

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 investigate 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
<i>Brian Leonard, Alabama A&M University, USA</i>	
<i>Maurice Dawson, University of Missouri – St. Louis, USA</i>	

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
<i>Moutaz Alazab, Isra University, Jordan</i>	
<i>Lynn Batten, Deakin University, Australia</i>	

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
<i>Ryma Abassi, City of Communication Technologies, Tunisia</i>	

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.

Chapter 9

Insider Threats: Detecting and Controlling Malicious Insiders	162
<i>Marwan Omar, Nawroz University, Iraq</i>	

Malicious insiders are posing unique security challenges to organizations due to their knowledge, capabilities, and authorized access to information systems. Data theft and IT sabotage are two of the most recurring themes among crimes committed by malicious insiders. This paper aims to investigate the scale and scope of malicious insider risks and explore the impact of such threats on business operations. Organizations need to implement a multi layered defensive approaches to combat insider risks; safeguarding sensitive business information from malicious insiders require firstly, an effective security policy that communicates consequences of stealing or leaking confidential information in an unauthorized manner. Secondly, logging and monitoring employee activity is essential in detecting and controlling system vulnerabilities to malicious insiders. Thirdly, conducting periodic and consistent insider vulnerability assessments is critical to identifying any gaps in security controls and preventing insiders from exploiting them. And lastly, but certainly not least, taking extra caution with privileged users is important to proactively protecting information infrastructure from insider risks.

Chapter 10

Authorship Analysis: Techniques and Challenges	173
<i>Athira U., LBS Center for Science and Technology, India</i>	
<i>Sabu M. Thampi, IITMK, India</i>	

Authorship Analysis is 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 popularity of online communications has paved way to the promotion of numerous fraudulent acts. These illegal activities can be curbed to an extent by identifying the source of the postings, which is made possible by finding the real authors of online documents. Applicability of authorship analysis in the field of forensic linguistics also gathers great importance today. The automation of, process aimed at analyzing the authorship of forensic documents, eases the linguists of the high manual effort spent in analyzing documents and is also advantageous in terms of its accuracy. Here we discuss about 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	195
<i>Ivan Mugabi, Centre for Research into Online Communities and E-Learning Systems, UK</i>	
<i>Jonathan Bishop, Centre for Research into Online Communities and E-Learning Systems, UK</i>	

Since time immemorial, the legal systems of Great Britain have often been spoken of highly as pinnacles of democracy. However, the split between criminal law and tort law have often caused problems where the police has often focused on the prosecution of people in poverty and where only the wealthy can afford to use the system. This chapter discusses the extent and limitations of existing measures to tackle computer-related crime, particularly with regards to the abusive kind of Internet Trolling, namely “flame trolling.” The chapter 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 213
Ria Perkins, Aston University, UK

This chapter introduces Native Language Identification (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. The first chapter section outlines the area of Native Language Identification, and demonstrates its potential for application through a discussion of relevant case history. The next section discusses a development of methodology for identifying influence from L1 Persian in an anonymous blog author, and presents findings. The third part discusses the application of these features to casework situations as well as how the features identified can form an easily applicable model and demonstrates the application of this to casework. The research presented in this chapter can be considered a case study for the wider potential application of NLID.

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

According to the Ponemon (2012) Third Annual Benchmark Study on Patient Privacy & Data Security, 94 percent of healthcare organizations surveyed suffered at least one data breach; 45 percent experienced more than five in the past two years. Data breaches cost the U.S. healthcare industry an average of \$7 billion annually (Ponemon, 2012). Electronic health records are becoming more pervasive at hospitals and clinics in the United States. Meanwhile, healthcare organizations are taking small steps toward meaningful exchange and secure data security of patient information. This has created a need for new expertise in health data security from a newly degreed and young in information security professionals from the “Millennial Generation”. This chapter explores the attraction, recruitment, and retention of younger-generation professionals with critical and emerging health information security skills.

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

Learning management systems (LMSs) are significant in offering highly collaborative, widely accessible, and manageable learning solutions. It is feasible that learning solutions stakeholders pursue an in-depth understanding of the LMS and the vulnerabilities surrounding technology-enabled learning and teaching. The over 300 types of active LMSs, proprietary or open source, are not off limits to hackers. Past research shows that hackers compromise technology systems to ascertain personal identifiable information and interfere with the integrities of post-secondary institutions. Stakeholders must understand how to safeguard the LMS. To address LMS cybercrime concerns, this text reviews vulnerability information on over 12 LMS features. After reading this text, stakeholders will gain increased insight into their works to thwart security related LMS incidents. This text can support stakeholders' knowledge in actions to take prior to the LMS reaching unacceptable vulnerability levels. Researchers and practitioners will benefit from this text's perspective on the LMS and mitigating risk.

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

This text is an on-going study to provide current information regarding developing underrepresented student populations through STEM specific Charter schools to fulfill pipeline shortages. Current findings show that African Americans are underrepresented in high paying Science, Technology, Engineering, and Mathematics (STEM) fields, especially in cybersecurity. The U.S. pipeline of minority students studying STEM falls short in producing the next generation of cybersecurity professionals; thus, a salient need exists to design, pilot, and test a program to grow the minority student pipeline in the cybersecurity field. The charter school movement is one of the fastest growing education reforms with the ability to make a dramatic impact in the U.S. and internationally. Because charter schools often organize around a mission, theme, or curricular and enjoy freedoms, in organizational structure, mission, and academic program, with all held to high standards, this text proposes cybersecurity charter schools to fill technology voids. This organizational structure, mission, and academic programming, will enable students to become immersed in hands-on, real world applications allowing for experiential learning, which can develop students with cybersecurity expertise, technical knowledge, and skills, and competencies needed to take and pass cybersecurity and information security related certification assessments.

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

As a region that 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. This paper 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. Such topics will include a viable increased awareness of news, historical events, and recent gatherings of information on this main topic.

Related References 298

Compilation of References 328

About the Contributors 359

Index..... 366