IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Preventing Password Reuse and Stealing Attack Using Onetime Password And Iris Technology

Indu S.[*1], Saravana Kumar[2], M.Ramesh Kumar[3]

[*1,2,3] Vel Tech Multitech Dr.Rangarajan Dr.Sakunthala Engg College, India

induspt@gmail.com

Abstract

A secure network partially depends on user authentication and unfortunately authentication schemes used at present are not utterly secure. Most of the systems today rely on static passwords to verify the user's identity. This paper describes a method of implementing two factor authentication using mobile phones. The proposed system involves using a mobile phone as a software token for One Time Password generation. OTP algorithm powered with user's unique identifications like International Mobile Equipment Identification and Subscriber Identification Module; makes a finite alphanumeric token valid for a session and for a single use. The generated One Time Password is valid for only a short user defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization.

Keywords: One Time Password (OTP), Personal Identification Number(PIN),Short Message Service(SMS)..

Introduction

Security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions,etc. Most of the 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. Government organizations are setting standards, passing laws and forcing being met with organizations and agencies to comply with these standards with non-compliance 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. 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 'proper' strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's 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's 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. 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 fund transfers between accounts, stock trading, and WAP and Java together with GPRS to allow confirmation of direct payments via the phone's micro browser .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, 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 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.

oPass presents the following advantages.

1) Anti-malware—Malware (e.g., keylogger) that gather sensitive information from users, especially their passwords

are surprisingly common. In oPass, users are able to log into web services without entering passwords on their computers.

Thus, malware cannot obtain a user's password from untrusted computers.

2) Phishing Protection—Adversaries often launch phishing

attacks to steal users' passwords by cheating users when they connect to forged websites. As mentioned above, oPass allows users to successfully log into websites without revealing passwords to computers. Users who adopt oPass are guaranteed to withstand phishing attacks.

3) Secure Registration and Recovery—In oPass, SMS is an Out-of-band communication interface. OPass cooperates with the telecommunication service provider (TSP) in order to obtain the correct phone numbers of websites and users respectively. SMS aids oPass in establishing a secure channel for message exchange in the registration and recovery phases. Recovery phase is designed to deal with cases where a user loses his cell phone. With the aid of new SIM cards, oPass still works on new cell phones.

4) Password Reuse Prevention and Weak Password Avoidance—oPass achieves one-time password approach. The cell phone automatically derives different passwords for

each login. That is to say, the password is different during

each login. Under this approach, users do not need to remember any password for login. They only keep a long term password for accessing their cell phones, and leave the rest of the work to oPass.

5) Cell phone Protection—An adversary can steal users' cell phones and try to pass through user authentication. However, the cell phones are protected by a long-term password. The adversary cannot impersonate a legal user to login without being detected.

Background

oPass adopts the one-time password strategy; therefore, the strategy is given later. We also describe the secure features of SMS channel and explain why SMS can be trusted. Finally, introduce the security of 3G connection used in the registration and recovery phases of oPass.

A. One-Time Password

The one-time passwords in oPass are generated by a secure one-way hash function. With a given input, the set of onetime passwords is established by a hash chain through multiple hashing. Assuming we wish to prepare one-time passwords, the first of these passwords is produced by performing hashes on input. The next one-time password is obtained by performing hashes. For security reasons, we use these one-time passwords in reverse order, i.e., using, then. If an old one-time password is leaked, the attacker is unable to derive the next one. In other words, she cannot impersonate a legal user without the secret shared credential. Besides, the input is derived from a long-term password, the identity of server ID , and a random seed generated by the server ID .Note that function is a hash which is irreversible in general cryptographic assumption. In practice, is realized by SHA-256 in oPass. Therefore, the bit length of is 256.

B. SMS Channel

SMS is a text-based communication service of telecommunication systems. OPass leverages SMS to construct a secure user authentication protocol against password stealing attacks. As we know, SMS is a fundamental service of telecom, which belongs to 3GPP standards. SMS represents the most successful data transmission of telecom systems; hence, it is the most widespread mobile service in the world. Besides the above advantages chose SMS channel because of its security benefits. Compared with TCP/IP network, the SMS network is a closed platform; hence, it increases the difficulty of internal attacks, .g., tampering and manipulating attacks. Therefore, SMS is an out-of-band channel that protects the exchange of messages between users and servers. Unlike conventional authentication protocols, users securely transfer sensitive messages to servers without relying on untrusted kiosks. OPass resists password stealing attacks since it is based on SMS channels.

C. 3G Connection

3G connection provides data confidentiality of user data and signal data to prevent eavesdropping attacks. It also provides data integrity of signal data to avoid tampering attacks. The confidentiality and

integrity algorithms are f8 and f9, respectively. Algorithm f8 and f9 are based on a block cipher named KASUMI where f8 is a synchronous binary stream cipher and f9 is a MAC algorithm. OPass utilizes the security features of 3G connection to develop the convenient account registration and recovery procedures. Users can securely transmit and receive information to the web site through a 3G connection

Architecture of oPass

1) Each web server possesses a unique phone number. Via the phone number, users can interact with each website through an SMS channel.
2) The users' cell phones are malware-free. Hence, users can safely input the long-term passwords into cell phones.
3) The telecommunication service provider (TSP) will participate in the registration and recovery phases. The TSP is a bridge between subscribers and web servers. It provides a service for subscribers to perform the registration and recovery progress with each web service. For example, a subscriber inputs her id ID and a web server's id ID to start to execute the registration phase. Then, the TSP forwards
the request and the subscriber's phone number to the corresponding web server based on the received ID .Subscribers (i.e., users) connect to the TSP via 3G connections to protect the transmission. The TSP and the web server establish a secure sockets layer (SSL) tunnel. Via SSL protocol, the TSP can verify the server by its certificate to prevent phishing attacks. With the aid of TSP, the server can receive the correct sent from the subscriber.

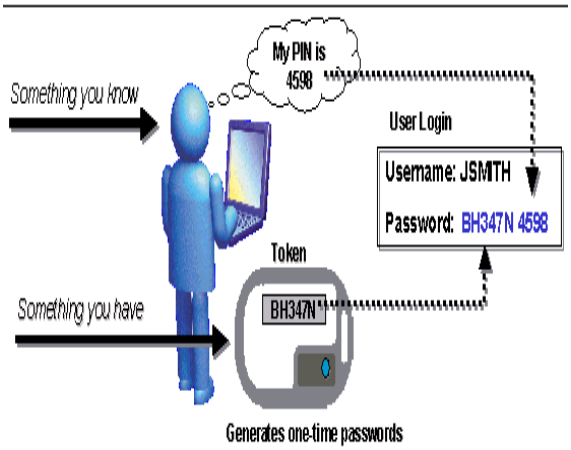

Fig 1.Architecture Diagram of Onetime Password

oPass consists of *registration*, *login*, and *recovery* phases.

A. Overview

Unlike generic web logins, oPass utilizes a user's cell phone as an authentication token and SMS as a secure channel. Different from regular login processes, additional steps are required for oPass and are marked in back rectangles in. In the *registration* phase, a user starts the oPass program to register her new account on the website she wishes to visit in the future. Unlike conventional registration, the server requests for the user's account id and phone number, instead of password. After filling out the registration form, the program asks the user to setup a long-term password. This long-term password is used to generate a chain of one-time passwords for further logins on the target server. Then, the program automatically sends a registration SMS message to the server for completing the registration procedure. The context of the registration SMS is encrypted to provide data confidentiality. OPass also designed a *recovery* phase to fix problems in some conditions, such as losing one's cell phone. Contrasting with general cases, *login* procedure in oPass does not require users to type passwords into an untrusted web browser. The user name is the only information input to the browser. Next, the user opens the oPass program on her phone and enters the long-term password; the program will generate a one-time password and send a login SMS securely to the server. The login SMS is encrypted by the one-time password. Finally, the cell phone receives a response message from the server and shows a success message on her screen if the server is able to verify her identity. The message is used to ensure that the website is a legal website, and not a phishing one. Protocol details of each phase are provided as follows.

B. Registration Phase

The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins by opening the oPass program installed on her cell phone. She enters ID (account id she prefers) and ID (usually the website url or domain name) to the program. The mobile program sends ID and ID to the telecommunication service provider (TSP) through a 3G connection to make a request of registration. Once the TSP received the ID and the ID , it can trace the user's phone number based on user's SIM card. The TSP also plays the role of third-party to distribute a shared key between the user and the server. The shared key is used to encrypt the registration SMS with AES-CBC. The TSP and the server will establish an SSL tunnel to protect the communication. Then the TSP forwards ID, and to the assigned server. Server will generate the corresponding information for this account and reply a response, including server's identity ID ,a random seed , and server's phone number . The TSP then forwards ID, and a shared key to the user's cell

phone. Once reception of the response is finished, the user continues to setup a long-term password with her cell phone. The cell phone computes a secret credential by the following Operation.

C. Login Phase

The *login* phase begins when the user sends a request to the server through an untrusted browser (on a kiosk). The user uses her cell phone to produce a one-time password, e.g., , and deliver necessary information encrypted with to server via an SMS message. Based on pre shared secret credential, server can verify and authenticate user based on. The protocol starts when user wishes to log into her favorite web server (already registered). However, begins the login procedure by accessing the desired website via a browser on an untrusted kiosk. The browser sends a request to with*'s* account ID. Next, server supplies the ID and a fresh nonce to the browser. Meanwhile, this message is forwarded to the cell phone through blue tooth or wireless interfaces. After reception of the message, the cell phone inquires related information from its database via ID, which includes server's phone number and other parameters. The next step is promoting a dialog for her long-term password. Secret shared credential can regenerate by inputting the correct on the cell phone.

D. Recovery Phase

Recovery phase is designated for some specific conditions; for example, a user may lose her cell phone. The protocol is able to recover oPass setting on her new cell phone assuming she still uses the same phone number (apply a new SIM card with old phone number).Once user installs the oPass program on her new cell phone, she can launch the program to send a recovery request with her account ID and requested server ID to predefined TSP through a 3G connection. As we mentioned before, ID can be the domain name or URL link of server. Similar to registration, TSP can trace her phone number based on her SIM card and forward her account ID and the to server through an SSL tunnel. Once server receives the request, probes the account information in its database to confirm if account is registered or not. If account ID exists, the information used to compute the secret credential will be fetched and be sent back to the user. The server generates a fresh nonce and replies a message which consists of ID and this message includes all necessary elements for generating the next one-time passwords to the user. When the mobile program receives the message, like registration, it forces the user to enter her long-term password to reproduce the correct one-time password (assuming the last successful login before lost her cell phone is). During the last step, the user's cell phone encrypts the secret credential and server nonce to a cipher text. The recovery SMS message is delivered back to the server for checking. Similarly, the server computes and decrypts this message to ensure that user is already recovered. At this point, her new cell phone is recovered and ready to perform further logins. For the next login, one-time password will be used for user authentication.

System Testing

The server was implemented using Java. A Siemens MC35i GSM modem was used for sending and receiving SMS messages on the server side. The smslib3.2.0 library was used to send the messages and the SHA 4j library was used to hash the password. An Oracle 10g was used as a database. The client was implemented using J2ME and installed on a Nokia E60 and Nokia E61 phone. Both methods, the connection-less and SMS-based, were tested. In the first method, fake user accounts were setup on both the mobile phone and server. The mobile phone was used to generate 5000 random OTPs at various times of the day and all 5000 generated OTPs matched the OTPs generated on the server side. The use of date and time from the telecommunication company helped solve the synchronization problem. Furthermore, using the first digit of the minute gave the user enough time, i.e. 10 minutes, to compute, read, enter, and send the OTP. The second SMS-based method was also tested. Once the client requests an OTP via an SMS, the server would check the user credentials, generate the OTP, and send it back instantly.

IRIS Recognition

The process of capturing an iris into a biometric template is made up of 3 steps:

1. Capturing the image
2. Defining the location of the iris and optimizing the image
3. Storing and comparing the image.

1. Capturing the Image

The image of the iris can be captured using a standard camera using both visible and infrared light and may be either a manual or automated procedure. The camera can be positioned between three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the iris in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. The automatic procedure uses a set of cameras that locate the face and iris automatically thus making this process much more user friendly.

2. Defining the Location of the Iris and Optimizing the Image.

Once the camera has located the eye, the iris recognition system then identifies the image that has the best focus and clarity of the iris. The image is then analyzed to identify the outer boundary of the iris where it meets the white sclera of the eye, the pupillary boundary and the centre of the pupil. This results in the precise location of the circular iris. The iris recognition system then identifies the areas of the iris Image that are suitable for feature extraction and analysis. This involves removing areas that are covered by the eyelids, any deep shadows and reflective areas. The following diagram shows the optimization of the image.

3. Storing and Comparing the Image

Once the image has been captured, "an algorithm uses 2-D Gabor wavelets to filter and map segments of the iris into hundreds of vectors (known here as phasors)"9. The 2-D Gabor phasor is simply the "what" and "where" of the image. Even after applying the algorithms to the iris image
there are still 173 degrees of freedom to identify the iris. These algorithms also take into account the changes that can occur with an iris, for example the pupil's expansion and contraction in response to light will stretch and skew the iris. This information is used to produce what is known as the Iris Code®, which is a 512-byte record. This record is then stored in a database for future comparison. When a comparison is required the same process is followed but instead of storing the record it is compared to all the Iris Code® records stored in the database. The comparison also doesn't actually compare the image of the iris but rather compares the hexadecimal value produced after the algorithms have been applied. In order to compare the stored Iris Code® record with an image just scanned, a calculation of the Hamming Distance is required.

The Hamming Distance is a measure of the variation between the Iris Code® record for the current iris and the Iris Code® records stored in the database. Each of the 2048 bits is compared against each other, i.e. bit 1 from the current Iris Code® and bit 1 from the stored Iris Code® record are compared, then bit 2 and so on. Any bits that don't match are assigned a value of one and bits that do match a value of zero. Once all the bits have been compared, the number of non-matching bits is divided by the total number of bits to produce a two-digit figure of how the two Iris Code® records differ.

IRIS Recognition Based on Sift Features

The Scale Invariant Feature Transformation (SIFT) is using for biometric recognition using iris images. SIFT extracts repeatable characteristic feature points from an image and generates descriptors describing the texture around the feature points. The SIFT technique has already demonstrated its efficacy in other generic object recognition problems, and it has been recently proposed for its use in biometric recognition systems based on face, fingerprint and iris images. One of the advantages of the SIFT approach is that it does not need transfer to polar coordinates. We have used for our experiments the BioSec multimodal baseline corpus which includes 3,200 iris images from 200 individuals acquired in two different sessions.

Furthermore, since the SIFT technique does not require polar transformation or highly accurate segmentation, and it is invariant to changes in illumination, scale and rotation, it is hoped that this technique will be feasible with unconstrained image acquisition conditions. One of the major current practical limitations of iris biometrics is the degree of cooperation required on the part of the person whose image is to be acquired. All existing commercial iris biometrics systems still have constrained image acquisition conditions. Current efforts are aimed at acquiring images in a more flexible manner and/or being able to use images of more widely varying quality, e.g. the "Iris on the Move" project, which is aimed to acquire iris images as a person walks at normal speed through an access control point such as those common at airports. This kind of systems would drastically reduce the need of user's cooperation, achieving transparent and low-intrusive biometric systems, with a higher degree of acceptance among users.

Scale Invariant Feature Transformation (SIFT) was Originally developed for general purpose object recognition.

SIFT detects stable feature points of an object such that the same object can be recognized with invariance to illumination, scale, rotation and affine transformations. A brief description of the steps of the SIFT operator and their use in iris recognition is given next.

A. Scale-space local extrema detection

The first step is to construct a Gaussian is done by convolving a variable scale 2D Gaussian operator G (x, y, a) with the input image I (x, y):

$$L(x, y,O')=G(x,y,O')*I(x,y)$$

Difference of Gaussian (DoG) images D (x, y, a) are then Obtained by subtracting subsequent scales in each octave:

$$D (x, y,O') = L (x, y, kO') - L (x, y,O')$$

where k is a constant multiplicative factor in scale space. The set of Gaussian-smoothed images and DoG images are called an octave. A set of such octaves is constructed by successively down sampling the original image. Each octave
(i.e., doubling of a) is divided into an integer number 8 of scales, so k = 21/8• we must produce 8+3 images

for each octave, so that the final extrema detection covers a complete Octave. In this paper we have used 8=3, thus producing six Gaussian-smoothed images and five DOG images per octave, and a value of 0'=1.6 Local extrema are then detected by observing each image point in D (x, y, a) . A point is decided as a local minimum or maximum when its value is smaller or larger than all its surrounding neighboring points. Each sample point in D (x, y, a) is compared to its eight neighbors in the current image and nine neighbors in the scale above and below.

B. Accurate Keypoint Localization

Once a key point candidate has been found, if it observed to have low contrast (and is therefore sensitive to noise) or if it is poorly localized along an edge, it is removed because it cannot be reliably detected again with small variation of viewpoint or lighting changes. Two thresholds are used, one to exclude low contrast points and other to exclude edge points. More detailed description of this process can be found in the original paper by Lowe.

C. Orientation assignment

An orientation histogram is formed from the gradient orientations within a 16 x 16 region around each key point. The orientation histogram has 36 bins covering the 360 degree range of orientations. Each sample added to the histogram is weighted by its gradient magnitude and by a Gaussian weighted circular window centered at the key point. The purpose of this Gaussian window is to give less emphasis to gradients that are far from the center of the local extremum.

D. Keypoint descriptor

In this stage, a distinctive descriptor is computed at each key point. The image gradient magnitudes and orientations, relative to the major orientation of the key point, are sampled

Within a 16 x 16 region around each key point. These samples are then accumulated into orientation histograms summarizing the contents over 4 x 4 sub regions. Each orientation histogram has 8 bins covering the 360 degree range of orientations. Each sample added to the histogram is weighted by its gradient magnitude and by a Gaussian circular window centered at the local extremum. The descriptor is then formed from a vector containing the values of all the orientation histogram entries, therefore having a 4 x 4 x 8=128 element feature vector for each key point.

E. Keypoint matching

Matching between two images is performed by comparing each local extrema based on the associated descriptors. Given a feature point Pu in h, its closest point P21, second closest point P22, and their Euclidean distances d1 and d2 are calculated from feature points in [2. If the ratio dd d2 is sufficiently small, then points Pu and P21 are considered to match. Then, the matching score between two images can be decided based on the number of matched points. According to we have chosen a threshold of 0.76 for the ratio ddd2.

F. Trimming of false matches

The key point matching procedure described may generate some erroneous matching points. We have removed spurious matching points using geometric constraints [10]. We limit typical geometric variations to small rotations and displacements. Therefore, if we place two iris images side by side and draw matching lines as shown in Figure 5 (top), true matches must appear as parallel lines with similar lengths.

Conclusion

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 authentications have 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 SMS based method. Both methods have been successfully implemented and tested, and shown to be robust and secure. The iris recognition technique is using for providing more mobile authentication in case of mobile stealing which provide more security to the onetime password which is generated to the users mobile phone.

References

[1] Jøsang and G. Sanderud, “Security in Mobile Communications: Challenges and Opportunities,” in *Proc. of the Australasian information security workshop conference on ACSW frontiers*, 43-48, 2003.

[2] Aladdin Secure Safe Word 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-*BankiSecurity---*Layers-of-Protection&id=1353184*

[4] B. Schneider, "Two-Factor Authentication: Too Little, Too Late," in *Inside Risks 178*, *Communications of the ACM*, 48(4)**,** April 2005.

[5] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005. Available at *http://www.silicon.com/ Financial services/0, 3800010322, 39153981, 00.htm*

[6] D. de Borde, "Two-Factor Authentication," *Siemens Enterprise Communications UK-Security Solutions*, 2008. [7] A. Herzberg, "Payments and Banking with Mobile Personal Devices, "*Communications of the ACM*, 46(5), 53-58, May 2003.

[7] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth-Factor Authentication: Somebody You Know," *ACM CCS*, 168-78. 2006.

[8] NBD Online Token. Available at *http://www.nbd.com/NBD/NBD_CDA/CDA_ Web_pages/Internet_Banking/nbdonline_top banner*

[9] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services, *"Communications of the ACM*, 47(8), 42-46, May 2004.

[10] "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*

[11] R. Groom, "Two Factor Authent*ication Using BESTOKEN Pro USB Token*." Available a*http://bizsecurity.about.com/ od/mobilesecurity/a/twofactor.htm*

[12] Sha4J. Available at *http://www.softabar.com/home/content/ View/46/68/*
SMSLib. Available at *http://smslib.org/*