WHY DOES IT FAIL TO OPERATE?

Csaba Otti

Abstract: The aim of this study to examine the user attitude towards errors experienced when using biometric access control systems. In the 20th century using access control systems within the corporate sector became natural. Biometric identification of users and employees in Hungary at companies began to spread mainly after 2000. Biometry is the first access control method that requires true cooperation from users, successful and unsuccessful identification can be defined by probability variables and authorised users can be rejected even if the biometric sample was perfectly positioned. Based on case studies, the biggest risk is if a large throughput system has the false rejection of authorised users. This study examines what users think of the system if they are rejected at an access point while being authorised. According to one respondent's answer on the question of how one would feel if rejected at the access point also served as the title of this paper.

Keywords: biometry, access control system, user behaviour, qualitative technique

Introduction

Nowadays biometrics has become an everyday feature in all aspects of life. Looking at security a wide array of solutions is at the disposal of experts, yet we still hear about a large number of unsuccessful projects.

One of the purposes of this study is to identify the typical usage areas of biometrics through a scientific approach and determine the factors that make the introduction of such a system more risky in certain cases. Risk factors will be examined based on which we will demonstrate the two areas that suffer from the biggest risk of a failed system deployment. These are the large user base access control and attendance tracking systems. The manufacturers of biometric identification systems provide false acceptance and false rejection rates, however, these are algorithmic values – in reality, the performance is worse by several orders of magnitude. Nevertheless, devices operating even within this range can be considered good based on the experience. The other purpose of this publication is to examine the hypothesis which states that false rejection rates at 1-5% which are worse than 0.01% by orders of magnitude are still considered good by users, as in practice they get stuck at the various physical restrictive elements of access control systems with that probability. To determine the threshold of user tolerance towards an access process within which they still consider it good or adequate, we plan to perform a questionnaire based research. A step in this was a focus group research, the result of which can be read in this publication.

Usages of biometric identification

Automatised electronic biometric personal identification has gone through a tremendous development in the past fifty years. Law enforcement agencies have an ever

growing need for the ability to identify people anywhere, anytime with high speed and certainty. Parallel to this, there is also an ever expanding need to identify users, incoming people and authenticate access throughout all aspects of life. It can be observed that the acceptance of such systems and the attitude of the users towards them largely influence the success and usability (Dillon, 1996).

When considering security applications users are general much more suspicious and rejecting than in the case of commercial applications where it is up to them whether they wish to use the solution or not, the biometric sample never leaves their possession and it is convenient to use. A good example that while general purpose biometry is rejected by the users (Suplicz, et al., 2006) (Földesi, 2015), 89% of iPhone users employ biometry in their phones (appleinsider.com, 2016).

One might justly ask what distinguishes the various applications, what their properties are and how they can be classified. The next part of the chapter will answer this. (Otti, 2016.)

1. **Law enforcement:** Biometry has been used to identify suspects for a long time by law enforcement agencies. These are mostly AFIS solutions, short for Automated Fingerprint Identification System. This system works by analysing fingerprints and fingerprint fragments then returning the best possible matches. Then forensic investigators check these results with traditional methods (Komarinski, 2005). However, multiple research projects are underway to enable real time support of law enforcement units in the field (Földesi, 2017).

    - A Hungarian connection is the deployment of the new biometric personal identification cards, started in 2016. This allows for the further spreading of law enforcement solutions and a much more efficient identification process. Similarly to biometric passports these cards feature an RFID smartcard which can hold the fingerprint of the user along with other possible biometric samples and data (Balla, 2013).
    - Biometric personal identification enables law enforcement to automatise identity checks with a portable device that facilitates data acquisition, database queries and provides a high accuracy verification. This technology does not allow for general identification for regular citizens as biometric data can only be stored on the card itself according to Hungarian law. If, however, the person is wanted, their data are held within a central database. A properly deployed system has a constant connection to this database and allow for the identification of people who otherwise would hide their true identities. Protection of the data on the cards is a risk factor, however, since depending on the security level of the chip, swapping the data stored within with forged credentials might be possible. A further risk factor is the large userbase. While law enforcement officers do not have to care about the required time for an identity check – at most, only for the sake of increasing their own performance – the system has to be extremely accurate to ensure that it does not falsely identify an innocent person as a wanted one. This requires a proper algorithm and high system performance.

2. **Background checks:** Many government agencies and private companies require biometric identification to fulfil certain roles and positions. Biometric features of candidates are taken (generally face and fingerprint) and sent to the authorities to gain information about any past transgressions. In case of private checks, the biometric data is destroyed at the end of the process.[1] In essence, this can be considered an extension of the law enforcement application.
3. **Video surveillance systems (CCTV):** The traditional CCTV systems were observed in 24 hours by the guard detail. This task is extremely monotone and tiresome – thus biometric facial recognition and other intelligent algorithms help to keep up their concentration and performance efficiently. *„The purpose of these upgrades was to support surveillance crew, because surveys show that any person tasked by surveillance can ignore up to 95% of events on screen after just 20 minutes."* (Berek, 2014, p. 34). The backbone of such systems is the face recognition enabled camera and control software. For ideal operation, the system must learn the biometric samples – for which an adequate biometric sample must be presented to the system. If the surveillance system covers most of the protected area there is a possibility to automatically track the movement and actions of the surveyed people (Otti, 2014).
4. **Border Control:** The constantly rising passenger numbers resulted in a need for advanced technologies that automatise, speed and ease up border passing. Based on international standards an ever-growing number of biometric passports gets issued that contain iris patterns, fingerprints and facial information. An ever-growing number of countries deploy biometric passports based on international standards that can contain fingerprints, iris patterns and faces. Some countries like the USA requires the presence of a biometric passport (for countries from which the USA does not require a tourist visa, in the case of a visit not exceeding 90 days) while others only provide an opportunity to obtain and use them. Properly designed biometric systems relieve pressure from live force and allow them to focus their attention on risky individuals. The database of dangerous individuals contains the templates of people who are dangerous to society, and as such, their disposition and acceptance towards the handling of their data can be disregarded. Their operation can be supported with other systems which provide further filtering levels. False identification rates of biometric systems used for border control are smaller by several orders of magnitude than their false rejection rates, and as such, if someone was to sabotage the identification process, it would be much easier to provide an unidentifiable sample than to spoof the system such that it identifies the attacker as a different person. A major property of this application is that the user acceptance is generally not a factor. The users – if no alternative method is made available to them – must use the system whether they like it or not. If they arrive at a border where biometric identification is compulsory, they will either cooperate or turn back (risking drawing the attention of the border guards with suspicious activity and ultimately, arrest). Authorities

[1] Private enterprises have no possibility to do so, and in my opinion, government agencies are very limited, as well in Hungary.

can disregard user opinions, the singular criterium in this case is efficiency. Naturally, however, this does not mean that the authorities shouldn't develop a high-performance system for at least their own sake – but this is not a risk factor. Compatibility of biometric passports is ensured by adhering to ICAO9303, which allows for any country to read them and utilise the samples stored within.

For the EU, and within, for Hungary, migration is one of the biggest challenges nowadays. (Balla, 2013). *"Migration did, does and will exist. One of the most marked globalisation factor within the 21st century is migration, which causes social-economical-ethnical-religious etc. problems. It is a complex process that can gravely endanger national-regional security but it can be a source of wealth, ending population decline, good statistics and a humanitarian solution. In summary: though it is very hard to handle, it must be handled."* (Görbe Zán, 2010, p. 4). Miklós Böröcz police lieutenant colonel have been examining the terrorist attacks targeting the western countries since 2001 and showed that they were committed generally by second or third generational migrants, however, it is a fact that illegal migration and organized crime are in close relation (Böröcz, 2015). Hence, recording biometric data from immigrants would be paramount in order to allow law enforcement agencies to root out criminalising individuals early on and in time.

Employing biometric passports raise several data security questions though from multiple standpoints. These passports, are in essence, RFID Smart Cards (radio frequency contactless intelligent chipcard) where the actual template is stored on the chip. They have to be adequately protected since they can be read from a short distance, and with a proper reader, data can be obtained from them, hence it is important to consider what kind of data are stored and how it is encrypted. Based on the standard ISO/IEC 14443 at least 32 kb of data is stored. The previously mentioned ICAO document states that different manufacturers use proprietary methods to encode samples and match them to the stored templates. Due to this, passports actually store raw biometric data in the form of images to ensure interoperability. This is a huge security risk as obtaining raw biometric data can be the source of a whole host of abuse as opposed to obtaining a template encoded with non-reversible coding.

5. **Reduction of frauds:** The various methods of fraud – abusing personal data or financial abuses – present a good opportunity to deploy biometrics in an effort to reduce or eliminate them. ATMs protected by biometry reduce the risk of fraud and also make banking services available for those who would not be able to use them otherwise. There are plans for this in India, where one of the biggest biometric databases were established by the authorities which is supposed to provide access to banking and state services for everybody (and also render citizens reachable for the state). The first such ATM was deployed in 2016. With this device, either the credit card or the ID number of the owner starts the transaction, but to authorise it the biometric sample is required. When signing contracts proper biometric samples provide an established personal identity and a record that can be traced back. Such samples include signatures or general writing).
6. **Trusted passengers:** This application would allow otherwise trustworthy passengers to pass through access points faster and be selected for in-depth security checks at a reduced rate. Participation in such programmes is

voluntary and is only available after clean background check results. Passengers can use their fingerprints or irises to pass through the simplified check-in process. Samples are recorded on authority issued smart cards. (Kovács, 2015).

7. **Access control systems:** Biometric identification is an effective method to facilitate physical access control as it allows for personal identification rather than object or knowledge based identification. (Kovács, et al., 2012, pp. 486-487). The most popular samples used in access control are fingerprints, irises, face and vein patterns. The systems can be broken down to two large groups, which are 1:1 and 1:N. In the first case, the system matches the presented sample against a pre-selected template and determines whether the two are similar enough. The sample can either be stored in a local database or can be owned by the user. In Hungary, the latter solution is the only legal possibility, such that the samples are stored on an RFID smart card. In 1:N operation, the presented sample is matched against the entire database of users, and the system looks for the best matching template – with regards to the general security level determined by the actual setup. The application is negative – its aim is to filter anybody who is not authorised to pass through a given access point at a given time. There are alternative – albeit older – methods to biometry, which are knowledge based (PIN or password) or possession based (card based) systems, however, they can be circumvented rather easily, which, in some cases might demand a higher security level. Biometric identification systems generally face higher performance expectations from the users since they have to strike a balance between the low false acceptance rates required by the negative identification method and the low false rejection rates that corresponds to the required throughput (although in application where access speed is not cardinal, the latter can be disregarded).
8. **Attendance tracking:** Biometrically tracking employee worktime can minimalise both administration and errors, mistakes, over- or underpayment and fraud. (Otti Csaba, 2011). Attendance tracking systems can exist as parts of an access control system or as individual systems. Their objective is to clearly assign a personal identity to a check-in, preventing any controversial situations in the future. Furthermore, it allows for automatized processing of worktime data and provides an easy access to them for the employees as well – if needed. The criteria set up for access control systems are expanded with proper identification speed as it is imperative to prevent the forming of large lines. It is important for both access control and attendance tracking systems that users accept and effectively use them.
9. **Customer identification**: Nowadays, mostly PIN codes, tokens and signatures are used to identify members of trade transactions. With biometry these solutions can be phased out or at least reduced to increase security and the sense of security as well. Furthermore, users can be brought into trade who are not skilled the traditional identification methods like very young and elderly people. (ISO, 2011) (ISO, 2010).
10. **Remote authentication:** A cardinal question in the creation of information security is the security of remote access and rights management for

computer networks. The most frequent usages are mobile or computer based bank services, web based applications and employee remote access to the company network.

11. **Protection of property:** Biometric identification replaces or supplements the classical security systems in this case – for example, in a NATO document repository protecting the safes containing paper based documents with fingerprints or disabling alarm systems with a palm vein identification system. (Berek, 2014). This application is intertwined with access control.
12. **Logical access control:** Using biometrical identification to access servers, databases, health- or financial data. According to Michelberger logical access control means protection of data integrity, virus protection, encryption methods and control to computer access. (Michelberger, 2013). Employing biometry in this application reduces the dependence of security level on the end user and is more convenient than traditional solutions – as one does not have to demand learning long passwords (that are hard to crack and to remember as well) from users.

The above list has to be expanded with a 13th item, which is the biometric protection of mobile devices. Laptops and Android-based devices have featured biometric identification since the early 2010's but the breakthrough came in 2014, when the iPhone 5S came out with fingerprint recognition capabilities which introduced several million users to the world of biometry. Parallel to this, biometric identification (fingerprint, iris, face) became a base functionality on newer Android-based devices. The iPhone 6S device features secure mobile payment through the Apple Pay service. It is important to note, however, that biometry in these cases is never the only solution – as there is always a compulsory fallback option to be used which is one of the traditional methods. Moreover, when starting up the device biometric sample cannot be used for the first unlock – it has to be either PIN, password or an unlock pattern.

This means that the protection of the phone is only as strong as the fallback option. Since most phones do not enforce a password policy (they do not require a secure password), biometry in this case can be reduced to a simple convenience option. For example, in the case of a pattern based screenlock[2], biometry only spares the user from drawing the pattern every time they wish to unlock their phone and allow for a simpler unlocking process. However, anybody can get the pattern by simply looking at the phone when the user unlocks it using that method – which is much easier than obtaining a difficult password) and bypass the biometric protection. Since the biometric settings can usually be found deeply in the setup menu of the phone, one can essentially record themselves into the phone without a high risk of detection if not all pattern slots are used. The number of recorded templates can generally only be seen from the enrolment menu which most users do not visit often (and which is, again, protected by the fallback option). This enables a silent, nearly undetectable access to the target phone although the attacker can also opt to simply lock the original user out of the device.

Many mobile devices have a safety feature which essentially factory resets the device deleting all data irrecoverably in the process if a certain number of failed login

[2] A pattern lock is a 3x3 grid consisting of nodes, where one has to use the nodes to create a pattern of straight line sections that will unlock the device. The sections can overlap each other, but every node can only be used once. A pattern must consist of at least three nodes.

attempts are made (the actual number varies between devices). A further possibility is to expand biometric identification to log into certain websites. In that case, the username/password combination is swapped in favour of a biometric sample, which unequivocally identifies the user. The application range of biometric identification is far-reaching, and even this short summary shows that every application has its own set of criteria towards the biometric devices. In the next chapter, I will introduce the circumstances of the applications, the attitude of their users and demonstrate why access control and attendance tracking are the two highest risk applications that prove to be the most challenging for companies.

Biometry and human attitude

Throughout our research we regularly faced a problem regarding the application of biometric systems. There are no biometric systems or devices that are universally good for any application and perform with the same efficiency throughout the full usage spectrum. Thus, the areas mentioned in the previous chapter should be further classified and grouped by several factors, as they have significantly different properties. Analysis of these will prove that the critical applications are access control and attendance tracking systems. But before the detailed factors let me be clarified the most important Rates:

- False Accept Rate: This is the possibility of the system accepting a person who should not be – either because not being in the database or because misidentifying him/her as a different person.
- FRR: False Reject Rate – This is the possibility of the system rejecting a person who otherwise should be accepted and is legitimately present in the database. The FRR is the ratio of false rejections and all transactions. Experience shows that this is one of the most important factors that truly define the usability of a biometric system. With an increase of user number, obviously there is a bigger statistical chance that false rejections will cause problems for the users.
- EER: Equal Error Rate: This is the ratio where the probability of false acceptance and false rejections are the same. This is the optimal setup point for a device and algorithm, because the FRR and FAR graphs intersect here. Deviating from this point in either the direction of security or convenience can only be done at the expense of the other. A system is more convenient, if it rejects authorised people less often, and it is more secure if the false acceptance rate is lower.

All of them are general probability variables and are treated as a quality control of a biometrics system.

1. **The number of people to be identified:** One of the biggest adversaries of biometric identification systems is the user number. While a smartphone usually has to recognise a single person – or a few at best –, in the case of a biometric identification document, the user number can be in the range of hundreds of millions. The problem stems from the probability nature of biometry. The general probability variables characterising biometry, such as FAR (False Accept Rate: This is the possibility of the system accepting a person who should not be – either because not being in the database or because misidentifying him/her as a different person.), FRR (False Reject

Rate – This is the possibility of the system rejecting a person who otherwise should be accepted and is legitimately present in the database. The FRR is the ratio of false rejections and all transactions. Experience shows that this is one of the most important factors that truly define the usability of a biometric system. With an increase of user number, obviously there is a bigger statistical chance that false rejections will cause problems for the users.), EER (Equal Error Rate: This is the ratio where the probability of false acceptance and false rejections are the same. This is the optimal setup point for a device and algorithm, because the FRR and FAR graphs intersect here. Deviating from this point in either the direction of security or convenience can only be done at the expense of the other. A system is more convenient, if it rejects authorised people less often, and it is more secure if the false acceptance rate is lower.) will not have perfect values and as such, will not guarantee a 100% acceptance or rejection even if the device and algorithm is extremely good. Generally, EER is given around 0.01% by manufacturers, and if we consider that, the system will make a mistake in every 10,000 transactions. In reality, however, capabilities are worse with 1-2 orders of magnitude, which means that the system will have problems in every 100 transactions (Otti, 2014).

2. **Convenience or compulsory use:** Obviously, if the user has an interest in using the technology, the attitude will be significantly different. For example, the biometric identification in mobile phones is clearly a convenience feature while the biometric reader of an attendance tracking system is a compulsory one – and the one that is the most rejected by users.
3. **Is there an alternative identification method:** Is it possible and acceptable to use a different method for identification in the particular application?
4. **Another important question is whether the identification is positive or negative:** Within the publication of Bunyitai, (Bunyitiai, 2011) positive identification is used in 1:1[3] verification, while negative is 1:N identification. Within this study the meaning is different. By positive identification we mean that certain individuals from a populace is sought: for example, identifying a VIP or wanted people or finding a terrorist. By negative identification, we mean identification of the authorised people and having the guard detail intervene when somebody is rejected.

Classification of applications

We classify the applications shown in the introduction by the standpoints in the previous point and see which ones should be put under further scrutiny.

Regarding user opinions, any application that has a viable alternative or is used for convenience is of less importance because who cannot use or do not want to use biometry can opt out. I have highlighted the two applications from the table above in which users must either use the system or there is no real alternative to biometric

[3] 1:1 verification is when identity is established by an identification step (e.g. by card or PIN) and the identity is then verified by biometry. 1:N identification is when the device looks up a database for the most likely match only by a biometric sample.

identification (naturally, this requires further explanation) and selection is negative – which altogether means that every user must use the system. These will put under further scrutiny.

Application	Typical user number	Convenience/ Compulsory	Alternative method	Positive/ Negative
Law enforcement	100.000+	Compulsory	Yes	Positive
Background checks	100.000+	Compulsory	Yes	Positive
Video Surveillance	1.000.000+	Compulsory	Yes	Positive
Border control	1.000.000+	Compulsory	Yes	Positive
Fraud prevention	100.000+	Compulsory	Yes	Positive
Travel	1.000.000+	Compulsory	Yes	Positive
Access control	1 - 5.000	Compulsory	Problematic	Negative
Attendance tracking	100 - 5.000	Compulsory	No	Negative
Customer verification	10.000+	Convenience	Yes	Positive
Remote authentication	10-100.000+	Convenience	Yes	Positive
Property protection	10-100	Compulsory	Yes	Positive
Logical protection	10.000+	Compulsory/ Convenience	Yes	Positive
Mobile	1-10	Convenience	Yes	Positive

Table 1 Applications of biometric identification

Source: author's own editing

Critical applications

Access control systems are a definitive area of electronic protection. Their objective is to restrict access to an area to only authorised people. Within the particular area further sub-areas can be created in order to fine-tune access rights and access levels – for example, a person who can enter the main gate might not be authorised to enter any server rooms, as well. While the basic function of access control systems is to restrict access to certain areas, the owner can opt for other functions as well – for example, attendance tracking. (Berek, 2014).

Evaluation of the table seen in the previous point will reveal the applications where introducing biometric identification bears the greatest risks.

User number

At low user numbers – about 50 people – using biometry generally causes no problems since company leadership can rather easily test prospective devices on every user and operation is more transparent and controllable. Beyond this, statistically there is a smaller chance to actually encounter a problematic biometric sample due to the low headcount. In practice, this means that virtually any biometric identification device will work according to its specifications if no other disturbing factors are present – for example, if a face recognition system is not installed at an external location where the sun periodically shines into the sensor.

Motivation for usage

It is obvious that if the users use biometry on their own accord or for their own convenience, their willingness of cooperation is vastly different when compared to situations where they are forced to use such a system. From this standpoint, both access control and attendance tracking is a critical application. These have the lowest acceptance rates of all biometric applications (Suplicz et al., 2006).

The task of attendance tracking is to record the presence (and in certain cases, the activity) of employees and pass the summarised data on to payroll at the end of the month. An accurate attendance tracking system is an advantage for any given company, as it allows for a more rigorous record keeping of actually performed work activity, which in turn allows for significant savings as they only have to pay for what the employee really did. However, it is also beneficial for the employees because in any controversial situation the system will clearly show the truth if the correct data are available.

In the case of an attendance tracking system opposing interests meet: the incentive of the employer is to only pay for the work done based on the narrowest possible interpretation of worktime while the interest of the employee is to have the most possible time accounted as worktime. We know of several methods to circumvent traditional attendance tracking systems, like “buddy punching”, when a colleague checks in with the credentials of another employee making it seem that the particular employee is present and is indeed working, hiding tardiness and unauthorised absences. The other neuralgic area is overtime because employees are entitled to extra benefits above the normal wage.

Such abuses generally happen when the employees work without a more rigorous oversight, in flexible schedules or the headcount is too high to effectively keep tabs on everybody.

Alternative identification methods

The opposing interests and operational features described in the previous point result in the fact that it is very hard to find an alternative for high userbase access control and attendance tracking, if it is possible at all. Naturally, the methods are available – such as PIN or card based identification for such purposes, but it is not prudent to use them due to the high risk of illegal access and fraud. These risks might rise past a point where deploying a biometric system loses its purpose altogether. Furthermore, the phenomenon of exists that those who have a vested interest in a less reliable attendance record will sabotage the system to try to coerce the deployment of a less secure “legacy” method. If companies allow this to happen, at worst case, the deployed biometric system has to be phased out (Otti, 2015).

The terminals employed for the task must also comply to a number of other criteria as well:

- It must feature an adequate interface to (depending on application) allow extra data to be input to the system.
- Tamper/vandal proof design: an attendance tracking system might cause animosity with employees if they feel that the company intrudes their private sphere too much – or if they in fact want to cheat and the new system is preventing them from doing so (the latter is a definite purpose

of a biometric system). By harming the device, they might try to emphasize that the system is fundamentally useless and pointless.

- The system must operate efficiently for users of any demographics, age and sex, for the number of employees that can be present at the given location: general employee number, borrowed workforce, guests, subsidiaries, employees of other factory units, inactive users, etc.

Type of the selection

In the case of attendance tracking and access control, selection is negative: the system must determine who is not allowed to enter. We have to examine which properties of access control systems are the most important in this case. The relevant performance indicators such as FAR, FRR, operational times and enrolment values were defined within Chapter 3.

FAR and FRR values are usually set to their intersecting point, the EER value by default (with a usual value of 0.001%-0.1% (Figure 1).

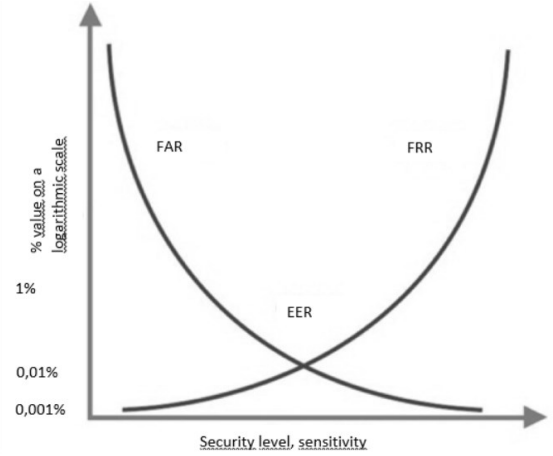

Figure 1 Sensitivity of biometric systems

Source: author's own editing

Given that we are considering a security system, FAR might seem to be the most important factor however this, in itself, is not true. In high userbase applications two factors modify this. The first is that at a manufacturing corporation it is rather hard to create access points which ensure that only one person can pass through at any given moment. Let us just imagine a truck entrance or a loading ramp where 10-15 trucks can park in simultaneously. In such a case, using only the technology without the help of a security detail, it is impossible to guarantee that no unauthorised entry occurs. The other factor is that the valuables to be protected are easily attacked with different methods (e.g. hacking, social engineering, etc.) than with the illegal physical access of attackers.

If we look at the FRR values, however, we can see that a bad performance on that front can fully cripple the system operation. In high userbase applications, a high FRR will cause a serious problem even if the protected facility justifies it and personnel is also trained to accept it because in practice even the first failed identification attempt might require the intervention of the security detail and they might even need to perform a manual identity check.

Considering attendance tracking systems, we have to take further factors into account – but to do so, we must understand what a faulty attendance record will result in and what kind of disadvantages it can cause. In the best case scenario, it will take extra worktime and administration to correct the errors while the workforce could have been doing something productive had the register been correct. The worst case scenario can have legal consequences ranging up to a direct lawsuit. Due to this it is very important that users can only use the system as themselves (which is its purpose). However, as we have described in the previous point, a negligently planned system might motivate users to try and circumvent or sabotage it. This means that it is not enough for the system to determine whether the person presenting the sample is the same person who was enrolled in the system – it has to do it with certainty, in other words, it should not reject authorised users falsely, or at least, in a minimal amount. Biometric identification is always relatively unpleasant when compared to knowledge and possession based methods as the user has to put in extra effort to achieve a successful identification. If the system does not work efficiently, the users can easily get frustrated (especially if they already have a negative disposition towards the system). Good performance is also very important when we consider the operation times of the system. It is not an easy task to define fast but it can be stated that the fastest biometric system is slower than any card based system – which in turn means that even that system will cause relative inconvenience for the users. Enrolment performance is important for both operation and system deployment. The most important question for an operator is whether the system will work for every user with an adequate security level (for example, hand geometry identification requires every finger on the hand to be fully present). For users, the more important factor is that they most likely meet the system first during the enrolment process and the first impression might be the key to the future disposition towards the system.

Further factors

While the parameters described in the previous point are subjective from a user viewpoint, it is possible to define them objectively. In the following section, a number of other factors will be listed which cannot be measured objectively but are very important regarding the acceptance of the system nonetheless:

- Misconceptions: a number of technologies are plagued with misconceptions that dominate the initial disposition and user attitude towards the particular system. A good example for this is the suspicion regarding iris scanners: many popular movies portray “eye scanning” (which they call retina scanning although in reality scanners examine the iris) where a laser beam scans the sample. Users might be afraid that the scanners will damage their eyes while the device actually uses harmless near infrared (NIR) light to illuminate the iris. Another misconception is that devices are extremely dirty because everybody has to use them resulting in user reluctance to touch them pondering how contaminated they are and what negative effects it might have – while they happily grab a doorknob without any second thoughts. Proper education and the deployment of appropriate technology (for example, contactless devices) can solve these problems.
- Privacy: As it has been stated, some companies handle biometric samples in their own local databases (although some countries mandate that the samples are

stored on devices which are in possession of the user)4 and employees might be worried about the safety of their data – for example, what third party gets hold of their biometric data or whether it can be obtained anybody – as data security is largely dependent on the software, hardware and protocol environment. The templates generated by biometric devise are irreversibly encoded, the original sample cannot be restored from them but this is not a well known fact among end users – and even if they know it, they are usually sceptical about this.

- Morale: certain employees (who otherwise do their work well) might feel that they are not trusted, which causes tension to build up in them – while the system will specifically protect their interests as well, since the company will not have to spend as much money on the employees who do not work well. As such, it is very important that the company communicates the reasons and advantages of the system before deployment. It will naturally also cause a morale drop for those who were behaving fraudulently because chances are that this possibility will end with deployment (Kovács, 2015).

Disregarding these factors is a big mistake for any operator since it will cause employee unrest, which is harder to solve than taking preventive measures with proper planning and preparation and communication. This naturally does not mean that the system has to cater for the needs of every single employee but the reason of deployment and the advantages must be clearly communicated.

The critical point of biometric access control systems at large headcount companies is whether the system can facilitate its tasks with adequate speed and certainty while providing the required security level.

Access control systems in practice

Virtually everybody has met access control systems: at work, in office buildings, preschool, school, university, museums, municipal offices or at airports. Most of them use some kind of proximity card based technology but PIN code and magnetic stripe cards also exist. These systems are almost always paired with some kind of physical barrier, for example a gate, turnstile, automatic door or revolving door. Figure 2 will show the general scheme of such systems.

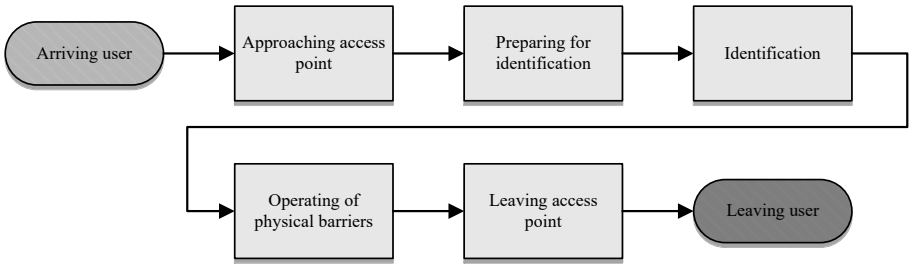

Figure 2 The general access process

Source: author's own editing

Their common property is that people can only pass through them with the proper clearance. Studying many implemented and currently working solutions we can say that many times that the physical barriers also stop authorised people as well, in cases like:

[4] Based on the currently valid NAIH opinions (Nemzeti Adatvédelmi és Információszabadság Hatóság – National data protection and information freedom authority) (19 March 2017) for Hungary as well.

1. The door warps and get stuck.
2. The electric lock gets strained in the door so it has to be moved into the opposite direction first to open it.
3. The sensor of an automatic door does not detect the person.
4. The user tries to pass through the turnstile to quickly while the lock did not release just yet, the arm gets strained and cannot be opened.
5. Drops the card while trying to hold it to the reader.
6. The system selects the user for bag/alcohol check.

When attendance tracking systems are concerned, we can say that in many instances it is tied to the access control system such that they use the same terminal – and if not, the same identification method is used nevertheless.

In case of biometric access control systems, the 0.01%-0.0001% false rejection rate (FRR) given by manufacturers only applies if the user presents the sample perfectly (4th stage: Identification) (Otti, 2016). However, in practice, experience shows that this value is a few magnitudes worse – between 1% and 20%. This value contains the physical access problems as well, but the user does not recognise this difference (Otti, 2015, p. 70.). Customer satisfaction must be measured in every case to ease the use of the IT system. To ensure this it is imperative that the customer company creates an even image of the system with every employee through internal marketing. This is important for the company as the employee is the face of the company but it is also important for the developer because a dissatisfied user is ultimately a negative advertisement (Reicher and Szeghegyi, 2015).

Examining the true FRR values is of critical importance for determining how good the system is. This paper begins the work of discovering user attitude and discover whether they experience false rejection in their everyday life and if so, what they think about it.

The research

When considering large user number biometric access control projects, we always see that the main concern of decision makers is the successful and fast admission of employees. But what can be considered successful if a number of employees regularly get stuck in the identification process? What is the user attitude regarding the everyday use of such a system? My hypothesis for which we seek an answer is that rejection rate orders of magnitude worse than the 0.01% (around 1-5%) is still considered good by users since they get held up by the physical barriers in similar amounts. In order to understand where the limits of user patience lie – the line between acceptable and unacceptable operation we planned to perform a questionnaire survey. An important step was a focus group survey the results of which will be disclosed in the following points.

Research pertaining the topic

Professional literature features user acceptance research in order to examine the various biometric technologies regarding human factors. Most of these researches reference Andrew Dillon's and Michael G. Morris' 1996 „User acceptance of new information technology: theories and models" paper, which sums up the models for user acceptance of information technologies and the psychological background (Dillon, 1996). According to this paper the definition of user acceptance is the proven willingness within the user group to use the information technology for the purpose it was created to.

The user acceptance research of biometric systems is summarised in the chapter of Marek Rejman-Greene in the Encyclopedia of Biometrics book (Li and Jaiw 2015).

The first such research in Hungary was performed in 2006 at the Budapest Technical College Bánki Donát Engineering and Security engineering faculty, with a Panasonic BM-ET 330 iris recognition access control system, „Research of the attitudes and aversive reactions generated by access control systems" (Suplicz, et al., 2006). Following this in 2014, Földesi Kriszta and Kovács Tibor performed a niche research project featuring 333 examined people with the help of the students of Óbuda University and the police (Földesi and Kovács, 2015).

Researches and studies focus on biometric devices and technologies as well as their quality and acceptance. Throughout my research I did not find any material that evaluates the access point as a whole although that is the environment the user meets in reality. Although it might be possible that at other parts of the world, access points where the negative factors determined above are negligible can be built, but I doubt it – and for Hungary, it is certainly not true. In the over 300 installations I have knowledge about, there are fewer than 10 where the problems examined previously do not exist.

Methodology

The nature of the question pointed into the direction of focus group research method as we asked open questions and expected spontaneous answers. The objective of the focus group system was clearly to discover the spontaneous feelings and reactions of the users. The qualitative technique gives space to map the thoughts, logic and feelings of users. Through the introspection, we gained an insight into their attitude towards access control system. This way we can summarize the thoughts that may arise in users when faced with the problems and errors of the system and what their experiences are. However, this technique is not suitable to make quantitative inferences, the results can be projected on the surveyed sample. Nevertheless, they help understanding immensely and provides a solid base for the research of a future, large size sample (Vicsek, 2006).

Sample and results

The survey was done by asking corresponding students of Óbuda University Keleti Károly Faculty within classes. An important factor was to ensure that the responding students should not have any previous experience within this field – as it was in previous studies. This way we ensured that we reached users (and not developing engineers) who do not have specialist knowledge about such systems and as such, their preconceptions stem from their own experience. The questions were compiled based on previous researches, brainstorming and professional opinions in such a way that they would not influence the answers in any way. We aimed not to change any questions from other surveys. This research can be considered as a pilot project as in further research, we will use the terms and words used and understood by the survey participants – ensuring the validity of the research.

Properties	Values
Answers:	13
Gender ratio:	Female: 6, Male: 7
Age groups:	Minimum: 25, Maximum: 49 Average: 37

Table 2 Sample (N = 13)

Source: author's own editing

The groups were moderated by two of us. The focus group discussion was performed within the frame of Statistics lesson on an early Friday afternoon within the classroom. Notes were taken of the answers and additional information was gained by written comments of the participants.

1. "Have you ever met an access control system?"

   100% of the participants answered yes to this question, which is not a surprise as access control systems are rather widespread nowadays and due to age dispersion, most users already had/has either a main or a secondary job.

2. "What is your first impression regarding access control systems?"

   In this question, we looked at the attitude of the participants regarding access control systems. Based on the answers we created the categories with the inductive method.

No.	Answer	Usability	General attitude
1	Operational.	Positive.	Positive
2	I find it slow, the possibility for malfunctions is high which causes disruptions	Slow.	Negative
3	It slows me down and restricts me	Slow.	Negative
5	Positive, people without access rights can be filtered out	Secure.	Positive
6	Many errors, if the "network" is saturated, it won't let me in	Slow.	Negative
8	I find it good to increase security	Secure.	Positive
9	Slow pass-through, in case of disturbances, it can cause delays. In case if the turnstile gets stuck, it poses a threat for accidents.	Slow.	Negative
10	They aren't always justified and they are sometimes slow.	Negative.	Negative
11	Useful, I have no bad experience.	Positive.	Positive
12	As a leader, I find it good as it can be used in case of working hours dispute. As a quality control person who is involved in fire protection, I also find it useful as it can give information about where people currently are. As a football fan, I hate it.	Secure.	Positive
13	Maybe a bad thing that is required. I hate it at my workplace.	Negative.	Negative

Table 3 What is the first impression? (N = 11)

Source: author's own editing

The categories can be laid out along three dimensions: general attitude: negative – positive, usability: the most frequent answer was that it is secure and slow. Also in several cases, a distinction was made between the standpoints of a user and an operator.

Figure 3. Word cloud of the first impressions.

Source: author's own editing

Altogether we had 11 answers, which is an 85% ratio. We used positive and negative categories to encode general answers.

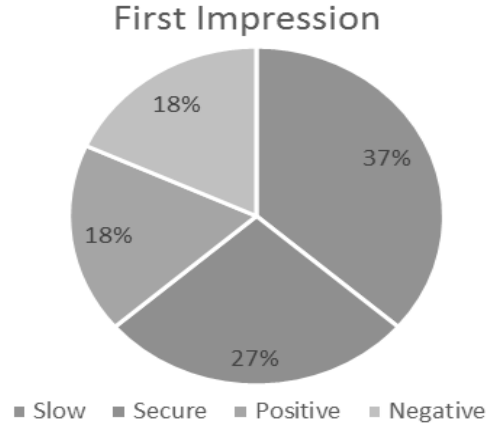

Figure 4 What is the first impression? (N = 11)

Source: author's own editing

55% of the answerers had negative statements regarding access control systems and 37% gave the specific reason that they are slow.

3. „Where did you meet an access control system?"

   Most of them reported their workplace, they most likely met access control systems bound together with attendance tracking.

No.	Answer	Location 1	Location 2
1	Multiple systems	Multiple	
4	Basically, everything works based on this system at my workplace. If the system fails, there are big problems.	Workplace	
7	I arrived to a big firm as a guest. We were registered at the reception and given a card.	Workplace	
12	Workplace: stadium	Workplace	
13	Workplace	Workplace	Stadium

Table 4 Where did they meet? (N = 5)

Source: author's own editing

4. „What kind of systems you know?"

Most of the respondents have met turnstile based systems – and an important conclusion here is that most of the users consider physical barriers as part of the identification process.

No.	Answer
1	Turnstile Detector gate Automatic gate PIN based Card based
2	Access control system RTG gate Revolving gate
3	Turnstile Metal detector
4	Turnstile It opens a door in my office
5	Turnstile Metal detector
6	Turnstile
7	Card that was given at the reception opened the door (proximity card)
8	Doesn't know the type
9	Honeywell Turnstile Man sized bars Photocell door Metal detector gate
10	Polip armed Metal detector gate Proxy key with no gate
11	Card based Turnstile
12	Turnstile Revolving door Gate
13	Turnstile Detector gate

Table 5 What kind of systems you know? (N = 13)

Source: author's own editing

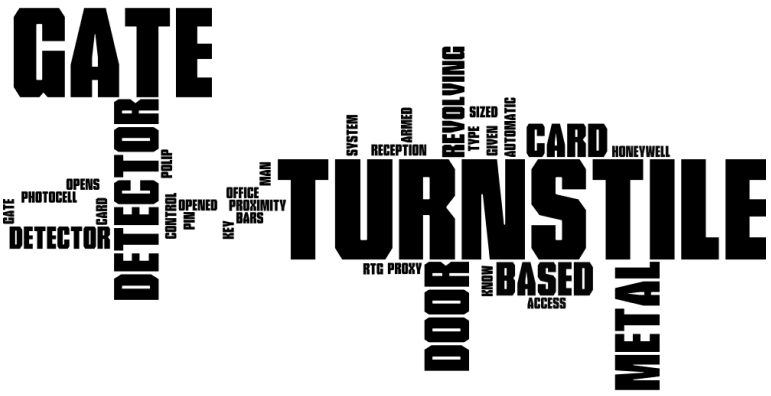

Figure 5 Wordcloud of the known systems

Source: author's own editing

5. „What kind of problems can an access control system face?"

The problems can be tied to the actual malfunctions of the physical barriers as seen above – like getting stuck or getting held back either by the error of the reader system or an access level. Actual slow reaction and false rejection only rises in two instances.

No.	Answer
3	Gets stuck
4	Gets stuck Slow Blocking me
6	Won't let me in.
9	Gets stuck
11	Disruption Barricade

Table 6 What kind of problems can access control systems face? (N = 5)

Source: author's own editing

6. "How would you feel in such an event?"

An access control system requires a human operator who helps access and can answer questions if any rejection occurs. This is also true if the user is selected for random search as personnel can disperse user uncertainty.

No.	Answer	Category	Note
1	Impatient		The impatient answer was swearing.
5	Impatient		The impatient answer was swearing.
7	I get embarrassed and look questioningly to the operator: "Why won't it open?"		
8	"The damn gate selected me again." I have been beeped in.		
10	Waste of time.		
12	What happened? Why does not it work??		
13	Junk.		

Table 7 How would you feel in such an event? (N = 7)

Source: author's own editing

Conclusions

The first part of this study collected the applications of biometry and defined the critical areas and the aspects on which this definition is based. A significant property of high user base access control and attendance tracking systems is that they are used by a large amount of people mandatorily, there are no alternative identification methods and selection is negative. The most important factor in these applications is the False Rejection Rate (FRR), since that defines whether everybody can use the system with sufficient speed and low rejection rate. Manufacturers of biometric devices generally provide algorithmic FRR values (0.001%-0.01%) which are better than the values achievable in practice. These values are practically unreachable. The difference is so big compared to our actual measurements (1-25%) that we started to examine the threshold of adequate performance a biometric system can provide within a real situation. The second part of the study summarises this.

Our results naturally cannot be generalised from a statistical standpoint, however, they are adequate as a pilot research as we can utilise the phrases used and understood by the research subject in future researches ensuring their validity. Access control systems are generally known to users, everybody has already met them somewhere. An expert

will have a fully different opinion than a general user, therefore in future research, they should be filtered. Regarding this issue, another question arises: how much can prior Hungarian research be generalised because they were mostly conducted on experts and university students studying in security directions?

More than half of the answers were negative regarding access control systems and 37% pointed out slow speed as a disadvantage. Parallel to this, 27% said that the system is secure. It would be beneficial to ask both questions in future research to determine whether the two concepts hold themselves together: biometry is slow but secure.

Users mentioned mostly revolving doors, turnstiles and metal detector gates so they encountered fully equipped access points. This means that the false rejection rates (FRR) specified by biometric equipment manufacturers are not met by the users. The given algorithmic FRR values move within the 0.01%-0.0001% range, thus users encounter these problems in every 10,000-100,000 transactions. Calculating with an average of four transactions per day, they should only be falsely rejected in about every 15-150 years (!), which they obviously would not even notice and most users would not even face such issues. It would be a proper course of action to seek the practical rate of rejections where the users might fail to pass through due to either user, system or physical errors but still accept the system as useful and properly operating. This is important because in that case biometric access control systems could not simply be gauged and ranked by the algorithmic performance values. The practical rejection rates are what must be sought and tested –that are generally between 1% and 20%.

References

Anil K. Jaina, K. N. A. R., 2016. 50 years of Biometric Research: Accomplishments, Challenges and opportunities. Pattern Recognition Letters, pp. 1-26.

Anon., 2010. First biometric ATMs roll out in Poland. Biometric Technology Today, June, pp. 5, 12.

HYPERLINK "http://appleinsider.com/articles/16/04/19/average-iphone-user-unlocks-device-80-times-per-day-89-use-touch-id-apple-says" http://appleinsider.com/articles/16/04/19/average-iphone-user-unlocks-device-80-times-per-day-89-use-touch-id-apple-says , Retrieved 12 November 2016.

ISO., 2011. Banks secure customer access with fingerprint and fingervein. Biometric Technology Today, November-December, p. 2.

ISO., 2014. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems. Requirements.. s.l.:Magyar Szabványügyi Testület.

Balla, J., 2013. A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ- es közbiztonság alakulására. Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola: s.n.

Berek, L., 2014. Biztonságtechnika. Budapest: Nemzeti Közszolgálati Egyetem.

Böröcz, M., 2015. Az illegális migráció és a terrorizmus közti összefüggések vizsgálata. Budapest: Terrorelhárítási Központ.

Bunyitiai, Á., 2011. A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból. Hadmérnök, Volume 1,

pp. 22-35.

Dillon, A. M. M., 1996. User acceptance of new information technology: theories and models.. Annual Review of Information Science and Technology, Volume 31, pp. 3-32..

Földesi, K., Kovács, T., 2015. Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendsze-rek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára. s.l.:Securinfo.

Földesi, K., 2017. PhD Értekezés. s.l.:Óbudai Egyetem, Biztonságtudományi Doktori Iskola.

Görbe Zán, K., 2010. A magyarországi migráció helyzete, kezelésének feltételei és lehetıségei, doktori (PhD) értekezés. Budapest: Zrinyi Miklós Nemzetvédelmi Egyetem.

Komarinski, P., 2005. Automated fingerprint identification systems (AFIS). USA: Academic Press.

Kovács, T., 2015. Biometrikus Azonositás. Budapest: Óbudai Egyetem.

Kovács, T., Milák, I., Otti, C., 2012. A biztonságtudomány biometriai aspektusai. In: A biztonság rendészettudományi dimenziói: Változások és hatások.. Pécs: Magyar Rendészettudományi Társaság, pp. 485-496.

Michelberger, P., 2013. Információbiztonság. Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar.

Otti, Cs., 2011. “Termelő cégeknél használt kézgeometria azonosítóval megvalósított munkaidő elszámoló rendszerek gyakorlati tapasztalatai és megtérülés-számítása,” in Óbudai Egyetem, Nemzetközi Gépész, Mechatronikai és Biztonságtechnikai Szimpózium, Budapest,

Otti, Cs., 2014. Arcfelismerő rendszerek gyakorlati problémái. Budapest, Vállalkozásfejlesztés a XXI. században : IV. tanulmánykötet. Budapest: Óbudai Egyetem Keleti Károly Gazdasági Kar, 2014. pp. 409-426.

Otti, Cs., 2015. Classification of biometric access control systems based on real-time throughput,” in Proceedings of Fifth International Scientific Videoconference of Scientists and PhD. students or candidates, Bratislava, s.n., pp. 63-71..

Otti, Cs., 2015. Comparison of hand geometry and fingerprint based identification,” in Proceediengs of the 3rd international conference and workshop Mechatronics in 78 Practice and Education, MECHEDU 2015, Subotica, Serbia, s.n., pp. 118-122.

Otti, Cs., 2016.. THE PAST, PRESENT AND FUTURE OF BIOMETRICS. Óbuda University and University of Economics in Bratislava, s.n.

Otti, Cs., 2016. “Biometrikus rendszerek felhasználói minta pozicionálásának kérdései,” in Tavaszi Szél, Tavaszi Szél, 2016., pp. 251-260.

Reicher, R. Z., Szeghegyi, Á., 2015. Factors Affecting the Selection and Implementation of a Customer Relationship Management (CRM) Process. Acta Polytechnika Hungarica, 12(4), pp. 183-200.

Li, S. Z., Jain, A. 2015, Encyclopedia of Biometrics - Second Edition. Springer New York Heidelberg Dordrecht London : Springer.

Suplicz, S., Főzi, B., Horváth, S., 2006. Írisz felismerésen alapuló beléptetı rendszer által

keltett attitődök és averzív reakciók vizsgálata.. Budapesti Műszaki Főiskola, s.n.

Trauring, M., 1963. Automatic Comparison of Finger-Ridge Patterns. Nature, Volume 197, pp. 938-940.

Vicsek, L., 2006. Fókuszcsoport. Budapest: Osiri