International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Blocking Misbehaving User & Activities in Social Network

Rashmi Gourkar[1], Garima Singh[2]

PG. Department of Computer Science and Engineering, Wainganga College of Engineering and Management

Abstract: ***Social network security and privacy issues result from the astronomical amounts of information these sites process each day. Features that invite users to participate in messages, invitations, photos, open platform applications and other applications are often the venues for others to gain access to a user's private information.Social networking has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms, storing and sharing a wealth of personal information [1]. This information, as well as the possibility of contacting thousands of users, also attracts the interest of cyber criminals. For example, cybercriminals might exploit the implicit trust relationships between users in order to make the malicious website. cybercriminals might find personal information valuable for identity theft or to drive targeted spam campaigns [2]. In this paper, we detect & block the misbehaving user in social network by using nymble unique token provided by nymble manager and pseudonym manager to which detect and block to misuse or spam things.***

Keywords: Nymble, Pseudonym, Nymbles manager, Pseudonym manager

1. Introduction

Social networking sites vary in the levels of privacy offered. For some social networking sites like Facebook, providing real names and other personal information is encouraged by the site (onto a page known as a „Profile„)[1] These information usually consist of birth date, current address, and telephone number(s) which is easily accessible. Here we implemented to identify the following features. Misbehaving users who are using Social network. Pseudonymous credential systems. User will use pseudo names.

- Anonymous Authentication.
- Subjective Blacklisting.
- Rate limited anonymous & social connections.
- Revolution Audit ability.

Users are often the targets as well as source of information in social networking. Users leave digital imprints during browsing of social networking sites or services. It has been identified from few of online studies conducted, that users trust websites and social networking sites. These results show that the interaction of trust and privacy concern in social networking sites is not yet understood to a sufficient degree to allow accurate modeling of behavior and activity[5]. The results of the study encourage further research in the effort to understand the development of relationships in the online social environment and the reasons for differences in behavior on different sites. The large user base of these social networks has attracted the attention of cyber-criminals. According to a study from 2008, 83% of social network users received at least one unwanted message on such networks that year. Also, largescale malware campaigns have been carried out over social networks and previous work has shown that spam, and malware are real threats on social networking.

2. Our Solution

We present a secure system called Nymble, unique token which provides all the following properties anonymous and social authentication, backward unlink & link ability, subjective blacklisting, fast authentication speeds, rate limited anonymous connections, revocation audit ability (where users can verify whether they have been blacklisted), and also addresses. We now present a high-level overview of the nymble system, and defer the entire protocol description and security analysis to subsequent sections[6]. The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM direct. We assume the PM has knowledge about transaction on dependable and secure computing.

A user‟s requests to the NM (nymble manager) are therefore pseudonymous, and nymbles are generated using the user‟s pseudonym and the server‟s identity. These nymbles are thus specific to a particular user-server pair. Nevertheless, as long as the PM and the NM do not collude, the Nymble system cannot identify which user is connecting to what server; the NM knows only the pseudonym-server pair, and the PM knows only the user identity-pseudonym pair [9]. To provide the requisite cryptographic protection and security properties, the NM encapsulates nymbles within nymble tickets. Servers wrap seeds into linking tokens and therefore we will speak of linking tokens being used to link future nymble tickets. The importance of these constructs will become apparent as we proceed. Nymble aims for four security goals. We provide informal definitions here a detailed formalism can be found in our technical report which explains how these goals must also resist coalition attacks. We design the following algorithms.

1) Start the algorithms
2) User Register with Pseudonym Manger to get Pseudonym (unique token)
3) Request to Nymble Manger to get Nymble to access main Server
4) If the User have already taken Nymble within 24 hours then reject request else give Nymble.
5) Request to main server using nymble
6) If user behaviour is classified as Misbehaviour then block the user and add him in Blacklist and inform NymbleManger
7) End.

IP-address blocking by picking IP addresses as the resource for limiting the Sybil attack, our current implementation closely mimics IP-address blocking employed by Internet services. There are, however, some Inherent limitations to using IP addresses as the scarce resource. If a user can obtain multiple addresses she can circumvent both nymble-based and regular IP-address Blocking [10]. Subnet-based blocking alleviates this problem, and while it is possible to modify our system to support subnet-based blocking. prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else‟s misbehavior. This property assumes each user has a single unique identity [12]. When IP addresses are used as the identity, it is possible for a user to "frame" an honest user who later obtains the same IP address. Non-frameability holds true only against attackers with different identities (IP addresses). A user is legitimate according to a server if she has not been blacklisted by the server, and has not exceeded the rate limit of establishing Nymble-connections. Honest servers must be able to differentiate between legitimate and illegitimate users.

3. Conclusion

We have proposed and built a comprehensive credential system called Nymble, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services. We hope that our work will increase the mainstream acceptance of anonymizing networks such as Tor, which has thus far been completely blocked by several services because of users who abuse their anonymity. Issues relating to privacy and employment are becoming a concern with regards to social networking sites. As of 2008, it has been estimated by CareerBuilder.com that one in five employers search social networking sites in order to screen potential candidates (increasing from only 11% in 2006).for the majority of employers, such action is to acquire negative information about candidates. For example, 41% of managers considered information relating to candidates‟ alcohol and drug use to be a top concern.

References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In CRYPTO, LNCS 1880, pages 255–270. Springer, 2000.
[2] G. Ateniese, D. X. Song, and G. Tsudik. Quasi-Efficient Revocation in Group Signatures. In Financial Cryptography, LNCS 2357, pages 183–197. Springer, 2002.
[3] M. Bellare, R. Canetti, and H. Krawczyk. Keying Hash Functions for Message Authentication. In CRYPTO, LNCS 1109, pages 1–15. Springer, 1996.
[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A Concrete Security Treatment of Symmetric Encryption. In FOCS, pages 394–403, 1997.
[5] M. Bellare and P. Rogaway. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In Proceedings of the 1st ACM conference on Computer and communications security, pages 62–73. ACM Press, 1993.
[6] M. Bellare, H. Shi, and C. Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In CT-RSA, LNCS 3376, pages 136–153. Springer, 2005.
[7] D. Boneh and H. Shacham. Group Signatures with Verifier-Local Revocation. In ACM Conference on Computer and Communications Security, pages 168–177. ACM, 2004.
[8] S. Brands. Untraceable Off-line Cash in Wallets with Observers (Extended Abstract). In CRYPTO, LNCS 773, pages 302–318.
[9] E. Bresson and J. Stern. Efficient Revocation in Group Signatures. In Public Key Cryptography, LNCS 1992, pages 190–206. Springer, 2001.
[10] J. Camenisch and A. Lysyanskaya. An Efficient System for Nontransferable Anonymous Credentials with Optional Anonymity Revocation. In EUROCRYPT, LNCS 2045, pages 93–118. Springer, 2001.
[11] J. Camenisch and A. Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In CRYPTO, LNCS 2442, pages 61–76. Springer, 2002.
[12] J. Camenisch and A. Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In CRYPTO, LNCS 3152, pages 56–72. Springer, 2004.
[13] D. Chaum. Blind Signatures for Untraceable Payments. In CRYPTO, pages 199–203, 1982.
[14] D. Chaum. Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms. In AUSCRYPT, LNCS 453, pages 246–264. Springer, 1990.
[15] D. Chaum and E. van Heyst. Group Signatures. In EUROCRYPT,