Preface

Mobile Forensic has grown from relatively obscure tradecraft to an important part of many investigations. Mobile Forensic tools are now used on a daily basis by examiners and analysts within local, state and Federal law enforcement; within the military and other US government organizations; and within the private "e-Discovery" industry. Developments in forensic research, tools, and process over the past decade have been very successful and many in leadership positions now rely on these tools on a regular basis frequently without realizing it. Moreover, there seems to be a widespread belief, buttressed on by portrayals in the popular media, that advanced tools and skillful practitioners can extract actionable information from practically any device that a government, private agency, or even a skillful individual might encounter. The field of Mobile forensic analysis is as rapidly changing as other security fields.

OBJECTIVE OF THE BOOK

Mobile security when combined with mobile forensic gives rise to a term known as mobile investigation and analysis, which is nothing but a type of digital forensics which aims at the analysis of mobile device and data of a system for collection of information pertaining to the legal evidence related to various security breaches and intrusion detection. The mobile network investigations that are performed by it utilize the dynamic information characteristic of a system which changes rapidly with time; hence it is a crucial task.

The two major tasks that are performed by it include:

- Keeping a check over anomalous traffic
- Intrusion detection

The intruder tries to steal significant information from the communication that takes place in the mobile network. The mobile forensic analysis deals with identifying all such vulnerable operation along with the legal law enforcement that will be triggered after that. Example: analyzing the chat sessions. Several tools

are available for performing mobile forensics like Wireshark. Another category of mobile forensic is mobile data analysis which deals with Android and iOS and its applications. The use of malware analysis plays a crucial role in this.

ORGANIZATION OF THE BOOK

This book consists of 11 chapters which are organized in two sections. The first section of the book comprises of five chapters that contain the chapters focusing mainly on forensic investigations and analysis in a smartphone, and wireless transmission. The second section contains six chapters focusing mainly on the security and privacy issues in mobile and wireless communication. A brief description of each of the chapters follows:

Section 1: Forensic Investigation and Issues in the Mobile and Wireless Device

Chapter 1

As the world is moving towards digitization, security has become a major concern. The improper usage of mobile devices, giving permission to every downloaded application has increased criminal activities. Criminals are finding new ways to compromise mobile systems and servers to gain access to sensitive information. The field of Digital Forensics has grown rapidly with the increased trends in mobile devices in every sector. Mobile Forensics is the emerging pattern of work. The analysis of today's trends shows that the complexity of crime has increased with human errors. This paper discusses the increased dependency of all age groups, mostly senior citizens and Teenagers on internet and smartphone. Both of these groups spend maximum time on the internet without checking the corners cases and the vulnerability in using the required application. Some safeguard measures have been discussed in this Paper to educate them. The Paper also discusses digital forensics that is the solution to the data breach. The systematic steps followed by forensics investigator for identification, preservation of the evidence and the importance of maintaining the Chain of custody is discussed. The comparative study of various models of mobile (iPhone, Android, Windows-based, Blackberry) based on their acquisition techniques are explained. How Android is vulnerable and how Geodata and Metadata of inbuilt sensors (with explicit or implicit permission) can help digital investigators as context awareness for solving the case is discussed here. At the end of Paper, the real-time example is illustrated explaining how an application with Geodata records on smartphones can provide forensic investigators with valuable information on the whereabouts of a person at certain timestamps.

Chapter 2

The 21st century has seen rapid developments in technology. The journey from small, heavy mobile phones to ultra-slim smartphones has been extremely fast. The present generation smartphones are capable of performing every task that a normal desktop computer can perform and therefore is evident that smartphones have become the most powerful and most popular choice of a hardware device. Improved technology adds with its security concerns and network risks. Modern day smartphones can be easily hacked and data can be stolen, modified or removed from the cell phone devices in a matter of seconds. The unprecedented growth of smartphone calls for improved security services through deep forensic research and investigation processes.

The chapter, Smartphone Security and Forensic Analysis focuses on smartphone vulnerabilities and forensic tasks that can be carried out on smartphones. Vulnerabilities to smartphone security and threats associated with them like malware, network attacks etc have been discussed. Different techniques of forensic analysis like port scanning and monitoring have been investigated. Experiment based case study has been presented along with its results. Furthermore, the chapter presents possible security threats on smartphones and analyses ways to tackle them. Future research areas and work related to the field of smartphone security have been presented at the end.

Chapter 3

This research contributes towards designing a mathematical prototype of the malicious e-worms that are developing and spreading in the wireless IoT communications every hour of every day or even lesser. The sensor nodules are most exposed to the e-worms' attack. The e-worms infiltrate into the sensor networks through snooping, analyzing, modifying the traffic at any nodule and various other occasions during a huge amount of information transmission. E-worms considered in the study are the ones' that are vulnerable to bout during the data or statistics transfers in the network. Such nodules further turn infective having the capability to spread the infection throughout the structure. This condition worsens when the malware consisting e-worms have the ability to kill the infected nodules before they can be recovered with the help of any safety measure such as anti-malware or security patches. If the safeguard entity reaches the infected nodule, the infected ones into the recovered nodule. In the article, safekeeping of IoT-based infrastructures has been investigated. Altering the crashing rate of e-worms may turn the system to chaotic-conduct. It can be concluded that the chaotic behavior in the functioning may lead to shutting down of the complete-integration. The study focuses on the system's randomness being

caused by the various forms of e-worms in the present day being attacked at various points of the integration. It is observed that motivating the malware to flourish hastily causes nodules to absorb an increased amount of the finite-energy that endangers durability and steadiness. Based on the case study, understanding of e- worms' danger among sensors improves. Also, discover the relationships among various components as node sensors, snooping behaviors, and attack's surface. Simulations recorded that intimidating propagation methods prove to be counterproductive in securing nodes. This research will enable the developers in developing highly efficient anti-dotes that may optimize i.e. minimize actions of e-worms into sensor-nodules. This will serve as an advantage to consumers for proper-vaccination, i.e. implementation for apt antiviruses towards sensor nodules into sensor-spaces to provide strengthened defence-mechanism and to the minimization of attacks.

Chapter 4

Biometric authentication is being preferred over traditional authentication techniques in real-world applications. However, there are various risks associated with these techniques as intruders can get hold of personal information or breach an individual's privacy over the web. The chapter discusses the implementation of biometric identification on various web platforms as well as social networking sites. Various aspects like biometric template protection are important as personal information needs to be secured on the server while using such applications. The use of Software Development Kits can help to identify biometric traits. Also, the use of deep learning approaches can ensure excellent performance in these applications. We have demonstrated the use of Verilook SDK and Convolutional Neural Networks to perform facial recognition using the CASIA Face Image Database.

Chapter 5

The rising interest in technological enhancement has increased the number of security issues in network communication. Today Denial of service (DOS) attack becomes immense to any type of attack on a networking structure and disables a network server from servicing its client networks. The main aim of attackers is to break the server security of the web server, application server and data server using the DOS softening technique. Within a short duration, DoS attacks are capable of tiring out any networks computing and communication resources. The attackers initiate the DoS attack with or without advance warning messages. The attacker sends a huge amount of request messages to the server network, thereby slowing down its operating speed. DoS attack may also be initiated by sending request messages with the spoofed IP address or flooding a huge amount of invalid data packets to the

server network. Thus, it is essential to develop a dose detection technique to detect and protect network services. This chapter provides an extensive study on the Botnet and Denial of Service (DoS) attack as well as the different classification of botnet and DoS attacks. It discusses the important features and defense techniques of each attack. The chapter also discusses the various detection and prevention techniques using up to now. We also present the details of some very frequent DoS attack techniques to other systems and at the end; we have also discussed some research gaps in the development of DoS detection and protection mechanisms. The main goal of this chapter is to facilitate a better understanding of DoS attacks and the new coming research areas in this era to find out the research problems and provide the efficient defense solutions for those problems.

Section 2: Security and Privacy Issues in Mobile and Wireless Communication

Chapter 6

Intrusion detection systems provide the facility to track the abnormal activity in the network and detect malicious activity in the network. The objective of this chapter is to provide the performance of various protocols for intrusion detection systems by using different protocols of MANETs. The chapter also covers different types of intrusions, different kinds of attacks, and intruders. The chapter provides detailed information for the IDS, various attacks, simulations, simulators, TCP/IP suits and other various network simulators.

Chapter 7

Mobile Ad-hoc Network (MANET) is a wireless, and self-organizing network of various nodes/systems. The aim of this chapter is to provide a detailed overview of various MANET protocols, and vulnerabilities in different secure routing algorithms of MANETs. This chapter also provides the detailed discussion of various routing protocols such as ARAN (authenticated routing for ad-hoc networks), SAR (Security aware routing), SRP (Secure routing protocol), SEAD (Secure Efficient Ad-hoc Distance Vector), ARIADNE (Secure On-Demand Routing Protocol for Ad-hoc Networks), SLSP (Secure Link State Routing Protocol), and Secure Ad-hoc On-Demand Distance Vector (SAODV) algorithms. Finally, the chapter presents the comparative analysis of various security routing protocols of MANET.

Chapter 8

In Ad-hoc and wireless networks routing protocols are designed to direct about the correct communication guidelines while data and information are passed from one station to other. The basic challenge in these powerful networks lies among machines to coordination, control, register and manage data delivery in networks. Designing an efficient ad hoc network (both in mobile network based and vehicle based) is a very challenging issue because of the way that the vitality controlled nodes are required to run autonomously for extensive stretched duration. Communication over remote media inside time compelled is expected to allow continuous mobile applications like a collaboration between mobile stations or mobile devices or now and then entomb communication among mobile vehicles. The current chapter presents a complete analysis on the current state of the art of the spectacular network of VANET and MANET communication and the vibrant routing schemes used by different networks and in research work as well as provides a learning platform to the new researchers to extend their study and advance in various security concern in the network.

Chapter 9

This chapter is focused on security and privacy aspects when deploying 5G networks/ cloud services. Cloud computing models convenient, on-demand network access to a shared pool of configurable computing resources. However, it makes the client data and computation vulnerable to attacks from potential threats as well as from the untrusted system administrator. Many trials have been done to address the security concerns in cloud computing but not too much help came around, since using a traditional CPU based system, we are unable to fabricate these computing nodes. In this book chapter, a cognitive radio based simultaneous wireless information and power transfer system consisting of one base station, one desired information receiver, multiple primary users, and multiple energy harvesting receivers are considered. Each link in the system suffers from small scale fading and path loss. We focus on the secrecy outage in this network, keeping in mind that the multiple energy harvesting receivers may act as potential eavesdroppers. This chapter is focused on secrecy performance analysis for cognitive radio network where information and power both are extracted from the same received signal with multiple licensed users. This work can be extended to find a relationship for secrecy outage probability using best possible antenna selection scheme so as to improve the secrecy outage probability when the ratio of maximum possible SNR of the channel between transmitters and intended receiver to maximum possible SNR between transmitters and eavesdropper channels. This chapter details cognitive radio network based design and security challenges in 5G communication.

Chapter 10

In this chapter, Ethereum cryptocurrency is discussed, where each transaction is secured by using cryptographic algorithms and there is no need of the third party for completing the transactions. Initially, Ethereum is introduced by giving analogous examples. Thereafter, the backbone of the Ethereum is discussed that is Blockchain with its block diagram and architecture. The authors addressed many questions concerned with Ethereum like who created it? How Does Ethereum Works? etc. Later in this chapter, the application of Ethereum along with apps of Ethereum is served. The various characteristics of Ethereum as well as how the transaction took place in the context of Ethereum is demonstrated. For better understanding, we considered a few examples and facts, each example presented by some easy to read figures. Eventually, challenges are discussed.

Chapter 11

Nowadays, the investment market is growing very fast and is very volatile due to the exponential growth in the use of the Internet. People have a large number of options to purchase an investment in the market. There is always a risk associated with the investment which is proportional to the possible profit. With the growth of Internet use, the fraud is also increasing, thus, this chapter provides details of various security threats associated with the use of online tools for the investments. The chapter also presents various security challenges involved in investment tools. In addition, the chapter presents the proposed solutions and recommendations to avoid loss in investment. This chapter could be a good read for the awareness of an emerging investor.

Kavita Sharma
National Institute of Technology Kurukshetra, India

Mitsunori Makino
Chuo University, Japan

Gulshan Shrivastava
National Institute of Technology Patna, India

Basant Agarwal
Indian Institute of Information Technology Kota (IIIT Kota), India