Security Analysis and Implementation of 3 level security using Grids,OTP and GSM

Student:Pranav Patki[1], Swapnil Patil[2],Nagesh Jadhav[3],Gaurang Nimbalkar[4] , Prof.N.J.Kulkarni[5]

pbp6704@gmail.com[1]
srp05@rocketmail.com[2]
jnagesh@outlook.com[3]
g.nimbalkar1991@gmail.com[4]
nikitajkulkarni@yahoo.com[5]
Zeal Education Society's Dnyanganga College of Engineering and Reasearch,Pune 411041

***Abstract*— Increasing security has always been an issue since Internet and Web Development came into existence, text based passwords is not enough to counter such problems, which is also an anachronistic approach now. Therefore, this demands the need for something more secure along with being more userfriendly.**

Therefore, we have tried to increase the security by involving a 3-level security approach, involving text based password at Level 1, Image Based Authentication at Level 2, and automated generated one-time password (received through an automated email to the authentic user) at Level 3.And an assiduous effort has been done for thwarting Shoulder attack, Tempest attack, and Brute-force attack at client side , through the use of unique image set in the IBA System.

Keywords*—*Image Based Authentication System(IBA), AJAX, Ke ystroke Logging,Tempest Attack,Shoulder Attack and Bruteforce Attack,,GSM.

1.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. 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. 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 ligh enough to be remembered by you and equally hard to be hacked by someone else.

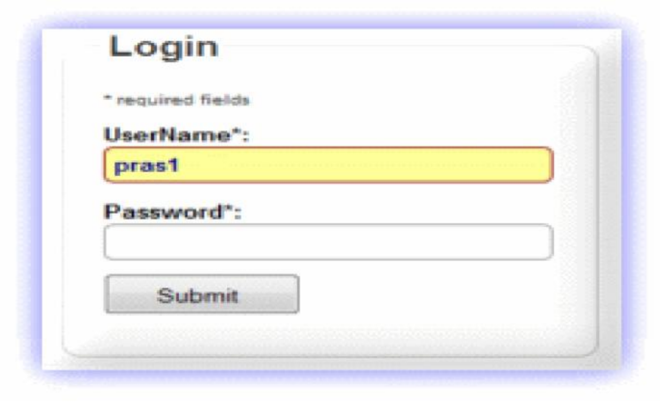
This paper is a unique and an esoteric study of using images as password and implementation of an extremely secured system, employing 3 levels of security-(Text Password, Image Password, and One-Time automated generated password). This unique user-friendly System named as 3 Level Security that can be employed in any organization for storing crucial and confidential documents, and ensures the security through its three levels–Firstly-through Text Password, Secondly-through Image based Password, and Thirdly-through One-Time Automated Password.An assiduous research is being done for choosing image sets, which is the essence of this paper, involving images that thrusts for thwarting Shoulder Attack, Tempest attack, and brute force attack at the client side. This paper describes how our system works and how it eliminates different attacks at the client side, by employing unique image sets.

2. PROPOSED SYSTEM

This unique and user-friendly 3-Level Security System is involving three levels of security, where the preceding level must be passed in order to proceed to next level.

a) Level 1

Security at this level has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach.



Login

* required fields

UserName*:

pras1

Password*:

Figure 1.Level 1 Text Password Authentication

b) Level 2

At this level the security has been imposed using Image Based Authentication (IBA), where the user will be asked to select from the two difficulty levels. Both the levels will be having three unique Image grids, from where the user has to select three images, one from each grid.

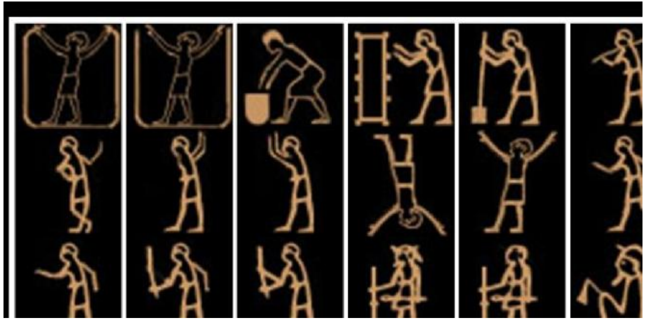
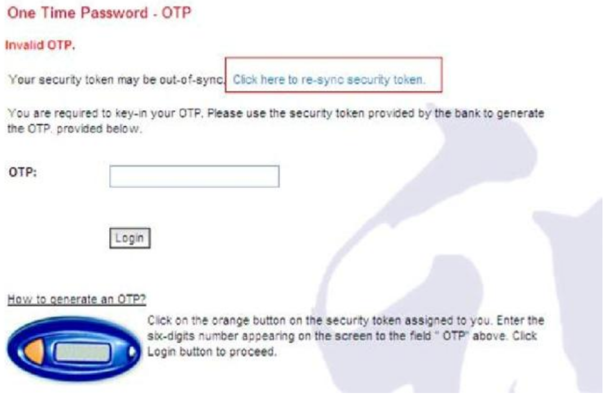


Figure 2. IBA Difficulty Level 2

c) Level 3

After the successful clearance of the above two levels, the 3-Level Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his mobile.Any hacker if in the extreme case, suppose (although difficult) will cross through the above two mentioned security levels, will definitely not be able to cross the third security level, unless he has access to the original user’s mobile. The user will be authenticated as an authentic user, and will be awarded access to the stored information, only after crossing the three security levels (Security level1-Text password,Security level2-Image Based password, and Security level3-One-Time Automated password) be used.



One Time Password - OTP

Invalid OTP.

Your security token may be out-of-sync. Click here to re-sync security token.

You are required to key-in your OTP. Please use the security token provided by the bank to generate the OTP. provided below.

OTP:

How to generate an OTP?

Click on the orange button on the security token assigned to you. Enter the six-digits number appearing on the screen to the field " OTP" above. Click Login button to proceed.

Figure 3. Security Level 3

Security at level 3 has been imposed by generating a onetime random code. This random code or can say the password will be generated each time during the specific login session, for the user to login to his account after the successful completion of two authentication processes (security level1-Text password and security level2-Image based Authentication). This unique code will be updated in the database on the server. And the user will be informed of this one-time password through an automated message. This will definitely help in thwarting Brute force attack (can be attempted upon the previous two security levels), as this unique one-time password will be send on user’s mobile number saved in the database. And the user will be granted access to that one-time password, only upon having access to that mobile. Therefore, the hacker if successful(although difficult) to cross through the above two mentioned security levels, will definitely not be able to cross the third security level, unless he has access to the original user’s mobile.

A GSM modem is a wireless modem that works with a GSM wireless network.A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. GSM modem can be an external device or a PC Card / PCMCIA Card. Typically, an external GSM modem is connected to a computer through a serial cable or a USB cable.Like a GSM mobile phone, a GSM modem requires a SIM card from a wireless carrier in order to operate.

.

CONCLUSION

This is a software provides better security as there are 3 security levels used together as well as features like, use of GSM to send OTP(One Time Password) on mobile phone via text message instead of sending it on user's email-id ensures the best security.

Thus, this technology can be used to secure personal data, important documents and can be used in Internet Banking where the transactions are need to be secured, in reservation systems like railway, aeroplane etc, in military to send important data from source to destination without using encryption and decryption technology.

REFERENCES

[1] 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

[2] 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.

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

[4] http://en.wikipedia.org/wiki/Color_vision

[5] http://en.wikipedia.org/wiki/Indigo

[6] http://www.ancientegyptonline.co.uk/hieroglyphs.html