Update on PIN or Signature
(Transcript of Discussion)

Vashek Matyas

Masaryk University, Brno

We promised a year back[1] some data on the experiment that we ran with chip and PIN. If you recall, it was the first phase that we reported on here last year, where we used the University bookstore, and two PIN pads, one with very solid privacy shielding, the other one without any. We ran 17 people through the first one, 15 people through the second one, and we also had the students do, about half of them forging the signature, half of them signing their own signature, on the back of the card that is used for purchasing books, or whatever. We had a second phase of the experiment, after long negotiations, and very complicated logistics, with a supermarket in Brno where we were able to do anything that we wanted through the experiment for five hours on the floor, with only the supermarket manager, the head of security, and the camera operators knowing about the experiment. So the shop assistants, the ground floor security, everybody basically on the floor, did not know about the experiment. That was one of the reasons why the supermarket, or management, agreed to take part, they wanted to control their own internal security procedures.

We had to create our own accounts, and we had people using these accounts with real cards, but not compromising their own PINs. Comparing the results from the first phase and this second phase, the shielding really matters in the bookstore experiment, this was not confirmed in the second one. I believe that there are two reasons for that. In the first case we used really heavy security shielding, the shield around the keyboard was the most extreme case of shielding that I've ever seen. In the second case, in the second phase, the shielding was negligible, and it played basically no role, from the angle of the observers in the shop. What played a critical role, as you can see here, was basically the assertiveness, (or aggressiveness) of the bad guys, the observers. We had three groups of observers, two of them scored about a quarter of the PIN digits at the till, and as you will see, those performing really well were able to observe correctly about two thirds of the digits at the PINs. I believe that these numbers are more indicative, these are the percentage of the correct digits that the observers would get from you in a shop if they watch you typing in your PIN.

In the first experiment the percentage was slightly higher because the bookstore was a closed environment, where we did not have more customers coming in, it was just one customer, and the people were really able to focus, and get around that customer. In the supermarket experiment, it was Friday late morn-

[1] D. Cvrcek, J. Krhovjak, V. Matyas, *PIN (and chip) or Signature: Beating the Cheating?*, LNCS 4631, pp 69–81.

B. Christianson et al. (Eds.): Security Protocols 2006, LNCS 5087, pp. 128–131, 2009.

ing and early afternoon operations, so you had many customers in the shop, it was not always possible to get the observers right in front, and right behind the guy who was shopping. In both cases their primary task was to observe, their secondary task was not to be spotted by the subjects.

George Danezis: The question is, what could someone do if they spot one of your observers. I as a customer, I could maybe hide my PIN when I type it, but fundamentally you can't really tell the shop assistant or the security guard, oh you know what, he's been looking at my PIN.

Reply: Why wouldn't you say, tell it to the security guard?

George Danezis: I don't know, how many people here would?

Mike Bond: Security guards tend not to wear hats in the UK, so you need to find a security guard.

Reply: These were uniformed security guys who stood behind the tills, definitely less than 15 metres away, so you could just call, hey, come and help me, this guy's watching me. So yes I believe most of the people there would report.

George Danezis: Did anyone report?

Reply: No. At the end of the four hour period, one of the till assistants started watching the guys because she saw the same faces running round for four hours. [Laughter] She has a phone connection to security on the first floor of the supermarket management offices, but she didn't report anything; our guys just told us that she looked a little bit more cautious.

Tuomas Aura: That's funny because a long time ago I worked in a supermarket, and I think that normally people working in the store are thinking, oh, no, something's wrong, we've got to catch them.

Reply: Yes, but first they have to get the suspicion, and the point is how long it takes them to get there, if it takes them four hours with the same people running on the floor. We did not have the same people running around the same till all the time, but we had a row of a dozen tills, where we had three groups of participants. These groups didn't change formation so it was the first group, second group, and third group, who were just moving and going between different tills. I would think that people would figure out that there are people who are always rushing there to be one of them in front of the customer, one of them being after the customer; they didn't.

I will get to the signatures, that's the last slide. In the first case we used for signature verification a guy who owns (and performs signature checks in) a jewellery shop, so the success rate there was only 30%, he was quite thorough in his checks, as I mentioned last year. In this followup case every one went through

at the first try. I've seen some of the signatures, some were pretty much plausible, but some of the signatures, with a reasonable way of thinking you would never, ever accept such a signature comparing it to the card. In some cases the assistants didn't even bother looking at the signature itself, they were just happy with the people signing the paper, and giving them the paper that's signed, so all the people went through at the first try, no-one had to sign twice. And my personal experience is that in the Czech Republic they sometimes can get a bit thorough so that you have to sign more than once because your signature doesn't look entirely the same. Because my shopping usually goes by two orders higher than this small shopping that we did in the supermarket, I asked in the supermarket whether they have some thresholds over which the thoroughness of the check of the signature should be better; the response was "no", that it's up to the individual decision of the shop assistant, and they should check everything.

Matt Blaze: What is the liability if there's a fraudulent transaction, is it the store, or the credit card?

Reply: I don't know about this specific supermarket, but generally they can have liability which is limited, typically it's 150, 160 euros.

Matt Blaze: So it may just not be worth it to risk offending customers by checking at all? If you think it doesn't match, then you've got a dilemma if you're a shopkeeper, because if you ask you may offend the customer, and risk losing the sale, right, why do you think I'm a thief?

Reply: Well I definitely agree with that, the point is that some of the assistants didn't bother checking the signatures.

Ross Anderson: One of the reasons often cited is that the shop assistants were reluctant to say, this card is a forgery, even when it was blatantly in an experimental context. Now I can recall some other work, that you got shop assistants challenging people doing credit card forgery more or less only where the rewards offered by the credit card brands were actually passed on to the shop staff. If they were just trousered by the shop, then the shop staff wouldn't bother. So another thing to look at here is the policy of the supermarkets in terms of rewarding shop staff detecting stolen cards, if a stolen card is worth $50, say in America, does the shop assistant get $50 or $10 or nothing?

Matt Johnson: With the new self-service tills they're doing in some of the supermarkets over here, they don't do chip and PIN when you pay with your card, if it's above £100 then someone comes over and gets you to sign a piece of paper, and if it's below that it just goes through without any checks whatsoever.

Reply: Basically you enter the PIN, and you are still asked to sign that paper. I personally tested this on the day when we went to the experiment just to check the floor and everything. I falsified a signature that I hadn't seen before, I just

knew Marek's name, I didn't know whether he signs his first name in full or just the initial, I obviously did the contrary, the assistant looked at the signature, it was considerably different in my handwriting, and it was not saying M Kumpost, but he was saying Marek Kumpost, she looked at that and she said, oh, but the PIN was alright, go ahead, that's fine.

Anyway, the second phase indicates to us that PINs are slightly better than signatures, but as you see, the figures for the assertive guys getting two thirds of the digits of customers' PIN is quite a good success rate. The secondary observation of no reaction from the shop ground security or assistants, was quite interesting, because it was a five hour experiment.