Premier Reference Source

New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson and Marwan Omar

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE

New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri-St. Louis, USA

Marwan Omar
Nawroz University, Iraq

A volume in the Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Managing Editor: Austin DeMarco
Director of Intellectual Property & Contracts: Jan Travers
Acquisitions Editor: Kayla Wolfe
Production Editor: Christina Henning
Development Editor: Brandon Carbaugh
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

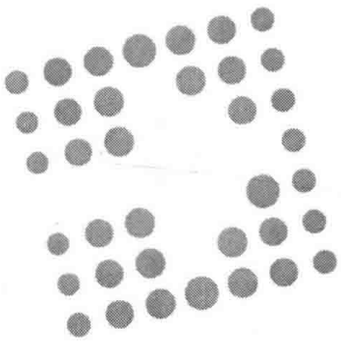
Library of Congress Cataloging-in-Publication Data

New threats and countermeasures in digital crime and cyber terrorism / Maurice Dawson and Marwan Omar, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-8345-7 (hardcover) -- ISBN 978-1-4666-8346-4 (ebook) 1. Computer crimes--Prevention. 2. Cyberterrorism--Prevention. 3. Computer security. I. Dawson, Maurice, 1982- II. Omar, Marwan, 1982-
HV6773.N4745 2015
005.8--dc23

2015006753

This book is published in the IGI Global book series Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) (ISSN: 2327-0381; eISSN: 2327-0373)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.



Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series

ISSN: 2327-0381
EISSN: 2327-0373

Mission

The digital revolution has allowed for greater global connectivity and has improved the way we share and present information. With this new ease of communication and access also come many new challenges and threats as cyber crime and digital perpetrators are constantly developing new ways to attack systems and gain access to private information.

The **Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series** seeks to publish the latest research in diverse fields pertaining to crime, warfare, terrorism and forensics in the digital sphere. By advancing research available in these fields, the **ADCFCT** aims to present researchers, academicians, and students with the most current available knowledge and assist security and law enforcement professionals with a better understanding of the current tools, applications, and methodologies being implemented and discussed in the field.

Coverage

- Digital Surveillance
- Encryption
- Data Protection
- Information warfare
- Cyber warfare
- Telecommunications Fraud
- Identity Theft
- Database Forensics
- Global Threat Intelligence
- Malware

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series (ISSN 2327-0381) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-digital-crime-forensics-cyber/73676. Postmaster: Send all address changes to above address.

Titles in this Series

For a list of additional titles in this series, please visit: www.igi-global.com

Cybersecurity Policies and Strategies for Cyberwarfare Prevention
Jean-Loup Richet (University of Nantes, France)
Information Science Reference • copyright 2015 • 393pp • H/C (ISBN: 9781466684560) • US $245.00 (our price)

Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance
Maria Manuela Cruz-Cunha (Polytechnic Institute of Cavado and Ave, Portugal) and Irene Maria Portela (Polytechnic Institute of Cávado and Ave, Portugal)
Information Science Reference • copyright 2015 • 602pp • H/C (ISBN: 9781466663244) • US $385.00 (our price)

The Psychology of Cyber Crime Concepts and Principles
Gráinne Kirwan (Dun Laoghaire Institute of Art, Design and Technology, Ireland) and Andrew Power (Dun Laoghaire Institute of Art, Design and Technology, Ireland)
Information Science Reference • copyright 2012 • 372pp • H/C (ISBN: 9781613503508) • US $195.00 (our price)

Cyber Crime and the Victimization of Women Laws, Rights and Regulations
Debarati Halder (Centre for Cyber Victim Counselling (CCVC), India) and K. Jaishankar (Manonmaniam Sundaranar University, India)
Information Science Reference • copyright 2012 • 264pp • H/C (ISBN: 9781609608309) • US $195.00 (our price)

Digital Forensics for the Health Sciences Applications in Practice and Research
Andriani Daskalaki (Max Planck Institute for Molecular Genetics, Germany)
Medical Information Science Reference • copyright 2011 • 418pp • H/C (ISBN: 9781609604837) • US $245.00 (our price)

Cyber Security, Cyber Crime and Cyber Forensics Applications and Perspectives
Raghu Santanam (Arizona State University, USA) M. Sethumadhavan (Amrita University, India) and Mohit Virendra (Brocade Communications Systems, USA)
Information Science Reference • copyright 2011 • 296pp • H/C (ISBN: 9781609601232) • US $180.00 (our price)

Handbook of Research on Computational Forensics, Digital Crime, and Investigation Methods and Solutions
Chang-Tsun Li (University of Warwick, UK)
Information Science Reference • copyright 2010 • 620pp • H/C (ISBN: 9781605668369) • US $295.00 (our price)

Homeland Security Preparedness and Information Systems Strategies for Managing Public Policy
Christopher G. Reddick (University of Texas at San Antonio, USA)
Information Science Reference • copyright 2010 • 274pp • H/C (ISBN: 9781605668345) • US $180.00 (our price)

www.igi-global.com

701 E. Chocolate Ave., Hershey, PA 17033
Order online at www.igi-global.com or call 717-533-8845 x100
To place a standing order for titles released in this series, contact: cust@igi-global.com
Mon-Fri 8:00 am - 5:00 pm (est) or fax 24 hours a day 717-533-8661

Editorial Advisory Board

Foreword

Further, North Korea's attack on SPE [Sony Pictures Entertainment] reaffirms that cyber threats pose one of the gravest national security dangers to the United States, the FBI said. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. – https://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/

The research and insights contained within this text could not be more timely or important at a time where the U.S. has seen one of its most brazen cyber attacks in recent history. It has now been proven that terrorist groups, Nation-States, and even individuals can hold major corporations hostage with nothing more than a cheap laptop, the wherewithal and an Internet connection. Cyber terrorism will continue to be one of the governments and law enforcements top priorities. More devices then ever are being connected to mobile networks, while more and more zero-day attacks and vulnerabilities are being designed, shared and made easily accessible to take advantage of vulnerabilities in these networks. The black market is now a vast and complex set of anonymous nodes, servers, and front-end store fronts where attacks, code, stolen information, and everything illegal in-between is being exchanged. Hidden in the deep Internet, goods and services are traded, sold, and purchased with nearly untraceable currency with the advent of Bitcoin. Newly developed malware that could be used to bring down major infrastructure (i.e. Stuxnet) is being traded for freshly stolen Amazon credentials and lifted credit cards as the ink dries on these very pages. Without major cyber security research and innovation, a major cyber attack equivalent to 9/11 is all but inevitable.

The authors' ability to provide new concepts and techniques that can be shared with academia, industry, governments and corporations will enhance cyber security programs and processes as well as lead to innovation in the cyber security field. As data continues to exponentially grow and become one of the most valued commodities of the 21st century, the information contained within these chapters are of utmost value as we continue to attempt to defend and protect our data. All chapters were subjected to a rigorous peer-review process. The first section of the book tackles security in mobile computing. Some of the topics covered include mobile phishing, wireless and ad-hoc networks, privacy, and Smartphone malware. The second portion of the book covers cyber security techniques and cases. Highlights from these chapters include Smartphone malware analysis techniques, and QoS enhancement in mobile ad-hoc networks. The third and final section of the book discusses leadership, communication, and education in cyber security. Topics from this chapter range from learning management systems security, the innovation and promise of STEM oriented cyber security education, and insider threats.

Providing the process for the communication and dissemination of the data within these chapters is vital to the security of every network. The internationally recognized experts, authors and editors have compiled an impressive and comprehensive set of cyber security topics and information on the most important subject of our time.

America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas. – President Obama – http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Ronnie S. Kurlander
Global Technology Solutions, USA & T. Rowe Price, USA

Preface

This book explores multiple aspects of cyber terrorism and cyber crime in today's society. This book provides insights on the negatives uses of technology with comprehensive review of the associated vulnerabilities and mitigations. In the recent events of cyber warfare most notable are the Flame computer virus, expansion of the National Security Agency (NSA) monitoring programs, and suspected attack on Sony for a movie poking fun at North Korea. As governments scramble for cyber security resources whether technological or people it evident that cyber security is the new war being fought.

Our intention in editing this book was to provide new concepts and techniques that are deployed in secure computing, mobile computing, training, and laws. This book is to provide frontier research to include cases that are applicable to modern events. Since the book covers case study-based research findings, it can be quite relevant researchers, university academics, secure computing professionals, and probing university students. In addition, it will help those researchers who have interest in this field to keep insight into different concepts and their importance for applications in real life. This has been done to make the edited book more flexible and to stimulate further interest in topics.

This book is comprised of three sections.

1. Security in Mobile Computing
2. Cyber Security Techniques and Cases
3. Leadership, Communication, and Education in Cyber Security.

ORGANIZATION OF THIS BOOK

In this book, we present 16 chapters aimed at emphasizing threat and countermeasures that are applicable in today's society. For coherency, we have ordered the chapters in terms of similarity of topic. The topic covered range from threats in mobile devices to developing leaders in cyber security.

Chapter 1, "A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism", presents the some of the concepts contained within the book. Further discussed are emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.

Chapter 2, " Mobile Devices: The Case for Cyber Security Hardened Systems", discusses how mobile devices are the preferred device for web browsing, emailing, using social media and making purchases. Due to their size, mobile devices are easily carried in people's pockets, purses or briefcases. Unfortunately, the popularity of mobile devices is a breeding ground for cyber attackers. Operating systems on mobile devices do not contain security software to protect data.

Chapter 3, " Security Threats on Mobile Devices", contains basic introduction into security models of modern operating system like Android, iOS or Windows Phone. There are described the methods of attacks to the mobile devices. Such attacks consist of application based threats and vulnerabilities, network based attacks and internet browser vulnerabilities. Another section in this chapters contains a description of defensive strategies and steps for securing the device. There is also section about securing mobile device for enterprise environment.

Chapter 4, "The Human Factors in Mobile Phishing", presents the use of electronic media, like emails and mobile text messages, to fraudulently elicit private information or obtain money under false pretence.

Chapter 5, " Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Networks", investigates and exposes methods and techniques developed to provide security in wireless ad hoc networks. are investigated and effectiveness and efficiency of these mechanisms are exposed.

Chapter 6, "Legal Issues: Security and Privacy with Mobile Devices", raises the issues of privacy and security being woven into the fabric of American law concerning mobile devices. It is essential to fully understand associated laws and policies to ensure proper execution while upholding the law. As the American society significantly uses mobile devices it is imperative to understand the legal actions surrounding these technologies to include their associated uses. With 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Mobile devices are not like the devices of the past as the computing power is on par with that of some desktops to include these devices have the ability to execute malicious applications.

Chapter 7, "Survey in Smartphone Malware Analysis Techniques", surveys various approaches used in Mobile malware detection and Investigates weaknesses of existing countermeasures such as signature-based and anomaly-based detection.

Chapter 8, "Trust Management in Mobile Ad hoc Networks for QoS Enhancing", is the proposition of a trust based environment for MANET and securing it against collusion attack in order to enhance the network QoS. This is achieved using three steps: (1) the definition of a formal trust based environment (2) the addition of a process handling collusion attack and (3) the extension of the whole proposition by a delegation process allowing nodes functionalities sharing.

Chapter 9, "Insider Threats: Detecting and Controlling Malicious Insiders", presents how malicious insiders are posing unique security challenges to organizations due to their knowledge, capabilities, and authorized access to information systems. This chapter investigates the scale and scope of malicious insider risks and explore the impact of such threats on business operations.

Chapter 10, "Authorship Analysis: Techniques and Challenges", discussed the process of examining documents to determine the stylistic details underlying the document and hence inferring about the characteristics of the author of document in order to attribute the authorship to a particular author or to confirm the authenticity of a claimed authorship. The authors discuss the existing methods that have been used so far to deal with automation of authorship analysis and the challenges faced by them

Chapter 11, "The Need for a Dualist Application of Public and Private Law in Great Britain Following the Use of "Flame Trolling" During the 2011 UK Riots: A Review and Model", recommends further research to establish whether it should be the case that in a society based on dualism that criminal and civil cases should be held at the same time, and that in both instances those being accused of an offence or tort should be allowed to bring a counter-claim. It is discussed that in such a system the cases that would be brought are where there is a clear victim who had no part in the offence against them, such as murder, rape, theft and burglary, which are usually carefully planned and orchestrated acts.

Chapter 12, "Native Language Identification (NLID) for Forensic Authorship Analysis of Weblogs", presents introduces NLID and considers the casework applications with regard to authorship analysis of online material. It presents findings from research identifying which linguistic features were the best indicators of native (L1) Persian speakers blogging in English, and analyses how these features cope at distinguishing between native influences from languages that are linguistically and culturally related.

Chapter 13, "Leadership Approaches for Managing Healthcare Information Security Millennial Employees: Health Information Security Leadership Approaches", presents

Chapter 14 "Learning Management Systems: Understand and Secure Your Educational Technology" presents background data concerning breaches and the lack of associated talent to support these cyber attacks. This chapters explores how to achieve this among millennial employees.

Chapter 15, "The Innovation and Promise of STEM Oriented Cyber Security Charter Schools in Urban Minority Communities: Cyber Terrorism Workforce Development", provides insight on how the US pipeline of minority students studying STEM falls short in producing the next generation of cybersecurity professionals.

Chapter 16, "Communication, Technology & Cyber Crime in Sub-Saharan African", discusses mobile and internet technologies currently being utilized in Sub-Saharan Africa as well as some of the major cybersecurity concerns threatening networks in the region that are associated with the new economic growth on the African continent. This is important as this region is rapidly developing its technology base. Sub-Saharan Africa is experiencing many of the issues associated with the benefits of cyber technology as well as its many negative sides.

Maurice Dawson
University of Missouri – St. Louis, USA

Marwan Omar
Nawroz University, Iraq

Table of Contents

Foreword xvi

Preface xviii

Chapter 1
A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism 1
Maurice Dawson, University of Missouri – St. Louis, USA

Chapter 2
Mobile Devices: The Case for Cyber Security Hardened Systems 8
Maurice Dawson, University of Missouri – St. Louis, USA
Jorja Wright, Florida Institute of Technology, USA
Marwan Omar, Nawroz University, Iraq

Chapter 3
Security Threats on Mobile Devices 30
Lukáš Aron, Brno University of Technology, Czech Republic

Chapter 4
The Human Factor in Mobile Phishing 53
Rasha Salah El-Din, University of York, UK
Paul Cairns, University of York, UK
John Clark, University of York, UK

Chapter 5
Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks 66
Arif Sari, European University of Lefke, Cyprus

Chapter 6
Legal Issues: Security and Privacy with Mobile Devices 95
Brian Leonard, Alabama A&M University, USA
Maurice Dawson, University of Missouri – St. Louis, USA

Chapter 7
Survey in Smartphone Malware Analysis Techniques 105
Moutaz Alazab, Isra University, Jordan
Lynn Batten, Deakin University, Australia

Chapter 8
Trust Management in Mobile Ad Hoc Networks for QoS Enhancing 131
Ryma Abassi, City of Communication Technologies, Tunisia

Chapter 9
Insider Threats: Detecting and Controlling Malicious Insiders 162
Marwan Omar, Nawroz University, Iraq

Chapter 10
Authorship Analysis: Techniques and Challenges 173
Athira U., LBS Center for Science and Technology, India
Sabu M. Thampi, IIITMK, India

Chapter 11
The Need for a Dualist Application of Public and Private Law in Great Britain Following the Use of "Flame Trolling" During the 2011 UK Riots: A Review and Model 195
Ivan Mugabi, Centre for Research into Online Communities and E-Learning Systems, UK
Jonathan Bishop, Centre for Research into Online Communities and E-Learning Systems, UK

Chapter 12
Native Language Identification (NLID) for Forensic Authorship Analysis of Weblogs 213
Ria Perkins, Aston University, UK

Chapter 13
The Critical Need for Empowering Leadership Approaches in Managing Health Care Information Security Millennial Employees in Health Care Business and Community Organizations 235
Darrell Norman Burrell, Florida Institute of Technology, USA
Darryl Williams, Walden University, USA
Taara Bhat, George Mason University, USA
Clishia Taylor, National Graduate School of Quality Management, USA

Chapter 14
Learning Management Systems: Understand and Secure Your Educational Technology 253
Sharon L. Burton, American Meridian University, USA
Rondalynne McClintock, Claremont Graduate University, USA
Darrell N. Burrell, Florida Institute of Technology, USA
Kim L. Brown-Jackson, National Graduate School of Quality Management, USA
Dustin Bessette, National Graduate School of Quality Management, USA
Shanel Lu, National Graduate School of Quality Management, USA

Chapter 15
The Innovation and Promise of STEM-Oriented Cybersecurity Charter Schools in Urban Minority Communities in the United States as a Tool to Create a Critical Business Workforce 271
Darrell Norman Burrell, Florida Institute of Technology, USA
Aikyna Finch, Strayer University, USA
Janet Simmons, The National Graduate School of Quality Management, USA
Sharon L. Burton, Florida Institute of Technology, USA

Chapter 16
Communication, Technology, and Cyber Crime in Sub-Saharan Africa 286
Dustin Bessette, National Graduate School of Quality Management, USA
Jane A. LeClair, National Cybersecurity Institute at Excelsior College, USA
Randall E. Sylvertooth, National Cybersecurity Institute at Excelsior College, USA
Sharon L. Burton, Florida Institute of Technology, USA

Related References 298

Compilation of References 328

About the Contributors 359

Index 366

Detailed Table of Contents

Foreword xvi

Preface xviii

Chapter 1
A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism 1
Maurice Dawson, University of Missouri – St. Louis, USA

Cyber security is becoming the cornerstone of national security policies in many countries around the world as it is an interest to many stakeholders, including utilities, regulators, energy markets, government entities, and even those that wish to exploit the cyber infrastructure. Cyber warfare is quickly becoming the method of warfare and the tool of military strategists. Additionally, it is has become a tool for governments to aid or exploit for their own personal benefits. For cyber terrorists there has been an overwhelmingly abundance of new tools and technologies available that have allowed criminal acts to occur virtually anywhere in the world. This chapter discusses emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.

Chapter 2
Mobile Devices: The Case for Cyber Security Hardened Systems 8
Maurice Dawson, University of Missouri – St. Louis, USA
Jorja Wright, Florida Institute of Technology, USA
Marwan Omar, Nawroz University, Iraq

Mobile devices are becoming a method to provide an efficient and convenient way to access, find and share information; however, the availability of this information has caused an increase in cyber attacks. Currently, cyber threats range from Trojans and viruses to botnets and toolkits. Presently, 96% of mobile devices do not have pre-installed security software while approximately 65% of the vulnerabilities are found within the application layer. This lack in security and policy driven systems is an opportunity for malicious cyber attackers to hack into the various popular devices. Traditional security software found in desktop computing platforms, such as firewalls, antivirus, and encryption, is widely used by the general public in mobile devices. Moreover, mobile devices are even more vulnerable than personal desktop computers because more people are using mobile devices to do personal tasks. This review attempts to display the importance of developing a national security policy created for mobile devices in order to protect sensitive and confidential data.

Chapter 3
Security Threats on Mobile Devices 30
Lukáš Aron, Brno University of Technology, Czech Republic

This chapter contains basic introduction into security models of modern operating system like Android, iOS or Windows Phone. There are described the methods of attacks to the mobile devices. Such attacks consist of application based threats and vulnerabilities, network based attacks and internet browser vulnerabilities. The following section contains description of defensive strategies and steps for securing the device. There is also section about securing mobile device for enterprise environment. At the end of this chapter are discussed recommendations for security practices for mobile devices.

Chapter 4
The Human Factor in Mobile Phishing 53
Rasha Salah El-Din, University of York, UK
Paul Cairns, University of York, UK
John Clark, University of York, UK

Phishing is the use of electronic media, like emails and mobile text messages, to fraudulently elicit private information or obtain money under false pretence. Though there is considerable interest in phishing as a security problem, there is little previous research from the human factors perspective and in particular very little empirical support for what makes mobile phishing effective or successful and therefore how best to defend people from it. This chapter describes some of the research conducted from the field of traditional phishing that already embraces the effect of human factors on phishing vulnerability. The limited amount of research exploiting mobile phishing is discussed; including a review of our previous work involving evaluating mobile users' strategies for managing mobile phishing attacks. By reflecting on how these subjects investigating the threat of phishing, this chapter aims to show that empirical research on mobile phishing is scarce and falling behind in terms of identifying underlying psychological processes and inspire future research in this area.

Chapter 5
Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks 66
Arif Sari, European University of Lefke, Cyprus

The purpose of this chapter is to investigate and expose methods and techniques developed to provide security in wireless ad hoc networks. Researchers have proposed variety of solutions for security problems of Wireless Mobile Ad-Hoc Networks (MANET) against Distributed Denial of Service (DDoS) attacks. Due to the wireless nature of the channels and specific characteristics of MANETs, the attacks cannot be defeated through conventional security mechanisms. An adversary can easily override its medium access control protocol (MAC) and continually transfer packages on the network channel and the access point node(s) cannot assign authorization access to shared medium. These attacks cause a significant decrease on overall network throughput, packet transmission rates and delay in the MAC layer since other nodes back-off from the communication. In this chapter the proposed methods are applied for preventing and mitigating different wireless ad hoc network attacks are investigated and effectiveness and efficiency of these mechanisms are exposed.

Chapter 6
Legal Issues: Security and Privacy with Mobile Devices 95
Brian Leonard, Alabama A&M University, USA
Maurice Dawson, University of Missouri – St. Louis, USA

Privacy and security are two items being woven into the fabric of American law concerning mobile devices. This chapter will review and analyze the associated laws and policies that are currently in place or have been proposed to ensure proper execution of security measures for mobile and other devices while still protecting individual privacy. This chapter will address the fact that as the American society significantly uses mobile devices, it is imperative to understand the legal actions surrounding these technologies to include their associated uses. This chapter will also address the fact that with 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Furthermore, this chapter will examine how mobile devices are not like the devices of the past as the computing power is on par with that of some desktops and the fact that these devices have the ability to execute malicious applications. In addition, this chapter will discuss the reality, significance, legal and practical affects of the fact that suspicious programs are being executed offensively and security based attacks can be performed as well with the use of programs such as Kali Linux running on Android.

Chapter 7
Survey in Smartphone Malware Analysis Techniques 105
Moutaz Alazab, Isra University, Jordan
Lynn Batten, Deakin University, Australia

Smartphone Malware continues to be a serious threat in today's world. Recent research studies investigate the impacts of new malware variant. Historically traditional anti-malware analyses rely on the signatures of predefined malware samples. However, this technique is not resistant against the obfuscation techniques (e.g. polymorphic and metamorphic). While the permission system proposed by Google, requires smartphone users to pay attention to the permission description during the installation time. Nevertheless, normal users cannot comprehend the semantics of Android permissions. This chapter surveys various approaches used in Smartphone malware detection and Investigates weaknesses of existing countermeasures such as signature-based and anomaly-based detection.

Chapter 8
Trust Management in Mobile Ad Hoc Networks for QoS Enhancing 131
Ryma Abassi, City of Communication Technologies, Tunisia

In a collaborative environment such as MANET, nodes reliability evaluation is vital. Trust Management can be used to ensure such healthy collaboration it offers a formal and unified framework for trust specification and interpretation. Establishing trustworthy relationships is generally done by maintaining a reputation for each node computed based on direct observations or neighbors' observations exchanged using recommendations. Unfortunately, for malicious reason, such method may be faked by cheaters: several nodes collude in order to rate each other with the maximum value and decrease other nodes' reputations by giving negative recommendations. The main contribution of this chapter is then, the proposition of a trust based environment for MANET and securing it against collusion attack in order to enhance the network QoS. This is achieved using three steps: (1) the definition of a formal trust based environment (2) the addition of a process handling collusion attack and (3) the extension of the whole proposition by a delegation process allowing nodes functionalities sharing.