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

S. Lakshmi, Nuni Sri Annapurna and T. Sharmila Latha
Department of Electronics and Communication Engineering, Sathyabama University, Chennai, Tamil Nadu, India
E-Mail: slakmy@yahoo.co.in

ABSTRACT

Lack of proper security in identification of a remote client in distributed systems, unauthorized access of various services and resources in different areas such as Banking, military government organizations has been increased enormously. The generally used technique to decide the uniqueness of a remote client is two factor authentication and the two factors are user id and password and one time password. This paper investigates basic and safe framework to improve 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 guarantee at little expenditure but also defend privacy of the client in dispersed systems.

Keywords: security, RFID, MMS, face recognization.

INTRODUCTION

Two factor authentications is common method used to decide the identity of a remote client and two factors are namely user id and password and one time password and Lamport proposed a validation proposal to provide authentication among the users and the distant server and the challenger is molded:

- The challengers know how to intercept the contact channel connecting the clients as well as the server in the login and authentication phase.
- The challenger can get in sequence by finding the smart card or receive a client'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 client but also a client can verify the server even though security of the distributed systems is not improved effectively.

So, this paper investigates a systematic approach to improve two-factor authentication to three-factor authentication. This conversion not only signifies in the improvement of information guarantee at little expenditure but also defend privacy of the client in dispersed systems. Additionally, our framework keeps several practice-friendly belongings 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 assaulter could imitate authorized user to login as well as contact the remote server. So, in three factor authentication we investigate the Fan-Chan-Zhang's security proposal which is not vulnerable to replay attacks and impersonation attacks.

SYSTEM MODEL

In this proposed system in Figure-1 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 recognisation). 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.

BLOCK DIAGRAM

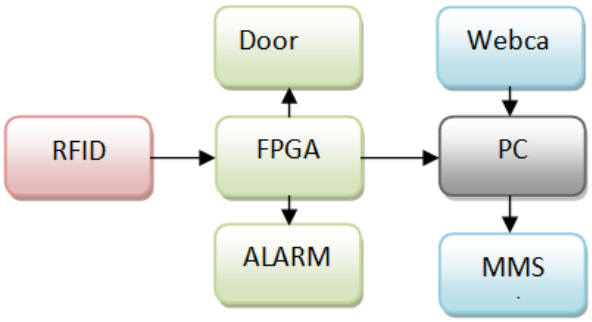


Figure-1. Proposed authentication architecture.

NON PROGRAMMABLE CARD

Radio frequency identification (RFID) system in Figure-2 is used to transmit the individuality of an object or person wirelessly, using radio waves as in the type 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.

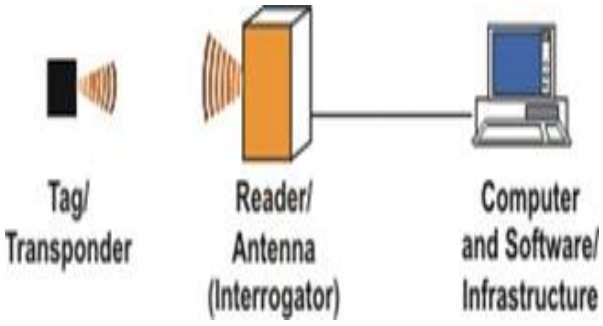


Figure-2. RFID system.

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 have at least two components namely, an antenna and integrated circuit. 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.

READER

There are two types of readers i.e. An Active Reader Passive Tag (ARPT), An Active Reader Active Tag (ARAT). In APRT as in Figure-3 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.

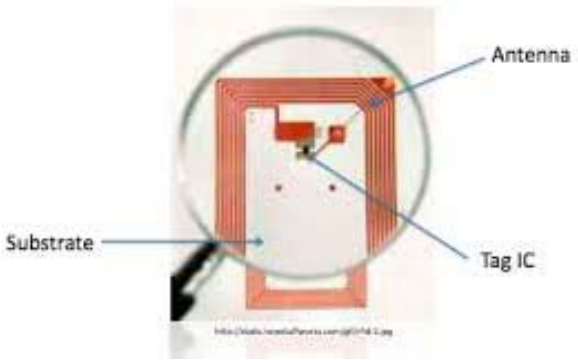


Figure-3. Overview of RFID reader.

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.

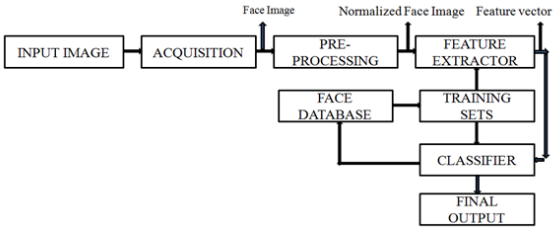
Image of a particular person who is accaessing the ATM will be captured with the help of a Webcam after reading the card.

FACE RECOGNIZATION

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

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.



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 below otherwise equivalent to the quantity of unique variables.

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.

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.

- Image that is stored in database.
- Image from the webcam.

Both the inputs are preprocessed to get arithmetic and photometric standardize 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.

Training sets

The image is divided into small sets called as training sets or training images. In the m*n configuration assume there are 'P' patterns and each one pattern has t training image.

- The database record is reorganized within the structure of a matrix in which every column signifies an image.
- By means of Eigen values and Eigen vectors, co variance matrix is calculated.
- After that calculation of signature matrix of a database is analyzed.
- Confined image Euclidian distance is calculated by means of signatures present in the database.
- Image is recognized as the individual that provides smallest amount distance by the signature of the image to make a distinction.

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.

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.

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

- Personal Computer
- GSM modem
- MMS gateway software
- This MMS modem helps to send the image to client or owner.
- If the person is known to the client or owner, then an SMS is sent to bank as reply. Immediately transaction process continues
- If the person is not known to the client or owner, interrupts activates.

Interrupts

Two types of interrupts are activated.

- 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.

- Motor

The instant the buzzer rings, motor also activates and closes the door of the ATM.

INDIVIDUAL DATABASE SECURITY

User Authentication

User authentication occurs in two steps

- Creating a file that contains user name and passwords.
- Assuring with the server about the resources to be protected

Server authentication

In Server Authentication, RSA algorithm is enabled. It is implemented as follows

- After receiving the response, the client checks the CA. if the server2 and server1 is signed by same CA then a new secure session is formed with server2.
- Before sending the information, client compares and checks weather the internet name is same or not.
- 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 server1.
- If internet name is not same then connection discontinued.
- Because of this server authentication and user authentication, the data is kept secure.

CONCLUSIONS

In this paper, we analyzed the problems due to lack of security. This issue can be over taken by propose a new support for security called three factor authentication. Three factor authentications are based mainly on three factors - RFID, face reorganization 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] Alim O.A, Shaaban S, Bahy H. 2006. Speech and Video transmission over Wireless ATM Networks. Radio Science Conference, Proceedings of the Twenty Third National.

[2] A. Kobsa, R. Nithyanand, G. Tsudik and E. Uzun. 2011. Usability of display-equipped RFID tags for Security purposes. Proceedings of 12th ACM international conference on Ubiquitous computing. pp. 331-340.

[3] Di Ma, Nitesh Saxena, Tuo Xiang and Yan Zhu. 2007. Location-aware and safer cards: Enhancing RFID

security and privacy via location sensing. IEEE Transactions on dependable and secure computing. 6(1).

[4] E. Thambiraja, G. Ramesh, Dr. R. Umarani. 2012. A survey on various most common Encryption techniques. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper. 2(7).

[5] Taranpreet Singh Ruprah, IET-DAVV, Indore, India. 2010. Face Recognition based on PCA algorithm. International Journal of Computer Science and Informatics (IJCSI), ISSN. 2(5), December 2011.

[6] QinganXiao; Defence R and D Canada Ottawa, Ont., Canada. 2004. A biometric Authentication approach for high Security Ad-Hoc Networks. Information assurance Workshop. Proceedings from the Fifth Annual IEEE Smc. 4: 250- 256.

[7] A. Y. Yang, A. Ganesh, Z. Zhou, S. Sastry and Y. Ma. 2010. Fast 1-Minimization Algorithms and Application in Robust Face Recognition. Vol. 6.