Chapter 13
Digital Forensics in Distributed Environment

Asha Joseph
VIT University, India

K. John Singh
VIT University, India

ABSTRACT

This chapter is about an ongoing implementation of a digital forensic framework that could be used with standalone systems as well as in distributed environments, including cloud systems. It is oriented towards combining concepts of cyber forensics and security frameworks in operating systems. The framework consists of kernel mechanisms for data and event monitoring. The system monitoring is done in kernel mode by various kernel modules and forensic model mapping is done in user mode using the data collected by those kernel modules. Further, the authors propose a crime model mapping mechanism that makes use of rule sets that are derived from common cyber/digital crime patterns. The decision-making algorithm can be easily extended from a node in a computing cluster, to a cloud. The authors discuss the challenges to digital forensics in distributed environment and cloud extensions and provide some case studies where the proposed framework is applied.

INTRODUCTION

This chapter is about an ongoing implementation of the framework in the field of digital forensic which could be used with the standalone system as well as for forensics in the distributed environment. It is oriented towards combining the concepts of cyber forensics, security frameworks in Operating Systems, digital forensic support integrated with Operating Systems, challenges of digital forensics and proposed solution for such challenges in a typical distributed computing environment.

Digital forensics is around for a while and is rapidly becoming a specialized and accepted investigative technique with its own tools and legal precedents that validate the discipline. The aim of digital forensics is not to prevent the crime as and when it happens, but to identify the victim and criminal either proactively or after the attack or incident occurs in the system or in the network; analyze it in depth

DOI: 10.4018/978-1-5225-4100-4.ch013

and record it for further reference. Computer forensics can be defined as "the application of computer investigation and analysis techniques in the interests of determining potential legal evidence"; while digital forensics can be defined as "the application of scientifically established methods in preserving, collecting, validating, identifying, analysing, interpreting and presenting digital evidence to the court of law after obtaining the evidence from reconstruction of events if possible". Digital forensics can be categorized into different groups such as Cyber Forensics, Disk Forensics, Memory Forensics, Cloud Forensics, Network forensics etc. And the attackers are usually referred as cyber criminals not as digital criminals and the crime is referred as cybercrime.

BACKGROUND

Digital Forensics

The application of scientifically established methods in collecting, preserving, validating, identifying, analyzing, interpreting and presenting digital evidence to the court of law after obtaining the evidence from the reconstruction of events if possible.

Memory Forensics

It is the forensic analysis of a computer's memory dump. Advanced computer attacks will use stealth techniques to avoid leaving traceable evidence data on the computer's non-volatile memory (hard drive, SSD etc). In those situations, the computing system's memory (RAM) dump is taken using OS tools or third-party tools for further forensic analysis. Using OS tools and symbolic debugging information of the OS components, it is possible to substantially recreate the state of the computing system to a reasonable analysis at the process and resource level.

Disk Forensics

It is the analysis of storage devices which comes in numerous categories in terms of physical interfaces and storage technologies. The forensic analysis of disks mainly consists of the application and operating system logs, picture analysis, signature/keyword analysis of known digital entities of criminal nature, timeline analysis, mailbox, databases, cookies, registry – virtually any persistent data that is commonly used by various application software and operating system.

Network Forensics

It is all about the monitoring and analysis of computer network traffic for evidence collection, information gathering or even intrusion detection. Compared to the other areas of digital forensics, network forensics deal with more volatile data and thus it is considered as a proactive approach to forensic investigation (Sammons, 2015)

Network security should be a huge concern to all of us since the networks are under near-constant attack from lone hackers, organized criminals, and foreign countries. Cybercrime, Cyberwar, and cyberterrorism are major problems threatening not only our countries and companies but our personal computers