Misben: Reliable and Risk Free Approach of Blocking Misbehaving Users in Anonymizing Networks

Nikita L. Vikhar, G.R.Bamnote

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 limitation which we identified for Nymble is that if the Nymble manager fails, then whole security system is fails. And hence this approach is heavily vulnerable for failure risks. Thus in this paper we are presenting the new extended method for overcoming above said problems. In this paper we propose a secure Misben system, where users acquire an ordered collection of Misbens, a special type of pseudonym, to connect to Websites. Without additional information, these Misbens are computationally hard to link and hence, using the stream of Misbens simulates anonymous access to services. Web sites, however, can blacklist users by obtaining a seed for a particular Misben, allowing them to link future Misbens from the same user. 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 Misben, and disconnect immediately if they a0072e blacklisted. For the risk free and reliability of proposed approach we also proposed architecture with details that if first misben manager failed to generate seed when it get complaint from server, in previous systems in that condition system get collide and then anonymizing network in trouble ,so provide solution to this problem we introduced new 2^{nd} misben manager.

Index Terms— Anonymizing Networks, TOR, Pseudonym, Anonymous Access, 2^{nd} Misben Manager, Misben.

I. INTRODUCTION

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 blocking for disabling access to misbehaving users, but blocking IP addresses is not practical 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.

Tor is an anonymizing network—it hides a client's identity (actually, your computer's IP address) from the servers that it accesses.

Tor keeps a client's IP-address anonymous by bouncing its data packets through a random path of relays. Each relay knows only of the relay that sent it data and the next relay in the random path. As long as the entry and exit nodes do not collude, the client's connections remain anonymous.

Tor provides anonymity, but some people abuse this anonymity. Since website administrators depend on blocking the IP addresses of misbehaving users, they are unable to block misbehaving users who connect through Tor—their IP address is hidden after all. Frustrated by repeated offenses through the Tor network, the usual response for websites such as Slashdot and Wikipedia is to block the entire Tor network. This is hardly an optimal solution, as honest users are denied anonymous access to these websites through Tor (or any anonymizing network for that matter).

The Solution: Using Misben for Blacklisting Anonymous Users

By providing a mechanism for server administrators to block anonymous misbehaving users, we hope to make the use of anonymizing networks such as Tor more acceptable for server administrators everywhere. All users remain anonymous misbehaving users can be blocked without deanonymization, and their activity prior to being blocked remain unlinkable (anonymous).

Also to improve system performance, we implement 2^{nd} misben manager, when 1^{st} manager fail call pass to 2^{nd} misben manager.

II. LITERATURE REVIEW

2.1Related Work:

2.1.1Nymble: Anonymous IP-address Blocking [3]:

Anonymizing networks such as Tor provide privacy to users by hiding their IP addresses from servers. For example, Tor uses a volunteer network of nodes, which help redirect users' communications thereby making it difficult to infer the users' IP addresses. Unfortunately, some users have abused such networks to deface websites such as Wikipedia. Since servers are unable to block anonymous users, their normal response is to simply block the entire anonymizing network, denying anonymous access to *honest and dishonest users alike* Misben is a credential system that can be used in conjunction with anonymizing networks such as Tor to selectively block anonymous users *while maintaining their privacy*.

2.1.2 A Model of Onion Routing with Provable Anonymity [6]:

"Onion Routing" refers to the layered nature of the encryption service: The original data are encrypted and reencrypted multiple times, then sent through successive Tor relays, each one of which decrypts a "layer" of encryption before passing the data on to the next relay and, ultimately, its destination. This reduces the possibility of the original data being

Manuscript received May, 2013.

Ms. Nikita L.Vikhar,Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati, India.

Dr. G.R. Bamnote, Computer Science and Engineering, SGBA University**,** Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati, India.

unscrambled or understood in transit. Onion Routing is a distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell, and instant messaging. Clients choose a path through the network and build a *circuit*, in which each node (or “onion router” or “OR”) in the path knows its predecessor and successor, but no other nodes in the circuit. Traffic flows down the circuit in fixed-size *cells*, which are unwrapped by a symmetric key at each node (like the layers of an onion) and relayed downstream.

2.1.3 A Survey of the Sybil attack [7]:

The Sybil attack is a fundamental problem in many systems, and it has so far resisted a universally applicable solution. Many distributed applications and everyday services assume each participating entity controls exactly one identity. When this assumption is unverifiable or unmet, the service is subject to attack and the results of the application are questionable if not incorrect. A concrete example of this would be an online voting system where one person can vote using many online identities. Notably, this problem is currently only solved if a central authority, such as the administrator of a certificate authority, can guarantee that each person has a single identity represented by one key; in practice, this is very difficult to ensure on a large scale and would require costly manual attention..

2.1.4 Pseudonym Systems [1]:

Pseudonym systems allow users to interact with multiple organizations anonymously, using pseudonyms. The pseudonyms cannot be linked, but are formed in such a way that a user can prove to one organization a statement about his relationship with another. Such statement is called a credential. Previous work in this area did not protect the system against dishonest users who collectively use their pseudonyms and credentials, i.e. share an identity. Previous practical schemes also relied very heavily on the involvement of a trusted center. In the present paper we give a formal definition of pseudonym systems where users are motivated not to share their identity, and in which the trusted center's involvement is minimal. We give theoretical constructions for such systems based on any one-way function.

Advantages:

□ Simple to implement

□ Less computational

Drawbacks:

□ It results in pseudonymity for all users

□ Weakens the anonymity

2.2 Existing Systems:

2.2.1 Pseudonymous Credential Systems

Pseudonymity technology is technology that allows individuals to reveal or prove information about themselves to others, without revealing their full identity. A credential system is a system in which users can obtain credentials from organizations and demonstrate possession of these credentials.Pseudonyms are generated by Tor client program itself and they are used to log into websites.Server maintains the blacklist of mischievous users by using pseudonyms provided by the users.

Advantages:

□ Simple to implement

□ Less computational Drawbacks:

□ It results in pseudonymity for all users

□ Weakens the anonymity

2.2.2Anonymous credential systems

Anonymous credential system was the innovation of ―J.Camenisch‖ and ―Anna Lysyanskaya‖ in the year 2001.They used the concept of ―Group signatures‖ to make the system more efficient and anonymous. Anonymous credential system consists of three parties i.e. users, an authority, and verifiers. These systems employ group signatures which 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 hence this system lacks scalability.

Advantages:

□ Digital signatures ensure the security of system to some extent. Drawbacks:

□ Lacks scalability

□ Backward unlinkability is not possible

□ Servers can find users’ IP addresses by using traceable Signature.

2.2.3Traceable signatures

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 unlinkability 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. In contrast, approaches without backward unlinkability need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviors will be judged fairly.

2.2.4 Dynamic accumulators

With dynamic accumulators [11], a revocation operation results in a new accumulator and public parameters for the group, and all other existing users’ credentials must be updated, making it impractical.

2.2.5 Verifier-local revocation (VLR)

In order to overcome the problem of lack of backward unlinkability VLR is proposed in 2004 by ―Dan Boneh‖ and ―Hovav Shacham‖.An approach of membership revocation in group signatures is verifier local revocation. In this approach,only verifiers are involved in the revocation mechanism,while signers have no involvement. Thus, since signers have no load, this approach is suitable for mobile environments.This scheme satisfies backward unlinkability to some extent.

III. PROPOSED ALGORITHM

We present a secure system called Misben, 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.

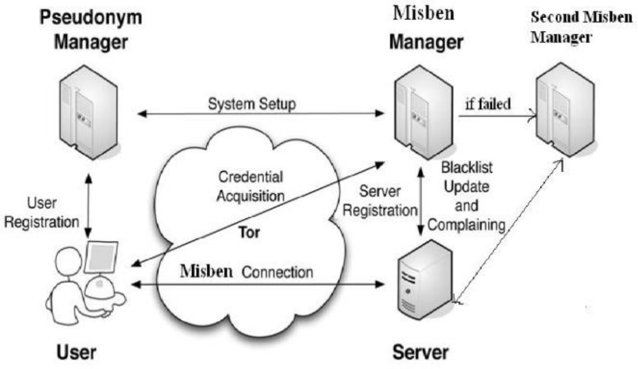


Fig 1: Credential System Architecture

3.1 Resource-Based Blocking

To limit the number of identities a user can obtain (called the Sybil attack), the Misben system binds Misbens to resources that are sufficiently difficult to obtain in great numbers. For example, we have used system Mac addresses as the resource in our implementation, but our scheme generalizes to other resources such as email addresses, identity certificates, and trusted hardware.

3.2 The Pseudonym Manager

The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for mac-address blocking, the user must connect to the PM directly (i.e., not through a known anonymizing network), as shown in Fig. 1.

Note that the user does not disclose what server he or she intends to connect to and the PM's duties are limited to mapping mac addresses (or other resources) to pseudonyms. As we will explain, the user contacts the PM only once per linkability window (e.g., once a day).

3.3The Misben Manager

After obtaining a pseudonym from the PM, the user connects to the Misben Manager (MM) through the anonymizing network, and requests Misbens for access to a particular server (such as Wikipedia). A user's requests to the MM are therefore pseudonymous, and

Misbens are generated using the user's pseudonym and the server's identity. These Misbens are thus specific to a particular user-server pair. Nevertheless, as long as the PM and the MM do not collude, the Misben system cannot identify which user is connecting to what server; the MM 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 MM encapsulates Misbens within Misben tickets. Servers wrap seeds into linking tokens, and therefore, we will speak of linking tokens being used to link future Misben tickets. The importance of these constructs will become apparent as we proceed.

2nd Misben Manager

Here we proposed architecture with details that if first misben manager failed to generate seed when it get complaint from server,in previous systems in that condition system get collied and then anonymizing network in trouble ,so provide solution to this problem we introduced new 2nd misben manager[13]. 2nd misben manager will be in focus when 1st misben manager failed, in that condition backup of 1st misben manager send to 2nd misben manager, using that 2nd misben manager generate seed then immediately send to server for further process.

IV. EXPERIMENTAL ANALYSIS

4.1 Requirement Analysis

For implementation of this system, we used .Net technology. A main part of the .Net technology and structure is the ASP.net set of technologies. These web development technologies are used in the making of Websites and net services working on the .NET infrastructure. ASP.NET was billed by Microsoft from one of their big technologies and web programmers can make use of any encoding language they want to write ASP.NET, from Perl to C Sharp (C#) and of course VB.NET and a few extra language unspoken with the .NET technology.

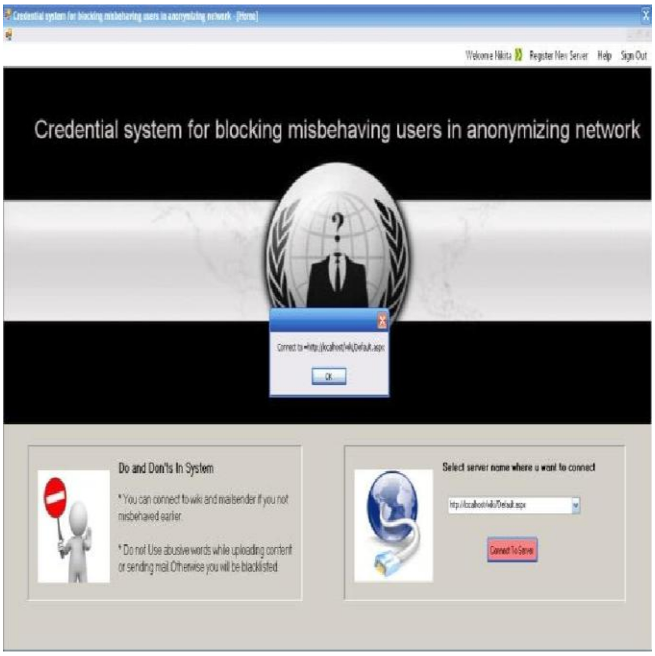
4.2Hardware and Software requirements

- HARDWARE REQUIREMENTS
- Windows XP
- RAM – 1GB
- Hard Disk - 40GB
- SOFTWARE REQUIREMENTS
- .Net Framework
- IIS 7.0
- SQL Server

4.3Result

Here we show Credential system for blocking misbehaving users in Anonymizing network working screen shots

1. Connect To Server


Credential system for blocking misbehaving users in anonymizing network - [Home]
Welcome Nikita
Register New Server
Help
Sign Out
Credential system for blocking misbehaving users in anonymizing network
OK
Connect To Server

Connect to =http://localhost/wiki/Default.aspx

Do and Don'ts In System

* You can connect to wiki and mailsender if you not misbehaved earlier.

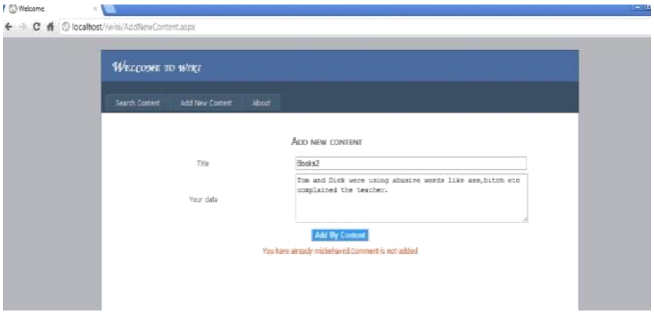
* Do not Use abusive words while uploading content or sending mail.Otherwise you will be blacklisted

Select server name where u want to connect

http://localhost/wiki/Default.aspx

Fig 2: Server Connection

2. User Misbehave on Website



ADD NEW CONTENT

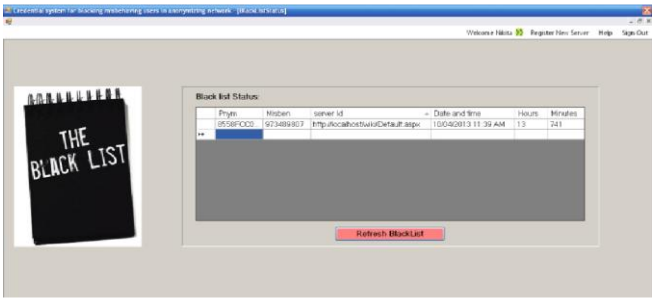
Title: Books2

Your data: Tom and Dick were using abusive words like ass,bitch etc complained the teacher.

You have already misbehaved.Comment is not added

Fig 3: Misbehaving Activity of Users on Website

2. Check Blacklist Status

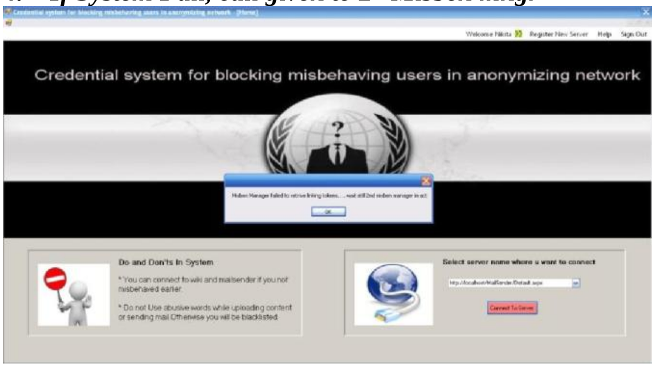

Credential system for blocking misbehaving users in anonymizing network - [BlackListStatus]
Welcome Nikita
Register New Server
Help
Sign Out
THE BLACK LIST
Refresh BlackList

Black list Status

Prym	Misben	server id	Date and time	Hours	Minutes
8558FOC0...	973489807	http://localhost/wiki/Default.aspx	10/04/2013 11:39 AM	13	741

Fig 4: End user blacklist who’s performing misbehave

4. If System Fail, call given to 2nd Misben mngr


Credential system for blocking misbehaving users in anonymizing network - [Home]
Welcome Nikita
Register New Server
Help
Sign Out
Credential system for blocking misbehaving users in anonymizing network
OK
Connect To Server

Misben Manager failed to retrive linking tokens.....wait still 2nd misben manager in act

Do and Don'ts In System

* You can connect to wiki and mailsender if you not misbehaved earlier.

* Do not Use abusive words while uploading content or sending mail Otherwise you will be blacklisted.

Select server name where u want to connect: http://localhost/MailSender/Default.aspx

Fig 5: Risk Free and Reliable Misben Approach

4.4 System Performance

Fig. shows the size of the various data structures. The Y-axis represents the number of entries in each data structure—complaints in the blacklist update request, tickets in the credential.The X-axis represents time duration in sec. Yellow line graph represent no. of credential records.Red line graph represents no. of blacklist user’s entries in system.

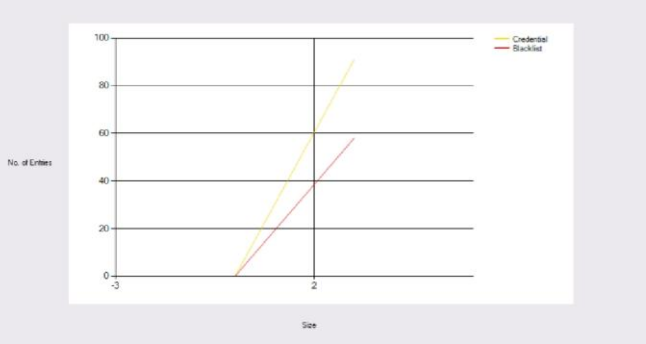


Fig 6: Credential and Blacklist entries system graph

V. CONCLUSION AND FUTURE WORK

We have proposed and built a comprehensive credential system called Misben, 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.

We also proposed a system when 1st misben manager failed then 2nd misben manager in picture, so system performance will increases. 2nd misben manager hand over the work of 1st misben manager till 1st misben get repaired, so it solves the performance issue.

In future 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.

Server-specific likability windows

An enhancement would be to provide support to vary T and L for different servers. As described, our system does not support varying linkability windows, but does support varying time periods.

Side-channel attacks

While our current implementation does not fully protect against side-channel attacks, we mitigate the risks. We have implemented various algorithms in a way that their execution time leaks little information that cannot already be inferred from the algorithm’s output.

REFERENCES

[1] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. Pseudonym Systems. In Selected Areas in Cryptography, LNCS 1758, pages 184–199. Springer, 1999.

[2] B. N. Levine, C. Shields, and N. B. Margolin. A Survey of Solutions to the Sybil Attack. Technical Report Tech report 2006- 052, University of Massachusetts Amherst, Oct 2006.

[3] P. C. Johnson, A. Kapadia, P. P. Tsang, and S. W. Smith. Nymble: Anonymous IP-Address Blocking. In Privacy Enhancing Technologies, LNCS 4776, pages 113–133. Springer, 2007.

[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A Concrete Security Treatment of Symmetric Encryption. In FOCS, pages 394–403, 1997.

[5] R. Dingledine, N. Mathewson, and P. Syverson, ―Tor: The Second- Generation Onion Router,‖ Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.

[6] J. Feigenbaum, A. Johnson, and P.F. Syverson, “A Model of Onion Routing with Provable Anonymity,” Proc. Conf. Financial Crypto-graphy, Springer, pp. 57-71, 2007.

[7] J.R. Douceur, “The Sybil Attack,” Proc. Int’l Workshop on Peer-to-Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

[8] 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.

[9] 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.

[10] 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.

[11] J. Camenisch and A. Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In CRYPTO, LNCS 2442, pages 61–76. Springer, 2002.

[12] 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.

[13] 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.