Web Browser Artefacts using Cryptographic Examination

Yamunah Kathiravan, Mohd Fahmi Mohamad Amran, Noor Afiza Mat Razali, Afiqah Mohammad Azahari, Suhaila Ismail

Abstract*: Private browsers, in general, offer security and privacy by allowing users to browse the web without leaving usual traces on their computers. However, private browsing has been proven not to deliver the security as they ensure they would. Previous researchers concluded that web browsers often failed to provide the intended privacy protection to their users. Even with third-party PC cleaning tools, web browser data can still be accessed using computer forensic tools. This paper aims to perform research and development of a framework with the help of cryptography that will support high accessibility of evidence until the evidence should be erased, at a point where it will be impossible to recover. Cryptography consolidates innumerable algorithms which are used in building a secured application. This application mainly focusses on the implementation of a system capable of encrypting of browser artefacts using encryption techniques. Advanced Encryption Standard (AES) is one of the best-known and most robust symmetric encryption algorithms. The AES rule is capable of using 128, 192, and 256 bits of cryptographic keys. The proposed system makes use of the advantages of both the methods by presenting a hybrid technique of encoding and encryption, resulting in a much secured and faster alternative of storing web browser artefacts. Regardless of whether the attacker gets access to any of the keys, the attacker won't be in position to unmask the data in an expected certain amount of time. This system will hopefully contribute to a better web browser over the existing techniques by doing some minor changes in the implementation framework.

***Index Terms*: Browser Artefacts, Computer Forensic, Encryption, Private Browsing.**

I. INTRODUCTION

Modern web browsers such as Internet Explorer, Firefox, Chrome and Safari have indicated more concern with their users' privacy while surfing the Internet [1]. Due to this problem, web browser companies introduced a new feature on the web browser called Private Browsing mode to maintain the privacy of user's web activity. Private Browsing mode is used by users who wish to keep their browsing activities a secret from other users of the same machine and network [2]. This mode allows user to browse without worrying about their activity being exposed to the outside work. Whereas in Private Browsing mode, some information such as cookies, and temporary files are temporarily stored. All new cookies and history are deleted once browsing session is ended.

Over the years, a few papers have been published which utilises computer forensic analysis to discover evidence on the local machine despite using various Counter Digital Forensics (CDF) [3]. Researchers have implied to conduct more experiments in this area as browsing activities could be a potential evidence in a digital forensic investigation. This is the first attempt to address such CDF mechanism by overwriting the artefacts left by web browsers.

Like every other web browser cryptography project out there, the main focus has been securing the browser's network traffic. Encryption protects the data that is stored on and between physical assets; computers, databases, servers and etc. The real problems as to why there still has not been a cryptography-based web browser is because current browsers are lacking the basic cryptographic primitives. The most well-known problem is the lack of cryptographic secured random number generator and efficient implementation of key stretching algorithms. This paper describes a research and development of web browser encryption by replacing the file on the receiver's directory as an encrypted file.

II. PRIVATE BROWSING

Private Browsing was first introduced back in 2005 with the intention to protect the privacy of a user. However, most of computer forensic software have successfully recovered a browser's artefacts even if the user used private mode the entire session. There are many researches involved in cryptographic browser but have focused only on encrypting the network traffic. Unfortunately, implementations of private browsing mode still allow sensitive information to leak into persistent storage. One of the many problems with existing private browsing is that it does not entirely hide its entries from writing in the hard disk [4]. The current browser vendors have only focused on keeping their web protocol encrypted but seem to have forgotten about the web browsing data created on the local computer. Therefore, all records will remain on the hard disk until it is overwritten by different data. This does not only show private browsing are not entirely private but makes it simple for forensic investigators to extract private web activities from a suspects' computer.

Revised Manuscript Received on November 22, 2019

Yamunah Kathiravan, Department of Computer Science, National University of Defense Malaysia, Kuala Lumpur, Malaysia.
Mohd Fahmi Mohamad Amran, Department of Computer Science, National University of Defense Malaysia, Kuala Lumpur, Malaysia.
Noor Afiza Mat Razali, Department of Computer Science, National University of Defense Malaysia, Kuala Lumpur, Malaysia.
Afiqah Mohammad Azahari, Department of Computer Science, National University of Defense Malaysia, Kuala Lumpur, Malaysia.
Suhaila binti Ismail, Department of Computer Science, National University of Defense Malaysia, Kuala Lumpur, Malaysia.

With acquisition tools like EnCase and FTK, the browser artefacts files are highly retrievable. Moreover, current browsers are lacking essential cryptographic primitives. Data cannot be read and write on the same time. This could cause a corruption to the data as well as the browser. The objectives of private browsing mode according to [4] are for users to browse the Internet anonymously and not leave any bits of data on their machine. At the moment, private browsing functionality of mainstream browsers have successfully achieved one of the objectives which is to browse without being detected.

However, through thorough examination, every browser has the intention to record its browser artefact in the operating system [4]. There are a few procedures which can help a client to abstain from leaving follows (Digital Evidence) of Internet action so one can disappoint criminological examination, one of which being cryptography. Cryptography fill this void to enable individuals to keep their browsing data highly available and protected from unauthorized access at the same time.

III. CRYPTOGRAPHY AS A SECURITY TOOL

Cryptography is technology that can play important roles in tending to certain types of data vulnerability. In the traditional application of cryptography for confidentiality, a sender creates a message intended for a recipient, protects it by a cryptographic process [5]. Cryptography empowers the recipient to verify the message received with a specific key; the key is the source of the message. Essentially, the sender can encode the message, and only to be decoded with a specific key. Basically, cryptography is an art of hiding information by encrypting message [6].

According to [7] and [8], encryption is a technique used to transmit secure information. Over the years several encryption techniques have been implemented. An encryption algorithm enables the sender to ensure that only the targeted computer is having a specific key can read the message.

Although asymmetric key algorithm uses great computational assets in contrast with symmetric counterparts and therefore are commonly not used to encrypt bulk data streams [9]. Therefore, this paper has chosen to use symmetrical method.

IV. RESEARCH METHODOLOGY

In this research, the Evolutionary Prototype will be used because this prototype repairs the inadequacies that emerge during the development of the system. It is also known to be more economical and easier for software development. Fig. 1 shows the Flowchart of Evolutionary Prototype Model.

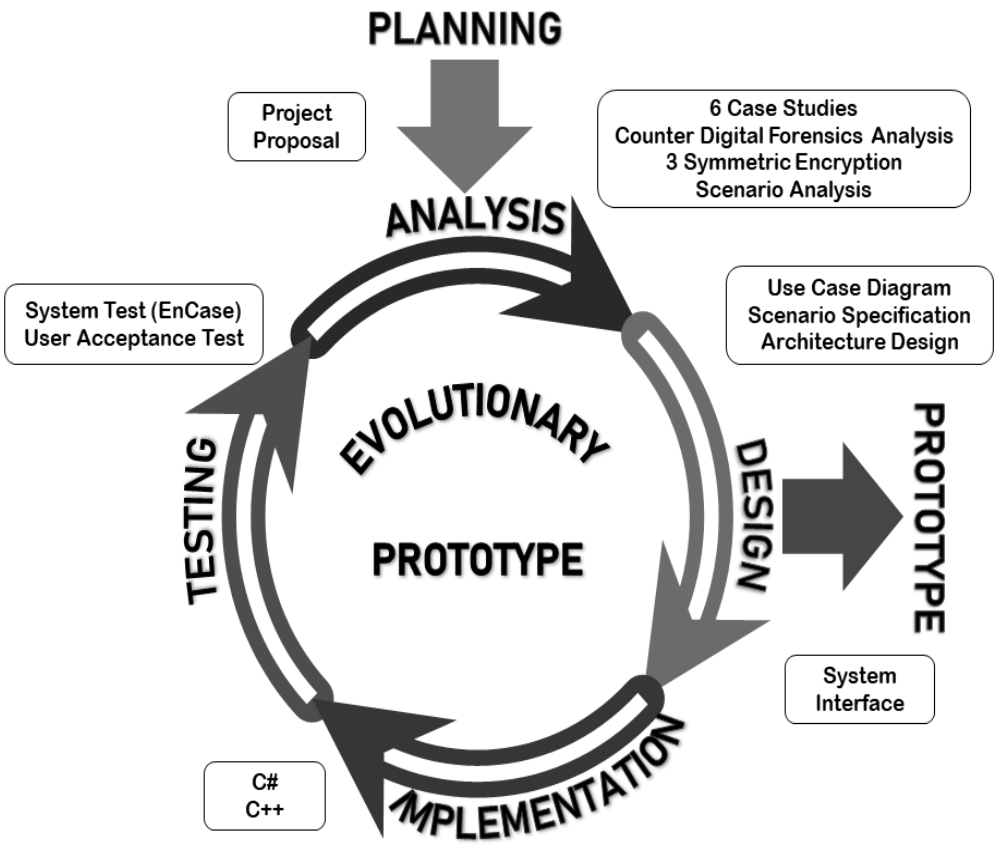

Fig. 1: Flowchart of Evolutionary Prototype Model [10]

Level 1: Planning Phase

In the planning and analysis phase of the requirement, the purpose of web browser encryption is determined to develop an enhanced security and improved speed browser.

The purpose of the system design is to identify the problems faced by the current system and subsequently submit proposals for the resolution of the problems encountered. Additionally, it also aims to improve the shortcomings in existing browsers. The utilization of hardware also requires initial planning so that all type of hardware is sufficient when the browser is to be developed.

Level 2: Analysis Phase

After gathering the data and information, the data were analysed for their legitimacy and possibility of consolidating the requirements in the system development was studied. The analysis of the current systems has also been done in this stage. It is vital to study the limitations of the current systems because limitations provide very good analysis how certain current system would behave in worst conditions thus can be improved and implemented for the proposed method. When all the data have been analysed, a proposed framework will be produced. This proposed framework is often a layered structure indicating what kind of systems need or should be built and how the system would interrelate.

Level 3: Design Phase

The results based on the analysis phase will be used as a contribution to determine the system design. This involves the architecture of web browser encryption, input design, output design, layout, and system procedures. The purpose of the design phase is to change the specification of the study to a statement. The most important step is to define and analyse the AES encryption. The following table gives the description about the different AES key sizes.

Bit pattern	Key Lengths	Block Size	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table 1: Key-Block-Round Combinations

Level 4: Implementation Phase

In the implementation phase, the web browser, encryption algorithms will be executed. Once the prototype of this system is completed, encryption implementation will also be ready to be developed. This requires making a comparison of AES key lengths to get a clearer idea. The final testing phase will be implemented so that users are satisfied with the outcome and the objective of the research is achieved. If the system does not work as planned or interrupted during testing then this prototype will be tested and re-investigated to assess the problems encountered and subsequently improvements will be implemented.

Level 5: Testing Phase

Testing will be an on-going process until verified that the new web browser leaves no traces of the user's browsing activity. Once the web browser is launched, a few steps will be performed, such as: searching for articles, images, and videos, keywords, logging into social media accounts, and uploading/sending attachments. The experiment is performed on a few websites such as Facebook, YouTube, Gmail, Google, Dropbox, and Wikipedia, to imitate a realistic situation as much as possible. After conducting the testing scenario on the web browser, the operating system will be shut down for acquisition. Each snapshot of the virtual machine will later be analysed using EnCase 8.08 to ensure that the web browser leaves no browsing artefacts. The research testing process is simplified in Fig. 2.

V. TESTING SCENARIO

The testing plan will be held on two virtual machines to test how the new browser encryption is secure compared to existing private browsing. The latest operating system will be used, and the latest web browsers will be installed to test their reliability in leaving traces of browsing activity.

Each scenario will be to test if the web browsers leak any information regarding the user's browsing activity. The testing will be conducted through different browsers on the same platform; Windows 10, with two modes, enabled separately, private browsing, and the new browser encryption to compare and verify till the new browser is proved to be more reliable and secured than private browsing mode. The same steps will be repeated for each browsing session and browsing mode, such as: searching for news articles, specific keywords, downloading images, and sign in to social media account. A group of targeted websites was chosen to imitate a real user's behaviour. The testing will be conducted using unique keywords to ensure the validity of the test.

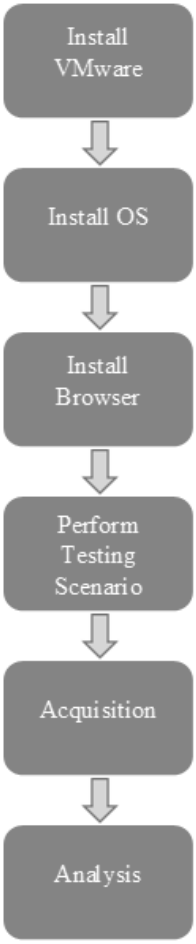

Fig. 2: Research Testing Process

VI. DATA COLLECTION

Data collection is a vital procedure in the proposed research. The data collection from test scenarios must be collected properly and be exact so as to produce meticulous research. There will two virtual machines that will be utilized for data collection. The data collection will be conducted using recognised forensic frameworks. Tableau Forensic Imager TD3 are used to prevent the forensic workstation from any data tampering on the acquired digital evidence.

The forensic workstation is Windows 10 operating system with the latest version of EnCase installed. The hard disks are entirely acquired using EnCase version 8.08 to analyse the data for investigation. The original evidence is safe and the integrity and authenticity of the evidence could be proved through hash values using EnCase.

VII. CONCLUSION

This paper focused on developing a newer technique of browser data being written on the local machine to fulfil user privacy which many major browsers failed to so. This paper also describes the research and development of a framework that will support high accessibility of evidence, until the evidence should be erased, at a point where it will be impossible to be recovered. The model used to develop the system is a prototype model. In our future research, we will focus more detailed on the findings and analysis process. First, the testing shall focus on Non-Volatile memory with EnCase. Second, extract browser artefacts on different operating system instead of one specified platform. This information is important forensics artefacts for a forensic investigator.

ACKNOWLEDGMENT

The authors honourably appreciate National Defence University of Malaysia for the research university grant UPNM/2019/GPJP/TK/17.

REFERENCES

1. Frackman, A., Martin, R. C., & Ray, C. (2002). Internet and Online Privacy: A Legal and Business Guide: ALM Publishing
2. Lerner, B. S., Elberty, L., Poole, N., & Krishnamurthi, S. (2013). Verifying web browser extensions' compliance with private-browsing mode. Paper presented at the Computer Security--ESORICS 2013: 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013, Proceedings.
3. Kwak, J., Kim, H. C., Park, I. H., & Song, Y. H. (2016). Anti-Forensic Deletion Scheme for Flash Storage Systems.
4. Aggarwal, G., & Bursztein, E. (2010). An Analysis of Private Browsing Modes in Modern Browsers. USENIX Security, 1–8.
5. Kishor, K., & Garg, V. (1996). Cryptography's Role in Securing the Information Society. Trans-Stellar, 1(1), 28–41.
6. Thomas, B. A., Swathi, S. V, & Lahiri, P. M. (2016). Encryption Algorithms: A Survey, 4(2).
7. Stallings, W. (2005). Cryptography and Network Security: Principles and Practices. Cryptography and Network Security, 592.
8. Forouzan, B. A., Mukhopadhyay, D. (2008). Cryptography and Network Security, [Second Edition], McGraw Hill Education Private Ltd.
9. Indu, I., Anand, P. M. R., & Shaji, S. P. (2017). Secure File Sharing Mechanism and Key Management for Mobile Cloud Computing Environment. Indian Journal of Science and Technology, 9(48).
10. Dennis, Wixom & Roth (2012). System Analysis and Design (5th ed). John Wisley & Sons, Inc