Update on PIN or Signature
(Transcript of Discussion)

Vashek Matyas
Masaryk University, Brno

We promised a year back 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.

© Springer-Verlag Berlin Heidelberg 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