Security of electronic transactions – theory and practice

Jan Krhovják, Marek Kumpošt, Vašek Matyáš

{xkrhovj, xkumpost, matyas}@fi.muni.cz

Faculty of Informatics
Masaryk University
Brno, Czech Republic

Abstract

In this paper we discuss selected security aspects of electronic transactions. Firstly, we focus mainly on the operational security and our experiment undertaken in Brno in 2005–2006. Secondly, we review basic features and security impacts of the EMV (Europay, MasterCard and Visa) standard and of the upcoming Chip&PIN technology.

Keywords: Authentication, electronic transaction, Chip&PIN, EMV, smart card.

1 Introduction

This paper deals with issues related to the security of electronic transactions. We first present results from our experiment with authorisation of online electronic transactions. We start this part with a review of some critical issues regarding the introduction of Chip&PIN (Personal Identification Number) technology into practice and the main focus is our two-phase experiment which took place in 2005–2006. The goal of our experiment was to find out whether the introduction of this new authorisation method discourages an opportunistic thief and whether customers benefit from this technology with respect to this opportunistic thief. The first phase of the experiment was done in our faculty's bookstore and our customers were mainly students. The second phase was carried out in a large supermarket. Each phase was further split into two rounds – first one with the Chip&PIN technology, where customers authorised their payments with PINs, and second round where customers authorised their payments with handwritten signatures. Results from the second phase brought even more interesting findings. Results of our experiment have also been published in Czech in [1].

In the second part of our paper we focus mainly on new technologies introduced in recent years and specified in the EMV (Europay, MasterCard and Visa) standard. Both offline and online transaction processing will be described and their security aspects will be discussed in detail together with mechanisms as offline data authentication, user authentication, or automatic risk analysis. EMV approach exploits smart cards required instead of magnetic stripe cards. Moreover, user authentication which is required for authorisation of electronic transactions can be based on verification of PIN instead of handwritten signature. These two "improvements" are sometimes referred as Chip&PIN technology and will be discussed similarly as other real-world implementation specific problems and security impacts of EMV, parts of this discussion have also been published in Czech in [2].

2 Experiment

The goals of our experiment were to find out:

1) How difficult is it to observe someone's PIN while it is entered at a till?

2) How easy is it to forge someone's handwritten signature?

The whole experiment was split into to phases where the first one took place in 2005 at our bookstore at the Faculty of Informatics, Masaryk University, Brno. The second phase was undertaken in a more realistic environment in a Brno supermarket in 2006. Each part of the experiment was further split into two parts regarding our goals 1) and 2). In this report we provide the most interesting findings from both parts of our experiment.

Figure 1: Our faculty bookstore.

2.1 First phase of the experiment

This phase involved thirty two undergraduates, seven Ph.D. students (some of them were observing students while entering PINs, the others were pretending ordinary customers) and three coordinators of the experiment (sending students into the bookstore, measuring time of executed operations and recording tips of PIN observations from the observers).

Let us describe the first part of this phase of the experiment – PIN observation. We had two different PINpads for this part – one with a massive privacy shielding and the other without any privacy protection. All students were split into two sets (seventeen used the former PINpad and fifteen used the latter one). Results provided later are split accordingly to show the difference between these two PINpads so that we can see the impact of a massive shielding on the successfulness of PIN observations.

Each student was provided with a faked chip card and PINpads were not anyhow connected (this was then found as a subtle problem since we were not able to check whether the entered PIN was entered correctly or not). Once a student entered a bookstore he selected one book to buy and then proceed with a simulated card payment. At this point it is necessary to mention that all students were not informed about the real purpose of the experiment. This deception was done to ensure a realistic behaviour of the students. The real goal of the experiment was revealed individually as the student left the bookstore and proceed to the second room to get prepared for the second part.

First we provide results from the first part for the *privacy-shielded* PINpad:

- observers successfully observed 6 out of 17 PINs (35.5 %);
- 3 PINs were observed by two observers independently;
- 2 PINs were observed by only one observer;
- 1 PIN was reconstructed based on partial observations from more than one observer;
- in five cases the PIN was observed exactly (i.e., only one attempt is enough to enter the correct PIN), the last one would be successfully guessed within the three allowed attempts;

- from the total number of digits reported from 39 four-digit PIN observations (i.e., 156 digits), 75 digits were successfully observed (48 %).

Now, we provide results from the first part for the *non-shielded* PINpad:

- observers were able to successfully observe 12 out of 15 PINs (80 %);
- in only two cases more than one attempt would be needed to guess the correct PIN (max. 3 attempts), the other PINs were observed without any uncertainty;
- 2 PINs were observed by four observers independently;
- 1 PIN was observed by three observers;
- 4 PINs were observed by two observers;
- 3 PINs were observed by one observer;
- 2 PINs were reconstructed using a shared knowledge;
- from the total number of digits reported from 45 four-digit PIN observations (i.e., 184 digits), 129 digits were successfully observed (70.1 %).

In the second part of the first phase, fifteen students were provided with a card to be signed with their own signature and seventeen students were given a signed card. The latter group has 20–30 minutes to practise the given signature and than proceed with a shopping trying to get successfully authorised. There was a real merchant in our bookstore (just for the purpose of our experiment) that was carrying out the authorisations. He did not know that some people will try to cheat with someone else's signature. At this point (regarding the results that will be provided) it is important to mention that this shopping assistant works in jewellery where higher prices are paid and therefore the procedure of signature checking was very thorough. We consider this fact as a main reason for a great difference among results from the bookstore and the real supermarket.

Results from the second part of the first phase:

- merchant discovered 12 out of 17 faked signatures – only five were accepted as correct (i.e., 29.4 % success rate for cheating customers);
- out of 12 identified signatures, 8 were refused after the first signature and 4 after they were asked to sigh again;
- 20 signatures were successfully accepted (out of which 15 were genuine signatures and 5 cheater) – 16 were accepted right after they signed, 4 were accepted after their second attempt;
- one cheating student gave up once he was asked to sign again.

From the first phase of the experiment we concluded that under the conditions we had, authorisation with a signature is (from the point of a customer) more secure than authorisation with a PIN. Other finding was that really massive privacy shielding is a way to protect PINs since the success rate of observations was significantly lower.

2.2 Second phase of the experiment

Second phase of our experiment took place in one big supermarket in Brno to achieve realistic conditions for both our customers and observers. We needed to convince appropriate number of "customers" for our first part and so we asked our relatives and some students whether they would be willing to take part. In order to get as realistic conditions and results as possible it was vital for our experiment to hide its real purpose. Only few people from the supermarket management and from the Faculty of Informatics knew about the experiment. Neither the till assistants nor the ground security staff were informed about the experiment – the supermarket's management wanted to test their own security procedures.

The last thing was the legal protection of our "customers". The responsibility for the abuse of the cards was turned to the real holders of cards.

Overall there were about 50 people involved in the second phase of the experiment – 20 "customers", 15 observers and other people who were informing customers what they should buy, which till they must use, how they will pay and what they should do if the transaction is not successfully authorised. We did not influence the other customers in the supermarket.

Upon arrival each "customer" was informed about the purpose of the experiment (not the real one), i.e., security procedures of the supermarket are being tested and we would like to find out the friendliness of card transactions. "Customers" were also given a simple questionnaire to support our cover story. "Customer" then obtained a card (and a respective PIN), cash money for the case that the authorisation will not succeed, instruction what to buy and a number of till to use. The set of tills that we were allowed to use was agreed prior to the experiment start. When the "customer" entered the supermarket a team of observers got activated. "Customer" was tracked at the supermarket and observers tried to observe a PIN that he or she entered at the till desk. We had three teams of observers operating independently and one at the time. This was also due to the fact that we had 20 "customers" but only five different PINs. So we wanted to minimise the situation when one observer observes the same PIN several times. Each observer recorded his tip and reported to one of the coordinators afterwards.

After the first part was over we conducted the second part where the payments were authorised with a signature. "Customers" in this part were mainly observers from the first part and some students that wanted to participate. Each "customer" got a signed card and was allowed to practise this signature for about 20 minutes. Then he or she got some cash for the case that the authorisation will not succeed and went shopping. After the shopping they reported whether their signature was accepted or not.

Results from the first part of the experiment – **authorisation with PIN**:

- 13 customers did the payment at a till equipped with a privacy-shielded PINpad and 7 used non-shielded PINpad;
- 4 PINs out of 20 were observed successfully (i.e., three attempts would be enough to guess the correct PIN) – 20 %;
- reconstruction was based on tips from all observes within one team (i.e., some of them were sure about the beginning of the PIN, some of them about the end…);
- 3 out of 4 observed PINs were entered on a privacy-shielded PINpad;
- next 3 PINs would be guessed with 10 attempts; next 3 PINs with 222 attempts;
- overall from 26 tips of 4-digit PIN (91 numbers reported) 38 digits were observed successfully (42 %).

It is also interesting to see the success rate for each team:

- first team observed 25 % digits correctly (6 out of 24);
- second team observed 27 % digits correctly (9 out of 39);
- third team observed 68 % (!) digits correctly (23 out of 34).

It is not surprising that it is the third team who observed those four PINs. One member of this team was very "active" and was able to observe "customers" from good positions without any suspicion.

For every team of observers one member was replenishing goods nearby tills (these observers were provided with some goods before the experiment started). They were also labelled with respective cards so they were not suspicious for the ground security staff. Our expectations were that these observers will have a nice view on the tills and will provide useful tips of PIN numbers. But once the experiment finished and we collected all observations these tips were not as good as we have expected. Results received from these observers were not considered in the overall results evaluation because it did not bring any improvement and sometimes had even a bad influence on the other tips.

Results from the second part of the experiment – **authorisation with signatures**:

- every "customer" had 20 minutes for practising signature and then performed a shopping;
- this part was stopped after 17 successful attempts (out of 17);
- no "customer" experienced any problem or was asked to sign twice;
- some "customers" reported that their signature was verified very poorly or not at all.

2.3 Summary of both phases of the experiment

A really massive privacy-shielded PINpad can help to protect entered PIN with respect to a possible observer. But at this time such a massive privacy-shielding is not very widely deployed and many PINpads do not offer even a little shielding.

If we compare both phases of the experiment the overall success rate of observations is 60 % vs. 42 %. As such this is not a big difference but we have to keep in mind that there is a great difference between the amounts of successfully observed full PINs. In the first phase observers managed to observe (or reconstruct) 18 out of 32 PINs (56.25 %) in the second phase it was only 4 PINs out of 20 (20 %).

A significant difference can also be seen in the second part – authorisation with a signature. In the second phase, there was not even one detected cheating customer. If we compare this result with the 70 % detection rate from the first phase, the difference is staggering. One possible explanation could be that in the first phase the merchant that was cooperating with us was from a jewellery shop where it is normal to pay higher amounts than in a supermarket. Our second but unfortunately not confirmed speculation was that there is possibly a threshold from which the signature verification is done more precisely (like 1000 CZK or more). To sum up we have experimentally proved that if you lose your card then even not very skilled person can learn your signature in about 20 minutes and has a very significant chance to stay undetected in an ordinary supermarket.

Observers involved in our experiments were not trained "professionals". These were mainly Ph.D. students and they had two hours at maximum to train how to observe with a model of PINpad.

From the results above it is obvious that signature verification, which is currently the most common payment authorisation method in shops is not very secure and a card can be easily abused in a case of loss. Regarding the PIN-based authorisation the situation is slightly better (from the customer's point of view). To forge a signature an attacker needs only a card, to forge a PIN an attacker needs both the card and the PIN. So the situation gets a bit more difficult, but not too significantly.

3 EMV Specification

The EMV specification (precisely its version 4.1 [3]) is described in four separate documents. The first of them specifies application independent requirements for integrated chip cards and payment terminals including electromechanical characteristics (e.g., chip size, voltage levels), transmission protocols (e.g., character-oriented T=0 and block-oriented T=1), application selection process, and structure of files and commands. The second document specifies security requirements as offline data authentication, PIN encryption, and cryptographic key management. The third document focuses on application requirements and contains exact definition of particular APDU (application protocol data unit) commands. Finally, the fourth document specifies mandatory, recommended and optional terminal requirements that are necessary to maintain compatibility with chip cards. EMV 4.1 is sometimes also referred as EMV2004.

We focus mainly on the security of electronic transactions and on mechanisms that would prevent frauds performed by customers, merchants, or even banks. From our point of view the customer is also a cardholder and in the next parts will be often denoted as a user. The bank will be a card issuer which also maintains a user's account. Communication between banks will be omitted and we will expect that transactions from online terminals will always be automatically delivered to the correct bank. All activities that lead to financial losses on the site of customers, merchants, or banks will be considered as a fraud – typical example is a transaction performed by forged or stolen payment card. EMV chip cards (in the following text often denoted only as cards) should mitigate this kind of risks, but as we saw in the previous part of this paper, other new security risks are arising with this new technology.

3.1 Offline data authentication

The first security mechanism is offline data authentication – capable to detect false (i.e., after personalization altered or duplicated) cards inserted into payment terminal (e.g., ATM or POS terminal) without any online communication with a bank. This authentication mechanism utilizes asymmetric cryptography (namely the RSA cryptosystem) and trusted certification authority that signs public keys of payment card issuers (i.e., particular banks). Each EMV compatible terminal must therefore contain a public key of this certification authority. We distinguish among two basic authentication mechanisms: static data authentication (SDA) and dynamic data authentication (DDA). In principle, both these mechanisms are fairly similar to passive and active authentication for electronic passports.

Static data authentication (see figure 2) is a mechanism capable to check the validity of static application data stored inside the chip card. These data are always signed by the issuer and stored together with his certified public key. The first operation (performed after the card is inserted into terminal) is sending static data together with certified public key to the terminal. Then the terminal uses embedded public key of the certification authority to check the validity of issuer's public key and finally, using the valid issuer's public key, checks the validity of static application data. Security of this mechanism is based on the secrecy of private RSA signature keys – their compromise could lead to false cards creation with fake static application data.

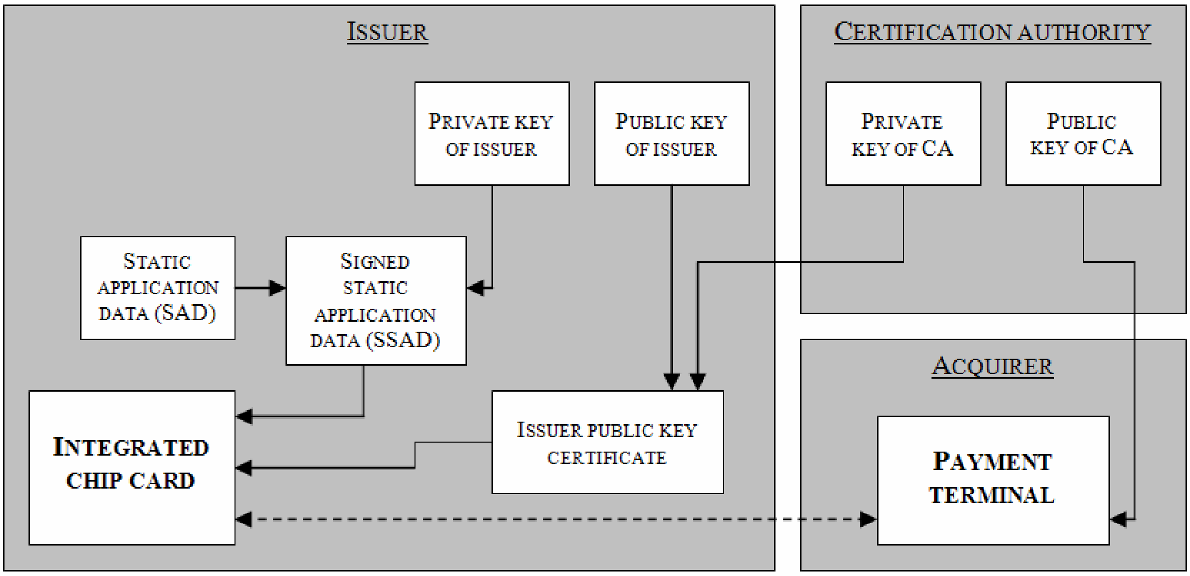

Figure 2: Static data authentication.

However, signed data sent for verification to the terminal can be misused to create a chip card copy. A big disadvantage of the SDA is an impossibility to detect such duplicated cards. This problem is solved using a more sophisticated dynamic data authentication (see figure 3) that allows to check the validity of static application data and also genuineness of the card itself. For this purpose on each card a new unique RSA key pair is stored. Private key is securely stored inside the chip and never leaves it (i.e., there is no possibility to read the key). Public key, together with static application data (i.e., as one data block), is signed by the issuer's private key. Certified issuer's public key is also stored on the card. The first operation (performed after the card is inserted into a terminal) is sending static data together with certified public keys to the terminal. Terminal uses embedded certification authority public key to check the validity of issuer's public key and finally, using the valid issuer's public key, checks the validity of static application data and card's public key.

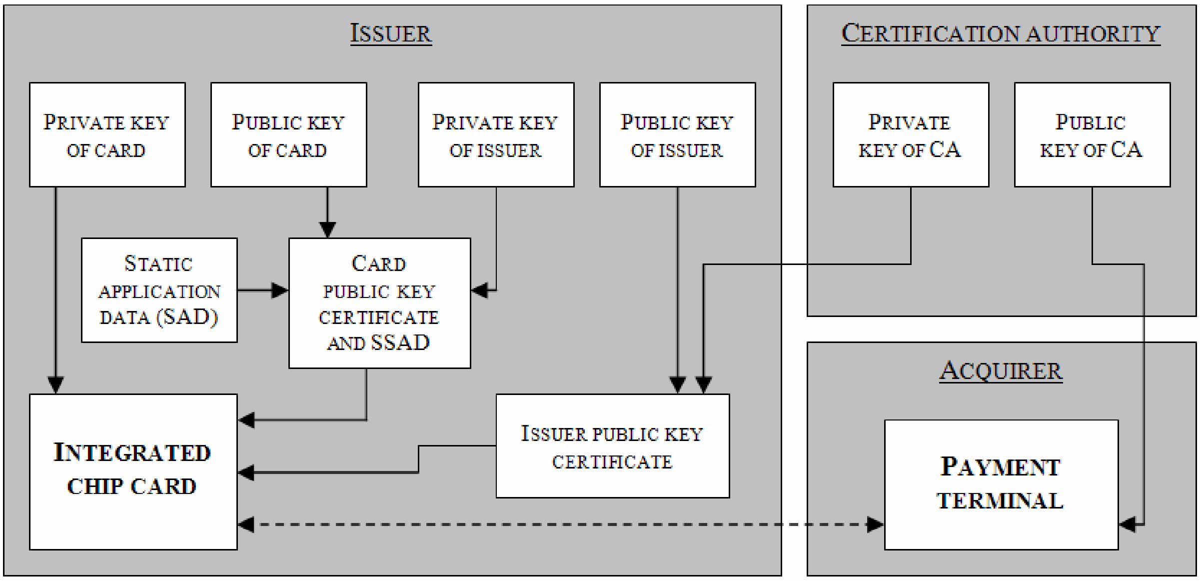

Figure 3: Dynamic data authentication.

DDA utilizes random data generated and sent by the terminal. These data are signed with a private key of the card and sent back for verification by the terminal. Security of this mechanism is based also on secrecy of private RSA signature keys, but the difficulty/impossibility of obtaining private key of the card (to prevent duplication attacks) must also be assured. Fast signing of terminal random challenges implies the need for a coprocessor for accelerating asymmetric cryptography (especially RSA). The consequence of this requirement is the increased cost of the chip cards.

The last method of offline authentication is combined DDA/application cryptogram generation (CDA). This method allows performing DDA simultaneously with so called card action analysis – in previous cases performed always after a successful data authentication (for details see part 3.3). The terminal random data utilized in DDA is also a mandatory part of application cryptogram that contains the result of card action analysis. This simplifies the whole process and implies signing (by the private key of the card) directly application cryptogram. CDA is thus useful in the situations where the communication between card and terminal can not be assured.

3.2 User authentication

Once an offline data authentication has been performed, the scheme can proceed with the user (cardholder) authentication – typically through a handwritten signature or PIN, eventually a combination of both. All EMV compatible payment cards may contain sorted priority list of supported authentication/verification methods (CVMs). Note that one of these supported methods can also be "No CVM Required". These methods are compared with methods supported by the terminal and first method on the list that is also supported by terminal is selected for user authentication (i.e., the used method depends on both the card and the terminal). Verification process is completed when at least one CVM is successfully performed or when the list is exhausted.

Authentication based on handwritten signature or online PIN verification is performed by the same way as in the case of magnetic stripe cards. In the case of online PIN verification the PIN is formatted to the PIN-block, symmetrically encrypted by the 3DES algorithm and sent back to the bank for verification. Of course, these "old methods" are also supported by the EMV specification and the only significant change is introduction of more secure chip cards that should be able to prevent unauthorised copying. This statement does not need to be true if the application itself allows sending the data outside the protected environment of the card (as in the case of SDA).

Newly, EMV also supports offline user authentication by using plaintext or enciphered PINs. For PIN encryption, asymmetric cryptography (namely RSA) is used and the chip card should (again) contain new key pair dedicated solely for securing transfers of PINs into the card. These key pairs must be stored/certified in the same way as the key pair necessary for DDA. Entered PIN is (after secure transfer inside the chip) compared with the PIN inside the card. Security of this mechanism is based on the difficulty/impossibility of obtaining private key and PIN stored inside the card for offline verification purposes. The PINpad (where encryption is often performed) or even the whole terminal (especially if PIN is sent in plaintext form) should be also physically protected.

3.3 Automatic risk analysis

The main function of automatic risk analysis is mitigation of the probability of fraud and thus protection of all participants of transaction. The analysis is typically performed after successful user authentication and can be divided to: terminal risk management, terminal action analysis, and card action analysis. The result will indicate whether the transaction should be approved/declined offline, or transmitted online to the card issuer. Terminal risk management allows for example that: several small split sales/transactions cannot be greater than the floor limit set by a merchant; some transactions will be randomly selected for online processing; the number of consecutive offline transactions will be limited. Terminal risk management is followed by a terminal action analysis that always has a higher priority for negative results always than the result of concluding card action analysis (for a better protection against a fraudulent card). Preliminary decision to reject the transaction (decline offline) can never be changed by the card action analysis. The preliminary decision for transaction online processing can be approved or rejected (the transaction will be declined offline). Only preliminary decision of a terminal to accept the transaction offline can be arbitrary changed according to the result of card action analysis. The final result of the card action analysis is sent to the terminal as so-called application cryptogram.

3.4 Online transaction authorisation

Online transaction authorisation is based on the symmetric cryptography (it uses the 3DES algorithm) and requires one on-card securely stored secret key that is shared with the issuing bank. This key then serves as a basis for creating temporary per-transaction key that is used for creating message authentication code (MAC) of transaction data. The resulting MAC, together with the transaction data, is sent to the bank where it is compared with a MAC computed analogically. Their equality then implies that the card is genuine. This procedure is followed by a verification of account balance and similarly authenticated bank response.

4 Security of EMV in practice

EMV standard specifies a large spectrum of security mechanisms. However, not all of them are mandatory and the security of the system often depends on its particular implementation. The fundamental issue here is to find a compromise between price, performance, and security. If, for example, the banking network utilizes only online cash machines and payment terminals, it is not necessary to implement the costly combined DDA/application cryptogram generation (CDA) – the genuineness of a payment card can be checked by the means of symmetric cryptography. On the contrary, the support for offline transaction processing should imply that better mechanisms then static data authentication (SDA) will be used.

4.1 Real-world implementation

The first European country that implemented the EMV compatible payment systems was Great Britain. The reason was the highest percentage of forgeries with payment cards in the Europe by the end of nineties (75 % in the year 2000 [4]). The implemented solution is based on a combination of EMV 4.0 (sometimes referred as EMV2000) and VISA VIS (or equivalent MasterCard M/Chip). This technology is alternatively also sometimes denoted as “Chip&PIN” [5]. Its security issues are the subject of public interest and even academic research [6].

The most frequently criticized fact is the implementation of weak static data authentication. This mechanism does not require chip cards with the support of the asymmetric cryptography and the banks thus can reduce the costs – but unfortunately with a negative influence on the security. Omitting asymmetric cryptography allows intercepting all communications between the card and the payment terminal – including the account number and the PIN. The first experimental EMV interceptor prototype was constructed at the price less then $150 [7, 8]. The intercepted data can be easily used to make false magnetic stripe cards that are still widely accepted in many countries. Chip cards can be forged only in the case that static data authentication is used and moreover, they can be accepted only in offline payment terminals where symmetric secret 3DES key (that can not be copied) is not required. Fortunately, a lot of countries currently implement the more secure dynamic data authentication and banks in Britain are expected to do it as soon as possible.

The next weakness of EMV2000 [9] is insufficient protection of the list of authentication/verification methods (CVMs) that can degrade the whole process of user authentication. CVMs list interception and modification can lead to substitution of required PIN-based authentication for authentication based on handwritten signature. Several standards applied together with EMV2000 makes the British system resistant to this simple attack.

Quite important problem is also the EMV support in various hardware security modules (HSMs) and their application programming interfaces (APIs). These security devices are a very important part of banking (or PIN processing) centres and apart from the secure storage (e.g., for long-term cryptographic keys) serves as secure computing environment for performing sensitive cryptographic operations (e.g., encrypting sensitive data or PIN verification). However, EMV specification does not mitigate the risks closely connected to the bank employees – especially bank programmers. The first attack is briefly described in [8] and misuses the extension of IBM Common Cryptographic Architecture (CCA) for EMV support – concretely the functions that implement the secure messaging.

4.2 Other security impacts

The security issues of electronic transactions are more complicated from the customer's point of view. The payment terminals protect interests of merchants, payment cards protect interests of banks, and the interests of customers are typically overlooked. Unfortunately, this is not only a problem of the EMV specification. The malicious merchant is always able to cheat the customer. He can simply (especially in the case of magnetic stripe cards) copy the data from the card and using a forged payment terminal he can also get customer's PINs. In the case of EMV compatible chip cards he is able to redirect the EMV protocol and perform remote authorisation of much valuable payment realised by his accomplice. A demonstration kit for this attack has already been constructed [10]. In Britain several problems with modified "tamper resistant" payment terminals were revealed [11, 12]. Solution that was proposed in [13] is so-called electronic advocate that enters to the EMV protocol (without participation/permission of merchant or bank) and protects only interests of the customer (that paid for it). This advocate could be practically realised as a small portable electronic device that should enter the protocol between payment terminal and chip card and that should display the details of each transaction. According to the displayed value the whole transaction should also be either rejected or accepted (e.g., by entering a correct PIN).

Moving to the chip cards and PIN-based user authorisation (often referred as a Chip&PIN technology) brings also another serious problem – the liability of such authorised payments is typically transferred from the bank to the customer [9] (if the law do not order the converse). Currently there are only few banks in the Czech Republic that take partial liability for PIN-based transaction. However, often used argument that only the customer knows the correct PIN is not always substantiated and correct [14, 15]. Experimental results described in part 2 of this paper (and also in [1]) show that an opportunistic attacker/thief can simply observe the PINs entered by a customer to the payment terminal or cash machine. After a successful PIN observation the only thing that the attacker needs is to steal the corresponding payment card (and go shopping).

5 Conclusion

The EMV specification is (after many years) the first noticeable step forward to better security of electronic transactions and improving interoperability of payment systems. The Chip&PIN technology should prevent card copying and thus help to decrease the amount of card forgeries. Although the first EMV specification is roughly ten years old, there are still many security issues or problems. Some of them are embedded in the specification itself, the others are specific for the particular payment systems or implementations of functions in particular hardware security module. However, many countries are moving to the EMV very slowly and the introduction of Chip&PIN technology brings new opportunities to the attackers – the process of decreasing the amount of all card forgeries is thus very slow.

Since most European countries use online payment systems together with dynamic data authentication (or expect to move to DDA soon), the weakest part of the system infrastructure is the payment terminal. This terminal should be strongly physically protected (tamper evidence, tamper detection, tamper response, etc.), but this requirement is hardly achievable in practice. The problem is that the customers are not aware of individual types of terminals (and even they never can be) and recognizing that a terminal is slightly modified (e.g., allows saving user PINs) or forged (allows to redirect the EMV protocol) is currently nearly impossible.

The problem of the Chip&PIN technology is also the cardholder that enters the PIN. For the opportunistic attacker a success rate of PIN observations is 60 % vs. 42 % (for both phases of our experiment). This success rate is sufficient, because the attacker knows when he saw all PIN digits correctly and he will steal the card from the victim only after successful observation. The handwritten signature alone is a very weak authentication mechanism and the card should contain at least the cardholder photography. Unfortunately, manual correctness checking of these biometric data is always a very subjective process.

Acknowledgement: The experiment described in the first part of this paper was sponsored by the FIDIS consortium and VaF Bratislava. We would like to thank all who took part in our experiment and helped to get very interesting results and findings. Without this kind help nothing like this would have ever been possible. Many thanks for the cooperation with the management of the supermarket who allowed us to perform the experiment in a real environment and also provided us with a room where we could instruct our "customers".

References

[1] Krhovják J., Kumpošt M., Matyáš V.: *Platby kartou s použitím PINu.* Data Security Management (DSM), Vol. 2006, No. 5, ISSN 1211-8737 *(in Czech).*

[2] Krhovják J., Matyáš V.: *Platební systémy a specifikace EMV.* Data Security Management (DSM), Vol. 2006, No. 6, ISSN 1211-8737 *(in Czech).*

[3] EMVCo, LLC. *EMV 4.1 specifications* (book 1–4), 2004. Available at: http://www.emvco.com/ *(last check: 13/3/2007).*

[4] Rolfe R.: *The European Card Review*, November/December 2001. Available at: http://www.epaynews.com/downloads/ECR_01.pdf *(last check: 13/3/2007).*

[5] *Chip and PIN.* Available at: http://www.chipandpin.co.uk/ *(last check: 13/3/2007).*

[6] *Chip and Spin.* Available at: http://www.chipandspin.co.uk/ *(last check: 13/3/2007).*

[7] Bond M.: *Chip and PIN (EMV) Point-of-Sale Terminal Interceptor.* Available at: http://www.cl.cam.ac.uk/research/security/projects/banking/interceptor/ *(last check 13/3/2007).*

[8] Anderson R., Bond M., Clulow J., Rivest R., at all: *Phish and Chips (Traditional and New Recipes for Attacking EMV).* Available at: http://www.cl.cam.ac.uk/~mkb23/research/Phish-and-Chips.pdf *(last check: 13/3/2007).*

[9] Anderson R., Bond M., Murdoch S.: *Chip and Spin.* Available at: http://www.chipandspin.co.uk/spin.pdf *(last check: 13/3/2007).*

[10] Drimer S., Murdoch S.: *Chip & PIN (EMV) relay attacks.* Available at: http://www.cl.cam.ac.uk/research/security/projects/banking/relay/ *(last check: 13/3/2007).*

[11] Schneier's Weblog on Security. *Shell Suspends Chip&PIN in the UK.* Available at: http://www.schneier.com/blog/archives/2006/05/shell_suspends.html *(last check: 13/3/2007).*

[12] Drimer S., Murdoch S.: *Tamper resistance of Chip & PIN (EMV) terminals.* Available at: http://www.cl.cam.ac.uk/research/security/projects/banking/tamper/ *(last check: 13/3/2007).*

[13] Anderson R., Bond M.: *The Man-in-the-Middle Defence*. Available at: http://www.cl.cam.ac.uk/~mkb23/research/Man-in-the-Middle-Defence.pdf *(last check: 13/3/2007)*.

[14] Anderson R.: *Why Cryptosystems Fail*. Available at: http://www.cl.cam.ac.uk/ftp/users/rja14/wcf.pdf *(last check: 13/3/2007)*.

[15] Bond M., Clulow J., Murdoch S.: *Laser-printed PIN Mailer Vulnerability Report*. Available at: http://www.cl.cam.ac.uk/~mkb23/research/PIN-Mailer.pdf *(last check: 13/3/2007)*.