Oct 30th, 11:00 AM - 11:30 AM

Analyzing Robotics Software Vulnerabilities

Hossain Shahriar
Kennesaw State University, hshahria@kennesaw.edu

Md Jobair Hossain Faruk
mhossa21@students.kennesaw.edu

Shahriar Sobhan
ssobhan@students.kennesaw.edu

Mohammad Nazim
Kennesaw State University, mnazim@students.kennesaw.edu

Abstract

Robots are widely used in our day-to-day life in various domains. For example, eldercare robots, such as CareO-Bots [1]are used to perform household tasks and provide mobility assistance [2]. Amazon uses manufacturing robots to accomplish manufacturing labor activities, such as welding and assembling equipment [2]. According to the International Data Corporation, spending on robotics is expected to reach USD 241.4 billion by the end of 2023 [4].

However, malicious users can exploit security vulnerabilities in hardware and software components of robotics systems to conduct security attacks and cause malfunction, i.e., deviate robots from their expected behaviors. Security attacks on robots can have serious consequences such as (i) bottlenecks and shutdowns in the assembly line, (ii) disruption in the food supply chain, (iii) incorrect treatment for patients, and (iv) unwanted military attacks injuring or killing civilians and military personnel [2].

Researchers [3] have observed a lack of awareness amongst practitioners related to security issues that can exist in robotics systems. Using qualitative analysis, the project aims to determine the software vulnerabilities that commonly appear in robotics systems.

In this work in progress, we plan to discuss our initial findings using Robotics Vulnerability Database (RVD) repositories [5] the following questions – (i) what are the most frequent security vulnerabilities in robotics systems? (ii) what types of components are affected by the vulnerabilities? (iii) what categories of vulnerabilities exist and severity for robotics systems?

Location

Online Zoom Session

Disciplines

Information Security | Management Information Systems | Technology and Innovation

Comments

This is work-in-progress is to discuss updated results from ICWD 2021 summer grant work.

ABSTRACT

Robots are widely used in our day-to-day life in various domains. For example, eldercare robots, such as CareO-Bots [1] are used to perform household tasks and provide mobility assistance [2]. Amazon uses manufacturing robots to accomplish manufacturing labor activities, such as welding and assembling equipment [2]. According to the International Data Corporation, spending on robotics is expected to reach USD 241.4 billion by the end of 2023 [4].

However, malicious users can exploit security vulnerabilities in hardware and software components of robotics systems to conduct security attacks and cause malfunction, i.e., deviate robots from their expected behaviors. Security attacks on robots can have serious consequences such as (i) bottlenecks and shutdowns in the assembly line, (ii) disruption in the food supply chain, (iii) incorrect treatment for patients, and (iv) unwanted military attacks injuring or killing civilians and military personnel [2].

Researchers [3] have observed a lack of awareness amongst practitioners related to security issues that can exist in robotics systems. Using qualitative analysis, the project aims to determine the software vulnerabilities that commonly appear in robotics systems.

In this work in progress, we plan to discuss our initial findings using Robotics Vulnerability Database (RVD) repositories [5] the following questions – (i) what are the most frequent security vulnerabilities in robotics systems? (ii) what types of components are affected by the vulnerabilities? (iii) what categories of vulnerabilities exist and severity for robotics systems?

ACKNOWLEDGEMENT

The work is partially supported by ICWD Summer Research Grant 2021.

REFERENCE

[1] Care-o-bot, https://www.care-o-bot.de/en/care-o-bot-4.html

[2] G. W. Clark, M. V. Doran, and T. R. Andel. Cybersecurity issues in robotics. In *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, pages 1–5, 2017.

[3] Carlos Gonzalez. Fear the hacker! robot security is a growing threat. https://www.machinedesign.com/mechanical-motion-systems/article/ 21835782/fear-the-hacker-robot-security-is-a-growing-threat, 2017.

[4] Statista. Global spending on robotics and drones in 2020 and 2023. https://www.statista.com/statistics/441948/forecast-for-roboticmarket-spending-worldwide/, 2021.

[5] Victor Mayoral Vilches, Lander Usategui San Juan, Bernhard Dieber, Unai Ayucar Carbajo, and Endika Gil-Uriarte. Introducing the robot vulnerability database (rvd). *arXiv preprint arXiv:1912.11299*, 2019.