Forensic Investigation for Web Forgery through Java Script Obfuscation

Rahul Raj[*] and D. K. Malhotra[#]
raj_rahul@gmail.com[*] dk_malhotra@gmail.com[#]

Abstract: **Internet is the basic requirement in the present era. As it is an open source, it is more vulnerable to serious defacement. Even it is a secure website; hackers have developed advanced ways to attack on the contents of web pages. With the evolution of web application technologies a revolutionary profile of attack trends are arises. The current profile highlights the main issues affecting the state of website security for any potential attack target. The ability to follow the evolution of malicious parties through the association of individual attacks on a target system is essential for incident response recorded events. Digital forensic science concerns itself with the collection, preservation and documentation of evidentiary data. It is the analysis of all data present on a computer system which aided the commission of a criminal offence. The data capacity to convince with a high level of confidence that there has been a particular action and its suitability for admission classified as forensic evidence.**

Keywords: Script Kiddies, Obfuscation, Web Forensics, Web Application, Client Side Evidences, Server Side Evidences

I. INTRODUCTION

The rapid growth of the Internet, cyber attacks are increasing and can easily cause millions of dollars damage to an organization. Internet is a very easy way to reach any system. If confidential data is not properly protected, then it becomes opens to vulnerable access and misuse. Cyber-crime can cause varying degrees of damage by hackers. So, detailed forensic analysis is required to come to a conclusion about an incident and to prove or disprove someone's guilt.

"A web application is an application that is accessed by end user over a network such as the Internet or an intranet."[1] Web applications include e-mail, e-commerce, wikis, online auctions and more functions. Despite its advantages, web applications do raise a number of security issues.

Web forensics relates to cyber-crime on the Internet. Some criminal activities like child pornography, hacking, and identity theft can be traced and the criminals can be punished if proper evidence is found against them. Web forensic analysis highlights some details such as when and in what sequence someone accesses a Web page. Attacks through web applications can be used to force the end user or client applications to perform searches and all forms of illegal actions for the attacker.

With respect to each of the individual areas touched by the subject matter, this work looks to provide the researchers with sufficient understanding of the methodology chosen for investigation of digital data for attacks in web environment. The areas discussed are web-forensics, tab-nabbing attack, web environment and their components. The complexity of forensic web applications increases with the number and variety of underlying components in a web application only depends. These components include network structure; operating system files structure as well as additional service dependencies.

Web forensic involves investigation of the digital evidences on the web by preventing, detecting and responding to the attacks on websites. The prevention is done by authenticating the users who access the web. This can be done in two ways – basic access and digest access. In the basic access authentication, that the user requires a user name and password to make a request. This method is implemented on HTTPS protocol. This does not provide any confidentiality. This is the simplest method to provide access control as it does not require any cookies rather it uses static HTTP headers. HTTP headers are components of the message header of requests and responses in the Hypertext Transfer Protocol (HTTP). Define the operating parameters of an HTTP transaction.

In digest access authentication, a hash function is applied on password before sending it through the internet. This method is implemented using HTTP protocol. This is more secure as it encrypts the data which keeps confidentiality and prevents any replay attacks. But this is not enough, a secure connection is also required to maintain security.

II. JAVA SCRIPT OBFUSCATION:

Conceivably nearly all technical inventiveness in the phishing community today exists in the art of misleading end users through e-mailing the URLs. Several strategies have been scrutinized over 2004 and 2005 [4], however forensic analyst and researchers explore a new attack called obfuscation technique as emergence of new approach. Attacker uses different scenarios to mischief end users by playing Java Script functionalities like obfuscation; such attacks are as follows-

- Tab-nabbing Attacks
- Click-jacking Attacks
- Misdirection and Redirection
- Sending HTTP links into clickable Graphical mails

III. WEB FORENSICS:

The victims of Web attacks are clients and Web servers. Both clients and server side protection is necessary. The attacks can be performed by using false URLs or redirects for malicious sites. The medium of attack on the Internet are Web Browser, database servers and application servers. On the client side, forensic analysis is done to find out if a user has been involved or has been a victim of the crime. Digital Evidences can be found at both client and server side-

A. Client Side Evidences-

Evidence for investigation of web attacks at client side may be extracted from Browser, OS web page and memory. Browser evidences such as history files, Temporary files, cookies, index.dat, and favourites. OS evidences such as Registry entries, recorded process log, etc. More evidences such as .html pages in unallocated space, Cache Memory, E-mails sent and received by the user etc.

B. Server Side Evidences-

Evidence for investigation of web attacks at server side may be extracted from log files and Network traffic. Log file includes web server log files such as Access log, Error logs, FTP log. Other log files such as Antivirus server logs, Web filter logs, Spam filter logs and Firewall logs.

There are five basic steps to computer forensics [Ashcroft 2001]:

1. *Preparation*

The investigator should be aware of the problem fully. He/she should have a proper (could be abstract) plan for investigation. Acquire permissions to access the information that investigation process may need.

2. *Backup of System*

Create a bit-by-bit copy of whole system as possible for preserving from actual data.

3. *Collection of Digital Data*

Collect the data required for the investigation. Proper precautions need to be taken while collecting the information. Safety devices like write blockers should be used. All the data should be collected according to a plan of investigation.

4. *Examination*

A careful examination of data should be done. Sophisticated tools should be used to make sure the tests give accurate results.

5. *Analysis*

Analysis of results to reach a conclusion should be transparent. Analyzing could not lead to the actual facts. If possible an interview should be conducted to backup the results.

6. *Reporting*

Reports should be reported to the concerned authority with utmost secrecy and integrity. The reports should be archived and saved for future references.

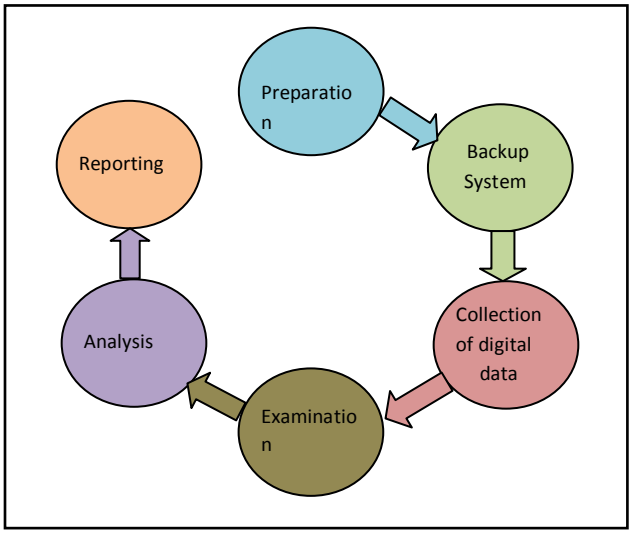


Figure 1: Digital Forensic Investigation

IV. LITERATURE SURVEY

There is no single consistent framework to forensically investigate web services, existed yet. However, the purpose of work mentioned in paper is to spread some most frequent features with Forensic Web Services (FWS)'.

Michael et al [10] proposed a tool to reconstruct the browsing activity like a slideshow unlike some of the tools which parse the cache into URLs. Web Cache Illuminator and IE History & Cache Viewer are the tools which can parse the cache to URLs. This tool can effectively show the intension of the user because the investigator can visually inspect the activity and help in deeper understanding of the activity and specific intensions of the user. Although the downsides of adopted technique are that the client side scripting interaction is totally lost. Whenever the URL is accessed, the older version of Web page is lost and is overwritten. There are some compatibility problems with the CSS and AJAX technology files. [10]

Murillo et. Al enlightens process to delete history from IE Browser and approaches to retrieve the deleted history files. In addition, author presented a detailed forensic analysis of Firefox browser through different forensic utility tools. Finally, proposed a recovery algorithm to retrieve deleted SQLite entries on the basis of well-known internal record structures.

Windows registry is a central hierarchical database. It is used to store essential information of system

configuration for one or more end users, applications and hardware devices [Microsoft 2010].

Robinson [6] induced a model that is employed by FWS to generate pair-wise evidence with few distinctions. Also present a framework to endorse adequate B2B communications based on a trusted delivery agent notion. It implements Coeffey-Saidha [7] protocol to provide non-repudiation in their protocols. Robinson [6] proposes delivering of evidences rather than preservation.

Herzberg [8] brings in an idea of Evidence Layer for e-commerce transactions. It support from the bottom of the e-commerce stack and on top of a transport layer. This layer contains two separate protocols one for generating and another for delivering the evidence to concern party. FWS modify layering approach presented by Herzberg [8] for the web service stack. Similar to different techniques, Herzberg et al [8] is not perfectly appropriate for forensics investigation.

V. Issues in Windows Digital Evidences

Presently, with the increasing prevalence of crimes associated with digital devices, applying scientific processes to obtain evidentiary data has become a necessity. Organization of service log events of targeted system is the most critical issue for forensic analyst. Another issue of existing log analysis approaches is that they do not apply compulsory principles such as qualify as forensic analysis solutions. Ensuring the validity of events and provide an agile method is necessary to efficiently carry out forensic analysis of web application.

Variety of dependencies on which web application relies as well as any correspondence between them, comprise the security landscape of a target system. These dependencies include the operating system foundation, back-end services such as databases and the web service itself, and potentially many other interoperable web applications. This record establishes that log analysis is an eminent and necessary module for the analysis of an organization's security stage from both administrative as well as forensic standpoints.

Each network device such as a workstation, server, router, switch, Virtual Private Network (VPN), Virtual Machine (VM), firewall, Intrusion Detection System (IDS), or Host Integrity Monitoring System (HIMS) generates Digital Evidences that contain records of system, device, and user activities that have taken place within the infrastructure.

A. Issue1: Prefetch

Windows keeps track of the way the system starts and which programs the user commonly opens. This information is saved as a number of small files in the Prefetch folder. Subsequent cache files are most alike to prefetch files. These files are not possible to investigate simply, but they may contain digital evidences.

- C:\Users\runa\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
- C:\Users\runa\AppData\Local\Microsoft\Windows\Caches{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
- C:\Windows\AppCompat\Programs\RecentFileCache.bcf

B. Issue 2: Registry

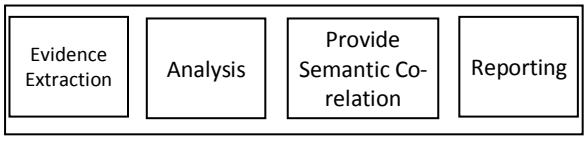
The Windows Registry is a database that stores various configuration settings and options for the operating system. HKEY_CURRENT_USER, abbreviated HKCU, stores settings that are specific to the currently logged-in user. Each user's settings are stored in files called NTUSER.DAT and UsrClass.dat. We would have seen different results had we used Windows XP, due to a change in registry handling between Windows XP/Vista and Windows 7.

VI. Proposed Methodology

Forensic analysis of web services/applications has few critical issues such as a need for neutrality and comprehensiveness. The primary purpose of digital forensics is to present digital evidence in legal proceedings. Therefore, the techniques used to extract digital evidence from devices must comply with legal standards. Reliability is also an essential issue to forensically analyze the web services. This work provides two essential services-

1. *Pair-wise evidence generation:* Pair-wise evidence generation is the transactional evidence gathering process that occurred among the pair of services at the time of invocation.

2. *Comprehensive evidence generation:* It generates evidences on demand. Web forensic investigators create pairs of transactional evidence gathered at service invocation time. Uncover global views of complicated transactional scenarios that occurred at specified period of time. Finally provides them to investigator for forensic examination.



VII. Conclusion

Accordingly, single vulnerability of a web service/application may be exploited to influence more than one service on the same web server. In Web Environment it is a challenge to investigate the semantic relation and source of an attack. Hence, this paper proposes a framework that provides this capability as a

service to other web services by logging service invocations. It depicts that log extraction and correlation may offer the potential to yield the collection of digital evidences to expose the attack from its logs.

REFERENCES

1. Dr. Robert J. Boncella, "A Tutorial on Web Security for E-Commerce", proc. AMCIS, Paper-179, 2000.
2. Ahmed, Muhammad Kamran.; Hussain, Mukhtar.; Raza, Asad; "An Automated User Transparent Approach to log Web URLs for Forensic Analysis," Fifth International Conference on IT Security Incident Management and IT Forensics, 2009. IMF 2009, pp.120-127.
3. Ashcroft, John; "Electronic Crime Scene Investigation Guide: A Guide for First Responders," National Institute of Justice, 2001. Available from: http://www.ncjrs.gov/pdffiles1/nij/187736.pdf.
4. Eric A. Benson, "User of Browser Cookies to store Structured Data", United States Patent Application Publication, Publication number: US 2008/0228794 A1, Seattle, WA, USA (May 2008).
5. H. Berghel, "The Disipline of Internet Forensics", In UMUC, ACM Maryland Digital Library Database, July-2010.
6. P. Robinson, N. Cook, and S. Shrivastava, "Implementing fair non-repudiable interactions with Web services," in EDOC Enterprise Computing Conference, 2005 Ninth IEEE International, 2005, pp. 195-206.
7. T. Coffey and P. Saidha, "Non-repudiation with mandatory proof of receipt," ACMCCR: Computer Communication Review 26.
8. A. Herzberg and I. Yoffe, "The Delivery and Evidences Layer" Cryptology ePrint Archive Report 2007/139, 2007.
9. B. Rosers and wiki "List of Web Browsers" [Online]. 2010 Available: http://en.wikipedia.org/wiki/List_of_Web_Browsers, [Visited: 24-Sept-2014]
10. M. Campidoglio, F. Frattolillo and F. Landolfi, "The Copyright Protection Problem: Challenges and Suggestions," in Fourth Int. Conf. on Internet and Web Applications and Services, 2009 (ICIW-2009), pp.522-526, pp. 24-28.
11. J. Keith and B. Rohyt, "Web Browser Foensics, Part 2" [Online]. 2010 Available: http://www.symantec.com/connect/articles/Web-Browser-forensics-part-2.

