Chapter 19

Forensic Investigative Process for Situational Awareness in Information Security

Khidir Mohamed Ali
Jubail University College, Saudi Arabia

Thomas John Owens
Brunel University, UK

ABSTRACT

As a starting point for the development of a common visualization of the forensics process by the members of an investigating team, this chapter provides algorithms that provide guidance and step by step instructions on how to deal with computer forensics and the investigations they carry out. A general introductory overview of computer forensics is provided, and the framework of a forensic investigation is summarized. On the basis of this framework, three algorithms are provided, one for each phase of a forensic investigation, which cover the different aspects of computer forensics and address key elements to be considered when attacked systems are investigated.

INTRODUCTION

Essential security features of Computer Network Defense Situational Awareness (SA) are integrity, forensics, availability, intelligence capability and confidentiality. One of the core objectives of Cyber-SA is to ensure the mission has the capability to carry out post incident analysis, investigation, and possesses forensic readiness capability. The aim of the mission to ensure it detects and stops potential security incidents, however, incidents do succeed and in such situations forensic readiness capabilities are required for situational awareness. Forensic analysis can ensure that the investigative team is aware of the nature of an incident. Lessons learned from analyzing the parts of the path of the attack vector can inform the strengthening of mission security (Onwubiko 2011). In seeking to discover additional evidence the investigative team may generate hypothetical

DOI: 10.4018/978-1-4666-0104-8.ch019

intrusion scenarios and try to fit them against discovered intrusion evidence. The results can be used to help the investigative team determine the origin and complete path of an attack vector, and ultimately lead to the discovery of additional evidence (Hawrylak et al 2011).

Visualization and collaboration are key enablers in the overall Cyber-SA command and control process (Ruiz and Redmond 2011). Therefore, they are essential for the effective working of an investigating team. However, a major issue in cyber security is the lack of shared mental models of the elements of the problem space of Cyber-SA. Different analysts often have different mental models of a problem because the "terrain" is virtual and because they possess different expertise. The defended network can be represented as the physical interconnection of devices but the possibility of attackers getting access to the physical devices means that there is in reality no physical space constraint. Consequently, logical topologies are more suitable to representing a workspace (Ballora et al 2011).

As a starting point for the development of a common visualization of the forensics process by the members of an investigating team this chapter provides algorithms which give guidance and step by step instructions on how to deal with computer forensics and the investigations they carry out. These algorithms cover different aspects of computer forensics and address key elements to be considered when attacked systems are investigated. Algorithms are unlikely to be created that provide a complete model of the forensics process but they are a starting point from which additional guidance can be provided to analysts on the basis of their particular expertise that leverages their existing understanding of the workspace.

Computer and information crimes can be looked at as the result of the growing trend of society depending upon and improving its use of technology.

As e-commerce and online business become part of today's business world, computer attacks and cybercrimes are continually on rise. The legal system, law enforcement, computer forensics and investigations seem to be behind in their efforts to track down criminals and successfully to prosecute them.

Computer forensics is a new discipline in computer science. It is concerned with the gathering, retrieving and evaluating of electronic data, for the purpose of stopping and preventing computer fraud, or gather and preserve digital evidence for a criminal investigation, or to recover data accidentally lost or deleted.

Computer forensics requires detailed and comprehensive knowledge in all aspects of computing such as computer architecture, hardware design, programming, and operating systems.

This chapter addresses some of the most important elements of computer forensics and evidence including issues that deals with investigations and enforcement. The emphasis of this chapter is on creating and developing a computer forensics investigation framework.

Computer forensics is an approach or method used by investigators to identify the source of an attack on computer and data-related resources and systems. Investigations should be conducted in a predefined and structured manner that enables the information and data collected to be used as evidence in a court of law during criminal prosecution of the attacker. We can conclude from what was stated above the primary goals of computer forensics as follows:

- Identification of undesirable events and activities that occurred.
- Gathering, processing, storing and preserving evidence to be introduced in the court of law.
- To use that knowledge to prevent future occurrences. (ISACA 2011).