# PIN (& Chip) or signature – beating the cheating?

Dan Cvrcek, Jan Krhovjak, Vashek Matyas

Masaryk University in Brno, Faculty of Informatics
cvrcek@math.muni.cz, xkrhovj@fi.muni.cz, matyas@fi.muni.cz

**Abstract.** Our paper first reviews some of the most critical issues related to the introduction of Chip & PIN card payment authorisation, and then outlines one part of our experiment[1] that we decided to undertake to validate some of our views and ideas. Our experiment examines, in two phases, whether introduction of this authorisation method is advantageous for an opportunistic thief and whether the customer truly benefits from the Chip & PIN technology with respect to this opportunistic thief.

## 1 Introduction

Many discussions of the ongoing introduction of the Chip & PIN "technology" for purchase authorisation – and hopefully also authorised cardholder authentication – end up with a declaration that the new means obviously are – or are not – easier to circumvent for an opportunistic thief. We see this opportunistic thief as an individual or a small group of loosely organised individuals that do not have any special hardware for card analysis, cloning, etc. And it is the opportunistic thief we focus on in our experiment proposed farther below.

Card PINs are typically restricted to the length of four digits (only rarely one can see systems allowing for use of up to six digits, e.g. in Switzerland) and even then is their entropy rather questionable [1]. A reasonable assumption is that such short strings typed onto a "3-by-3" PIN keyboard are easy to spy on.

### 1.1 Problems with PINs

We are currently of the view that while Chip & PIN authorisation will likely increase the cost of card counterfeiting as well as complicate (at least at the first sight) abuse of stolen cards, it may have an adverse effect on Chip & PIN card users in the time prior to card loss detection and reporting. We see two potential problems here.

The first problem with PIN authorisation lies in repudiation – while the customer can fight reasonably well against a loss with a track in the form of a poorly faked signature, it will be quite hard to fight the loss after one's correct PIN has

[1] This experiment was partly supported by the FIDIS (Future of Identity in the Information Society) Network of Excellence.

been entered. There will be no track in the purchase/authorisation documents, and relevant camera recordings might be hard to get from the merchant – either due to their short retention time, or perhaps when considering where lies the interest of the merchant in an investigation of a disputed purchase. A closely related issue here is the use of cards stolen from mail, where the thief will quite likely also get the PIN – this can be partly addressed by the card activation procedure.

And a second drawback follows – current systems do not deploy different security mechanisms (or at least settings) for differing threat environments – different PINs for low- and high-level transactions. And so if the opportunistic thief can spy on your PIN while you do your bookstore or restaurant transaction, he can use that PIN with your card for a merry shopping spree at a jeweler.

While signatures in general have more entropy than PINs, their long-term problem has been that merchants often did not bother checking them (for a number of reasons) as many investigators have verified in reality [2]. Some of the indirectly related (yet that we do not want to treat in detail in this experiment and related discussions unless really useful or necessary) issues are:

- we have to allow for a co-existence of both Chip & PIN and signature authorisations and so we get drawbacks of both combined;
- the technology change introduces the opportunity for some participants to shift the parameters of risk exposure;
- what information can be read from the card chip at any merchant's reader and how can this information be used for other fraud, e.g. in countries or shops not involved in the Chip & PIN exercise?

The technological change from strip and signature to Chip & PIN surprisingly lowers the difficulty of some of low-tech attacks on cards. The main reason lies in the change in handling the cards. It is easier to spy on PINs than before (since they have to be used more frequently, and often in overcrowded shops where spying on one's PIN is much easier than at ATM machines). It will also be easier to create a satisfactory surface of the cards – the necessity of a PIN-card being inserted in the reader during the entire transaction also reduces the opportunity for the merchant to check some card details such as the physical security when compared with the signature purchase authorisation. The one (and only?) thing that will improve is the difficulty to obtain the machine-readable information from the card.

Let us assume that the opportunistic thief (working on his/her own or in a small loosely organised group) without a dedicated hardware will stick to the use of genuine (pickpocketed) cards, and let us examine whether the new or old authorisation approach is more favourable to this thief. We refer the reader to [3] for a detailed discussion of most problems with the Chip & PIN card payment authorisation.

## 2 The experiment – PIN v signature

We are verifying whether it is easier to get a correct PIN than to forge a signature. And so we decided to undertake an experiment where in realistic conditions the following would be examined:

1. Can the PIN entry spying be easier than the signature falsification?
2. Under what conditions does the above hold true or false?
3. What are other alternatives for purchase authorisation using chip-equipped payment cards?

Results from this experiment can help us and indeed the broader community (since Chip & PIN is in fact one of the largest computer deployment exercises with security as a major factor) answer the question related to this year's Workshop – is such a system your friend and should you like it?

We decided to abstract from the possibility of merchants colluding with the attackers, e.g. through the use of cameras, and so we have to stress that the experiment results are based on the assumption of honestly behaving merchant. (We disregard the possibility that the merchant is able to easily eavesdrop PINs, e.g. by installing CCTV or modified PIN-pads. Yet we understand that this type of attack has a very high potential.)

This experiment is being undertaken in at least two phases throughout the year 2005:

1. *Trial phase* – at this stage we examined the success rates of PIN observation and signature falsification in near-realistic conditions as described in this paper. Results from this phase are provided in this paper.
2. *Mature test* – we will undertake this phase of our experiment in realistic conditions this Autumn, with settings modified according to both our experience from the trial phase and also feedback from the discussion of the trial phase results.

## 3 Trial phase

This phase was undertaken in two rounds, the first round focusing on the success rates of observing a customer entering the PIN and the second round (more-or-less a verification round at this phase) on the success rates of falsifying someone else's signature (without the shop assistant's detection). Students and staff of our university took part in this phase, and the payment operations happened in the university bookstore.

The first round was undertaken with 32 "customers", 4 observers (of which typically only 3 were active at any given time), 3 (plus one of the observers) bystanders that did not cooperate with the observers and were not observing the customer, and obviously the shop assistants (2 – the bookstore owner and another person from a jewelry store to verify the signatures since the bookstore we used does not accept card payments), and three experiment supervisors. We

also made sure in both rounds (using the shop plus two other separated rooms) that customers after their participation in a given round of the experiment did not exchange information with customers who were yet to take part in the given round of the experiment.

### 3.1 Cover story

A good cover story is critical for customers' as well as merchants' behaviour to be unbiased (or, better said, as little biased as possible) when they participate in the payment operations. We therefore decided to inform both the merchants and the customers at the start that this experiment is conducted to survey pros and cons of two different methods of payment authorisation (PIN-based authorisation is used only in a minority of card payments in the Czech Republic, so it is known as an authorisation method overshadowed by signatures). We stressed that we would focus on measuring the time that all related operations take and on the issue of user comfort and acceptance, together with the facts that we use two different types of PIN-pads (and customers would be split into two groups). We also emphasized the request that both the customers and the merchant followed all security and logistic provisions they are supposed to follow in reality. The customers were requested to fill opinion survey questions at the start of the experiment to assure them in this belief.

Last but not least, the cover story was presented by a person who was not known to the "customers" and who posed herself as a researcher from the School of Social Studies, with members of our research group posing as technology consultants in this experiment.

At the end of the experiment, obviously, the participants were informed about the real purpose of the experiment.

### 3.2 Round one

In this round we took all thirty-two customers into one room and gave each of them a purchase card with a PIN that we randomly generated. Then we split them into two groups (one for each of the PIN-pads used) of 17 and 15 participants where each group used a different PIN-pad – one with a massive security/privacy shielding, and one without any shielding. Then we sent the customers one by one into the bookstore. Each of them had to pick one item at random and to approach the counter (or the queue at the counter). We started timing the operation once the customer handed the selected item to the merchant, let the card operation with PIN entry (correct at the first attempt) be performed and set the delay for purchase authorisation and receipt printing at a constant time of ten seconds. We read the time at the moment when the merchant handed the item and a receipt to the customer.

Once the customer left the bookstore we recorded the guesses of the PIN from our observers, and called the following customer.

### 3.3 Round two

In this round we took all thirty participants from the first round and split them into two groups of fifteen and seventeen members. The first group was issued cards with own signatures on the back, the second was given cards with signatures of someone else. Participants from the second group were given time of twenty, and at a special request thirty, minutes to practice the given signature.

The merchants were informed that there would be some customers falsifying someone else's signatures, without any indication of the rate of these customers.

The customers attended the bookstore again one at a time and their purchase time was measured as in the first round. The merchants, however, had to decide about the signature validity right at the time of the purchase (and were allowed to request the signature to be repeated if in doubt).

## 4 Results from the trial phase

### 4.1 Opinion survey

While we asked the participants to fill the opinion survey forms at the start of the trial phase of our experiment in order to strengthen their belief that this experiment was about the user friendliness of customer authorisation technologies, results of this survey are worth mentioning before we discuss the ultimate experiment results.

There were 25 participants (out of the total 32) who used magnetic strip cards for payments and about half ever used a Chip & PIN payment cards. The overall level of satisfaction with magnetic strip card payments was substantially worse than that with Chip & PIN card payments (3.4 mark against 2.5 on a five-point scale where 1 is the best and 5 is the worst mark).

Given the options of 10, 20, 30, 40 and 50 seconds as the maximum acceptable time for the entire payment operation the participants agreed on 21 seconds on average. And finally, the participants have experienced (on average) in 89% of their transcations no problem with the card payment, in about 7.5% experienced a minor nuisance, in 2% a major problem, and in less than 2% were unable to pay with their card.

### 4.2 PIN-pad with privacy/security shielding

For the seventeen "customers" who performed their experiment card payments using PINs there were six (35.3%) cases where the observers would succeed in guessing the PIN. And in five of those six hits the thieves would guess the PIN right at the first attempt, where for three PINs two observers got the PIN right and for two PINs one observer learned the PIN. In the sixth case the observers were able to build the PIN based on their shared knowledge.

Viewing the recordings from another point of view, the observers correctly guessed 75 digits (48%) in 39 tips of the four-digit PINs (i.e., for 156 digits altogether).

### 4.3 No privacy/security shielding PIN-pad

Results for this PIN-pad were shockingly different – for the participants "lost" their PINs to the observers in twelve out of fifteen, i.e. 80%, cases! And ten PINs out of this unlucky dozen would be guessed correctly right at the first attempt, with two PINs being seen by all four[2] observers, one PIN was seen by three observers, four by two, and finally three just by one observer. The remaining two correct guesses were built from the shared knowledge.

Using the alternative view, from the 46 tips of 4-digit PINs (i.e., 184 digits) provided by the observers there were 129 digits guessed correctly (70.1%).

### 4.4 Round two – signatures

For the seventeen cheating "customers" the merchants have correctly identified twelve of them as fraudsters, i.e. five of them bypassed the merchant control. Eight out of the identified dozen there were pointed out as fraudsters right after their first attempt, and four after their second signature. In the group of twenty (five fraudsters and fifteen signing their own signatures) successful "customers" there were only four participants who had to sign twice to convince the merchants. It is worth noting that both the participants and the supervisors for this experiment were of the view that the merchant check was quite thorough – we are of the view that this was caused mainly by the fact that the signature verifier works in a luxury jewelry store where the checks are on a higher level than in a supermarket or bookstore.

## 5 Conclusions

Considering that both signature forgers and PIN-entry observers were new to their tasks, the results of 29.4% signature forgeries going undetected and 35.3% or even 80% PINs being observed are rather unpleasant for most card users. With no paper trail allowing for later verification in case of disputed transactions, the figures for the Chip & PIN card are not exactly encouraging. Also, the comparison of the last two above mentioned figures definitely supports the view that privacy/security shielding for PIN-pads makes a lot of sense.

While we want to undertake the second phase of our experiment before we start with a detailed discussion of the results, the first phase indicates that we are perhaps going for a replacement of a weak biometric by even weaker secret information as the means for customer authorisation of their(?) payments. However, we see the biggest problem not in going for a weaker authorisation

[2] While the instructions said that always one of the four observers should abstain from watching the "customer" and engage in some interaction with the bystanders, in four cases all four observers reported some results with the fourth observer noting that "he couldn't have helped it" seeing the ease of PIN entry observation even at a distance, while talking to the bystanders.

method – we see the related problem of repudiability for PIN-based authorisation as the issue customers should worry about.

Results from the second phase of our experiment, together with a detailed discussion of results from both phases will be provided in a follow-up to this paper than can be requested from the authors (contact the last author regarding this experiment).

## Acknowledgements

Thanks are due to the FIDIS NoE for supporting our experiment, to Monet+ for providing the PIN-pads, to Pavel Marecek for the cooperation in and with his bookstore, to Dalibor Hanak for his cooperation in verifying the customer signatures, and last but not least to more than three dozen students who assisted us in this experiment. We also wish to thank Petr Hanacek, Marek Kumpost and Petr Svenda for stimulating discussions about the experiment plan.

## References

[1] M. Kuhn. Probability Theory for Pickpockets – ec-PIN Guessing. COAST Laboratory, Purdue University, USA, http://www.cl.cam.ac.uk/~mgk25/ec-pin-prob.pdf.
[2] J. Hargrave. Credit Card Prank. http://www.zug.com/pranks/credit/.
[3] R. Anderson, M. Bond, S. Murdoch. Chip and Spin. Paper available at http://www.cl.cam.ac.uk/~mkb23/spin/spin.pdf, webpage "Chip and SPIN!" at http://www.chipandspin.co.uk/.