SHIV SHAKTI

International Journal of in Multidisciplinary and Academic Research (SSIJMAR)

Vol. 4, No. 3, June 2015 (ISSN 2278 – 5973)

Network Security From Sybil Attack

Jyoti Sambharya

M.Tech. Scholar, Deptt. Of ECE, S (PG) I T M, Rewari

Impact Factor = 3.133 (Scientific Journal Impact Factor Value for 2012 by Inno Space Scientific Journal Impact Factor)

Global Impact Factor (2013)= 0.326 (By GIF)

Indexing:

ABSTRACT

Open-access distributed systems like peer-to-peer systems area unit significantly at risk of Sybil attacks, wherever a malicious user creates multiple pretend identities (called Sybil nodes). While not a sure central authority which will tie identities to real citizenry, defensive against Sybil attacks is sort of difficult.

Among the little variety of decentralized approaches, our recent Sybil Attack protocol leverages a key insight on social networks to sure the quantity of Sybil nodes accepted. Despite its promising direction, Sybil Attack will permit an outsized variety of Sybil nodes to be accepted. What is more, Sybil Attack assumes that social networks area unit fast-mixing, which has ne'er been confirmed within the planet.

This project presents the novel Sybil Limit protocol that leverages identical insight as Sybil Attack, however offers dramatically improved and near-optimal guarantees. The quantity of Sybil nodes accepted is reduced by an element or around two hundred times in our experiments for a million-node system. We have a tendency to more prove that Sybil Limit's guarantee is at the most a log n issue aloof from best once considering approaches supported fast-mixing social networks. Finally, supported 3 large-scale real-world social networks, we offer the primary proof that real-world social networks area unit so fast-mixing. This validates the elemental assumption behind Sybil Limit's and Sybil Attack's approach.

INTRODUCTION

Definition

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. The name was suggested in or before 2002 by Brian Zill at Microsoft Research.

In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

Peer To Peer Network

A Peer to Peer (P2P) network is a distributed network composed of a large number of distributed, heterogeneous, and independent peers. P2P networks provide an alternative to the traditional client-server communication model in which a node in a P2P network can act as a server and a client at the same time. The P2P computing provides properties like no central point of failure and no service bottlenecks by decentralizing the service among participating nodes. In recent years many research work have been done and are still in progress to improve their robustness, security and scalability. P2P networks are less secure than a client-server network because of their decentralized nature.P2P specific security problems include [1] targeted denial of service attacks, forgery, pollution attack, Sybil attack, attacks on routing queries and attacks on data integrity.

For efficient routing and load balancing in P2P networks, every node should have a unique identifier and there should be an identity management scheme for handling identities in distributed environment. The term identity refers to information about an entity that is sufficient to identify that entity in a specific context and any entity, either in the digital world or in real world, is associated with an identity. Identity management plays a crucial role in operational efficiency, management control and cost savings. Systems need to manage the growing number

of users, their dynamicity, their access to information and applications scattered across heterogeneous systems. Identity management includes three major aspects: acquisition of identities, authentication, and authorization. Authentication is the process that verifies the association between an entity and the corresponding identity. Different authentication mechanisms have been widely used like password checking, challenge and response and biometric verification. Authorization grants the permission to an authenticated identity for accessing resources that it is eligible for (example, by using Access Control List).

Sybil Defense

Sybil defenses aim at limiting the number of Sybil identities, but false positives and false negatives [2] are acceptable to an extent in this process. Complete elimination of false negatives (Assigning Sybil identity as genuine) are not necessary since the distributed system should be able to tolerate some fraction of byzantine identities, otherwise, even without Sybil attack it is not Robust. Thus, a Sybil defense should be able to limit the total number of false negatives below the tolerance threshold of the system. Most of the applications can easily tolerate with a small fraction of false positives (labeling genuine nodes as Sybil). For example, in a P2P backup system, if a node considers another one as Sybil, then it will not trust that node for storing its data. A false positive rate of 20% means that, the given node will still trust 80% of the genuine nodes, and can use these. Also, if it is a recommendation system, then it can use votes from 80% of the genuine identities. From these observations, we can conclude that defenses against Sybil attack permit some bounded fraction of false positives and false negatives also.

LITERATURE SURVEY

John R. Douceur [3] - Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these "Sybil attacks" is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

Result section presents four simple lemmas, with nearly trivial proofs, that collectively show the impracticality of establishing distinct identities in a large-scale distributed system. An entity has three potential sources of information about other entities: a trusted agency, itself, or other (untrusted) entities. In the absence of a trusted authority, either an entity accepts only identities that it has directly validated (by some means) or it also accepts identities vouched for bother identities it has already accepted.

For direct validation, we show:

- Even when severely resource constrained, a faulty entity can counterfeit a constant Number of multiple identities.
- Each correct entity must simultaneously validate all the identities it is presented; Otherwise, a faulty entity can counterfeit an unbounded number of identities.

Large-scale distributed systems are inevitably heterogeneous, leading to resource disparities that exacerbate the former result. The latter result presents a direct impediment to scalability. For indirect validation, in which an entity accepts identities that are vouched for by already accepted identities, we show:

- A sufficiently large set of faulty entities can counterfeit an unbounded number of Identities.
- All entities in the system must perform their identity validations concurrently; Otherwise, a faulty entity can counterfeit constant number of multiple identities.

Since the number of faulty entities in the system is likely to grow as the system size increases, the former result places another limit on system scale. The latter restriction becomes harder to satisfy as system size increases.

Zied Trifa, Maher Khemakhem [2] -The survey and classification of the different security attacks in structured peer-to-peer (P2P) overlay networks can be useful to computer system designers, programmers, administrators, and users. In this paper, we attempt to provide taxonomy of structured P2P overlay networks security attacks. We have specially focused on the way these attacks can arise at each level of the network. Moreover, we observed that most of the existing systems such as Content Addressable Network (CAN), Chord, Pastry, Tapestry, Karelia, and Viceroy suffer from threats and vulnerability which lead to disrupt and corrupt their functioning. We hope that our survey constitutes a good help for who's working on this area of research.

Brian Neil Levine, Clay Shields, N. Boris Margolin [5] -There are a variety of attacks that hinge on the issue of identity. In this paper, authors presented an overview of work related to analyzing or solving the Sybil attack, in which one entity appears as or controls many different identities. We have demonstrated the breadth of applications that are subject to the attack, including the widely used systems Google, eBay, SETI@HOME, and Tor. The attack also presents a problem for peer-to-peer networks, mobile networks, and reputation systems. While we lack an efficient, general solution that scales well to large systems, there are a variety of solutions that can limit or prevent the attack in several individual application domains.

Nikita Borisov[6]-The problem of defending against Sybil attacks using computational puzzles. A fundamental difficulty in such defenses is enforcing that puzzle solutions not be reused by attackers over time. We propose a fully decentralized scheme to enforce this by continually distributing locally generated challenges that are then incorporated into the puzzle solutions. Our approach consists of an all-to-all broadcast of challenges, with a combining function to ensure this can be done efficiently. The combining function generates certificates that can be used to prove that each node? Challenge was delivered to and used by each other node, therefore proving the freshness of each puzzle.

Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons [7]-Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to *Sybil attacks*. In a Sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system.

METHODOLOGY

- First we created the main server who has its own database.
- Then the main server created the trusted server and the main server has it unique ID and details.
- Now, suppose the new member came with the request to join the group and send request to the trusted server.

  (For all the new members join the group or send request to the group, for all of them the trusted server is act as the main server)
- The trusted server sends the group joining form with the unique ID.
- New member fill the form and send back to the trusted server.
- Now the trusted server checks the details filled by the member with their database.
- This check is performing on the different parameters like house no., mobile no., landline no., email ID and so on…
- While the check performs we leave some parameter like name, city, and state because these parameter are commonly same with the other members.
- Now once this checking is done, then the trusted server decide that this member is Sybil or genuine and label them.
- If the member is genuine, then only he/she will join the group.
- Otherwise the request is rejected and labels it as ‘SYBIL’.

CONCLUSION

The idea of this survey was formed once we were considering the way to secure structured P2P overlay networks from security attacks while not a central coordination. We tend to convinced that knowing however systems have unsuccessful will facilitate United States to create systems that resist to failure. This paper provides an outline of various classes of graded P2P systems and took a significant security attacks threatening the perform of structured P2P overlay networks. We tend to classify these attacks into 2 main groups: general network attacks and specific structured P2P network attacks. Finally, we tend to shut this survey with a discussion of the various links between attacks and that we ensure that making certain that a structured P2P overlay network are going to be spare and appropriate involves the equalization of the many factors like trust, privacy and security. In lightweight of this study we are able to affirm that existing structured P2P overlay networks are still the way from a secure utilization. Thus, the event of acceptable security measures appears to be a compulsory.

REFERENCES

[1] Wallach, D. S. 2002. A survey of peer-to-peer security issues, In Proceedings of the International Symposium on Software Security (ISSS), Springer-Verlag.

[2] Yu, H. 2011. Sybil Defenses via Social Networks: A Tutorial and Survey, SIGACT News.

[3] Douceur, J. R. 2002. The Sybil attack, In Proceedings of the International Workshop on Peer To-Peer Systems (IPTPS), Springer-Verlag

[4] Castro, Druschel, P., Ganesh, A., Rowstron, A., and Wallach, D. S. 2002. Secure routing for structured peerto- peer overlay networks. In Proceedings of 5th ACM Symposium on OSDI.

[5] Levine, B. N., Shields, C. and Margolin. N. B. 2006, a survey of solutions to the Sybil attack. Tech report, University of Massachusetts, Amherst.

[6] Borisov. N, 2006. Computational puzzles as Sybil defenses, In Proceedings of the 6th IEEE International Conference on Peer-to-Peer Computing, IEEE Computer Society.

[7] Yu, H., Kaminsky, M., Gibbons, P. B. and Flaxman, A. 2006. Sybilguard: defending against Sybil attacks via social networks, In Proceedings of the ACM SIGCOMM Conference.