A Survey on Privacy Preserving Technique for Blocking Misbehaviors in Anonymous Networks

Shatadal Patro and Asha Ambhaikar

RCET, Bhilai, Department of Computer Science & Engineering, RCET, Bhilai, India

E-mail: shatdalpatro22@gmail.com, asha31.a@rediffmail.com

(Received on 25 September 2012 and accepted on 30 November 2012)

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 web sites. Web site administrators routinely rely on IP-address for blocking or disabling access to misbehaving users, but blocking IP addresses is not practical if the abuser routes through an 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 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 server definitions of misbehavior servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained.**

Keywords: **Anonymizing network, Anonymous blacklisting, Credential system, Revocation, Ticket Method, Anonymous blacklisting, Privacy**

I. Introduction

Anonymizing networks such as Tor route traffic through independent nodes in separate administrative domains to hide a client's IP address. Unfortunately, some users have misused such networks-under the cover of anonymity, users have repeatedly defaced popular Web sites. Since web site administrators cannot blacklist individual malicious users' IP addresses, they blacklist the entire anonymizing network. Such 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. 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 considered misbehaviour in anonymous e-cash systems. An anonymous P2P communication system is a peer-to-peer distributed application in which the nodes or participants are anonymous or pseudonymous. Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participants.

A. Anonymity and Pseudonymity

Some of the networks commonly referred to as "anonymous P2P" are truly anonymous, in the sense that network nodes carry no identifiers. Others are actually pseudonymous: instead of being identified by their IP address, nodes are identified by pseudonyms such as cryptographic keys. For example, each node in the MUTE network has an overlay address that is derived from its public key. This overlay address functions as a pseudonym for the node, allowing messages to be addressed to it. In Frenet, on the other hand, messages are routed using keys that identify specific pieces of data rather than specific nodes; the nodes themselves are anonymous.

The term anonymous is used to describe both kinds of network because it is difficult—if not impossible—to determine whether a node that sends a message originated the message or is simply forwarding it on behalf of another node. Every node in an anonymous P2P network acts as a universal sender and universal receiver to maintain anonymity. If a node was only a receiver and did not send, then neighboring nodes would know that the information it was requesting was for itself only, removing any reasonable deniability that it was the recipient (and consumer) of the information. Thus, in order to remain anonymous, nodes must ferry information for others on the network.

B. Anonymizing Networks — Presentation Transcript

Different types of anonymous networks, how they work, the advantages and weaknesses of each anonymous communication network. Everyone's daily life, People access to Internet to do business, to find job, to contact friends, to pay bills. Internet has become another utility like water and electricity, which plays more and more significant role in everyday life. With the impact of Internet on society,

people became more sensitive regarding privacy issues in the Internet. They realized that they leave all kinds of traces and personal information while surfing websites and exchanging emails. In some cases, people do not want others know what they are talking. So, encryption like Pretty Good Privacy (PGP) was introduced, eavesdropping on content becoming very difficult. However, preserving privacy means not only the content of messages, but also hiding routing information which means who is talking to whom. Unfortunately, the Internet was not designed with anonymity in mind; in fact, one of the original design goals was accountability. IP packet which is one of the most important infrastructure protocols in network contains lots of fingerprint. Demand and interest in anonymous network has increased recently for many reasons. The material or its distribution is illegal or incriminating. Music and movie files sharing in peer-to-peer network applications, e. g. Kazaa, Bit Torrent. Material is legal but socially deplored, embarrassing or problematic in the individual's social world. For example, people may openly discuss personal stuff which would be embarrassing to tell many people about, such as sexual problems fear of retribution.

(Whistleblowers, unofficial leaks, and activists who do not believe in restrictions on information or knowledge), Censorship at the local, organizational, or national level. Cisco designed and deployed packet content filtering equipments in every ISP access point's mainland China. The TCP connection will be reset if it contains susceptive domain name, IP address or even key words. Personal privacy preferences such as preventing tracking or data mining activities MAC and IP address can be used to identify one device. Furthermore these persistent addresses can be linked to physical persons, seriously compromising their privacy. People can use anonymity in different purpose, good or bad.

C. Back Ground Survey

Achieving anonymity in a network is very difficult. Encryptions are used to protect data's confidentiality, while anonymity means protect both data and participants in this communication. Unfortunately, the Internet was not designed with anonymity in mind; in fact, one of the original design goals was accountability. In packet switching network, every IP packet contains a header to describe the packet itself: The header contains Identification—contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments; Time-to-Live—maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly; Source Address—specifies the sending node; Destination Address—specifies the receiving node. What more is, there is plenty of useful information within packet for network analyzers to identify communication between two parties. This information includes source port, destination port, sequence number, window size. So the first step to anonymize communication is to encrypt the data in the packet, change source IP address, modify port number and Time-to-Live value to hide the fingerprint of initiator. However, these methods are not enough to counter network traffic analyzers. More sophisticated anonymous methods are desired. Terminology Based on previous papers in this field, researchers proposed a set of precise terminologies. These definitions might help researchers invents new word with same meaning. I am going to use these terminologies in later sections. Anonymity: Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set. Unlinkablity: Unlinkablity of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not. Unobservability: Unobservability of an Item of Interest (IOI) means undetectability of the IOI against all subjects uninvolved in it and anonymity of the subject (s) involved in the IOI even against the other subject (s) involved in that IOI.

D. Pseudonymity

Pseudonymity is the use of pseudonyms as identifiers. Taxonomy According to the architecture and usability, anonymity communication can be classified into four categories: High latency, Low latency, Central Email relay, Web proxy Distributed and N/A Tarzan/Tor Pseudo-distributed. Central/High latency: There is a central server that provides anonymity service to clients, for example email relay service like anon.penet.fi and MixMaster. Central/ Low latency: Clients can send requests to the central server, the server modify the packet and resend these requests to destinations. For instance, Anonymizer and Safe Web are such type of service. Pseudo-Distributed/High Latency and Distributed High Latency: Due to the volatile of distributed networks and interaction like AJAX and Flash between user and server is desired nowadays, we are not interested in these categories.

E. Collusion Attack

This happens if a certain number of involved parties collide to break the anonymity of connections. Flooding attack: Anonymity is usually achieved with respect to a certain group. In this attack, an adversary floods the system to separate certain messages from the group. Message volume attack: In this attack, it is tried to detect an end-to-end connection by observing the message volume at the endpoints. Timing attack: A timing attack tries to observe the duration of a connection by correlating its establishment or release at the possible endpoints.

II. Existing System

There are many solutions for the problems and difficulties in anonymous networks. But each method has some limitations and issues. They are as follows: In pseudonym Systems, an individual will be known to other users by a pseudonym which is blacklisted if a user misbehaves. But this results in pseudonymity for all users and weakens the anonymity. Also the users should be prevented from sharing their pseudonyms. Group signature is a method by which a member of a group anonymously signs the message on behalf of the group. Hers the server sends complaints to the Group Manager (GM) if a user misbehaves which lacks scalability. Traceable signatures traces the signatures signed by a single party without opening the signature and revealing the identities of any other users. This method does not provide backward unlinkability, where the previously issued signatures remain anonymous even after the signer's revocation. Since there is no backward unlinkabilty, there will be no subjective blacklisting. Subjective blacklisting is the process by which the server can blacklist the user for whatever reason the server desires. Dynamic accumulator is cryptographic accumulator that allows dynamically adding or deleting a value. But here a single revocation operation results in a new accumulator and public parameters for the group. Thus updating all the values is impractical. In Verifier Local Revocation (VLR), the verifier performs local updates but there will be heavy computation at the server or the verifier. These approaches do not provide revocation auditability by which the users can verify their status before accessing the server.

III. Proposed System

We 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 complaints remain unlikable. 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, we 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. An anonymous P2P communication system is a peer-to-peer distributed application in which the nodes or participants are anonymous or pseudonymous .Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participants. Interest in anonymous P2P systems has increased in recent years for many reasons, ranging from the desire to share files without revealing one's network identity and risking litigation to distrust in governments, concerns over mass surveillance and data retention, and lawsuits against bloggers.

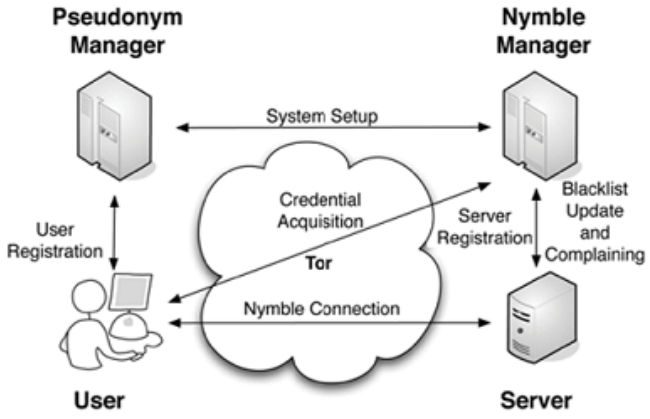

Fig.1 The nymble system architecture showing the various modes of interaction. Note that users Interact with the nm and servers though the anonymizing network

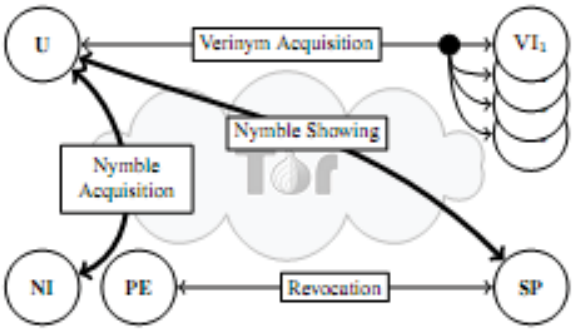

Fig. 2 Architecture of our extended nymble framework: this figure illustrates the parties in our extended nymble framework and the interactions between them. Arrows that pass through the tor cloud represent anonymous connections, while those that do not pass through the tor cloud represent direct (nonanonymous) connections.

A. Trust and Threat Model

Nymbler's threat model allows for any subset of users or SPs to be compromised and hence under adversarial control. The security and privacy properties of the system therefore make no assumptions about the honesty of its users, and require that an SP is honest only to guarantee the availability of that SP's own services. As noted by Tsang, "not trusting these entities is important because encountering a corrupt server and/or user is a realistic threat."However, as with Nymble, our approach does require certain trust assumptions regarding the VIs, NI and PE. Table 1 summarizes these trust assumptions and describes which security properties rely on each assumption.

Note that Nymbler requires a dramatically reduced level of trust as compared to Nymble.

B. Design Issues

The proposed system should be constructed in such a way that all the entities in the system should be honest. An entity is honest when its operations are performed according to the system's specification. An honest entity becomes corrupt when it is compromised by an attacker. Once it gets compromised then the entity will operate under the full control of the attacker and starts functioning against the system's specification. The proposed system should also satisfy the following security properties. They are:

1. Blacklistability

This property assures that any honest server can block misbehaving users. If an honest server complains that a user misbehaved in the current time period, then the complaint will be successful and the user will not be able to establish a connection to the server successfully for the following time periods.

2. Rate limiting

This property assures that any honest server can prevent the user from the successful connection to it, when user attempts to connect to the server more than once within any single time period.

3. Nonframeability

This property assumes that each user has a single unique identity, since it is possible for the user to frame some other identities. So any honest server can provide connection to the server only if it is proved to be an honest user. According to any honest server, a user is honest if he/she has not been blacklisted by the server thus far and has not exceeded the rate limit of establishing connections.

4. Anonymity

This property protects the anonymity of honest users such that the server cannot know any information about the user.

IV. Conclusion & Future Work

A new system is proposed that adds an additional layer of security to the anonymous networks. This system is used to block the misbehaving users in anonymizing networks. It is automatically finds the misbehaving user and blacklists them without affecting their privacy and anonymity. This method is a cryptographic construction that provides anonymous authentication, fast authentication speeds, subjective blacklisting, backward anonymity and revocation auditability. This method is practical, effective and efficient to the needs of both users and services. The proposed method motivates the need for 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. Currently the proposed system has been simulated with PM, SM and server on the local network. In future this work will be enhanced to work on a remote machine. This work can also be extended into a multiple rounds of pseudonym construction in which the PM participates in multiple rounds of communication with the user. This adds one more layer of security to the system.

References

[1] Patrick P. Tsang, Apu Kapadia, Cory Cornelius, Sean W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," *IEEE Transaction on Dependable and Secure Computing,* Vol. 8, No.2, March-April ,2011.

[2] Reed S. Abbott, W. Timothyvan der Horst, and E. Kent Seamons. CPG: Closed Pseudony-mous Groups. In Vijay Atluri and Marianne Winslett, editors, Proceedings of WPES, pp. 55–64. Association for Computing Machinery (ACM) Press, New York, NY,USA, (One citation on page 17.) October 2008.

[3] Peter C. Johnson, Apu Kapadia, P. Patrick Tsang, and Sean W. Smith. Nymble:Anonymous IP-Address Blocking. In Privacy Enhancing Technologies, LNCS 4776, pp. 113–133, Springer, 2007.

[4] P. P. Tsang, M. H. Au, A.Kapadia, and S.W.Smit, "Blacklistable Anonymous Credentials: Blockin Misbehaving Users without TTPs," *Proc. 14th ACM Con Computer and Comm.Security* (CCS '07), pp. 72-81, 2007.

[5] Tadayoshi Kohno, Andre Broido and K. C. Clay, "Remote physical device finger-printing", *In Proceedings of the 2005 IEEE Symposium on Security and Privacy,* pp. 211–225, Washington, DC, USA, IEEE Computer Society, 2005.

[6] Toru Nakanishi and Nobuo Funabiki. Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps. In ASIACRYPT, LNCS3788, pp. 533–548. Springer, 2005.

[7] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In CT-RSA, LNCS 3376, pp. 136–153. Springer, 2005.

[8] Dan Boneh and Hovav Shacham. Group Signatures with Verifier-Local Revocation. *In ACM Conference on Computer and Communications Security,* pp. 168–177. ACM, 2004.

[9] RogerDingledine, Nick Mathewson, Paul Syverson,"Tor: The Second-Generation Onion Router," *Proc.Usenix Security Symposium,* pp. 303-320, 2004.

[10] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. I(EUROCRYPT), Springer, pp. 571-589, 2004.

[11] Jan Camenisch and Anna Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In CRYPTO, LNCS 3152, pp. 56–72. Springer, 2004.

[12] I. Teranishi, J. Furukawa and K. Sako, "k-Times Anonymous Authentication (Extended Abstract)," *Proc. Int'l Conf. Theory and Application of Cryptology and Information Security* (Asiacrypt), Springer, pp. 308-322, 2004.

[13] Giuseppe Ateniese, Dawn Xiaodong Song, and Gene Tsudik. Quasi-Ecient Revo-cation in Group Signatures. In Financial Cryptography, LNCS 2357, pp. 183–197, Springer, 2002.

[14] Jan Camenisch and Anna Lysyanskaya. An Ecient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In Eurocrypt,Lncs 2045, pp. 93–118, Springer, 2001.

[15] Emmanuel Bresson and Jacques Stern. Ecient Revocation in Group Signatures. In Public Key Cryptography, LNCS 1992, pp. 190–206, Springer, 2001.

[16] 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.