UNIVERSITY OF TARTU

Institute of Computer Science

Cybersecurity Curriculum

Joosep Parts

Analyzing user data security in telepresence robotics using Robot Security Framework

Master’s Thesis (21 ECTS)

Supervisor(s): Kaido Kikkas

Tartu 2023

Table of Contents

[Introduction 4](#_Toc129183308)

[1 Terms and Notations 5](#_Toc129183309)

[2 Background 6](#_Toc129183310)

[3 Literature review 7](#_Toc129183311)

[Conclusions 8](#_Toc129183312)

[References 9](#_Toc129183313)

[Appendix 10](#_Toc129183314)

[I. Glossary 10](#_Toc129183315)

[II. License 11](#_Toc129183316)

# Introduction

**Overview**

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. This increase in usage of TPRs in the near future also means the number of users of the system and the possible security risks associated with it will increase.

Consumer-oriented products tend to choose usability over privacy/security, which inherently means they adopt insecure system options. Robotics systems which are developed by thirdy party organisations may use proprietary hardware and software with little configuration options.

General-purpose domestic robotics security concerns could be categorized into four categories: physical, network, OS, and application security. In that sense, telepresence robotics will probably share common ground on security concerns. Key differences between telepresence robotics and other domestic robots 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. Deploying TPR on-premise means that the organization has to consider the security risks TPR pose on their infrastructure and how user data is handled. Recent publications in the field show good attempts to create applicable threat models and standardize risk assessment methodology regarding robotics. Though there is research on potential risks regarding the use of robotic systems – previous works have not specifically addressed issues in depth that TPR may pose on user security.

**Main Research Question**

What kind of security risks are the users of TPR exposed to?

The scope of this thesis is to identify cyber security risks related to users of TPRs and provide mitigation strategies to reduce identified risks. This thesis will analyze user data security in telepresence robotics (TPR) using a Robot Security Framework (RSF) [1]. The thesis will focus on analyzing how user data is handled from the CIA triad perspective to identify potential risks that may arise from user interaction with TPRs. Risk assessment will be conducted using existing methodologies in the field of robotics that can be applied to TPRs (OCTAVE A, ISO27005, NSMROS).

**More Specific Research Questions**

1. How is user data handled from the CIA triad perspective?

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

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

**Objectives**

The objectives of this thesis are to analyze TPR cyber security from the CIA Triad perspective using Robot Security Framework (RSF) to find possible vulnerabilities regarding user security. The analysis could create a comprehensive report on TPR and user security, provide recommendations for further research, and propose mitigation strategies to reduce found security risks.

**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 RSF, CIA, and other applicable methodologies to analyze TPR security systems to identify possible security risks.

2. Case Studies to better understand the practical implications of telepresence robotics and user interaction with them. Validate security risks in real-life scenarios, which were identified in the theoretical part.

3. Interviews with technical staff who integrated TPR, which the users are using. This will allow us to better understand observed phenomena from the case studies and expand the theoretical framework.

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.

# Terms and Notations

# Background

# Literature review

# Conclusions

References

|  |  |
| --- | --- |
| [1] | . A. H. Cordero, V. M. Vilches, L. A. Kirschgens, A. B. Calvo, R. I. Pisón, D. M. Vilches, A. M. Rosas, G. O. Mendia, L. U. San 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. |

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

**Analyzing user data security in telepresence robotics using Robot Security Framework**,

*(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, **08.03.2023**