2013 Third International Conference on Advances in Computing and Communications

# Non repudiation for internet access by using browser based user authentication mechanism

Nithesh K.Nandhakumar
IT department,
Salalah College of Technology
Dhofar Governorate, Salalah,
Sultanate of Oman
nitesh.n@sct.edu.om

Binu A.
Dept. of Information Technology
Rajagiri School of Engieering &
Technology, Ernakulam , India
binu_a@rajagiritech.ac.in

Viji Paul
IT department,
Salalah College of Technology
Salalah, Sultanate of Oman
viji.p@sct.edu.om

*Abstract*— **Having a secured internet transaction is a real big challenge in this new era of net-based social engineering, hacking, impersonation and fraud. Hence, user authentication has become really important for all kinds of internet browsing transactions. This is especially true when we need to identify the exact users who have actually used the system, irrespective of the device address or location, from where the user committed internet access. The main aim of this paper will be to present a model for validating user-identity especially for internet browsing using browser software. This user validation will be carried over with respect to the ISPs which were used for service access. The main reason behind this spurred from the thought of different users using internet cafes, borrowed wireless modems or just temporary kiosks available in transport transit points like airports, restaurants and other public spots, anonymously and thus posing the danger of violating the security principle of non-repudiation. Another dangerous trend which is observed is the use of proxy programs, because of which any banned or blocked sites, can be accessed with ease. This all leads to the scenario where any unregistered user can visit, access and download any internet placed resources, for which de-centralized network infrastructures have no control of. In this paper, we are recommending a browser based user authentication scheme that can be combined with hashing and biometrics to properly validate a user so that he will be held liable for all actions committed by him in the cyber-world.**

***Keywords- Browser security; internet authentication; browser based validation; user identification; non-repudiation; internet transaction; secured internet sessions***

## I. INTRODUCTION

User authentication refers to the process of validating the identity of a user. This would mean that the system has to identify the user and check against a stored database to see if the user is permitted to use the system. For that, various schemes have been identified including user-name/passwords, one-time passwords, KERBEROS authentication, biometrics etc. that are having its own benefits and demerits.[10]

Web browser is an application-software which is used to access the internet resources available in the internet. These information resources exist as files and grouped together under a domain name which can be identified as well as referred by using a Uniform Resource Identifier (URI). Browsers are primarily being used to access the World Wide Web contents and can be used to get access to intranet/ private networks too or network file systems based on protocols like FTP, Telnet etc. The major web browsers are Firefox, Google Chrome, Internet Explorer, Opera, and Safari.[8]

Users access internet using Internet service provider (ISP) which are usually huge organizations that can be public/private in ownership. They are having huge network infrastructure for forwarding data traffic to devices. They use channels laid across the region using copper-wires, optical fibers and also wireless medium. [1] The different technologies that exist for user connection are also varied, based on the transmitting speed and bandwidth. We have ISPs that can be grouped as Transit and Hosting ISPs based on the server space, and are leased. [2]

User authentication for Internet access in ISP works as follows- Users can access internet using the different technologies available at his disposal as described above. For dial-up and DSL connections the user has to login using the user-name and password, where as for shared network, just plugging in the device using the cable is enough. Proxy setting using IP address and the port number may be necessary in a shared network setting, if that is not supplied by the DNS server running DHCP.[8]

Wireless connections require the use of authentication too; WPA2 being the new encryption standard used, offering more security than WEP.[3]

Web access security is of concern here as the basic security concepts critical to Internet information security are confidentiality, integrity, and availability, which is left as a future discussion topic as far as our paper is concerned. The concepts of authentication, authorization, and non-repudiation are what are related to the people who are using that information, which is what this paper is all about. Out of that, non-repudiation is what is of concern to web authentication to make the users accountable for the actions that they do in the internet and also for the usage of accessed information at a later stage.

There are some studies conducted in the same line which are discussed in the next section of related works.

978-0-7695-5033-6/13 $26.00 © 2013 IEEE
DOI 10.1109/ICACC.2013.62



IEEE computer society

### A. REVIEW OF PRIOR WORK

M.Mallikarjuna, et.al [11] discusses the technique of using a universal web authentication system by using a unique web identity. Here the gist is to use a Universal Web Id for net based authentication system. The system however doesn't venture into maintaining their own database, which becomes a problem for tracking users accessing across diverse domains. Work of Yu Sheng and Zhu Lu[12] is also worth discussing here which envisages a scheme to combine the password entered by user, password associated with private key protected by trusted platform module and user certificate given by a trusted computing platform. Because of this, picking the password alone on the web will not have an effect on user's security.

A study by Ayu Tiwari and Sudip Sanyal[13] proposed a new protocol using multifactor authentication system that is both secure and highly usable, using Transaction Identification Code and SMS to give extra security level using username/password system. This approach requires an additional reliance on external SMS services that may hinder the performance of the system.

### B. PRINCIPLES OF SECURITY

The following principles which are of vital importance for any internet based transactions [6] [7] are discussed here.

*a) Integrity*

This principle refers to security features which will enable data transfer so that message is not altered in an unauthorized manner. This is called Data Integrity and can apply to items while in storage or process too. This principle is critical in financial and other sensitive digital transactions and storage.

*b) Confidentiality*

Confidentiality essentially means secrecy and requires that the private information may not be leaked outside authorized entities. Data has to be kept secret in transit, saving or processing. Research data, copyrighted materials, insurance and other corporate records will come in this category.

*c) Availability*

Availability principle is required for prompt working of the system so that its service is not denied to valid users. The main emphasis will be on authentication and authorization, which are discussed next.

*d) Authentication*

Authentication will let the system identify who is who. It will let a user to validate themselves and then identify him. This can be done using username/password technique( what the user knows) or by what the user carries, like his smart-access card. It can be done by using person's identity too like using biometrics (example:-fingerprint, eye-scan, voice recognition etc.). Authorization is another act which goes along with authentication and gives rights or privileges to authenticated users on the computer resources. [10]

*e) Non repudiation*

Non-repudiation, with reference to ISP authentication for internet browsing activities is related to an assurance for which the 'doer 'or user is responsible. Non-repudiation is like a non-bail warrant because of which, the party in contract or communication cannot deny the actions because of the authenticity of their signature affixed while committing the action. This can be just an act of sending an email, browsing an internet resource or downloading/uploading file in the net. Repudiate or deny with respect to a digital action can be challenged by using a digital signing, biometrics or by digital certificates. [4]

## II. PROBLEM DEFINITION

There can be a situation where different users will use internet for downloading illegal stuff or use net resources for transactions against the law of the land. How is it possible to ever track these users and record the actions that they commit? What all evidences can be there for a forensic investigator so that it can be used effectively against them? And lastly but not the least, how to employ non-repudiation principle effectively so that these perpetrators don't escape the punishment they ought to receive.

The major hurdle is the de-centralized network infrastructures from where these types of illegal activities occur over which there is little monitoring or control. Also logging the user identity is also a big challenge, based on which only we can initiate legal actions. MAC address recording is a long soughed solution, along with tracing the IP address of the machine to which it is leased to by the ISP of. These can be easily circumvented by the use of MAC address altering software, which are so easy to achieve.[5] Again the use of proxy services, both online and application ones that can run from your PC will defeat all attempts to log IP address.

Use of unregulated internet cafes, borrowed wireless modems or ad-hoc temporary Wifi spots can all lead to situations where tracking of user authentication difficult. Now the problem that is worrying for all forensic investigation is this scenario where any anonymous user can visit, access, download and transact these illegal digital contents with ease, leaving no trace and identity of the user.

## III. PROPOSED SOLUTION

For achieving Non repudiation for digital transactions, digital signatures can be used. This is more applicable for document or messages by which we can ensure that the signature will identify the people who send/typed it, and also, since a digital signature can only be created by one party, it will ensure that a person cannot later deny his actions. [10]

Also as no security technology is perfect and fool-proof, it's suggested that multiple approaches may be used. This will include capturing biometric information and other data about the sender or signer. This will make the whole process more difficult to repudiate and identify the user in the most precise manner.

In our case, repudiation has to be applied to web-browsing. This is more tricky compared to the earlier scenarios, viz., message/document sending or email transmission. Here sessions have to be identified for each user and then the system has to identify who the user is, the one doing internet browsing at that particular point of time. Logging of this information needs to be done also in a perfect manner. This logging has to be centrally stored and administered so that it will be easy for any forensic investigator or legal agency to check the status of a valid browser at a particular session even in a remote manner. Apart from that, this identity information system has to be fail-safe in case of a system failure. In the event of an illegal login attempt, the system has to have a fool-proof mechanism encompassing the biometric techniques to invalidate the session and prevent the users from logging in and using internet.

### *A. Public User validation- Region or country specific*

Just like getting a SIM card for mobile connections, there is the need to establish a centralized governmental agency to validate internet users. This is synonymous of getting a phone connection or gun license or liquor permit where the users have to furnish their details before hand. In this case, users need to validate using their credentials and submit their biometric information in the central system. A trusted 3rd party can be used for this purpose, similar to certification authorities like verisign and thawte. This will be individualistic for a country or province where laws and cyber-acts need to be amended to achieve this. This will also help the state to fight cyber-crimes and apply penalties to those who are acting illegally in the cyber-world.

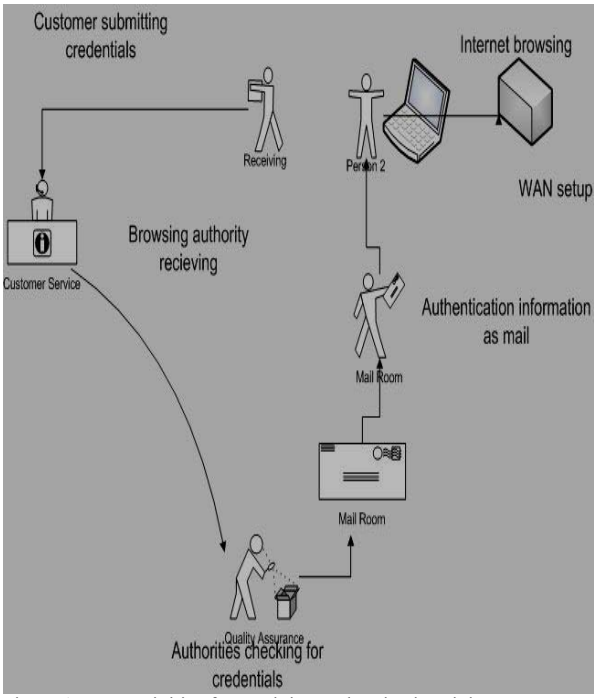

Figure 1. User activities for receiving authentication rights

Figure1 gives an idea about the intended internet user actions which are mandatory for enabling browsing rights. For using internet in a specific regional network provided by the ISP, the end user has to first submit his credentials to the browsing authority (BA) who will check for credentials, much similar to the way a Certification Authority do. This can be time consuming as the BA need to co-ordinate with other agencies like police and emigration departments to check the credentials. Here the user will be registering his biometric information also like iris-scan images or fingerprints. Once that is recorded, the customer has to wait for a period of time before he can start browsing. Mail will be send to the user at his registered address which will contain his session user name and password, which has to be changed as per his convenience.

After the above said procedures are completed, the user can browse the internet provided by his subscribed Internet Service Provider. The purpose of non-repudiation is achieved thus, but it must be noted that non-repudiation is possible without identity information too as per [6]. But this is not recommended as any authentication without using identity information can jeopardize the very intention of this scheme, that is, to give maximum level of personalization for all browsing session done by a party.

### *B. User validation using browser in the application level*

Once the user receives his username and password he can start using the browser for accessing the net. But here also there is a need for checking the user identity that will form the second level of surveillance. For achieving this, we need to change the basic working of the browser itself.

Currently all browsers will just start working and will fetch internet data once it detects a net connection directly or through proxy. This has to be changed. Our proposal is to change the application level code itself to include an authentication dialog box as soon as the browser is run, and thus prevents the users from directly accessing the internet data. This dialog box or authentication window will run on top of the browser window and on successful login only will the users be allowed to see the internet data.

Design of the authentication module in the browser will be country specific too and while installation or after setting up, the users (or administrators preferably) should be allowed to configure the browser to supply the server address that will be authenticating the users. Now if it is region-wise, we can easily supply the local server address of Authentication Agency or Browsing Authority (BA) that will be handling the authentication by means of an ip-address or DNS name.

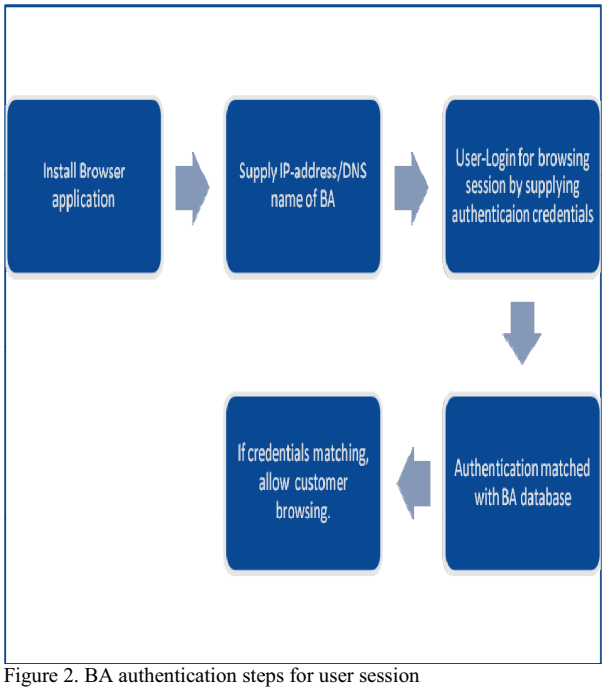

Figure 2. BA authentication steps for user session

As shown in Figure2, the credentials entered by the user in the form of username password, session key or biometric information will be sent to the BA and will be validated. If the credentials are matching, the user will be allowed to do internet browsing.

## IV. CONCLUSION

The proposed solution addresses the problem of identifying and enforcing non-repudiation for all internet transactions including just browsing. These mechanisms are justifiable and enforceable in regions where the infrastructure is ready for user registration and systems which can generate non-breakable random passwords for individual user sessions. This is having an additional overhead of setting up the centers in many places according to the density of population. Additionally it needs a radical change in all browser software s too which has to dealt in a more comprehensive way. This is because of the reason that even the availability of one browser not needing authentication in the market will jeopardize the whole mechanism. But the way to deal with these kinds of "no-authentication-needed browsers" will be to block all requests in the ISP level itself by matching the browser meta information send along with all internet packet data. An additional hurdle will be to apply this in a network domain under a common management. Here the task of administrator to enable route forwarding of all traffic to ISP and the systems in the ISP for invoking additional session management by BA validation to authenticate the user is a huge challenge for future work. The need to enhance non-repudiation by using timeout management of the session, on user inactivity has also to be studied.

## REFERENCES

[1] Daview D. and Price W(1989)., *Security for Computer Networks,* New York Wiley.

[2] Chalie Kaufman, Radia Perlman, Mike Speciner, *Network Security* Pearson Education. B. Schnier,

[3] Steve Burnett & Stephen Paine(2001), *RSA Security's official guide to cryptography* McGraw-Hill, Mar 29

[4] Dieter Gollmann(2007), *Computer Security*, John Wiley, pp-56-60

[5] Security+ Training Guide by Todd King Que Publishing, Apr 1, 2003 – P- 36-42

[6] Charles A. Shoniregun(Jul 2007), Synchronizing Internet Protocol Security (SIPSec) Springer, , page 151

[7] L. Jean Camp Trust and Risk in Internet Commerce, MIT Press, Sep 1, 2001 page 76 77

[8] Electronic Publication: *World Wide Web Security FAQ: at* http://www.w3.org/Security/Faq/www-security-faq.html [Accessed 10/4/2013]

[9] Electronic Publication: *OpenSSL Project:available at* http:/www.openssl.org [Accessed 10/4/2013]

[10] Electronic Publication: *Request for Comments 2617 : HTTP Authentication available at* http://www.ietf.org/rfc/rfc2617.txt [Accessed 10/4/2013]

[11] M.Mallikarjuna,et.al(2013) *Universal web authentication system using unique web identity*- - Dept. of ISE, Reva Institute of Technology and Management . (Proceedings of Seventh International Conference on Bio-Inspired Computing:Theories and Applications, Advances in Intelligent Systems and Computing, Springer India)

[12] Yu Sheng and Zhu Lu(2008) *An Online User Authentication Scheme for Web-Based services*- Proceeding ISBIM '08 Proceedings of the 2008 International Seminar on Business and Information Management - Volume 02 Pages 173-176 , IEEE Computer Society

[13] Ayu Tiwari and Sudip Sanyal (2011)-*A Multi-Factor Security Protocol for Wireless Payment* - Secure Web Authentication using Mobile Devices-IADIS International Conference on Applied Computing Proceedings of the IADIS International Conference on Applied Computing, Salamanca, Spain.