Phish and Chips
(Transcript of Discussion)

Mike Bond

University of Cambridge

Chris Mitchell: From your paper I got the impression you were implying there was only one API, I think actually different banks use different HSMs, with different APIs.

Reply: Yes, I'm going to talk about one API that we looked at, the API produced by IBM, and some of the issues we found with that. We have found issues also with an API from another manufacturer, Thales, and we've got a much larger paper, which is really rather long and tedious, describing all the different APIs we have looked at, the APIs we don't know about, and what we suspect are the cases with those, and I think there's a link to that towards the end.

We talked to IBM about it, there are ways that they can go to fix this by changing the API, but unfortunately they then start to lose the generic functionality, they lose the ability to make this command general enough to capture a load of different messages, and then you have problems. Every time the EMV specification, or a smartcard manufacturer wants a new command, how are you going to change the firmware of the security module to make sure that that particular message can now be added? It's quite a lot of hard work to change the firmware of these things because they're so deeply embedded in a large security system.

So what I've shown you here is specific to the IBM device, but we are writing a paper called, On the Security of EMV Messaging[1], which considers the larger arena.

Kenny Paterson: A quick question, to get that to work presumably you would need to have access to its encryption oracle, does that place limitations on what type of attack can be done, or who can do it?

Reply: Oh yes, if we look at the big picture, different parts of the protocol have access by different people, so customer and card protocol here has access to the customer and access to the merchant, so pretty much anyone. Stuff here is extremely closely protected, and so you've got all sorts of other layers of security surrounding banks and their data centres, where this runs. In practice, despite a wide variety of security vulnerabilities being found in hardware security modules, they can normally go until the next update cycle, without being fixed, or even several update cycles over a couple of years, in my experience, before they're

[1] In Security Protocols Workshop 2007.

B. Christianson et al. (Eds.): Security Protocols 2006, LNCS 5087, pp. 49–51, 2009.

updated, because there are so many other layers of security. Banks simply are not experiencing a practical problem with vast quantities of cash going missing from this sort of attack. Although one bank recently did get in the news for a large PIN theft, and we don't know quite what went on there.

The UK banks have decided that they will issue re-advice of your PIN, so if you forget your PIN, you can be sent a letter which tells you what the PIN you chose was. It doesn't give you a brand new one randomly thought up, but tells you your old PIN. So now you can open a dummy bank account, maybe stick $100 in it, and set the pin to all zeros. You capture the details of some victim Alice, and prepare a counterfeit card, so you need a card printing facility, and you make up a fake card, a fake hologram, but you put Bob's details on, and Alice's name. Then you put this in the post to Alice. In the United States, you get sent unsolicited credit cards all the time, you either make it unsolicited, or you say it's a replacement, and you tell Alice there's a $100 free gift if you start using our credit card, by the way, your initial PIN is all zeros, be sure to change it to a memorable number as soon as possible. So Alice goes away with her brand new card, oh this is good, I'll spend $100. Bob whose actual card it is, and whose authentication mechanisms to the bank, via postal address and passwords, are all set up, then phones the bank and says, "I've forgotten my PIN, could I have re-advice please", and Alice's new PIN will be sent to Bob's address.

Michael Roe: Don't they send you a new random key when you do that?

Reply: No, they don't, not all banks do. Quite a lot of banks in the UK issue PIN re-advice, which is your same PIN that you've forgotten sent back to you.

Michael Roe: Which is a bad idea for the reason that you've just told us.

Chris Mitchell: I guess the stuff at the end is really neat, and it applies to just about any conceivable smartcard based payment system, it's not specifically EMV really?

Reply: Yes, I would suppose not. It is specific to EMV, and specific to the UK, I suppose, in that there are options for where a PIN can be routed. You don't have to send the PIN to the smartcard, you could design an electronic payment system with smartcards that sent the PIN over the phoneline back to the bank.

Chris Mitchell: But then I'd worry that there are other scams?

Reply: But then there are different tricks, yes.

Bruno Crispo: To activate a card don't you need a phone?

Reply: In some systems you do, other systems you don't, it depends. That's very much a practical issue: none of these last attacks presented are practical, they're all trying to prove the concept. I think about one in five UK banks require you to phone to activate, mainly the internet banks. The High Street ones don't tend to bother their customers with that.

Srijith Nair: Actually that's the same question I wanted to ask, isn't there a set of guidelines for all of the EMV countries stating how to issue cards? In the

Netherlands, if you want to activate the card, I think you have to bring the card back to the bank to activate it, or if you are asking for a replacement card, your PIN is actually the same as the previous PIN, so you can't put it as 0000.

Reply: Well if so, the trip-up that's happened is that they called the document "guidelines", because the UK banks aren't following it. The UK banks have decided to prize convenience over everything, and make sure that the transition is really easy for the customer.

Richard Clayton: If you're actually sending bad cards to Alice with evil chips on them, not only has the bank not read the guidelines, Alice hasn't read the guidelines either, so she won't ring up the issuing bank in order to get it validated. It really doesn't matter whether that's the normal practice, since you're sending her a special card, you can put a big thing on the top saying, you do not need to ring up in order to activate this card, we'll send you a magic PIN.

Bruce Christianson: Well if it's really Bob's card, and he hasn't rung up about it yet, she might get noticed.

Reply: Oh well, I mean, one of the drawbacks of these things is that some of these attacks are predicated on being able to open bank accounts in false names. If you can do that, you might as well just get an overdraft and start spending. Talking about what is practical and easiest for criminals is a different matter from talking about what's possible.

Alex Shafarenko: Within the same assumption that you can open a bank account, I think, stop this smartcard, they charge £25.37 to Bob, which would be the communication of the PIN 2537, right, so you don't need to print anything on the receipt, it's accomplished two transactions in one go.

Reply: The smartcard doesn't have much control over the value in the transaction in EMV. The smartcard just MACs the transaction data, it's the terminal which controls how much money is spent, so you would have to have a dodgy terminal as well, which would change the threat model a little bit. To be honest, the first avenue of attack is interception relay, this is the area of contention for chip and PIN, whilst magnetic stripe fallback runs alongside it. About 450,000 point of sale terminals in the UK accept PINs, thus increasing dramatically the number of different places that attackers can skim PINs for use with the old system. Once they can shut down magnetic stripe, then it's not an issue, but that's not going to happen for a while.