International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 3 (2011) pp. 174-184

Security of Biometric Authentication Systems

Vashek Matyáš [1], **Zdeněk Říha** [2]

[1] Faculty of Informatics, Masaryk University
matyas@fi.muni.cz

[2] Faculty of Informatics, Masaryk University
zriha@fi.muni.cz

***Abstract*: This paper outlines our views of actual security of biometric authentication and encryption systems. The attractiveness of some novel approaches like cryptographic key generation from biometric data is in some respect understandable, yet so far has lead to various shortcuts and compromises on security.**

This paper starts with an introductory section that is followed by a section about variability of biometric characteristics, with a particular attention paid to biometrics used in large systems. The following sections then discuss the potential for biometric authentication systems and for the use of biometrics in support of cryptographic applications as they are typically used in computer systems.

***Keywords*:** IT security, biometrics, authentication.

I. Introduction

This paper summarizes our opinions and findings after more than a decade of studying biometric authentication systems and their security. This is an extended version of our work presented at the Computer Information Systems and Industrial Management Applications (CISIM) 2010 conference, held in Cracow, Poland. The paper summarizes our personal views and opinions on selected issues in the area of biometric authentication and related areas of cryptography.

Proper user identification/authentication is an essential requirement for reliable access control and as such is a key enabler for electronic commerce. There are three types of identification/authentication methods that can be used either on their own or in various combinations. Identity verification (authentication) in computer systems has been traditionally based on something that *one has* (key, magnetic or chip card) or *one knows* (PIN, password). Biometrics are based on the principle of measurable physiological or behavioural characteristics such as a fingerprint or a voice sample.

Biometric systems can be used in two different modes. Identity *verification* (also called *one-to-one* comparison or authentication) occurs when the user[1] claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user are compared to the user's data already stored in the database. *Identification* (also called *search*, *recognition* or *one-to-many* comparison) occurs when identity of the user is a priori unknown. In this case the user's biometric data are compared against all records in the database as the user can be anywhere in the database or she actually does not have to be there at all. Authentication is typically a pre-requirement of authorization (to log in, to access files, to enter an aircraft, etc.). While biometric authentication is attractive because it principally authenticates the user (and not something that can be disclosed or passed to a colleague), its shortcomings relate to problems with accuracy, privacy protection, secrecy of the biometric data and therefore to the need for a reliable liveness testing.

Before a user can be successfully verified or identified by the system, she must be registered with the biometric system. User's biometric data are captured, processed and stored. The process of the user's registration with the biometric system is called *enrolment*.

There are basically two kinds of biometric systems:

- Automated identification systems operated by professionals (e.g., police Automated Fingerprint Identification Systems – AFIS). The purpose of such systems is to identify an individual in question or to find an offender of a crime according to trails left at the crime scene. Enrolled users do not typically have any access to such systems and operators of such systems do not have many reasons to cheat.

- Biometric authentication systems used for access control. These systems are used by ordinary users to gain a privilege or an access right. Securing such a system is a much more complicated task.

It is worth noting that the involvement of a human factor in the former type of biometric system enormously reduces the problems of the latter type of system. This paper will focus on the latter type of systems as improvement of their security, without human intervention in the process, has considerably more impact on computer security and also is more challenging.

[1] We shall use the term 'data subject' according to [32] later in the paper when we relate the user directly to his/her biometric data.

II. Accuracy of biometric systems

The most significant difference between biometric and traditional authentication techniques lies in the answer of the biometric system to the authentication/identification request. Biometric algorithms do not give simple YES/NO answers. Instead, we are being told how similar or dissimilar the current biometric data are to the record stored in the database. We have to allow for some variability of the biometric data in order not to reject too many authorized users (this would be a case of the false rejection error). However, the greater variability we allow the greater is the probability that an impostor with similar biometric data will be accepted as an authorized user (this is a case of the false acceptance error). The variability allowed is usually called a *(security) threshold* or a *(security) level*.

A. Variability of biometric characteristics

The performance of a biometric technique depends on which characteristics – whether genotypic or phenotypic – the technique is based on. Genotypic characteristics do not change over time. This is good news for the false rejection rate which may remain low as the matching algorithm does not have to adapt to changes. The bad news is that genotypic characteristics cannot distinguish monozygotic twins. So the percentage of identical twins[2] in population sets the lower limit on the false acceptance rate (so called *genotypic error rate*). The phenotypic characteristics do not set limits on the false acceptance rate, but it is clear that the phenotypic variation over time imposes a lower limit on the false rejection rate (so called *phenotypic error rate*).

More precisely, the performance of biometric techniques is determined by two kinds of variability among the acquired biometric characteristics:

- **Within-subject variability:** As the results of biometric measurements are never the same the biometric system must accept similar samples stemming from one biometric characteristic as a true match. Although the matching algorithm may allow for a variability of the input measurements, it is clear that higher within-subject variability implies more false rejects. Therefore within-subject variability sets the lower limit on the false rejection rate.

- **Between-subject variability:** If between-subject variability is low then it is more difficult to distinguish two subjects and a false accept may occur. The lower the between-subject variability the higher the false acceptance rate. Therefore between-subject variability sets the lower limit on the false acceptance rate. An ideal biometric characteristic impacts very high between-subject variability.

B. Error rates

The interaction with a biometric system starts with the enrolment, where the quality of enrolment data is very important and significantly influences the system performance. Often several input samples (e.g., 3 or 5) are combined to create one biometric reference (or to verify usability of the newly created biometric reference).

The probability of a person not being able to enrol in a biometric system is called the Fail to Enrol rate (FTE). It is computed as a fraction of people who could not enrol in the system out of the complete group of people. The FTE rate includes people without fingers (for fingerprint systems), visually impaired people (for iris-based systems), etc.

The FTE rate is generally estimated as 1-2% for fingerprint based systems and 1% for iris based systems. Real values of the FTE rate are dependent on the particular scanner, the enrolment policy and the user population.

A good illustration of numbers from the real life can be the fingerprint enrolment of epassport applicants. In Germany [7, 51] good quality optical scanners with 500 or 1000 DPI have been used for the enrolment. During the three month enrolment trials 99% of the applicants could be enrolled with fingerprints of 2 fingers and 0.9% with a fingerprint of one finger. Only 0.1% of applicants could not be enrolled by the fingerprint system at all. Over 80% of the enrolled images were of the highest quality (NFIQ[3]=1), while approximately 2% were of low and very low quality (NFIQ=4 or NFIQ=5).

For verification/identification attempts, the biometric input sample is obtained and its quality is verified. If the quality does not satisfy certain minimal quality requirements, the acquisition process must be repeated. If all repeated acquisitions do not yield sufficiently good samples, the person cannot be identified/verified and such an attempt increases the Failure To Acquire (FTA) rate. Sometimes the minimal quality can be configured and then the stricter we are with the quality check the better results we get during the biometric comparison and vice versa. The FTA rate can be therefore traded off with biometric matching error rates.

Input samples of sufficient quality are processed in the biometric matching algorithm. The matching algorithm compares the input sample with a biometric reference (in the case of verification) or number of references (in the case of identification). The result of the matching algorithm is either correct or incorrect. If an error occurs, the resulting decision can either incorrectly refuse an authentic person (this is so-called false non-match – FNM) or match an impostor with another person's biometric reference (this is so called false match – FM). What happens next depends on the system policy. In the case of single attempt scenario, the verification/identification ends. In the case of, for example three-attempt scenario, re-acquisition is possible if the person is not being recognized (either false non-match or correct refusal of an impostor).

The final result of an authentication/verification attempt is either correct acceptance or correct refusal, false acceptance or false rejection. In the case of single-attempt scenario the FRR and FAR can be computed as:

$$FRR = FTE + (1 - FTE) \cdot FTA + (1 - FTE) \cdot (1 - FTA) \cdot FNMR$$

$$FAR = (1 - FTE)^2 \cdot (1 - FTA) \cdot FMR$$

For the purpose of FAR computations the so-called *zero-effort* (also called *random forgery*) unauthorized authentication attempts are taken. In this case attackers are not actively changing their biometric characteristics (for example in the case of dynamic signature systems they sign as usual).

[2] The probability that a person has an identical twin is estimated as 0.8% [17].

[3] NIST Fingerprint Image Quality – quality assessment (prediction of matcher performance) ranging from 1 (best) to 5 (worst).

Sometimes the minimal quality required for a successful enrolment can be configured. It is, however, clear that the stricter we are with the quality control at the time of enrolment (i.e., the better quality of the biometric reference), the better results we achieve later in verification/identification attempts and vice versa. Therefore matching error rates can be traded off with the enrolment quality requirements. In 2004 Atos Origin (commissioned by the UK Passport Service) ran a biometric trial. Facial, iris and fingerprint systems were tested in 'real' conditions with 3 groups of participants: Quota (representative sample of the population), Opportunistic (volunteers) and Disabled (several types of disabilities). The Quota and Disabled results can be briefly summed in the table 1. The results are not particularly good and the study points to negative extremes from the biometric usability point of view. For details (explanation of some of the results, shortcomings of the trial, etc.) see the final report of the trial [8].

	Face			
	FTE	**FTA**	**FNMR**	**FRR**
Quota	0.15	0.00	30.82	**30.92**
Disabled	2.27	0.00	51.57	**52.67**

	Iris			
	FTE	**FTA**	**FNMR**	**FRR**
Quota	12.30	0.44	1.75	**14.21**
Disabled	39.00	0.68	8.22	**44.39**

	Fingerprint			
	FTE	**FTA**	**FNMR**	**FRR**
Quota	0.69	6.98	11.70	**18.43**
Disabled	3.91	3.14	16.35	**22.14**

Table 1. The error rates of facial, iris and fingerprint systems in a UK 2004 trial [8]. All values are expressed in %.

More favourable error rates have been achieved during the real operation of biometric systems deployed at airports. The iris based system at Amsterdam airport [22] is operating with FRR of 1.5%. The fingerprint based system at Paris CDG airport [22] (when operational) was achieving similar FRR. The biometric system at Portuguese airports [23] is based on facial recognition and operates with FRR of 4-5%.

The correct way to calculate error rates is to compute error rates for each person who contributes to the tests and then to average[4] the rates over the group of all the people. Otherwise the results can be biased by an unbalanced number of verification/identification attempts done by different people.

As we have seen, the accuracy/usability of biometric systems can be measured in the terms of FTE, FTA, FMR, FNMR, FAR and FRR. When comparing different systems, typically only the resulting FR and FA rates are used. The FAR and FRR can be graphically expressed in a FAR-FRR graph, where both the error rates are a function of the threshold value or can be plotted in a ROC graph where the FAR is a function of FRR or vice-versa (thus eliminating the threshold value from the graph). The point where FAR and FRR have the same value is called the equal error rate (EER) or the crossover accuracy. Such a threshold does not have a particular importance, but the resulting EER can be used as a (rather simplified) performance value of a biometric system in evaluations.

Now let us review some real numbers. There are several types of tests [10] and not all the results must necessarily be comparable.

The American NIST has been regularly testing the accuracy of fingerprint, iris and facial biometric systems.

The facial recognition algorithms were tested during the FRVT (Face Recognition Vendor Test) 2002 and FRVT 2006 tests. Iris recognition algorithms were tested in ICE (Iris Challenge Evaluation) 2005 and 2006. Fingerprint algorithms were tested during the FpVTE (Fingerprint Vendor Technology Evaluation) 2003, Slapseg (Slap Fingerprint Segmentation Evaluation) 2004 and II (2008), PFT (Proprietary Fingerprint Template Evaluation) 2003 and II (2010), MINEX (Minutiae Interoperability Exchange Test) 2004 and ELFTO (Evaluation of Latent Fingerprint Technologies) 2007 tests. As an example of the results of the NIST test effort we include here the ROC graph of facial biometric systems from 2006. The details of the NIST tests can be found at fingerprint.nist.gov, iris.nist.gov and face.nist.gov.

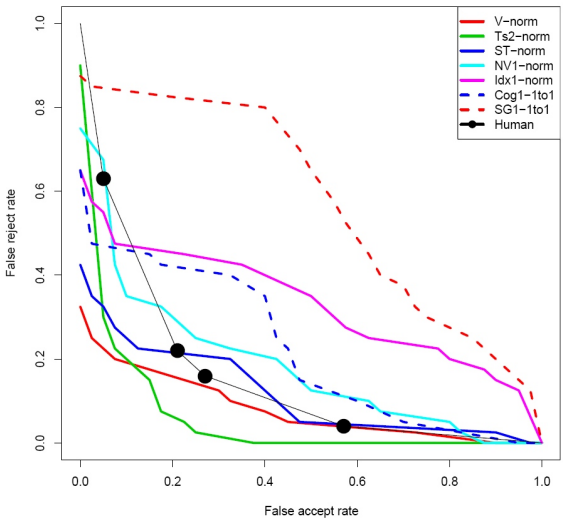

Figure 1. The ROC graph of several facial recognition algorithms and human ability to recognise faces (FRVT 2006 run by NIST [45] for facial images with illumination changes).

C. Large scale systems

Designing a biometric system for few data subjects (as users are called according to [32]) is relatively easy. Tuning a system for millions of data subjects is significantly more challenging.

While the *verification* speed and accuracy is essentially same for a system with 10 data subjects and for a system with 10 million data subjects, the *identification* mode makes the difference.

In identification mode the biometric system can incorrectly reject the data subject (and this affects the false-negative identification-error rate – FNIR) or incorrectly accept an impostor (and this is measured by the false-positive identification-error rate – FPIR).

In the case of a single attempt scenario the values of FNIR and FPIR can be estimated from the verification FMR and FNMR as follows:

[4] Weighted average corresponding to the target population can also be used.

$$FNIR = FTA + (1 - FTA) \cdot FNMR$$

$$FPIR = (1 - FTA) \cdot (1 - (1 - FMR)^x)$$

where x is the number of biometric references in the database. Let us illustrate the identification accuracy with an example, consider a biometric system with the verification FMR of 0.5% and FNMR of 5%. The false match rate of 0.5% (FMR=0.005) may look attractive. Let us further have a small organization with 100 data subjects. If this organization uses the aforementioned biometric system in the identification mode, the following identification accuracy is achieved (for simplicity we calculate with FTA set to 0):

$$FPIR = 1-(1-FMR)^{100} = 1-0.995^{100} \cong 0.3942 = 39.42\%$$

$$FNIR = FNMR = 5\%$$

A system with an FPIR of nearly 40% is useless. Even if the verification FMR of 0.5% may look impressive it is not suitable for identification even within a small group of dozens of data subjects. Large scale identification systems need algorithms with much better accuracy.

III. Secrecy and diversity of biometric data

As we all suspect, most biometric data are not secret. Photos, fingerprints and other biometric data can be more-or-less easily obtained by a targeted attack. Therefore security of any system cannot be fully based on the secrecy of biometric data. Having said that we have to admit that the need of the acquisition of the biometric data is a factor that can make overall attack more expensive in the terms of time, money and/or effort. Therefore the use of biometric data as an additional security factor can have a (security) value in some cases. Other issues related to the secrecy of biometric data include unchangeableness of most biometric characteristics (it would be useful after compromise of biometric data) and small diversity in the choice of parameters of biometric systems (like which finger to scan) resulting in several biometric systems storing basically the same data of a data subject (and administrators having access to such data). Data subjects moreover will not learn that their biometric data has been stolen (in contrast with, e.g., tokens) until a misuse is detected.

The secrecy of biometric data relates to ease of covert and overt acquisition of such data and to the diversity of such data in separate instances of biometric systems. Naturally, there are differences between the various biometric techniques. Let us now look at particular biometric techniques:

- **Facial systems:** facial biometric systems are based on 2D or 3D representations of faces. The face is typically the most visible part of the human body and can be easily watched and/or photographed and/or recorded. Covert acquisition of a 2D facial image is simple and can be made even from a long distance (as every paparazzo could describe). Even if faces change with time and other influences (like fashion), people only have one face and therefore all biometric systems based on faces use the same information.

- **Infrared facial systems** use photographs or recordings of peoples' faces imaged in infrared wavelengths. Infrared devices are more expensive, but are widely available. The secrecy of such biometric data is comparable to data used in facial systems based on visible light wavelengths. Remote acquisition of infrared images is also not problematic (only the required optics are more expensive).

- **Fingerprint systems** use images of ridge patterns on finger tips or hand palms [37]. Biometric systems use live fingerprint scanners for fingerprint acquisition but people leave fingerprints on anything they touch. Latent fingerprints are in fact the fat (and some other substances) left by the finger on the touched object. The best objects to look for fingerprints are glass, doorknobs and glossy paper [14]. There are several techniques to visualize and digitalize the latent fingerprint. Both the forensic practice and experiments [14] show that this is relatively simple. It is said that on average people leave 25 perfect fingerprints every day [47]. People normally have 10 fingers and 10 toes. Toes are not currently used for biometric purposes. Little fingers often do not convey enough biometric information for reliable identification/verification. Typically left and right thumbs and index fingers are used in fingerprint systems, the right index finger being the most popular finger used. Most fingerprint-based biometric systems will in fact use the same finger(s).

- **Iris based systems** use images of the iris. The iris is an internal organ, but it is directly visible and can be observed easily. For better imaging of brown irises the near-infrared band is often used, but good quality images can be obtained also in the visible part of the spectrum. For reliable identification or verification the diameter of the iris in a digital image of the eye should be at least 100 pixels [31]. A good quality camera and zoom lens can be used to acquire an image of the iris with sufficient quality even from mediate distances. Covert image capture is also possible as the cooperation of the data subject is not necessarily required. People have two eyes, typically both eyes are enrolled and only the dominant eye is used for identifications/verifications.

- **Voice based systems** use the information about the vocal tract conveyed in the voice to identify/verify humans. The voice based biometric systems can be divided into text-dependent (always use the same phrase), text-prompted (computer generated phrase is used) and text-independent (data subject can pronounce any phrase) systems. The data subject uses his vocal tract not only for the biometric authentication but also during normal conversation and these are both situations where an attacker can record the data subjects's voice (overtly or covertly). The situation of the attacker is different in different system types. In the text-dependent systems all the attacker needs is the fixed phrase which can be user-specific or the same for all the data subjects. In text-independent system any recording of the data subject is sufficient. In text-prompted systems the attacker does not know in advance what phrase will be required; still the attacker can assemble the required phrase from several

other recorded phrases or create a model of the speaker, train the model with the available recordings of the data subject and use the model to approximate the pronunciation of the required phrase. This area is currently open for research.

- **Subskin biometric characteristics** are not directly visible and a special scanner (e.g., ultrasonic) is required to get the biometric data. While completely covert scanning is difficult, it may be possible to obtain the scan by using some cover stories, as the scanning devices can be easily masked as looking as something else. Usually subskin fingernail characteristics are used for biometric purposes.

- **Authentication based on the mind** [56] is measuring the brain activity during the authentication process. To obtain such biometric data we would have to use similar measurement devices (difficult to do covertly) and make the data subject to authenticate (to perform the same brain activities, e.g. to think a password). The brain activity is different for every combination of a person and a password. It is difficult to estimate how hard it would be to create a model of a human brain, train it with known combinations of persons and passwords and then derive the biometric data for another person or password.

- **Retina based systems** use the pattern of vessels behind the retina in **choroid** to identify/verify humans. The retina is an internal part of the eye and is not directly visible. To obtain the image of blood vessels in choroid a special instrument must be used. Ophthalmologists use devices called retinoscopes, automated biometric systems use specific optical devices to acquire the image of the blood vessels. Covert retina scan is not possible, overt retina scan without the cooperation of the data subject is also not possible. People only have two eyes, so the biometric systems based on retina usually share the same biometric information.

As we can see there are substantial differences between various systems. The order of biometric technologies in which they are presented above reflects our opinion about the difficulty of obtaining relevant biometric data (from easy to get to more difficult to get). It is, however, only a rough estimate and different people can have different opinions and there are several factors which need to be taken into account (like the type of the system in voice-based biometric solutions). Some biometrics are not secret because their traces are left all over the place. Others are potentially insecure as they are not revocable and their use in multiple systems can lead to problems with secrecy in case one copy of the biometric sample or characteristic leaks.

IV. Template protection

Attacks similar to dictionary attacks in the password world exist also in the biometric world – as for passwords, also not all the biometric references are equally probable. Some combinations of features are more likely than other. Additionally, biometric data of some data subjects contain significantly less features (than the average). Therefore some biometric references can be 'weaker' than others, and so the biometric dictionary attacks will focus on more probable and weaker biometric references. Unlike in the password world, there is not much that the data subjects can do to improve the situation. The system designer can opt for a more restrictive configuration, with both positive and negative effects of such configuration.

Biometric dictionary attacks are only relevant to remote (and API) authentication, as locally the liveness test should stop non-genuine biometric samples. The problem of biometric dictionary attacks can be mitigated similarly as in the case of password dictionary attacks, for example by limiting the number of unsuccessful trials or progressively extending the timeout after unsuccessful attempts.

If a biometric system returns not only the YES/NO answer, but also the resulting score, then this score return can be misused. Using so called hill climbing [3, 53, 57] the score can be used to progressively improve the biometric data being evaluated until a successful comparison is achieved. It seems that even quantization of the score does not help significantly [2].

Other discussions relate to the format of the biometric reference. Although there are several ISO standards (ISO/IEC 19794 series) defining open and interoperable biometric reference formats, most of these formats are based on images. The notable exception is the fingerprint minutiae format (ISO/IEC 19794-2). Independent tests (the MINEX 2004 [26] and MTIT [42]), however, concluded that the accuracy of comparison algorithms is significantly better when the algorithms use their own proprietary template formats. Therefore systems that have strict demands on accuracy (and prefer to use templates) still rely on proprietary template formats. In some cases raw biometric data (e.g., the image) are stored in addition to or instead of the template. The reasons for doing so include the need of original data for legal proofs or for interoperability between a number of system which do not necessarily share the same biometric reference format (e.g., electronic passports) and possibility to reuse the data in an upgraded biometric system with an enhanced biometric reference format. The storage of raw biometric data raises privacy issues (the biometric data can contain some sensitive personal information) and fears about easier misuse of the data (in the case of compromise the full data is compromised and better interoperability implies also easier crossmatching between multiple databases).

Even in situations where only the template is stored (and not the raw biometric data) such templates can be misused to crossmatch several databases. Researchers are designing schemes where two templates from two different databases cannot be directly compared, such templates can only be used for comparisons against raw biometric data (e.g., images). The naïve solution is to encrypt the templates, but then the templates need to be decrypted before the comparison. Some more advanced solutions, like the use of shielding functions [38, 54] or so called cancellable templates [49, 48, 40] can help to limit the misuse of the templates (a closely related subject of fuzzy vaults is discussed later in this paper). It is, however, necessary to understand that having access to the raw biometric data enables comparisons against any kind of template, as this is the inherent property of biometric templates. And all biometric systems need to process the raw data (which can be potentially misused).

V. The liveness problem

As we have discussed above, biometric data are not secret. We cannot expect that the biometric characteristics are not available to attackers. Therefore the knowledge and presentation of the data subject's biometric data should not directly lead to a successful authentication. This is why remote biometric authentication does not work (is not secure) in most cases (despite of some broad framework specifications [33]). Locally we can try to verify so called *liveness* (also called *liveliness*) to make sure we are processing the fresh biometric data originating from the person being authenticated.

Liveness tests are specific for a particular biometric modality and can be roughly divided into two categories. Static tests measure some physiological characteristics (like the finger temperature or conductivity) that should discriminate between the living human and an artificial fake. Dynamic tests verify the reaction of the person to an impulse. The impulse can be the increase in light intensity to see the pupil contraction or asking the subject to pronounce a particular phrase.

There are many various kinds of liveness tests used today. For example to verify the liveness of the fingerprints it is possible to measure the temperature, reaction to hot and cold stimulus or pressure stimulus, conductivity and other electrical properties [36], the perspiration [19], optical properties of the skin, contact scattering [9], pulse or blood oxygenation. We can use hippidus effect in the case of the iris liveness test, reaction to the volume or position of the illumination source or look at the Fourier plane to deal with colour contact lenses [18]. Facial recognition systems either use several cameras to obtain 3D properties of the head (to avoid simple attacks with a photo) or ask the subject for a particular reaction (to blink, to move left or right, to open or close the mouth). Text prompted voice systems ask the subject to pronounce a random phrase. A combination of facial and voice recognition can also verify the lip movement.

Unfortunately, most liveness tests are weak and can be easily fooled by using materials having the same properties as the human body or can be simulated in other ways. For the discussion how easy it is to fool common fingerprint scanners with silicon or gelatine copies (so called 'gummy fingers') see [41, 14]. It is also necessary to mention that liveness tests cannot detect changes of biometric characteristics (e.g., a plastic surgery). It is by no means trivial to come up with a liveness test that would be difficult to fool and would not cause a high FRR of the entire system. From the medical point of view, liveness would primarily be tested by means of the EEG. But that is not exactly what we need in liveness testing for biometric authentication systems. It is not sufficient to measure the brain activity of the subject to verify that she is indeed alive when she could use a plastic layer on her finger to fool the scanner. The liveness test is therefore not only about measuring the liveness of the subject, but more-or-less about resistance to attacks with non-genuine biometric samples (sometimes the term *liveness+* is used). According to our experience and private discussions with experts in the field you can always bypass the liveness test if you know what the liveness test is looking for. This is also the reason why details of many liveness tests are kept secret and evaluation of their security is not possible or at least not straightforward [39]. Many scanners were easily fooled with simple biometric copies in the past. There are, however, a few biometric sensors which are believed to be moderately spoof-resistant. One of such sensors is the Lumidigm fingerprint sensor that combines optical fingerprint scanner with multispectral imaging [50]. No independent evaluation of the technology is publicly available, but the US Transportation Security Administration (TSA) tested the sensor and approved it in 2007. Currently (2010) the biometric Qualified Product List (QPL) [29] lists 2 Lumidigm, 1 Bioscript, 1 Cogent and 1 Integrated Biometrics scanners.

VI. Secure biometric authentication

We have discussed the secrecy of biometric data and the need for liveness testing. For secure authentication the biometric system must be convinced that the presented biometric measurements are coming from a trusted and unmodified input device and are fresh. The biometric system should verify the liveness, otherwise the system could be cheated with copies of biometric characteristics. Sometimes the liveness test can be replaced with a human guard, it is however questionable whether a human guard can protect against more advanced biometric fakes (like a thin silicon layer at the fingerprint).

If the authentication is done on-device, the device itself should be trustworthy. If the authentication is done off-device, then the operating environment of the software and the communication link between the software and the device have to be secured. For example, in a client-server application, if the client workstation is not trusted, then there is no point authenticating the person using that workstation. If one chooses to run the authentication software at the server side, then the communication link between the server and the device itself (not just the client workstation) has to be secured. Otherwise, a malicious party or even the workstation itself may intercept the communication and replay recorded biometric data. One way to defeat replay attacks is to put a separate secret key in the device and to use challenge/response protocol with this key. Obviously, the device has to be trustworthy. One possible solution would be to use a tunnelling protocol with mandatory authentication of both parties. To protect the keys and to avoid modification of the liveness test the device must be tamper-resistant or physically secured.

As we have already mentioned, remote biometric authentication is mostly not secure. There is no sense to send a fingerprint to log-in to a web server if the fingerprint scanner is not trusted by the web server. And to be trusted can imply to have a reliable liveness test, to have a secret key to support data authenticity and to be tamper resistant (to protect the keys and to protect against modification of the liveness test or direct injection of attacker's data – the device is fully in the hands of users and potential attackers). It is quite difficult to make a small smartcard tamper resistant. To design a tamper resistant fingerprint scanner is a real challenge.

The raw biometric sample or templates need to be supplied for comparisons. Hashing the biometric data by a cryptographic hash function and sending only the hash [13] for comparison does not work (unlike for passwords). Biometric measurements never yield the same values, therefore cannot be directly compared in hashed or encrypted domain. There are some efforts of how to avoid the transmission of the full sensitive biometric data [11] and we discuss relevant issues below.

VII. Biometric encryption

The idea of cryptographic keys derived exclusively from biometric data bears some very attractive advantages, e.g., the keys being used only with the rightful owner present (and being re-generated 'on the fly', then could be destroyed after use).

However, such derived keys also have some unpleasant properties that make them useless in many traditional cryptographic applications [5]. Such keys have limited entropy [46], are created through a deterministic process from non-secret biometric data, and also cannot be changed (or only several times). Invariant features can obviously be extracted from a biometric sample and encoded so that they can be used as an encryption key. The basic problem with this concept is that such a key cannot be treated in the same way cryptographic keys are usually treated. Here we shall again stress the fact that biometrics are not secret. Other factors may include the volume of data that is truly invariant over time and the problems with changing one's key as soon as the data subject actually finds out that her fingerprint has been disclosed. Moreover, a damaged fingerprint would disable any operations with the derived key.

Biometric encryption (together with other methods of template protection like cancellable biometrics and shielding functions) belong to the area called renewable biometrics and has been already studied for some time. The emerging ISO standard 24745 Information technology – Biometric information protection [30] (currently, November 2010, in its FCD – Final Committee Draft) is unifying the terminology, explaining the basic principles and refers to example technologies [12].

A. Entropy of biometric characteristics

While unprocessed biometric samples have the size of kilobytes or megabytes (e.g., the scan of a hand palm in a high resolution), the entropy of the repeatable invariant biometric features is much smaller. The estimation of the entropy of biometric characteristics has recently become an area of active research [1, 4, 59]. The entropy estimates cannot evaluate the entropy of general biometric samples, but are specific for biometric modality (fingerprints) and the particular features used for identification (fingerprint minutiae). It should be noted that it is hard to pin down the entropy in a precise way. A. Adler et al. [1] estimate the entropy of facial biometric information to 40-50 bits. M. Young [59] estimates the entropy of fingerprint minutiae to 82 bits. The iris template (in Daugman based algorithms) is 2048 bits long. When combined with error correction codes the iriscode is able to produce repeatable strings of 140 bits with a low false rejection rate (experiments produced bitstrings of 42-224 bits with various error rates, for details see [27]). Other estimates quote 250 bits of entropy per iriscode [34] or 260 bits per iris image [60].

Interestingly, the noisy part of raw biometric data that is ignored by biometric algorithms (when searching for the invariant features) can be used to generate random numbers [24].

B. Secrecy and changeability of biometric data

Important properties of cryptographic (symmetric and private asymmetric) keys include secrecy of the keys and changeability after a key compromise. As we have discussed above, biometric data are neither secret nor changeable. This means that 'keys' derived by publicly available algorithms from non-secret data cannot be considered secret and do not fulfil this critical requirement of cryptographic keys.

To improve secrecy of the resulting data we can either make the algorithm secret (but security-by-obscurity is not a good design principle) or make the result a function of not only the biometric data, but other secret data as well (password or secret key). Then the biometric data are only *one of* several authentication factors.

C. Repeatability of biometric data

One of the most serious problems any implementation of biometric key derivation has to face is the variability of the biometric data. The raw biometric samples are never the same, they only are similar. In biometric authentication, we need a metric of such a similarity. For encryption, we have to derive exactly the same bitstring as we know that a single changed bit will radically change the results of cryptographic operations (as a consequence of the required avalanche effect). Deriving exact repeatable bitstrings from noisy biometric data is not a simple task.

One of the possible options is to use discretization with a sufficient margin for errors (e.g., only 1 bit per feature which is normally measured in several bits). Another approach is to use error correction codes. The problem with biometric data is the correlation of errors (a whole part of the fingerprint missing, not just random features). To solve such difficulties a combination of error correction codes can be used [27]. The theoretical work in this field includes the notion of *fuzzy extractor* [21] (error correction followed by hashing) and *fuzzy commitment* scheme (a standard random key is generated, then redundancy for error correction is added and result is XORed with the biometric data) [35].

Relevant to this field are also advances in threshold cryptography (secret sharing, etc.) [20]. It is also worth mentioning the work carried out by Wheeler [58], which focuses on the agreement on a key using faulty (analogue biometric) data from separate measurements, where error-correction is involved and at the end of such protocol execution both the sender and the receiver have the same bitstring. Another work [16] focuses on MACs of noisy data like biometrics.

D. 'Biometric keys'

There are several types of keys, which are somehow protected by biometrics. According to how exactly biometric data is applied to get the so-called biometric key, we can divide the systems into three categories: systems with key unblocking, key derivation and key locking.

1) Key unblocking

The first option where biometrics can meet cryptography is securing access to a secret key. Access to secret keys is commonly protected by passwords or PINs. Securing the secret key also with a biometric system might improve its protection. In such a case, the cryptographic key is a standard (random) key and it is released only after successful biometric authentication.

If biometric measurements are not acquired by the signing device itself, the signing device must verify that the data were really captured by an authentic biometric sensor and are fresh, otherwise the use of biometrics does not provide much security.

The protection of the cryptographic key by biometrics requires the use of a trusted component (a trusted workstation or a secure hardware). An attacker cannot have a direct access to the biometric reference and the key, otherwise the biometric authentication can be bypassed completely and the cryptographic key can be recovered directly without any authentication.
Key unblocking is not a proper biometric key scenario rather than a kind of biometric authentication.

2) Derivation of encryption keys directly from biometric data

Another option is to derive the biometric key solely from the biometric data. Here the principal engineering problem is the variability of the biometric samples. Such noisy data have to be transformed into a repeatable bitstring. Discretization, error correction codes and other techniques can be used to help to implement such a scheme.
There have been several attempts to implement such schemes. One of the first systems was based on keystroke dynamics [44]. Biometric information (here in the terms of the key-down time and the inter-key delay) was added to the typed password after discretization. Such 'hardened password' was the resulting biometric key. Another approach used voice biometric data to generate the key [43]. The system was also based on discretization. Handwritten signatures can also produce a biometric key [28]. Many encoded dynamic properties like the velocity, pressure and direction are concatenated to form the resulting key.
All these implementations suffer from high false rejection rates (the legitimate data subject is unable to reproduce the original key) in the range of 20-50%, which makes them practically unusable. Even with so high FRR the length of the resulting biometric key is quite short (being in the range of 12-46 bits).
Keys derived directly from biometric data are of limited use no matter what type of key is generated (symmetric, asymmetric) or the kind of application the key is intended for (digital signatures, encryption and decryption of documents). This relates to the fact that there is no secret information involved in the entire process. Such biometric keys can be considered as a form of a biometric template.

3) Key locking

The third approach of cryptography meeting biometrics combines the first two methods. Unlike during the key unlocking the data subject's biometric data is *applied* to a random cryptographic key. The resulting *locked key* should not leak information neither about the original biometric data nor about the cryptographic key. Only the correct biometric data (biometric sample similar to the original one – practically a sample originating from the same person) should be able to unlock the key and produce the same cryptographic key to which the biometric data was applied at the beginning [6].
Several implementations have tried to follow such a scheme. A fingerprint based implementation [52] called Bioscript used phase information of the Fourier transformation of fingerprint images and majority coding for locking the randomly generated key (so-called *biometric locking*). Another fingerprint implementation [15] used minutiae points (plus other chaff points) to create a locking set, from which a secret key could be recomputed. The technique is called the *fuzzy vault*. Another implementation based on biometric locking appeared in the area of facial biometric systems [25]. Here the facial eigen projections are used as the primary biometric data and majority coding and polynomial thresholding are used in the process of the key generation. These implementations also suffer from high FRRs and short resulting bitstrings.
Another implementation [27] is based on iris biometric data. First a random 140-bit cryptographic key is taken and encoded using Reed-Solomon and Hadamard codes to form a 2048-bit string. This bitstring is then locked by XORing it with the data subject's iriscode. The result is called pseudoiriscode. The process of decoding XORs the pseudoiriscode with a fresh iriscode and applies the Hadamard and Reed-Solomon decoding to obtain the original 140-bit key. The authors claim the FRR to be 0.47% and FAR to be 0% (for the 140-bit keys).
In fact any algorithm reliably deriving a biometric key from the biometric data can be enhanced by XORing the key with a random key to design a key locking scheme. Also locked biometric keys have to cope with the low secrecy of biometric data as any biometric sample of the correct data subject can be used to unlock the key. Therefore the locking cannot be considered as a sufficient protection and the locked key must be kept secret.
The main advantage is changeability of the cryptographic key which is being locked. The recovery after a key compromise is easy. On the other hand if the biometrics are compromised, there is no easy recovery and the same biometric data can unlock next locked keys as well (unless other biometrics – like another finger for fingerprint systems – is used).

VIII. Conclusions

The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they do authenticate the *user*. They do not rely on objects the user carries or something the user has remembered. Biometric authentication methods use the real human physiological or behavioural characteristics to authenticate users. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample. Well-known investigations [41, 55] confirmed our earlier findings that attacks may be much easier than generally accepted.
The biometric authentication also has some other advantages. Most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the management of lost, reissued or temporarily issued tokens/cards/passwords can be avoided.
So why do not we use biometrics everywhere instead of passwords or tokens? Nothing is perfect and biometric authentication methods also have their own shortcomings. First of all the performance of biometric systems is not ideal (yet?). Getting the result is quite clear and quick when comparing two passwords. Comparing two sets of biometric characteristics is not so straightforward. Biometric systems still need to be improved in the terms of accuracy (and sometimes also speed).
The fail to enrol rate (FTE) brings another important problem. Not all users can use any given biometric system. People without hands cannot use fingerprint or hand-based systems. Visually impaired people have difficulties using iris or retina

based techniques. Even enrolled users can have difficulties using a biometric system.

Biometric data are not secret and the security of a biometric system cannot be based solely on the secrecy of the biometric characteristics. The server cannot authenticate the person just after receiving her correct biometric characteristics. User authentication can be successful only when the person's characteristics are fresh and have been collected from the person being authenticated. This implies that the biometric input device must be trusted. Its authenticity should be verified (unless the device and the link are physically secure) and the liveness should be checked.

We believe that the biometric authentication is a good *additional* authentication method. Even cheap and simple biometric solutions can often increase the overall system security if used *on top* of existing traditional authentication methods. Replacing a current traditional authentication method with a biometric one, on the other hand, may be risky and requires deeper analyses. Biometric authentication systems often replace traditional authentication systems not because of their higher security but because of higher comfort and ease of use.

Biometric key generation is far from mature. The high false rejection rate and short key length are the common shortcomings of most current systems, yet the first practically usable implementations are appearing. However, the use of biometric keys has to cope with the fact that biometric data are not (fully) secret. This makes the use of directly derived biometric keys very problematic, but also biometrically locked cryptographic keys have to take into account that compromise of the biometric data implies easier access to the locked keys – and prudent implementers will protect the secrecy of the locked keys by additional means.

References

[1] Adler, A., Youmaran, R., Loyka, S. (2009) 'Towards a Measure of Biometric Information' in *Pattern Analysis & Applications*, Volume 12, Number 3, Springer London, September 2009.

[2] Adler, A. (2004) 'Reconstruction of source images from quantized biometric match score data' at *Biometrics Consortium Conference 2004*, Washington, DC, USA, September 2004.

[3] Adler, A. (2004) 'Vulnerabilities in biometric encryption systems', at *NATO RTA Workshop: Enhancing Information Systems Security – Biometrics*, IST-044-RWS-007.

[4] Adler, A., Youmaran, R., Loyka, S. (2005) 'Information content of biometric features', at *Biometrics Consortium Conference 2005*, Washington, DC, USA, September 2005.

[5] Ballard, L., Kamara, S., and Reiter, M. K. (2008) 'The practical subtleties of biometric key generation', in *Proceedings of the 17th Conference on Security Symposium*, San Jose, CA, USA, USENIX Association.

[6] Ballard, L., Kamara, S., Monrose, F., Reiter, M. K. (2008). 'Towards practical biometric key generation with randomized biometric templates', in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA. ACM, New York, NY, USA.

[7] Bausinger, O., Seidel, U. (2007) 'Next Generation German e-Passport Fingerprint Enrolment - Quality vs. Time' at *NIST Biometric Quality Workshop 2007*, NIST, 2007.

[8] UK Passport Service (2005) 'Biometrics, enrolment trial', Management Summary. http://www.ips.gov.uk/cps/files/ips/live/assets/documents/UKPSBiometrics-Enrolment-Trial-Report-Management-Summary.pdf

[9] Bicz, W. (2003) 'The Impossibility of Faking Optel's Ultrasonic Fingerprint Scanners', February 2003, http://www.optel.pl.

[10] Biometrics Working Group (2000) 'Best Practices in Testing and Reporting Performance of Biometric Devices'.

[11] Boyen, X et al (2005) 'Secure Remote Authentication Using Biometric Data' in *Advances in cryptology – EUROCRYPT 2005*, pp. 147–163.

[12] Breebaart, J., Yang B., Buhan-Dulman I., Busch Ch. (2009) 'Biometric template protection' in *Datenschutz und Datensicherheit - DuD*, Volume 33, Number 5, Vieweg Verlag,.

[13] Calabrese, C. (1999) 'The trouble with biometrics' in *;login:*, Vol 24, No 4, ISSN 1044-6397.

[14] Chaos Computer Club (2004) 'How to fake fingerprints?'. http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en.

[15] Clancy, T.C., Kiyavash, N., Lin, D.J. (2003) 'Secure Smart Card-Based Fingerprint Authentication' in *Proc. 2003 ACM SIGMM Workshop Biometrics Methods and Application*, 2003.

[16] Crescenzo, G. et al. (2005) 'Approximate Message Authentication and Biometric Entity Authentication' in *Financial Cryptography and Data Security*, LNCS 3570, 2005.

[17] Daugman, J. (1998) 'Phenotypic versus genotypic approaches to face recognition', in *Face Recognition: From Theory to Applications*, Heidelberg, Springer-Verlag, ISBN 3-540-64410-5.

[18] Daugman, J., 'Anti-spoofing Liveness Detection'. Exchanged by personal communication in April 2001.

[19] Derakhshani, R., Schuckers, S., Hornak, L., O'Gorman, L. (2001) 'Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners' in *Pattern Recognition Journal*, Vol. 36, pp. 383-396, December 2001.

[20] Desmedt, Y. (1997) 'Some Recent Research Aspects of Threshold Cryptography' in *Information Security, Proceedings*, LNCS 1396, pp. 158-173, Springer-Verlag.

[21] Dodis, Y., Reyzin, L., Smith, A. (2004) 'Fuzzy extractors: How to Generate Strong Keys from Biometric and Other Noisy Data' in *Proc. Eurocrypt 2004*, pp. 523-540, Springer-Verlag, 2004.

[22] FRONTEX (2007) BIOPASS – Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. 2007.

[23] FRONTEX (2010) BIOPASS II – Automated biometric border crossing systems based on electronic passports

and facial recognition: RAPID and SmartGate. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. 2010.

[24] Gerguri, S., Matyas, V., Riha, Z., Smolik, L. (2010) 'Random Number Generation Based on Fingerprints' in *Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices*. Berlin, Springer, 2010.

[25] Goh, A., Ngo, D.C. L. (2003) 'Computation of Cryptographic Keys from Face Biometrics', in *Proc. 7th IFIP TC6/TC11 Conf. Commun. Multimedia Security*, pp. 1-13, Springer-Verlag, LNCS 2828, 2003.

[26] Grother P. et al. (2006) 'MINEX, Performance and Interoperability of the INCITS 378 Fingerprint Template', NISTIR 7296.

[27] Hao, F., Anderson, R., Daugman, J. (2006) 'Combining Crypto with Biometrics Effectively' in *IEEE Transactions on Computers*, Vol. 55, No. 9, 2006.

[28] Hao, F., Chan, C.W. (2002) 'Private Key Generation from On-Line Handwritten Signatures' in *Information Management & Computer Security*, Vol. 10, No. 2, pp. 159-164, 2002.

[29] Hendricks R. (2010) 'Airport Biometrics Access Control Qualified Products Lists (QPL)' at *Qualifying Identity and Privilege Credential Products for the Transportation Worker Identification Credential (TWIC) and other DHS/TSA programs Qualified Product Lists (QPL)*, NIST, Gaithersburg, MD, USA, 2010.

[30] ISO/IEC JTC 1/SC 27 (2010) 'ISO/IEC FCD 24745 Information technology – Biometric information protection'.

[31] ISO/IEC JTC 1/SC 37 (2004) 'ISO 19794-6 Biometric Data Interchange Formats – Part 6: Iris Image Data'.

[32] ISO/IEC JTC1/SC 37 (2006) 'Harmonized Biometric Vocabulary'.

[33] ITU-T (2004) 'X.1081 - The Telebiometric Multimodal Model - A Framework for the Specification of Security Aspects of Telebiometrics'.

[34] Juels, A. (2004) 'Fuzzy Commitment' at *DIMACS Workshop on Cryptography: Theory Meets Practice*, October 2004.

[35] Juels, A., Wattenberg, M. (1999) 'A Fuzzy Commitment Scheme' in *Proc. Sixth ACM Conf. Computer and Comm. Security*, 1999.

[36] Kallo, P., Kiss, I., Podmaniczky, A. (2001) 'Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus', US patent 6175641, January 2001.

[37] Krishneswari, K., Arumugam, A. (2010) 'A Review on Palm Print Verification System', International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), ISSN: 2150-7988 Vol.2 (2010), pp.113-120.

[38] Linnartz, J.-P., Tuyls P. (2003) 'New shielding functions to enhance privacy and prevent misuse of biometric templates' in *Proc. 4th Int. Conf. AVBPA*, pp. 393–402, 2003.

[39] Liveness Detection in Biometric Systems, http://www.biometricsinfo.org/whitepaper1.htm.

[40] Maiorana, E. (2010) 'Biometric cryptosystem using function based on-line signature recognition' in *Expert Systems with Applications: An International Journal*, April 2010.

[41] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S. (2002) 'Impact of Artificial 'Gummy' Fingers on Fingerprint Systems', SPIE Vol. #4677, *Optical Security and Counterfeit Deterrence Techniques IV*, January 2002, http://cryptome.org/gummy.htm.

[42] MTIT, Minutiae Template Interoperability Testing, http://www.mtitproject.com.

[43] Monrose, F., Reiter, M.K., Li, Q., Lopresti, D.P., Shih, C. (2002) 'Toward Speech-Generated Cryptographic Keys on Resource Constrained Devices', in *USENIX Security Workshop 2002*.

[44] Monrose, F., Reiter, M.K., Wetzel R. (1999) 'Password Hardening Based on Keystroke Dynamics' in *Proc. Sixth ACM Conf. Computer and Comm. Security*.

[45] Phillips P. J. et al (2007) 'FRVT 2006 and ICE 2006 Large-Scale Results', http://www.frvt.org/.

[46] Plaga R. (2009) 'Biometric keys: suitable use cases and achievable information content' in *International Journal of Information Security*, Volume 8, Number 6, Springer Berlin / Heidelberg, 2009.

[47] van der Putte, T., Keuning, J. (2000) 'Biometrical Fingerprint Recognition Don't Get Your Fingers Burned' in *Fourth Working Conference On Smart Card Research and Advanced Applications*, pp. 289-303, Kluwer.

[48] Ratha N.K., Chikkerur S., Connell J. H., Bolle, M. B. (2007) 'Privacy Enhancements for Inexact Biometric Templates' in *Security with Noisy Data*, Springer London.

[49] Ratha N.K., Chikkerur S., Connell J. H., Bolle, M. B. (2007) 'Generating Cancelable Fingerprint Templates' in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Volume 29, Issue 4, IEEE Computer Society, Washington, DC, USA, 2007.

[50] Rowe, R. (2005) 'A Multispectral Sensor for Fingerprint Spoof Detection' in *SENSORS*, 22(1), p. 1-4., January 2005.

[51] Seidel U. (2009) 'Fingerprint capture and the German Experience' in *MRTD Report*, Number 2, Volume 4, International Civil Aviation Organization.

[52] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Vijaya Kumar, B.V.K. (1999) 'Biometric Encryption' in *ICSA Guide to Cryptography*, McGraw-Hill, 1999.

[53] Soutar, C. 'Biometric System Security', White Paper, bioscrypt, http://www.bioscrypt.com/.

[54] Tuyls, P. et al. (2005) 'Practical Biometric Authentication with Template Protection' in *AVBPA 2005*, LNCS 3546, pp. 436-446, 2005.

[55] Thalheim, L., Krissler, J., Ziegler, P.-M. (2002) 'Body Check' in *c't magazine* 11/2002.

[56] Thorpe, J., van Oorschot, P.C., Somayaji, A. (2005) 'Pass-thoughts: Authenticating With Our Minds', in *Proceedings of the ACSA 2005 New Security Paradigms Workshop*, Lake Arrowhead, California, USA, September 2005.

[57] Uludag, U, Jain, A.K. (2004) 'Attacks on biometric systems: a case study in fingerprints', in *Proc. SPIE-EI 2004*, pp. 622-633, San Jose, CA, January 2004.

[58] Wheeler, D. (2001) 'Protocols Using Keys from Faulty Data', in *Security Protocols Workshop 2001*, Springer-Verlag LNCS 2467.

[59] Young, M. (2006) 'Equating Biometric Entropy' in *Biometric Consortium Conference*, Baltimore, MD, 2006.

[60] Ziauddin S., Dailey M.N. (2010) 'Robust iris verification for key management' in *Pattern Recognition Letters*, Elsevier, 2010.

Author Biographies

Václav (Vashek) Matyáš is a Professor at the Masaryk University Brno, CZ, chairing its Department of Computer Systems and Communications. His research interests relate to applied cryptography and security, where he published nearly hundred peer-reviewed papers and articles, and co-authored six books. He worked with Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and was a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek is one of the Editors-in-Chief of the Identity in the Information Society journal, he edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. He received his PhD degree from Masaryk University, Brno and can be contacted at matyas@fi.muni.cz

Zdenek Riha is an Assistant Professor with the Masaryk University in Brno, Czech Republic, working in the area of computer security. He received a PhD degree in Computer Science from the Faculty of Informatics, Masaryk University in Brno. Between 2005 and 2008 he was seconded as National Detached Expert to the Joint Research Centre of the European Commission. His interests include authentication, identity documents, PKI and security of operating systems.