State-of-the-Art Survey

LNCS 13049

Lejla Batina
Thomas Bäck
Ileana Buhan
Stjepan Picek (Eds.)

Security and Artificial Intelligence

A Crossdisciplinary Approach

Springer

Lecture Notes in Computer Science 13049

Founding Editors

Gerhard Goos
Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis
Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino
Purdue University, West Lafayette, IN, USA

Wen Gao
Peking University, Beijing, China

Bernhard Steffen
TU Dortmund University, Dortmund, Germany

Gerhard Woeginger
RWTH Aachen, Aachen, Germany

Moti Yung
Columbia University, New York, NY, USA

More information about this series at https://link.springer.com/bookseries/558

Lejla Batina · Thomas Bäck · Ileana Buhan ·
Stjepan Picek (Eds.)

Security and Artificial Intelligence

A Crossdisciplinary Approach

Springer

Editors
Lejla Batina
Radboud University Nijmegen
Nijmegen, The Netherlands

Thomas Bäck
Leiden University
Leiden, The Netherlands

Ileana Buhan
Radboud University Nijmegen
Nijmegen, The Netherlands

Stjepan Picek
Radboud University Nijmegen
Nijmegen, The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-98794-7 ISBN 978-3-030-98795-4 (eBook)
https://doi.org/10.1007/978-3-030-98795-4

© Springer Nature Switzerland AG 2022
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

In recent years, artificial intelligence (AI) has become an emerging technology to assess security and privacy. There are many security challenges and potential solutions for AI systems at the algorithm, architecture, and implementation levels. So far, research on AI and security has looked at the various sub-problems in isolation, primarily relying on best practices in the domain. At the same time, future solutions will require fostering the sharing of experiences and best practices between those domains. To address some of those challenges, we organized a Lorentz workshop in 2019 called AI+Sec that considered several research topics on the intersection of AI and security. We covered topics like side-channel attacks and fault injection, cryptographic primitives, adversarial machine learning, and intrusion detection. The Lorentz workshop had around 50 participants, where 45% were junior scientists. During the group discussions, we realized that no texts provide a broad view of security and AI, and we decided to write a book covering such topics. After more discussion, 41 people showed interest in contributing to the book, and we selected 14 chapters to be included. We approached Springer, who agreed to publish the book, and helped in the procedure.

The book chapters were evaluated based on their significance, technical quality, and relevance to the topics of security and AI. Each book chapter submission was reviewed in a single-blind mode by at least three authors of other book chapters. After the first review round, the authors had the opportunity to improve the book chapters and update the manuscripts to keep them up-to-date.

Part I, "AI for Cryptography", contains five chapters. We discuss how AI can be used to construct cryptographic primitives. Next, we provide a detailed exposure on AI for implementation attacks, first side-channel analysis, and then fault injection. Finally, the last chapter of this part discusses physically unclonable functions and AI.

Part II, "AI for Authentication and Privacy", contains four chapters. We focus on AI techniques to improve privacy in the first two chapters, which are followed by two chapters on authentication approaches.

Part III, "AI for Intrusion Detection" contains two chapters. This part discusses how AI can be used for malware detection and network intrusion detection.

Finally, Part IV, "Security of AI", contains three chapters. In the previous book parts, we focused our attention on how AI can be used in security. Now, we discuss the security of AI. This part presents topics like adversarial examples, backdoor attacks, and implementation attacks on AI.

A long list of volunteers invested their time and energy to create this book. We are grateful to the PhD students who helped in coordinating the effort, the Lorentz workshops staff (Wendy van der Linden, Tara Seeger, Sietske Kroon) for their support in organizing the event that led to this book, Marina Krček, who helped with the editorial tasks, and the team at Springer.

Last but not least, we thank all the authors for putting much effort into producing the high-quality content we are proud to present here. With this book, we hope to provide

the community with insights into recent and latest developments in artificial intelligence and security.

February 2022

Lejla Batina
Thomas Bäck
Ileana Buhan
Stjepan Picek

Organization

Editors

Lejla Batina	Radboud University, The Netherlands
Thomas Bäck	Leiden University, The Netherlands
Ileana Buhan	Radboud University, The Netherlands
Stjepan Picek	Radboud University and Delft University of Technology, The Netherlands

Reviewers

Lejla Batina	Radboud University, The Netherlands
Thomas Bäck	Leiden University, The Netherlands
Shivam Bhasin	Nanyang Technological University, Singapore
Jakub Breier	Silicon Austria Labs, Austria
Lukasz Chmielewski	Radboud University and Riscure, The Netherlands
Fatemeh Ganji	Worcester Polytechnic Institute, USA
Giuseppe Garofalo	KU Leuven, Belgium
Carlos Javier Hernandez-Castro	Complutense University, Spain
Julio Hernandez-Castro	University of Kent, UK
Annelie Heuser	French National Center for Scientific Research (CNRS), IRISA, France
Xiaolu Hou	Slovak University of Technology, Slovakia
Domagoj Jakobovic	University of Zagreb, Croatia
Dirmanto Jap	Nanyang Technological University, Singapore
Sander Joos	KU Leuven, Belgium
Wouter Joosen	KU Leuven, Belgium
Alan Jovic	University of Zagreb, Croatia
Marina Krcek	Delft University of Technology, The Netherlands
Martha Larson	Delft University of Technology and Radboud University, The Netherlands
Huimin Li	Delft University of Technology, The Netherlands
Shaofeng Li	Shanghai Jiao Tong University, China
Zhuoran Liu	Radboud University, The Netherlands
Shiqing Ma	Rutgers University, USA
Luca Mariot	Delft University of Technology, The Netherlands
Azqa Nadeem	Delft University of Technology, The Netherlands
Servio Paguada	Radboud University, The Netherlands, and Ikerlan Technological Research Centre, Spain

Louiza Papachristodoulou	Fontys University of Applied Sciences, The Netherlands
Guilherme Perin	Delft University of Technology, The Netherlands
Davy Preuveneers	KU Leuven, Belgium
Christian Rechberger	Graz University of Technology, Austria
Vera Rimmer	KU Leuven, Belgium
Unai Rioja	Radboud University, The Netherlands, and Ikerlan Technological Research Centre, Spain
Alex Serban	Radboud University, The Netherlands
Manel Slokom	Delft University of Technology, The Netherlands
Shahin Tajik	Worcester Polytechnic Institute, USA
Ilias Tsingenopoulos	KU Leuven, Belgium
Tim Van hamme	KU Leuven, Belgium
Sicco Verwer	Delft University of Technology, The Netherlands
Roman Walch	Graz University of Technology and Know-Center GmbH, Austria
Lichao Wu	Delft University of Technology, The Netherlands
Minhui Xue	University of Adelaide, Australia
Benjamin Zi Hao Zhao	Macquarie University, Australia

Contents

AI for Intrusion Detection

Security of AI