A SECURE COMMUNICATION IN SMART PHONES USING TWO FACTOR AUTHENTICATIONS

Soumya Murali[1], Anitha .B[2], Anitha Mary Paul[3]

[1, 2, 3] Assistant Professor, [1, 2] Sree Buddha College of Engineering, Pattoor, Alappuzha, Kerala
[3]Adi Sankara Institute of Science and Technology, Kalady, Ernakulam, Kerala
Soumya4687@gmail.com, ianithaberny@gmail.com, anithamary@gmail.com

Abstract

Most secure systems face security attacks mainly at the client side. Two Factor Authentication (TFA) provides improved protection to the system at the client side by prompting to provide something they know and something they have. This system uses a one time password(OTP) generation method which doesn't require client-server communication, which frees the system from cost of sending a dynamic password each time the client wants to login. The OTP generation uses the factors that are unique to the user and is installed on a smart phone in Android platform owned by the user. An OTP is valid for a minutes time, after which, is useless. The system thus provides better client level security – a simple low cost method which protects system from hacking techniques like key logging, phishing, shoulder surfing, etc.

Keywords*—Authentication, OTP, key logging, phishing*

---***---

1. INTRODUCTION

Security is one of the major concerns of all organizations which uses online ways of communications especially banks. Of this, client side is most vulnerable to hacking, as the system cannot be completely closed when use over internet by a common client is to be allowed. Most systems use a static password –based authentication method which is easy to hack. There are various other authentication methods existing like cards, biometric identification, etc. These methods provide better security, but are not applicable to online client communication as these methods require special devices for their implementation. One possible method for applying a second factor of authentication for online access to the system is a dynamic password. Many systems have realized this on an SMS base, i.e. each time the server sends a one time password on client request, via sms.

Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. [1]

But this technique has several drawbacks, some of which are

1) SMS cost: On each request for login by the user, a sms is sent from the server. This will make it costly for the organization to provide online services to their clients.

2) Delivery delays: Due to network problems, delay may occur to the delivery of sms and when it is delivered it might have expired.

3) Security issues: Even though GSM was considered secure, it proved not to be, opening its doors to hackers. Thus sending the OTP as sms proved to be a bad idea.

Current technology uses TFA system.TFA uses a static password as one factor authentication and a one time dynamic password as second factor. The dynamic password generation here doesn't require a communication between server and client. Some organizations have realized this with a device which generates such an OTP, but carrying separate devices for each site we want to access, wherever we go is a bad idea. The system uses a smart phone working on Android platform which has software installed in it for OTP generation at the client side. The OTP is different for each minute, though it is generated using the same algorithm. The OTP is entered to login and the server runs the same OTP generation algorithm and matches this with the user entered OTP.

The method protects the system from attacks like key logging, shoulder surfing and phishing and various other issues in technique like sms based OTP.

2. RELATED WORKS

By definition, authentication is the use of one or more mechanisms to prove that you are who you claim to be. Once the identity of the human or machine is validated, access is granted.

Three universally recognized authentication factors exist today: what you know (e.g. passwords), what you have (e.g. ATM card or tokens), and what you are (e.g. biometrics).Recent work has been done in trying alternative factors such as a fourth factor, e.g. somebody you know, which is based on the notion of vouching.[4]

Two factor authentication [4] is a mechanism which implements two of the above mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. Withdrawing money from an ATM machine utilizes two factor authentication; the user must possess the ATM card, i.e. what you have, and must know a unique personal identification number (PIN), i.e. what you know.

Passwords are known to be one of the easiest targets of hackers. Therefore, most organizations are looking for more secure methods to protect their customers and employees. Biometrics are known to be very secure and are used in special organizations, but they are not used much in secure online transactions or ATM machines given the expensive hardware that is needed to identify the subject and the maintenance costs, etc. Instead, banks and companies are using tokens as a mean of two factor authentication.

Enhancing the level of security by using personal mobile devices is attracting attention due to the increasing number of users adopting mobile technologies. Security researchers have started to devise approaches that may increase the level of security in accessing critical information by end users through the employment of mobile devices [MvO07, MWL04, MPR06, OBDS04, PKP06, and WGM04]. [3]

A security token is a physical device that an authorized user of computer services is given to aid in authentication. It is also referred to as an authentication token or a cryptographic token. Tokens come in two formats: hardware and software. Hardware tokens are small devices which are small and can be conveniently carried. Some of these tokens store cryptographic keys or biometric data, while others display a PIN that changes with time. At any particular time when a user wishes to log-in, i.e. authenticate, he uses the PIN displayed on the token in addition to his normal account password. Software tokens are programs that run on computers and provide a PIN that changes with time. Such programs implement a One Time Password (OTP) algorithm. OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in the sequence. The sequence should be random to the maximum possible extent, unpredictable, and irreversible. Factors that can be used in OTP generation include names, time, seed, etc. Several commercial two factor authentication systems exist today such as BestBuy’s BesToken [8], RSA’s SecurID [8], and Secure Computing’s Safeword [9]. BesToken applies two-factor authentication through a smart card chip integrated USB token. It has a great deal of functionality by being able to both generate and store users’ information such as passwords, certificates and keys. SecurID from RSA uses a token (which could be hardware or software) whose internal clock is synchronized with the main server. Each token has a unique seed which is used to generate a pseudo-random number. This seed is loaded into the server upon purchase of the token and used to identify the user. An OTP is generated using the token every 60 seconds. The same process occurs at the server side. A user uses the OTP along with a PIN which only he knows to authenticate and is validated at the server side. If the OTP and PIN match, the user is authenticated [10].

Online banking requires strong user authentication. User authentication is often achieved by utilizing a two-factor authentication technique based on something the user knows, i.e., a static password, and something the user has, i.e., an OTP. The major advantage of involving a mobile phone is that most users already have mobile phones, and therefore no extra hardware token needs to be bought, deployed, or supported [2]

The idea of an OTP was first suggested by Leslie Lamport in the early 1980s. The OTP principle emphasizes that each time the user tries to log on, the algorithm produces pseudorandom output, thus improving the security. Thus, to avoid replay attack vulnerability, an OTP is a password that is only valid for a single login session or transaction. [2]

In 2005 the National Bank of Abu Dhabi (NBAD) became the first bank in the Middle East to implement two factor authentication using tokens. It employed the RSA SecurID solution and issued its 19000 customers small hardware tokens [5]. The National Bank of Dubai (NBD) made it compulsory for commercial customers to obtain tokens; as for personal customers the bank offered them the option to obtain the tokens [6]. In 2005, Bank of America also began providing two factor authentication for its 14 million customers by offering hardware tokens. Many international banks also opted to provide their users with tokens for additional security, such as Bank of Queensland, the Commonwealth Bank of Australia and the Bank of Ireland.[7]

3. DESIGN AND IMPLEMENTATION

The OTP concept is implemented in a banking system. The system is designed to have four main modules.

1) Administrator module
2) Server module
3) Client module
4) Mobile module

Administrator module consists of a group of users. These users have access to the system under different privileges. The administrator module has different levels of user accounts for various staff of the bank. This includes an administrator account and other accounts which provide access to the desktop application different levels of staff in the bank. This is a closed system in which no access from website is possible. Server module works when a request is given from the website for login. When username and password is entered by the user and login button is pressed, a request is sent to the server. In the server, the OTP generation algorithm is run on the receipt of a request. Generated OTP is matched with the user entered OTP. Only if both OTPs are the same, a positive acknowledgement is given to the website and leads to the next page where server password is displayed. The user can check if the server password from the website and that on the phone matches and then only enter his/her actual password.

Client module is the web side of the system. Client is given an account name and password for this purpose. When client enters the username and correct OTP, it leads to the next page where the client password has to be entered. If this is also correct, user home page is reached. Here the client can view his account details, past transactions, balance, etc. and also transfer cash from his account to other accounts.

Mobile module is an application installed in the client's smart phone. It is protected using application password. This password can be set by the client. Once the client gives correct password, he enters the application and is asked for username and password. The user name and password is received and an OTP is generated using this username and password the server password generated along with OTP is used to manually validate the website. Android platform is preferred for smart phone because of its growing popularity, increasing usage and its open source nature.

The first three modules works by accessing the database in which the info regarding the bank and its services is started as tables each user is given a certain privilege of access according to their designations to provide security. A database is needed on the server side to store the client's identification information such as the first name, last name, username, pin, password, mobile IMEI number, IMSI number, unique symmetric key, and the mobile telephone number for each user. The password field will store the hash of the 10 minute password. It will not store the password itself. Should the database be compromised the hashes cannot be reversed in order to get the passwords used to generate those hashes. Hence, the OTP algorithm will not be traced.

In order to setup the database, the client must register in person at the organization. The client's mobile phone/SIM card identification factors, e.g. IMEI/IMSI, are retrieved and stored in the database, in addition to the username and PIN. The Android OTP generating software is installed on the mobile phone. The software is configured to connect to the server's GSM modem in case the SMS option is used. A unique symmetric key is also generated and installed on both the mobile phone and server. Both parties are ready to generate the OTP at that point.

3.1 OTP Algorithm

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it's very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. The OTP algorithm uses many factors which are hard to guess or retrieve by hackers, so that the system is most secure. The chosen factors are made to available in the server also, so that the same password is generated in both the server and mobile. The factors that can be considered include:

IMEI number (international mobile equipment identity) which is unique to each mobile phone and hence to the owner of that phone. This is accessible on the mobile phone and is saved in the server.

IMSI number (International mobile subscriber identity) is a unique number associated with all GSM and universal mobile telecommunication system (UMTS) network mobile phone users. It is stored in the SIM card in the mobile phone. This is also saved in the server

Username: The mobile identifying factors like IMEI and IMSI numbers provide uniqueness to the OTP, but in case the mobile is stolen, these can be retrieved by others. For an additional security, OTP generation uses the username and PIN number as well.

PIN serves the purpose of a password. Only the user will know the PIN and hence serves as a private key in the OTP generation.

Hour: This makes the OTP for each hour unique.

Minute: This would make the OTP generated in each minute to be unique; hence the OTP will be valid only for one minute. Another option is to take only the digit at the ten's place of the minute so that an OTP will be valid for ten minutes.

Day: This makes the OTP unique for each day of the week.

Year/Month/Date: Using date information like year, month and date makes the OTP unique for a particular date.

The time in the mobile should be synchronized with the time in the server in order to get the correct OTP in both sides.

The basic idea of the algorithm is to concatenate the required factors from the above mentioned factors into a string and then convert it into a hex string using suitable conversion, divide it into two halves and XOR the halves. The division of the resultant string of hex values and XOR-ing the halves is repeatedly performed till the obtained result has the desired length. The system repeats the process till a specific number of digits is attained, first half of which serves as the OTP which is used for log in process and the second half as server password used in validating the website. The method of generating OTP can vary from this procedure. The advantage of this procedure is that even a slight change in the procedure will make it difficult to trace out back what have been done even though the hackers get the OTP.

<u>Skelton OTP generation algorithm</u>

1. The factors IMEI number, username, password, time (hour and minute), date are concatenated.

2. This string is passed to an encryption code where the ASCII value of the string is found.

3. Length of the string is appended with the value obtained in step 2.

4. Convert this string to a hex code.

5. This hex code is divided into 2 halves.

6. XOR the halved hex codes.

7. Repeat steps 5 and 6 until we get a 5 digit OTP code.

8. Hence unique password is obtained.

4. ADVANTAGES

The system has many advantages over other systems. Some of them are listed below:

1. Provides better security than one factor authentication methods
2. When compared to other two-factor authentication methods, an OTP based two-factor authentication proved easier and hard to guess password in textual format which is also less expensive.
3. This method overcame the drawbacks of SMS based OTP method. Issues like SMS delays, message lose in network, SMS cost, etc were not raised in this new OTP generation method
4. Switching the application from a separate device to the form of software in smart phones frees the client from carrying such separate devices provided by each organization.
5. There was no need to keep any extra database space to realize this OTP. i.e., there was no space overhead, unlike picture or audio passwords.
6. No additional devices were required to realize this as in biometric identification techniques.

5. DISADVANTAGES

1. Not as much safe when compared to graphical passwords.
2. Once the technique is found out, it will be easy to find out all the OTPs.
3. Proper time synchronization is necessary for correct working of the system.
4. User need to have a smart phone in order to use this facility.

CONCLUSIONS

Today, single factor authentication, e.g. passwords, is no longer considered secure in the internet and banking world. Easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs. Two factor authentication has recently been introduced to meet the demand of organizations for providing stronger authentication options to its users. In most cases, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is becoming a burden on both the client and organization. Since many clients carry a mobile phone today at all times, an alternative is to install all the software tokens on the mobile phone. This will help reduce the manufacturing costs and the number of devices carried by the client.

The system proved better than many previously existed systems. The OTP based two factor authentication system using a connectionless generation technique was found efficient than many other existing techniques when factors like storage space, time, etc were considered. All that is required for this purpose is a smart phone with a simple application installed in it. As phone is a common device used by almost all common people today, this technique will not require much effort for its implementation. The system proved to be protected from normal kind of attacks like hishing, key-logging, shoulder surfing, etc. The OTP generated each time was unique so that one OTP was not usable the next minute.

FUTURE WORK

Future works include developing an OTP generating application which can work on other phones as well so that all users can make use of the feature. Another work is to give this OTP a graphical face so that it becomes harder to decipher by the hackers. Also a more user friendly GUI and extending the algorithm to work on Blackberry, Palm, and Windows-based mobile phones can be included. In addition to the use of Bluetooth and WLAN features on mobile phones for better security and cheaper OTP generation.

REFERENCES

[1]Two Factor Authentication Using Mobile Phones[Fadi Aloul, Syed Zahidi, Wassim El-Hajj]
[2]OTP-Based Two-Factor Authentication Using Mobile Phones[Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan]
[3]A Two-Factor Authentication Using Mobile Phones[Nima Kaviani, Kirstie Hawkey, Konstantin Beznsov]
[4]N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services," Communications of the ACM, 47(8), 42-46, May 2004.
[5]A. Herzberg, "Payments and Banking with Mobile Personal Devices," Communications of the ACM, 46(5), 53-58, May 2003.
[6]"RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005.
[7]D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005.
[8]SMSLib. Available at http://smslib.org/
[9]Aladdin Secure SafeWord 2008. Available at http://www. securecomputing.com/index.cfm?skey=1713
[10]J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth- Factor Authentication: Somebody You Know," ACM CCS, 168-78. 2006.