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

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Robotics

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

Quanyan Zhu, Stefan Rass, Bernhard Dieber, Víctor Mayoral Vilches. *Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice*. Foundations and Trends® in Robotics, vol. 9, no. 1, pp. 1–129, 2021.

ISBN: 978-1-68083-861-9

Foundations and Trends® in Robotics
Volume 9, Issue 1, 2021

Editorial Board

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

Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice

Quanyan Zhu[1], Stefan Rass[2], Bernhard Dieber[3] and Víctor Mayoral Vilches[4]

[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

Quanyan Zhu, Stefan Rass, Bernhard Dieber and Víctor Mayoral Vilches (2021), "Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice", Foundations and Trends® in Robotics: Vol. 9, No. 1, pp 1–129. DOI: 10.1561/10.1561/2300000061.

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.

1

Introduction to Robot Security

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

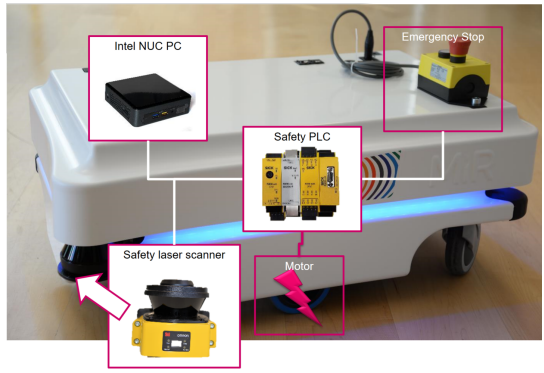

Figure 1.1: A logical overview of the internals of an MiR-100 robot (from Taurer *et al.* (2019)

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.

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.

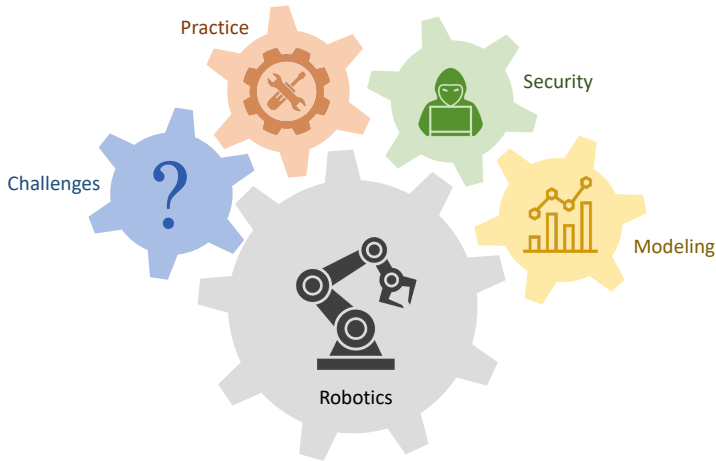

Figure 1.2: This book investigates challenges, quantitative modeling and the practice of cybersecurity issues in robotic systems.

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

aspects. We pay explicit attention to such methods, specifically the Robot Vulnerability Scoring System (RVSS) (Mayoral-Vilches *et al.*, 2018) as an extension to the popular Common Vulnerability Scoring System (CVSS), later in Section 4.2.

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.

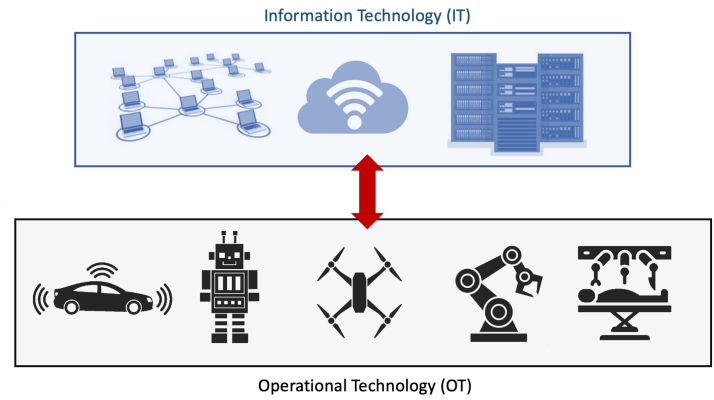

Figure 1.3: The integration and interaction between IT and OT in robotics

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.

References

Aghassi, M. and D. Bertsimas. (2006). "Robust game theory". *Mathematical Programming*. 107(1-2): 231–273. DOI: 10.1007/s10107-005-0686-0.

Alias Robotics. (2020). "Red Teaming ROS-Industrial, extended version". https://aliasrobotics.com/files/red_teaming_rosindustrial.pdf.

Alpcan, T. and T. Başar. (2004). "A game theoretic analysis of intrusion detection in access control systems". In: *Decision and Control, 2004. CDC. 43rd IEEE Conference on*. Vol. 2. IEEE. 1568–1573.

Alzahrani, N. and N. Bulusu. (2018). "Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness". In: *Decision and Game Theory for Security*. Ed. by L. Bushnell, R. Poovendran, and T. Başar. Vol. 11199. Cham: Springer International Publishing. 465–485. DOI: 10.1007/978-3-030-01554-1_27. (Accessed on 07/19/2019).

Basak, A., J. Čern, M. Gutierrez, S. Curtis, C. Kamhoua, D. Jones, B. Bošansk, and C. Kiekintveld. (2018). "An initial study of targeted personality models in the flipit game". In: *International conference on decision and game theory for security*. Springer. 623–636.

Basar, T. (1983). "The Gaussian test channel with an intelligent jammer". *IEEE Transactions on Information Theory*. 29(1): 152–157.

Başar, T. and G. J. Olsder. (1999). *Dynamic noncooperative game theory*. Vol. 23. Siam.

Bianchin, G., Y.-C. Liu, and F. Pasqualetti. (2020). "Secure Navigation of Robots in Adversarial Environments". *IEEE Control Systems Letters*. 4(1): 1–6. DOI: 10.1109/LCSYS.2019.2921753. (Accessed on 05/13/2020).

Bolot, J. and M. Lelarge. (2009). "Cyber Insurance as an Incentivefor Internet Security". In: *Managing information risk and the economics of security*. Springer. 269–290.

Boumkheld, N., S. Panda, S. Rass, and E. Panaousis. (2019). "Honeypot Type Selection Games for Smart Grid Networks". In: *Decision and Game Theory for Security*. Ed. by T. Alpcan, Y. Vorobeychik, J. S. Baras, and G. Dán. Cham: Springer International Publishing. 85–96.

Canzani, E. (2018). "Risk Management in (Cyber-) Terrorism: Modeling Insights and Perspectives". *Countering Terrorist Activities in Cyberspace*. 139: 131.

Carroll, T. E. and D. Grosu. (2011). "A game theoretic investigation of deception in network security". *Security and Communication Networks*. 4(10): 1162–1172.

Casey, W., J. A. Morales, E. Wright, Q. Zhu, and B. Mishra. (2016). "Compliance signaling games: toward modeling the deterrence of insider threats". *Computational and Mathematical Organization Theory*. 22(3): 318–349. URL: http://link.springer.com/article/10.1007/s10588-016-9221-5.

Chauveau, T. (2012). "Subjective risk and disappointment". *Documents de travail du Centre d'Economie de la Sorbonne*. Université Panthéon-Sorbonne (Paris 1), Centre d'Economie de la Sorbonne. URL: https://EconPapers.repec.org/RePEc:mse:cesdoc:12063.

Chen, J., C. Touati, and Q. Zhu. (2017). "Heterogeneous multi-layer adversarial network design for the IoT-enabled infrastructures". In: *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE. 1–6.

Chen, J., C. Touati, and Q. Zhu. (2019a). "A dynamic game approach to strategic design of secure and resilient infrastructure network". *IEEE Transactions on Information Forensics and Security*. 15: 462–474.

Chen, J., C. Touati, and Q. Zhu. (2019b). "Optimal Secure Two-Layer IoT Network Design". *IEEE Transactions on Control of Network Systems*: 1–1. DOI: 10.1109/TCNS.2019.2906893.

Chen, J. and Q. Zhu. (2016a). "Interdependent Network Formation Games". *arXiv preprint arXiv:1602.07745*. URL: https://arxiv.org/abs/1602.07745.

Chen, J. and Q. Zhu. (2016b). "Interdependent network formation games with an application to critical infrastructures". In: *American Control Conference (ACC), 2016*. IEEE. 2870–2875. URL: http://ieeexplore.ieee.org/abstract/document/7525354/.

Chen, J. and Q. Zhu. (2016c). "Optimal Contract Design Under Asymmetric Information for Cloud-Enabled Internet of Controlled Things". In: *International Conference on Decision and Game Theory for Security*. Springer International Publishing. 329–348. URL: http://link.springer.com/chapter/10.1007/978-3-319-47413-7_19.

Chen, J. and Q. Zhu. (2016d). "Optimal contract design under asymmetric information for cloud-enabled internet of controlled things". In: *International Conference on Decision and Game Theory for Security*. Springer. 329–348.

Chen, J. and Q. Zhu. (2016e). "Resilient and decentralized control of multi-level cooperative mobile networks to maintain connectivity under adversarial environment". In: *IEEE Conference on Decision and Control (CDC)*. 5183–5188.

Chen, J. and Q. Zhu. (2017). "Interdependent strategic cyber defense and robust switching control design for wind energy systems". In: *2017 IEEE Power & Energy Society General Meeting*. IEEE. 1–5.

Chen, J. and Q. Zhu. (2019a). *A Game-and Decision-Theoretic Approach to Resilient Interdependent Network Analysis and Design*. Springer.

Chen, J. and Q. Zhu. (2019b). "Control of multi-layer mobile autonomous systems in adversarial environments: A games-in-games approach". *IEEE Transactions on Control of Network Systems, submitted*.

Choudhury, A., D. McGrew, and J. Salowey. (2008). *AES Galois Counter Mode (GCM) Cipher Suites for TLS*. URL: https://tools.ietf.org/html/rfc5288 (accessed on 11/26/2020).

Cichy, C. and S. Rass. (2019). "An Overview of Data Quality Frameworks". *IEEE Access*. 7: 24634–24648. DOI: 10.1109/ACCESS.2019.2899751. (Accessed on 07/04/2019).

Clark, A., Q. Zhu, R. Poovendran, and T. Başar. (2012). "Deceptive routing in relay networks". In: *Decision and Game Theory for Security*. Springer. 171–185.

Clark, A., Q. Zhu, R. Poovendran, and T. Başar. (2013). "An impact-aware defense against Stuxnet". In: *2013 American Control Conference*. IEEE. 4140–4147.

Commission, I. E. *et al.* (2009). "Industrial Communication Networks Network and System Security Part 1-1: Terminology, Concepts and Models, IEC". *Tech. rep.* TS 62443-1-1 ed1. 0, Geneva, Switzerland.

CyVision Technologies. (2020). *Cauldron*. URL: https://www.benvenisti.net/cauldron (accessed on 11/30/2020).

Dieber, B., S. Kacianka, S. Rass, and P. Schartner. (2016). "Application-level security for ROS-based applications". In: *2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. 4477–4482. DOI: 10.1109/IROS.2016.7759659.

Dieber, B., B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner. (2017). "Security for the Robot Operating System". *Robotics and Autonomous Systems*. 98: 192–203. DOI: 10.1016/j.robot.2017.09.017.

Dieber, B., R. White, S. Taurer, B. Breiling, G. Caiazza, H. Christensen, and A. Cortesi. (2020). "Penetration Testing ROS". In: *Robot Operating System (ROS)*. Ed. by A. Koubaa. Vol. 831. Cham: Springer International Publishing. 183–225. DOI: 10.1007/978-3-030-20190-6_8. (Accessed on 11/26/2020).

Directive, E. M. (2006). "42/EC of the European Parliament and the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)". *Official Journal of the European Union L*. 157(09): 07.

Farhang, S., M. H. Manshaei, M. N. Esfahani, and Q. Zhu. (2014). "A dynamic bayesian security game framework for strategic defense mechanism design". In: *International conference on decision and game theory for security*. Springer. 319–328.

Fung, C., Q. Zhu, R. Boutaba, and T. Başar. (2011). "SMURFEN: A system framework for rule sharing collaborative intrusion detection". In: *2011 7th International Conference on Network and Service Management*. IEEE. 1–6.

Fung, C. J. and Q. Zhu. (2016). "FACID: A trust-based collaborative decision framework for intrusion detection networks". *Ad Hoc Networks*. 53: 17–31.

Fung, C. J., Q. Zhu, R. Boutaba, and T. Başar. (2010). "Bayesian decision aggregation in collaborative intrusion detection networks". In: *2010 IEEE Network Operations and Management Symposium-NOMS 2010*. IEEE. 349–356.

Gibbons, R. S. (1992). *Game theory for applied economists*. Princeton University Press.

Greenbone Networks GmbH. (2020). *OpenVAS - OpenVAS - Open Vulnerability Assessment Scanner*. URL: https://www.openvas.org/ (accessed on 11/27/2020).

Gul, F. (1991). "A Theory of Disappointment Aversion". *Econometrica*. 59(3): 667. DOI: 10.2307/2938223.

Hansen, T. and D. E. Eastlake. (2006). *US Secure Hash Algorithms (SHA and HMAC-SHA)*. (Accessed on 11/26/2020).

Hansen, T. and D. E. Eastlake. (2011). *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*. (Accessed on 11/26/2020).

Hayel, Y. and Q. Zhu. (2015). "Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks". In: *Decision and Game Theory for Security*. Springer. 22–34.

Heartfield, R., G. Loukas, S. Budimir, A. Bezemskij, J. R. Fontaine, A. Filippoupolitis, and E. Roesch. (2018). "A taxonomy of cyber-physical threats and impact in the smart home". en. *Computers & Security*. 78(Sept.): 398–428. DOI: 10.1016/j.cose.2018.07.011. (Accessed on 03/04/2021).

Houmb, S. H. and V. N. L. Franqueira. (2009). "Estimating ToE Risk Level using CVSS". In: Proceedings of the International Conference on Availability, Reliability and Security. IEEE Computer Society Press. 718–725.

Huang, J. W., Q. Zhu, V. Krishnamurthy, and T. Başar. (2010). "Distributed correlated Q-learning for dynamic transmission control of sensor networks". In: *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*. IEEE. 1982–1985.

Huang, L., J. Chen, and Q. Zhu. (2017). "A large-scale markov game approach to dynamic protection of interdependent infrastructure networks". In: *International Conference on Decision and Game Theory for Security*. Springer. 357–376.

Huang, L., J. Chen, and Q. Zhu. (2018). "Distributed and optimal resilient planning of large-scale interdependent critical infrastructures". In: *2018 Winter Simulation Conference (WSC)*. IEEE. 1096–1107.

Huang, L. and Q. Zhu. (2018a). "Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-physical Systems". In: *International Conference on Decision and Game Theory for Security*.

Huang, L. and Q. Zhu. (2018b). "Analysis and computation of adaptive defense strategies against advanced persistent threats for cyber-physical systems". In: *International Conference on Decision and Game Theory for Security*. Springer. 205–226.

Huang, L. and Q. Zhu. (2019a). "Adaptive honeypot engagement through reinforcement learning of semi-markov decision processes". In: *International Conference on Decision and Game Theory for Security*. Springer. 196–216.

Huang, L. and Q. Zhu. (2019b). "Dynamic Bayesian Games for Adversarial and Defensive Cyber Deception". In: *Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*. Ed. by E. Al-Shaer, J. Wei, K. W. Hamlen, and C. Wang. Cham: Springer International Publishing. 75–97.

Huang, Y., J. Chen, L. Huang, and Q. Zhu. (2020a). "Dynamic Games for Secure and Resilient Control System Design". *National Science Review*: to appear. URL: https://doi.org/10.1093/nsr/nwz218.

Huang, Y., J. Chen, L. Huang, and Q. Zhu. (2020b). "Dynamic games for secure and resilient control system design". *National Science Review*. 7(7): 1125–1141.

Huang, Y. and Q. Zhu. (2019c). "Deceptive reinforcement learning under adversarial manipulations on cost signals". In: *International Conference on Decision and Game Theory for Security*. Springer. 217–237.

"ICRA 2020 Workshop". (2020). https://sites.google.com/view/icra-workshop-2020.

Jajodia, S., A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang. (2011). *Moving target defense: creating asymmetric uncertainty for cyber threats*. Vol. 54. Springer Science & Business Media.

Jajodia, S., V. Subrahmanian, V. Swarup, and C. Wang. (2016). *Cyber deception*. Vol. 6. Springer.

Joanneum ROBOTICS. (2020). "jr-robotics/ROSPenTo". (Accessed on 11/30/2020).

Jonsson, J., K. Moriarty, B. Kaliski, and A. Rusch. (2016). *PKCS #1: RSA Cryptography Specifications Version 2.2*. URL: https://tools.ietf.org/html/rfc8017 (accessed on 11/26/2020).

Josang, A. and R. Ismail. (2002). "The beta reputation system". In: *Proceedings of the 15th bled electronic commerce conference*. Vol. 5. 2502–2511.

Joseph, A. D., B. Nelson, B. I. Rubinstein, and J. Tygar. (2018). *Adversarial machine learning*. Cambridge University Press.

Kehoe, B., S. Patil, P. Abbeel, and K. Goldberg. (2015). "A survey of research on cloud robotics and automation". *IEEE Transactions on automation science and engineering*. 12(2): 398–409.

König, S., A. Gouglidis, B. Green, and A. Solar. (2018). "Assessing the Impact of Malware Attacks in Utility Networks". In: *Rass, S. and Schauer, S. (eds.) Game Theory for Security and Risk Management: From Theory to Practice*. Cham: Springer International Publishing. 335–351. DOI: 10.1007/978-3-319-75268-6_14.

Konnov, I. (2003). "On Lexicographic Vector Equilibrium Problems". en. *Journal of Optimization Theory and Applications*. 118(3): 681–688. DOI: 10.1023/B:JOTA.0000004877.39408.80. (Accessed on 06/12/2020).

Kurt, M. N., O. Ogundijo, C. Li, and X. Wang. (2018). "Online cyber-attack detection in smart grid: A reinforcement learning approach". *IEEE Transactions on Smart Grid*. 10(5): 5174–5185.

La, Q. D., T. Q. S. Quek, and J. Lee. (2016). "A game theoretic model for enabling honeypots in IoT networks". In: *2016 IEEE International Conference on Communications (ICC)*. Kuala Lumpur, Malaysia: IEEE. 1–6. DOI: 10.1109/ICC.2016.7510833. (Accessed on 05/13/2019).

Lera, F. J. R., C. F. Llamas, A. M. Guerrero, and V. M. Olivera. (2017). "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety". en. In: *Robotics - Legal, Ethical and Socioeconomic Impacts*. Ed. by G. Dekoulis. InTech. DOI: 10.5772/intechopen.69796. (Accessed on 03/04/2021).

Liu, N., M. Du, and X. Hu. (2020). "Adversarial Machine Learning: An Interpretation Perspective". *arXiv:2004.11488 [cs, stat]*. Apr. URL: http://arxiv.org/abs/2004.11488 (accessed on 07/10/2020).

Manshaei, M. H., Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux. (2013). "Game theory meets network security and privacy". *ACM Computing Surveys (CSUR)*. 45(3): 25.

Masinter, L., T. Berners-Lee, and R. T. Fielding. (2016). "Uniform Resource Identifier (URI): Generic Syntax". URL: %5Curl%7Bhttps://tools.ietf.org/html/rfc3986%7D (accessed on 11/26/2020).

Mayoral-Vilches, V., E. Gil-Uriarte, I. Zamalloa Ugarte, G. Olalde Mendia, R. Izquierdo Pisón, L. Alzola Kirschgens, A. Bilbao Calvo, A. Hernández Cordero, L. Apa, and C. Cerrudo. (2018). "Towards an open standard for assessing the severity of robot security vulnerabilities, the Robot Vulnerability Scoring System (RVSS)". *ArXiv e-prints*. July. arXiv: 1807.10357 [cs.RO].

Mayoral-Vilches, V., L. A. Kirschgens, A. B. Calvo, A. H. Cordero, R. I. Pisón, D. M. Vilches, A. M. Rosas, G. O. Mendia, L. U. S. Juan, I. Z. Ugarte, E. Gil-Uriarte, E. Tews, and A. Peter. (2019). "Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics". arXiv: 1806.04042 [cs.CR].

Mayoral-Vilches, V., I. Abad-Fernández, M. Pinzger, S. Rass, B. Dieber, A. Cunha, F. J. Rodrıguez-Lera, G. Lacava, A. Marotta, F. Martinelli, *et al.* (2020a). "alurity, a toolbox for robot cybersecurity". *arXiv preprint arXiv:2010.07759*.

Mayoral-Vilches, V., N. Garcıa-Maestro, M. Towers, and E. Gil-Uriarte. (2020b). "DevSecOps in Robotics". *arXiv preprint arXiv:2003.10402*.

Mayoral-Vilches, V., M. Pinzger, S. Rass, B. Dieber, and E. Gil-Uriarte. (2020c). "Can ROS be used securely in industry? Red teaming ROS-Industrial". *arXiv preprint arXiv:2009.08211*.

McClean, J., C. Stull, C. Farrar, and D. Mascarenas. (2013). "A preliminary cyber-physical security assessment of the robot operating system (ros)". In: *Unmanned Systems Technology XV*. Vol. 8741. International Society for Optics and Photonics. 874110.

McCloghrie, K., U. Blumenthal, and F. Maino. (2004). "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model". (Accessed on 11/26/2020).

Miao, F. and Q. Zhu. (2014). "A moving-horizon hybrid stochastic game for secure control of cyber-physical systems". In: *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*. IEEE. 517–522.

Miura-Ko, R., B. Yolken, J. Mitchell, and N. Bambos. (2008). "Security decision-making among interdependent organizations". In: *Computer Security Foundations Symposium, 2008. CSF'08. IEEE 21st*. IEEE. 66–80.

Moghaddam, M. M., M. H. Manshaei, and Q. Zhu. (2015). "To Trust or Not: A Security Signaling Game Between Service Provider and Client". In: *Decision and Game Theory for Security*. Springer. 322–333.

Mokube, I. and M. Adams. (2007). "Honeypots: concepts, approaches, and challenges". In: *Proceedings of the 45th annual southeast regional conference*. 321–326.

Monga, A. and Q. Zhu. (2016). "On solving large-scale low-rank zero-sum security games of incomplete information". In: *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on*. IEEE. 1–6. URL: http://ieeexplore.ieee.org/abstract/document/7823923/.

Nash, J. F. *et al.* (1950). "Equilibrium points in n-person games". *Proceedings of the national academy of sciences*. 36(1): 48–49.

Neumann, C., T. Yu, S. Hartman, and K. Raeburn. (2005). "The Kerberos Network Authentication Service (V5)".

Noureddine, M. A., A. Fawaz, W. H. Sanders, and T. Başar. (2016). "A game-theoretic approach to respond to attacker lateral movement". In: *International Conference on Decision and Game Theory for Security*. Springer. 294–313.

Nugraha, Y., A. Cetinkaya, T. Hayakawa, H. Ishii, and Q. Zhu. (2020). "Dynamic resilient network games considering connectivity". In: *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE. 3779–3784.

Nugraha, Y., T. Hayakawa, A. Cetinkaya, H. Ishii, and Q. Zhu. (2019). "Subgame perfect equilibrium analysis for jamming attacks on resilient graphs". In: *2019 American Control Conference (ACC)*. IEEE. 2060–2065.

Open Robotics. (2020). *roswtf - ROS Wiki*. URL: http://wiki.ros.org/roswtf (accessed on 11/30/2020).

Open Source Robotics Foundation, Inc. (2021). "ROS 2 Robotic Systems Threat Model". URL: https://design.ros2.org/articles/ros2_threat_model.html.

Pan, Y., G. Peng, J. Chen, and Q. Zhu. (2020). "MASAGE: Model-Agnostic Sequential and Adaptive Game Estimation". In: *International Conference on Decision and Game Theory for Security*. Springer. 365–384.

Pawlick, J. (2018). "A Systems Science Perspective on Deception for Cybersecurity in the Internet of Things". English. *PhD thesis*. 227.

Pawlick, J., J. Chen, and Q. Zhu. (2018a). "iSTRICT: An interdependent strategic trust mechanism for the cloud-enabled internet of controlled things". *IEEE Transactions on Information Forensics and Security*. 14(6): 1654–1669.

Pawlick, J., E. Colbert, and Q. Zhu. (2017). "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy". *arXiv preprint arXiv:1712.05441*.

Pawlick, J., E. Colbert, and Q. Zhu. (2018b). "Modeling and analysis of leaky deception using signaling games with evidence". *IEEE Transactions on Information Forensics and Security*. 14(7): 1871–1886.

Pawlick, J., E. Colbert, and Q. Zhu. (2019). "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy". *ACM Computing Surveys (CSUR)*. 52(4): 82.

Pawlick, J., S. Farhang, and Q. Zhu. (2015). "Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats". In: *International Conference on Decision and Game Theory for Security*. Springer. 289–308.

Pawlick, J. and Q. Zhu. (2015). "Deception by design: evidence-based signaling games for network defense". *arXiv preprint arXiv:1503.05458*.

Pawlick, J. and Q. Zhu. (2016). "A Stackelberg game perspective on the conflict between machine learning and data obfuscation". In: *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on*. IEEE. 1–6. URL: http://ieeexplore.ieee.org/abstract/document/7823893/.

Pawlick, J. and Q. Zhu. (2017a). "Phishing for Phools in the Internet of Things: Modeling One-to-Many Deception using Poisson Signaling Games". *arXiv preprint arXiv:1703.05234*. URL: https://arxiv.org/abs/1703.05234.

Pawlick, J. and Q. Zhu. (2017b). "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control". *IEEE Transactions on Information Forensics and Security*. 12(12): 2906–2919.

Pawlick, J. and Q. Zhu. (2021). *Game Theory for Cyber Deception: From Theory to Applications*. Springer Nature.

Peng, G., T. Zhang, and Q. Zhu. (2020). "A Data-Driven Distributionally Robust Game Using Wasserstein Distance". In: *International Conference on Decision and Game Theory for Security*. Springer. 405–421.

Pornin, T. (2013). *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*. URL: https://tools.ietf.org/html/rfc6979 (accessed on 11/26/2020).

Quigley, M., K. Conley, B. Gerkey, J. Faust, T. Foote, J. Leibs, R. Wheeler, and A. Y. Ng. (2009). "ROS: an open-source Robot Operating System". In: *ICRA workshop on open source software*. Vol. 3. No. 3.2. Kobe, Japan. 5.

Rahman, M. A., M. H. Manshaei, and E. Al-Shaer. (2013). "A game-theoretic approach for deceiving remote operating system fingerprinting". In: *2013 IEEE Conference on Communications and Network Security (CNS)*. IEEE. 73–81.

Rass, S. (2014). "Complexity of Network Design for Private Communication and the P-vs-NP question". *International Journal of Advanced Computer Science and Applications*. 5(2): 148–157.

Rass, S. and B. Rainer. (2014). "Numerical Computation of Multi-Goal Security Strategies". In: *Decision and Game Theory for Security*. Ed. by R. Poovendran and W. Saad. *LNCS 8840*. Springer. 118–133. DOI: https://doi.org/10.1007/978-3-319-12601-2_7.

Rass, S. (2018a). "Perfectly Secure Communication, based on Graph-Topological Addressing in Unique-Neighborhood Networks". *arXiv preprint arXiv:1810.05602*.

Rass, S. (2018b). "Security Strategies and Multi-Criteria Decision Making". In: *Game Theory for Security and Risk Management.From Theory to Practice*. Ed. by S. Rass and S. Schauer. *Static & dynamic game theory : foundations & applications*. Cham, Switzerland: Birkhäuser. 47–74.

Rass, S. (2018c). "Security Strategies and Multi-Criteria Decision Making". In: *Game Theory for Security and Risk Management*. Ed. by S. Rass and S. Schauer. Cham: Springer International Publishing. 47–74. DOI: 10.1007/978-3-319-75268-6_3. (Accessed on 09/18/2018).

Rass, S., S. Konig, and S. Schauer. (2017a). "Defending Against Advanced Persistent Threats Using Game-Theory". *PLoS ONE*. 12(1): e0168675. DOI: 10.1371/journal.pone.0168675.

Rass, S. and S. König. (2018). "Password Security as a Game of Entropies". *Entropy*. 20(5): 312. DOI: 10.3390/e20050312.

Rass, S., S. König, and E. Panaousis. (2019a). "Cut-The-Rope: A Game of Stealthy Intrusion". In: *Decision and Game Theory for Security*. Ed. by T. Alpcan, Y. Vorobeychik, J. S. Baras, and G. Dán. Vol. 11836. Cham: Springer International Publishing. 404–416. DOI: 10.1007/978-3-030-32430-8_24. (Accessed on 06/19/2020).

Rass, S., S. König, and S. Schauer. (2017b). "On the Cost of Game Playing: How to Control the Expenses in Mixed Strategies". In: *Decision and Game Theory for Security.8th International Conference, GameSec 2017*. [S.l.]: Springer. 494–505. DOI: 10.1007/978-3-319-68711-7_26.

Rass, S. and S. Kurowski. (2013). "On Bayesian Trust and Risk Forecasting for Compound Systems". In: *Proceedings of the 7th International Conference on IT Security Incident Management & IT Forensics (IMF)*. IEEE Computer Society. 69–82. DOI: 10.1109/IMF.2013.13.

Rass, S., B. Rainer, M. Vavti, J. Göllner, A. Peer, and S. Schauer. (2015). "Secure Communication over Software-Defined Networks". *Mobile Networks and Applications*. 20(1): 105–110. DOI: 10.1007/s11036-015-0582-7.

Rass, S., B. Rainer, M. Vavti, and S. Schauer. (2013). "A Network Modeling and Analysis Tool for Perfectly Secure Communication". In: *Proceedings of the 27th IEEE International Conference on Advanced Information Networking and Applications*. IEEE Computer Society Press. 267–275. DOI: 10.1109/AINA.2013.3.

Rass, S. and P. Schartner. (2010). "Multipath Authentication without shared Secrets and with Applications in Quantum Networks". In: *Proceedings of the International Conference on Security and Management (SAM)*. Vol. 1. CSREA Press. 111–115.

Rass, S. and P. Schartner. (2020). "Authentic Quantum Nonces". en. In: *Quantum Random Number Generation: Theory and Practice*. Ed. by C. Kollmitzer, S. Schauer, S. Rass, and B. Rainer. *Quantum Science and Technology*. Cham: Springer International Publishing. 35–44. DOI: 10.1007/978-3-319-72596-3_3. (Accessed on 04/26/2021).

Rass, S. and S. Schauer. (2019). "Refining Stochastic Models of Critical Infrastructures by Observation". In: *Proceedings of the 56th ESReDA Seminar, European Atomic Energy Community. JRC Publications*. No. No JRC118427. Publications Office of the European Union. 212–223. URL: https://ec.europa.eu/jrc/en/publication/critical-services-continuity-resilience-and-security-proceedings-56th-esreda-seminar.

Rass, S., S. Schauer, S. König, and Q. Zhu. (2020a). *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*. SpringerNature.

Rass, S., A. Schorn, and F. Skopik. (2019b). "Trust and Distrust: On Sense and Nonsense in Big Data". en. In: *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*. Ed. by E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, and S. Krenn. Vol. 547. Cham: Springer International Publishing. 81–94. DOI: 10.1007/978-3-030-16744-8_6. (Accessed on 02/04/2020).

Rass, S., A. Wiegele, and S. König. (2020b). "Security Games over Lexicographic Orders". en. In: *Decision and Game Theory for Security*. Ed. by Q. Zhu, J. S. Baras, R. Poovendran, and J. Chen. Vol. 12513. Cham: Springer International Publishing. 422–441. DOI: 10.1007/978-3-030-64793-3_23. (Accessed on 01/14/2021).

Rass, S. and Q. Zhu. (2016). "GADAPT: a sequential game-theoretic framework for designing defense-in-depth strategies against advanced persistent threats". In: *International Conference on Decision and Game Theory for Security*. Springer International Publishing. 314–326. URL: http://link.springer.com/chapter/10.1007/978-3-319-47413-7_18.

Rieger, C., I. Ray, Q. Zhu, and M. Haney. (2019). *Industrial Control Systems Security and Resiliency: Practice and Theory. Advances in Information Security*. Springer.

Rieger, C., Q. Zhu, and T. Başar. (2012). "Agent-based cyber control strategy design for resilient control systems: Concepts, architecture and methodologies". In: *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*. IEEE. 40–47.

Ruan, Y., S. Kalyanasundaram, and X. Zou. (2016). "Survey of return-oriented programming defense mechanisms: Survey of return-oriented programming defense mechanisms". en. *Security and Communication Networks*. 9(10): 1247–1265. DOI: 10.1002/sec.1406. (Accessed on 11/08/2019).

Simmons, C. B., C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu. (2009). "AVOIDIT: A Cyber Attack Taxonomy". *CTIT technical reports series*.

Singhal, A. and X. Ou. (2011). "Security risk analysis of enterprise networks using probabilistic attack graphs". No. NIST IR 7788. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.7788. (Accessed on 05/03/2019).

Skopik, F., M. Landauer, M. Wurzenberger, G. Vormayr, J. Milosevic, J. Fabini, W. Prüggler, O. Kruschitz, B. Widmann, K. Truckenthanner, S. Rass, M. Simmer, and C. Zauner. (2020). "synERGY: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems". en. *Journal of Information Security and Applications*. 54(Oct.): 102544. DOI: 10.1016/j.jisa.2020.102544. (Accessed on 06/15/2020).

Stouffer, K., J. Falco, and K. Scarfone. (2011). "Guide to industrial control systems (ICS) security". *NIST special publication*. 800(82): 16–16.

Stroetmann, L. and H. Pohl. (2014). "Robot Operating System (ROS): Safe & Insecure".

System Security Research Group. (2019). *Implementation of the Cut-The-Rope Game" of Stealthy Intrusion | SYSSEC*. URL: https://www.syssec.at/de/publikationen/description/cuttherope (accessed on 11/30/2020).

Taurer, S., B. Breiling, S. Svrta, and B. Dieber. (2019). "Case study: Remote attack to disable MiR100 safety". In: *Proceedings of the first Cybersecurity for Robotics 2019 Conference (CSfR2019)*.

Tenable. (2020). *Nessus Vulnerability Assessment*. URL: https://de.tenable.com/products/nessus (accessed on 11/27/2020).

Van Dijk, M., A. Juels, A. Oprea, and R. L. Rivest. (2013). "FlipIt: The game of "stealthy takeover"". *Journal of Cryptology*. 26(4): 655–713.

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

Vilches, V. M., E. Gil-Uriarte, I. Z. Ugarte, G. O. Mendia, R. I. Pisón, L. A. Kirschgens, A. B. Calvo, A. H. Cordero, L. Apa, and C. Cerrudo. (2019). "Towards an open standard for assessing the severity of robot security vulnerabilities, the Robot Vulnerability Scoring System (RVSS)". *arXiv:1807.10357 [cs]*. Sept. arXiv: 1807.10357. URL: http://arxiv.org/abs/1807.10357 (accessed on 11/26/2020).

Wachter, J., T. Grafenauer, and S. Rass. (2017). "Visual Risk Specification and Aggregation". In: *SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies*. Ed. by IARIA. 93–98.

Wachter, J., S. Rass, S. König, and S. Schauer. (2018). "Disappointment-Aversion in Security Games". In: *International Conference on Decision and Game Theory for Security*. Springer. 314–325. DOI: http://doi.org/10.1007/978-3-030-01554-1_18.

White, R. (2018). *ruffsl/roschaos*. URL: https://github.com/ruffsl/roschaos (accessed on 11/30/2020).

Xu, Z. and Q. Zhu. (2015a). "A cyber-physical game framework for secure and resilient multi-agent autonomous systems". In: *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE. 5156–5161.

Xu, Z. and Q. Zhu. (2015b). "Secure and resilient control design for cloud enabled networked control systems". In: *Proceedings of the first ACM workshop on cyber-physical systems-security and/or privacy*. 31–42.

Xu, Z. and Q. Zhu. (2016). "Cross-layer secure cyber-physical control system design for networked 3D printers". In: *2016 American Control Conference (ACC)*. IEEE. 1191–1196.

Xu, Z. and Q. Zhu. (2017a). "A Game-Theoretic Approach to Secure Control of Communication-Based Train Control Systems Under Jamming Attacks". In: *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*. ACM. 27–34. URL: http://dl.acm.org/citation.cfm?id=3055381.

Xu, Z. and Q. Zhu. (2017b). "A game-theoretic approach to secure control of communication-based train control systems under jamming attacks". In: *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*. ACM. 27–34.

Xu, Z. and Q. Zhu. (2017c). "Secure and practical output feedback control for cloud-enabled cyber-physical systems". In: *Communications and Network Security (CNS), 2017 IEEE Conference on*. IEEE. 416–420.

Xu, Z. and Q. Zhu. (2018). "Cross-layer secure and resilient control of delay-sensitive networked robot operating systems". In: *2018 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE. 1712–1717.

Yuan, X., P. He, Q. Zhu, and X. Li. (2018). "Adversarial Examples: Attacks and Defenses for Deep Learning". *arXiv:1712.07107 [cs, stat]*. July. URL: http://arxiv.org/abs/1712.07107 (accessed on 02/26/2020).

Zhang, R. and Q. Zhu. (2015). "Secure and resilient distributed machine learning under adversarial environments". In: *2015 18th International Conference on Information Fusion (Fusion)*. IEEE. 644–651.

Zhang, R. and Q. Zhu. (2016a). "Attack-Aware Cyber Insurance of Interdependent Computer Networks". URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2848576.

Zhang, R. and Q. Zhu. (2017a). "A game-theoretic analysis of label flipping attacks on distributed support vector machines". In: *Information Sciences and Systems (CISS), 2017 51st Annual Conference on*. IEEE. 1–6. URL: http://ieeexplore.ieee.org/abstract/document/7926118/.

Zhang, R. and Q. Zhu. (2017b). "A game-theoretic defense against data poisoning attacks in distributed support vector machines". In: *Decision and Control (CDC), 2017 IEEE 56th Annual Conference on*. IEEE. 4582–4587.

Zhang, R. and Q. Zhu. (2018a). "A game-theoretic approach to design secure and resilient distributed support vector machines". *IEEE transactions on neural networks and learning systems*. 29(11): 5512–5527.

Zhang, R. and Q. Zhu. (2018b). "A game-theoretic approach to design secure and resilient distributed support vector machines". *IEEE transactions on neural networks and learning systems*. 29(11): 5512–5527.

Zhang, R. and Q. Zhu. (2019). "FlipIn: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things". *IEEE Transactions on Information Forensics and Security*.

Zhang, R., Q. Zhu, and Y. Hayel. (2017). "A bi-level game approach to attack-aware cyber insurance of computer networks". *IEEE Journal on Selected Areas in Communications*. 35(3): 779–794.

Zhang, T., L. Huang, J. Pawlick, and Q. Zhu. (2019). "Game-Theoretic Analysis of Cyber Deception: Evidence-Based Strategies and Dynamic Risk Mitigation". *arXiv preprint arXiv:1902.03925*.

Zhang, T. and Q. Zhu. (2016b). "Dynamic differential privacy for ADMM-based distributed classification learning". *IEEE Transactions on Information Forensics and Security*. 12(1): 172–187.

Zhu, Q. (2021). "Control Challenges". In: *Resilient Control Architectures and Power Systems*. Ed. by C. Rieger. Wiley-IEEE Press. Chapter 14 (in press).

Zhu, Q. and T. Basar. (2015). "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems". *IEEE Control Systems Magazine*. 35(1): 46–65.

Zhu, Q. and T. Başar. (2009). "Dynamic policy-based IDS configuration". In: *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*. IEEE. 8600–8605.

Zhu, Q. and T. Başar. (2011a). "Indices of power in optimal IDS default configuration: theory and examples". In: *Decision and Game Theory for Security*. Springer. 7–21.

Zhu, Q. and T. Başar. (2011b). "Robust and resilient control design for cyber-physical systems with an application to power systems". In: *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE. 4066–4071.

Zhu, Q. and T. Başar. (2012). "A dynamic game-theoretic approach to resilient control system design for cascading failures". In: *Proceedings of the 1st international conference on High Confidence Networked Systems*. 41–46.

Zhu, Q. and T. Başar. (2013). "Game-theoretic approach to feedback-driven multi-stage moving target defense". In: *International Conference on Decision and Game Theory for Security*. Springer. 246–263.

Zhu, Q., L. Bushnell, and T. Başar. (2013a). "Resilient distributed control of multi-agent cyber-physical systems". In: *Control of Cyber-Physical Systems*. Springer. 301–316.

Zhu, Q., L. Bushnell, and T. Başar. (2013b). "Resilient distributed control of multi-agent cyber-physical systems". In: *Control of Cyber-Physical Systems*. Springer. 301–316.

Zhu, Q., C. Fung, R. Boutaba, and T. Basar. (2009). "A game-theoretical approach to incentive design in collaborative intrusion detection networks". In: *2009 International Conference on Game Theory for Networks*. IEEE. 384–392.

Zhu, Q., C. Fung, R. Boutaba, and T. Başar. (2012). "GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks". *Selected Areas in Communications, IEEE Journal on*. 30(11): 2220–2230.

Zhu, Q., Z. Han, and T. Başar. (2010a). "No-regret learning in collaborative spectrum sensing with malicious nodes". In: *Communications (ICC), 2010 IEEE International Conference on*. IEEE. 1–6.

Zhu, Q., H. Li, Z. Han, and T. Başar. (2010b). "A stochastic game model for jamming in multi-channel cognitive radio systems". In: *2010 IEEE International Conference on Communications*. IEEE. 1–6.

Zhu, Q. and S. Rass. (2018). "On Multi-Phase and Multi-Stage Game-Theoretic Modeling of Advanced Persistent Threats". *IEEE Access*. 6: 13958–13971.

Zhu, Q., S. Rass, and P. Schartner. (2019). "Community-Based Security for the Internet of Things". In: *Smart Cities Cybersecurity and Privacy*. Elsevier. 11–19.

Zhu, Q., C. Rieger, and T. Başar. (2011a). "A hierarchical security architecture for cyber-physical systems". In: *2011 4th international symposium on resilient control systems*. IEEE. 15–20.

Zhu, Q., W. Saad, Z. Han, H. V. Poor, and T. Başar. (2011b). "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach". In: *Military Communications Conference (MILCOM), 2011*. IEEE. 119–124.

Zhu, Q., J. B. Song, and T. Başar. (2011c). "Dynamic secure routing game in distributed cognitive radio networks". In: *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE. 1–6.

Zhu, Q., H. Tembine, and T. Başar. (2010c). "Heterogeneous learning in zero-sum stochastic games with incomplete information". In: *49th IEEE conference on decision and control (CDC)*. IEEE. 219–224.

Zhu, Q., H. Tembine, and T. Başar. (2010d). "Network security configurations: A nonzero-sum stochastic game approach". In: *American Control Conference (ACC), 2010*. IEEE. 1059–1064.

Zhu, Q., H. Tembine, and T. Başar. (2011d). "Distributed strategic learning with application to network security". In: *American Control Conference (ACC), 2011*. IEEE. 4057–4062.

Zhu, Q., H. Tembine, and T. Başar. (2013c). "Hybrid learning in stochastic games and its applications in network security". *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control*: 305–329.

Zhu, Q., D. Wei, and K. Ji. (2015). "Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics and Design Principles". In: *Cyber Security for Industrial Control Systems: from the viewpoint of close-loop*. Ed. by J. C. P. Cheng H. Zhang. CRC Press.

Zhu, Q. and Z. Xu. (2020). *Cross-Layer Design for Secure and Resilient Cyber-Physical Systems: A Decision and Game Theoretic Approach*. Springer Nature.

Zhuang, J., V. M. Bier, and O. Alagoz. (2010). "Modeling secrecy and deception in a multiple-period attacker–defender signaling game". *European Journal of Operational Research*. 203(2): 409–418.