VOL. 10, NO. 8, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURITY ANALYSIS OF THREE FACTOR AUTHENTICATION SCHEMES FOR BANKING

Albert Mayan J., Sharmila Latha T. and Kislay Kumar Sinha
Department of Computer Science and Engineering, Sathyabama University, Chennai, India
E-Mail: albertmayan@gmail.com

ABSTRACT

Lack and resources in different areas such as Banking, military, government organizations has been increased enormously. The commonly used method to determine the identity of a remote client is two factor authentication and the two factors are user id and password and one time password. This paper investigates generic and secure framework to upgrade two-factor authentication to three-factor authentication. In three factor authentication identity of remote client is determined by three factors, namely MULTIPLE PASSWORDS to the distributed systems, NON-PROGRAMMABLE CARD and BIOMETRIC (face reorganization) along with MMS facility. This conversion not only signifies in the improvement of information assurance at low cost but also protects client privacy in distributed systems.

Keywords: security analysis, RFID, MMS, face recognization, multiple passwords.

1. INTRODUCTION

Two factor authentications is common method used to determine the identity of a remote client and two factors are namely user id and password and one time password and Lamport proposed an authentication scheme to provide authentication between the users and the remote server and the adversary is modeled as follows:

(a) The adversary can intercept the communication channel between the users and the server during the login and authentication phase.
(b) The adversary can get the information by obtaining the smart card or receive a user's password and biometric feature such as finger print, but adversary cannot do both.

In this authentication scheme, not only the server can verify the user but also a user can verify the server even though security of the distributed systems is not improved effectively. So, this paper investigates a systematic approach to upgrade two-factor authentication to three-factor authentication. This conversion not only signifies the information assurance at low cost but also protects client privacy in distributed systems.

In addition, our framework retains several practice-friendly properties of the underlying two-factor authentication like using a common storage device (universal serial bus memory). However, this authentication scheme is vulnerable to attacks namely impersonation attack, middle man attack and replay attack. An attacker could impersonate authorized user to login and access the remote server. So, in three factor authentication we analyze the Fan-Chan-Zhang's security scheme which is not vulnerable to replay attacks and impersonation attacks.

2. SYSTEM MODEL

In this proposed system we are using non-programmable card that is RFID tag and all the bank information is present in the same card. So, Negative of the pin number won't present behind the card and for authenticating this card we should use multiple passwords i.e. (pin number, authentication password and face recognization). If any one of these passwords are wrong then the image of the person who is authorizing the account will be send MMS to the account holder. If he knows that person he will send pin number directly to the bank. Then transaction will be opened for him to do the transaction. If he doesn't know the person then he can send a unique password to the bank by which alarm will be ringing and doors of the ATM closes automatically, information is sent to nearby police station.

a) Block diagram

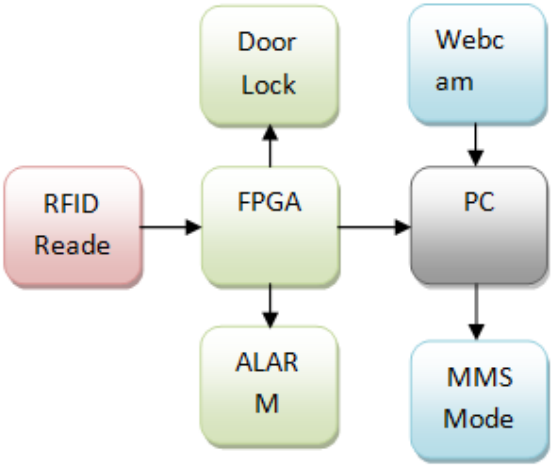

Figure-1. Proposed authentication architecture.

2.1 Non programmable card

Radio frequency identification (RFID) system is used to transmit the identity of an object or person wirelessly, using radio waves as in the form of a unique serial number. For RFID line of sight or contact is not needed for communication. Data in RFID tag can be read through any obstacle like clothing, non-metallic material etc.

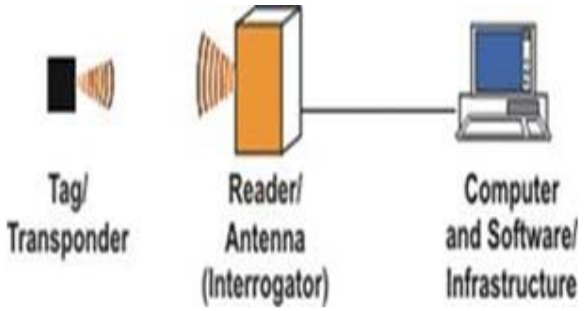

Figure-2. RFID block diagram.

2.1.1 Tag:

The information present in RFID tag is URL of the database where data of the accountant will be stored in the bank. This URL will be stored in ASIC form in the tag. The tag used here is passive because it is cheaper and smaller and the power to the tag is send using transmitting antenna. RFID tags contain at least two parts namely, an integrated circuit and antenna. An IC is used to store and process the data and the type of IC used here is non-volatile because the card should be non-programmable that is chip wired logic and antenna is used to transmit and receive the signals from reader.

2.1.2 Reader:

There are two types of readers i.e. An Active Reader Passive Tag (ARPT), An Active Reader Active Tag (ARAT). In APRT system interrogator signals are transmitted with the help of an active reader and also receive authentication replies from passive tags, whereas ARAT system uses active tags awoken with an interrogator signal from the reader.

But in short range RFID systems the antenna used is wounded copper coil which is inductively coupled with the tag. In this system a capacitor is connected in parallel to the wounded coil to from an LC resonant circuit in order to select the desired frequency. The information is passed to the antenna continously at a desired frequency. Image of a particular person who is accaessing the ATM will be captured with the help of a Webcam after reading the card.

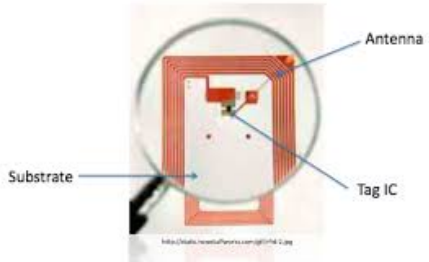

Figure-3. Overview of RFID reader.

2.2 Face recognization

Biometrics is an automatic method for verifying the person by his behavioral characteristics. Because of high Robustness and reliability, Face recognization is one of the best biometric methods to identify the person.

2.2.1 PCA algorithm

PCA algorithm is implemented with the help of Eigen values. The block diagram of the PCA algorithm is shown in Figure-3 respectively.

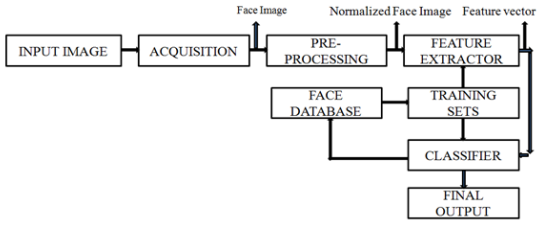

Figure-4. PCA algorithm.

PCA algorithm uses orthogonal transformation for the conversion of set of linearly correlated variables to set of linearly uncorrelated variables which are called as principle components. The number of principal components is less than or equal to the number of original variables.

2.2.2 Webcam

Feature extraction process takes place with the help of webcam. Webcam is used to take the image of a particular person. Image is based on lighting, pose and expressions of the face. Webcam is directly connected to the PC throw Wi-Fi and the data is stored in the computer. After storing that particular image, comparison of the image takes place with the image that is present in data base.

2.2.2.1 Face detection and verification module

The image that is obtained from webcam is resized and the back ground is eliminated, finally the face of that particular person is left in face detection module. The next step is verification. Here two inputs are given.

(a) Image that is stored in database.
(b) Image from the webcam.

Both the inputs are preprocessed to get geometric and photometric normalized form of face. Therefore the face obtained is free from illumination variations. The following step is feature extraction. Feature vectors are obtained in feature extraction process that is used in Principle Component Analysis.

2.2.2.2 Training sets

The image is divided into small sets called as training sets or training images. Suppose there are P patterns and each pattern has t training images of m x n configuration.

(a) The database is rearranged in the form of a matrix where each column represents an image.
(b) With the help of Eigen values and Eigen vectors covariance matrix is computed.
(c) Feature vector for each image is then computed. This feature vector represents the signature of the image. Then computation of signature matrix of a database is computed.
(d) Captured image Euclidian distance is computed with the help all the signatures present in the database.
(e) Image is identified as the one which gives least distance with the signature of the image to recognize.

Finally the identification of the image takes place. This is done by comparing the acquired biometric training sets with the training sets that is present in database and the output is obtained.

2.2.3 Analysis

The output s received in two cases from Principle Component Analysis

Case-1: Authorized person

When the output is authorized person, immediately details (name, address and phone number) of the client are taken and stored in database. A new window opens, where the person can perform his/her transaction like withdraw the money or check his/her balance etc.

Case-2: Unauthorized person

When the output is unauthorized person, immediately MMS modem is activated.

2.3 MMS modem

MMS (Multimedia Message Service) which is used to send or receive multimedia messages from PC's or mobile phones. The basic requirements for activating this MMS is

(a) Personal Computer
(b) GSM Modem
(c) MMS gateway software

This MMS modem helps to send the image to client or owner.
(d) If the person is known to the client or owner, then an SMS is sent to bank as reply. Immediately transaction process continues
(e) If the person is not known to the client or owner, interrupts activates.

2.4 Interrupts

Two types of interrupts are activated.
a) Buzzer: Buzzer or beeper is audio producing device. When the person is not known to owner or client, immediately the buzzer activates to alert nearby security.
b) Motor: The instant the buzzer rings, motor also activates and closes the door of the ATM.

2.5 Individual database security

Individual database security is provided because if someone hacks account, details of hacker i.e. unauthorized person can be obtained easily.

2.5.1 User authentication

User authentication occurs in two steps
1) Creating a file that contains user name and passwords.
2) Assuring with the server about the resources to be protected

2.5.2 Server authentication

In Server Authentication, RSA algorithm is enabled. It is implemented as follows
a) After receiving the response, the client checks the CA. if the server 2 and server 1 are signed by same CA then a new secure session is formed with server 2.
b) Before sending the information, client compares and checks weather the internet name is same or not.
c) If internet name is same then, server2 receives the information from client and decrypts the information. Finally the server2 re-encrypts the information and sends to server 1.
d) If internet name is not same then connection discontinued.

Because of this server authentication and user authentication, the data is kept secure.

3. RESULT

The input is given to the personal computer with the help of RFID.RFID is used to transmit the identity of a person wirelessly, using radio waves. As RFID receiver receives information from transmitter, it compares the user tag and if it matches with database then Face Detection System is opened. Immediately image of the person is captured which is shown in Figure-5.

Figure-5. Face reorganization.

3.1 Case-1: Authorized person

Step-1

Immediately when the image is captured, the image is converted into gray scale. Finally comparison takes place between the captured image and the image present in database using Webbers law

Figure-6. Comparison between the images.

Step-2

After comparison, if majority of pixels are equal then the output is displayed as authorized. Immediately a new pop-up window appears on the screen as shown in Figure-7 where the person can continue his/her transaction.

Figure-7. Authorized Person.

Step-3

Here Name, Address and Phone Number of that person who is with drawing the money from automatic teller machine are taken and stored in data base.

Figure-8. User information.

Step-4

For different services like banking, railway, medical single card can be used in Figure-9, the card for banking purpose.

Figure-9. Service provider.

Step-5

A new window opens where the person can with draw the money or check his/her balance which is shown in Figure-10, respectively.

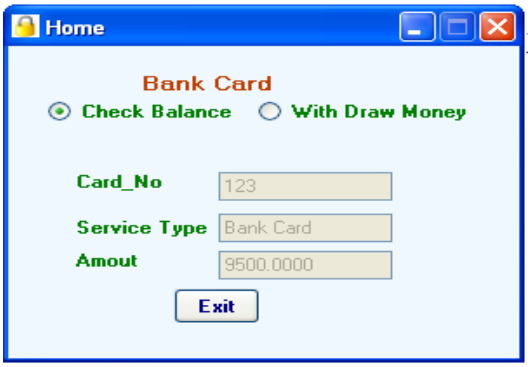

Figure-10. Banking card.

3.2 Case-2: Unauthorized person

Step-1

Comparison takes place between the captured image and the image

Present in database using Webbers law. After comparison, if majority of pixels are not equal then the output is displayed as not authorized.

Figure-11. Person not authorised.

Step-2

Immediately a popup window appears where the person should enter the phone number as shown in Figure-12. Then MMS modem is activated.

Figure-12. Phone number as input.

Step-3

The face of that particular person is sent as MMS to the owner.

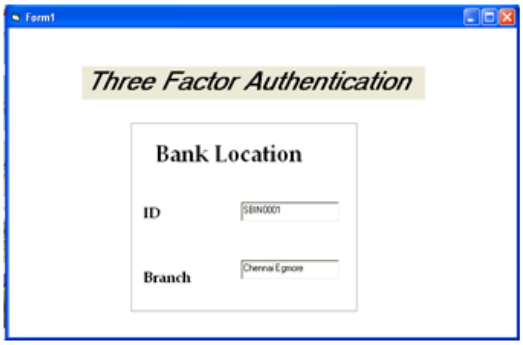

Figure-13. MMS service.

Step-4

When owner replies a password to the bank then transaction will be opened. It indicates that the person is known to the owner.

Figure-14. Authorized person.

Step-5

Within a limited delay, if the owner doesn't reply any password to the bank then transaction will be denied. Immediately ATM doors will be closed and alarm rings to alert the security. This information will be sent to nearby police station.

3.3 Individual database security

Here individual data base security is provided. This can be verified by following steps:

Initially open sequential query language (SQL) server management and then go to smart card and Right click on tables icon and select rows. Figure-15 shows the encrypted form of the card number which is stored in data base. This encryption is done using RSA algorithm.

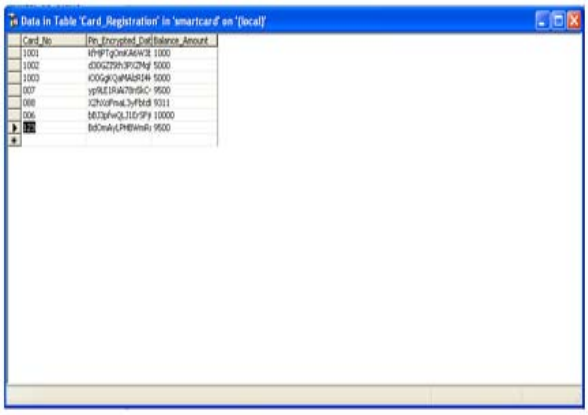

Figure-15. Individual data base security.

4. CONCLUSIONS

In this paper, we analyzed the problems due to lack of security. This issue can be over taken by proposing a new framework for security called three factor authentications. Three factor authentications are based mainly on three factors - RFID, face recognization and individual database security. This reduces the complexity of the existing system and it can be used in different fields like military sectors, banking sectors, government sectors etc...

REFERENCES

[1] E. Thambiraja, G. Ramesh, Dr. R. Umarani. 2013. A Survey on Various Most Common Encryption Techniques "International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.

[2] Kobsa, R. Nithyanand, G. Tsudik, and E. Uzun. 2012. Usability of Display-Equipped RFID Tags For Security Purposes," Proc. European Symp. Research in Computer Security (ESORICS), 2012.

[3] Di Ma, Member, IEEE, Nitesh Saxena, Member, IEEE, Tuo Xiang, and Yan Zhu. 2013. "Location-Aware And Safer Cards: Enhancing RFID Security And Privacy Via Location Sensing", IEEE Transactions on dependable and secure computing.

[4] Taranpreet Singh Ruprah, IET-DAVV, Indore, India. 2011. Face Recognition Based on PCA Algorithm. International Journal of Computer Science and Informatics (IJCSI), ISSN.

[5] Alim O.A., Dept. of Electr. Eng., Alexandria Univ., Shaaban, S., Bahy, H. 2006. Speech and Video Transmission over Wireless Atm Networks, Radio Science Conference, 2006 NRSC 2006. Proceedings of the Twenty Third National (Volume: 0).

[6] QinghanXiao ; Defence R and D Canada, Ottawa, Ont., Canada. 2013. "A Biometric Authentication Approach For High Security Ad-Hoc Networks", Information Assurance Workshop, 2013. Proceedings from the Fifth Annual IEEE SMC.

[7] C.T. Li, M-S. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme using Smart Cards," J. Network and Computer Applications, vol. 33, no. 1, pp. 1-5, 2010.

[8] Ed. Dawson, J. Lopez, J. A. Montenegro, and E. Okamoto, "BAAI: Biometric Authentication and Authorization Infrastructure," Proc. IEEE Intern. Conference on Information Technology: Research and Education (ITRE'03), pp. 274-278, 2010.

[9] N.K. Ratha, J.H. Connell, and R.M. Bolle,"Enhancing Security and Privacy in Biometrics-based Authentication Systems," IBM systems Journal, vol. 40, no. 3, pp. 614-634, 2007.

[10] Simon Robinson, Christian Nagel, Karli Watson, "Professional C#", Wiley Dream tech India Pvt. ltd., third edition.

[11] Elias M.Award's, "System Analysis and Design", Galgotia Publications Private Limited Companies, 2006 Edition.

[12] Herbert Scheldt, "The Complete Refernce C# 2.0", Tata McGraw Hill Publications, second edition.

[13] G. Song, Z. Wei, W. Zhang and A. Song, "Design of a networked monitoring system for home automation," IEEE Trans. on Consumer Electronics, vol. 53, no. 3, pp. 933-937, August 2007.