Blocking Misbehaving Users In Anonymizying Networks-Embedded Based

R.Divya
2nd year ME communication systems
S.A Engineering College
Chennai-600077
divyarajaa@gmail.com

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 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.

There are several solutions to this problem, each providing some degree of accountability. In pseudonymous credential systems users log into Web sites using pseudonyms, which can be added to a blacklist if a user misbehaves. Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network. Anonymous credential systems employ group signatures. Basic group signatures 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 thus, lacks scalability. 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 as desired, where a user's accesses before the complaint remain anonymous. With dynamic accumulators 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.

In higher level of networking blocking misbehaving users in anonymizying networks in computers is done. Here in this project the misbehaving users are blocked in lower level of networking that is in mobile networking by using software simulation in first phase and hardware implementation will be done in second phase.

1. INTRODUCTION

In this paper the misbehaving users are blocked in lower level of networking that is mobile networking. This is done by using software simulation in first phase and based on embedded systems in second phase.

2. NETWORK SECURITY

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 is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password 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.

3. EXPERIMENTAL SETUP

The software used here is 'proteus'. In 'proteus' pic microcontroller is used along with rs232 cables. The experimental setup or the block diagram can be given as in figure.

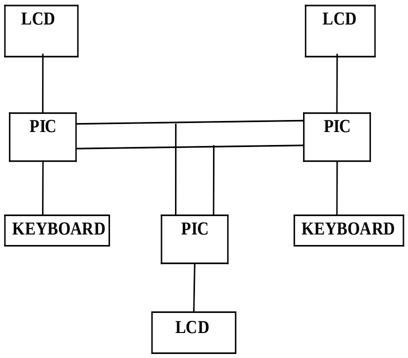

Figure.1 block diagram

First the microcontroller pic (peripheral interface controller) is connected with the mobile LCD display in the hardware setup. In the software setup the microcontroller is connected with rs232 cable. One will be the transmitter side other receiver side and the centre one is the unauthorized person.

4. ANONYMIZYING NETWORKS

Tor (short for The Onion Router) is a system intended to enable online anonymity. Tor client software routes Internet traffic through a worldwide volunteer network of servers in order to conceal a user's location or usage from someone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity, including "visits to Web sites, online posts, instant messages and other communication forms", to the user. It is intended to protect users' personal freedom, privacy, and ability to conduct confidential business by keeping their internet activities from being monitored. "Onion routing" refers to the layered nature of the encryption service: The original data are encrypted and re-encrypted 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 the destination. This reduces the possibility of the original data being unscrambled or understood in transit.

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. 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 clear text at any hop along the way (and at middle relays neither piece of information is in clear text), 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.

I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.

Many applications are available that interface with I2P, including mail, peer-peer, IRC chat, and others.

The I2P project was formed in 2003 to support the efforts of those trying to build a more free society by offering them an uncensorable, anonymous, and secure communication system. I2P is a development effort producing a low latency, fully distributed, autonomous, scalable, anonymous, resilient, and secure network. The goal is to operate successfully in hostile environments - even when an organization with substantial financial or political resources attacks it.

A. What to hide?

Sender anonymity: attacker cannot determine who the sender of a particular message is.

Receiver anonymity: attacker cannot determine who the intended receiver of a particular message is.

Unlinkability: attacker may determine senders and receivers but not the associations between them (attacker does not know who communicates with whom)

B. From whom to hide?

Communication partner (sender anonymity) External attackers: local eavesdropper (sniffing on a particular link (eg: LAN)), global eavesdropper (observing traffic in the whole network).

Internal attackers.

5. ANONYMITY

Sender anonymity: A particular message is not linkable to any sender and that to a particular sender, no message is linkable.

Recipient anonymity: A particular message cannot be linked to any recipient and that to a particular recipient, no message is linkable.

Relationship anonymity: The sender and the recipient cannot be identified as communicating with each other, even though each of them can be identified as participating in some communication.

6. TYPES OF ATTACKS

Insider Attack: it is significant percentage of breaches. For example, Run-on fraud, disgruntled employees.

Lunchtime Attack: this attack takes place during a small window of opportunity. For example during a lunch or coffee break. Focused Attack: for this attack time, money, and resources not an issue.

7. TYPES OF ATTACKERS

Clever Outsiders: they may be intelligent, but have limited knowledge of the product. They usually take advantage of a known weakness. For example Curious kids, college students.

Knowledgeable Insiders: persons having Substantial specialized technical experience and have highly sophisticated tools and instrument. For example, Professional engineers.

8. GOALS OF ATTACK

Competition (or Cloning): It is a Specific theft done to gain market place.

Theft-of-Service: It is obtaining a service for free that normally costs money.

User Authentication (or Spoofing): It is forging a user's identity to gain system access.

Privilege Escalation (or Feature Unlocking): It is gaining increased command of a system or unlocking hidden and undocumented features.

9. CONCLUSION

The encrypted data can be decrypted only by the receiver and not by the unauthorized person. The unauthorized user cannot even hack the encrypted data. It can hack only some fake data.

REFERENCES

1. D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.
2. 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.
3. P.C. Johnson, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.
4. G. Ateniese, D.X. Song, and G. Tsudik, "Quasi-Efficient Revocation in Group Signatures," Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2002.
5. 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.
6. S. Goldwasser, S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Computing, vol. 17, no. 2, pp. 281-308, 1988.