ISSN:0975-9646

Detection And Prevention of Misbehaving Users in Anonymizing Networks

Anuse A.A, Prof. Rachana A. Satao

Department of Computer Engg,
SKN, Vadgaon (Bk), Pune.
University of Pune

Abstract: - As we studied in our literature, the recent method was presented for blocking of misbehaving user in the Tor networks called as Nymble. However the first limitation which we identified for Nymble is that if the Nymble manager fails, then whole security system is fails second limitation is blocking IP address is not feasible because if we reconnect it we get new IP address by dynamic property IP addressing.Drawback of existing system can be overcome by our proposed system i.e "Detection and Prevention of misbehaving users in anonymzing network". MAC address is used for blocking misbehaving users in anonymizing network. which cover MAC address as user identity, as IP address can be dynamically generated,it is not useful to solve above problem As ,we use MAC address, there is no chance for Sybil attack, as MAC address is physical address it cannot be change at any cost.As existing system is totally centralized to nymble manager, to overcome above all drawback, we use reliable system where second manager may handle task of first nymble manager failure.current system has scalability property as well as it can handle multiple server requestsat a time .We use strongly cryptography algorithm it's hard to break security of our system.

Key Words:- Anonymizing,blacklisting, Sybil attack, MAC addresss

1. INTRODUCTION

The networks like Tor (Anonymizing networks) allows users to access Internet services privately by using a series of routers to hide the client's MAC address from the server.by blocking IP address is not a effective solution in case of nymble system as mentioned in above case. To overcome drawback of nymble system like sybil attack, revealing identity, centralized system. To overcome above all drawback we are designing new system called as "Detection and Prevention of misbehaving users in anonymizing network" in this system complete MAC address is blocked if user misbehaves. User will block depending upon window size .But this networks success is limited up to users those are employing this anonymity for abusive purposes like defacing popular Web sites. In such cases, the administrator of website depends on solution of periodic MAC-address blocking for disabling access to misbehaving users, however blocking IP addresses is not practical if the abuser routes through an anonymizing network. And hence, administrators block all known exit nodes of anonymizing networks, denying anonymous access to misbehaving and behaving users alike, however this makes problem for know and real users and preventing them from access website. Thus, in this project we are presenting the new solution to overcome this problem. We presented 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 misbehavior — servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

2. RELATED WORK:

To overcome the above said problem, several researchers come with different solutions, each providing some degree of accountability. *1: In pseudonymous credential system* users log into Web sites using pseudonyms, which can be added to a blacklist if a user misbehaves. Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network. 2*: Anonymous credential systems* employ group signatures. Basic group signatures allow servers to revoke a misbehaving user's anonymity by complaining to a group manager. Servers must query the group manager for every authentication, and thus, lacks scalability. 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 unlinkability that we desire, where a user's accesses before the complaint remain anonymous. Backward relinkability where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, approaches without relinkability need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviours will be judged fairly. Later many additions done into this approach such as *Verifier-local revocation (VLR),* however this also requires heavy computation at server.

3.PROPOSED WORK:

3.1 *Anonymous MAC-address Blocking*

"Detection and Prevention of misbehaving users in anonymzing network". MAC address is used for blocking misbehaving users in anonymizing network. which cover MAC address as user identity, as IP address can be dynamically generated,it is not useful to solve above problem As ,we use MAC address, there is no chance for Sybil attack, as MAC address is physical address it cannot be change at any cost.As existing system is totally centralized to nymble manager, to overcome above all drawback, we use reliable system where second manager may handle task of first nymble manager failure.current system has scalability property as well as it can handle multiple server requestsat a time .We use strongly

cryptography algorithm it's hard to break security of our system.Here we present a secure system called "Detection and Prevention of misbehaving users in anonymizing network" , which provides all the following properties: anonymous authentication,relinkability,subjective blacklisting, fast authentication speeds, rate-limited anonymous connections, revocation auditability (where users can verify whether they have been blacklisted), and also addresses the Sybil attack to make its deployment practical. In this system, users acquire an ordered collection of nymbles, a special type of pseudonym, to connect to websites. Without additional information, these nymbles are computationally hard to link and hence using the stream of nymbles simulates anonymous access to services. Following figure shows the basic architecture of proposed approach:

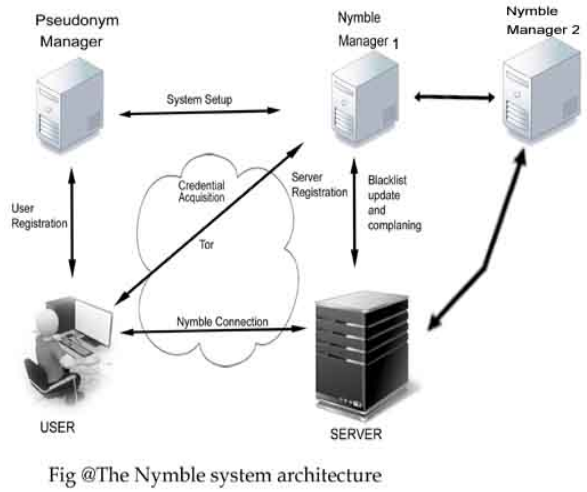

Fig @The Nymble system architecture

Fig. 1: The Nymble system architecture showing the various modes of interaction. Note that users interact with the NM and servers though the anonymizing network.

3.2 Nymble Manager:

Servers can therefore blacklist anonymous users without knowledge of their IP addresses while allowing behaving users to connect anonymously. Our system ensures that users are aware of their blacklist status before they present a nymble, and disconnect immediately if they are blacklisted.

3.3 Pseudonym Manager:

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 directly, ensuring that the same pseudonym is always issued for the same resource.

3.4 Blacklisting a user:

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. It is of utmost importance, then, that users be notified of their blacklist status before they present a nymble ticket to a server. In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

3.5 Nymble-authenticated connection:

Blacklistability assures that any honest server can indeed block misbehaving users.

3.6 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 that user, however, it can link that user's subsequent connections. It is of utmost importance then that users be notifieded of their blacklist status before they present a nimble ticket to a server. In our system, the user can download the server's blacklist and verify her status. If blacklisted, the user disconnects immediately.

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 told is fresh as of time period tnow"). As discussed in Section 4.3.4, these daisies are elements of a hash chain, and provide a lightweight alternative to digital signatures. Using digital signatures and daisies, we thus ensure that race conditions are not possible in verifying the freshness of a blacklist.Auser 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.

3.7 Time:

Nymble tickets are bound to specific time periods. As illustrated in Fig. 2, time is divided into linkability windows of duration W, each of which is split into L time periods of duration T (i.e W ¼L _ T). We will refer to time periods and linkability 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, while longer time periods allow servers to rate-limit the number of misbehaviors from a particular user before he or she is blocked. For example, T could be set to five minutes, and W to one day (and thus, L ¼ 288). The linkability window allows for dynamism since resources such as IP addresses can get reassigned and it is undesirable to blacklist such resources indefinitely, and it ensures forgiveness of misbehavior after a certain period of time. Weassume all entities are time synchronized (for example, with time.nist.gov viathe Network Time Protocol (NTP)), and can thus calculate.

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 Fig. 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 misbehavior and complains to the NM in time period tc (t_ < tc _ tL) of the same linkability window .

3.8 Summary of Updates to the Nymble

We highlight the changes to Nymble since our conference paper . Previously, we had proved only the privacy

properties associated with nymbles as part of a two-tiered hash chain. Here, we prove security at the protocol level. This process gave us insights into possible (subtle) attacks against privacy, leading us to redesign our protocols and refine our definitions of privacy. For example, users are now either legitimate or illegitimate, and are anonymous within these sets (see Section 3). This redefinition affects how a user establishes a "Nymble connection" (see Section 5.5), and now prevents the server from distinguishing between users who have already connected in the same time period and those who are blacklisted, resulting in larger anonymity sets. A thorough protocol redesign has also resulted in several optimizations. We have eliminated blacklist version numbers and users do not need to repeatedly obtain the current version number from the NM. Instead servers obtain proofs of freshness every time period.

4 SECURITY MODEL

can be found in our technical report, which explains how these goals must also resist coalition Nymble aims for four security goals. We provide informal definitions here; a detailed formalism attacks.

4.1 Goals and Threats

An entity is honest when its operations abide by the system's specification. An honest entity can be curious: it attempts to infer knowledge from its own information (e.g., its secrets, state, and protocol communications). An honest entity becomes corrupt when it is compromised by an attacker, and hence, reveals its information at the time of compromise, and operates under the attacker's full control, possibly deviating from the specification. Blacklistability 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 (following the time of complaint) 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. Nonframeability guarantees that any honest user who is legitimate according to an honest server can 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 misbehavior. 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. Nonframeability 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.

4.2 Trust Assumptions

We allow the servers and the users to be corrupt and controlled by an attacker. Not trusting these entities is important because encountering a corrupt server and/or user is a realistic threat. Nymble must still attain its goals under such circumstances. With regard to the PM and NM, Nymble makes several assumptions on who trusts whom to be how for what guarantee. We summarize these trust assumptions as a matrix in Fig. 3. Should a trust assumption become invalid, Nymble will not be able to provide the corresponding guarantee.For example, a corrupt PM or NM can violate Blacklistability by issuing different pseudonyms or credentials to blacklisted users. A dishonest PM (resp., NM) can frame a user by issuing her the pseudonym (resp., credential) of another user who has already been blacklisted. To undermine the Anonymity of a user, a dishonest PM (resp., NM) can first impersonate the user by cloning her pseudonym (resp., credential) and then attempt to authenticate to a server—a successful attempt reveals that the user has already made a connection to the server during the time period. Moreover, by studying the complaint log, a curious NM can deduce that a user has connected more than once if she has been complained about two or more times. As already described in Section 2.3, the user must trust that at least the NM or PM is honest to keep the user and server identity pair private.

4. PRELIMINARIES

4.1 Notation The notation a 2R S represents an element drawn uniformly at random from a nonempty set S.NN0 is the set of nonnegative integers, andNNis the setNN0nf0g. s½i_ is the ith element of list s. skt is the concatenation of (the unambiguous encoding of) lists s and t. The empty list is denoted by ;. We sometimes treat lists of tuples as dictionaries.For example, if L is the list ((Alice, 1234), (Bob, 5678)), then L[Bob] denotes the tuple (Bob, 5678). If A is an (possibly probabilistic) algorithm, then AðxÞ denotes the output when A is executed given the input x. a :¼ b means that b is assigned to a.

4.2 Data Structures

Nymble uses several important data structures:

4.2.1 Pseudonyms

The PM issues pseudonyms to users. A pseudonym pnym has two components nym and mac: nym is a pseudorandom mapping of the user's identity (e.g., IP address),7 them linkability window w for which the pseudonym is valid, and the PM's secret key nymKeyP ; mac is a MAC that the NM uses to verify the integrity of the pseudonym. Algorithms 1 and 2 describe the procedures of creating and verifying pseudonyms.

4.2.2 Seeds and Nymbles

A nymble is a pseudorandom number, which serves as an identifier for a particular time period. Nymbles (presentedmby a user) across periods are unlinkable unless a server hasmblacklisted that user. Nymbles are presented as part of amnymble ticket, as described next.mAs shown in Fig. 4, seeds evolve throughout a linkabilitymwindow using a seed-evolution function f; the seed for themnext time period (seednext) is computed from the seed for the current time period (seedcur) as seednext ¼ fðseedcurÞ:The nymble (nymblet) for a time period t is evaluated.

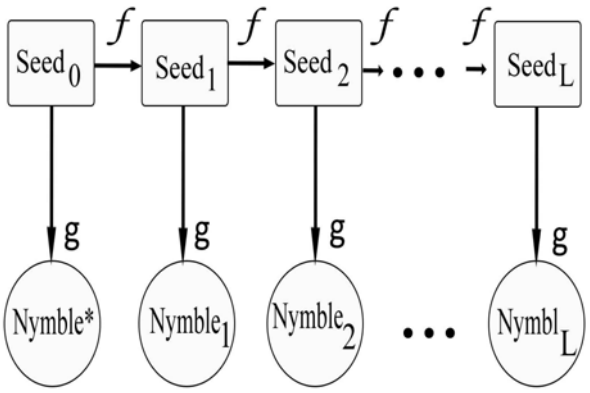

Fig. 2. Evolution of seeds and nimble

The NM sets seed0 to a pseudorandom mapping of the user's pseudonym pnym, the (encoded) identity sid of the server (e.g., domain name), the linkability window w for which the seed is valid, and the NM's secret key seedKeyN. Seeds are therefore specific to user-server-window combinations. As a consequence, a seed is useful only for a particular server to link a particular user during a particular linkability window. In our Nymble construction, f and g are two distinct cryptographic hash functions. Hence, it is easy to compute future nymbles starting from a particular seed by applying f and g appropriately, but infeasible to compute nymbles otherwise. Without a seed, the sequence of nymbles appears unlinkable, and honest users can enjoy anonymity. Even when a seed for a particular time period is obtained, all the nymbles prior to that time period remain unlinkable.

4. 2.3 Nymble Tickets and Credentials

A credential contains all the nymble tickets for a particular linkability window that a user can present to a particular server. Algorithm 3 describes the following procedure of generating a credential upon request: A ticket contains a nymble specific to a server, time period, and linkability window. ctxt is encrypted data that the NM can use during a complaint involving the nymble ticket. In particular, ctxt contains the first nymble (nymble_) in the user's sequence of nymbles, and the seed used to generate that nymble. Upon a complaint, the NM extracts the user's seed.

CONCLUSIONS

We have proposed and built a comprehensive credential system called "Detection and prevention of misbehaving user in anonymizing network", which can be used by blocking misbehaving user in anonymizing network by using MAC address. Which can overcome the drawback of nymble system, where IP address is used, but in our system instead of IP address MAC address is used to block the user , 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 the 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.

REFERENCES

[1] Giuseppe Ateniese and Breno de Medeiros. Efficient group signatures without trapdoors.In Chi-Sung Laih, editor, Advances in Cryptology — ASIACRYPT 2003, volume 2894 ofLecture Notes in Computer Science, pages 246–268. Springer Verlag, 2003.

[2] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Mihir Bellare, editor, Advances in Cryptology — CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pages 255–270. Springer Verlag, 2000.

[3] D.Chaum and E.van Heyst, "Group Signatures," Proc.Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT) pp.237-265, 1991.

[4] S. Brands, "Restrictive Blinding of Secret-Key Certificates,"in *Proceedings of EUROCRYPT 1995*, Saint-Malo, France,May 1995.

[5] Boukerche, A.; El-Khatib, K.; Li Xu; Korba, L., SDAR: *"A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks"*, IEEE Comput. Soc. 29 -2004.

[6] Ray Dillinger, Cyclopedia Cryptologia-an online encyclopedia of cryptographic protocols. http://www.disappearing-inc.com.

Mrs Anuse A.A received the B.E.from Shivaji University Kolhapur and appears M.E. degree, from SKN College of engg. Pune, Pune University.