International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228118

Secure Transfer of Digital Evidence from the Crime Scene

Santhosh B.*[1], K. Annapoorneshwari Shetty[2]

*[1]Associate Professor, Department of MCA, AIMIT, St Aloysius College (Autonomous), Mangalore, Karnataka, India

[2]Assistant Professor, Department of MCA, AIMIT, St. Aloysius College (Autonomous), Karnataka, India

Article Info
Volume 8, Issue 1
Page Number : 123-127
Publication Issue :
January-February-2022
Article History
Accepted : 15 Jan 2022
Published : 28 Jan 2022

ABSTRACT

The essential task in tracing the source of the theft is to secure the digital proof from the location where the data was misused. But, more significantly, the data evidence must be sent to the main server without being intercepted by a Man-in-the-Middle assault. Diffie-Hellman Key Exchange Algorithm is used to securely exchange cryptographic keys from the admin and investigator. Here different layers of security have been identified. The proposed method uses message digest, encryption and steganography to implement secure transfer of digital evidence from the crime scene.

Keywords - Diffie-Hellman Key Exchange, message digest, Advanced Encryption Standard (AES), digital evidence

I. INTRODUCTION

Digital forensic science is a branch of forensic science that focuses on recovering and investigating data from digital devices used in crimes. This is done so that, if necessary, evidence can be presented in a court of law. Digital forensics is becoming an increasingly important part of law enforcement agencies and enterprises as society's reliance on computer systems and cloud computing grows. Digital forensics is concerned with the identification, preservation, examination, and analysis of digital evidence, both inside and outside of a court of law, using scientifically established and proven techniques. [1]

The Lollipop Model and the Onion Model are the two security defensive models. The Onion Model, a defence concept based on an onion analogy, is used in this study. An onion is a vegetable with several layers. We can only reach the center of the onion by removing each layer. To get access to the asset, the hacker must first breach all levels of security. In this case, breaching each layer should be difficult and time-consuming for the hacker to enter. As a result, the onion model has gained acceptance as a solid network security paradigm. As a result, this study focuses on the onion model of defence. [2]

There are several digital forensics process models that specify how forensic examiners should gather, handle, and analyses data. Digital media is confiscated prior to the actual inspection. To maintain the chain of custody in criminal instances, this will be done by law enforcement officers. Following the seizure of evidence, a forensic replica of the data is made. To prevent manipulation, the original drive is returned

to a secure storage location after being duplicated using a hard drive duplicator or software imaging tool. [1]

For the system image, a message digest is computed using a hash function. A message digest is a fixed size numeric representation of the contents of a message. Message digests should be used to ensure data or media integrity by identifying any modifications or alterations to any component of the message. The system image is compressed. Before transferring the System-image is encrypted with AES. Taparia et. al., [3] mentioned the work of W. Diffie and M. Hellman, "New directions in cryptography," [4] to explain that the creation of a shared secret key is the most critical step in establishing safe connection between two devices. However, communication is challenging because to the lack of a trustworthy third party in peer devices. We will look at how to safely transfer data between two devices in this paper. One such ideal protocol is the simple Diffie-Hellman key exchange protocol (DHKEP). Which is used to securely send the system image over the network. The Message Digest is integrated into the image and hidden. LSB (Least Significant Bit) Steganography is used to conceal the message digest, in this type of steganography, the information hider embeds the secret information in the least significant bits of a media file. [5]

II. DIGITAL FORENSICS STEPS

Digital forensics investigation requires systematic and widely accepted steps in the law of court. starting from identification of the crime to report generation there is a need of unambiguous, well-defined steps. These steps include

i) Identification: the main two phases are identification of crime and digital evidence.

ii) Collection: In this phase, an investigator collects digital evidence from the crime scene for analysis and examination. It includes collecting the evidence, secure transfer and store of evidence in investigation agency server. Sometimes it is hard to collect the evidence in that case system/device is shifted to the investigation agency office.

iii) Extraction: This phase deals with extraction of information from various devices

iv) Analysis: In this phase investigator performs various types of analysis. Report thus generated could be used to n prove or disprove criminal charges.

v) Examination: In this phase investigator the investigator extracts and inspects characteristics of the data.

vi) Report: Finally, report has been created to present their findings from their forensic analysis.

III. PROBLEM DEFINITION

In the crime scene digital evidence is present within the server or the hard disk. Because of the advent of technology to make the server fault tolerance, high availability and security made server configuration very complex. It is not easy to create copy. Since the business continuity also very important first they try to create the copy of it in a secure hard disk or seize the server and take it to the investigation office. During the transit it is very important to make sure that content has not been altered. In the literature we found there are many mechanisms proposed in other problem domain which requires some modifications with respect to digital forensics evidence transit. To fill this research, gap this paper deals with how to transfer data securely to the investigation agency server.

IV. CHALLENGES IN TRANSFERING DIGITAL EVIDENCE FROM THE CRIME SCENCE

One of the main challenges while taking the snapshot, the size of the server or hard disk and to make the data high availability and reliability may require multiple instances. Seize of server and other computing resources could be the best choice but it

may affect the business continuity. During the transit there may be some damage to the physical machines which may result data retrieval more difficult. In datacenter isolation of one physical machine to another may require some networks specialist personnel. Time requires to take the snapshot of the system is another concern.

V. THE PROPOSED METHOD

From the crime scene, digital evidence is transferred to the investigation ever/office in the form of snapshot or physical machine. To implement the integrity of the data the following procedure has been proposed. The proposed method uses message digest, encryption, secure key exchange and steganography. The proposed methods are;

A. At Crime Scene:

i). Take the snapshot of the server.
ii). Calculate message digest of the snapshot. To send message digest securely and to manage integrity of the data.
iii) Generate the key using diffie hellman key exchange by connecting with admin of investigation office.
iv) Encrypt the message digest using Symmetric key cryptography.
v) Embed the message in a cover image and send to the investigation office.

B. At Investigation Office

i) Decode the message from the image
ii) Decrypt the message using the key generated during the diffie hellman key exchange
iii) Decompress the message
iv) For the received snapshot calculate message digest independently
v) If the calculated message digest is same as that of the received message digest, then the integrity of the message has not been altered.

VI. IMPLIMENTATION & EXPERIMENTAL RESULTS

A. Experimental Setup:

The encryption algorithm used in the proposed system is Advanced Encryption Standard [AES] [8]. It is a symmetric cipher model which uses the same key for encryption and decryption. To generate the key Diffie hellman key exchange algorithm is used. To encode the image, steganography algorithm used is LSB [9]. MD5 message digest algorithm is used to find the message digest. The forensic dataset used is chatlogs [10]. It's a user generated dataset created by University of new Haven ,USA. We assume chatlogs datasets collected from the crime scene. The experiment can be further generalized for different types of data sets.

B. Experimental Results:

Chatlogs dataset consists of Jesse's Chat Logs – 2010, 2011 and 2012. Each year file consists of 12 directories of each month. Each directory consists of chatlogs created for each communication. Sample of each communication is as shown in fig [1].

Figure 1. chat log sample

For each file message digest has been calculated independently. Encrypted using the key generated using Diffie hellman key exchange with the admin. Then it is encoded inside the cover image and sent to admin via email or other communication method.

Hex encoded message digest of the file aerosmith_tyler@msn.com is e08b116d049904904da43b794b38f907. Similarly, every file is been calculated and stored in

mesgdigest.txt file. Then connected to the admin and generated key using Diffie hellman key exchange algorithm. This is the secure method of generating and exchanging the key without actually exchanging the key over the insecure communication channel. The 16 bit Key generated is 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75 (key in Hex). Then using the key AES algorithm is applied to each dataset. The encrypted value of the above data set is zaM5dUo6eu0itGl33B+oLi+wLHXw7wR/ME0Q5FglNBbZXaZw6znI5c+8QYC9aItI then the encrypted value is embedded inside the image in the format total no of datasets, encrypted datasets. To encode the message the algorithm used is LSB. The fig [2] and fig [3] shows the cover image before encoding and after encoding.

Fig[2]:before encoding

Fig[3] : after encoding:

At the investigation office the decoding is exactly reverse of the steps executed at the crime scene. Here first encrypted message digest is collected from the image. Then decrypted using AES algorithm which generates message digest of each file. Then again message digest is been calculated independently for each files received and compared with received message digest. We found that there is an exact match. if there is any mismatch, we can conclude that received may not be the actual file collected during the forensics investigation.

VII. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

In this research paper, we propose a novel methodology to transfer the data securely and to check the integrity of the data. The onion model is used to implement the integrity and security. Three levels of security have been implemented – message digest, Encryption and Steganography. The data can be accessed only after breaking all the three layers. AES is the standard encryption algorithm and it is difficult to break. But practically no system provides 100 % secure.to achieve still higher security by using advanced encryption techniques, adding some more layers of security. The experiment further applied for snapshot of the server.

VIII. ACKNOWLEDGEMENTS

The authors would like to acknowledge the funding support from "MJES Minor Research Projects grant", St Aloysius college, Mangalore. Thanks also go to the dedicated research group in the area of information security, cloud computing & digital forensics at the Dept of MCA, AIMIT, St Aloysius College (Autonomous), India, for many stimulating discussions. Lastly but not least the author would like to thank everyone, including the anonymous reviewers.

IX. REFERENCES

[1]. M. A. Caloyannides, N. Memon and W. Venema, "Digital Forensics," in IEEE Security & Privacy, vol. 7, no. 2, pp. 16-17, March-April 2009, doi: 10.1109/MSP.2009.34

[2]. Basant Kumar, 2019, Effective Approach Toward Intrusion Detection and Pretention Systems in Implementing Defense in Depth, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) CICTAB – 2019 (Volume 7 – Issue 04),

[3]. A. Taparia, S. . K. Panigrahy and S. K. Jena, "Secure Key Exchange Using Enhanced Diffie-Hellman Protocol Based on String Comparison," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), no. 2017, 2017.

[4]. W. D. a. M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. vol. 22, no. 6, pp. pp. 644-654, 18 July Nov. 1976

[5]. B. Dickson, "Portswigger," 06 February 2020. [Online]. Available: https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealing-messages.

[6]. H. Q. Beyers, "Database forensics: Investigating compromised database management systems", 2014.

[7]. Iacob, N.-M. (2011). Fragmentation and data allocation in the distributed environments. Annals of the University of Craiova, Mathematics and Computer Science Series. 38. 76-83.

[8]. Dworkin, M. , Barker, E. , Nechvatal, J. , Foti, J. , Bassham, L. , Roback, E. and Dray, J. (2001), Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.197.

[9]. K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751.

[10]. Cinthya Grajeda, Frank Breitinger, and Ibrahim Baggili. “Availability of Datasets for digital forensics – and what is missing”. In: Digital Investigation (2017). (Presented at DFRWS 2017, Austin

Cite this article as :

Santhosh B, K. Annapoorneshwari Shetty, "Secure Transfer of Digital Evidence from the Crime Scene", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 1, pp. 123-127, January-February 2022. Available at

doi : https://doi.org/10.32628/CSEIT228118

Journal URL : https://ijsrcseit.com/CSEIT228118