ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

QR CODE BASED ENCRYPTED MATRIX REPRESENTATION FOR ERADICATING HARDWARE AND SOFTWARE KEYLOGGING

R.Sangeetha, N.Harsha Vinodha, A.V.Kalpana
Computer Science and Engineering,Velammal Institute of Technology, Tamilnadu, India.

ABSTRACT

The design of secure authentication protocols is quite challenging. Involving human authentication protocols is not easy because of their limited capability of computation and memorization. Keylogging is a major problem faced in internet banking. Keylogger is a software designed to capture all a users keyboard strokes and then make use of them to impersonate a user in financial transaction, also relying on users to enhance security necessary degrades the usability. In order to enhance security as well as usability here we use RSA algorithm which avoid some problems in e-banking such as session hijacking , monitoring using video sensor etc. By providing unique key to the users after scanning the QR code available in screen. According to the unique key,the user will be given a specific 4*4 matrix keyboard in user's smart phone which reposition the keys every time inorder to avoid hacking. To that end, there are two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. Through rigorous analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature.

KEYWORDS: Keylogger, Smartphone, QR code, Authentication, Malicious code

1. INTRODUCTION

Threats against electronic and financial services can be classified into two major classes: credential stealing and channel breaking attacks. Credential stealing is nothing but username , password and pin number can be stolen by the attacker if they are poorly managed. Channel breaking attacks is nothing but eavesdropping on communication between users and a financial institution. Keylogging attack, session hijacking, phishing and pharming are some of the attacks. A keylogger is a software designed to capture all the activities of the user when they are typing something in the keyboard. For example whenever the user types her password in the bank website, the keylogger intercepts the password. To mitigate the keylogger attack, virtual or onscreen key- boards with random keyboard arrangements are widely used in practice. Both techniques, by rearranging alphabets randomly on the buttons, can frustrate simple keyloggers. Unfortunately, the keylogger, which has control over the entire PC, can easily capture every event and read the video buffer to create a mapping between the clicks and the new alphabet. Keylogging is the major problem in e-banking. Keylogger is a software designed to capture all a user's keyboard strokes, and then make use of them to impersonate a user in financial transaction.Two virtual authentication protocols(OTP) One Time Password and password based authentication is used to transfer the fund/amount in another account. In this system ,e-banking virtual keyboard is used in which allows the other persons to hack the password , hijack the session id etc. Each and every time , randomized OTP is generated and encrypted then form the QR code . User will scan the QR code . The QR code is decrypted using his private key , then OTP is displayed on mobile phone.User views a randomized(0 to 9) number placed in different places in 4 * 4 matrix in his phone. Then user click the password in plain keyboard using mouse. Safeslinger is the first complete system that provides privacy-preserving and secure group credential

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

exchange without any external trusted parties, restricting the exchanged information to other group members only. Safeslinger is also the first secure group credential exchange system that can be used remotely over a telephone or video conferencing line[12]. Use graphical password instead of text based password so that the user can easily remember their graphical password. Using this shoulder surfing attacks can be reduced[11]. Malware detection and analysis is a challenging task, and current malware analysis and detection techniques often fall short and fail to detect many new, unknown malware samples. In order to avoid that ,they proposed panorama detect and analyze malware by capturing this fundamental trait. User personal information will be hacked[9]. When the roaming users who use untrusted machines to access password protected accounts have few good options. An internet cafe machine can easily be running keylogger. The roaming user has no reliable way of determining whether it is safe, and has no alternative to typing the password[10].

2. SCOPE AND CONTRIBUTION

In this paper, we demonstrate how visualization can enhance not only security but also usability by proposing two visual authentication protocols: one for password- based authentication, and the other for one-time-password (OTP). The original contributions this paper are Two protocols for authentication that utilize visuali- zation by means of augmented reality to provide both high security and high usability. We show that these protocols are secure under several real-world attacks including keyloggers. Both protocols offer advantages due to visualization both in terms of security and usability.

3. ALGORITHM

In this section, we describe two protocols for user authenti- cation with visualization. Before getting into the details of these protocols, we review the notations for algorithms used in our protocols as building blocks. Our system utilizes the following RSA algorithms:

- $Encr_K$- An encryption algorithm which takes a key k and a message M from set $\mathcal{M}$ and outputs a cipher- text C in the set $\mathcal{C}$.
- $Decr_K$- A decryption algorithm which takes a ciphertext C in $\mathcal{C}$ and a key k, and outputs a plaintext (or message) M in the set $\mathcal{M}$.
- Sign - A signature generation algorithm which takes a private key SK and a message M from the set $\mathcal{M}$, and outputs a signature s.
- Verf - A signature verification algorithm which takes a public key PK and a signed message ðM; sÞ, and returns valid or invalid.
- QREnc - A QR encoding algorithm which takes a string S in S and outputs a QR code.
- QRDec - A QR decoding algorithm which takes a QR code and returns a string S in S.

In this algorithm, we used two keys which public keys and private keys. Public keys can be accessed by anyone. Private keys is only for the authorised users.Steps followed in this algorithm are

Step: 1. Choose two very large random prime integers: p and q

Step: 2. Compute n and φ(n)(TOTIENT): n = pq and φ(n) = (p-1)(q-1)

N=Modulus of public and private key
Step: 3. Choose an integer e, 1 < e < φ(n) such that: gcd(e, φ(n)) = 1(where gcd means greatest common denominator)

Step: 4. Compute d, 1 < d < φ(n) such that: ed ≡ 1 (mod φ(n))

- the public key is (n, e) and the private key is (n, d)
- the values of p, q and φ(n) are private
- e is the public or encryption exponent
- d is the private or decryption exponent.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Encryption

The cipher text C is found by the equation 'C = M^e mod n' where M is the original message.

Decryption

The message M can be found form the cipher text C by the equation 'M = C^d mod n'.

4. WORKING OF PROTOCOLS

1. The user connects to the server and sends her ID.

2. The server checks the ID to retrieve the user's public key (PK_{ID}) from the database. The server then picks a fresh random string OTP and encrypts it with the public key to obtain E_{OTP} ¼ $Encr_{PK_{ID}}$ ðOTPÞ.

3. In the terminal, a QR code $QR_{E_{OTP}}$ is displayed prompting the user to type in the string.

4. The user decodes the QR code with E_{OTP} ¼ $QRDecð QR_{E_{OTP}} Þ$. Because the random string is encrypted with user's public key (PK_{ID}), the user can read the OTP string only through her smartphone by OTP ¼ $Decr_k$ ðE OTP Þ and type in the OTP in the ter- minal with a physical keyboard.

5. The server checks the result and if it matches what the server has sent earlier, the user is authenticated. Otherwise, the user is denied.

5. ARCHITECTURE DIAGRAM

The overall architecture diagram says that the user is creating a account in the bank. Retail login is nothing but user's own login. Log into retail login, here deposit and enquiry option will be there. User can apply net banking for their own account. After applying net banking , user will entered into the net banking login, it will ask user-id and password and after entered all those details, the paper contain QR code and plain keyboard. Scan the QR code using mobile phone and select decrypt option , it will display private key user has to type that private key in the mobile phone and then OTP keyboard will be displayed in user mobile phone. User will type their transaction number using that keyboard which contain number in the mobile phone.

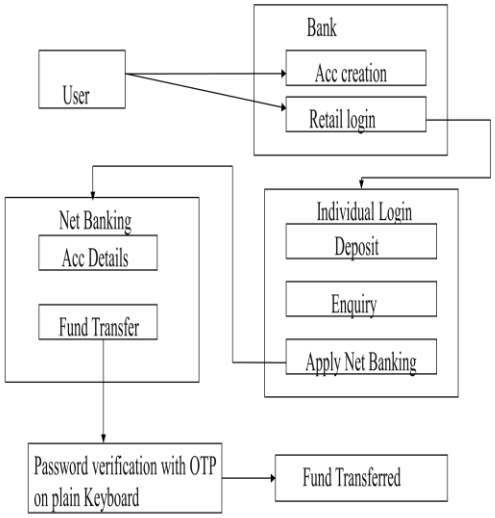


Fig 1 Architecture Diagram

6. IMPLEMENTATION AND USER STUDY

In this section, we describe the details of the prototype implementations and show the results of the user study for protocol 2 using numeric keyboard.The numeric keyboard study was to know the speed and the error of the PIN entry.

6.1 Numeric Keyboard with Blank Space

We implemented protocol to see its usability for PIN, which is widely accepted for authenticating a person during banking transactions.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

(a) QR Code Scanning (before) (b) QR Code Scanning (after) (c) Keyboard on Terminal

(d) Keyboard on Smartphone

Fig. 2. Photographs of the prototype we have developed to demonstrate our authentication protocols. (a) and (b) show the moments of a QR code scanning of a keyboard layout. (c) shows the blank keyboard shown at the terminal (on LCD screen). (d) shows the decoded randomized layout of the keyboard obtained from the QR code after decryption as viewed on smartphone. Note that the yellow square on which the mouse cursor is hover- ing in the terminal is shown through the smartphone to assist user's input.

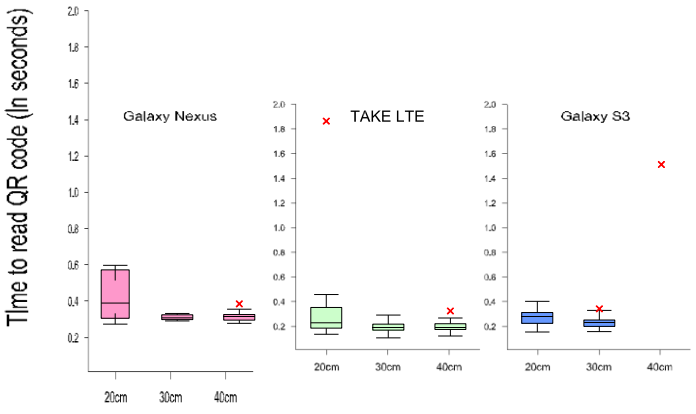
First we need to scan the QR code and after scanning private key will be generated for authorized user. Otherwise encrypted text will be displayed for unauthorized user. Type the private key in the mobile phone and then 4 * 4 matrix table will be displayed with numbers. In the system we have only plain keyboard, we have to enter password using that numeric keyboard which is there in the mobile phone.

Fig 3 High-level description of an authentication protocol with password and a randomized onscreen blank keyboard.

```
user::user.send(server, id)
server::__upon_id_arrival:
    if(server.verify(id) == true):
        pkid = server.db.find(id)
        pi = server.generate_random_kb()
        ekbd = server.encrypt(pkid, pi)
        qrekbd = server.qrencode(ekbd)
        server.send(user, qrekbd)
terminal::__upon_qrekbd_arrival:
    terminal.view(qrekbd)
    terminal.view_blank_kb(pi)
smartphone::__upon_qrekbd_view:
    qrekbd = smartphone.capture(qrekbd)
    ekbd = smartphone.qrdecode(qrekbd)
    pi = smartphone.decrypt(skid, ekbd)
    smartphone.view(pi)
user::__upon_pi_view:
    pw = user.inputpassword(terminal)
terminal::upon_pw_input:
    terminal.send(server, pw)
server::__upon_pw_arrival:
    if(server.verify(id, pw) == true):
        server.authenticate(user)
    else
```

6.2 Hardware Performance

To understand how smartphones can read QR codes, we measured the time taken to read QR codes by different distances from an LCD monitor. We performed experiments on Samsung galaxy.



(a) times to read QR codes

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Fig. 4. Time to read QR codes of three different smartphones by different distances from a smartphone to an LCD monitor. (a) shows the box plots with 1:5 IQR whiske

7. ENHANCEMENT

We proposed two enhancement that is offline transaction and IMEI security. Mostly transactions are done through online only . But for time consuming and quick transaction we proposed offline transaction. Details are entered by user when they are in offline . when user entered into online , they just load this file into the applications for fund transaction. Another enhancement is IMEI security . The main purpose of this is , to avoid malicious transaction. When other user knows my username and password means , they can use my details for fund transfer without my knowledge . To avoid this we are providing IMEI security. Every user registration server store their IMEI number into their database . Another malicious user , use my username and password in their mobiles means IMEI number vary so proper transaction will not occur.

8. RELATED WORK

There has been a large body of work on the problem of user authentication in general [3], [4], [5], [6], [8], and in the context of e-banking. Inorder to reduce those attacks we have related techniques. To the best of our knowledge, our protocols are the first of their type to use visualization for improving security and usability of authentication protocols as per the way reported in this paper. Our protocols are tailored to the problem settings in hand, e- banking, with a different trust and attack model than that used in [16]—which results into different guarantees as explained earlier in this paper. To prevent against phishing, we suggested the use of trusted devices to perform mutual authentication and eliminate reliance on perfect user behavior [7]. In this paper we have shown that our protocols are secure even when one of the participants in the authentication process (the terminal or smartphone) is compromised.

9. CONCLUSION

In this paper, we proposed and analyzed the use of user- driven visualization to improve security and user-friend- liness of authentication protocols. Moreover, we have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Our protocols utilize simple technologies available in most out-of-the- box smartphone devices. We developed Android applica- tion of a prototype of our protocol and demonstrate its feasibility and potential in real-world deployment and operational settings for user authentication. We are providing security and it is also user friendly even the uneducated people can easily understand.

REFERENCES

[1] Google Authenticator, http://code.google.com/p/google-authenticator/, 2014.

[2] H. Moon, H. Lee, J. Lee, K. Kim, Y. Paek, and B.B. Kang, "Vigilare: Toward Snoop-Based Kernel Integrity Monitor," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 28-37, 2012.

[3] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hash- ing for Message Authentication," RFC 2104, http://www.ietf. org/rfc/rfc2104.txt, 1997.

[4] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772,1981.

[5] M. Naor and B. Pinkas, "Visual Authentication and Identi- fication," Proc. Advances in Cryptology (CRYPTO), 1997.

[6] D. Otway and O. Rees, "Efficient and Timely Mutual Authentication," ACM SIGOPS Operating Systems Rev., vol. 21, no. 1, pp. 8-10, 1987.

[7] B. Parno, C. Kuo, and A. Perrig, "Phoolproof Phishing Pre- vention," Proc. Financial Cryptography, pp. 1-19, 2006.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

[8] J. Steiner, C. Neuman, and J. Schiller, "Kerberos: An Authentica- tion Service for Open Networks," Proc. USENIX Ann. Technical Conf, pp. 191-201, 1988.

[9] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing System-Wide Information Flow for Malware Detection and Analysis," Proc. ACM Conf. Computer and Comm. Security (CCS), 2007.

[10] C. Herley and D. Florencio, "How to Login from an Internet Caf e without Worrying about Keyloggers," Proc. ACM Symp. Usable Privacy and Security (SOUPS), 2006.

[11] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. 12th European Symp. Research in Computer Security (ESORICS), 2008.

[12] M. Farb, M. Burman, G. Chandok, and J. McCune, "A. Perrig, "SafeSlinger: An Easy-to-Use and Secure Approach for Human Trust Establishment," Technical Report CMU-CyLab-11-021, Car-negie Mellon Univ., 2011.

[13] Q. Yan, J. Han, Y. Li, J. Zhou, and R.H. Deng, "Designing Leakage- Resilient Password Entry on Touchscreen Mobile Devices," Proc. Eighth ACM SIGSAC Symp. Information, Computer and Comm. Secu- rity (ASIACCS), pp. 37-48, 2013.

[14] D. MRaihi, S. Machani, M. Pei, and J.Rydell, "TOTP: Time-Based One-Time Password Algorithm," RFC 6238, http://www.ietf. org/rfc/rfc6238.txt, 2011.

[15] T. Holz, M. Engelberth, and F. Freiling, "Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones," Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 1-18, 2009.

[16] J.M. McCune, A. Perrig, and M.K. Reiter, "Seeing-is-Believing: Using Camera Phones for Human-Verifiable Authentication," Proc. IEEE Symp. Security and Privacy, pp. 110-124, 2005.