IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Foiling Keylogger Attacks using Virtual Onscreen Keyboard

Jayalekshmi K.S

M.Tech in Computer Science and Engineering, UGC NET Scholar, Thiruvananthapuram, India

DOI: https://doi.org/10.26438/ijcse/v7i2.635639 | Available online at: www.ijcseonline.org

Accepted: 21/Feb/2019, Published: 28/Feb/2019

Abstract**—**Key loggers are hardware or software tools designed to record user's keyboard strokes. They are a threat during authentication as they can capture important information from the target computers through secret installation. They are largely undetected by most anti-virus software. To prevent key logger attacks, virtual on-screen keyboard with random keyboard arrangement is used**.** Unfortunately, the key loggers have improved tremendously. They take control of the personal computer and can capture every event and read the video buffer. By using cryptographically strong keys and passwords information can be delivered securely to the user's computer. But humans may not have sufficient memory to remember cryptographically strong keys. This can be solved by introducing an intermediate device that bridges humans and user terminal. The proposed authentication scheme is a password-based authentication method using a randomized onscreen keyboard. The scheme utilizes a smartphone as the intermediate device which contains the keys required for decryption. The encrypted contents are encoded into QR (Quick Response) codes. QR codes can be scanned using the smartphone. The user owns a user id and a password. The user terminal will display a blank keyboard and the QR code which carries the encrypted random permutation of keyboard arrangement. The QR code will be decoded using the intermediate device. Looking at the keyboard arrangement in the intermediate device the user needs to click the buttons on the blank keyboard to input the password. The use of IMEI (International Mobile Equipment Identity) of the smartphone prevents the attackers from using any other phones for authentication even if he knows the user-id, password and the key for decryption.

Keywords**—** QR code, password based authentication, smartphone, IMEI

I. INTRODUCTION

Spyware attacks have become one among the greatest threats to enterprise security [1]. They have resulted in extracting sensitive information from the target computer. The use of textual passwords for authentication is common today. But the stealing of textual passwords has become a common occurrence due to spyware attacks. Keyloggers are capable of residing in systems by sharing the system resources with other legitimate programs for a long time. Keyloggers functionality have extended beyond recording keyboard characters. Some can function as screen scrapers which can take snapshots of screen periodically. These snapshots may contain credentials used for authentication. The use of virtual onscreen keyboards for authentication fails due to such key loggers

A key logger attack is similar to shoulder-surfing attack as a key logger can see the characters entered by the user. To prevent shoulder surfing attack, various graphical password methods have been introduced [2]. But they aren't usable like textual passwords. Information could be delivered securely to the user's computer by using cryptographically strong keys and passwords. But humans don't have enough memory to memorize these keys. Therefore an intermediate device is used to store the keys.

A novel authentication protocol is proposed that can mitigate key logger attacks. A blank keyboard (no characters shown) will be displayed on the screen of the user terminal and the user authentication should be done using this keyboard. The full keyboard (with characters are shown) will be displayed on an intermediate device looking at which the user needs to input the credentials on the user terminal. The intermediate device used is a smartphone. The smartphone also stores cryptographically strong keys which are required to deliver the information securely. The user will have a user-id and a password. Initially the user will input the user-id. On the basis of the user-id received, a random permutation of the keyboard is generated and encrypted at the server. A QR (Quick Response) code is also generated which consists of the encrypted permutation of the keyboard. The QR code along with the blank keyboard is displayed on the user terminal screen. The user needs to use the smartphone to scan the QR code and decrypt the contents in the code. The full keyboard will be displayed on the intermediate device. Looking at the intermediate device, the user needs to input his/her password by clicking on the buttons that corresponds to the password of the user on the user terminal. To ensure that the user is using his/her smartphone to scan the QR code the IMEI (International Mobile Equipment Identity) of the phone is verified.

The paper is organized as follows. Section II contain various works on avoiding key logger attacks. Section III deals with the proposed authentication scheme. Section IV presents the result of the authentication protocol. Section V concludes the paper with conclusion and future scope

II. Related Work

Many works were published based on how to resist the key logger's attack [3], [4], [5]. The proposed authentication protocol uses two concepts: the concept of a visual channel and the concept of a intermediate device. In [6], a system called SiB (Seeing-Is-Believing) is introduced that utilizes 2D barcodes and camera phones to implement a visual channel for authentication and demonstrative identification of devices. In SiB, visual channel means a device using its camera takes a snapshot of a barcode that has a cryptographic material encoded with it. The visual channel can be applied to several problems in computer security, including an authenticated key exchange between devices that share no prior context. Bar codes can be generated on demand and displayed on the screen. Demonstrative identification is a property which means that the user is sure his/her device is communicating with the device it really wants to communicate by visually identifying the device.

The visual channel is implemented with a 2D bar code displayed on a device's screen and the device that needs to communicate with it will aim the camera at the 2D barcode. Demonstrative identification of the target device is achieved through the act of aiming the camera at the desired device. The authors have introduced show mode and find mode. A device displaying the 2D bar code is in show mode and the device whose camera is active is in find mode. Suppose Alice and Bob want to set up a secure channel between their camera phones. A 2D bar code is generated in Alice's phone encoding appropriate public cryptographic material and *Shows* it on its screen, while Bob uses his phone's digital camera in *Find* mode. In *Find* mode snapshot of Alice's screen displaying the barcode is taken. Bob must watch his phone's LCD, acting as viewfinder, updating in real time in response to his positioning of his camera-phone. A bar code recognition algorithm processes each image in the viewfinder in real time and overlays a coloured rectangle around recognised barcodes. Once a bar code is successfully recognised, the view-finding process stops and the barcode and error-correcting algorithms return the data represented by the barcode.

In [7] authors have introduced two visual authentication protocols that prevent key logging attacks. Using the smartphone the QR code, which is displayed on the user's terminal is scanned. The QR code has encrypted information. The two visual authentication protocols are authentication using OTP (One Time Password) and authentication using a password and randomized onscreen keyboard. These protocols use QR codes to represent the encrypted information and the visual channel to communicate the information. The encryption is done using the RSA encryption algorithm. In the first protocol, the QR code has encrypted OTP and the other has the encrypted permutation of the keyboard. The QR code is decoded with the smartphone using a QR code scanner. The decryption is done with the smartphone and the result is displayed on the smartphone screen. In the first protocol, the information decrypted is the OTP which is typed on the keyboard in the user terminal for authentication. In the second protocol, the permutation of the keyboard is displayed on the smartphone's screen looking at which the user needs to click on the keys of the blank keyboard displayed on the user terminal screen

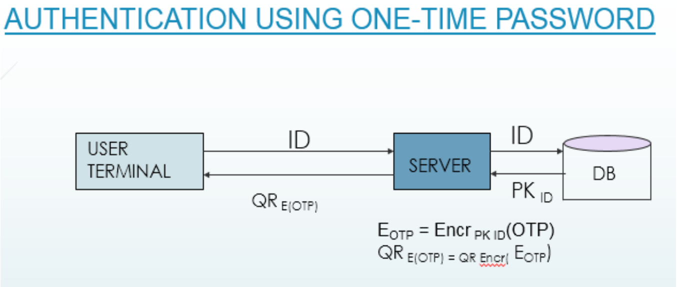

AUTHENTICATION USING ONE-TIME PASSWORD
USER TERMINAL
ID
SERVER
ID
DB
PK ID
QR E(OTP)
E_OTP = Encr PK ID(OTP)
QR E(OTP) = QR Encr(E_OTP)

Figure 1. Authentication using OTP- QR code generation

- ID -user-id.
- PK $_{ID}$ - the public key of the user.
- Encr $_{PK\ ID}$ (OTP) – Encryption of OTP using public key (PK $_{ID}$) of user. (RSA)
- QR $_{Encr}$ (E$_{OTP}$) – Encoding of encrypted OTP using QR encoding algorithm

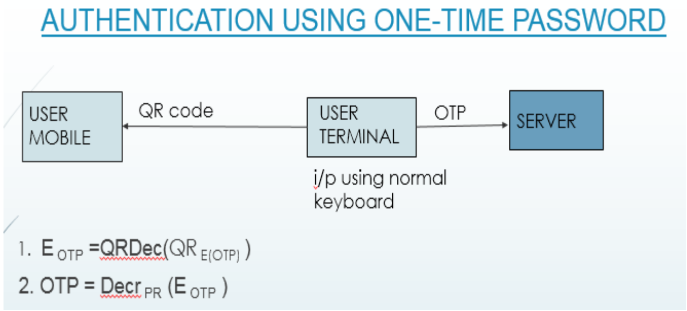
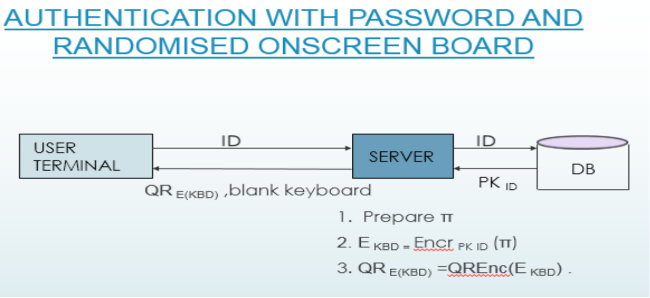

AUTHENTICATION USING ONE-TIME PASSWORD
USER MOBILE
QR code
USER TERMINAL
OTP
SERVER
i/p using normal keyboard
1. E OTP =QRDec(QR E(OTP))
2. OTP = Decr PR (E OTP)

Figure 2. Authentication using OTP- Decoding of QR code and decryption of OTP

- QR$_{Dec}$ (QR $_{E\ (OTP))}$ – Decoding of QR code using QR decoding algorithm.
- Decr $_{PR}$ (E$_{OTP}$) – Decryption of E$_{OTP}$ using private key (PR)of user.(RSA)

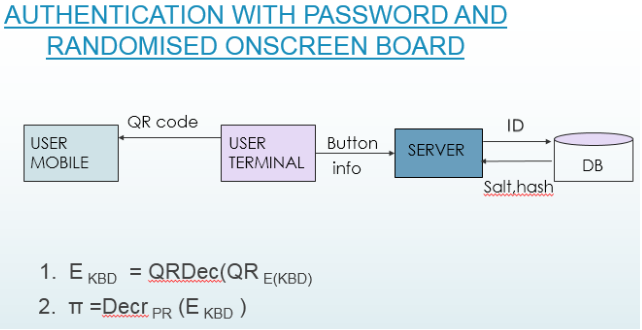


AUTHENTICATION WITH PASSWORD AND RANDOMISED ONSCREEN BOARD

1. Prepare π
2. $E_{KBD} = Encr_{PK\ ID}$ (π)
3. $QR_{E(KBD)}$ =QREnc(E_{KBD}) .

Figure 3. Authentication with password and randomized onscreen board- QR code generation

- Π- Permutation of keyboard.
- Encr $_{PK\ ID}$ (Π) – Encryption of Π using public key (PK_{ID}) of user.(RSA)
- QR $_{Encr}$ (E_{KBD}) –Encoding of encrypted Π using QR encoding algorithm



AUTHENTICATION WITH PASSWORD AND RANDOMISED ONSCREEN BOARD

1. E_{KBD} = QRDec(QR $_{E(KBD)}$
2. π =Decr $_{PR}$ (E_{KBD})

Figure 4. Authentication with password and randomized onscreen board- Decoding of QR code and decryption of Π.

- QR_{Dec} (QR $_{E\ (KBD)}$)- Decoding of QR code using QR decoding algorithm.
- Decr $_{PR}$ (E $_{KBD}$) – Decryption of E_{KBD} using private key (PR)of user.(RSA)

III. PROPOSED AUTHENTICATION SCHEME

In [7] there are certain drawbacks:

- The protocols fail if smartphone theft happens or some damage occurs to the phone.
- If an authorized user becomes an attacker and if he has the secret key and password of the victim then the second protocol is compromised as the attacker can use any smartphone for the attack.
- Shoulder surfing attacks are possible.

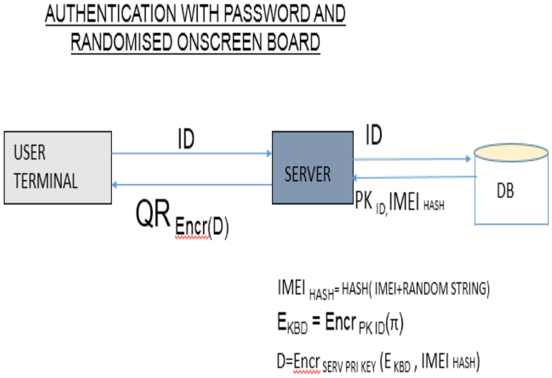
To avoid the second drawback, a number that uniquely identifies the device can be used. The IMEI number could be used. It can be found printed inside the battery compartment of the phone. The number is used by the GSM network to identify valid devices. A stolen phone can be blocked from accessing the network based on IMEI.

The proposed protocol is illustrated in an online banking scenario. There will be a registration phase initially in which the employee of a bank register the customer's basic details and sends the customer id to the customer's email. The customer registers in the smartphone app using the customer-id. The private-public key pair generation occurs and the public key of the customer is sent to the server. At the end of the registration phase, the IMEI will be retrieved from the smartphone. A random string is also generated for each new user. The IMEI is concatenated with the random string and the hash value is taken. A random string is concatenated with IMEI so that an attempt of IMEI duplication is foiled. The hash value is encrypted using the server public key and sent to the server. The login process is as follows:

After the customer has successfully completed the second phase of registration a customer can login into the account.

1. Initially customer-id needs to be provided.
2. On the basis of the customer-id the public key as well as the IMEI $_{HASH}$ is retrieved from database.
3. Random arrangement of a 36 character (0-9, a-z) keyboard is generated which is encrypted using the public key of the user.
4. Along with the encrypted permutation, the IMEI $_{HASH}$ is added and encrypted using the server private key.
5. The QR code of the above is generated and sent to the user terminal.
6. At the user terminal the QR code along with the blank keyboard will be displayed.
7. The QR code displayed on the screen is decoded by customer's smartphone.
8. Decryption is done using the server public key that is present in the smartphone. After decryption we will get the IMEI $_{HASH}$ and the encrypted keyboard. At this stage, the decrypted IMEI $_{HASH}$ is checked with the hash of IMEI and random string. IMEI and random string are dynamically retrieved from the phone the customer is using. If both are same then the keyboard will be decrypted using the private key of the customer. Else the authentication fails.
9. The customer needs to click on the buttons on the screen by looking at the keyboard displayed on the phone's screen. On the phone's screen all characters will be displayed whereas on the terminal only blank keyboard will be displayed.
10. Passwords are not stored in database as such. The hash value of password together with the random string or salt is stored in the database.
11. During authentication, the hash value and the salt is retrieved from the database. The salt is concatenated

with the password received from the customer. The hash value of it is taken. If the computed hash value and the retrieved hash are equal then the user is directed to his/her homepage.



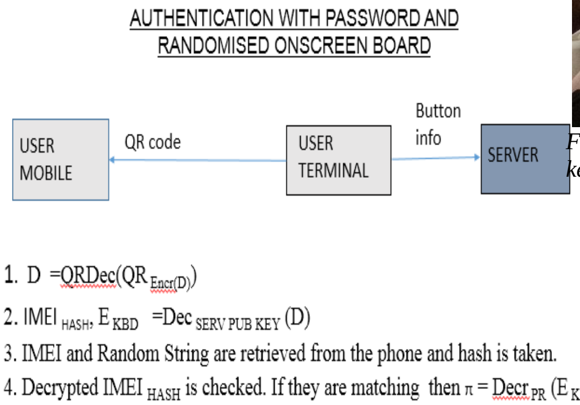
$IMEI_{HASH}$= HASH(IMEI+RANDOM STRING)

E_{KBD} = $Encr_{PK\ ID}(\pi)$

D=$Encr_{SERV\ PRI\ KEY}$ (E_{KBD} , $IMEI_{HASH}$)

Figure 5. Authentication with password and randomized onscreen board- QR code generation

- Π- Permutation of keyboard.
- Encr $_{PK\ ID}$ (Π) – Encryption of Π using public key (PK_{ID}) of user.(RSA)
- D=Encr $_{SERV\ PRI\ KEY}$ (E $_{KBD}$, IMEI)- Encryption of E $_{KBD}$ and IMEI using server private key.
- QR $_{Encr}$ (D) –Encoding of encrypted Π and the IMEI using QR encoding algorithm

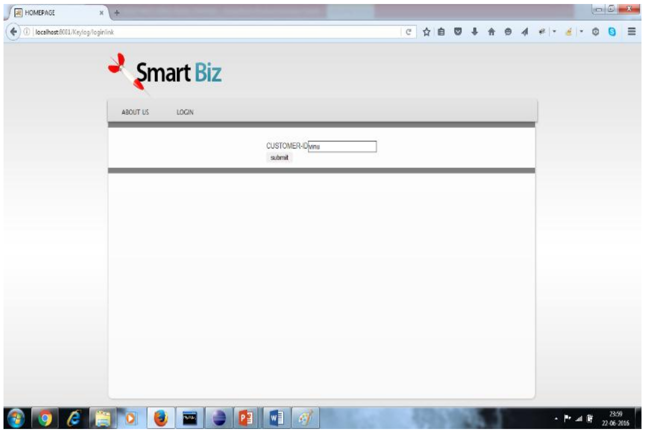


1. D =QRDec(QR $_{Encr(D)}$)
2. IMEI $_{HASH}$, E $_{KBD}$ =Dec $_{SERV\ PUB\ KEY}$ (D)
3. IMEI and Random String are retrieved from the phone and hash is taken.
4. Decrypted IMEI $_{HASH}$ is checked. If they are matching then π = Decr $_{PR}$ (E $_{K}$

Figure 6. Authentication with password and randomized onscreen board- Decoding of QR code and decryption of Π.

- QRDec (QR $_{Encr(D)}$))- Decoding of QR code using QR decoding algorithm
- Dec $_{SERV\ PUB\ KEY}$ (D) - Decryption of D using server public key.
- Decr $_{PR}$ (E $_{KBD}$) – Decryption of E_{KBD} using private key (PR)of user.(RSA)

IV. Results and Discussion



CUSTOMER-ID vinu

Figure 7. Login page of customer-Customer entering Customer-id

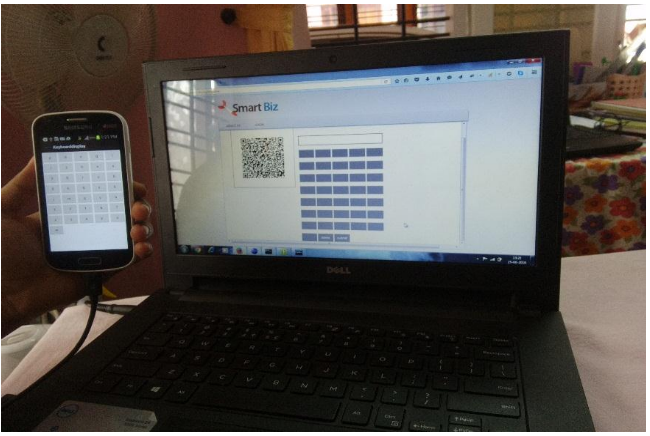


Figure 8. Customer scanning the QR code using smartphone and keyboard displayed on smartphone

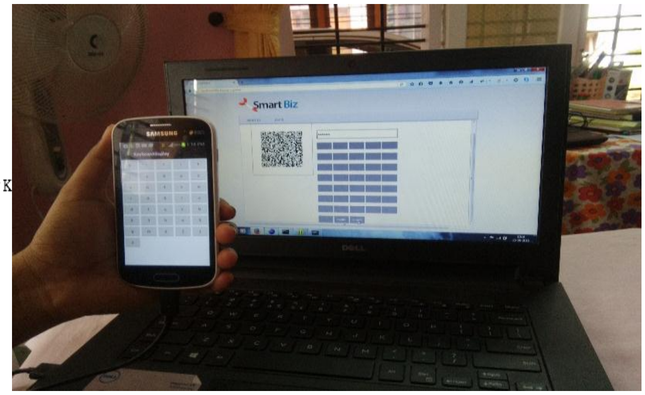


Figure 9. Customer inputs the password by clicking buttons on the screen.

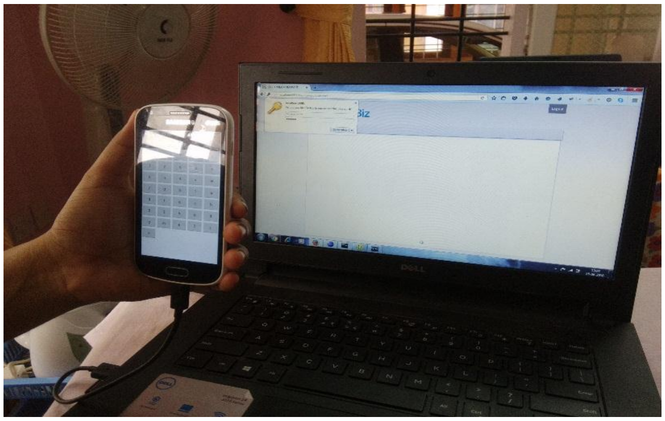


Figure 10. Customer is directed to homepage

The proposed protocol has eliminated the attack stated as the 2nd drawback with IMEI. The random string foiled the attempt of IMEI duplication

V. CONCLUSION AND FUTURE SCOPE

The possibility of shoulder-surfing attack still exists. During authentication when a user is using the smartphone to click on the buttons on the phone screen an attacker can view the process from behind of the user.

REFERENCES

[1] Seref Sagiroglu and Gurol Canbek, "*Key loggers –Increasing threats to Computer Society and Privacy*" IEEE TECHNOLOGY AND SOCIETY MAGAZINE | FALL 2009.

[2] Reza Jalili, "Secure *Data Entry and Visual Authentication System and Method*", U.S Patent Appl No: 08/980,748, March 27 2001.

[3] Timothy William Cooper, "*System and login resistance to compromise*", U.S Patent Appl No:12/070 627, June 2011

[4] Ramarao Pemmaraju, "*Methods and apparatus for securing keystrokes from being intercepted between the keyboard and a browser*" U.S Patent, Appl. No: 11/656,236, August 2007

[5] Stuart P. Goring, Joseph R. Rabaiotti and Antonia J. Jones," *Anti-key logging measures for secure Internet login: an example of the law of unintended consequences*", Computers and Security, February 2007

[6] McCune, J.M., Perrig, A. and Reiter, M.K. (2009) '*Seeing-Is-Believing: using camera phones for human- verifiable authentication*', Int. J. Security and Networks, Vol. 4, Nos. 1/2, pp.43–56

[7] DaeHun Nyang, Aziz Mohaisen, Jeonil Kang," *Key Logging-Resistant Visual Authentication Protocols*" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.13, NO. 11, NOVEMBER 2014

Author Profile

Jayalekshmi K.S completed Bachelor of Technology in Information Technology from University of Kerala in 2014 and Master of Technology in Computer Science and Engineering from University of Kerala in 2016.