ISSN No. 0976-5697

Volume 5, No. 3, March-April 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Attaining Credential Privacy by Soundness Preventive Click Point Password (SPCP) Scheme

D. Devipriya*
P.G. Scholar
Nandha College of Technology Erode, India

M. Vijayakumar
Professor and Head
Nandha College of Technology Erode, India

Abstract: Bogus servers and user collusion are malicious activities present in Distributed computer networks which illegally access and enjoy the resources. Bogus servers are service providers who communicate with legal users to obtain valid credential and User collusion is the process done by malicious users without legal credential. Both the activities are protected by Primary and Secondary Authentication System which is introduced in this paper. Primary authentication system deals with CRH (Collusion resistant hash) Function which is one way hash function. It is the unitary token method and HMAC function is used for stronger security. Secondary authentication system works with two dimensional passwords. Two dimensional passwords are the combination of Text and click point password. The implementation of AES Encryption helps to make click point to be confidential. In this paper, we can prevent bogus servers and user collusion and forgery activities in distributed networks efficiently. This paper is implemented to provide greater security in confidential applications especially in banking and mobile phones.

Keywords: key logger, phishing, shoulder-surfing, credential privacy, unforgeability, soundness

I. INTRODUCTION

Distributed Computer Networks consists of the multiple numbers of service providers and the multiple numbers of users connected by the internet. The geographically distributed resources are interconnected as a unified single resource. The distributed networks may be loosely or tightly coupled systems. It contains the heterogeneous collection of systems and the collection of hardware and software systems that have components. The components are not sharing the memory. Instead the synchronous and asynchronous messages are being passed.

The current research area works on providing the assurance of the legitimate users connected by the legal service providers. But it is very difficult in the real time applications to provide the valid credential which is authenticated by the legitimate server. An example of such usage of distributed applications is Peer to peer networks. P2P networks [3] are the overlay networks using over the physical or logical network. The distributed Computing is done in the Distributed Computer Networks. The Computing Process can be done by dividing the whole task into the subtasks. The message is passed for the communication.

The problem occurred in the Distributed Computer Networks can be solved by any of the computer. An Objective of the distributed computer networks are location transparency and security. The security must be established by attaining unforgeability, soundness and credential Privacy. Unforgeability assures that the untrusted users must not enter into the system and access the services. Soundness proves that the uncivilized users must not enter into the system. Credential Privacy assures that the credential must not be obtained by the illegal users. This paper is organized as follows: Section 2 discusses about the authentication and section 3 discusses about the existing systems.

Section 4 introduces the unitary token methodology and Section 5 introduces the two dimensional passwords. Section 6 explains about the implementation and Section 7 figures out the System Architecture of the project.

II. AUTHENTICATION

The major part of the system involves by identifying the authenticated users. So the authentication takes place as an important role. The authentication is the process done in all the websites. An initial process involves by doing the registration. It is an initial step which is done by getting the details from the users like user name, password, phone number, mail id. After the registration phase has been completed the authentication is done. There are several authentication schemes used.

A. Knowledge based Scheme:

Textual password is the best example of this authentication scheme. It can be done by the traditional password scheme like login and password.

B. Token based Scheme:

Token based scheme includes the generation of token and can be used in Credit cards and ATM cards.

C. Biometrics based Scheme:

Biometrics scheme includes thumb impression and face recognition. It includes graphical password [1], iris recognition, face recognition, retina, etc.

Ideally there are many types of Authentication schemes are available according to nature of scheme & techniques used.

D. Recall based Scheme:

In this authentication technique, users need to recall or remember his/her password which is created before. Knowledge based authentication is a part of this technique like textual password and graphical password. This technique is commonly used all over the world where security needed.

E. Recognition based Scheme:

In this scheme, user need to identify, recognize password created before. Recognition based authentication is used in graphical password. This technique is not used frequently like the Recall based technique. Still both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time.

III. EXISTING SYSTEM

When the prevention of bogus servers and user collusion takes place we need to study about the following existing Systems.

*A. Persuasive Cued Click-point Authentication Mechanism with Dynamic User Blo*cks:

The persuasive technology is used for the guidance to provide the efficiency in all fields. In the security this technology helps to provide the stronger security [2]. The usability goal is to guide the users in creating graphical passwords to implement efficient security. Security is done efficiently in remote field bus access in some papers [4]. In RFID based product can also be protected with new mechanisms [5].

The security level is not fixed for all the applications. The PCCP with dynamic user blocks approach presents a more feasible way of varying the security level. It depends upon the user's requirements. Disadvantage is the hotspots of small number of users can be collected and an attack dictionary can be formed. This system refers to overcome the drawbacks of base paper [6].

B. 3D Password Authentication System with Sound Signature:

This system provides the Authentication to any system leads to provide more security to that system. There are many drawbacks arised in Generalized digital signature [7]. For overcoming the drawbacks the new system has been evolved. A new 3D improved authentication technique is used here [8]. It consists of Biometrics, text and the graphical passwords.

Sound Signature is used by the sound clips and the pause time. If the pause time and the sound clip entered previously are correct the user is authenticated otherwise the user is considered as outsider. Disadvantage is most of the biometric systems require a scanning device to authenticate users.

C. Differentiated Virtual Passwords:

A virtual password is a dynamic password that is generated differently each time from a virtual password scheme and then submitted to the server for authentication [9]. It contains the user defined function which is called as the secret little function.

The function is the bijective function which is the combination of injective and surjective function. Disadvantage is an extra effort is required in programming the function into the server upon the creation of an account, so human effort may be need.

D. Pass points graphical password scheme:

A Pass point password is a repeated sequence of points which is selected by a user in an image which is displayed on the screen [10]. To log in, it needs to repeat the sequence of clicks in the correct order. Users may select any pixels in the image as click-points for their password. Disadvantage is lower memorability of pass points and prone to shoulder-surfing attack.

E. Click-Based Graphical Passwords:

The user is required to select one or more predetermined positions on the displayed image in a particular order to indicate his or her authorization to access the resource [11]. Disadvantage is an extra hardware may be needed and it is difficult to remember.

F. Proximity Authentication for Mobile Devices:

Proximity based system explores the location oriented user authentication [12]. If a user is in the location which is outside the predefined boundary, the authentication framework rejects the user else authenticated. Otherwise the user is accepted as the legitimate person. It can be used in Government applications. Disadvantage is the handler has to maintain a table of potential beacons to carry out its function.

IV. UNITARY TOKEN METHODOLOGY

a. The unitary token method is the one way collusion resistant hash function. It cannot be reversible and it can be done efficiently in the distributed networks. On receiving the token of the existing session the new session is opened. CRH(Collusion resistant Hash) is the Unitary token methodology which can be used as the Primary Authentication scheme in
b. In this module, the user is generated and issued an one time token which can be later used by the user for authentication and to access the services.
c. The secret token Si is computed as $Si = (IDi||h(IDi))d \bmod N$, where $h(\cdot)$ is a collusion-resistant cryptographic one-way hash function.
d. In this module, if the user Ui wants to access the resources of the provider Pj, Pj must authenticate the legitimacy of Ui. The user identification phase performs the following steps.
e. The service request with a random nonce is submitted by the user to the provider.
f. Provider computes session token and hash code using HMAC function and sends it to the user.
g. Upon receiving the session token from the provider, the user checks the integrity of the token by applying hash function to the session key.
h. After ensuring the integrity and the validity of the token, the user can use it for login to get access to the services.

V. TWO DIMENSIONAL PASSWORDS

Efficient Usage of Two Dimensional Passwords acts as the secondary authentication scheme. Passwords are the secret string of characters that can be used for the identification which helps the user to access the resources. Single Dimensional passwords are used to provide the simple security with the username and passwords as the knowledge passed authentication.

The two Dimensional passwords are the text password and the graphical passwords. Graphical passwords are used

for the identification with the images and the click points in the images. The three Dimensional Passwords are the text, graphical and biometrics passwords. The biometrics password are identified by the face recognition, retina, etc.

The process of getting into each dimension and then enter into the system tends to be difficult and it seems like the overload for the user. It needs to be avoided to improve the performance since the speed of the distributed system is very important.

It improves the usability of the system in the banking sectors if the simpler authentication system is used by the customers. The interface guides them step by step fashion. The secondary authentication scheme in this paper is two dimensional passwords along with the onetime token generation.

VI. IMPLEMENTATION

For the efficient authentication, IBRAS (Image Based Registration and authentication System) is a simple authentication system, which uses images as passwords as an enhancement with the AES cipher. The user submits user ID and an image click point as credentials to the system. If it matches with the one stored in the system, the user is authenticated. It is explained with the Fig.1. Images are not difficult to remember and it is not difficult to guess images.

The process of performing brute force attacks on such systems is very difficult. Whenever the user enters into the system at the first time, user has to register him with the system with all his details. The interface is used for the user in a step-by step gradual fashion. There is only minor change is to be made to the existing password based Systems to incorporate the use of images. The system is simple. It is the Password based one. The original images are not stored in the system. Only the calculated hashed values are stored. The same desired image can be carried by the user.

This system is easy for Internet applications IBRAS is designed as an efficient security tool for demonstrating basic security mechanisms or as an access control system in any of the applications needing authorization.

- ***a. Mail Sending-***The user can utilize this module to send mails as the legitimate user. For this, the user has to register with original mail id. Internet connection is needed.
- ***b. Data Download-*** The user can view the data in the provider's database. The user can download the data from the provider database. The user can store it in the local drive for their personal or official use with respect to the user's wish.

VII. SYSTEM ARCHITECTURE

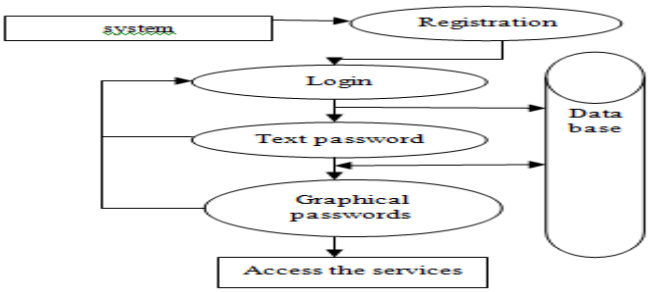

Figure.1. System Architecture

VIII. CONCLUSION

In this paper, we demonstrated how the collusion resistant hash function along with two dimensional passwords is implemented to protect the distributed computer networks against the phishing, key-logger and shoulder-surfing attacks. It is done as the efficient single sign-on method that helps to protect from the bogus servers and the user collusion by the implementation of unforgeable authentication scheme.

IX. REFERENCES

[1]. Alankrita Ladage, Swapnil Gaikwad, Chougule A B, ”Graphical Based Password Authentication”, International Journal of Engineering Research and Technology, volume 2, no.4, April 2013.

[2]. Anu Radha D, Abdul Hakeeem C,” A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks”, International Journal of Research in Engineering and Advanced Technology, volume 1, no. 1, March 2013.

[3]. Barolli L and Xhafa F, “A P2P platform for distributed, collaborative computing”, IEEE Transaction in India, volume 58, no. 6, pp. 2163–2172, October 2010.

[4]. Cheminod M, Pironti A, and Sisto R, “Formal vulnerability analysis of a security system for remote field bus access”, IEEE Transaction in India, volume 7, no. 1, pp. 30–40, February 2011.

[5]. Fabian B, Ermakova T, and Muller C, “A privacy-enhanced discovery service for RFID-based product information,” IEEE Transaction in India, volume 8, no. 3, pp. 707–718, August 2012.

[6]. Guilin Wang, Jiangshan Yu, and Qi Xie, “Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks”, IEEE Transactions on Industrial Informatics, volume 9, no.1, February 2013.

[7]. Harn L and Ren J, “Generalized digital certificate for user authentication and key establishment for secure communications”, IEEE Transaction in Wireless Communication, volume 10, no. 7, pp. 2372–2379, July 2011.

[8]. Jay want N, Khedkar, Pragati P, Katalkar, Shalini, Pathak V, “Integration of Sound Signature in 3D Password Authentication System”, International Journal of Innovative Research in Computer and Communication Engineering, volume 1, no. 2, April 2013.

[9]. Kanagaraj S, Javith Ibram Sha M, Madhan Kumaran D, Rajkumar D, “Differentiated Virtual Passwords For Protecting Users From Password Theft”, International Journal of Engineering Research Science and Technology, volume 2, no. 2, May 2013.

[10]. Memon N, Dirik A E “Modeling user choice in the PassPoints graphical password scheme”, Proceedings of the third symposium on Usable privacy and security in ACM, 2007.

[11]. Van Oorschot P C, Sonia Chiasson, Robert Biddle,”A Second Look at the Usability of Click-Based Graphical

Passwords", Symposium On Usable Privacy and Security (SOUPS), July 18-20, 2007.

[12]. Wayne Jansen, Vlad Korolev, Serban Gavrila, "Proximity-based Authentication for Mobile Devices", Springer, volume 22, June 2005.