Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems

Dushyant Goyal[1] and Shiuh-Jeng Wang [2]

[1]B-Tech. Department of Electronics and Communication Engineering
The LNM Institute of Information Technology, Jaipur, India
Email: goyal1dushyant@gmail.com

[2]Department of Information Management
Central Police University
TaoYuan, Taiwan, 33304
Email: sjwang@mail.cpu.edu.tw

Abstract

Recently, with the awareness of businessmen and consumers and the development of mobile technologies, the potential use of mobile devices in financial applications such as banking and stock trading has seen a rapid increase. However, the security challenges being faced are diverse and increasing in number because of huge amount of money flowing across the mobiles. There have been several attempts in the field to preserve anonymity of user and protect them from several attacks but due to many security flaws these schemes are not feasible for real-life implementation. In this paper we focus on mobile banking and provide a scheme based on 2-factor biometric authentication for a user i.e. face and voice recognition. We also propose the use of steganography as a means to improve the communication channel for any intrusion by the hackers.

Keywords: *legitimacy, authenticity, biometrics, mobile banking, transactions, security, steganography*

1. Introduction

With the evolvement of banking over the recent years many different electronic banking systems have emerged like Automated Teller Machine (ATM) and telephone banking. With the help of ATM's the users could perform transactions activities while in the later approach requires users to can make a telephone call to the bank's computer system and use the phone's key pad to perform banking operations.

But, an ever-increasing growth in the mobile technology, growing economy and the use of mobile devices becoming more and more diversified, these devices are used for banking and stock trading nowadays through WAP. Mobile banking gives opportunity for everybody for easy banking activities substantially increasing the interaction between the user and the bank. It has enabled to increase financial access for people in rural areas and paved the way for integrating rural people into the mainstream financial system. Some of the mobile banking services may include:

a. Viewing A/C statement
b. Fixed Deposit Enquiry
c. Online payment (Tax, electricity bill, etc)
d. Funds Transfer
e. Shopping/ Purchasing items [4,6]

However, the amount of transaction money that flows through mobile banking has led to attract criminal attention.
Security concerns are important for customers and the Banks alike. Findings from studies in eBanking also have applications in the wider field of transaction security for eCommerce activities. Bank log-in security has to be strong and supervised as banks are an integral part of the defense against money laundering.

Concerns about security of prospective consumers are considered to be the most important factors influencing demand [1, 5]. Serious operational risks and potential liabilities are associated with security breaches in the transfer of funds over the Internet [2]. The 2002 US CSI/FBI Computer Crime and Security Survey reports that 70% of respondents sites suffered from vandalism attacks, where 12% included theft of transaction information and 6% financial fraud. Bank systems and services are reported to be important targets among fraudsters with 42% of cases related to credit card fraud, 20% to phone or utility bills, 13% to bank fraud, and 7% to loan fraud.
Concern about security has led to a major barrier for mobile banking adoption by several banks.

Apart from the authentication problems for successful remote banking transactions there are issues related to the transfer of information over the insecure communication channel as shown in Fig. 1.

Many malicious codes like Trojans steal confidential data like passwords for online banking services. In phishing a spoof web page imitating that of the user's online bank is designed and used to encourage the user to enter bank details in this false page. The data entered is sent to the cyber crooks.

A recent study has revealed that phishing attacks caused losses of $3.2 billion among US consumers in 2007 and in 2006, the average amount stolen from each victim of phishing and Trojans was €6,383.

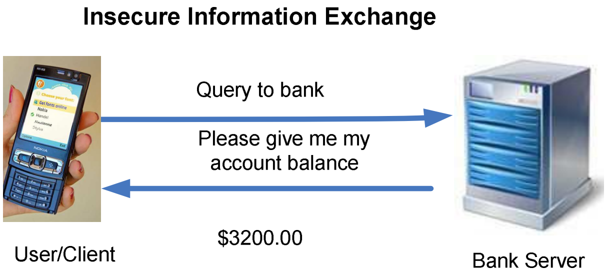

Insecure Information Exchange
Query to bank
Please give me my account balance
$3200.00
User/Client
Bank Server

Fig. 1 Insecure Communication channel

Recent increases in online fraud have encouraged Banks to think about some different multiple-factor solutions for their remote authentication procedures [3].

In this paper we discuss about the security of today's electronic banking systems and present an overview and evaluation of the techniques that are used in the current systems in section 2. We propose an authentication mechanism for mobile banking using multiple authentication components of biometrics for more robust authentication in section 3. We further try to explore some of the problems in the transmission phase of the information and present the use of steganography for secure communication. Finally some implementation details, conclusions and future work are presented in the next sections.

2. Review of some Authentication mechanisms and pitfalls

In this section we will review some of the existing methods (Fig.2) used for the authenticity purposes and also discuss some of their weaknesses:

2.1 Fixed passwords

Till today, many remote e-banking systems rely on traditional fixed passwords to authenticate the user. The password's form can be a combination of the account number and PIN number or be a character-based sequence.

2.2 MAC

MAC is based on idea of a challenge/response scheme in which a client proves his identity to the bank (i.e., entity authentication) by demonstrating the knowledge of a secret key and producing a proper response to a random challenge using this secret.

2.3 Digital signatures

Besides entity authentication, digital signatures can also be used for transaction authentication. The private signing key is usually stored on the user's computer and is only protected with a password.

2.4 Hardware tokens/ Smart Cards

Private digital signature keys and passwords for transaction authentication can be kept on smart cards. Smart cards have been widely used as a means for entity authentication like electronic identity cards etc. Mobile devices can enhance an Internet or WAP banking system's security and being personal these can perform cryptographic protocols to provide both entity and transaction authentication. The communication between WAP phone is realized manually with Bluetooth or with an infrared interface.

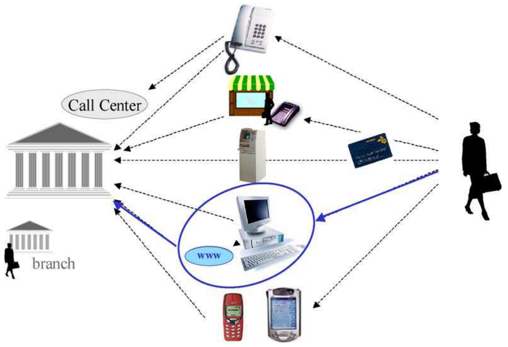


Fig. 2. Banking distribution channels.

Security pitfalls of previous schemes

a. In many schemes [9], password is chosen by the remote server which might be long, random and difficult for a user to remember. The scheme is a threat to the insider attack that has come to know the password of the user and can misuse the system in future [7]. Passwords are vulnerable to dictionary attacks, guesses and social engineering [10].

b. Previous schemes do not preserve the anonymity of the user. In the verification phase the transmission to the authentication server over insecure channel in the login message. In case of transaction scenario it is very important to preserve the privacy of a user because an adversary sniffing the communication channel can eavesdrop the communication parties involved in the authentication process to analyze the transaction being performed by the user.

c. Previous literature does not have provision to provide the mutual authentication between the user and server.

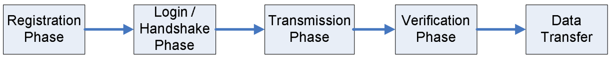
d. Losing of smart cards is one of the very serious problems because the lost card can impersonate valid registered user.

e. Traditional authentication system is based on secret key based on public key infrastructure (PKI). But the key has many disadvantages as it can be forgotten or stolen and can be easily cracked.

3. Proposed Scheme

In our proposed scheme we lay emphasis on biometrics to describe the authentication as in real life. Biometrics characteristics cannot be lost or forgotten and are extremely difficult to copy, share and distribute. It requires the person to be physically present as in real life at the time and point of authentication. This kind of security can enable clients/users to use their bank ID and biometrics to log in to the bank server remotely to access their account.
In this paper we will use two-factor (2-factor) authentication approach. 2-factor authentication is a security solution requiring the verification of two different modalities of authentication components and provides enhanced security.

We also propose to combine biometric security with steganography to enhance security over insecure channel.
The following fig. illustrates the general authenticating model procedure:



3.1 Authentication Process

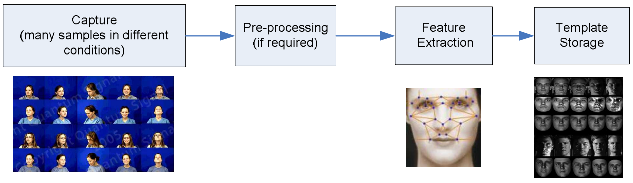
The complete authentication model is discussed below and illustrated in Fig. 3.

A. Registration phase

The registration can be performed either personally or remotely using the mobile by a user. During the registration phase the following steps are performed by the bank server:

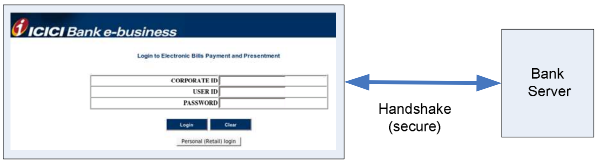
i. The biometric data of the user is captured, preprocessed and the features are extracted. The feature templates are formed and stored as enrolled templates. These saved templates are referred during the verification phase. Face and voice samples are taken in our scheme for the purpose for final template storage in the user database.

ii. The user is also given an eID as well as a password apart from (i) as an additional parameter for small processing through his identity.



B. Login / Handshake Phase

When the user wants to login into the server or account, he is required to enter his eID and password.
The server performs the following preliminary steps:
i. Checks T is the current time stamp of the user's machine.
ii. Verifies initial login details i.e. the ID and password.
iii. If the prior information entered is correct, the user is redirected to the biometrics authentication page and the user is asked to start video and voice transmission through the mobile.



C. Transmission Phase

This phase takes care of the transmitting information through the internet as we have no control over the insecure channel.

i. In order to avoid the interruption of hackers and intruders we propose to hide the video and audio data into some images or videos related to normal life or otherwise which when encountered by the hacker can be ignored and transmission can be proceeded safely.
ii. Even if the transmitting data is suspected by the hacker he cannot extract the secret data.

D. Verification phase

Upon receiving the login information and the stego file, the authentication server performs the following steps:

i. The server applies the reverse of the embedding secret data procedure to recover the biometric information from the stego file.
ii. Checks the validity of time stamp with the current date and time T' and T_1. If $(T'-T_1) \geq \Delta T$ then the server rejects the login request of the user otherwise accepts the request. Here ΔT denotes the expected valid time interval for transmission delay and T' denotes the receiving timestamp of login attempt by the user.
iii. Once the biometrics is successfully derived from the stego file, the face and voice recognition takes places

as discussed in section 3.3 and the suitable candidate is matched from the database.

iv. Computes T'' and T_s from the MAC sent from the server for confirmation. If $(T''-T_s) \geq \Delta T$ then the user rejects this message otherwise calculates the MAC hash function using his private key.

v. After receiving the response message from server user compares the two hash values i.e. calculated from MAC and the original value. If the two are equal the server gets authenticated otherwise the operation is terminated.

E. Data Transfer

Once the user is successfully authenticated the data (transaction details, etc) can be transferred over the channel using the secure WTLS protocols after common encryption techniques.

F. Mutual Authentication

Once all the steps i.e. A-E are completed the status of authentication result is generated by the server. This can be done either by using MAC or sending a SMS to the user. This will further strengthen the security aspect of the proposed scheme as this would serve as an alarm in case of false intrusion.

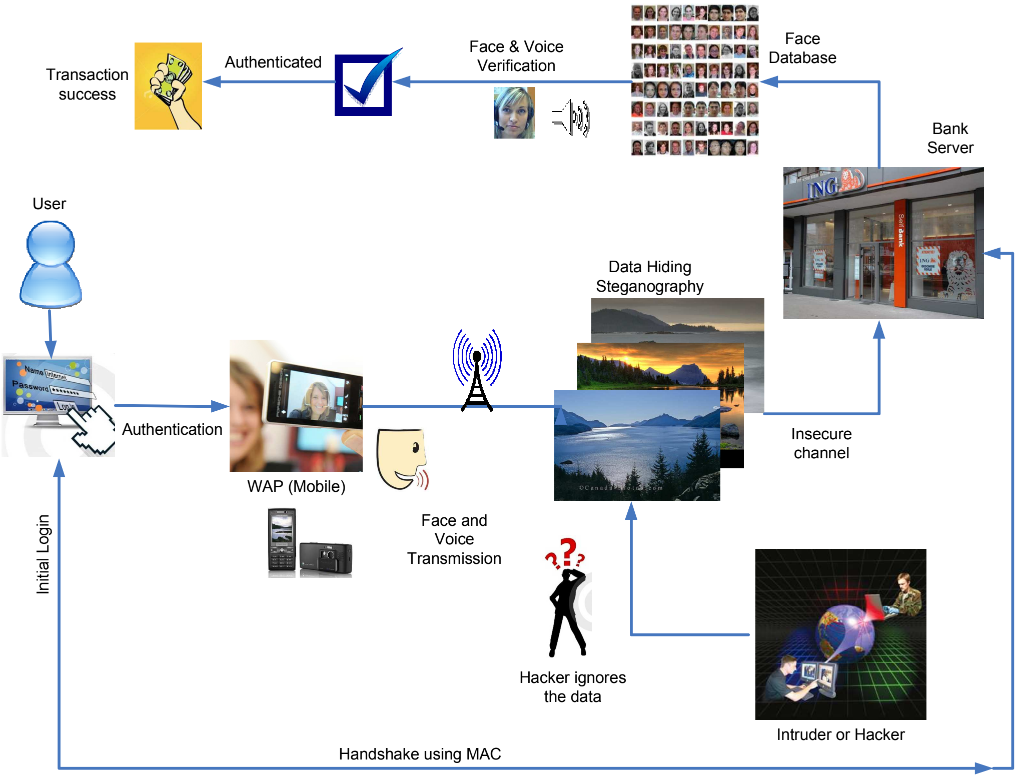


Fig. 3. Proposed secure Authentication model

3.2 Steganography

Steganography is an of art hiding secret messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The message is altered in a way to disguise the secret message in images, videos etc. In our scheme also we use steganography to hide the video and voice information before transmitting.
The hiding technique used must have sufficiently high capacity and must be robust.

3.3 Face and Voice Recognition

Face recognition is non-intrusive, hands-free, can provide for continuous authentication, and can be accepted by most users. The face recognition technology captures the face images using mobile camera (visible spectrum) and extracts key features that do not change over time (e.g., face shape, eyes, nose, mouth, ears, forehead, and chin) from the images. Then verification and identification can be performed by comparing the face features stored in the database of faces.

Similar to face voice also plays a very important role for an individual. The voice and video are captured simultaneously with the help of camera and microphone present in users mobile.
In case of voice transmission the user is asked to speak the text displayed on his authenticating window of his mobile which is dynamic and thus changes each time the

user wishes to login. The server matches the speech with the text. In this way it provides yet another attempt for secure voice authentication.

The scheme provides security against an attacker who is looking over the shoulder or is sniffing the keyboard or some software which are taking images of the desktop to intrude into a users account.

Some of the state of art techniques has been proposed in the literature for robust face and voice recognition [8].

Besides this the distribution data i.e. video is also embedded a tag like a tracing key value (timestamp) to offer fidelity to uniquely identify a particular session of login. The proposed model can also be extended to multi users to facilitate secure multi user transactions.

4. Implementation

The client must be equipped with a mobile phone with a camera and the capability of browsing the internet through WAP (Wireless Access Protocol).

Apart from this a dedicated standalone client/server application is needed for the successful realization of communication between the user and the bank. However, the bank must provide the user with the necessary software. A Java applet for that matter would be the best solution.

5. Extensions

The concept of mobile banking and the proposed authentication mechanism can be extended to mobile shopping which has also grown quite rapidly in the recent era with the introduction of online marts. Government institutions can increase use, supply and promotion of electronic services through mobiles. Mobile voting can also be introduced which will uniquely identify each individual and they could cast their votes remotely. In all of the above applications the role of authentication becomes very important and our scheme proves to be very robust and secure in such scenarios.

6. Conclusion

In this paper, we have presented weaknesses of some of the previous remote user authentication schemes. Firstly, we showed that how the previous schemes were vulnerable to insider attack and did not preserve anonymity of a user, long and random password for a user to remember, no provision for revocation of lost or stolen smart card and no support for session key agreement during authentication process. To overcome the identified problems we proposed an enhanced biometrics based steganographic approach which improves all the identified weaknesses and is more secure and robust for real-life use. The proposed scheme can withstand the forged authenticating attacks besides providing better communication with the system as the information traveling across the insecure channel is always hidden. The system is very secure as mutual authentication takes place between the communicating parties for processing of the supplied information. Moreover, our scheme is robust, practical and more efficient than other schemes.

7. Future Work

In future, more practice handling and using such schemes especially the biometrics within the experimental setting might provide more realistic data, reducing the potential strain and bias of first-time use. Practical implementation of the same is also required to have a real life environment for more developments to take place. Use of biometrics may certainly lead to real life physical authentication systems. More robust techniques for face and voice recognition need to be explored.

References

[1] H. Christiansen, 2001. Electronic Finance: Economics and Institutional Factors. OECD Financial Affair Division Occasional Paper No. 2, 2001.

[2]. K. Furst and D.W.W. Lang, 2002. Internet Banking: Developments and prospects. Center for Information Policy Research, Harvard University, April 2002.

[3]. A. Hiltgen, T. Kramp, and T. Weigold, 2006. Secure internet banking authentication. IEEE Security and Privacy (March/April), 21–29.

[4]. B. Ives, K.R. Walsh, and H. Schneider, 2004. The domino effect of password reuse. Communications of the ACM 47 (4), 75–78.

[5]. M. Mattila, H. Karjaluoto, and T. Pento, 2002. Internet banking adoption factors in Finland.

[6] S. Ranger, 2005. Chip and PIN heads for Cyberspace. Silicon.com Financial Services News, CNET Networks, UK.

[7].W.C. Ku and S.M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2004).

[8]. W. Zhao, R. Chellappa, A. Rosenfeld, and P.J. Phillips, Face Recognition: A Literature Survey, ACM Computing Surveys, 2003, pp. 399-458

[9]. Y.Y. Wang, J.Y. Kiu, F.X. Xiao, and J. Dan, A more efficient and secure dynamic ID based remote user authentication scheme, Computer Communications 32 (2009) 583–585.

[10]. M. Zviran and W.J. Haga, 1990. Cognitive passwords: the key to easy access control. Computers and Security 9 (8), 723–736.