Computer and Network Security Essentials

Kevin Daimi
Editor

Computer and Network Security Essentials

Springer

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

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
Xiujuan 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 Guardeño, 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
Jibran 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

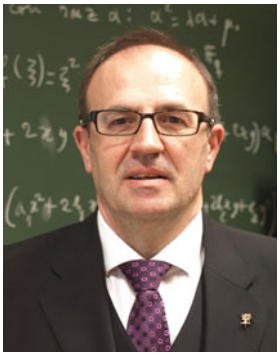
Contents

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.