Assessing Security of Mobile Robots in Public Spaces

Roel Deimann BSc
Fontys University of Applied Science
r.deimann@student.fontys.nl

Tom Broumels MSc
Fontys University of Applied Science
t.broumels@fontys.nl

ABSTRACT

In our research we present an initial version of an attack- and defense matrix for mobile robots in public spaces.

These matrices are the result of modeling threats and performing security tests on robots by teams of student researchers. Although we found considerable overlap with existing Mitre matrices, some of the identified attack tactics and techniques are specific to mobile robots in public places: physical tampering, reconnaissance by visual inspection, targeting ROS. Given the possible consequences on the physical security of everything in close proximity to the robot, we recommend the addition of views for mobile robots in public places to the MITRE matrices.

1 INTRODUCTION

Mobile robots are more and more deployed in the public domain where interaction with individuals is more common compared to robots operating in closed (production) environments [1, 2]. Safety incidents already occured in closed production environments, such as the fatal incident in South Korea in November 2023, and it is not unthinkable that security issues with robots in public spaces could lead to (serious) safety issues as well [3].

Developments in more mature security areas, such as enterprise security, have lead to overviews of attack tactics, techniques and procedures and defensive measures [?]. These overviews, managed by MITRE corporation, provide security professionals with a complete picture and common understanding of adversary behaviour in these domains. The level of technical detail helps understanding, mitigating and replicating attacks in practice. The existence of different views on the matrices for different security domains emphasises the need for context specific overviews.

There is no recognized equivalent of these matrices for the domain of mobile robots in public spaces at the time of writing.

The Safety & Security Campus [4] and Fontys University of ICT [5] aim to contribute to a common understanding of attacks and corresponding mitigations on mobile robots in public spaces to support (security) professionals in the development and testing of these robots.

To achieve this we created an overview of (possible) attacks on mobile robots in public spaces by compiling matrices based on published research and custom, hands-on, security assessments on robotics hardware.

2 DEFINITIONS

To facilitate the understanding of this paper, different terms are defined in this section.

2.1 Public Spaces

In this research we define public spaces as areas or places that are accessible and open to the general public and where people can come together for recreational, social or cultural purposes.

2.2 Mobile Robots

The definition of mobile robots in ISO 8373:2021(en) mobile robots is rather broad and includes a.o. industrial robots and self driving cars [?]. To tailor our resulting matrices to a more specific security domain, we define mobile robots in our studies as follows:

- A device, physical hardware (running software)
- The device is able to change its physical position in two or three dimensions (mobile robot).
- The device is operating in an environment that is not (entirely) controlled and in the presence of people that are not trained in interacting with it.
- The device makes its own decisions to some extent (autonomous robot). This might mean that the device is fully functioning on its own (e.g. vacuum robot), or that a controller is used to instruct the device to perform a certain task and the device plans and executes the necessary steps to achieve the task.
- There is no human physically present inside of the device (unmanned vehicle). If a human would be present, different safety and security regulations would apply (e.g. regulations related to automotive and/or attractions).

The items in Table 1 comply to the definition except "Robotic Arm" because it has no capability to move itself, "Self-Driving Vehicle" because it is not considered a mobile robot since there is a human present in the vehicle and "AGV" because these typically operate in controlled areas among instructed personnel.

	Environment	**Control**
Robot Vacuum Cleaner	Indoor	Autonomous
~~AGV~~	Warehouse, Factory	Fleet Manager
Spot	Indoor, Outdoor	Manual or Autonomous
~~Robotic Arm~~	Factory	Automatic
Drone	Indoor, Outdoor	Manual or Autonomous
Atlas	Indoor, Outdoor	Manual or Autonomous
~~Self-Driving Vehicle~~	Outdoor	Manual or Autonomous

Table 1: Mobile robots in public space

3 RELATED WORK

3.1 MITRE matrices

MITRE manages a knowledge base of tactics, techniques and procedures used by adversaries. Information in the knowledge base is based on observations of real world attacks and different views for different security domains are provided to parties involved in security.

Although MITRE is involved in robotics, there are no robotics specific ATT&CK and/or D3FEND matrix views available yet [6]. There are, however, MITRE ATT&CK matrices views for:

- Enterprise (https://attack.mitre.org/matrices/enterprise/)
- Mobile (https://attack.mitre.org/matrices/mobile/)
- Industrial Control Systems (https://collaborate.mitre.org/attackics/index.php/Main_Page)

For some years, Android smartphones have been used as an operating system for controlling autonomous robots [**?**]. For such robots we can expect (part of) the Mobile matrix to be relevant. The Industrial Control Systems matrix could also (partly) be relevant for (industrial) robots if we take the environment where the robots operate into account. A similar overlap can be expected with Enterprise matrix for those robots with a common OS (e.g. Linux as host OS, possibly combined with ROS2).

3.2 Robotics Security initiatives

The commercial organization Alias Robotics focuses on robot security and is a.o. a CVE Numbering Authority [7]. It is one of the few parties that publish whitepapers and blogs referring to standardisation in relation to robotics.

In 2021, Alias Robotics made a proposal for a robotics-specific vulnerability scoring system called Robot Vulnerability Scoring System (RVSS) and suggested to be more transparent about robot vulnerabilities, comparable to the way transparency is increasing regarding vulnerabilities in software [8]. Some examples show that the probability of attacks (e.g. physical accessibility) and impact (consequences for safety) for robotics can be different than in other environments such as IT and ICS/OT.
Alias Robotics also introduced an adapted version of the Cyber Kill Chain and a custom MITRE ATT&CK framework for robotics in the whitepaper Red Teaming ROS Industrial [9]. While this matrix is a more specialized one for industrial robots running ROS, it is still aimed at an industrial environment and not tailored towards mobile robots in public spaces as defined in our research.

4 RESEARCH QUESTIONS

The main research question is formulated as follows:

"What would security matrices, tailored towards mobile robots in public spaces, look like?"

5 BACKGROUND

This section describes Robot Operating System (security maturity).

5.1 Robot Operating System

Robot Operating System (ROS, https://www.ros.org/) is a collection of open-source tools and libraries used for controlling robots. Where ROS, in the early days, was mainly used in the academic world, it has now become a de-facto standard for robot control [2]. An important security-related change in version 2 compared to version 1 is the introduction of an abstract middleware interface for serialization, transport, and discovery. All current implementations are based on the Data Distribution Service (DDS) standard.

5.2 Robot Operating System security maturity

Brief exploration of literature related to ROS security shows that security features that can be enabled (e.g. DDS security) are mainly focused on authentication and authorization and encrypted traffic [10].

A more holistic view of security (one that approaches the security of the entire system in its context) does not seem to be a common practice in autonomous robot development yet [2]. An interview with Daniel Meinsma, Security Researcher involved in the Endurable Case project confirms this, as well as interviews with student teams at FHICT responsible for design and implementation of autonomous robotics.

6 METHODOLOGY

We started by identifying security threats to mobile robots in public spaces. Based on these threats we created initial attack and defense matrices. Finally, security tests have been performed on mobile robots to confirm the possibility of such attacks in practice.

6.1 Threats to mobile robots in public spaces

The properties of mobile robots in public spaces, as mentioned in the definition section, allowed us to model threats.

We started by listing hypothetical threats in a series of brainstorm sessions, to some extent involving Safety & Security Campus. Next, we added existing threats based on successfully executed attacks that we found in documented incidents and vulnerability research papers.

In addition, we performed vulnerability research on several mobile robots running up-to-date firmware ourselves, i.e.: Spot by Boston Dynamics, Unitree A1, DJI Mavic 2 Enterprise, DJI Tello drone. For practical reasons, the amount of mobile robots we tested was limited.

Because ROS is considered a de-facto standard for robot control [2], additional vulnerability research is performed on the, at the time of research, current version 2 of ROS (ROS2 2023-1118, ros-iron-desktop version 0.10.0-3jammy.20231118.021141 for amd64 architecture).

6.2 Attack/defense matrices

Based on the found literature and performed tests we identified techniques that apply to the security domain under investigation. We manually clustered similar techniques to a limited amount of tactic, where possible using the MITRE attack/defend names for the clusters we created.

Per technique we created a description and referred, where available, to descriptions of practical examples for mobile robot hardware. Techniques that we successfully performed on mobile robot hardware were marked with a green color, the ones not validated this way were marked orange.

7 RESULTS

The resulting attack- and defend matrix can be found in “Appendix A - Attack Matrix for Mobile Robots in Public Spaces” and “Appendix B - Defend Matrix for Mobile Robots in Public Spaces” respectively. An online version contains more detailed information for the techniques mentioned [11].

The result of the vulnerability research on version 2 of ROS (ROS2 2023-1118, ros- iron-desktop version 0.10.0-3jammy.20231118.021141 for amd64 architecture) is a document containing practical hardening guidelines for ROS2 and is available online [12].

8 DISCUSSION

The tactics in the resulting defend matrix are similar to the ones used by MITRE. The tactics in the created attack matrix are a subset of the MITRE Enterprise matrix. Only one additional tactic has been added. This means that, generally speaking, attacking mobile robots in public spaces is not that different from attacking any other IT system in general. Depending on the target architecture (e.g. Linux based OS) and the layer that is under attack (e.g. transport layer), techniques used might be exactly the same as the ones used for e.g. attacking enterprise software (e.g. nmap). But there are some differences:

- Attackers are able to physically approach mobile robots in public places. This is essentially different from other IT systems, e.g. enterprise systems which hardware is securely stored in a serverroom or industrial robots or AGV’s that operate in an environment where there is some form of control over which people are able to get close to the hardware. This allows for techniques that can impact a target without getting digital access to it first, e.g., influencing sensors, factory resetting and jamming radio signals. We placed these techniques in the newly added tactic "Disturbance".
- During the reconnaissance phase of an attack, visual inspection might result in valuable information about brand and/or model of device. This turned out to be useful for determining which wifi access point belongs to a robot based on determining the vendor part of the access point MAC addresses that were visible and for searching for model specific vulnerabilities.
- Robot Operating System (ROS) might be used to control mobile robots. This is a framework on top of an operating system such as Ubuntu or Windows and adds another layer in the architecture stack of the robot. The default settings of applications using ROS (both ROS and ROS2) do not enable all available security measures and will as such introduce security risks by default.
- Depending on how safety mechanisms are implemented, techniques mentioned for tactic Impact might have consequences for the physical safety of entities in the environment the robot operates in. Either by no longer securing the environment as planned, but also by becoming a physical hazard itself (e.g. hitting a person on purpose), depending on the safety (sub)systems implemented.

9 LIMITATIONS

Although the student researchers are trained in OWASP Top 10 [13] and Certified Ethical Hacker (CEH) [14] subjects, no structural method of security testing has been used. The testcases that did not yield security issues have not been documented. For practical reasons, the amount of mobile robots tested was limited.

10 CONCLUSIONS AND RECOMMENDATIONS

The main research question is formulated as follows: “What would security matrices, tailored towards mobile robots in public spaces, look like?” We have presented an initial version of an attack and defend matrix for mobile robots in public spaces that is based on literature and experiments. Although we found considerable overlap with existing MITRE matrices, some of the identified attack tactics and techniques are specific to mobile robots in public places. We recognize that tests on different hardware by different student teams could have led to different matrices. However, because of the possible consequences on the physical security of the robots surrounding we recommend the addition of views for mobile robots in public places to the MITRE matrices.

11 FUTURE WORK

Additional iterations of research by different student researchers and/or on different robots might lead to additional tactics and techniques.

Not yet confirmed (orange) techniques should be either confirmed or removed from the matrices.

12 RESPONSIBLE DISCLOSURE

Any vulnerabilities and weaknesses found in the operational robots of the Safety & Security Campus have been solved before the publication of this document.

13 ACKNOWLEDGEMENTS

We extend our sincere thanks to the Safety & Security Campus for generously lending us the professional robot hardware that was essential for our research. We appreciate the hard work and dedication of three student teams. We respect their decision not to have their names published in this paper.

REFERENCES

[1] Giovanni Mazzeo and Mariacarla Staffa. Tros: Protecting humanoids ros from privileged attackers. International Journal of Social Robotics, 12(3):827–841, 2020.

[2] Vincenzo DiLuoffo, William R Michalson, and Berk Sunar. Robot operating system 2: The need for a holistic security approach to robotic architectures. International Journal of Advanced Robotic Systems, 15(3):1729881418770011, 2018.

[3] Man crushed to death by robot in south korea. https://www.bbc.com/news/world-asia-67354709. Accessed: 2024-05-14.

[4] Safety security campus. https://safetysecuritycampus.com/. Accessed: 2024-05-14.

[5] Fontys university of ict. https://www.fontys.nl/en/About-Fontys/Fontys-ICT.htm. Accessed: 2024-06-10.

[6] Do you understand and trust your teammate, the robot? https://www.mitre.org/news-insights/impact-story/do-you-understand-and-trust-your-teammate-robot. Accessed: 2024-05-14.

[7] Our cve story: From robot security research to managing robot vulnerabilities. https://cve.mitre.org/blog/June102021_Our_CVE_Story_From_Robot_Security_Research_to_Managing_Robot_Vulnerabilities.html. Accessed: 2024-05-14.

[8] Víctor Mayoral Vilches, Endika Gil-Uriarte, Irati Zamalloa Ugarte, Gorka Olalde Mendia, Rodrigo Izquierdo Pisón, Laura Alzola Kirschgens, Asier Bilbao Calvo, Alejandro Hernández Cordero, Lucas Apa, and César Cerrudo. Towards an open standard for assessing the severity of robot security vulnerabilities, the robot vulnerability scoring system (rvss). arXiv preprint arXiv:1807.10357, 2021.

[9] Red teaming ros. https://aliasrobotics.com/files/red_teaming_rosindustrial.pdf. Accessed: 2024-05-14.

[10] Bernhard Dieber, Benjamin Breiling, Sebastian Taurer, Severin Kacianka, Stefan Rass, and Peter Schartner. Security for the robot operating system. Robotics and Autonomous Systems, 98:192–203, 2017.

[11] Attack- and defense matrices for assessing security of mobile robots in public spaces. https://i878261.apollo.fontysict.net/robot_security. Accessed: 2024-07-12.

[12] Security by default in ros2. https://i878261.apollo.fontysict.net/robot_security/SecurityByDefaultInROS2.pdf. Accessed: 2024-07-12.

[13] Owasp top 10. https://owasp.org/www-project-top-ten/. Accessed: 2024-06-10.

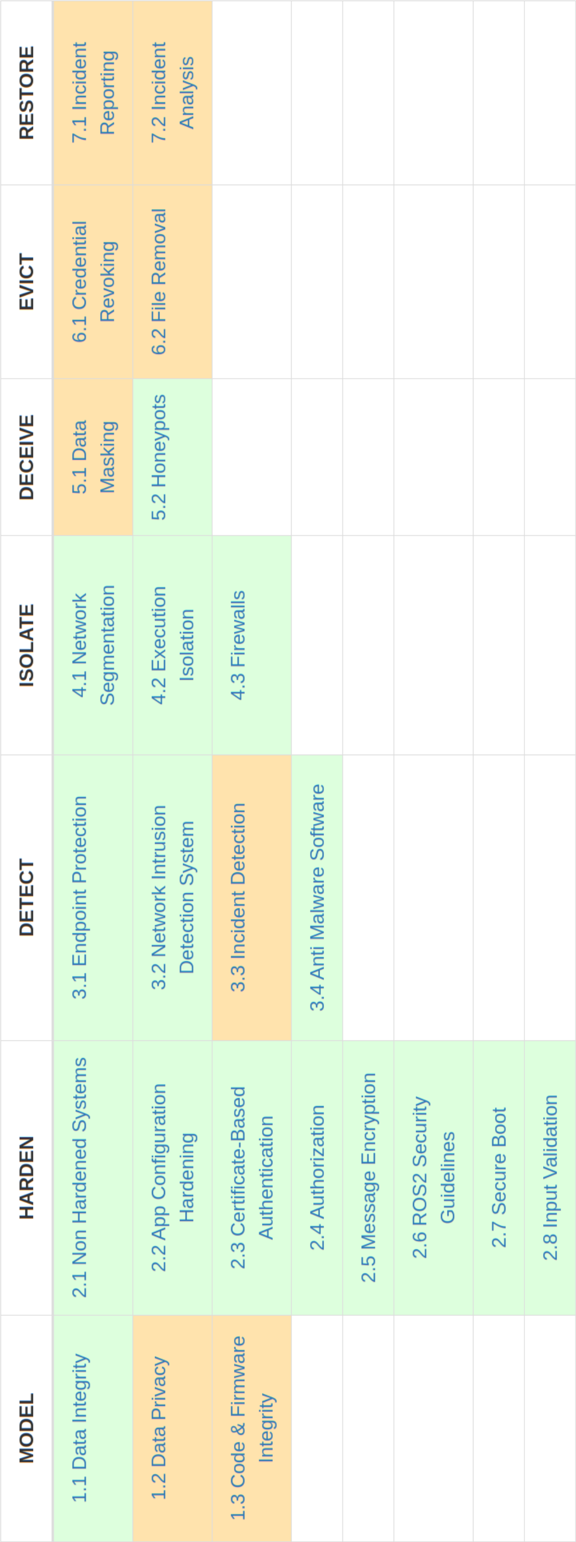
[14] Certified ethical hacker (ceh). https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/. Accessed: 2024-06-10.

APPENDIX A - ATTACK MATRIX FOR MOBILE ROBOTS IN PUBLIC SPACES

Tactic: Intel Gathering	Tactic: Disturbance	Tactic: Initial Access	Tactic: Privilege Escalation	Tactic: Persistence	Tactic: Lateral Movement	Tactic: Impact
🟩 Identify Platform	🟩 Deauth Wireless Protocol	🟩 Default Credentials	🟧 Modify Control Logic	🟧 OS Specific	🟩 Through (Custom) Communication Protocol	🟩 Eavesdrop
🟩 Scan Radio Frequencies	🟧 Jam Radio Frequency	🟩 Wifi Cracking	🟧 ROS Specific		🟩 Through Subsystem	🟧 Tamper Control Logic
🟩 Service Scanning	🟧 Sensor Tampering	🟧 Known Vulnerabilities	🟧 OS Specific			🟧 Denial Of Control
	🟩 Trigger Safety Measure	🟧 Physically Access Controller				🟧 Denial Of Availability
	🟧 Hardware Factory Reset	🟧 Supply Chain Compromise				🟧 Tamper With Safety System
	🟧 Electro Magnetic Pulse	🟧 Access Hardware Interfaces				🟧 Software Factory Reset
	🟧 Environmental Challenge	🟧 Compromise Controller				🟧 Control OS
	🟩 Physically Power Off or Reset					
	🟩 Software Power Off or Reset					
	🟩 Replay Controller Traffic					

Figure 1: Possible attack matrix for mobile robots in public spaces. Green techniques have been demonstrated in experiments. We expect orange techniques to be feasible on robots based on similar successful attacks in literature (on comparable devices).

APPENDIX B - DEFEND MATRIX FOR MOBILE ROBOTS IN PUBLIC SPACES



MODEL	HARDEN	DETECT	ISOLATE	DECEIVE	EVICT	RESTORE
🟩 1.1 Data Integrity	🟩 2.1 Non Hardened Systems	🟩 3.1 Endpoint Protection	🟩 4.1 Network Segmentation	🟧 5.1 Data Masking	🟧 6.1 Credential Revoking	🟧 7.1 Incident Reporting
🟧 1.2 Data Privacy	🟩 2.2 App Configuration Hardening	🟩 3.2 Network Intrusion Detection System	🟩 4.2 Execution Isolation	🟩 5.2 Honeypots	🟧 6.2 File Removal	🟧 7.2 Incident Analysis
🟧 1.3 Code & Firmware Integrity	🟩 2.3 Certificate-Based Authentication	🟧 3.3 Incident Detection	🟩 4.3 Firewalls			
	🟩 2.4 Authorization	🟩 3.4 Anti Malware Software				
	🟩 2.5 Message Encryption					
	🟩 2.6 ROS2 Security Guidelines					
	🟩 2.7 Secure Boot					
	🟩 2.8 Input Validation					

Figure 2: Possible defend matrix for mobile robots in public spaces. Green techniques have been demonstrated in experiments. We expect orange techniques to be feasible on robots based on similar defensive measures in literature (on comparable devices).