ISSN 2349-9842, Volume 1, Issue 1, March 2014

International Journal of Innovative Trends and Emerging Technologies

RECOGNITION AND ANTICIPATION OF UNCONSTITUTIONAL USERS IN PRIVATE NETWORK

M.KALAISELVI
Department of Computer science and Engineering, Dhaanish Ahmed College of Engineering
E-mail :kalai31selvi@gmail.com

***Abstract*--private networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of those networks has been limited by users employing this anonymity for abusive purposes such as defacing popular Web sites. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but the blocking IP addresses is not practical if the abuser routes through an private network. As a result, administrators block all known exit nodes of private networks, denying anonymous access to misbehaving and behaving users the same. To address this problem, we present Nymble, a system in which servers can "blacklist" misbehaving users, thus blocking users without compromising their anonymity. Thus this system is agnostic to different servers' definitions of misbehavior— servers can blacklist users for whatever reason, and the privacy of black listed users is maintained.**

Key words: Anonymous, privacy, revocation, blacklisting.

1.INTRODUCTION

Private networks such as Tor [18] route traffic through independent nodes in separate administrative domains to hide a client's IP address. Unfortunately, some users may misuse such networks—under the cover of ambiguity, users have repeatedly defaced popular Web sites such as Wikipedia. while Website administrators cannot blacklist individual malicious users' IP addresses, they black list the entire anonymizing network. This measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users. In other words, a few "bad apples" can spoil the fun for all. (This happened repeatedly with Tor.1)There are several solutions to this problem, with each providing some degree of accountability. In pseudonymous credential systems [14], [17], [13], [18], users log into Web sites using pseudonyms, which can be added to a black list if a user misbehaves. But this approach results in pseudonymity for all users and weakens the anonymity provided by the anonymizing network.

Anonymous credential systems [10], [12] employ group signatures. Basic group signatures [1], [6], [15] allow servers to revoke a misbehaving user's anonymity by complaining to the group manager. Each servers must query the group manager for every authentication, thus, lacks scalability. Traceable signatures [16] allow the group manager to release a rapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlinkability [20] that we desire, somewhere a user accesses before the complaint remain unidentified. Backward unlinkability allows for what we call subjective black listing, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In disparity, approaches without backward unlinkability need to pay careful attention to when and why the user must have all their connections linked, as well as users must worry about whether their behaviors will be judged fairly.

Subjective black listing is also better suited to servers such as Wikipedia, where misbehaviors edits to a Webpage, are hard to describe in mathematical terms. In some systems, misbehavior can definitely be defined precisely. For instance, double spending of an "e-coin" is considered a misbehavior in anonymous e-cash systems [8], [13], following which the offending user is deanonymized. Unfortunately, those systems work for only narrow definitions of misbehavior—it is difficult to map more complex notions of misbehavior onto "double spending" or related approaches [12]. With dynamic accumulators [11], [3], a revocation operation results in a new accumulator and public parameters for the group, and all further existing users credentials must be updated, makes it impractical. Verifier-local revocation (VLR) [2], [7], [9] fixes this shortcoming by requiring the server ("verifier") to perform only local updates during revocation. Regrettably, VLR requires heavy computation at the

server that is linear in the size of the blacklist. For example, for a black list with 1,000 entries, each authentication would take tens of seconds, to a prohibitive cost in practice. In disparity, our scheme takes the server about one millisecond per authentication, which is several thousand times quicker than VLR. We believe these low down overheads will incentivize servers to adopt such a solution when weighed against the potential benefits of anonymous publishing

A. Our Solution

We present a secure system called Nymble, that provides all the subsequent properties: anonymous authentication, backward un link ability, subjective black listing, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack [19] to make its exploitation practical. In Nymble, the users acquire an ordered collection of nymbles, a particular type of pseudonym, to connect to Websites. Without supplementary information, these nymbles are computationally tough to link,4 and therefore, using the stream of nymbles simulates anonymous access to services. Web sites, however, can black list users by obtaining a seed for a particular nymble, agree them to link future nymbles from the identical user—those used before the complaint remain un linkable. Servers can therefore black list anonymous users without knowledge of their IP addresses while allowing behaving users to connect incognito. This system ensures that users are aware of their blacklist status before they present a nymble, furthermore detach immediately if they are black listed. Although our work applies to anonymizing networks in general, we consider Tor for purposes of description. In fact, many number of anonymizing networks can rely on the same Nymble system, black listing anonymous users regardless of their anonymizing network(s) of choice.

B. Contribution of this paper

This paper makes the subsequent contributions:

Blacklisting anonymous users. We provide a means by which servers can blacklist users of an anonymizing network while maintaining their privacy.

Practical performance. Our protocol makes use of inexpensive symmetric cryptographic operations to significantly outperform the alternatives.

Open-source implementation. With the goal of contributing a effective system, we have built an open-source implementation of Nymble, which is in public. We provide performance statistics to show that our system is indeed practical.

Some of the authors of this paper have published two anonymous authentication schemes, BLAC [13] and PEREA 14], which eliminate the need for a trusted third party to revoke users. While BLAC and PEREA provide better privacy by eliminating the TTP, Nymble provides validation rates that are several orders of magnitude faster than BLAC and PEREA. Nymble hence represent a practical solution for blocking misbehaving users of anonymizing networks. We note that an extended description of this paper is available as a technical report [16]. Reminder that users interact with the NM and servers though the anonymizing network

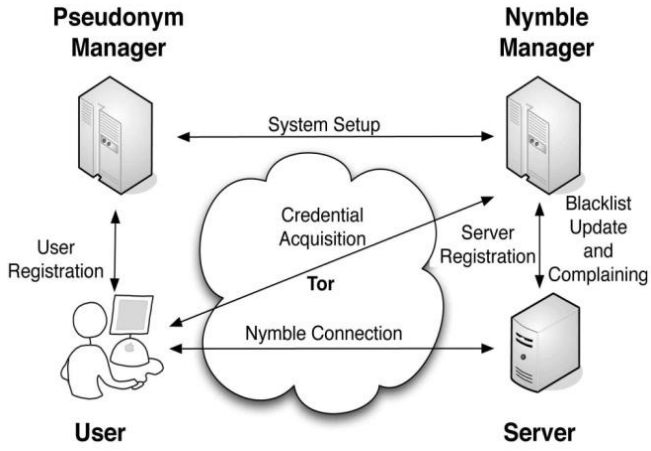

Fig. 1. The Nymble system architecture showing the various modes of interaction.

2 AN OVERVIEW TO NYBLE

This paper presents a sophisticated summary of the Nymble system, and defers the entire protocol description and security analysis to subsequent sections.

A. Resource-Based Blocking

To limit the number of identities a user can obtain (called the Sybil attack [19]), the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. For instance, we have used IP addresses as the resource in our implementation, but our design generalizes to other resources such as email addresses, trusted hardware, and identity certificates. We deal with the practical issues related with resource-based blocking in Section 8, and recommend other alternatives for resources.

We do not claim to solve the Sybil attack. This difficulty is faced by any credential system [19], [17], and we suggest some promising approaches based on

resource-based blocking since we aim to create a real-world deployment.

B. The Pseudonym Manager

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user have to bond to the PM directly (i.e., not through a known anonymizing network), as shown in Figure. We believe the PM has knowledge about Tor routers, for instance, and can ensure that users are communicating with it straightforwardly. Pseudonyms are deterministically chosen based on the controlled resource, ensure that the identical pseudonym is always issued for the identical resource. Note that the user does not disclose what server he or she intends to connect to, and the PM's responsibilities are limited to mapping IP addresses (or other resources) to pseudonyms. As we will explicate, the user contacts the PM only once per linkability window (e.g., once a day).

C. The Nymble Manager

After obtaining a pseudonym from the PM, the user ties to the Nymble Manager (NM) through theanonymizing network, and requests nymbles for access to a particular server (such as Wikipedia). A users requests to the NM are therefore pseudonymous and nymbles are generated using the user's pseudonym and the server's identity. These nymbles are thus efinite to a particular user-server pair. however, as long as the PM and the NM do not work together, the Nymble system cannot identify which user is connecting to what server, the NM identifies only the pseudonym server pair, and the PM identifies only the user identity pseudonym pair.

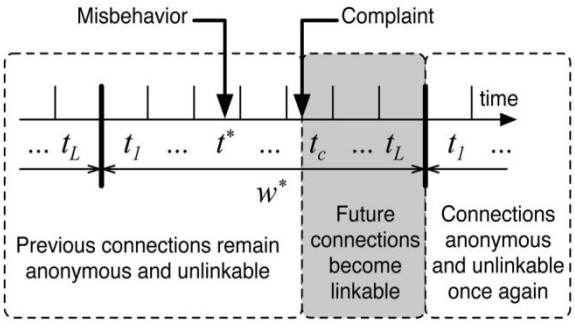

Fig. 2. The life cycle of a mischievous user. If the server complains in time period of tc about a user's connection in to the user becomes linkable starting in t_c. The complaint in t_c can include nimble tickets from only t_c_1 and earlier.

To provide the requisite cryptographic protection and security properties, the NM summarizes nymbles within nymble tickets. Servers enfold seeds into linking tokens, and hence, we will speak of linking tokens being used to link future nymble tickets. The significance of these constructs will become apparent as we proceed.

D. Blacklisting a User

If a user misbehaves, the server may link any future connection from this user within the current link ability window (e.g., the same day). Consider the Fig. 2 as an example: A user tie and misbehaves at a server during time period t_ within link ability window w. The server afterwards detects this misbehavior and complains to the NM in time period tc ($t_ < t_c$ _ t_L) of the same link ability window w. As part of the grumble, the server presents the nimble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then capable to link future connections by the user in time periods tc; tc þ 1; . . . ; t_L of the identical linkability window w_ to the complaint. Thus, once the server has complained about a user, that user is black listed for the rest of the day. Note that the user's connections in t_1; t_2; . . . ; t_; t_ þ 1; . . . ; tc remains unlinkable (i.e., including those since the misbehavior and until the time of complaint). Although misbehaving users can be blocked from making connections in the prospect, the users precedent connections remain unlinkable, therefore providing backward unlink ability and subjective blacklisting.

3 DISCUSSIONS

*A. **IP-address blocking**:*

By picking IP addresses as the resource for limiting the Sybil attack, this current implementation closely mimics IP-address blocking employed by Internet services. There are, still, some inherent limitations to using IP addresses as the sparse resource. If a user can obtain multiple addresses, it can avoid both nymble-based and regular IP-address blocking. Subnet based blocking improves this problem, and while it is feasible to modify our system to support subnet based blocking, new privacy challenges will appear; a more thorough description is left for future work.

B. Other resources:

Users of anonymizing networks would be reluctant to use resources that directly reveal their identity (e.g., passports). Email addresses could provide more privacy, but provide weak black listability guarantees because users can easily create new email addresses. Other feasible resources include

client puzzles [15] and e-cash, where users are required to perform a certain amount of computation or pay money to acquire a credential. These ways would limit the number of credentials obtained by a single individual by raising the cost of acquiring credentials.

D. Server-specific likability widows

An improvement would be to provide support to vary T and L for different servers. As illustrated, our system does not support varying linkability windows, but does sustain varying time periods. This is because the PM is not aware of the server the user wishes to connect to, yet it must issue pseudonyms specific to a linkability window. We do make a note of that the use of resources such as client puzzles or e-cash would eliminate the need for a PM, and users might obtain Nymbles directly from the NM. In that casing, server-specific linkability windows could be used.

E. Side-channel attacks

While our current implementation does not fully protect against side-channel attacks, we mitigate the risks. We have implemented various algorithms in a way that their execution time leaks little information that cannot already be inferred from the algorithm's output. Also, while a confidential channel does not hide the size of the communication, we have created the protocols so that each kind of protocol message is of the same size regardless of the identity or current legitimacy of the user.

4 CONCLUSIONS

We have proposed and built a comprehensive credential system called Nymble, which can be used to insert a layer of accountability to any publicly known anonymizing network. Servers can black list misbehaving users while maintaining their privacy and it show how these properties can be attained in a way that is practical, proficient, and perceptive to the needs of both users and services.

Thus it is evident 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.

REFERENCES:

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature, Scheme," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 255-270, 2000.

[2] G. Ateniese, D.X. Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.

[3] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 1-15, 1996.

[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proc. Ann. Symp. Foundations in Computer Science (FOCS), pp. 394-403, 1997.

[5] M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security, pp. 62-73, 1993.

[6] M. Bellare, H. Shi, and C. Zhang, "Foundations of Group Signatures: The Case of Dynamic Groups," Proc. Cryptographer's Track at RSA Conf. (CT-RSA), Springer, pp. 136-153, 2005.

[7] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.

[8] S. Brands, "Untraceable Off-Line Cash in Wallets with Observers (Extended Abstract)," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 302-318, 1993.

[9] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, 2001.

[10] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non- Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.

[11] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002.

[12] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

[13] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), pp. 199-203, 1982.

[14] D. Chaum, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-

264, 1990.
[15] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
[16] C. Cornelius, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," Technical Report TR2008-637, Dartmouth College, Computer Science, Dec. 2008.
[17] I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.
[18] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303-
[19] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002.
[20] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Schemes," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 263-275, 1989.

M.KALAISELVI received her Bachelor of technology degree in Information Technology from Anna University, Master of Engineering degree in computer Science and Engineering from Anna University. Currently she is serving for AIAIE's.