Computer Communications and Networks

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at http://www.springer.com/series/4198

Simon Parkinson · Andrew Crampton
Richard Hill
Editors

Guide to Vulnerability Analysis for Computer Networks and Systems

An Artificial Intelligence Approach

Springer

Editors

Simon Parkinson
Department of Computer Science,
School of Computing and Engineering
University of Huddersfield
Huddersfield, UK

Richard Hill
Department of Computer Science,
School of Computing and Engineering
University of Huddersfield
Huddersfield, UK

Andrew Crampton
Department of Computer Science,
School of Computing and Engineering
University of Huddersfield
Huddersfield, UK

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-319-92623-0 ISBN 978-3-319-92624-7 (eBook)
https://doi.org/10.1007/978-3-319-92624-7

Library of Congress Control Number: 2018944334

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, express 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

Performing vulnerability assessment of any computing infrastructure is an essential component towards improving a system's security. This is achieved through identifying and mitigating security weaknesses on a recurring basis. Undertaking vulnerability assessment requires in-depth knowledge of the underlying system architecture, available data sources for assessment, algorithmic techniques to assist in identifying vulnerabilities through data processing, and visualisation technologies capable of increasing human understanding and minimising cognitive load.

Artificial Intelligence has great potential to improve the Vulnerability Assessment of computing systems. This book presents key research in the discipline and aims to provide a key body of work for researchers and practitioners. This book covers various aspects of vulnerability assessment, including recent advancements in reducing the requirement on expert knowledge through novel applications of Artificial Intelligence. This book contains many case studies and can be used by security professionals and researchers as reference text, detailing how they can develop and perform Vulnerability Assessment techniques using state-of-the-art intelligent mechanisms.

Organisation

This book is organised into the following four parts:

- Part I introduces the area of Vulnerability Assessment and the use of Artificial Intelligence, as well as providing reviews into the current state of the art.
- Part II provides and discusses Vulnerability Assessment frameworks, including those for industrial control and cloud systems.
- Part III contains many applications that use Artificial Intelligence to enhance Vulnerability Assessment processes.
- Part IV presents and discussed visualisation techniques that can be used to assist the Vulnerability Assessment process.

Target Audience

This book has been created for the following audiences:

- Students and instructors will benefit from using this book as a key reference source and as a subject ‘primer’, describing fundamental background as well as providing educational examples of how Artificial Intelligence can be used in Vulnerability Assessment.
- Researchers will benefit from using this book as a key reference text, providing surveys of the state of the art as well as a collection of key works in the subject area.
- Security practitioners will benefit from using this book to identify the challenges of Vulnerability Assessment and using case study examples to identify how Artificial Intelligence can be used to improve the Vulnerability Assessment process.

Suggested Instructor Use

Instructors are recommended to use this book to either form an ‘Artificial Intelligence for Vulnerability Assessment’ module or to use aspects within the core of other Computer Security, Networking and Artificial Intelligence modules.

Each chapter contains a series end of chapter questions that can be used to form tutorial activities in taught content or as thought-provoking questions for researchers and security practitioners.

The below list provides an example of how this book’s chapters can be used to create 12 teaching sessions:

- Week 1–2: Part I Introduction and State of the Art;
- Week 3–4: Part II Vulnerability Assessment Frameworks;
- Week 5–10: Part III Applications of Artificial Intelligence;
- Week 11–12: Part IV Visualisation.

Acknowledgements

The editors would like to express their sincere thanks to Saad Khan of the University of Huddersfield for assisting with editorial and administrative duties in the preparation of this book.

The authors would also like to express their thanks to the following individuals who contributed to this book’s review process:

- Arosha Bandara, The Open University, UK
- Andrea Cullen, University of Bradford, UK
- Amani Ibrahim, Deakin University, Australia

- Artemios Voyiatzis, SBA Research, Austria
- David Rosado, University of Castilla–La Mancha, Spain
- Dimitrios Zissis, University of the Aegean, Greece
- Emlyn Butterfield, Leeds Beckett University, UK
- Jesus Luna Garcia, Technische Universitt Darmstadt, Germany
- John Mace, Newcastle University, UK
- Kieran Mclaughlin, the Centre for Secure Information Technologies, Belfast
- Marjan Gusev, the Ss. Cyril and Methodius University of Skopje, Macedonia
- Martin Boldt, Blekinge Institute of Technology, Sweden
- Mohamed Amine Ferrag, Guelma University, Algeria
- Sasko Ristov, University of Innsbruck, Austria
- Shujun Li, University of Surrey, UK
- Sokratis Katsikas, University of Piraeus, Greece
- Tiago Cruz, University of Coimbra, Portugal

Huddersfield, UK
April 2018

Simon Parkinson
Andrew Crampton
Richard Hill

Contents

Part I Introduction and State-of-the-art

Part II Vulnerability Assessment Frameworks

Part III Applications of Artificial Intelligence

Part IV Visualisation