

Intelligent Systems, Control and Automation:
Science and Engineering

Martti Lehto

Pekka Neittaanmäki *Editors*

Cyber Security: Analytics, Technology and Automation

 Springer

Intelligent Systems, Control and Automation: Science and Engineering

Volume 78

Series editor

S.G. Tzafestas, Athens, Greece

Editorial Advisory Board

P. Antsaklis, Notre Dame, IN, USA

P. Borne, Lille, France

D.G. Caldwell, Salford, UK

C.S. Chen, Akron, OH, USA

T. Fukuda, Nagoya, Japan

S. Monaco, Rome, Italy

R.R. Negenborn, Delft, The Netherlands

G. Schmidt, Munich, Germany

S.G. Tzafestas, Athens, Greece

F. Harashima, Tokyo, Japan

D. Tabak, Fairfax, VA, USA

K. Valavanis, Denver, CO, USA

More information about this series at <http://www.springer.com/series/6259>

Martti Lehto · Pekka Neittaanmäki
Editors

Cyber Security: Analytics, Technology and Automation



 Springer

Editors

Martti Lehto
Department of Mathematical Information
Technology
University of Jyväskylä
Jyväskylä
Finland

Pekka Neittaanmäki
Department of Mathematical Information
Technology
University of Jyväskylä
Jyväskylä
Finland

ISSN 2213-8986

ISSN 2213-8994 (electronic)

Intelligent Systems, Control and Automation: Science and Engineering

ISBN 978-3-319-35203-9

ISBN 978-3-319-18302-2 (eBook)

DOI 10.1007/978-3-319-18302-2

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2015

Softcover reprint of the hardcover 1st edition 2015

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.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Foreword

Global cyberspace is made of complex, multi-layered information networks which encompass the communication networks of the public sector, business community, security authorities and control and monitoring systems used by industry and critical infrastructure which, by means of the Internet, create a worldwide network.

Imaginative data processing and utilization, arising from the needs of citizens and the business community, are some of the most important elements of a thriving society. Information and know-how have become key 'commodities' in society, and they can be utilized all the more efficiently through information technology. Different interactive electronic services are ubiquitously available, irrespective of time and place. While the public sector, the economy, the business community and citizens benefit from globally networked services, the digital IT society contains inherent vulnerabilities which can generate security risks to citizens, the business community or the vital functions of society.

Society is gradually becoming an information-based service culture providing, to an ever greater extent, both public and commercial digital services to citizens. Electronic ICT networks and digital services are vital to the functioning of society. Along with the general trends of change, the advancements in technology and the utilization of the Internet, the operating environment is heavily influenced by the global nature of this increasingly expanding sector and the changing habits among users as well as the challenges associated with reliability and security.

Cyber security risks have become more and more commonplace. Risks which were once considered improbable are now appearing all the more regularly. This trend epitomizes the new forms of instruments and methods being used in attacks, as well as ever-increasing vulnerabilities and the higher motivation of the attackers. The growing impact of cyber-attacks calls for new, creative and innovative solutions so as to mitigate the risks. In the past, individual persons or small hacker groups were the attackers, nowadays, however, various state-run organizations employing state-of-the-art cyber weapons are, in particular, carrying out targeted attacks. These so-called Advanced Persistent Threats (APTs) focus on carefully selected targets; their development requires sophisticated expertise and ample resources.

One global trend is that services are being moved to the cloud. Public officials, companies and citizens alike are increasingly switching to cloud storage and cloud computing. As a concept, cloud computing illustrates a change in the paradigm, one in which services are provided within a ‘cloud’ whose technical details remain opaque to and beyond the control of the users of the service. Cloud computing exhibits a new model of generating, using and providing ICT services, which includes dynamically scalable virtual resources as services provided over the Internet. In accordance with the prevailing trend government organizations are increasingly moving critical IT infrastructure-related data to the cloud, which brings about new cyber security challenges. Cloud computing and cloud services are integrally linked with Big Data, which is being used on a platform for the creation of new services to end users. This, in turn, necessitates close cooperation between cloud service providers and cyber security solution providers. In the future cloud services will lay emphasis on the generation of specific cyber security solutions and the protection of identity and privacy as well as miscellaneous solutions associated with data encryption.

The Internet of Things (IoT) stands for the transformation of industry where industrial products and industrial production utilize the Internet, nanotechnology and the entire ICT sector. The IoT gives objects, or “things”, recognizable identities and they communicate across the global ICT network. New equipment, such as different industrial and service robots as well as information-gathering sensors, are linking into such networks at an increasingly accelerated pace. The latest step in this development involves different kinds of vehicles, such as cars, trolleys and buses as well as different types of heavy machinery.

Modern cars are smart devices with most of their systems controlled by computers. Communication between other cars, traffic control systems and user devices (e.g. smart phones) is also increasing. While infotainment systems provide many services for the driver, they can also be a distraction. All of this information traffic poses the risk of technical or user errors, and even enables remote attacks against cars.

Cross-disciplinary and holistic cyber security research is needed to solve these new challenges. Due to the complexity of the field, research must meet the four basic paradigms of science: the theoretical, experimental, model-based and data-based computational approaches.

Computational science represents the third paradigm of science, one which uses computers to simulate phenomena or situations which may not yet exist in the real world. Rapid advances in IT technology and methodological competence facilitate the introduction of increasingly complex and realistic computational models for solving research related problems. The methods of computational science can also be successfully employed when seeking solutions to situations where traditional methods fail to generate sufficiently accurate results. A computational approach can increase awareness among those sectors of cyber security which are important to society. The computational approach does not only strengthen multi- and cross-disciplinary research, it also expedites and intensifies product development. Simultaneously, it helps lower the barriers between fields of research in both the

public and private sector. It also boosts innovation and generates new breakthroughs in research and product development.

In many cases, large-scale simulations are accompanied by challenges in data-intensive computing. Overcoming the challenges in data-intensive computing has required the optimization of data-movement across multiple levels of memory hierarchies. These considerations have become even more important as we are preparing for exascale computing.

The volume of information and recorded data in the digital world is vast. By intelligently combining real time information, compiled from different sources, it is possible to create entirely new kinds of information which can help break down barriers between sectors. Cyber security is vital to all Big Data-type applications and the integration of the morsels of information generated through data mining demands high-level software and ICT competence. The development of Big Data-research methods provides better opportunities for scientists in different fields to conduct research in different areas and also find solutions to their questions. In addition to development in Big Data methodology, it is important to pay attention to multidisciplinary and promote cross-disciplinary cooperation inter alia between mathematicians, information technology scientists and social scientists.

Comprehensive security builds on the most effective elimination of all threats to the lives of individuals. These days ICT and concomitant cyber security solutions play a critical role in safeguarding comprehensive security. Security in its myriad forms, and especially cyber security, is a field which will only grow in terms of competence and business opportunities.

Cyber security competence cuts across the different sectors and spheres of education. Top-level expertise in cyber security is needed to generate and improve situational awareness in cyber security as well as effective contingency plans against cyber threats, create systems that defend critical infrastructures and to develop functional cyber security solutions.

Jyväskylä
October 2014

Pekka Neittaanmäki
Martti Lehto

Contents

Part I Cyber World Today

Phenomena in the Cyber World	3
Martti Lehto	
Cyber World as a Social System	31
Tuija Kuusisto and Rauno Kuusisto	
Citizens in Cyber World—Despatches from the Virtual “Clinic”	45
Torsti Sirén and Aki-Mauri Huhtinen	
Powers and Fundamental Rights in Cyber Security	63
Riitta Ollila	

Part II Cyber Security Threats, Legality and Strategy

Coder, Hacker, Soldier, Spy	73
Kenneth Geers	
Cyber Warfare	89
Rain Ottis	
Deception in the Cyber-World	97
William Hutchinson	
Legal Framework of Cyber Security	109
Eneken Tikk-Ringas	
Finnish Cyber Security Strategy and Implementation	129
Antti Sillanpää, Harri Roivainen and Martti Lehto	

Part III Cyber Security Technology

Clustering-Based Protocol Classification via Dimensionality Reduction	147
Gil David	
Timing and Side Channel Attacks	183
Nezer Zaidenberg and Amit Resh	
Knowledge Discovery from Network Logs	195
Tuomo Sipola	
Trusted Computing and DRM	205
Nezer Zaidenberg, Pekka Neittaanmäki, Michael Kiperberg and Amit Resh	

Part IV Cyber Security and Automation

Cyber Security and Protection of ICS Systems: An Australian Example	215
Matthew J. Warren and Shona Leitch	
Towards Dependable Automation.	229
Jari Seppälä and Mikko Salmenperä	
Specialized Honeypots for SCADA Systems	251
Paulo Simões, Tiago Cruz, Jorge Proença and Edmundo Monteiro	

Intelligent Systems, Control

Martti Lehto · Pekka Neittaanmäki

Cyber Security: Analysis

Biblioteka Główna
Akademii Sztuki Wojennej

26633/III (CB)



03-026633-000-0

Over the last two decades, cyber security has had a tremendous impact on all parts of society. Governments across the world have started to develop cyber security strategies and to consider cyberspace as an increasingly important international issue. The book, in addition to the cyber threats and technology, processes cyber security from many sides as a social phenomenon and how the implementation of the cyber security strategy is carried out.

The book gives a profound idea of the most spoken phenomenon of this time. The book is suitable for a wide-ranging audience from graduate to professionals/practitioners and researchers. Relevant disciplines for the book are Telecommunications/Network security, Applied mathematics/Data analysis, Mobile systems/Security, Engineering/Security of critical infrastructure and Military science/Security.

Professional Computing

ISBN 978-3-319-35203-9

9 "783319"352039"

► springer.com

