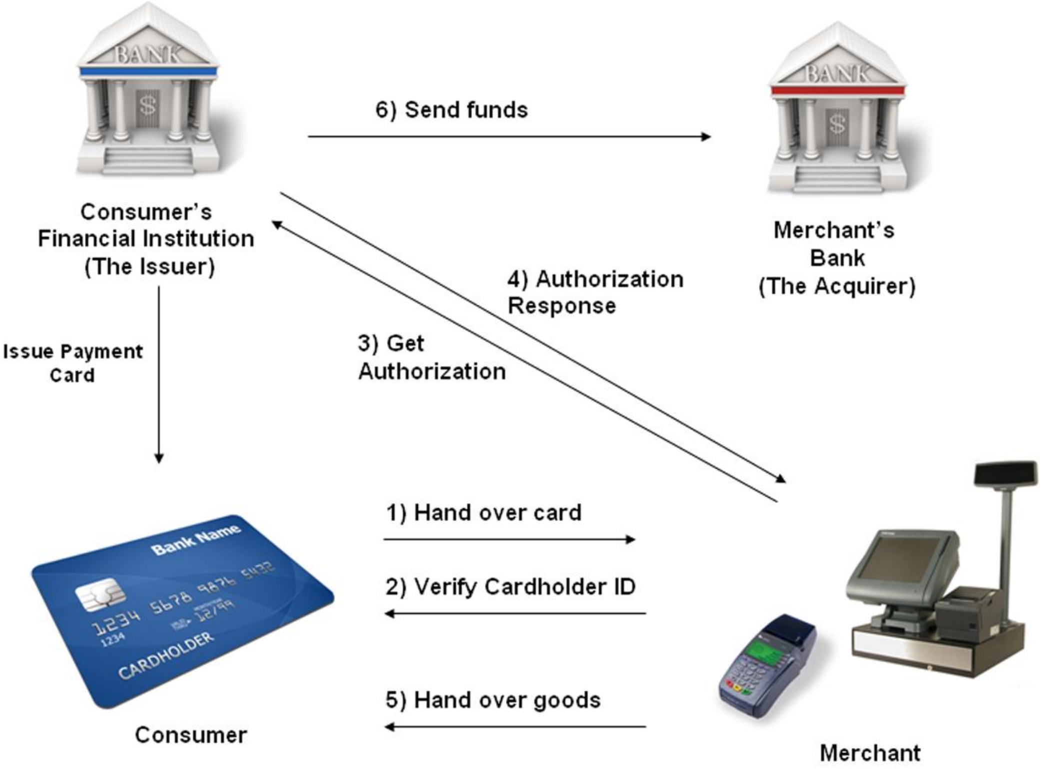
# Terminal Decline in Cambridge

This month the media has been full of it, The Computer Laboratory from the University of Cambridge has reported[1] (yet again) that Chip & PIN (EMV) is broken although many others seem unconvinced. We are happy to be able to tell you that EMV is probably all right, certainly fit for purpose, but that the real problem is the Point of Sale (POS) terminals. These terminals can (in principle) be interfered with ad infinitum and can cause vast numbers of fraudulent transactions both direct and indirect and it's only going to get worse.

So who is right, has it or hasn't it been broken? To get at the answer we need to understand the principles behind electronic payments and more particularly the credit and debit card transactions we are all so familiar with at the Point of Sale. In particular we will show you why as a result of this attack some of the banks need to tidy up their back end systems, why we all need to worry about the security of the POS terminals and why we probably don't need to lose too much sleep over the EMV protocols.

Let's first look at it from the point of view of the cashier in the retailer; he wants to be paid in exchange for the goods he sells you. If we pay for goods at the POS with cash we are effectively handing over the financial asset from our pocket to that of the cashier's cash box. He gets the funds immediately, nobody else is involved in the transaction and all he needs to know is that the cash is genuine, i.e. not counterfeit. At the end of the day the retailer will deposit the cash collected at his bank.

Now let's look at a consumer with a bank account at some Financial Institution (FI) and a debit card that allows the user to make payments against that current account held by the FI. Who are the participants in this transaction?



Suddenly life gets far more complicated and we enter the world of the 4-Party model. The reason for this complication is that the consumer no longer holds the cash or funds in his pocket, they are actually held by his bank which in the 4-P model is called the Issuer (of the card representing the account held by the bank). When the consumer purchases goods at the merchant he is not handing over cash or funds but instead an instruction to his bank (the Issuer) to make payment to the merchant's bank (called the Acquirer because in practice all the merchant terminal transactions pass through the Acquirer in order to get to the Issuer). Doesn't this sound like an electronic version of a cheque?

Yes, it's exactly that and do you remember what used to happen (a long long time ago)? The consumer would write the details of the transaction and sign the cheque, the merchant would then hand in the cheque at his bank that would go and get the funds from the consumer's bank by passing over the cheque. The consumer's bank would look at the cheque and check the signature, then check the account has funds and if all is well make a funds transfer to the benefit of the merchant's account at its bank.

It seems remarkable but not that many years ago you could pay for goods with a cheque and take the goods away there and then. But things have changed and clearly we have all become more dishonest so the merchant would like to be assured that he is going to get paid before he hands over the goods. So what is required?

- The merchant wants authorisation (that says he will be paid) from the Issuer before handing over the goods
- The issuer needs proof of the consumer identity and the transaction details that need to be authorised (as an agent of the account holder) for payment

So for identity authentication you will remember the three Factors,

- Something you know
- Something you own
- Something you are

Well the card acts as something you own but on its own this would just be single factor authentication (1-F) so it's nice to have at least 2-F authentication. Well in the original world we used a signature (something you are, a sort of biometric) on the cheque so we could just use a signature at the merchant's POS. It provides forensic evidence in the event of a dispute and the cashier can compare signatures, it could even be done electronically. Of course we know this is not very good and the cashier could easily be fooled or even bullied. So enter the Personal Identification Number or PIN.

The PIN is clearly something you know and in conjunction with a card would provide the 2-F authentication. Now how can you actually authenticate the cardholder using the PIN without revealing its secret to all and sundry? Well you can't just give it to the cashier so either the terminal has to check the PIN or you have to send the PIN to the Issuer for checking. You can imagine the security problems of making the terminal adequately secure for PIN checking, the big problem is that you are in danger of creating a systemic attack on all PINs created by that Issuer and of course each Issuer is going to have his own method of protecting PINs. Let's quickly pass on and decide that the PIN needs to be sent to the Issuer. Without entering a long discussion it is readily apparent that the PIN will need to be securely encrypted at the POS terminal and that the Issuer will need to send an encrypted response to the merchant's terminal. If you didn't some hacker might decide to interfere with the communications channel between the merchant and Issuer and yes, don't ask, it's been done in the past.

Fast forward to Chip & PIN which is a colloquialism for the EMV (Europay, Mastercard and Visa) standards first publicly released in 1995. The chip was seen as the way of mitigating the forecasts for increased fraud in the electronic payments world. Not needing to go into too much detail here but the chip card allows 3 security functions to be achieved,

1. Cardholder authentication (by checking the PIN in the chip)
2. Card authentication (proof that the chip knows a secret)
3. Card data authentication (by application of a trusted digital signature)

Now we are starting to get to the problems so in reverse order, it is easy for the Issuer to digitally sign the data held on the card and to ensure that the POS terminal has the appropriate public key (let's avoid the detail of the Public Key Infrastructure or PKI for this discussion) to check the signature and therefore to be assured of the authenticity of the data. Problem is anybody can read this data and signature (after all the specifications are in the public domain) and could easily create a counterfeit chip holding this same data.

Card authentication, this is really the Achilles heal of the payment card's world. The concept is straight forward, the card needs to show it knows (contains) a secret without revealing the secret.

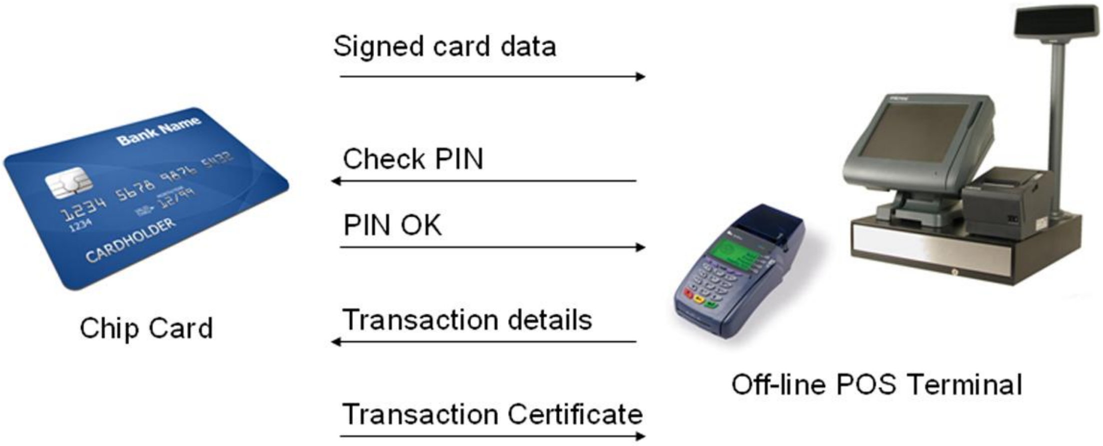
And last but not least we need to get the PIN to check the card and to know the PIN has been checked.

Here we come to the nasty problems that happen in the real world, perhaps the bank's customer can't manage a PIN, for example they may have some memory disorder. Then there are those occasions where it might be impractical to have a PIN pad like at vending machines. And all the time we must remember that the Issuer is holding the account on behalf of the cardholder, the bank must be assured of the identity of the cardholder and the genuineness of the transaction details. To make it worse there are good business reasons that not all transactions are handled by an on-line connection to the Issuer they may be handled by the terminal off-line. So in these cases the Issuer has to trust the POS terminal and the processes applied by the cashier. So what do we get,

- The chip does not mandate a PIN check
- The chip may not implement public key cryptography
- The terminal does not hold Issuer secret keys
- The terminal may operate off-line

There are two scenarios to consider,

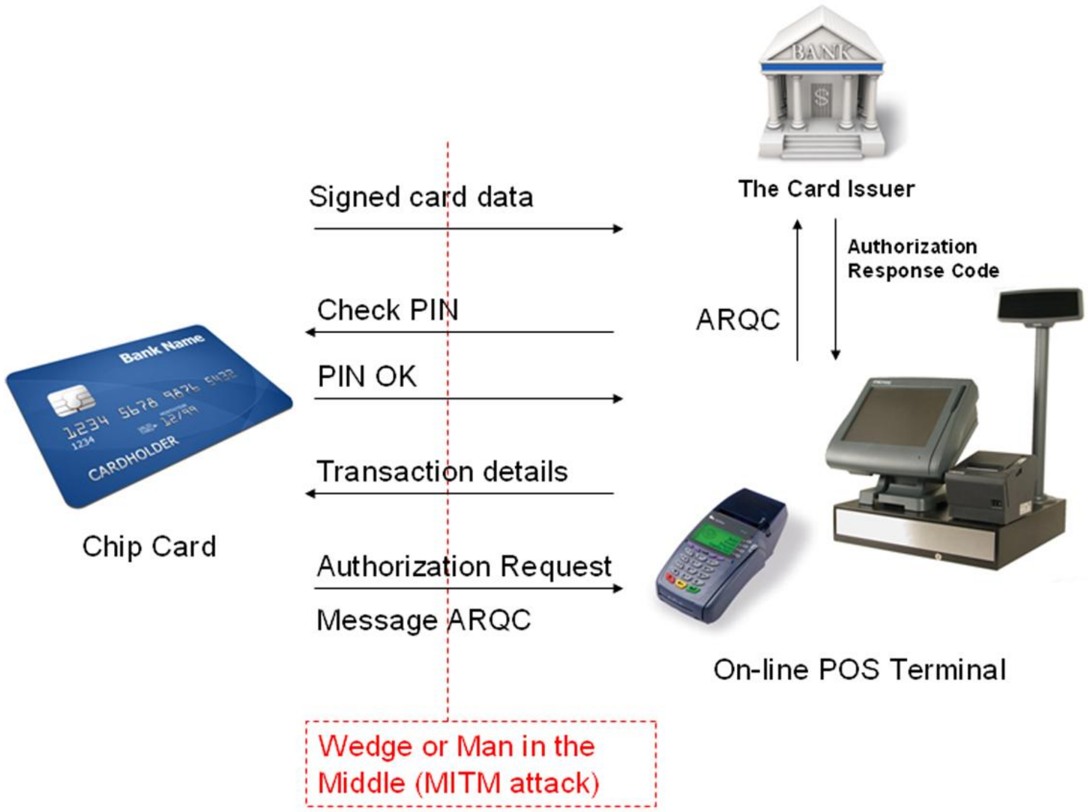
An off-line transaction where the chip doesn't implement public key cryptography, in this case the terminal is incapable of checking any data created by the card because it would require a secret key in the terminal.



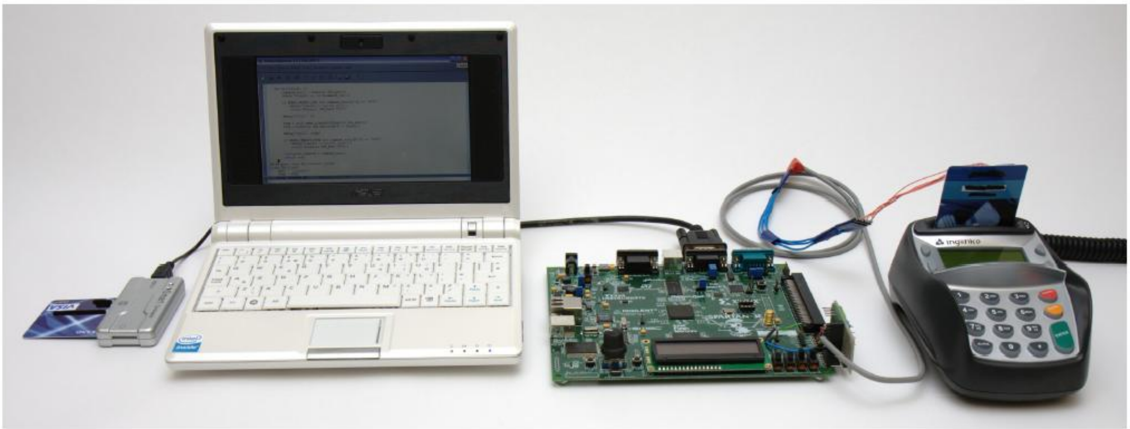
So in this case the terminal sends the PIN to the chip card for checking and the chip replies effectively with an OK message. This message is unprotected because the terminal doesn't have any secret keys that would be necessary for an encrypted message. The Transaction Certificate (TC) is also a problem because the terminal doesn't have the necessary secret key to check it, it could be total garbage and it wouldn't know. The signed card data is initially sent by the card to the terminal and this can be checked by the terminal with the public keys previously provided.

Now we can quickly see that it would be easy to make a counterfeit card that will provide a copy of some genuine signed card data, which could say OK to any PIN check and could also create a fraudulent Transaction Certificate that the terminal can't check. The issuer would spot the problem when it gets sent the TC but that would be too late, the goods have gone. If the terminal is operating on-line the fraudulent card (which has to in this case generate an encrypted authorisation request message) would be spotted immediately and the transaction would be declined.

So in the second scenario let's look at an attack on an on-line POS terminal,



For simplicity we have left out some of the messages but this is enough to show the problems and the basis of the latest attacks form the Cambridge Computer Laboratory. Here it is assumed that an attacker intercepts the communication path between the POS terminal and the chip card. This could be done in the terminal or by inserting a skeleton card with wires to the interception system in a genuine terminal as shown below from the Cambridge University paper. In this scenario it is assumed that the card is genuine, it was stolen or found by the attacker, but the attacker doesn't know the PIN.



We can already see where this attack is going, the chip card knows that a PIN check is optional and so will be very happy not to get a check PIN message. The attacker who is intercepting the messages between the card and terminal just removes the PIN check message and sends the necessary (unprotected) OK message to the terminal. The terminal is now satisfied that a PIN check was successfully completed and carries on with the rest of the transaction. The flaw detected by the Cambridge researchers is that the Issuer is not checking the Authorisation Request Message (ARQC) which is encrypted (to create an authentication code) to determine if the card has checked the PIN. This information is in practice included in the ARQC but arguably what the Issuer does about it is outside the EMV specifications. So what they have shown is that you can make a transaction (against some Issuers) at an online POS terminal with a lost or stolen Card without any knowledge of the PIN.

One would want to argue that this is not a break in Chip & PIN but more a lax attitude by some of the Issuer banks who are perfectly capable of checking this information. One of the nasty problems here is that the consumer could be accused of using a PIN (and therefore liable for the transaction) when he didn't. I believe the banks really need to put this right.

But where does all this lead us? It's really an understanding that the POS terminal environment is truly hostile, on-line or off-line and that no matter how secure the individual components any interception between the constituent parts can lead to fraud. We have also discussed previously the TJ-Maxx attack in the USA where the attackers intercepted the terminal Wi-Fi connections to get the details of over 40 million credit cards that could then be used to make fraudulent transactions.

What must be clear here is that if an attacker can interfere with the POS terminal environment then only the imagination can limit the levels of possible fraud. For instance the consumer doesn't actually know what the terminal is doing. It could easily use a genuine card to make transactions of a totally different value to what they expect and of course the terminal could be modified to make a transaction to the benefit of a totally different merchant (depending on the terminal acquisition architecture), the point here is that no matter how good the security of the chip card a fraudulent terminal can be the source of rampant fraud which has already been shown to be the case.

How can the user of a POS terminal (or a PC or a mobile phone) be assured of the authenticity and integrity of that device? Don't laugh we looked at this problem over 25 years ago, I still remember the conversations with David Chaum who I think was the first person to address this problem with the concept of a trusted device that you carry in your pocket. It connects the card to the terminal and has its own keyboard and screen so you can see what is going on. You might be thinking that the mobile phone is the modern equivalent? It could be if it did nothing else, but an internet connected device with downloaded applications – Oh no, not yet, and not in the foreseeable future!

Dr David Everett. – February 2010

[1] *Chip and PIN is Broken; Steven J Murdoch, Saar Drimer, Ross Anderson, Mike Bond; University of Cambridge, Computer Laboratory; To appear at the 2010 IEEE symposium on Security and Privacy*