Graphical Password Authentication for Securing Online Banking System

Anju Marium Abraham[1] Bibin Varghese[2] Smita C Thomas[3]
[1,2,3]Mount Zion College of Engineering Kadamanitta, Pathanamthitta, India

Abstract— Securing online banking system authentication plays an important role, mainly user's use username and password combo for verifying users. Memoring username and password is a difficult task. Attackers can easily attack users account. Here proposing graphical password scheme for online banking system. Users can set their own live picture as their password. It will help to overcome the password related attacks. Highly distinctive optical features are extracted from these selections and used as the password, and also resist shoulder surfing, phishing attack, and data breach incident. The proposed system user needs to select the password from live image taken and select points from the image, the server need to extract the features of the image. User can enter the password by using the registered device, here personal device such as smart phone or smart watch etc. which should perform cryptographic primitives such as encryption, digital signature and hashing.

Key words: Graphical Password Authentication, Online Banking System

I. INTRODUCTION

Traditional authentication [3] schemes such as the username/ password combo face a serious threat to the online banking services, financial systems, and their users. Most current authentication systems allow a user to choose a static and unique user id that acts as a security barrier. Unfortunately, users tend to use the same user id in many different websites and systems. Furthermore, many users continue to employ the same password across online accounts and systems. Common practice might lead to security risks such as insider attacks. Malicious administrators or insiders, who have access to username and password tables, can leverage the information to access other services and websites. Furthermore, this practice could allow a phisher to utilize users' credentials on more than one website. Phishing is a type of social engineering attack in which a malicious user, also known as a phisher, attempts fraudulently to acquire legitimate users' credentials by masquerading as a trustworthy entity or public organization. A phishing attack [4] can be carried out using different communication means, such as emails or instant messages, and it usually directs the victim to a fake website that looks like the real one. Such an attacker could target a group of users or a single user and harvest their usernames and passwords and then try to login to critical systems such as online banking. Using static credentials is one of the core problems that allow phishing attacks to succeed. Changing this paradigm by abandoning the usage of static usernames and passwords could modify the game and yield better anti-phishing authentication schemes.

II. RELATED WORK

Graphical password [2] systems are knowledge-based authentication techniques that leverage peoples' ability to memorize and recognize visual information more readily than alphanumeric information. Researchers have explored three broad types of graphical passwords: recall-based draw metric schemes based on sketching shapes on screen, recognition based cognometric schemes based on selecting known items from large sets of options, and cued-recall loci metric schemes based on selecting regions of prechosen images. Cued-recall (loci metric) password schemes involve users selecting regions on one or more images. During login, users are shown a previously selected image, and they enter a password by clicking on a sequence of locations on the image. Authentication is successful if the XY coordinates of These clicks match a previously stored set of password points. A longitudinal study resulted in login times of 8.78–24.25 s and a failed authentication rate of 7–13%.While simple and effective; cued-recall graphical passwords present new security issues. For instance [1], users typically select hotspots, locations on an image that are highly distinguishable, memorable, and also predictable to attackers. In the Microsoft Windows 8 graphical password system, the most common password involved a photo of a person and triple tapping on the face, where one of the selection points was an eye. Addressing this issue, the cued-click points (CCP) system presented a series of images and allowed users to select only a single point per image, reducing the need to select common hotspots. Evaluations of this technique led to authentication times in the range of 7–8 s and success rates of 90–96%.

A second key problem with loci metric systems is observation, as password click-points can be acquired by attackers after viewing a single authentication process. Securing against observation attack for graphical password systems is critical. "User interface manipulations such as reducing the text size of the mouse cursor or dimming the image may offer some protection, but have not been tested." One exception is a variant of CCP that uses eye-tracking technology for input. This system increased resistance to observation but negatively impacted performance: login times rose to 47.1–64.3 s and only 67% of participants successful authenticated on their first attempt. Although more secure, this technique was prohibitively slow and error prone.

In this paper [2], the objectives of this study are to design a novel authentication scheme using dynamic usernames and to diminish the need for storing user's credentials at a centralized location. The envision that the new design should resist many attacks and issues such as key logger attacks, shoulder-surfing attacks, data breach incidents, password reuse, and other human factors. Key logger attacks are becoming more complex and could target static authentication schemes. A key logger can be a plug-in hardware device or a software program that acts as a malicious process residing on the victim's computer. The primary goal of using key loggers is to capture and observe every keystroke typed on the victim's computer, which certainly includes authentication information such as usernames and sensitive passwords. Generally speaking, key logger software and hardware are not easy to detect, especially on public computers. Some sophisticated key

logger software is rooted in the operating system and does not show up in the task manager process list. Although many countermeasures could mitigate the risk of key logger attacks, many new issues, tools, and techniques are still evolving. In 2011, with 80% accuracy, researchers illustrated that it is feasible to capture keystrokes of a nearby computer utilizing the accelerometer found in many smartphones.

This result emphasizes the belief that there is no silver bullet solution to tackle the key logger problem in a username and password system, and it is still necessary to improve the traditional authentication schemes. Shoulder-surfing is another issue that affects the security of traditional authentication schemes. Shoulder-surfing attacks occur when attackers utilize direct observation techniques such as looking over someone's shoulder or using a hidden camera to harvest sensitive information. Unfortunately, shoulder surfing is an effective way to target conventional authentication methods and get passwords, PINs, and other sensitive personal information. It is not hard to launch in practice as a shoulder-surfing attack does not require sophisticated knowledge or a high level of experience. Modern authentication schemes should consider the resistance of shoulder surfing attacks and shrink the attack surface. Another major driver is the data breaches that have been becoming increasingly sophisticated and daring. Data breaches could have a grave impact on users and financial Institutions. Many data breach incidents include the disclosure of usernames and passwords, and several leading experts consider data breaches as one of the biggest security problems faced by security professionals and system administrators.

III. PROPOSED SYSTEM

In this paper, here proposing a system for securing online banking system. In this system [3] we use laptop or desktop as user terminal, registered device such as personal devices (smart phone or smart watch) which should perform cryptographic primitives such as encryption, hashing and digital signature and sever here banking system is act as server. First user need to take live image by using registered device and send it to the server the server extract the features of the images. Then user needs to select the password points and the server store it in the system. When user want to enter in to the system user need to take the live image which is already set as the password and select the password points, the registered device send that to server .Server verify the user. After that the system will perform the online transaction [3], the user send request to the registered device and the ticket is generated encrypt it and send it to the server. After the show the ticket to the user with one time username, Access control, timestamp etc. Then the server verify the ticket and send verification to the user ,user enter the verification code then the server verify the code also. After that the transaction will proceed.

IV. CONCLUSION

The extraordinary growth of online banking and e-commerce systems has led to a huge increase in the number of usernames and passwords managed by individual users. Conventional static username and password protocols suffer from various security issues. Many users start using duplicated credentials over and over again in various accounts and systems. Leaking or compromising one account could cause an attacker to infiltrate other systems and endanger users' security and privacy. In this paper [3], we introduce a new authentication model that allows users to get rid of many issues such as memorizing usernames and passwords for many different websites and systems. The proposed authentication scheme paves the way for user-centric access control that helps minimize the risks of many attacks. There are several research directions that can be further explored in our future research. First of all, we would like to investigate using lightweight cryptographic techniques in our design. Second, we plan to scrutinize the design of different user-centric access control models. Also, we intend to study techniques for improving the authentication methods such as using visual decryption and visual signature verification. Finally, reporting on usability of the proposed authentication scheme should be further investigated in our future research.

ACKNOWLEDGMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount Zion College of engineering, for their immense support.

REFERENCES

[1] G. E. Blonder, “Graphical passwords,” U.S. Patent 5 559 961, 1996.
[2] Andrea Bianchi, Ian Oakley, and Hyoungshick Kim,”PassBYOP:Bring Your Own Picture for securing Graphical password”,IEEE Transaction On Human System.
[3] Abdulrahman alhothaily, chunqiang hu, (member, ieee), arwa alrawais, (member, ieee), tianyi song, xiuzhen cheng, (fellow, ieee), and dechang chen :”A secure and practical authentication schemeUsing personal devices”, Digital Object Identifier 10.1109/ACCESS.2017.2717862
[4] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, ``an attributebased encryption scheme to secure fog communications," IEEE Access, vol. 5, pp. 9131_9138, 2017, doi: 10.1109/ACCESS.2017.2705076.
[5] K. Aravindhan and R. Karthiga, ``One time password: A survey," Int. J. Emerg. Trends Eng. Develop., vol. 1, no. 3, pp. 613_623, 2013.

