International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Transaction monitor on Merchant & Buyers Privacy Data from UN authentication attacks

G.SRAVANI[1]&M. DHARANI KUMAR[2]

[1]M-Tech, Dept. of CSE P.V.K.K INSTITUTE OF TECHNOLOGY
Sanapa Road, Rudrampeta, Anantpaur,AP

[2]Assistant Professor, Dept. of CSE P.V.K.K INSTITUTE OF TECHNOLOGY
Sanapa Road, Rudrampeta, Anantpaur,AP

Abstract

Innominate dactylogram has been suggested as a convenient solution for the licit distribution of multimedia contents with copyright aegis whilst preserving the privacy of buyers, whose identities are only revealed in case of illicit re-distribution. However, most of the subsisting incognito fingerprinting protocols are impractical for two main reasons the utilization of intricate time-consuming protocols and/or homomorphism encryption of the content, and a unicast approach for distribution that does not scale for a sizably voluminous number of buyers. This paper stems from an antecedent proposal of recombined dactylograms which surmounts some of these drawbacks. However, the recombined dactylogram approach requires an involute graph search for apostate tracing, which needs the participation of other buyers, and veracious proxies in its P2P distribution scenario. This paper fixates on abstracting these disadvantages resulting in an efficient, scalable, privacy-preserving and P2P-predicated fingerprinting system.

Keywords: - Merchant, Buyers' Privacy, Transaction monitor, Database authentication attacks

1. INTRODUCTION

Licit distribution of multimedia contents is a recurrent topic of research. Broadband home Internet access has enabled the sustained magnification of e-commerce, including direct downloads of multimedia contents. However, copyright infringement is one of the most germane threats to the content industry. Fingerprinting emerged [1] as a technological solution to evade illicit content re-distribution. Rudimentally, fingerprinting consists of embedding an imperceptible mark dactylogram in the distributed content (which may be audio, still images or video) to identify the content buyer. The embedded mark is different for each buyer, but the content must stay perceptually identical for all buyers. In case of illicit re-distribution, the embedded mark sanctions the identification of the re-distributor by betokens of an apostate tracing system, making it possible to take

subsequent licit actions. Albeit fingerprinting techniques have been available for proximately two decades, the first few proposals in this field are far from nowadays' requisites such as scalability for thousands or millions of potential buyers and the preservation of buyers' privacy. This paper reviews the main features of the proposal suggested in [10], [09], highlights its main drawbacks, and suggests several paramount amendments to achieve a more efficient and practical system, especially as apostate tracing is concerned, since it evades the situations in which illicit redistributors cannot be traced with the proposal of [07], [10]. Furthermore, better security properties against potentially malignant proxies are obtained. Albeit the system proposed in this paper uses public key encryption in the distribution and apostate tracing protocols, it must be taken into account that this encryption is only applied to short bit strings, such as the binary dactylograms and hashes, not to the content. The fragments of the content are encrypted utilizing symmetric cryptography, which is much more efficient.

2. RELATED WORK

Existing System

The proposal presented in this paper stems from the fingerprinting system described in [1], [3], which introduced the concept of automatically recombined (additionally called DNA-inspired) dactylograms in P2P networks. The next sections present the main features and drawbacks of the anterior work. The content is divided into several authoritatively mandated fragments and each of them is embedded discretely with an arbitrary binary sequence. The binary sequence for each fragment is called segment and the concatenation of all segments forms the whole dactylogram. The merchant distributes different copies to a reduced set of M seed buyers. The dactylograms of these buyers are such that their segments have low pair-sagacious correlations. The buyers other than the seed ones engage on P2P transfers of the content in such a way that each incipient buyer obtains fragments from at least two other buyers. The dactylogram of each incipient buyer is built as a recombination of the segments of its parents.

Proposed System

The content is divided into several injuctively authorized fragments and each of them is embedded discretely with an arbitrary binary sequence. The binary sequence for each fragment is called segment and the concatenation of all segments forms the whole dactylogram. The merchant distributes different copies to a reduced set of M seed buyers. The

dactylograms of these buyers are such that their segments have low pair-sapient correlations. The buyers other than the seed ones engage on P2P transfers of the content in such a way that each incipient buyer obtains fragments from at least two other buyers. The total number of buyers is N _ M. The communication between peer buyers is innominate through an onion routing-like protocol utilizing a proxy. The dactylogram of each incipient buyer is built as a recombination of the segments of its parents. Proxies ken the pseudonyms of source and destination buyers and they have access to the symmetric keys utilized for encrypting the multimedia content. A transaction record is engendered by a transaction monitor to keep track of each transfer between peer buyers. These records do not contain the embedded dactylograms, but only an encrypted hash of them. The fingerprints' hashes are encrypted in such a way that the private key of at least one parent is required for obtaining their clear text. The authentic identities of buyers are kenned only by the merchant. The transaction monitor records buyers' pseudonyms. In case of illicit re-distribution, a search is required through the distribution graph. The search commences from the seed buyers and is directed by a correlation function between the traced dactylogram and the dactylograms of the tested buyers. These tested buyers must co-operate with a tracing ascendancy to compute the correlation between their dactylogram and the one extracted from the illicitly re-distributed file. The fingerprints' hashes recorded in the transaction monitor are enough to avert buyers from cheating in this step. At each step of the apostate tracing protocol, the buyer with maximum correlation is culled as the most likely predecessor of the illicit re-distributor. This criterion is mostly right, but some erroneous culls may occur during the search process, requiring the lassitude of a subgraph and backtracking. The search ends when perfect correlation is found between the dactylogram of the tested buyer and that of the illicitly re-distributed file. If a buyer relucts to take a correlation test, the hash recorded in the transaction monitor can be utilized as evidence against her.

3. IMPLEMENTATION

Merchant

He distributes facsimiles of the content licitly to the seed buyers. Each fragment of the content contains a different segment of the dactylogram embedded into it. The segments have low pair-sagacious correlations.

Buyer's privacy

The identity of a buyer who has purchased a concrete content could be revealed by a

coalition of two parties: one of the proxies culled by the buyer and the merchant (who can link her pseudonym to an authentic identity) or, similarly, the transaction monitor and the merchant. Better privacy could be achieved if, for example, the pseudonyms were encrypted by the proxies utilizing the public key of the tracing ascendancy.

Transaction Monitor

It keeps a transaction register for each purchase carried out for each buyer. This transaction register includes an encrypted version of the embedded dactylograms. In case of illicit re-distribution, it participates in the tracing protocol that is utilized to Identify the illicit re-distributor(s).

Database authentication attacks

An assailer may endeavor to obtain the dactylogram of a buyer that is stored in the transaction monitor's database. An assailant may endeavor to intercept the traffic between a buyer and one or more of her proxies and keep a facsimile of all the fragments of the content.

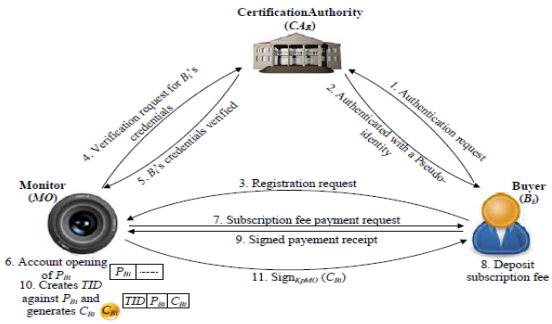

Fig 1 System Architecture

4. EXPERIMENTAL RESULTS

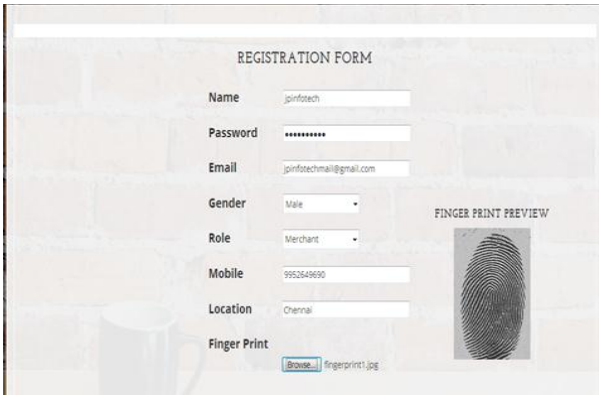

Fig 2 User Registration

Fig 3 Merchant details

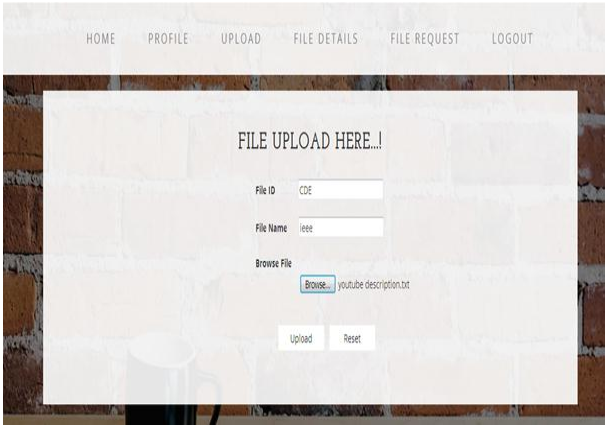

Fig 4 Data Upload

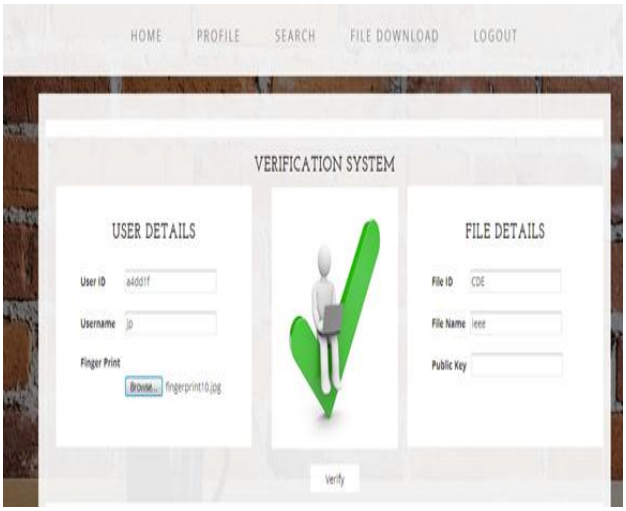

Fig 5 Verification System

Fig 6 File Download

5. CONCLUSION

The utilization of automatic recombined dactylograms has been recently suggested in the literature [8], [10], exhibiting remarkable advantages: the dactylograms of buyers areunknown to the merchant (achieving anonymity) and dactylogram embedding is required only for a few seed buyers, whereas the other dactylograms are automatically obtained as a recombination of segments. However, the published system has some shortcomings: 1) it requires a sumptuous graph search in order to identify an illicit re-distributor, 2) some irreprehensible buyers are requested to co-operate for tracing, and 3) the P2P distribution protocol requires veracious proxies. This paper shows that the co-operation of veracious buyers in apostate tracing entails several pertinent drawbacks that can make the published system fail under some circumstances. The amendments suggested in this paper overcome the draw backs of [2], [4] by recording the dactylograms utilizing multiple encryption in such a way that the graph search is superseded by a standard database search, whilst buyers' frame proof ness is retained. Additionally, misconducting proxies are dismayed by denotes of arbitrary checks by the ascendancy and utilizing a four-party innominate communication protocol to obviate proxies from accessing the clear text of the fragments of the content.

6. REFERENCES

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in Proc. 15th Ann. Int. Cryptology Conf. Adv. Cryptology, 1995, pp. 452–465.

[2] Y. Bo, L. Piyuan, and Z. Wenzheng, "An efficient anonymous fingerprinting protocol," in Proc. Int. Conf. Comput. Intell. Security, 2007, pp. 824–832.

[3] J. Camenisch, "Efficient anonymous fingerprinting with group signatures," in Proc. 6th Int. Conf. Theory Appl.

Cryptology Inf. Security: Adv. Cryptology, 2000, pp. 415–428.

[4] C.-C. Chang, H.-C. Tsai, and Y.-P. Hsieh, "An efficient and fair buyer-seller fingerprinting scheme for large scale networks," Comput. Security, vol. 29, pp. 269–277, Mar. 2010.

[5] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, pp. 84–90, Feb. 1981.

[6] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Burlington, MA, USA: Morgan Kaufmann, 2008.

[7] J. Domingo-Ferrer and D. Megıas, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community," Comput. Commun., vol. 36, pp. 542–550, Mar. 2013.

[8] M. Fallahpour and D. Megıas, "Secure logarithmic audio watermarking scheme based on the human auditory system," Multimedia Syst., vol. 20, pp. 155–164, 2014.

[9] S. Katzenbeisser, A. Lemma, M. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 783–786, Dec. 2008.

[10] M. Kuribayashi, "On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol," EURASIP J. Inf. Security, vol. 2010, pp. 1:1–1:11, Jan. 2010.