International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol. 1, Issue 2, December 2014

Multi Factor Authentication

[1]Miss Jyoti Madhkar.Shinde,[2]Prof .Seema singh Solanki
[1][2]Everest College of engineering Aurangabad,Maharashtra India.
[1]shinde.jyoti1486@gmail.com,[2]seemasingh986@gmail.com

*Abstract:***Many fields in the world requires authentication of the users. We use authentication in day today life. Most authentications are protected only by Passwords. Passwords are known to be one of the easiest targets of hackers. So the authentication is easily broken. The Solution to this problem is Multi Factor Authentication. Different problems with passwords are Finding written password, Post-It Notes, Guessing password/ pin, Shoulder surfing, Keystroke logging, Screen scraping (with Keystroke logging) and Brute force password crackers. Multi Factor Authentication is the most commonly used authentication means. It is based on the following factors: 1) something you know (as a secret password). 2) Something you have (as a secure device with a secret key). 3) Something you are (E.g.: Biometrics).Multi Factor Authentication implements two or more of the above factors. Stronger and more secure than the traditionally implemented one factor authentication system. An approach to authentication which requires the presentation of two different kinds of evidence that someone is who they say they are. From a security perspective, the ideas is to use evidences which have separate range of attack vectors (e.g. logical, physical)leading to more complex attack scenario and consequently lower risk. It is commonly found in electronic computer authentication, where basic authentication is the process of a requesting entity presenting some evidence of its identity to a second entity. It seeks to decrease the probability that the requester is presenting false evidence of its identity.**

*Keywords:***Global System for Mobile Communication (GSM); Automated Teller Machine (ATM); Personal Identification Number (PIN); Short Message Services (SMS);**

I. 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 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. Several 'proper' strategies for using passwords have been proposed [1]. 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 has 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 [1]. 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 [2].

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 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 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.

II. Multi Factor Authentication Example

To provide an everyday example: an automated teller machine (ATM) typically requires two-factor verification [3]. To prove that users are who they claim to be, the system requires two items: an ATM smartcard and the personal identification number (PIN). In the case of a lost ATM card, the user's accounts are still safe; anyone who finds the card cannot withdraw money as they do not know the PIN. The same is true if the attacker has only knowledge of the PIN and does not have the card. This is what makes two-factor verification more secure: there are two factors required in order to authenticate.

If the ATM smartcard is merely a magnetic-stripe card it is capable then the process is only two-step authentication but not two-factor authentication since the ATM is only verifying that the user knows the data encoded on the magnetic stripe (knowledge factor) and presented it in magnetic-stripe form. A smartcard with a chip performs a challenge/response authentication; the information transmitted from the card to the ATM is not the information required to duplicate the card's abilities.

An example of two-factor authentication system is one of the most widely used online services Gmail [4]. Many people authenticate to their Gmail account or other Google services with their username and password. Google now offers improved security with two-factor authentication, or what Google calls two-step verification. Google's two-step verification requires two things for authentication: your password (something you know) and your smart phone (something you have). To prove you have your smart phone, Google will send it a one-time verification code via SMS that is unique for you (note that messaging charges may apply; check your service plan for information). You then enter the code. Also, if you prefer, instead of Google sending you the one-time verification code via SMS, you can install an app that generates the unique code for you. This way you do not even need access to your service provider, just your smart phone. The value of this stronger authentication is even if an attacker has compromised your Google password, they cannot access your Google accounts unless they also have physical access to your smart phone. You and your valuable information are protected. Keep in mind, these verification codes sent to your smart phone are unique; they are different every time you authenticate. As such, you will have to go through this two step process every time you have to authenticate to your Google account.

III. Method Of Multi Factor Authentication

In art, antiques, and anthropology, a common problem is verifying that a person has the said identity, or a given artifact was produced by a certain person or was produced in a certain place or period of history. There are three types of techniques for doing this.

The first type of authentication is accepting proof of identity given by a credible person who has evidence on the said identity, or on the originator and the object under assessment as the originator's artifact respectively

The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist might use carbon dating to verify the age of an artifact, do a chemical analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos.

Attribute comparison may be vulnerable to forgery. In general, it relies on the facts that creating a forgery indistinguishable from a genuine artifact requires expert knowledge, that mistakes are easily made, and that the amount of effort required to do so is considerably greater than the amount of profit that can be gained from the forgery.

In art and antiques, certificates are of great importance for authenticating an object of interest and value. Certificates can, however, also be forged, and the authentication of these poses a problem. For instance, the son of Han van Meegeren, the well-known art-forger, forged the work of his father and provided a certificate for its provenance as well.

Criminal and civil penalties for fraud, forgery, and counterfeiting can reduce the incentive for falsification, depending on the risk of getting caught

The third type of authentication relies on documentation or other external affirmations. For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and perjury, and are also vulnerable to being separated from the artifact and lost.

Currency and other financial instruments commonly use the first type of authentication method. Bills, coins, and cheque incorporate hard to duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify.

Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name goods

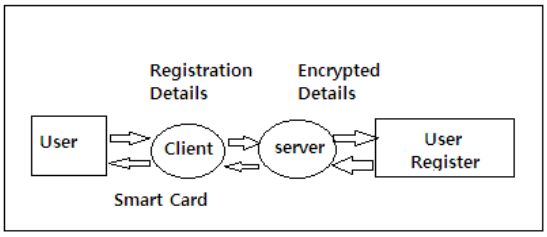

Figure 1 Operational Feasibility

The figure shows the example that offers user friendliness; Great understand ability, Less Restriction on companies and Simplicity. The operations of this application are absolutely simple. Handling this application does not need much training. so the system is operationally feasible. There is no need for much initial investment for software or hardware. The total cost is reduced to a maximum extend because the cost that should be expended in gateway of service providers is not presented here. The system is economically feasible because of the reduced cost as compared to the existing system

CONCLUSION

Therefore I conclude that this Paper is focus on the implementation of Multi factor authentication methods using Smart Card. 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.

REFERENCES

[1] A. Josang 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] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," in Inside Risks 178, Communications of the ACM, 48(4), April 2005.
[3] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005.
[4] D.de Borde,"Two-Factor Authentication," Siemens Enterprise Communications UK Security Solutions, 2008.
[5] A. Herzberg, "Payments and Banking with Mobile Personal Devices," Communications of the ACM, 46(5), 53-58, May 2003.
[6] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth- Factor Authentication: Somebody You Know," ACM CCS, 168-78.2006.
[7] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services,"Communications of the ACM, 47(8), 42-46, May 2004
[8] "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005

About Author

Mr sseema singh Solanki is currently working as Asst prof in department of computer Dr.seemaQuadri institute of Tech, Aurangabad, India .Her research area include reusability of software components.