University of Tartu
Institute of Computer Science
Cybersecurity Curriculum

Joosep Parts

Cyber security risks in telepresence robotics within higher education and their mitigation

Master's Thesis (21 ECTS)

Supervisor: Kaido Kikkas, PhD

Tartu 2023

Cyber security risks in telepresence robotics within higher education and their mitigation

Abstract:
Telepresence robotics (TRPs) have become increasingly popular, particularly in higher education systems, as they enable users to remotely partake in events. However, this increased usage also presents potential security risks specific to TRPs, such as cyber-physical risks, and exposure of sensitive data among other risks. Current risk assessment models do not adequately address these unique concerns, leading to a gap in understanding and mitigating TRPs related risks. This thesis aims to map potential security issues, offer mitigation strategies for found weaknesses, and bridges the gap by conducting case studies and expert interviews. This research will provide organizations utilizing TRPs with a better understanding of security risks and effective solutions to protect their systems and users.

Keywords: Cyber security, risk assessment, telepresence robotics

CERCS: T120 System technology, computer technology

Küberturvalisuse riskid kaugosalus robootikas kõrgharidussüsteemis ja nende vähendamine

Lühikokkuvõte:
Kaugosalus robotid on muutunud üha populaarsemaks, eriti kõrgemas haridussüsteemis, kuna need võimaldavad kasutajatel osaleda üritustel kaugjuhtimise teel. Siiski kaasnevad selle suurenenud kasutamisega ka kaugosalus robotitele omased potentsiaalsed turvariskid, nagu näiteks küber-füüsiline kohalolek ning tundliku info lekke. Praegused riskihindamise mudelid ei käsitle piisavalt neid ainulaadseid probleeme, ning on olemas lünk seotud riskide mõistmisel ja nende leevendamisel. Käesoleva magistritöö eesmärk on kaardistada potentsiaalsed turvaprobleemid ja pakkuda leitud nõrkuste leevendamiseks strateegiaid ning ületada lünk, viies läbi juhtumiuuringuid ja ekspert intervjuusid. See uurimus annab kaugosalus roboteid kasutavatele organisatsioonidele parema arusaama turvariskidest ja tõhusatest lahendustest nende süsteemide ja kasutajate kaitsmiseks.

Keywords: Küberturvalisus, riskianalüüs, kaugosalus robootika

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

List of Abbreviations and Terms

HE Higher Education

HEI Higher Education Institutions

ICT Information and Communication Technology

SEN Special Education Needs

TRPs Telepresence robotics

UI User interface

Contents

1 Introduction

1.1 Problem Statement

With the increasing popularity of TRPs in higher education systems, enabling users to remotely partake in events, new security risks which could be characterized specific to TRPs have emerged [1–4]. These risks include abuse of privilege, unauthorized access, cyber-physical risks, and exposure of sensitive data among other risks [3, p. 120]. However, current risk assessment models do not adequately address these unique concerns, resulting in a knowledge gap in understanding and mitigating TPR-related risks [3]. This master's thesis aims to explore potential security issues associated with TRPs and propose methods to mitigate them by reviewing the state of art, conducting case studies and interviewing experts.

The research will involve identifying and validating potential risks through case studies and expert interviews, with a focus on identifying cybersecurity risks TRPs may pose to higher education systems. By proposing mitigation strategies and emphasizing cybersecurity, this study seeks to provide organizations utilizing TRPs with a better understanding of security risks and effective solutions to protect their systems and users. Ultimately, this research will contribute to bridging the gap between existing knowledge and the unique security concerns presented by the growing use of TRPs in higher education systems.

1.2 Objectives and Roadmap

1.2.1 Research Objective

The primary objective of this thesis is to identify cybersecurity risks related to organizations using TRPs and propose mitigation strategies to reduce the identified risks, focusing on user data security.

1.2.2 Research Questions

RQ: To what kind of security risks are organisations using TRPs exposed to, and how to mitigate the risks?

The main research question is divided into three different how questions, the potential security risks posed by TRPs, how organisations have assessed the potential risks and the solutions that can be provided to reduce the identified risks. The following sub-research questions are formulated in sequential order according to their importance:

1. **RQ1**: What are the potential security risks posed by TRPs, and how do these risks uniquely impact organizations utilizing these systems?

2. **RQ2**: How have organizations implemented assessment and management strategies to address cybersecurity risks associated with telepresence robotics?

3. **RQ3**: What potential solutions can be provided to reduce identified security risks?

RQ1: Identification of potential security risks posed by TRPs is the first step. In this step the possible security risks will be identitified by analyzing existing frameworks, migigation strategies and previous works in the field. This sub-research question focuses on uncovering the distinct security risks associated with telepresence robotics and examines their implications for organizations that deploy TRPs. By identifying these risks, the research will contribute to a comprehensive understanding of the challenges and vulnerabilities that need to be addressed in order ensure secure operation of TRPs systems. This exploration will consider various aspects of TRPs, such as remote connectivity, cyber-physical presence, and live video and audio feeds, to highlight the unique security concerns that arise from their use. Additionally, the research will investigate how these risks may differ from those faced by organizations using other types of robotics and what factors contribute to the increased vulnerability of TRPs systems.

RQ2: Once we have identified possible security risks the next step is to examine how have organizations implemented assessment and management strategies to address cybersecurity risks associated with TRPs? This sub-research question focuses on understanding the mechanisms and processes involved in managing TRPs systems. Finding the issues and gaps in current implementation is important to validate found security risks from teoretical material, but is also important before appropriate mitigation strategies can be considered. Addressing this question is essential for identifying potential vulnerabilities and areas where security improvements can be made.

RQ3: Following the identification of security risks associated with TRPs, this sub-research question concentrates on investigating and proposing potential mitigation strategies that effectively address the recognized risks. The study will explore a range of solutions, including technological advancements, policy implementation, and organizational practices, to provide a comprehensive understanding of how organizations can secure their TRPs systems. The proposed solutions should be practical, effective to the needs of organizations using TRPs. This will involve considering the unique security risks posed by TRPs and the distinct contexts in which they are deployed. The focus will be on user data security and the interaction between external users and TRPs, ensuring that the proposed mitigation strategies safeguard sensitive information and maintain the privacy and security of all parties involved.

By addressing these three sub-research questions, the thesis aims to provide a comprehensive understanding of the security risks faced by organizations using TRPs and offer practical solutions for mitigating these risks, ultimately contributing to a more secure and reliable TRPs environment.

1.2.3 Roadmap and Structure

To achieve the research objective, the following roadmap and structure will be followed:

1. Literature Review and analysis: A comprehensive review of existing research on TRPs, risk assessment models, and related frameworks will be conducted to identify potential issues within TRPs systems.
2. Case Studies: Case studies will be conducted to validate existence of possible security risks by analyzing real-life scenarios involving TRPs usage in organizations;
3. Expert Interviews: Interviews with technical staff who have experience in integrating TRPs into organizations will be conducted to confirm the identified risks and explore possible mitigation strategies proposed by the experts;
4. Data Analysis and Proposed Mitigation Strategies: The findings from case studies and expert interviews will be analyzed to identify potential security concerns and risks posed by TRPs, as well as potential solutions to these risks;
5. Conclusion: The thesis will conclude by summarizing the key findings, discussing the limitations of the research, and suggesting avenues for future research.

Following this roadmap, the thesis will contribute to bridging the gap between existing cybersecurity knowledge regarding robotics in higher education systems and the unique security concerns presented by the growing use of TRPs.

1.3 Preliminaries

2 Background / State of the Art

The rapid growth of technology, multimedia, and robotics has led to significant advancements in Information and Communication Technology (ICT) infrastructure worldwide, prompting the development of various educational programs. The evolution of technology has boosted the field of robotics, resulting in a wide array of potential applications in Higher Education (HE). The use of robotics in education is increasing, with TRPs being applied in Higher Education Institutions (HEI), and other diverse roles in the industry [5; 6].

TRPs have great potential for pedagogic reasons within education at all levels, as they benefit HE personnel the replacement of physical presence and allow students with Special Education Needs (SEN) have access to education they might miss otherwise due to their disabilities [5, p. 546]. TRPs have ability to create interaction between individuals which can be an opportunity for learning not only from a three-dimensional inanimate object but also through interaction with other people. This interaction enables TRPs to aid in improving social skills in individuals with disabilities [5, p. 541].

Although the advantages of TRPs in education are numerous, this technology also creates new possible security risks that need to be assessed. Interconnectivity with TRPs by the internet to the HEI means that the organization needs to be aware of possible security risks [3, p. 120]. Cybersecurity is crucial in HEI due to the vast amount of computing power and access to other resources universities have. These institutions hold large volumes of personal, financial, and intellectual data that can be attractive targets for cybercriminals.

It is inherently difficult to ensure security within robotics systems due to the complexity of robotic systems in general, which leads to wide attack surfaces and a variety of potential attack vectors [4, p. 2]. In addition, robotics manufactures often struggle to mitigate vulnerabilities in reasonable time periods [4, p. 12]. The lack of investment in cybersecurity and the immature state of the field in robotics cybersecurity contribute to the challenges in securing robotic systems [4, p. 12]. Most current robots are vulnerable, and defensive approaches are struggling to keep up with the need for security [4, p. 12]. Therefore it is reasonable to assume that TRPs are also vulnerable to similar security risks. Though there exists a veriety of risk assessment models, frameworks and methodolgies to assess cybersecurity risks within robotics systems in general, the studies which focus on TRPs usage in HEI are limited and scattered.

Because of the lack of research on TRPs in HEI regarding cybersecurity risks, and the usage of TRPs is increasing, this thesis aims to bridge the gap in the literature by providing a comprehensive review on the state of the art of TRPs cybersecurity risks in HEI and offers possible mitigation strategies for identified cybersecurity risks.

2.1 Related Work

2.2 Telepresence Robotics

2.3 Cyber Security Risks in Robotics

2.4 Existing Risk Assessment Models

3 Data Analysis

3.1 Identified Security Risks in TPRs

3.2 Existing risk assessment and management strategies

3.3 Proposed Mitigation Strategies

4 Case Study: TalTech IT College (ICO)

4.1 Context and TRPs Deployment

4.2 Results and Findings

4.3 Recommendations

5 Expert Interviews

5.1 Participant Selection

5.2 Interview Results

5.3 Expert Validation and Proposed Solutions

6 Contribution

6.1 Research method

Primarily focus is on exploring and understanding the cybersecurity risks, and the underlying perspectives of the participants involved in HEI where TRPs have been deployed. Given the nature of the study, the absence of known empirical data, and the limited time for conducting case studies, a qualitative research approach will help to gain deeper insights. Thus it is important to develop a review protocol which sets the framework for conducting a thorough and unbiased review of the literature [7, p. 8]. It ensures that systematic and rigorous approach is followed, which enhances the credibility and reliability of the review. Following review protocol steps helps to minimize the risk of bias in the review process by establishing predefined criteria for study selection, quality assessment, and data extraction:

1. Establish the background and context of the study;
2. Formulate clear and specific research questions;
3. Define the search strategy, including search terms and resources to be used;
4. Set the study selection criteria and procedures;
5. Develop study quality assessment checklists and procedures;
6. Design a data extraction strategy tailored to the research questions;
7. Plan the synthesis of the extracted data, including descriptive and quantitative methods, as appropriate;
8. Outline a dissemination strategy for the review findings;
9. Set a project timetable to ensure timely completion of the review [7, pp. 4–5].

6.2 Search strategy

Search strategy was developed to identify relevant literature for this review following the search strategy generation guidelines [7, pp. 7–8]. Search strategy for the following thesis consists of 3 steps:

1. Generation of keywords and search terms;
2. The use of search filters;
3. Selection of credible sources.

Keywords: Initially, the search keywords were created by breaking down the research questions into their main concepts. A list of search terms and phrases related to each key concept was generated by applying term harvesting to each research question. Main keywords were complemented by secondary keywords (synonyms), alternative spellings, and related terms to ensure a comprehensive search. The result was a list of search terms and phrases used to query the databases. To narrow down the search, the terms were combined using Boolean operators (where applicable).

Table 1. Selected keywords and synonyms

Primary keywords	**Secondary keywords**
telepresence	telerobotics, tele-education
robotics	robot
cybersecurity	cyber, security, digital
risks	compromise, assessment
education	organization

Filters: The search filters were used to limit the search to the relevant studies. Most common filters used were: publication date, type of publication, discipline and language. The filters were applied to the search results to ensure that only relevant studies were included in the review. Most important filter being the publication year. The search was limited to the last 10 years (2014-2023) to ensure that only the most recent and relevant studies were included in the review. Primary studies were limited to maximum age of 5 years and secondary studies to maximum age of 10 years. Search filters of primary studies complemented the secondary seach filters. Secondary studies were extended to other languages than English (incl. Estonian).

Table 2. Used search filters

Primary studies			**Secondary studies***		
Date Range	Type	Discipline	Date Range	Type	Discipline
2019…2023	Reports, Journals, Experiments, Datasets	Computer Science, Engineering	2014…2023	Articles, Conference Proceedings, Whitepapers	Social Sciences, Psychology

* Includes primary search terms

Sources: After conducting preliminary searches using chosen search terms, and filters in the selected resources, search queries were refined as needed to obtain required materials. Preliminary searches showed that using main keywords in serch strategy produced large number of results but highly relevant studies, thus the use of secondary keywords was not optimal in search for primary studies. Record the search terms used and the number

of results obtained from each resource was recorded for later use to check for updates on the subject. Most filtering refinements were done in User interface (UI). To identify relevant research several databases were queried with the same search terms. Database selection was based on the main category of hosted works (technology), the number of publications published and the age of the portal. In the execution phase main databases were (SpringerLink, IEEExplore, Scopus, ScienceDirect, Web of Science) due to their large number of publications and relvance on the topic. Initial queries yeilded small number of results, thus the search was extended to secondary sources (LISTA, Frontiers, Google Scholar).

Table 3. Selected sources in order of relevance

	Publisher	**Metrics**	**Year**	**Topics**
1	SpringerLink	1,200 journals	1996	Computer science, Engineering, Environment
2	IEEExplore	5,360,654 articles	2000	Computer science, Electrical Engineering and Electronics
3	Scopus	34,346 journals	2004	Life sciences, Social Sciences, Physical Sciences
4	ScienceDirect	15,000,000 articles	1997	Physical Sciences and Engineering, Life Sciences
5	Web of Science	200 million records	1998	Physical Sciences, Technology, Life Sciences &Biomedicine
6 *	LISTA	513 million records	2005	Automation, Classification, Electronic resources and ERM systems
7 *	Frontiers	185 academic journals	2007	Education, Computer Science, Robotics and AI
8 *	Google Scholar	389 million records	2004	Various topics

* Secondary sources

Search scope default language selection was English. Examples of search search string composition used with combination of search terms, filters on the selected resources can be seen in Table 4. The search string used all possible combinations. Preliminary searches showed that using main keywords yielded best results.

Table 4. Composition of search strings

#	**String**
1	telepresence AND cybersecurity OR risks AND assessment AND robots AND education
2	tele-robotics AND cybersecurity AND risks AND robots OR education AND assessment AND compromise OR mitigation
2	telepresence AND cybersecurity AND risks AND assessment AND robots AND education AND management AND mitigation AND security AND compromise

The databases used in this study contained scientific journals, conference proceedings, books, and trade journal articles. The sole limitation imposed was that the analyzed articles had to be in English. In April 2023, the database search was conducted, yielding a total of 778 publications. Some references were found in multiple databases. To eliminate duplicates, a unified list featuring the titles of the chosen publications was created. The abstracts of these publications were reviewed to confirm their relevance to product design and development. After implementing this exclusion criterion, 10 publications were chosen for more in-depth analysis as seen in Table 5.

Table 5. Number of selected studies found primary search stategy

		Journal		**Conference Paper**		**Book Chapter**		**Whitepaper**	
Year	**Total**	**T**	**S**	**T**	**S**	**T**	**T**	**S**	**T**
2014	14	6		6		2			
2015	6	5		3		2			
2016	3	5				1			
2017	11	11		5		1			
2018	14	19		3		6			
2019	34	36	1	15		9			
2020	50	60	1	16		20			
2021	174	89	5	60	1	88			
2022	252	89	2	95		131			
2023	97	30		34		52		1	

* T - total, S - selected

6.3 Selection of primary and secondary studies

To identify primary studies that provide direct evidence about the research question, specific selection criteria was defined during the protocol definition stage. Although criteria was refined during the search process, it served as a foundation for identifying relevant studies. The selection criteria included factors such as study design, levels of evidence, and outcome measures, ensuring that the chosen studies directly addressed our research question [7, pp. 10–16]. TRPs in the context of cybersecurity and education is a relatively new field of robotics with most research starting from 2015. Therefore, the selection of primary studies was extended to include secondary studies that provide indirect evidence about the research question.

In the context of assessing cybersecurity risks in telepresence robotics for higher education systems, the literature analysis process identified 7 key findings that directly influence the assessment of cybersecurity risks in HEI or in other ways support the answering of research questions. Among these studies, it was taken into account that

secondary studies within the timerange of 2014. . . 2023 may have outdated information and as such their findings were noted and used as supportive information. Throughout the discussion of each study, the aspects related to cyber security risks in TRPs are highlighted. Table 6 lists findings and the corresponding references:

1. Identification of security risks associated with TRPs.
2. Analysis of existing risk assessment models and their limitations in addressing TRPs-specific security challenges.
3. Potential security vulnerabilities in robotics, including hardware, software, and network-related issues.
4. Usage of TRPs in HEI.
5. Examination of studies that highlight TRPs security incidents and the effectiveness of implemented countermeasures.
6. Exploration of future research directions to enhance the security of TRPs in higher education and other settings.
7. Investigation of mitigation strategies and best practices to address identified weaknesses in TRPs security.

Table 6. Selected sources

#	Evidence level	Year	References	1	2	3	4	5	6	7
1	5	2021	Lacava et al. [2]	X					X	
2	5	2022	Yaacoub et al. [3]	X	X	X		X	X	X
3	5	2020	Pessoa et al. [8]					X	X	
4	5	2021	Zhu et al. [9]	X	X			X		X
5 *	5	2022	Lei et al. [1]				X			
6 *	5	2022	Mayoral-Vilches [4]			X		X		
7 *	5	2022	Leoste et al. [6]				X			
8 *	5	2018	Vilches et al. [10]	X						
9 *	5	2020	Singar et al. [11]				X			X
10*	5	2019	Reis et al. [5]				X			

* Secondary studies

6.4 Extracted data

7 Validation

7.1 Experimental validation

8 Conclusion

8.1 Summary

8.2 Implications for TRPs Users and Organizations

8.3 Limitations and Future Research

Time, resources, nr of case studies and access to experts are the main limitations of this research.

References

[1] M. Lei, I. Clemente, H. Liu, and J. Bell, "The acceptance of telepresence robots in higher education," *International Journal of Social Robotics*, vol. 14, pp. 1–18, Jun. 2022. DOI: 10.1007/s12369-021-00837-y.

[2] G. Lacava *et al.*, "Cybsersecurity issues in robotics.," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 12, no. 3, pp. 1–28, 2021.

[3] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, pp. 1–44, 2022.

[4] V. Mayoral-Vilches, "Robot cybersecurity, a review," *International Journal of Cyber Forensics and Advanced Threat Investigations*, 2022.

[5] A. Reis, M. Martins, P. Martins, J. Sousa, and J. Barroso, "Telepresence robots in the classroom: The state-of-the-art and a proposal for a telepresence service for higher education," in May 2019, pp. 539–550, ISBN: 978-3-030-20953-7. DOI: 10.1007/978-3-030-20954-4_41.

[6] J. Leoste, S. Virkus, A. Talisainen, K. Tammemäe, K. Kangur, and I. Petriashvili, "Higher education personnel's perceptions about telepresence robots," *Frontiers in Robotics and AI*, vol. 9, 2022, ISSN: 2296-9144. DOI: 10.3389/frobt.2022.976836. [Online]. Available: https://www.frontiersin.org/articles/10.3389/frobt.2022.976836.

[7] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, Aug. 2004.

[8] M. Pessoa and J. Jauregui-Becker, "Smart design engineering: A literature review of the impact of the 4th industrial revolution on product design and development," *Research in Engineering Design*, vol. 31, pp. 1–21, Apr. 2020. DOI: 10.1007/s00163-020-00330-z.

[9] Q. Zhu, S. Rass, B. Dieber, V. M. Vilches, *et al.*, "Cybersecurity in robotics: Challenges, quantitative modeling, and practice," *Foundations and Trends® in Robotics*, vol. 9, no. 1, pp. 1–129, 2021.

[10] V. M. Vilches *et al.*, "Introducing the robot security framework (rsf), a standardized methodology to perform security assessments in robotics," *CoRR*, vol. abs/1806.04042, 2018. arXiv: 1806.04042. [Online]. Available: http://arxiv.org/abs/1806.04042.

[11] A. Singar and K. Akhilesh, "Role of cyber-security in higher education," in Jan. 2020, pp. 249–264, ISBN: 978-981-13-7138-7. DOI: 10.1007/978-981-13-7139-4_19.

Appendix

I. Data collected from case study

II. Interview Guide and Consent Form

III. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Joosep Parts**,
*(*author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Cyber security risks in telepresence robotics within higher education and their mitigation,
   *(*title of thesis)

   supervised by Kaido Kikkas.
   *(*supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Joosep Parts
08/04/2023