Stamping Wildcat Users in Stripping Mesh for Secluded Networks by Using Nymble

C.Murugan[1] and R.Sudha[2]
[1]Department of Computer Science and Engineering, PRIST University - Trichy Campus, Tiruchy, India, Email ID: cmurugan123@gmail.com
[2]Department of Computer Science and Engineering, PRIST University - Trichy Campus, Tiruchy, India.

Abstract - Anonymizing 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 such networks, however, has been limited by users employing this anonymity for abusive purposes such as defacing popular websites. 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 misbehavior — servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.

Keywords – Anonymous blacklisting, privacy, revocation.

1. INTRODUCTION

This paper present a secure system called Nymble, which provides all the following properties: anonymous authentication, backward unlinkability, 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 Nymble, 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.

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 unlinkable. 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.

Although our work applies to anonymizing networks in general, This paper consider Tor for purposes of exposition. 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

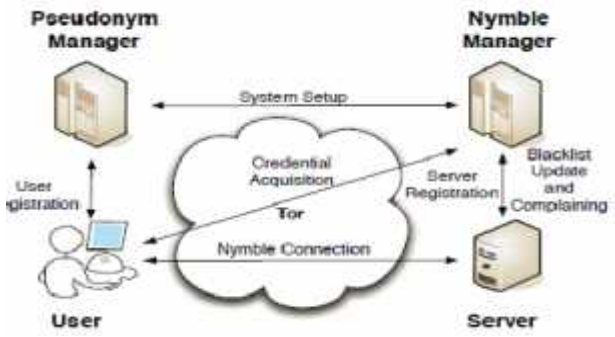

Figure 1. The Nymble system architecture

• Blacklisting anonymous users. I 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, I have built an open source implementation of Nymble, which is publicly available. In this project provide performance statistics to show that our system is indeed practical.

The characteristics of self-organization and wireless medium make Mobile Ad hoc NETwork (MANET) easy to set up and thus attractive to users. The open and dynamic operational environment of MANET makes it vulnerable to various network attacks.

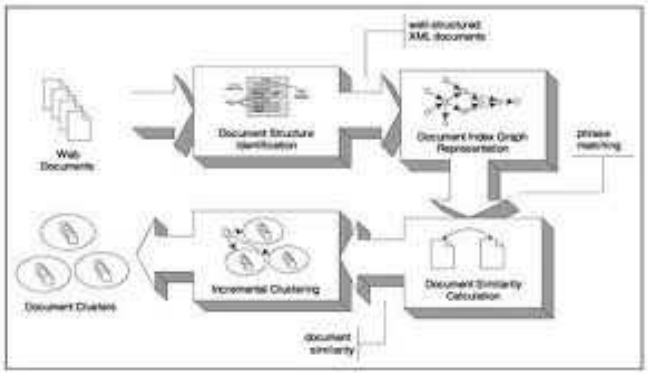

Figure 2. Overview of Nymble in wireless model

A common type of attacks targets at the underlying routing protocols. Malicious nodes have opportunities to modify or discard routing information or advertise fake routes to attract user data to go through themselves. Some new routing protocols have been proposed to address the issue of securing routing information. However, a secure routing protocol cannot single-handedly guarantee the secure operation of the network in every situation.

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure 1.1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.

The mobile ad hoc network is a new model of wireless communication and has gained increasing attention from industry. As in a general networking environment, mobile ad-hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is understandable that most security threats target routing protocols – the weakest point of the mobile ad-hoc network.

2. METHODS AND MATERIALS USED

2.1 SECURITY MODEL FOR NYMBLE-AUTH

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. Although our work applies to anonymizing networks in general, In this project is consider Tor for purposes of exposition. 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.

2.2. 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 (i.e., not through a known anonymizing network), ensuring that the same pseudonym is always issued for the same resource.

2.3 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). A user's 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 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.

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.

2.4. SERVER REGISTRATION

To participate in the Nymble system, a server with identity initiates a type-Auth channel to the NM, and registers with the NM according to the Server Registration protocol. Each server may register at most once in any linkability window.

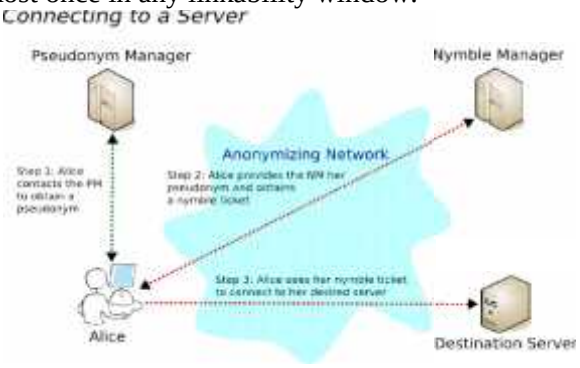

Figure 3. Connecting to server

2.5 USER REGISTRATION

A user with identity uid must register with the PM once in each linkability window. To do so, the user initiates a type- Basic channel to the PM, followed by the User Registration protocol described below.
1. The PM checks if the user is allowed to register. In our current implementation, the PM infers the registering user's IP address from the communication channel, and makes sure that the IP address does not belong to a known Tor exit node. If this is not the case, the PM terminates with failure.

2.6 USER BLOCKING

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.

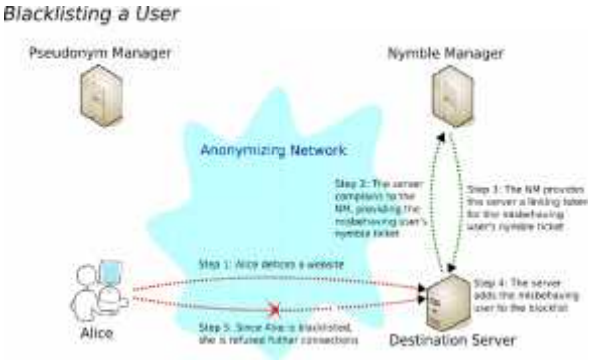

Figure 4. Blacklisting a user

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. Subnet-based blocking alleviates this problem, and while it is possible to modify our system to support subnet-based blocking, new privacy challenges emerge; a more thorough description is left for future work.

2.7 AUTHENTICATED CONNECTION

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. Non-frameability 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. 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.

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

3. SECURITY MODEL

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

3.1. 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 betIen 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.

3.2 TRUST ASSUMPTIONS

I 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. I 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 the user must trust that at least the NM or PM is honest to keep the user and server identity pair private.

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]. 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- 320, Aug. 2004.

[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.

[21]. J. Feigenbaum, A. Johnson, and P.F. Syverson, "A Model of Onion Routing with Provable Anonymity," Proc. Conf. Financial Cryptography, Springer, pp. 57-71, 2007.

[22]. S. Goldwasser, S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Computing, vol. 17, no. 2, pp. 281-308, 1988.

[23]. J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity for Anonymous Networks," Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.

[24]. P.C. Johnson, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.

[25]. A. Juels and J.G. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), 1999.