Social Acceptance of Biometric Technologies in Germany: A Survey

A. Krupp, C. Rathgeb and C. Busch
da/sec Biometrics and Internet Security Research Group,
University of Applied Sciences Darmstadt, Germany
{christian.rathgeb,christoph.busch}@h-da.de

Abstract: Since the past decade biometric technologies are field-proven, facilitating reliable and secure access control. Numerous successful deployments on large-scale systems, e.g. airports, confirm the feasibility of biometric recognition. However, applications of biometric systems involve privacy concerns, i.e. debates on social and ethical acceptance of biometrics reached levels never previously witnessed.

In this work a comprehensive questionnaire regarding social acceptance of biometric technologies in Germany is presented. Results are obtained from a total number of 140 respondents, allowing a representative analysis of citizens’ attitudes towards biometric technologies. Relevant questions are put into view and perceptions of German citizens regarding the rise of biometric technologies are discussed in detail and interesting conclusions are drawn.

1 Introduction

Biometric recognition [JRP04] refers to automatic authentication of humans by their physiological or behavioral characteristics or traits. Several biometric characteristics, e.g. fingerprints, iris, or face, have been discovered for robust and reliable recognition and reveal impressive performance in terms of recognition accuracy holding tremendous promise for applying biometric technologies in diverse application scenarios [JFR08]. So far, the vast majority of existing research conducted in biometrics in mainly focused on technical aspects. Without a doubt, biometric technologies are on the rise enforcing an integration of biometrics into daily life, e.g. passports or door-locks, which often leaves citizens with no choice but to accept biometrics. While majorities are convinced of the need for improved authentication controls and biometrics are claimed to provide secure long-time solutions for fundamental problems, public issues arise which citizens need to be heard on, e.g. convenience or transparency. Contemporary attitudes of citizens towards biometric recognition must be considered important, since a wide-spread use of biometrics may cause even more issues. For instance, attacks on biometric systems [RCB01], e.g. spoofing, hacking, reconstructing biometric information from templates, insider attacks, or even theft of body parts may all seem far-fetched now, but they could become common if the use of biometrics and the value of the information protected by biometrics increases [Pat08]. While research already tackles some issues, e.g. privacy-protecting technologies [RU11, JNN08], others may not be considered a technical or scientific question. In con-
contrast, issues such as social acceptance can only be taken into account by understanding the ‘people’-side of biometrics [CSR04].

The contribution of this work is the investigation of social acceptance of biometric technologies within Germany. Based on a comprehensive questionnaire, which focuses on current issues regarding deployments of biometric technologies, attitudes of 140 citizens of all over Germany are aggregated. Obtained results are interpreted and discussed in detail, whereat interesting conclusions emerge.

The remainder of this paper is organized as follows: in Section 2 related studies are briefly summarized. The proposed questionnaire, obtained results and a discussion of these are presented in Section 3. In Section 4 conclusions are given.

2 Related Studies

As previously mentioned, only a few scientific works regarding biometric recognition focus on social acceptance of users. Furnell et al. [FDMR00] proposed a questionnaire on the user-acceptance of biometric technologies which was completed by 175 respondents living in the UK. Interestingly, the survey has shown that, although demonstrably weak, typed passwords remained the most popular form of authentication in the minds of users. In [PW06] a survey is proposed in order to measure perception based on various uses of biometric technology as well as implantable RFID-chips in the human body as an enhanced biometric method. It was found that the 141 respondents in this survey were most willing to employ biometric identifiers into the United States Passport system (almost half of respondents). Conversely, respondents were least willing to employ biometric identifiers into a system to obtain a credit card with results showing nearly two-thirds of respondents unwilling. With respect to the implantable RFID-chips only less than half of respondents are unwilling to implant these. Heckle et al. [HPO07] presented a study, in which 24 participants were asked to role-play the use of a fingerprint biometric identification system when making purchases at an online bookstore. The results showed that 21 out of 24 participants found it beneficial to use the fingerprint system. Participants were also asked why they might prefer to use a biometric system when making an online purchase. The most frequent response was that the system would be easier to use than a traditional username and password (60% of responses). Only 35% of the participants said they would prefer to use a biometric system because of an increase in security. The authors found that the participants relayed a sense of confusion when it came to assessing the security strength of biometrics. Interestingly, subjects stated that they would accept biometrics if it was the social norm. Jones et al. [JAE07] investigated the users’ perceptions of biometrics with respect to various application scenarios, e.g. building access, computer access, or financial transactions. Overall, the use of biometrics did not receive more acceptability compared to conventional authentication mechanisms, e.g. password-based authentication. In contrast, regarding biometrics the majority of the 115 respondents raised concerns about misuse with respect to fraud and tracking. Similar results were obtained in [FE07], in particular, ~38% of 209 respondents were far from confident that biometric information will only be used for authentication purposes. In [EAGHR10] 70 volunteers were enrolled
in biometric systems based on keystroke dynamics and face recognition. Interestingly, the majority of respondents found that the system based on keystroke dynamics outperformed the face recognition system, i.e. they were more satisfied with the system based on keystroke dynamics, although it actually revealed higher error rates compared to the face recognition system. Furthermore, the authors identified significant correlations between education level and respondents’ opinions about secret-based solutions against fraud and their concerns about privacy issues. In [BS00] the procedure of selecting Passfaces from a grid of faces displayed on the screen is compared to conventional passwords. In this study, which was carried out with 34 student participants in a 3-month field trial, password caused substantial login failure rates compared to the Passface approach, i.e. the latter achieved improved usability. Recently, Mok and Kumar [MK12] investigated privacy related concerns in the deployment of biometrics and data protection technologies in China. In a survey in which 305 subjects participated it was found that the most acceptable biometric characteristics are fingerprint, iris, and face. In addition, it was found that Airports and Banks are the most preferred venues of deploying biometrics technologies.

3 Social Acceptance of Biometric Technologies in Germany

In order to give an insight to the social acceptance of biometric technologies in Germany, a comprehensive questionnaire was proposed. In the following subsections the questionnaire, according evaluations are described in detail, obtained results are presented and the most interesting findings are discussed.

3.1 Proposed Questionnaire

The survey which consists of 56 question was completed by a total number of 140 respondents, the distribution of respondents across different states of Germany is summarized in Table 1. As can be seen nearly all states are represented which forms an adequate basis for an representative investigation. This national distribution was achieved by publishing
3.2 Obtained Results

Within initial questions emphasis was put on the convenience of knowledge-based authentication mechanism, in particular PINs and passwords. As shown in Fig. 1 (b) the majority of respondents finds it hard to remember PINs or passwords. As a consequence, see Fig. 1 (c), people tend to forget PINs and passwords, interestingly, passwords are forgotten more often than PINs. Fig. 2 (a) illustrates the amount of PINs or passwords, physical keys,
and chip cards German citizens have to maintain on average. While most respondents posses only 4-5 physical keys, the majority of participants has to remember more than 7 passwords. Based on the fact that most respondents find it hard to remember PINs and passwords these are re-used at various application scenarios while the majority does not frequently change their PINs or passwords, as shown in Fig. 2 (b)-(c). Based on these results, knowledge-based authentication systems requiring PINs or passwords appear inconvenient.

Focusing on biometrics, which may represent a suitable solution to these issues, the most well-known biometric characteristics are fingerprints, iris, face and speaker/voice recognition, see Fig. 3 (a). In addition, the acceptability of biometric characteristics is depicted in Fig. 3 (a). Obviously, the highest acceptability is gained for fingerprint recognition which is also the most well-known technology, which coincides with the findings in [HPO07], where participants state that a more common use of technology brings about more social acceptance. In contrast, while the majority of respondents is familiar with face and speaker/voice, recognition based on these characteristics is only accepted by a few. The majority of respondents answered in the negative when they were asked whether they consider biometric recognition as too personal, intimate or even frightening, as illustrated in Fig. 3 (b).

While biometrics are deployed at a great variety of applications still only $\sim 45\%$ of respondents have already registered with at least one biometric system, see Fig. 4 (a) (in most cases fingerprint recognition systems). While only a slight majority believes that biometric systems facilitate everyday lives $\sim 75\%$ are convinced that biometric access control systems are necessary at distinct venues, as illustrated in Fig. 4 (a). The effects of aging on biometric recognition [Lan10] has been investigated in past years and numerous biometric characteristics, e.g. fingerprints [HGL+11, DAB04] and iris [FB12], were found to be highly influenced by aging. When asking participants what they consider an adequate time lapse after which a re-registration with the biometric system is required, rather short time lapses of 3 or 6 months are acceptable for only a few respondents, as shown in Fig 4 (b), again, convenience plays an important role.
(a) Have you used biometrics? Do biometrics facilitate daily life/ are they necessary?

(b) What do you consider as an adequate time lapse after which re-registration is required?

Figure 4: Amount of respondents which have already used biometric systems, the common attitude with respect to daily life, and time-lapses considered adequate for re-registration.

(a) How do you face the future development of biometric technologies?
(b) Do you consider biometrics or knowledge-based authentication more tamper-proof?
(c) Which type of authentication do you think provides more advantages?

Figure 5: Future perspectives of respondents regarding biometric technologies and the comparison between knowledge-based authentication and biometric systems.

While \( \sim 25\% \) of respondents are not concerned about the future of biometric technologies a majority of \( \sim 45\% \) face a positive future for the development of biometric systems, see Fig. 5 (a). Compared to knowledge-based authentication schemes most respondents believe that biometrics are more tamper-proof while improved security may not be considered as a major advantage as shown in Fig. 5 (b)-(c).

3.3 Discussion

Users seem to be annoyed by maintaining several PINs and passwords, i.e. biometrics, which can not be lost or forgotten, bring about substantial benefits with respect to usability. However, while citizens are familiar with most biometric characteristics, in general the acceptance of biometrics appears quite disillusioning. For instance, while \( \sim 25\% \) (!) of respondents did not accept biometric recognition at all, only one third or less of the
respondents which are familiar with face and speaker/voice recognition accept these technologies. These results may be influenced by negative recent press releases, e.g. regarding Facebook’s face recognition software.

Generally speaking, based on the obtained results deployments of biometric systems need not face refusal due to physical invasion of privacy or even fear. While less than half of the participants have experience with biometric systems these are not considered as more convenient than, for instance, knowledge-based approaches. This implies biometric systems require improvements with respect to usability (which is also related to biometric performance rates). Usability is influenced by aging effects as well, while most participants accept only long time lapses ($\geq 1$ year) between re-enrollments. Overall, attitudes towards future developments of biometric technologies are positive while at the time citizens do not discover major advantages of biometrics over knowledge-based authentication mechanisms, despite improved security.

Obtained results confirm that general awareness regarding biometric technologies requires major improvement in Germany, which may also improve the social acceptance of biometrics which appears still unsatisfying.

4 Conclusion

In this paper results obtained from a survey on the social acceptance of biometric technologies, which was completed by 140 German citizens, are presented. Results of the comprehensive questionnaire, which was completed by people of almost all states of Germany, reflect the current general attitudes towards different biometrics-related topics within Germany, providing interesting insights. Nevertheless, the evaluation of the presented survey appears rather disillusioning confirming the fact that general awareness of biometric recognition technologies needs to be improved.

Acknowledgment

This work has been partially supported by the the Center for Advanced Security Research Darmstadt (CASED), Germany.

References


