Study of Sybil Attack for E-Commerce In P2P Domain

Rohan Raj[1]

[1](Computer Science & Engineering , RGPV, Jabalpur, India ,rohan123@gmail.com)

Abstract—*As we Know that the term Security . Security is involve in the each and every internet related domain. Hues amount fro person are used the facilities of Internet for the various purpose , like Email , Chatting , Transition , some kind of Online Payment , and E-Commerce . Now In this survey paper I am Focused the work for E-Commerce related issue in the Peer to Peer Network Domain . This survey paper include the some cyber Security Related Information over the internet .various issue in the cyber security for the E-commerce, Introduction part of E-commerce its application and some of the security issue in the E-commerce .This paper is mainly work for the Sybil attack in the E-commerce in the Peer to peer network ,so this paper is also include the some information about the Sybil Attack , its degree, its Type over the E-Commerce . in this paper we are also make a proper prevent Technique that related to sybil attack for E-Commerce in the Peer to peer Network .*

Keywords— *Sybil Attack; E-commerce; P2P Domain;*

1. INTRODUCTION OF CYBER CRIME

Cybercrime [1] is a range of illegal digital activities targeted at organizations in order to cause harm. The term applies to a wide range of targets and attack methods. It can range from mere web site defacements to grave activities such as service disruptions that impact business revenues to e-banking frauds. The first cybercrime was noted in 1820 by Joseph-Marie Jacquard, a textile manufacturer in France which produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. In the past, India used to be a target of cyber attacks for political motivation only. Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels.

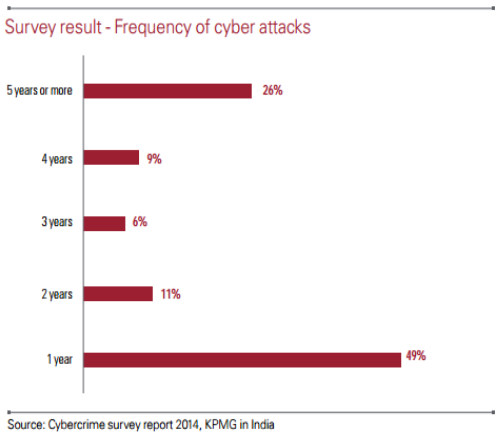

Figure 1.1 Cyber Attacks

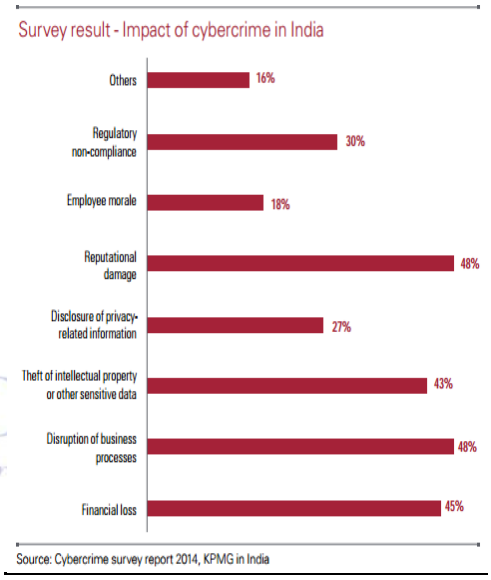

Figure 1.2 Cyber Crime in India

Cyber attacks [1] by their very nature are multi-dimensional and complex. As cybercrime progressively evolves into an organized activity, the motives of intruders are no longer limited to stealing information only, but potentially to disrupt business or conduct espionage on behalf of competing organisations. Although organisations understand the need to safeguard their IT infrastructure, intruders have often been a step ahead at exploiting new vulnerabilities in IT systems and processes of their target. Needless to say, target organisations have been found wanting when it comes to countering these cyber attacks.A cyber attack [2]is an assault by a third party via a computer against another computeror computer system, which is intended to compromise the integrity, availability or confidentiality of that computer or computer system. For example:

• A remote attack on a business's IT systems or website.

• Attacks on information held in third-party systems (for example, the company bank account).

2.INTRODUCTION

P2P networks range from communication systems like email and instant messaging to collaborative content rating, recommendation, and delivery systems such as YouTube, Gnutela, Facebook, Digg, and BitTorrent. They allow any user to join the system easily at the expense of trust, with very little validation control. P2P overlay networks are known for their many desired attributes like openness, anonymity, decentralized nature, self-organization, scalability, and fault tolerance. Each peer plays the dual role of client as well as server, meaning that each has its own control. All the resources utilized in the P2P infrastructure are contributed by the peers themselves unlike traditional methods where a central authority control is used.

3.PROBLEM DEFINITION

Peers can collude and do all sorts of malicious activities in the open-access distributed systems. These malicious behaviors lead to service quality degradation and monetary loss among business partners. Peers are vulnerable to exploitation, due to the open and near-zero cost of creating new identities. The peer identities are then utilized to influence the behavior of the system. However, if a single defective entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining the redundancy. The number of identities that an attacker can generate depends on the attacker's resources such as bandwidth, memory, and computational power.

4.SYBIL ATTACK OVERVIEW

A peer can give positive recommendation to a peer which is discovered is a Sybil or malicious peer. This can diminish the influence of Sybil identities hence reduce Sybil attack. A peer which has been giving dishonest recommendations will have its trust level reduced. In case it reaches a certain threshold level, the peer can be expelled from the group. Each peer has an identity, which is either honest or Sybil.

5.LITERATURE SURVEY

Experience with an object reputation system for peer to peer file sharing. Credence, a decentralized object reputation and ranking system for large-scale peer-to-peer filesharing networks. Credence counteracts pollution in these networks by allowing honest peers to assess the authenticity of online content through secure tabulation and management of endorsements from other peers. Our system enables peers to learn relationships even in the absence of direct observations or interactions through a novel, flow-based trust computation to discover trustworthy peers.

Footprint: Detecting Sybil attacks in urban vehicular networks. In urban vehicular networks, where privacy, especially the location privacy of anonymous vehicles is highly concerned, anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining a disproportionately large influence. In this paper, we propose a novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the appearance time at this RSU.

Detecting Sybil attacks in VANETs

Sybil attacks have been regarded as a serious security threat to Ad hoc Networks and Sensor Networks. They may also impair the potential applications in Vehicular Ad hoc Networks (VANETs) by creating an illusion of traffic congestion. In this paper, we make various attempts to explore the feasibility of detecting Sybil attacks by analyzing signal strength distribution. First, we propose a cooperative method to verify the positions of potential Sybil nodes. We use a Random Sample Consensus (RANSAC)-based algorithm to make this cooperative method more robust against outlier data fabricated by Sybil nodes. However, several inherent drawbacks of this cooperative method prompt us to explore additional approaches.

6.CONCLUSION

SybilTrust, a defense against Sybil attack in P2P e-commerce is proposed. Compared to other approaches, this approach is based on neighborhood similarity trust in a group P2P e-commerce community. This approach exploits the relationship between peers in a neighborhood setting. The results on real-world P2P e-commerce confirmed fastmixing property, hence validated the fundamental assumption behind SybilGuard's approach. Also describe defense types such as key validation, distribution, and position verification. This methods can be done at in simultaneously with neighbor similarity trust which gives better defense mechanism.

Reference

[1] J. Douceur, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[2] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close: Incorporating trust into social network-based Sybil defenses," in Proc. IEEE Int. Conf. Comput. Commun., 2011, pp. 1–9.

[3] K. Walsh and E. G. Sirer, "Experience with an object reputation system for peer to peer filesharing," in Proc. 3rd USENIX Conf. Netw. Syst. Des. Implementation, 2006, vol. 3, pp. 1–14.

[4] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil attacks in urban vehicular networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[5] B. Yu, C. Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," J. Parallel Distrib. Comput., vol. 73, no. 3, pp. 746–756, Jun. 2013.

[6] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, "Optimal Sybil-resilient peer admission control," in Proc. IEEE Int. Conf. Comput. Commun., 2011, pp. 3218–3226.

[7] K. Wang, M. Wu, and S. Shen, "Secure trust-based cooperative communications in wireless multi-hop networks," in Communications and Networking J. Peng, Ed., Rijeka, Croatia: InTech, Sep. 2010 ch. 18, pp. 360–378,.

[8] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A nearoptimal social network defense against Sybil attack," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 3–17, Jun. 2010.