World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 155-159, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2250

Extra Authentication in ATM Using Bluetooth

K.P. Thooyamani, R. Udayakumar and V. Khanaa

School of Computing Science, Bharath University, Chennai-73, India

Abstract: This paper deals with the authentication mechanisms in ATM that is done in two unique stages using Bluetooth. Two factor authentication is the mechanism of using two authentication to make it secure than one factor authentication. Here an innovative Bluetooth based mechanism is used to replace the existing hardware or biometric applications. Here a dynamic password generation is used to generate an one time password which is to authenticate a user. Transferring message via INTRANET and Bluetooth overcomes the flaws in the traditional GSM based message transfer mechanism

Key words: WAP · GPS · GPRS · Tokens · Static · GSM

INTRODUCTION

Today security concerns are on the rise in all areas such as banks, governmental applications, healthcare, industry, military organization, educational institutions, etc. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. Most systems today rely on static passwords to verify the 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. Several strategies for using passwords have been proposed [1]. Some of which are very difficult to use and others might not meet the security concerns.

Two factor authentication using devices such as tokens and ATM cards have been proposed to solve the password problem and have shown to be difficult to hack. Two factor authentications also have disadvantages which include the cost of purchasing, issuing and managing the tokens or cards. From the customer point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen. Mobile phones have traditionally been regarded as a tool for making phone calls. But today, given the advances in hardware and software, mobile phones use have been expanded to send messages, check emails, store contacts, etc. Mobile connectivity options have also increased [8] [9]. After standard GSM connections, mobile phones now have infra- red, Bluetooth, 3G and WLAN connectivity. Most of us, if not all of us, carry mobile phones for communication purpose. Several mobile banking services available take advantage of the improving capabilities of mobile devices. From being able to receive information on account balances in the form of SMS messages to using WAP and Java together with GPRS to allow fund transfers between accounts, stock trading and confirmation of direct payments via the phone's micro browser [12]. Installing both vendor-specific and third party applications allow mobile phones to provide expanded new services other than communication.

Consequently, using the mobile phone as a token will make it easier for the customer to deal with multiple two factor authentication systems; in addition it will reduce the cost of manufacturing, distributing and maintaining millions of tokens. In this paper, we propose and develop a complete two factor authentication system using mobile phones instead of tokens or cards. The system consists of a server connected to a GSM

Corresponding Author: K.P. Thooyamani, School of Computing Science, Bharath University, Chennai-73, India.

modem and a mobile phone client running a J2ME application. Two modes of operation are available for the users based on their preference and constraints. The first is a stand-alone approach that is easy to use, secure and cheap. The second approach is an SMS-based approach that is also easy to use and secure, but more expensive. The system has been implemented and tested. In the next section we provide a general background about authentication factors and existing two factor authentication systems. Section III describes the proposed system, the OTP algorithm, client, server and the database. Section IV provides results of testing the system. Section V concludes the paper and provides future work.

Background: 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 [10]. *Two factor authentications* [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 authentications; 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. 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 those 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 [11], RSA's SecurID [14] and Secure Computing's Safeword [2]. 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 user's information such as passwords, certificates and keys. One application is to use it to log into laptops. In this case, the user has to enter a password while the USB token is plugged to the laptop at the time of the login. A hacker must compromise both the USB and the user account password to log into the laptop. 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 [8]. In services such as ecommerce, a great deal of time and money is put into countering possible threats and it has been pointed out that both the client and the server as well as the channel of communication between them is imperative [1]. 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 [7, 14].

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 [11]. In 2005, Bank of America also began providing two factor authentications for its 14 million customers by offering hardware tokens [5]. 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 [3]. Using tokens involves several steps including registration of users, token production and distribution, user and token authentication and user and token revocation among others [6]. While tokens provide a much safer environment for users, it can be very costly for organizations.

For example, a bank with a million customers will have to purchase, install and maintain a million tokens. Furthermore, the bank has to provide continuous support for training customers on how to use the tokens. The banks have to also be ready to provide replacements if a token breaks or gets stolen. Replacing a token is a lot more expensive than replacing an ATM card or resetting a password [17]. From the customer's prospective, having an account with more than one bank means the need to carry and maintain several tokens which constitute a big inconvenience and can lead to tokens being lost, stolen, or broken. In many cases, the customers are charged for each token. We propose a mobile-based software token that will save the organizations the cost of purchasing and maintaining the hardware tokens [16]. Furthermore, will allow customers to install multiple software tokens on their mobile phones. Hence, they will only worry about their mobile phones instead of worrying about several hardware tokens.

Proposed System: In our project we propose a innovative blue tooth based software token mechanism to replace the existing hardware token or biometric devices. Our system has three main parts namely software installed on mobile, server software and a Bluetooth device on ATM machine and user mobile Bluetooth mobile device. The main disadvantages of using traditional GSM is that Traditional GSM based message transfer mechanism has Latency in message delivery, Tower reliability and Cost of messaging service. The main flexibility of Bluetooth is in current technological advancement, Bluetooth has a huge scope in various fields. No new technology can ignore the use of Bluetooth.The international market of Bluetooth mobile phones is growing early at an average of 35%. In current world market there are 100 million Bluetooth mobiles.

Architecture: When the ATM card is swiped in the machine, it asks for a static password from the user. After verifying the first authentication, the server present in the bank validates the pin and generates a One Time Password (OTP) using the OTP algorithm with the parameters such as IMEI number, IMSI number etc...Then the remote user enters the Password.

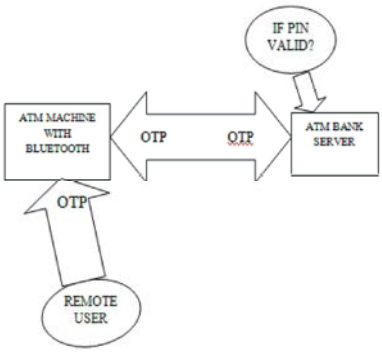

Fig. 1 Architectural Diagram

Dynamic OTP: In our project dynamic password generation is used to generate an one time password which is to authenticate a user. When the remote user authenticates himself using his PIN NUMBER ,the server runs a dynamic password generation n program to generate a otp which is encrypted using symmetric encryption and sent to the remote user via the intranet and the Bluetooth. The criteria for developing using symmetric encryption and sent to the remote user via the intranet and the Bluetooth. The criteria for developing OTP are synchronous, efficient and disposable.

OTP Algorithm: In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it is 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.

Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micropayments [9]. Note that these factors must exist on both the mobile phone and server in order for both sides to generate the same password. In the proposed design, the following factors were chosen:

IMEI Number: The term stands for International Mobile Equipment Identity which is unique to each mobile phone allowing each user to be identified by his device. This is accessible on the mobile phone and will be stored in the server's database for each client.

IMSI Number: The term stands for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the Subscriber Identity Module (SIM) card in the mobile phone. This number will also be stored in the server's database for each client.

Username: Although no longer required because the IMEI will uniquely identify the user anyway. This is used together with the PIN to protect the user in case the mobile phone is stolen.

PIN: This is required to verify that no one other than the user is using the phone to generate the user's OTP. The PIN together with the username is data that only the user knows so even if the mobile phone is stolen the OTP cannot be generated correctly without knowing the user's PIN. Note that the username and the PIN are never stored in the mobile's memory. They are just used to generate the OTP and discarded immediately after that. In order for the PIN to be hard to guess or brute-forced by the hacker, a minimum of 8-characters long PIN is requested with a mixture of upper- and lower-case characters, digits and symbols.

Hour: This allows the OTP generated each hour to be unique.

Minute: This would make the OTP generated each minute to be unique; hence the OTP would be valid for one minute only and might be inconvenient to the user. An alternative solution is to only use the first digit of the minute which will make the password valid for ten minutes and will be more convenient for the users, since some users need more than a minute to read and enter the OTP. Note that the software can modified to allow the administrators to select their preferred OTP validity interval.

Day: Makes the OTP set unique to each day of the week.

Year/Month/Date: Using the last two digits of the year and the date and month makes the OTP unique for that particular date.

The time is retrieved by the client and server from the telecommunication company. This will ensure the correct time synchronization between both sides. The above factors are concatenated and the result is hashed using SHA-256 which returns a 256 bit message. The message is then XOR-ed with the PIN replicated to 256 characters. The result is then Base64 encoded which yields a 28 character message. The message is then shrunk to an administrator-specified length by breaking it into two halves and XOR-ing the two halves repeatedly. This process results in a password that is unique for a ten minute interval for a specific user. Keeping the password at 28 characters is more secure but more difficult to use by the client, since the user must enter all 28 characters to the online webpage or ATM machine. The shorter the OTP message the easier it is for the user, but also the easier it is to be hacked. The proposed system gives the administrator the advantage of selecting the password's length based on his preference and security needs.

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.

This paper focuses on the implementation of two-factor authentication methods using mobile phones. It provides the reader with an overview of the various parts of the system and the capabilities of the system. The proposed system has two option of running, either using a free and fast *connection-less* method or a slightly more expensive *SMSbased* method. Both methods have been successfully implemented and tested and shown to be robust and secure. The system has several factors that makes it difficult to hack. Future developments include a more user friendly GUI and extending the algorithm to work on Blackberry, Palm and Windows-based mobile phones. In addition to the use of Bluetooth and WLAN features on mobile phones for better security and cheaper OTP generation.

REFERENCES

1. Jøsang, A. and G. Sanderud, 2003. "Security in Mobile Communications: Challenges and Opportunities," in Proc. of the Australasian information security workshop conference on ACSW frontiers, pp: 43-48.
2. Aladdin Secure SafeWord 2008. Available at http://www. securecomputing.com/index.cfm?skey =1713.

3. A. Medrano, "Online Banking Security – Layers of Protection," Available at http://ezinearticles.com/ ?Online-Banking-Security---Layers-of-Protection &id=1353184
4. Schneier, B., 2005. "Two-Factor Authentication: Too Little, Too Late," in Inside Risks 178, *Communications of the ACM*, 48(4).
5. Ilett, D., 2005. "US Bank Gives Two-Factor Authentication to Millions of Customers,". Available at http://www.silicon.com/ financialservices/ 0,3800010322,39153981,00.htm.
6. Borde De D., 2008. "Two-Factor Authentication," Siemens Enterprise Communications UK- Security Solutions, Available at http://www.insight.co.uk/ files/whitepapers/Twofactor%20authentication%20 (White%20paper).pdf.
7. Herzberg, A., 2003. "Payments and Banking with Mobile Personal Devices," Communications of the ACM, 46(5): 53-58.
8. Brainard, J., A. Juels, R.L. Rivest, M. Szydlo and M. Yung, 2006. "Fourth- Factor Authentication: Somebody You Know," *ACM CCS*, 168-78.
9. NBD Online Token. Available at http://www. nbd.com/NBD/ NBD_CDA/CDA_Web_pages/ Internet_Banking/nbdonline_topbanner.
10. Mallat, N., M. Rossi and V. Tuunainen, 2004. "Mobile Banking Services," Communications of the ACM, 47(8): 42-46.
11. "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005. Available at http://www.rsa.com/press_release. aspx?id =6092
12. Groom, R., 0000. "Two Factor Authent ication Using BESTOKEN Pro USB Token." Available at http:// bizsecurity.about.com/d/mobilesecurity/a/ twofactor.htm
13. Sha4J.Availableat http://www.softabar.com/home/ content/view/46/68/
14. SMSLib. Available at http://smslib.org/
15. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013, Images segmentation via Gradient watershed hierarchies and Fast region merging, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12), pp.1680-1683
16. Thooyamani, K.P., V. Khanaa and R.Udayakumar , 2013, Online answerback and reply-voice recording , Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12):.1861-1865.
17. Udayakumar, R., V. Khanna, T. Saravanan, G. Saritha, 2013, Cross Layer Optimization For Wireless Network (Wimax), Middle-East Journal of Scientific Research, ISSN:1990-9233, 16(12):.1786-1789.