International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Forestalling Of Data Leakage In Malicious Environment

N.V.H.Madhuri & Md.Asim
[1]M.Tech, Dept. of CSE,Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool
[2]Assistant Professor, Dept. of CSE,Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool

ABSTRACT

Social Networking was reported as a third party applications that was widely being used online social network Facebook is a sensitive private information about the users or even their friends to advertising companies

.Information that has been spread through unintentional exposures or intentional shortage by disgruntled employees and malicious external entities, present one of the most serious threats to organizations.The outsourcing company that was handed by a sensitive data is been hired as further subcontractor that hired another subcontractor in India itself. Although its a offshore subcontractor is suspected, each of them had access to the data and could have possibly leaked it. I have to find that other scenarios can be associated to an mechanisms during data transfers.third parties don't either focus on protection, as they are say that the leaked data cannot be linked to them.

Keywords: Distributed Usage Control; Policy Enforcement; Security And Privacy; Outsourcing Companies

I. INTRODUCTION

The social networking generate substantial revenue whether its internet the worth of using on the mobile devices is more as the device gets involved more in media delivery platforms. Moreover, considering that a decent fraction of these users own smart phones or tablets certainly expands this opportunity. These users spend significant time browsing the different multimedia and gaming capabilities of their devices, making them more exposed .Also, these devices now come with Wi-Fi and 3G, meaning they can be reached virtually everywhere. Add to this GPS capability and computing user preferences, and a new level of targeted advertising can be attained. Personalized ads that can match users' references with products and services in their have much higher chances of succeeding in capturing this user's attention and achieving better customer satisfaction, consequently increasing the profitability of ads. The same aspects that make these devices great platforms for advertising also impose strict guidelines since they contain key private data, like contacts information and calendar entries. Hence, proper use and confidentiality of this data should be respected. Privacy preserving techniques are better implemented by design, which is the approach taken in this paper. We propose a system for providing security preferences whilst Preserving their privacy and taking into consideration context, time, and location. This is done by aggregating requests and sending them through one of the users, who later anonymously contacts the server with the list of aggregated interests.

Data leakage is a challenging issue in the industries and different institutes.even though there are number of systems designed for the purpose of the data security by using different encryption algorithms, there is a big issue of the integrity for the users of systems. It is difficult for any system administrator to find out the data leaker among the system users. It creates many ethical issues in

working environment . The data leakage detection industry is very heterogeneous as it of ripe product lines of leading IT security vendors. The technologies such as firewalls, encryption, access control, identity management, machine learning content based detectors and others have already been to offer protection against various factors of the data leakage threat. The competitive benefits of developing a bullet data leakage detection suite. It is mainly in using effective orchestration enabling technologies to provide the highest degree of protection by ensuring an optimal solution of specific data leakage detection technologies with a "threat landscape" they operate in. The landscape is characterized by types of channels, states, users, and IT platforms.

II. SYSTEM ARCHITECTURE 2.1

Proposed System

In this project we define LIME method (Lineage in Malicious Environment) to identity the guilty party. In this method we are clearly defined the role to each involved party and define the inter-relationships between these roles. Three different roles are play a vital role owner, consumer, auditor. The data owner role is to maintain the documents (images).The data consumer receives the document and also forward the document to another consumer. Auditor is invoked when a leakage is occurs, he is only responsible to find a leakage(guilty party). He is invoked by an owner and provided with the leaked data. If the data leaked was transferred using our method, there is identifying information embedded for each consumer who might have received it. Using this information the auditor can create a lineage, and he find the last consumer in the lineage is the leaker.info, and thus it can easily profile users. Even though such privacy invasion of user personal information is currently .

2.2 System Overview

The idea in our system is for users to aggregate their interests when requesting advertisements to hide their identities from the ad server. Since not all users can trust each other, the aggregation should not expose their interests to each other. One solution is for each user to encrypt his interests with the server's public key, but this would result in separately encrypted set of interests, giving them away to the ad server without hiding their identities from it. Hence, the system should ensure the privacy of users in relation to the server, and relative to each other. The ad server delivers ads and collects billing reports. It stores a database of ads tagged by context, location, time, and personal preferences. Service providers (merchants) subscribe with the ad server and supply it with the ads and their intended targets. The server stores these ads and maintains for each ad a log of total number of clicks, which are aggregates of numbers of clicks received along with the requests for ads. The server bills the service providers according to the number of clicks by users on their ads. Content providers (mobile app providers) also subscribe with the ad server and get a unique ID whose purpose is to identify each content provider so that it can be reimbursed by the ad server for hosting the ads.

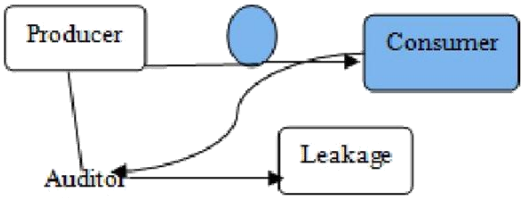

Figure 1 : System Architecture

2.3 System Operations

2.3.1 Requesting Image

In each organization having some documents like image, who is having the own document and that person is responsible for manage the document. The consumer chooses the provider and get the owner document list. Consumers choose the document which one he wants and give the request to respective owner. Watermarking Method and Access control

Data owner after accepting the request, then the document to be send after watermarking process is done. Here robust watermarking method is used. Here stenography method is used to embed a information. The embed information is, consumer name, provider name and filename, this three information is change to signature using HMAC algorithm, the whole information is encrypted using RSA algorithm .The encrypted information is embedded into image.

2.3.2 Access Control

Access Control Mechanism means restricts the consumer to forward the documents, how many times the documents can be transferred to another consumer. So that user cannot forward the documents to many user.

2.3.3 Data lineage Method

Consumer can forward the documents to any consumer who is giving request to that consumer. Every consumer forwards the documents only after watermarking the documents. If sender (consumer) tries to send that restricted documents more times than restriction, they cannot forward the documents in trusted manner. Malicious method data forwarding is the consumer forwards the documents to malicious person in malicious user page. While sending malicious method they cannot watermark image in a proper manner. After leakage the document. The owner of this document invoke the auditor to identify the leakage. The auditor initially takes the owner as the current suspect sends the leaked document to the current suspect and asks him to provide the decryption key for the watermarks in this document. Using the key, auditor can decrypt the document .The consumer name is registered user then the consumer is trusted. If user is not registered user, the embedded information length is varying, then auditor appends the lineage in consumer and that consumer is a leaker .these packets, it decrypts them using its private key, and aggregates them to be sent to the server. When the ad server receives the interests, it replies with ads to the primary peer, who will then broadcast them to the group. Each peer will filter out his own ads, and rebroadcasts the ads to ensure reach ability of all peers. There are two types of ad requests that can be issued: 1) when the user needs particular services or products given his location, the time of the request, and his personal preferences, or 2) when the mobile app needs to refresh expired ads which were requested before and are cached. When a user requests ads to be displayed, the system will check for the request in the cache. If the request

and all its corresponding ads are not outdated and are still viable in terms of location and time, the ads will be fetched directly from memory. Else, the request is sent to the server in accordance with the system mechanisms.

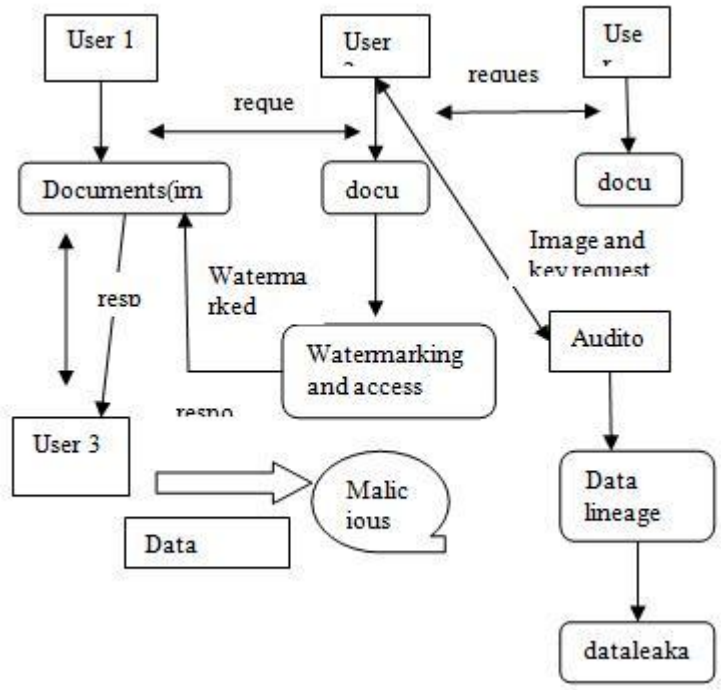

Figure 2: System Operations

III. RELATED WORK

A preliminary shorter version of this paper appeared at the STM workshop [21]. This version constitutes a significant extension by including the following contributions: We give a more detailed description of our model, a formal specification of the used primitives, an analysis of the introduced protocol, a discussion of implementation results, an application of our framework to example scenarios, a discussion of additional features and an

IV. CONCLUSION

We present LIME, a model for accountable data transfer across multiple entities. We define participating parties, their inter-relationships and give a concrete instantiation for a data transfer protocol using a novel combination of oblivious transfer, robust watermarking and digital signatures. We prove its correctness and show that it is realizable by giving micro bench-marking results. By presenting a general applicable framework, we introduce accountability as early as in the design phase of a data transfer infrastructure. Although LIME does not actively prevent data leakage, it introduces reactive accountability. Thus, it will deter malicious parties from leaking private documents and will encourage honest (but careless) parties to provide the required protection for sensitive data. LIME is flexible as we differentiate between trusted senders (usually owners) and untrusted senders (usually consumers). In the case of the trusted sender, a very simple protocol with little overhead is possible. The untrusted sender requires a more complicated protocol, but the results are not based on trust assumptions and therefore they should be able to convince a neutral entity (e.g. a judge).Our work also motivates further research on data leakage

detection techniques for various document types and scenarios. For example, it will be an interesting future research direction to design a verifiable lineage protocol for derived data.

REFERENCES

[1] "Chronology of data breaches," http://www.privacyrights.org/data-breach.

[2] "Data breach cost," http://www.symantec.com/about/news/release/article.jsp?prid=20110308 01.

[3] "Privacy rights clearinghouse," http://www.privacyrights.org.

[4] "Electronic Privacy Information Center (EPIC)," http://epic.org, 1994.

[5] "Facebook in Privacy Breach," http://online.wsj.com/article/SB100 01424052702304772804575558484 075236968.html.

[6] "Offshore outsourcing," http://www.computerworld.com/s/article/109938/Offshore outsourcing cited in Florida data leak.

[7] 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.

[8] P. Papadimitriou and H. Garcia-Molina, "Data leakage detection,"Knowledge and Data Engineering, IEEE Transactions on, vol. 23, no. 1,pp. 51–63, 2011.

[9] "Pairing-Based Cryptography Library (PBC),"http://crypto.stanford.edu/pbc.

[10] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Image Processing, IEEE Transactions on, vol. 6, no. 12, pp. 1673–1687, 1997.

[11] B. Pfitzmann and M. Waidner, "Asymmetric fingerprinting for larger collusions," in Proceedings of the 4th ACM conference on Computer and communications security, ser. CCS '97, 1997, pp. 151–160.

[12] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM J. Comput., vol. 17, no. 2, pp. 281–308, 1988.

[13] A. Adelsbach, S. Katzenbeisser, and A.-R. Sadeghi, "A computational model for watermark robustness," in Information Hiding. Springer, 2007, pp. 145–160.

[14] J. Kilian, F. T. Leighton, L. R. Matheson, T. G. Shamoon, R. E. Tarjan, and F. Zane, "Resistance of digital watermarks to collusive attacks," in IEEE International Symposium on Information Theory, 1998, pp.271–271.

[15] M. Naor and B. Pinkas, "Efficient oblivious transfer protocols," in Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms, 2001, pp. 448–457.

[16] "GNU Multiple Precision Arithmetic Library (GMP),"http://gmplib.org/.

[17] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in Advances in Cryptology-ASIACRYPT 2001. Springer,2001, pp. 514–532.

[18] W. Dai, "Crypto++ Library," http://cryptopp.com.

[19] P. Meerwald, "Watermarking toolbox," http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/source.

Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently," in Advances in Cryptology-CRYPTO 2003.Springer, 2003, pp. 145–161.

[21] M. Backes, N. Grimm, and A. Kate, "Lime: Data lineage in the malicious environment," in Security and Trust Management - 10th International Workshop, STM 2014, Wroclaw, Poland, September 10-11,2014. Proceedings, 2014, pp. 183–187.

[22] R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in FAST, 2009, pp.1–14.

[23] A. Pretschner, M. Hilty, F. Sch¨utz, C. Schaefer, and T. Walter, "UsageControl Enforcement: Present and Future," IEEE Security & Privacy, vol. 6, no. 4, pp. 44–53, 2008.