Towards a User-centred Security Framework for Social Robots in Public Spaces

Samson O. Oruma
samsonoo@hiof.no
Supervised by: Prof. Dr. Ricardo Colomo-Palacios
Østfold University College
Halden, Viken, Norway

ABSTRACT

The use of social robots in public spaces is becoming increasingly popular due to their ability to provide personalized services to users. However, the convergence of different technologies and software applications has raised concerns regarding security requirements, standards, and regulations. Specifically, there are significant concerns about the evolving threat landscape for software applications in public settings, where social robots interact without supervision and are in direct contact with threat actors. During the development of social robots software, developers and practitioners need practical tools to continuously assess their products' security profiles. This paper presents a preventive approach to the dynamic evolving security landscape of Social Robots in Public Spaces (SRPS) using design science research (DSR) methodology to develop a security framework. The study investigates security threats, vulnerabilities, and risks associated with SRPS software development and analyzes existing related frameworks to design a security framework for SRPS software developers. The research aims to provide insights into the security aspects of SRPS software application development processes and contribute to developing effective security frameworks to mitigate evolving risks and ensure secure operation and acceptance in public spaces.

CCS CONCEPTS

• **Security and privacy → Software security engineering**.

KEYWORDS

social robots, cybersecurity framework, threat landscape, public space.

ACM Reference Format:
Samson O. Oruma. 2023. Towards a User-centred Security Framework for Social Robots in Public Spaces. In *Proceedings of the International Conference on Evaluation and Assessment in Software Engineering (EASE '23), June 14–16, 2023, Oulu, Finland*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3593434.3593446

EASE '23, June 14–16, 2023, Oulu, Finland
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0044-6/23/06.
https://doi.org/10.1145/3593434.3593446

1 MOTIVATION, RATIONALE, AND CONTRIBUTION OF THE RESEARCH

The convergence of robotics, automation, and Artificial Intelligence (AI) in social robots (SR), which can naturally interact with humans, is a promising solution to address a wide range of societal needs [17]. The use of social robots (SR) has promising potential in various fields, such as healthcare [13], education [4], retail services [22] and public space [18]. The market for social humanoid robots is expected to reach $11.24 billion by 2026 [23]. However, deploying social robots in public spaces raises concerns regarding security, privacy, safety, and reliability [7]. Protecting users' data and SR from attacks, thefts, sabotage, and vandalism is crucial in such settings [19].

A recent systematic literature review of 1469 studies on the threat landscape of SRPS [18] revealed seven interrelated sub-components for SR, namely hardware, software, communication, human, cloud services, AI services, and supply chain. Existing security frameworks, such as SOC 2, ISO 270001, NIST cybersecurity framework, HIPAA, PCI DSS, and FISMA, are not tailored to address all these security aspects; hence researchers are calling for new standards [27], and laws [7] for SRPS. A user-centred security framework emphasises all users' needs, preferences, and behaviours interacting with the SRPS system. To effectively address the diverse security requirements, such a framework should incorporate key aspects like (i) understanding user needs, (ii) usability, (iii) user involvement, (iv) accessibility, (v) flexibility, (vi) training and education, and (vii) continuous evaluation and improvement [10]. One challenge software developers and designers face is the tendency to focus on creating functional software rather than addressing the comprehensive security needs of all users [1]. During testing and evaluation, the emphasis is often placed on specific use cases rather than potential misuse (abuse) cases, which are crucial to achieving a robust and secure software system. A secure software development process should anticipate and attempt to mitigate threats targeting all SRPS sub-components.

The Robot Operating System (ROS), a fundamental platform for social robots, is susceptible to several software vulnerabilities [24]. In the case of SRPS, one challenge is that malicious actors can potentially gain physical access to the robots and exploit the Linux Kernel vulnerability in ROS using a USB drive [14]. The public spaces where social robots operate are dynamic, with various actors and unpredictable variables. Assuming that the AI of social robots will continue to evolve, adapt, and learn from its context to optimise user experience, it is essential to anticipate and prepare for emerging threats in the future. However, SRPS software developers often rely heavily on code reuse without adequately considering known vulnerabilities in the reused code. Developers can create more secure software solutions by incorporating security-by-design principles into the SRPS application development lifecycle [30].

This PhD research aims to create a user-centric security framework for social robot software developers, facilitating the development of secure-by-design software. The framework incorporates continuous vulnerability and threat assessments, assisting targeted users in creating software that addresses security needs and maintains regulatory compliance as technology advances. This research is part of a larger interdisciplinary project, SecuRoPS, with a broader scope than this study alone. The user study will include participants (users) from the project consortium.

The SecuRoPS consortium comprises five partners, each representing various targeted users of the proposed framework [31]: (i) Institute for Energy Research (IFE): A research institute contributing to robotics security expertise and managing the overall project pilot cases. The IFE team represents IT system administrators, practitioners, and robot software developers from their robotics section. (ii) Østfold University College (HIØF): An academic research institution responsible for developing the SecuRoPS framework. As part of this team, We represent the academic research community. HIØF will provide researchers from the robotics and automation laboratory as user study participants. (iii) Fredrikstad Municipality: A public sector actor experienced in public space management, representing business owners in the consortium. They will provide a business environment (a sustainable water ferry use case) for pilot cases, where end-users needs will be studied. (iv) SNØ design: A private robot design company in Norway responsible for customizing social robot hardware to meet end-users preferences, representing the social robot designer category of targeted users. (v) Institut de Robòtica i Informàtica Industrial (IRI): An internationally renowned robotics research partner responsible for procuring the ARI social robot from PAL Robotics and customizing its human interaction design. This partner and researchers at the Perception and Manipulation Laboratory represent social robot developers for this study.

This research's expected impact and contribution to science, innovation, and society is summarized below.

Science: Currently, no security framework exists that addresses the management of threats to the dynamic environment of SRPS through continuous vulnerability, threat, and risk assessments. Given the recognized benefits of continuous risk assessment in software development, this framework is expected to be beneficial to the targeted stakeholders.

Innovation: The integration of automation in security applications for SRPS represents a significant innovative step towards developing high-performance collaborative and interactive social robots that can be widely used for different societal tasks. This disruptive innovation, which continuously incorporates vulnerability, threat, and risk assessment in its development processes, will significantly impact society and the economy.

Society: In the future, social robots will have a crucial role in critical infrastructure, essential services, major sectors, and national security. To promote acceptance and reliability, a security framework that ensures continuous vulnerability, threat, and risk assessment during the development of software products for these robots will be essential.

2 KEY RESEARCH QUESTIONS

The SecuRoPS PhD research shall address the following five Research Questions (RQ).

- **RQ1:** *How can the security of social robots in public spaces be compromised, and what are the potential vulnerabilities and threats that need to be addressed?*
- **RQ2:** *What are the best practices for conducting continuous vulnerability and threat assessments to ensure the security of social robots software in public spaces?*
- **RQ3:** *How can a security framework for social robots software be developed to integrate continuous vulnerability and threat assessments?*
- **RQ4:** *What are the essential metrics for measuring the impact of a continuous vulnerability assessment-based security framework?*
- **RQ5:** *Is the SecuRoPS framework more effective in addressing the complex security challenges posed by social robots operating in dynamic public spaces than existing methodologies, such as the MITRE security framework?*

3 RESEARCH METHODOLOGY AND WORK PLAN

3.1 Design Science Research Methodology

The SecuRoPS research will employ an iterative co-creation research and innovation process based on the Design Science Research (DSR) methodology [20] to address its research questions. Design Science Research is an appropriate fit for this thesis as its primary purpose is to develop knowledge and gain an understanding of a problem domain (in this research, knowledge of SR and it's continuously evolving threat landscape in public spaces) by building and applying practical and innovative artefacts to address identified complex problems.

The information system DSR research framework proposed by Hevner et al. [9] will be adopted, which consists of three components: **environment, design research, and knowledge base**. Three research cycles will be followed: **relevance, design, and rigour**, as presented in Figure 1. The **environment** defines the problem space of interest, which, in this case, is SRPS. It comprises *people* with different roles, capabilities, and characteristics, *organizations* with different goals, tasks, problems, and opportunities, and *technology* with diverse infrastructures, applications, communication technologies, risks, barriers, and mitigations. In the **design research** component, artefacts will be developed and evaluated through an iterative assessment and refinement process. The **knowledge base** component will comprise applicable *knowledge* on SRPS theories, patterns, frameworks, security, privacy, models, human-machine interaction - HRI, and other educational materials (security courses), *methodologies* for data collection, analysis, and evaluation, including appropriate metrics and *standards/laws* such as GDPR, NIST, ISO, and best industrial practices for SRPS in public spaces. During the **relevance cycle** (cycle 1), business needs will be matched with research objectives, focusing on software developers' needs in terms of threat landscape awareness. Feedback from assessment during the evaluation will refine the artefacts during the **design cycle** (cycle 2). The design cycle will involve at least

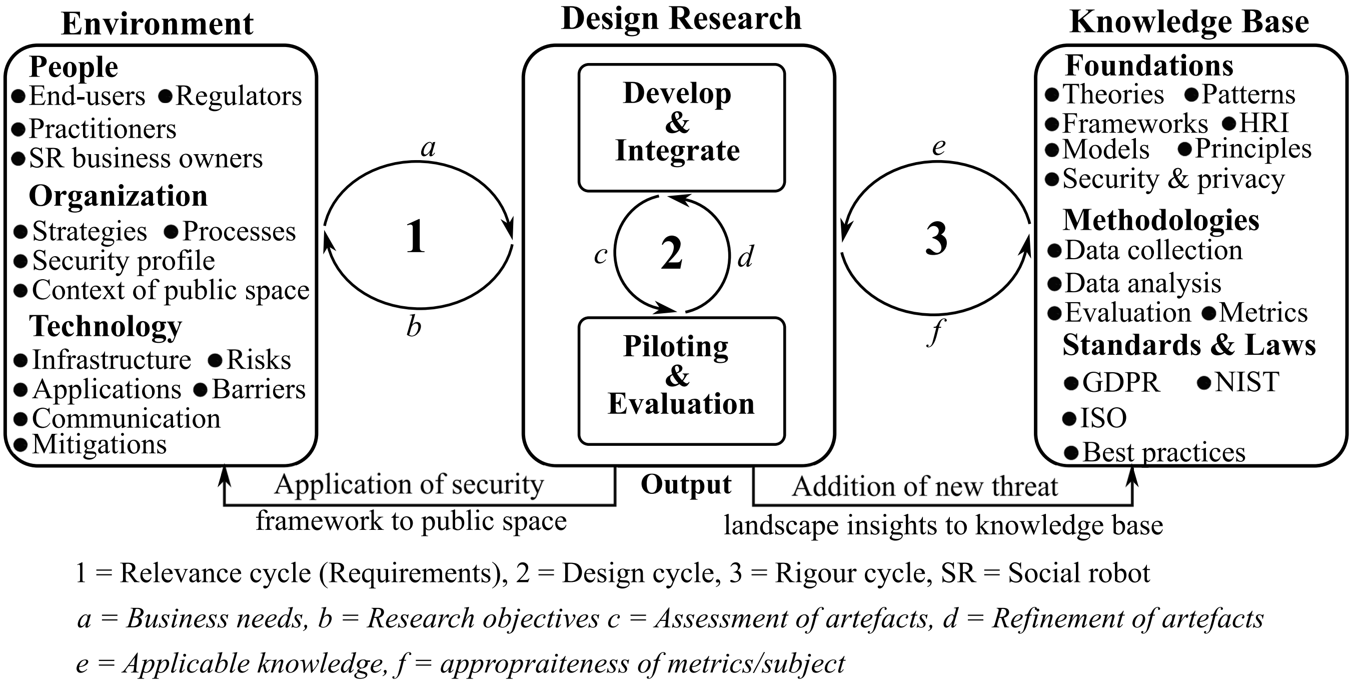

Figure 1: SecuRoPS' design science research

three iterations, each corresponding to the three versions of the security framework. During the **rigour cycle** (cycle 3), applicable knowledge will be rigorously retrieved from the existing body of knowledge and refined based on their suitability in subjects and metrics for a given problem space. Specifically, expert interviews, literature surveys, and systematic literature reviews (SLRs) will be conducted to ascertain the threat landscape concerning the seven components of SRPS. Threats related to communication networks, AI, SRPS data storage, and AI will be gathered from the literature and vulnerability reports.

3.2 Mapping DSR Guidelines and methods

This research methodology follows the guidelines for conducting Design Science Research (DSR) proposed by Hevner et al. [8]. The guidelines are summarized below:

3.2.1 Design as an artefact. In software engineering, an artefact refers to any tangible, digital, or physical item created during the software development process. It could be a document, diagram, model, specification, code file, or any other deliverable that serves a context-specific purpose and comprises a physical representation, syntactic structure, and semantic content, forming three levels of perception [15]. For this research, artefacts will be a continuous vulnerability-based security framework for SR software developers.

3.2.2 Problem relevance. This research aims to develop a technology-based solution (security framework) to address the problems faced by business users (SR software developers). The solution would ensure the security and acceptance of SRPS. The relevance of this research is evident in the fact that it addresses a business problem faced by practitioners in an emerging field while contributing to the existing knowledge base on how to manage the evolving threat landscape for SRPS.

3.2.3 Design evaluation. The usability, quality, and effectiveness of the SecuRoPS framework will be rigorously evaluated through well-executed evaluation methods, including observation, experiments, testing, and descriptive scenarios. The evaluation will include the integration of developed artefacts within the technical infrastructure of an existing business environment. The research's evaluation criteria, metrics, and research questions align with Philippou et al.'s GQM approach for information security [21]. Several criteria for evaluating a security framework include availability, security and performance as proposed by ENISA [6], security, resilience and risk as proposed by MITRE [16], and implementation, effectiveness and impact as proposed by NIST [29] will be considered in this study, and backed with measurable metrics linked to critical elements of the framework in its application domain. The SecuRoPS framework will be evaluated using the following criteria;

1. **threat and vulnerability metrics:** a measure of the number and severity of threats and vulnerabilities identified and addressed by the framework. Specific metrics under the group include the number and severity of vulnerabilities, number and frequency of attacks, detection and response time, false negatives and positives.
2. **risk management metrics** measure the framework's effectiveness in identifying and mitigating risks. Specific metrics under this category include risk exposure of the particular SR scenario.

(3) **compliance metrics:** a measure of the extent to which the security framework complies with applicable laws, regulations and standards of SRPS. Examples include the number and severity of identified compliance violations and the percentage of compliance with applicable laws and regulations.
(4) **incidence response metrics** measure the framework's ability to respond to incidents. Some applicable metrics here would be mean time to detect and respond (MTTD, MTTR), time to contain, and recovery time objective.
(5) **business impact metrics** a measure of the impact of a security incident on the business in terms of operation, customers trust and satisfaction, regulatory/legal sanctions, etc.

3.2.4 Research contributions. This research's main contribution will be the artefact, which is the continuous vulnerability-based security framework. The research will benefit users (SR software developers), society (end-users in this case, ferry passengers), and the research community (knowledge contribution in the form of SRPS continuous threat assessment and security). Identifying suitable evaluation criteria and metrics from RQ4 will also contribute to the research methodology of SRPS.

3.2.5 Research rigour. This research will apply rigorous methods in developing and evaluating the security framework. The research methods adopted to answer the research questions will be based on well-known methodologies in software engineering. The evaluation criteria and metrics will be based on software security and information system knowledge base.

3.2.6 Design as a search process. The final artefacts of DSR will contain a set of satisfactory design solutions resulting from an iterative search process involving ends, means, and applicable laws. **Ends** are requirements (utility function represented by goals and constraints); **means** are implementation design decision variables, while **applicable laws** are uncontrollable forces that can be viewed as both design variables and constants [9]. The iterative search process is between the *application domain* (involving requirements and constraints) and the *solution domain* (involving technology and organization-specific use cases). This research will adopt an iterative identification of security vulnerabilities in SRPS to find a satisfactory solution.

3.2.7 Communication of research. In accordance with the guidelines, this research aims to communicate its findings to three specific audiences: (i) technology-oriented, (ii) management-oriented, and (iii) end-users. The **technology-oriented** audience includes academic researchers, and practitioners, while management representatives and business owners are examples of the **management-oriented** audience. Academic research publications such as journal articles, conference papers, and book chapters will be the communication medium for technology-oriented audiences. In contrast, workshops and conferences will be used to reach management-oriented audiences, specifically the annual "TDS (The Digital Society) Gathering" of Østfold University College. **End-users** will be communicated with through internet blogs, the Østfold University website, social media, and the mass media (TV and newspapers).

3.3 Mapping Research Questions and Methods

To answer the research questions of this study, various methods will be employed, such as systematic literature reviews (SLRs), case studies, controlled experiments, and expert interviews, all using appropriate guidelines related to software engineering. To conduct SLRs, the procedures by Kitchenham [11] will be adopted, while the new SEGRESS guidelines will be adopted for secondary studies [12]. The guidelines by Runeson et al. [25] will be adopted for case studies and interviews. Table 1 presents the mapping of research questions to methods for this study.

Table 1: Mapping research questions with research methods

RQs	Proposed research method
RQ1	SLR, surveys and mining of vulnerability data (e.g. CVEs)
RQ2	Expert interviews and surveys
RQ3	DSR, field studies and controlled experiments
RQ4	Systematic literature review and surveys
RQ5	Field study

3.4 The SecuRoPS Framework

The primary output of this research is the SecuRoPS framework, a generic (i.e. it can be used irrespective of the software development approach) and comprehensive set of policies, procedures, controls, and tools for social robot designers and developers to create secure software using the security-by-design concept throughout the Software Development Life Cycle (SDLC), focusing on the evolving vulnerability of SRPS. The framework consists of four components: a threat model based on SRPS threat landscape insights; a list of controls for each threat category; a security profile for each SRPS use case; and practical implementation guidelines. The secure SRPS software, resulting from applying the framework within the SDLC, will feature multiple security layers, with the software code forming the innermost layer.

During three pilot studies involving ARI water ferry guide use cases, we will apply the framework to develop a secure social robot application (ROS node), emphasising secure design, implementation, threat awareness, and coding practices. The SecuRoPS framework is not a software program, security monitoring tool, or intrusion detection system but a planning tool for software developers to create secure products while considering SRPS's evolving vulnerabilities.

To develop this framework, the research will conduct systematic literature reviews, surveys, expert interviews, and field studies on SRPS. Field studies will observe and collect data on software development practices, security measures, and potential vulnerabilities in real-world settings to understand developer and user interactions, challenges, and security measure effectiveness in practical contexts.

4 DATA COLLECTION AND ANALYSIS TECHNIQUES

The data types, sources, collection methods, data analysis, validity threats and controls, the scope of work, limitations, project risks, and contingency plans for this study are detailed in the subsequent subsections.

4.1 Data types and sources

The SecuRoPS research will collect mixed data, comprising quantitative information from surveys, experiments, and field studies, as well as qualitative insights from interviews, scenario descriptions, and field studies. User study participants will be selected from the wider SecuRoPS project partners and end-users who engage with the social robot during pilot cases. While recruiting user study participants can be difficult, the target users in this instance are partners in the SecuRoPS project who have been part of the framework's design process since its inception.

4.2 Data collection

Data will be gathered through observations, controlled experiments involving the social robot and users, functionality testing, and expert-provided descriptive scenarios. Collection methods will include system logs, intrusion detection system alerts, scan results, vulnerability database mining, and other telemetry or automated data-capture tools related to software applications.

4.3 Data analysis

The research will employ data analysis tools such as Nvivo for thematic analysis of qualitative data, while Python, Matlab, or SPSS will be adopted for quantitative data analysis. Metrics will drive data analysis for each research method.

4.4 Validity Threats and Controls

The trustworthiness of the SecuRoPS framework will be ensured by controlling threats to its validity. Runeson et al. [26] identified four threats relevant to software engineering case studies: construct, internal, external, and reliability.

4.4.1 Construct validity. measures the degree to which the study measures its intended purpose. This threat arises from insufficient empirical data or mismatched interpretations between researchers and interviewees. Controls include adopting proper research guidelines, designing explicit constructs, researcher triangulation, and avoiding subject bias.

4.4.2 Internal validity. assesses whether study findings can be attributed to studied variables rather than extraneous factors. This can occur due to deliberate mistakes or researcher biases when extracting data. This study adopts the GQM approach, ensuring clear evaluation metrics driven by goals and related questions.

4.4.3 External validity. gauges the generalizability of study findings to other populations and settings. Controls to mitigate this threat include testing the framework on applicable, related pilot cases involving ARI SR.

4.4.4 Reliability. evaluates the dependence of data and analysis on specific researchers. This study adopts a rigorous, detailed research methodology with publicly available supplemental materials to mitigate reliability and repeatability threats.

Other constraints include (i) a lack of a benchmarking baseline for comparison, (ii) generalisation limitations due to unexplored SR use cases, and (iii) a lack of established data collection tools and procedures in the SRPS field. These constraints motivate this research to produce artefacts and new research directions.

4.4.5 Scope and Limitations. The scope of a research project defines its boundaries and focus areas. In contrast, the limitations refer to the constraints and weaknesses that may impact the study's results. The project aims to develop a security framework for social robot application developers, to create more security and vulnerability-conscious robotics software. The framework's application will be limited to the Linux Operating System with the Robot Operating System (ROS) framework. The programming languages covered will be C++ and Python. The research will focus on ROS node programming for ARI robots by PAL Robotics.

4.4.6 PhD Research Risks and Contingencies. Six risks have been identified with their respective impact and proposed mitigations. These include: (i) Medium risk of regulatory sanctions - obtain necessary approvals and assessments before the pilot cases; (ii) High risk of delay from partners - regular meetings with stakeholders to prevent delays; (iii) High risk of end users not participating fully - incorporate end-user opinions and preferences in use case design; (iv) Medium risk of delay in ethical and regulatory approval - obtain all approvals before the pilot cases; (v) Medium risk of social robot not performing as expected - communicate required services and functionalities to partners; and (vi) Medium risk of inadequate funds - keep the sponsor happy by ensuring quality research and meeting promised milestones.

4.5 Current Status and Next Steps

The SecuRoPS research has completed its first year, focusing mainly on requirement gathering and the threat landscape for SRPS. Our preliminary findings on RQ1 are contained in a systematic literature review on the threat landscape and attack surface of SRPS [18]. In the second year, we will investigate the best practices in this research direction and release the first version of the SecuRoPS framework, thereby addressing RQ2 and partially RQ3. In the third year, we will test, evaluate, and improve the SecuRoPS framework from practical pilot cases and answer RQ4 and RQ5. We plan to release a final version of the framework before the end of the third year.

5 SUMMARY OF POINTS FOR ADVICE

We would appreciate constructive feedback on the following from this proposal:

- **Research methods:** Are the proposed research methods sufficient to address our research questions? Are there any additional tips or advice to implement them effectively?
- **Data collection and analysis:** Is there a specific tool or approach you would recommend for this task?
- **Evaluation of the proposed SecuRoPS framework:** What do you think can be done better in this regard?

6 RELEVANT PRIOR WORK

Birk et al. [5] proposed a networking framework for Safety, Security, and Rescue Robots (SSRR) focusing on network security. Shyvakov

[28] suggested a security framework for general robots using four-layer and four-level security protection approaches but did not provide test and evaluation results. Basan et al. [3] offered a security framework for robotic control systems with seven security levels and six degrees of protection but lacked evaluation and practical application. Baraka et al. [2] characterised social robots' appearance and design space without addressing security and privacy. Tonkin [32] investigated socially responsible design for social robot public spaces from a User Experience (UX) and HRI perspective but did not address privacy and security. None of these works addressed the challenges social robot software developers face in dealing with the continuously evolving threat landscape during application development, which this research aims to address.

ACKNOWLEDGMENTS

This paper is funded by the Research Council of Norway under the SecuRoPS project "User-centered Security Framework for Social Robots in Public Spaces" with project code 321324.

REFERENCES

[1] Hala Assal and Sonia Chiasson. 2019. 'Think Secure from the Beginning': A Survey with Software Developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300519

[2] Kim Baraka, Patrícia Alves-Oliveira, and Tiago Ribeiro. 2020. An Extended Framework for Characterizing Social Robots. In *Human-Robot Interaction: Evaluation Methods and Their Standardization*, Céline Jost, Brigitte Le Pévédic, Tony Belpaeme, Cindy Bethel, Dimitrios Chrysostomou, Nigel Crook, Marine Grandgeorge, and Nicole Mirnig (Eds.). Springer International Publishing, Cham, 21–64. https://doi.org/10.1007/978-3-030-42307-0_2

[3] Elena Basan, Anton Gritsynin, and Tatyana Avdeenko. 2019. Framework for Analyzing the Security of Robot Control Systems. In *2019 International Conference on Information Systems and Computer Science (INCISCOS)*. IEEE, Quito, Ecuador, 354–360. https://doi.org/10.1109/INCISCOS49368.2019.00062

[4] Tony Belpaeme, James Kennedy, Aditi Ramachandran, Brian Scassellati, and Fumihide Tanaka. 2018. Social Robots for Education: A Review. *Science Robotics* 3, 21 (Aug. 2018), eaat5954. https://doi.org/10.1126/scirobotics.aat5954

[5] Andreas Birk, Sören Schwertfeger, and Kaustubh Pathak. 2009. A Networking Framework for Teleoperation in Safety, Security, and Rescue Robotics. *IEEE Wireless Communications* 16, 1 (Feb. 2009), 6–13. https://doi.org/10.1109/MWC.2009.4804363

[6] ENISA. 2011. *Measurement Frameworks and Metrics for Resilient Networks and Services: Technical Report.* Technical Report. ENISA. 119 pages. https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport

[7] Eduard Fosch-Villaronga, Christoph Lutz, and Aurelia Tamò-Larrieux. 2020. Gathering Expert Opinions for Social Robots' Ethical, Legal, and Societal Concerns: Findings from Four International Workshops. *International Journal of Social Robotics* 12, 2 (May 2020), 441–458. https://doi.org/10.1007/s12369-019-00605-z

[8] Alan Hevner and Samir Chatterjee. 2010. Design Science Research in Information Systems. In *Design Research in Information Systems: Theory and Practice*, Alan Hevner and Samir Chatterjee (Eds.). Springer US, Boston, MA, 9–22. https://doi.org/10.1007/978-1-4419-5653-8_2

[9] Alan R Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. 2004. Design Science in Information Systems Research. *MIS Quarterly* 28, 1 (2004), 77–105. https://www.in.th-nuernberg.de/professors/Holl/Personal/Hevner_DesignScience_ISRes.pdf

[10] Rafiq Ahmad Khan, Siffat Ullah Khan, Habib Ullah Khan, and Muhammad Ilyas. 2022. Systematic Literature Review on Security Risks and Its Practices in Secure Software Development. *IEEE Access* 10 (2022), 5456–5481. https://doi.org/10.1109/ACCESS.2022.3140181

[11] Barbara Kitchenham. 2004. Procedures for Performing Systematic Reviews. *Keele University Technical Report TR/SE-0401* 33 (2004), 1–26.

[12] Barbara Kitchenham, Lech Madeyski, and David Budgen. 2023. SEGRESS: Software Engineering Guidelines for REporting Secondary Studies. *IEEE Transactions on Software Engineering* 49, 3 (March 2023), 1273–1298. https://doi.org/10.1109/TSE.2022.3174092

[13] Maria Kyrarini, Fotios Lygerakis, Akilesh Rajavenkatanarayanan, Christos Sevastopoulos, Harish Ram Nambiappan, Kodur Krishna Chaitanya, Ashwin Ramesh Babu, Joanne Mathew, and Fillia Makedon. 2021. A Survey of Robots in Healthcare. *Technologies* 9, 1 (March 2021), 8. https://doi.org/10.3390/technologies9010008

[14] Giovanni Mazzeo and Mariacarla Staffa. 2020. TROS: Protecting Humanoids ROS from Privileged Attackers. *International Journal of Social Robotics* 12, 3 (July 2020), 827–841. https://doi.org/10.1007/s12369-019-00581-4

[15] Daniel Méndez Fernández, Wolfgang Böhm, Andreas Vogelsang, Jakob Mund, Manfred Broy, Marco Kuhrmann, and Thorsten Weyer. 2019. Artefacts in Software Engineering: A Fundamental Positioning. *Software & Systems Modeling* 18, 5 (Oct. 2019), 2777–2786. https://doi.org/10.1007/s10270-019-00714-3

[16] MITRE. 2018. *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods.* Technical Report AD1108019. MITRE, United States. 119 pages.

[17] Nikola Naumov. 2019. The Impact of Robots, Artificial Intelligence, and Service Automation on Service Quality and Service Experience in Hospitality. In *Robots, Artificial Intelligence, and Service Automation in Travel, Tourism and Hospitality*, Stanislav Ivanov and Craig Webster (Eds.). Emerald Publishing Limited, Emerald Publishing Limited, Bingley, 123–133. https://doi.org/10.1108/978-1-78756-687-320191007

[18] Samson O. Oruma, Mary Sánchez-Gordón, Ricardo Colomo-Palacios, Vasileios Gkioulos, and Joakim K. Hansen. 2022. A Systematic Review on Social Robots in Public Spaces: Threat Landscape and Attack Surface. *Computers* 11, 12 (Dec. 2022), 181. https://doi.org/10.3390/computers11120181

[19] Batuhan Özdol, Elif Köseler, Ezgi Alçiçek, Süha Eren Cesur, Perif Jan Aydemir, and Şerif Bahtiyar. 2021. A Survey on Security Attacks with Remote Ground Robots. *El-Cezeri* 8, 3 (Sept. 2021), 1286–1308. https://doi.org/10.31202/ecjse.916532

[20] Ken Peffers, Tuure Tuunanen, Charles E Gengler, Matti Rossi, and Wendy Hui. 2006. THE DESIGN SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH. *Proc. of First International Conference on Design Science Research in Information Systems and Technology* (2006), 83–106. https://doi.org/10.48550/arXiv.2006.02763

[21] Eleni Philippou, Sylvain Frey, and Awais Rashid. 2020. Contextualising and Aligning Security Metrics and Business Objectives: A GQM-based Methodology. *Computers & Security* 88 (Jan. 2020), 101634. https://doi.org/10.1016/j.cose.2019.101634

[22] Samantha Reig, Michal Luria, Elsa Forberger, Isabel Won, Aaron Steinfeld, Jodi Forlizzi, and John Zimmerman. 2021. Social Robots in Service Contexts: Exploring the Rewards and Risks of Personalization and Re-embodiment. In *Designing Interactive Systems Conference 2021 (DIS '21)*. Association for Computing Machinery, New York, NY, USA, 1390–1402. https://doi.org/10.1145/3461778.3462036

[23] Research and Markets. 2022. Global Social Robots Market - Growth, Trends, COVID-19 Impact, and Forecasts (2022 - 2027). https://www.researchandmarkets.com/reports/5120156/global-social-robots-market-growth-trends.

[24] Sean Rivera and Radu State. 2021. Securing Robots: An Integrated Approach for Security Challenges and Monitoring for the Robotic Operating System (ROS). In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, Bordeaux, France, 754–759.

[25] Per Runeson and Martin Höst. 2009. Guidelines for Conducting and Reporting Case Study Research in Software Engineering. *Empirical Software Engineering* 14, 2 (April 2009), 131–164. https://doi.org/10.1007/s10664-008-9102-8

[26] Per Runeson, Martin Höst, Austen Rainer, and Björn Regnell. 2012. *Case Study Research in Software Engineering: Guidelines and Examples* (first ed.). Wiley, Hoboken, New Jersey. https://doi.org/10.1002/9781118181034

[27] Pericle Salvini, Diego Paez-Granados, and Aude Billard. 2021. On the Safety of Mobile Robots Serving in Public Spaces: Identifying Gaps in EN ISO 13482:2014 and Calling for a New Standard. *ACM Transactions on Human-Robot Interaction* 10, 3 (July 2021), 19:1–19:27. https://doi.org/10.1145/3442678

[28] Oleksandr Shyvakov. 2017. *Developing a Security Framework for Robots.* Master's thesis. University of Twente.

[29] M Swanson, N Bartol, J Sabato, J Hash, and L Graffo. 2003. *Security Metrics Guide for Information Technology Systems* (zeroth ed.). Technical Report NIST SP 800-55. National Institute of Standards and Technology, Gaithersburg, MD. NIST SP 800–55 pages. https://doi.org/10.6028/NIST.SP.800-55

[30] Mohammad Tahaei and Kami Vaniea. 2019. A Survey on Developer-Centred Security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Stockholm, Sweden, 129–138. https://doi.org/10.1109/EuroSPW.2019.00021

[31] The Research Council of Norway. 2021. User-Centred Security Framework for Social Robots in Public Space (SecuRoPS) - Prosjektbanken. https://prosjektbanken.forskningsradet.no/project/FORISS/321324.

[32] Margaret V. Tonkin. 2020. *Socially Responsible Design for Social Robots in Public Spaces.* Ph. D. Dissertation. University of Technology Sydney.