Avoid Key Logger Attacks Using Blank Virtual Onscreen Keyboard

Jayalekshmi K S[1], Sunitha S[2]

[1] M. Tech Student, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India

[2]Assistant Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India

Abstract: ***Keyloggers are hardware or software tools that record keyboard strokes. They are a threat during authentication as they can steal important information from the target computers through hidden installation. Nowadays to avoid keylogger attacks, virtual on-screen keyboards are used. But the keylogger has control over the entire Personal Computer (PC) and can read the video buffer. A novel authentication scheme is proposed using blank onscreen keyboard known as password based authentication protocol.***

Keywords: Visual channel, password based authentication, smartphone, IMEI

1. Introduction

Spyware has become one among the greatest threats to enterprise security [7]. Attacks made by them have resulted in extracting sensitive information from the target computer. The use of textual passwords for authentication has become common nowadays. But the spyware attacks have resulted in stealing of passwords becoming a common occurrence.

Keyloggers pose a serious problem as they remain invisible to anti-virus software. They are capable of residing in the system by sharing the system resources with other programs for a long time until their tasks is done. Key loggers have functionality that extend beyond recording keyboard characters. Some can function as screen scrapers which are capable of taking snapshots of screen periodically. These snapshots may contain some valuable information which may include the credentials used for authentication.

A keylogger attack is identical to shoulder-surfing attack as a keylogger can see the characters typed by the user. To avoid shoulder surfing attack, numerous graphical password methods have been introduced [6]. But they aren"t usable like textual passwords. Information can be delivered securely to the user"s computer by using cryptographically strong keys and passwords. Since humans don"t have sufficient memory to memorize cryptographically strong keys an intermediate device is used to store the keys [1]. A smartphone is used as the intermediate device. Quick Response codes (QR codes) are used to store encrypted contents. QR codes are scanned using the smartphone

2. Related Works

In [1] two visual authentication protocols that prevent key logger attacks are introduced. The authors have proposed the idea of an intermediate device that bridges between humans and terminal. A smartphone, as the intermediate device is used to scan the QR code. QR code is displayed on the user"s terminal. The credentials for authentication is encrypted and encoded in QR code. In [3] an approach called Seeing is Believing (SiB) is introduced to prevent man in the middle attack. In this approach a device using its camera takes a snapshot of a barcode encoding cryptographic material identifying public key of the device with which it needs to pair. The approach of taking the snapshot using camera is known as visual channel. They also use 2D barcodes to resist man-in-the middle attack in device pairing. The two visual authentication protocols in [1] are: authentication using One Time Password (OTP) and authentication using password and randomized onscreen keyboard. Both authentication protocols use 2D barcodes to represent encrypted information and the visual channel to communicate this information.

The encryption is done using RSA. In the first protocol encrypted OTP is encoded in QR code and the other has encrypted permutation of keyboard encoded in QR code. The QR code is decoding is done in the smartphone using QR code scanner. The decryption process is also done with the smartphone and the result is displayed on the smartphone screen. In the first protocol the decrypted OTP is displayed on the phone"s screen which is typed on the keyboard for authentication. In the second protocol the permutation of keyboard is displayed on the smartphone screen looking at which the user needs to click on the keys of the blank keyboard displayed on the terminal screen.

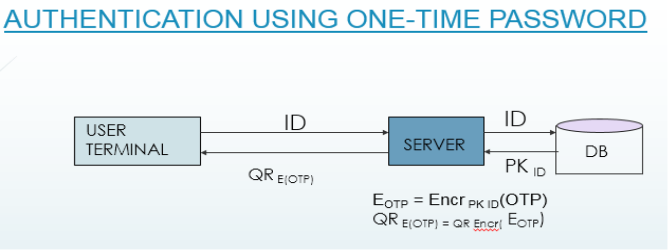
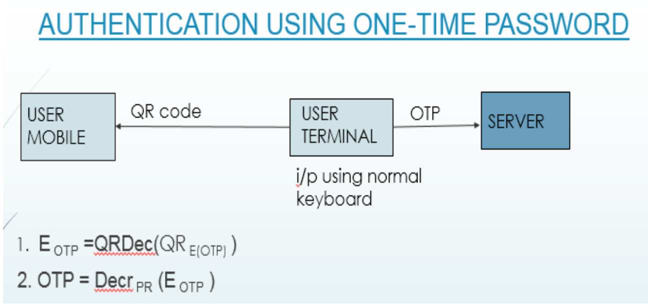

AUTHENTICATION USING ONE-TIME PASSWORD
USER TERMINAL
ID
SERVER
ID
DB
QR E(OTP)
PK ID
E_{OTP} = Encr $_{PK\ ID}$(OTP)
QR $_{E(OTP)\ =\ QR\ Encr(}$ E_{OTP})

Figure 1 (a): Authentication using OTP- QR code generation

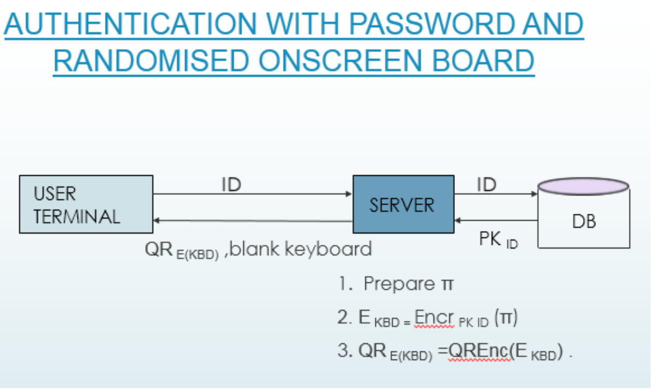
- ID -user-id of the customer.
- PK $_{ID}$ - the public key of the customer.
- Encr $_{PK\ ID}$ (OTP) – Encryption of OTP using public key (PK $_{ID}$) of user. (RSA)
- QR $_{Encr}$ (E_{OTP}) – Encoding of encrypted OTP using QR encoding algorithm


AUTHENTICATION USING ONE-TIME PASSWORD

1. E_{OTP} =QRDec($QR_{E(OTP)}$)
2. OTP = $Decr_{PR}$ (E_{OTP})

Figure 1(b): Authentication using OTP- Decoding of QR code and decryption of OTP

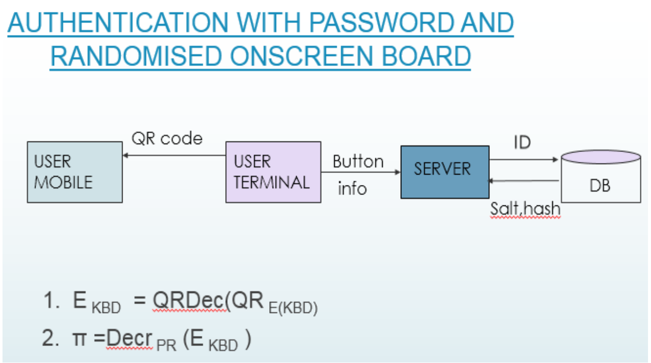
- QR_{Dec} (QR $_{E\ (OTP)}$) – Decoding of QR code using QR decoding algorithm.
- Decr $_{PR}$ (E_{OTP}) – Decryption of E_{OTP} using private key (PR)of user.(RSA)


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 2(a): 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 2(b): Authentication with password and randomized onscreen board- Decoding of QR code and decryption of Π.

3. Proposed Authentication Scheme

Certain drawbacks can be pointed out in [1]:

- The protocols will get compromised if smartphone theft happens or some damage occurs to the phone.
- If an authorized user is an attacker and if he has the secret key and password of the victim then the second protocol is compromised since the attacker can use any smartphone for the attack.
- Attacks due to shoulder surfing are possible.

To avoid the second drawback, a number that uniquely identifies the device could be utilized. The IMEI (International Mobile Station Equipment Identity) number is preferable.

The protocol is implemented in a net banking scenario. For customer authentication only the proposed protocol is implemented. For customers, there will be a 2 phase registration. The initial phase of registration is done by the bank employee during which the basic details of the customer is collected from the customer. When the initial phase is successfully completed a customer-id will be sent to the customer‟s mail-id. Using the customer-id the customer needs to do the second phase of the registration using the smartphone. In the second phase the public-private key pair is generated in the smartphone. The public key is sent to the server. In addition to it the IMEI of the phone will be also sent to the server. The IMEI will be encrypted using the server public key before sending.

3.1 Login process

The login process is as follows:
After the customer has successfully completed the second phase of registration a customer can login into his account.
1) Initially customer needs to provide the customer-id.
2) On the basis of the customer-id the public key as well as the IMEI is retrieved from database.
3) Permutation 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 of the smartphone 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 will be displayed along with the blank keyboard on the screen.
7) The customer now uses his/her smartphone to decode the QR code displayed on the screen.
8) Initial decryption is done using the server public key that is present in the smartphone. After initial decryption we will get the IMEI and the encrypted keyboard. At this stage, the decrypted IMEI is checked with the IMEI dynamically retrieved from the phone the customer is using.
9) If both are same then the keyboard will be decrypted using the private key of the customer.
10) Else the authentication fails.
11) The customer needs to click on the buttons on the screen by looking on the keyboard displayed on the phone‟s screen. On the phone all characters will be displayed whereas on the terminal only blank keyboard will be displayed.

12) Passwords are not stored in database whereas the hash of the concatenation of password and a random string or salt is stored in the database.
13) So during authentication, the hash value and the salt is retrieved from the database. The salt is concatenated again with the password received from the customer and the hash value of it is taken if this hash value and the retrieved hash is the same then the user is directed to his/her homepage.

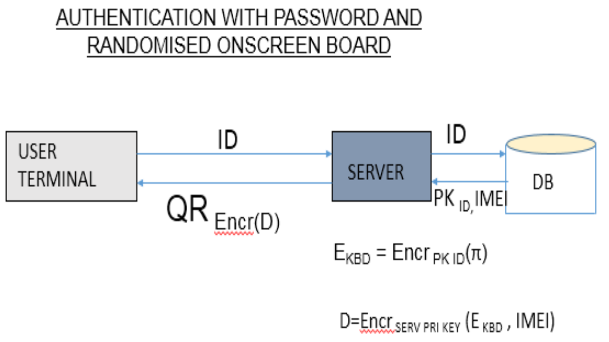
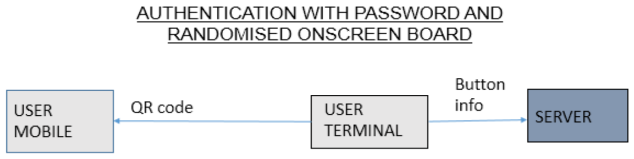

AUTHENTICATION WITH PASSWORD AND
RANDOMISED ONSCREEN BOARD
USER TERMINAL
ID
SERVER
ID
DB
QR Encr(D)
PK ID, IMEI
E_KBD = Encr PK ID(π)
D=Encr SERV PRI KEY (E KBD , IMEI)

Figure 3(a): 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, E $_{KBD}$ =Dec $_{SERV\ PUB\ KEY}$ (D)
3. IMEI retrieved from mobile and decrypted IMEI is checked. if they are matching then π = Decr $_{PR}$ (E $_{KBD}$).

Figure 3(b): Authentication with password and randomized onscreen board- Decoding of QR code and decryption of Π.

4. Results and Simulation

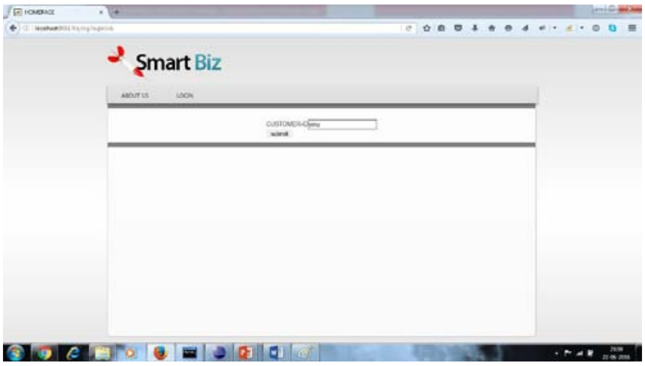


Figure 4: Login page of customer-Customer entering Customer-id

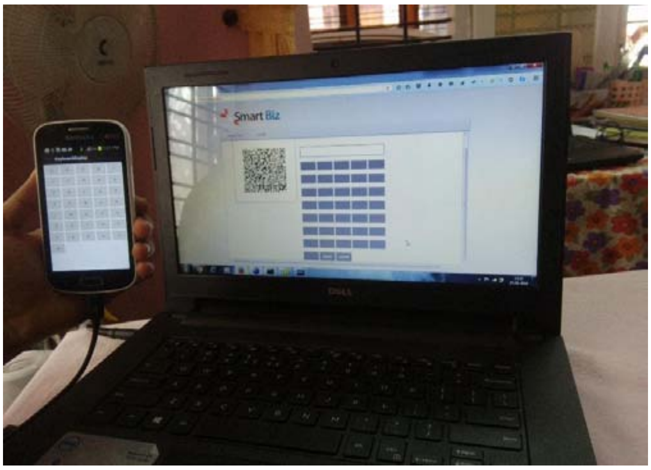


Figure 5:.Customer scanning the QR code using smartphone and keyboard displayed on smartphone

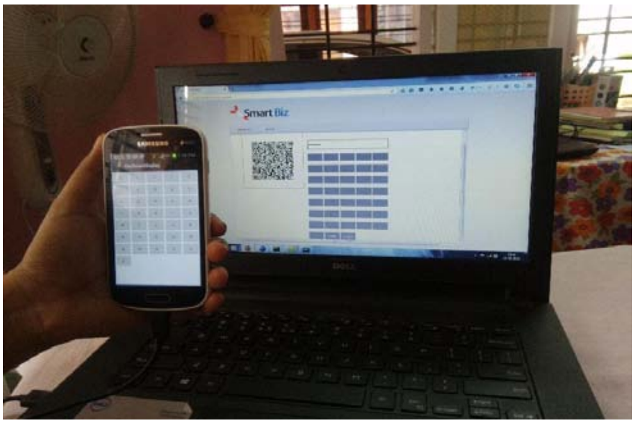


Figure 6: Customer inputs the password by clicking buttons on the screen

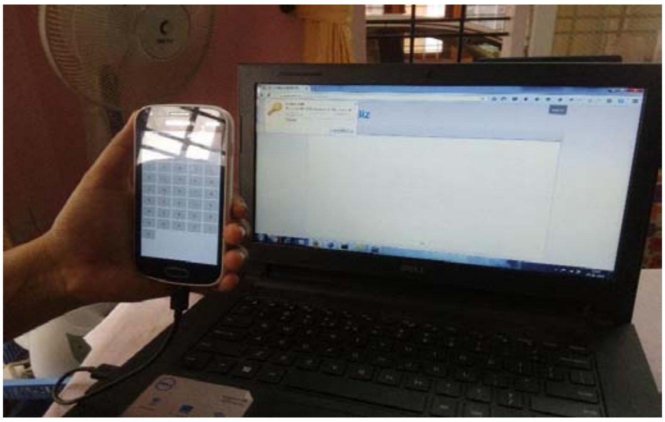


Figure 7: Customer is directed to homepage

The protocol has eliminated the attack stated in 2nd drawback with IMEI effectively.

5. Conclusion and Future works

There exist a possibility of shoulder-surfing attack. It is while authentication when a user is using the smartphone to click on the buttons on the screen an attacker can view the process from behind of the customer.

References

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

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

[3] 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

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

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