HADMÉRNÖK
BIZTONSÁGTECHNIKA

15. évfolyam (2020) 4. szám 15–28.
DOI: 10.32567/hm.2020.4.2

Kata Rebeka Szűcs,[1] Arnold Őszi,[2] Tibor Kovács[3]

Mobile Biometrics and their Risks

Mobil biometrikus megoldások és kockázataik

The present article aims to introduce the ways of secure access control, with a special emphasis on biometric solutions on mobile devices. Apart from secure biometric data storage, which is also a very important aspect of this topic, there are several other types of threats. On the following pages we provide a short description of the possible risks of biometric systems. In order to understand the current status and attitude towards biometrics, we introduce our own survey as well.

Keywords: biometric authentication, biometric data, data protection

Jelen cikk célja a hozzáférés-ellenőrzés módjainak bemutatása, különös tekintettel a mobil biometrikus megoldásokra. A biztonságos biometrikus adattárolás mellett, amely nagyon fontos szempont ebben a témában, számos más típusú kockázat is létezik. A következő oldalakon rövid leírást adunk a biometrikus rendszerek lehetséges veszélyeiről. A biometria jelenlegi állapotának, valamint az ahhoz való hozzáállásnak megértésére saját kutatást is végeztünk, amelyet szintén ismertetünk.

Kulcsszavak: biometrikus hitelesítés, biometrikus adatok, adatvédelem

Introduction

Our lives have changed a lot recently and our mobile devices have become an integral part of our new lifestyle. ISQ Online and Google conducted a survey in Hungary to examine the role of smartphones in our lives and found that the second most frequently checked object when we leave our homes for work or school is our phones,

[1] Óbuda University, Doctoral School of Safety and Security Sciences, PhD student, e-mail: szucs.rebeka@phd.uni-obuda.hu, ORCID: https://orcid.org/0000-0002-2965-6295

[2] Óbuda University, Bánki Donát Faculty of Mechanical and Security Technology Engineering, lecturer, e-mail: oszi.arnold@bgk.uni-obuda.hu, ORCID: https://orcid.org/0000-0001-5988-0143

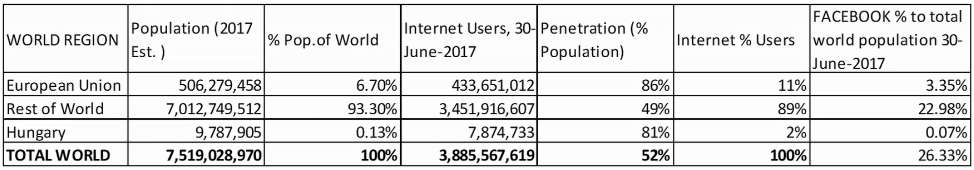
[3] Óbuda University, Bánki Donát Faculty of Mechanical and Security Technology Engineering, Associate Professor, e-mail: kovacs.tibor@bgk.uni-obuda.hu, ORCID: https://orcid.org/0000-0001-7609-9287

after our wallets.[4] Looking at the statistics, we can also get a sense of how deeply the world is affected by this phenomenon. According to the Hungarian Central Statistical Office (KSH), there were 11 million mobile subscriptions in Hungary in 2018, which means 121.2 subscriptions for 100 inhabitants.[5] As the below table (Table 1) shows, according to Internetworldstats.com, more than half of the world's population are internet users, and at the same time, Eurostat states that out of ten internet users, eight are surfing via a mobile or smartphone.[6]

Table 1

Internet usage around the world

Source: www.internetworldstats.com/stats9.htm (29. 08. 2019.)



WORLD REGION	Population (2017 Est.)	% Pop.of World	Internet Users, 30-June-2017	Penetration (% Population)	Internet % Users	FACEBOOK % to total world population 30-June-2017
European Union	506,279,458	6.70%	433,651,012	86%	11%	3.35%
Rest of World	7,012,749,512	93.30%	3,451,916,607	49%	89%	22.98%
Hungary	9,787,905	0.13%	7,874,733	81%	2%	0.07%
TOTAL WORLD	**7,519,028,970**	**100%**	**3,885,567,619**	**52%**	**100%**	26.33%

According to the European Parliament, last year (in 2018) 71% of the European population shared their personal data online, but only 15% of them felt that they have control over it,[7] which shows that we need better and more secure ways to protect our personal data. With this said, we also store a huge amount of personal data on our mobile devices, which obviously needs to be protected. One of the trendiest ways to protect our data is by using biometrics. This article aims to introduce the ways to secure data with a special emphasis on mobile biometrics, and the possible risks they hold. Later, we will also show the results of a survey we conducted to find out more about the attitude of users to biometrics and to examine their usage and knowledge of it.

2. Mobile biometrics

In this section we are going to introduce methods of secure access control, with a special focus on biometric identification.

[4] 'Az új általános adatvédelmi rendelet (GDPR),' Európai Parlament, Hírek, 22. 08. 2018. Available: www.europarl.europa.eu/news/hu/headlines/society/20180522STO04023/az-uj-altalanos-adatvedelmi-rendelet-gdpr (04. 30. 2018.)

[5] 'Digital Transformation Monitor,' European Commission. Available: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Secure%20access%20control%20v1.pdf (10. 01. 2017.)

[6] Vishwath Mohan, 'Better Biometrics in Android P.', Google Security Blog, 2018. Available: https://security.googleblog.com/2018/06/better-biometrics-in-android-p.html (28. 10. 2020.)

[7] 'Az új általános adatvédelmi rendelet.'

2.1. Secure access control

There are several ways to protect personal data on our mobile devices with secure access control, which 'can be defined as a system capable of identifying who enters or leaves an area of control and managing the admittance of the person to the building, a specific space or site.'[8] In this group we can differentiate:

- Mechanical keys;
- PIN codes (via various solutions);
- Passwords;
- Identifying cards (for example badges, magnetic strips);
- Biometric systems (for example fingerprints, face scanners);
- Combined solutions.[9]

There is another way of grouping authentication methods, based on the mechanism:

- knowledge factors: they require something the user knows (for example password or PIN);
- possession factor: they require something that the user has (for example badge or token);
- biometric factor: they ask for something on the user's body (for example fingerprint or iris).[10]

During the more traditional authentication methods, systems are just verifying if you have or know the key, but they do not check whether the owner of that particular badge or password is the one trying to access the protected area. This concern can be addressed by biometrics.

From the above list, passwords are among the most known methods of authentication. Passwords are convenient to implement, require minimal hardware and exact match. They can be most effective if they are hard to guess (they do not contain words, but random characters, numbers, upper and lower case and special characters as well). As mobile devices are used frequently and users require fast experience, difficult passwords are not the best choice. While we are discussing authentication methods used in mobile phones, we have to mention pattern locks, which allow users to choose a preselected sequence of points as authentication. These are almost as secure as PINs, they are convenient and easy to remember, but they can be also seen by others and the oil from the skin can leave a trace on the unlit screen which can indicate the used pattern.[11]

2.2. Biometric identification

From the above list, biometric identification is an automated technique which measures and registers the physical and behavioural features of an individual and use them for

[8] 'Digital Transformation Monitor.'

[9] Ibid.

[10] Mohan, 'Better Biometrics.'

[11] Liam M. Mayron, 'Biometric Authentication on Mobile Devices,' *IEEE Security & Privacy* 13, no 3 (2015), 70–73.

identification and authentication purposes.[12] We can distinguish two main categories: physical and behavioural. The most commonly known in the physical category are fingerprint, iris and face. The most prevalent behavioural are voice, handwriting and walking for example.

Mobile biometrics refers to the application of biometric authentication on mobile devices like smartphones and tablets, usually with the following methods:

- fingerprint recognition;
- face recognition;
- iris recognition;
- voice recognition.

Each of these methods try to recognise as many unique points from respective body parts as possible. Once these are recorded and stored in the system, new samples (when an individual is trying to access the system) are collected and compared to the stored template. If they match, the access is granted, if not, the access is denied.

In mobile biometrics in general, it is easy to implement most of these methods in smart phones and tablets as they already have the necessary sensors (for example camera or microphones), the computing power and storage in most cases.

Biometric authentication is very convenient as we can just use our body parts which are always with us, we do not have to remember and type in difficult PINs or passwords, and we do not have to have our badges with us. The main disadvantage though is that they cannot be or are much harder to be changed. Once they are compromised, misused, they cannot be used again, so those systems which are using biometrics require a higher level of security, more advanced or new methods of protection. Biometrics can be most effective if they are used combined with other methods of authentication.

3. Risks

As every method and system, biometric identification and authentication has its risks and threats as well, and it is important to highlight these, in order to avoid overconfidence in it. Security threats which can cause system failures can be divided into four categories for biometrics:

- DoS (Denial of Service): it means that a legitimate user is not able to access the system.
- Intrusion: it means that an unauthorised user accesses the system.
- Repudiation: it means that an authorised user accesses the system and denies it, claiming that an unauthorised user was acting instead of them.
- Function creep: it appears when a biometric system is exploited and data is used to access another application than originally intended, connection

[12] Tibor Kovács, István Milák and Csaba Otti, *A biztonságtudomány biometriai aspektusai* (Pécs: Magyar Hadtudományi Társaság, 2012).

between two identity records of the same person can be linked from two different sources (without their knowledge).[13]

Based on the source of threats we can distinguish between intrinsic limitations and adversaries. The first means false matches and false non-matches, when the system lets unauthorised people in or when authorised people are not let in. The latter, the adversaries, can be divided into further groups, namely internal and external threats aiming to abuse the system. These attacks can appear at any time of the identification process which we already outlined, so during the enrolment and the recognition phases there are several ways to attack a system. The types of internal attacks are briefly the following:

- Collusion: it means that an authorised user abuses and attacks the system, possibly in collaboration with external forces with malicious intentions.
- Coercion: similarly to the previous one, this includes an authorised user's attack, but with an important difference: the user is forced, coerced by an external threat to attack.
- Negligence: negligence of the authorised users can be a source of threat, too, for example, allowing tailgating or failing to log out from systems can also grant unauthorised people access.
- Enrolment fraud: it occurs when an originally unauthorised person is enrolled in the system, so they can access easily. To avoid this, systems can use de-duplication, which means that they do not allow the system to have the same records for more than one identity. (This process is a bit difficult for mobile application use, but can be useful for example in border control, when this kind of risk is higher.)
- Exception abuse: it means that the attacker abuses the system's fall-back mechanism which allows it to handle exceptions. Handling exceptions in systems increases risk, so it should be kept on a minimum level if possible.

Other types of adversary attacks target the different parts of the system:

- Infrastructure: in this group are sabotage (physical damage to infrastructure) and overloading (flooding with access requests so that it stops working).
- User interface: these include impersonation (unauthorised user tries to access disguised as an authorised one), obfuscation (trying to avoid being identified by changing characteristics intentionally) and spoofing. This is the most commonly known and interesting method, it means that artificial, counterfeit traits or body parts are submitted to be checked, for example rubber fingers, photos of a face or recorded audio.Biometric security systems aim to check if the submitter of the live sample is indeed live, in order to avoid this threat.
- System modules: these can be unauthorised modification (of a software component in the system) or exploitation fault (looking for loopholes or faults in the configuration to abuse the system).

[13] Anil K. Jain, Arun A. Ross and Karthik Nandakumar, *Introduction to Biometrics* (London: Springer, 2011), 260.

- Interconnections: these include man-in-the-middle (a third party is joining the communication between two sides without their knowledge, influencing the communication), replay (holding back parts of communication and resending it later for the recipient) and hill-climbing attacks (basically a brute-force attack of the biometric system).
- Template database: it means that the templates could be accessed or modified or that they are accessible for unauthorised people in case of leakage.[14]

So in short, we can see that there are several ways to attack and abuse these kind of systems as well.

According to Ashbourn, biometric data can be a good source of identification, however they cannot be considered unique. This means that the risk of false positive is real, so a person can be identified and matched to an incorrect sample. In theory, gathering more and more samples over time, the risk of false positive matches can increase, so the threshold percentage of acceptable difference between the stored and live sample can be changed accordingly. Lowering the threshold means a lower level of security and therefore trust in the system, so it is hard to find the balance.[15]

Another important aspect of biometric solution risks to highlight is that attacks can target the biometric data itself, as we could already see from the previous section. So generally we need to apply a higher level of security on the template as well, since once this data is compromised, it is harder to be modified and used again for the same purpose. This is why the above mentioned big players answered to this threat by paying special attention to secure storage. According to Veridium, the other possible solutions for adding more security can be for example de-identifying data or using a visual cryptography scheme. De-identifying means that the biometric data is stored in a transformed format and it is paired with a cryptographic key which makes data dissimilar to the actual biometric data.[16] Visual cryptography scheme on the other hand suggests that instead of using the usual public and private key method, the data is encrypted into multiple folders, so they mean nothing if checked by themselves. To see the original data, you have to combine them and you also have to have the right to do that.[17] Using these principles, this company uses a distributed model for smartphones, which means that the biometric data is divided into two files or sheets (using the above mentioned extra security actions), one is stored in a trusted server, and the other half is on the smart phone's secure storage.

Now that we know the possible type of risks, we can have a brief look at the performance measurement as it can help measuring how the system operates, how healthy it is and where possible risks can appear. As we already mentioned, there is a possibility of false match or acceptance and false non-match or non-acceptance, which can both be turned into rates showing the amount of these scenarios with FMR (false match rate), FAR (false accept rate) and FNMR (false non-match rate) and FRR (false reject rate). False or true match refers to the situation where a live sample is or

[14] Ibid. 266–284.

[15] Julian Ashbourn, *Biometrics in the new world* (Berkhamsted: Springer, 2014), 26.

[16] 'Biometric Privacy is of the Utmost Importance,' Veridium: Hands On Security, 2017.

[17] 'Protecting Your Most Private Data – Your Biometrics,' Veridium: Hands On Security, 2017.

is not matched against the template, so these rates show the accuracy of the system. Accept and reject measurements are quite similar to match measurements, but they are transaction oriented, they examine if an identification was successful or not.[18] At the point where FAR and FRR are equal, we can get the EER (equal error rate). ACOM (Anti-Cloning Operation Methods) shows the extent to which the device's operating principle excludes the use of a counterfeit sample. MOA (Mission Oriented Application) shows the possible security-related tasks of a given device.[19] Android uses some other metrics too, such as SAR (spoof accept rate) and IAR (imposter accept rate), which shows how easily an attacker can access the system with these methods.[20]

4. Survey

To get a picture of the attitude of peers and people around us, we conducted an online survey with 9 questions (plus demographics). As this article was created at the time when biometric authentication was considered to be implemented at the university faculty, we took the opportunity and examined the attitude there, which can explain the sample characteristics. We gathered 224 answers: 66% of the respondents were male, 34% female. 53% of them live in the capital, Budapest, and 40% of them live in a city in the countryside, so most of them are from cities and only 8% of them live elsewhere. 54% of the respondents are students (university), the rest of them have a job already (9% of them in a leader position). 54% of them has a graduation certificate and 35% of them have finished college or university. Our sample is quite young: only a few (3%) are Baby boomers (born 1946–1964), 13% are from generation X (born 1965–1979), 33% are from generation Y (born 1980–1994) and half of them (50%) belong to generation Z (born 1995–2010). All of the above mentioned features can influence the results of the survey, which cannot be considered representative.

Before we present the questions and answers, let us provide a short overview of generations, as those are the basis of our age group divisions. Generations are a group of people born in the same period, who were about the same age at the important points of their lives (e.g. finishing school, getting married, starting a job, etc.). In this article we mention four generations, Baby boomers (people born 1946–1964), generation X (1965–1979), generation Y (1980–1994) and generation Z (1995–2010). These groups were at different ages when new technologies such as smart phones and internet became parts of our lives, so they reacted differently and they feel differently about this new world. Those who were born before the age of internet and have lived their childhood without it, they had to learn how to use it, they trust less this new era generally, and they are less comfortable using it.[21] Baby boomers are considered to reject and redefine traditions (compared to their parents), generation X are usually skeptical, self-reliant and risk-takers, generation Y are the hopeful generation who want to achieve self-actualization with meaningful work and generation Z are the

[18] Jain, Ross and Nandakumar, *Introduction to Biometrics.* 18.

[19] Kovács, Milák and Otti, *A biztonságtudomány.*

[20] Mohan, 'Better Biometrics.', 488.

[21] Dóra Gelencsér 'Generációk különbségei: X, Y, Z és alfa az iskolában,' TanTrend, 02. 28. 2018.

ones who receive the greatest impact on their lives from technological development and globalisation. They are the smallest group from the smallest families of the oldest mothers with the longest life expectancy.[22] According to another differentiation, certain parts of the Y and Z generations are also called 'digital natives'. They are those who were born in the world of digital media and the Internet after 1980. It is not difficult for them to adapt to new technologies and use them. As they were born later in development, these qualities become more and more natural to them. Another grouping category is 'digital immigrants', suggesting that members of this group have learned to use new technologies, and that it is difficult for them to adapt these technologies to their abilities compared to their digital native peers.[23]

The first question was about identification methods used by the respondents (they could mark multiple answers). Below we can see the figure (Figure 2) which shows the results according to to generations. It is visible that the three most popular answers are PIN codes, passwords and biometric identification, which is not very surprising. We can also observe that the answers are not related to age.

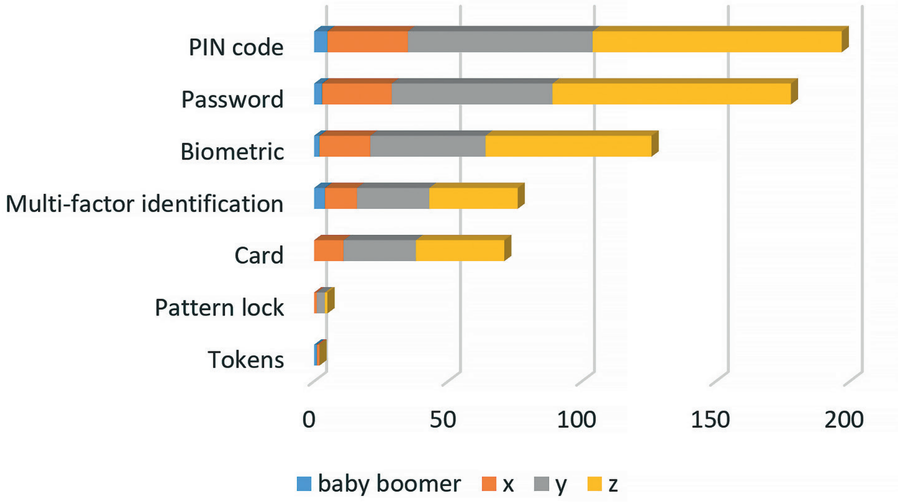


Figure 2

Identification methods used by respondents, n=224

Source: edited by the authors

If we examine this compared to gender, using Pivot tables and frequency analysis, we can see that male respondents are familiar with more identification methods than females. We can also observe that older generations know more types than younger

[22] Anita Kolnhofer-Derecskei and Regina Reicher, *GenYus – Y generáció az Y generáció szemével*, Vállalkozásfejlesztés a XXI. században, Vol. VI, 2016.

[23] John Palfrey and Urs Gasser, *Born digital* (New York: Basic books, 2008), 1–33.

ones. This can be due to lack of experience in this field for the young, or this can also be due to the recent changes in technology which made certain techniques for identification (such as biometrics) more popular.

The next question was about which biometric identification methods are known by respondents. The result is shown on the below figure (Figure 3). It is visible that the fingerprint and palm print recognition (19%), eye based (18%) and face (17%) recognition are the most well-known, possibly because recently they have been built into smartphones and they are getting more popular every day. Interestingly, for a test, we included a fake possibility, too, and noticed that 17 respondents said that they are familiar with muscle tone based identification, which shows that there might be some respondents who marked that they know a certain method, but are not really familiar with it. It was also visible that only younger respondents said they are familiar with this made up method.

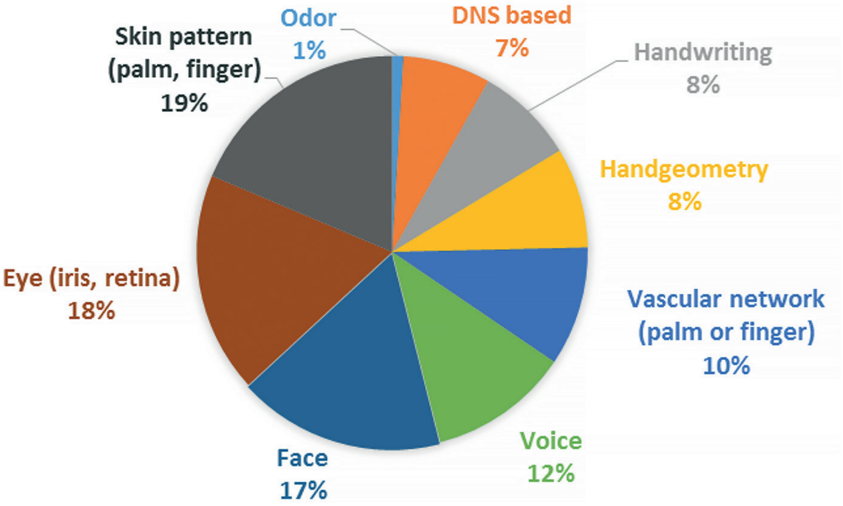


Figure 3

Types of biometrics known by respondents, n=224

Source: edited by the authors

One quarter (24%) of the respondents said they did not use biometric identification in their daily life. 70% of the respondents, however, uses biometrics on their phone, 39% of them uses biometrics in access control systems (at work or university), and about 27% uses it on other type of devices such as tablets or laptops. We studied these responses in relation with demographics using Pivot tables and we saw that if we consider generations, the older the respondents are, the more likely they use other devices than smart phones with biometrics, generation X and baby boomers reported to use tablets and laptops with this feature more frequently. Of course these answers were possibly affected by the fact that 17% of the respondents' phones do not have sensors for biometric identification. The respondents use biometric identification to unlock their phone (70%), accessing applications (30%) and verifying payments (30%).

Respondents were also questioned about their attitude to biometric identification; firstly, about their opinion about the usage of this method on a scale from 1 to 10 (1 means they would never use it, 10 means they would always). In average the answer was 7, the median was 9, which shows that users are happy to use this method in general. Based on the scale from 1 to 10, we created three main categories of attitude, which will be true for the next two questions as well. An answer from 1 to 4 means rejection towards biometrics, from 5 to 7 the answer means uncertainty, 8 and above means openness to biometrics. We discovered that age does not affect the usage or acceptance of biometrics (p=0.54) despite our preliminary assumptions, because more than 60% of both digital natives and immigrants answered that they were open to use it.

We were also interested how safe they think biometric identification is, where 1 meant not at all, 10 meant that they trust it completely. The summary of the answers are visible in Table 2. The average and median for this point were both 8, which means that this method is considered to be quite trustworthy. We examined the answers in relation with generations with Chi-square test as well, because our hypothesis was that digital natives are more comfortable with this technology. We discovered, however, that based on the sample, age does not affect the sense of security for biometrics (p=0.47), because more than half of both age groups answered that they think it is safe to use.

Table 2

Summary of the scale questions, n=224

Source: edited by the authors

	Like using biometrics	**Think biometrics are safe**	**Would pay/is paying with biometrics**
Median	9	8	7
Average	7	8	6

The last question was if they like to pay or would pay with this method if it were possible for them (1 meaning not at all, 10 meaning every time). The median was 7, the average was 6, which shows that payment is something they consider more private, where they need to be more careful. We also examined the answers in relation to age, and found that age does not affect the attitude towards biometric payments (p=0.59). Interestingly, however, we could notice with frequency analysis that for younger generations, the answers were more on the upper side of the scale, and the older the respondents, the less trust they have.

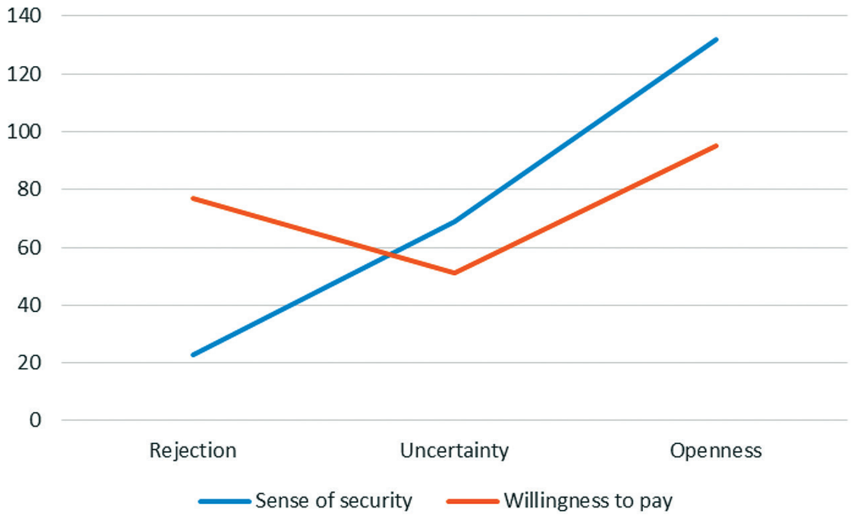


Figure 4

Sense of security vs. Willingness to pay, n=224

Source: edited by the authors

We compared the perception of security with the willingness to pay with biometric data. The diagram above (Figure 4) shows the distribution of the answers. It is remarkable that while the question about the sense of security can be represented in a linear line, which means that most people are open to it in the sample, this cannot be said about the line representing the willingness to pay with biometric data. There we can also see a higher rate of clear rejection and clear openness at the same time. We examined the grouped answers to these two questions together as well and we discovered that there is a significant relationship between the sense of security and the willingness to pay with biometrics (p= 0.000000006). This means that some of those who think the method is safe, are not always comfortable paying with biometrics. That can mean that the amount of available information about biometric payment, practices and security measures are not sufficient for them to feel comfortable to pay. This suggests that transparency, awareness and openness about this technology is important on the providers' side, and to raise trust on the users' side.

In summary, based on the sample it can be stated that biometrics have a good reputation among the respondents, they feel that it is safe and reliable, but they are still uncertain about paying with it, they have doubts about the technological background. We can also see that being a digital native does not necessarily mean stronger knowledge and awareness of new technologies, digital immigrants in this analysis were competent as well. Implementing the biometric authentication system at the university seems to be an acceptable solution based on this survey.

5. Summary

In this article we introduced the ways of secure access control, with a special emphasis on biometric solutions. Apart from secure biometric data storage, there are several other types of threats, so we provided a short description of the possible risks of biometric systems. In order to understand the status and attitude towards biometrics, we conducted a survey as well. According to our respondents, PIN codes and passwords are still the most familiar types of identification, biometrics are the third, and it is also well-known by each age group. Within biometrics, fingerprint, iris and face recognition were the most known, but in general 24% still do not use biometrics in their routine. If they use it, it is most likely they are doing so on their smart phones: older people possibly on more types of devices, but younger generations usually use it only with phones. The most common use is to unlock phones, only around 30% are paying or accessing applications with this method. In summary we can observe that biometrics are thought to be reliable and popular, but when it comes to paying with biometric data, respondents are less decisive.

In the future, we are planning to examine how the above outlined mobile biometrics related risks can be avoided or handled.

References

Ashbourn, Julian. *Biometrics in the new world.* Berkhamsted, Springer, 2014. DOI: https://doi.org/10.1007/978-3-319-04159-9

'Az új általános adatvédelmi rendelet (GDPR).' Európai Parlament, Hírek, 22. 08. 2018. Available: www.europarl.europa.eu/news/hu/headlines/society/20180522STO04023/az-uj-altalanos-adatvedelmi-rendelet-gdpr (04. 30. 2018.)

'Biometric Privacy is of the Utmost Importance.' Veridium: Hands On Security, 2017. Available: www.veridiumid.com/blog/biometric-privacy-is-of-the-utmost-importance/. (28. 10. 2020.)

'Digital Transformation Monitor.' European Commission. Available: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Secure%20access%20control%20v1.pdf (10. 01. 2017.)

Gelencsér, Dóra: 'Generációk különbségei: X, Y, Z és alfa az iskolában.' TanTrend, 02. 28. 2018. Available: http://tantrend.hu/hir/generaciok-kulonbsegei-x-y-z-es-alfa-az-iskolaban. (28. 10. 2020.)

Jain, Anil K. – Ross, Arun A. – Nandakumar, Karthik. *Introduction to Biometrics.* London, Springer, 2011. DOI: https://doi.org/10.1007/978-0-387-77326-1

Kolnhofer-Derecskei, Anita – Reicher, Regina. *GenYus – Y generáció az Y generáció szemével.* Vállalkozásfejlesztés a XXI. században, Vol. VI, 2016. Available: http://kgk.uni-obuda.hu/sites/default/files/17_Derecskei-Reicher.pdf (28. 10. 2020.)

Kovács, Tibor – Milák, István – Otti, Csaba: *A biztonságtudomány biometriai aspektusai.* Pécs, Magyar Hadtudományi Társaság, 2012.

Mohan, Vishwath. 'Better Biometrics in Android P.' Google Security Blog, 2018. Available: https://security.googleblog.com/2018/06/better-biometrics-in-android-p.html (28. 10. 2020.)

Mayron, Liam M.: 'Biometric Authentication on Mobile Devices.' *IEEE Security & Privacy* 13, no 3 (2015), 70–73. Available: https://ieeexplore.ieee.org/document/7118088. (03. 20. 2019.) DOI: https://doi.org/10.1109/MSP.2015.67

Palfrey, John – Gasser, Urs. *Born digital.* New York, Basic books, 2008.

'Protecting Your Most Private Data – Your Biometrics.' Veridium: Hands On Security, 2017. Available: www.veridiumid.com/blog/protecting-private-data-biometrics/. (28. 10. 2020.)