Advances in Information Security 72

Mauro Conti · Gaurav Somani
Radha Poovendran *Editors*

Versatile Cybersecurity

Springer

More information about this series at http://www.springer.com/series/5576

Mauro Conti • Gaurav Somani • Radha Poovendran
Editors

Versatile Cybersecurity

Springer

Editors
Mauro Conti
Department of Mathematics
University of Padua
Padua, Italy

Gaurav Somani
Department of Computer Science
and Engineering
Central University of Rajasthan
Ajmer, India

Radha Poovendran
Department of Electrical Engineering
University of Washington
Seattle, WA, USA

ISSN 1568-2633
Advances in Information Security
ISBN 978-3-319-97642-6 ISBN 978-3-319-97643-3 (eBook)
https://doi.org/10.1007/978-3-319-97643-3

Library of Congress Control Number: 2018959413

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

Preface

Cybersecurity is one of the important areas in the computer science domain which also plays a major role in the life of almost every individual, enterprise, society, and country. After the IT revolution, an unprecedented growth has been seen in the number of cyber-attacks and their impact in terms of financial damages and data losses. A steady growth is also visible in the newer forms of attacks with sophistication, stealth, scale, persistence, and intelligent penetration. Cyber-attacks also necessitate continuous and unified efforts on designing defensive mechanisms to combat the range of evolving attacks and minimizing the damages incurred by various attacks. Cybersecurity as a discipline is also able to attract a good number of young minds opting to study and divulge into this area. There is a range of online and printed resources available to study various research topics, relevant contributions, and open problems related to cybersecurity.

A large number of advanced security books focus on either cryptography or system security which covers both information and network security. However, there is hardly any text available for advanced students and research scholars in security research to systematically study how the major attacks are studied, modeled, planned, launched, and combated by the community. The *Versatile Cybersecurity* book aims to fill this gap by providing focused content related to specific attacks or attack families. These dedicated discussions in the form of individual chapters cover the application or area-specific aspects while discussing about the placement of defense solutions to combat the attacks. This book has eight high-quality chapters from established security research groups worldwide which address important attacks from theoretical (modeling) as well as practical aspects.

We anticipate that this edited book can serve as a good resource to security researchers and students as each chapter brings comprehensive and structured information about an attack or an attack family. The authors in these chapters present crisp detailing on the state of the art with quality illustration of defense mechanisms and open research problems. This book covers various important attack families such as insider threats, semantics social engineering attacks, distributed denial of service attacks, botnet-based attacks, cyber physical malware-based attacks,

cross-vm attacks, and IoT covert channel attacks. We hope that this book will serve the interests of many of the cybersecurity enthusiasts including undergraduates, postgraduate, and doctoral students.

The first chapter on "An Android-Based Covert Channel Framework on Wearables Using Status Bar Notifications" focuses on covert channel attacks on Internet of Things (IoT) devices using notifications. The authors in this chapter show cases of novel covert channel attacks where instead of using global shared resources, attack is performed using common status notifications to users. The chapter shows a detailed description of threat model, types, and motivations of covert channel attacks. Later in the chapter, authors describe a novel Android-based covert channel attack which is based on status bar notifications. Authors also discuss various important parameters behind the success of these attacks. Authors also describe the performance of the covert channel attacks based on throughput analysis and covert analysis. At the end of the chapter, the authors discuss a set of open research directions in this area to help the researchers to ponder on newer problems.

The second chapter on "Insider Threat Detection: Machine Learning Way" aims to cover and analyze contributions from machine learning domain to provide solutions to various kinds of insider threats. The authors in this chapter provide various attack launch mechanisms and details the impacts of an insider attack on various domains. The authors also presents interesting state-of-the-art work on insider threat detection which includes methods based on psychology, criminology, and game theory. The chapter covers various case studies covering usages of machine learning techniques in anomaly detection. The chapter also describes some experimental studies on insider threat detection over large datasets with low frequency anomalies. The authors describe methods such as linear regression followed by Cook's and Mahalanobis distance to identify malicious activities of the user. The authors also show usages of neural network and support vector machines to demonstrate detection of an anomalous behavior. The chapter concludes by providing a glimpse of future research directions from natural language processing, behavioral analysis, sentiment analysis, and machine learning areas for insider threat detection.

DDoS attacks are among the top cyber threats for many years. The third chapter of this book on "Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions" aims to provide a comprehensive description of the state-of-the-art techniques for DDoS attack detection and defense mechanisms. In addition, the authors in this chapter provide a detailed taxonomy of various DDoS attacks to help the reader understand the types of attack methods used to plan the DDoS attacks. The authors provide a detailed description of various launch methods and also give a light to various reasons for success of notorious DDoS attacks. In the later part of the chapter, authors describe various attack characterization, prevention, detection, and trace-back methods. Authors also discuss the attack sophistication and newer trends in the DDoS attacks space and also provide a list of future research directions at the end of the chapter.

Social engineering attacks lead to multiple threats which may in turn lead to many other security attacks such as phishing, drive-by downloads, file and

multimedia masquerading, domain typosquatting, and malvertising. The fourth chapter on "Protection Against Semantic Social Engineering Attacks" focuses on various kinds of semantic social engineering attacks. The authors provide a detailed coverage of over 35 diverse types of semantic attacks. The authors in this chapter provide an in-depth coverage to the semantic attack launch methods using a generic attack structure. A major contribution of this chapter is in providing a detailed yet comprehensive treatment to the solutions in the form of a three-dimensional defense framework for the semantic social engineering attacks. We are sure that the readers will benefit from the application of three-dimensional defenses on popular semantic attack cases such as "Podesta Emails" and "WhatsApp QRishing." The authors also provide three important open research directions in the form of emerging threats in "Internet of Everything," Human-as-a-Security-Sensor, and Cyber Hygiene 2.0.

Program obfuscation makes it difficult for the detection methods to understand the program semantics. Chapter 5 of this book aims to provide details about cryptographic program obfuscators. The authors in this chapter introduce the program obfuscation and its importance in general and provide a detailed description of cryptographic program obfuscation. In this chapter, the authors show the practical implementations of point function obfuscators, provably secure under widely used intractability assumptions and in theory-oriented models and definitions of cryptographic program obfuscation. The authors describe different point function obfuscators based on cryptographic hashing, decisional DH, discrete logarithms, decisional residuosity, the LWR problem, and the LWE problem. Later, the chapter provides guidelines to generate application-oriented models and definitions of cryptographic program obfuscations, addressing more practical classes of attacks.

Chapter 6 of this book focuses on "Botnet-Based Attacks and Defense Mechanisms." The authors in this chapter provide an in-depth discussion to botnet lifecycle and give a comprehensive classification of botnets. The authors detail the launching of botnet-based attacks in the form of compromise attacks (initial threats) and follow-up attacks (continuous threats). The authors also provide a list of reasons behind the success of botnet-based attacks. The major contribution of this chapter is to provide a comprehensive solution hierarchy for botnet-driven attacks. We hope that readers would benefit from the list of newer form of botnets such as mobile, social network-based, IoT-based, cloud-based, and crypto-mining-based botnets. At the end of the chapter, the authors provide a number of future research directions related to the botnet-based attacks, newer sophistications, and related possible solutions.

Highly sophisticated attack incidents in the form of cyber-physical malware (CPM) such as "Industroyer" can virtually paralyze nations. Chapter 7 is dedicated to "Catastrophic Cyber-Physical Malware" and provides an in-depth coverage to diverse aspects of CPM based attacks from the perspective software vulnerabilities. The authors in this chapter provide a detailed description of CPM metrics and various phases of CPM-based attack launch. We feel that the contributions made by the authors in this chapter would greatly benefit readers who are interested in newer form of cyber-attacks. The authors detail the needs of security measures related to CPM and provide connections to the national cybersecurity. The authors discuss

various risks related to telecommunication infrastructure, industrial control systems, vulnerable mission-critical software, and IoT and provide critical needs for software assurance and practical tools, and cyber-force training. The authors also describe various practical difficulties in detecting CPM malware with the examples such as GPS malware. In addition, authors also discuss challenges related to software assurance. At the end of the chapter, authors provide interesting discussion to the open research directions including threat modeling and describe their DARPA research on software analysis.

The last chapter of this book is on "Cross-VM Attacks: Attack Taxonomy, Defense Mechanisms, and New Directions". The authors in this chapter focus on cloud-based cyber-attack among the virtual machines. The authors in this chapter focus on cross-VM attacks which are mostly side-channel attacks based on shared resources in a multi-tenant cloud environment. The authors provide a detailed description of cross-VM attacks and provide detailed attack taxonomy based on various shared resources in the cloud. The authors detail about five categories (CPU-based, cache-based, memory-based, network-based, and I/O device-based) of cross-VM attacks in their attack taxonomy. In addition, the authors provide an attack model and threat model for cross-VM attacks and various launch methods. The authors also enlist a number of success factors behind these attacks and provide a detailed survey of various mitigation mechanisms. At the end of the chapter, the authors provide a discussion on newer forms of sophisticated cross-vm attacks and a list of open research problems.

Padua, Italy — Mauro Conti
Ajmer, India — Gaurav Somani
Seattle, WA, USA — Radha Poovendran

Acknowledgments

The Editors of this book would like to thank:

- Prof. Sushil Jajodia, George Mason University, USA, and Series Editor, Advances in Information Security (Springer)
- Susan Lagerstrom-Fife, Springer
- Caroline Flanagan, Springer
- Anonymous reviewers
- Authors of various chapters in the book
- University of Padua, Italy
- Central University of Rajasthan, India
- University of Washington, USA

Contents

Advances in Information S

Mauro Conti · Gaurav Soma

Versatile Cybersecu

Computer Science

ISBN 978-3-319-97642-6

▶ springer.com