Implicit Password Authentication System

Mr. Amit R. Gadekar, Ms. Pallavi S. Shendekar,

Abstract— Authentication is an important process which assures the basic security goals, viz. *confidentiality and integrity.* Also**,** adequate authentication is the first line of defense for protecting any resource. It is important that the same authentication technique may not be used in every scenario. Though traditional login/password based schemes are easy to implement, they have been subjected to several attacks. As an alternative, token and biometric based authentication systems were introduced. However, they have not improved substantially to justify the investment. Thus, a variation to the login/password scheme, viz. graphical scheme was introduced. But it also suffered due to shoulder-surfing and screen dump attacks. We introduce a framework of our proposed (IPAS) Implicit Password Authentication System, which is immune to the common attacks suffered by other authentication schemes.

Index Terms— Authentication, Implicit Password Authentication System, Login attacks, Security.

1 INTRODUCTION

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device. This is an important process which assures the basic security goals, viz. *confidentiality and integrity.* Also**,** adequate authentication is the first line of defense for protecting any resource. It is important that the same authentication technique may not be used in every scenario. For example, a less sophisticated approach may be used for accessing a "*chat server*" compared to accessing a *corporate database*. Most of the existing authentication schemes require processing both at the client and the server end. Thus, the acceptability of any authentication scheme greatly depends on its robustness against attacks as well as its resource requirement both at the client and at the server end. The resource requirement has become a major factor due to the proliferation of mobile and hand-held devices. Nowadays with the use of mobile phones, users can access any information including banking and corporate database. In this paper, we specifically target the mobile banking domain and propose a new and intelligent authentication scheme. However, our proposal can also be used in other domains where confidentiality and integrity are the major security requirements.

In this project, we propose our Implicit Password Authentication System. IPAS is similar to the PassPoint scheme with some finer differences. In every "what you know type" authentication scheme we are aware of, the server requests the user to reproduce the fact given to the server at the time of registration. This is also true in graphical passwords such as PassPoint. In IPAS, we consider the password as a piece of information known to the server at the time of registration and at the time of authentication, the user give this information in an implicit form that can be understood only by the server. We explain this through a Mobile Banking case-study.

- *Mr. Amit R. Gadekar is currently woringas a assistant professor in* Department of CSE *at DES'sCOET Dhamangaon [Rly], Amravati, India, E-mail:amit.gadekar1@gmail.com*
- *Ms. Pallavi S. Shendekar is currently pursuing masters degree in information technology in Amravati University, India, E-mail: pshendekar@yahoo.com.*

There are several authentication schemes available in the literature. They can be broadly classified as follows:

What you know?
What you have?
and What you are?

The traditional *username/password* or *PIN* based authentication scheme is an example of the "what you know type". Smartcards or electronic tokens are examples of "what you have type of authentication" and finally biometric based authentication schemes are examples of the "what you are" type of authentication. Some authentication systems may use a combination of the above schemes. In this project, we focus only on "what you know" types of authentication.

Although traditional alphanumeric passwords are used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering. In addition to these types of attacks, a user may tend to choose a weak password or record his password. This may further weaken the authentication schemes. As an alternative to the traditional password based scheme, the biometric system was introduced. This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc. The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process. The false-positive and false-negative rate may also be high if the devices are not robust. Biometric systems are vulnerable to replay attack (by the use of sticky residue left by finger on the devices), which reduces the security and usability levels. Thus, recent developments have attempted to overcome biometric shortcomings by introducing *token-based* authentication schemes.

Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose. This may also be used in conjunction with the traditional password based system. Token based systems are vulnerable to man-in-the middle attacks where an intruder intercepts the user's session and records the credentials by acting as a proxy between the user and the authentication device without the knowledge of the user. Thus as an alternative, *graphical based*

passwords are introduced to resolve security and usability limitations mentioned in the above schemes.

Graphical-based password techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text. Psychologists have confirmed that in both recognition and recall scenarios, images are more memorable than text. Therefore, graphical-based authentication schemes have higher usability than other authentication techniques. On the other hand, it is also difficult to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware which have been affecting text-based and token-based authentication. Thus, the security level of graphical-based authentication schemes is higher than other authentication techniques.

Traditional alphanumeric passwords are always vulnerable to guessing and dictionary attack. There may even be a rogue program that may record the key strokes and publish it on a remote website. In order to overcome the key logger based attacks, newer systems may show a graphical keyboard and the user has to press the correct password using "mouse clicks". This may also be defeated if the attacker uses a screen capture mechanism, rather than using a key logger. Since new video-codec is providing higher compression ratio, an attacker may use a screen capture program and record a short video clip and send it to a remote server for publishing. So, as an alternative, a token based authentication method may be used either as a stand-alone authentication or used in addition to the traditional alphanumeric password. But this technology is not pervasive. The user may have to carry a trusted token card reader. With unknown token readers, a user may not be aware whether they are using a trusted legitimate reader or using an un-trusted one that may clone the token (similar to the recent ATM card scam).

Although image based authentication systems reviewed in our paper address most of the threats, still they suffer from the following attacks: replay, Shoulder-surfing, and recording the screen.

One may argue that replay attack can be prevented using encryption and tamper-proof time stamps, and physical shoulder-surfing may be known to the user as this process is invasive. However, due to the availability of high-bandwidth to mobile devices and light-weight, high-efficient video codecs, a rogue program may still capture and publish remotely. Since all the image based password schemes known to us use static passwords, the recorded movie may be replayed and with some human-interaction, the user's password may be decoded.

2 LITERATURE SURVEY

A **literature review** is a text written by someone to consider the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work. Also, a literature review can be interpreted as a review of an abstract accomplishment.

Most often associated with academic-oriented literature, such as a thesis, a literature review usually precedes a research proposal and results section. Its main goals are to situate the current study within the body of literature and to provide context for the particular reader.

Existing System

The example of "what you know type" is The traditional username/password or PIN based authentication scheme. The biometric system was introduce, as an alternative to the traditional password based scheme,. This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc. Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose. Graphical-based password techniques , supported partially by the fact that humans can remember images better than text, which have been proposed as a potential alternative to text-based techniques. In general, the graphical password techniques can be classified into two categories: recall based and recognition-based graphical techniques. In recall-based systems, the user is asked to reproduce something that he/she created or selected earlier during the registration phase. Recall based schemes can be broadly classified into two groups, pure recall-based technique and cued recall-based technique. In recognition-based systems, a group of images are displayed to the user and an accepted authentication requires a correct image being clicked or touched in a particular order.

Disadvantages

- Alphanumeric passwords have problems such as being hard to remember, dictionary attack, key-logger, vulnerable to guessing, shoulder-surfing and social engineering.
- The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process.

Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure. It needs several rounds of image recognition for authentication to provide a reasonably large password space, which is tedious.

2.1 Biometric-based authentication

Biometric authentication verifies a user based on the user's properties; the system can only work if it recognizes the user. To do so, users are required to participate in an enrolment process beforehand. In which, the system captures the users' biometric data to create a digital template and stores the template in a database. To authenticate, the user presents his/her biometrics. The verification is essentially pattern recognition by acquiring the user's biometric data, extracting features from the collected data, and comparing the features against the template in the database.

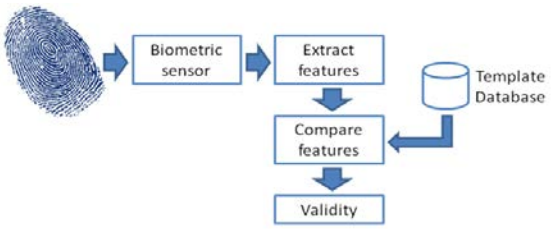

Fig. 1. Biometric Verification Process.

As biometrics are impossible to lose, there is no memorability requirement when using them. Biometrics are distinctive and intrinsic to each person; they are inherently more reliable and more capable than the other authentication techniques in differentiating people. As a result, biometrics scheme can be used for identification and verification, which is deemed as advantageous. Although biometrics are unique, not all biometric authentications are perfect; some biometrics can be forged. For example, if a system employs facial recognition, an attacker can use a photograph of the user to fool the system. Biometrics authentication, especially physiological biometrics, does not handle forgery well. If a biometric is forged, it remains stolen for life, and there is no changing back to a secure situation (Schneier, 1999). This is because biometrics have the property of being permanent, unlike passwords where they can be reset, biometrics cannot be replaced.

People believe facial recognition could work, as that is the natural way humans identify each other.People also perceive fingerprints must work because they are used as evidence in law enforcement. In fact, the general perceptions are wrong. Iris verification, using the complex visual texture of the iris for distinctive identification, is the most reliable biometric authentication. The accuracy of iris verification is much greater than fingerprints. It is advantageous because iris images can be acquired from the individuals without physical contact , and forgeries, such as artificial irises (e.g. contact lenses), are easy to detect. Iris scanners use a high resolution camera with a zoom lens to capture an image of the user's iris, and the patterns of the iris are then used for verification. Furthermore, the iris images must be acquired in a non-obtrusive manner, i.e. the system cannot expect the user to be standing with the eye in a predefined position; consequently, the sensor unit must cope with a wide range of angles and positions.

Fig. 2. ATM with fingur print verification.

Biometric authentication has been adopted for banking interfaces. Integration of fingerprint authentication into ATMs is feasible. Although ATMs with fingerprint verification are not common, they have been put into practical use. Besides fingerprints, other biometrics have been proposed for ATM verification. Iris verification is one of the possibilities, and it has already been piloted in ATMs. Coventry conducted usability studies of biometric verification at the ATM interface. Their initial study shows biometrics technology has usability issues, but successful login experiences can influence user opinion and confidence in using the technology in the future. further conducted a field trial study, their results show over 90% of the interviewees were satisfied with iris verification, and would prefer it over PIN authentication. However, it is arguable their result may not apply in the developing world. Many people from the developing world are less experienced with biometric authentication; the lack of understanding of biometrics may influence those people's opinion of adoption.

Any software has its own merits and demerits. Though the biometric system is designed to provide the best office security, there are even chances of errors to occur.

Recognition Errors Faced with Biometric System

The two basic recognition errors found in biometric is the 'false accept rate' (FAR) and the 'false reject rate' (FRR).

False Accept – When a non-matching pair of biometric data is wrongly accepted as match by the system it is then a 'false accept'.

False Reject – When a matching pair of biometric data is wrongly rejected as non-match by the system, it is then a 'false reject'.

The measure to lower any one of the errors automatically increases the other error rate. But, most of the biometric systems operate at a low FAR than FRR.

Non-Economical

Biometrics like iris, face and fingerprint recognition is a better option for security system, but unfortunately the means for acquiring it is neither convenient nor affordable.

A Biometric can be Copied

Finding a copy of an individual's biometric is not a hard task nowadays. There are incidents where a person takes another person's fingerprint for illegal usage. There are also devices that can capture iris images of a person from a video camera, so that it can be duplicated and used.

Voice recognition biometric system is also very expensive and not sufficiently reliable. As it is difficult to implement, it suffers from many disadvantages.

The issue with biometrics is mainly because, when an individual's biometrics has been compromised, then it is the same way maintained by the system forever.

As the authentication method of the biometrics is completely relied on a specific central database and graphic templates,

they are many possibilities of errors to occur.

Even after facing such issues, most entrepreneurs still prefer biometrics for their office security, for its easy access and mass management. They feel it is comparatively a better option than locks and passwords.

2.2 Token-based authentication

The concept of token-based authentication consists of two steps. Initially, the system assigns each legitimate user with a token, and the tokens are assumed to be used only by the assigned users. The system verifies a user based on the user's possession of a valid token. The system is not responsible for checking the legitimacy of the token holder; instead the responsibility of keeping the token protected belongs to the assignees. The process of key ignition for a vehicle for example, regardless of the identity of the driver, as long as the person uses the correct key to start the vehicle, the engine will run.

A good example of a token-based payment system is Octopus card in Hong Kong. It is a contactless payment system where a user places an RFID[1] card over the reader to conduct payment. The system employs the single-factor token authentication strategy, which is based on the presentation of the RFID card. Although using such strategy increases usability, as no prior enrolment and no memorability are required, however, the system cannot verify the user if the token is not presented. Therefore, the user has to remember to carry the token.

A token can be stolen and used by others. To reduce the possibility of illegal access, a system can employ a strategy called *two-factor authentication*; the system requires the user to perform multiple authentications during login. This strategy is most commonly used with the combination of a token and a password.

2.3 Knowledge-based authentication

The use of secret knowledge for authentication is not a new concept. Indeed, it was used before computers are existed. In ancient time, Julius Caesar used a key cryptography technique, called *Caesar cipher*, to communicate with his generals. He used a key to cipher messages; the key is essentially the secret knowledge. Although the example above is for cryptography, the main concept of using a password for protection remains the same; without the correct secret knowledge, it is difficult to gain access to the system and its information.

Nevertheless, there are also flaws in knowledge-based authentication. Usability and security problems arise because passwords are expected to comply with two conflicting requirements, but meeting those requirements is almost impossible. The requirements are identified by Wiedenbeck:

Passwords should be easy to remember; authentication should be executable quickly and easily by humans.

Passwords should be secure; they should look random and hard to guess; they should be changed frequently, and should be different on different accounts for the same user; they should not be written down or stored in plain text.

In computing systems, a secure authentication system requires strong passwords to prevent attacks. Ideally, a strong password is highly randomized. However, "human beings being what they are, there is a strong tendency for people to choose relatively short and simple passwords that they can remember". This means there is a conflict in satisfying those requirements.

To increase password memorability, suggest a method of using the pass phrase approach for password generations. For example, using the phrase "My sister Peg is 24 years old" and choosing the first letters of each word, the password would be "MsPi24yo". Although this approach helps users to choose password that are harder to guess with a mnemonic phrase, this method is only suitable for alphanumerical passwords; the approach cannot be applied for PIN selections, as logical phrases are seldom made up of numbers only.

An alternative to simple passwords is cognitive passwords, also known as semantic passwords Instead of requesting a user to present a password, the system asks a set of questions and authenticates the user based on the semantic answers. This solution improves memorability by asking questions that the user has already known. However, this solution suffers the same problem as normal syntactic passwords: the user's details are predictable, especially if the attacker knows the user well.

3 System Analysis

3.1 Requirement analysis

In our project, our proposed (IPAS) may also be implemented in any client-server environment, where we need to authenticate a human as a client (IPAS will not work in machine-to-machine authentication). We also assume that the server has enough hardware resources like RAM and CPU. This is not un-realistic as high-end servers are becoming cheaper day-by-day. The bank may have a database of 100 to 200 standard questions. During the time of registration, a user should pick 10-20 questions from the database (depending upon the level of security required) and provide answers to the selected questions. For example, the user may choose the following questions:

The maker of your first car?
The city you love to visit or visited?
Date of birth?

For each question, the server may create an intelligent authentication space using images, where the answers to the particular question for various users are implicitly embedded into the images. During the time of authentication, the server may pick one or more questions selected by the users at the time of registration randomly (the number of questions depends on the level of service requested). For each chosen question, the server may choose an image randomly from the authentication space and present it to the user as a challenge. Using the stylus or the mouse, the user needs to navigate the image and click the right answer

3 System Architecture

Figure 1: Represents the architecture of an extended ImplcitPassword Authentication system. It consists of Sev-

enModules. They are,

- Client
- Server
- Encryption and Decryption
- Image Generation
- Key generation using sms
- Authentication
- Transaction

The proposed algorithm efficiently handles the security issues. The entire processing of the system is depicted throughthe architecture phase.The flow for the entire process is manipulated. The literature reviews are made after which the modules are identified, apart from which the functions of the modules are stated.

The proposed algorithm fits itself perfectly by improving the efficiency of the password and also makes the authentication more safe and secure.The extended IPAS makes the transactions more convenient by presenting the password more securely.This depicts itself a perfect authentication scheme and the chances of fraudulent and hacking are much reduced.

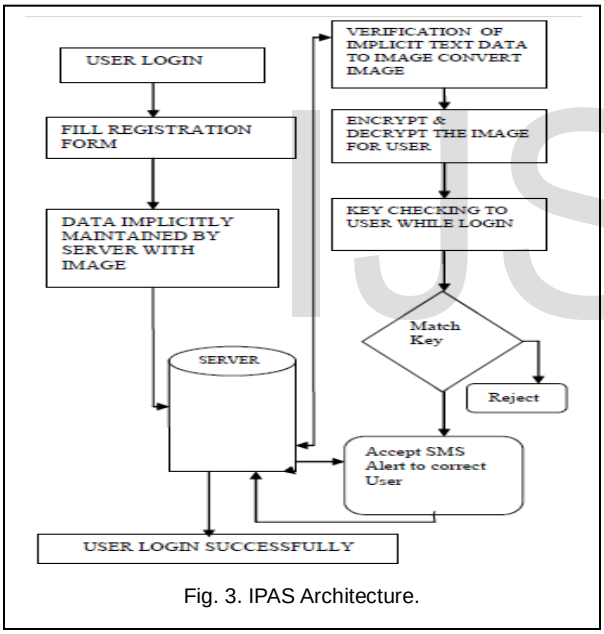

Fig. 3. IPAS Architecture.

4 Requirement Analysis

Operating System : Windows XP
Development Tool : C# (.Net)
Database : HiediSQL powered by MySQL

5 Conclusion

Implicit password is a more secure compared with the existingsystem. This system can be implemented in places where security is poor or additional security is needed. This concept can be used extensively in the field of banking since

transactions are prone to more fraudulent. Hacking of password is impossible because password can be hacked but the implicit password cannot be hacked , only the legitimate user identify the implicit password. Also, text passwords can be retrieved through techniques like key logger , shoulder

surfing and screen dump so on. But, implicit password cannot

be retrieved since no trial and error methods can be applied on

it. The reference observations clearly state that passwords face

a number of issues regarding their security and those issues

References

[1] Sabzevar, A.P. & Stavrou, A., 2008," Universal Multi-Factor Authentication Using Graphical Passwords", *IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS).*

[2] Haichang, G., L. Xiyang, et al. (2009). "Design and Analysis of a Graphical Password Scheme", *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on Graphical Passwords.*

[3] Pierce JD, Jason G. Wells, Matthew J. Warren, & David R. Mackay. (2003). "A Conceptual Model for Graphical Authentication", *1st Australian Information security Management Conference*, 24 Sept. Perth, Western Australia, paper 16.

[4] Xiaoyuan, S., Z. Ying, et al. (2005). "Graphical passwords: a survey", *Computer Security Applications Conference*, 21st Annual.

[5] Wells, Jason; Hutchinson, Damien; and Pierce, Justin, "Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, formation Security Management *Conference. Paper* 58.

[6] Takada, T. and H. Koike (2003). "Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images", *Human-Computer Interaction with Mobile Devices and Services, Springer Berlin* / Heidelberg. 2795: 347-351.

[7] Dirik, A. E., N. Memon, et al. (2007). "Modeling user choice in the PassPoints graphical password scheme", *Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, ACM.

[8] Wei-Chi, K. and T. Maw-Jinn (2005). "A Remote User Authentication Scheme Using Strong Graphical Passwords", *Local Computer Networks, 2005*. 30th Anniversary.

[9] Lashkari, A. H., F. Towhidi, et al. (2009). "A Complete Comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms", *Computer and Electrical Engineering, 2009.* ICCEE '09. Second International Conference.

[10] Renaud, K. (2009)."On user involvement in production of images used in visual authentication." *J. Vis. Lang. Comput.* 20(1): 1-15.

[11] Masrom, M., F. Towhidi, et al. (2009). "Pure and cued recall-based graphical user authentication", *Application of Information and Communication Technologies, 2009*. AICT 2009. International Conference.

[12] Birget, J. C., H. Dawei, et al. (2006). "Graphical passwords based on robust discretization", *Information Forensics and Security, IEEE Transactions* on 1(3): 395-399.