Impact of Globalisation on Data Security – Authentication Issues

Miloslav Hub[1,*], *Agnès Kateřina* Příhodová[1]

[1]Faculty of Economics and Administration, University of Pardubice, Czech Republic

Abstract.

Research background: In today's globalised world, there is an increasing need for reliable verification of users' identity accessing various types of information systems. This verification is realised through authentication, which is traditionally divided according to the kind of identification mark that is used: knowledge authentication (e.g., passwords, control questions), authentication through an authentication object (e.g., magnetic cards, smart cards) and biometric authentication (e.g., voice, face recognition). However, it should be noted that this identity may not only be the specific identity of the user but also, for example, his group affiliation or ability.
Purpose of the article: This paper aims to identify and describe the impact of globalisation on selected types of authentication.
Methods: As the representative of the current methods of authentication of persons are selected a password authentication and hand-based biometric authentication. The most often used methods of password attacks are simulated through mathematical modelling, and the results are compared concerning the timeline. Through modelling, multi characteristics authentication using the thermal characteristics of the hand will be presented.
Findings & Value added: Through mathematical modelling, the article demonstrates the influence of globalisation on the resilience of passwords to the most commonly used attacks and discusses the impact of globalisation on the requirements for modern forms of authentication.

Keywords: *global changes; security; authentication; passwords; hand-based biometric*

JEL Classification: *L86*

1 Introduction

As noted in [1], at the end of the 20th century, globalisation became the motto for the international economy. Nations have indeed become interconnected through the flow of goods, services, and financial capital since the 1970s. The growing importance of export-oriented industrialisation has made integration into the global economy virtually synonymous with development for many countries. Most recently, cross-border projections

* Corresponding author: miloslav.hub@upce.cz

of national production systems through direct investment and international subcontracting have deepened interdependence and the functional integration of the world economy.

Globalisation has brought people many new opportunities, services and benefits. At the same time, however, globalisation has created ways in which dangerous and harmful events can spread rapidly. An analysis of financial, information, telecommunications, environmental and health systems has identified these systems as vulnerable worldwide [2]. The country has already faced and continues to face some consequences: such as the global COV-19 pandemic, global migration and terrorism, the global economic crisis. In combating risks and their consequences, it is important to identify risks.
The division of global threats can be as follows [2]:

- Economic risks (fiscal crises, extreme energy price volatility, global imbalance and currency volatility, regulatory failures);
- Geopolitical risks (global governance failures, fragile states, geopolitical conflict, terrorism, organised crime, corruption, illicit trade);
- Environmental risks (climate change, biodiversity loss, flooding, storms and cyclones, air pollution);
- Societal risks (economic disparity, demographic challenges, migration, water and food security, infectious diseases);
- Technological risks (online data and information security, critical information infrastructure breakdown, threats from new technologies).

Furthermore, in the article, we will deal only with information security. Information security deals with the protection of information in all its forms and throughout its life cycle (creation, processing, storage, transmission and disposal). The basic requirements for secure information are to ensure its confidentiality, integrity and availability of data (CIA). The requirement of confidentiality of information means that only authorised persons have access to the information. This can be done by subject authentication. Authentication is defined as the process of verifying the identity of an entity with the required degree of security. There are different types of authentication:

- Knowledge authentication (password, PIN)
- Authentication using an authentication object (magnetic card)
- Biometric authentication (fingerprint, iris, walking)

2 Methods

The aim of this article is to identify the impact of globalization on data security. The basic requirements for secure data are availability, confidentiality and integrity. These requirements are also achieved through access control, which includes identification, authentication and authorization. For this reason, authentication was chosen as an area of research interest. The results of this analysis will then be summarized and generalized.

A case study and an analysis of the findings from these studies were chosen as the methods. As a representative of biometric authentication, hand-shaped biometric authentication is chosen. It is currently a progressive method of authentication, which is a frequent topic of scientific discussions. Password authentication is chosen as a representative of real-time authentication, because it is the most commonly used method of authentication due to its low cost and ease of implementation.

3 Results

3.1 Biometric authentication

In biometrics, the term biometric authentication is often considered synonymous with biometric recognition, which is defined as biometrics automated recognition of individuals based on their biological and behavioural characteristics [3]. Biological characteristics are such characteristics with which we were born, for example, fingerprint, face, iris, hand geometry. The second group consists of behavioural characteristics such as walking, signature, the dynamics of typing on the keyboard. In this article, we will deal with hand-based biometric systems, which include hand geometry, palm print, fingerprint and bloodstream topography, and fingerprint [4]. The reason why the hand was chosen is mainly its user-friendliness, which is often neglected. However, in recent years, this characteristic has become increasingly important.

Rapid developments in information technology and the increase in security risks on a global scale are leading to efforts to improve the reliability of hand-based biometric systems. One way to improve the reliability of a biometric system is to use the infrared part of the electromagnetic spectrum. Infrared radiation is radiation with a wavelength between 760 nm and 1 mm. It is used in two ways in hand-based biometrics. The first method is irradiation of the hand with IR radiation, which enhances the contrast between the vascular bed and the surrounding skin [5, 6]. The second method uses the fact that every object with a temperature higher than absolute zero (-273 ° C) emits infrared radiation and can be used to measure the temperature on the body surface.

Infrared thermography is an imaging technique in which the emitted infrared radiation is measured, and the surface temperature of the observed object is graphically displayed. Currently, thermograms are obtained with the help of an infrared camera, which measures and displays the emitted infrared radiation of an object. The fact that the radiation is a function of the surface temperature of the object allows the camera to calculate and display this temperature. However, the radiation measured by the camera depends not only on the temperature of the object but also on the emissivity function. The thermogram can be further affected by radiation coming from the environment, and its subsequent reflection, the radiation of the object can also affect the absorption of the atmosphere. For accurate temperature measurement, it is, therefore, necessary to compensate for the effects of a number of different radiation sources.

Currently, in biometrics, most person recognition techniques work with images from the visible part of the electromagnetic spectrum. Thermograms are not used often, mainly due to the higher purchase price of a thermal camera [7]. However, the use of thermograms has indisputable advantages, among them we can include the complexity of imitating an uneven temperature map of the body or the ability to detect liveliness, last but not least, they can be used to check whether a person has a fever. Elevated temperature is one of the hallmarks of infectious diseases such as COV-19, and this pandemic already has a global dimension. Temperature information can be used as another biometric characteristic. Because the temperature map of our skin is a consequence of cellular metabolism, processing of nutrients (carbohydrates, lipids and proteins), it is an individual anatomical characteristic [8].

Given the current global threats, such as information security and the worldwide spread of infectious diseases, it is proposed the use of hand-based biometric recognition using multispectral images. Multispectral images will be created using an image from the visible part of the electromagnetic spectrum and an infrared image. Multispectral images are advantageous in low lighting conditions; the quality of input data decreases less because the thermogram is not dependent on lighting conditions. When using a multispectral image,

some types of attacks on biometric systems are also eliminated, because the thermal map of the hand, which is captured by the thermogram, is complicated to imitate and at the same time liveness is detected. Last but not least, it is possible to determine a person's temperature when an elevated temperature can signal an infectious disease. Thus, it can also help prevent the spread of infectious diseases.

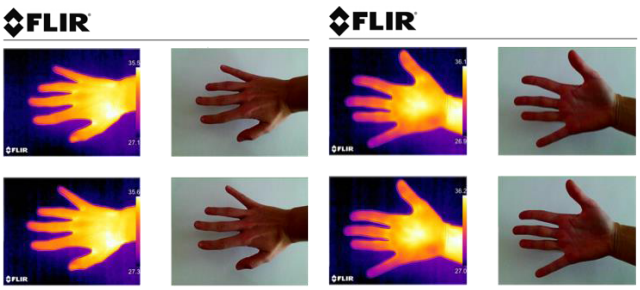

Fig. 1. Examples of multispectral images (visible and infrared spectrum) and visible light images.

3.2 Biometric authentication

Although a lot of biometric authentication methods exist [9], even for continuous authentication [10], and authentication through passwords is often used because of easy implementation and low financial requirements. However, this way of authentication is not generally considered to be too secure because users often choose easy to guess short passwords, divulge their passwords to others, remark their passwords, and often use the same password for different services. Many existing passwords are not resilient to various forms of attack, such as a dictionary attack or brute force attack that also has relatively high economic impacts.

Already in 2003, a hypothesis about the impact of globalisation on passwords selection was formulated [11]. This hypothesis was then discussed somewhat fuzzily and not very concretely. Therefore our research aims to analyse the long-term trend of choice of passwords by end-users and to discuss the effects of global social trends on this trend.

For the quantitative analysis of long-term trends in password selection by end-users, the four datasets are used:

1. The first dataset of 2,958 passwords that were collected in 2005 [12].
2. The second dataset of 1,895 passwords that were collected in 2008 [13].
3. The third dataset of 1,048 passwords that were collected in 2008 [14].
4. The fourth dataset of 1,238 passwords that were collected in January – June 2020.

It is necessary to emphasise that conditions of the fourth dataset collecting were the same as the conditions of the previous datasets collecting, that is, specifically:

- all users who choose passwords were native Czech speakers,
- the password had to contain one character at a minimum,
- the maximum length of the password was not restricted,
- users had no time limit when choosing a password, a password could contain arbitrary characters typed using a Czech keyboard.

Although, some tool for password security estimation exist [15], as a measure of security of a given password the expected Value of the number of attempts an attacker has to carry out to break the password S(pi) is used [16] (see Eq. 1). The reason for this model using is because of resulting in a specific value that can be compared.

$$S(p_i) = \frac{N_i + 1}{2} + \sum_{j=1}^{i-1} N_j \quad (1)$$

Where S(pi) is a security of a password p that is a word from i-th reduced dictionary, I is the order of the reduced dictionary that contains a password p, and Ni is the size of the i-th reduced dictionary. It must be noted, that the creation of a reduced dictionary is created on the base of its success rate SDA(d) (see Eq. 2) that is detailed described in [16].

$$SDA(d) = \frac{NBP_d}{N_d \cdot NP} \quad (2)$$

Where SDA(d) is a success rate of the dictionary attack on dictionary d, NBPd is the number of passwords that would be broken by dictionary d, Nd is the size of dictionary d, and NP is the total number of tested passwords used in the attack simulation.

In the next step, the passwords collected in periods 2005, 2008, 2018, and 2020 were inserted to the model of dictionary and brute-force attack, and results from these model situations were compared (see figure 1). From this figure, it is possible to see that after 400,000 attempts, a password will be broken with the probability of 0.28.

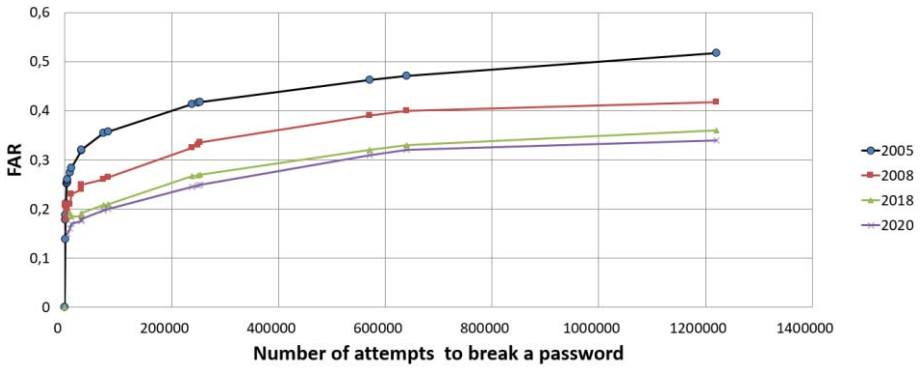

Fig. 1. Security of passwords collected in periods 2005, 2008, 2018, and 2020.

In the next step, the correlation between the occurrence of individual letters in passwords and Czech and English languages. As a correlation coefficient, the Kendall Tau coefficient was used. The results are shown in Table 1.

Table 1. Correlation between the occurrence of individual letters in passwords and selected languages (Kendall Tau)

Year	Passwords-Czech	Passwords-English
2005	0.780	0.624
2008	0.625	0.687
2018	0.598	0.712
2020	0.612	0.723

From this table, it is possible to see that the Value of Kendall Tau correlation coefficient between characters in passwords and characters in Czech texts is decreasing by the time. Furthermore, otherwise, that the Value of Kendall Tau correlation coefficient between characters in passwords and characters in English texts is increasing by the time. Because users are Czech, this fact suggests that Czech users are increasingly advocating the choice of a password that is made up of an English word.

3.3 Summary

Rapid developments in information technology and the increase in security risks on a global scale are leading to efforts to improve the reliability of hand-based biometric systems. In the article is proposed that the security of information systems be increased by hand-based biometric identification using multispectral images eliminates some types of attacks on biometric systems. They are also advantageous in low lighting conditions because the quality of the thermogram is not dependent on light. Last but not least, when recognising a person with the help of a multispectral image of the hand. It is also possible to determine the increased temperature of a person, which is one of the symptoms of infectious diseases and early detection of the patient can contribute to solving a global problem such as the spread of infectious diseases, nowadays mainly COV-19.

The analysis of passwords used in periods 2005, 2008, 2018 and 2020 shows the impact of globalisation on passwords selections, and it is possible to say that this impact is positive because of results in more secure passwords. Although end-users are instructed to select a long password that is created by randomly generated alphanumerical string, they do not do it because it would be difficult to remember these passwords. Instead, they use common words instead of random text. Globalisation affects end-user language range and therefore the size of the set of candidate passwords from which a potential attacker must look for the appropriate password. Users use less and less Czech words for their passwords, but increasingly also words from other languages, such as English. This fact makes it difficult for potential attackers to attack the dictionary because, in addition to Czech words, they must also test foreign words.

4 Discussion

In this paper, the impact of globalisation on data security was discussed, with hand-held biometric authentication and password-based knowledge authentication being selected as case studies. Of course, it should also be mentioned that there are other methods of authentication, such as object authentication or multifactor authentication. However, the results of this research suggest the influence of globalization on data security, specifically on authentication, it can be assumed that other such influences will be identified in the future.

However, the results of this research identify the impact of globalization on data security, specifically on authentication, it can be assumed that other such influences will be identified in the future. However, this research provides a framework for other work that will follow.

This article was supported by grant No. 2020_018 supported by the Student Grant Competition.

References

1. Gereffi, G., Kaplinsky, R. (2001). Introduction: Globalisation, Value Chains and Development. *IDS Bulletin*, 32(3) 1-8.
2. Helbing, D. (2013). Globally networked risks and how to respond. *Nature,* 497(7447), 51-59.
3. Wayman, J. (2003). *A Definition of "Biometrics".* Collected works 1997-2000. U.S. National Biometric Test Center. San José State University.
4. Unar, J.A., Seng, W., Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*., 47(8), 2673-2688.
5. Toro, Ó. F. M., Correa, H. L. (2009). Biometric identification using infrared dorsum hand vein images. *Ingeniería e Investigación*., 29(1), 90-100.
6. Zhu, Q., Zhang, Z., Liu, N., Sun, H. (2015). Near infrared hand vein image acquisition and ROI extraction algorithm. *Optik.,* 126(24), 5682-5687.
7. Bentez-Restrepo, H. D., Bovik, A. C., Rodriguez Pulencio, C. G. (2017). Image quality assessment to enhance infrared face recognition. In *2017 24th IEEE International Conference on Image Processing (ICIP)* (pp. 805-809). IEEE, New York: USA.
8. Smrž, M. (2013). *Bezkontaktní měření teploty*. Brno. Bachelor thesis. Technical University Brno. Faculty of Electrical Engineering and Communication Technologies.
9. Alyanis, N., Razak, S., Al-Dhaqm, A. (2020). Biometrics authentication techniques: A comparative study. *International journal of advanced and applied sciences*. 7(9), 97-103.
10. Dahia, G., Jesus, L., Segundo, M. P. (2020). Continuous authentication using biometrics: An advanced review. *Wiley interdisciplinary reviews-data mining and knowledge dicsovery.* 10(4), Art. No. 1365.
11. Hub, M. (2003). Bezpečnost znalostní autentizace. In *Sborník příspěvků 3. mezinárodní konference doktorandů Partipácia doktorandov na vedecko-výskumnej činnosti*. (pp. 53-57). Bratislava: Slovakia.
12. Hub, M. (2005). *Bezpečnost informací - autentizace*. Pardubice: University of Pardubice.

13. Hub, M., Čapek, J. (2011). Security Evaluation of Passwords Used on Internet, *Journal of Algorithms & Computational Technology,* 5(3), 437-450.
14. Hub, M., Příhodová, K. (2018). The impact of global changes on the security of password authentication. In T. Kliestik (Ed.). *Globalisation and Its Socio-Economics Consequences. 18th International Scientific Conference* (pp. 2061-2066). Zilina: Slovak Republic.
15. Doucek, P., Pavlicek, L., Sedlacek, J., Nedomova, L. (2020). Adaptation of password strength estimators to a non-English environment-the Czech experience. *Computers & security,* 95, UNSP 101757.
16. Hub, M., Čapek, J. (2009). Method of Password Security Evaluation. In *The 8th International Symposium on Distributed Computing and Applications to Business, Engineering and Science* (pp. 401-405).