

# **SpringerBriefs on Cyber Security Systems and Networks**

## **Editor-in-Chief**

Yang Xiang, Digital Research and Innovation Capability, Swinburne University of Technology, Hawthorn, Melbourne, VIC, Australia

## **Series editors**

Liqun Chen, University of Surrey, Guildford, UK

Kim-Kwang Raymond Choo, University of Texas at San Antonio, San Antonio, TX, USA

Sherman S. M. Chow, Department of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong

Robert H. Deng, School of Information Systems, Singapore Management University, Singapore, Singapore

Dieter Gollmann, Hamburg University of Technology, Hamburg, Germany

Javier Lopez, University of Málaga, Málaga, Spain

Kui Ren, University at Buffalo, Buffalo, NY, USA

Jianying Zhou, Singapore University of Technology and Design, Singapore, Singapore

The series aims to develop and disseminate an understanding of innovations, paradigms, techniques, and technologies in the contexts of cyber security systems and networks related research and studies. It publishes thorough and cohesive overviews of state-of-the-art topics in cyber security, as well as sophisticated techniques, original research presentations and in-depth case studies in cyber systems and networks. The series also provides a single point of coverage of advanced and timely emerging topics as well as a forum for core concepts that may not have reached a level of maturity to warrant a comprehensive textbook. It addresses security, privacy, availability, and dependability issues for cyber systems and networks, and welcomes emerging technologies, such as artificial intelligence, cloud computing, cyber physical systems, and big data analytics related to cyber security research. The main focus is on the following research topics:

#### *Fundamentals and Theories*

- Cryptography for cyber security
- Theories of cyber security
- Provable security

#### *Cyber Systems and Networks*

- Cyber systems security
- Network security
- Security services
- Social networks security and privacy
- Cyber attacks and defense
- Data-driven cyber security
- Trusted computing and systems

#### *Applications and Others*

- Hardware and device security
- Cyber application security
- Human and social aspects of cyber security

More information about this series at <http://www.springer.com/series/15797>

Chee Keong Ng · Lei Pan  
Yang Xiang

# Honeypot Frameworks and their Applications: A New Framework

Chee Keong Ng  
School of Information  
Deakin University  
Burwood, Melbourne, VIC  
Australia

Yang Xiang  
Digital Research and Innovation Capability  
Swinburne University of Technology  
Hawthorn, Melbourne, VIC  
Australia

Lei Pan  
School of Information  
Deakin University  
Burwood, Melbourne, VIC  
Australia

ISSN 2522-5561                      ISSN 2522-557X (electronic)  
SpringerBriefs on Cyber Security Systems and Networks  
ISBN 978-981-10-7738-8              ISBN 978-981-10-7739-5 (eBook)  
<https://doi.org/10.1007/978-981-10-7739-5>

Library of Congress Control Number: 2018938790

© The Author(s) 2018

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, 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.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.  
part of Springer Nature  
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721,  
Singapore

*This book is dedicated to those who are interested to know more about honeypots. It does not matter whether you are an expert or novice, this book is for you.*

# Preface

Most people understand honeypots as systems sit in an isolated corner of the network waiting for attacker to discover and compromise them. This is often untrue, in fact, in some frameworks, honeypots have enjoyed the prime spot in an organisational network to lure potential hacker. As new instances of malware appear so rapidly that more spotlight has been placed in honeypot technology.

This book gives a detailed description of honeypots including their forms, purposes, natures and interaction. It also gives an in-depth introduction of different types of honeypot, their applications in monitoring and capturing of malware and adversary tactic to detect honeypot.

The main role of honeypot which effectively assists the researcher to derive solutions for the deadly malware attack has been outlined in the book. This book also gives rich information of other roles and uses of honeypot not only in the area of cyber and network security, but also in collecting proof for forensic investigation.

Finally, this book addresses the importance of honeypot as a learning tool for detecting future malware such as ransomware.

Burwood, Melbourne, Australia  
Burwood, Melbourne, Australia  
Hawthorn, Melbourne, Australia

Chee Keong Ng  
Lei Pan  
Yang Xiang

# Acknowledgements

Thanks to Almighty God for enabling and helping me to complete this book.

I would like to first express my appreciation to my family, especially my wife, Xinying Liu, for her support and love. I would like to also express my most sincere gratitude to my supervisor, Prof. Xiang Yang, and Dr. Lei Pan for their wisdom and advice which is essential for the completion of this book.

Next, I would like to also express my token of appreciation to NSCLab, especially Dr. Jun Zhang for their moral support.

Lastly, I would like to thank Springer Publication for giving me this opportunity to spare my knowledge and finding in their book. I would also like to express my thanks to the editor, Dr. Xiaolan Yao, for her patient and assistance.

# Contents

- 1 Introduction to Honeypot . . . . . 1**
  - 1.1 Introduction . . . . . 1
  - References . . . . . 3
- 2 Design Honeypots . . . . . 7**
  - 2.1 The Concept of Honeypot (Basic Taxonomy). . . . . 7
  - 2.2 Advanced Taxonomy of Honeypot . . . . . 10
  - 2.3 Roadmap of the Honeypot Concept . . . . . 11
  - 2.4 Challenges in Designing Honeypot . . . . . 11
  - References . . . . . 13
- 3 Specialized Honeypot Applications . . . . . 15**
  - 3.1 Web-Server Based Honeypot. . . . . 15
  - 3.2 Web Client-Based Honeypot . . . . . 18
  - 3.3 Worm Detection Honeypot . . . . . 21
  - 3.4 Bot Detection Honeypot . . . . . 25
  - 3.5 Honeytoken . . . . . 29
    - 3.5.1 Anti-phishing Honeypot . . . . . 29
    - 3.5.2 Insider Detection Honeypot . . . . . 32
  - 3.6 Advanced Persistent Threat Honeypot . . . . . 36
  - References . . . . . 39
- 4 General Purposed Honeypot Applications . . . . . 43**
  - 4.1 Dynamic Honeypot. . . . . 43
  - 4.2 Artificial Intelligent Honeypot . . . . . 47
  - 4.3 Shadow Honeypot . . . . . 48
  - References . . . . . 50



<b>5</b>	<b>Other Honeypot Applications</b>	51
5.1	Concealment of Honeypot	51
5.2	Application of Forensic in Honeypot	53
5.2.1	Honeypot Forensic for General Type Attack	55
5.2.2	Honeypot Forensics for Botnet	62
5.3	Direct Role of Honeypot in a Security System	64
	References	65
<b>6</b>	<b>Honeypot Framework, Limitation and Counter-Measure</b>	67
6.1	Conceptual Framework	67
6.2	Common Features of Honeypot	69
6.3	Other Honeypot Detection Method	71
	References	73
<b>7</b>	<b>Ramsonware and Honeypot</b>	75
7.1	Ransomware	75
7.2	Ransomware Honeypot	76
7.3	Bitcoin Honeytoken	77
	References	77
<b>8</b>	<b>Conclusions and Future Work</b>	79
8.1	Conclusion	79
8.1.1	Summary	79
8.1.2	Future Research Work	81