International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Secure Authentication Using 2 Level Security

Mohankumar Vadlamudi [1]& Ms. V Lakshmi Chetana[2]
[1]PG Scholar,Dept of MCA ,MIC College of Technology, Krishna Dist, A.P. India
[2]Assistant Professor,Dept of MCA, MIC College of Technology, Krishna Dist, A.P. India

ABSTRACT:
Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer.Due to unavoidable hacking of the database on the internet. To solve this problem of authentication, we are proposing an algorithm based on image processing. The goals and objectives of this application which are to be achieved are as follows: Initially client needs to be registered and registered details saved in the database. While registering client, the client wants to upload image from the database or local system. During the register the client submitted image was segmented into two shares (shares means part of the image) and each share is encrypted. The encrypted two shares are one encrypted share is saved in database and another share is send to the mail during the registration the client given mail address. During the login form the client enters user name, password and upload encrypted share which was send to the user given mail address on registration form. After successfully login the client perform his transactions, after transactions he will logout. Visual Cryptography is a special encryption system. Total number of shares to be created is depending on the scheme chosen by the bank when two shares are created one is stored in the database and the other is kept by customer. The customer has to present the share during all of his transactions. This share is stacked with the first to get original image Then decoding method is used to take the hidden password on acceptance or rejection n of the output and authenticate the customer. Another mechanism are used for providing the security, methods like generation of OTP and security question are added for extra safety of user's transaction. Finally the user will get extra safety measures so that and illegal hack-in and accessing can be prevented.

Keywords: Key logger; Authentication; Malicious attacks; Android smart phones; Keyboard

I. INTRODUCTION

Keylogging exhibits an extraordinary test to security supervisors. Dissimilar to customary worms and viruses, certain sorts of keyloggers are everything except difficult to discover. Keyloggers are a kind of malware that malignantly track customer information from the comfort attempting to recuperate individual and private information. Growing machine use for essential business and individual activities using the Internet has made feasible treatment of keylogging basic. Cybercriminals have fictional various schedules to get sensitive information from your endpoint devices. On the other hand, few of them are as effective as keystroke logging. Keystroke logging, generally called keylogging, is the hold of imprint characters. The data caught can incorporate report content, passwords, user ID's, and other potentially touchy bits of information. Using this approach, an assailant can get essential data without breaking into a cemented database or file server.A keylogger is modifying, proposed to capture the larger part of a customer's support strokes, and a while later make use of them to copy a customer in money related

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

trades. Case in point, at whatever focuses a customer sorts in her watchword in a bank's sign in box, the keylogger gets the mystery word.

The risk of such keyloggers is pervasive and can be display both in PCs and open corners; there are constantly circumstances where it is imperative to perform monetary trades using an open machine regardless of the way that the best concern is that a customer's watchword is prone to be stolen in these machines. Far and away more terrible, keyloggers, frequently root kitted, are tricky to identify since they won't appear in the assignment director methodology list. To relieve the keylogger attack, virtual or onscreen consoles with random console game plans are generally utilized as a part of practice. Both procedures, by revising letter sets randomly on the catches, can baffle basic keyloggers. Lamentably, the keylogger, which has control over the entire PC, can without much of a stretch capture each occasion and read the video buffer to make a mapping between the clicks and the new letter set. An alternate moderation procedure is to utilize the console snaring counteractive action strategy by bothering the console interferes with vector table.

On the other hand, this strategy is not general and can interfere with the working framework and local drivers. It is insufficient to depend just on cryptographic strategies to counteract attacks which mean to swindle clients' visual experience while living in a PC. Regardless of the fact that all vital data is safely conveyed to a client's machine, the attacker living on that client's machine can without much of a stretch watch and change the data and show legitimate looking yet misleading data. Human client's contribution in the security convention is off and on again important to keep this sort of attacks however people are bad at muddled estimations and don't have a sufficient memory to recall cryptographically solid keys and marks. Accordingly, ease of use is a critical variable in outlining a human-including convention. Our methodology to taking care of the issue is to present a transitional gadget that extensions a human client and a terminal. At that point, rather than the client straightforwardly conjuring the general confirmation convention, she conjures a more complex yet easy to use convention by means of the moderate helping gadget. Each association between the client and a middle of the road helping gadget is envisioned utilizing a Quick Response (QR) code.

The main contributions of this paper are as follows:

- Two protocols for authentication that uses visualization by method for increased reality to give both high security and high convenience. We demonstrate that these conventions are secure under a few certifiable attacks including keyloggers. Both conventions offer favorable circumstances because of visualization both as far as security and ease of use.
- Model usage as Android applications which show the ease of use of our conventions in true organization settings

II. EXISTING SYSTEMS

A. Existing System Whenever a user types in her password in a bank’s sign in box, the keylogger intercepts the password. The threat of such keyloggers is pervasive and can be present both in personal computers and public kiosks; there are always cases where it is necessary to perform financial transactions using a public computer although the biggest concern is that a user’s password is likely to be stolen in these computers. Even worse, keyloggers, often root kitted, are hard to detect since they will not show up in the task manager process list.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Our approach to solving the problem is to introduce an intermediate device that bridges a human user and a terminal. Then, instead of the user directly invoking the regular authentication protocol, she invokes a more sophisticated but user-friendly protocol via the intermediate helping device. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code. The goal is to keep user-experience the same as in legacy authentication methods as much as possible, while preventing keylogging attacks.

C. Modules

The system is proposed to have the following modules along with functional requirements.

1. System Model
2. Linear and Matrix Barcodes
3. Message signing
4. Prevention of Session Hijacking with Visual Signature Validation

1.System Model

Our system model consists of four different entities (or participants), which are a user, a Smartphone, a user's terminal, and a server. The user is an ordinary human, limited by human's shortcomings, including limited capabilities of performing complex computations or remembering sophisticated cryptographic credentials, such as crypto-graphically strong keys. With a user's terminal such as a desktop computer or a laptop, the user can log in a server of a financial institution (bank) for financial transactions. Also, the user has a Smartphone, the third system entity, which is equipped with a camera and stores a public key certificate of the server for digital signature verification. Finally, the server is the last system entity, which belongs to the financial institution and performs back-end operations by interacting with the user (terminal or Smartphone) on behalf of the bank.

Fig.1. Three different barcodes encoding the statement "Virtual reality". (a) is a linear barcode (code 128), and (b) and (c) are matrix barcodes (of the QR code standard). While (b) encodes the plain text, (c) encodes an encrypted version using the AES-256 encryption algorithm in the cipher-block chaining (CBC) mode (note this last code requires a password for decryption).

B. Linear and Matrix Barcodes

A barcode is an optical machine-readable drawing of data, and it is widely used in our everyday life cycle meanwhile it is close to all types of goods for identification. In acasing, barcodes are chiefly two kinds:

1) Linear barcodes and
2) Matrix (or two dimensional, also known as 2D) barcodes.

Even though linear barcodes—shown in Figure 1(a)—have a partial capacity, which rest on on the coding method used that can range from 10 to 22 characters, 2D barcodes—shown in Figure 1(b) and Figure 3(c)—have higher capacity, which can be extra than 7000 characters. For instance, the QR code—a widely used 2D barcode—can grip 7,089 numeric, 4,296alphanumeric, or 2,953 binary characters [4], assembly it a identical good high-capacity candidate for packing plain and encoded contents alike.

3. Message signing

For the generality of the purpose of this protocol and the following protocols, and to prevent the

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

terminal from misrepresenting the contents generated by the server, one can establish the authenticity of the server and the contents generated by it by adding the following verification process. When the server sends the random permutation to the user, it signs the permutation using the server's private key and the resulting signature is encoded in a QR code. Before decrypting the contents, the user establishes the authenticity of the contents verifying the signature against the server's public key. Both steps are performed using the Sign and Verf algorithms. Verification is performed by the smart phone to avoid any man-in-the-middle attack by the terminal.

4.Prevention of Session Hijacking with Visual Signature Validation

- A user requests via terminal to the server money transfer denoted as T that describes sender name/account, recipient name/account, a timestamp, and amount of money to transfer.
- The server checks the ID to retrieve the user's public key (PKID) from the database. Then, it picks a fresh OTP to prepare QR = QREnc (EOTP; T; _ = Sign (PrK; T)), where PrK is a signing key of the server. Then, it sends QR to the user to authorize the transaction.
- On the terminal, a QR code QR is displayed prompting the user to type in the OTP string.
- The user decodes the QR code to get (EOTP = QRDec (QREOTP); T; _) with her smart phone application. Here the application verifies the time stamp and the signature by Verf (PubK; T; _) to show the result (Valid/Invalid) on the screen with the decrypted OTP and T. If the application fails to validate the signature, it does not show neither the decrypted OTP nor T, but displays an error message to alert the user. When the user is confirmed with the signature verification result and with T, she inputs the OTP to the terminal, which is sent back to the server.

III Algorithm

3.1 Data Encryption Standard:

The DES system is essentially a loop with 16 iterations, called rounds. There is also an initial permutation ***IP*** which the entire block is subjected to before entering the first round. Similarly, there is an inverse permutation IP^{-1} that is performed on the block after the last round.

Each round breaks the message block into two halves, ***L*** and ***R***, and concentrates on only one half of the message block (say, the right half ***R***). Each round also generates a48 bit sub keyK_i from the original 56-bit key. To do so, it uses a sub key function ***SK***. The round will subject ***R*** to a transformation, which is a function ***F*** of the sub key and ***R***. It then sets the left side ***L*** to XOR of itself and the result of $F(K_i, R)$. Finally, the two halves are swapped so that the other half can be processed in the next round. Below is a blockdiagram of the algorithm, and shows how it is usually represented in terms of hardware.

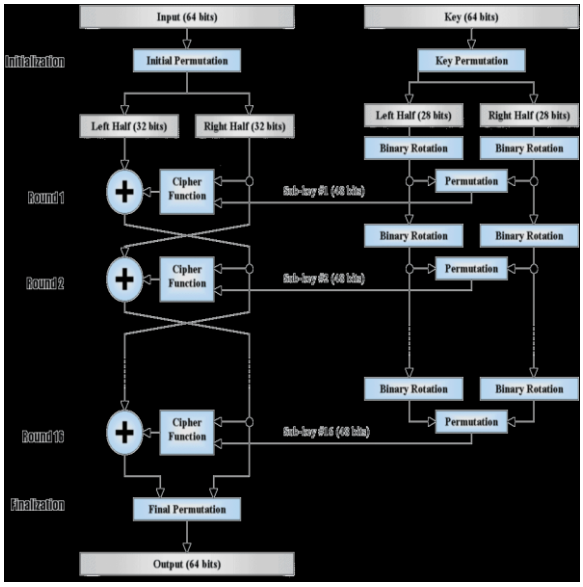

Figure.2 Block diagram of the DES algorithm

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

IV. ENHANCEMENT

We are having 2 modules:

1.Client:

- **Registration:** The user can register with his details like username, password, phone number, email address and address of the user.
- **Upload Image:** In the registration we are uploading image form the database otherwise user can upload image form the local drive and saved into the database.

That upload image segmented into two shares one is send to user email and other one is saved in database.

- **Login:** In login we are giving the username, password and encrypted share with this we can login.
- **Upload Encrypted Share:** In the login form we are having upload encrypted share that encrypted share is taken from the user email address and uploaded into the login page.
- **Transactions:** After login we are performing transaction like create account, check balance and mini statement.
- **Logout:** After performing all transaction the user can be logout

2.Administrator:

- **Admin login:** in admin login form he can login with username and password.
- **Upload images:** here admin can upload images and saved into database.
- **View images:** after uploading images he can view the images which are saved in database.
- **Segmentation and encryption, decryption:** when user upload images from the database the image will be segmented, encrypted and dividing into two shares one is send to the user email and other one is saved in the database. In the login form we are decrypting the two shares.

Authentication: when user upload image in registration form the user uploaded image and encrypted share save in the database ,while client login first encrypted share was uploaded and retrieve second share from database and both shares are decrypted and then both are merged and merged image compare with the original image which is saved in the database if it is valid then the user will be authenticated otherwise invalid image authentication.

V. CONCLUSION

Here we conclude with specifying a two level security for user authentication. The mechanism one time password on a timely basis is proposed. And also another security mechanism like image based security authentication is also proposed. Image based authentication is performed by image segmentation. Image segmentation is secured because of divide and sharing image shared between user and database meanwhile the hacker/intruder may steal shares is no problem because of still some shares are remain at either sides so intruder fails to authentication

VI. REFERENCES

[1] DaeHun Nyang, Member, IEEE, Aziz Mohaisen, Member,IEEE, Jeonil Kang, Member, IEEE, ―Keylogging-resistant Visual Authentication Protocols‖, Transactions on Mobile Computing, Vol. 1, No. 8, August 2014.

[2] Cronto. http://www.cronto.com/.

[3]BS ISO/IEC 18004:2006. Information technology. automatic identification and data capture techniques. ISO/IEC, 2006.

[4] ZXing. http://code.google.com/p/zxing/, 2011

[5] D. Boneh and X. Boyen. Short signatures without random oracles. In Proc. of EUROCRYPT, pages 56–73, 2004.

[6] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web

authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.

[7] J. Brown. Zbar bar code reader, zbar android sdk 0.2. http://zbar. sourceforge.net/, April 2012.

[8] 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.

[9] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In Proc. of ESORICS, 2008.

[10] D. Crock ford. The application/json media type for javascript object notation (json). http://www.ietf.org/rfc/ rfc4627.txt?number=4627, July 2006.

[11] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In Proc. of USENIX Security, 2004.

[12] N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall, 2003.