are themselves difficult to write. A recent pilot project investigated using a broad-brush threat model and fiction samples derived from existing science fiction literature to help developers create threat assessments for Health Internet-of-Things devices. The preliminary results are encouraging, and open the possibility of developing a method to support developers in threat assessment in any domain.

CCS CONCEPTS

• **Security and privacy**; • **Human and societal aspects of security and privacy**; • **Software and its engineering**; • **Human-centered computing**; • **Empirical studies in collaborative and social computing**;

KEYWORDS

Health, Internet of Things, Software Security, Cybersecurity, Privacy, Design Fiction, Design Research, Science Fiction, Threats

ACM Reference Format:
Cecilia Loureiro-Koechlin, José-Rodrigo Córdoba-Pachón, Lynne Coventry, Soteris Demetriou, and Charles A. F. A. Weir. 2022. Vision: Design Fiction for Cybersecurity: Using Science Fiction to Help Software Developers Anticipate Problems. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29, 30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3549015.3554295

EuroUSEC 2022, September 29, 30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09…$15.00
https://doi.org/10.1145/3549015.3554295

1 INTRODUCTION

All too frequently, emerging and existing products can suffer from cybersecurity and privacy problems that were not identified or predicted during design. This can be costly in both monetary and reputational terms for businesses, such as if devices must be recalled or data breaches reported. It can also lead to consequences for the user ranging from data leakage and device misuse to human harms such as stalking, or to even human death such as from problems with medical equipment.

Moreover, current approaches to identifying security threats tend to rely on technical, adversary-based, knowledge, which makes it difficult for non-security experts to be involved [1, 22]. Even security experts may miss some threats, particularly those that arise from the social context in which technologies operate, or from human behaviour with technology. Relying solely on security specialists is itself problematic: there is a well-documented skills shortage, and many companies may not have sufficient staff in this space [33].

So, how are development teams to identify possible security and privacy threats without the support of security experts? We speculated that if we took inspiration from science fiction authors considering the impact of cybersecurity and privacy-related problems in the same general domain as the developers, those ideas might help those developers to ideate similar problems related to their own developing software. Specifically, the ideas might encourage 'lateral thinking:' generating different perspectives about a problem (stimulus) which complement rather than compete against each other [6]. This paper discusses our pilot study, FiVu, to use creative fiction—science fiction and speculative fiction—to help developers and product owners to identify and address relevant threats and vulnerabilities. In this study, we chose a particular application within the Health Internet of Things (HIoT) domain as a case study. We surveyed security experts and fans of science fiction for software threats, and relevant fictional texts; we then built them into 'fictional narratives' for a workshop and trialled these with a team of PhD and master's students with experience of software development. This paper shares the process followed, the fictional narratives generated and some preliminary insights into the role of this technique for identifying different types of threats.

The remainder of this paper is as follows: Section 2 explores the background related work around Design Fiction and its application to cybersecurity and privacy issues; Section 3 describes the methodology used in the pilot study; Sections 4 and 5 explore the insights

and outcomes from the writing of design fictions and the workshop; Section 6 provides preliminary conclusions and Section 7 presents a vision of how this work might be expanded in the future.

2 BACKGROUND

The term Design Fiction was first coined by Sterling [25] in his book *Shaping Things*, which explores how future, programable technology could interplay with society. Bleecker developed this concept in a short essay discussing technology design. In it, science fiction could bypass the constraints of fact science and "stretch the imagination" [4]. Bleecker's paper combined Sterling's concept with a variety of ideas which positioned Design Fiction as a research approach [19].

Currently, Design Fiction is situated within the field of Design Research [16, 31]. Design Research started as the study of design by adopting positivistic scientific values [32], but now includes speculative approaches such as Speculative Enactments [13]. Design Fiction's approaches aim to "focus on the world as it could be" [16], thus involving a degree of speculation that is based on fiction.

Specifically, Sterling [7] defines Design Fiction as "the deliberate use of diegetic prototypes to suspend disbelief about change". The term 'diegetic' means 'within the context of a story,' and implies the embedding of prototypes in 'story worlds' [18]. In words of Blythe [5], Design Fictions "present 'fantasy prototypes' in plausible near futures". Bleecker [4] sees Design Fiction as a "a conflation of design, science fact, and science fiction" practices. The outcomes of the design process "tell stories" [4] in the imagined contexts in which they are created. In doing so, they become places where discussions happen helping audiences to reflect and speculate. Moreover, Bleecker [4] believes that science fact and science fiction share the same goal and that they are "two ways of materialising ideas and imagination."

The 'suspending disbelief' element distinguishes Design Fiction from the related and widely used software analysis technique of Scenarios [2]: Scenarios are rooted in immediate practical reality; Design Fiction's 'story worlds' allow a wider range of possibilities.

Dourish and Bell [12] suggest a more specific relationship between science fact and science fiction as part of an enlightening analysis of the historical, cultural, social and political contexts in which ubiquitous computing is developed. The authors believe that socio-cultural forces "are already thoroughly implicated in how a technology is imagined and designed" [12]. Science Fiction might be playing a role already in design as it "does not merely anticipate but actively shapes technological futures through its effect on the collective imagination . . . [providing designers with] prototypes for future technological environments" [12]. Dourish and Bell agree that analyzing stories set in fictions can help designers identify the cultural, social and political contexts present which might otherwise be ignored and omitted by researchers [12].

A practical definition of Design Fiction is provided by Lindley and Coulton [10] "Design Fiction is: (1) something that creates a story world, (2) has something being prototyped within that story world, and (3) does so in order to create a discursive space." Design Fictions could take many forms, from Imaginary Academic Abstracts [5] and "short fiction pieces" [3] to drawings and mood boards [16]. Because of its qualities Design Fiction can facilitate the "thinking through specific details and ramifications of a technology without actually figuring out [its] implementation" [3] and therefore it is a valuable tool to study "the potential future adoptions" of emerging technologies subject to research [20].

2.1 Health IoT, Cybersecurity and Design Fiction

Due to its high potential of device connectivity, the Internet of Things or IoT facilitates access to devices' information and services, allowing coordination of devices, upgrading over the air, and 'smart' features. However, this same benefit of connectivity can turn into a risk as information can be compromised, by for example "inappropriate access, misuse and wrongful disclosure" [8]. Trust, Identity, Privacy and Security (TIPS) are critical issues for IoT applications particularly in the healthcare sector [14]. In order to sustain Health IoT adoption, it is imperative that TIPS considerations are taken into account. For example, Gordon et al. found that patients are more likely to adopt and utilize Personal Health Records "when care is taken to address privacy and security concerns." [15]

Design Fiction research has been applied to many technology-related issues. For example, Wong et al. [31] used Design Fiction to explore the privacy implications of emerging and near-future sensing technologies, using fictional technologies taken from a popular speculative fiction novel. Methodologically, Wong et al. started by creating visual representations of the fictional technologies, then identified potential privacy concerns in their designs, added further concerns, and finally analysed their findings against a privacy analysis framework.

Coulton et al. [10] discuss studies which use Design Fiction to explore challenges to the adoption of IoT devices particularly those related to "expectations and perceptions of personal privacy, security and trust". Their analysis of the studies suggests that design fiction is useful to "unpack what wider societal and technical challenges require consideration if future adoption is to be driven by acceptability".

Sturdee et al. [26] designed a fictional world in which human communication is dependent on algorithms which detect empathy in people. The authors used a fictional comic strip, because that format "encourages criticality" [11] and facilitates the discussion about how "practical and ethical implications of how such automatic emotion detecting technology might be used in practice" [26].

Wong et al. [29] use design fiction to explore the social implications for adoption of brain-computer interfaces, creating multiple, interconnected design fictions set in the same fictional world. Their conclusion is that the numerous "perspectives and interconnected relations in worlds that we imagine" help with the exploration of the sociotechnical issues of today as well as the ones of tomorrow.

Stead and Coulton [23, 24] use Design Fiction to create Health-Band, a fictional prototype to provide Do-It-Yourself healthcare. They used it to investigate issues of social equity, citizen empowerment, crowd funding, crowd sourcing of code, and implications for medical approvals processes and regulations. Design Fiction is found to be a useful tool to "address the implications for adoption of DIY medical devices" [24].

In the area of Design Fiction and cybersecurity, Merrill used a gamified workshop with software developers to develop 'security

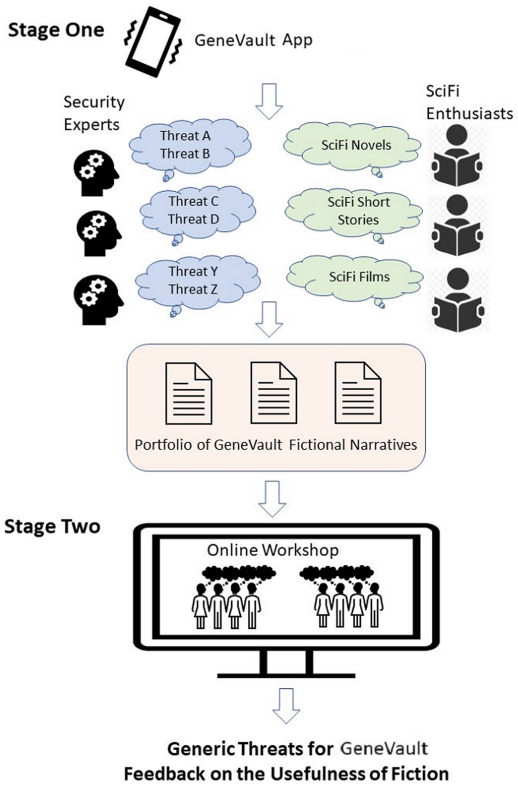

Figure 1: FiVu Methodology

fictions', scenarios representing cybersecurity threats [21]. There appears to have been little other Design Fiction work related to cybersecurity, an omission this paper seeks to address.

3 PILOT STUDY METHODOLOGY

The FiVu study contributes a methodological approach to create 'fictional narratives', based on existing science fiction work. Such science fiction has the potential to influence collective imagination and shape the future of technology designs [12]. Using science fiction in domains like human computer interaction often helps non-professional writers to design creative and believable 'life-worlds' [28], setting out the social and political contexts in which a technology prototype can be placed and discussed. With FiVu, we aimed to assess how fictional narratives could be used to nurture the imagination of software developers to predict future privacy and security implications.

The research was carried out in two stages, as shown in Figure 1. Stage One created three fictional narratives, which were then used as part of a creative enquiry to discover other threats and vulnerabilities in Stage Two. Following the 'Research through Design' tradition [9], FiVu's Stage One aimed to produce knowledge from the design process [19]. Specifically, we used the creation of the fictional narratives as a method of enquiry in itself [31]. Stage Two then tested those fictional narratives to see if and how they "elicited value reflections" [30] and heightened participants recognition of TIPS software development issues.

Specifically, in Stage One, three HIoT-related fictional narratives were designed following a 4-step process:

- **FiVu use case:** to kick-off the project, one of the project team members wrote a short use case for a fictional "Health IoT product from hell" called '*GeneVault*'. The use case included a diagram of the main components of the envisioned system. The intention was that the *GeneVault* prototype would generate knowledge not a product [5].
- **Threats:** Four Security Experts were contacted via email and sent the use case. They were asked to suggest a list of TIPS threats that an application like *GeneVault* might face.
- **Science fiction**: Three Science Fiction enthusiasts known by researchers were contacted by email, and sent the use case and the list of threats collected from the previous expert interviews. They were asked to identify examples in books and films which reminded them of *GeneVault* or any of the listed threats.
- **Fictional narratives**: With the information collected, the project team produced three one-page fictional narratives or stories for the *GeneVault* prototype using combinations of the collected threats and fictions. One illustration per story, drawn by a professional artist, was included too.

The fictional *GeneVault* itself was an extension of existing smartphone health tracking apps: it provides genome analysis and manages it that via the cloud; it can also integrate with third party services, track other user health information, and potentially control medical devices. Creating the FiVu fictional narratives effectively placed *GeneVault* in multiple lifeworlds [28]. This 'design tactic' [28] de-centred *GeneVault* as the main unit of analysis, and instead looked into the prototype-lifeworld combinations to encourage new questions and reflections on potential TIPS issues and ways to address them.

In FiVu's Stage Two, we organised a workshop with doctoral and masters' students, all with previous experience on software development. Participants were sent the *GeneVault* use case in advance. During the workshop they completed four 20-minute sessions:

- Session 1: Discuss and capture possible threats for an app such as *GeneVault*.
- Session 2-4: Read and discuss one of the fictional narratives and capture further threats.

The participants then completed a short online questionnaire about the workshop and the use of fictions for software development.

This research was approved by the Lancaster University Faculty of Science and Technology Ethics Committee.

4 INSIGHTS INTO WRITING THE *GENEVAULT* STORIES.

During the first stage of our project, information security experts were asked to provide a list of possible threats based on the *GeneVault* use case. Some experts explained both threats and their reasons for including them; others only reported a list of threats.

Next, the science fiction enthusiasts were given the use case along with a list of threats compiled from all the security experts.

The enthusiasts were asked to generate a list of science fiction short stories, novels, TV series and Films. For each item in their list, they were asked to explain how the science fiction situations were related to the use case. We received back some 20 suggested items, including short stories, film episodes and books. Not all suggested items involved the use of a specific piece of technology like *GeneVault*; some of them took place in worlds in which genetic enhancement was at the core.

The lead author then spent several days reading and reviewing these science fiction items and selected three to inspire the writing of fictional narratives for *GeneVault*. In writing, emphasis was placed on highlighting the reasons readers or enthusiasts gave to select the works. Care was taken to avoid any overt description of the threats suggested by security experts. The resulting 'fictions' were:

- Eat, Drink and Be Merry (inspired by Eat, Drink and Be Merry by Dian Girard),
- Ranjan's story (inspired by Black Mirror, Nosedive episode. S03E01), and
- Memorandum (inspired by Emergency Skin by N.K. Jemisin).

The lead author also sent the fictional narratives and illustration ideas to a professional artist, who created a cartoon for each[1].

5 PRELIMINARY RESULTS

There were three types of outputs from the workshop. First, four lists of threats and vulnerabilities were captured via an online collaborative whiteboard with four (4) slides: first, where the participants discussed the case study on its own, then after studying and discussing each of the three (3) fictional narratives in turn. Though participants discussed the same fictional product each time, all four lists are different. The second output was the workshop transcript (created by Microsoft Teams) with the discussions between participants ideating threats and debating their applicability. The fictional narratives encouraged much more discussion focusing on different aspects of *GeneVault* and the settings. The third output was the final online questionnaire completed by the participants.

One aspect in common for the use case and stories is that participants presupposed dystopian settings, perhaps because we asked them to focus on threats. Figure 2 shows one snapshot of the workshop output, with the list of threats for GeneVault where it is used to control home, work and public devices. In this particular output, the fictional narrative inspiring it was based on a short science fiction story titled *Eat, Drink and Be Merry* by Dian Girard, and the corresponding image in the top right corner shows a *GeneVault* user with a health condition failing to purchase alcohol.

With the support of the fictional narratives, participants identified examples of a wide range of security issues for *GeneVault*. These were broadly in two categories: **Technological threats, and Socio-political/safeguarding issues**. While the workshop participants did not identify all the problems identified by the security experts (code security vulnerabilities, and insider threats, for example, were not discussed), they did identify problems not mentioned by the experts, such as potential forms of bias, including agism.

[1]The GeneVault description and illustrated Fictions can be found online – see section 6.

Indeed, many of the threat ideas inspired by the Design Fiction were in the 'socio-political/safeguarding' category. It would need further discussion and possibly investigation to translate these socio-political/safeguarding threats into problems that could be enacted via the prototype and that might need addressing by development teams.

Evaluation feedback from workshop participants was collected using an online questionnaire system and was positive. As Figure 3 shows, participants felt that the fictions inspired new ideas, and to a slightly lesser extent, that this kind of workshop would be suitable for a real project. Suggestions from participants included:

- Distributing 'fictions' in advance,
- Defining the participants' roles clearly up-front, and
- Prompting the participants to give thoughts under different structured stages.

6 PRELIMINARY CONCLUSIONS

Our approach to use science fiction in a design fiction practical workshop was successful in producing fictional narratives for the *GeneVault* prototype. The process of using fictional narratives to explore cybersecurity issues with novel technologies was innovative, and it helped to consider relevant security issues for *GeneVault*. The fictional narratives created by the project are publicly available for further research and commercial use at *https://securityessentials.github.io/ThreatFictionBank/* .

To address the need identified above for *further discussion and possibly investigation to translate these socio-political/safeguarding threats into problems*, we concluded that with suitable facilitation, a second 'focusing' step for the workshop could converge the results back to a prioritised list of practical threats for software designers to mitigate. We observe that such an approach already exists, in the form of 'risk assessment', a very mature process widely used in industry [17], and that a simple workshop version is already publicly available [27].

We also observed that the approach we followed to generate the fictional narratives proved too laborious to replicate in commercial settings, and so we should look for ways to simplify it. Of the steps we used (Section 3), the security experts contributed least to the process; the science fiction enthusiasts tended to base their recommendations on the *GeneVault* description rather than on the security experts' threats. So, it might be possible to omit the security expert consultation.

7 VISION AND FUTURE WORK

Our vision is to generate a science-fiction-based threat assessment approach that can be used effectively in real-world commercial settings. From the workshop results, we can see that two aspects need addressing most:

- We need a structured way to help software developer participants 'focus in' on the threats that they will most need to address. We observe that such an approach already exists, in the form of 'risk assessment', a very mature process widely used in industry [17], and with a simple workshop version already publicly available [27].
- To support the use of the approach in other domains, we need a means for professional participants to generate 'fictions'

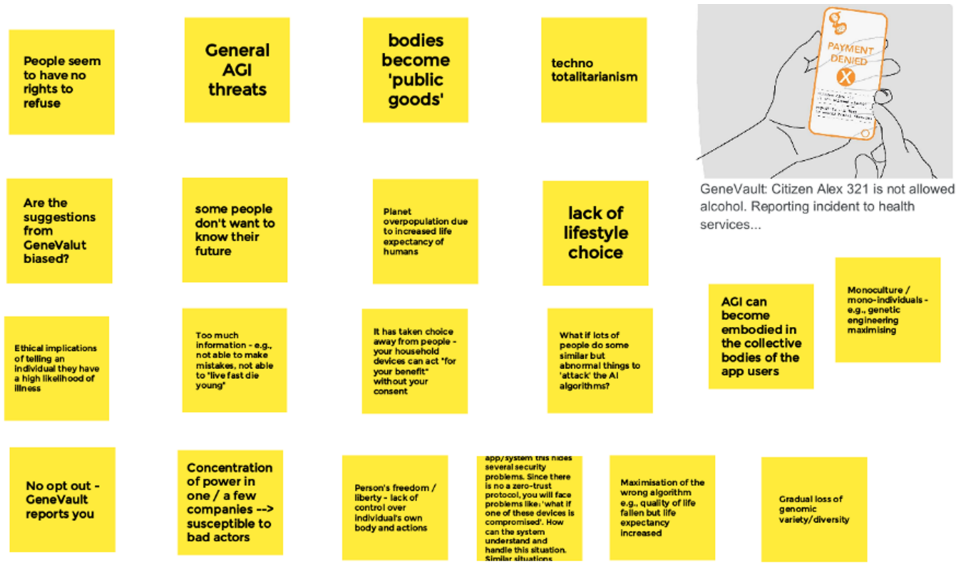

Figure 2: Threats for GeneVault in a world in which it can control devices

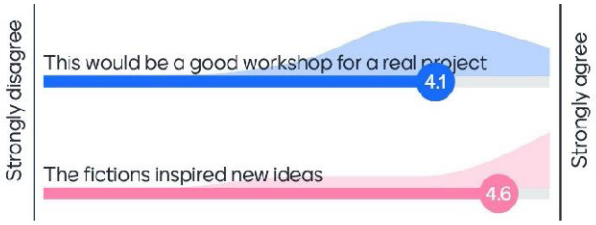

Figure 3: Participants' reactions

for themselves. The enthusiasm we found from our science fiction experts suggests that 'crowd sourcing', through social media channels is a realistic proposition. However, this requires trialling.

7.1 Next Steps

We therefore propose two further project steps to take the concept forward:

- Incorporating a risk assessment step to the workshops and trialling it with one or more commercial software teams.
- Detailing the 'fictional narrative creation' process as an instruction document, and trialling that—in a different domain—as a task for someone other than the researchers.

We anticipate trialling the first step in a sister project shortly; and plan a follow-up project to do the second.

We suggest that this approach, of using science-fiction-inspired Design Fiction to help software development teams identify security threats, has decided potential in the long term to help improve the software systems on which we all rely.

ACKNOWLEDGMENTS

Our thanks to the experts, both cybersecurity and science fiction, who supported us and helped deliver the Fictions.

This research was funded by SPRITE+ from the "Future Digital Vulnerabilities Sandpit 2", under EPSRC grant EP/S035869/1.

REFERENCES

[1] Ackoff, R.L. Creating the Corporate Future. In *Understanding Business Environments*. 2000, 217–227.
[2] Alexander, I. and Maiden, N. *Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle*. Wiley, 2005.
[3] Baumer, E.P.S., Berrill, T., Botwinick, S.C., *et al.* What Would You Do? Design Fiction and Ethics. *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work*, Association for Computing Machinery (2018), 244–256.
[4] Bleeker, J. Design Fiction: A Short Essay on Design, Science, Fact and Fiction - Near Future Laboratory. 2009. https://blog.nearfuturelaboratory.com/2009/03/17/design-fiction-a-short-essay-on-design-science-fact-and-fiction/.
[5] Blythe, M. Research Through Design Fiction: Narrative in Real and Imaginary Abstracts. *Proceedings of the SIGCHI Conference on Human Computer Interaction*, Association for Computing Machinery (2014), 703–712.
[6] de Bono, E. *Lateral Thinking: Creativity Step by Step*. Harper Perennial, New York, 1990.
[7] Bosch, T. Sci-Fi Writer Bruce Sterling Explains the Intriguing New Concept of Design Fiction. 2012. https://slate.com/technology/2012/03/bruce-sterling-on-design-fictions.html.
[8] Bussone, A., Stumpf, S., and Bird, J. Disclose-It-Yourself: Security and Privacy for People Living with HIV. *CHI EA '16: Proceedings of the 2016 ACM Human Factors in Computing Systems Extended Abstracts*, May (2016), 1–4.
[9] Christopher Frayling. *Research in Art and Design*. 1993.
[10] Coulton, P., Gradinar, A.I., and Lindley, J.G. Anticipating the Adoption of IoT in Everyday Life. In *Privacy by Design for the Internet of Things: Building accountability and security*. 2021, 229–252.
[11] Coulton, P., Lindley, J., Sturdee, M., and Stead, M. Design Fiction as World Building. *Proceedings of the Research Through Design Conference*, (2017), 1–16.
[12] Dourish, P. and Bell, G. "Resistance Is Futile": Reading Science Fiction Alongside Ubiquitous Computing. *Personal and Ubiquitous Computing 18*, 4 (2014), 769–778.
[13] Elsden, C., Chatting, D., Durrant, A.C., *et al.* On Speculative Enactments. *Conference on Human Factors in Computing Systems - Proceedings*, ACM (2017), 5386–5399.
[14] Frustaci, M., Pace, P., Aloi, G., and Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal 5*, 4 (2018), 2483–2495.

[15] Gordon, P., Camhi, E., Hesse, R., *et al.* Processes and Outcomes of Developing a Continuity of Care Document for Use as a Personal Health Record by People Living With HIV/AIDS in New York City. *International Journal of Medical Informatics 81*, 10 (2012).

[16] Grand, S. and Wiedmer, M. Design Fiction: A Method Toolbox for Design Research in a Complex World. *Design Research Society*, (2010).

[17] Hubbard, D.W. and Seiersen, R. *How to Measure Anything in Cybersecurity Risk*. Wiley, 2016.

[18] Lindley, J. A Pragmatics Framework for Design Fiction. *11th EAD Conference Proceedings: The Value of Design Research*, Sheffield Hallam University (2016).

[19] Lindley, J. and Coulton, P. Back to the Future: 10 Years of Design Fiction. *Proceedings of the 2015 British HCI Conference*, Association for Computing Machinery (2015), 210–211.

[20] Lindley, J., Coulton, P., and Sturdee, M. Implications for Adoption. *Conference on Human Factors in Computing Systems*, Association for Computing Machinery (2017), 265–277.

[21] Merrill, N. Security Fictions: Bridging Speculative Design and Computer Security. *DIS 2020 - Proceedings of the 2020 ACM Designing Interactive Systems Conference*, ACM (2020), 1727–1735.

[22] Midgely, G. Systemic Intervention: Philosophy, Methodology, and Practice. *Journal of Community and Applied Psychology*, (2000).

[23] Stead, M. and Coulton, P. HealthBand: Campaigning for an Open and Ethical Internet of Things Through an Applied Process of Design Fiction. *Cumulus REDO Conference*, (2017).

[24] Stead, M., Coulton, P., and Lindley, J. Do-It-Yourself Medical Devices: Exploring Their Potential Futures Through Design Fiction. *DRS2018: Catalyst*, Design Research Society (2018), 25–28.

[25] Sterling, Bruce. *Shaping Things*. MIT Press, 2005.

[26] Sturdee, M., Coulton, P., Lindley, J.G., Stead, M., Akmal, H.A., and Hudson-Smith, A. Design Fiction: How to Build a Voight-Kampff Machine. *Conference on Human Factors in Computing Systems*, Association for Computing Machinery (2016), 375–385.

[27] Weir, C., Becker, I., and Blair, L. A Passion for Security: Intervening to Help Software Developers. *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, IEEE (2021), 21–30.

[28] Wong, R.Y., Khovanskaya, V., Fox, S.E., Merrill, N., and Sengers, P. Infrastructural Speculations: Tactics for Designing and Interrogating Lifeworlds. *Conference on Human Factors in Computing Systems*, Association for Computing Machinery (2020).

[29] Wong, R.Y., Merrill, N., and Chuang, J. When BCIs Have APIs: Design Fictions of Everyday Brain-Computer Interface Adoption. *DIS 2018 - Proceedings of the 2018 Designing Interactive Systems Conference*, Association for Computing Machinery, Inc (2018), 1359–1372.

[30] Wong, R.Y., Mulligan, D.K., van Wyk, E., Pierce, J., and Chuang, J. Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks. *Proceedings of the ACM on Human-Computer Interaction 1*, CSCW (2017), 27.

[31] Wong, R.Y., van Wyk, E., and Pierce, J. Real-Fictional Entanglements: Using Science Fiction and Design Fiction to Interrogate Sensing Technologies. *DIS 2017 - Proceedings of the 2017 ACM Conference on Designing Interactive Systems*, Association for Computing Machinery, Inc (2017), 567–579.

[32] Yee, J.S.R. Implications for Research Training and Examination for Design PhDs. In *The SAGE Handbook of Digital Dissertations and Theses*. 2012, 461–489.

[33] Zatterin, G., Atkins, G., Bollen, A., Shah, J.N., and Donaldson, S. *Cyber Security Skills in the UK Labour Market 2022*.