|  |  |  |
| --- | --- | --- |
| **Proposed title of the thesis (English)** | Cyber security risks in telepresence robotics and their mitigation | |
| **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 adopts insecure system options [1]. Have all component security risks been addressed in TPR products [2]? Another concern is integrating such products into the existing infrastructure – does TPR pose security risks on the infrastructure where it’s deployed? | |
| **Goal (What will the thesis strive to achieve?)** | Perform assessments to identify and explore security weaknesses specific to TPR using Robot Security Framework (RSF) and other modeling tools to recommend hardening possible vulnerabilities. Explore infrastructure security implications where TRPs have been deployed on-premise. | |
| **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 [3] [4]. More devices will be exposed in the near future, and the need to mitigate risks before they occur is highly prominent. The increase in usage of TPR in the upcoming years also means the number of products released and affected users will increase. | |
| **Scope/limitations (What does the thesis deal with, and what falls outside of the scope?)** | The scope of this thesis is to assess cyber security risks in telepresence robotics and provide mitigation strategies to reduce identified risks. The thesis will focus on analyzing the security architecture of TPRs, the security implications of deploying TPRs on-premise, and the potential risks that may arise from user interaction with TPRs. Security architecture risk assessment will be conducted using existing methodologies in the field of robotics that can be applied to TPRs [5] [6] [7]. 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. Literature Review: A comprehensive and detailed literature review of the existing research on telepresence robotics and security concerns should be conducted. 2. Survey: Interview experts in the field to gain insights into potential security concerns that telepresence robotics may pose. 3. Case Studies (or experiments): Case studies could be conducted to gain a better understanding of the practical implications of telepresence robotics. Perhaps analyze a specific product security (Double 3) using RSF [8]. 4. Analysis: The data collected from the literature review, survey, case studies, and experiments could then be analyzed to identify potential security concerns and risks posed by telepresence robotics, as well as potential solutions to these risks. This analysis could create a comprehensive report on telepresence robotics security and provide recommendations for further research.   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 having physical access to only a handful of models. | |
| **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 [5, 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 the way a user interacts with the robot and how the user inadvertently exposes themselves through the system. This creates the need for greater user privacy and data security [7, p. 80]. Deploying TPR on-premise means that institution has to consider the security risks TPR pose on their infrastructure. Recent publications in the field show good attempts to create applicable threat models and standardize risk assessment methodology regarding robotics [3] [5]. Though there is research on potential risks regarding the use of robotic systems – previous works regarding cyber security and robots, have not specifically addressed issues in depth that telepresence robotics may pose. | |
| **Practical part (What is the tangible contribution of the thesis?)** | Consolidated structured literature review on TPRs and cyber security. After using frameworks to analyze TPRs in general and conducting case studies on a specific model to validate found risks, we could propose mitigation strategies to reduce risks. | |
| **Sources/references (provisional)** | 1. Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics [5]. 2. Cybersecurity Issues in Robotics [6]. 3. Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety [7] | |
| Notes to self: | | |
| Contact: Joosep Parts, 221963IVCM  TalTech, MSc in Cybersecurity [jopart@taltech.ee](mailto:jopart@taltech.ee), +372 53640102 | | Supervisor: |

# 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] | "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. |
| [3] | "TELEPRESENCE ROBOTS MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2023 - 2028)," [Online]. Available: https://www.mordorintelligence.com/industry-reports/telepresence-robots-market. |
| [4] | 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. |
| [5] | "INTRODUCING THE Robot Security Framework (RSF), A STANDARDIZED METHODOLOGY TO PERFORM SECURITY ASSESSMENTS IN ROBOTICS," 2018. [Online]. Available: https://arxiv.org/abs/1806.04042. |
| [6] | "Cybsersecurity Issues in Robotics," 2021. [Online]. Available: https://isyou.info/jowua/papers/jowua-v12n3-1.pdf. |
| [7] | "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety," 2017. [Online]. Available: https://cdn.intechopen.com/pdfs/56025.pdf. |
| [8] | "Double 3 Security," [Online]. Available: https://github.com/doublerobotics/d3-sdk/blob/master/docs/Security.md. |
| [9] | "Exploring Use Cases for Telepresence Robots," 2011. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1957656.1957664. |