International Journal of Web Services Research
Volume 17 • Issue 1 • January-March 2020

Applying Digital Forensics to Service Oriented Architecture

Aymen Akremi, Umm Al-Qura University (UQU), Makkah, Saudi Arabia

Hassen Sallay, Umm Al-Qura University (UQU), Makkah, Saudi Arabia

Mohsen Rouached, University of Bahrain, Manama, Bahrain

Rafik Bouaziz, University of Sfax, Sfax, Tunisia

ABSTRACT

Digital forensics is an emerging research field involving critical technologies for obtaining evidence in digital crime investigations. Several methodologies, tools, and techniques have been developed to deal with the acquisition, preservation, examination, analysis, and presentation of digital evidence from different sources. However, new emerging infrastructures such as service-oriented architecture has brought new serious challenges for digital forensic research to ensure that evidence will be neutral, comprehensive, and reliable in such complex environment is a challenging research task. To address this issue, the authors propose in this article a generic conceptual model for digital forensics methodologies to enable their application in a service-oriented architecture. Challenges and requirements to construct a forensically sound evidence management framework for these environments are also discussed. Finally, the authors show how digital forensics standards and recommendations can be mapped to service-oriented architecture.

KEYWORDS

Digital Forensics, Forensics Concepts, Forensics for Web Services, Forensics Taxonomy

INTRODUCTION

Digital forensics is the process of employing scientific principles and processes to deal with the acquisition, preservation, examination, analysis and presentation of digital evidence from diverse sources. The job of the forensic examiner is to analyze the digital information and reconstruct a timeline of events that describes, as best as possible, what happened, when it happened, and who did it. Digital forensics has become a prominent part of many criminal investigations. It is an important business and research area for solving computer crimes as well as the retrieval of evidence that resides in a digital format. The past decade has witnessed significant technological advancements to aid during a digital investigation (Raghavan, 2013). A lot of methodologies, tools, techniques, and approaches have been designed and developed to acquire and analyze digital evidence from different sources.

In recent years, the exponential growth of technologies and the appearance of new emerging paradigms has brought with it new serious challenges for digital forensic research. Existing digital

DOI: 10.4018/IJWSR.2020010102

forensics standards and regulations should be extended to cope with the increased new requirements and exigencies. However, despite significant efforts in this field, little has been written about the applicability of forensics to open environments and new infrastructures. The service oriented architecture (SOA) is one of these open environments which supports web services (WS) technology to implement and design everyday sensitive, mission-critical operational applications and business processes. Today, business processes are increasingly implemented by dynamically composing web services seen as the main contribution that the SOAs bring to enterprise business process automation, thus enabling the creation of complex systems that are interoperable, composable, extensible, and dynamically reconfigurable. Complex dependencies can be created between web services offered by different organizations using compositional techniques such as choreography, orchestration, dynamic invocation, and brokering. However, the SOA nature of orchestrating services supplied by different vendors in different geographic locations makes it harder for regular security measures to detect malicious activities. Many attractive features that web services offer, like greater accessibility of data, dynamic application-to-application connections, and relative autonomy, conflict with traditional security models and controls. Indeed, the complex interdependencies may be exploited by attackers to find some localized or compositional flaws. Such attacks can affect multiple servers and organizations, resulting in financial loss or infrastructural damage. Furthermore, it is difficult to investigate such incidents because these dependencies should be retained in a neutral and secure manner.

A forensic investigation framework for this type of application should enable the reconstruction of transactions spanning multiple organizations. Investigators should be able to identify scenarios of web services being misused, exploited, or otherwise compromised, which helps in redesigning Web services to mitigate identified risks. However, despite its importance, literature addressing the need for such framework is very scarce. Also, composition of web services has been an active area of research and several efforts have led to the development of platforms and languages to support composition and deployment of services. However, these approaches fail to recognize that even optimized strategies for service selection involve the exchange of large amounts of potentially sensitive data, causing potentially serious forensics leaks. Consequently, forensics is still among the key challenges that keep hampering service composition-based solutions and forensics breaching incidents on the Web continue to make the headlines. A standardized framework would make forensic investigations more efficient and raise consumer confidence in SOA security (Marrington, Branagan, & Smith, 2007).

In this context, we propose in this paper to review and analyze existing digital forensics methodologies to study their applicability in web services-based infrastructures. In contrast with several existing studies surveys about digital forensics (Sansurooah, 2006; Pollitt, 2008; Hall & Davis, 2005; Cohen, Lowrie, & Preston, 2011; von Solms & Louwrens, 2006), we draw our study from a technical point of view based on a generic conceptual model. After discussing challenges and requirements of applying digital forensics for SOA, we propose a mapping of digital forensics standards and recommendations to these open environments. The aim is to construct a forensically sound evidence management framework to accurately account for the global behaviors of Web services-based applications in a secure, participant-neutral, and non-refutable way.

The main contribution of this paper resides on the definition of new forensics taxonomy for web services enabling the understand of all required forensics information to be preserved and considered during any investigation case or even during the design of new record management system for any purpose. We based our research and taxonomy on existing standards to fulfill international forensics requirements. We extend those standards to cope with web services requirements since web services technology arises new forensics challenges discussed in this paper.

The remainder of this paper is organized as follows. Section 2 discusses the background about digital forensics. In section 3, we depict and detail our conceptual model to provide generic understanding of digital forensics concepts, properties, and requirements. Section 4 explores the requirements of a framework to perform effective forensic examinations in web services-based infrastructures. We discuss challenges in forensic investigations involving web services, describe how