International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Data Lineage in Cross-Site Scripting (XSS) Attack

Sunitha V.S ,Jissmol Jose

[1]*Student,Dept.ofCcomputer Science, St.Joseph's College, Irinjalakkuda , Kerala, India*
[1]*Professor,Dept.of Computer Science, St.Joseph's College, Irinjalakkuda ,Kerala, India*

Abstract - *In this digital era ,leakage of sensitive data is one of the most severe issue that the organization face. It is not only for organizations , the consequences are also faced by personal lives. Personal information is accessed through social networking sites or smart phones and it is indirectly transferred to unauthenticated persons for their personal gains. But we cannot identify the leaker in a provable manner. Now we introduce a frame work LIME, it has two characteristics :owner and consumer. And an important third party auditor to identify the leaker. The frame work provide some features to secure the data transfer such as novel accountable data transfer protocol, robust watermarking, and signature primitives. Cross -site scripting(XSS) attack and its prevention through three way handshaking protocol.*

***Key Words*: : LIME, Robust Watermarking ,Signature Primitives ,Novel Accountable Data Transfer Protocol XSS attack, Three way hand shaking**

1.INTRODUCTION

Sensitive data leakage is the present issue faced by the organization in this digital era. It is happened by malicious external entities or employees for their personal gains. But we cannot caught the leaker in a provable manner and identification of the leaker is not an accurate always. The data leakage not only faced by organizations but also personal lives. The personal information revealed to a third party is a serious issue. So we use a novel frame work LIME for secure data transfer. There will two characteristics for data transfer :owner and consumer. Here we use signature primitives such as symmetric key for data encryption and decryption. Cox algorithm for robust watermarking and HTTPA (Accountable Hyper Text Transfer Protocol), requires the data producer and the data consumer to come to an agreement before the data transfer. These features provides the transfer of data secure and identify the leaker in provable manner if it occur. In our system identify the leaker when XSS(Cross Site Scripting) attack occur and prevent from the lineage of data. To prevent data lineage in XSS attack use Three way hand shaking protocol.

2.EXISTING SYSTEM

In the existing system leakage of information through malicious external entities or malicious authorized user is a serious problem for person as well as organizations. The organization did not reveal if their confidential data is leaked because the fear of loss of customer confidence. The confidential digital data can be copied and spread through internet within short time by malicious authorized user. So primitives like encryption offers data protection only it to be decrypted. But we can't identify the leaker in a provable manner. In LIME the auditor is communicated to the owner and the consumer. So he can identify when data is accessed in unauthorized way. Some scenarios make questionable situation to prove the guilty party which make data leakage. The scenarios like:

Outsourcing : Companies transferring portions of work to outside suppliers rather than completing it internally, so it cost leakage of sensitive data. But cannot identify the person which cause data leakage

Online Social Networking Site : Like facebook which leak private information of the user to other users or companies. There are different methods to access the sensitive data but we cannot prevent from it and find the malicious user in a provable way.

Chart -1:

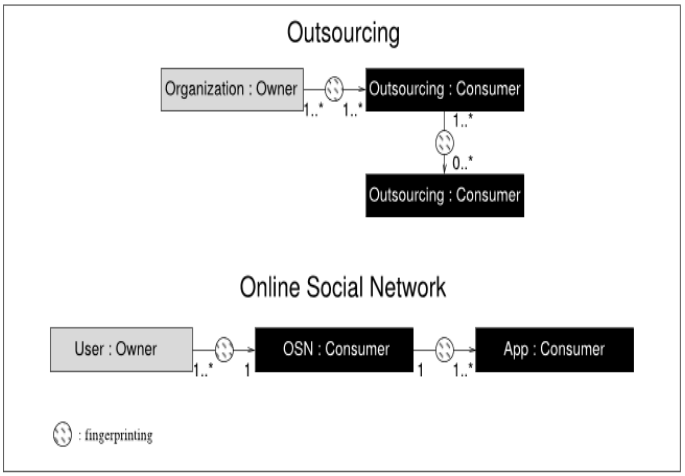

Fig -1: Outsourcing & Social networking site scenarios for data leakage

Another method is **forensic technique**. It is used to identify the leaker in a provable manner but it's not accurate always and it is costly.

3. PROPOSED SYSTEM

In our system introduce Cox algorithm for watermarking, HTTPA(Accountable Hyper Text Transfer Protocol) secure data transfer and signature primitives for data encryption and decryption and Three way handshaking protocol for secure data receiving when XSS attack occur. Auditor is communicating with involved parties in the communication (owner and consumer). So he get a notification when malicious practice is occur. And he can block the malicious user from post actions.

Chart -2:

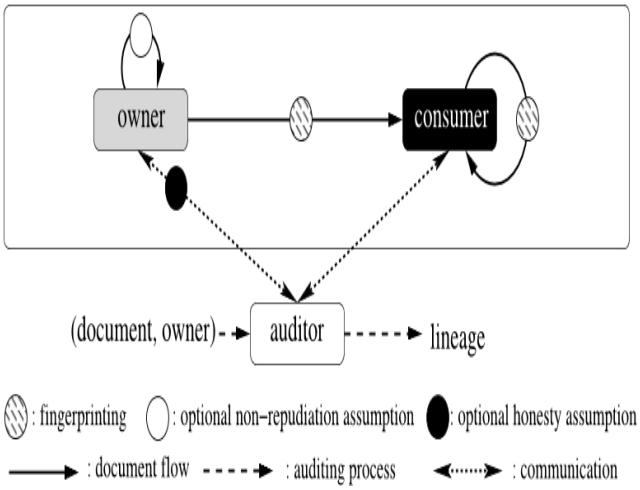

Fig -2: LIME framework

3.1.TDES And Signature Primitives

In our proposed work use Triple DES algorithm for data encryption., officially the Triple Data Encryption Algorithm (TDEA), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block .The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, it work effectively against brute-force attacks. Signature primitives like encryption and decryption use symmetric key .The key will allow only to the registered user when he request.

3.2.COX Watermarking algorithm

Cox algorithm is used for robust watermarking. It is the process of embedding data into a multimedia element such as an image, audio or video file. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or detection, algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. In cox method embedding of Gaussian noise to watermark images. To provide robustness ,watermark provide the most significant part of the picture ,so we cannot remove the watermark without destroying the underlying picture.. We use α factor as a parameter to determine the influence of Gaussian noise on original image.

3.3.Accountable Data Transfer Protocol

The protocol, HTTPA (Accountable Hyper Text Transfer Protocol), requires the data producer and the data consumer to come to an agreement before the data transfer, enabling both parties will be held accountable for the agreement they had entered into. The data consumer will express the intentions of data access and usage, whereas the data producer will express the usage restrictions on the data. This data transfer is facilitated by a trusted third party "Provenance Controller" in an "intentions and usage restrictions handshake".

3.4.Micro benchmarking

The sender splits a watermarked document into *n* parts and creates two different versions of each part by embedding another watermark. The recipient receives one of two versions of each and joins the individual parts.

3.5.Broadcasting

Identification of the recipient by their received files using encryption and decryption process .

Finger casting: Recipient automatically embed a watermark in files during decryption process. It is an anti-watermarking process user to get the original data.

3.6.XSS Attack

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can inject malicious client side scripts (also commonly referred to as a malicious payload) into a legitimate website or web application. Cross-site scripting attack is a SQL code injection attack. It is a computer security vulnerability , The attacker gains access to sensitive page content, session cookies and other information by the browser behalf of the user. To overcome the data lineage through this attack we use three way handshaking protocol.

Chart -3:

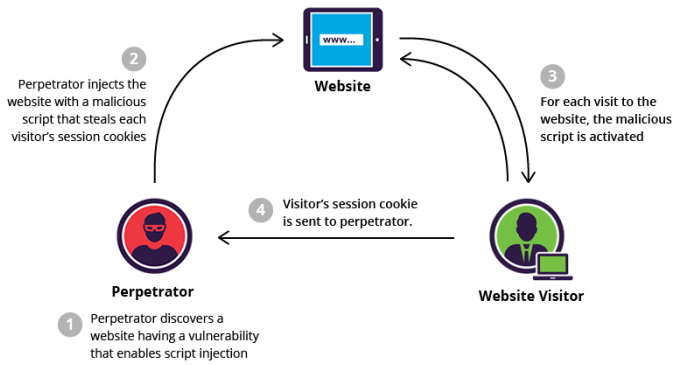

Fig -3:cross site scripting attack

3.7.Threeway hand shaking

This method is used in TCP/IP network to establish a secure connection between the client and server. It needs three step verification. SYN & ACK packets are transferred between the client and server before actual data is exchanged.

Chart -4:

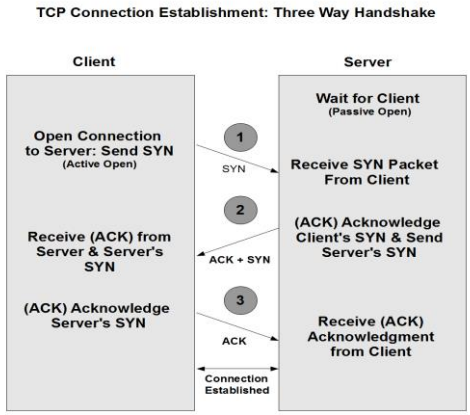

Fig -4:three way handshaking

4. CONCLUSIONS

LIME is a model for accountable data transfer across multiple entities. The secure data transmission using HTTPA, robust watermarking and signature primitives. LIME does not provide exact guaranty against data leakage but identify the leaker in a provable manner. But in our system identify the authorized user when he access the data in unauthorized way and prevent data leak through threeway hand shaking protocol.

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I am highly indebted to Ms.Jissmol Jose assistant professor of St.Joseph's college Irinjalakkuda for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to express my gratitude towards my parents & member of DC Infotech for their kind co-operation and encouragement which help me in completion of this project.
I would like to express my special gratitude and thanks to industry persons for giving me such attention and time.
My thanks and appreciations also go to my colleague in developing the project and people who have willingly helped me out with their abilities.

REFERENCES

[1] https://en.wikipedia.org/wiki/Wikipedia.
2 "Chronology of data breaches," http://www.privacyrights.org/data-breach.
3 "Data breach cost," http://www.symantec.com/about/news/release/article.jsp?prid=20110308 01
4 "Electronic Privacy Information Center (EPIC)," http://epic.org, 1994
5 A. Adelsbach, S. Katzenbeisser, and A.-R. Sadeghi, "A computational
model for watermark robustness," in Information Hiding. Springer,2007, pp. 145–160
6 A. Mascher-Kampfer, H. St ¨ogner, and A. Uhl, "Multiple re-watermarking scenarios," in Proceedings of the 13th International
Conference on Systems, Signals, and Image Processing (IWSSIP 2006).Citeseer, 2006, pp. 53–56.
7 J. Kilian, F. T. Leighton, L. R. Matheson, T. G. Shamoon, R. E. Tarjan,and F. Zane, "Resistance of digital watermarks to collusive attacks," inIEEE International Symposium on Information Theory, 1998, pp.
271–271.
8 Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivioustransfers efficiently," in Advances in Cryptology-CRYPTO 2003.Springer, 2003, pp. 145–161