

Computer and Network Security Essentials

Kevin Daimi
Editor

Computer and Network Security Essentials

 Springer

Editor

Kevin Daimi
University of Detroit Mercy
Detroit, MI, USA

Associate Editors

Guillermo Francia
Jacksonville State University, USA

Levent Ertaul
California State University East Bay
USA

Luis Hernandez Encinas
Institute of Physical and Information
Technologies (ITEFI), Spain

Eman El-Sheikh
University of West Florida, USA

ISBN 978-3-319-58423-2 ISBN 978-3-319-58424-9 (eBook)
DOI 10.1007/978-3-319-58424-9

Library of Congress Control Number: 2017943957

© Springer International Publishing AG 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 Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The constantly increasing trend of cyber-attacks and global terrorism makes it vital for any organization to protect and secure its network and computing infrastructure. With the continuous progress the Internet is facing, companies need to keep up by creating and implementing various software products and by utilizing advanced network and system equipment that need to be protected against various attacks. Data stored in our computers can also be subject to unauthorized access. Attackers can modify our data, steal our critical information including personal information, read and alter our e-mail messages, change program code, and possibly mess with our photos including using them for wicked purposes. Intruders can also employ our computers to attack other computers, websites, and networks without our knowledge. By enforcing security of networks and other computing infrastructure, the possibility of losing important data, privacy intrusion, and identity theft can be countermeasured. Many professionals working in computer technology consider security as an afterthought. They only take it seriously when a security problem occurs. It is imperative that society should start accepting security as the new norm.

Computer and Network Security Essentials will introduce the readers to the topics that they need to be aware of to be able to protect their IT resources and communicate with security specialists in their own language when there is a security problem. It introduces IT security to the public at large to improve their security knowledge and perception. The book covers a wide range of security topics including computer security, network security, cryptographic technologies, biometrics and forensics, hardware security, security applications, and security management. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse of future directions where security techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse security experts in the listed fields and edited by prominent security researchers.

University of Detroit Mercy, USA

Kevin Daimi

Acknowledgments

We would like to thank the following faculty and researchers for the generous time and effort they invested in reviewing the chapters of this book. We would also like to thank Mary James, Zoe Kennedy, Brinda Megasyamalan, Brian Halm, and Sasireka Kuppan at Springer for their kindness, courtesy, and professionalism.

Nashwa AbdelBaki, Nile University, Egypt
Hanaa Ahmed, University of Technology, Iraq
Ahmed Ali Ahmed Al-Gburi, Western Michigan University, USA
Abduljaleel Mohamad Mageed Al-Hasnawi, Western Michigan University, USA
Rita Michelle Barrios, University of Detroit Mercy, USA
Pascal Birnstill, Fraunhofer IOSB, Germany
Aisha Bushager, University of Bahrain, Bahrain
Ángel Martín del Rey, University of Salamanca, Spain
Alberto Peinado Domínguez, Universidad de Málaga, Spain
Xiujian Du, Qinghai Normal University, China
Luis Hernandez Encinas, Spanish National Research Council (CSIC), Spain
Patricia Takako Endo, University of Pernambuco, Brazil
Jason Ernst, Left™, Canada
Levent Ertaul, California State University, East Bay, USA
Ken Ferens, University of Manitoba, Canada
José María De Fuentes, Universidad Carlos III de Madrid, Spain
Alejandro Sánchez Gómez, Universidad Autónoma de Madrid, Spain
Arturo Ribagorda Grupo, Universidad Carlos III de Madrid, Spain
David Arroyo Guardeno, Universidad Autónoma de Madrid, Spain
Hisham Hallal, Fahad Bin Sultan University, Saudi Arabia
Tarfa Hamed, University of Guelph, Canada
Zubair Ahmad Khattak, ISACA, USA
Irene Kopaliani, Georgian Technical University, Georgia
Stefan C. Kremer, University of Guelph, Canada
Gregory Laidlaw, University of Detroit Mercy, USA
Arash Habibi Lashkari, University of New Brunswick, Canada

Leszek T. Lilien, Western Michigan University, USA
Lorena González Manzano, Universidad Carlos III de Madrid, Spain
Victor Gayoso Martínez, Spanish National Research Council (CSIC), Spain
Natarajan Meghanathan, Jackson State University, USA
Agustín Martín Muñoz, Spanish National Research Council (CSIC), Spain
Mais W. Nijim, Texas A&M University–Kingsville, USA
Kennedy Okokpujie, Covenant University, Nigeria
Saibal Pal, Defense R&D Organization, India
Ioannis Papakonstantinou, University of Patras, Greece
Keyur Parmar, Indian Institute of Information Technology, INDIA
Bryson R. Payne, University of North Georgia, USA
Slobodan Petrovic, Norwegian University of Science and Technology (NTNU),
Norway
Thiago Gomes Rodrigues, GPRT, Brazil
Gokay Saldamli, San Jose State University, USA
Jibrán Saleem, Manchester Metropolitan University, UK
Narasimha Shashidhar, Sam Houston State University, USA
Sana Siddiqui, University of Manitoba, Canada
Nicolas Sklavos, University of Patras, Greece
Polyxeni Spanaki, University of Patras, Greece
Tyrone Toland, University of South Carolina Upstate, USA
Jesús Díaz Vico, BEEVA, Spain

Contents

Part I Computer Security

1	Computer Security	3
	Jeffrey L. Duffany	
2	A Survey and Taxonomy of Classifiers of Intrusion Detection Systems	21
	Tarfa Hamed, Jason B. Ernst, and Stefan C. Kremer	
3	A Technology for Detection of Advanced Persistent Threat in Networks and Systems Using a Finite Angular State Velocity Machine and Vector Mathematics	41
	Gregory Vert, Ann Leslie Claesson-Vert, Jesse Roberts, and Erica Bott	
4	Information-Theoretically Secure Privacy Preserving Approaches for Collaborative Association Rule Mining	65
	Nirali R. Nanavati and Devesh C. Jinwala	
5	A Postmortem Forensic Analysis for a JavaScript Based Attack	79
	Sally Mosaad, Nashwa Abdelbaki, and Ahmed F. Shosha	

Part II Network Security

6	Malleable Cryptosystems and Their Applications in Wireless Sensor Networks	97
	Keyur Parmar and Devesh C. Jinwala	
7	A Survey and Taxonomy on Data and Pre-processing Techniques of Intrusion Detection Systems	113
	Tarfa Hamed, Jason B. Ernst, and Stefan C. Kremer	
8	Security Protocols for Networks and Internet: A Global Vision	135
	José María de Fuentes, Luis Hernandez-Encinas, and Arturo Ribagorda	

9	Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls	153
	A. Al-Gburi, A. Al-Hasnawi, and L. Lilien	
10	Reliable Transmission Protocol for Underwater Acoustic Networks	173
	Xiujuan Du, Meiju Li, and Keqin Li	
11	Using Sports Plays to Configure Honeypots Environments to form a Virtual Security Shield	189
	Tyrone S. Toland, Sebastian Kollmannsperger, J. Bernard Brewton, and William B. Craft	
Part III Cryptographic Technologies		
12	Security Threats and Solutions for Two-Dimensional Barcodes: A Comparative Study	207
	Riccardo Focardi, Flaminia L. Luccio, and Heider A.M. Wahsheh	
13	Searching Encrypted Data on the Cloud	221
	Khaled A. Al-Utaibi and El-Sayed M. El-Alfy	
14	A Strong Single Sign-on User Authentication Scheme Using Mobile Token Without Verifier Table for Cloud Based Services	237
	Sumitra Binu, Mohammed Misbahuddin, and Pethuru Raj	
15	Review of the Main Security Threats and Challenges in Free-Access Public Cloud Storage Servers	263
	Alejandro Sanchez-Gomez, Jesus Diaz, Luis Hernandez-Encinas, and David Arroyo	
16	Secure Elliptic Curves in Cryptography	283
	Victor Gayoso Martínez, Lorena González-Manzano, and Agustín Martín Muñoz	
17	Mathematical Models for Malware Propagation in Wireless Sensor Networks: An Analysis	299
	A. Martín del Rey and A. Peinado	
Part IV Biometrics and Forensics		
18	Biometric Systems for User Authentication	317
	Natarajan Meghanathan	
19	Biometric Authentication and Data Security in Cloud Computing ...	337
	Giovanni L. Masala, Pietro Ruiu, and Enrico Grosso	
20	Approximate Search in Digital Forensics	355
	Slobodan Petrović	

21 Privacy Preserving Internet Browsers: Forensic Analysis of Browzar 369
 Christopher Warren, Eman El-Sheikh, and Nhien-An Le-Khac

Part V Hardware Security

22 Experimental Digital Forensics of Subscriber Identification Module (SIM) Card 391
 Mohamed T. Abdelazim, Nashwa Abdelbaki, and Ahmed F. Shosha

23 A Dynamic Area-Efficient Technique to Enhance ROPUFs Security Against Modeling Attacks 407
 Fathi Amsaad, Nitin Pundir, and Mohammed Niamat

24 Physical Unclonable Functions (PUFs) Design Technologies: Advantages and Trade Offs 427
 Ioannis Papakonstantinou and Nicolas Sklavos

Part VI Security Applications

25 Generic Semantics Specification and Processing for Inter-System Information Flow Tracking 445
 Pascal Birnstill, Christoph Bier, Paul Wagner, and Jürgen Beyerer

26 On Inferring and Characterizing Large-Scale Probing and DDoS Campaigns 461
 Elias Bou-Harb and Claude Fachkha

27 Design of a Secure Framework for Session Mobility as a Service in Cloud Computing Environment 475
 Natarajan Meghanathan and Michael Terrell

Part VII Security Management

28 Securing the Internet of Things: Best Practices for Deploying IoT Devices 493
 Bryson R. Payne and Tamirat T. Abegaz

29 Cognitive Computing and Multiscale Analysis for Cyber Security ... 507
 Sana Siddiqui, Muhammad Salman Khan, and Ken Ferens

30 A Comparative Study of Neural Network Training Algorithms for the Intelligent Security Monitoring of Industrial Control Systems 521
 Jaedeok Kim and Guillermo Francia

31 Cloud Computing: Security Issues and Establishing Virtual Cloud Environment via Vagrant to Secure Cloud Hosts 539
 Polyxeni Spanaki and Nicolas Sklavos

32	A Survey and Comparison of Performance Evaluation in Intrusion Detection Systems	555
	Jason Ernst, Tarfa Hamed, and Stefan Kremer	
33	Accountability for Federated Clouds	569
	Thiago Gomes Rodrigues, Patricia Takako Endo, David W.S.C. Beserra, Djamel Sadok, and Judith Kelner	
34	A Cognitive and Concurrent Cyber Kill Chain Model	585
	Muhammad Salman Khan, Sana Siddiqui, and Ken Ferens	
35	Defense Methods Against Social Engineering Attacks	603
	Jibran Saleem and Mohammad Hammoudeh	

About the Editors



Kevin Daimi received his Ph.D. from the University of Cranfield, England. He has a long mixture of academia and industry experience. His industry experience includes working as senior programmer/systems analyst, computer specialist, and computer consultant. He is currently professor and director of computer science and software engineering programs at the University of Detroit Mercy. His research interests include computer and network security with emphasis on vehicle network security, software engineering, data mining, and computer science and software engineering education. Two of his publications received the Best Paper Award from two international

conferences. He has been chairing the annual International Conference on Security and Management (SAM) since 2012. Kevin is a senior member of the Association for Computing Machinery (ACM), a senior member of the Institute of Electrical and Electronic Engineers (IEEE), and a fellow of the British Computer Society (BCS). He served as a program committee member for many international conferences and chaired some of them. In 2013, he received the Faculty Excellence Award from the University of Detroit Mercy. He is also the recipient of the Outstanding Achievement Award in Recognition and Appreciation of his Leadership, Service and Research Contributions to the Field of Network Security, from the 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'10).



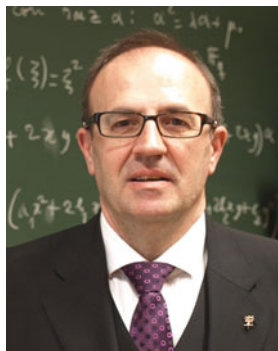
Guillermo Francia received his B.S. degree in mechanical engineering from Mapua Tech in 1978. His Ph.D. in computer science is from New Mexico Tech. Before joining Jacksonville State University (JSU), he was the chairman of the Computer Science Department at Kansas Wesleyan University. Dr. Francia is a recipient of numerous grants and awards. His projects have been funded by prestigious institutions such as the National Science Foundation, Eisenhower Foundation, Department of Education, Department of Defense, National Security Agency, and Microsoft Corporation. Dr. Francia served as a Fulbright scholar

to Malta in 2007 and is among the first cohort of cyber security scholars awarded by the UK Fulbright Commission for the 2016–2017 academic year. He has published articles and book chapters on numerous subjects such as computer security, digital forensics, regulatory compliance, educational technology, expert systems, computer networking, software testing, and parallel processing. Currently, Dr. Francia holds a distinguished professor position and is the director of the Center for Information Security and Assurance at JSU.



Levent Ertaul is a full professor at the California State University, East Bay, USA. He received a Ph.D. degree from Sussex University, UK, in 1994. He specializes in network security. He has more than 75 refereed papers published in the cyber security, network security, wireless security, and cryptography areas. He also delivered more than 40 seminars and talks and participated in various panel discussions related to cyber security. In the last couple of years, Dr. Ertaul has given privacy and cyber security speeches at US universities and several US organizations. He received 4 awards for his contributions

to network security from WORLDCOMP. He also received a fellowship to work at the Lawrence Livermore National Laboratories (LLNL) in the cyber defenders program for the last 4 years. He has more than 25 years of teaching experience in network security and cyber security. He participated in several hacking competitions nationwide. His current research interests are wireless hacking techniques, wireless security, and security of IoTs.



Luis Hernandez Encinas is a researcher at the Department of Information Processing and Cryptography (DTIC) at the Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC) in Madrid (Spain). He obtained his Ph.D. in mathematics from the University of Salamanca (Spain) in 1992. He has participated in more than 30 research projects. He is the author of 9 books, 9 patents, and more than 150 papers. He has more than 100 contributions to workshops and conferences. He has delivered more than 50 seminars and lectures. Luis is a member

of several international committees on cybersecurity. His current research interests include cryptography and cryptanalysis of public key cryptosystems (RSA, ElGamal, and Chor-Rivest), cryptosystems based on elliptic and hyper elliptic curves, graphic cryptography, pseudorandom number generators, digital signature schemes, authentication and identification protocols, crypto-biometry, secret sharing protocols, side channel attacks, and number theory problems.



Eman El-Sheikh is director of the Center for Cybersecurity and professor of computer science at the University of West Florida. She teaches and conducts research related to the development and evaluation of artificial intelligence and machine learning for cybersecurity, education, software architectures, and robotics. She has published over 70 peer-reviewed articles and given over 90 research presentations and invited talks. Dr. El-Sheikh received several awards related to cybersecurity education and diversity and several grants to enhance cybersecurity education

and training for precollegiate and college students that emphasize increasing the participation of women and underrepresented groups in cybersecurity. She leads the UWF ADVANCE Program, an NSF-funded grant aimed at enhancing the culture for recruiting, retaining, and advancing women in STEM. She enjoys giving presentations related to cybersecurity education and workforce development and mentoring students. El-Sheikh holds a Ph.D. in computer science from Michigan State University.