IJSEAT International Journal of Science Engineering and Advance Technology

Key logging Prevention by QR code with Visual Authentication

Kodiyala Devi Sireesha [1], D.Ramesh [2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: sireesha4cse@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract— Key logging is an activity of capturing users' keyboard the activity key logger hardware and software. The key loggers secretly monitor and log all keystrokes. Malicious programs, key loggers do not cause any threat to system can be used to intercept passwords unlike other and other of a computer confidential information entered via the keyboard by considering various root kits residing in PCs that breaches the security. Cyber criminals can get user names, email passwords, user in a covert manner. But it uses strokes and records PIN codes, passwords to online gaming accounts, e-payment systems, etc. As a result, it impersonates a user during authentication in financial transactions. To prevent keylogging, the strict authentication is required. The QR account numbers, email addresses, code can be used to design the protocols to achieve high usability and security. The two authentication protocols are Time based One-Time-Password protocol and Password-based the protocols are proved to be robust to several authentication attacks. And also by deploying these two protocols in authentication protocol. Through accurate analysis, real-world applications especially in online transactions, visual authentication the strict security requirements can be satisfied.

Key words: keylogging; phishing; QR code; authentication; malicious code attack; android; visualization pharming; session hijacking;

I. Introduction

The credential stealing and channel breaking attacks are the two major threats in electronic and financial services. The credential information such as users' identifiers, passwords, and keys can be easily stolen by the attacker from the target computers if they are less secured. On the other hand, channel breaking attacks allow eavesdropping of communication between the user and the financial institution. But the classical channel breaking attacks can be prevented by using IP sec and SSL security channels. The recent channel breaking attacks are more challenging like keylogging which utilizes session hijacking, pharming, phishing and visual fraudulence. It is difficult to prevent these attacks by simply encryption. For example, if a personal computer is infected with malicious software, then it is an easy target for credential attackers. Keyloggers are used as a surveillance tool by the employers to ensure employees use work computers for business purposes only. Unfortunately, key loggers are embedded in spyware and allow the information to be sent to unknown third party. Keyloggers can be used in some IT organizations to troubleshoot technical problems in computers and business networks. Keyloggers are also used by a family or business to monitor the people without their knowledge. Finally, keyloggers are installed in public kiosks to steal credit card information or passwords. Keylogging allows malicious software to capture keyboard strokes whenever the user types in the specific application or forms to obtain the passwords. Cyber criminals use keylogging to capture credentials and authentic information to hack the account and performs financial fraudulence and therefore gains access to confidential information. Malware uses several and other operating system services. The keylogger is present both in personal and public computers and it is pervasive. Techniques to log keystrokes such as hooking into the keyboard driver Keyloggers are often root kitted. So the presence of keyloggers cannot be detected. To overcome keylogging attack, virtual or onscreen keyboards are used. Both the techniques rearrange the alphabets randomly and therefore frustrate simple keyloggers. But the keylogger has control over the entire PC, which can capture every event and read the video buffer to create a mapping between the clicks and new alphabet. The keylogging attack is quite similar to the shoulder-surfing attack where the attacker sees the direct input of the client to the computer and also every behaviour of the client. Many graphical password schemes are introduced in to prevent shoulder-surfing attack. But many of these schemes are unusable. Even though the are securely delivered to the client's PC, the attacker residing on the client's PC can easily observe and deceive cryptographic secrets the information. To solve this problem, the intermediate to design a human involving protocol. Every interaction between the client and device is visualized using device between human the intermediate and terminal is introduced. This helps Quick Response (QR) code. In these protocols, the memorize any information other than password and PIN. However, the authentication process can be visualized does not which A smart phone with camera is used to visualize enhances security and usability to the client. The security protocol has the client involvement using smartphone with augmented reality. Authentication process.Instead of implementing the entire security protocol in computer, a part of it is moved to the smartphone. This visualization in smartphone offers protection against malware, keylogging attacks and shoulder-surfing attacks.

A. Scope and Contributions

The two visual authentication protocols are introduced to show how visualization can enhance security and usability.

The two authentications and password-based authentication protocol. Through accurate analysis, one can prove that these two protocols are resistant against many challenging attacks that are applicable in other protocols specified in the literature. Protocols are time-based one-time-password protocoltwo protocols are secure under many real-world attacks that visualize the authentication process to enhance both security and usability. The prototype implementation in the form of Android smartphone applications demonstrates the usability of protocols in real world deployment. The visual authentication protocols can be used in ATM and public computers which involve financial transformations. Moreover, it does not need any channel between the server and the smartphone.

B. Types of Keyloggers

Keyloggers are a serious security threat that can be extremely harmful to both businesses and consumers.The keylogging attack can be performed either using software keyloggers or hardware keyloggers.

1) Software-based Keyloggers

The keylogging software is a type of surveillance software which is the presence keyloggers cannot installed into the target be felt since it is not of software shown in the task manager. The keylogger creates the log file for every session which is sent to the specified receiver. This danger was recently highlighted when Sumitomo Mitsui Banking network in London. There have been other high-profile cases in keylogging computers and attack. the perpetrator Corporation discovered a key logger installed on its installed the software at more than locations in New York and using it to open bank accounts with the names of some of the, Valve Software founder found the source code to his company's game stolen after someone based, packet analyzers, and remote access software key loggers. planted a keylogger on his computer. Some of the software-based API-based, kernel-based, form grabbing based, memory injection.

2) Hardware-based Key loggers

The keyloggers are the hardware devices like USB or pendrive need any support of software componentswork which does not on computer. The hardware keyhardware-based to logger may be injected into the public computers without the knowledge of the user to monitor the behaviour of the users. The KeyGrabber USB is an USB hardware keylogger with a disk which internal flash is organized as a file system. Any information typed internal flash on the keyboard by the KeyGrabber and stored on the internal Flash special file. This captured data may be retrieved on any other computer containing a USB port and keyboard, by switching into the keylogger gives instant access to all transparent for computer operation which does not requires software or drivers. Drive in a Some of the hardware-based keyloggers are firm-based, wireless keyboard Flash Drive mode sniffers, captured data and keyboard overlays, acoustic keyloggers, evidence.Electromagnetic emissions, optical surveillance, and physical.

***C.* Organization**

The rest of this paper is organized as follows. In section II, the system, trust and attacker models, and comparison of linear barcode and QR code are explained. In section III, the working of two visual authentication protocols is briefly explained. In section IV, several issues related to two protocols are explained. Section V reviews the related works from the literature. In section VI, the conclusion is made.

II. System And Threat Model

A. System Model

The system model comprises of four different entities such as a client, a smartphone, and a client's terminal (PC) and a server. The client is a user or an ordinary human with limited capabilities of remembering cryptographic credentials such computations. Server or digital certificate equipped with a camera. The server is the system entity belongs to the financial institution which interacts with the user by performing all the back-end operations.

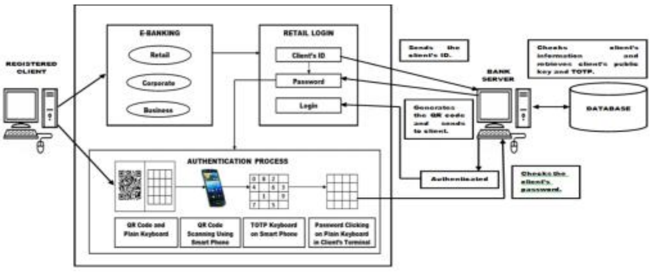

REGISTERED CLIENT
E-BANKING
Retail
Corporate
Business
RETAIL LOGIN
Client's ID
Password
Login
Sends the client's ID.
Checks client's information and retrieves client's public key and TOTP.
BANK SERVER
Generates the QR code and sends to client.
DATABASE
AUTHENTICATION PROCESS
Authenticated
Checks the client's password.
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

Fig1. Shows the overall system architecture.

Here, the e-banking is taken as an example to show how the authentication process works.The client or a user is registered in a particular bank for performing online transactions and provided with the unique client ID and password. The registered client can log on to particular bank site. The client must enter into retail login. When the client sends the unique ID to the server, the server checks the client's information from the bank database. If the client's information is correct, the server retrieves the public key and fresh random time-based one-time-password from the database. The server generates the QR code which comprises of unique client ID, public key, and TOTP and time slot. Then theQR code is sent to the client. On client's terminal, the QR code is displayed. Now, the client has to take his smartphone in which the QR code scanning application is already installed. The QR code has to be scanned. After scanning the QR code, the decoded information will be displayed in the smartphone. The randomized keyboard which looks like a 4x4 matrix with random arrangements of 0-9 digits is displayed in the smartphone. On the client's terminal the password box is replaced with the 4x4 blank keyboard matrix. Now, the client has to just click on the rows or columns of the blank keyboard matrix by seeing where password is have been arranged in the smartphone. Only the ID of the keyboard matrix is sent to the server. The server also does not know the password of the client. Based on the ID of the keyboard matrix, the client gets authenticated. If the client clicks on the wrong ID, again the previous steps are repeated by sending a newly generated QR code to the client. And also if the client fails to from the client's login within the allotted time slot, the server will automatically generates a new QR code with new TOTP. After the authenticated, the client can client gets enjoy all the e-banking services.

B. Trust and Attacker Models

The following must be assumed to ensure that the entities of the system are secure and trusted. First, the channel between server and is secured with an SSL or HTTPS connection. Second, to be the server is assumed immune to several attacks. So, the attacker concentrates on the client. Third, the keylogger attacker resides on the client's terminal. The attacker is capable of client's terminal capturing the security of the system.

The attacker has full control over the client's terminal. So,

1) The attacker can capture client's credential information such as password, private key and TOTP.

2) The attacker can perform session hijacking by showing a fake genuine looking webpage in financial transactions. Therefore the authenticated session can be hijacked by the attacker.

C. Comparison of Quick Response Code with Linear Barcode

QR code is developed by Japanese Denso Wave. It is a two dimensional barcode. There are 40 versions and four levels of error correction in QR code. The barcodes are attached to all sorts of products for identification which is an optical machine-readable representation of data. Linear barcodes are one dimensional and have a limited capacity of coding 10 to 22 characters. The QR code has the high capacity which can hold 7,089 numeric, 4,296 alphanumeric, and 2,953 binary characters. QR Code has been approved as an AIM Standard, a JIS Standard and an ISO standard. So QR Code is being used in a wide variety of applications, such as manufacturing, automotive, logistics, sales, and other business applications. The QR code has the efficiency to decode all types of information such as website URL, contact address, phone number, geographical location, a text message, s calendar event, etc. some of the features of QR code are given as follows:

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

Fig2. Barcode

Fig3. QR code

At first, the QR code has been designed to be used in automotive industries. But now, it has been widely used in the advertisement so that a client can use the smartphone and scan to know more information about the advertised products. The barcode scanner applications are created which is compatible for smartphones like android and ios.

III. An Impervious Qr-Based Visual Authentication Protocols

In this section, two visual authentication protocols are explained. Before getting into the protocols, it is necessary to know about the algorithms used in the proposed system. The algorithms are explained as follows. The public key encryption scheme with IND-CCA2 security would be good for the proposed system application. IND-CCA2 makes the cipher text different even though the plaintext is the same whenever encrypted by adding random padding to a plaintext. This restriction will prevent an attacker from checking whether his guess for the random layout is right or not. Thus, the security of the scheme is not dependent on the number of possible layouts but the used encryption scheme. If no such encryption is used, the adversary will be able to figure out the layouts used because he will be able to verify a brute-force attack by matching all possible plaintexts to the corresponding cipher text. On the other hand, when such encryption is used, the 1-1 mapping of plaintext to cipher text does not hold anymore and launching the attack will not be possible at the first place. Also, any signature scheme with EUF-CMA can be used to serve the purpose of proposed system. For details on both notions of security, see. In particular, and for efficiency reasons, the short signature is recommended.

A. *Time-based One-time-password protocol*

In this section, a Time-based One-time-password authentication protocol is introduced which is referred as first protocol. It use of random string for authentication. This protocol works 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
- 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
- the random string is encrypted with client's public key (PKID), the client can read the TOTP string only through her smartphone by terminal with a physical keyboard.
- the client has to type the TOTP in the terminal where the keyboard matrix is displayed.
- the server checks the result entered by the client and if it matches what the server has sent earlier, the client is authenticated.
- if the client does not authenticated, the access is denied.

B. Password-based authentication protocol with randomized onscreen keyboard

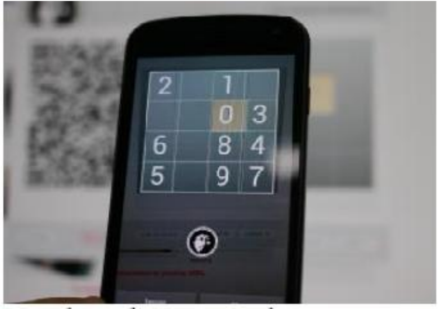
In this section, the second protocol password-based authentication protocol is described. Here, the password is shared between server and client, and a randomized keyboard. The protocol works as follows:

- 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 EKBD = Encr(PKID (π)). (1)
- The server encodes the ciphertext with QR encoder to obtain QR(EKBD) = QR(Enc(EkID (π))). (2)
- 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.

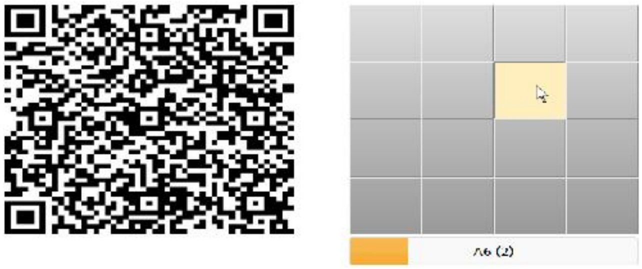
IV. Discussion

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) Clicking password on blank keyboard

***2)* Replacing Visual channels with Bluetooth**

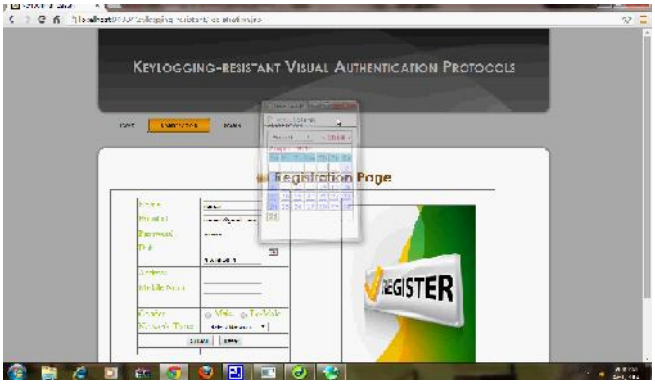
The visual channel in Protocol 1 (that uses TOTP) is used to transfer the encrypted TOTP from PC to the smartphone, and the client plays a role of another channel from the smartphone to PC by entering the decrypted OTP into PC. Here, both channels (from PC to the smartphone and vice versa) can be replaced with other channels such as Bluetooth, and the whole authentication procedure can be automated. This will significantly enhance the usability of the authentication protocol. However, in another aspect, not all PCs are equipped with the Bluetooth module. Also, even though PC has the Bluetooth module, it might be an annoying job to execute the pairing whenever the client uses a device that she has never paired before. In that sense, Protocol 1 with visual channel and client’s entering PIN are easier to be deployed in the current environment.

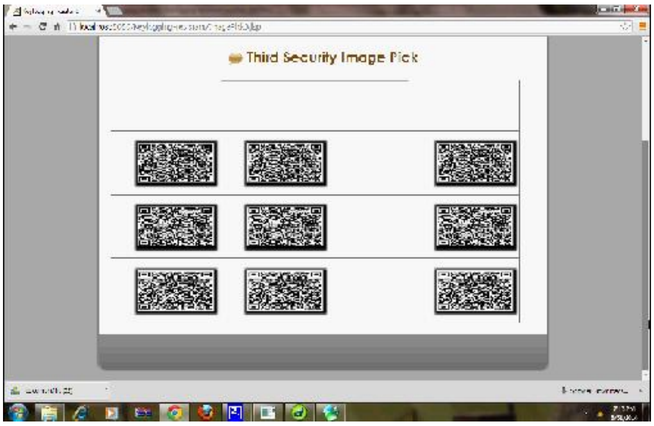
V. Related Work

A closely related vein of research is trust establishment for group communication using cognitive capabilities. Examples of such works include SPATE, GAnGS, and Safe Slinger. None of these works use visualization as reported in this work, although they provide primitives for authentication clients and establishing trust of 2D barcodes to resist the man-in-the-middle attack in device pairing. These protocols are tailored to the problem settings in hand, e-banking, with a different trust and attack model than tools by using the 2D barcodes for information representation, and the visual channel for communicating this information, these protocols are further more generic than those proposed in that used in which results into different guarantees as explained earlier in this paper. To prevent against phishing, Parno et al. suggested the use of trusted devices to perform mutual authentication and eliminate reliance on perfect client behaviour.

Results

Screen Shots





VI. Conclusion

The two securities moreover, these two protocols help and other malware attacks. This system can be implemented to can enhance overcome authentication protocols are proposed to show how visualization usability many challenging attacks such as key logging in many real world applications since it utilizes simple technologies and feasible to use as android application.

References

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

[2] D. Boneh and X. Boyen. Short signatures without random oracles. In Proc. of EUROCRYPT, pages 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, 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] N. Doraswamy and 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, and 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, and X. Liu. Yagp: Yet another graphical password strategy. In Proc. of ACM ACSAC, pages 121–129,2008.

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

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

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

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

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

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

[13] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd.Reducing shoulder surfing by using gaze-based password entry. In Proc. of ACM SOUPS, pages 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, and J. Lee. Spate: Small-group pki-less authenticated trust establishment. IEEE Trans. Mob. Comput., 9(12):1666–1681, 2010.

[15] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In Proc. of IEEE Symposium on Security and Privacy, pages 110–124, 2005.