Security by design: an interdisciplinary systematic review and conceptual framework

Real, C. del; Busser, E. de; Berg, B. van den

Protocol – Security by Design: An interdisciplinary systematic review and conceptual framework

Cristina Del Real[a] Els De Busser[a] Bibi van den Berg[a]

[a]Institute of Security and Global Affairs, Leiden University (The Netherlands)

Structured abstract

Background: Security by design is the approach to designing digital technologies that are foundationally secure. This approach has materialized in several software design methodologies. However, a close examination of these methodologies shows that digital technologies security is designed as a technical feature, with no concern for their interaction with human, social, and organizational factors. This research argues that, in order to produce a design methodology for developing secure software systems that integrates non-technical factors in their design, an interdisciplinary and integrative review of the 'security by design' concept is needed.

Objectives: The present protocol details the work plan for a systematic scoping review on security by design and related concepts. This review seeks to (1) synthesize current definitions of 'security by design', (2) elaborate a conceptual map that shows how 'security by design' connects to other related concepts, and (3) identify the key principles of the 'security by design' approach.

Design: This systematic review follows the PRISMA extension for scoping review. Six databases are searched for thematically relevant studies published in English. Studies included peer-reviewed publications, government or company documents, technical reports, or a doctoral theses. After the initial search, three researchers will screen the title and abstracts following a screening tool. The consistency of researchers' classification will be measured by calculating the inter-rater reliability. The reading of full texts will determine the final eligibility. Finally, data will be extracted from the final sample of documents.

1. Background

Security by design is an approach to designing products to ensure security and privacy foundationally (Masys, 2018). In particular, security by design has been extensively applied to the development of secure software systems[1]. When applied to software systems, this approach dates back to the late 20th century when some authors proposed a shift from a reactive approach to software security, based on 'penetrate and patch', to a proactive one, based on integrating security into the software development process (McGraw, 1998). This shift was motivated by the well-known fact that many security problems are caused by errors in software design and coding (Williams, 2021). Since then, many software development processes based on security by design have been developed. One of the best known is Microsoft's Security Development Lifecycle

[1] This study focuses on secure software systems, which can be defined as a system within a computer system composed of interconnected software-based components (Sommerville, 2007). Software systems should not be confused with system software, which is the platform for other software (e.g., an operating system like macOS and Microsoft Windows).

(SDL), which contains twelve practices aiming to improve the security of their products (Microsoft, 2022). A review of these twelve practices –and many other secure software lifecycle models (Williams, 2021)– yields a clear conclusion: the concept of security by design is defined in technical terms.

However, software systems are first of all designed and built by people and when operational, they rarely function in a purely technical environment. When implemented, they interact with human, social, and organizational factors. In the study of digital technology security, three approaches can be found that can be understood as part of a continuum: (1) researchers focusing only on the technical aspects of security; (2) researchers seeking to find a middle ground, though still leaning towards engineering (e.g., the 'socio-technical' approach) (e.g., Baxter & Sommerville, 2011); and (3) researchers focusing on the human-technology interaction, without discussing the technologies themselves.

In recent years, the demand for more social sciences and engineering integration has increased as research shows the critical role of human, social and organizational factors in cyber incidents (Leukfeldt & Holt, 2020). For example, 85% of data breaches involved a human element according to the 2021 Data Breach Investigations Report, including both malicious (i.e., criminal actions such as denial of service and privilege misuse) and unintentional errors (i.e., misconfiguration, misdelivery, publishing error, etc.) (Bassett et al., 2021). And yet, the security of software systems continues to be engineered exclusively with technical mechanisms.

This research is part of the NWO-funded project 'Cyber Security by Integrated Design' (Project C-SIDe). Our main goal is to produce a software design methodology[2] for developing secure software systems that integrate human, social, and organizational factors in their design. To achieve this main goal, we first analyze what is meant by 'security by design'. Since the phrase is used in a variety of disciplines, it is necessary to gain further insights in what exactly is covered by 'security by design' by the current body of research, what the common denominators are, what falls in and what falls out of its scope. We therefore argue that the first step of C-SIDe is to systematically review the current definitions of 'security by design' their related concepts and attributes. However, the existing definitions in the literature are diverse and disconnected. Roughly, sources can be clustered in two groups: empirical research focused on one specific step of the security by design approach (e.g., Casola et al., 2020), or conceptual research that broadly describes security by design principles (e.g., Williams, 2021).

However, it remains unclear how 'security by design' relates to other concepts, or the concept may or may not have traveled through different disciplines. Moreover, it remains unknown whether there is cross-fertilization between the computer science approach and the approaches to the design of secure products and environments developed by social disciplines (see, e.g., Clarke, 1999; Davey & Wootton, 2017; Ekblom, 2017; Kamalipour et al., 2014). In this research, we argue that as the calls for an interdisciplinary approach to design secure software systems becomes increasingly pervasive, even by computer scientists themselves (e.g., Casola et al., 2020; Dalpiaz et al., 2016), science needs to offer a framework for secure design that (1) integrates technical,

[2] A software design methodology (SDM) describes 'a collection of design methods chosen to complement one another, along with rules for applying them to arrive design decisions. [*The software design methodology is composed by*] concepts, artifacts, measures, guidelines, criteria, notations and procedures' (Xiping Song & Osterweil, 1994, p. 364).

organizational and behavioral aspects of secure technologies, and (2) combines conceptual work with empirical evidence. With this systematic literature review we aim to fill the first gap; the C-SIDe project seeks to fill the second.

To the best of our knowledge, no previous attempts have been made to synthesize a definition of security by design and propose a conceptual framework integrating the technical and the non-technical aspects of cyber security. With this review, we aim to (1) synthesize current definitions of 'security by design', (2) elaborate a conceptual map of this notion, i.e. show how 'security by design' connects to other related concepts, and (3) identify the key principles of the 'security by design' approach – i.e., the fundamental propositions that serve as the foundation of the 'security by design' approach. Therefore, this review is relevant for C-SIDe for many reasons. First, it will help us clarify the definition of security by design by finding convergence, gaps and distinctions between research disciplines. Second, it will equip the project with a summary of concepts and attributes that will help us better understand the security by design approach. Finally, it will serve as a directive for future studies and steps to both the broader academic community and the members of the C-SIDe project.

This document presents a systematic, interdisciplinary review protocol to get a comprehensive and integrative examination of the concept of security by design. Previous systematic reviews related to the same topic did not explicitly addresses a critical review of the security by design concept from an integrative perspective. Instead, these reviews focus only on the technical interpretation of security by design, most notably on security requirement engineering (SRE) (e.g., Anwar Mohammad et al., 2019). We found one systematic review that synthesized and evaluated SRE approaches generally (Anwar Mohammad et al., 2019), but most systematic reviews in this area have an even narrower focus. For example, authors have addressed security requirements for edge computing (Yahuza et al., 2020), the Internet of Things (Liao et al., 2021), and specific and well-established software design methodologies such as Agile (Villamizar et al., 2018). The related concept of *privacy* by design has also been the subject of a systematic literature review (for a definition, see Cavoukian, 2009), but here, too, the focus is narrow as it is limited to the healthcare sector (Semantha et al., 2020).

For the purposes of C-SIDe, these systematic reviews have two shortcomings. First, they focus on one of the many steps of security by design – i.e., the security requirements phase. This means they only focus on the phase immediately prior to the actual design of a new system or service: within a greenfield situation these kinds of studies stipulate which elements and features the system ought to have. Second, they have only reviewed computer science documents. Our systematic review distinguishes itself by taking an integrative perspective in reviewing the conceptual literature covering a variety of scientific disciplines.

2. Objectives

We propose a systematic, interdisciplinary literature review on security by design to offer an integrative conceptual model that strengthens the foundation for future work. This paper will elaborate an interdisciplinary definition of security by design following the four phases of the recommended process by Podsakoff et al. (2016) to create better definitions for organizational, behavioural and social sciences. Specifically, this paper will address the following research questions:

RQ_1: How have authors **defined** the security by design approach and what **common denominators, distinctions and gaps** can be found in the definitions?

RQ_2: What **related concepts** to security by design can be found in the literature?

RQ_3: What are the **key principles** of the security by design approach?

RQ_4: To what extent can the key principles of the security by design approach **be identified in the related concepts**?

3. Methods

3.1 Protocol and registration

This protocol was registered with the Open Science Framework (OSF) on [DATE]. The systematic, interdisciplinary review will be performed according to the Preferred Reporting Items for Systematic Reviews and Meta-analysis (PRISMA) guidelines, extension for scoping reviews (PRISMA-ScR), as they are appropriate when the research questions are broader (Tricco et al., 2018). Given the wide variety of definitions available in the discipline-crossing literature on security by design, an interdisciplinary review is the most appropriate technique for mapping and synthesizing the existing definitions, related concepts and key principles. Following the PRISMA guidelines, this paper will search specialized databases for thematically relevant studies published in English. We decided not to include a temporal restriction because the foundations of the security by design paradigm, developed at the beginning of the 21st century, still applies nowadays. This paper will revise peer-reviewed manuscripts, government and company documents, technical documents, or doctoral theses. After the initial search with elaborate queries, three researchers will screen a sample of 20 titles and abstracts of the search results. At this stage, the inter-rater reliability (IRR) score will be calculated to evaluate the degree of agreement in classifying the results as relevant or irrelevant (Belur et al., 2021). Subsequently, the eligibility of the results will be determined by reading the full texts. Once we have all the selection of studies, we will extract the data. Finally, we will evaluate the quality of the studies (see Petticrew & Roberts, 2007).

3.2 Eligibility criteria

To be included in the systematic review, searched documents must meet the following criteria:

- The full text is open access, available through institutional access, or provided by researchers that were contacted for this purpose;
- Is written in English;
- Is a peer-reviewed publication, book, book chapter, conference/proceeding paper, government or company document, technical report, or a doctoral thesis;
- Is not a correction, erratum or retracted article;
- Specifically addresses security by design (thematic relevance);
- The main topic of the research is the security of digital technology (focus);
- Answers at least one of the research questions.

3.3 Information sources

The following databases that are relevant in our field of study and suitable for systematic reviews (Gusenbauer & Haddaway, 2020) are searched:

- ACM Digital Library (the ACM Guide to Computing Literature);
- EBSCO library (Criminal Justice Abstracts and Library, Information Sciences & Technology Abstracts);
- IEEE Xplore;
- ProQuest, including Criminal justice abstracts;
- Scopus (via Elsevier);
- Web of Science (via Clarivate).

3.4 Search terms

We performed comprehensive searches for each database. We obtained access to databases through Leiden University and the Delft University of Technology. The search strategy for our systematic review includes three steps. First, we constructed search terms by identifying the three keywords of our study: the goal (i.e., security), the means (i.e., design) and the object (i.e., software systems). Second, we define our query by finding synonyms of the keywords and using Boolean operators:

- Security: secur*
- Design: "by design*" OR "through design*" OR "development lifecycle" OR "development life cycle"
- Software: software OR "operating system" OR "computer program" OR cod* OR digital* OR electronic* OR technolog*

Finally, we verified these terms in the selected databases to identify the best search string for the purposes of this paper. The design of the search strategy was assisted by two librarians from Leiden University, one of which was specialized in Science and the other one on Political Science, Public Administration, and Security and Global Affairs. Table 1 presents the search queries for each database and the results.

Table 1. Search terms within each database.

Database*	**Search query**	**Results**
ACM Digital Library	[Abstract: secur*] AND [[Abstract: "by design*"] OR [Abstract: "through design*"] OR [Abstract: "development lifecycle"] OR [Abstract: "development life cycle"]] AND [[Abstract: software] OR [Abstract: "operating system"] OR [Abstract: "computer program"] OR [Abstract: cod*] OR [Abstract: digital*] OR [Abstract: electronic*] OR [Abstract: technolog*]]	479
EBSCO Library	AB secur* AND AB ("by N2 design*" OR "through N2 design*" OR "development lifecycle" OR "development life cycle") AND AB (software OR "operating system" OR "computer program" OR cod* OR digital* OR electronic* OR technolog*)	11
IEEE Xplore	("Abstract":secur*) AND ("Abstract":"by design*" OR "Abstract":"through design*" OR "Abstract":"development lifecycle"	567

Database*	Search query	Results
	OR "Abstract":"development life cycle") AND ("Abstract":software OR "Abstract":"operating system" OR "Abstract":"computer program*" OR "Abstract":cod* OR "Abstract":digital* OR "Abstract":electronic* OR "Abstract":technolog*)	
ProQuest	ab(secur*) AND ab("by design*" OR "through design*" OR "development lifecycle" OR "development life cycle") AND ab(software OR "operating system" OR "computer program" OR cod* OR digital* OR electronic* OR technolog*)	489
Scopus	ABS ((secur*) AND ("by design*" OR "through design*" OR "development lifecycle" OR "development life cycle") AND (software OR "operating system" OR "computer program" OR cod* OR digital* OR electronic* OR technolog*))	1601
Web of Science	((TS=(secur*)) AND TS=("by design*" OR "through design*" OR "development lifecycle" OR "development life cycle")) AND TS=(software OR "operating system" OR "computer program" OR cod* OR digital* OR electronic* OR technolog*)	503
Total		**3651**

*Queries were adapted to each database. The total includes duplicates. Searches were carried out on 26 April 2022.

Search results will be then exported to the software Rayyan to remove duplicates.

3.5 Selection of sources of evidence

3.5.1 Screening

The screening will be conducted using Rayyan, a web and mobile tool designed for systematic reviews (see Ouzzani et al., 2016). Rayyan allows researchers to efficiently screen articles by offering three possibilities: 'include', 'exclude', or 'undecided'. Researchers then can label articles and select exclusion reasons. Furthermore, researchers can collaboratively work on the same dataset of articles while their responses remain blind during the screening process. Only when researchers decide to switch off blinding does Rayyan offer the results of the conflicts, pointing at those documents in which agreement was not achieved. Based on previous literature on best practices guidelines for the title and abstract screening (Polanin et al., 2019), we developed a screening tool (see Appendix A).

A pilot study will be carried out to assess the agreement degree between researchers. This pilot study may subsequently modify the screening tool proposed in this protocol. Three raters will randomly select 50 abstracts to classify them according to the screening tool. The process will assess both the screening tool and the exclusion and inclusion criteria. Documents will be labelled as 'include', 'exclude' or 'undecided'. The process will be repeated until we obtain substantial inter-rater reliability measured by a Cohen's kappa ≥ 0.6 (Cohen, 1960). If the agreement is low (kappa < 0.6), a meeting with the research team will take place, followed by the update of the screening tool. The team will meet regularly until a high inter-rater reliability is obtained. After concluding the pilot study, all titles and abstracts will be screened by the first author (van de Schoot et al., 2021). Once the papers have been selected according to the screening of titles and abstracts, the first author will then screen the full texts to select the final sample of documents.

3.5.2 Additional sources

Security by design is a complex topic developed mostly by the technology industry. As a result, many documents on security by design are not scholarly articles but policy and corporate reports. While our focus will be primary academic documents, we will supplement our sample with two additional resources: Google Scholar and backward searches. Any literature flagged as relevant by the first author will be selected for the full-text review.

Even though Google Scholar is widely popular, it will be used as a secondary resource because of its several limitations. Among others, Google Scholar lacks transparency, replicability and availability (Gusenbauer & Haddaway, 2020). We use the *Publish or Perish* software to make the Google Scholar search and download the results. The following query was used on 18 March 2022:

> (secur*) AND ("by design*" OR "through design*" OR "development lifecycle" OR "development life cycle") AND (software OR "operating system" OR "computer program" OR digital* OR electronic* OR technolog*)

Publish or Perish yielded the maximum number of results permitted, 1000. New literature –i.e., not previously featured in the primary searches– identified as relevant will be selected for full-text review.

The reference list from studies identified as 'relevant' in the Rayyan or Google Scholar will be reviewed for additional literature to further supplement the primary searches and identify policy documents and corporate reports. New documents identified as relevant will be included in the review of full texts.

3.6 Data charting

The literature identified for full-text review will be then summarized in a spreadsheet. The purpose is to provide a descriptive analysis of the characteristics of security by design literature. Moreover, this process will further help us assess the inclusion of studies. The spreadsheet will contain the following information:

- Identification number
- Author(s)
- Title of the publication
- Year of publication
- Journal
- Study region (if applicable)
- Type of publication (e.g., journal, book chapter)
- Discipline (e.g., computer science, criminology)
- Aims
- Data (if applicable)
- Methods (if applicable)
- Research question
- Reason for exclusion (if applicable)

The final selection of literature will be then imported into Atlas.ti (version 8) for systematic coding of themes. The analysis will start with three core themes, according to the research questions about

security by design – 'definition' (SxDD), 'key principle' (SxDKP), and 'related concept' (SxDRC). The information collected using each code will comprise the data to answer our four research questions. Further codes could be developed during the coding phase. The three researchers will develop the codebook. This code will include (a) the name of the code, (b) the description of the code, (c) instructions, and (d) the associated research question. Before coding all the documents, a second pilot study will be conducted to evaluate the agreement in the coding. After an acceptable agreement is reached, the first author will code the rest of the documents. Data from this study will be made publicly available once we finalize the coding.

3.7 Synthesis of results

The results of this study will be presented in the form of a narrative synthesis. This is the best option when research is heterogeneous (see, e.g., Popay et al., 2006). The presentation of the results will be organized according to the four research questions. First, a synthesis of security by design definitions will be presented. Second, the related concepts will be displayed through word clouds and network analysis. Third, we will summarize the key principles featuring security by design practices. Fourth, the related concepts from the network will be then connected to the key principles. The overall objective of this research is to propose an integrative definition of security by design. Following the recommendations by Podsakoff et al. (2016), responses to the research questions will be used to develop a preliminary definition. Finally, we will refine the conceptual definition by asking ourselves, 'What do we mean by that?' until all of the ambiguity in the words used to define the concept have been resolved.

References

Anwar Mohammad, M. N., Nazir, M., & Mustafa, K. (2019). A Systematic Review and Analytical Evaluation of Security Requirements Engineering Approaches. *Arabian Journal for Science and Engineering*, *44*(11), 8963–8987. https://doi.org/10.1007/s13369-019-04067-3

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2021). *2021 Data Breach Investigations Report* (p. 119) [Research report]. Verizon.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Belur, J., Tompson, L., Thornton, A., & Simon, M. (2021). Interrater Reliability in Systematic Review Methodology: Exploring Variation in Coder Decision-Making. *Sociological Methods & Research*, *50*(2), 837–865. https://doi.org/10.1177/0049124118799372

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2020). A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. *Journal of Systems and Software*, *163*, 110537. https://doi.org/10.1016/j.jss.2020.110537

Cavoukian, A. (2009). *Privacy by Design: The 7 foundational principles* (p. 12). Information and Privacy Commissioner.

Clarke, R. V. (1999). *Hot Products. Understanding, Anticipating and Reducing the Demand for Stolen Goods*. Home Office.

Cohen, J. (1960). A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement*, *20*(1), 37–46. https://doi.org/10.1177/001316446002000104

Dalpiaz, F., Paja, E., & Giorgini, P. (2016). *Security requirements engineering: Designing secure socio-technical systems*. The MIT Press.

Davey, C. L., & Wootton, A. B. (2017). *Design Against Crime: A Human-Centred Approach to Designing for Safety and Security* (1st ed.). Routledge.

Ekblom, P. (2017). Designing products against crime. In R. Wortley & M. Townsley (Eds.), *Environmental criminology and crime analysis* (2nd ed., pp. 304–333). Routledge.

Gusenbauer, M., & Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Research Synthesis Methods*, *11*(2), 181–217. https://doi.org/10.1002/jrsm.1378

Kamalipour, H., Faizi, M., & Memarian, G. (2014). Safe Place by Design: Urban Crime in Relation to Spatiality and Sociality. *Current Urban Studies*, *02*(02), 152–162. https://doi.org/10.4236/cus.2014.22015

Leukfeldt, E. R., & Holt, T. J. (Eds.). (2020). *The human factor of cybercrime*. Routledge, Taylor & Francis Group.

Liao, Z., Nazir, S., Khan, H. U., & Shafiq, M. (2021). Assessing Security of Software Components for Internet of Things: A Systematic Review and Future Directions. *Security and Communication Networks*, *2021*, 1–22. https://doi.org/10.1155/2021/6677867

Masys, A. J. (Ed.). (2018). *Security by Design: Innovative Perspectives on Complex Problems*. Springer International Publishing. https://doi.org/10.1007/978-3-319-78021-4

McGraw, G. (1998). Testing for security during development: Why we should scrap penetrate-and-patch. *IEEE Aerospace and Electronic Systems Magazine*, *13*(4), 13–15. https://doi.org/10.1109/62.666831

Microsoft. (2022). *Microsoft Security Development Lifecycle* [Company]. https://www.microsoft.com/en-us/securityengineering/sdl/

Ouzzani, M., Hammady, H., Fedorowicz, Z., & Elmagarmid, A. (2016). Rayyan—A web and mobile app for systematic reviews. *Systematic Reviews*, *5*(1), 210. https://doi.org/10.1186/s13643-016-0384-4

Petticrew, M., & Roberts, H. (2007). *Systematic Reviews In The Social Sciences: A Practical Guide*. John Wiley & Sons. http://www.123library.org/book_details/?id=5685

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2016). Recommendations for Creating Better Concept Definitions in the Organizational, Behavioral, and Social Sciences. *Organizational Research Methods*, *19*(2), 159–203. https://doi.org/10.1177/1094428115624965

Polanin, J. R., Pigott, T. D., Espelage, D. L., & Grotpeter, J. K. (2019). Best practice guidelines for abstract screening large-evidence systematic reviews and meta-analyses. *Research Synthesis Methods*, *10*(3), 330–342. https://doi.org/10.1002/jrsm.1354

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K., & Duffy, S. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews: A product from the ESRC Methods Programme*. Lancaster University. https://doi.org/10.13140/2.1.1018.4643

Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. *Electronics*, *9*(3), 452. https://doi.org/10.3390/electronics9030452

Sommerville, I. (2007). *Software engineering* (8th ed). Addison-Wesley.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Annals of Internal Medicine*, *169*(7), 467–473. https://doi.org/10.7326/M18-0850

van de Schoot, R., de Bruin, J., Schram, R., Zahedi, P., de Boer, J., Weijdema, F., Kramer, B., Huijts, M., Hoogerwerf, M., Ferdinands, G., Harkema, A., Willemsen, J., Ma, Y., Fang, Q., Hindriks, S., Tummers, L., & Oberski, D. L. (2021). An open source machine learning framework for efficient and transparent systematic reviews. *Nature Machine Intelligence*, *3*(2), 125–133. https://doi.org/10.1038/s42256-020-00287-7

Villamizar, H., Kalinowski, M., Viana, M., & Fernandez, D. M. (2018). A Systematic Mapping Study on Security in Agile Requirements Engineering. *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 454–461. https://doi.org/10.1109/SEAA.2018.00080

Williams, L. (2021). *Secure Software Lifecycle Knowledge Area Version 1.0.2* (p. 47). North Carolina State University.

Xiping Song, & Osterweil, L. J. (1994). Experience with an approach to comparing software design methodologies. *IEEE Transactions on Software Engineering*, *20*(5), 364–384. https://doi.org/10.1109/32.286419

Yahuza, M., Idris, M. Y. I. B., Wahab, A. W. B. A., Ho, A. T. S., Khan, S., Musa, S. N. B., & Taha, A. Z. B. (2020). Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities. *IEEE Access*, *8*, 76541–76567. https://doi.org/10.1109/ACCESS.2020.2989456

Appendix A. Screening tool

This tool follows the recommendations and best practices for abstract screening by Polanin et al. (2019).

Citation and title

1. Is the **title** written in English?
    a. Yes: continue screening
    b. No: stop screening
2. Is the **citation a** peer-reviewed publication, book, book chapter, conference/proceeding paper, government or company document, technical report, or doctoral thesis?
    a. Yes: continue screening
    b. No: stop screening
3. Does the **title** indicate that this is NOT a correction, erratum or retracted document?
    a. Yes: continue screening
    b. No: stop screening

Abstract screening

4. Does the **abstract** indicate that the central area of research is digital technologies security?
    a. Yes or Unclear: continue screening
    b. No: stop screening
5. Does the **abstract** indicate that the main approach is security by design?
    a. Yes or Unclear: continue screening
    b. No: stop screening
6. Does the **abstract** indicate that it is a technical paper?
    a. Yes or Unclear: continue screening
    b. No: Stop

Decision: Should this document be included?

- **Yes**, all screening questions answered "Yes" or "Unclear"
- **No**, at least one screening question answered "No"

Funding

This protocol is part of the NWO funded research project 'Cyber Security by Integrated Design' (NWA.1215.18.008).