International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-02, Issue 12, Mar 2017

Survey On Avoiding Keylogging Attack

[1]Prof.Harshali Rambade, [2]Mr.Abhishek Dattatray Nagare, [3]Mr.Abhishek Arjunrao Kenjale, [4]Mr.Abhilash Satish Raorane

[1,2,3,4]Information Technology Department, Vidyalankar Institute of Technology, Mumbai,India.

[1]harshali.rambade@vit.edu.in, [2]abhishek.nagare@gmail.com, [3]abhishek.kenjale@gmail.com, [4]raoraneabhilash124@gmail.com

Abstract— the construction of secure authentication method is quite difficult, considering that various kinds of root kits reside in user's system to observe user's behavior and to make PCs unreliable devices. Involving human in authentication protocols, while promising, is difficult because of their limited capability of computation and memorization. Therefore, depending on users to enhance security necessarily reduces the usability. There are multiple ways that banks can authenticate users. These methods range from combination of username and password to iris scanning. As technology changes continuously, banks must adapt their security systems to combat hackers and thieves effectively. Selecting the right technologies for each organization cannot be generalized. This paper gives insight into some of the efficient technologies currently being implemented in large organizations today. We would also demonstrate how precisely visualization design can improve the security as well as the usability of authentication. To that end, we offer a visual authentication method: QR based authentication method. To eradicate threat of phishing and to affirm user identity and to avoid Key-logging attack we can opt for QR-code.

KEYWORDS —Authentication, Smart-phone, Malicious code, QR based authentication, Key logging Attack

I. INTRODUCTION

Millions of internet users have access to servers each day. Many of these servers are freely available to the public. Everyone is allowed to use the service. Google.com for example allows anyone to use its search features with no need to cross check the user's identity. There are other circumstances, however, where the company needs to keep a vigilant watch over one who can access the services. These companies range from universities to gaming sites. Banking companies are a prime example of organizations that has to authenticate users before allowing them access to crucial resources.

Authentication is defined as a process in which the credentials provided are compared with the files in a database of authorized user's information within an authentication server[3]. If the credentials match, the process is completed and the user is authorized and can have access. Authentication can be achieved by many different methods. Some of these methods are far superior to others, but are not easy to implement and fund. Authentication is not enough to grant users access on its own.

Authorization comes after Authentication. Authorization is the process where a computer system or individual grants permissions to a user for many reasons. The user must first authenticate him-self to the system. The system will then check if the user is valid or not and decide if that user has sufficient access to the resource he is trying to access. Only then the system will grant permission to the user to access the resource. However, process doesn't ends here.

Accounting must also take place. Banking Authentication for Accounting is the process of recording access to a resource. Specifics on the accounting format may change from system to system, but is a crucial part of the authentication process. It is always a nice idea to know what user is accessing from the system and when the user does so. This can aid in investigations if problems appear in the future.

But as we talk of sensitive data and its protection, we also have to look upon various attacks that are done to destroy the secrecy of data. One of the major attacks on sensitive information is "key-logging" attack which utilizes phishing and pharming, and visual fraudulence which cannot be addressed by simply enabling encryption. Key-logger software is designed to capture all of a user's keyboard strokes, and then make use of those keyboard strokes to imitate a user in financial transactions. For example, whenever a user types password in a bank's sign-in box, the key-logger intercepts the password. The threat of such key-loggers is pervasive and can be present in personal computers as well as public kiosks; there are always cases where it is

important to perform financial transactions using a public computer although the biggest concern is that a user's password is likely to be hacked in these computers.

Even worse, key-loggers, often root kitted, are hard to detect since they are not visible in the task manager process list. [4]To avoid the key-logger attack, virtual or onscreen keyboards with random keyboard arrangements are widely used in practice. By rearranging alphabets randomly on the buttons, both techniques can frustrate simple key-loggers. Unfortunately, the key-logger, which has authority over the entire PC, can easily track each event and read the video buffer to create a mapping between the clicks and the new alphabet.

Considering that a key-logger sees users' keystrokes, this attack is quite same as the shoulder-surfing attack. To combat the shoulder-surfing attack, many graphical password schemes have been newly introduced in the literature. However, the common theme among many of these schemes is their non-usability: they are quite complicated for a person to use them. For some users, the usability is equally crucial as the security, so they oppose to change their online transaction experience for more level of security. The shoulder-surfing attack, however, is different from key-logging as that it allows an attacker to hack not only direct input to the computer but also the motion an user makes such as touching some parts of screen. To acquire shoulder-surfing resistant schemes as a solution for key-logger is rather excess considering the usability. Notice that while defending against the shoulder surfing attack is out of the scope of this work. It is not sufficient to depend only on cryptographic techniques to tackle attacks which aim to avert user's visual experience while residing in a PC. Even if all important information is securely transferred to a user's computer, the attacker on that user's computer can easily observe and modify the information and show valid-looking yet fake or invalid information. User's involvement in the security protocol is sometimes necessary to avoid this type of attacks but humans are bad at complicated calculations and do not have a enough memory to remember cryptographic-ally strong keys and signatures.

II. AUTHENTICATION METHODS

Authentication methods can be arranged into a few basic categories. They can be one of various things straightly related to the user. Primarily, this is something the user knows, something the user possesses, the way the user behaves, or a physical features of the user. The following figure classifies some of the authentication methods. Note that this is not a very long list.

III. CATEGORIZATION OF AUTHENTICATION METHOD

Authentication is based on three main factors,1. what user knows,2.what user possesses,3.Users unique character. This helps in authenticating a valid user who possesses all the above needs. User knows his/her password, pin. User may possess Swipe card, proximity card, USB token, OTP. User has his unique fingerprint, palm-veins, Iris .

User Knows	User Possesses	User Behaviors	User's Physical Characteristics
Password	Swipe Card	Speech	Fingerprint/Palm print
PIN	Proximity Card	Signature	Hand Geometry
Identifiable Picture	USB Token	Keyboarding Rhythm	Iris Features
	One Time Password		

IV. USERNAME & PASSWORD

Possibly, the most primary form of user authentication is by a username password combination. This type of authentication is extremely vulnerable. More and more issues are occurring with its use. The concept here is that a user possesses a distinct identifier such as an employee number. He also has a confidential phrase that is paired with the identifier. [10] When the user authenticates, he gives his unique identifier and provides his secret password. Taking into consideration, the user Banking Authentication person is the only one who is supposed to know the confidential password, he is authenticated.

Passwords are highly vulnerable to man in the in between attacks and if someone directly watches you confirm the code.

V. PIN

A personal identification number (PIN) can be utilized in much similar way as a password [5]. It is numerical in structure and like a password is supposed to be kept confidential. The most ordinary use of the PIN is for ATM. "Mainly PINs are four digit numbers in the scope of 0000-9999 resulting in 10,000 credible numbers, so that an attacker would need to extrapolate a mean of 5000 times to get the correct PIN."

PIN is highly prone to man in the middle attacks & shoulder-surfing attack and if anyone just watches you confirm the PIN.

VI. ONE TIME PASSWORD

Another similar technique is the one-time password[6]. This is extremely equivalent to the ordinary username and password combination besides that the password never

propagates from the public network. RFC 2289 describes one method for completing a OTP authentication. The system makes use of a client side creator and a server. Primarily, the generator takes a secret password from the user and combines it with information sent through the server in power of the authentication. Different calculations and hashes are carried out on the user's secret password which can be confirmed by calculations by every end of the communication. This type of system can defend against passive attacks against which primary password systems may be susceptible. OTP tokens are not trustworthy. They're vulnerable to man-in-the-middle (MITM) attacks, and can occasionally still be avoided by phishing.

VII. BIOMETRICS

There are several types of authentication devices accessible today that take benefit of biometry [2]. Merriam-Webster explains biometry as "the statistical analysis of biological observations and phenomena". (Biometry, 2005) They each have their advantages and disadvantages. "The very assured authentication methods contains layered or 'multi-factor biometric strategy'." (Artemis Solutions Group LLC, 2004) Biometric characteristics are difficult to imitate as each individual has special physical characteristics dependent on heredity.

But the disadvantage of this method is the massive amount of money needed for its hardware and nonstop[9].

VIII. QR CODE

QR codes are two dimensional quick response codes[8]. They are easy to use and adaptable. The code itself stores large amounts of information that is easily scanned and kept onto a mobile device. Large number of businesses is now adopting this code as modes of marketing and as different way to captivate customers to the internet for additional information. QR codes may have many advantages in authentication to very significant information.

Most important advantages of QR code over other methods of authentication are[1]:

- QR code is its adaptability.
- QR codes can be used for anything and everything

IX. CONCLUSION

Many of the methods are currently used in authentication system. Methods such as 'Username & Password', 'Pin', 'one time password' & 'Biometrics' have few disadvantages because of which the confidentiality of data is lost. If any bugs occurred in the later stage of deployment, unauthorized user may be allowed to use the services too. Due to all such harmful circumstances there's a need to come up with a unique and error free solution which may in turn help in authenticating only authorized user. Use of QR-code in authentication will help in improving the authentication. Due to generation of a random QR code each time user logins, changes of session hijacking is avoided. Login into the system without entering password avoids Keylogging and shoulder surfing attack. Thus by using QR code in authentication we can avoid loss of data and crucial information and can even avoid various forms of authentication attacks.

REFERENCES

[1] Wikipedia, (2005). Retrieved Jul. 04, 2005, from Authentication Web site: http://en.wikipedia.org/wiki /Authentication.

[2] Authentication, (2004). Glossary of Common Biometric Terms. Retrieved Jul. 14, 2005, from Biometric Glossary of Terms Web site: http://www.biometricsdirect.com/Content / BiometricTerms.

[3] Roland, J. (2004). CCSP Self-study: Securing Cisco IOS networks (SECUR). Indianapolis, IN: Cisco Press.

[4] Wiedenbeck, S., Waters J., Birget J., Brodskiy, A., & Nasir Memon (2005). Passpoints: Design and Longitudinal Evaluation of a Graphical Password System. International Journal of Human-Computer Studies, 63(1-2), 102-127.

[5] Wikipedia, (2005). Personal identification number. Retrieved Jul. 16, 2005, from http://en.wikipedia.org/wiki/ Personal_Identification_Number.

[6] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee," Online Banking Authentication System using Mobile-OTP with QR-code", Page(s): 644 – 648, Nov. 30 2010-Dec. 2 2010, E-ISBN : 978-89-88678-30-5.

[7] AntiPhishingGroup,"Phishing Activity Trends Report", from: http://www.antiphishing.org, dec. 2008.

[8] Advantages of using QR code http://www.estateqrcodes.com/ advantages-disadvantages.html

[9] Disadvantages of Currently used methods for authentication http://searchsecurity.techtarget.com/ answer/What-is-the-best-authentication-method-for-protecting-an-online-banking-site.

[10] Mobile-banking-authentication-challenge https://securityintelligence.com/are-you-ready-for-the-mobile-banking-authentication-challenge/

