Volume 8, No. 5, May – June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Mitigating Sybil Attack in Self-Destructing Data System

Mohd. Saif
Department of Computer Science
Jamia Hamdard
New Delhi, India

Bhavya Alankar*
Department of Computer Science
Jamia Hamdard
New Delhi, India

Abstract: Data privacy is an important concern in the digital computing environment. Personal data which is stored on the server may contain account numbers, passwords and other important information which can be theft and misused. Self-Destructing data therefore,is an important idea to have reliability over digital communication. Self-Destructing data provides data privacy by making all the copies of file unreadable after user specified time and that too without user's intervention. Most of the present Self-Destructing data models are prone to the Sybil attack. Thus this paper aims at proposing a solution to mitigate the Sybil attack on the self-destructing data systems.

Keywords: privacy; self-destruct data; Sybil attack; identity management.

I. INTRODUCTION

In today's world with the rapid development of Cloud computing and mobile Internet, Cloud services become increasingly important in people's life. People are pretty much requested to submit or post some personal and private information to Cloud by Internet. At the point when people do this, they subjectively due to trust hope that service providers will provide security policies to shield their data from revealing to the other people. As people depend more and more on the cloud and internet technology, probability of security breach of their privacy is at higher risk. Firstly, when data is processed, transformed and stored by computer system or network, computer systems or network must cache, archive or copy it because these copies are inevitable for network and system. However, people generally have no prior knowledge about these copies and therefore cannot control them, thus privacy of these copies is leaked to the public. Secondly, privacy leakage can also be attributed to intrusion by a hacker, cloud service provider's negligence or some legal actions. These issues present challenges to protect people's privacy in the vast cloud environment.

Self-Destructing data aims creating data that self-destructs automatically after it's no longer useful. Moreover it should destructs itself without user's intervention or any third party storing the data. [1]Many security mechanisms rely on particular assumptions of identity and are prone to attacks when these identity assumptions are violated. For instance, impersonation is the famous outcome when authenticating credentials are stolen by a third party.Majority of the earlier research on electronic identities has concentrated on endurance and unforgeability [2][3][4][5] instead of on distinctness.

The matter of establishing online identities for people has been contemplated for quite a while [6][7], with solutions that usually rely upon some immediate cooperation in the physical world [8][9].

The term Sybil attack is acquainted in [10] to represent an attack where the attacker tries to counterfeit multiple identification in a certain region. Basically Sybil is an attack against identity wherein an individual entity tries to masquerade as various simultaneous identities. The Sybil attack is an elementary problem in many peer-to-peer systems.

The paper is organized as follows. We motivate the need of reputed system for conducting identity audit. Continuing with this rationale, we discover how trusted certification hierarchy design can be applied to identity management to tackle Sybil attack. In the end we conclude.

II. LITERATURE REVIEW

Sybil attacks are a well-known problem in systems requiring participation from many different users [10]. Such attacks can compromise the correctness of systems providing online voting [15], that vote on correct solution to a distributed computation [16], or generate reputation from user feedback [17].

Frameworks like Vanish that endeavor to give anonymity or privacy through a distributed framework are similarly defenseless against Sybil attacks. For instance, a Sybil attack against the Tor overlay system can subvert secrecy guarantees. [18].

A pioneering analysis of Vanish [1] supplies another scheme for ensuring privacy.

In Vanish, a secret key is split and stored in a P2P (point to point) framework with distributed hash tables (DHTs). According to features of P2P, after every eight hour the DHT refreshes every node. With joining and leaving of the P2P node, the system manages secret keys. Vanish functions by encrypting every message with an arbitrary key and storing segments of the key in a large DHT. However, Sybil attacks [3] may be one of the problem for Vanish.

Wolchok et al. [11] concluded that public DHTs like VuzeDHT [12] is not capable to provide enough security for Vanish.

Anderson [13] stated three types of intruders:

Masqueraders: Unauthorized access to a system and get all rights to exploit the data belonging to a legitimate user.

Misfeasor: When authorized user accesses the data beyond his rights.

Clandestine user: When an individual captures the supervisory control over the system.

Freedman et al. [14] particularly propose testing for IP addresses in various areas or self-sufficient frameworks. Heterogeneous IP addresses requirement checks a few attacks however it limits the convenience of an application.

III. PROBLEM FORMULATION

The Sybil attack is the major threat in the self-destructing data models which compromises the data privacy in one or the other way. Thus self-destructing data model cannot be foolproof if the masquerader is able to represent itself as a part of the system.

IV. PROPOSED SOLUTION

A Masquerade happens when one entity disguises itself to be a different entity. A masquerade attack as a rule incorporates one of the other types of active attack. For example, verification arrangements can be caught and replayed after a legitimate validation sequence has occurred, subsequently empowering an approved entity with few benefits by impersonating an element that has those benefits. Addition of messages into the system from a fake source. This incorporates the production of messages by a rival that are indicated to originate from an approved entity. Likewise included are fake affirmations of messages receipt or non-receipt by somebody other than the message recipient. Sybil attack is possible generally due to flaw in the identity management system. Identity Management is thus an essential part for the reliable, secure and trustworthy network.

A. Reputed Systems:

Reliable and definite reputation information about peers can form the basis of an incentive system and can guide peers in their decision making. The reputation system uses an objective criterion to track each peer's input in the system and also allows to store peers reputations locally. .Peer-to-peer (P2P) networks have introduced a new paradigm in content distribution. Each peer is both a client and a server in these networks.Reliable and trustworthy peer reputations could be used in various ways. They can help well-reputed peers find other peers with good reputations and hence help them in making decisions about who to provide content to and who to request content from. The tracking of peer reputations in a centralized P2P network is not so difficult because a central server facilitates the search for the content.

But in the case of functioning of decentralized P2P networks, the lack of any central authority makes the difficulty of accurate reputation tracking a real challenge.

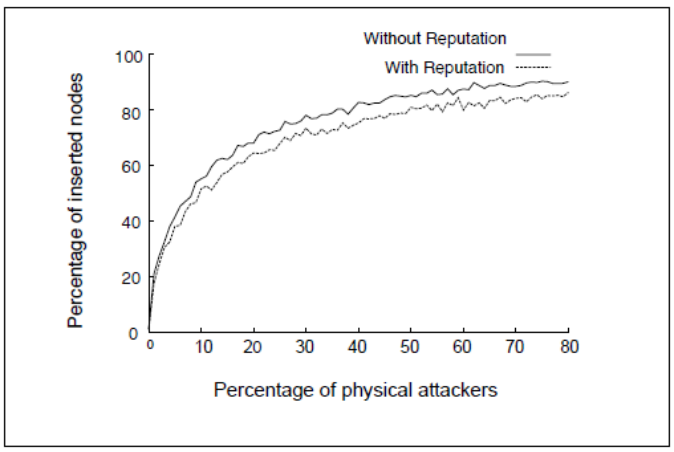

Figure 1. Performance analysis of peers

From the above figure, we analyze that peers with reputation are less prone to Sybil attack and thus are better in performance in the network as compared to the peers without reputation.

B. Conducting an Identity audit:

Certificate Authorities (CAs), issue Digital Certificates. Digital Certificates are verifiable compact information records that contain personality credentials to help websites and devices represent their genuine online identity (authentic as the CA has verified the identity). CAs play a key role in how securely the Internet operates and how transparent, trusted and secured transactions can take place online. Each year Issuing CA's provide millions of Digital Certificates, and these certificates are utilized to protect information, encode billions of transactions, and empower secure communication. Conducting identity audit is inevitable for prevention against most of the security vulnerabilities related to the identity verification based authentication. Identity auditing monitors from time to time the activities of certified entities.

C. Trusted Certification:

The centralized authentication approach requires hosts to trust and follow the defined policies by a central authentication authority. This may be just one of the hosts, or it may be a set of hosts forming a logical authentication authority. Authentication authority maintains the authentication database which can be used by all the hosts associated within the centralized authentication system domain. Trusted certification depends on a centralized authority that must take care that each individual entity is allocated exactly one identity, as indicated by ownership of a certificate. The certifying authority must make certain that lost or theft identities are find out and revoked.

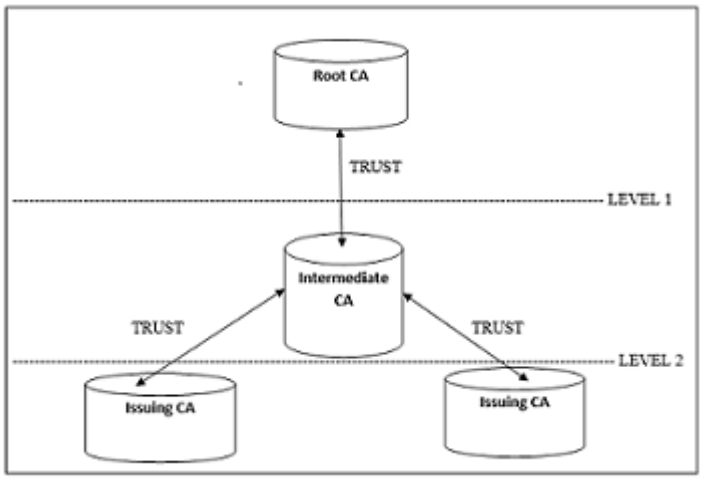

Figure 2. Trusted Certification hierarchy

Trusted Certification can be achieved in large scale p2p networks by hierarchical architecture design. Centralized and hierarchical CA design provides us the desired identity management system which is an integral part to avoid Sybil attack. Root Certifying authority plays a vital role in certifying every other entity. It is the centralized authority in certifying

entities which monitors issuing CA's and also intermediate CA between them. Root CA is the core of this framework which also regulates the total number of certificates to be issued for certification. Therefore, making issuing CA's and intermediate CA's dependent to root CA for each and every certifying action they do including distributing certificate. At level second there is an intermediate CA which connects root CA's to the issuing CA's. Intermediate CA also acts as a monitoring and functionality bridge between Root CA Issuing CA's.

If the performance and security implications can be solved, then this approach can eliminate the Sybil attack.

V. FUTURE SCOPE

We proposed a Sybil proof distributed scheme allowing for identifying peer reputation in P2P networks. This mechanism relies on a hierarchy based certification of the identities. Our proposed solution can also be used as a solution for various Sybil attack prone cyber domain.

VI. CONCLUSION

Self-Destructing data system is an efficient way for data confidentiality but the Sybil attack is the major concern for it. Reputation system for peers serves the purpose of security against attackers. A centralized and hierarchy based design of identity management serves as the basic monitoring body. The Trusted Certification mechanism is one of the most efficient, powerful and successful way of implementing secure self-destructing data system mitigating the Sybil attack.

VII. REFERENCES

[1] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy. Vanish:Increasing data privacy with self destructing data. In USENIX Security, pages 299–314, 2009.

[2] U. Feige, A. Fiat, A. Shamir, "Zero-Knowledge Proofs of Identity", Journal of Cryptology 1 (2), 1988, pp. 77-94.

[3] A. Fiat, A. Shamir, "How to Prove Yourself: Practical Solutions of Identification and Signature Problems", Crypto '86, 1987, pp. 186-194.

[4] K. Ohta, T. Okamoto, "A Modification to the FiatShamir Scheme", Crypto '88, 1990, pp. 232-243.

[5] A. Shamir, "An Efficient Identification Scheme Based on Permuted Kernels",Crypto '89, 1990, pp. 606-609.

[6] J. S. Donath, "Identity and Deception in the Virtual Community", Communities in Cyberspace, Routledge, 1998.

[7] S. Turkle, Life on the Screen: Identity in the Age of the Internet, Simon & Schuster, 1995.

[8] C. Ellison, "Establishing Identity Without Certification Authorities", 6th USENIX Security Symposium, 1996, pp. 67-76.

[9] P. Zimmerman, PGP User's Guide, MIT, 1994.

[10] J. R. Douceur. The Sybil attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pages 251–260, 2002.

[11] S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman, C. J. Rossbach, B. Waters, and E. Witchel, "Defeating vanish with low-cost Sybil attacks against large DHEs," in Proc. Network and Distributed System Security Symp., 2010.

[12] Azureus, 2010 [Online]. Available: http://www.vuze.com/

[13] Anderson,J. Computer Security Threat Monitoring and Surveillance. Fort Washington,PA: James P.Anderson Co.,April 1980.

[14] M. J. Freedman and R. Morris. Tarzan: A peer-to-peer anonymizing network layer. In Proc. ACM CCS, Nov. 2002.

[15] P. Judge. .Net vote rigging illustrates importance of Web services. http://news.zdnet.co.uk/software/0,1000000121, 2102244,00.htm.

[16] M. Yurkewych, B. N. Levine, and A. L. Rosenberg. On the cost-ineffectiveness of redundancy in commercial P2P computing. In CCS, pages 280–288, 2005.

[17] A. Cheng and E. Friedman. Sybilproof reputation mechanisms. In P2PECON: ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems, pages 128–132, 2005.

[18] K. S. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. C. Sicker. Low-resource routing attacks against Tor. In WPES, pages 11–20, 2007.