|  |  |  |  |
| --- | --- | --- | --- |
| **Proposed title of the thesis (English)** | Analyzing user data security in telepresence robotics using Robot Security Framework | | |
| **Problem (Which problem will the thesis offer a solution to?)** | Telepresence robotics (TPR) are consumer-oriented products that allow remote presence in a physical location. Consumer-oriented products tend to choose usability over privacy/security, which inherently adopt insecure system options [1] [2] [3].  Q1: To what kind of security risks are the users of TPR exposed to?  Q2: How is user data handled from the CIA triad perspective? | | |
| **Goal (What will the thesis strive to achieve?)** | Analyzing TPR cyber security from the CIA Triad perspective and using Robot Security Framework (RSF) to find possible vulnerabilities regarding user security. | | |
| **Relevance (Why does the problem matter? Is it state of the art?)** | The market of TPR has been on a steady incline which abruptly spiked in 2020 (COVID-19 impact), and the forecast shows that the market is growing [4] [5]. This increase in usage of TPR in the upcoming years also means the number of system users and the possible security risks associated with it will increase. | | |
| **Scope/limitations (What does the thesis deal with, and what falls outside of the scope?)** | The scope of this thesis is to identify cyber security risks related to users of TPR and provide mitigation strategies to reduce identified risks. 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 [6] [2] [3]. The limitations of this thesis are that it will not analyze other aspects of TPRs, such as hardware. Additionally, the thesis will not address the legal or ethical implications of using TPRs. Finally, the thesis will not provide a comprehensive survey of the available products in the market. | | |
| **Methodology (How will the problem be solved and why so?)** | 1. Building of the theoretical background. Using RSF, CIA, and other applicable methodologies, we will analyze TPR security systems to identify possible security risks. 2. Case Studies: will be conducted 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. Case study subjects: IT college and …? 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: the data collected from previous steps could then be analyzed to identify potential security concerns and risks posed by TPR, as well as potential solutions to these risks.   Overall 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. | | |
| **Theoretical/analytical part (What is the background, different players/options, previous studies etc?)** | General-purpose domestic robotics security concerns could be categorized into four categories: physical, network, OS, and application security [6, p. 2]. 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 [3, p. 80]. 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 [4] [6]. 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. | | |
| **Practical part (What is the tangible contribution of the thesis?)** | The analysis could create a comprehensive report on TPR and user security. Provide recommendations for further research. Propose mitigation strategies to reduce found security risks. | | |
| **Sources/references (provisional)** | 1. Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics [6]. 2. Cybersecurity Issues in Robotics [2]. 3. Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety [3] | | |
| Notes to self: | | | |
| Contact:  Joosep Parts, 221963IVCM  TalTech, MSc student in cybersecurity [jopart@taltech.ee](mailto:jopart@taltech.ee)  +372 53640102 | | Supervisor 1:  Kaido Kikkas  [Kaido.Kikkas@taltech.ee](mailto:Kaido.Kikkas@taltech.ee) | Supervisor 2: |

# References

|  |  |
| --- | --- |
| [1] | M. Gutfleisch, K. H. Jan, N. Busch, Y. Acar, M. A. Sasse and S. Fahl, "How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study," 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9833756. |
| [2] | "Cybsersecurity Issues in Robotics," 2021. [Online]. Available: https://isyou.info/jowua/papers/jowua-v12n3-1.pdf. |
| [3] | "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety," 2017. [Online]. Available: https://cdn.intechopen.com/pdfs/56025.pdf. |
| [4] | "TELEPRESENCE ROBOTS MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2023 - 2028)," [Online]. Available: https://www.mordorintelligence.com/industry-reports/telepresence-robots-market. |
| [5] | J. Leoste, M. Heidmets, S. Virkus, A. Talisainen, M. Rebane, T. Kasuk, K. Tammemäe, K. Kangur, K. Kikkas and K. Marmor, "Keeping distance with a telepresence robot: A pilot study," 2023. [Online]. Available: https://www.frontiersin.org/articles/10.3389/feduc.2022.1046461/full. |
| [6] | "INTRODUCING THE Robot Security Framework (RSF), A STANDARDIZED METHODOLOGY TO PERFORM SECURITY ASSESSMENTS IN ROBOTICS," 2018. [Online]. Available: https://arxiv.org/abs/1806.04042. |
| [7] | "Double 3 Security," [Online]. Available: https://github.com/doublerobotics/d3-sdk/blob/master/docs/Security.md. |
| [8] | "Exploring Use Cases for Telepresence Robots," 2011. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1957656.1957664. |
| [9] | "ISO 22166-1:2021(en) Robotics — Modularity for service robots," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22166:-1:ed-1:v1:en. |