Journal of Mobile, Embedded and Distributed Systems, vol. VII, no. 3, 2015
ISSN 2067 – 4074

Anonymous Mobile Payment Solution

Alhaj Ali JALILA
IT&C Security Master
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies
ROMANIA
jalila.aaj@gmail.com

Abstract: The evolution and increasing popularity of mobile handheld devices has led to the development of payment applications. The global acceptance of mobile payments is hindered by security and privacy concerns. One of the main problems evoked is the anonymity related with banking transactions. In this paper I propose a new secured architecture for mobile banking. Anonymity and privacy protection are the measures to be enhanced in order to satisfy people's current needs. The banking platform must provide the highest level of security for messages exchanged between bank and the customer.

Key-Words: anonymity, security, OTP, QR code, mobile payment, token, digital signatures

1. Introduction

The increasing usage of mobile handheld devices has led to the development of the most challenging services, such as mobile banking. Mobile banking systems are facing users' susceptibility in take-up of payments and bank transfers, one of the most important issues being the security. The emerging security risks are due to several factors such as: unprotected communication over wireless networks, user authentication systems that adopt incomplete and unsuitable security solutions and also the human factor.
As with physical cash, the proposed solution is designed to limit the link between a merchant and a client, in order to protect customers' privacy. Nevertheless, in order to create an anonymous mobile payment in accordance with the rules and country legislation and with the acceptance of banking institution, the payment system should be put under transparency in case of illegalities. The main advantage of supervised anonymity is the protection of clients' privacy and the limitation of data corruption. Mobile payments should ensure a high level of security and also a significant level of anonymity in accordance with users' needs. The solution presents unidirectional anonymity, the anonymous payment being defined as a transaction between a client which does not reveal personal or private information and merchants with acquainted identity.
The system must be protected against most popular attacks, such as: eavesdropping, sniffing, traffic analysis, man-in-the-middle, denial-of-service. Data and communication must be protected by a secure environment. The application describes a solution as an alternative to the use of bank cards, taking into account that nowadays people are using their smartphones for almost any service.
Firstly I will present existent methods of authentication that offer a trusted degree of security. Then are described the current methods of payment and the level of anonymity it ensure. In section 3 are introduced the steps that I took into consideration when I developed the application. The architecture of the system is shown in section 4. The conclusions of this paper can be found in section 5.

2. Mobile banking

The term, mobile banking, it is used to describe the performing of online banking services, account information, money transactions, account balance etc. Nowadays there is a buoyant growth tendency using the phone for any service, and one of this, is the use of mobile

banking applications downloaded onto the mobile device [2].
Banking transactions are made between two interfaces: customer-bank and bank - merchant. The problem that arises when initiating transactions is that although the way in which this takes place is safe, all buyer credentials get to the seller. The merchant must ensure that it uses the current security systems, strong enough to prevent theft, data manipulation and intrusions. Actual mobile banking solutions are designed to provide user security, but not all of them provide the necessary anonymity.

2.1 Mobile Banking Solutions for Authentication

The use of static passwords has some important security drawbacks: passwords can be stolen (by the use of key loggers), guessed, eavesdropped and forgotten [3]. Despite increasingly levels of attacks, most authentication applications rely on weak passwords for granting user access. To improve the use of passwords in authentication process, it is required a stronger model that implies several steps to provide protection. The two-factor authentication proves the identity of an entity, based on the assumption that an unauthorized person cannot find the two secrets required to access the resources. The main condition is that if one of the two components is incorrectly supplied, the two-factor authentication remains blocked. The login part of the application is based on one time passwords.

2.1.1 Tokens

A cryptographic token is a hardware device or a software application on which an authorized user relies to authenticate. The token can be used as an additional method to password based authentication, in order to enhance security. Generally, a token stores counters, cryptographic keys, such as digital signatures or biometrics. There are four types of tokens:

1) Token based on static passwords- it contains one password used for each authentication, the password it is not known by the owner of the token;
2) The token has asynchronous password - the one time password is generated by using a clock;
3) Token based on dynamic synchronous passwords- the password is generated by a cryptographic algorithm, which uses a timer combination; in this case is necessary synchronization between server and client;
4) Challenge –response token: it is used public key cryptography.

A set of algorithms are used to provide one-time passwords from a secret shared key. The algorithms are described in open standards, such as HOTP-HMAC-Based One-Time Password Algorithm (RFC 4226), TOTP-Time-Based One-Time Password Algorithm (RFC 6238), OCRA - OATH Challenge-Response Algorithm (RFC 6287).
The authentication relies on PIN (the secret password the person knows) and a token which generates passwords valid for a certain time. The most important fact in one-time password (OTP) is that the algorithm is not reversible, which means that even the key is known, the key generator cannot be accessed and the password is unique. It is almost impossible to find a pattern to guess the key and the current counter value. The strength of the OTP is given by the quality of the cryptographic algorithm used.
The HOTP algorithm, as described in (RFC 4226, 2005), is counter based:

$$HOTP(K, C) = Truncate(HMAC\text{-}SHA\text{-}1(K, C)) \quad (1)$$

where K-is the key initial seed (160 bits) and C – the counter (64 bit), which is incremented each time a new code is generated by the application token. The result is a 6-8 digit number. The seed and the counter are stored inside the application. There are cases when the counter on the token is different from the one on the server, because the counter on the client's token counter increases each time a HOTP is requested, while the counter on the server increments only on successful authentication. In this situation the server should calculate the next HOTP values until a defined limit. The restriction is necessary to avoid denial -of – service

ISSN 2067 – 4074

attacks. In order to avoid replay attacks the communication is made on a secure channel.
The authentication process:

a) The client introduces user name, PIN and requests to generate the OTP.
b) The counter is incremented by the token, and the next HOTP is computed.
c) The validation takes place on the server side. The HOTP succeeds if the same value is found on the server and on the token that generated it. The server increases the value of the counter by one.
d) In case the value received by the server does not correspond to the value calculated by the token, the server tries to resynchronize. The server counts the number of attempts and if the limit is reached it blocks the authentication process.
e) If authentication succeeds the client can access his resources.

The main difference between HOTP and TOTP is that in case of TOTP the password has a short life OTP value, whilst the HOTP is valid for a longer period of time. The TOTP enhances the security by replacing the counter with a time parameter.

$$TOTP = HOTP(K, T) \quad (2)$$

where K is a secret key and is an integer value calculated as a ratio between the difference between current time (default 0) and the initial counter time. If the OTP is generated within the same step, its value will be equal with the previous.

2.1.2 Mobile OTP Advantages and Disadvantages

The weakness in an authentication is usually the human factor. It is difficult to remember many complex passwords, so users often use the same one all across the internet and not really a strong one. OTP simplifies the need to memorize a complex password, everything is to remember the four digit PIN.
In the case of an OTP sent by a mobile phone, it is protected by the phone security.

The main benefits of OTP mobile token are:

- Authentication is made by adding a step that enhances security(two-factor authentication);
- The counter and the password cannot be guessed;
- The algorithm that generates the password is not reversible;
- Having a small lifetime the OTP cannot be reutilized by a third party and cannot be reused by the user in another session;
- the key is long enough;
- the key is hardware protected.

Disadvantages:

- synchronization between server and client token can cause significant problems

2.2 Available anonymous payments systems

Most widely used mean of electronic payments are bank cards. Bank card cryptography relies on the Triple DES (3DES) algorithm applied to the secret bank key and also to the account number combined with 4-digit PIN. Although it is safe, this method of payment does not provide a reliable customer anonymity. There are several cryptographic systems which ensure a certain level of anonymity, which I will describe further.
Bitcoin is a decentralized digital currency, invented by Satoshi Nakamoto, that allows instant payments anywhere on the globe. Bitcoin is a peer-to-peer system, where users can make transactions without the need of a trusted third party. All Bitcoin transactions are stored publicly and permanently on the network, making it one of the most transparent payment network in the word.

2.2.1 Bitcoin architecture Signatures

Users can spend only bitcoins associated with a specific address. A payer signs digitally the transaction using his private key, the network can use the payer's public key to verify that the entity that initiates the transactions really is the person who signed the money [7].

Validity of transactions: Transactions are declared valid if every signed input is an unspent output of a previous transaction.
In order to avoid coins double spending, the transaction is broadcast to the entire network and some nodes on the network, named miners are verifying owner's identity. The processing is done by miners that keep the chain constant an unalterable by checking every newly broadcasted transaction into group of transactions named block. The proof-of-work concept relies on two notions: the power of computation is costly for network users to validate transactions and miners are rewarded for their help.

2.2.2 Bitcoin Advantages and Disadvantages

Bitcoin system has many advantages, as following [8]:

- it is scalable;
- is based on public key cryptography that uses Elliptic Curve Digital Signature Algorithm (ECDSA);
- user privacy is assured by the use of addresses, because the user makes payments through addresses. In order to enhance privacy, is recommended to create a new address for each payment;
- every transaction is registered and stored in the block chain, which is a sequence of records called blocks;
- the proof-of-work is a secure function on which the miner's work is rewarded and they have to validate accordingly transactions;
- transactions are free of charge, or low cost, because fees are optional to be paid, but higher fees stimulate miners to prioritize their work and to give faster responses.
- fast international payments, the estimated time for a payment to a foreign country or local place is almost the same.

Even Bitcoin it is declared as a safe, instant and in most cases anonymous, it has some drawbacks:

- being a peer-to-peer network, the ip address can be logged, but computer's IP address can be hidden by tools like Tor;
- in Bitcoin system all transactions are irreversible;
- instant transactions are less secure, thus a client must wait to receive approval for at least six nodes. In some cases if the amount of bitcoins is small the number of answers to wait for can be less;
- wallet is vulnerable to theft, were registered many cases where the bitcoins were stolen from wallet [9];
- denial of Service (DoS) attacks that were registered in 2014 lead to rapid decrease in the value of satoshis;
- some other attacks can be performed on nodes, such as forcing clock drift against a target node;
- because of its not so good reputation and the lack of knowledge, not many sellers accept the use of bitcoins;
- many countries deem this cryptocurrency as illegal one and some associate it with criminals, offenders.

3. Methodology

In order to create a secure mobile banking system, some steps were taken into consideration:

a. the actual user necessities;
b. the platform on which the application is developed, in this case Android;
c. actual standards of security;
d. in order to create a connection between server and client were installed the appropriate developing tools and programs;
e. to ensure security of data exchanged between parties was used the HTTPs protocol.

The application is structured as client and server and it contains the most important, basic, banking transactions such as money transfer, check balance and the payment of a bill.
A simple form of login was initially designed to connect to the bank's server. The Android layout contained a username and a password. In order to avoid the use of blank spaces, weak passwords. With Retrofit library, were requested the Web services of a REST API with POST, GET, PUT and others. On server side was used a REST API. The bank server was

ISSN 2067 – 4074

initialized and a SSL certificate was created to allow HTTPs connection. At this stage were taken into consideration the issues of using simple passwords, and were introduced two-factor passwords.

4. Anonymous Mobile Transactions - Problem Solution

The mobile banking environment has three main actors: the bank, the costumer and the merchant. The costumer is the mobile user that holds a mobile handheld device with performing the steps to initialize a transaction.
The banking services are provided by the services provider, that are in accordance with Web services standards and REST.
Anonymous transactions are made by implementing a protocol that grants fully anonymity between the customer and the merchant. The problem that is attempted to be avert is the involvement of third parties.

4.1 Architecture

The proposed architecture is based on the two-factor authentication. The mobile OTP token is based on TOTP: Time-Based One-Time Password Algorithm (RFC 6238) and HMAC-based One-Time Password (HOTP) algorithm (RFC 4226). The HOTP algorithm is based on HMAC-SHA-1 algorithm and is applied to a counter value that increases, representing the HMAC computation [4].

$$HOTP(K,C) = Truncate(HMAC\text{-}SHA\text{-}1(K,C)) \quad (3)$$

where K and C represent the shared secret and counter value.

The implementation of security for the mobile banking is based on HTTPs and REST protocols. The SecAnonymous application is a mobile secure way to establish connection between bank and customer. The bank identifies individually each customer by authentication and authorization, before granting access to the resources and the bank generated token acknowledge these steps.
The registration process involves the filling of a registration form on bank's website, demanding access to mobile banking application. The bank checks customer's request and grants him access to download link and sends an initial id and registration number by SMS. After the customer downloads the application on the mobile device a validation should be performed in order to check bank's integrity, by using the bank's public key and the application hash. The first use of the banking application will request to introduce in the form fields the ID and activation code emailed by bank. The user logins and is requested to choose 4-digit PIN.
The QR code or Quick Response code was originally designed for industrial applications and nowadays become one of the most important marketing strategy for selling products. Even QR codes were created in the 90's they become popular only few years ago and with the use of smartphone and tablets they are the quickest method of payment. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) [14].
A QR code can contain:

- the contact information;
- event information;
- data configuration.

Figure 1. Authentication process

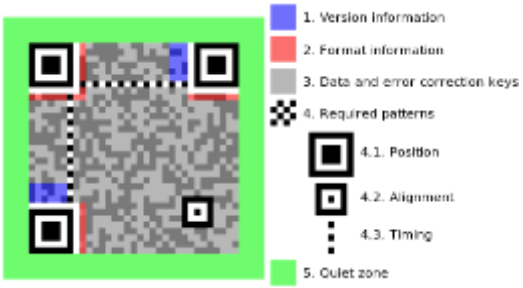

Figure 2. QR Code

QR code, compared to barcode, has some notable improvements:

- it is displayed on rows and columns, that makes it readable for any direction;
- can generate QR code from Kanji and Kana.

The popularity of QR codes has increased in such a way that people became more curious to know what is behind a QR code. Because of that, attackers become interested to create QR codes that are not linked with the information provided on panels and replaced the original QR code with those generated by them. In this way the QR code becomes vulnerability for the Android system, because behind the malicious QR code can be encoded a URL address which starts the download of a malicious application. The downloaded application can be a key logger [15] and there are many other methods used to inject JavaScript into the code, or install Trojans silently. The main risks are that after the malware is on the mobile, the attackers can access the messages stored on phone, turn on camera and most important to register conversations.

In order to avoid infringing QR codes, at the shopping market, the merchant generates in front of the client the code and signs it. The QR code contains the list of goods the client wants to buy.

4.2 Authentication

The mobile device creates a connection with the bank's server via HTTPs. Data transfer is made by a wireless network environment, thus the message must be encrypted. The message transferred to the server must be protected from eavesdroppers for this reason the user's bank account number is signed together with the message.

Authentication ensures that a person is that one that claims to be. To provide a satisfied level of protection there are some factors that have to be accomplished: the bank platform has to be a trusted one, with each user having its own credentials, the user's mobile device provides a good level of security, the mobile device has to enable the network connection.

The authentication process starts when the user wants to login by accessing the

ISSN 2067 – 4074

mobile banking application. The steps that take place in the authentication process are the following:

a. The client enters the username and PIN number.
b. A token password is generated.
c. The user must introduce the generated password in at least 30 seconds. If the time expires, the user can send a request to regenerate.
d. The bank's server verifies customer's identity. If the user name and PIN or the code is not the proper one, access is denied and the client is requested to reintroduce its credentials.
e. The access is granted if the server validation does not find irregularities.

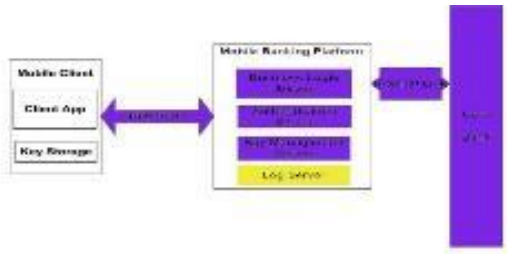

Figure 3. Authentication process.

4.3 Transactions

In order to buy goods from a store, without using a bank card, the customer will have the ability to utilize the smartphone he owns to initialize anonymous payments.

The transaction phase involves the anonymously transfer of money from user's account to merchant account. The transfer is done by the generating the bank code to the user smartphone. The code is generated using a transaction number combined with timestamp and credential parameters:

1) The user of a smartphone mobile baking system makes his market purchases as a customer, by adding each item in the physical shopping cart.
2) The seller scans each product, and introduces item by item in a list. From this list containing each item scanned and the total amount of money that the client owns to the bank is generated a QR code the attachment of the list.
3) The client scans the QR code, decodes the information stored in txt format, then signs the transaction and sends to the server of the bank for approval.
4) On client's mobile device the transaction has the state of pending. Meanwhile, the server of the bank receives the transaction with the message and its signature.
5) With client's public key, the bank verifies if the hash of the message it is the same as of that provided by the client.
6) The bank's server receives the request, checks the signed transaction with customer's public key and then verifies customer's account balance. There are two possibilities: if the user does not have enough money, the bank sends a message response rejecting the payment because of insufficient sold but if after the verification, the request is accepted as being true, bank withdraws the amount of money from user's account and generates a code tied to the account. This code represents the actual number of the transaction on which a timestamp is applied to ensure that money are not double spent and a client id to be stored by the merchant, in case of irregularities. The bank code is sent to the merchant.
7) The server of the bank will generate a temporary web address that contains the generated client id, the amount of money to be transferred to merchant's account. Once the transfer is made, the transaction changes it's state from pending to transaction done.
8) The merchant receives the code and accesses the web page sent by the server of the bank in order to credit their account.

The transaction contains the main fields are: id, timestamp, a hash generated by the account number and are paired with bank details. The merchant receives a code derived from the transaction, which he uses in order to get the payment. The code has as entries the transaction id, the paired hash, an id that can be used by the bank to associate with its clients. If the merchant has a complaint to address to

the bank he has to call the bank and send the code. Based on this code the bank contacts the client, makes an investigation and if the bank discovers any irregularities can provide client's details to the authorized institutions based on the policy and agreement established between bank and client.

5. Conclusion

The mobile user is able to connect in secure and in an anonymous manner. I proposed a secure architecture for two-party mobile payments. While other architectures and protocols have been proposed, they either are not well suited for mobile (and thus resource-constrained) devices or they do not satisfy all of the parties' concerns regarding security. In an anonymous payment the client's privacy is protected. It is an improved solution to card based payments because the user does not have to carry out for keeping all the time his card, the credentials are known only by bank and by the client, third parties are not implied in the process of receiving any direct link with client details, such as name, account and other information. The transaction made by client and merchant is composed of transaction id, timestamp and also some details that are retrieved from the user account.

Acknowledgement

Parts of this paper were presented at The 8th International Conference on Security for Information Technology and Communications (SECITC 2015), Bucharest, Romania, 11-12 June 2015.

References

[1] Consumers and mobile finacial, *Bord of governors of the federal reserve system*, pp. 6.[2]Tiwari, Rajnish and Buse, Stephan,The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector, 2007

[3] Fred Cheng,A Secure Mobile OTP Token, Mobilware, 2010.

[4]http://gizmodo.com/hackers-have-stolen-40-000-from-bitcoins-biggest-wall-1518184070

[5]http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf

[6] Sadiq Almuairfi, Prakash Veeraraghavan, Anonymous proximity mobile payment (APMP), Springer Science andBusiness Media New York 2012

[7] Constantin Popescu, An Anonymous Mobile Payment System Based on Bilinear Pairings, Institute of Mathematics and Informatics, Vilniu, 2009, pp 8.

[8] Bitcoin.org

[9] http://gizmodo.com/hackers-have-stolen-40-000-from-bitcoins-biggest-wall-1518184070

[10] Wiki.bitcoin.com

[11]http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5170848&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5170848

[12] http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

[13] Donal O'Mahony, Michael Peirce, Hitesh Tewari, Electronic payment systems for e-commerce, Artech House, 2001.

[14]http://www.qrcode.com/en/about/standards.html

[15]http://www.csoonline.com/article/2133890/mobile-security/the-dangers-of-qr-codes-for-security.html?page=2