Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.192 – 196

SURVEY ARTICLE

A Survey of Secondary Authentication Techniques

Mr. Devendra M. Fegade[1], Prof. Priti Subramanium[2]

M.E. Student, Computer Science & Engineering Dept., Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, India
devendraf@rediffmail.com [1]

Assistant Professor, Computer Science & Engineering Dept., Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, India
pritikanna559@gmail.com [2]

Abstract: ***In everyday life we use many websites. There might be user accounts on these websites. To use these website accounts we are required to authenticate ourselves. For this purpose we have to remember user name and password for these web sites. If we forget password, there must be some mechanism to regain access to web sites. This paper is a study of these techniques employed for this purpose. Secondary authentication can be of different types. Each type is having its own significance, this paper try to cover the characteristics of these types.***

Keywords: Secondary authentication, password, verification code, security question, pin.

I. INTRODUCTION

Web sites ask user a password for login purpose. If the password is forgotten by the user then there must be secondary authentication or backup authentication provided by the website so that the user will get quick access to his or her account.

The problem with the secondary authentication is that it should not be very easy to get the access to account with secondary authentication. The easy secondary authentication may be used by the attacker to get access to any ones account. If secondary authentication is hard then it will be very annoying or difficult for the true user to get access to his or her own account. The use of secondary authentication is very rare and it is used only when the primary authentication fails. Therefore the efficiency of secondary authentication can be sacrificed for reliability.

II. LITERATURE REVIEW

According to Robert W. Reeder et al. [1] the secondary authentication mechanism can be divided in two broad categories.

A. Knowledge based authentication.

B. Transitive authentication.

A. Knowledge based authentication.

In this authentication user retains some information to authenticate on web site. This information can be password, an answer to security question etc. Following secondary authentication mechanisms comes under knowledge based authentication.

1. Authentication by asking security question to the user.

Security question is very older and mostly used technique by websites for secondary authentication. Usage of security question is very easy. Generally web sites ask user a predefined set of questions. User has to answer any one of the question.

Though this is very simple technique to use but security question authentication may fail because of following reasons as explained by Ariel Rabkin[6].

1) The security question may not be applicable to all users.
2) The answer may not be remembered by the user.
3) The answer to the security question may be ambiguous.
4) The answer to security question may be guessable.
5) The attacker might know the user and therefore the answer may be guessable.
6) The answer to security question can be found automatically from social networking sites.

To make this method more secure the answers to the security questions should not be easily guessable, should not be publicly available. Web sites may ask user to change answers to security question frequently so that the user will always remember the answer to the security question [1].

2. Authentication by asking old password.

The old password can be used to identify the user when he or she loses the current password. But this technique may be useful when this account is compromised by the attacker. The attacker may change current password but he may not know the old or previously used password. The user has to remember previously used password and current password for account, this password can be used with other secondary authentication to gain the access to his or her account after attacker has compromised the account **[**1].

B. Transitive authentication

In this type of authentication the job of verifying the user is given to other hardware, software or person by the website. Following types of secondary authentication mechanisms comes under transitive authentication.

1. Alternative e-mail address

This is the most common method of authentication. In this method the web sites asks alternative email account id to the user at the time of registration. If the user forgets the password for the web site, the web site sends a link for recovery to the user

on this alternate email id. User is supposed to click the link to avoid the typing mistakes. After the verification the user is allowed to change the password.

But the limitation of this method is that the user might mistype the alternative email id at the time of registration. If this happens then the user may not be able to recover the password from the web site when he or she forgets the password. The solution to this problem is that the email id can be added to the user account after verification of the email id by the web site. The web site may send some verification code to the email id and that is asked to the user to reenter in the web site form. But this requires time [1]. This method is more secure than security question if properly employed [2].

2. Device based authentication

In this authentication the web site sends the verification code on the cell phone of user. The code might be sent by SMS or by automated voice system. Then the user is required to send this code to the web site for the authentication. After receiving the correct verification code from user the website allows user to set new password for his/her account.

This method is somewhat less efficient than email based approach because the user has to manually copy the verification code from cell phone to web site. While copying the user might fill wrong verification code to website. Another problem with this method is that the user may lose his/her cell phone [1].

3. Asking third party to verify user's identity

In this category of backup authentication there are sub types. Let us see two types of these.

3.1 Voucher based system [3].

3.2 Trustee based system [4].

3.1 Voucher based system.

In voucher based system, for authentication purpose two things are required i.e. tokencode and password or pin. The user is called as asker and there is one preregistered helper to assist him or her in authentication. The helper is registered for every asker [3].

If the asker loses the tokencode then he or she has to perform following steps.

1) Asker contacts helper. Asker may use telephone to contact.
2) Helper authenticates asker. The authentication might be by voice of asker or by phone with caller id or by face.
3) Helper authenticates to server. For authentication helper use his token and pin.
4) Helper obtains vouch code. After successful authentication server provides vouch code specific to asker.
5) Helper gives vouch code to asker.
6) Asker enters vouch code and pin.
7) Server authenticates asker.
8) After authentication asker is allowed to choose temporary password.

3.2 Trustee based authentication.

Neil Zhenqiang Gong and Di Wang explain [4] how trustee based system works. Trustee based system is kind of social authentication. In this system if the primary authentication fails, the user asks his or her friends for help. The friends must be having accounts on the same web site. Some of the friends may help the user to recover password.

Trustee based system is having two phases

- Registration phase.
- Recovery phase.

Registration phase

In this phase user and his/her friends are selected as trustees. The trustees may be selected by the user or by the system. The friends must have account in the same system. Neil Zhenqiang Gong et al. [4] assumes that there will be at least 10 friends to the user to use trustee based authentication.

Recovery phase

If the user forgets the password, he or she will recover his or her account with the help of friends. At first user will send recovery request to web site. A URL is shown by the web site to the user. This URL is shared by the user with friends who are trustees. Then trustees obtain verification code for the user from website. Then user obtains verification codes from trustees via email, by meeting in person or by calling them. If the user obtains sufficient number of verification code from trustees then the system allows user to reset the password.

The problem with this authentication is that the attacker may compromise the trustees and may change user account password. If one person is selected as trustee by many users, attacker may compromise that person and attacker will change password of many users one after other.

Stuart Schechter et al. [5] explained one another approach of trustee based authentication. In this method one server is used to help the recovery process. This method is also having two phases.

- Configuration phase
- Recovery phase

Configuration Phase

In this phase user enters names of the trustees and their email addresses. The system requires information of four trustees. The trustees are not informed about their selection as a trustee for the security point of view.

Recovery phase

When the user forgets the password, the user must obtain recovery code from trustees. The user tells the trustees to visit recovery server. When trustees visit recovery server, they are required to enter information about their email address and email address of the user to which they are helping.

After completing this step the trustee will receive the email from recovery server. The email contains a link to recovery server. The trustee copies this link to address bar of the browser. The trustee is required to fill the reason why he or she wants to help the user. After this the trustee is asked to sign the pledge that I understand what are the consequences of giving recovery code to the person other than true user. When the trustee signs the pledge, recovery code is given to him/her by recovery server. In this way all the trustee gets the recovery code. Then the trustees provide these recovery codes to user. The user then recovers the password.

4. Authentication by help-desk staff.

Some organizations can employ help desk staff as backup authentication for the users who forgets the password. The help – desk staff may ask security question to the user. The staff may recognize voice of the user or can verify contact number

of the user. But organization may dislike this approach due to its high labor cost. The other reason of dislike can be intervention of human in authentication may cause social engineering attack [3].

III. CONCLUSION

The secondary authentication methods like security question, alternative email address, and device based authentication are very simple to use. The setup time required is very less. But the attacker can easily guess the answers of security questions. The device may be lost. The trustee based system involves friends to help the user who lost password. This method is good but more set up time is required. Biometric devices can be used to identify the user. The biometric authentication is having its own limitations for example; these devices require special hardware and software.

ACKNOWLEDGEMENT

The author is very thankful to his guide Prof. Priti Subramanium for her valuable guidance and constant encouragement. The authors are also very thankful to Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal for providing all necessary facilities for this work.

REFERENCES

[1] Robert W. Reeder, Stuart Schechter "When the password doesn't work secondary authentication for websites" IEEE Security & Privacy, vol.9, no. 2, (March/April 2011), pp. 43-49

[2] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in Proc. 9th Workshop Economics of Information Security (WEIS), 2010.

[3] John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, Moti Yung "FourthFactor Authentication: Somebody You Know" in Proc. 13th ACM conference on Computer and communications security (CCS), 2006.

[4] Neil Zhenqiang Gong, Di Wang "On the Security of Trustee-Based Social Authentications". IEEE Transactions on information forensics and security, vol. 9, no. 8, August 2014

[5] Stuart Schechter, Serge Egelman, Robert W. Reeder "It's Not What You Know, But Who You Know", CHI 09: Proceeding of conference on Human factors in computing systems, ACM, 2009.

[6] Ariel Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook", Symposium on Usable Privacy and Security (SOUPS) 2008.

