Security Lancaster | Lancaster University

HIPSTER: Health IoT Privacy and Security Transferred to Engineering Requirements

State of the Art Technical Report – November 2021

Dr Charles Weir (Security Lancaster, Lancaster University)

Anna Dyson (Security Lancaster, Lancaster University)

Dr Dan Prince (Security Lancaster, Lancaster University)

Summary

Health IoT (HIoT) software offers thorny and complex security, privacy and safeguarding (SPS) problems and requirements, with huge potential impact. The HIPSTER project aims to help development teams in the Small-to-Medium Enterprise community, incorporating background information from cyber threat and risk intelligence to create a cost-effective intervention to support decision making around such threats and requirements.

This report outlines the approach we plan to use and explores the academic 'state of the art' literature around the project. It concludes that the areas of novelty for the project are in finding ways to make risk data meaningful and palatable for software development teams; and in finding objective sources of such security and privacy information for this domain.

To support readers in using the literature referenced, all citations and bibliography entries in this document have hyperlinks to the corresponding sources.

Contents

1 Introduction

The HIPSTER project, *Health Internet of Things Privacy and Security Transferred to Engineering Requirements*, researches how to use threat and risk intelligence to help improve decision-making about security, privacy and safeguarding (SPS) functionality and improvements in software, especially in Small-to-Medium enterprises (SME) with only limited access to security expertise.

While the research team have expertise in security risk assessment, vulnerability analysis, software development and working with SME software teams to improve security, several things in this project were deliberately selected as new fields of expertise for the team:

- Health-based software
- Internet of Things (IoT)
- Representing risk information for decision making
- Deriving practically useful SPS risk intelligence from public and other sources

To share knowledge between team members, avoid research duplication, and provide a basis for future papers and for the project going forward, we therefore start the project with a literature survey.

Our primary research question for the project was defined as follows:

> *How can cyber threat intelligence improve security, privacy and safeguarding outcomes in agile development approaches for Health IoT systems within resource constrained development teams?*

The research methodology we are using is Design Based Research, to create an intervention to use with development teams in Small to Medium Enterprises (SMEs). The question for this survey becomes, therefore:

> *RQ 1* *What is the important prior research related to aspects of 'using DBR to create an intervention that uses cyber threat intelligence to improve security, privacy and safeguarding outcomes in agile development approaches for Health IoT systems within resource constrained development teams'?*

The rest of this paper is as follows. Section 2 describes the survey method; Sections 3, 4 and 5 discuss the publications found; Section 6 discusses the implications of the results; and Section 7 provides a conclusion.

2 Survey Method

This section explores the method used in the survey. It addresses the problem of defining a survey scope, and outlines the practical method used.

2.1 Survey Scope

The immediate problem in doing a literature review is to define a scope specifying what publications might be included. We considered it unlikely (though not impossible) that any team has tackled this particular problem before, so a literature review for papers related to every aspect of the research question is likely to draw a blank. Since the project is cross-discipline, it is also difficult to define a suitable wider scope for the survey: even a topic such as 'Developer Centred Security' or 'SPS for Health IoT' in itself does not cover enough ground to provide a basis for the project.

As a first start, we brainstormed a selection of relevant topics related to the project. Figure 1 shows some of the resulting topics. We realised that a survey that covered each topic adequately would reach encyclopaedia-like proportions. Clearly, therefore, our interest is not the individual topics but the aspects of those topics that relate to the Hipster project.

We explored using searches to cover as many of those topics as possible, valuing papers that covered more topics over papers that covered fewer. The conventional approach of using a keyword query on a curated database would not work well for this; as an alternative, we used 'related literature' searches, starting with some appropriate papers (see Section 2.2). This provided a useful

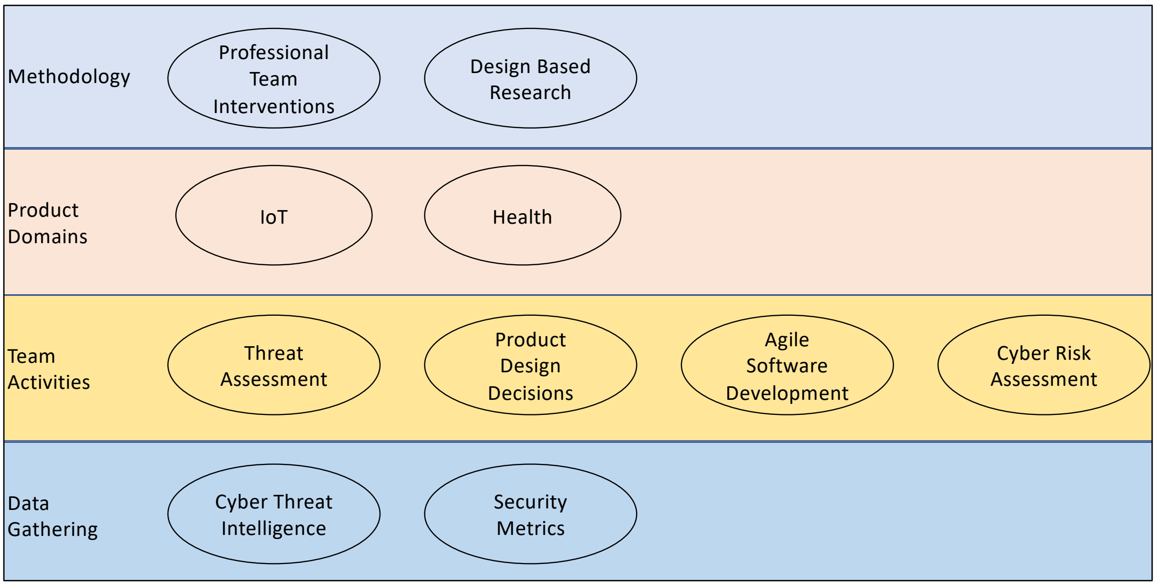

Figure 1: Relevant Topics

methodology for selecting related publications, but did not provide a particularly helpful approach to documenting them.

So, to provide a structure for this report, we have taken the approach we plan to use, and position the discussion of the selected publications around that approach. Section 2.3 provides that structure.

2.2 Finding Publications

A conventional approach to literature reviews is a keyword search of titles, paper keywords and abstracts, on a commercial database of publications, such as those provided by the ACM or Web of Science; and then to follow citations from the selected papers to add further candidates. We are aware of several problems, however, in this approach:

- Relevant papers are found in a wide range of different venues, from security and privacy venues through to software engineering management ones.
- Our trial keyword searches answered a huge number of papers; we could have limited the venues searched, but with the likelihood of omitting important publications.
- The lack of a common community means that paper authors have often been unaware of other work in the field, so following citation links doesn't necessarily find related publications.
- Titles, and even abstracts and paper keywords, are not always sufficient to identify papers as appropriate, so a keyword-based search is unlikely to deliver all the relevant papers
- Recent research [39] has shown that there are many errors and papers missing from well-known curated databases, and that even very respected survey papers have had errors in the search strings used.

An alternative approach was to start with a paper in the right area, and find others using a suggestion engine. We chose Google Scholar as providing probably the most comprehensive list of publications and being widely used for Systematic Literature Reviews [69];. We accessed it via a commercial Search Engine Results Pages (SERP) online API[1]; this generated a hundred suggestions of associated publications for each publication analysed. We used an iterative approach:

1. We started with a list of 2 appropriate publications [32,64] .

[1] https://serpapi.com

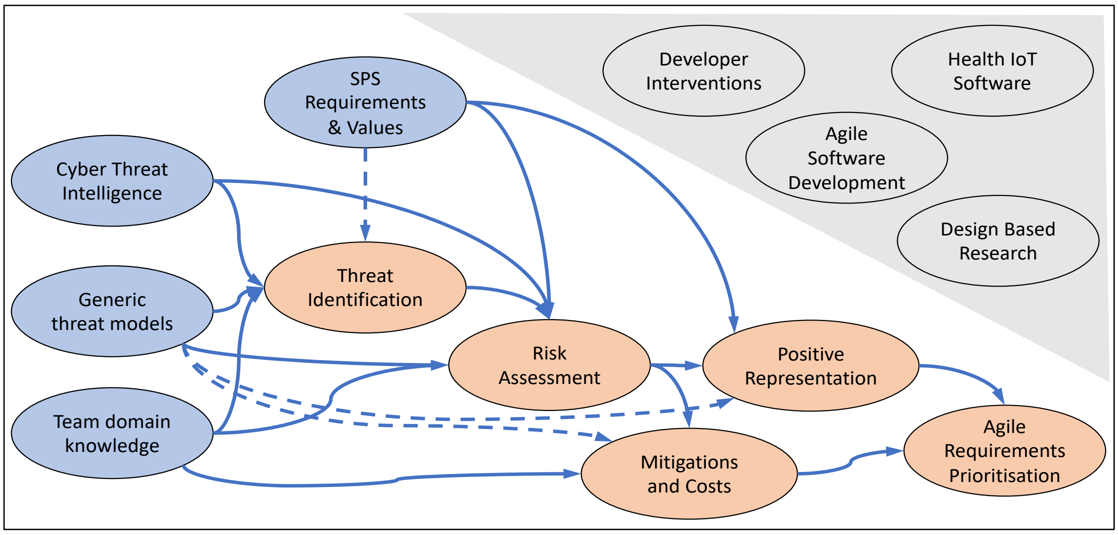

Figure 2: Hipster Process

2. We used the SERP API to obtain the publications suggested from each starting publication.
3. We filtered out duplicates and publications previously considered.
4. We manually dual coded each publication as relevant or not; accessing the publications is made easy by the Google links available from the API.
5. We then repeated steps 2 to 4 using the newly chosen publications as the starting list, iterating until no new papers were being added or sufficient papers had been found.

The search and analysis automation used Python packages, including NumPy and Pandas, in Jupyter Notebooks [36]. The software is publicly available on Github[2].

2.3 The Hipster Project

Figure 2 provides an outline of the activities in the Hipster project for an agile development team in an SME. Ovals show sources of information (blue) and activities (amber); those in the greyed out area represent context for the project. Arrows show how knowledge from each source or activity feeds to the next; dashed arrows show lesser knowledge feeds.

All of these activities except for Agile Requirements Prioritisation are in addition to the 'normal' activities we would expect an agile software development team to carry out, which are explored in Section 3.3

The new activities are as follows. Based on available cyber threat intelligence, appropriate threat models created for the product domain by the organisation or other people and the existing domain knowledge of the development team, the team identifies likely threats and requirements for security and privacy. For each, they then do a risk assessment, using the same sources but curated against the particular Security, Privacy and Safeguarding (SPS) requirements for the project and the values of the organisation, to assess how important each item might be to the team, to other stakeholders and to the organisation.

Next, the team choose the most important threats and establish possible mitigations and threats for each, estimating costs for the work and changes involved.

In addition, earlier work has identified a further step needed before product owners can prioritise the tasks: to represent the risks in question as positive aspects: product owners are used to contrasting and prioritising between different opportunities; their skillset does not include or find

[2] https://github.com/charlesweir/Google-Literature-Review

easy comparing risks with opportunities. And experimentation suggest that developers and product managers tend to be capable at doing this 'Positive Representation' [66].

Finally, based on the mitigations, mitigation costs, and the positive representations of the consequences, the product owners can then handle the task of using corporate values and priorities to prioritise the possible mitigations against other development tasks.

Four further ovals provide the context for the Hipster project in researching this activity: the need for 'interventions' to change the behaviour of developers to do these activities; Design-based Research, an accepted research method focussed on developing both an artefact such as an intervention, and relevant academic theory; the agile development process used by many software development teams; and, of course, the topic area: Health IoT.

2.4 Document Structure

From Figure 2, we can derive two further research questions for this survey, as follows:

RQ 2 *What is the prior work in the research context for the Hipster project?*

RQ 3 *What is the research work related to the processes the developer teams will carry out in the HIPSTER project?*

The following three sections address the topics in Figure 2. Section 3 explores the research context topics, addressing RQ 2 . Section 4 explores the information sources and Section 5 the activities, between them addressing RQ 3

3 Research Context

This section provides introductions to the three aspects of the research context, including one or more references to more extensive introductions. All three introductions are in the context of this project (e.g. risk management related to security, rather than every possible risk), rather than a complete introduction to the topic.

3.1 Design Based Research

Design-Based Research (DBR) has its roots, and is used most, in education research. Though it does not derive directly from Action Research [38], DBR shares the principle that the researcher may themself be part of the research project [4]. Initially used to support the design of 'Technology Enhanced Learning Environments', DBR is now an accepted research paradigm used to develop improvements ranging from tools to curricula [30], with online tutorials [63] and a recent comprehensive guide book for practitioners [3].

Design-Based Research is pragmatic (solving current real-world problems), grounded (in the practicalities of real-world trials), interactive (between researchers and practitioners), iterative (with repeated cycles developing both theory and the innovation), flexible (allowing process changes), and contextual (to the scope of the real-world trials) [65]. Figure 3, from [65], illustrates the parallel cycles developing theory and innovation.

DBR is also 'Integrative' in that it uses other research methodologies to provide the design and assessment techniques used in a practical project. Such research methodologies may be based on Action Research, Ethnography, and even Surveys, Case Studies and Controlled Experiments [16].

More general research methods for Cybersecurity are discussed in [17].

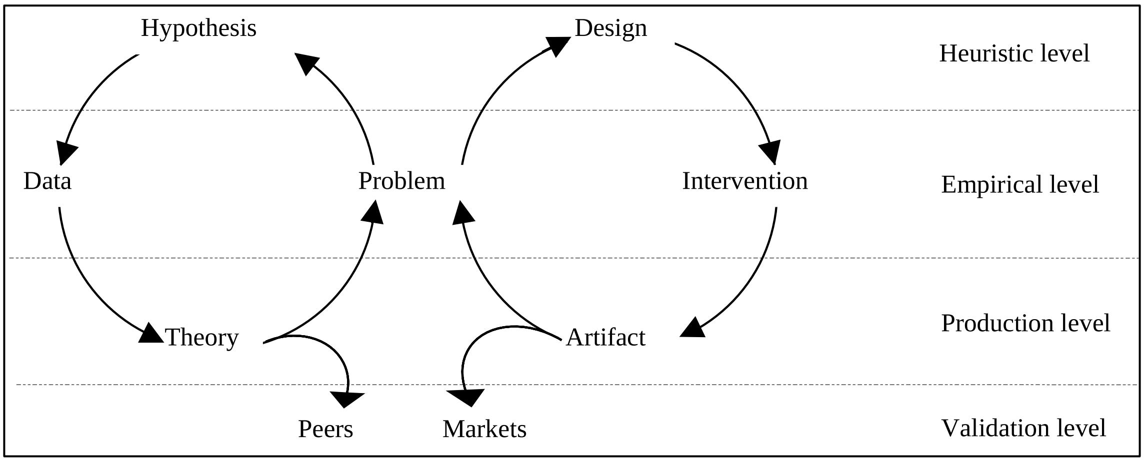

Figure 3: Design-Based Research Activities [65]

3.2 Health IoT Software

Health IoT software is software that powers, or provides assistance with managing and monitoring, IoT devices related to human health. Two recent surveys explore the topic [2], [26]. Although IoT devices include both sensors that collect data, and actuators that control physical devices [57], many typical Health IoT applications relate only to sensor devices. Typically these monitor aspects of individual health or safety, ranging from tracking running activity to heart function and wheelchair management [33]. However, actuators, such as implantable cardiac devices, are also starting to be deployed, with their potentially greater security problems [71].

Such devices generally connect via short-range radio communication (such as a 'body area network') via a gateway device (such as a mobile phone) to cloud or centrally based services; such services are accessed through the terminal devices of users such as the individual monitored and health or safeguarding professionals. A range of large suppliers offer infrastructure to support both communication and data analysis, and the medical aspects are heavily legislated, with notable differences between different jurisdictions [33].

Figure 5 illustrates typical Health IoT applications, ranging from smart watches, pacemakers and body-mounted devices connected via a mobile phone, through to safety alarms, smart wheelchairs and medical devices; with some controlled only via the user, and others managed by call centres and health professionals.

3.3 Agile Software Development

Agile Software Development combines a large variety of novel (since 2000) software development practices with a philosophy defined in its founding Agile Manifesto [6]. A good overview of Agile Software Development for non-specialists can be found in the book 'Agile Application Security' [7 ch. 3]. Agile is the development choice of most SMEs and startups [21], so is a primary focus for the Hipster project.

There are many different 'methodologies' associated with Agile Development, most notably Scrum, Lean and eXtreme Programming (XP) [5]. Figure 4 shows the main practices associated with different 'areas of concern' [1].

A given Agile development team will cherry-pick the practices from that list. In practice, many adopt combinations of Scrum and XP, which might typically involve two-weekly iterations [55] of:

1. Planning the tasks for this iteration.

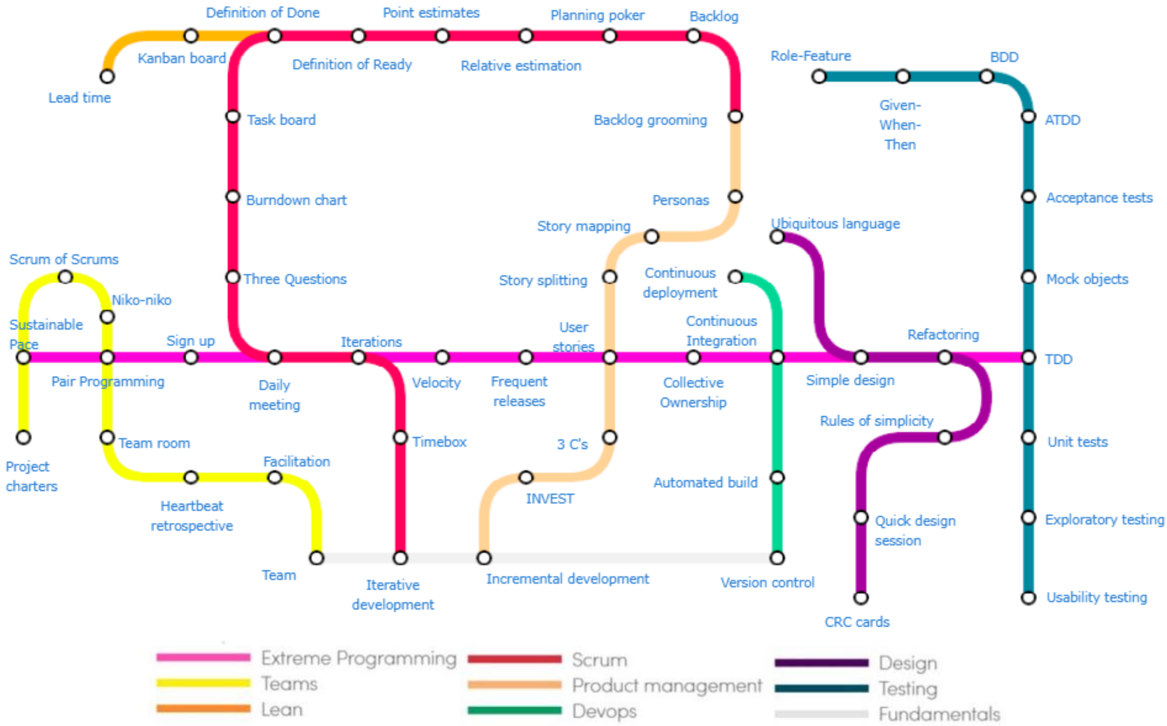

Figure 4: Agile Practice Subway Map [1]

2. Implementation for each chosen task, including creation of automated tests, implementation, test, release (see Figure 6 [3])
3. Retrospective

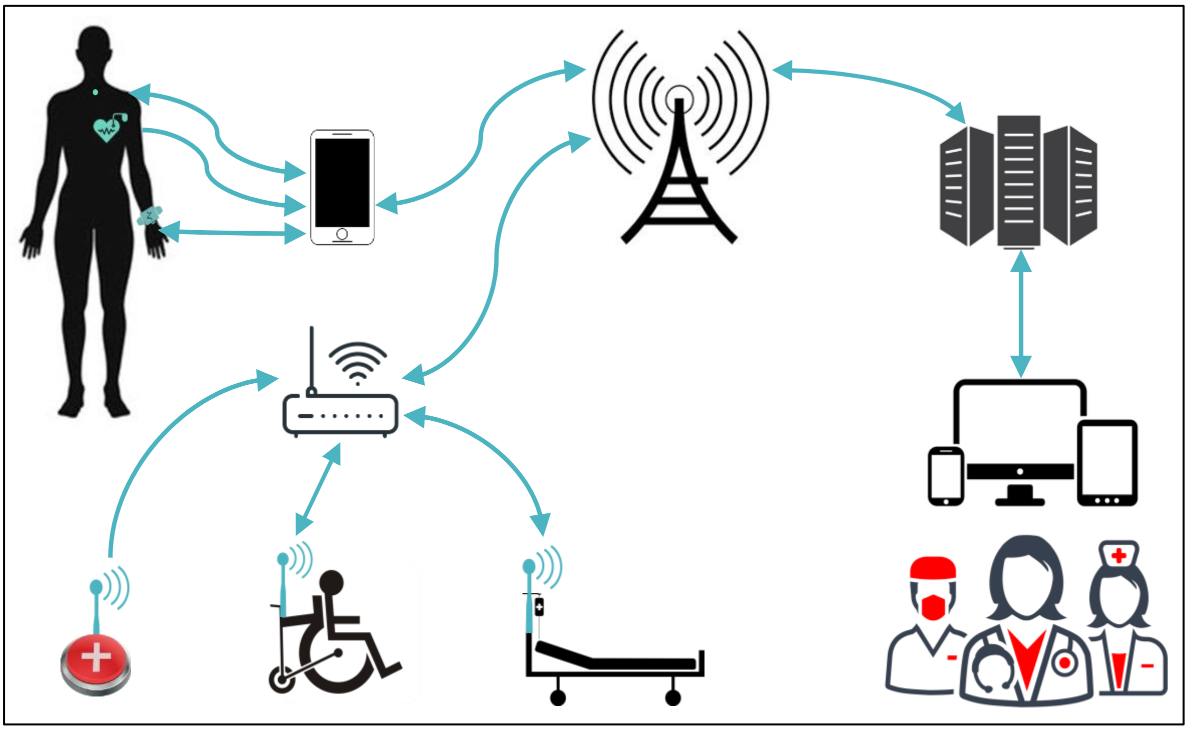

Figure 5: Example Health IoT Applications

[3] Cropped from an image by Planbox (CC BY-SA 3.0)

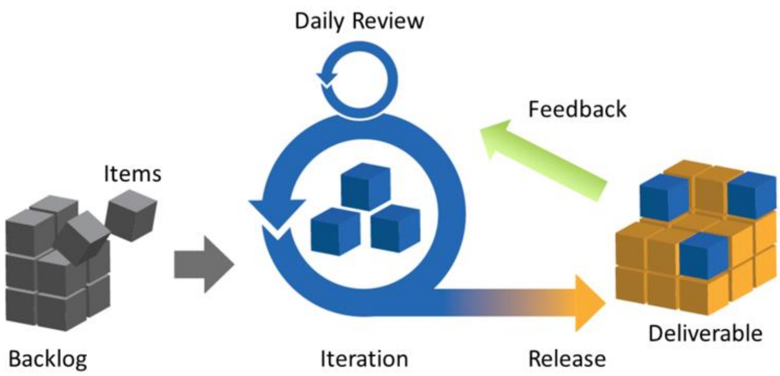

Figure 6: An Agile Development Cycle

Other commonly-used practices include user stories, daily stand-ups, use of a Kanban board, burndown charts, continuous integration and of course version control [1].

Agile is the development choice of most SMEs and startups [21], so Agile development teams are the primary focus for the Hipster project.

3.4 Development Team Interventions

'Intervention' is a term deriving from health literature [27] and means an activity carried out to positively influence a targeted group of people. Surprisingly, given academia's domination of the education space, there is a relatively small amount of literature on interventions to change the security behaviour of software developers.

In one case, a single penetration testing session and workshop failed to have much effect on a distributed development team [62]. *"Challenging and teaching [developers] about security issues of their product"* also proved unsatisfactory, due to the pressure to add functionality [44].

'Security Patterns' offered another approach, though the benefits proved inconclusive [70]. A recent book by Bell et al. [7] provides support for developers and tool recommendations, containing much valuable practitioner experience, but little objective assessment of the advice provided.

One more promising approach is to *"raise developers' security awareness,"* such as by using discussions about security [40]. Another is to use structured workshops to teach the importance of effective decision making, threat assessment and suitable presentation of the results [66]. Others have had success with workshops using less conventional approaches, such as design fiction [42].

4 Hipster Data Sources

This section explores RQ 3 , topics associated with the data and processes used by development teams involved in the Hipster processes.

4.1 Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is the gathering of information industry-wide about cyber-attacks and its timely dissemination [56]. It has many sources and a variety of applications [9]. Figure 7 [11] illustrates the collection and usage of CTI.

Because of the multi-party nature of this information gathering, CTI tends to be a commercial more than academic discipline, dominated by closed-source platforms and focussing on data gathering more than analysis [50]. [48] provides an introductory commercial overview, and [11] a recent literature survey.

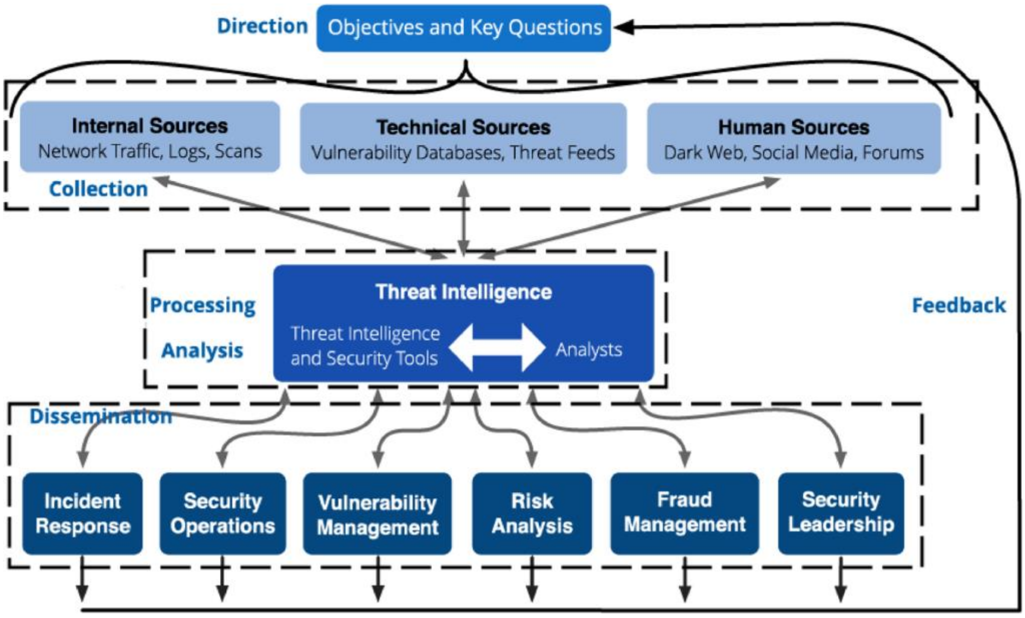

Figure 7: Threat Intelligence Lifecycle.

We should be aware, however, that threat intelligence can take many different forms. For example, threats to the internet backbone are shared on routing messages between operators [22]; discussions between professionals often convey cyber risks using 'war stories' [67]; organisations may have generic threat lists for their particular domain, or even distribute such lists in the form of automated tools, e.g. [54].

4.2 Risk Management

Cyber Risk Management in the software lifecycle is 'the process of identifying, analysing, evaluating and addressing an organisation's cyber security threats' [34]. The processes required to do this at a corporate level are now mature, and a variety of competing standards, such as ISO2001, PCI-DSS and (in the UK) Cyber Essentials each provide extensive prescriptions of checks and activities to carry out [34]. Figure 8 shows an example risk management strategy.

Academic work on the subject has included the quantification of cyber risks [32], and the evaluation of the effectiveness of particular standards, e.g. [59]. Surveys highlight overconfidence and lack of resources as particular problems in SMEs [31].

Much of Cyber Risk Management is out of scope for Hipster, which is interested only in the aspects of Risk Management that relate to software development product decisions – the processes of identifying threats and problems, and of estimating impact and likelihood. We shall refer to that as Cyber Risk Assessment.

It is quite surprising how little probability-of-problem information is available publicly, and there is even less information about its effectiveness:

> *A major challenge in the use of risk-driven security metrics is the lack of evidence for security effectiveness evidence in the early phases of product development and Risk Analysis, when the needs for it are at their greatest.* [52]

4.3 Security Requirements and Values

Traditional requirements engineering assumes an 'in or out' decision making process: each requirement makes it into the design specification or is effectively abandoned. There are many approaches to security requirements; most consider them part of a process that includes threat

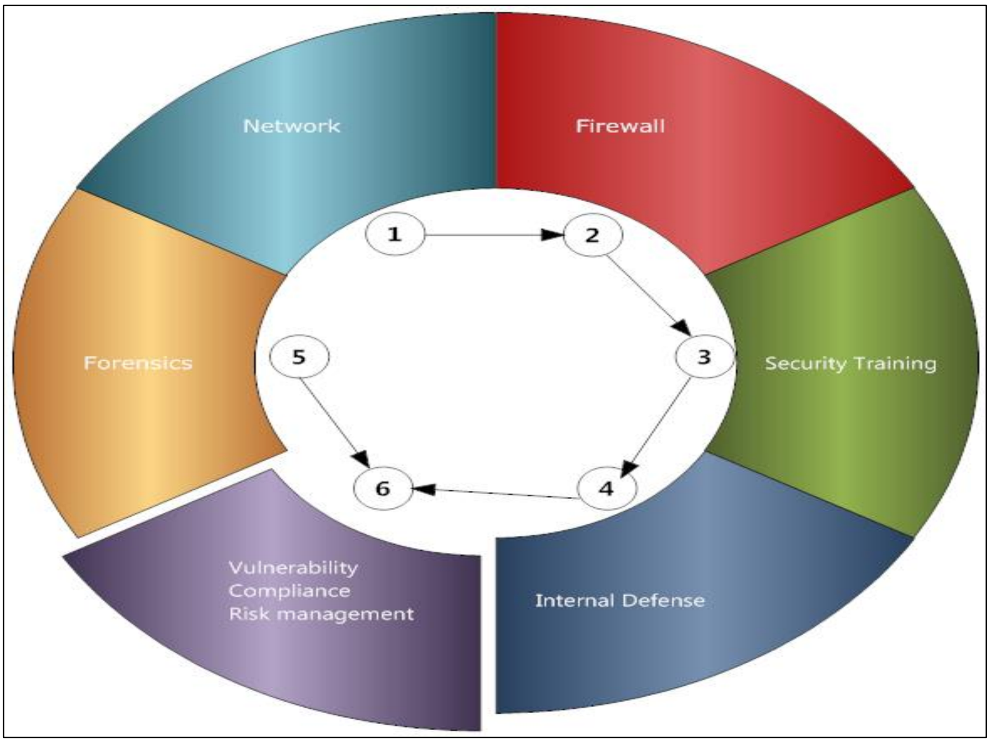

Figure 8: Example Cybersecurity Strategy (Sean P Connors, via Wikipedia)

identification and vulnerability detection, but CLASP and Secure Tropos exclude these 'implementation details' [49].

Agile approaches differ by providing a much more fluid approach to requirements: requirements are typically expressed as stories; the list of outstanding requirements is kept arranged in priority order; and only the highest priority stories are actioned in each development cycle [7]. Security requirements do not fit particularly well in this scheme: security, like performance and usability, is a 'cross-cutting concern,' and impacts every story. 'Abuser stories' are an attempt to add these requirements as separate concerns [8]. It is possible to incorporate security into many steps in an agile process [7 ch. 7], but there is little literature available on the effectiveness of doing so.

Corporate and commercial values can be captured with a range of techniques in the family of 'Value Centred Design,' and are frequently used to capture security and privacy requirements. [20]

5 Hipster Activities

5.1 Cyber Threat Intelligence – Risk Assessments

The emphasis on timeliness rather than analysis for Cyber Threat Intelligence makes it problematic to use for product-level decisions. Some approaches are as follows.

To assess industry-wide risks one survey used risk quantification techniques [14]; in particular it distinguished the expected loss from the insurance industry 'Value at Risk', the maximum loss from security breaches. It evaluates risk profile by distinguishing seven types of information, four reasons for attacks (espionage, advanced crime, mass crime and disturbance), and 'slow' and 'fast' attack types.

Another approach is to use data from the CAPEC and CWE databases to assess identified threats [19], [29].

Table 1: Comparison of Traditional Security Risk Management and Agile [xxx]

Security Risk Management	The Agile Philosophy
Top-down approach based on plan-do-check-act cycle	Incremental approach based on small speculate-collaborate-learn iterations and frequent feedback cycles
Upfront, fix planning which drives remaining risk management activities	Gradual planning of activities (planning game) driven by learning from feedback cycles
Documentation-centric approach which relies on documented knowledge	Light weight documentation driven by importance deemed by stakeholders; more tacit knowledge-oriented based on person-to-person communication
Upfront decision about level of security needed for the system reflected on a priori agreement on, e.g., risk evaluation criteria and risk acceptance criteria	Stakeholders establish an initial baseline for security level needed and adjust this along the way
Assumes complete and correct information and consensus about criteria used	Assumes that incomplete knowledge and uncertainty are part of the process, changes are inevitable and testing should start from the first iteration
Labor intensive and costly, causing time and budget overhead	Minimalist, lean approach which tends to be less demanding in terms of effort and time, therefore, less costly

5.2 Risk Assessment – Agile Product Requirements

How can we map security risk assessments as prioritised software requirements? While research on security requirements goes back to 1967 [43], much of the academic work on security requirements uses formal logic (e.g. [12], [24]) or prescriptive corporation-wide policies [28], making it inapplicable to SMEs unsupported by security groups.

Indeed, Table 1 illustrates a commonly-found tension between traditional risk management and Agile [18].

A 2008 survey of lightweight approaches identified 8 aspects of security requirements, and 9 approaches (Figure 9) [61]. Note that different methods are required for security requirements (objectives) and for threat identification. The approaches to threat documentation included Misuse Cases [58], Abuser Stories [8] and Attack Trees; the authors recommend Abuser Stories as a good approach for agile development projects.

One approach is to use a game such as Protection Poker to help development teams improve their risk estimation [68]. A practical trial found participants generally positive, but there was doubt that it increased the security of the products developed [60] .

It is, however, possible to reuse threat models expressed as misuse cases [35].

5.3 Security, Risks and Threats Related to Health IoT Software

Health IoT software has particular security issues, and medical devices, in particular, have much associated legislation [10]. Three specific problems make risk assessment difficult in IoT: the speed of change, that intangible information (such as protocol details and device locations) may itself be a target, and the possibility of devices themselves being attack platforms [15]. In practice, many commercial sensors have known defects [41]. Implanted Medical Devices (IMDs) offer particular

How different approaches to security requirements engineering handle requirements phase tasks

Approach	Definitions	Objectives	Misuse/ threats	Assets	Coding standards	Categorize & prioritize	Inspect & validate	Process planning
SQUARE[10]	√	√	√			√	√	
Charles Haley and colleagues[8]		√	√	√			√	
Gustav Boström and colleagues[11]			√	√	√	√		
CLASP		√	*	√			√	
Microsoft[3,12,13]		√	√ †	√ †				√
Axelle Apvrille and Makan Pourzandi[14]		√	√			√		
Eduardo Fernandez[15]			√					
Kenneth van Wyk and Gary McGraw[16]			√					
Gunnar Peterson[9]			√					

Figure 9: Lightweight Security Requirements Methods

security problems, and several problems have already occurred with commercially-deployed devices [71].

A Finnish project provides a case study of risk assessment for security threats in a Health IoT application, and offers insights into the risk assessment methodology of a large telecommunications company [53]. Participants assessed risks from both the service provider and the end user perspective. The method, though, does not include a method or data source for the risk assessments involved, nor do the reports discuss product management in the resulting decisions; indeed, their conclusion implies a lack of human intervention in the process:

> *Risk prioritization is not unambiguous, and even small changes in the system's assumptions can change it* [53]

The same group used a similar approach on several projects [52],[51]. Others have provided threat assessments without risk analysis [23].

A recent UK project investigated Cyber Risk assessment for the IoT [45]. They identified 10 different risk assessment methods commonly in use [46], and proposed a method based on combining two methods: Cyber Value at Risk and MicroMort [47].

One risk quantification approach to the changing nature of Health IoT is 'adaptive security', using game theory to address the implications of changing needs and provide quantitive assessments of threats [25]; this has been demonstrated on a case study [37]. Another quantitative approach is 'composing threats', demonstrated assessing the threats from adding further IoT components [13].

6 Discussion

6.1 Agile Software Development and Hipster

Returning to the discussion of Agile Software Development (Section 3.3), we observe that Agile's preference for "Individuals and Interactions over Processes and Tools" [6] and for self-organising teams [6] gives control to those development teams over process and tools. Thus, for Hipster to influence the security practices of a team requires 'grassroots hearts and minds' persuasion rather than corporate adoption of tools or processes.

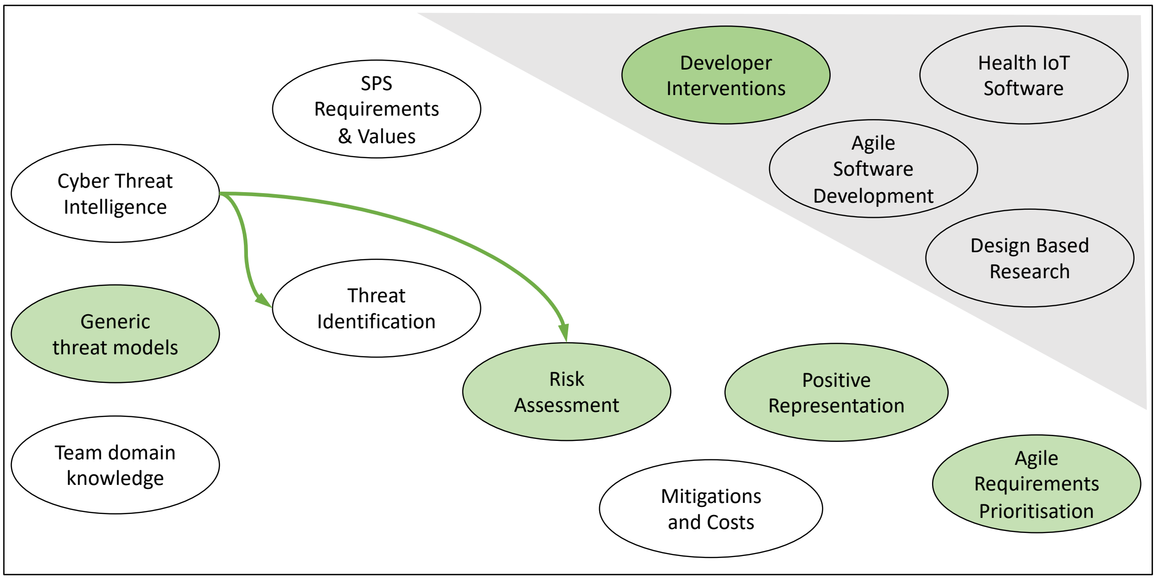

Figure 10: Key Research Areas

Also, from Table 1 in Section 5.2, we see that the Agile philosophy and incremental development approaches do not mesh well with traditional cybersecurity approaches. It is possible to integrate cyber risk management into an agile process (Section 4.3), but the impact analysis of doing so appears as yet to be lacking in academic literature.

6.2 Research Topics

Returning to Figure 2 and considering Sections 4 and 5, we see that certain of the topics and connections in Figure 2 are supported much less by existing research than others. Figure 10 highlights these topics and connections.

Those topics will form the main thrust of research in the Hipster Project.

6.3 Research Questions

Returning to the research questions, we can now address each in turn. Since the later research questions expand on the first, we return to them in reverse order.

RQ 3 , *"What is the research work related to the processes the developer teams will carry out in the HIPSTER project?",* we found a good deal of work related to security requirements in general, to the identification of security issues in Health IoT, and to the handling of security issues within the agile development lifecycle. Far less supported are means to use threat intelligence for practical risk assessment, and means to reuse prior threat assessments in different areas

Addressing RQ 2 "*What is the prior work in the research context for the Hipster project?*", we found comprehensive literature related to Agile Development, Design Based Research and to Health IoT as a topic in itself. We found less literature related to development team interventions, and conclude this subject is relatively new as a research topic.

Section 5, therefore, provides an answer to RQ 1 "*What is the important prior research related to aspects of 'using DBR to create an intervention that uses cyber threat intelligence to improve security, privacy and safeguarding outcomes in agile development approaches for Health IoT systems within resource constrained development teams'?*"

7 Conclusion

This report summarises the current state of the art related to the Hipster project. Figure 10 summarises the resulting main areas of research for the project itself.

The mission of the Hipster project is to provide workable and practical improvements in those areas.

Credit

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

References

[1] Agile Alliance. Subway Map to Agile Practices. https://www.agilealliance.org/agile101/subway-map-to-agile-practices/.

[2] Baker, S.B., Xiang, W., and Atkinson, I. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access 5*, (2017), 26521–26544.

[3] Bakker, A. *Design Research in Education: A Practical Guide for Early Career Researchers*. Routledge, Abingdon, 2018.

[4] Barab, S. and Squire, K. Design-Based Research: Putting a Stake in the Ground. *Journal of the Learning Sciences 13*, (2004).

[5] Bass, J.M. Artefacts and Agile Method Tailoring in Large-Scale Offshore Software Development Programmes. *Information and Software Technology 75*, (2016), 1–16.

[6] Beedle, M., Van Bennekum, A., Cockburn, A., et al. Manifesto for Agile Software Development. (2001), 2–3.

[7] Bell, L., Brunton-Spall, M., Smith, R., and Bird, J. *Agile Application Security: Enabling Security in a Continuous Delivery Pipeline*. O'Reilly, Sebastopol, CA, 2017.

[8] Boström, G., Wäyrynen, J., Bodén, M., Beznosov, K., and Kruchten, P. Extending XP Practices to Support Security Requirements Engineering. *Proceedings of the 2006 international workshop on Software engineering for secure systems*, IEEE Computer Society (2006), 11–18.

[9] Brown, R., Lee, R.M., and SANS. *2021 SANS Cyber Threat Intelligence (CTI) Survey*. 2021.

[10] Burns, A.J., Johnson, M.E., and Honeyman, P. A Brief Chronology of Medical Device Security. *Communications of the ACM 59*, 10 (2016), 66–72.

[11] Cascavilla, G., Tamburri, D.A., and Van Den Heuvel, W.J. Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review. *Computers & Security 105*, (2021), 102258.

[12] Chivers, H. Information Modeling for Automated Risk Analysis. *IFIP International Conference on Communications and Multimedia Security*, Springer (2006), 228–239.

[13] Darwish, S., Nouretdinov, I., and Wolthusen, S.D. Towards Composable Threat Assessment for Medical IoT (MIoT). *Procedia Computer Science 113*, (2017), 627–632.

[14] Deloitte and Buith, J. *Cyber Value at Risk in the Netherlands*. 2016.

[15] Douglas, K.M., Sutton, R.M., Nurse, J.R.C., Radanliev, P., Creese, S., and De Roure, D. If You Can't Understand It, You Can't Properly Assess It! The Reality of Assessing Security Risks in

Internet of Things Systems. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, IET (2018), 1.

[16] Easterbrook, S., Singer, J., Storey, M.-A., and Damian, D. Selecting Empirical Methods for Software Engineering Research. In *Guide to Advanced Empirical Software Engineering*. Springer, London, 2008, 285–311.

[17] Edgar, T. and Manz, D. *Research Methods for Cyber Security*. Syngress, 2017.

[18] Franqueira, V.N.L., Bakalova, Z., Tun, T.T., and Daneva, M. Towards Agile Security Risk Management in RE and Beyond. *Proceedings - 1st International Workshop on Empirical Requirements Engineering, EmpiRE 2011*, IEEE (2011), 33–36.

[19] Franqueira, V.N.L., Tun, T.T., Yu, Y., Wieringa, R., and Nuseibeh, B. Risk and Argument: A Risk-Based Argumentation Method for Practical Security. *Proceedings of the 2011 IEEE 19th International Requirements Engineering Conference, RE 2011*, IEEE Computer Society (2011), 239–248.

[20] Friedman, B. and Hendry, D.G. *Value Sensitive Design: Shaping Technology With Moral Imagination*. Mit Press, 2019.

[21] Giardino, C., Unterkalmsteiner, M., Paternoster, N., Gorschek, T., and Abrahamsson, P. What Do We Know about Software Development in Startups? *IEEE Software 31*, 5 (2014), 28–32.

[22] Giotsas, V. CommunityWatch: The Swiss-Army Knife of BGP Anomaly Detection. *Proceedings of the Applied Networking Research Workshop*, (2018), 24.

[23] Habib, K., Torjusen, A., International, W.L.-T.S., and 2015, U. Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth. *The Seventh International Conference on eHealth, Telemedicine, and Social Medicine (TELEMED 2015)*, (2015).

[24] Haley, C., Laney, R., ... J.M.-I.T. on, and 2008, U. Security Requirements Engineering: A Framework for Representation and Analysis. *IEEE Transactions on Software Engineering 34*, (2008).

[25] Hamdi, M. and Abie, H. Game-Based Adaptive Security in the Internet of Things for eHealth. *2014 IEEE International Conference on Communications, ICC 2014*, IEEE Computer Society (2014), 920–925.

[26] Hassanalieragh, M., Page, A., Soyata, T., et al. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, Institute of Electrical and Electronics Engineers Inc. (2015), 285–292.

[27] Hawe, P. and Potvin, L. What Is Population Health Intervention Research? *Canadian Journal of Public Health 2009 100:1 100*, 1 (2009), I8–I14.

[28] Higgins, H.N. Corporate System Security: Towards an Integrated Management Approach. *Information Management and Computer Security 7*, 5 (1999), 217–222.

[29] Hilde Houmb, S., Franqueira, V.N., and Engum, E.A. Quantifying Security Risk Level From CVSS Estimates of Frequency and Impact. (2009).

[30] Hoadley, C., Baumgartner, E., Bell, P., et al. Design-Based Research: An Emerging Paradigm for Educational Inquiry. *Educational Researcher 32*, 1 (2002), 5–8.

[31] Hoppe, F., Gatzert, N., and Gruner, P. Cyber Risk Management in SMEs: Insights From Industry Surveys. *The Journal of Risk Finance*, (2021).

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

[33] Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., and Kwak, K.S. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access 3*, (2015), 678–708.

[34] IT Governance UK. Cyber Risk Management. https://www.itgovernance.co.uk/cyber-security-risk-management.

[35] Jensen, J., Tøndel, I.A., and Meland, P.H. Experimental Threat Model Reuse With Misuse Case Diagrams. *International Conference on Information and Communications Security*, Springer (2010), 355–366.

[36] Kluyver, T., Ragan-kelley, B., Pérez, F., et al. Jupyter Notebooks: A Publishing Format for Reproducible Computational Workflows. In *Positioning and Power in Academic Publishing: Players, Agents and Agendas*. IOS Press, 2016, 87–90.

[37] Leister, W., Hamdi, M., Abie, H., and Poslad, S. An Evaluation Framework for Adaptive Security for the Iot in Ehealth. *International Journal on Advances*, (2014).

[38] Lewin, K. Action Research and Minority Problems. *Journal of Social Issues 2*, 4 (1946), 34–46.

[39] Li, Z. Stop Building Castles on a Swamp! The Crisis of Reproducing Automatic Search in Evidence-based Software Engineering. *2021 IEEE/ACM 43rd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)*, IEEE (2021), 16–20.

[40] Lopez, T., Sharp, H., Tun, T., Bandara, A., Levine, M., and Nuseibeh, B. Talking about Security with Professional Developers. *Workshop on Conducting Empirical Studies in Industry - CESSER-IP*, IEEE Computer Society (2019).

[41] McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., and Chen, H. Assessing Medical Device Vulnerabilities on the Internet of Things. *2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017*, Institute of Electrical and Electronics Engineers Inc. (2017), 176–178.

[42] 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.

[43] Peters, B. Security Considerations in a Multi-Programmed Computer System. *AFIPS Conference Proceedings - 1967 Spring Joint Computer Conference, AFIPS 1967*, Association for Computing Machinery, Inc (1967), 283–286.

[44] Poller, A., Kocksch, L., Türpe, S., Epp, F.A., and Kinder-Kurlanda, K. Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group. *Conference on Computer Supported Cooperative Work - CSCW*, ACM (2017), 2489–2503.

[45] Radanliev, P., Charles, D., Roure, D., et al. *Methodology for Designing Decision Support Systems for Visualising and Mitigating Supply Chain Cyber Risk from IoT Technologies*. 2019.

[46] Radanliev, P., De Roure, D., Maple, C., Nurse, J.R.., Nicolescu, R., and Ani, U. *Cyber Risk in IoT Systems*. Preprints.org, 2019.

[47] Radanliev, P., De Roure, D.C., Nurse, J.R.C., et al. Future Developments in Standardisation of Cyber Risk in the Internet of Things (IoT). *SN Applied Sciences 2020 2:2 2*, 2 (2020), 1–16.

[48] Recorded Future. *The Threat Intelligence Handbook: Moving toward a Security Intelligence Program*. CyberEdge Group, Annapolis, MD, USA, 2019.

[49] Salini, P. and Kanmani, S. Survey and Analysis on Security Requirements Engineering. *Computers & Electrical Engineering 38*, 6 (2012), 1785–1797.

[50] Sauerwein, C., Sillaber, C., Mussmann, A., and Breu, R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. *The 13th International Conference on Wirtschaftsinformatik*, (2017), 837–851.

[51] Savola, R.M. and Abie, H. Metrics-Driven Security Objective Decomposition for an E-Health Application With Adaptive Security Management. *Proceedings of the International Workshop on Adaptive Security, ASPI 2013*, (2013).

[52] Savola, R.M., Frühwirth, C., and Pietikäinen, A. Risk-Driven Security Metrics in Agile Software Development-An Industrial Pilot Study. *J. Univers. Comput. Sci. 18*, 12 (2012), 1679–1702.

[53] Savola, R.M., Savolainen, P., Evesti, A., Abie, H., and Sihvonen, M. Risk-Driven Security Metrics Development for an E-Health IoT Application. *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*, Institute of Electrical and Electronics Engineers Inc. (2015).

[54] Schmittner, C., Chlup, S., Fellner, A., Macher, G., and Brenner, E. ThreatGet: Threat Modeling Based Approach for Automated and Connected Vehicle Systems. *AmE 2020 - Automotive meets Electronics; 11th GMM-Symposium*, (2020), 1–3.

[55] Schwaber, K. *Agile Project Management with Scrum*. Microsoft press, 2004.

[56] Shackleford, D. and SANS. *Who's Using Cyberthreat Intelligence and How?* 2015.

[57] Shah, S.H. and Yaqoob, I. A Survey: Internet of Things (IOT) Technologies, Applications and Challenges. *2016 4th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2016*, Institute of Electrical and Electronics Engineers Inc. (2016), 381–385.

[58] Sindre, G. and Opdahl, A.L. Eliciting Security Requirements with Misuse Cases. *Requirements Engineering 10*, 1 (2005), 34–44.

[59] Such, J.M., Vidler, J., Seabrook, T., and Rashid, A. *Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials*. 2015.

[60] Tøndel, I.A., Jaatun, M.G., Cruzes, D.S., and Williams, L. Collaborative Security Risk Estimation in Agile Software Development. *Information and Computer Security 26*, 4 (2019), 508–535.

[61] Tøndel, I.A., Jaatun, M.G., and Meland, P.H. Security Requirements for the Rest of Us: A Survey. *IEEE Software 25*, 1 (2008), 20–27.

[62] Türpe, S., Kocksch, L., and Poller, A. Penetration Tests a Turning Point in Security Practices? Organizational Challenges and Implications in a Software Development Team. *Workshop on Security Information Workers - SIW*, USENIX Association (2016).

[63] University of Georgia. A PEER Tutorial for Design-Based Research. 2006. http://dbr.coe.uga.edu/enact01.htm.

[64] Wagner, T.D., Mahbub, K., Palomar, E., and Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. *Computers and Security 87*, (2019), 101589.

[65] Wang, F. and Hannafin, M.J. Design-Based Research and Technology-Enhanced Learning Environments. *Educational Technology Research and Development 53*, 4 (2005), 5–23.

[66] 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.

[67] Weir, C., Blair, L., Becker, I., Sasse, M.A., and Noble, J. Light-touch Interventions to Improve Software Development Security. *Cybersecurity Development Conference - SecDev*, IEEE (2018), 12.

[68] Williams, L., Meneely, A., and Shipley, G. Protection Poker: The New Software Security "Game." *IEEE Security and Privacy 8*, 3 (2010), 14–20.

[69] Yasin, A., Fatima, R., Wen, L., Afzal, W., Azhar, M., and Torkar, R. On Using Grey Literature and Google Scholar in Systematic Literature Reviews in Software Engineering. *IEEE Access 8*, (2020), 36226–36243.

[70] Yskout, K., Scandariato, R., and Joosen, W. Do Security Patterns Really Help Designers? *International Conference on Software Engineering - ICSE*, IEEE (2015), 292–302.

[71] Zaldivar, D., Tawalbeh, L.A., and Muheidat, F. Investigating the Security Threats on Networked Medical Devices. *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, Institute of Electrical and Electronics Engineers Inc. (2020), 488–493.