Potential Security Weakness with Biometric Match-on-Card

Prepared for BSI Committee IST/44 on Biometric Standards

Editorial Contact: Nigel Sedgwick, Cambridge Algorithmica Limited

15th September 2004

Referenced Documents: None.

Introduction and Overview

1   The primary purpose of this paper is to bring to attention the fact that there is a potential security weakness with match-on-card[1], that is not present with match-on-station[2] (both using template-on-card).

2   With match-on-station, with template-on-card, it is usual (and well understood) practice to secure the template against substitution or modification. This is done, as described below, using encryption or a digital signature. However, with match-on-card, this cryptographic protection could be rendered ineffective.

3   In summary, this security weakness with match-on-card is as follows. First, the attacker must have access to the card contents (eg of a lost or stolen card). Using this information, it is possible to create a forged card that can respond correctly to all cryptographic checks (eg authentication by digital signature) while allowing template substitution (or in fact any user to be accepted). A more detailed description of the security weakness is given below.

4   This particular potential security weakness does not seem to be well recognised, at least not as widely as some other security weaknesses[3]. Nor is it always given balanced consideration, when considered with various issues relating to personal privacy and misuse of private data.

5   It is, perhaps, the case that security aspects of biometric systems have not yet been subject to analysis to the same extent as systems not involving biometrics. Concerning this particular security weakness, it is the presence of a biometric template (rather than say a PIN[4]) that makes this particular weakness more useful.

6   It is, of course, the case that the security of systems involving biometrics, as with security of all IT systems, should be done on a "whole system" basis. Where such a system-wide security evaluation is done, the overall relevance

---

[1] With match-on-card, the biometric template (or reference pattern) is stored on the card, which must be a smartcard with computational capability. The biometric sample, obtained from the user to be verified, is matched against the template by the smartcard. Thus, the template never leaves the card.

[2] With match-on-station, the template is stored on the card, which need only provide memory for the storage. The template is transferred to the station (ie the biometric subsystem installed at the Point-of-Use, or PoU, such as for passport control at an airport). It is matched there against the biometric sample obtained from the user.

[3] Such as weaknesses arising from unauthorised access to templates, with template-on-card and match-on-station (considered below), and with template-on-central-system.

[4] PIN is an abbreviation for Personal Identification Number.

of this particular security weakness might be, or might not be, material. Further discussion on this is given below.

7   However, it is possible to make a reasonable comparison between match-on-card and match-on-station[5], assuming that (from a security viewpoint) all other aspects of the whole system are substantially equivalent.   That comparison is made below.

8   This particular security weakness should be noted, in the case of Machine-Readable Travel Documents (MRTDs) such as passports, visas and national identity cards.   This is because biometric verification at the Point-of-Use (PoU) is currently being considered for serious worldwide application to MRTDs.   Security weaknesses in MRTDs, that circumvent the additional protection provided by biometrics, need to be thoroughly considered in balance with all other aspects of security.

9   Misuse scenarios differ between applications and security measures, no less for MRTDs than for any other applications. For example, the current balance of benefit for credit/debit cards is against the use of biometrics, and PINs are favoured.   Likewise, the use of Chip-and-PIN (with match-on-card) is currently being introduced into the United Kingdom.   However, match-on-card for Chip-and-PIN does not introduce the same additional security weakness as it does with biometric verification (see below for further detail). Thus the conclusions of security analysis applicable to credit/debit cards (and also all other applications) and to PINs should never be taken as equally applicable to MRTDs (or to any other different applications) and to biometric verification.

10   In conclusion, all other security measures being equal, there is a difference between: match-on-card and match-on-station.

11   Namely, with match-on-card, the ability to read[6] the data (and software) on the card allows a forged card to be made, that effectively allows circumvention (by non-cryptographic means) all of the cryptographic protection intended to prevent substitution of the biometric template.

12   This particular security weakness does not apply with match-on-station[7], when templates are properly secured and linked to the genuine user's identity through the use of appropriate encryption or digital signatures.

13   The significance of this security weakness depends on the application of the card and biometric verification.   A full security evaluation is required to answer the question of significance.

14   It is quite likely that this particular security weakness is material in the application of biometric verification to MRTDs.

---

[5] It is also possible to extend the comparison to be three-way, between match-on-card, match-on-station and match-on-central server. In fact it is desirable to consider that 3-way comparison for most, if not all, systems using biometrics that have widely distributed points of use. Here, for brevity and speed of issue, only the 2-way comparison is considered.

[6] Or otherwise obtain.

[7] Match-on-station is, itself, vulnerable to different forms of attack from match-on-card.

Protection Against Template Substitution with Match-on-Station

15   Readers already familiar with IT security techniques (including public key encryption, cryptographic authentication techniques and digital signatures) could skip this section.

16   It is possible to link inextricably[8], two pieces of information stored together, such that neither can be changed without the change being obvious to an informed reader of the data.

17   In the current case, this is applicable to storage on a card or other token, of a biometric template (relating to the genuine cardholder) linked to unique identification information (such as the cardholder's name, address, date of birth, and/or Unique Reference Number, URN). The storage mechanism could be semiconductor memory, an optically readable barcode, semiconductor memory within a smartcard (ie with processing capability as well as data storage) or some other data storage mechanism.

18   There are two methods of protection commonly used. Both depend on the use of an asymmetric block encryption algorithm.

19   An asymmetric encryption algorithm[9] is one with different keys for encryption and decryption. Typically, one of these (the private key) is kept secret and known only to the originator of the data (here the card issuer). The other key (the public key) will be known to all users of the data, in particular the PoU station software. Furthermore, it is not necessary to keep secret the public key. This simplifies key distribution and reduces the need for protection of that key, both of which are usually significant operational advantages.

20   Block encryption[10] is the cryptographic technique in which all of the data to be encrypted (or digitally signed) is treated together. This is done in such a way that changing a single bit in the plaintext[11] will change, on average, half of the bits in the ciphertext[12]. This extensive change is a highly desirable effect, to avoid vulnerability to changes in the ciphertext leading to planned changes in the plaintext, which would then be accepted in its entirety as genuine.

21   The two techniques for linking together the biometric template data and unique identification data are as follows.

22   The first technique is encryption together of the biometric template and unique identification information, using the private key.

23   An attacker that does not know the public key will not be able to decrypt the data.

---

[8] That is to the full extent of the protection used. In the case of cryptographic protection, that could be arbitrarily great.

[9] The alternative to an asymmetric encryption algorithm is a symmetric one, in which the encryption and decryption keys are one and the same. Thus, cryptographic protection is only provided by the single key being kept secret. In this case, theft and reverse engineering of a PoU station could make available the single key, which would compromise the security of the whole system.

[10] The main alternative to block encryption is stream encryption, in which the number of bits changed in the ciphertext is small (sometimes only one bit), for each bit changed in the plaintext.

[11] Plaintext is the unencrypted data.

[12] Ciphertext is the encrypted data.

24   An attacker that does know the public key would be able to decrypt the data, so making available attacks based on knowledge of the data (as discussed below in the section on the possible security benefit from match-on-card).

25   However, neither of these attackers would be able to change the encrypted data, or replace it on a forged card, for example to substitute the biometric template of an impostor. This is because neither sort of attacker knows the private (encryption) key.

26   As the template and identification data are encrypted together, it is not possible to substitute a validly encrypted template from the impostor's own card. This is because that template is inextricably linked with the unique identification of the impostor himself, and cannot be separated from it. Neither can the unique identification information of the genuine cardholder be substituted for that of the impostor, on the impostor's own card (or any copy).

27   The second technique is that of digital signatures. Here, the original data (template and unique identification) are not encrypted. However, they are combined together and with a digital signature. The signature is rather like a sophisticated checksum on the combined data, that also requires knowledge of one of the cryptographic keys. Changing a single bit (or any number of bits) in any of the original data would cause the digital signature to change totally (ie around half of bits of the digital signature would flip). The station, and anyone else knowing the public key, can check that the digital signature is the one that goes with the original data on the same card. Thus, the original data can be read by anyone, the consistency of the digital signature with the signed data on the card can be checked, but no attacker can calculate the digital signature for substituted or changed data (as he has no access to the private key).

Description of the Security Weakness with Match-on-Card

28   The security weakness with biometric match-on-card is as follows.

29   **Step 1**. First, it must be possible to discover the full contents of a genuine card. This would most likely be by reverse engineering of a lost or stolen card.   However, it could be by legitimate interrogation of a carelessly designed card, or by intercept of unprotected contactless communications (eg with RF[13] or IR[14] communications). It could also be by suborning a staff member of the card issuing authority.

30   **Step 2**. Then a forged card is made, with a mixture of copied material and additional material. The additional material could be both data and computer software.

31   **Step 3**. The forged card is used, by someone other than the genuine cardholder. The modified computer software on the card uses the copied data (and perhaps copied authentication software) to give the correct response to all cryptographic authentication checks.

32   **Step 4**. On presentation of a biometric sample for verification, the additional material (software and data) is used to report the decision of the biometric pattern matching. In its simplest form, the card responds OK on the match of any biometric sample to (the unused or missing) template on the card. A

---

[13] Radio Frequency.

[14] Infrared (optical).

more sophisticated approach is to put on the card a template for the impostor, so matches against anyone or corrupt or test biometric samples would not raise suspicions.

33   The result of these 4 steps is that the forged smartcard authenticates itself using a perfect copy of all the authentication data and software. It then "lies" concerning the result of the biometric pattern matching.

34   One way of viewing this weakness is that the ability of the card to process data has allowed separation of the two key functions of the card: (a) to ensure that the card is genuine; and (b) to binding the card to the person presenting it.

35   The result of this weakness is that knowledge of the data and software on the card allows creation of a forged card that circumvents of all of the cryptographic protection intended to prevent substitution of the biometric template.

Possible Security Benefit from Match-on-Card

36   Now, there are some security weaknesses with match-on-station[15]. These provide, presumably, some of the justification for match-on-card.

37   However, these weaknesses with match-on-station have different levels of significance, depending on other aspects of the whole system. Some consideration is given here on those weaknesses, to assist in such wider security evaluation.

38   The primary difference is that, with match-on-station, the biometric template is intended to be transferred from the card to the station. In the case of match-on-card, the intention is to avoid template transfer off the card.

39   Therefore, the security weaknesses potentially stopped by match-on-card are those weaknesses arising from exposure of the biometric template to the station.

40   The primary issue here arises from the attack of tampering with the station or making a modified station (eg using knowledge of standards on card interfaces and contents), to expose the genuine template.

41   However, it should be noted that other tampering attacks on the station are not protected by match-on-card. In particular, the station could be modified to ignore the result of the biometric verification (whether that verification was done by the card or the station).

42   As an example, consider the case of merchant fraud with credit/debit cards. The merchant (or his staff) could collude with impostors by tampering with their station(s) to accept transactions using lost/stolen cards, irrespective of biometric check. However, in the eventuality (quite likely) of discovery of the fraud, there would be an audit trail identifying the particular compromised station(s), the merchant, and (presumably) his staff who might have been involved without his knowledge.

43   Another example is tampering with the station to allow injection (electronically) of a copy of the genuine user's template (obtained from the card by data transfer using the legitimate protocol) in place of the biometric

---

[15] Here the discussion is limited to match-on-station with template-on-card. Options including template-on-central-system are not considered.

sample that should have been obtained from the actual user (an impostor in this case). However, again and following repudiation of the transaction, the audit trail would lead to suspected culprits.

44   An attack that does not include tampering with a particular operational station, but exploits access to the template on the card is as follows.

45   A lost/stolen card is obtained and the template is read from it. This could be done using a legitimate station that had been stolen and tampered with, or using knowledge of card interface protocols. It would also require obtaining a copy of the public key (in the event of the template and unique identification data being encrypted).

46   Then the attacker selects a colleague who has the best match to the template. Given use of a biometric of modest technical performance (eg operating point set to a false match rate of 1% or worse) this attack is not beyond the bounds of possibility, eg to use pre-block a lost or stolen credit/debit card.

47   There is a similar attack, appropriate to infiltration by an impostor (eg a terrorist wishing to travel anonymously by using a stolen passport). Here a sufficiency of passports are stolen, from targeted individuals of some physical similarity (or even with knowledge of their biometric, eg fingerprints from a wineglass), such that the biometric of one might match sufficiently well to support the infiltration[16].

48   Thus it can be seen that, though difficult to exploit, there are security weaknesses that are made possible, or of improved viability, by match-on-station.

49   Match-on-card does provide protection against those attacks, though introducing the particular weakness that is the topic of this paper.

50   In addition, match-on-central-system also provides protection against those weaknesses, though adding its own particular security weaknesses (which are, arguably, mostly lesser weaknesses). However, match-on-central-system does require, in particular, a reliable wide area communications system.

51   Concerning the security weakness introduced by access to the biometric template of the target user, there are two other aspects that should be considered.

52   Firstly, access to example biometric samples of the target genuine user can be of similar technical use to an attacker as access to the biometric template. Thus, knowledge of and/or access to the genuine user may create a vulnerability (eg fingerprint on wineglass[17], facial photograph[18]). The relative risk of attacks depends on the circumstances (eg stolen, or lost and found, card versus specifically targeting against a known genuine user by, for

---

[16] It is obviously the case that such an attack requires extensive planning and support. However, it is not beyond the bounds of possibility. It might also be the case that the legitimate passport holders may be subject to action to extend the pre-block period (in the event of on-line passport checks or stolen/lost passport watchlists being used). Such action could include kidnap, detention and even murder.

[17] Or even fingerprint on the card or token itself.

[18] Face is, of course, also one of those biometrics that is more easily vulnerable to effort attack, ie by disguise for imitation purposes.

example, tampering with a PoU station) and motivation of the attacker; it also depends on technical details of the implementation[19].

53   Secondly, where a station is used to obtain the biometric sample for verification (as is usually the case), tampering with the station can provide access to the required biometric sample of the genuine user (even in the cases of match-on-card and match-on-central-system). That user can then be targeted for card theft.

54   In this second case, with match-on-card, the attack against the user's biometric sample is not available if the biometric sensor is part of the smartcard. However, this is only likely to be practical and beneficial in the case of fingerprint.

55   Thus, it can be seen that the security weakness of template exposure (or biometric sample exposure), is often not solely due to match-on-station. Therefore, the primary benefit of match-on-card over match-on-station can sometimes be little more than a figment of the imagination.

56   Finally, there is the issue of "template protection", in terms of personal privacy; though less commonly cited, there is also the issue of protection of biometric samples. There is a well accepted body of law and practice relating to the use and protection of personal data[20]. The same law and practice should be applied to biometric samples, templates and other information derived from them. In this paper, the particular issue is protection of templates against misuse (ie use not intended by those operating the biometric system). The known risks are those of access to the template or substitution of the template, both of which allow actions detrimental to the interests of genuine users and of operators of biometric systems. Template protection is applicable to the three main architectures, of match-on-station, match-on-card and match-on-central-system, and to template-on-card and template-on-central-system. Compromise of a template on one biometric system could also have implications for other biometric systems using the same biometric modality. However, care should be taken against giving disproportionate credence to arguments, regrettably heard from some civil liberties and privacy lobbyists, that go beyond those supported by careful analysis. Only with detailed and proper system-wide security analysis can these potential attacks be placed in balanced opposition to each other, and with identity verification approaches that do not use biometrics at all.

---

[19] Access to a biometric sample may be more useful than access to a template, in making of an artefact to represent the genuine biometric sample (eg gelatine artificial fingerprint or coloured contact lens of iris image), or for copying or imitating (eg facial disguise). This is especially the case where templates are a processed versions of images or other representation of biometric samples, as is sometimes the case. Then, although theoretically possible, it is much more difficult to create a substitute biometric sample from the template. Only where the template includes additional information, above being a copy of a biometric sample, is this a lesser vulnerability. Such additional information includes characterisation of user-specific variability in genuine biometric samples.

[20] Use should be limited to purposes declared in advance to the owner/provider of the data. Retention should be limited to just the timescale necessary for the declared purpose(s). Private data should not be passed to others without prior permission (explicit or implicit) of the owner/provider of the data; those others should be limited by the same or equivalent data privacy regulations. Private data should be adequately protected from misuse by those who fail to comply with the regulations.

General Issues of Security Evaluation

57   As a general point, it is certainly the case that any security system must be evaluated as a whole, against all types of attack[21].

58   In the case of the weakness of match-on-card, this must be placed in perspective, with respect to all other security vulnerabilities and potential attacks. In particular, this covers the following.

59   Reading smartcard contents is intrinsically very difficult (even where card security is not a specific design feature). It is, arguably but not certainly, too difficult for anyone at this time to form a practical cost-effective attack[22].

60   Furthermore, on smartcard reading, many manufacturers have added protections to make currently known attacks more difficult to perpetrate.

61   In any particular system, with or without biometrics, there are quite likely to be other security weaknesses that are currently easier to exploit.

62   Usually, any security system is as weak as its weakest link. Improving security of some links will not necessarily improve overall system security (that is unless the improved link was the weakest link). Therefore investment in security improvements should be directed at the weakest link, or the several weaker links, in the whole system.

63   However and obviously, in designing a new security system, it would be better not to include design features that introduce security weaknesses without sufficient (analysed and acknowledged) compensating benefits, such as reduced overall cost and increased convenience.

64   Whether a security system is subjected to a particular attack will depend on the ease of that particular attack and the benefit arising from successful attack.

65   Removal of a particular security weakness in one link, can in some circumstances, create a weakness to another sort of attack.

66   An example of this is the case under consideration. Using match-on-station rather than match-on-card may increase the potential benefit arising from attacks on the station, even though it reduces the potential benefit from attacks on the card (ie reading and forging).

Match-on-Card Weakness Not Material to Chip-and-PIN Cards

67   Now, in theory of course the same weakness in match-on-card as identified above is capable of being exploited against the new APACS[23] Chip-and-PIN credit/debit cards.

---

[21] In practice, it is only possible to evaluate a system against particular and known types of attack (or perhaps particular classes of attack or those against identified vulnerable points). Security evaluation should include specific combination attacks too, though that markedly increases the required effort for analysis. Thus, security evaluation calls, to an extent, for the evaluators to be as knowledgeable and innovative as all the attackers put together.

[22] Except against an unusually valuable target that, most likely, would be protected by multiple security measures.

[23] APACS is the abbreviation for the Association for Payment Clearing Services. This is the UK organisation that defines standards and operates procedures for funds transfer between banks, including standards for credit/debit cards.

68   However in the worst case, if the card contents can be read (eg by be reverse engineering), the 4-digit PIN can be found by exhaustive search of all possible PINs encrypted through the key present on the card. Thus the card only needs to be copied (or the original used if not destroyed in the reverse engineering process) and used with the true PIN so found. It is not necessary to add additional software to a forged card, in the same way as for a biometric.

69   It is also worth noting that the benefit to the attacker of compromising a single credit/debit card is (in the grand scale of things) less than the benefit to a terrorist impostor of acceptance of his forged MRTD.

70   Thus, for a credit/debit card, the cost of reverse engineering a single card may well exceed the likely financial benefit from using it in fraudulent transactions.

71   However, for MRTDs, though the cost of reverse engineering may well be very high, it would probably be going too far to assume it would be greater than the potential benefit (now or in the future). Also, suborning and employee of the passport issuing authority might be both cheaper and quicker, but equally effective.

Aspects of Cost/Benefit of Match-on-Card

72   The above analysis has been directed almost entirely at the issue of security. In addition, each and every security feature will have an impact on the cost of the system. This will be in terms of equipment procurement cost, system implementation cost and operational costs. Costs of compliance with national laws and international standards, interfaces and regulations will also be pertinent issues.

73   However, in the narrow comparison of match-on-card with match-on-station, again looking for a comparison in which all other aspects are assumed equal, the following points are somewhat against match-on-card.

74   Template on card allows the use of smaller, lower cost cards with less functionality. Match on card requires larger more expensive cards with more extensive functionality (particularly processing capability, at all or to deliver a response within a short time).

75   Match on card puts a limitation on the size of the software code that can be used for the pattern matching. Whilst it is possible to get good results with small code, in general more extensive code would deliver better pattern-matching performance.

76   Should multi-modal biometric combination be found desirable, the costs of doing this with match-on-card would be greater than for match-on-station, again through the need for greater processing power to satisfy response time requirements, and also to have sufficient memory for algorithmic software for all the biometric modalities to be used.