### Poster: On the Cyber-Physical Security of Commercial Indoor Delivery Robot Systems

Fayzah Alshammari, Yunpeng Luo, and Qi Alfred Chen Univesity of California, Irvine

Abstract—Indoor Delivery Robots (IDRs) play a vital role in the upcoming fourth industrial revolution, autonomously navigating and transporting items within indoor environments. In this work, we thus aim to conduct the first security analysis of the IDR systems considering both cyber- and physical-layer attack surface and domain-specific attack goals across security, safety, and privacy. As initial results, we formulated a general IDR system architecture from 40 commercial IDR models, and then performed an initial cyber-physical attack entry point identification. We also performed an experimental analysis of a real commercial IDR robot-side software and identified several vulnerabilities. We then discuss future steps.

### I. INTRODUCTION

Indoor Delivery Robots (IDRs) are crucial participants in the upcoming fourth industrial revolution, autonomously navigating and transporting items within indoor environments. The global market for IDRs was valued at USD 6.106 Million in 2020 and is projected to reach USD 157.618 Million by 2027. Furthermore, IDRs are complex automation devices that can interact with people through multiple control systems in public places such as hospitals, hotels, restaurants, and airports. They can also interact with other indoor existing systems, such as facility management systems, and remotely with vendors for support and maintenance. This brings critical cyber security, physical security, and safety concerns. To address these concerns and to ensure the security of IDRs and, more importantly, the safety of people around them, it is vital to understand the potential security challenges that assist in developing robust security strategies for IDR systems. Various prior works are studying the security of robotic systems generally such as as [1], where they mainly report vulnerabilities in network surface attacks, but no comprehensive security analysis of the indoor delivery robot has been done.

In this work, we thus aim to conduct the first comprehensive security analysis of commercial IDRs, addressing a gap in systematic evaluations of their attack surface and cyberphysical impacts. We aim to consider cyber- and physical-layer threats in our threat model and identify domain-specific attack goals across security, safety, and privacy. As an initial step, we survey the market of commercial IDRs, coming up with a list of 40 commercial models. We then utilize this list to derive the system architecture for commercial IDRs to identify attack entry points, and also perform an experimental analysis of a commercial IDR robot-side software. In the future, we will perform further domain-specific attack class discovery, experimental analysis, and defense discussions.

### II. THREAT MODEL AND PROBLEM FORMULATION

**Threat model.** This work assumes local-environment attackers when carrying out physical-layer attacks or cybercriminals when conducting cyber-layer attacks. The attacker is assumed to possess the required skills to reverse engineer the IDR's software and know the target delivery robot's structure. This can be realistically achieved by purchasing the same IDR model herself or renting one.

Attack goals. By targeting an IDR, an attacker can achieve various domain-specific security, safety, and privacy breaches, for example: (1) *delivery service manipulation* which includes altering the destination, replacing the delivered item with harmful or unexpected substances, or simply preventing the delivery from happening at all, (2) *safety damages*, including crashing into people, and other robots, and (3) *sensitive information stealing* such as information about the indoor environment's maps, surroundings and people.

### III. ANALYSIS METHODOLOGY

With the threat model and attackers' goals described above, we plan to systematically analyze the security of the state-ofthe-art commercial IDRs by the following steps:

- Comprehensive attack surface analysis. To perform a comprehensive attack surface analysis of IDR systems, we must first obtain a general IDR system architecture that can comprehensively describe their stateof-the-art system components and interaction designs in indoor environments. To achieve this, we exhaustively search for all IDR models from the companies dominating the IDR market today and then use their publicly available information (e.g., user manuals) to derive such a general IDR system architecture. From this derived system architecture, we can then comprehensively identify potential attack entry points at both the cyber- and physical-layers;
- **Domain-specific attack class discovery.** Based on the system architecture, system requirements, and attack entry points, we plan then to systematically identify concrete IDR-specific attack classes driven by the domain-specific attack goals stated earlier;
- Experimental security analysis of a real IDR system. To understand the feasibility of these identified domain-specific attack classes, we plan to perform an experimental security analysis of real IDR systems and components guided by the discovered attack classes above. We will finally discuss potential defense strategies based on the insights from these analyses.

### IV. EARLY RESULTS

**IDRs list and information gathering.** To establish the IDR system architecture, we identified 14 leading companies from recent market reports and manually reviewed their websites for IDR products available between April 3 and June 7,



Fig. 1. Venn diagram for the used information sources for deriving the general IDR system architecture. As shown, 39 of 40 IDRs are covered by at least 1 type of information source (i.e., dataset, user manual, or video).



Fig. 2. General Indoor Delivery Robot (IDR) system architecture and an initial cyber-physical attack entry point analysis, where [%] denotes the percentage of robots with a specific feature/component.

2023. This included all robots designed for indoor delivery in environments like hospitals and restaurants, resulting in a list of 40 IDR models. We collected information on 40 robot models using publicly-available datasheets, user manuals, and videos as visualized in Fig. 1. Specifically, datasheets were found for 21 models, which provided technical specifications; user manuals for 15 models, which offered operational details; and videos for 24 models, which further helped to understand robot functionality and interactions.

General IDR system architecture. We then use the gathered information above to derive a general system architecture of today's commercial IDR systems, which involves various types of domain-specific system components such as door/evaluator control, multi-robot collaboration, phone/watch robot calls, pager, markers on the ceiling, etc. as shown in Fig. 2. The diagram presents a detailed overview of the IDR system's architecture, highlighting its integration with facility management systems like elevators, a heavy reliance on the vendor's cloud (30%), and diverse control systems like mobile apps and wearables, reflecting operational flexibility and user preference accommodation. Robot features such as navigation, obstacle avoidance, and emergency stop buttons are standard in all robots despite some limitations in robot collaboration capabilities. Touchscreens and expression interaction emphasize user-friendliness, and guest notification systems focus on enhancing service efficiency and guest interaction.

Initial attack surface analysis. Based on the derived general IDR system architecture, we perform an initial attack surface analysis for each IDR system component by analyzing their potential cyber- and physical-attack entry points. Specifically, for cyber-attack entry points, components are categorized based on their reliance on software or firmware, like control systems and communication protocols; their need for network connectivity, which includes elements like LAN and cloud services; their involvement in data storage, retrieval, or transmission, which can be vulnerable to breaches and unauthorized access; and the ability for remote control or access, such as mobile apps or web interfaces, due to hacking risks. On the other hand, physical-attack entry points are defined by hardware-based components, including sensors, cameras, and ports; components requiring physical interaction or vulnerable to tampering, like touchscreens and docking stations; elements dependent on the physical environment, such as navigation systems; and manual safety controls like emergency stop buttons, which can be directly and manually interfered with. Such initial analysis results are also visualized in Fig. 2.

Initial robot-side software security analysis. Meanwhile, we obtained the robot-side software of one of the commercial IDRs we examined. This software is an Android app, and through static penetration testing, we uncovered two types of software vulnerabilities based on the OWASP Mobile Top 10 vulnerability categorizations [2]. The first, Insufficient Binary *Protection*, enabled us to reverse-engineer the app, exposing crucial details about its functionality. This vulnerability also allowed us to modify the app's code due to the absence of code tampering detection or protection mechanisms. An example is our successful manipulation of the app's user interface, demonstrating the potential for altering IDR functionalities, such as delivery details. The second vulnerability pertains to Insecure Data Storage, as we discovered that the app's android: allow Backup attribute is set to True. This setting permits the creation of backups that include application data, which could lead to the theft of sensitive information such as indoor maps, delivery schedules, and customer details.

### V. CONCLUSION AND FUTURE PLANS

In this work, we aim to perform the first security analysis of IDR systems that encompass both cyber and physical layers and target specific attack goals related to security, safety, and privacy. As an initial result, we formulated a general IDR system architecture based on 40 commercial IDR models today and then performed an initial cyber-physical attack surface analysis. We also performed an initial experimental security evaluation of an actual commercial IDR software, yielding two critical vulnerabilities. In the future, we plan to (1) build upon the derived general IDR system architecture and the concrete cyber-physical attack surface analysis to start the IDR-specific attack class discovery and (2) extend the security analysis to a complete IDR system (not just the robot-side software).

### REFERENCES

- A. Giaretta, M. De Donno, and N. Dragoni, "Adding Salt to Pepper: A Structured Security Assessment over a Humanoid Robot," in (ARES), 2018.
- [2] "OWASP Mobile Top 10 OWASP Foundation owasp.org."

# Poster: On the Cyber-Physical Security of Commercial Indoor Delivery Robot Systems



Fayzah Alshammari, Yunpeng Luo, and Qi Alfred Chen University of California, Irvine (UCI)

# **Indoor Delivery Robots (IDRs)**

- Indoor delivery robots IDRs are professional robots that autonomously navigate and transport items within indoor environments.
- IDRs are becoming crucial participants in the upcoming 4<sup>th</sup> industrial revolution.
- Their global market was valued at USD 6.106 Million in 2020 and is projected to reach USD 157.618 Million by 2027.

### **Prior Works & Problem Statement**

- Prior works studied the security of robotic systems generally, but none of them has studied the attack surface and implications specific to the IDR systems.
- To ensure the security of IDRs and the safety of people around them, it is vital to understand their potential security challenges, which assist in developing robust security strategies. Phsical

## **Problem Setup & Analysis Methodology**

### Threat model

## • Attacker types

- Local physical attackers when carrying out physical-layer attacks.
- Cyber criminals when conducting cyber-layer attacks against IDR systems.
- Attacker capabilities
  - Knows the target delivery robot's structure.
  - Possesses reverse engineering skills.

## Attack goals

- **G1** delivery service manipulation, e.g., altering the destination of delivery.
- **G2** safety damages, e.g., crashing into wall, people or other robots in the environment.
- **G3** sensitive information stealing, e.g., learning the environment maps.

# Analysis methodology design

- 1) Comprehensive attack surface analysis by obtaining a general IDR system architecture to describe the state- of-the-art system components and interactions.
- 2) *Domain-specific attack class discovery* by using the system architecture, system requirements, and attack entry points, to systematically identify concrete IDR-specific attack classes driven by the domain-specific attack goals.
- 3) *Experimental security analysis* of a real IDR system to concretely understand the feasibility of the identified domain-specific attack classes.



### Contact







Initia	l Results
Vendor's	s cloud [30%]
Attack er	ntry points
	Physical Cyber
ڲٮۺڮ	Cybol
+F0/1 / /	1
^[%] denotes	s percentage c
	Ini
	ined the robor ormed a station
🛛 Durin	ng the testing, <b>V1</b> - the <i>bin</i>
	• V2 - it does
	• V3 - <i>insecul</i> configuration
	biting these ענ to achieve <b>G</b> נ
	ential explo
The ro	<b>Benign</b> bot's app ice before



of robots with a specific feature/component.

ons of the robot.

**1** and/or **G2**. Furthermore, exploiting **V3** can enable the attacker to achieve **G3**.





