XML Injection Attacks in Digital Forensic Investigations and Proposed Defense Mechanisms

Introduction

Modules, systems and network with content based on XML are no longer secure against malicious activities now-a-days. Various vulnerabilities are encountered in the operations of such components, which take advantage in executing XML attacks. Attackers misuse XML content and its features in systems to carry out Denial of Service (DOS) attacks, access logical files remotely, generate network connections to other machines and bypassing firewalls. XML attacks are categorized as XML External Entity (XXE) attacks, XXE Injection attacks, Resource Exhaustion attacks, Data Extraction attacks, SSRF attacks and Advanced XXE Injection attacks, and they are conducted by different mechanisms to exploit vulnerabilities. All these XML attacks; XML poisoning are used to tamper data in systems and network which ultimately results in destroyed and malfunctioned systems, especially at present in the Digital Forensics field. As Digital Forensics is a rapid advancing area, where procedures related to cyber-crimes, victims and suspects are evaluated and penalized successfully at present, attackers too tend to use their exploiting skills to degrade the performance of Forensics Investigations. Due to the conducted XML based attacks, specifically XML External Entity (XXE) attacks and XXE Injection attacks, attackers are capable of altering and hiding evidence and interrupting investigation processes. As a result of failed forensic investigations, investigators become vulnerable in front of the truth to and unable to extract the actual evidence from digital devices and network. This paper describes about the current approaches of XML attacks in Forensic investigations and proposes a defense mechanism.

Problem Statement

In Digital Forensics it was identified that investigators face a lot of issues when dealing with evidence after being tampered due to XML attacks. Attackers uses techniques to identify vulnerabilities against XML based content and try to maliciously upload illegitimate files to systems, hide sensitive files and modify evidence. XML based applications allow attackers to upload files which are then processed server-side. These misconducts, result forensics investigations and investigators to end the procedures without coming up with the accurate decisions.

Solution

The main objective of this research paper is to express a mechanism proposed for XML injection attacks conducted by cyber-criminals during digital forensic investigations. Evidence containing in documents, files and message contents are modified and hidden from investigators, and those data are not able to be discovered as true information. Thereby, this research proposes a solution to convert all text based files and messages, compromised by XML injections, to the original state of information and present them in a meaningful manner. For this mechanism the Digital Forensic XML (DFXML) toolkit is utilized to express the evidence in an authentic way to the investigators.