An Effective Authentication Technique to Prevent Keylogging

Badiga Neeraja
P.G College of Science, Saifabad, India

Abstract

Keylogging is an activity to capture user keystrokes and records the activity of a computer user in a covert manner using keyboard logger hardware and software. Secretly monitors and keyloggers record all keystrokes. Unlike other malware, keyloggers cause any threat to the system. But it can be used to intercept passwords and other confidential information entered via the keyboard, residents are considering various rootkits on computers (PCs) that violates safety. Cybercriminals can get user names, email passwords, PIN codes, account numbers, email addresses, account passwords, online games, electronic payment systems, etc. As a result, it is seen as a user authentication for financial transactions. To prevent keylogging, strict authentication is required. The QR code can be used to design the visual authentication protocols to achieve high ease of use and safety. The two authentication protocols are One-Time-Password Authentication Protocol and time-based protocol based passwords. Through accurate analysis, protocols have proven robust authentication several attacks. And also for the deployment of these two protocols in real-world applications, especially in online transactions, the strict safety requirements can be met.

Keywords

Keylogging, QR Code; Authentication, Android; Visualization Session Hijacking

I. Introduction

Credential stealing attacks and breaking the chains [9] are the two major threats to electronic and financial services. The identification information as user IDs, passwords, can be easily robbed by an attacker to target computers if they are less secure. Additionally, the channels through attacks allow listeners to break the communication between the user and the financial institution. [10] But break attacks conventional channels can be prevented by using IPsec channel [4] and SSL security. Recent attacks are more challenging to break channel as a keylogger that uses session hijacking, pharming, hashing and evasion visual. It is hard to simply avoid these encoded attacks. For example if a home computer gets infected with malicious software, then it is an easy target for the ID of attacker information.

Keyloggers are used by employers as a monitoring tool to ensure that employees use work computers for businesses. Unfortunately, keyloggers are integrated into spyware and allows information to be sent to an unknown third party. Keyloggers can be used in some IT organizations solve technical problems with computers and business networks. Keyloggers are also for a family or a company used to monitor people without their knowledge. Finally, keyloggers are installed in public kiosks to steal information or credit card passwords.

To solve this problem, the intermediate device between the human and the terminal is introduced. This allows to design a protocol involving human. Each interaction between the client and the intermediary device is displayed using Quick Response (QR) code. In these protocols, the client does not need to store information other than password and PIN. However, the authentication process can be visualized which improves safety and ease of use for the customer. The involvement of security protocol client using smartphone with augmented reality. A smartphone with camera is used to visualize the authentication process.

Instead of implementing the overall security protocol in the computer, part of it is moved to the smartphone. This Smartphone viewing offers protection against malware attacks and attacks by shoulder-surfing keylogging.

A. Related Work

Both the Visual authentication protocols are introduced to show how visualization can improve security and usability.

The two authentication protocols are protocol password one-time-password authentication protocol and password based on time. Through careful analysis, we can prove that thesis two protocols are resistant Against the Many attacks are that difficulty applicable in other protocols specified in the literature. Both protocols are in safe numerous attacks in the real world view the Who authentication process to improveboth security and usability.

The implementation of the prototype in the form of applications for Android smartphones demonstrates the ease of use of protocols in the real-world deployment. Visual authentication protocols can be used in ATM (Automatic Teller Machine) and public computers qui Implies financial transformations. In addition, it requires no channel entre the server and the smart phone.

B. Types of Keyloggers

Keyloggers are a serious security threat that can be extremely dangerous for Businesses and consumers. The keylogging attack either can be Performed using software or hardware keyloggers keyloggers.

1. Software based Keyloggers

Keylogging software is a type of software that monitoring is installed in the target computers and the Presence of software keyloggers cannot be estimatedbecause it is not in the task manager. The keylogger creates the log file for each session which is sent to the specified receiver. This danger was Recently Highlighted When Sumitomo Mitsui Banking Corporation discovered a keylogger installed on STI network in London [1]. There havebeen other high profile cases in the keylogging attack. Kinko In 2003, the author has installed the software over 14 locations in New York and used to open bank accounts with the names of some of the 450 users Whose Collected Personal information it has [2]. Also in 2003, the founder Gabe Newell Valve Software have found the source code for Half-Life 2 The Game of His stolen company after someone planted a keylogger on His [3] computer.

2. Hardware-based Keyloggers

Keyloggers are hardware-based devices like USB sticks or USB key that does not need the support of software components for computer work. The hardware keylogger can be injected into public computers without the knowledge of the user to monitor user behavior. The Key Grabber USB is a USB hardware keylogger with a 16 MB or 2 GB internal flash drive that is organized as a file system. All information typed on the keyboard will be captured by the USB KeyGrabber and stored on the internal flash drive in a special file. The captured data can be retrieved on any other computer with a USB port and keyboard, by switching to Flash Drive mode. The keylogger Gives instant access to all the data captured and pop up as a removable drive. The USB KeyGrabber is 100% transparent to the operation of the computer that requires no software or drivers.

C. Organization

The rest of His paper is organized as Follows. In Section II, the system, trust and models of attackers, and comparison of linear barcodes and QR codes are explained. In section III, the work of visual two authentication protocols is briefly explained. In Section IV, several issues related to the two protocols are explained. Section V reviews the related work of literature. In Section VI, the finding is made.

II. System and Threat Model

A. System Model

The model system is comprised of four various entities: as a client, a smartphone, the terminal (PC) of a client and a server. The client is a user or ordinary man with limited abilities remembering the credentials: including cryptographic keys and robust mathematical calculations. The device of a client is a client PC which is used to log on to a server to perform financial transactions. The client has a smartphone which stores the public key certificate of a server certificate or fitted with a digital camera. The server system is an entity belongs to the financial institution that interacts with the user by effecting all the back-end operations.

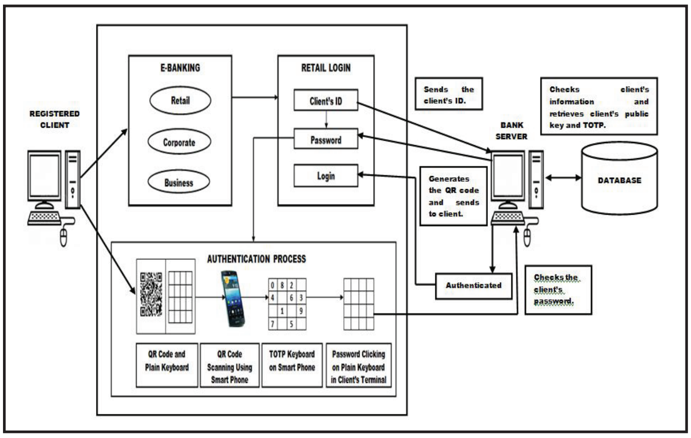

REGISTERED CLIENT
E-BANKING
Retail
Corporate
Business
RETAIL LOGIN
Client's ID
Password
Login
Sends the client's ID.
Checks client's information and retrieves client's public key and TOTP.
BANK SERVER
DATABASE
Generates the QR code and sends to client.
Authenticated
Checks the client's password.
AUTHENTICATION PROCESS
0 8 2
4 6 3
1 9
7 5
QR Code and Plain Keyboard
QR Code Scanning Using Smart Phone
TOTP Keyboard on Smart Phone
Password Clicking on Plain Keyboard in Client's Terminal

Fig. 1: Demonstrates the Overall System Architecture. Here, e-banking is taken as an example of how the Authentication Process Works

The customer or user is registered in a particular bank to conduct online transactions and provided with the unique client ID and password. The registered client can connect to a particular site of the bank. The customer must enter connection details. When the client sends the unique ID for the server, the server checks the customer information from the bank's database. If customer information is correct, the server retrieves the random time base of a password and fresh public key (TOTP) from the database. The server generates the QR code which includes single customer ID, the public key, and TOTP time slot. Then, the QR code is sent to the client. The client terminal, the QR code is displayed. Now, the customer must take his smartphone in which the QR code scanning application is already installed. The QR code to be scanned. After scanning the QR code, the decoded information will be displayed in the smartphone. The randomized keyboard that looks like a 4x4 matrix with random arrangements of Figures 0-9 is displayed on the smartphone.

B. Comparison of Quick Response Code with Linear Barcode

QR code developed by Denso Wave Japanese Company in 1994. It is a bar code in two dimensions. There are 40 versions and four error correction levels in the QR code. Barcodes are attached to all kinds of products for identification, which is a readable representation of data optical machine. Linear bar codes are one-dimensional and have a limited capacity of coding 10 to 22 characters. The QR code has the great capacity that can hold 7089 numeric, alphanumeric 4296 and 2953 binary characters. [1] QR Code was approved as a standard AIM, a JIS standard and ISO standard. So QR code is used in a wide variety of applications, such as manufacturing, automotive, logistics, sales, and other business applications. The QR code has the efficiency of decoding all kinds of information such as website URL, contact address, telephone number, geographical location, a text message, calendar event s, etc. some of the QR code features are distributed as shown below

- High capacity data encoding
- High-speed reading
- Chinese encoding capability
- Readable from any direction from 360 degree
- Dirt and Damage Resistant
- Structured Append Feature

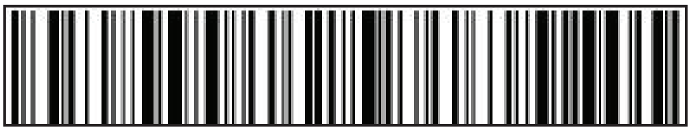


Fig. 2: Barcode

Fig. 3: QR Code

In early, the QR code was designed to be used in the automotive industry. But now it has been extensively used in advertising so that a client can use the smartphone and scan more information about the advertised products. The barcode scanner applications were created which is compatible for smartphones like Android and iOS.

III. An impervious qr-based visual Authentication

In this part two visual authentication protocols are explained. Before going into the protocols, it is need to know the algorithms used in the proposed system. The algorithms are described as follows.

A. Time-based One-Time-Password Protocol

In this part of a One-Time-Password an authentication protocol based on time was introduced that is identified as an early protocol. It is making use of captcha for authentication. The protocol was as follows:

The client sends the unique client ID to the server.

The server checks the client's information from the database and retrieves the client's public key (PKID).

The server then picks a fresh random string TOTP with a time slot and encrypts it with the public key to obtain

$$ETOTP = Encr(PKID\ (TOTP)) \quad (1)$$

The server generates the QR code and sends it to the client.

In the client's terminal, a QR code QREOTP is displayed.
The client decodes the QR code with

$$ETOTP = RDec(QR(ETOTP)). \quad (2)$$

The random string is encrypted with client's public key (PKID), the client can read the TOTP string only through her smartphone by

$$TOTP = Decrk(ETOTP\ ) \quad (3)$$

And type in the TOTP in the terminal with a physical keyboard.

B. Password-based Authentication Protocol With Randomized Onscreen Keyboard

In this section, the second protocol password-based authentication protocol is described. Here, the password is shared between server and client, and a randomized keyboard. The protocol works as follows:

- The client connects to the server and sends unique client ID to the server.
- The server checks the received unique client ID to retrieve the client's public key (PKID) from the database.
- The server prepares a random permutation of a keyboard arrangement, and encrypts it with the public key to obtain.

$$E_{KBD} = Encr(PK_{ID}\ (\pi)) \quad (4)$$

- The server encodes the cipher text with QR encoder to Obtain

$$QR(E_{KBD}) = QR(Enc(E_{kID}\ (\pi))) \quad (5)$$

- The server sends the result to the client with a blank keyboard.
- In the client's terminal, a QR code (QR(EKBD)) is displayed together with a blank keyboard.
- The onscreen keyboard does not have any alphabet on it, the client cannot input her password.
- The client executes her smartphone application which first decodes the QR code by applying to get the cipher text

$$QR(Dec(QR(E_{KBD})) \quad (6)$$

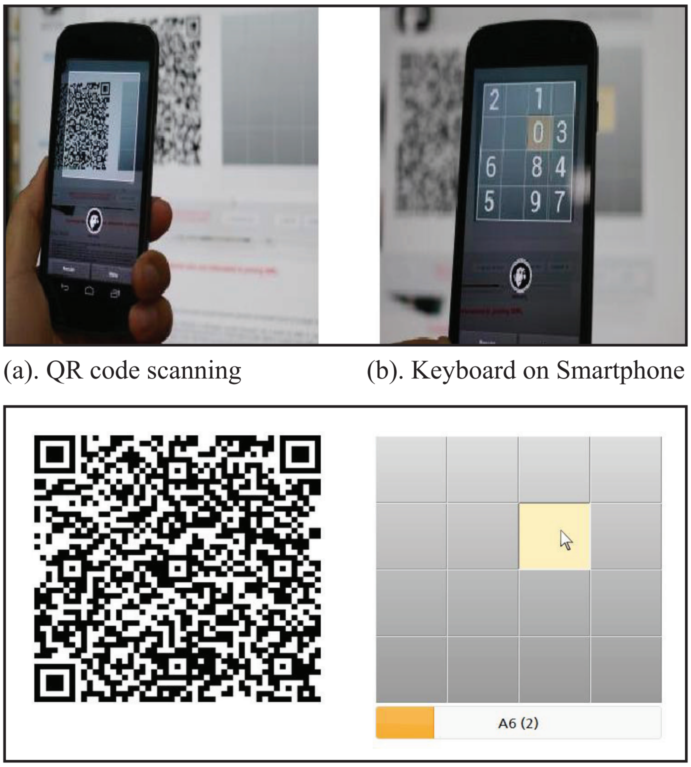
(E_{KBD}).

- The cipher text is then decrypted by smartphone application with the private key of client to display results on the smartphone'sscreen

$$\pi = Decr(SKID(EKBD)) \quad (7)$$

IV. Results

In this section, the several issues related to two protocols are discussed. Some of the issues are session hijacking, keylogging, transaction verification, securing transactions, visual channels and visual signature validation.



(a). QR code scanning (b). Keyboard on Smartphone

(c). Entering password for Empty Keyboard

Fig. 4 Shows the expected outcomes of the authentication protocols, (a) shows the QR code scanning at the terminal using smartphone. (b) Shows the encoded keyboard layout on the smartphone with the random arrangements of digits. (c) Shows the blank keyboard layout at the terminal which is prompting to click the password.

A. Preventing Session Hijacking

The attacker can divert the authentication session with malware immediately after the client enters a password. Session hijacking is detectable by the sending of the details linked to the server by using the smartphone transaction triggered by the customer via a side channel introduced in section E. Just after executing the password entry process the smartphone app can send more transaction information of customer demand is signed by signing private key of the smartphone and / or encrypted with the public key of the server over the cellular network.

B. Preventing Keylogging

The visual authentication protocols aims to prevent keylogging attacks. The customer simply clicks the password on the white keyboard. This ensures that only identity of the white keyboard are sent to the server. The keylogger cannot register the customer's strikes because the mouse is used to click on the password.

If smartphone has installed keylogger software installed, it can also capture every keystroke on client smartphone. But the customer is not using smartphones for authenticating. The smartphone shows only the QR code scanned say randomly arranged 4x4 keypad and if the shot is taken, there was no use. Because the keyboard layout will varies whenever the shopper scans the QR code for the authentication process.

C. Transaction Verification

Suppose a particular client is currently visiting a bank server and is about to transfer funds with another account. Even if the client terminal becomes infected with some malicious items or the customer is currently visiting a phishing site, it is unable to recognize easily, because the HTML page that the client is visually looks identical to the authentic page. Even when a server of the bank asks the customer to input powers as a password, one-time password produced by a hardware token and a certificate-based signatures confirming the transaction, the customer is prepared to entry his credentials at the request and with the identification information the attacker is able to prepare a valid request for transfer on its behalf.

D. Securing Transactions

Financial transactions are usually secured by encrypting all transaction-related information during the transmission. In many cases, the encrypted information should be decrypted at the terminal (client's PC, most likely, or a PC at public place) to be shown to the client. However, under the assumption that there is a malware inside the terminal, the attacker does not need to break the cipher, but is enough to read the information after being correctly decrypted. The encrypted channel is established just between the server and the client's terminal.

To make transactions more secure, it is needed to extend the encrypted channel beyond the client's terminal. Accordingly, instead of decrypting the cipher text at the client's terminal, decrypt it at the smartphone.

V. Conclusion

Both authentication protocols are provided to demonstrate how visualization can enhance the usability and security. In addition, these both protocols helps in overcoming many difficult as keylogging attacks and other malware attacks. This system can be carried out in many real world applications as it using simple and achievable technologies using the app as Android.

References

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

[2] D. Boneh, X. Boyen,"Short signatures without random oracles", In Proc. of EUROCRYPT, pp. 56–73, 2004.

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

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

[5] M. Farb, M. Burman, G. Chandok, J. McCune, A. Perrig. Safeslinger: An easy-to-use and secure approach for human trust establishment. Technical report, CMU, 2011.

[6] H. GAO, X. Guo, X. Chen, L. Wang, X. Liu. Yagp: Yet another graphical password strategy. In Proc. of ACM ACSAC, pp. 121– 129, 2008.

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

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

[9] E. Hayashi, R. Dhamija, N. Christin, A. Perrig,"Use your illusion: Secure authentication usable anywhere", In Proc. of ACM SOUPS, 2008.

[10] A. Hiltgen, T. Kramp, T. Weigold,"Secure internet banking authentication", IEEE Security and Privacy, 4, pp. 21–29, March 2006.

[11] N. Hopper, M. Blum,"Secure human identification protocols", In Proc. of ASIACRYPT, 2001.

[12] J. Katz, Y. Lindell,"Introduction to modern cryptography. CRC Press, 2008.

[13] M. Kumar, T. Garfinkel, D. Boneh, T. Winograd,"Reducing shoulder surfing by using gaze-based password entry", In Proc. of ACM SOUPS, pp. 13–19, 2007.

[14] Y.-H. Lin, A. Studer, Y.-H. Chen, H.-C. Hsiao, E. L.-H. Kuo, J. M. McCune, K.-H. Wang, M. N. Krohn, A. Perrig, B.-Y. Yang, H.-M. Sun, P.-L. Lin, J. Lee,"Spate: Small-group pki-less authenticated trust establishment. IEEE Trans. Mob. Comput. 9(12), pp. 1666–1681, 2010.

Badiga Neeraja, working as Asst. Professor in P.G College of Science, Saifabad, Hyderabad, India.