ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

Creating Obstacles to Screened networks

P.Muppidathi[1], S.Muthuselvi[2], P.Mathumitha[3], M.Mohaideen Fathima[4], M.Muthulakshmi[5], Christo Ananth[6]

U.G.Scholars, Department of ECE, Francis Xavier Engineering College, Tirunelveli[1,2,3,4,5]

Associate Professor, Department of ECE, Francis Xavier Engineering College, Tirunelveli [6]

***Abstract*— In this paper the proposed system adds a layer of accountability to any publicly known anonymizing network is proposed. Servers can blacklist misbehaving users while maintaining their privacy, and this system shows that how 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, thus far, been completely blocked by several services because of users who abuse their anonymity. In future the Nymble system can be extended to support Subnet-based blocking. If a user can obtain multiple addresses, then nymble-based and regular IP-address blocking not supported. In such a situation subnet-based blocking is used. Other resources include email addresses, client puzzles and e-cash, can be used, which could provide more privacy. The system can also enhanced by supporting for varying time periods.**

Index Terms—Screened networks, Subnet based blocking,privacy,revocation

I. INTRODUCTION

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.

In today's technological world, millions of individuals are subject to privacy threats. Companies are hired not only to watch what you visit online, but to infiltrate the information and send advertising based on your browsing history. People set up accounts for facebook,enter bank and credit card information to various websites.

Those concerned about Internet privacy often cite a number of privacy risks events that can compromise privacy which may be encountered through Internet use. These methods of compromise can range from the gathering of statistics on users, to more malicious acts such as the spreading of spyware and various forms of bugs (software errors) exploitation.Privacy measures are provided on several social networking sites to try to provide their users with protection for their personal information. On facebook for example privacy settings are available for all registered users. The settings available on facebook include the ability to block certain individuals from seeing your profile, the ability to choose your "friends," and the ability to limit who has access to your pictures and videos. Privacy settings are also available on other social networking sites such as E-harmony and MySpace.

People with only a casual concern for Internet privacy need not achieve total anonymity. Internet users may achieve an adequate level of privacy through controlled disclosure of personal information. The revelation of IP addresses, non-personally- identifiable profiling, and similar information might become acceptable trade-offs for the convenience that users could otherwise lose using the workarounds needed to suppress such details rigorously. On the other hand, some people desire much stronger privacy. In that case, they may try to achieve Internet anonymity to ensure privacy, use of the Internet without giving any third parties the ability to link the Internet activities to personally-identifiable information (P.I.I.) of the Internet user. In order to keep their information private, people need to be careful on what they submit and look at online. When filling out forms and buying merchandise, that becomes tracked and because the information was not private, companies are now sending Internet users spam and advertising on similar products.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

Anonymity is a result of not having identifying characteristics (such as a name or description of physical appearance) disclosed. This can occur from a lack of interest in learning the nature of such characteristics, or through intentional efforts to hide these characteristics. An example of the former would include a brief encounter with a stranger, when learning the other person's name is not deemed necessary. An example of the latter would include someone hiding behind clothing that covers identifying features like hair color, scars, or tattoos, in order to avoid identification. Anonymity may also be created through a gradual eroding of ownership information, such as the passage of time and loss of attribution to a saying. For example, the quote, "Ignorance is Bliss" originally had a known author, but, over time, information on author's identity was obscured and has disappeared. Anonymizer provides fast, anonymous, interactive communication services. Anonymizer in this approach is essentially a web proxy that filters out the identifying headers and source addresses from web client requests. Instead of a user's true identity, a web server can only learn the identity of the Anonymizer- Server. In this approach, all rerouting paths have a single intermediate node, which is the Anonymizer-Server. Anonymous Remailer is mainly used for e-mail anonymity. It uses rerouting of an e-mail through a sequence of mail remailers, and then to the recipient such that the true origin of the e-mail can be hidden.

Tor aims to conceal its users' identities and their network activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers throughout the globe. Tor operation shown *Figure (2.4)* .These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location. That anonymity extends to the hosting of censorship-resistant content via Tor's anonymous hidden service feature. By keeping some of the entry relays secret (bridge relays), users can evade Internet censorship that relies upon blocking public Tor relays.

Because the internet address of the sender and the recipient are not both in cleartext at any hop along the way (and at middle relays neither piece of information is in cleartext), someone eavesdropping at any point along the communication channel cannot directly identify both ends. Furthermore, to the recipient it appears that the last Tor node (exit relay) is the originator of the communication rather than the sender. Users of a Tor network run an onion proxy on their machine. The Tor software periodically negotiates a virtual circuit through the Tor network, using multi-layer encryption, ensuring perfect forward secrecy. At the same time, the onion proxy software presents a SOCKS interface to its clients. SOCKS-aware applications may be pointed at Tor, which then multiplexes the traffic through a Tor virtual circuit. The Polipo proxy server can speak the SOCKS 4 & SOCKS 5 protocols and therefore is recommended to be used together with the Tor anonymising network. Polipo is a web proxy that does HTTP 1.1 pipelining well, so it can enhance Tor's communication latency.

Once inside a Tor network, the traffic is sent from router to router, ultimately reaching an exit node at which point the clear text packet is available and is forwarded on to its original destination. Viewed from the destination, the traffic appears to originate at the Tor exit node. Tor's application independence sets it apart from most other anonymity networks: it works at the Transmission Control Protocol (TCP) stream level. Applications whose traffic is commonly anonymised using Tor include Internet Relay Chat (IRC), instant messaging and World Wide Web browsing. When browsing the Web, Tor is often coupled with Polipo or Privoxy proxy servers. Privoxy is a filtering proxy server that aims to add privacy at the application layer. Polipo can speak the SOCKS protocol and does HTTP 1.1 pipelining for enhancing latencies, therefore is now recommended to be used together with the Tor anonymising network.

The aim of [1] is to provide backward unlinkability means that even after a member is revoked, signatures produced by the member before the revocation remain anonymous. Since signers have no load, signer's cost are lower and this approach is suitable for mobile environments. This paper focuses on the membership

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

revocation. By adopting time intervals all signatures from an illegal person should be traced. Revoked member remains excluded forever after revocation. By reducing the revocation tokens data size the signer has to perform additional computations which result in communication and computational overhead. In this scheme the signature are constructed from elements of groups that are created as multiplicative cyclic groups. It is better to construct a signature from only elements of initial groups.

In [2], the accumulator scheme is used along with bilinear pairings thus it allows to create a constant size signatures and providing membership revocation to group signatures. The size of our group signatures with membership revocation is only half the size of the well-known scheme, which does not provide membership revocation. Accumulator scheme allows aggregation of a large set of inputs into one constant-size value. There are three security requirements for ID-based ring signature schemes: Correctness, Unforgeability against Chosen Message, Group and Signer Attacks, and Unconditional Anonymity. The advantage of this method is creating constant size signatures and another advantage of our group signature scheme is perfect trapdoor-freeness, which allows sharing of public parameters among groups and organizations. The demerit of this paper is a need of more scalar multiplications for pairing operations.

In [3], a practical anonymous credential system that is based on the strong RSA assumption and the decisional Diffie-Hellman assumption modulo is proposed. To prevent misuse of anonymity, this scheme is the first to offer optional anonymity revocation for particular transactions. The communication and computation costs of this method are small, thus introducing almost no overhead to realizing privacy in a credential system. Separability ensures they can choose the encryption keys that they are needed. The drawbacks are the system lacks in scalability and for each revocation operation more exponentiations needed. The computation complexity arise due to more exponentiation affects the storage of bits.

The protocol implemented in [4] aimed to achieve mutual anonymity by constructing anonymous paths automatically. This protocol reduces the cryptographic overhead and there is no requirement on extra information for constructing paths. The protocol described in this paper is Rumor Riding (RR), a lightweight and non-path-based mutual anonymity protocol for decentralized P2P systems. RR takes advantage of lower overhead by mainly using the symmetric cryptographic algorithm. RR significantly increases the anonymity degree of a system. Random walk mechanism increases the difficulty for attackers to trace back to the initiator or responder. This mechanism is invulnerable to collaborating attack, timing attack, predecessor attack, traffic analysis and trace back attacks. The throughput of an initiator query depends on the rumor generation speed.

[5] provides a deep analysis of both the HTTP and BitTorrent protocols and its usage in terms of traffic size and number of connections but also depict how users behave on top of Tor. This paper show that many Tor users do not comply with the protocol, and rather prefer creating tunnels making Tor acting as a simple (1- hop) SOCKS proxy. This provide the proof for showing that it is easy to circumvent the bridges collection limits. Deep Packet Inspection (DPI) is mainly used in this method for the purposes of traffic shaping based on intrusion detection. The anonymization of the captured packets allows for preserving useful information. Using this method useless traffic is discarded. DPI is the most accurate and useful techniques to characterize the traffic. It also tackle the problem of application identification through deep packet inspection. In essence, more than half of the traffic carried over Tor is BitTorrent. It provide strong level of anonymity in favor of lower latency. This technique is vulnerable to crawling in which the exit nodes collects identities.

II. PROPOSED SYSTEM

To limit the number of identities a user can obtain the Nymble system binds nymbles to resources that are sufficiently difficult to obtain in great numbers. This implementation use IP addresses as the resource and this scheme also generalizes to other resources such as email addresses, identity certificates, and trusted hardware. This system suggest some promising approaches based on resource-based blocking since the aim is to create a real-world deployment. 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, as shown in *Fig.4.1* 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 pseudonym is always issued for the same resource. 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 IP addresses (or other resources) to pseudonyms. The user contacts the PM only once per linkability window.

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.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, linking tokens being used to link future nymble tickets.

If a user misbehaves, the server may link any future connection from this user within the current linkability

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

window (e.g., the same day). Consider *Fig. 4.2* as an example: A user connects and misbehaves at a server during time period t* within linkability window w*. The server later detects this misbehavior and complains to the NM in time period tc (t*< tc <= tL) of the same linkability window w*.As part of the complaint, the server presents the nimble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the user in time periods tc; tc +1; . . . ; tL of the same linkability window w_ to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day, for example (the linkability window). Note that the user's connections in t1; t2; . . . ; t*; t*+ 1; . . . ; tc remain unlinkable (i.e., including those since the misbehavior and until the time of complaint). Even though misbehaving users can be blocked from making connections in the future, the users' past connections remain unlinkable, thus providing backward unlinkability and subjective blacklisting.

III. SYSTEM DESIGN

Design Engineering deals with the various UML [Unified Modeling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product. A user with identity uid must register with the PM once in each likability window. To do so, the user initiates a type-Basic channel to the PM, followed by the User Registration protocol described below. A login generally requires the user to enter two pieces of information, first a user name and then a password. A user name, also referred to as an account name, is a string (i.e., sequence of characters) that uniquely identifies a user. User name can be the same as or related to the real names of users, or they can be completely arbitrary. A password is likewise a string, but it differs from a user name in that it is intended to be kept a secret that is known only to its use.

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, and can ensure that users are communicating with it directly. Pseudonyms are deterministically chosen based on the controlled resource, ensuring that the same pseudonyms always issued for the same resource.

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.

Servers update their blacklists for the current time period for two purposes. First, as mentioned earlier, the server needs to provide the user with its blacklist (and blacklist certificate) for the current time period during a Nymble connection establishment. Second, the server needs to be able to blacklist the misbehaving users by processing the newly filed complaints (since last update).

IV. RESULTS AND DISCUSSION

The user registration page is used for new user to login this application by providing full personal details. It checks the user name and password of particular user and if it is valid then allow user to navigate into nymble system.

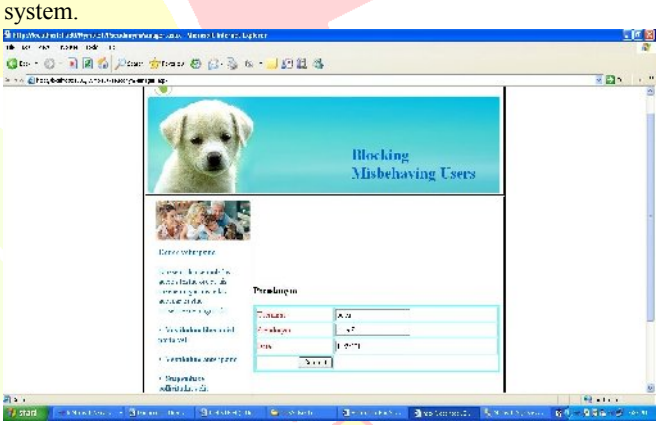

Fig.1. Pseudonym Generation

The above page represents pseudonym generation which are deterministically chosen based on the controlled resource and given to the user.

Fig.2.Ticket Generation

The user connects to the Nymble Manager through the anonymizing network, and requests for nymble ticket

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

for gaining access to a particular server. This page generates nymble ticket for particular user-server pair.

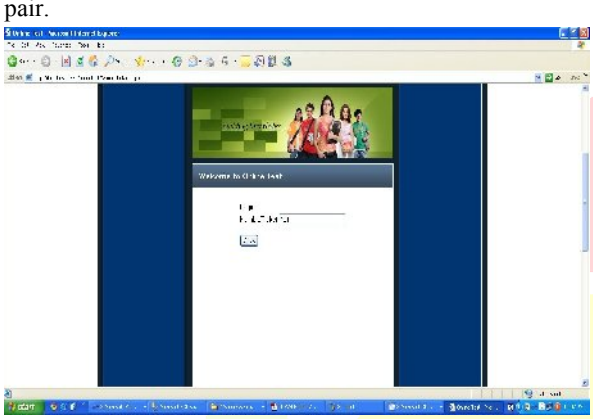

Fig.3.Online Test

This is the Home page of user selected server and in this page user enter the nymble ticket and enter into online test application.

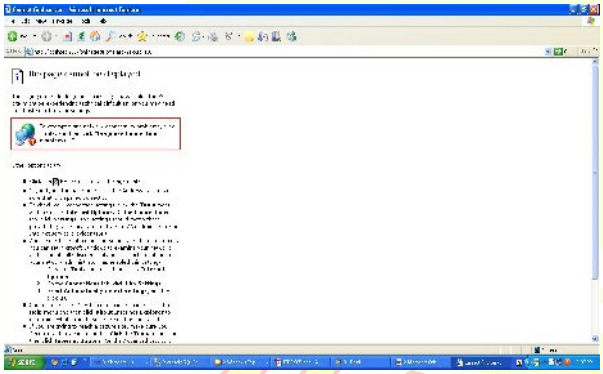

Fig.4. Blocked Message

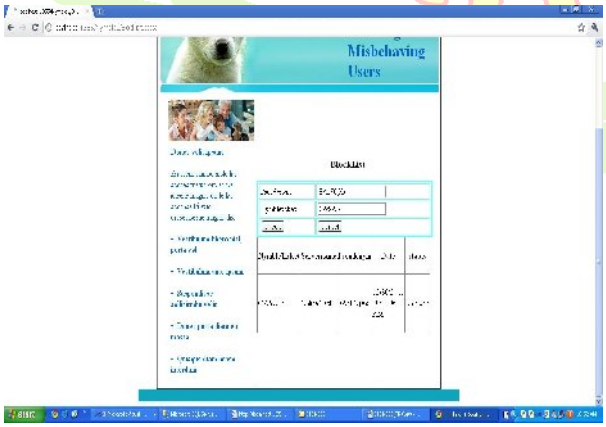

Fig.5. Blacklist Status After Updation

V. CONCLUSION

In this paper the proposed system adds a layer of accountability to any publicly known anonymizing network is proposed. Servers can blacklist misbehaving users while maintaining their privacy, and this system shows that how 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, thus far, been completely blocked by several services because of users who abuse their anonymity. In future the Nymble system can be extended to support Subnet-based blocking. If a user can obtain multiple addresses, then nymble-based and regular IP-address blocking not supported. In such a situation subnet-based blocking is used. Other resources include email addresses, client puzzles and e-cash, can be used, which could provide more privacy. The system can also enhanced by supporting for varying time periods.

REFERENCES

[1] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures,"Proc. Conf. Public Key Cryptography, Springer, pp. 190-206,2001.
[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] 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.
[4] I. Damga°rd, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'lCryptology Conf. (CRYPTO), Springer, pp. 328-335, 1988.
[5] 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.
[6] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators andApplication to Efficient Revocation of Anonymous Credentials,"Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76,2002.
[7] J. Camenisch and A. Lysyanskaya, "Signature Schemes andAnonymous Credentials from Bilinear Maps," Proc. Ann. Int'lCryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.
[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] 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.