International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

SECURED AUTHENTICATION USING IMAGE SHIELD PROTECTION AND DATABASE CRYPTOGRAPHY

Nivetha S & Anitha S

[1]*Professor: Mrs.R. Jothi,MCA.,M.Phil.,Associate Professor,Dept. of Computer Science, Dhanalakshmi Srinivasan College Of Arts And Science For Women , Perambalur, Tamil Nadu, India.*

Abstract - Nowadays, Websites are the backbone of online business and informative services in the world. Website security is the most important aspect in web technology. Data privacy and security is very important in all web applications. Secured Authentication is the key point to prevent the data access from unauthorized users. Existing Login Authentication is implemented by using unique username and password as text format. But this system faces huge challenges from hackers, network intruders where people get the user's password easily by several hacking methods. This project proposed the system for secured login authentication system using image hotspot security. The architecture for image hotspot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password. Initially authorized user need to identify the exact hotspot from the image. In earlier algorithm nearly five hot spot is used. Since this process has high probability of finding the password, proposed system with one hot spot password is designed. User has to click exact co-ordinate of the image to be authenticated by our web application. This process will confuse hackers and will not let them hack an account. This process developed for more security at authentication.

***Key Words*: Image Hotspot,Authentication, Security**

1. INTRODUCTION

An Online Social Network (OSN) is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), user's social links, and a variety of additional services such as career services.

Online social network sites are web-based services that allow individuals to create a public profile, create a list of users with whom to share connections, and view and cross the connections with in the system.

Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.

Online community services are sometimes considered a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network.

Online social networks enable and encourage third party applications (apps) to enhance the user experience on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Face book provides developers an API that facilitates app integration into the Face book user-experience.

There are 500K apps available on Face book and on average, 20 M apps are installed every day Furthermore, many apps have acquired and maintain a large user base.

Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Face book leading the way with 900M active users.

There are many ways that hackers can benefit from a malicious app:

(a) The app can reach large numbers of users and their friends to spread spam,

(b) The app can obtain users' personal information such as email address, hometown, and gender, and

(c) The app can "re-produce" by making other malicious apps popular. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Face book every day.

And additional feature we added into this project Image hotspots. It can be useful for creating info graphics fast and simple. Use any image and enrich it with points of interest and in-depth information about the details depicted. The user is activated by interacting with the image. When the user clicks inside the image the browser will append the X and Y coordinates (relative to the upper-left corner of the image) to the anchor URL as a query string and will access the resulting URL.

Users create different gestures on any image of user choice and use those gestures as user password. The gesture can be any combination of circles, pixels, and taps.

Pixel is a sample of an original image; more samples typically provide more accurate representations of the original. The intensity of each pixel is variable. In color image systems, a color is typically represented by three or four component intensities such as red, green, and blue, or cyan, magenta, yellow, and black. The term pixel is used to refer to a single scalar element of a multi-component representation.

Image Hotspot Security

The architecture for image hot spot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password. Initially authorized user need to identify the exact hot spot from the image. In earlier algorithm nearly five hot spot is used.

Since this process has high probability of finding the password, proposed system with one hot spot password is designed. The user is asked to click the exact point and to confuse the hackers for each hot spot clicked; a duplicate image is generated so that hackers found difficult for accessing the password. Second step is once hot spot is clicked a matrix with list of alphabet is displaced user need to choose the character with intersecting points. To make the process more difficult for hackers each time a new matrix is generated.

In this method user created two passwords one is textual password and another one is graphical password. In graphical password particular hot spot is allowed to click by using segmentation algorithm spot from the image is compared and alpha numeric matrix algorithm used.

2. Existing System

Hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Face book leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app.

DEMERITS OF EXISTING SYSTEM

(a) The app can reach large numbers of users and their friends to spread spam,

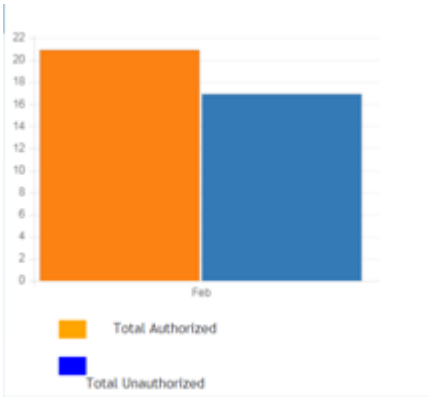
(b) The app can obtain users' personal information such as email address, home town, and gender, and

(c) The app can "re-produce" by making other malicious apps popular.

3. Proposed System

Users develop Frappe (Face book's Rigorous Application Evaluator), a suite of efficient classification techniques for identifying whether an app is malicious or not. To build Frappe, we use data from My Page Keeper, a security app in Face book that monitors the Face book profiles of 2.2 million users. This is arguably the first comprehensive study focusing on malicious Face book apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective detection approach.

And additional feature users added into this project **Image hotspots.** It can be useful for creating info graphics fast and simple. Use any image and enrich it with points of interest and in-depth information about the details depicted. The user is activated by interacting with the image. When the user clicks inside the image the browser will append the X and Y coordinates (relative to the upper-left corner of the image) to the anchor URL as a query string and will access the resulting URL.



PROBLEM DEFINITION AND DESCRIPTION

Online social networks enable and encourage third party applications (apps) to enhance the user experience on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Face book provides developers an API that facilitates app integration into the Face book user-experience.

There are 500K apps available on Face book and on average, 20 M apps are installed every day Furthermore, many apps have acquired and maintain a large user base.

Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Face book leading the way with 900M active users.

There are many ways that hackers can benefit from a malicious app:

(a) The app can reach large numbers of users and their friends to spread spam,

(b) The app can obtain users' personal information such as email address, hometown, and gender, and

(c) The app can "re-produce" by making other malicious apps popular. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Face book every day.

And additional feature we added into this project Image hotspots. It can be useful for creating info graphics fast and simple. Use any image and enrich it with points of interest and in-depth information about the details depicted. The user is activated by interacting with the image. When the user clicks inside the image the browser will append the X and Y coordinates (relative to the upper-left corner of the image) to the anchor URL as a query string and will access the resulting URL.

Users create different gestures on any image of user choice and use those gestures as user password. The gesture can be any combination of circles, pixels, and taps.

And additional feature we added into this project Image hotspots. It can be useful for creating info graphics fast and simple. Use any image and enrich it with points of interest and in-depth information about the details depicted. The user is activated by interacting with the image. When the user clicks inside the image the browser will append the X and Y coordinates (relative to the upper-left corner of the image) to the anchor URL as a query string and will access the resulting URL.

Users create different gestures on any image of user choice and use those gestures as user password. The gesture can be any combination of circles, pixels, and taps.

Pixel is a sample of an original image; more samples typically provide more accurate representations of the original. The intensity of each pixel is variable. In color image systems, a color is typically represented by three or four component intensities such as red, green, and blue, or cyan, magenta, yellow, and black. The term pixel is used to refer to a single scalar element of a multi-component representation

4. Conclusion

Data privacy and security is very important in all web applications. Secured Authentication is the key point to prevent the data access from unauthorized users. Existing Login Authentication is implemented by using unique username and password as text format. But this

system faces huge challenges from hackers, network intruders where people get the user's password easily by several hacking methods. This project proposed the system for secured login authentication system using image hotspot security.

The architecture for image hotspot is used to avoid the unauthorized user assessing the system and it also prevent from hacking the password. Initially authorized user need to identify the exact hotspot from the image.

REFERENCES

[1] Luke Welling & Laura Thompson ,"PHP & MySQL Web Development – by Luke Welling & Laura Thompson" , Developers Library , 4th edition , 2015.

[2] Robin Nixon," Learning PHP, MySQL, JavaScript, and CSS: A Step-by-Step Guide to Creating Dynamic Websites " ,O'Reilly, 2nd edition , 2000.

[3]Davey Shafik , "PHP Master (Paperback)" (Goodreads Author) published 2011.

BIBLIOGRAPHY

	**Mrs. Jothi.R** – Received MCA.,M.Phill., Degree In Computer Science. She Has 13 Years Of Teaching Experience. She Had Presented 5 Papers In International Conference And Also She Presented 4 Papers In National Conference. She Is Currently Working As Associate Professor In Department Of Computer Applications In Dhanalakshmi Srinivasan College Of Arts And Science For Women , Perambalur, Tamil Nadu, India.
	Ms. S. Nivetha , PG scholar, Department of Computer Science, Pursuing MCA in Dhanalakshmi Srinivasan College Of Arts And Science For Women , Perambalur-621 212, Tamil Nadu, India
	Ms. S. Anitha , PG scholar, Department of Computer Science, Pursuing MCA in Dhanalakshmi Srinivasan College Of Arts And Science For Women , Perambalur-621 212, Tamil Nadu, India.