ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Resisting Key logger Attacks Using Visual Channel

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

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

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

ABSTRACT: Key loggers are surveillance software designed to capture user's keyboard strokes.They pose a threat while authentication as they can capture credentials from the target computers through covert installation. To avoid key logger attacks, virtual on-screen keyboards with random keyboard arrangement are used. Unfortunately the key logger has control over the entire Personal Computer (PC) and can capture every event and read the video buffer. An innovative authentication scheme is designed using visual channel known as password based authentication protocol. QR code is used to achieve high security.

KEYWORDS: QR code; Password based authentication; smartphone; IMEI

I. INTRODUCTION

The use of passwords for user authentication has become common in our life. Despite having been used for many years, textual passwords remain as the important credential for authentication due to its convenience and simplicity. However many attacks such as spyware and phishing attacks have been used to extract sensitive information from computers resulting in password theft becoming a common occurrence. Spyware is reportedly one among the greatest threats to enterprise security [7].

Key loggers have become a serious problem as they are largely undetectable by most anti-virus software [7].They share the system resources with legitimate programs and stay on the system invisibly as long as required and do their task without attracting the attention of users. Although the main purpose of key logger is to monitor a user's keyboard actions, they now have capabilities that extend beyond that functionality. They can track virtually anything on a computer. Some key loggers are known as screen scrapers which are capable of taking periodic snapshots of the screen. These images may contain valuable information of user. Even though key loggers have some legitimate uses, the functionality of key loggers like concealment, data gathering, reporting etc. make them a favourite tool of hackers.

A key logger attack is similar to shoulder-surfing attack as key logger sees user's keyboard strokes. To prevent shoulder surfing attack, many graphical password schemes have been introduced [6]. But this isn't usable like textual passwords. 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 terminal [1]. The intermediate device used is a smartphone with camera. Quick Response codes (QR codes) are used to store plain and encrypted contents alike. QR codes can be scanned using the smartphone.

II. RELATED WORK

In [1] authors have introduced two visual authentication protocols that resist key logging attacks. They have proposed the concept of an intermediate device between humans and terminal. A smartphone is used as the intermediate device. Using the smartphone the QR code is scanned, which is displayed on the user's terminal. The QR code carries encrypted information. In [3]authors have introduced an approach called Seeing is Believing (SiB) in which a device uses its camera to take a snapshot of a barcode encoding cryptographic material identifying public key of the device. This is termed as visual channel. They also use 2D barcodes to resist man-in-the middle attack in device pairing. In [1] the two visual authentication protocols i.e. authentication using One Time Password (OTP) and authentication using password and randomized onscreen keyboard use 2D barcodes to represent encrypted information and the visual channel to communicate this information.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The encryption is done using RSA encryption algorithm. In the first protocol the QR code contains encrypted OTP and the other has encrypted permutation of keyboard. The QR code is decoded with the smartphone using QR code scanner. The decryption is also 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 for authentication. In the second protocol the permutation of keyboard is displayedlooking at which the user needs to click on the keys of the blank keyboard displayed on the terminal screen.

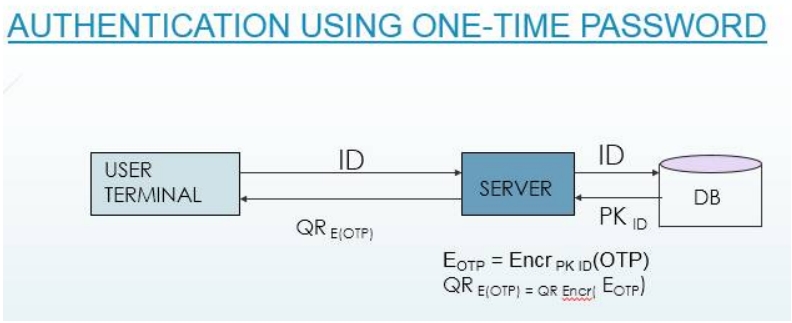

Fig 1. Authentication using OTP- QR code generation

- 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

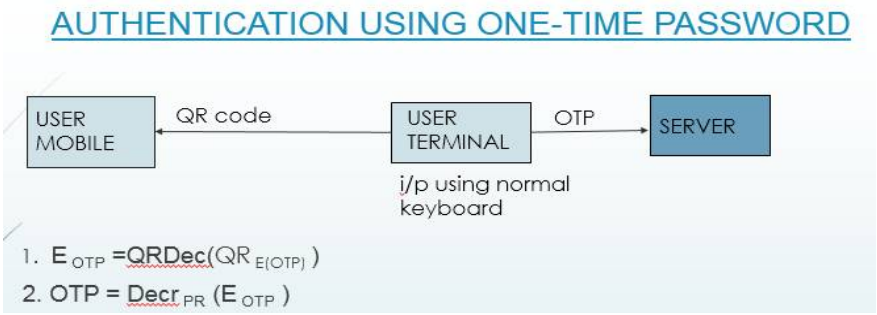

Fig. 2 Authentication using OTP- Decoding of QR code and decryption of OTP

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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

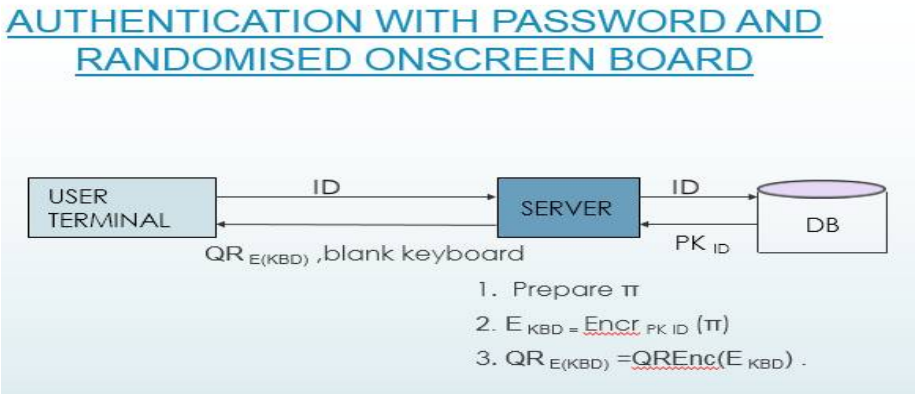

Fig. 3 Authentication with password and randomized onscreen board- QR code generation

- 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

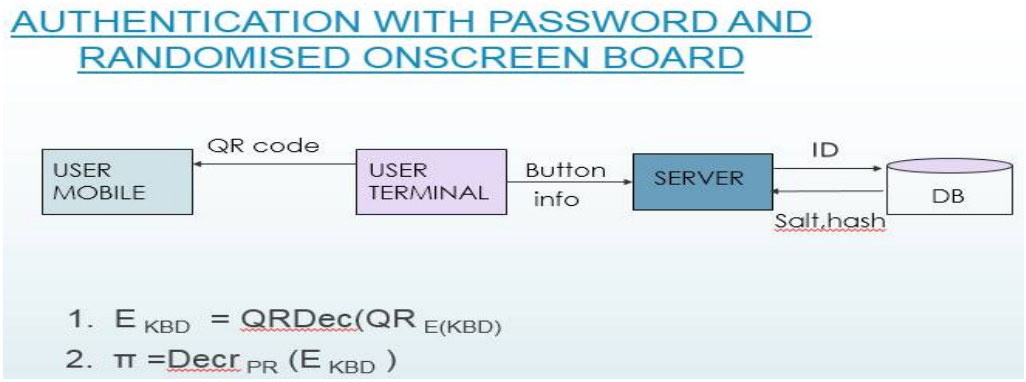

Fig 4.Authentication with password and randomized onscreen board- Decoding of QR code and decryption of Π.

- 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 [1] there are some drawbacks:

- The protocols will fail if smartphone theft happens or some damage occurs to the phone.
- If an attacker is an authorized user 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 eliminate the second drawback, a number that uniquely identifies the device could be utilized.The IMEI (International Mobile Station Equipment Identity) numbercould be used preferably. It is usually found printed inside

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

the battery compartment of the phone.The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network.

The protocol is illustrated with an online banking scenario. Initially there will be registration phase in which the employee of a bank register the customer's basic details and sends the customer id to customer's email. The customer using the customer-id register in the smartphone app. Private-public key pair generation occurs and public key is sent to server. At the end of registration phase the IMEI will be retrieved from the smartphone. The hash value of IMEI, which is encrypted using server public key is sent to the server.

1. When a customer tries to login in, he/she needs to provide the customer-id.
2. Based on the customer-id the public key as well as the hash of IMEI is retrieved from database. Permutation of a 36 character (0-9, a-z) keyboard is generated.
3. To encrypt the permutation we prepare a 128 bit key using the hash of IMEI and a random string. Hash of IMEI is concatenated with the random string. AES is used for encryption.
4. The random string is encrypted using the public key of the customer using RSA algorithm.
5. QR code is generated which consists of the two encrypted entities.
6. The terminal will display the QR code along with a blank keyboard.
7. The user using the smartphone decodes the QR code. After decoding we get the two encrypted entities.
8. The random string should be decrypted first using the private key of user present in the smartphone.
9. The IMEI should be retrieved from the phone which the customer is using currently. The hash of it is computed and concatenated with the random string. Using this key the encrypted permutation should be decrypted. If the attacker is trying to login from his phone he won't be able to see the permutation as the key formed will not be correct.
10. After decryption the permutation is displayed on the smartphone screen.
11. Looking at the keyboard on the phone the user needs to click on the keys of the blank keyboard to input the password.
12. The password is not stored in the database as such. The password is concatenated with a salt value and hash of it is taken. The salt value and the hash value is stored in the database.
13. To validate the user, the password input by the user is concatenated with the salt value retrieved from the database and hash value of it is taken. This hash is compared with the hash value stored in the database.
    If they are equal the user is directed to homepage.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

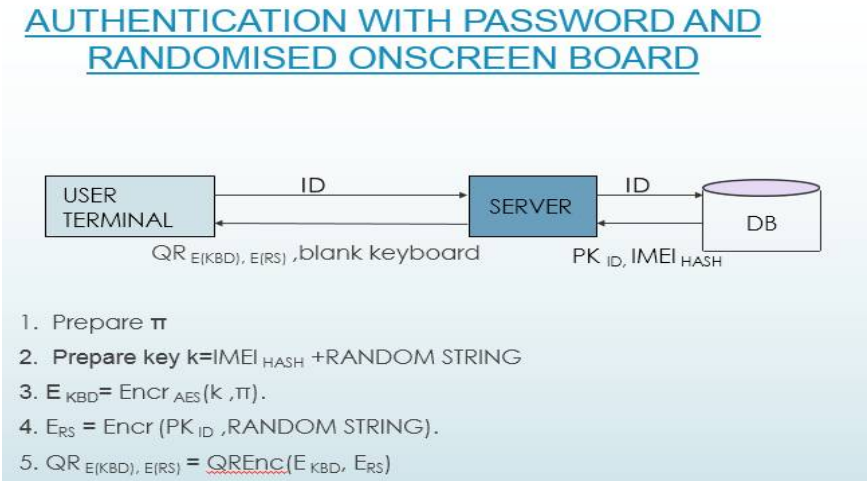

Fig.5 Modified password based authentication protocol-QR code generation

- k- Key used for encrypting permutation using AES algorithm.
- $IMEI_{HASH}$ – hash of IMEI
- $Encr_{AES}$ (k, Π)-Encrypting Π with k using AES.
- Encr(PK_{ID}, RANDOM STRING)-Encrypting RANDOM STRING using public key PK_{ID}. (RSA)
- QREnc(E_{KBD}, E_{RS})-Encoding of encrypted permutation and random string using QR encoding algorithm

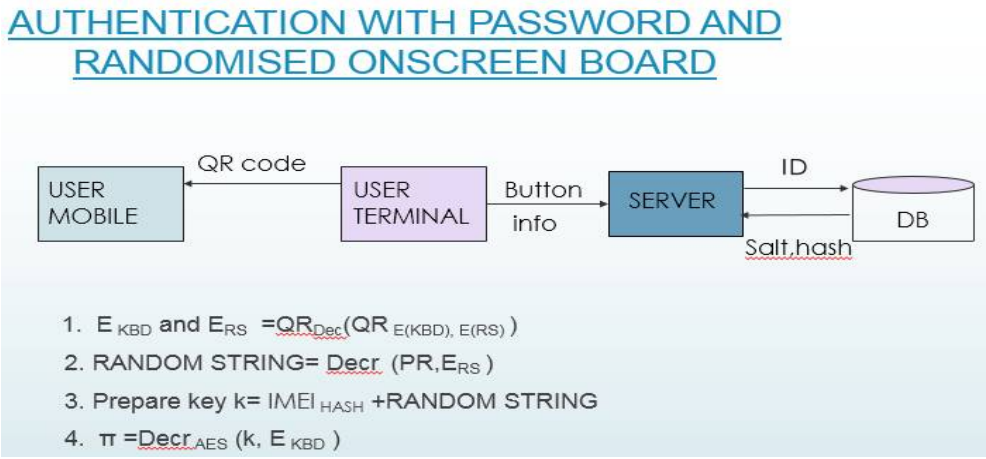

Fig 6. Modified password based authentication protocol-QR code decoding and decryption of Permutation

- QR_{Dec}($QR_{E(KBD), E(RS)}$)-Decoding of QR code using QR decoding algorithm
- Decr(PR,E_{RS})- Decryption of encrypted random string using private key(PR) of the user.(RSA)
- $Decr_{AES}$ (k,E_{KBD})-Decryption of encrypted permutation with the key k using AES algorithm.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. RESULTS AND SIMULATION

The application domain chosen to implement the proposed protocol is net banking. For customer login only the proposed protocol is implemented.

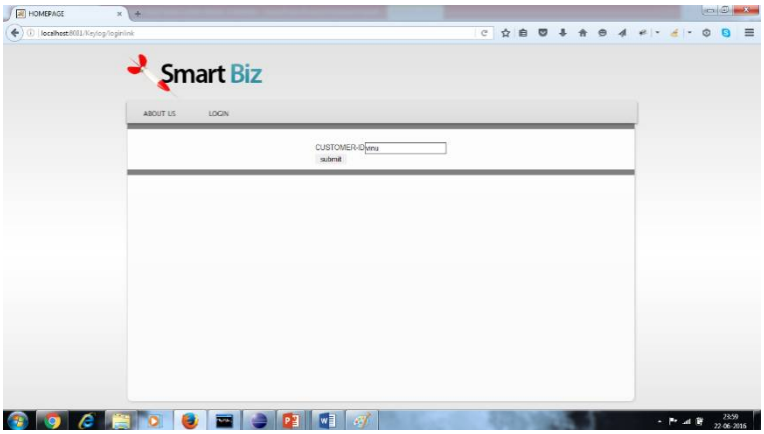

Fig 7. Login page of customer-Customer entering customer-id

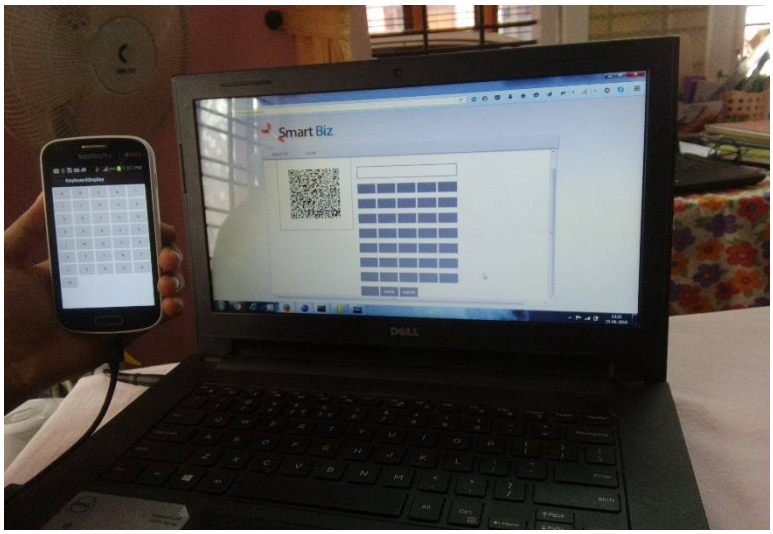

Fig 8.Customer scanning the QR code using smartphone and keyboard displayed on smartphone

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

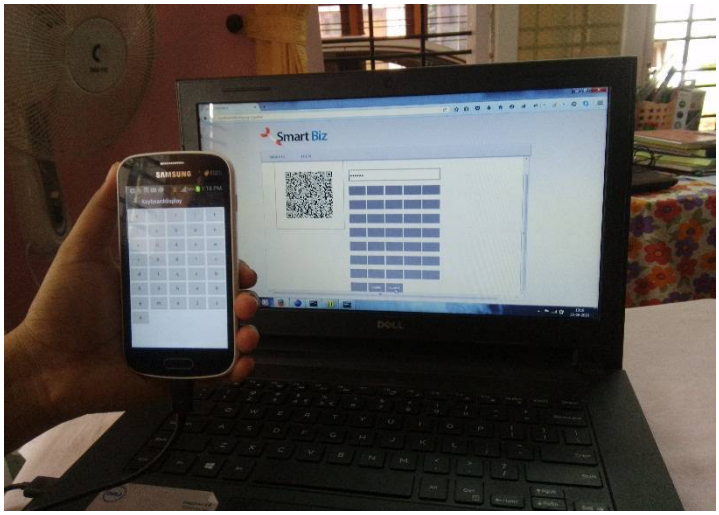

Fig 9. Customer inputs the password by clicking buttons on the screen.

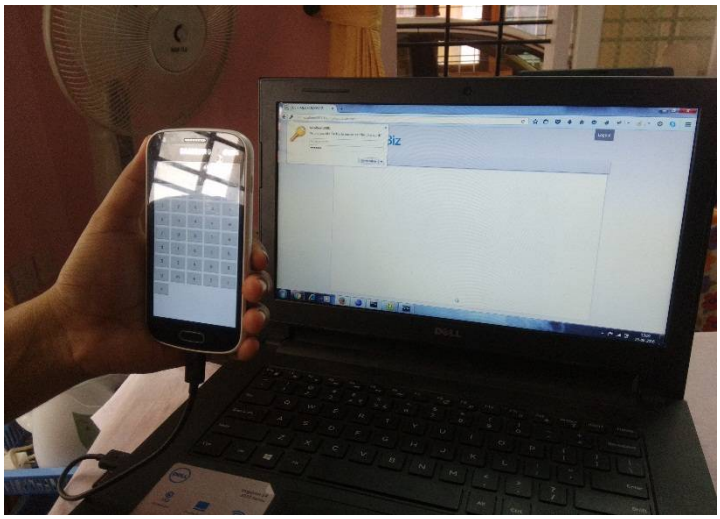

Fig.10.Customer is directed to homepage

The authentication protocol has effectively eliminated the attack stated in2nd drawback with IMEI. Here hash of IMEI along with random string is used to make a key which is required for encryption. The random string has ensured that the key is different each time for encryption. If IMEI is used just as a feature to be checked before decrypting the permutation i.e. the QR code contains the IMEI and the permutation encrypted with public key of user then IMEI shouldn't be sent in plain form as there is a possibility that IMEI could be captured by the attacker through a shoulder surfing attack and a phone with same IMEI could be made. This will again lead to a failure of protocol. But this possibility is also eliminated in the proposed authentication.

V. CONCLUSION AND FUTURE WORK

The results show that the proposed authentication scheme performs much better with the existing scheme. There is a possibility of shoulder surfing attack while the user is clicking on the keys of the blank keyboard on the screen. The

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

attacker can identify which key is being clicked on the blank keyboard by looking at both smartphone display and terminal screen simultaneously. Even though such an attack is difficult there is a possibility.

REFERENCES

1. DaeHunNyang, 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. RamaraoPemmaraju, "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. SerefSagirogluand GurolCanbek, "Key loggers –Increasing threats to Computer Society and Privacy"IEEE TECHNOLOGY AND SOCIETY MAGAZINE | FALL 2009.