IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 313-315

Web Forensics System on the Basis of Evidence Gathering with Code Injection Attack

Deepak Singh Tomar[1], J.L.Rana[2] & S.C. Shrivastava[3]

[1,3]Department of Computer Science & Engineering, MANIT, Bhopal, India
[2]Department of Computer Science & Engineering, RITS, Bhopal, India
Email: [1]deepaktomar@manit.ac.in, [2]jl_rana@yahoo.co.in, [3]scs_manit@yahoo.co.in

ABSTRACT

In Web environment a major challenge facing by the law enforcing agency is to collect accurate & effective evidences from the growing volumes of crime data. In cyber space multi-step attack involve group of action where some of these actions may be legitimate but when combine together constitute malicious activity. Code injection attack is a type of multi step attack which may be carried out by potentially malicious invaders through inserting script code and SQL statement into available feedback form or Suggestion box on vulnerable web site. In this paper architecture for gathering evidence subjected to code injection attack is proposed. The work presented in this paper focuses upon the correlation of various sources of evidences, protection of evidences and preservation of evidences in cyber space.

Keywords: Web Forensics, Multi Step Attack, Code Injection Attack, Evidences Preservation

1. INTRODUCTION

Web forensic is the use of tools and technology to investigate and establish facts to facilitate decisive action in cyber space. The objective of the web forensic is to discovery digital evidences in internet environment. Digital evidence is data in digital storage that can be used to prove the criminal behavior. Forensic analysis is the process of understanding, re-creating, and analyzing arbitrary events that have gathered from digital sources [01]. In Cyber space the forensic analysis can be applied to media: examining physical media for evidence, code: Review of software for malicious signatures and network: scrutinize network traffic and logs to identify and locate activity of cyber criminal [02]. In web environment multi-step attack involve group of action where some of these actions may be legitimate but when combine together constitute malicious activity. Code Injection Attack (CIA) is a type of multi step attack carried out by the suspicious user via entering vulnerable code into the web form or address bar of web browser. More detail about code injection attacks are available in our previous work [3].Without an adequate validation, the injected code by suspicious user may be send to other client/victim through vulnerable web site and unexpectedly executed by the client/victim browser, that causes a security attack depicted in Figure - 01. The detection of a multi-step attack is very troublesome and time consuming process because it is difficult to detect since detection require the correlation of event recorded by multiple heterogeneous source. In Internet environment the goal of forensic to determine if an end user has been involved in a crime or if a user has been victim of a crime.

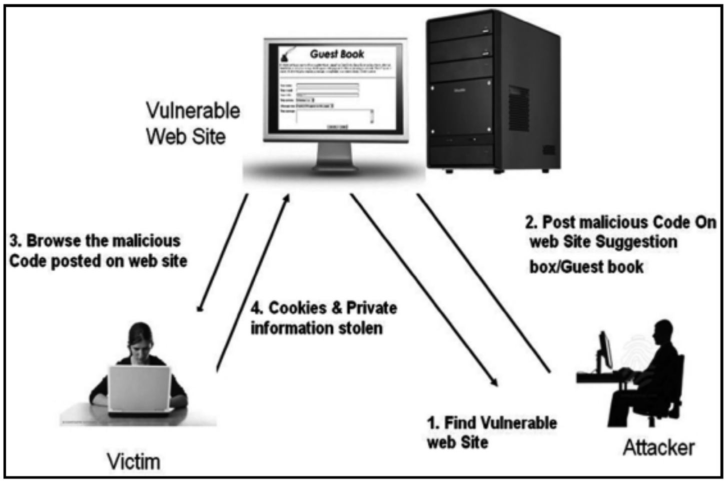
Vulnerable Web Site
Guest Book
3. Browse the malicious Code posted on web site
4. Cookies & Private information stolen
2. Post malicious Code On web Site Suggestion box/Guest book
1. Find Vulnerable web Site
Victim
Attacker

Fig. 1: Code Injection Attack Scenario

2. CHALLENGES IN CODE INJECTION ATTACK INVESTIGATION

Code Injection attack is a result of suspicious behavior of end user through exposing the vulnerability of poor written web application code. In the cyber space the available logging system are more interested to capture the machine behavior rather than end user behavior. Web server log is used to store application layer activity like IP address, Date Time, URL, Byte transfer etc. Firewall log is used store transport layer activity like TCP OR UDP Protocol, IP, Date & Time, Packet drop or allowed. None of these two logs are recorded the sufficient evidence for code injection attack. In our previous work [3] the logging system has been developed to monitor the code injection attack by capturing the code injected by the suspicious user. The major problems in the CIA investigation are correlation, protection and preservation of the digital evidences.

3. ARCHITECTURE FOR WEB FORENSIC SYSTEM SUBJECTED TO CODE INJECTION ATTACK

Code injection attack is a Multi-step attack which generate the data into multiple locations. For effective investigation available log sources of evidence must be linked in order to extract complete chain of evidence [4]. To investigate CIA attack the investigator must consider sources of evidence at vulnerable web site victim side and attacker side. To investigate CIA the investigator must consider the following activity point depicted in the proposed architecture (Figure -02)

A. Client Side Investigation: It is carried out to determine if a user has been involved in a crime or if a user has been victim of a crime. End user activity like email, visited pages, internet searches is audited in the client side logs.

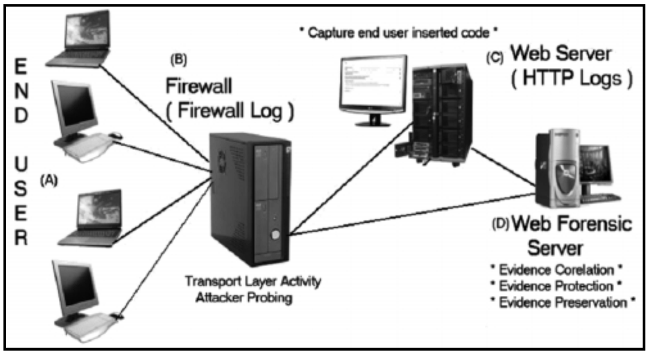

Fig. 2: Proposed Architecture for CIA Investigation

B. Firewall Logs: Firewall keeps track of probing the system by end user. Before attacking the web site suspicious user first check what type of ports are open on web server and what type of services are running, so firewall may be a useful source of evidence which provides the information about inbound and out bound traffic, The firewall also maintains the used protocol and packet which are allowed and dropped. The suspicious use may conduct SYN/ACK flag, FIN flag, XMAS or NULL Scanning using available the scanning tools like nmap, cping or super scan for this purpose. The firewall log mainly contain the transport layer activity which is very important to analyze the CIA attack scenario that how many times suspicious user try to probe the system.

C. *HTTP Logs:* In Cyber space HTTP logs are used to track the end user navigation. When identifying suspect from web server log, information related to the end user activity, host behavior and server behavior should be taken note of, as this item will be help to track down the attacker. Presently the log representation can represent only host based recorded event. Hence there is the need of logging system which record both host based and HTTP communication based recorded event.

D. *Web Forensics Server:* The function of Web forensic Server is to extract evidences from firewall log, Windows log, Web server log and developed HTTP log and maintain the secure centralized log under uniform scheme. For effective evidence collection and preservation following strategy is suggested.

i. *Log Files Analysis:* The purpose of log analysis to indentify evidence of interest stored in the various log files. For effective analysis it is recommended that the two or more logs may integrate using various Relational join operations. The join dependency column for firewall log and HTTP log are IP address and port number. By applying natural join between these two logs the transport layer activity and application layer activity may be correlated.

$$\text{Firewall\_Log} \bowtie \text{HTTP\_Log}$$

Left outer join is applied from firewall log to HTTP log may give the attacker probing details before entering into vulnerable web site.

$$\text{Firewall\_Log} ⟕ \text{HTTP\_Log}$$

Code injection attack is conducted by entering script code, SQL Statement, PHP code and ASP Code into vulnerable web side. Domain dictionary based on script code and SQL is used for pointing the suspicious activity in the correlated evidence.

ii. Log file protection and Preservation: - To conduct efficient investigation confidentiality, integrity and availability of the log analysis result should be protected and preserve while in storage and in transits. To protect archived log files Secure message digest (MD5 or SHA) is enforced. In the related work [5] for evidence preserve the evidence multi thread server is implemented which stores the image files of the web URL pages and makes log files. To store each end user hit may take huge amount of space on web server and also make searching the evidences difficult. To reduce the space overhead on image server only suspicious activity pointed through domain dictionary may be store and preserve.

Currently the we are at the stage of developing Web forensics image server for effective evidence preservation by storing the interested evidence based on domain dictionary, which may reduce the Web server storage space overhead as required in the previous work[5]. The implementation of code injection attack scenario, HTTP logging, Domain dictionary based evidence retrieval is almost completed.

4. CONCLUSION AND FUTURE SCOPE

In this paper discussed architecture will facilitate deeper understanding of captured HTTP behavior of web server. The proposed architecture focuses on integrating the various source of evidence in cyber space by applying natural join and left outer join on firewall logs and developed HTTP logging system which may provide useful aids to cyber crime investigation agency. The strategy to reduce the space overhead on web image server is also present. In Future work includes the development of module based on temporal mining to analyze and correlate the evidence for forensic investigation.

REFERENCES

[1] Caloyannides, Michael A." Computer Forensics and Privacy. Artech House", Inc. 2001.

[2] Digital Forensics Research Workshop. "A Road Map for Digital Forensics Research" 2001. www.dfrws.org.

[3] Deepak Singh Tomar, Dr.J.L.Rana and Dr.S.C.Shrivastava, "Evidence Gathering System for Input Attacks " (Paper ID: 091032) Published in International Journal of Computer and Network Security(IJCNS), 67 Vol. 1, No. 1, October 2009 ISSN Print 2076-2739 & ISSN Online 2076-9199.

[4] Ahmad, A., "The Forensic Chain of Evidence Model: Improving the Process of Evidence Collection in Incident Handling Procedures" *In the Proceedings of the 6th Pacific Asia Conference on Information Systems*, Tokyo, Japan, 2-4 Sept, 2002.

[5] Seunghee Yoo, Yilhyeong Mun, Dongsub Cho " Implementation of the Image Logging Server for Web Forensics" *In the proceeding of First International Conference on the Applications of Digital Information and Web Technologies*, 2008. ICADIWT 2008.