Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Authentication Approaches for Online-Banking

Ms. Arati A. Gadgil
ME (appearing) Computer Science
Miraj, India

Abstract: The security models for online banking systems currently in use are strongly based on, user identification and authentication methods. Therefore different authentication approaches are introduced. There are multiple ways through which banks can authenticate users. These range from the simple systems such as a combination of the username and password to complex systems such as biometric or one time usage based variable tokens. This paper gives insight into some of the more prevalent technologies currently being implemented in large organizations today.

Keywords—security model, online banking, authentication, biometric, variable tokens

I. INTRODUCTION

Online-banking the possibility to initiate financial transaction via an online (Internet)-connection to one's bank or other financial institution is an appealing way of doing business. As online-banking is used widely, malicious and criminal users have become interested in it. Especially organized criminal attempts are on the rise. As online transactions require new authentication methods, some new approaches are introduced in order to prevent attacks being successful and to increase security. The trend goes towards multiple-factor-authentication (mainly two-factor authentication).Mostly used approach i.e. two-factor authentication, yet in different ways. Besides usual username/password (or similar) approaches, additional tokens are applied for authentication in order to make online-banking more secure. Authentication plays a vital role especially in the cases where the customer is not present in front of the banker or its authorized representative. This assumes more significance in online banking as well, where a public medium of access such as the Internet is used as the means of accessing the bank's IT systems. There are multiple ways through which banks can authenticate users. These range from the simple systems such as a combination of the username and password to complex systems such as biometric and / or one time usage based variable tokens.

II. BACKGROUND AND RELATED WORK

Authentication is the process of verifying a claim made by a subject that it should be allowed to act on behalf of a given person, computer, process, etc. In other words, someone has the need to verify that someone else is who they say they are. Authentication can be completed via the use of many different methods. Some of these methods are far superior to others, but are more difficult to implement. Authentication process is preceded by Authorization, which in the banking context, is preceded by Identification. Authorization, involves verifying that an authenticated subject has permission to perform certain operations or access specific resources. Accounting is the process of recording access to a resource. Specifics on the accounting format may vary from system to system, but is a key part of the authentication process.
Authentication methods can be organized into some categories. Method can be directly related to the user that is, something user knows such as id, password or something user possess such as one time password, tokens etc. or physical characteristics of user such as Fingerprint, Hand Geometry.

III. AUTHENTICATION APPROACHES

A. Usernames and Passwords

The most common method for user identification is username password [2]. The idea behind this is user has a unique identifier and also one password, when user authenticates, user provides his unique identifier and password. The user is only one who knows the password, so he is authenticated. This approach is very simple as assigning a unique identifier and user supply password.

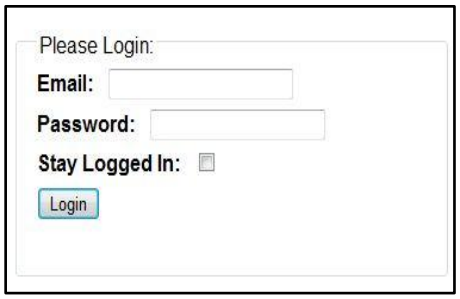

Fig.1 Username password for authentication

Fig.1 shows simple authentication that is user enter unique identifier, here is email and secret password. This is most widely used method for authentication but this is not a secure. Password should be difficult to guess. So it is difficult to user to remember password. User mostly select password such as easy to remember. So passwords are man in the middle attacks.

Since password are widely used for identification of user. Some credentials are provided for password. Password should be alphanumeric, have a minimum length of six characters and consist of special characters like the asterisk (*), semi-colon (;), or dollar sign ($).This password credentials are provided for security in online banking computer systems.

One-Time Password

One-Time Password approach is similar to the simple username password. This method uses client side generator and server. Generator accepts a secret password from user and concatenates it with some information sent from the server in control of the authentication various computations and hashes are performed on the user's secret password which can be verified by computations by each end of the communication. This type of system can protect against passive attacks against which basic password systems maybe vulnerable.

B. Two Way Authentication

Two factor authentication [1] approach uses two things. Things can be user knows, user possesses and user has, to give a much stronger level of authentication. The first factor is something user knows, in this case username and password. The second factor is something user has, in this case your phone or app-running tablet. Two-factor authentication is a way of logging into websites that requires more than just a password. Using a password to log into a website is susceptible to security threats, because it represents a single piece of information. The added security that two facto authentication provides is requiring additional information to sign in.

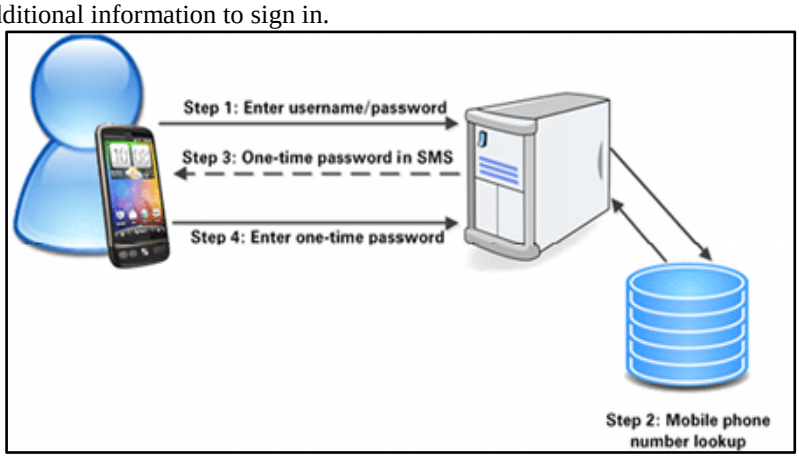

Fig .2 Two way authentication

As shown in fig. 2 after entering username and password one time password is send to the user cell phone. User is only authenticated after entering the one time password send to the user.

Mutual authentication

Mutual authentication or two way authentication can be provided between the user and the organization. It refers to two parties authenticating each other. When describing online authentication processes, mutual authentication is referred to as website-to-user authentication. By means of this authentication, the user knows that he/she is on the valid banking website.

C. Short-time Password using cryptography

Short-time password authentication [3] method using symmetric cryptography in combination with a Software Security Model is a one approach for authentication. In this approach encryption and decryption is performed by software system.

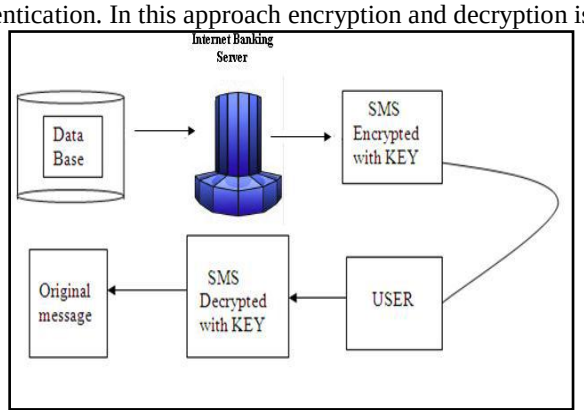

Fig.3 Challenge/response-based short-time Password authentication

The Fig.3 shows the Challenge/response-based short-time password authentication approach in which bank server sends an encoded message to the user. User decodes that message and he get one time password. Decoding is performed by software installed on user phone using secret key. This approach is secure because the one time password is in the encrypted form. But the limitations are the software that is responsible for decryption of message. This uses a secret key that is symmetric key. So key must be kept secret.

D. Virtual keyboard

Virtual keyboard [7] is one approach for authentication consists of a software based keyboard displayed on the screen. These keyboards could be as simple as numeric keyboards or could involve a fully qwerty or a randomized keyboard; these keyboards are often credited for minimizing keylogger based attacks on personal information. This approach is quite popular in Indian banking.

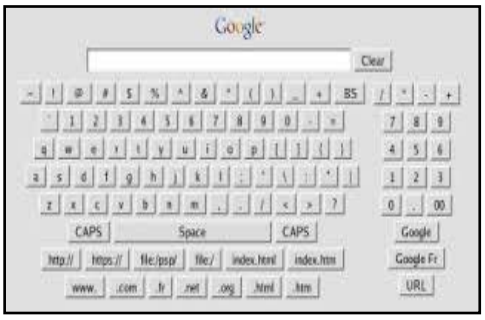

Fig.4 Virtual keyboard

Virtual keyboards are very similar to normal password based systems. They only differ in the use of a none hardware based keyboard; instead the keyboard is shown on the screen of the user. Some virtual keyboards use random positioning of the characters. These virtual keyboards come in all kinds of different shapes

E. Signature

Signature is a one secure authentication approach used in online banking. Users are required to register their signature before using the system or actively use it and let the system learn the signature over time.

Approaches to signature verification fall into two categories, On-line and Off-line. On-line data records the motion of the stylus, while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time.

Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics.

F. Partial password

Partial Password [7] is a one approach of password authentication in which the user is made to supply only a partial part of the user account password while authenticating. This sequence of the partial part is dictated randomly by the server and the user is asked to provide only a partial portion of his credential from the client side. This prevents the user from typing his full password. This method of authentication protects the user from password theft in the form of client side attacks like keystroke capture or network sniffing.

Fig.5 Partial Password

As shown in fig only the characters at particular position are entered, that is 2, 4, 5 and 6.

At each login process the partial part of the password that is typed in by the user is different and it makes the whole password a little bit safer from client side data theft. This kind of implementation can utilize existing technology and needs no need of additional software or physical devices on the client side.

G. Biometrics

Biometric is one best and secure approach for authentication of user. Biometrics uses physical characteristics of user such as fingerprint, hand geometry etc. Biometrics is a method by which a person's authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. Biometric authentication [2] verifies user's identity by comparing an encoded value with a stored value of the concerned biometric characteristic.

No two humans have the same fingerprint. Even each finger for the same person has a different pattern. Users are first required to scan a specific finger into a computer system. User's unique fingerprint get stored, then a device can be deployed at any point that authentication is necessary. The user then applies his finger which is initially scanned to the biometric reader. The system calculates a score based on the fingerprints on record and the currently scanned fingerprint. The system checks for similarities between the fingerprints and allows or denies access if the score is above or below a certain threshold. Biometric is secure approach for authentication as physical characteristics of a user are unique

Fig. 6 Authentication using Biometric

H. Identifiable Picture

Identifiable picture [5] are user for authentication as image is easy to remember for a user. The user selects the image that is identifiable pictures, image title and a text phrase. From a collection of images which are provided in the banking website at the time of creating account. Image title and text phrase is optional part. The user can further change this image during his first login. Further when user enters login id and before entering the password, the site displays the image, title and phrase. If the displayed image is correct then customer can enter the password and can login in. If not the user stop logging in and can contact to the organization or bank. This makes the customer to know whether it is a real banking website or fake website. This facility provides the customer and server to authenticate mutually so it can reduce phishing attacks.

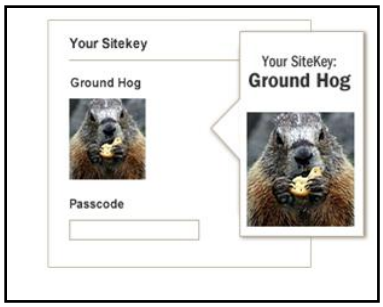

Fig. 7 Image used for authentication

Identifiable pictures (images) [7] are one of the authentication factors that can be used to provide website authentication. Identifiable pictures used for authentication can be stored at server side or at client side.

Images are used for authentication in online banking but this approach is not effective. Sometimes users paid less attention to security images. User awareness is also play important role.

I. Use Of sitekey

Fig.8 Sitekey used for authentication

The new technique is used by bank, is consist of sitekey. Sitekey consists of 3 parts a unique image user chooses, image title that is a unique phrase and three challenge questions that are secrets between user and Bank.
The questions will be asked only if user sign in from a computer that systems don't recognize. Sitekey is an online security feature that is a standard part of Online Banking sign-in experience. Sitekey helps to prevent unauthorized access to accounts while reassuring you that user is at the valid Bank.
When user is at his own computer, enters his online id and click the sign in button, then bank website shows users secret sitekey image and image title, which help to the user that he is at the valid online banking site of bank. When user signing in from a different computer, bank site asks one of the challenge questions to verify user identity. When user answers the question correctly, the secret sitekey image title and image appear.

J. Graphical Password

Graphical Password [5] is new approach for authentication of user, it allows user to select any image e.g. natural images, paintings, etc. The images could be provided by the system or chosen by the user. The only practical requirement is that the image be intricate and rich enough so that many possible click points are available. Another source of flexibility is that we do not need artificial predefined click regions with well-marked boundaries. A user's password consists of any arbitrarily chosen sequence of points in the image. Since an intricate image easily has hundreds of memorable points, not many click points are needed to make a password hard to guess.
This approach uses a technique in which discretize [6] the image into squares is take place. The squares are large enough so the user can click at same square. One possibility is that user can click at points which are close to the edge of discretization square.

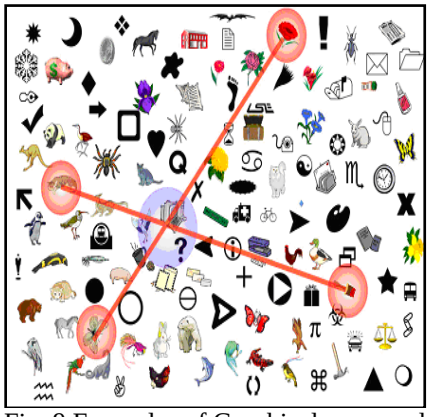

Fig. 9 Examples of Graphical password

Every possible click point is within a safe distance from the edges of at least one of the discretization grids; at password creation, for each click point the system remembers the safe grid for that click, and it hashes the location of the click square relative to that grid. Finding a discretization of images that allows hashing of the graphical passwords, without inconveniencing the user, is one of the main achievements of Graphical Password Design.
A graphical password is easier than a text-based password for most people to remember. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds.

K. Multi factor authentication

Multi-factor authentication [6] involves two or more o different types of authentication. An authentication mechanism where two or more factors are used in which one of the factors is necessarily pertaining to 'the user is'. For example, a large value transaction authorized in a bank by using a combination of the person's user id, a smart card and his biometric authentication factor.
The goal of multifactor authentication is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

IV. CONCLUSIONS

In this paper we have discuses different authentication approaches for online banking. This approach ranges from simple system such as login using password to the complex system. Banks in general are incorporating various authentication methods to grant access to users. To this date, there is no single best solution for authentication. Multiple layers of authentication have proven to be the most effective. Multifactor authentication is currently the most complete solution there is a need for standardization in the security mechanism used by banks.

REFERENCES

[1] A Comparative Usability Study of Two-FactorAuthentication" Emiliano De Cristofaro, Honglu Du , Julien Freudiger Greg Norcie arXiv:1309.5344v2 [cs.CR] 31 Jan 2014.
[2] Authentication factors for Internet banking By M V N K Prasad and S Ganesh Kumar.IDRBT Working Paper.

[3] A Practical Approach for Secure Internet Banking Based on Cryptography Syeda Farha Shazmeen1,Shyam Prasad2 International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2253153

[4] Studying the Effectiveness of Security Images in Internet Banking Joel Lee ,Lujo Bauer ,Michelle L. Mazurek. Digital Object Indentifier 10.1109/MIC.2014.101089-7801/$26.00 2014 IEEE.

[5] Graphical Password Authetication Using Persuasive Cued Click Iranna A M,Pankaja Patil. IJAEEIE.

[6] PassPoints: Design and longitudinal evaluation of a graphical password system Susan Wiedenbeck,Jim Waters,Jean-Camille Birget, Alex Brodskiy,Nasir Memon.

[7] Secure User Authentication in Internet Banking:A Qualitative Survey Janardan Choubey and Bhaskar Choubey. International Journal of Innovation, Management and Technology,Vol. 4, No. 2, April 2013

[8] Bank of America, "SiteKey FAQs," https://www.bankofamerica.com/privacy/faq/sitekey- faq.go, 2013.

