Security analysis of smartcard to card reader communications for biometric cardholder authentication

Luciano Rila and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
Surrey TW20 0EX, UK.
luciano.rila@rhul.ac.uk and c.mitchell@rhul.ac.uk

Abstract

The use of biometrics, and fingerprint recognition in particular, for cardholder authentication in smartcard systems is growing in popularity. In such a biometrics-based cardholder authentication system, sensitive data may be transferred between the smartcard and the card reader. In this paper we identify and classify possible threats to the communications link between card and card reader during cardholder authentication. We also analyse the impact of these threats. We consider five different architectures and use the threat analysis to indicate the relative security of the various possible architectures.

1 Introduction

1.1 Biometrics and smartcards

Biometrics has been widely recognised as a powerful tool for problems requiring personal identification. Most automated identity authentication systems in use today rely on either the possession of a token (magnetic card, USB token) or the knowledge of a secret (password, PIN) to establish the identity of an individual. The main problem with these traditional approaches to identity authentication is that tokens or PIN/passwords can be lost, stolen, forgotten, misplaced, guessed, or willingly given to an unauthorised person. Biometric authentication, on the other hand, is based on physiological or behavioural characteristics of the individual, such as fingerprints, and therefore does not suffer from the disadvantages of the traditional methods.

In parallel, smartcards have steadily become more popular. Their increasing storage capacity and processing capabilities have enabled their deployment in a widening range of applications, varying from support for PKI to decentralised systems requiring off-line transactions [1, 2, 3]. Generally any application using smartcards requires a method for cardholder authentication, and biometrics-based authentication has emerged as an appropriate technology.

Combining the security of biometrics and the computing power of a smartcard is a very elegant solution to cardholder authentication. On the one hand biometrics can provide the level of security required by applications using smartcards. On the other hand, smartcards enable the biometrics technology by offering a secure and portable way of storing the biometrics template, which would otherwise need to be stored in a central database. Fingerprint recognition appears particularly appropriate for use in biometric systems using smartcards.

A smartcard system is composed of two main physical units: the smartcard itself and the card reader. In biometrics-based cardholder authentication, transmission of sensitive data between the smartcard and the card reader may occur depending on how the biometric system is distributed between these two units. In this paper, we consider the security issues associated with the communications link between the smartcard and the card reader during the biometrics-based cardholder authentication process.

Before we set out the objectives of this paper in detail, it is important to clarify the biometrics-based cardholder authentication process.

1.2 General model for biometric authentication

According to [4], a general biometric system is composed of the following logical modules:

1. Data collection subsystem;
2. Signal processing subsystem;
3. Matching subsystem;
4. Storage subsystem;
5. Decision subsystem;
6. Transmission subsystem.

The data collection subsystem contains the input device or sensor that captures the biometric information from the user. It is the link between the physical domain and the logical domain. The signal processing subsystem receives the raw biometric data from the data collection subsystem and extracts the distinguishing features from the raw data, transforming it into the form required for matching. The matching subsystem receives the processed data from the signal processing subsystem and compares it with the biometric template retrieved from the storage subsystem. The matching subsystem measures the similarity of the submitted biometric sample with an enrolled reference template. Each comparison yields a score, which is a numeric value indicating how closely the submitted sample and the reference template match. The decision subsystem receives the score from the matching subsystem and, using a confidence value based on security risks and risk policy, interprets the result of the score, thus reaching an authentication decision. The transmission subsystem provides the system the ability to exchange information between all other subsystems. Figure 1 shows a block diagram for the general biometric authentication model.

Note that these are logical modules, and therefore some systems may integrate several of these components into one physical unit.

1.3 Scope and purpose

In this paper we focus on the security issues associated with the communications link between the smartcard and the card reader during fingerprint-based cardholder authentication. PIN-based cardholder authentication has been well researched and understood, giving rise to a variety of industry standards, such as [5, 6, 7]. Encryption is typically used to provide security for PINs during transmission, either from the keypad to the card (for local cardholder authentication) or from the keypad to a remote server (for remote authentication of the cardholder).

However, for the purposes of our analysis, we do not make any assumptions about encryption or other cryptographic protection of the card/card reader communications link. This is because, whereas PINs are very short, biometric samples, e.g. fingerprint images, are rather large, and the limited computational and storage capabilities of the card may severely limit the possibilities for such protection.

Given our focus on card/reader communications, and the objective of assessing the best level of integration of the biometric technology, we make certain other simplifying assumptions. We assume that the smartcard is a tamper-proof device and any transmission between biometric system modules taking place within the card is therefore secure. We do not discuss the impact of using fake biometrics, such as plastic fingers, to fool the system, although it was shown in [8] that this is a possible attack with the current technology. We feel that this issue concerns fingerprint-based biometric technology in a wider sense and is therefore beyond the scope of our discussion.

In previous related work [9], a number of weaknesses in the biometric system model have been identified, and countermeasures suggested. However, in that analysis no assumptions as to the actual architecture of the system are made, and the analysis is rather general in nature. By contrast, the main purpose of this paper is to understand what security gains can be made from the various possible levels of integration of the biometric system on the smartcard.

Depending on how the logical modules of the biometric system are distributed between the smartcard and the card reader, different threats may arise. We consider five scenarios for the biometric system and, for each scenario, we identify and classify possible threats to the communications link and assess the impact of these threats. In all scenarios we assume that the smartcard stores the template for the

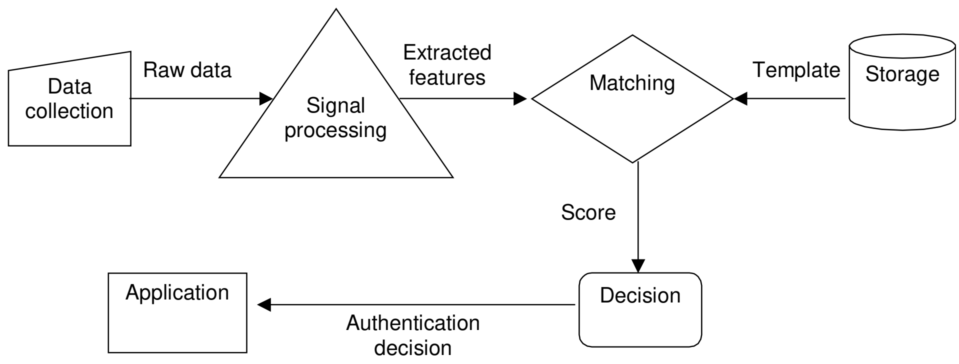

Figure 1: General model for biometric authentication.

cardholder fingerprint. We also assume throughout that fingerprint recognition is used as a method of cardholder authentication to the smartcard.

In Section 2 we describe the five biometric system architectures considered in this paper. In Section 3, we discuss the sources of communications link threats and then identify and classify the possible threats. In Section 4, we assess the impact of the threats identified in the previous section. Finally, we present our conclusions in Section 5.

2 Possible biometric system scenarios

Five different scenarios are considered, and the relative risks associated with each scenario are analysed. The scenarios cover various possibilities for the distribution of the modules of the biometric system between the smartcard and the card reader. Note that in all cases we assume that the fingerprint template is stored in the smartcard.

The scenarios are as follows:

S1. The fingerprint sensor is built into the card reader. The user template is transferred from card to reader. The reader takes the image provided by its built-in fingerprint sensor, performs the feature extraction, and also matches the features to the template provided by the card. The reader then informs the card whether or not authentication has been successful.

S2. The fingerprint sensor is built into the card. The fingerprint image and user template are transferred from card to reader. The reader performs feature extraction and matching of features to the template. The reader then informs the card whether or not authentication has been successful.

S3. The fingerprint sensor is built into the card reader. The reader takes the image provided by the built-in fingerprint sensor and performs the feature extraction. The extracted features are sent to the card, which then performs the matching process and reaches the authentication decision.

S4. The fingerprint sensor is built into the card. The fingerprint image is transferred from card to reader. The reader performs feature extraction only, and transfers the extracted features back to the card. The card then performs the matching process.

S5. All fingerprint processing takes place on the card.

Figure 2 shows the first four scenarios and their corresponding data flow during biometric cardholder authentication. Table 1 below defines all the scenarios in terms of the location of the various biometric modules.

3 Security threats

The focus of this paper is on the communications link between smartcard and card reader, and hence we only consider threats that relate, directly or indirectly, to this link. The main threats to this link can be divided into threats to the up-link (i.e. smartcard to reader) and down-link (i.e. reader to smartcard). The threats also vary depending on the scenario.

Note that, before identifying the threats to the up and down links, we briefly consider the possible source of these threats. Also, as well as identifying threats to the up-link and down-link, we briefly consider threats to the card reader itself. This is because the threats to the card reader indirectly relate to communications link protection (see below).

3.1 Sources of communications link threats

There would appear to be three main ways in which an attacker could intercept and/or manipulate data being transferred between card and card reader.

- The card reader (and/or smartcard) may emit electromagnetic signals which are data dependent, and which can be intercepted using an antenna located close to the reader. Such an approach would only enable passive (interception) rather than active (manipulation/replacement) attacks. The seriousness of this threat depends on the design of smartcard and card reader.
- A special interception device could be inserted into the read slot of the card reader, and the device would then be located between any inserted smartcard and the card reader. By this means, and without any modifications to the card reader, both passive and active attacks may be realised. The seriousness of such a threat will depend on a variety of factors including the design of the card reader and the environment in which the reader itself is located. Observe that, given that the primary threat would appear to arise from an attacker equipped with a lost, stolen or borrowed card, the seriousness of this threat will relate to whether or not use of the card reader is supervised by trusted personnel (who might detect the use of additional devices).
- The card reader could be modified. At the simplest level this could mean the insertion of a 'bug' designed to monitor and perhaps modify data communications. (See also Section 3.4 below).

We do not discuss the magnitude of these threats further here, since all three threats are very much implementation-dependent and therefore any further analysis would be highly speculative. However, it is clear that, wherever possible, card readers should be designed to minimise these threats, particularly if sensitive information is transferred between smartcard and reader without cryptographic protection.

3.2 Up-link threats

The main up-link threats are as follows:

U1. (**S1** and **S2** only). Interception (leading to loss of confidentiality) of the user fingerprint template.

U2. (**S1** and **S2** only). Manipulation (or replacement) of the user fingerprint template.

U3. (**S2** and **S4** only). Interception (leading to loss of confidentiality) of the fingerprint image.

U4. (**S2** and **S4** only). Manipulation (or replacement) of the fingerprint image.

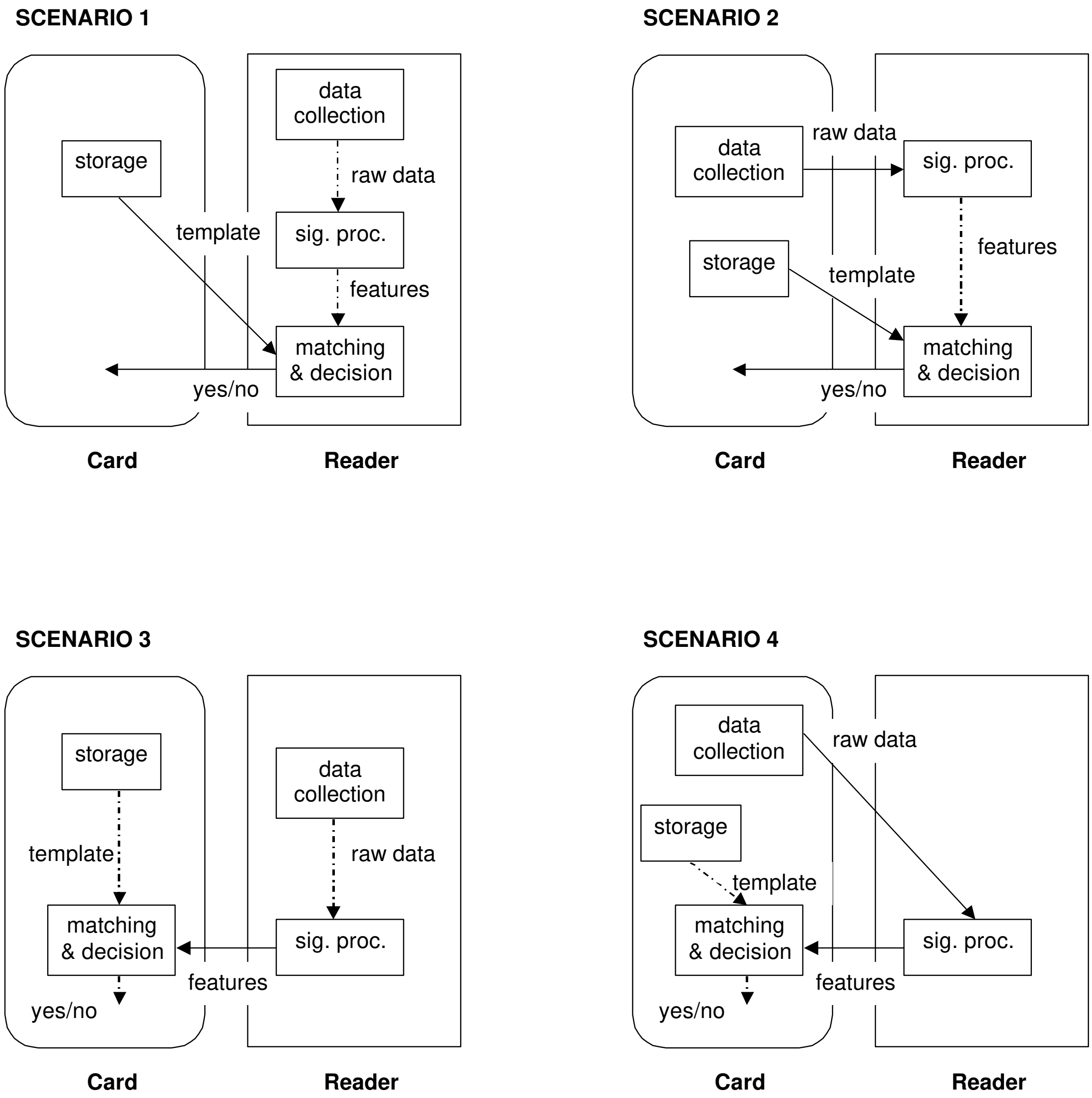

Figure 2: Four different scenarios and their corresponding data flow during cardholder authentication.

	System modules in smartcard	**System modules in card reader**
Scenario 1	Template storage	Data collection Signal processing Matching and Decision
Scenario 2	Template storage Data collection	Signal processing Matching and Decision
Scenario 3	Template storage Matching and Decision	Data collection Signal processing
Scenario 4	Template storage Data collection Matching and Decision	Signal processing
Scenario 5	All modules	No modules

Table 1: Five different biometric system scenarios in increasing order of integration of the biometric modules.

Threats **U1** and **U3** could be addressed by encrypting the communications path, although the effectiveness of such a measure would depend on the physical security of the card reader (since keys necessary to decrypt the transferred data would need to be available to the card reader). Addressing threats **U2** and **U4** would require the provision of data integrity and origin authentication services for the data transfer between card and reader (e.g. as provided by a Message Authentication Code (MAC) or a digital signature — see, for example, [2]).

3.3 Down-link threats

The main down-link threats are as follows:

D1. (**S1** and **S2** only). Modification of the authentication decision.

D2. (**S3** and **S4** only). Interception (leading to loss of confidentiality) of the fingerprint features.

D3. (**S3** and **S4** only). Manipulation (or replacement) of the fingerprint features.

Threat **D2** could be addressed by encrypting the communications path, although the effectiveness of such a measure would depend on the means used to protect the necessary key(s). Addressing threats **D1** and **D3** would require the provision of data integrity and origin authentication services for the data transfer between reader and card (e.g. as provided by a MAC or a digital signature).

3.4 Threats to card reader

Three main types of threat to the card reader can be identified. Although these threats are not directly relevant to smartcard/reader communications security, they do have indirect relevance (see below). The three main classes of threat are as follows.

- *Manipulation* of a genuine card reader. This includes the insertion of a 'bug' (as mentioned in Section 3.1), but also includes threats where the operation of the reader is modified, e.g. by changing stored software.
- *Replacement* of the card reader. This refers to the substitution of the genuine reader with a fraudulent replacement. (Whether or not this could be achieved without preventing correct operation of the system depends on both the card reader design and the design of the remainder of the system).
- *Theft* and/or *reverse engineering* of the card reader. Such a threat could be very serious if the reader contains secrets on which the system security depends.

4 Impact of security threats

We next consider the impact of the various threats identified in the previous section. We divide this discussion into the following sub-categories:

- threats arising from attempted use of a lost, stolen or borrowed card;
- threats to integrity of card transactions;
- threats to cardholder privacy.

4.1 Use of lost, stolen or borrowed cards

As a basis of this discussion we assume that the possessor of a misappropriated (lost, stolen or borrowed) card wishes to make use of this card, e.g. to perform some kind of transaction. In order to do so, he/she will need to find some way of 'fooling' the cardholder authentication process.

There are a variety of ways this could be achieved, as follows. Note that in each case we indicate which threat identified in Section 3 above is giving rise to the issue.

- Arising from **U2** (and hence applying to **S1** and **S2** only): replace the fingerprint template as sent on the up-link with a fingerprint template belonging to the possessor of the misappropriated card.

  For such an attack to be viable, the attacker will need to have a fingerprint template for his/her own fingerprint in the format used by the scheme. There are a number of possible ways in which this could be obtained.

- If the attacker has his/her own card, this could easily be obtained by monitoring the output from the attacker's own card.
- If the attacker knows the type of fingerprint reader in use (either built into the card reader (**S1**) or built into the card (**S2**)) and the method used to obtain the template, then the attacker could obtain a fingerprint reader of this type and use it, together with appropriate software, to compute a template.
- The attacker could use a misappropriated card to obtain a copy (or many copies) of a fingerprint image (from threat **U3** — i.e. **S2** only) for his/her own fingerprint. With knowledge of the method used to extract a template, together with appropriate software, the attacker could compute a template.

If **U2** is realisable, then this risk has to be classified as **high**, since, for many systems, protecting one cardholder against another fraudulent cardholder is a necessary requirement.

• Arising from **U4** (and hence applying to **S2** and **S4** only): replace the fingerprint image as sent on the up-link with a fingerprint image belonging to the legitimate cardholder.

For such an attack to be viable, the attacker will need to have a fingerprint image for the genuine cardholder. There are a number of possible ways in which this could be obtained.

- From threat **U3** (and hence applying to **S2** and **S4** only). Note that this would require threat **U3** to be realised before the time of misappropriation. This may not be easy to arrange.
- If the attacker knows how the fingerprint reader in use operates, and has access to a fingerprint image of some kind for the genuine user (e.g. by taking an image from an object touched by the genuine cardholder) then it may be possible to transform this latter image into one conforming to the scheme in use.

If **U4** and **U3** are realisable for the same card, then this risk has to be classified as **high**. Note that even if both threats are realisable, successfully taking advantage of both threats with respect to the same card may be much more difficult. If **U4** is realisable but not **U3**, then the risk is lower — say **medium** — depending on the details of the fingerprint imaging technology being used.

• Arising from **D1** (and hence applying to **S1** and **S2** only): change the authentication decision sent from reader to card from 'Reject' to 'Accept'.

This is trivially easy to perform (given that threat **D1** is realised). If **D1** is realisable, then this risk has to be classified as **very high**.

• Arising from **D3** (and hence applying to **S3** and **S4** only): replace the fingerprint features sent on the down-link with features extracted from the cardholder's fingerprint.

For such an attack to be viable, the attacker will need to have a copy of fingerprint features for a fingerprint of the genuine cardholder in the format used by the scheme. There are a number of possible ways in which this could be obtained.

- From threat **D2** (and hence applying to **S3** and **S4** only). Note that this would require threat **D2** to be realised before the time of misappropriation. This may not be easy to arrange.
- If the attacker knows how the fingerprint feature extraction method in use operates, and has access to a fingerprint image of some kind for the genuine user (e.g. by realising threat **U3** before the time of misappropriation, or by taking an image from an object touched by the genuine cardholder) then it may be possible to derive a workable set of features conforming to the scheme in use.

If **D3** and **D2** are realisable *for the same card*, then this risk has to be classified as **high**. Note that even if both threats are realisable, successfully taking advantage of both threats with respect to the same card may be much more difficult. If **D3** is realisable but not **D2**, then the risk is lower — say **medium** — depending on the details of the fingerprint imaging and feature extraction technology being used. Note also that threat **D3** could be reduced if a secret feature extraction technique is used — for this to be effective the card readers in use would need to possess physical security features (see Section 3.4). Threat **D3** could also be reduced (if not eliminated) if it was possible for the card to verify that the fingerprint features provided by the card reader indeed belong to the image provided to the card reader.

Note that none of these threats apply to scenario **S5**, which is not prone to attack on the communications path since this path is not used for the cardholder authentication process.

We summarise the results of the above analysis in Table 2.

4.2 Card transaction integrity

Whilst there may be many risks to the integrity of card transactions, we restrict our attention here to the impact of threats to the card/reader communications link.

The only impact which results from the analysis described here is an indirect one. If any of the threats relevant to the particular scenario are realisable, then this may give a cardholder the ability to dispute transactions after they have occurred. That is, if a fraudulent cardholder knows of the existence of certain threats which would allow successful use of a lost, stolen or borrowed card, then the cardholder could, after completion of a genuine transaction, claim that the transaction had been performed by someone else using a lost, stolen or borrowed card.

4.3 Cardholder privacy threats

The other main area of impact of the threats identified in Section 3 is to the privacy of the cardholder. That is, the cardholder may have concerns relating to who has access to information relating to his or her fingerprint. Note that we are concerned here purely with privacy concerns, unrelated to any possible threat of fraud.

The following impacts arise from the identified threats.

- Arising from **U1** (and hence applying to **S1** and **S2** only): loss of confidentiality of user fingerprint template.
- Arising from **U3** (and hence applying to **S2** and **S3** only): loss of confidentiality of user fingerprint image.
- Arising from **D2** (and hence applying to **S3** and **S4** only): loss of confidentiality of user fingerprint features.

The three impacts are rather similar to one another, and all have an impact on user privacy. The choice of scenario (apart from the fact that **S5** is unaffected) has little bearing on the degree of the impact.

5 Conclusions

The main purpose of the analysis in this paper is to understand how to integrate biometric cardholder authentication with a smartcard in the most cost effective manner. In particular we have sought to understand what is to be gained from the various possible levels of integration of biometric system with the smartcard.

First and foremost it is clear that scenario **S5** is unaffected by the security of the communications path since in that scenario the card/reader communications path is not used (at least for the cardholder authentication process). Thus scenario **S5** is clearly the best in an absolute sense — however it is also likely to be the most costly to deploy. It is therefore interesting to understand how the other four scenarios compare, bearing in mind that, of these four, scenario **S1** is likely to be the cheapest option and scenario **S4** the most expensive, since they represent the lowest and the highest level of integration respectively.

For the other four scenarios, the cardholder privacy threat is very similar regardless of the scenario. The main issue would appear to be fraudulent use of misappropriated cards.

Of scenarios **S1**, **S2**, **S3** and **S4**, it would appear that scenarios **S1** and **S2** are very similar with respect to their vulnerability to attacks on the card/reader communications path. The degree to which scenarios **S3** and **S4** reduce the risk depends

Scenario	Degree of risk
S1	Very high (if **D1** realisable). High (if **U2** realisable).
S2	Very high (if **D1** realisable). High (if **U2** realisable). High (if **U3** and **U4** realisable for the same card). Medium (if **U4** realisable).
S3	High (if **D2** and **D3** realisable for the same card). Medium (if **D3** realisable).
S4	High (if **U3** and **U4** realisable for the same card). High (if **D2** and **D3** realisable for the same card). Medium (if **D3** realisable).
S5	None.

Table 2: Summary of impacts of misappropriated cards.

partly on technical issues relating to the format and use of fingerprint images and features, and also depending on how easy it would be to both steal a card and monitor its use prior to its theft.

S4 represents a higher level of integration of the biometric system with the smartcard than **S3**. However the integration of the fingerprint sensor with the smartcard in **S4** makes the system vulnerable to threats **U3** and **U4** in the uplink. From that point of view, **S4** would appear to be an architecture more open to attacks than **S3**. Note, however, that when the fingerprint sensor is built into the card reader, the system becomes vulnerable to threats to the card reader (see Section 3.4). As suggested in [9], a fake card reader could be used to record the biometric data of legitimate users in an attack similar to a false ATM attack, which may potentially be an attack more easily realisable and more damaging than threats **U3** and **U4**. Moreover, given that the sensor is a fragile piece of equipment, integrating the sensor with the card reader is not a viable solution for many applications since it makes the system vulnerable to vandalism.

The gain to be derived from integrating the fingerprint sensor with the smartcard is minimal if all fingerprint feature extraction and matching are done off the card. However, depending on the environment, significant gains can be achieved as long as the matching is performed on card, even when the feature extraction is performed off-card.

It is interesting to note that almost all the most serious threats arise from an assumed lack of integrity for the data link. If it is assumed that the card reader is a trusted device and has not been interfered with or replaced (see also Section 3.4), then guaranteeing the integrity of the link between the card reader and the card would effectively prevent all the threats, even in the absence of any confidentiality for data transferred.

Finally note that, given that the threats discussed mostly relate to use of misappropriated cards, the use of secure auditing and blacklisting measures within the application can help to minimise the impact of such threats.

6 Acknowledgments

The work described in this paper has been supported by the European Commission through the IST Programme under Contract IST-2000-25168 (Finger_Card). The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The authors would like to thank their colleagues in the Finger_Card Project for their encouragement and advice.

References

[1] M. Hendry, *Smart Card Security and Applications.* Artech House, 1997.

[2] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1997.

[3] W. Rankl and W. Effing, *Smart Card Handbook.* John Wiley & Sons, 2001.

[4] ISO/DIS 21352: 2001, Biometric information management and security, ISO/IEC JTC 1/SC 27 N2949.

[5] ANSI X9.8 — 1995, Banking — Personal identification number management and security — Part 1: PIN protection and principles.

[6] ISO 9564-1: 2002, Banking — Personal identification number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems.

[7] EMV 2000, Integrated circuit card specification for payment systems, Book 2 — Security and key management. Version 4.0, 2000.

[8] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned", in *Proc. 4th IFIP WG8.8 Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000)*, Bristol (UK), 2000, J. Domingo-Ferrer, D. Chan, and A. Watson (editors), Kluwer Academic Publishers, pp. 273-288.

[9] G. Hachez, F. Koeune, and J.-J. Quisquater, "Biometrics, access control, smart cards: a not so simple combination", in *Proc. 4th IFIP WG8.8 Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000)*, Bristol (UK), 2000, J. Domingo-Ferrer, D. Chan, and A. Watson (editors), Kluwer Academic Publishers, pp. 273-288.