Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice
Other titles in Foundations and Trends® in Robotics

A Roadmap for US Robotics – From Internet to Robotics 2020 Edition
Henrik Christensen, Nancy Amato, Holly Yanco, Maja Mataric, Howie Choset, Ann Drobnis, Ken Goldberg, Jessy Grizzle, Gregory Hager, John Hollerbach, Seth Hutchinson, Venkat Krovi, Daniel Lee, Bill Smart, Jeff Trinkle and Gaurav Sukhatme
ISBN: 978-1-68083-858-9

The State of Industrial Robotics: Emerging Technologies, Challenges, and Key Research Directions
Lindsay Sanneman, Christopher Fourie and Julie A. Shah
ISBN: 978-1-68083-800-8

Semantics for Robotic Mapping, Perception and Interaction: A Survey
Sourav Garg, Niko Sünderhauf, Feras Dayoub, Douglas Morrison, Akansel Cosgun, Gustavo Carneiro, Qi Wu, Tat-Jun Chin, Ian Reid, Stephen Gould, Peter Corke and Michael Milford
ISBN: 978-1-68083-768-1
Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice

Quanyan Zhu
New York University
qz494@nyu.edu

Stefan Rass
Universität Klagenfurt
stefan.rass@aau.at

Bernhard Dieber
Joanneum Research
bernhard.dieber@joanneum.at

Víctor Mayoral Vilches
Alias Robotics
& Universität Klagenfurt
victor@aliasrobotics.com
Editorial Scope

Topics

Foundations and Trends® in Robotics publishes survey and tutorial articles in the following topics:

• Mathematical modelling
• Kinematics
• Dynamics
• Estimation Methods
• Robot Control
• Planning
• Artificial Intelligence in Robotics

• Software Systems and Architectures
• Mechanisms and Actuators
• Sensors and Estimation
• Planning and Control
• Human-Robot Interaction
• Industrial Robotics
• Service Robotics

Information for Librarians

Foundations and Trends® in Robotics, 2021, Volume 9, 4 issues. ISSN paper version 1935-8253. ISSN online version 1935-8261. Also available as a combined paper and online subscription.
## Contents

1 Introduction to Robot Security ......................................................... 3
   1.1 The Need for Cybersecurity in Robotics ................................. 4
   1.2 Overview of Security Challenges and Solutions ....................... 6
   1.3 Need for Quantitative Methods ........................................... 9

2 Cyber Issues, Security Architectures and Robot Operating System (ROS) Vulnerabilities .............................. 13
   2.1 The Robot Operating System ............................................ 13
   2.2 Vulnerabilities of the Robot Operating System ....................... 15
   2.3 Securing the Application Programmers Interface (API) ............. 18
   2.4 Vulnerabilities of AI-Enabled Robotic Systems ........................ 29

3 Security of Networked Robotic Systems ........................................ 35
   3.1 Security in ROS Networked Systems ..................................... 35
   3.2 Security for Industrial Multi-Agent Robotic Systems ............... 43

4 Security Practice and Design ....................................................... 53
   4.1 Penetration Testing ....................................................... 54
   4.2 Vulnerability Scanning ................................................... 54
   4.3 DevSecOps .............................................................. 58
   4.4 Relevant International Standards ....................................... 64
5 Game Theory for Security 68
5.1 Introduction by Example: Chasing the Adversary on Attack Graphs 69
5.2 Introduction to Security Games and Strategic Defenses 76
5.3 Multi-Stage and Multi-Phase Games 84
5.4 Examples of Game-Theoretic Analysis 94

6 Discussions and Conclusions 99

Acknowledgements 106

References 110
Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice

Quanyan Zhu, Stefan Rass, Bernhard Dieber and Víctor Mayoral Vilches

1 New York University, USA; qz494@nyu.edu
2 Universität Klagenfurt, Austria; stefan.rass@aau.at
3 Joanneum Research, Austria; bernhard.dieber@joanneum.at
4 Alias Robotics, Spain and Universität Klagenfurt, Austria; victor@aliasrobotics.com; v1mayoralv@edu.aau.at

ABSTRACT

Robotics is becoming more and more ubiquitous, but the pressure to bring systems to market occasionally goes at the cost of neglecting security mechanisms during the development, deployment or while in production. As a result, contemporary robotic systems are vulnerable to diverse attack patterns, and an a posteriori hardening is at least challenging, if not impossible at all. This book aims to stipulate the inclusion of security in robotics from the earliest design phases onward and with a special focus on the cost-benefit tradeoff that can otherwise be an inhibitor for the fast development of affordable systems. We advocate quantitative methods of security management and design, covering vulnerability scoring systems tailored to robotic systems, and accounting for the highly distributed nature of robots as an interplay of potentially very many components. A powerful quantitative approach to model-based security is offered.

by game theory, providing a rich spectrum of techniques to optimize security against various kinds of attacks. Such a multi-perspective view on security is necessary to address the heterogeneity and complexity of robotic systems. This book is intended as an accessible starter for the theoretician and practitioner working in the field.
Robotic technology has been around for many years now with its main application being in automation where millions of robots have been deployed over the past decades. In recent years, inflexible automation is starting to shift out of focus of the robotics research and we move towards using robots in flexible manufacturing (marching towards lot size 1) and intralogistics. Service robots are set out to pervade also non-industrial areas like healthcare as well as public and private spaces. The gain in flexibility and capabilities of modern robots has been largely fuelled by the convergence of classical computing and networking technology with robotics. The new generation of robots cannot perform their tasks without being connected to the outside world. Flexible manufacturing and intralogistics robots need to be connected to manufacturing execution systems and fleet management services. Service robots are supposed to provide more value by being connected to the cloud to retrieve commands and updates. While the new capabilities make the areas of application for robots broader, they also become susceptible to external manipulation. This new threat from the cyber world has not yet been sufficiently addressed up to now.
In this book, we review the causes of robot insecurity also reflecting the underlying causes like complexity and market pressure. We present the vulnerabilities and potential fixes of the most important software framework in robotics. Then, we describe modern approaches to securing robots including processes and standards but most importantly also present the potential benefits promised by the introduction of quantitative security methods.

1.1 The Need for Cybersecurity in Robotics

A robot is in general a complex machine which is by itself difficult to design, build and program. The main focus when building a robot is in making it reliable and safe. Security is often of a lower priority since it adds even more complexity to building the robot. In addition, cybersecurity has traditionally not been a concern when designing or using robots since classical industrial applications of robots did not require any connectivity to the outside. With the current trend towards connected robots, however, a technology that is not fit for this trend meets all the threats that come with connecting robots. Generally speaking, today’s robots are easy prey even for less skilled attackers since security achievements that have been successfully used in the Information Technology (IT) area in the past three decades like firewalls, hardened endpoints, or encrypted communication are typically not part of a robotic system. In addition, a security-oriented mindset is also hardly taught in the education of roboticists.

1.1.1 What are special requirements for cybersecurity in robotics?

In general, cybersecurity for robotics draws from the methods of IT-security. However, there are specialties in robotics, that need additional consideration (Mayoral-Vilches et al., 2019). First and most obviously, robots are cyber-physical systems and as such, they have a representation in the physical world. This yields two security-relevant aspects. First, robots can be physically manipulated. Too often, we find exposed network- or USB-ports in robots that can easily be exploited by an attacker. This is especially problematic with mobile robots that move...
autonomously in little-controlled areas. Second, robots can have significant impacts on the physical safety of persons around them. In general, the regulations for robot safety are very strict to prevent any human harm by a robot. However, much of the required safety functions can be attacked remotely thus, effectively rendering the safety methods useless. Despite this, safety regulations do not (yet) require security measures to be put into place. Section 1.1.1 shows a Proof of Concept (PoC) attack that demonstrates the seriousness of this issue.

Robots that are used in automation are also aimed at high availability. This means that they should preferably operate non-stop. Thus, as it is common in Operational Technology (OT), industrial robots are not commonly supplied with regular updates that could fix vulnerabilities.

A PoC to remotely disable a robot’s safety subsystem

A practical attack on a robot’s safety subsystem has been presented in Taurer et al. (2019). The target of the PoC was a mobile robot for transport tasks in the industry. The safety system of the robot is responsible to stop the platform before it hits an obstacle. This is realized using safety-rated laser scanners connected to a safety Programmable Logic Controller (PLC) which cuts the power to the motors in case an object is too close to the robot. Figure 1.1 shows a logical overview of the aforementioned components and their interconnections.

Due to several misconfigurations and negligence of standard security procedures (like changing default passwords), it is possible to retrieve, manipulate and re-upload the safety program logic running on the dedicated safety PLC in the robot. The robot itself hosts a WiFi hotspot that uses a default password. Access to the WiFi also provides access to all connected devices since no network separation policy is in place. Thus, an attacker could easily gain access to the robot’s internal network. The safety PLC is connected to the robot’s internal network. During its integration, the default password required to upload a program to the PLC was not changed. The attacker can access the PLC via WiFi and download the program stored on it. After a simple change that renders the laser scanners’ inputs useless, the program can be re-uploaded. From this point on, the robot will still detect obstacles but it will not stop for
them. Since those robots can carry up to 250kg, they pose significant health risks when they collide with a person. Note, that in course of the modifications, not only the safety laser scanners but also the emergency stop can be rendered useless.

The vulnerability described has been acknowledged by the robot manufacturer and was fixed in the meantime. Still, it shows how easily robots can be attacked and that establishing security practices in robotics is highly necessary.

1.2 Overview of Security Challenges and Solutions

Robotic security adds a dimension of physical interaction to the requirements of general information security. Contrary to classical protection of data from theft, manipulation, etc., a physical consequence of a data breach is usually not in the center of attention there, but not so for robotics. The intended close contact, up to collaboration, with humans, adds its own set of security requirements beyond the classical CIA+ (confidentiality, integrity, availability, and authenticity), and also induces ethical challenges. Those get more involved by the fact that robot systems are often heterogeneous, making the assignment and taking of responsibilities difficult in light of many actors being involved.
1.2. Overview of Security Challenges and Solutions

This book is focused on the technical possibilities of implementing security, reaching up to industrial standards, and best practices to follow when building a secure robot. Chapter 2 sets the ground by reviewing the ROS as a popular (de facto standard) platform to run robot systems, thereby pointing out some threats and countermeasures that can be addressed “classically” (i.e., using standard security mechanisms). The distributed nature of robotics, however, calls for a broader view extended to cover the interaction of possibly many components, which has its challenges. Among them are the necessary division of views (dividing data layers vs. computational graphs, etc.) and the treatment of multi-agent systems as groups in which possibly many players can become hostile or otherwise deviate from the intended orchestration. We discuss security along these lines in Chapter 3. Experience with vulnerabilities and successful attack reports have led to the development of various tools and methods to help designers of a robot system with testing and general security management, and Chapter 4 is devoted to an introduction and overview of these practices. Conditional on an understanding of the overall diversity and interdependency in robot systems, partially gained with help of tools, but also proper design processes (e.g., DevSecOps), one can proceed further by defining mathematical models to quantify and thereby optimize security systematically, as an account for the tradeoff between investment, time to market pressure, and the security achievable under budget and time limitations. This model-based economic approach to security, see Figure 1.2, including the technical and organizational practices relative to security cost-benefits, is what game-theoretic techniques can help with.

Chapter 5 provides a primer of game theory, starting with an introduction by the example of a game describing a penetrating adversary versus a defending security officer, to illustrate the overall idea of how mathematical games are applicable to security. From this, we take a deeper dive into the variety of game-theoretic models designed for security, and how to combine them into bigger models of robot systems. The diversity and heterogeneity of a robot system are thereby matched with the (equal) diversity of game-theoretic security models tailored to many different scenarios of attack and defense. Chapter 5 is meant as a starting point here.
We remark that this book does not intend to cover non-technical matters like ethics or the generalities of development processes, staff recruiting and human resources security, or legal issues like liabilities or insurance. Without doubting their relevance for robot security, their discussion and treatment are out of our scope here. A survey of all known threats is not the focus of this book. We refer the reader to the lot of existing work in this direction, partly coming from other domains (as provided by Heartfield et al., 2018, Simmons et al., 2009 and others) but also related explicitly to robotics, such as the work of Lera et al. (2017) and the Open Source Robotics Foundation, Inc. (2021). Since robots are special cases of general distributed cyber-physical systems, threat taxonomies from this larger area apply well for robotics too. Furthermore, risk management standards like ISO31000 or IEC-62443, discussed in Section 4.4, provide threat categorizations and ways to systematically identify, classify, and address cyber-security along all virtual and physical aspects. We thus refrain from deep dives into taxonomies here, for the sake of discussing a useful practical tool being the classification of threats along with a common set of attributes to rank threats and vulnerabilities in terms of severity, efforts to fix, and other security management related...
1.3 Need for Quantitative Methods

A robot is a system of systems. One that comprises sensors to perceive its environment, actuators to act on it and computation to process it all and respond coherently to its application (Vilches, 2020). We can divide robotic systems into two layers, as illustrated in Figure 1.3. One is the OT layer which consists of devices and components that directly monitor and control the mechatronic processes and events, such as autonomous vehicles, robotic arms, and humanoids. The other one is the IT layer which consists of information and communication devices that collect, communicate, and process data, such as computer networks, cloud computing, and servers. Many robotic system designs often view safety as one of the major OT-level system criteria. The design for safety is an integral part of the systematic methodologies in the design process. On the contrary, cybersecurity at the IT-level is not yet a key factor considered in the design of robotic systems. When security issues arise, add-on solutions such as patching and firewalls are introduced to harden the system security. However, these solutions can be easily evaded by a sophisticated attacker as we have seen in recent Advanced Persistent Threats (APTs). An attacker can leverage social engineering, stay stealthy in the system for a prolonged period of time, and learn the system configurations to acquire credentials and escalate privilege to reach the asset. The defective IT-security is a potential cyber hazard for OT-safety.

It is essential to see that OT-level safety and IT-level security are intertwined. The ignorance of IT-security will enable an attacker to take over the control of OT and create human-induced devastating incidents. Reversely, the goal of IT-security is to provide the necessary support to OT to provide performance assurance and dependability. It is insufficient to focus merely on OT-level safety issues and adopt perfunctory solutions to protect the IT from advanced attacks.
Figure 1.3: The integration and interaction between IT and OT in robotics

Quantitative metrics and frameworks play an essential role in a formal understanding of the IT/OT interdependencies and the development of risk assessment tools and security solutions. Game theory is a promising scientific method to address this need. Game theory has a long history since the 1950s and a rich set of analytical and computational tools that can be used to capture the competitive and strategic behaviors between an attacker and a defender. The solid mathematical foundation of game theory provides a rigorous framework to analyze and predict the outcome of the interactions between an attacker and a defender.

Game theory provides a theoretical underpinning for the analysis of this tradeoff between security and performance under a prescribed set of attack models. A standard normal-form game is composed of three elements: players, action sets, and utility functions or preferences over action sets. The action sets can encode the system constraints, while the utility function can capture the IT and OT performances and their interplay. The interdependencies between the IT and the OT can be formally described by specifying the preferences over the set of joint IT/OT configurations and designs.

Not only does the game framework encode the key design features, the equilibrium concept of games but also provides a predictive outcome of the interactions, where no parties have the incentive to deviate...
from their actions unilaterally. The analysis of the equilibrium solution enables the quantitative risk assessment in a strategically adversarial environment. In addition, the analysis of equilibrium strategies of the game leads to a new paradigm of security solutions. Instead of aiming for a perfect security solution, which is either cost-prohibitive or practically impossible, game theory enables the design of best-effort IT-and-OT-security by taking into account the security objectives of the systems, the system resource constraints, and the attacker’s capabilities.

Modern extensions of the game-theoretic framework by including uncertainties, epistemic modeling, and learning dynamics enable the creation of sophisticated defense mechanisms such as autonomous and adaptive strategies, moving target defense, and cyber deception. The defense mechanisms can go beyond the traditional manual and static configurations to dynamic, data-driven, and automated operations of defense. In addition, the game models can be sequentially composed to capture the multi-stage and multi-phase nature of APTs. Each game model represents a modularized interaction in a subsystem. The composition of multiple games pieces together a holistic view of the multi-dimensional dynamic interactions in the entire system, which include the ones between the defender and the attacker, as well as the ones between subsystems. The holistic game is also called games-in-games, where one game is nested in the other games. This structure enables the defense to localize the attack behaviors by zooming into a local subsystem and optimize the system-wide performance by zooming out to view the system holistically.

Chapter 5 will first provide an introduction to game-theoretic methods by an example of an attack-graph game. The second part of the chapter will present an overview of security games and their applications. One important class of games that are useful to address sophisticated attacks is the multi-stage and multi-phase security game. Game models for multiple subsystems at different phases can be composed together to address the complex security problems holistically. The chapter presents several case studies to elaborate on game-theoretic methodologies. One case study presents a cyber-physical signaling game to develop an impact-aware trust mechanism that can reject high-risk inputs and mitigate the physical damages. The second case study introduces a jam-
ming game between a jammer and a team of robots that aim to reach consensus through mutual pursuits and communications. A multi-stage game is formulated to analyze the equilibrium and develop anti-jamming strategies.


Full text available at: [http://dx.doi.org/10.1561/2300000061](http://dx.doi.org/10.1561/2300000061)


References


References


Vilches, V. M. (2020). “IT, OT, IoT and Robotics, a security comparison”.


References


