A Note on the Protection Level of Biometric Data in Electronic Passports

Harald Baier, CASED / Hochschule Darmstadt,
baier@cased.de

Tobias Straub, Duale Hochschule Baden-Württemberg Mannheim,
straub@dhbw-mannheim.de

Abstract: Following regulations of the EU Council in 2004, the member states have deployed electronic passports according to ICAO standards. Such documents contain an embedded radio frequency chip for storing personal data. The chip of a first generation German passport only duplicates the information which is already printed on the passport. In the current second version there are now also two fingerprints as additional biometric attributes apart from the digital facial image of the document owner.

The note at hand concentrates on attack vectors of biometric characteristics contained in the RF chip and discusses which threats towards fingerprints are thwarted. Our gist is to point to the low protection level of the facial image on the one hand and the high protection level of fingerprints on the other hand although both biometric characteristics are easy to gather.

1 Introduction

Following the regulation 2252/2004 of the Council of the European Union, Germany started in November 2005 to deploy the first generation of electronic passports (abbreviated ePass 1.0 in this document). Each ePass 1.0 contains a radio frequency chip (RF chip), which stores electronically the printed data in different data groups (DG). As a biometric attribute, the ePass 1.0 stores the facial image of its owner in data group 2 (DG2, see e.g. [KN07]). The choice of an RF chip and the organization of the data groups was due to international commitments as standardized by the International Civil Aviation Organization (ICAO) for machine-readable travel documents (MRTDs).[1]

In order to comply entirely with the regulation, Germany came up with a second generation of electronic passports (ePass 2.0) in November 2007. Besides the data of DG1 and DG2, the ePass 2.0 stores in data group DG3 two fingerprints of its owner (typically the two forefingers[2]). While fingerprints are currently checked in an automated fashion by inspection systems, the facial image is still controlled by a border official.

Up to now, the discussion on the security of electronic travel documents focuses on the wireless communication channel and the privacy issues [JMW05, MVV07, HHJ+06]. This

[1] see Document 9303, Part I, Volumes 1 and 2, `http://www.icao.org`

[2] see Passgesetz § 4, Abs. 4: `http://bundesrecht.juris.de/bundesrecht/pa_g_1986/`

is due to the fact that sniffing attacks and unauthorized access requests to the passport are much easier to put in practice than with a contact chip. In this note, we concentrate on alternative attack vectors to gather fingerprints with or without using the ePass 2.0. Some real-world attacks are described and assessed in Section 2. In Section 3 we come to the conclusion that facial images on the one hand and fingerprints on the other hand require the same protection level.

We aim at initiating a discussion on protection levels of different biometric characteristics. To our mind facial images and fingerprints are rather public and thus their protection level is comparable. Finally, we emphasise that we do not address the question whether biometric authentication is superior or not to other user authentication methods.

2 Attack Vectors on Fingerprints

In this section we reason about the appropriateness of the protection mechanisms for biometric data in electronic passports. Both in the public discussion accompanying the legislation process and among privacy experts it is up to now common sense that fingerprints have to be considered sensitive personal data[3]. At the same time the digital facial image of the ID card holder is deemed less critical as it can be captured easily anyway.

However, we argue that in the context of electronic passports threats towards fingerprints and towards facial images are comparable.[4] As we show below, our main argument is that fingerprints are also very easy to capture – even in the presence of sophisticated protection mechanisms like EAC (Extended Access Control, see e.g. [BSI08]), which we nevertheless consider a sound protocol to prevent unauthorized access to stored fingerprint images.

2.1 Gathering Fingerprints by Real-World Attacks

There are obvious and easy ways to obtain fingerprints which have not been discussed thoroughly in the context of passport security mechanisms. The key point is that each person carries her biometric characteristics with herself all the time. Hence it is not necessary to use a passport or other ID card as an attack vector, but the person herself will suffice. This has already been anticipated when considering the facial image as less sensitive information. We claim that this holds also true for fingerprints when taking into account practical real-world attacks. Here we distinguish two categories.

Analogue attacks without victim's active interaction: In everyday life it is virtually impossible for a human to avoid leaving fingerprints on objects that may fall into the hand of an attacker. Consider for instance doorknobs, handrails, a coffee cup, a hotel key card, or even a piece of (glossy) paper. Five years ago the German Chaos Computer Club (CCC)

[3] [KN07, p.178]: *Sensitive personenbezogene Daten wie Fingerabdrücke bedürfen eines besonders starken Schutzes [...].*

[4] Interestingly enough classical paper-based passports of some nations (e.g. from Africa) comprise fingerprints besides the facial image.

has already demonstrated how cheap it is to digitize a fingerprint and to prepare a dummy.[5] We estimate the cost to be less than 5 euros. Thus even less experienced attackers may use analogue fingerprints to surmount automated fingerprint authentication systems.

Digital attacks with victim's active interaction: There are two ways to obtain a person's fingerprint by interacting with her: Voluntarily and under pressure.

1. *Voluntarily*: Using some kind of social engineering or persuasion, an attacker may request the user to show her passport (as this is common practice in business transactions, e.g. when renting a car) and ask to provide the fingerprint as 'additional security measure to prevent misuse'. In this case the attacker only pretends to check it against the one stored in the ID card's chip (which he is not able to access). Such an attack is likely to succeed when users are not completely sure which parties are entitled to access fingerprints. We are very interested which result a lifelike study would deliver. We estimate that there would be a success ratio high enough to make this method promising for an interested attacker.

2. *Using Pressure*: A typical example is the recording of fingerprints and facial images by U.S. border control personnel in the aftermath of the 9-11 terror attacks. For a traveller to the U.S., the only alternative to providing biometric characteristics at the airport is to board the return flight. It is obvious that rogue nations will circumvent EAC by proceeding in a similar way.

2.2 Attacks on the Enrollment Process

Besides the storage medium of fingerprints (i.e. ePass 2.0) privacy concerns also seem appropriate concerning the enrollment procedure, that is the process of taking and storing fingerprints in the registry office and transmitting them to ID card producers.

In the context of biometrics it is a fundamental question where to store the reference data. In view of the ePass 2.0 a centralized nationwide database is currently not allowed.[6] While the protection provided by the chip is very high there seem to be probable attacks in order to apply for an authentic passport which contains the fingerprints of a different person:

1. A malware attack on the IT system of the registry office in order to steal or exchange fingerprints during enrollment has already been demonstrated.[7]

2. In order to call attention to potential weaknesses the CCC has published the fingerprint of the German Minister of the Interior, Wolfgang Schäuble, and asks citizens to apply for an ePass 2.0 using a dummy made out of it.[8]

[5] http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml

[6] With the deployment of electronic passports in Switzerland fingerprints will be stored in a central database (http://www.heise.de/newsticker/meldung/137989). Similar plans are discussed in the Netherlands (http://www.nrc.nl/international/Features/article2059482.ece).

[7] http://wiso.zdf.de/ZDFde/inhalt/9/0,1872,7510025,00.html,

[8] http://ccc.de/images/misc/schaeuble-attrappe.png?language=en

3 Conclusion and Future Prospects

We conclude from the real-world threats presented in Section 2 that it is easy to get fingerprints even if they are protected by EAC. We point out that this is simply a consequence of the fact that every individual carries his biometric characteristics with him all the time and that even a less-experienced attacker may harvest fingerprints without active interaction of his victim. In particular we do not consider this a weakness of biometrics or the cryptographic protocols.

We therefore assert that facial images and fingerprints require the same protection level in general. In case of electronic passports this means that either both should be protected by Basic Access Control (BAC, see e.g. [KN07]) or EAC. Because of the low threshold to get either a facial image or a fingerprint, BAC is sufficient to our mind.

To emphasize this assumption we quote the Ministry of the Interior[9] in the context of discussing the relevance of publishing the fingerprint of Wolfgang Schäuble: *So habe gerade das Bundesinnenministerium vor Einführung des E-Passes betont, dass es kaum Unterschiede zwischen einem Passfoto und dem elektronisch gespeicherten Fingerabdruck gebe.* Consequently for the prospective electronic ID cards in Germany, the same protection level for fingerprints and facial images will be implemented (using EAC and PACE [BKMN08]).

As a future work a classification of protection levels of biometric data should be developed. Since facial images are very easy and fingerprints are rather easy to gather, they belong to the class of 'public biometric characteristics'. In contrast, biometric data of iris, retina or veins belong to the 'private' class. Additionally, a study based on the *voluntarily digital attack* from Section 2.1 should be accomplished to confirm our assumption of this note.

References

[BKMN08] J. Bender, D. Kügler, M. Margraf, and I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. *Datenschutz und Datensicherheit (DuD)*, 3:173–177, 2008.

[BSI08] BSI. *Advanced Security Mechanisms for Machine Readable Travel Documents*. TR-03110. German Federal Office for Information Security, 2008.

[HHJ+06] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. *IWSEC*, pages 152–167, 2006.

[JMW05] A. Juels, D. Molnar, and D. Wagner. Security and Privacy Issues in E-Passports. *IEEE. SecureComm 2005*, pages 74–88, 2005.

[KN07] D. Kügler and I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. *Datenschutz und Datensicherheit (DuD)*, 3:176–180, 2007.

[MVV07] J. Monnerat, S. Vaudenay, and M. Vuagnoux. About Machine-Readable Travel Documents – Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication. *RFIDSEC '07*, 2007.

[9] `http://www.heise.de/newsticker/meldung/105701`