Behavioral Biometry as a Cyber Security Tool

Maryna Chyzhevska[1], Nataliia Romanovska[2], Andrii Ramskyi[3], Vitalii Venger[2], and Mykola Obushnyi[4]

[1] *National University "Yuri Kondratyuk Poltava Polytechnic," 24 Pervomaiskyi ave., Poltava, 36011, Ukraine*
[2] *State Institution "Institute for Economics and Forecasting, NAS of Ukraine," 26 Panasa Myrnoho str., Kyiv, 01011, Ukraine*
[3] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[4] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01033, Ukraine*

Abstract

With the intensification of digitalization of all processes and activities, the issue of information protection and increasing the level of cyber security is becoming important. Particular attention in this aspect should be focused on the field of queuing. The article provides a brief overview of digital transformation and data protection, which shows that the largest share is occupied by accidents of server equipment, infrastructure / network equipment, applications, data storage system equipment and cyber attacks. The authors focus on key aspects and trends related to the cyber threat landscape; argued the need to introduce new tools for biometric identification and authentication, the most promising of which is behavioral biometrics. The proposed comparative characteristic of types of behavioral biometrics allowed to define spheres of their application and to reveal the drawbacks and advantages.

Keywords

Cybers security, cyber attack, cyber threats, identification, authentication, digitalization, behavioral biometrics.

1. Introduction

The last two years have been significant for the whole world in the paradigm shift of public communications, which has led to the intensification of their digitalization. Despite the fact that traffic in certain industries and activities has decreased, the number of fraudsters remains the same or even increases. This makes the security situation much more complex and dynamic, as new threats become much larger than before. There is a need to develop new approaches to effective technical solutions and take into account the problem of cyber security. In addition, the global COVID-19 pandemic and the resulting quarantine restrictions have changed the global communication landscape and approaches to the use of digital services. Businesses and consumers around the world are forced to respond quickly to changing realities.

2. Digital Transformation and Data Protection

2.1. The Main Problems of Cyber Security

Following the landmark attacks on SolarWinds in December 2020 and Microsoft Exchange in January 2021, new attempts have been made in recent months. The operators of the extortionist programs carried out incidents with high consequences - at Colonial Pipeline and JBS Foods, at Quanta, Acer and Kaseya - and demanded ever higher ransoms.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: marfin.poltava@gmail.com (M. Chyzhevska); romnatalina@gmail.com (N. Romanovska); a.ramskyi@kubg.edu.ua (A. Ramskyi); vengerv@ukr.net (V. Venger); mobushnyy@gmail.com (M. Obushnyi)
ORCID: 0000-0003-1637-9564 (M. Chyzhevska); 0000-0002-1377-7551 (N. Romanovska); 0000-0001-7368-697X (A. Ramskyi); 0000-0003-1018-0909 (V. Venger); 0000-0002-9121-5095 (M. Obushnyi)

For industrial organizations, the number of attacks by extortionist programs increased by 500% in the period from 2018 to 2021, and another 116% - only in the period from January to May 2021 [1].

A total of 20120074547 records were broken. In early 2021, Veeam conducted extensive research on data protection. Based on the results, the Veeam Data Protection Report-2021 was written (Table 1). The data show that the largest share is occupied by accidents of server equipment, infrastructure / network equipment, applications, storage system equipment and cyber attacks. According to Forbes, in 2020, 1120 leaks and cyber attacks were recorded. Most of these incidents have been reported by the world's leading media.

Table 1

Causes of equipment failure and disconnection of services, %

Indicator	Causes of accidents	The most important for 2020	The most important for 2021
Server equipment failure	57	13	12
Infrastructure / network equipment failure	57	8	16
Application crash	56	6	11
Data storage system hardware failure	51	15	8
Cyber attacks	51	7	16
Operating system failure	50	22	9
Administrator error in settings	46	6	6
Public cloud failure	45	10	8
Accidental deletion, overwriting or data corruption	44	3	8
Intentional actions by the administrator or user	37	8	5

2.2. Cyber Threats During the COVID-19 Pandemic

Countries, organizations and citizens have been greatly affected by the COVID-19 pandemic, which has changed the conditions of activity, the activity itself and even life as a whole. Note that most cyber attacks are usually not publicized due to reputational risks, and therefore it is extremely difficult to calculate the exact number of threats, even for organizations involved in investigating incidents and analyzing the actions of hacker groups. Most of these studies aim to draw the attention of organizations and ordinary citizens who are interested in the current state of information security, to the most relevant methods and motives of cyber attacks as well as to identify major trends in the change of the landscape of cyber threats [2].

Let’s highlight key aspects and trends related to the cyber threat landscape [3–5]:

- during the COVID-19 pandemic, the number of fake websites for online shopping and fraudulent online sellers increased. From copies of popular brand websites to fraudulent services that never supply the product, the corona virus has identified weaknesses in the trust model used in online stores;
- with the COVID-19 pandemic, the number of cyber bullying and extortion cases has also increased. The introduction of mobile technologies and subscriptions to digital platforms make both the younger generation and the elderly more vulnerable to these types of threats;
- fraudsters use social media platforms to increase the effectiveness of targeted attacks, and financial rewards are still the main motivation for most cyber attacks;
- clearly targeted and ongoing attacks on valuable data, such as intellectual property and state secrets, are carefully planned and often carried out by state-funded entities. Massive attacks with a short duration and wide impact are used for various purposes, such as, for example, theft of credentials;

- the number of phishing victims in the EU continues to rise when criminals use the COVID-19 theme to lure "customers." COVID-19-themed attacks include messages and file attachments that contain malicious links to redirect users to phishing sites or malware;
- business e-mail manipulation and attacks are used in cyber fraud, resulting in the loss of millions of Euros for EU citizens and corporations. European small and medium-sized enterprises have also fallen victim to these threats;
- many cases of cyber security still go unnoticed or are detected over time. The number of potential threats in the virtual or physical environment continues to expand as a new phase of digital transformation emerges.

Organized crime groups are taking advantage of the situation, uncertainty and doubts caused by COVID-19 and inventing new ways to pose threats to IT and cyber security. In turn, businesses and people want to have more information and support and be protected. Consumers want more control over personal information and guarantees about its security in terms of content and secrecy from third parties [6–9].

3. Biometric Information Protection

3.1. Biometric Authentication Technologies

In these conditions the use of biometrics as an effective means of confirming the correctness of identification is important in solving queuing problems. It is quite attractive for an organization to control any access, as biometrics provides a high level of authentication and can be integrated into any access control system with different keys and passwords [10].

Threats to biometric systems can occur in the form of fictitious data transmission, when an attempt is made to undermine the principles of system security by providing natural biometric characteristics or artifacts that contain copied or forged characteristics in the middle.

Control access systems can be divided into three classes according to what a person has to present: what he or she knows; what he or she owns; what is part of himself/ herself.

Biometrics uses scientifically justified methods to describe and measure the characteristics of the body of living beings [11]. In relation to automatic identification systems, the term "biometric" means that these systems and methods are based on the use of unique qualities of the human body for identification and authentication.

Biometric identification is often called real authentication because it is based on a person's personal characteristics, not on virtual keys or passwords. A feature of biometric identification is the large size of biometric databases: each of the samples is compared with all available records in the database. For use in real life, such a system requires a high speed comparison of biometric characteristics.

Two methods of authentication are used in biometrics:

1. Verification:

- measurement data are compared with one record offered by an external identifier (nickname, password or other identifier) from the database of registered users;

2. Identification:

- the measurement data is compared with all entries in the database of registered users, and not only with one of them, selected on the basis of the identifier.

The main purpose of biometrics is to create a registration system that rarely denies access to legitimate users and at the same time completely eliminates the possibility of authorization of attackers.

3.2. Features of Application of Behavioral Biometrics

Modern authentication technology is behavioral biometrics, which involves the collection of a variety of data [12,13]. For example, a smart phone that collects behavioral information may obtain multiple measurement points to estimate the likelihood of fraudulent activity, while static biometrics provides less raw data [14]. The combination of behavioral characteristics in different mathematical algorithms makes it possible to obtain a more multifaceted user profile, which allows you to weed out fraudsters. Its value lies in the fact that it can detect fraud at an early stage before the cyber attack.

Behavioral biometrics can be adapted to a variety of devices, including smart phone operating systems as a whole, not just applications. Each person has unique features of interaction with their digital devices: the speed of typing on the keyboard, the force of pressing or the angle at which the fingers move across the screen. It is almost impossible to reproduce such behavior by any another person.

While behavioral biometrics is most commonly used by banks and financial institutions today, experts are expected to use it in e-commerce, online services, healthcare, government and in many more spheres in the near future [15].

Of course, as in any promising technology, there are pros and cons. Among the first are: inaccuracies in identification due to the fact that user behavior is not always constant, which is associated with, for example, fatigue, intoxication, malaise or haste, as well as the availability of many personal data to determine standard behavior of a user. The positive features include the fact that each user has their own unique set of behavioral characteristics that are analyzed; to perform the identification does not require a change in the script intended for the user: the method of seamless integration; increased recognition accuracy in multifactor identification systems [16].

There are several methods of behavioral biometrics [17]. Their comparative characteristics are presented in Table 2.

Table 2
Methods of behavioral biometrics

Method	Description	Industry leaders	Usage scenarios or scope	Security level / accuracy level	Pros	Cons
Keystroke dynamics	Brings standard passwords to a new level by tracking the rhythm of their input. Such sensors can respond to the time required to press each key, the delay between the keys, the number of characters entered per minute, etc. Keyboard templates work with passwords and PINs to increase security.	Typing DNA, ID Control, BehavioSec	Device user identification, part of multifactor authentication, is used for surveillance	High/high	No special equipment required; speed and safety; difficult to copy by observation	The rhythm of typing may change due to fatigue, illness, exposure to drugs or alcohol, changes in the keyboard; it is not possible to identify the same person using different keyboard layouts
Signature recognition	A pen and a special tablet connected to a computer are used to	Aerial, Redrock Biometrics, Sense, Oxford University,	Verification and authorization of documents, identification	High/ average	It is almost impossible to forge; Widespread in	High error rate until the user gets used to the notebook for

	compare and check patterns. A high-quality tablet can capture behavioral characteristics such as speed, pressure, and time spent signing. At the registration stage, a person must sign up several times on a tablet to collect data. Then, signature recognition algorithms extract unique characteristics such as time, pressure, speed, direction of impact, important points on the signature path, and signature size. The algorithm assigns different degrees of importance to these points	Mobbeel	in the banking sector		business practice; fast and safe; ease of integration	signing; hand injuries can affect the recognition accuracy
Recognition of the speaker	The user must say the word or phrase into the microphone. This is necessary to obtain a sample of human language. The electrical signal of the	Apple Inc, Microsoft, Google LLC	Telephone and Internet transactions, audio signatures for digital documents, online education systems, emergency services	High/low	Ease of integration; fast recognition time; contactless scanning	Sensitivity of technology to quality of a microphone and noise; risk of counterfeiting

	microphone will be converted to digital using an analog-to-digital converter. It is written to computer memory in the form of a digitized sample. The computer then compares and tries to compare the voice of the person speaking with the stored digitized sample and identifies the person. Speaker recognition focuses on the context of the phrase said by the user, not on the recognition of his voice					
Voice recognition	Voice recognition function compares a spoken phrase to a digital pattern. It is used as a means of identification and authentication in security systems such as access control and timekeeping. The system creates digital	Nuance Communications, Google LLC, Amazon.com, Apple Inc.	Online banking sector, emergency services, call center recognition, high demand for voice recognition in healthcare	High/low	Ease of integration; fast recognition time; contactless scanning. .	Risk of counterfeiting; inability to reduce external noise; problems with recognition accuracy

	templates with a very high probability of correct interpretation. Each person's voice includes physiological and behavioral characteristics. Physiological aspects depend on the size and shape of the mouth, throat, larynx, nasal cavity, body weight and other factors. Behavioral traits depend on language, level of education and place of residence, which can lead to certain intonations, accents and dialects					
Recognition on the go	Stroke biometrics captures step patterns using video and then converts the mapped data into a mathematical equation. This type of biometrics is invisible, making it ideal for mass crowd monitoring. Another	SFootBD, Watrix, Cometa Srl	Medicine and criminology	Low/low	Contactless scanning; possibility to cover a large area; fast recognition time. Technology is evolving rapidly	Not as reliable as other biometric methods; clothing and footwear can affect the accuracy of recognition

Movement of lips` recognition	advantage is that these systems can quickly identify people at a long distance Lip recognition is one of the newest forms of biometric verification. Just as a deaf person can track the movement of the interlocutor's lips, biometric systems record the activity of the muscles around the mouth, forming a pattern of movement. Biometric sensors of this type often require the user to repeat the password to determine the appropriate lip movements, and then allow or deny access based on a comparison with the recorded sample.	Hong Kong Baptist University, AimBrain, Liopa	Can be used to improve security systems and complement biometrics such as face recognition, retina scanning, and fingerprinting	High/low	Contactless scanning; fast recognition time; increases the accuracy of recognition in combination with other forms of biometrics	The technology is being refined

Biometric data can be stored on different media depending on the type and specific biometric technology. Data can be stored on a biometric database server as part of public infrastructure or can be physically distributed to private companies. Biometric data can also be stored on smart phones that use fingerprint and face recognition technology.

None of the above personal characteristics of an individual can be compared in reliability of recognition with the genetic code of a person. However, practical methods of identification that use the

unique features of fragments of the genetic code are currently rarely used due to their complexity and high cost.

4. Conclusions

Thus, the identification of the individual as the consumer of information is becoming increasingly important. It explains the huge interest in biometric technologies and the role of information, and hence its protection from unauthorized access. They are quite attractive for the organization in charge of access, as they provide a high level of authentication, can be integrated into any access control system simultaneously with different keys and passwords.

5. References

[1] Dangerous extortionist programs attack: how not to become the next victim. https://eset.ua/ua/news/view/903/opasnyye-programmy-vymogateli-atakuyut-kak-ne-stat-sleduyushchey-zhertvoy

[2] M.TajDini, et al., Wireless Sensors for Brain Activity—A Survey. In Electronics, Vol. 9, Issue 12, 2092. MDPI AG., 2020. https://doi.org/10.3390/electronics9122092

[3] Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence. In Advances in Computer Science for Engineering and Education IV, 374–388, 2021. https://doi.org/10.1007/978-3-030-80472-5_31

[4] H. Shevchenko, et al., Information security risk analysis SWOT, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923, 309–317, 2021.

[5] The threat of cyberattacks is growing due to the pandemic: EU report. https://yur-gazeta.com/golovna/zagroza-kiberatak-zrostae-cherez-pandemiyu-zvit-es.html

[6] V. Buriachok, V. Sokolov, P. Skladannyi, Security rating metrics for distributed wireless systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 222–233, 2019.

[7] D. Berestov, et al., Analysis of features and prospects of application of dynamic iterative assessment of information security risks, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), vol. 2923, 329–335, 2021.

[8] F. Kipchuk, et al. Investigation of Availability of Wireless Access Points based on Embedded Systems. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019. https://doi.org/10.1109/picst47496.2019.9061551

[9] V. Astapenya, et al., Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PICST), 2021. IEEE. https://doi.org/10.1109/picst54195.2021.9772161

[10] L. Banga, S. Pillai, Impact of Behavioural Biometrics on Mobile Banking System, Journal of Physics: Conference Series, Vol. 1964, 2021. https://iopscience.iop.org/article/10.1088/1742-6596/1964/6/062109/pdf

[11] M. Shopon; S.N. Tumpa; Y. Bhatia; K.N. Pavan Kumar; M.L. Gavrilova. Biometric Systems De-Identification: Current Advancements and Future Directions. J. Cybersecur. Priv. 2021, 1, 470–495.

[12] A. Dantcheva; P. Elia; A. Ross. What else does your biometric data reveal? A survey on soft biometrics. IEEE Trans. Inf. Forensics Secur. 2015, 11, 441–467.

[13] M. Sultana; P.P. Paul; M. Gavrilova. Social behavioral biometrics: An emerging trend. Int. J. Pattern Recognit. Artif. Intell. 2015, 29, 1556013.

[14] S.N. Tumpa; K.P. Kumar; M. Sultana; G.S.J. Hsu; O. Yadid-Pecht; S. Yanushkevich; M.L. Gavrilova. Social Behavioral Biometrics in Smart Societies. In Advancements in Computer Vision Applications in Intelligent Systems and Multimedia Technologies; IGI Global: Hershey, PA, USA, 2020; pp. 1–24.

[15] F. Bahmaninezhad; C. Zhang; J.H. Hansen. Convolutional Neural Network Based Speaker De-Identification. Odyssey, 2018, 255–260. https://www.semanticscholar.org/paper/Convolutional-Neural-Network-Based-SpeakerBahmaninezhad-Zhang/f2cd2f81b188166058ea04b454a4c59135d744a5
[16] Y.R. Vampolskiy, V. Govindaraju. Behavioural biometrics: a survey and classification, Int. J. Biometrics, 2008, Vol. 1, No. 1, 81–113.
[17] A.K. Anil, K. Jain, Biometrics of Next Generation—An Overview. http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainKumarNextGenBiometrics_BookChap10.pdf