 doi:10.20944/preprints201706.0036.v1

Two-Factor Authentication and Its Adaptation to Online Education Systems

Elif Karakaş, İlhan Öztozlu and Volkan Erol *

Okan University Computer Engineering Department, Tuzla Campus, 34959, Istanbul, Turkey
* Correspondence: volkan.erol@okan.edu.tr; Tel.: +90-533-3621947

Abstract: This study examines the evolution of the two-factor authentication method and its adaptability to the online education system. Two-factor authentication is a security measure used especially in areas where information such as banking is valuable. Parallel to technological developments, it has developed as much as daily. It aims to take security one step forward because it is composed of two phases. Today, banking, IOT devices, public transport tickets and many other areas are used. Two-factor authentication methods against security attacks in the field of information are also being updated. In recent years, new technologies such as biometric (iris pattern, retinal pattern, etc.) or behavioral biometry (location tracking, walking information, touch speed etc.) were studied. Instead of physically studying somewhere like going to a course in modern society, online trainings become more advantageous. Most of these online trainings are given certificates such as participation certificate, success certificate, etc. The main problem here is whether the person who is being certified is true. In the study conducted in line with these details, there is a proposal for the application of the Mimic Control Method with Sound Intensity (MCMSI) method for on-line training by examining the two-factor authentication techniques up to the day.

Keywords: two-factor authentication; online training; biological and behavioral features; mimic control method with sound intensity

1. Introduction

Nowadays, rapid developments in the information technology sector are important to safety. When information security is referred to, the most common method is the two-step auhtentication technique. According to this technique, when it is desired to access to any web site, mobile application or electronic device; the user is required to have a two-step control by asking for a second information such as password, biometric information (fingerprint, iris, face recognition etc.).

Over the years, two-factor authentication options have been diversified in line with technological developments. Two-step authentication methods can be collected under three headings until today [1]. Hardware-based encryption and related techniques are using alpha-numeric / graphical encryption, biological and behavioral features [2-4]. We can separate the biological and behavioral properties into two as physical biology and behavioral biometry. Behavioral biometrics consist of compiling information such as location traces, walking

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

information, touch-screen dynamics. Technological developments point to us in the future two-step verification will in demand more of the behavioral biometric properties. Two-step verification was first developed in areas such as finance and banking where security is very important. Nowadays, that are used many areas to smart home, NFC devices, public transport tickets, transportation and etc. [4]. The spreading of information to so many areas shows the importance of technological developments and the increase of information immorality and the verification of information.

Time management is an indispensable necessity for modern life. For this reason, many people are turning to online trainings to improve themselves. Online trainings allow you to participate in currencies anywhere in the world, and receive online certifications. In this way, we will be able to save considerable time in terms of material and time.

Just like every other area, there are people who can abuse online education. When no authentication is used, online education provider / person cannot know whether the student is true or not. Security is provided by adapting a measure such as two-step verification to this system.

Verification of the identity for the entire time slot in which the student is connected to the system, not just the login screen, should be made to determine if the person is authentic. For this reason, it is necessary to perform verification for the whole active period in the system by making various improvements on the two-step verification method used at the user entry in any site.

In this study, it is provided to examine the two-factor authentication techniques which are up to date and to search and adapt the most appropriate verification technique for online education.

2. Authentication Methods

The security structure created by requesting multiple login information from a user to access a particular system is called two-step authentication.We can think of this as having two locks on the outer door to prevent theft in our homes. Even if we play one of the keys in this way, a two-factor authentication affirmation is made because the thief will need the other key. Basically two-factor authentication was performed on the door example.However, parallel to technological advances, door locks can break without a key.At this stage, the question of “what kind of features can we add to the two-factor authentication” is asked and should be improved on the basis of science. For example, biometric features such as fingerprinting and face recognition have been added to ensure that our two-stage verification is adapted to today's conditions.

2.1. One-factor Authentication Basic Layout Features

Single Factor Authentication (PAGE) was a security structure based on only one factor such as username / password. According to the researches made, the users use simple passwords that are easy to remember.For example, in December 2009, a security company

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

made an analysis of 32 million passwords for Rockyou.com. The most common passwords used by 32 million users are 123456, 12345, 123456789, Password, and iloveyou [5]. It seems that users have difficulty remembering, if the passwords have letters, numeric expressions, capitalization, etc. [6].

Nowadays, although it is a weak method, it is used in many sites. There seems to be no solution other than to raise the awareness of users and strengthen internet security infrastructure in Single Factor Authentication systems.

2.2. Two-Factor Authentication

Two-factor authentication began with the most primitive method. Subsequently, it has made great progress by incorporating features such as biological and behavioral.

2.2.1. Hardware-Based Two-factor Authentication

Two-Factor Authentication (T-FA) was first used physically with ATM cards (smart card [5]). The user places the card in the ATM device in the first stage, and in the second stage enter the password. In this way, a two-factor safety stage is passed. Although this system is safe for those years, it is not a very successful two-step verification method because of the lack of being seen by someone else and the stolen / copied ATM card.

In addition to this hardware-based method today, biometric two-step verification has begun, such as ATM devices that recognize fingerprints. In the future, we will be able to perform our transactions safely by performing two-step verification with behavioral biometrics, without the need for a magnetic-specific hardware structure such as a debit card.

The two-phase verification was first used in the years since the internet speeds were very low and mobile phone usage was not common, so it was provided with a device called "RSA SecurID" to generate the password [6]. In Figure 2, a screenshot of the "RSA SecurID" device is given.The algorithm in this device is capable of generating a complex PIN number. Apart from "RSA SecureID", there are many commercial devices such as "Safeword of Secure Computing" [6]. If we are carrying these devices with us in today's conditions, it is still a fact that the algorithm is still considered secure for large keys lengths.

Figure 1. RSA SecurID

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

The concept of Internet of things (IOT) was first heard in 1999. This system aims to connect various devices and communicate with each other using the same communication protocol. With the development of IOT and robotics work, security especially on the hardware side has gained a great importance.

The fact that many devices are connected to a single network reveals the importance of network security [7]. In order to provide this security, the use of two-factor authentication in robot technology is inevitable [8]. Thanks to NFC technology, data can be exchanged at a short distance with low bandwidth. NFC technology can be used on the hardware side for two-factor authentication. Figure 2 shows the two-step verification using NFC [9].

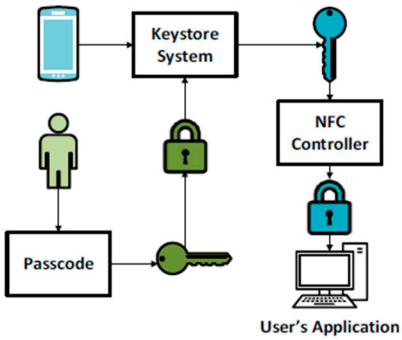

Figure 2. NFC working principle [9]

With the increasing number of NFC-enabled devices, it has begun to be used especially in cars, at home street gates. At this point, users are not limited to carrying a physical key, but they are secured with smaller NFC controllers (such as the NFC Controller Chip on mobile phones).

2.2.2. Alpha Numerical/Graph Based Two-Factor Authentication

It is one of the most commonly used two-step verification methods today. Alpha-Numerical validation is especially important in mobile phone technology. In the general usage example, the user enters the password on the input screen of any system. Then, the alphanumeric code consisting of the combination of letters and numbers coming to the mobile phone enters the corresponding screen and performs two-factor authentication.

There are two basic problems in alpha-numeric two-factor authentication. First, the user becomes dependent on the mobile phone and does not have access to his account because he cannot perform two-factor authentication in cases such as undoing the base station network, corruption of the phone. Another problem is to provide the mobile phone with SMS to forward the code to another phone by hackers with various malicious software.

With the advances in touch screen technologies, graphics-based verification has entered our lives. The user specifies a pattern, such as touching a particular point on a pattern or a photo, and the generated graphical password is recorded in the device. This graphical pattern is actually the password of the user.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

The most fundamental problem with graph-based verification is that graphs manually drawn on the screen in public areas are easily observable by malicious people [10]. To prevent this, the option to prevent the graphic template drawn on the Android 7.0 version from being displayed on the screen has been introduced. However, it is not a sufficient measure. Because of the research done, malicious people can predict the graph based password from fingerprints on the screen [1].

A new technology called TouchIn has been developed [1], with security improvements such as the ability to view graphical passwords by others, predictions from fingerprint traces, and improvements in touch screen and sensor technologies [1]. This technology uses the 3D accelerometer sensor;

- Direction: x-coordinate, y-coordinate
- Speed: x-speed, y-speed
- Acceleration : x-acceleration, y-acceleration
- Finger press:
- Hand geometry

features a new approach to graph-based validation.

2.2.3. Biological Based Two-Factor Authentication

The biologically based two-factor authentication is divided into Physiological Biology and Behavioral Biometry in itself. Physiological biometry uses media in the devices have entered our lives with the development of sensors such as fingerprint detection. Behavioral biometrics is still a developing technology. It aims to provide security by evaluating features such as the brain wave, thoughts, and movements of the person.

2.2.3.1. Physiological Biometry Based Two-Step Verification

Physiological biometry aims to verify the identity of a person depending on their physical characteristics. Physical properties used today;

- Fingerprint [11]
- Iris pattern
- Retina pattern
- Face features
- Hand geometry etc.

In today's mobile phones (e.g. Samsung Galaxy S8), fingerprints, iris recognition, face recognition features are beginning to be used at the same time. In this way it can be verified in many ways.

Face recognition has also been made available to the end user in the computer world. For example, on Windows 10 computers, face recognition is performed with the help of webcam

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

with Windows Hello application.

The main problem with fingerprinting is that malicious people can get into the system when their finger is torn off and the relevant sensor is read. In order to prevent this, it is only possible to read finger vein information instead of fingerprint. Especially in ATM machines, airports have started to be used in areas where information is very valuable.

2.2.3.2. Behavioral Biometry-Based Two-Step Verification

It is a security verification method which is made by adding the parameters that measure the behavior of the person on the physiological biometrics together with the developments in the technology.

Behavioral biometrics uses features;

- Personal behavior
- Location tracks
- Brain waves
- Thoughts etc.

RhyAuth system with rhythm-based verification has been introduced [12]. This system is based on the creation of a melody with various notes. It is secure according to the graphical encryption used on the phone. Because a long note is required to create a melody. This system is also useful for visual impairments to use two-factor authentication. However, it can cause problems in noisy environments such as libraries. It has also been shown to be safe in research on 32 users on Android devices.

The verification of the password in the smart card technology has been studied [13]. Utilizing the cryptography method, SHA-256 algorithm is used to validate while waiting for the devices in the queue, thus saving time in this way.

Behavioral biometry is a method of verification that has not been fully developed. But with future developments in technology, it will be something that end users can take advantage of.

3. Online Education System

With the advancement of technology, we are able to take online trainings with the help of virtual classes (MOOC etc.) without the limitation of time and space in the comfort of our home. There are also disadvantages to this system, which are the advantages of this system.

As the training is provided online, it is not known whether the person using the system is real or not. For this reason, many authentication methods are proposed for online education [14]. These methods include multiple verification methods.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

3.1. MOOC Intelligent Identitiy Tool (MOOC-SIA) Model

This model differentiates the security method as the evaluation part progresses, such as activity, homework. etc. Classical lessons use email and password.In more important areas such as homework, lesson activities, security is expanded further and biometric verification, login and sms verification, system planning and data mining techniques etc. are based on the information and training of users on the system. Continuous user authentication is provided with [15].

The schematic of the MOOC model is shown in Figure 3.

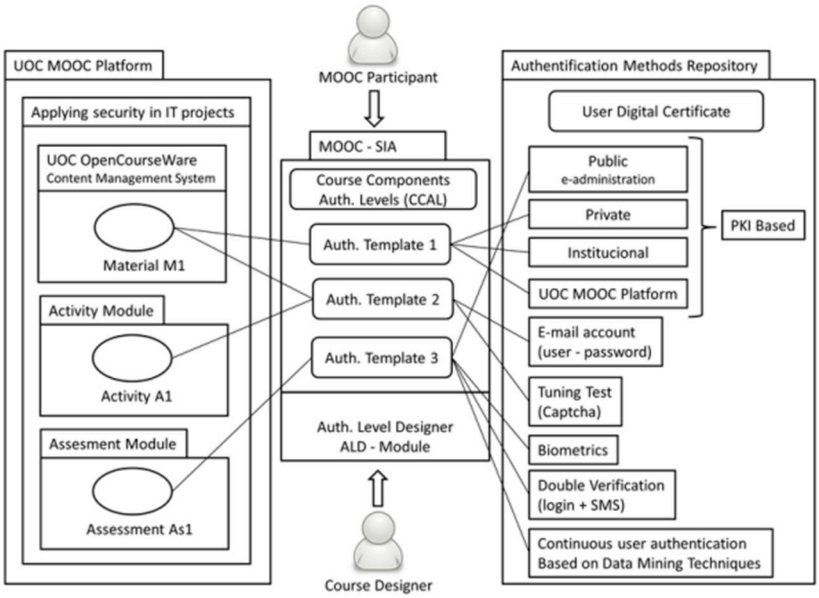

Figure 3. MOOC Intelligent Identity Tool (MOOC-SIA) model [12]

3.2 Resistance against imitation

Using the following features, the algorithm maintains the security of the system by deciding whether or not the person has real identity [16]:

- Word Length Frequency
- Sentence Length Frequency
- Part of Speech Tag Disclosure
- Word Specific Frequency
- Model Learning

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

3.3. Classical methods

Password, CAPTCHA, SMS, as well as traditional methods such as Face, Fingerprint, Sound, Keystroke; On the same system, biological and behavioral validation are used at the same time [17]. In this method, face recognition is performed by looking at eyebrow, cheek, eye and lip measurements. Volume control is calculated in vector form.

In these popular methods we have mentioned above, one of our focus points is constant identity verification based on data mining techniques. Because the system cannot be sure if the user has forged his identity at first. It is difficult to deceive the system when continuous authentication is done.

Similarly, in [16], the character of the counterfeit person is also recorded. Even if the operation of this system is correct and does not fail, the system will accept it forever as the right person if the user does not give the correct identity information since the first time it entered the system.

We need to be sure that the person entering the system is the same person from the first moment in order to be authenticated in online trainings. In addition to this, the identity information declared at the beginning and the identity information declared at the end of the last one should be compared.

If you need to elaborate, you should identify the person with the online tutorial record (before you enter the tutorial first) with certain features in the system. For example, while enrolling at the university, we are registering with our ID and as a result we are giving us a username and password. In online education, such a user name and password should be given so that those who register to the system in the future will be able to check the same one that is logged into the system online. First of all, it is necessary to register the student in the real environment.

3.4. Mimic Control Method with Sound Intensity (MCMSI)

The preparation phase of the MCMSI method;

- The person to be authenticated is created in the system in the real environment.
- The camera and microphone are used when creating the ID recording on the system.
- The person who is to be authenticated goes to the camera and reads the alphabet one by one in the microphone. He then reads the basic two- and three-letter hypotheses.
- With the help of artificial intelligence, the next system finds the phonetic pattern of the phonetic alphabet, which is formed by the syllabic combination of the letters in the alphabet, and prompts the user to read the words with this different phonetic pattern.
- An ID record is created in the system.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 June 2017 doi:10.20944/preprints201706.0036.v1

The working principle of the MCMSI method;

- Since the face of the system user models the behavior of Gabor wavelet transform, sensory regions in the human vision system, the feature vector is created and face recognition control is performed by the facial features [18].
- The user reads the words on the screen, and the system controls user's face and face from the PCA base [20]. On the other hand, the voice of the user controls the voice of the user using the Shell Frequency Cepstrum, Coefficients, Wavelet or Peak frequencies properties [17].
- The system overlaps the sound intensity and sound characteristics of the user with the face and mouth gestures, and if these two features are true, the identity is authenticated.

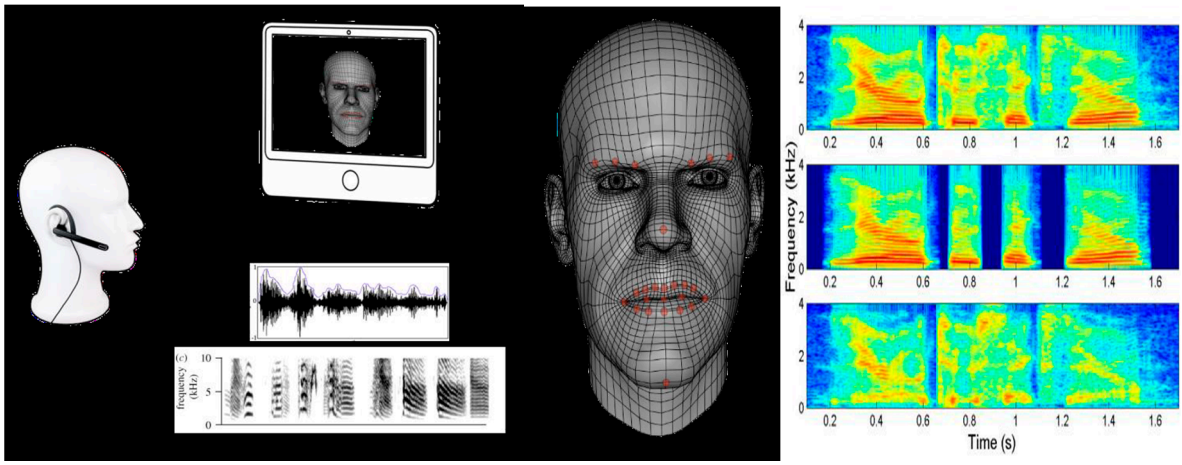

Figure 4. Mimic Control with Sound Intensity

8. Conclusions

With this study, it is possible to examine the two-factor authentication methods which are up to date and adapt to the online education sector. In the study, it is observed that two-step verification confirms that people are moving toward behavioral biometrics such as thinking and reading.

Online education is becoming more and more popular day by day. However, the main problem is that the security verification phase cannot be fully achieved. We recommend using a unique feature of the person to provide this security. Because it is imitated and prevented from being used by someone else.

By using the camera and sound, unique authentication is ensured by allowing simultaneous control of the mouth, mimic movement and sound movement of the person. Although it is more secure than existing systems, there are problems to be overcome such as providing the required internet bandwidth and computer hardware power. With the progress

of the technology, this system can in theory be transformed into a structure that can be applied by the end user.

References

[1] Jingchao Sun, Rui Zhang, Jinxue Zhang, and Yanchao Zhang, TouchIn: Sightless Two-factor Authentication on Multi-touch Mobile Devices, IEEE Conference on Communications and Network Security, 2014.

[2] Dogukan Aydinli, Emre Koroglu, Volkan Erol, Abuse of Mobile Devices by Making Reverse Proxy Server, Preprints 2017, 2017050123 (doi: 10.20944/preprints201705.0123.v1), 2017.

[3] Kadir Imamoglu, Volkan Erol, Gorkem Cetin, Enabling Secure Platforms with Trusted Computing, IEEE 2nd Conference on Homeland Safety and Security (TEHOSS 2006), 2006.

[4] Oguz Ercakir, Orkun Kizilirmak, Volkan Erol, Network Security Issues and Solutions on Vehicular Communication Systems. Preprints 2017, 2017060001 (doi: 10.20944/preprints201706.0001.v1), 2017.

[5] Jing-Chiou Liou, Sujith Bhashyam, A Feasible and Cost Effective Two-Factor Authentication for Online Transactions , 2nd International Conference on Software Engineering and Data Mining (SEDM), 2010 .

[6] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, Two Factor Authentication Using Mobile Phones, International Journal of Mathematics and Computer Science, 4(2009), no. 2, 65–80, 2009.

[7] Herman Engström, Martin Larsson, Joel Wikberg, Factors in Two-Factor Authentication, INFC40 - Information Systems Security

[8] Dhvanik Miglani, Arnold Hensman, Vision for Secure Home Robots: Implementation of two–factor authentication, IEEE International Symposium on Technology and Society (ISTAS), 2015.

[9] Matthew A. Crossman, Hong Liu, Two-Factor Authentication through Near Field Communication, IEEE Symposium on Technologies for Homeland Security (HST), 2016.

[10] Alireza Pirayesh Sabzevar, Angelos Stavrou, Universal Multi-Factor Authentication Using Graphical Passwords, IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS '08), 2008.

[11] Hugh Wimberly, Lorie M. Liebrock, Using Fingerprint Authentication to Reduce System Security: An Empirical Study, IEEE Symposium on Security and Privacy (SP), 2011.

[12] Yimin Chen , Jingchao Sun , Rui Zhang , Your Song Your Way: Rhythm-Based Two-Factor Authentication for Multi-Touch Mobile Devices, IEEE Conference on Computer Communications (INFOCOM), 2015.

[13] Edna Elizabeth N., S. Nivetha, Design of a Two-factor Authentication ticketing system for Transit Applications, IEEE Region 10 Conference (TENCON), 2016.

 doi:10.20944/preprints201706.0036.v1

[14] Abhijit Kumar Nag and Dipankar Dasgusta, Kalyanmoy Deb, An Adaptive Approach for Active Multi-Factor Authentication, Annual Symposium on Information Assurance (ASIA'14), 2014.

[15] Jorge Miguel, Santi Caballé, Josep Prieto , Providing Information Security to MOOC: Towards effective student authentication, 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2013.

[16] Markus Krause, "A Behavioral Biometrics based Authentication Method for MOOC's that is Robust against Imitation Attempts", Proceedings of the first ACM conference on Learning.

[17] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, "Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound", Proceedings of the 24th USENIX Security Symposium

[18] Halit Ergezer, Face Recognition: Eigenfaces, Neural Networks, Gabor Wavelet Approaches, 12th Turkish Symposium on Artificial Intelligence and Neural Networks (TAINN'03), 2003.

[19] Mike Seymour, https://www.fxguide.com/featured/performance-driven-facial-animation/, Performance driven facial animation

[20] Koichiro Niinuma, Unsang Park, "Soft Biometric Traits for Continuous User Authentication", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, 2010.

[21] Philip Jackson, David Moreno, Javier Hernando, Martin Russell, http://personal.ee.surrey.ac.uk/Personal/P.Jackson/Columbo/, Columbo Project