Toward Understanding the Challenges and Countermeasures in Computer Anti-Forensics

Kamal Dahbur, New York Institute of Technology, Jordan

Bassil Mohammad, New York Institute of Technology, Jordan

ABSTRACT

The term computer anti-forensics (CAF) generally refers to a set of tactical and technical measures intended to circumvent the efforts and objectives of the field of computer and network forensics (CF). Many scientific techniques, procedures, and technological tools have evolved and effectively applied in the field of CF to assist scientists and investigators in acquiring and analyzing digital evidence for the purpose of solving cases that involve the use or misuse of computer systems. CAF has emerged as a CF counterpart that plants obstacles throughout the path of computer investigations. The purpose of this paper is to highlight the challenges introduced by anti-forensics, explore various CAF mechanisms, tools, and techniques, provide a coherent classification for them, and discuss their effectiveness. Moreover, the authors discuss the challenges in implementing effective countermeasures against these techniques. A set of recommendations are presented with future research opportunities.

Keywords: *Computer Anti-Forensics (CAF), Computer Forensics (CF), Data Hiding, Digital Evidence, Network Forensics*

INTRODUCTION

The use of technology is increasingly spreading covering various aspects of our daily lives. An equal increase, if not even more, is realized in the methods and techniques created with the intention to misuse the technologies serving varying objectives being political, personal or anything else. This has clearly been reflected in our terminology as well, where new terms like cyber warfare, cyber security, and cyber crime, amongst others, were introduced. It is also noticeable that such attacks are getting increasingly more sophisticated, and are utilizing novel methodologies and techniques. Fortunately, these attacks leave traces on the victim systems that, if successfully recovered and analyzed, might help identify the offenders and consequently resolve the case(s) justly and in accordance with applicable laws. For this

DOI: 10.4018/ijcac.2011070103

purpose, new areas of research emerged addressing Network Forensics and Computer Forensics in order to define the foundation, practices and acceptable frameworks for scientifically acquiring and analyzing digital evidence in to be presented in support of filed cases. In response to Forensics efforts, Anti-Forensics tools and techniques were created with the main objective of frustrating forensics efforts, and taunting its credibility and reliability.

This paper attempts to provide a clear definition for Computer Anti-Forensics and consolidates various aspects of the topic. It also presents a clear listing of seen challenges and possible countermeasures that can be used. The lack of clear and comprehensive classification for existing techniques and technologies is highlighted and a consolidation of all current classifications is presented.

Please note that the scope of this paper is limited to Computer-Forensics. Even though it is a related field, Network-Forensics is not discussed in this paper and can be tackled in future work. Also, this paper is not intended to cover specific Anti-Forensics tools; however, several tools were mentioned to clarify the concepts.

After this brief introduction, the remainder of this paper is organized as follows: we provide a description of the problem space, introduce computer forensics and computer anti-forensics, and provide an overview of the current issues concerning this field; an overview of related work is presented with emphasis on Anti-Forensics goals and classifications; we provide detailed discussion of Anti-Forensics challenges and recommendations; and we provide our conclusion, and suggested future work.

THE PROBLEM SPACE

Rapid changes and advances in technology are impacting every aspect of our lives because of our increased dependence on such systems to perform many of our daily tasks. The achievements in the area of computers technology in terms of increased capabilities of machines, high speeds communication channels, and reduced costs resulted in making it attainable by the public. The popularity of the Internet, and consequently the technology associated with it, has skyrocketed in the last decade (Table 1 and Figure 1). Internet usage statistics for 2010 clearly show the huge increase in Internet users who may not necessary be computer experts or even technology savvy (Thuen, 2007).

Unfortunately, some of the technology users will not use it in a legitimate manner; instead, some users may deliberately misuse it. Such misuse can result in many harmful consequences including, but not limited to, major damage to others systems or prevention of service for legitimate users. Regardless of the objectives that such "bad guys" might be aiming for from such misuse (e.g., personal, financial, political or religious purposes), one common goal for such users is the need to avoid detection (i.e., source determination). Therefore, these offenders will exert thought and effort to cover their tracks to avoid any liabilities or accountability for their damaging actions. Illegal actions (or crimes) that involve a computing system, either as a mean to carry out the attack or as a target, are referred to as Cybercrimes (Internet World Stats, n. d.). Computer crime or Cybercrime are two terms that are being used interchangeably to refer to the same thing. A Distributed Denial of Service attack (DDoS) is a good example for a computer crime where the computing system is used as a mean as well as a target.

Fortunately, cybercrimes leave fingerprints that investigators can collect, correlate and analyze to understand what, why, when and how a crime was committed; and consequently, and most importantly, build a good case that can bring the criminals to justice. In this sense, computers can be seen as great source of evidence. For this purpose Computer Forensics (CF) emerged as a major area of interest, research and development driven by the legislative needs of having scientific reliable framework, practices, guidelines, and techniques for forensics activities starting from evidence acquisition, preservation, analysis, and finally presentation.