Improving Security in Anonymizing Networks using a Privacy Enhancing System

Chandhana.S.D, E.A.Mary Anita

***Abstract* – Users are allowed to access the anonymity network while they are blocked from tracing their identity on the internet. Tor is open-source anonymity software free to public use. Online anonymity moves Internet traffic through a network of servers. Traffic analysis and network surveillance are prevented by the networks which are anonymized or at least makes it more difficult. Website administrators can disable access to abuser by blocking their IP addresses. But when an abuser routes through an anonymizing network it is not practical to block the IP address. So, all the known exit nodes of anonymizing networks have been blocked by the administrators. As a result, anonymous access has been denied to both misbehaving and behaving users alike. A privacy maintaining system called Nymble has been developed to blacklist the misbehaving users and the security of the system is improved..**

***Index Terms* - Anonymous blacklisting, privacy, rate-limited , revocation.**

I. INTRODUCTION

Anonymizing networks hides the client's address from the server by allowing users to access Internet services privately using a series of routers. Anonymizing networks such as Tor[2] route traffic through independent nodes in separate administrative domains to hide a client's IP address. Tor is open-source anonymity software free to public use. The user's location and/or usage is concealed by Tor sortware. Users can make use of Tor by running onion routing which encrypts and then rebounds communications onto a network of relays run by volunteers throughout the world.

Manuscript received Jan 09, 2012.

Chandhana.S.D, Department of Computer Science and Engineering, Prathyusha Institute of Technology and Management, Chennai, India, 9176384644, (e-mail: chandhana.sd@gmail.com).

Dr.E.A.Mary Anita, Professor and Dean, Department of Computer Science and Engineering, Prathyusha Institute of Technology and Management, Chennai, India,9443500550, (e-mail: anitareginald@yahoo.co.in).

Users who want their Internet searches to remain private make use of anonymity networking. Within the Tor network, Internet traffic is sent to various routers, one at a time. In anonymous system the nodes are anonymous or pseudonymous. Anonymity networks hides the physical location of each node from other nodes. Unfortunately, some users have misused such anonymizing networks. Website administrators cannot blacklist individual malicious users without knowing their IP addresses. Hence, the entire anonymizing network have been blacklisted by them. Such measures eliminate malicious activity through anonymizing networks at the cost of denying anonymous access to behaving users.

Pseudonymous credential systems which use pseudonyms results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network. Anonymous credential systems employ group signatures[8][9] which lacks scalability. Traceable signatures traces all the signatures generated by a particular user which does not provide the backward unlinkability which in turn allows for subjective blacklisting, where servers can blacklist users for whatever reason, since the privacy of the blacklisted user is not at risk.

Dynamic accumulators[1] performs revocation operation. Verifier-local revocation (VLR)[7] makes it possible to update the credentials of all the existing users by requiring the verifier to perform only local updates during revocation but it requires heavy computation at the server that is linear in the size of the blacklist.Nym[3] allows pseudonymous access to the internet services to achieve cryptographically protected pseudonymity for privacy protecting systems. Pseudonym systems[5] issue unlinkable pseudonyms to the users to interact with multiple organizations.

II. EXISTING METHODOLOGY

A secure system called Nymble[6] was designed to provide anonymous authentication, subjective

blacklisting, backward unlinkability, fast authentication speeds, rate-limited anonymous connections, revocation auditability and also addresses sybil attack[10][11]. Servers can blacklist anonymous users without the knowledge of their IP addresses while allowing behaving users to connect anonymously. This system ensures that users are aware of their blacklist status and they disconnect immediately if they are blacklisted. Any number of anonymizing networks rely on the same system, blacklisting anonymous users regardless of their anonymizing network(s) of choice.

Website administrators rely on IP-address blocking for disabling access to misbehaving users, but this is not possible if the abuser routes through an anonymity network. As a result, they block all the exit nodes of network, denying anonymous access to both honest and dishonest users. A system called Nymble[4] addresses the above problem by having honest users to remain anonymous and their requests unlinkable, a server can gain the ability to blacklist the user by making a complaint, blacklisted user's accesses before the complaint remain anonymous and users are aware of their blacklist status before accessing a service. The algorithms used are RSA and MAC. The advantages of this system are privacy of the blacklisted users is maintained, cryptographic functions are used for security and also prevents malicious attack.

A. RSA algorithm

The RSA algorithm is used to provide confidentiality. The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977 [RIVE78]. The most widely-used public key cryptography algorithm is the RSA cryptosystem. RSA encrypts a message without the need to exchange a secret key separately. Both public key encryption and digital signatures can use RSA algorithm. The security of RSA is based on the difficulty of factoring large integers.

B. MAC algorithm

Message Authentication Code algorithm is to provide authentication to message. A MAC algorithm, sometimes called a keyed (cryptographic) hash function, accepts a secret key and an arbitrary-length message to be authenticated as input and outputs a MAC. The MAC value protects both data integrity as well as its authenticity of the message, by allowing verifiers to detect any changes to the message content. MAC is different from digital signatures. MAC values are generated and verified by using the same secret key. This implies that the sender and receiver of a message must have known the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not offer the property of non-repudiation provided by signatures specifically in the case of a network-wide shared secret key. Any user who can verify a MAC of a message is also capable of generating MACs for other messages. In contrast, a digital signature is asymmetric encryption, which is generated using the private key of a key pair. A digital signature proves that a document was signed by none other than that holder since this private key is only accessible to its holder. Thus, digital signatures provides the property of non-repudiation.

III. PROPOSED METHODOLOGY

The existing methodologies have some drawbacks. If the message frequency is very high at a node, the NM forwards only the simple messages. Latency is more and hence the speed gets reduced. In proposed methodology, the credential system is secured by the hashing algorithm. The algorithms used are RSA for confidentiality and MD5 for authentication. The advantages are that it is more secure, increased speed so that latency will be less and the NM(Nymble Manager) can forward all the messages even if the frequency of messages is very high at a node.

A. MD5 algorithm

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, MD5 message-digest algorithm takes a message of arbitrary length as input and produces output as a 128-bit fingerprint or message digest of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA. Fig.1 shows the MD5 algorithm structure. MD5 is simple to implement. It provides a fingerprint or message digest of a message of arbitrary length. It performs very fast on 32-bit machine.

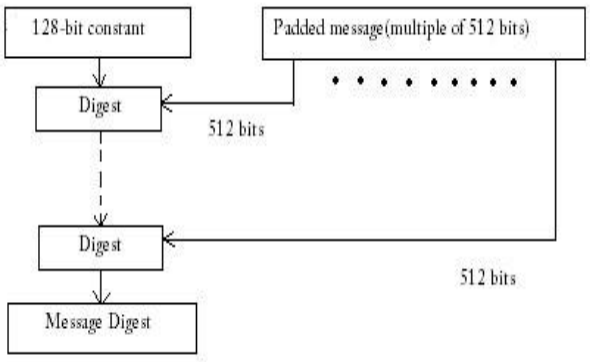

Fig.1 MD5 algorithm structure

Implementation steps in MD5

Step 1: Append padding bits.
Step 2: Append length.
Step 3: Initialize MD buffer.
Step 4: Process the message in 16 word blocks.
Step 5: Output (message digest).

The advantages of MD5 algorithm are the generation of a digest is very fast and the digest itself is very small and can easily be encrypted and transmitted over the internet. It is very easy and fast to check some data for validity. The algorithms are well known and implemented in most major programming languages, so they can be used in almost all environments.

IV. PERFORMANCE EVALUATION

The Dijkstra's Algorithm is implemented and the results are simulated. The Algorithm proves to find the shortest path from source to destination to transmit the packets. The start time is noted when the algorithm starts to execute. The end time is also noted when the packets reach the destination. The time difference is calculated based on the start time and end time. The graph is plotted with time against algorithm types. Thus the comparison is made with the key based routing and the Dijkstra's algorithm and is shown in the fig.2

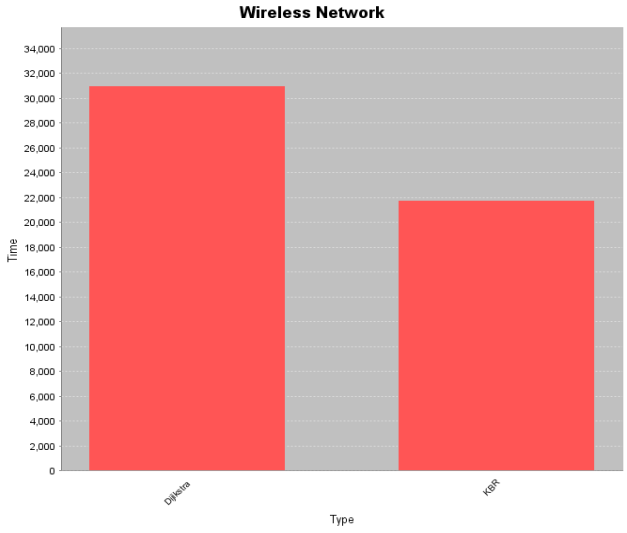

Fig.2 Comparison of time difference between Dijkstra's Algorithm and KBR Algorithm

V. CONCLUSION

The major issues in anonymizing networks are misbehaving user access and blacklisting the misbehaving users without knowing their IP addresses. The paper proposes a more secure system which can be used to add a layer of accountability to any known anonymizing network. This system allows websites to selectively block users of anonymizing networks such as Tor. Servers can blacklist misbehaving users while maintaining their privacy and these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. This work will increase the mainstream acceptance of anonymizing networks such as Tor, which has been completely blocked by several services because of users who abuse their anonymity.

REFERENCES

[1] Camenisch.J and Lysyanskaya.A, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, 2002..
[2] Dingledine.R, Mathewson.N, and Syverson.P, "Tor: The Second-Generation Onion Router," Proc. Usenix Security Symp, pp. 303-320, Aug. 2004.
[3] Holt.J.E and Seamons.K.E, "Nym: Practical Pseudonymity for Anonymous Networks," Internet Security Research Lab Technical Report 2006-4, Brigham Young Univ., June 2006.
[4] Johnson.P.C, Kapadia.A, Tsang.P.P, and Smith.S.W, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.
[5] Lysyanskaya.A, Rivest.R.L, Sahai.A, and Wolf.S, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, 1999.
[6] 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.
[7] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security,pp. 168-177, 2004.
[8] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures,"Proc. Conf. Public Key Cryptography, Springer, pp. 190-206,2001.
[9] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.
[10] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002.
[11] B.N. Levine, C. Shields, and N.B. Margolin, "A Survey of Solutions to the Sybil Attack," Technical Report 2006-052, Univ. of Massachusetts, Oct. 2006.