SHORT NOTES

MSC 68-02 **DOI: 10.14529/jcem160307**

DEVELOPMENT OF TWO-FACTOR AUTHENTICATION SYSTEM FOR EMPLOYEES'S PERSONAL OFFICE OF "UNIVERIS" SYSTEM

P.S. Gritsenko[1], pavel.gritsenko@mail.ru,
N.D. Zulyarkina[1], toddeath@yandex.ru,
[1] South Ural State University, Chelyabinsk, Russian Federation.

The work is dedicated to the development of two-factor authentication system for employee's personal office of "Univeris" system. The general concepts of multifactor authentication system, the methods to implement two-factor authentication systems, their advantages and disadvantages are presented.

Keywords: two-factor authentication, 2FA, multifactor authentication.

Introduction

The use of passwords is the most common form of authentication, which is used in the world. Most users of the Internet network use passwords to access to various services such as mailbox, online banking, online shopping and others. But password is one of the least secure forms of authentication. Indeed, if it is a meaningless set of letters and numbers, then one can easily forget it. Also one can crack it, for example, by an exhaustive search. The purpose of two-factor authentication system is to strengthen the authentication process. The simplest example of two-factor authentication system is a credit card: to withdraw money the user must know the PIN-code, and must also has a bank card.

1. General Concepts

Two-factor authentication (2FA, TFA, two-step verification) is an additional level of protection, also it is known as "multi-level authentication which requires not only a username and password, but also something that belongs only to this user [1, 2].

In order to an authorization system can be called a two-factor one, user must have at least two things from the following list:

1) something that the user knows (login and password, PIN-code);

2) something that the user owns (bank card, the USB-key, telephone);

3) the user's biometric data (fingerprint, retinal scan of the eye).

Requirements for reliability, type of technology and authentication facilities depend on the rights and powers of system administrators and users, the importance of the processed information, the probability of the incident and are determined on the basis of an analysis of possible damage risk. Authentication can be a simple, enhanced, or strong [2].

Unlike the simple authentication (username and password), the strong authentication requires that the user owns a physical device (smart card). The most reliable and secure way of authentication is a strong authentication technology. The user must prove that he has a secret (private cryptographic key), which is previously received in a safe way. During the proof, the parties exchange successively signed information in the protected mode. Strong authentication prevents forgery or cloning of a personal secret, which is a private cryptographic key.

2. Methods of Two-Factor Authentication

2.1. SMS-Code

It is the most common second step of an authentication. The basis of this authentication method is OTP (one time password) technology. In the first step of authentication, the user enters his personal data (username and password). Then, SMS-code, which user must enter on the second step of authentication, is sent to the user phone [3–5].

There are following advantages of this type of authentication:

1) generation of new code for each input;

2) binding to a phone number.

There are following disadvantages:

1) one can not authorize, if there is no cellular network;

2) there is a possibility of substitution of number through a service of operator or employees of cellular shops;

3) in the case of authorization and receipt codes on the same device (smartphone), a protection ceases to be a two-factor.

2.2. Authenticator Applications

It is similar to the variant with produce a code by SMS, but at this type the special codes are generated directly on the device using a special application (Authy, Google Authenticator). During initial setup, the user receives a primary key. One-time passwords with a limited validity period from 30 to 60 seconds are generated based on this key using various algorithms [4].

Advantages:

1) in order to authorize, the signal of cellular network does not need, an internet connection during the initial setup is enough;

2) support for several accounts in one application.

Disadvantages:

1) in the event that the attackers gained access to the primary key, they will be able to generate future passwords;

2) in the case of authorization and receipt codes on the same device (smartphone), a protection ceases to be a Two-Factor.

2.3. Checking Login Using Mobile Applications

This type of authentication is a combination of the preceding. For authorization in the system, there is no need to enter one-time passwords. User must confirm the entry with the mobile device with installed service application (Twitter, Snapchat). The device stores the private key, which is checked every time user logs in to account. For example, to enter a Twitter account in the web version, user must enter login and password, and then confirm the request on a smartphone with the notification of the entrance, after that an authorization is carried out (Fig. 1) [3–5].

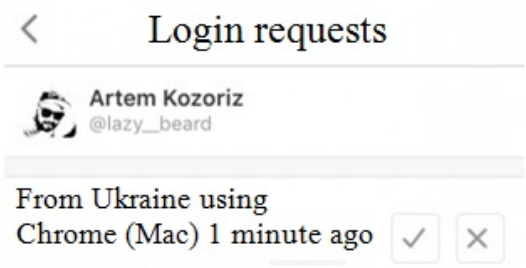

Fig. 1. Notification with an input request

Advantages:

1) it is no need to enter additional codes for the authorization;

2) independence from the cellular network;

3) support for several accounts in one application.

Disadvantages:

1) in the case of interception of a private key, hackers could impersonate the owner of the key;

2) a meaning of two-factor authentication is lost, if the device, which is used to enter, is the same each time.

2.4. Hardware Tokens

It is one of the most reliable methods of two-factor authentication. Hardware tokens can not lose their two-factor component, because they are separate devices. Hardware tokens can be several types: USB-keychain, which is connected directly to the computer and generates keys (Fig. 2) or key chain with a screen, which shows the generated key that is necessary to enter(Fig. 3) [4, 5].

Advantages:

1) no need for SMS and applications;

2) it does not require a mobile phone;

3) fully independent device.

Disadvantages:

1) must be purchased separately;

Fig. 2. USB-keychain

Fig. 3. Keychain with the code

2) not all services support it;

3) user having several accounts should has several tokens.

2.5. Redundant Keys

It is fallback in case of loss or theft of a smartphone, which gets one-time password or confirmation code. Backup keys for use in emergency situations are given in each service, when user sets up two-factor authentication.

Conclusion

Currently, there are several ways to protect user account from unplanned invasion. The easiest one is a password, but this method is not very reliable. 2FA is one of the most reliable ways to protect user accounts. There are several types of two-factor authentication.

Some of them are more reliable, some less. But they all have one purpose. It is to protect users from hacking.

Different services may use different types of multi-factor authentication. For example, website yandex.ru offers one-time passwords, and use of applications for authentication.

References

1. 2FA, Inc. (2014). Two factor strong authentication, simplified. http://www.statsoft.ru/home/textbook/modules/stneunet.html (Date: 7.06.2016) (in Russian)
2. SecurEnvoy, ltd. (2016). What is Two Factor Authentication. https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm (Date: 7.06.2016)
3. Konyavskaya, S. Pros and cons of two-factor authentication / S. Konyavskaya, N. Komarova // *Information Security*, 2007, no. 6, pp. 163–166. (in Russian)
4. Kaspersky Lab. (2016). Two-factor authentication: what is it and why is it necessary. https://blog.kaspersky.ru/what_is_two_factor_authenticatio/4272/ (Date: 7.06.2016) (in Russian)
5. Aladdin R.D. (2016). Solutions for strong authentication.http://www.aladdin-rd.ru/solutions/authentication/ (Date: 7.06.2016) (in Russian)

Pavel S. Gritsenko, Undergraduate, faculty of Mathematics, Mechanics and Computer Science, South Ural State University (Chelyabinsk, Russian Federation), pavel.gritsenko@mail.ru.

Natalya D. Zulyarkina, Doctor of Physics and Mathematics, faculty of Mathematics, Mechanics and Computer Science, South Ural State University (Chelyabinsk, Russian Federation), toddeath@yandex.ru.

Received June 28, 2016

УДК 004.056.53 **DOI: 10.14529/jcem160307**

РАЗРАБОТКА ДВУХФАКТОРНОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ДЛЯ ЛИЧНОГО КАБИНЕТА СОТРУДНИКА СИСТЕМЫ УНИВЕРИС

П. С. Гриценко, Н. Д. Зюляркина

Работа посвящена разработке двухфакторной системы аутентификации для личного кабинета сотрудника системы Универис. Приведены общие понятия многофакторной системы аутентификации, способы реализации двухфакторной системы аутентификации, их преимущества и недостатки.

Ключевые слова: двухфакторная аутентификация, 2FA, многофакторная аутентификация.

Литература

1. 2FA, Inc. (2014). Two factor strong authentication, simplified. http://www.statsoft.ru/home/textbook/modules/stneunet.html (Дата обращения: 7.06.2016)
2. SecurEnvoy, ltd. (2016). What is Two Factor Authentication. https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm (Дата обращения: 7.06.2016)
3. Конявская, С. Плюсы и минусы двухфакторной аутентификации / С. Конявская, Н. Комарова // *Информационная безопасность*. – 2007. – № 6. – С. 163–166.
4. Kaspersky, Lab. (2016). Что такое двухфакторная аутентификация и зачем она нужна. https://blog.kaspersky.ru/what_is_two_factor_authenticatio/4272/ (Дата обращения: 7.06.2016) (in Russian)
5. Aladdin R.D. (2016). Решения для строгой аутентификации. http://www.aladdin-rd.ru/solutions/authentication/ (Дата обращения: 7.06.2016)

Гриценко Павел Сергеевич, магистрант, факультет Математики, механики и компьютерных наук, Южно-Уральский государственный университет (г. Челябинск, Российская Федерация), pavel.gritsenko@mail.ru.

Зюляркина Наталья Дмитриевна, кафедра Дифференциальных и стохастических уравнений, факультет Математики, механики и компьютерных наук, Южно-Уральский государственный университет (г. Челябинск, Российская Федерация), toddeath@yandex.ru.

Поступила в редакцию 28 июня 2016 г.