ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Nymble: Restricting Suspicious Users in Anonymizing Networks using Nymbles

Ashwini Hiwale [1], A P Kankale [2]

M.E. Student, Department of Computer Science and Engineering, Rajshri Shau Engineering College, Buldana, Maharashtra, India[1]

HOD, Department of Computer Science and Engineering, Rajshri Shau Engineering College, Buldana, Maharashtra, India [2]

ABSTRACT: Anonymizing networks such as re-route a user's traffic between several nodes in different domains. Since these nodes are operated independently, users are able to trust the anonymizing network to provide anonymity. Developed software that would hide IP address, outlined a security protocol that uses resource constrained trusted hardware to facilitate anonymous IP-address blocking in anonym zing networks such as Tor. Website administrators routinely rely on IP-address blocking for disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an anonymizing network. As a result, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike. To address this problem, we present Nymble, a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. Our system is thus agnostic to different servers' definitions of misbehaviour servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

KEYWORDS: anonymous blacklisting, privacy, revocation, misbehaviour servers.

I. INTRODUCTION

Anonymous authentication, backward unlink ability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation audit ability (where users can verify whether they have been blacklisted). In this system we aim to generate nymbles, which are not easy to connect, however a stream of these nymbles assures we a simulation to anonymous access. Here we provide a means where the website administrator can block user without knowing his IP address (i.e. through pseudonym generated: which is a random secret identity with the pseudonym manager) without hindering the remaining network. User also has his complete privacy without having to compromise until he behaves.

Anonymous credential systems such as Camenisch and Lysyanskaya's systems use group signatures for anonymous authentication Basic group signatures allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. In these schemes, servers must query the group manager for every authentication, and this lack of scalability makes it unsuitable for our goals. Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlink ability that we desire, where a user's accesses before the complaint remain anonymous. Backward unlink ability allows for what we call subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, approaches without backward unlink ability need to pay careful attention to when and why a user must have all their connections linked, and users must also worry about whether their (mis)behaviors will be judged fairly. Subjective blacklisting is also better suited to servers such as Wikipedia, where misbehaviours such as questionable edits to a webpage, are hard to define in mathematical terms. In some systems, misbehaviour can indeed be defined precisely. For instance, double-spending of an "e-coin" is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

considered misbehaviour in anonymous e-cash systems following which the offending user is deanonymized. Unfortunately, such systems work for only narrow definitions of misbehaviour — it is difficult to map more complex notions of misbehaviour onto "double spending" or related approaches. With dynamic accumulators, a revocation operation results in a new accumulator and public parameters for the group, and all other existing users' credentials must be updated, and it is thus difficult to manage in practical settings. Verifier-local revocation (VLR) fixes this shortcoming by requiring the server ("verifier") to perform only local updates during revocation. Unfortunately, VLR requires heavy computation at the server that is linear in the size of the blacklist. For example, for a blacklist with 1,000 entries, each authentication would take tens of seconds, 2 a prohibitive cost in practice. In contrast, our scheme takes the server about one millisecond per authentication, which is several thousand times faster than VLR. Lastly, any practical deployment of a credential scheme must address the Sybil attack, where a malicious user can potentially assume multiple identities.

II. RELATED WORK

Anonymous credential systems like Camenisch and Lysyanskaya's use group signatures for anonymous authentication, wherein individual users are anonymous among group of registered users. No revocable group signatures such as Ring signatures provide no accountability and thus do not satisfy our needs to protect servers from misbehaving users. Basic group signatures allow revocation of anonymity by no one except the group manager. As only the group manager can revoke a user's anonymity, servers have no way of linking signatures to previous ones and must query the group manager for every signature; this lack of scalability makes it unsuitable for our goals. Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward anonymity that we desire, where a user's accesses before the complaint remain anonymous. Specifically, if the server is interested in blocking only future accesses of bad users, then such reduction of user anonymity is unnecessarily drastic.. And misbehaving users should be blocked from making further connections after a complaint. In some systems, misbehaviour can be defined precisely. For instance, double-spending of an e-coin is considered misbehaviour in anonymous electronic cash systems. Likewise, compact e-cash, k-times anonymous authentication and periodic n times anonymous authentication deem a user to be misbehaving if she authenticates—too many times. In these cases, convincing evidence of misbehaviour is easily collected and fair judgment of misbehaviour can be ensured. While such approaches can encourage certain kinds of fair behaviour in anonymzing. It is difficult to map more complex notions of misbehaviour onto ―double spending or related approaches. It may be difficult to precisely define what it means to ―deface a webpage and for Wikipedia to prove to a trusted party that a particular webpage was defaced. How can the user be sure these ―proofs are accurate and fairly judged? Can we avoid the problem of judging misbehaviour entirely? In this paper we answer affirmatively by proposing a system that does not require proof of misbehaviour. Websites may complain about users for any reason; our system ensures users are informed of complaints against them, thus ―making everybody happy—except, of course, the misbehaving users, who remain anonymous but are denied access.

III. SYSTEM OVERVIEW

We now present a high-level overview of the Nymble system, and defer the entire protocol description and security analysis to subsequent sections.

A. *RESOURCE-BASED BLOCKING*

Our system provides servers with a means to block misbehaving users of an anonymizing network. Blocking a particular user, however, is a formidable task since that user could possibly acquire several identities (called the Sybil attack). The Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. For example, we have used IP addresses as the resource in our implementation, but our scheme generalizes to other resources such as email addresses, identity certificates, trusted hardware, and so on. We note that if two users can prove access to the same resource (e.g., if an IP address is reassigned), they will obtain the same stream of nymbles. We will

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

address the practical issues related with resource-based blocking, along with other examples of resources that would be useful in limiting the Sybil attack. At this point we emphasize that creating Sybil-free credentials is an independent research topic in itself and we do not claim to solve the Sybil attack in this paper. This problem is faced by any credential system 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 is required to connect to the PM directly (i.e., not through a known anonymizing network).We assume the PM has knowledge about Tor routers, for example, and can ensure that users are communicating with it directly. Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonym is always issued for the same resource. Note that the user does not disclose what server he or she intends to connect to, and therefore the user's connections are anonymous to the PM. The PM's duties are limited to mapping IP addresses (or other resources) to pseudonyms. As we will explain, the user contacts the PM only once per likability window (e.g., once a day).

C. THE NYMBLE MANAGER

After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) through the anonymizing network, and requests nymbles for access to a particular server (such as Wikipedia). Nymbles are generated using the user's pseudonym and the server's identity. The user's connections, therefore, are pseudonymous to the NM (as long as the PM and the NM do not collude) since the NM knows only the pseudonym-server pair, and the PM knows only the IP address-pseudonym pair. Note that due to the pseudonym assignment by the PM, nymbles are bound to the user's IP address and the server's identity. To provide the requisite cryptographic protection and security properties (e.g., users should not to be able to fabricate their own nymbles), 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.

D. *TIME*

Nymble tickets are bound to specific time periods. As illustrated in Figure 1, in our system time is divided into likability windows of duration W, each of which is split into L time periods of duration T (i.e., W = L∗ T). We will refer to time periods and likability windows chronologically as t1, t2,. . . tL and w1, w2, . . . respectively. While a user's access within a time period is tied to a single nymble ticket, the use of different nymble tickets across time periods grants the user anonymity between time periods — smaller time periods provide users with higher rates of anonymous authentication, and likewise longer time periods rate-limit the number of misbehaviours from a particular user before he or she is blocked. For example, T could be set to 5 minutes, and W to 1 day (and thus L = 288). The linkability window serves two purposes — it allows for dynamism since resources such as IP addresses can get reassigned to different well-behaved users, making it undesirable to blacklist such resources indefinitely, and it ensures forgiveness of misbehaviour after a certain period of time

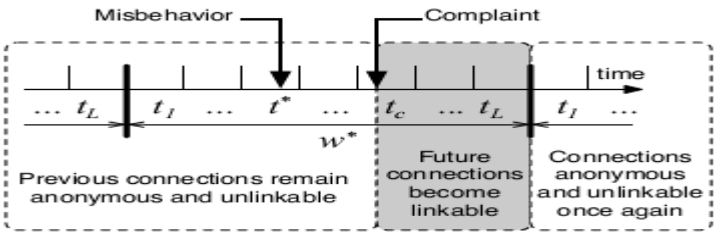

Figure 1: The life cycle of a misbehaving user.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

If the server complains in time period tc about a user's connection in t *, the user becomes linkable starting in tc. Note that the complaint in tc can include nymble tickets from only tc-1 and earlier linkability window and time period. Time-synchronization protocols such as NTP reduce but do not eliminate clock skews. Nymble does not attempt to defend against remote device-fingerprinting at-tacks, which attempt to reduce the anonymity of users by, e.g., inferring their clock skews.We leave such defences to future work

E. ***BLACKLISTING A USER***

If a user misbehaves, the server may link any future connection from this user within the current linkability window (e.g., the same day). Consider Figure 2 as an example: A user connects and misbehaves at a server during time period t * within linkability window w * . The server later detects this misbehaviour and complains to the NM in time period tc (t * < tc = t L) of the same linkability window w * . As part of the complaint, the server presents the nymble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the user in time periods tc, tc + 1, . . . , t L of the same linkability window w * to the complaint. Therefore, users are blacklisted for the rest of the day, for example (the linkability window), once the server has complained about that user. Note that the user's connections in t 1 , t 2 , . . . , t * , t * + 1, . . . , tc remain unlink able (i.e., including those since the misbehaviour and until the time of complaint). Even though misbehaving users can be blocked from making connections in the future, the users' past connections remain unlink able. This property allows the NM to be agnostic of servers' complaints; servers can subjectively judge users for any reason because users' privacy is maintained. We now describe how users are notified of their blacklisting status.

F. ***NYMBLE-AUTHENTICATED CONNECTION:***

Blacklist ability assures that any honest server can indeed block misbehaving users. Specifically, if an honest server complains about a user that misbehaved in the current linkability window, the complaint will be successful and the user will not be able to? nymble-connect? i.e., establish a Nymble-authenticated connection, to the server successfully in subsequent time periods of that linkability window. Rate -limiting assures any honest server that no user can successfully nymble-connect to it more than once within any single time period. Non-frame ability guarantees that any honest user who is legitimate according to an honest server cans nymble -connect to that server. This prevents an attacker from framing a legitimate honest user, e.g., by getting the user blacklisted for someone else's misbehaviour. This property assumes each user has a single unique identity. 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-frame ability 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.

Anonymity protects the anonymity of honest users, regardless of their legitimacy according to the (possibly corrupt) server; the server cannot learn any more information beyond whether the user behind (an attempt to make) a nymble-connection is legitimate or illegitimate

G. ***NOTIFYING THE USER OF BLACKLIST STATUS***

Users who make use of anonymizing networks expect their connections to be anonymous. If a server obtains a seed for that user, however, it can link that user's subsequent connections (we emphasize that the user's previous connections remain anonymous to the server). It is of utmost importance, then, that users be notified of their blacklisting status before they present a nymble ticket to a server. In our system, the user can download the server's blacklist and verify whether she is on the blacklist. If so, the user disconnects immediately (the server learns that "some user disconnected probably because he or she has been blacklisted"). Since the blacklist is cryptographically signed by the NM, the authenticity of the blacklist is easily verified if the blacklist was updated in the current time period (only one update to the blacklist per time period is allowed). If the blacklist has not been updated in the current time period, the NM provides servers with "daisies" every time period so that users can verify the freshness of the blacklist ("blacklist from time period t old is fresh as of time period t now"). As we will discuss later, these daisies are elements of a hash chain, and provide a lightweight alternative to digital signatures. Using digital signatures and daisies, we thus

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

ensure that race conditions are not possible in verifying the freshness of a blacklist. A user is guaranteed that he or she will not be linked if the user verifies the integrity and freshness of the blacklist before sending his or her nymble ticket.

IV. RESULTS AND PROPOSED SYSTEM

We present a secure system called Nymble, which provides all the following properties: anonymous authentication, backward unlink ability, subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation audit ability Without additional information, these nymbles are computationally hard to link, and hence using the stream of nymbles simulates anonymous access to services. Websites, however, can blacklist users by obtaining a seed for a particular nymble, allowing them to link future nymbles from the same user — those used before the complaint remains unlink able. Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. In fact, any number of anonymizing networks can rely on the same Nymble system, blacklisting anonymous users regardless of their anonymizing network(s) of choice

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 workable system, we have built an open source implementation of Nymble, which is publicly available. I provide performance statistics to show that our system is indeed practical.

Advantages:

1. Intends to bind identity of an anonymous user to a pseudonym, generated from user's IP address. This idea enables a server to complain about misbehaviour of a user and blacklist his future tickets.
2. Honest users remain anonymous, &blacklist futures connections of particular users and their requests remain unlink able.
3. All connections of a blacklisted user before the complaint will remain anonymous.
4. A user can check whether he is blacklisted or not at the beginning of a connection.
5. Users are aware of their blacklist status before accessing a service.
6. Servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

A. MATHEMATICAL MODEL :

Pseudonym Creation

Equation:

$$(a)\quad f(x)=\sum_{i=0}^{i=n} U_i$$

$$(b)\quad Ps= P\ (f(x))$$

Where

- f(x) is function to concatenate all string of the field from the user profile
- Ui -> each profile attributes
- Ps-> Pseudonym
- P(f(x)) -> Random Function to calculate Pseudonym

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Algorithm:

Input: Set U ={ u1,u2,u3.....un}
Output: pseudonym (Ps)
Step 0: Get the User Profile attribute set U
Step 1: Convert all the attributes to String type
Step 2: Concatenate all the String to get a single String
Step 3: Get the auto incremented User ID as I
Step 4: x=ID mod 7
Step 5: for i=0 to String length
Step 6: Fetch xth character from the String
Step 7: Continue till 7 characters are selected
Step 8: concatenate all the 7 characters
Step 9: return Pseudonym

ATTACKS: A={A1,.....An} is Attack Set

A1 Attack

Equation:

$$f(A1) \Rightarrow UP_{data} > lim$$

Where

- f(A1) is function to identify uploading excess amount of data attack
- UP_{data} -> Uploading data
- Lim -> Limits

Algorithm:

Input: User Uploading data UPdata, threshold size (lim)
Output: User Blocked State
Step 0: Get the User data on the web server
Step 1: Get the Current of the file size as C_{lim}
Step 2: if(C_{lim} > lim)
Step 3: Tag user as misbehavior user
Step 4: Get Pseudonym
Step 5: Add Pseudonym in blocked list
Step 6: Update User's state
Step 7: return user state

A2 Attack

Equation:

$$f(A2) \Rightarrow U_{data} \notin U_i$$

Where

- f(A2) is function to identify DMA attack
- U_{data} -> Users Uploaded data
- U_i ->Respective User

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Algorithm:

Input: User accessing data Udata

Output: User Blocked State

Step 0: Allow User to access data on the web server

Step 1: Get the user accessed data name as U_{data}

Step 2: if U_{data} does not belongs to him

Step 3: Tag user as misbehavior user

Step 4: Get Pseudonym

Step 5: Add Pseudonym in blocked list

Step 6: Update User's state

Step 7: return user state

A4 Attack

Equation:

$$f(A4) \Rightarrow U_{pwd} \notin U_i$$

Where

- f(A4) is function to identify Password attack
- U_{pwd} -> Users Password
- U_i ->Respective User

Algorithm:

Input: User password U_{pwd} and U_{name}

Output: User Blocked State

Step 0: Allow User to login in his account

Step 1: Get the user's credential like U_{name} and U_{pwd}

Step 2: if U_{pwd} does not belongs to U_{name}

Step 3: then warn user for 3 times

Step 4: Reset Password

Step 5: Mail New Password to Original user

Step 6: Get Pseudonym

Step 7: Add Pseudonym in blocked list

A5 Unblocking User

Equation:

$$f(A5) \Rightarrow (t_c - t_b) > T$$

Where

- f(unb) is function to identify unblocking user
- t_c -> Current time
- t_b -> blocked time
- T-> threshold time

Algorithm:

Input: Blocked time as t_b, Current time as t_c and Threshold time as T

Output: Unblocked Blocked State

Step 0: Get tb and t_c and T

Step 1: if $(t_c - t_b) > T$

Step 2: Get Pseudonym

Step 3: Add Pseudonym in unblocked list

Step 4: Update User's state

Step 5: return user state

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

V. 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. Our new design is not only scalable and robust, but also securer under various types of attacks. A new system is proposed that adds an additional layer of security to the anonymous networks.

In Our system we tried to blacklist user's activities, we have considered several types of attacks. This system is used to block the misbehaving users in anonymizing networks. It automatically finds the misbehaving user and blacklists them without affecting their privacy and anonymity. This adds one more layer of security to the system. The proposed method motivates the need for dynamic forgiveness and security in anonymous networks and this system will increase the acceptance of anonymous networks that is blocked by several services because of users who misuse their anonymity

REFERENCES

Stefan Brands. Untraceable off-line cash in wallets with observers (extended abstract). In Douglas R. Stinson, editor, CRYPTO, Volume 773 of LNCS, pages 302–318. Springer, 1993.

Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, CT-RSA, volume 3376 of LNCS, pages 136–153.Springer, 2005.

[1] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik.A practical and provably secure coalition-resistant group signature scheme. In Mihir Bellare, editor, CRYPTO, volume1880 of LNCS, pages 255–270. Springer, 2000.

[2] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In Eli Biham, editor, EUROCRYPT, volume 2656 of LNCS, pages 614–629. Springer, 2003.

[3] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and MiraMeyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. InAri Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, ACM Conference on Computer and Communications Security, pages 201–210. ACM, 2006.

[4] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya .Compact e-cash. In Ronald Cramer, editor, EUROCRYPT, volume 3494 of LNCS, pages 302–321. Springer, 2005.

[5] Paul F. Syverson, Stuart G. Stubblebine, and David M. Goldschlag.Unlinkable serial transactions.In Rafael Hirschfeld, editor, Financial Cryptography, volume 1318 of LNCS, pages39–56.Springer, 1997.

[6] Isamu Teranishi, Jun Furukawa, and Kazue Sako.k-times anonymous authentication. In Pil Joong Lee, editor, ASIACRYPT, volume 3329 of LNCS, pages 308–322.Springer, 2004.

[7] Jan Camenisch and Anna Lysyanskaya.An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, EUROCRYPT, volume2045 of LNCS, pages 93–118. Springer, 2001.

[8] David Chaum. Blind signatures for untraceable payments. In CRYPTO, pages 199–203, 1982.LNCS, pages 246–264. Springer, 1990.

[9] Patrick P. Tsang, Apu Kapadia, and Sean W. Smith.Anonymous IP-address blocking in torwith trusted computing (work-in-progress). In The Second Workshop on Advances in TrustedComputing (WATC '06 Fall), November 2006.

[10] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor,ASIACRYPT, volume 2248 of LNCS, pages 552–565. Springer, 2001