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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Identification Abuser in Anonymous Network Using Credential System

K.Sivaraman

Assistant Professor, Dept. of Computer Science Engineering, Bharath University, Chennai, India

ABSTRACT: Mysterious 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. 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. Web site 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.

I.INTRODUCTION

Anonymizing networks such as Tor [5] 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 such as Wikipedia. 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. There are several solutions to this problem, each providing some degree of accountability. In pseudonymous credential systems [3], [4], [7], [10], users log into Web sites using pseudonyms, which can be added to a blacklist if a user misbehaves. Anonymous credential systems [1], [2] employ group signatures. Servers must query the group manager for every authentication, and thus, lacks scalability. Traceable signatures [8] allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced.

II.OUR SOLUTION

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 (where users can verify whether they have been blacklisted), and also addresses the Sybil attack [6] 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,4 and hence, using the stream of nymbles simulates anonymous access to services.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Resource-Based Blocking

To limit the number of identities a user can obtain (called the Sybil attack [6]), the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in greatnumbers. 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, and trusted hardware. We do not claim to solve the Sybil attack. This problem is faced by any credential system [6],[9], and we suggestsome promising approaches based on resource-based blocking since we aim to create a real-world deployment.

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. Subjective blacklisting is also better suited to servers such as Wikipedia, where misbehaviors such as questionable edits to a Webpage, are hard to define in mathematical terms.[12]

The 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. 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 pseudonymis always issued for the same resource.

The Nymble Manager

After obtaining a pseudonym from the PM, the user connects to the Nymble Manager (NM) through theanonymizing 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. [11]

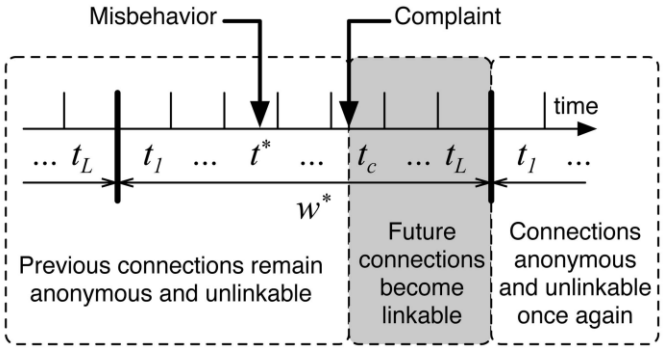

Fig. 2.The life cycle of a misbehaving user.

Time

Nymble tickets are bound to specific time periods. As illustrated in Fig. 2, time is divided into link ability windows of duration W, each of which is split into L time periods of duration T

Blacklisting a User

If a user misbehaves, the server may link any future connection from this user within the current linkabilitywindow (e.g., the same day). Consider Fig. 2 as an example A user connects and misbehaves at a server during time period t* within link ability window w*. [13]

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

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. It is of utmost importance then that users be notified of their blacklist status before they present a nimble ticket to a server. [14]

III.OUR NYMBLE CONSTRUCTION

System Setup

During setup, the NM and the PM interact as follows:

1. The NM executes NM Init State() and initializes its state *nm State* to the algorithm's output.
2. The NM extracts$macKey_{NP}$ from *nm State* and sends it to the PM over a type-Auth channel. *Mac* Key_{NP} is a shared secret between the NM and the PM, so that the NM can verify the authenticity of pseudonyms issued by the PM.
3. The PM generates $nymKey_P$ by running Mac.Key-Gen() and initializes its state *pmState* to the pair ($macKey_{NP}$,$nymKey_P$)

Server Registration

To participate in the Nymble system, a server with identitysid initiates a type-Auth channel to the NM, and registers with the NM according to the Server Registration protocol below.

1. The NM makes sure that the server has not already registered: If (sid,; .)€*nmEntries* in its *nmState*, it terminates with failure; it proceeds otherwise.
2. The NM reads the current time period and linkabilitywindow as t_{now} and w_{now}, respectively, and thenobtains an *svrState*.
3. The NM appends *svrState* to its *nmState*, sends it tothe Server, and terminates with success.
4. The server, on receiving *svrState*, records it as itsstate, and terminates with success.

User Registration

A user with identity *uid* must register with the PM once in each link ability window. protocol described below.

1. The PM checks if the user is allowed to register.
2. Otherwise, the PM reads the current link ability window as w_{now}, and runs *pnym*:=$PMCreatePseudonym_{pmState}$(uid,$w_{now}$) The PM then gives *pnym* to the user, and terminates with success.
3. The user, on receiving *pnym*, sets her state *usrState*to (*pnym*,£), and terminates with success.

Validation Blacklist

1. The server sends (*blist*,*cert*) to the user, where *blist* is its blacklist for the current time period and*cert* isthe certificate on *blist*.
2. The user reads the current time period and linkability window as $t^{(U)}_{now}$ and $W^{(U)}_{now}$ and assumes these values to be current for the rest of the protocol.
3. For freshness and integrity, the user checks if VerifyBLusrState(sid; $t^{(U)}_{now}$ and $W^{(U)}_{now}$,*blist*,cert)=true.If not, she terminates the protocol with failure.[15]

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Ticket Examination

1. The user sets *ticketDisclosed*in *usrEntries[sid]usrState* to true. server, where *ticket* is *ticket[*$t^{(U)}_{now}$*]*in *creed* in *usrEntries[sid]usr State*.
2. On receiving <ticket>, the server reads the current time period and link ability window as, $t^{(S)}_{now}$ and $W^{(S)}_{now}$ respectively. The server then checks that:
   - 2.1.ticketis fresh
   - 2.2. ticketis valid
   - 2.3.ticket is not linked , Server $LinkTicket_{svrState}$(ticket)=False.
3. If any of the checks above fails, the server sends<goodbye> to the user and terminates with failure. Otherwise, it adds *ticket* to *s list* in its state, sends<okay>to the user, and terminates with success.

IV.CONCLUSIONS

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 anonym zing network.. We hope that our work will increase the mainstream acceptance of anonym zing networks such as Tor, which has, thus far, been completely blocked by several services because of users who abuse their anonymity. 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.

REFERENCES

[1].J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional AnonymityRevocation," Proc. Int'l Conf. Theory and Application of CryptographicTechniques (EUROCRYPT), Springer, pp. 93-118, 2001.
[2] Langeswaran K., Revathy R., Kumar S.G., Vijayaprakash S., Balasubramanian M.P., "Kaempferol ameliorates aflatoxin B1 (AFB1) induced hepatocellular carcinoma through modifying metabolizing enzymes, membrane bound ATPases and mitochondrial TCA cycle enzymes", Asian Pacific Journal of Tropical Biomedicine, ISSN : 2221-1691, 2(S3)(2012) pp.S1653-S1659.
[3] J. Camenisch and A. Lysyanskaya, "Signature Schemes andAnonymous Credentials from Bilinear Maps," Proc. Ann. Int'lCryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.
[4] Rajendran S., Muthupalani R.S., Ramanathan A., "Lack of RING finger domain (RFD) mutations of the c-Cbl gene in oral squamous cell carcinomas in Chennai, India", Asian Pacific Journal of Cancer Prevention, ISSN : 1513-7368, 14(2) (2013) pp.1073-1075.
[5] D. Chaum, "Showing Credentials without Identification TransfeeringSignatures between Unconditionally Unlinkable Pseudonyms,"Proc. Int'l Conf. Cryptology (AUSCRYPT),Springer,
pp. 246-264, 1990.
[6] I. Damga°rd, "Payment Systems and Credential Mechanisms withProvable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO),Springer,pp.328-335,1988.
[7] Anbazhagan R., Satheesh B., Gopalakrishnan K., 'Mathematical modeling and simulation of modern cars in the role of stability analysis", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4633-4641.
[8] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," Proc. Usenix Security Symp., pp. 303-320, Aug. 2004.
[9] Murugananthan S., Srivastha P.K., Khanaa, "Object based middleware for grid computing", Journal of Computer Science, ISSN : 1552-6607, 6(3) (2010) pp.336-340.
[10] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002.
[11] Sengottuvel P., Satishkumar S., Dinakaran D., "Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling", Procedia Engineering, ISSN : 0975 – 7384, 64() (2013) pp.1069-1078.
[12] J.E. Holt and K.E. Seamons, "Nym: Practical Pseudonymity forAnonymous Networks," Internet Security Research Lab TechnicalReport 2006-4, Brigham Young Univ., June 2006.
[13] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures,"Proc. Int'l Conf. Theory and Application of Cryptographic Techniques(EUROCRYPT), Springer, pp. 571-589, 2004.
[14] B.N. Levine, C. Shields, and N.B. Margolin, "A Survey ofSolutions to the Sybil Attack," Technical Report 2006-052, Univ. of Massachusetts, Oct. 2006.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

[15] A. Lysyanskaya, R.L. Rivest, A. Sahai, and S. Wolf, "PseudonymSystems," Proc. Conf. Selected Areas in Cryptography, Springer,pp. 184-199, 1999.
[16] Bharthvajan R, Human Resource - Strategy and Outsource, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 15273-15276, Vol. 3, Issue 8, August 2014
[17] Bharthvajan R, Human Resource Management and Supply Chain Management Intersection, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 10163-10167, Vol. 3, Issue 3, March 2014
[18] Bharthvajan R, Women Entrepreneurs & Problems Of Women Entrepreneurs, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 16105-16110, Vol. 3, Issue 9, September 2014
[19] Bharthvajan R, Organizational Culture and Climate, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 8870-8874, Vol. 3, Issue 1, January 2014
[20] C.Rathika Thaya Kumari , Dr.A.Mukunthan, M.Nageshwari, Electric and Magnetic Properties of Semiconductors and Metals in One, Two and Three Dimensions, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 271-279, Vol. 2, Issue 1, January 2013
[21] C.Tamil Selvi & Dr. A. Mukunthan, Different Varieties of Plantain (Banana) and Their Estimation by Chemical Tests, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1099-1105, Vol. 2, Issue 4, April 2013