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(s): Kaido Kikkas

Tartu 2023

Table of Contents

[Introduction 3](#_Toc129425092)

[1 Terms and Notations 6](#_Toc129425093)

[2 Background 7](#_Toc129425094)

[3 Literature review 8](#_Toc129425095)

[Conclusions 9](#_Toc129425096)

[References 10](#_Toc129425097)

[Appendix 11](#_Toc129425098)

[I. Glossary 11](#_Toc129425099)

[II. License 12](#_Toc129425100)

# Introduction

Telepresence robotics (TPRs) represent a unique segment of remotly controlled robotics which allow users to remotly partake events. Usually, such robots are connected to organisation network over internet and they use integrated tablets to provide video and audio capabilities. The market for such robotics has been on a steady incline which spiked in 2020 (COVID-19 impact), and the forecast shows that the market is growing. More recently, higher education systems have begun integrating such systems to enhance virtual transnational education [1]. This increase in the usage of TPRs in the near future of the education system also means the possible security risks associated with TPRs it will also increase.

General-purpose domestic robotics security concerns could be categorized into four categories: physical, network, OS, and application security [1]. In that sense, telepresence robotics share common ground with general-purpose robotics regarding security concerns. Key differences between TPRs and other robotics are how users interact with the robot and how they inadvertently expose themselves through the system. This creates the need for greater user privacy and data security. According to Verizon 2022 Data Breach Investigation Report (DBIR), educational services’ main threat actors are external (75%) who leverage system intrusion and web application attacks (80%) to penetrate a system and target personal data (63%) or credentials (41%) [3, p. 57].

Deploying TPRs on-premise means that the organization has to consider the security risks TPRs pose on their infrastructure and how user data is handled. Organizations need to be aware that allowing users to connect to their network remotely using TPRs needs to be handled correctly in all stages to prevent data compromise which could later be used against the organization itself. Recent publications in the field show good attempts to create applicable threat models and standardize risk assessment methodology regarding robotics to tackle such issues (RSF, OCTAVE A, ISO27005, NSMROS). Though there is research on potential risks regarding the use of robotic systems in general, however, previous works have not specifically addressed issues that are specific to TPRs (e.g. remote connection, cyber-physical presence, live video, and audio feed).

This is a problem because there is a gap between existing risk assessment models and how existing work is applicable to TPRs’ specific properties, which this thesis strives to fulfill. Also, the usage of TPRs is on the rise, and educational systems are most vulnerable to stolen credentials. The thesis will focus on user data security more specifically as according to DBIR, 40% of breaches in educational systems included the use of stolen credentials and with each breach personal (63%) and credentials (41%) information was compromised [3, pp. 57-58].

The proposed solution for this thesis is to create a new model based on a combination of existing models which can assess specific cybersecurity risks associated with TPRs. Using the new model, potential risks can be identified and validated through case studies. Expert interviews will then help to further confirm the found risks, improve the proposed model, and offer mitigation strategies to address the risks.

**Main Research Question:** To what kind of security risks are organisations using TPRs exposed to, and how to mitigate the risks?

The scope of this thesis is to identify cyber security risks related to the organisations who are using TPRs and provide mitigation strategies to reduce identified risks with an emphasis on user data and how external users interact with TPRs.

**More Specific Research Questions:**

1. How is user data handled in TPRs systems?

2. What are the potential security risks posed by TPR?

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

**Objectives:**

This thesis aims to identify cyber security risks related to organizations using telepresence robotics (TPRs) and propose mitigation strategies to reduce the identified risks with focus on user data. To achieve this, the research will leverage various frameworks such as RSF, CIA, OCTAVE A, ISO27005, and NSMROS to create a new risk assessment model for TPRs. The research will also use case studies and interviews with technical staff to validate the security risks and explore possible solutions proposed by the experts.

**Initial Plan for Masters Project:**

The study will mostly inherit qualitative research properties due to the nature of the study, lack of (known) empirical data on the subject, and limited time to conduct case studies. The steps of the initial plan for the Masters’ project will be:

1. Building of the theoretical background using a combination of possible frameworks: RSF, CIA, OCTAVE A, ISO27005, NSMROS. Use applicable methodologies to analyze TPR security systems to identify possible security risks. This is to create a new risk assessment model that is specific to TPRs and helps us to identify risks.

2. Case Studies will be conducted to better understand the practical implications of telepresence robotics and user interaction with them. We validate security risks in real-life scenarios using the newly created risk assessment model in the theoretical part. One possible case study subject is Tallinn, IT College (ICO).

3. Interviews with technical staff who integrated TPRs into the organization, which the users are using. This will allow us to better understand observed phenomena from the case studies and expand the theoretical framework. Interviews will help us to confirm if the risk identified in the theoretical framework or case study is an actual risk in the real world and explore possible mitigation strategies proposed by the interviewed experts.

4. Analysis of the data collected from previous steps to identify potential security concerns and risks posed by TPR, as well as potential solutions to these risks.

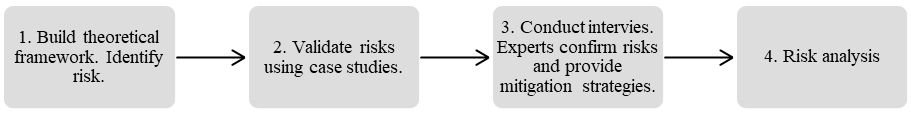


Figure 1. The initial plan for Master Project.

# Terms and Notations

# Background

# Literature review

# Conclusions

References

|  |  |
| --- | --- |
| [1] | J. Leoste, M. Heidmets, S. Virkus , A. Talisainen, M. Rebane, K. Tiina , K. Tammemäe, K. Kangur, K. Kikkas ja K. Marmor, „Keeping distance with a telepresence robot: A pilot study,“ kd. 7, pp. 1-10, 2023. |
| [2] | V. M. Vilches, L. A. Kirschgens, A. B. Calvo, A. H. Cordero, R. I. Pisón, D. M. Vilches, A. M. Rosas, G. O. Mendia, L. U. S. Juan, I. Z. Ugarte, E. Gil-Uriarte, E. Tews and A. Peter, "Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics," 2018. |
| [3] | S. Widup, A. Pinto, D. Hylender, G. Bassett ja P. langlois, „2022 Data Breach Investigations Report,“ Verizon, 2022. |

Appendix

1. Glossary
2. License

**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:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

**Cyber security risks in telepresence robotics and their mitigation**,

*(title of thesis)*

supervised by Kaido Kikkas,

*(supervisor’s name)*

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **11.03.2023**