Preface

In spite of the increasing efforts in designing preventive security measures, new attack types arise on a regular basis. The reasons for these include: programming errors, design flaws, insider threats, and the inadequate security tools being used by organizations. Additionally, attackers keep evolving attack strategies, resulting in new attack variations being undetected at a system's real-time execution. Therefore, academic efforts with supporting material are needed to advance the existing attack prediction models, recognize the threats and vulnerabilities in the existing techniques, and learn how to create new intrusion detection systems in the future.

To this end, Internet communications and distributed networked environments have become rich media for electronic data transfer. Due to a huge amount of data transmission, it becomes vital to build effective security policies and threat detection systems that are capable of analyzing network data. As such, providing appropriate protection mechanisms and techniques is significant to combat cyber-threats and to preserve information systems' integrity, confidentiality, and availability. This book discusses several trending topics in the area of information security. Since there is an increase in the volume of malicious cyber-attacks which demands a collaborative effort between security professionals and researchers to design and utilize cyber-defense systems, the first part of this book discusses the recent attack prediction techniques that infuse one or more aspects of information to create attack prediction models. The second part is dedicated to new trends on cybersecurity such as graph data analytics for cybersecurity, unwanted traffic detection and control based on trust management software-defined networks, security in wireless sensor networks and their applications, and emerging trends in security system design using the concept of social behavioral biometric.

By creating this book, from the perspective of information-based security systems, we hope to close the gap in most of the existing systems which mainly focus on low-level data analytics to predict attacks. In addition, we hope to make readers gain a clear understanding of recent techniques in cybersecurity.

San Antonio, TX, USA Izzat M. Alsmadi
Baltimore, MD, USA George Karabatis
Irbid, Jordan Ahmed AlEroud

http://www.springer.com/978-3-319-44256-3

Information Fusion for Cyber-Security Analytics

Alsmadi, I.; Karabatis, G.; Aleroud, A. (Eds.)

2017, X, 379 p. 85 illus., 61 illus. in color., Hardcover
ISBN: 978-3-319-44256-3