International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 4 (May 2013), PP. 55-58

Image Based Authentication for E-Mail System

Parimita Das, Prof. Kavita P. Shirsat
M.E (Computer Engg.), VIT,Wadala(E),Mumbai,India
Dept. Computer Engineering, VIT,Wadala(E),Mumbai,India

Abstract:- Secure environments protect the resources against unauthorized access by enforcing access control mechanisms. Therefore, when increasing security is an issue, text based passwords are not enough to counter such problems. Security has always been an issue since Internet and Web Development came into existence, numeric based passwords is not enough to counter such problems, which is also an out dated approach now. Therefore, this demands the need for something more secure along with being more user- friendly. Therefore, we have tried to increase the security by involving an image based authentication approach, involving text based password , Image Based Authentication and automated generated one-time password (received through an automated process on mobile of the authentic user). And an assiduous effort has been done for preventing Shoulder attack, Tempest attack, and Brute-force attack at client side , through the use of unique image in the Image Based Authentication (IBA) System for e-mail communication**.**

Keywords:- Image Based Authentication system (IBA), AJAX , Keystroke Logging, One Time Password, Tempest Attack, shoulder Attack and Brute force Attack.

I. INTRODUCTION

Authentication plays a crucial role in protecting resources against unauthorized and illegal use. Authentication processes may vary from simple password based authentication system to costly and computation intensified authentication systems[1].Passwords are more than just a key. They serve several purposes. They ensure our privacy, keeping our sensitive information secure. Passwords authenticate us to a machine to prove our identity-a secret key that only we should know. They also enforce non repudiation, preventing us from later rejecting the validity of transactions authenticated with our passwords. Our username identifies us and the password validates us. But passwords have some weaknesses: more than one person can possess its knowledge at one time. Moreover there is a constant threat of losing your password to someone else with venomous intent. Password thefts can and do happen on a daily basis, so we need to defend them. Now merely using some random alphabets grouped together with special characters does not assure safety[2]. We need something esoteric, something different along with being user-friendly as our password, to make it secure. Besides being different it should also be light enough to be remembered by us and equally hard to be hacked by someone else [3,4,5].

II. ATTACKS OVERVIEW

In *computer* and *computer networks* an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. An attack can be *active* or *passive*. An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. An attack can be perpetrated by an *insider* or from *outside* the organization. An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider")[6].
In this paper we are discussing the attacks as mentioned below:

(a) Tempest Attacks :

Work on the principle that electronic devices such as monitors and fax machines emit electromagnetic radiation during normal use. With correct equipment such as antennas, receivers and display units an attacker could in theory intercept those emissions from a remote location (from across the street perhaps) and then replay the information that was captured. Imagine if this were possible how it could be misused to violate your privacy.

Closing doors and blinds wouldn't do anything to stop a TEMPEST attack. If your monitor was displaying sensitive material then it would be exposed. However don't become paranoid as it's extremely difficult to execute an attack to "capture" what's being displayed, but in theory it's certainly possible[7].

(b) Shoulder Attacks :

Refer to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they:

- fill out a form
- enter their PIN at an automated teller machine or a POS terminal
- use a telephone card at a public payphone
- enter a password at a cybercafé, public and university libraries, or airport kiosks
- enter a code for a rented locker in a public place such as a swimming pool or airport.

(c) Brute Force Attacks :

Cracking in the context of computer security, a brute force attack is a particular strategy used to break your lovingly crafted password. This is the most widely used method of passwords and it involves running through all the possible permutations of keys until the correct key is found. For example, if your password is 2 characters long and consists of letters and numbers – and is case sensitive, then a brute force attack would see a potential 3,844 different "guesses" at your password. This is because:

- First character: lower case letters (26) + upper case letters (26) + numbers (10) = 62
- Second character: same = 62
- Total permutations = 62*62 = 3,844
- You can see that the longer the password, the more "guesses" and time are needed for the brute force attack to be successful[8].

III. STUDY AND ANALYSIS OF EXISTING SYSTEMS

In this existing system after the user login , have to select the images in levels sessions and each level has to select the three images and then we are able to give the password, can go through the email.

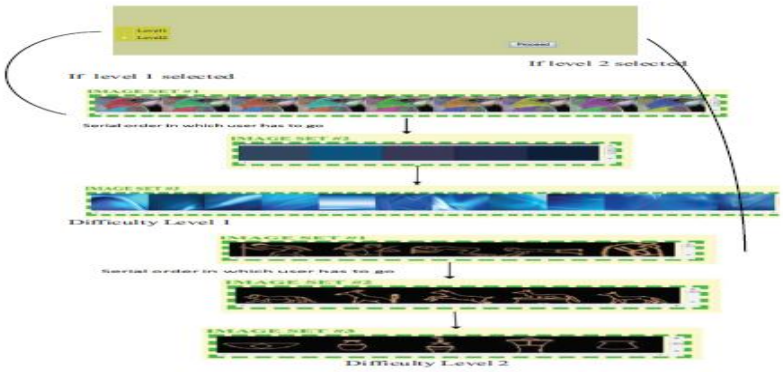

Fig. 1: Image selected in three layers

So it is very complex system and is very difficult to remember the selected images. The main disadvantage that it's very time consuming process[9,10,11]. At last completing the process the user details (email-id, image, password) is not secure sending into the users mail box[12].

IV. PROPOSED SYSTEM

Avoiding these attacks we proposed an IBA system. This unique and user-friendly 3-Level Security System involves three levels of security, where the preceding level must be passed in order to proceed to the next level.

- **Level 1** – The user login the account by entering the email-id.
- **Level 2** - At this level the security is been imposed using Image Based Authentication (IBA), where this will be asked to select the image. After selecting the image it will verify the authentication from the server side, as the server encrypt and decrypt the image. After completion of the image authentication process, it will proceed to the next level.

➢ **Level 3** - After the successful clearance of the above authentication for image, then the user is able to enter one-time numeric password that would be valid just for that login session. Then it will be verified by the server by encrypting and decrypting this. After completion of this process, user will be able to access his e-mail. So to remember, all these mail-id, IBA and password information are sent to the user mobile.

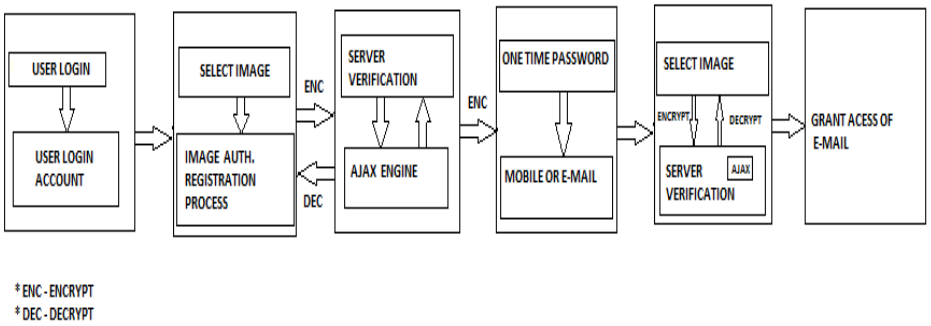

Fig. 2 : Block Diagram of IBA for E-mail System

V. AJAX CLIENTS-SERVER COMMUNICATION

AJAX, which is Asynchronous Java script and XML, is a web development technique . It is meant to increase the web page's interaction, its speed and usability[13].

AJAX web application model :

(1) User interaction invokes the AJAX cell.
(2) The AJAX engine creates an XML to Http Request to the server.
(3) Web server processes the request and then returns the data.
(4) AJAX engine returns data back or renders the data on the user interface.

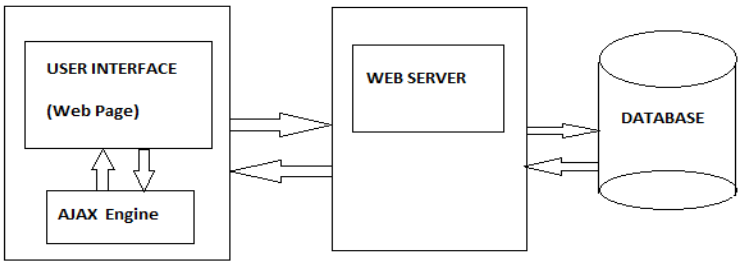

Fig. 3 : AJAX Clients-Server Communication

VI. CONCLUSION

The levels of security approach applied on the above System, makes it highly secure along with being more user friendly.This system will definitely help to protect from Shoulder attack, Tempest attack, and Brute-force attack at client side. It is a very fast process which helps us to secure our mail system. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

VII. FUTUREWORK

Thus, for developing the system using the MD5 algorithm which is more secure. We are implementing this algorithm by using ASP.NET with C# and for database SQL 2008. So the user can use this system for any confidential purpose. In future this system will be more user friendly.

REFERENCES

[1] Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing".
[2] William Stalling, "Cryptography and Network Security", Pearson Education.
[3] B. Clifford Neuman n and Theodore Ts'o , Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9)pp33-38.September 1994.
[4] U. Manber. A simple scheme to make passwords based on one-way functions much harder to crack. Computers & Security, 15(2):171{176, 1996.
[5] Nitin, Durg Singh Chauhan, Sohit Ahuja, Pallavi Singh, Ankit Mahanot, Vineet Punjabi, Shivam Vinay, Manisha Rana, Utkarsh Shrivastava and Nakul Sharma, Security Analysis and

Implementation of JUIT-IBA System using Kerberos Protocol, Proceedings of the 7th IEEE International Conference on Computer and Information Science, Oregon, USA, pp. 575-580, 2008.

[6] http://en.wikipeddia.org/wiki/attacks.

[7] Information Service Enterprise Network Security Guidelines: Prevention and Response and HackerAttacks, Digital Edition, June 2001

[8] Nitin, Durg Singh Chauhan and Vivek Kumar Sehgal, On a Software Architecture of JUIT-Image Based Authentication System, Advances in Electrical and Electronics Engineering, IAENG Transactions on Electrical and Electronics Engineering Volume I-Special Edition of the World Congress on Engineering and Computer Science, IEEE Computer Society Press, ISBN: 978-0-7695-3555-5, pp. 35-46, 2009.

[9] N. Haller. The s/key(tm) one-time password system. In Proceedings of the 1994 Symposium on Network and Distributed System Security, pages 151{157, February 1994.

[10] http://en.wikipedia.org/wiki/Hue.

[11] R. Biddle, S.Chiasson and P. van Oorschot "Graphics Passwords: Learning from the First Twelve Years", ACM Computing Surveys(to appear).School of Computer Science, Carleton University,2010.

[12] http://en.wikipedia.org/wiki/Hue.

[13] www.ajax.org/