A Risk Analysis Approach for Biometric Authentication Technology

Arslan Brömme

AGN Science & Research Group, Department of Informatics University of Hamburg
(Email: arslan.broemme@aviomatik.de)

(Received July 10, 2005; revised and accepted Aug. 12, 2005)

Abstract

Current approaches for risk analysis of biometric authentication technology are limited to enrollment and identification/verification processes with biometric algorithms mainly considered as black-boxes, only. This paper presents a systematic approach for a *holistic security risk analysis of biometric authentication technology* based on the *high-level component & process model for integrated security risk analysis of biometric authentication technology*, also proposed here. The processes and components used within this model are introduced together with a comprehensive *terminology for biometric authentication technology* especially developed for the research area of *IT security biometrics*. *Biometric authentication risk matrices* are used to show that single *possible risk effect classes* can be identified. A discussion on the enabled possibilities for risk analysis shows the significant advantage of this integrated approach for holistic security risk analysis of biometric authentication technology in comparison to other approaches.

Keywords: Authentication, biometric authentication technology, holistic security risk analysis, IT security biometrics, risk analysis

1 Introduction

After having established the legal basis for the broad usage of biometric technology the adequate evaluation of resulting technical and societal risks in a holistic manner is of high importance. With the already started international governmentally supported standardization projects and working groups (for instance ISO/IEC SC 37) for biometric person identification and authentication technology, it can be stated that biometric technology should be available for example with standardized data formats for biometric data interchange, communication protocols, and unified programming interfaces for enabling the interoperability of different biometric systems and components in existing (national) information and communication technology (ICT) infrastructures. Biometric technology for person authentication, identification, surveillance, and other applications itself contains core processes and components, which are the main subject of the risk analysis and evaluation approach in this paper. The paper starts with selected terminology from *IT security biometrics*, *privacy*, *safety, performance, and security risk analysis for biometric authentication technology* and a comprehensive approach for *biometric authentication systems* in Section 2. In Section 3 a *high-level component & process model for integrated security risk analysis of biometric authentication technology* is presented. A *holistic security risk analysis approach for biometric authentication technology* based on the predefined model and on *biometric authentication risk matrices* is discussed in Section 4. This paper closes with conclusions in Section 5.

2 Fundamentals

Fundamentals are given in two subsections dedicated to *terminology* (2.1) and *biometric authentication systems for ICT infrastructures* (2.2).

2.1 Terminology on IT Security Biometrics, Privacy, and Risks

IT Security Biometrics. For authentication, identification, and surveillance purposes *IT security biometrics* uses the mathematical definitions of *metrics* and *metric spaces* as explained in [2], which are defined by *Weisstein* in [35]. *Jain and Dubes* are defining in [13, 19] distance measures based on the *Minkowski metric* $d(i,k) = (\sum_{j=1}^{d} |x_{ij} - x_{kj}|^r)^{\frac{1}{r}}$, where $r \geq 1$ and $x_{(i|k)j}$ is the jth feature of the $(i|k)$th pattern in a pattern matrix. The Minkowski metric defines for $r = 2$ the *Euclidean distance*, for $r = 1$ the *Manhattan distance*, and for $r \to \infty$ the *sup distance*. If all features are binary the Manhattan distance is called *Hamming distance*, which is known from the comparison of iris codes (=biometric signatures)

of *Daugman*'s method in [12]. *IT security biometrics* is defined in [2]:

> Definition: **IT security biometrics** is the study on person recognition methods based on the sensing of a person's biological characteristics, measuring of the captured or scanned biometric characteristics (raw data and sensor system calibration data), computing of biometric signatures and biometric templates, and verifying and identifying against biometric templates and (hashed) biometric signatures with regard to the mathematical definitions of metrics and metric spaces. The (hashed) biometric signatures are used for authentication purposes against and identification and surveillance purposes by IT systems within ICT infrastructures.

Privacy. Privacy is everyone's fundamental human right, which is documented in the *Universal Declaration of Human Rights* by the General Assembly of the United Nations [16]. In this paper a definition of privacy by *Westin* from [34] is used: *"**Privacy** is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others". Fischer-Hübner* formulates in [14] basic privacy principles, which summarize the most essential privacy requirements. Concerning the analysis of risks for privacy in biometric IT systems, the discussion focusses on the *privacy principles of purpose binding and necessity of data collection.* The principle of purpose binding limits the subsequent use of personal data to the specified purposes. The principle of necessity of data collection means to avoid or at least to minimize personal data within an ICT system.

Safety and Performance Risks of Biometric Authentication Technology. *Leveson* delivers in [24] the terminology used in IT safety for defining risks. Based on a definition of *hazard (level)* she defines the notion of risk: "**Risk** is the hazard level combined with (1) the likelihood of the hazard leading to an accident ([...] danger) and (2) hazard exposure or duration ([...] latency)". Leveson additionally proposes that "The likelihood of hazard occurrence can be specified quantitatively or qualitatively.". With regard to wider safety issues she defines the terms *failure* and *fault*: "**Failure** is the nonperformance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions. **Fault** is a higher-order event. [...] In general all failures are faults, but not all faults are failures.". Leveson further presents a distinction of faults in subcategories cited from *McCormick* in [27] for clarifying the term higher-order event. A detailed classification of faults is given by *Laprie* in [23]. Focussing on the aspects of safety (e.g. reliability, availability) and performance (e.g. throughput, latency) a specific definition is used here:

> Definition: A **safety risk of biometric authentication technology** is the *risk* of degradation of the biometric authentication system's *safety* and performance caused by *failures* and *faults*.

Security Risk of Biometric Authentication Technology. *Kossakowski* describes in [21] a risk management process based on the three main parts *risk analysis*, *crisis management*, and *insurances*, where he extends a risk analysis phase for *evaluation of threats and risks* by *Bhaskar* in [1] to a control cycle subsuming: 1. initiation and determination of goals, 2. evaluation of threats and risks, 2a. identification of assets, 2b. identification and evaluation of threats, 2c. identification and evaluation of vulnerabilities, 2d. identification and evaluation of risks, 2e. identification and evaluation of security measurements, 3. selection of measurements, 4. execution of measurements, and 5. control and improvement of measurements and personnel; goto 4. With regard to 2b.-2d. it can be concluded for a risk analysis approach for biometric technology that *threats* need to be identified and evaluated revealing *vulnerabilities* from which specific *risks* for biometric technology are derived. By taking the general aspects of the definitions of the terms *threat* and *vulnerability* by *Pfleeger and Pfleeger* in [29], *Bishop* in [3], and *Shirey* in [33] into account specific definitions are used here:

> Definitions: A **threat to biometric authentication technology** is the potential of a circumstance or an action that causes loss of security, degradation of the technology's reliability or performance, or the harm to a person's privacy. The **vulnerability of biometric authentication technology** is a flaw or weakness that makes it possible for a *threat to biometric authentication technology* to occur.

Shirey defines in [33]: *"**risk** [...] expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.".* Kossakowski defines in [21]: *"**risk** [...] the extent of a threat. For this the probability of the vulnerability's exploitation is combined with the expected degree of damage."* (translated from German). The above IT security definitions of risk are focussing on probabilities of threats exploiting vulnerabilities with expected harmful results or damages. A specific security risk is used here:

> Definition: A **security risk of biometric authentication technology** is an expectation of loss expressed as the probability that a specific *threat to biometric authentication technology* will be exploited against a specific *vulnerability of biometric authentication technology* with potentially hazardous consequences and effects.

Brunnstein defines in [8] a *Security & Application Risk Traffic Light Model* to cope with quantitative probabilities, which are difficult and sometimes impossible to determine for IT security (biometrics) issues. Within this model colors are used to indicate the probability of an exploited vulnerability, representing the risk, in a qualitative way. Green represents a low probability, yellow a medium, and red a (very) high probability for a risk to manifest. This approach modified for the field of application risk management has been presented in [9], where the colors are indicating the states of application processes ranging from green for no risk (OK), over yellow for low risk, and orange for medium risk to red for high risk (ALERT). Brunnstein's model is used here as follows:

> Definition: A **security* risk of biometric authentication technology** is a *security risk of biometric authentication technology* expressed along *Brunnstein's Security & Application Risk Traffic Light Model*.

2.2 Biometric Authentication Systems for ICT Infrastructures

A biometric authentication system can be considered as a part of a biometric authentication infrastructure where a person is subjected to a *general authentication process*, which is given by [2]:

1) **Enrollment**:
   During the phase of *enrollment* appropriate biometric raw data of a person is captured, the biometric signature (template|class) for the biometric authentication is computed, and the relevant biometric and personal data is stored in a biometric database.

2) **(Biometric) Authentication (1:c, 1:1)**: A person's authenticity is checked by an identification (1:c) or verification (1:1) comparison of the present computed biometric signature with the previously computed biometric signature (template|class) in the phase of *biometric authentication* with(out) being combined with authentication methods based on a person's knowledge, possession, location, and time (*(single|multi)factor biometric authentication*).

3) **Authorization**:
   Implicit and explicit authorizations are given to the person in the *authorization* phase with respect to strong and weak authorizations.

4) **Access Control**:
   In the *access control* phase the access to e.g. IT system resources or activity control within electronic business processes is granted by an *access management system* (AMS), which can be based on the concepts of mandatory, discretionary, or role-based access control (M/D/RBAC).

5) **Derollment and Authorization Withdrawal**:
   In the phase of *derollment and authorization withdrawal* a person is derolled and the access rights, relevant biometric and personal data are removed from a biometric database.

A set of basic elements can be identified from which biometric authentication systems along the general (biometric) authentication process can be constructed. These elements are wetware entities (persons) and hardware components, biometric communication channels, biometric processes for (en|de)rollment and authentication, biometric algorithms, biometric signatures, and biometric databases.

> Definition: A **biometric authentication system** is defined as a set of hardware components, processes, algorithms, data structures, and databases fulfilling internal and/or external communication between the elements for the purpose of biometric authentication.

Biometric Processes. Based on the general (biometric) authentication process four core processes can be identified: *sensing* and *biometric (en|de)rollment and authentication processes*. Figure 1 shows the biometric (en|de)rollment processes from [2] and the extension of the biometric authentication process from [2, 7].

> Definitions: **Biometric enrollment** is the process of training a person's biometric (characteristics|patterns) into a biometric person recognition system and storing of the biometric data in a biometric database. **Biometric authentication** is the process of verifying a person's claimed identity by comparison of a computed biometric signature from the person's biometric (characteristics|patterns) against a stored biometric template. **Biometric derollment** is the process of detraining a person's biometric (characteristics|patterns) from a biometric person recognition system and removal of the biometric data from a biometric database.

A *sensing process* within an *(active) sensor system* is used, which delivers a *human-sensor-system-interface* for capturing/scanning a person's biological characteristics. The *capturing/scanning process* results in *biometric raw data and sensor system calibration data*, called *biometric characteristics*. The captured data is handed over to the biometric (en|de)rollment or authentication algorithm. For authentication the authorized users are assumed to be already enrolled and their biometric templates to be stored in a secure biometric database.

Biometric Algorithms. Within the sequential biometric processes for (en|de)rollment and authentication several algorithms – also called *modules* with regard to their implementations – are used for different computations (Figure 1): P: *preprocessing*, Q:

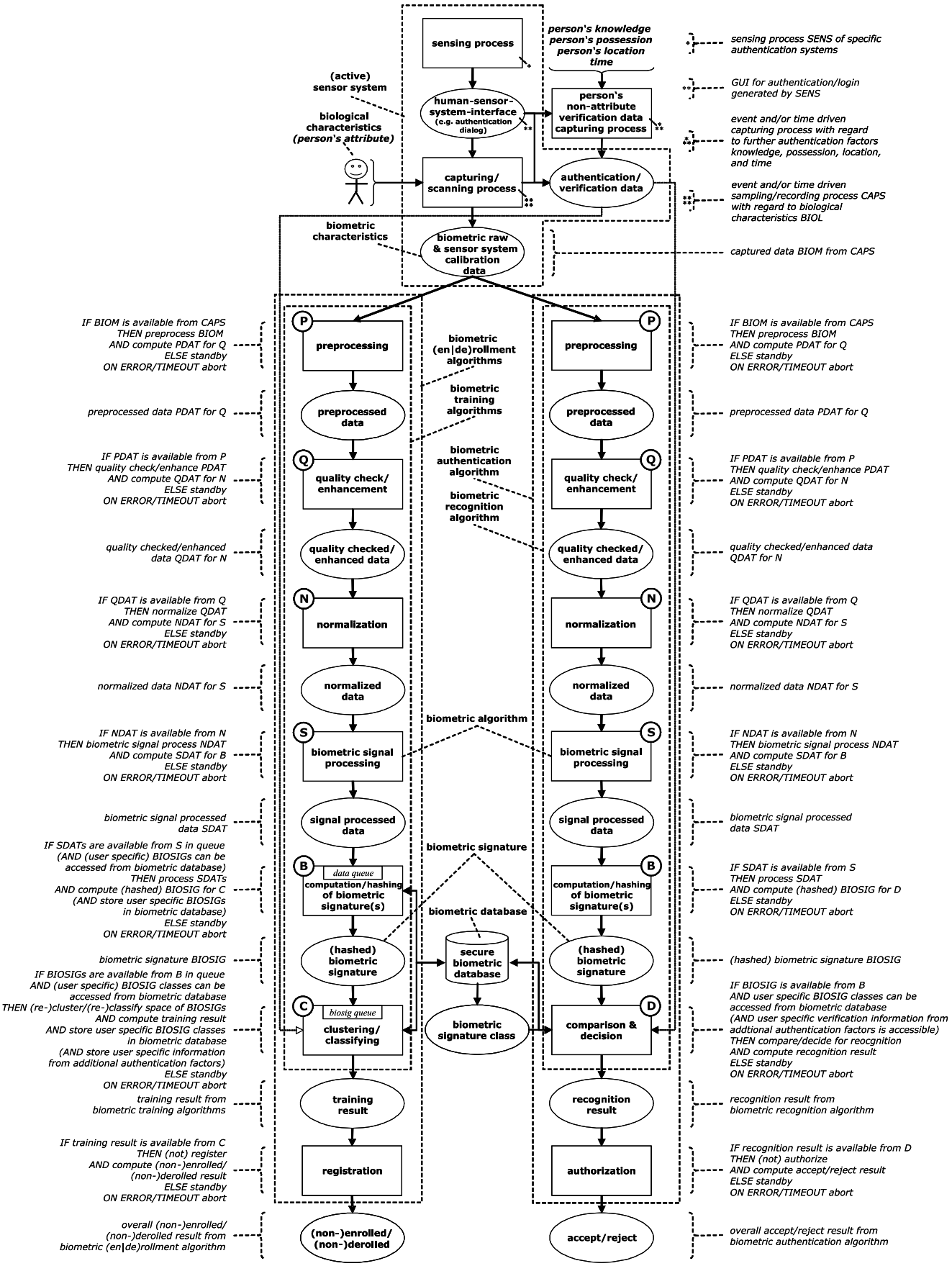

Figure 1: Biometric sensing, enrollment, authentication, and derollment processes for (Single|Multi)factor and (Mono|Multi)modal biometric authentication systems

quality check/enhancement & decision, *N*: *normalization*, *S*: *biometric signal processing*, *B*: *computation/hashing of biometric signature*, *C* [en-/derollment]: *[re](clustering/classifying)*, and *D* [authentication]: *comparison & decision* algorithm. Homonymously, complete biometric processes are called biometric algorithms due to their application-specific dedication as parts of biometric authentication systems. Here a *biometric algorithm* is defined as follows:

> Definition: In the broader sense a **biometric (enrollment | authentication | derollment) algorithm** is an algorithm for the enrollment, authentication, or derollment of a person's biometric characteristics against a biometric (authenti|identifi)cation system or abortion of an attempt. In the narrower sense a **biometric algorithm** is a *biometric signal processing algorithm* used within (en|de)rollment and authentication.

> Definitions: A **biometric signature** is a (bin|n-)ary coded representation of biometric characteristics for (distributed) computing systems. A **biometric template** is a biometric signature (class|cluster) representing a set of biometric signatures. Biometric signatures/templates can be hashed which results in **hashed biometric signatures/templates**.

Biometric Databases. According to [5] a biometric database is defined as:

> Definitions: A **biometric database** is a database which holds data about biometric characteristics, biometric signatures, and personal data. A biometric database which subsumes biometric characteristics (raw data and calibration data), biometric signatures, personal data, and a rule-based access control mechanism is defined to be a **complete** biometric database. A **partial** biometric database represents a subset of a complete biometric database.

Biometric Communication Channels. A threat for biometric authentication via insecure networks is given by replay attacks. A concept of a technical solution for this problem is presented in Figure 2 by using an active sensor system with an emitter for security information, which is controlled over a control channel by a biometric authentication server. The biometric raw data with the added security information is captured and transferred to the server over the data channel. The server accepts received biometric raw data, if the expected and valid security information is included. The cryptographic secured control and data channels, the active sensor system and security information enhanced biometric raw data are defined together as *secure biometric communication channels*.

3 A High-Level Component & Process Model for Integrated Security Risk Analysis of Biometric Authentication Technology

In this section a *high-level component & process model for integrated security risk analysis of biometric authentication technology* (ComProMiSe·Risk·of·BiT) (Figure 3) is introduced, which is at least applicable for security analysis methods of *attack trees* by *Schneier* in [32], safety analysis methods of *fault trees* like e.g. by *Leveson* in [24], performance testing methods like e.g. by *Bolle et al.* in [4], and privacy related analysis like taught by *Fischer-Hübner* and *Brunnstein*. According to the *BSI* in [10] security attacks on biometric technology can be classified using three basic categories: **1. sensor attacks** (copy, falsification, similarity attacks), **2. data communication attacks** (replay attacks), and **3. database attacks** (integrity attacks). The model introduced here extends this set of categories by a fourth category **4. computation attacks** and, therefore, delivers a detailed understanding of the biometric processes used in biometric authentication technology as defined here (2.2). This new category with strong relation to security attacks is the starting point for the notion of the model to extend all four categories to risks integrating (classical|holistic) security, safety, performance, and privacy aspects: **1. capture risks, 2. transmission risks, 3. storage risks, and 4. computation risks**. In Figure 3 the main components of biometric authentication technology are listed on the top level *high-level methods* with the methods *capture*, *transmission*, *storage*, and *computation*. On the level below, titled *high-level processes/functions*, the different processes for the components of the upper level can be found. The capture method includes a *sensing process*. The transmission method is associated with processes of *sending*, *receiving*, and *(en|de)cryption*. The method storage is related with processes of *query*, *update*, and *write*. Finally, the computation method is combined with processes for *(en|de)rollment* and *authentication*. Biometric authentication technology investigated in the granularity of high-level processes enables black box tests, which are limited in behalf of more detailed evaluation and testing within risk analysis procedures integrating aspects of security, privacy, safety, and performance. The scope of the model presented here includes another level titled *high-level process components/function modules* which enables the study on risks based on process components/function modules *preprocessing* **P**, *quality check/enhancement & decision* **Q**, *normalization* **N**, *biometric signal processing* **S**, *computation/hashing of biometric signature/s* **B**, *[re](clustering|classifying)* **C** [en-/derollment], and *comparison & decision* **D** [authentication] within the biometric processes (2.2) in addition to the components of the other high-level methods. A subdivision of the

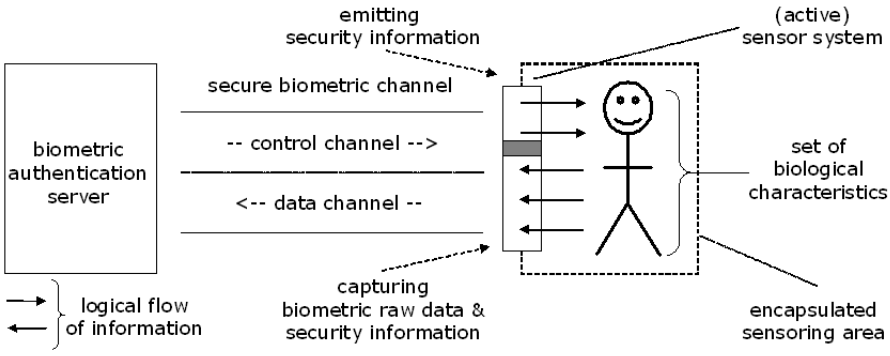

Figure 2: Secure biometric communication channel (biochannel)

high-level process components/function modules reveals *sub-level processes/functions* and *sub-level process components/function modules*, which are out of the model's scope due to their algorithm-specific content.

What types of risks can be discussed with the model? The model enables different types of **single and integrated risks** to be discussed specifically for biometric authentication technology: *classical security*, *privacy*, *safety*, *performance*, and *holistic security risks*. The *classical security risks* are based on the criteria of *confidentiality* (e.g. secrecy, authenticity), *integrity*, and *availability*. The availability aspect obviously reveals that even in first approaches security risks are considered as an integrated aspect. Within the determination of classical security risks both qualitative and quantitative analysis has been done. One main research aspect are **attacks** threatening the resources and systemic assets by exploiting vulnerabilities. The understanding of **faults** has been inherited from IT safety for discussing availability. *Privacy risks* are mainly a qualitative analysis criterion and can be explained by considering **misuses** which can be (non-)intentional. Research aspects in privacy analysis are e.g. anonymity, pseudonymity, purpose binding of data processing, and necessity of data collection like presented by Fischer-Hübner in [14]. Research has also been done with regard to *safety risks* defined on hazards and which are based on an understanding of **faults** for discussing e.g. aspects of reliability and availability. A strong relation is given to performance analysis methods for explaining faults based on **failures**. The quantitative aspect of *performance risks* (e.g. throughput, latency) can be discussed using the criterion **failures**, which is jointly used within safety and performance risk analysis. Current IT security discussions are integrating aspects of classical security risks, privacy risks, safety, performance, and other relevant risks into a joint holistic understanding of risks for IT systems. For this model a *holistic security risk* is understood with regard to a technical system's *functionalities* in order to integrate different risk criterions into a joint view. Furthermore it is assumed that security, privacy, safety, and performance requirements in all life cycle phases of biometric authentication technology can be explained as functionalities. *Brunnstein* defines in [11]: *"A program's or module's or object's* ***functionality*** *is characterized by the set of all specifications, formal or informal, from which information about 'proper work' of a program can be concluded, and from which certain undesired functions can be excluded."*. The holistic risk criterion shall be defined on the core notion of **dysfunctionality** by Brunnstein in [11]: *"A software or module is called* ***dysfunctional*** *when at least one function deviates from the specification."*:

> Definition: A **holistic security(*) risk of biometric authentication technology** is a *security(*) risk of biometric authentication technology* which is based on *dysfunctional* biometric authentication technology with regard to security, privacy, safety, and performance described along the *high-level component & process model for integrated security risk analysis of biometric authentication technology*.

4 A Discussion on a Holistic Security Risk Analysis Approach for Biometric Authentication Technology

This section evaluates related security risk analysis approaches (4.1) and performance evaluation approaches (4.2). Finally, a holistic risk analysis approach enabled by the ComProMiSe·Risk·of·BiT model from Section 3 is proposed (4.3).

4.1 Evaluation of Related Security Risk Analysis Approaches

Only few partial risk analysis studies with relation to *biometric authentication systems* exist. Selected related work, initiated and supervised mainly by Brunnstein and Brömme, is evaluated against the understanding of *holis-*

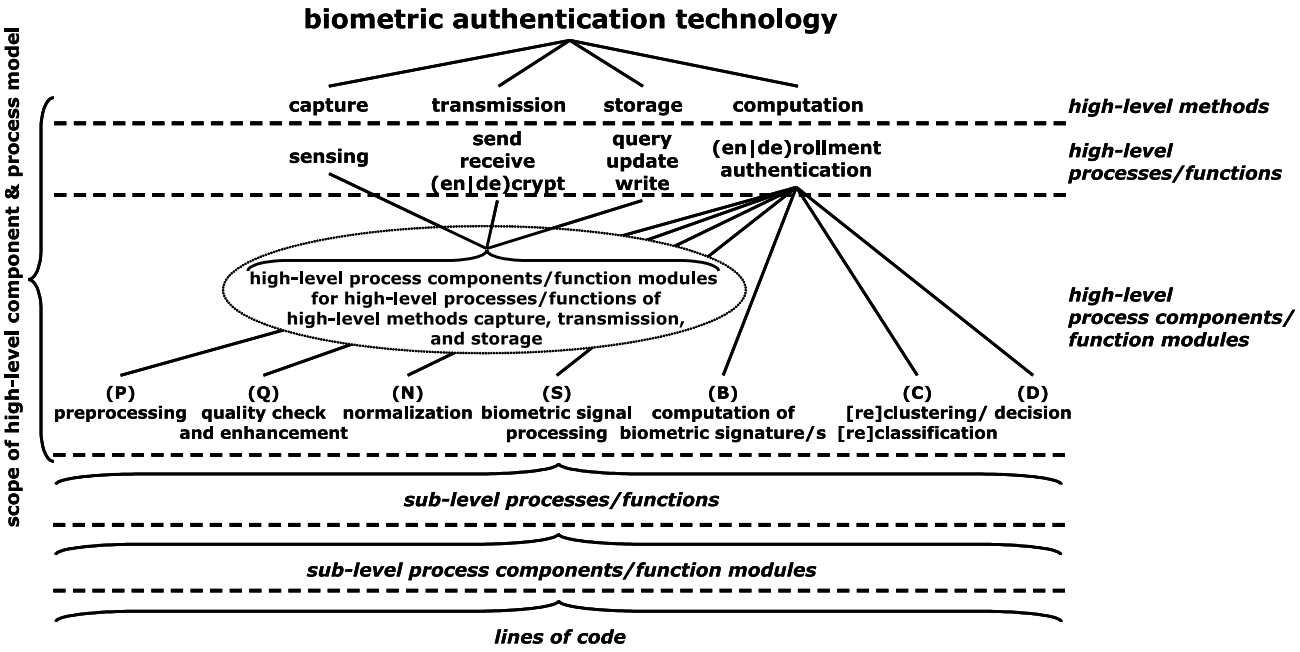

Figure 3: High-Level Component & Process Model for integrated Security Risk Analysis of Biometric Authentication Technology (ComProMiSe·Risk·of·BiT)

tic security(*) risk of biometric authentication technology as defined here. **Capture Risks.** A risk analysis approach of biometric systems is presented in [28] by *Paulsen*. Within this work a qualitative risk analysis approach, which is based on a model and terminology by Brömme, focussing on sensor attacks is discussed for fingerprint, face, hand geometry, iris, and speaker recognition. Aspects of attacks against operating systems and organizational risks are described. With regard to the *holistic security(*) risk of biometric authentication technology* Paulsen's work supports no qualitative risk analysis on the training algorithms of biometric authentication systems and delivers neither a risk analysis discussion on the methods of transmission, storage, nor computation. **Transmission Risks.** *Froehling* describes in [15] an encrypted transmission channel for biometric data based on the idea and concept of *secure biometric channels* (2.2) by Brömme. This work finally avoids to deliver the intended qualitative risk analysis approach with focus on the transmission of biometric data and presents the prototypical development of the communication channel, only. With regard to the *holistic security(*) risk of biometric authentication technology* Froehling's work is neither discussing a single transmission risk analysis approach nor an integrated risk analysis approach. **Storage Risks.** *Kronberg* presents in [22] a.o. an approach integrating an iris recognition method into Windows NT/2k's logon. In behalf of integrating the algorithm and storing and accessing computed biometric signatures/templates and the users' verification information, he studies different locations for biometric databases. Kronberg discusses partial resulting risks for biometric databases from different attack types within Windows. A discussion on *holistic security(*) risks of biometric authentication technology* like proposed here is not delivered. **Computation Risks.** *Johns* studies in [20] the applicability of wavelet transformations for biometric authentication with strong focus on the mathematics of wavelets. For the link to IT security Johns uses the terminology and parts of the model from Brömme's previous work and demonstrates the applicability of the *biometric authentication process* from [7] for testing and evaluation of an iris recognition algorithm's reliability and performance. With regard to the *holistic security(*) risk of biometric authentication technology* Johns' work supports a single partial risk analysis of biometric algorithms only and enables neither an integrated nor a holistic risk analysis approach.

4.2 Evaluation of Selected Performance Testing Approaches of Biometric Algorithms and Systems

Assuming that biometric systems and algorithms are understood as pure *pattern recognition systems and algorithms* test and evaluation approaches regarding their performance exist. An introduction to evaluating biometric systems with strong regard to their performance is given by *Phillips et al.* in [31]. Here some characteristics for ideal biometric systems are assumed: all members of a population possess the needed biometric characteristic for recognition, every biometric signature differs from all others within the controlled population, biometric signatures don't vary under the conditions in which they are collected, and the biometric system resists countermeasures.

The evaluation is understood as the quantification of how well biometric systems meet these properties. Phillips et al. present performance evaluations (focussing their results on the *false alarm/reject rate* - different terms for *false acceptance/rejection rate*) done within laboratory and/or scenario tests at the *NIST* with regard to face (face recognition technology - FERET 1993-98), voice, and fingerprint recognition. The FERET tests have been followed by *face recognition vendor tests* (FRVT) in 2000-02. Phillips et al. are presenting within the FRVT 2002 report [30] an evaluation methodology for face recognition systems which is claimed to be adequate for general testing of biometric systems. The FRVT tests are also focussing on performance aspects. The herein used specific performance measures *medium computational intensity* (MCInt) and *high computational intensity* (HCInt) were generated for the evaluation of large-scale real world applications. For fingerprint verification several international *fingerprint verification competitions* (FVC) were executed in 2000-02 and initiated for 2004. Like reported by *Maio et al.* in [25] these tests of pattern recognition applications focus on measuring the performance of the submitted fingerprint recognition algorithms along a predefined protocol. The *genuine and imposter score distributions*, *false (non-)match rates* (F(N)MR), *receiver operating curves* (ROC), and *enrollment and matching times* were determined, recorded and compared. A general approach for testing and reporting the performance of biometric devices has been presented by *Mansfield and Wayman* in [26]. They acknowledge that technical performance testing is only a single form of biometric testing. Other types of testing, like e.g. reliability, availability, maintainability, vulnerability, security, and more, are listed within this report but are explicitly not addressed. So far it can be concluded that none of the performance testing approaches presented above enables a discussion on *holistic security(*) risks of biometric authentication technology* like proposed here.

4.3 Towards a Holistic Security Risk Analysis Approach for Biometric Authentication Technology

By studying security risks of biometric authentication methods, researchers come to more secure and reliable prototypical research solutions like presented for instance with *multimodal biometric methods* (biometric fusion techniques) by *Hong and Jain* in [17] and with *multifactor multimodal biometric authentication methods* by Brömme in [6]. Based on adapted fault trees for security analyses, introduced by *Schneier* in [32] as *attack trees*, a general attack tree for different types of biometric methods can be constructed showing a security risk analysis in a qualitative way (Figure 4). By increasing the complexity of the biometric authentication method from *(single|multi)factor monomodal* to *(single|multi)factor multimodal biometric authentication methods*, a higher security benefit is produced. From a non-holistic security engineering point of view *multifactor multimodal biometric authentication methods should be preferred with regard to (high) security requirements.* This result enables a lot of research potential for promising innovative biometric authentication approaches. Instances from the application class of multifactor multimodal biometric authentication technology can be developed for fulfilling technical requirements for performance, safety (reliability), and classical security (confidentiality, integrity, availability). Therefore, the described type of biometric authentication technology from Section 2.2 can be used to derive different design patterns for modularization and interfaces of processes and components. Single technical risk analysis approaches and methods can show risks with regard to specific aspects like safety and performance issues. By also considering integrated risk analysis approaches like in classical security, generic data formats and interfaces between communicating modules and processes have to be defined for enabling an integrated view and evaluation of the resulting combined or overall system risks. So far, pure technical development methods for minimizing risks can be used as long as the different technical requirements from the different technical fields are fulfilled within an integrated system. For the technical aspects of security, safety, and performance it can be concluded for a holistic security risk analysis approach for biometric authentication technology that a *well-defined* understanding of the processes and components involved in the used biometric technology is necessary (2.2). For a holistic security risk analysis it can also be concluded that it is of little help that processes and components of biometric technology are covered as so called *company secrets*. Within a holistic security risk analysis approach also non-technical but societal demands arise, for example from the field of privacy. Here a simple technical solution for biometric systems with strong regard to the classical security aspect of confidentiality (especially secrecy) is stated for instance by *Jain* in [18] with a slide showing *"Protect the template!"* (it has not been stated to protect the biometric raw data). This statement implies that the uncontrolled collection and storage of biometric (raw) data can be done as long as a protection mechanism in form of cryptographic security or organizational and governmental policies exists. From a holistic security point of view, this is a restricted view on *privacy-enhancing biometric authentication technology* for bypassing the technical problems arising with privacy demands directly influencing the system design of biometric authentication technology down to very low technological levels. With Westin's understanding of privacy in mind it can be obviously concluded that *individuals, groups and institutions* **cannot** *determine for themselves, when, how and to what extent information about them is communicated to others* due to the fact that a different type of biometric technology with controlled collection, storage, and if demanded avoidance of biometric (raw) data depending on the purpose of usage is not offered, even if a development of such a system is possible. Based on this knowledge there is

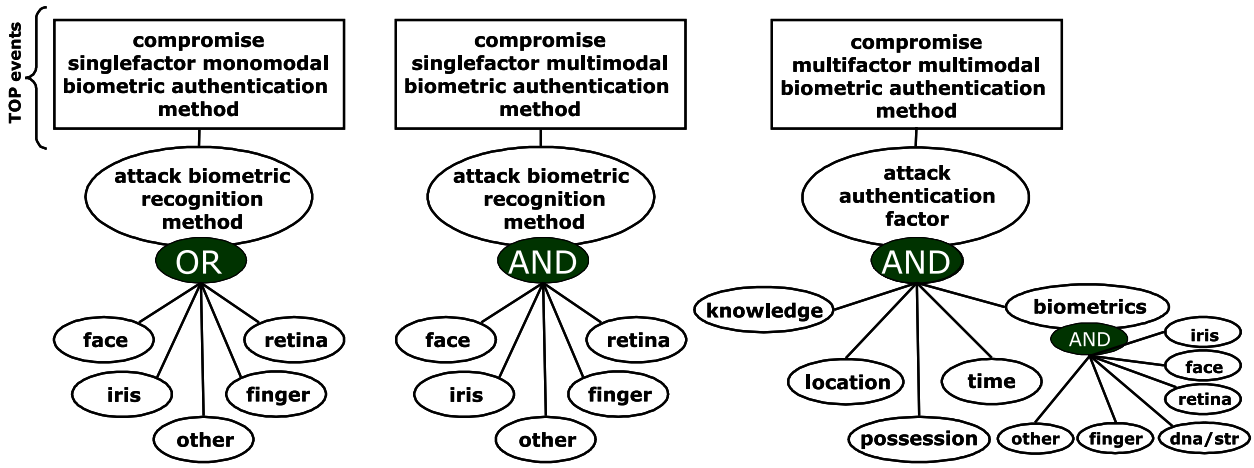

Figure 4: General attack trees for (single|multi)factor (mono|multi)modal biometric authentication methods

a need of a systematic approach for finding holistic security risks in biometric authentication technology as a basis for risk analysis and evaluation. One such approach is presented here by using *biometric authentication risk matrices*.

Enabling Holistic Security Risk Analysis by using Biometric Authentication Risk Matrices. Within this section *biometric authentication risk matrices*, which are based on the model ComProMiSe·Risk·of·BiT, are introduced to systematically show and selectively discuss aspects of the area of holistic security risks for biometric authentication technology. A *risk matrix for biometric authentication methods* is constructed from the elements (processes and components) used within the method with the intention to show specific scopes of potential risk interrelations between these elements. A *potential* for a risk interrelation is given if there is no assumption or no evidence for the absence of a risk. The relation $\perp$ between these elements is called *has potential risk effect on*. If there exists at minimum one case confirming this risk effect then $\perp$ changes to $\vdash$ representing *has risk effect on*. If there is an assumption or for sure no risk effect then the symbols $\pm$ for *has no potential risk effect* and $\top$ for *has no risk effect* are used. Processes are abbreviated with small latin letters and components with capital latin letters. The placeholder $\star$ remains empty or can be replaced by specific risk aspects of **secu**rity, **priv**acy, **safe**ty, and **perf**ormance. The symbol $\diamond$ is a placeholder that remains empty or can be replaced by **att**a**c**k, **misu**se, **faul**t, and **fail**ure (Table 1).

The risk matrix in Table 2 visualizes the *potential risk effects* between the three main biometric processes. The matrix entry $\mathbf{e}_{\diamond}\perp_{\star}\mathbf{a}$ represents in general risk influences of biometric enrollment processes on biometric authentication processes. This can be instantiated for example with $\mathbf{e_{faul}}\perp_{\mathbf{safe}}\mathbf{a}$ describing a less reliable enrollment process which has a *potential safety risk effect on* the authentication process resulting in the false recognition and/or acceptance of persons. Another example is given with matrix entry $\mathbf{d}_{\diamond}\perp_{\star}\mathbf{a}$ of Table 2 as representation of general risk influences of biometric derollment processes on biometric authentication processes. Given the instantiation of an attack for a derollment process $\mathbf{d_{attc}}\perp_{\mathbf{secu}}\mathbf{a}$ a *potential security risk effect on* a subsequent authentication process can arise resulting for example in the non-derollment of the selected person or derollment of a third not selected person with the intention to later on falsely recognize and/or accept the person which should be derolled. It can be concluded that the flexibility of the $_{\diamond}\perp_{\star}$ relation in combination with the risk matrix enables the systematic discussion of holistic security risks based on different security risks between the processes for (en|de)rollment and authentication. By taking the components of the three main processes into account a more complex matrix (Table 3), called *full biometric authentication risk matrix*, can be generated to show the risk interrelations between the process components and the processes with regard to the single risk aspects described by the $_{\diamond}\perp_{\star}$ relation. From the overall *more than seven thousand*[1] single *possible risk effect classes* (PREC) given here, three attack examples are introduced (emphasized in Table 3) to demonstrate the strength of this approach in systematically exploring and discussing holistic security risks for biometric authentication technology.

Example PREC#1 $\boldsymbol{eB}_{attc}\perp_{secu}\boldsymbol{aD}$. This class of possible risk attacks describes the manipulation of enrollment computations of biometric signatures (enrollment B module) for intended false acceptance of imposters and/or false rejection of genuines in subsequent authentication attempts (authentication D module).

Example PREC#2 $\boldsymbol{dC}_{attc}\perp_{safe}\boldsymbol{eC}$. Within this class the possible manipulation of a derollment reclustering of the feature space for biometric templates (derollment C module) of all enrolled persons during the derollment of a sin-

[1] 7056 = (4 × 4) × [(3 × 3) + (3 × 18) + (18 × 3) + (18 × 18)]=(risk aspect vs risk aspect)×[(processes vs processes)+(processes vs components)+(components vs processes)+(components vs components)]

Table 1: Notation for $\perp$ and ${}_{\diamond}\perp_{\star}$ relations of biometric authentication risk matrices

$x \perp y$	process x *has potential risk effect on* process y	$x {}_{\diamond}\perp_{\star} y$	$\diamond$ *of* process x *has potential* $\star$ *risk effect on* process y
$xA \perp yB$	process x component A *has potential risk effect on* process y component B	$xA {}_{\diamond}\perp_{\star} yB$	$\diamond$ *of* process x component A *has potential* $\star$ *risk effect on* process y component B
$xA \perp y$	process x component A *has potential risk effect on* process y	$xA {}_{\diamond}\perp_{\star} y$	$\diamond$ *of* process x component A *has potential* $\star$ *risk effect on* process y
$x \perp yB$	process x *has potential risk effect on* process y component B	$x {}_{\diamond}\perp_{\star} yB$	$\diamond$ *of* process x *has potential* $\star$ *risk effect on* process y component B

Table 2: Risk matrix for the ${}_{\diamond}\perp_{\star}$ relation between biometric processes for (En|De)rollment and authentication with emphasized examples $e_{\diamond}\perp_{\star}a$ and $d_{\diamond}\perp_{\star}a$

${}_{\diamond}\perp_{\star}$	enrollment	authentication	derollment
enrollment	$e_{\diamond}\perp_{\star}e$	$a_{\diamond}\perp_{\star}e$	$d_{\diamond}\perp_{\star}e$
authentication	$\mathbf{e}_{\diamond}\perp_{\star}\mathbf{a}$	$a_{\diamond}\perp_{\star}a$	$\mathbf{d}_{\diamond}\perp_{\star}\mathbf{a}$
derollment	$e_{\diamond}\perp_{\star}d$	$a_{\diamond}\perp_{\star}d$	$d_{\diamond}\perp_{\star}d$

gle person with the intended reliability risk effect on the enrollment reclustering of the feature space for persons to be enrolled (enrollment C module) is described.
Example PREC#3 $\boldsymbol{aD}_{attc}\perp_{secu}\boldsymbol{dC}$. This class outlines the manipulation of the decision within an authentication attempt (authentication D module) with the intention to falsely remove a person's biometric template within a subsequent derollment procedure (derollment C module). An automatic biometric authentication system with a limited number of entrance allowances per person for public transportation could be, for example, target of such an attack.

For the holistic security risk analysis approach for biometric authentication technology presented here it can be concluded that the flexibility of the ${}_{\diamond}\perp_{\star}$ relation in combination with a risk matrix enables the systematic exploration and discussion of holistic security risks by a security analyst with(out) help of an inference system guiding through the single implicit possible risk effects along the risk matrix of a biometric authentication system, which is under study. The holistic security risks are based on different security risks between the biometric processes and/or their components.

5 Conclusions

This paper presents a systematic approach for a *holistic security risk analysis of biometric authentication technology* based on the *high-level component & process model for integrated security risk analysis of biometric authentication technology* also proposed here. The processes and components used within this model are developed together with a *terminology for biometric authentication technology* for the research field of *IT security biometrics*, which is comprehensively presented here for the first time. Current approaches for risk analysis of biometric authentication technology are limited to enrollment and identification/verification processes with biometric algorithms mainly considered as black-boxes, only. By using the *biometric authentication risk matrices* introduced here it is shown that more than seven thousand single *possible risk effect classes* can be identified, which should be examined for an overall holistic security risk analysis of biometric authentication technology. With the systematic discovery of such a large amount of possible risk effect classes in this paper, it can be concluded that current biometric authentication technology contains inherent holistic security risks, which are not systematically explored. For this reason, the specific risk analysis approach presented here has a *strong advantage* in comparison with other evaluation and risk analysis approaches in this area. More generally speaking, the presented approach is a significant contribution on the way to the possible development of more (holistic) secure biometric authentication technology.

References

[1] K. Bhaskar, *Computer Security - Threats and Countermeasures*, NCC Blackwell, 1993.

[2] A. Brömme, "A classification of biometric signatures," in *IEEE International Conference on Multimedia & Expo ICME 2003*, vol. 3, pp. 17–20, Baltimore, MD, USA, July 6-9, 2003.

Table 3: Full risk matrix for the $_{\diamond}\perp_{\star}$ relation between biometric process components P, Q, N, S, B, C, D (see Section 3) for (En|De)rollment and authentication with emphasized examples

$_{\diamond}\perp_{\star}$		enrollment P Q N S B C	authentication P Q N S B D	derollment P Q N S B C
enrollment	P	eP$_{\diamond}\perp_{\star}$eP...eC$_{\diamond}\perp_{\star}$eP	aP$_{\diamond}\perp_{\star}$eP...aD$_{\diamond}\perp_{\star}$eP	dC$_{attc}\perp_{safe}$eC
	Q	eP$_{\diamond}\perp_{\star}$eQ...eC$_{\diamond}\perp_{\star}$eQ	aP$_{\diamond}\perp_{\star}$eQ...aD$_{\diamond}\perp_{\star}$eQ	
	N	eP$_{\diamond}\perp_{\star}$eN...eC$_{\diamond}\perp_{\star}$eN	aP$_{\diamond}\perp_{\star}$eN...aD$_{\diamond}\perp_{\star}$eN	
	S	eP$_{\diamond}\perp_{\star}$eS...eC$_{\diamond}\perp_{\star}$eS	aP$_{\diamond}\perp_{\star}$eS...aD$_{\diamond}\perp_{\star}$eS	
	B	eP$_{\diamond}\perp_{\star}$eB...eC$_{\diamond}\perp_{\star}$eB	aP$_{\diamond}\perp_{\star}$eB...aD$_{\diamond}\perp_{\star}$eB	
	C	eP$_{\diamond}\perp_{\star}$eC...eC$_{\diamond}\perp_{\star}$eC	aP$_{\diamond}\perp_{\star}$eC...aD$_{\diamond}\perp_{\star}$eC	
authentication	P	eB$_{attc}\perp_{secu}$aD	aP$_{\diamond}\perp_{\star}$aP...aD$_{\diamond}\perp_{\star}$aP	dP$_{\diamond}\perp_{\star}$aP...dC$_{\diamond}\perp_{\star}$aP
	Q		aP$_{\diamond}\perp_{\star}$aQ...aD$_{\diamond}\perp_{\star}$aQ	dP$_{\diamond}\perp_{\star}$aQ...dC$_{\diamond}\perp_{\star}$aQ
	N		aP$_{\diamond}\perp_{\star}$aN...aD$_{\diamond}\perp_{\star}$aN	dP$_{\diamond}\perp_{\star}$aN...dC$_{\diamond}\perp_{\star}$aN
	S		aP$_{\diamond}\perp_{\star}$aS...aD$_{\diamond}\perp_{\star}$aS	dP$_{\diamond}\perp_{\star}$aS...dC$_{\diamond}\perp_{\star}$aS
	B		aP$_{\diamond}\perp_{\star}$aB...aD$_{\diamond}\perp_{\star}$aB	dP$_{\diamond}\perp_{\star}$aB...dC$_{\diamond}\perp_{\star}$aB
	D		aP$_{\diamond}\perp_{\star}$aD...aD$_{\diamond}\perp_{\star}$aD	dP$_{\diamond}\perp_{\star}$aD...dC$_{\diamond}\perp_{\star}$aD
derollment	P	eP$_{\diamond}\perp_{\star}$dP...eC$_{\diamond}\perp_{\star}$dP	aD$_{attc}\perp_{secu}$dC	dP$_{\diamond}\perp_{\star}$dP...dC$_{\diamond}\perp_{\star}$dP
	Q	eP$_{\diamond}\perp_{\star}$dQ...eC$_{\diamond}\perp_{\star}$dQ		dP$_{\diamond}\perp_{\star}$dQ...dC$_{\diamond}\perp_{\star}$dQ
	N	eP$_{\diamond}\perp_{\star}$dN...eC$_{\diamond}\perp_{\star}$dN		dP$_{\diamond}\perp_{\star}$dN...dC$_{\diamond}\perp_{\star}$dN
	S	eP$_{\diamond}\perp_{\star}$dS...eC$_{\diamond}\perp_{\star}$dS		dP$_{\diamond}\perp_{\star}$dS...dC$_{\diamond}\perp_{\star}$dS
	B	eP$_{\diamond}\perp_{\star}$dB...eC$_{\diamond}\perp_{\star}$dB		dP$_{\diamond}\perp_{\star}$dB...dC$_{\diamond}\perp_{\star}$dB
	C	eP$_{\diamond}\perp_{\star}$dC...eC$_{\diamond}\perp_{\star}$dC		dP$_{\diamond}\perp_{\star}$dC...dC$_{\diamond}\perp_{\star}$dC

[3] M. Bishop, *Computer Security - Art and Science*, Addison-Wesley, 2003.

[4] R. M. Bolle, J. H.Connell, S. Pankanti, N. K. Ratha and A. W. Senior, *Guide to Biometrics*, Springer-Verlag, New York, USA, 2004.

[5] A. Brömme, "A discussion on privacy needs and (mis)use of biometric IT-Systems," in *IFIP WG 9.6/11.7 Conference on SCITS-II*, pp. 145–156, Bratislava, Slovakia, 2001.

[6] A. Brömme and C. Busch, "Biometrics and electronic signatures," in *(BIOSIG 2003), Conference Proceedings of GI Working Group BIOSIG*, Darmstadt, Germany, 2003.

[7] A. Brömme, M. Kronberg, O. Ellenbeck, and O. Kasch, "A conceptual framework for testing biometric algorithms within operating systems' authentication," in *ACM Symposium on Applied Computing SAC 2002*, pp. 273–280, Madrid, Spain, Mar. 11-14, 2002.

[8] K. Brunnstein, *AGN Oberseminar - Discussion on Risk Analysis of Biometric Technology*, 6th Nov. 2003, AGN, Department of Informatics, University of Hamburg, 2003.

[9] K. Brunnstein, *AGN Projektseminar - Talk on Risk Management*, 9th Dec. 2003, AGN, Department of Informatics, University of Hamburg, 2003.

[10] *Bundesamt für Sicherheit in der Informationstechnik (BSI): Vergleichende Untersuchung biometrischer Identifikationssysteme - BioIS*, Bonn, Germany, 2000.

[11] K. Brunnstein, "From antiVirus to antiMalware software and beyond: another approach to the protection of customers from dysfunctional system behaviour," in *22nd National Information Systems Security Conference (NISSC) Arlington/Washington*, USA, Oct. 18-21,1999.

[12] J. G. Daugman, *Biometric Personal Identification based on Iris Analysis*, U.S. Patent 5,291,560, inventor: J.G. Daugman, assignee: IriScan Inc., filed: 15.07.1991, date of patent: 01.03.1994, 1994.

[13] R. C. Dubes, *Cluster Analysis and Related Issues, in: C. H. Chen et al. (eds.)*, Handbook of Pattern Recognition & Computer Vision, 2nd ed., World Scientific, 1999.

[14] S. Fischer-Hübner, *Privacy-Enhancing Design and Use of IT-Security Mechanisms, habilitation*, AGN, Department of Informatics, University of Hamburg, 1999.

[15] W. Froehling, *Konzept und exemplarische Implementation eines gesicherten Kanals zur Übertragung biometrischer Daten*, bachelor thesis, supervisors: K. Brunnstein, A. Brömme, AGN, Department of Informatics, University of Hamburg, 2003.

[16] *General Assembly of the United Nations: Universal Declaration of Human Rights*, http://www.un.org/Overview/rights.htm, Dec. 10th, 1948.

[17] L. Hong and A. K. Jain, *Multimodal Biometrics*, in: Jain, Bolle, and Pankanti (eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Press, 1999.

[18] A. K. Jain, *Invited Talk on Biometrics at DAGM 2003*, Magdeburg, Germany, 2003.

[19] A. K. Jain and R. C. Dubes, *Algorithms for Data Clustering*, Prentice-Hall, 1988.

[20] M. Johns, *Anwendungen von Wavelets für die biometrische Authentikation*, diploma thesis, supervisors: K. Brunnstein, H.-S. Stiehl, A. Brömme, AGN, Dep. of Inf., Univ. of Hamburg, 2002.

[21] K. P. Kossakowski, *Information Technology Incident Response Capabilities*, doctoral thesis, supervisor: K. Brunnstein, Department of Informatics, University of Hamburg, 2000.

[22] M. Kronberg, *Implementierung einer Iris-Biometrik in ein Client-Server-Authentisierungssystem*, diploma thesis, supervisors: K. Brunnstein, A. Brömme, AGN, Department of Informatics, University of Hamburg, 2002.

[23] J. C. Laprie, (ed.), *Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese*, Springer-Verlag, Wien, Austria, 1992.

[24] N. G. Leveson, *Safeware - System Safety and Computers*, Addison-Wesley, 1995.

[25] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, *FVC2002: Second Fingerprint Verification Competition*, Biometric System Lab, University of Bologna, Biometric Test Center, San Jose State University, Pattern Recog. and Image Proc. Lab., Michigan State University, 2002.

[26] A. J. Mansfield and J. L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices*, National Physics Laboratory, Middlesex, UK, 2002.

[27] N. J. McCormick, *Reliability and Risk Analysis*, Academic Press, N.Y., USA, 1981.

[28] C. Paulsen, *Risikoanalyse von biometrischen Systemen*, diploma thesis, supervisor: K. Brunnstein, AGN, Department of Informatics, University of Hamburg, 2003.

[29] C. P. Pfleeger and S. L. Pfleeger, *Security Computing*, 3rd edition, Prentice Hall, 2003.

[30] P. J. Phillips, P. Grother, R. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, *Face Recognition Vendor Test 2002*, DARPA, NIST, DoD, NAVSEA, USA, 2003.

[31] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction to evaluating biometric systems," *IEEE Computer*, vol. 33, no. 2, pp. 56–62, Feb. 2000.

[32] B. Schneier, "Attack trees," *Dr. Dobb's Journ. of Softw. Tools*, vol. 24, no. 12, 1999.

[33] R. Shirey, *Internet Security Glossary*, NWG, RFC 2828, The Internet Society, 2000.

[34] A. F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967.

[35] E. W. Weisstein, *CRC Concise Encyclopedia of Mathematics*, Chapman & Hall, 1999.

Arslan Broemme Dipl.-Inform. B.Sc. Arslan Broemme studied Computer Science with specialization in IT security and privacy at the University of Hamburg. In 1999 he started as a research assistant at the Hamburg University's IT-Security Research Group AGN and selected IT security biometrics as a promissing research field. He was responsible for the lectures in biometrics, initiated and supervised several diploma theses and published his first results at international conferences.

As a founding member Arslan Broemme started in 2001 to establish the Department for IT-Security and IT-Safety (Fachbereich Sicherheit - Schutz und Zuverlaessigkeit) at the German Computer Society (GI e.V.) and concentrated on constructing the GI Special Interest Group on Biometrics and Electronic Signatures (BIOSIG). During his time as the chairman of BIOSIG from 2002-2005 he initiated and co-organized several annual national onferences and workshops (BIOSIG 2002-2005, QSIG 2005). Additionally he is a co-founder of the German national standardization committee DIN NI-37 on biometrics.

Since 2003 Arslan Broemme works as a research assistant in the Computer Vision Group at the University of Magdeburg and gathers deeper insights into pattern recognition and image processing. In the summer semester 2003 he was able to establish a university lecture on "Biometrics - An Introduction to the Scientific Fundamentals". Further he is main supervisor of diploma and master theses and works in a biometrics project for rapid human iris feature tracking (RHIFT) dedicated to the development of fast and accurate human iris detection and tracking methods.