Detailed Table of Contents

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

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

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.

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

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

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.