Alexandria Engineering Journal (2012) **51**, 185–191

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

ORIGINAL ARTICLE

A model to authenticate requests for online banking transactions

Saad M. Darwish *, Ahmed M. Hassan

Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, 163 Horreya Avenue, El Shatby 21526, P.O. Box 832, Alexandria, Egypt

Received 16 March 2011; revised 9 December 2011; accepted 28 February 2012
Available online 12 April 2012

KEYWORDS

Identity Based Encryption (IBE);
Electronic transactions;
Online banking security

Abstract As the number of clients using online banking increases, online banking systems are becoming more desirable targets for attacks. To maintain the clients trust and confidence in the security of their online banking services; financial institutions must identify how attackers compromise accounts and develop methods to protect them. Towards this purpose, this paper presents a modified model to authenticate clients for online banking transactions through utilizing Identity-Based mediated RSA(IB-mRSA) technique in conjunction with the one-time ID concept for the purpose of increasing security, avoiding swallow's sorties and preventing reply attacks. The introduced system exploits a method for splitting private keys between the client and the Certification Authority (CA) server. Neither the client nor the CA can cheat one another since one-time ID can be used only once and each signature must involve both parties. The resulting model seems to be practical from both computational as well as storage point of view. The experimental results show the effectiveness of the proposed model.

1. Introduction

Electronic banking that allows people to interact with their banking accounts via the Internet from virtually anywhere in the world provides enormous benefits to consumers in terms of the ease and cost of transactions. This system permits consumers to request information and carry out most of banking services such as balance reports, inter-account transfers, and bill payment. The basic architecture of online banking system consists of three major components [1]: (1) Client; (2) Application server that takes care of the server script and checks for the ODBC connectivity for mapping to the database in order to fulfill client and administrator's requests; and (3) Database, which stores client and bank data.

* Corresponding author. Tel.: +20 1222632369; fax: +20 3 4285792.
E-mail addresses: saad.darwish@gmail.com, saad.darwish@alex-igsr.edu.eg (S.M. Darwish), Ahassan1968@hotmail.com (A.M. Hassan).

Peer review under responsibility of Faculty of Engineering, Alexandrian University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aej.2012.02.005

While online banking offers enormous advantages and opportunities, it faces different kinds of risks that are specific to conduct sensitive business over the Internet. So, it is imperative that banks implement strong security approaches that can adequately address, monitor, manage and control risks and security threats to the bank. Security aims to prevent fraudsters from accessing online banking accounts that don't belong to them, and subsequently viewing confidential information, causing malicious damage and stealing funds. In order to provide effective and secure banking transactions, there are two technology issues needed to be resolved [2]: (1) Security: is the primary concern of the Internet-based industries. The lack of security may result in serious damages and (2) Authentication: Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction.

In general, the solutions to the online banking security issues require the use of software-based systems or hardware-based systems or a hybrid of them. The software-based solutions involve the use of encryption algorithms while hardware-based solutions involve the use of devices such as the smartcard. Software-based protection is easily obtained at lower costs than hardware-based protection. Consequently, due to the easy portability and ease of distribution through networks; software-based systems are more abundant in the market. However, software-based protection has many potential hazards like attacking the encryption algorithms by means of brute force and analysis attacks [1–3].

Encryption, which modifies information in a way that makes it unreadable until the exact same process is reversed, is one of the methods used to solve the problem of attack trees, which identify how attackers compromise accounts and develop methods to protect them [4]. In the literature, there exist many algorithms available to implement the public key cryptography, like Rivest–Shamir–Adleman (RSA) encryption, Advanced Encryption Standard (AES) and Data Encryption Standard (DES). However, these techniques are slow when large volumes of data are to be encrypted [5]. Other encryption techniques include mediated RSA (mRSA) [6], which is a simple and practical method of splitting RSA private keys between user and the online trusted server. Both the user and the trusted server employ their respective half-keys in a way that is functionally equivalent to (and indistinguishable form) standard RSA. Neither the user nor the server knows the factorization of the RSA modulus and neither can decrypt/sign message without the other's help. The main problem of mRSA encryption approach is that it still relies on public key certificates to derive private/public keys. This leads to the issues of certificate management like revocation, distribution, storage and verification. Refer to [7,8] for a detailed description and security analysis of the mRSA algorithm.

Recently, Identifier-Based Encryption (IBE) is emerged as a cryptographic scheme in modern secure banking systems to protect online transactions. Identity-based public key encryption facilitates easy introduction of public key cryptography by allowing an entity's public key to be derived from arbitrary identification values, such as name or e-mail address. The main practical benefit of identity-based cryptography is in greatly reducing the need for, and reliance on, public key certificates and solving certain public key management problems since there is no need to maintain a great database containing a list of public keys and their respective owner [7]. A more recent work is proposed to combine identity-based encryption with mRSA in one framework, IB-mRSA, to improve security against adaptive chosen cipher attacks that represent the immense threat in RSA algorithm. IB-mRSA protocol allows the sender (encryptor) to skip the costly checking of individual public key certificates. Furthermore, for real time applications IB-mRSA algorithm takes roughly 4–5 times less than plain RSA technique [8].

The major weakness of the IB-mRSA based online banking systems is that their disability to prevent reply attacks and their vulnerability against denial of the services (DoSs) attacks since an attacker can send many requests to the trusted server. In the literature, there are three types of DoS attacks [9]: against server's bandwidth, memory, and CPU. The purpose of the first attack is that a server cannot receive any more messages. The second one is performed to make a server stores large quantities of waste states. The last one is the attack, which makes a server computes a lot of quite inefficient processing. Most previous security researches focus on DoS attacks against server's CPU. To handle the problem of DoS attack, the idea of employing one-time ID is suggested in order to make the attackers cannot reuse the requests generated by legal user because one-time ID dynamically changes.

1.1. Contribution

Our contribution in this paper is to blend the attractive features of IB-mRSA protocol with one-time ID based DoS prevention technique in an integrated model to authenticate requests for online banking transactions. The proposed model represents a variant of IB-mRSA technique that can avoid DoS attacks and prevent leakage of user's identity. The rationale of using IB-mRSA protocol is that it combines the advantages of fast revocation and identity based public keys, which makes it difficult to control a user's security privileges for identity revocation.

This model is simple, secure and very efficient to protect the privacy of clients since one-time ID can be used only once. Moreover, the established model gives extra security against hackers to guess private keys and possesses the ability of supporting revocation not just for signatures but also for (public key) encryption as well. Both the architecture and an implementation of this model are discussed as well as the performance, compatibility, and usability aspects.

The rest of the paper is organized as follows. Next section provides a brief synopsis of our work, its contribution and describes the proposed security model in details. Subsequently, implementation and performance measurements are discussed in Section 3; it is followed by efficiency and security analysis in Section 4. In Section 5, the paper concludes with the summary of benefits of the presented model.

2. Methodology

This section describes the proposed model that is derived from Rajalakshmi et al. approach [8] with some necessary modifications to satisfy our new requirement such as certainty and simplicity in the dispute resolution and avoiding swallow's attacks (generating a signature for any other message using the proxy's