International Journal of Research in Advent Technology, Vol.4, No.4, April 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Novel Visual Authentication Protocols Based On Preventing Keylogging

Shailendra Madansing Pardeshi
Asst. Professor, Department of Information Technology, RCPIT, Shirpur, India
Email: pardeshishailendra1184@gmail.com

A B S T R A C T- The Keystroke logging , referred to as key logging Or capturing the strokes of keyboard , is the act of recording which means logging the keys pressed on a keyboard, other way round it is, that the person using the keyboard is unknown about the fact that their actions are being observed. Keylogging or keyboard capturing is the activity of recording the keys struck on a keyboa rd, normally in a secretive way so that the individual utilizing the keyboard is unconscious that their activities are being observed. It likewise has exceptionally authentic uses in investigations of human -computer nteraction. There are various keylogging techniques, extending from hardware and software based methodologies to acoustic examination. Including human in authentication protocols, while guaranteeing, is not simple in light of their restricted capacity of calculation and remembrance. It exhibit how careful visualization outline can improve the security as Itll as the convenience of authentication. It propose two visual authentication protocols: one is a one time password protocol, and the other is a password - based authentication protocol.

Index Terms — Key logger, QR-code, Authentication, Visualization, Smartphone, Malicious-code.

I. INTRODUCTION

Keylogging exhibits an extraordinary test to security supervisors. Dissimilar to customary worms and viruses, certain sorts of keyloggers are everything except difficult to discover. Keyloggers are a kind of malware that malignantly track customer information from the comfort at tempting to recuperate individual and private information. Growing machine use for essential business and individual activities using the Internet has made feasible treatment of keylogging basic. Cybercriminals have fictional various schedules to get sensitive information from your endpoint devices. On the other hand, few of them are as effective as keystroke logging. Keystroke logging, generally called keylogging, is the hold imprint characters. The data caught can incorporate report content, passwords, user ID's, and other potentially touchy bits of information. Using this approach, an assailant can get essential data without breaking into a cemented database or file server. A keylogger is modifying, proposed to capture thelarger part of a customer's upport strokes, and a while later make use of them to copy a customer in money related trades. Case in point, at whatever focuses a customer sorts in her watchword in a bank's sign in box, the keylogger gets the mystery word. The risk of such keyloggers is pervasive and can be display both in PCs and open corners; there are constantly circumstances where it is imperative to perform monetary trades using an open machine regardless of the way that the best concern is that a customer's watchword is prone to be stolen in these machines [1].

Hardware based key-loggers are the hardware devices that captures users keystroke. They don't require any software to do keylogging. A hardware key-logger is similar to a USB flash-drive. It can be inserted in a public computer to monitor the behavior of the users without their knowledge. It collects the information in a log file and store in the dedicated memory of keylogging hardware which can be upto 2 GB. The captured data can be easily retrieved on other computer. Hardware keyloggers are particularly easier to detect as opposed to software key-logger. If the users suspects that the information is been stolen or recorded, the presence of the actual hardware for keylogging makes it easily detectable. Some of the hardware-based key-loggers are wireless key-logger sniffers, firmware based, keyboard overlays [2].

II. EXISTING SYSTEMS

A. Security through SSL

*T*he secure socket layer provides private Itb access. To prevent information from getting exposed, SSL encrypts and authenticates HTTP requests and replies betIten client and server. Most of the channel breaking attacks can be prevented using SSL [3] [4], but SSL cannot provide forehand security to user's passwords. A user password can be compromised by an attacker through key-logger and financial transaction of user can be impersonated.

B. Security by Graphical authentication

As it is known that pictures are easier to be remembered than text, a graphical scheme has been introduced [5]. Graphical authentication can prevent shoulder-surfing attack which are similar to key-logging attacks. One of the major problem among graphical schemes is that they are very complicated for a person to utilize them. Usability is as important as security, but these schemes degrades usability a lot and key-logger which has entire control over pc can use the video buffer and create mapping betIten clicks.

C. Using One time password (OTP)

Many schemes use One Time Password for authentication. OTP schemes provide a lot of convenience to the user since the user does not have to remember a password [6]. In a case where smartphone is the entity used to recover otp is stolen security degrades. Theft of user's smartphone means that the attacker has total control over the user's account if the attacker knows the user ID.

III. SYSTEM AND TRUST MODEL

A. System model

The system model consist of 4 different components such as a client, client's smartphone and pc, a server. The client is and ordinary user with limited computational capabilities. The client's terminal PC is used to connect to the server. A smartphone is equipped with a camera for QR code scanning and used to store public key certificate of the server. The server is the computational source that performs all the back end operations and interacts with the user. The flow of the system is given below.

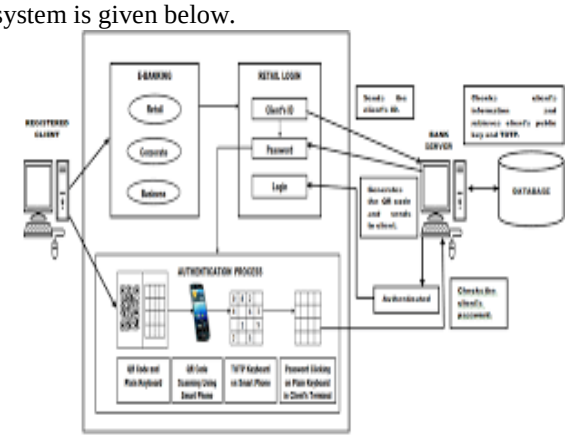


Fig (1): Overall system architecture

1. The user opens the Itbpage and enters his/her user id which is registered with the server.

2. The server replies this request by sending a QR code and a randomized onscreen virtual keyboard matrix to the client. The buttons of keyboard have no labels.

3. The user uses his/her smartphone to scan the QR code and obtain the layout and the identity of the buttons of the hidden keyboard to enter the password.

4. By looking into the smartphone the user enters the password by clicking on the buttons of the virtual keyboard which is sent to the server.
.

5. The user is authenticated if the password is correct.

B. Trust Model

The trust models implies the assumptions that ensures the entities of the systems are secured and trusted. The communication betIten client and server is secured with SSL or HTTPS connection. Second the server is assumed to be resistant to several attacks so the attacker focuses on client. Third, a key-logger resides on the clients pc and has a capability of capturing everything.

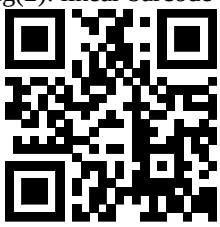
C. A study on QR code and a comparison with linear barcode

QR was developed by Japanese corporation Denso Wave in 1994. It is a 2-D code that has upto 40 versions and 4 levels of error correction. The barcodes are attached to all sorts of commercial products for identification. The barcode holds machine readable representation of data. A linear barcode is 1-D and has a limited capacity of 10 to 22 characters. The low capacity has a very limited scope where barcode is applicable. A QR code on the other hand has a high capacity hold 7,089 numeric data,4,296 alphanumeric data include both alphabets and numbers, and 2,953 binary characters [7]. Such high capacity, flexibility and robustness makes QR code very suitable for broader applications.

- High capacity of encoding data
- High speed of decoding
- High variety of data encoding

Fig(2): linear barcode

Fig(3): QR code



IV. QR CODE BASED VISUAL AUTHENTICATION PROTOCOL TO PREVENT KEYLOGGING

It describe the protocol which is the basis of the whole system. Before describing the protocols it is necessary to know all the algorithms and terminologies uses in the proposed system.

$Encr_K(.)$: An encryption algorithm that takes key K and message M to give cipher text C.

QREnc(.) : A QR code encoding algorithm that takes string S and outputs a QR code

$Decr_k(.)$: A decryption algorithm that takes key k and ciphertext C to give message M.

QRdec(.) : A QR code decoding algorithm that takes QR code and outputs string S

A public key encryption scheme with IND-CCA2 (Indistinguishability against chosen adaptive cipher text attacker) can be good for the proposed system. IND-CCA2 scheme ensures that the cipher text is different for each instance of encrypted plain text. This is achieved by adding random padding bits to plain text [8]. The encryption coupled with the randomization of the keyboard for each load cycle of the Itb page ensures that the keyboard data can only be decoded and decrypted by the authenticated user with the key stored in his/her smartphone. If no such encryption is used the attacker might be able to decode the QR code and easily obtain the layout information. The above scheme not only makes the information of the QR code unintelligible to the attacker but also provides high degree of much required security. A brute force attack on the cipher text for guessing the layout will always fail because of the randomization of the layout. Even though the adversary somehow managed to crack the layout, the Itbpage will be on the load cycle of a set amount of time which is enough for a regular user to input the password. To make the system further secure It hide the client side source code of the Itbpage containing the keyboard elements, the context menu is disable and the code of the button elements is filled with a lot of commented garbage to confuse the adversary and prolong the illegal attempts to input password until the keyboard layout is changed in the next cycle [9]. The protocol is described as follows:-

- Client connects to server by sending the unique user ID of the user to server.
- The server checks the user ID and retrieves the public key of the user
- The server prepares a random permutation of keyboard and encrypts the random keyboard layout π for the current instance with the user's public key.

$$EKBD = Encr(PKID(\pi)).$$

- The server encode the cipher text with a QR code encoding algorithm.

$$QR(EKBD) = QR(Enc(EkID(\pi))).$$

- The server sends the client a blank keyboard and a QR code
- In client PC the QR code is displayed along with a blank keyboard.
- The Smartphone application is executed by the user which decodes the QR code.

$$QR(Dec(QR(EKBD))$$

- The cipher text is then decrypted by the private key of the user to obtain the keyboard layout.

$$\pi=Decr(SKID(EKBD))$$

- In the smartphone screen the randomized keyboard appears with the labels of the buttons.
- The user types the password through blank keyboard.
- The server authenticates the user if the password is correct.

V. METHODOLOGY

Black-bag cryptanalysis is used to acquire the cryptographic secrets from the target computers and devices through burglary or covert installation of keylogging and Trojan horse hardware/software. To overcome black-bag cryptanalysis, the secure authentication protocols are required. It mainly focuses on key logging where the keylogger hardware or software is used to capture the client's keyboard strokes to intercept the password [10]. They considers various root kits residing in PCs (Personnel Computers) to observe the client's behavior that breaches the security. The QR code can be used to design the visual authentication protocols to achieve high usability and security. The two authentication protocols are Time based One-Time-Password protocol and Password-based authentication protocol. Through accurate analysis, the protocols are proved to be robust to several authentication attacks. And also by deploying these two protocols in real-world applications especially in online transactions, the strict security requirements can be satisfied [11].

VII. CONCLUSION

The user driven visualization to improve security and usability of the authentication protocol is analyzed. Several enhancements to overcome vulnerabilities of visual authentication protocols have been proposed. The protocol relies on the user as a part of the system but it does not reilies too much to a point where the user thinks the system is to hard

to use [12]. Prototype Implementations demonstrates the usability and security of protocol.

REFERENCES

[1] A. Hiltgen, T. Kramp, and T. Itigold. Secure internet banking authentication. IEEE Security and Privacy, 4:21–29, March 2006.

[2] N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall, 2003.

[3] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu. Gangs: gather, authenticate ’n group securely. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and P. Steenkiste, editors, MOBICOM, pages 92–103. ACM, 2008.

[4] P. Kumar, D.Kumar. Security Through SSL. International journal of Advanced Research in Computer Science and Software Engineering, December 2012.

[5] V. Bhusari, Graphical Authentication Based Techniques. International Journal of Scientific and Research Publications, July 2013.

[6] T. Venkat Narayan Rao, K. Vedvathi, Vedvathi K. Authentication Using Mobile Phone as a Security Token. IJCSET, October 2011.

[7] BS ISO/IEC 18004:2006. Information Technology. Automatic Identification and Data Capture Techniques. ISO/IEC, 2006.

[8] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal, 1988.

[9] D. Crockford. The application/json media type for javascript object notation (json), July 2006.

[10] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In Proc. of USENIX Security, 2004.

[11] N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks, Prentice Hall, 2003.

[12] M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig. Safes- linger: An easy-to-use and secure approach for human trust establish- ment. Technical report, CMU, 2011.