Using Two-Factor Authentication for Securing User Accounts in an Online Testing and Education System

Gavrikov I. (Russian Federation)

Использование двухфакторной аутентификации для защиты учётных записей пользователей в системе онлайн тестирования и обучения

Гавриков И. В. (Российская Федерация)

Гавриков Илья Владимирович / Gavrikov Ilya Vladimirovich – студент,
кафедра бизнес-информатики и математического моделирования,
Институт экономики и управления,
Крымский федеральный университет, г. Симферополь

Abstract: *the article describes two-factor authentication technology and its working principles, as well as its advantages and disadvantages, and presents an example of its use in an online testing and education system developed for use in a university environment.*
Аннотация: *в статье описывается технология двухфакторной аутентификации, принципы её работы, её преимущества и недостатки, а также рассматривается пример её использования в системе онлайн тестирования и обучения, разработанной для применения в университете.*

Keywords: *authentication, two-factor authentication, information security, privacy, mobile devices.*
Ключевые слова: *аутентификация, двухфакторная аутентификация, информационная безопасность, приватность, мобильные устройства*

User authentication through a username-password combination has long since been the norm in the vast majority of all computer systems. The key to securing the account has therefore been the use of a complex password, which would be practically unfeasible for a hacker to guess. Passwords are secured further through applying hashing algorithms, making it harder still for a hacker to gain access [1].

However, reality can be starkly different from expectation—users often neglect to use strong passwords [2], companies fail to implement proper security procedures, and the tools available to hackers become ever more efficient and complex. This means that simple username-password authentication is becoming obsolete [3].

One replacement for it that is gaining traction today is two-factor authentication. At its core, two-factor authentication (also 2FA) is a method of confirming a user's identity by utilising two different components, which may be something the user knows, possesses, or something that is inherently inseparable from the user (such as biometric data — fingerprints, voice patterns etc.). The concept in itself is not new—withdrawing money from a cash machine has always been a process that uses two-factor authentication by combining a factor that the user possesses (the bank card) and one that the user knows (the PIN).

With the threats to account safety growing ever larger, two-factor authentication is becoming the norm for securing accounts in major services like Google, Facebook, Steam, etc. Up to 37 % of organisations today use multi-factor authentication, and the number is expected to rise to 56 % by the end of 2016 [4]. Most implementations today employ the user's mobile phone as the second factor, in tandem with a strong password. The second step in the authentication process is performed by either delivering a one-time code in a text message sent to the phone, or generating one in an authenticator app provided by the service—the code that is then received or generated is used to authenticate the user and confirm the action.

Mobile two-factor authentication has a number of advantages in comparison with other designs. Mobile phones are usually carried by the user, which means that no additional hardware or tokens will be necessary, and, if text messages are used to deliver codes to the user, no additional software will be necessary either. However, this approach also has its disadvantages. Users' phones must be carried by the user, as well as kept charged and within range of a cellular or Wi-Fi network (depending on the implementation). Additionally, if text messages are used, the user is required to share their mobile number with the service, which may raise privacy concerns.

The online testing and education system developed for the Crimean Federal University also makes use of two-factor authentication to secure accounts. Mobile two-factor authentication was chosen as the most widespread and easiest method, and SMS text messages were chosen as the delivery vessel. Although using a mobile app for authentication was considered, ultimately it proved to be impractical, and in some cases impossible, to develop apps for every type of phone used by professors and students. SMS, on the other hand, is universally available and requires no additional configuration to deliver messages to different types of devices.

References

1. *Karen Scarfone, Murugiah Souppaya* Guide to Enterprise Password Management: Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD, 2009. 38 c.

2. Weak Password Vulnerability: More Common than You Think. [Электронный ресурс]: Acunetix. URL: http://www.acunetix.com/blog/articles/weak-password-vulnerability-common-think (дата обращения: 13.06.2016).
3. *Sami Luukkonen* Are Passwords Becoming Obsolete? [Электронный ресурс]: Forbes. URL: http://www.forbes.com/sites/valleyvoices/2015/10/12/are-passwords-becoming-obsolete (дата обращения: 13.06.2016).
4. 2014 Global Annual Authentication Survey. [Электронный ресурс]: SafeNet. URL: http://www.safenet-inc.com/resources/data-protection/2014-authentication-survey-executive-summary (дата обращения: 13.06.2016).