International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

SECURE NET BANKING USING GRAPHICAL PASSWORD

S.Karpagam [1], M.Pavithra [2], V.Priyanka [3], K.Ranjitha [4] , Dr.K.Saravanan,B.E.,M.E.,P.Hd [5]

B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [1]
B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [2]
B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [3]
B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [4]
Associate Professor & Head of the Dept, Dept. of CSE, Pavai College of Technology, Tamilnadu, India [5]

***Abstract*--Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this Problem of authentication, the proposed system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner. The proposed system combines the Persuasive features with the cued click point to make authentication system more secure. Basically during password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).Also it removes the shoulder surfing attack.**

I. INTRODUCTION

The Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this Problem of authentication, we are proposing an algorithm based on image processing, improved steganography which is visual cryptography.

The problem of Knowledge based authentication mechanism (KBAM) typically text based password are well known. The goal of an authentication system is to support users in selecting the superior password. An alternative to alphanumeric password is the graphical password. Graphical password uses images or representation of an image as a password. Human brains easily recognize pictures than the text. Most of the time user create memorable password which is easy to guess but strong system assigned password are difficult to remember. An authorization system should allow user choice while influencing user towards stronger passwords
An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random
click point which is difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of increasing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click point technique which uses one click point on five different images. The next image to be displayed is based on previous click-point
and the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point.

An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of increasing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click

point technique [8] which uses one click point on five different images. The next image to be displayed is based on previous click-point and the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point.

II. EXISTING WORK

Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness.
Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

Disadvantages

- Most of the applications are giving high protection towards the Password Security and they are not concentrate on phishing attacks, So by phishing attackers are directly getting the passwords from the user and they enter into the relevant web sites with correct password.
- There is no efficient technique to safe guard the users of phishing websites

III. PROPOSED SYSTEM

The proposed system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner. The proposed system combines the Persuasive features with the cued click point to make authentication system more secure. Basically during password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).Also it removes the shoulder surfing attack.

Advantages

- An important usability goal of proposed system is to support users in selecting password of higher security with larger password space.
- Proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).
- Also it removes the shoulder surfing attack.

IV. METHODOLOGY

The Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this Problem of authentication, we are proposing an algorithm based on image processing, improved steganography which is visual cryptography.

The problem of Knowledge based authentication mechanism (KBAM) typically text based password are wellknown. The goal of an authentication system is to support users in selecting the superior password. An alternative to alphanumeric password is the graphical password. Graphical password uses images or representation of an image as a password. Human brains easily recognize pictures than the text. Most of the time user create memorable password which is easy to guess but strong system assigned password are difficult to remember. An authorization system should allow user choice while influencing user towards stronger passwords

V. OVERVIEW OF THE PROJECT

An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is

difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of increasing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click point technique which uses one click point on five different images. The next image to be displayed is based on previous click-point and the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point.

An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of increasing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click point technique [8] which uses one click point on five different images. The next image to be displayed is based on previous click-point and the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry where as explicit indication is provided after the final click point.

VI. CONCLUSION AND FUTURE WORK

In this project we did an Adding Persuasive features in Graphical Password to increase the capacity of KBAM. It's to develop this project; we used J2EE as a front end and MY SQL as backend. A major advantage of proposed scheme is that it provides larger password space then the alphanumeric passwords. For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also it removes the pattern formation and hotspot attack since it provides the system suggestion. Also the proposed system removes the shoulder surfing attack.

In this project we can implement this with 2d images in future we can implement with 3d images or digital signature login process.In this project we prevent from some basic attacks, but in future we can try to implement with some high capacity attacks also.

REFERENCES

[1] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorabilityand Security of Passwords," Security and Usability: Designing SecureSystems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7,pp. 129-142, O'Reilly Media, 2005.

[2] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for UserAuthentication," Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.

[3] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for InformationSecurity," IEEE Trans. Information Forensics and Security (TIFS), vol.1, no. 2, pp. 125-143, June 2006.

[4] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc.,Murray H*ill, NJ*, U. S. Patent, Ed. United States, 1996.

[5] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and Longitudinal Evaluation of a GraphicalPassword System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2,pp. 102-127, 2005.

[6] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Authentication Using Graphical Passwords: Effects of Tolerance andImage Choice," Proc. First Symp. Usable Privacy and Security(SOUPS), July 2005.