University of Tartu
Institute of Computer Science
Cybersecurity Curriculum

Joosep Parts

# Cyber security risks in telepresence robotics and their mitigation

Master's Thesis (21 ECTS)

Supervisor: Kaido Kikkas, PhD

Tartu 2023

## Cyber security risks in telepresence robotics 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 remote connections, cyber-physical presence, and live video and audio feeds. 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 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 kaugühendus, küber-füüsiline kohalolek ning reaalajas video- ja heliside. 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

**TRPs** Telepresence robotics

# Contents

# 1 Introduction

Todo

## 1.1 Problem Statement

With the increasing popularity of TRPs in higher education systems, enabling users to remotely partake in events, new security risks specific to TRPs have emerged. These risks include remote connection, cyber-physical presence, and live video and audio feed vulnerabilities. However, current risk assessment models do not adequately address these unique concerns, resulting in a knowledge gap in understanding and mitigating TPR-related risks. This master's thesis aims to explore potential security issues associated with TRPs and propose methods to mitigate them by incorporating existing frameworks, such as RSF, CIA, OCTAVE A, ISO27005, and NSMROS.

The research will involve identifying and validating potential risks through case studies and expert interviews, with a focus on user data security. By proposing mitigation strategies and emphasizing user data security, 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 risk assessment models 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

None?

# 2 Background / State of the Art

## 2.1 Telepresence Robotics

## 2.2 Cyber Security Risks in Robotics

## 2.3 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 underlying perspectives, and experiences of the participants involved where TRPs have been deployed. Given the nature of the study, the absence of 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. It ensures that systematic and rigorous approach is followed, which enhances the credibility and reliability of the review. Following review protocol 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. [1, pp. 4–5]

## 6.2 Search strategy

Search strategy was developed to identify relevant literature for this review following the search strategy generation guidelines [1, 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 terms were complemented by synonyms, alternative spellings, acronyms, and related terms to ensure a comprehensive search. To narrow down the search, the terms were combined using Boolean operators (where applicable). The result was a list of search terms and phrases used to query the databases.

**Filters:** The search filters were used to limit the search to the relevant studies. Most common filters used were: publication year, language, and type of publication. 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 (2013-2023) to ensure that only the most recent and relevant studies were included in the review. Primiary studies were limited to maximum age of 5 years and secondary studies to maximum age of 10 years.

**Sources:** 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. were:

Table 1. Selected sources in order of relevance

| | **Publisher** | **Metrics** | **Topics** | **Foundation** |
|---|---|---|---|---|
| 1 | SpringerLink | 1,200 journals | Computer science, engineering, environment | 1996 |
| 2 | IEEExplore | 5,360,654 articles | Computer science, electrical engineering and electronics | 2000 |
| 3 | Scopus | 34,346 journals | Life sciences, social sciences, physical sciences | 2004 |
| 4 | ScienceDirect | 15,000,000 articles | Physical Sciences and Engineering, Life Sciences | 1997 |
| 5 | Web of Science | 200 million records | Physical Sciences, Technology, Life Sciences & Biomedicine | 1998 |
| 6 | LISTA | 513 million records | Automation, Classification, Electronic resources and ERM systems | 2005 |
| 7 | Google Scholar | 389 million records | Various topics | 2004 |

After conducting preliminary searches using chosen search terms, and filters in the selected resources, search queries were refined as needed to obtain required materials. Record the search strings used and the number of results obtained from each resource was recorded for later use to check for updates on the subject.

# 7 Validation

## 7.1 Experimental validation

# 8 Conclusion

## 8.1 Summary

## 8.2 Related work

## 8.3 Implications for TRPs Users and Organizations

## 8.4 Limitations and Future Research

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

# References

[1] Barbara Kitchenham. “Procedures for Performing Systematic Reviews”. In: *Keele, UK, Keele Univ.* 33 (Aug. 2004).

# 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 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
***06/04/2023***