



The security of the 'Chip and PIN' scheme has been attacked by numerous commentators in the media resulting in a significant misrepresentation of the facts. It is of course always easier to attack a system than to defend it and purists may easily lose sight of an optimum solution, perfect security is not economically viable even if practically achievable. The objective of the scheme operators must be to achieve a solution that is 'Fit for Purpose'.

In May 2006 the press was full of the Fraud resulting from card skimming in Shell filling stations in the UK, reportedly at just three sites but which has resulted in customer accounts losing over £1 million. Shell has subsequently stopped using the PIN at its own filling stations.

In June there have been more stories most notably in the Daily Mail (Monday June 5th) that the chip and PIN bank card system is so seriously flawed that millions of customers are dangerously exposed to criminals.

These criticisms are based on two vulnerabilities:

- 1) That you can construct a counterfeit magnetic stripe card using information obtained from a genuine chip card in a compromised terminal (or with collusion) and that this same terminal would allow the hacker to obtain the PIN.
- 2) That you can construct a counterfeit chip and pin card using information obtained from a genuine card in a compromised terminal (or with collusion).

The value of the counterfeit magnetic stripe card arises because there are still a number of magnetic stripe terminals in Asia and America. The problem here really has nothing to do with the chip and PIN scheme it is purely a matter of implementation and operation. Assuming the specifications are followed then there is insufficient information in the chip to construct the magnetic stripe data, in particular you need the CVV which should not be stored in the chip. This means the hacker has to also read the magnetic stripe on the card. It is a security vulnerability that some terminals have been implemented to read both the chip and the magnetic stripe (from the same card). That the tamper resistance of the terminal can be easily broken is obviously a security violation. Clearly this attack has no value in a total chip and PIN world.

The second vulnerability involves an understanding of the underlying chip and PIN architecture. Apart from the card holder verification where the chip can validate the customer's PIN, the account data (as would be stored on a magnetic stripe) is also protected by a digital signature which can be checked by the terminal. Remember checking a digital signature only requires an authentic public key.

The second security feature is a digital signature that protects the transaction data to prove that it is coming from a genuine card.

There are two options in the chip and PIN specifications (EMV) for how this is done,

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)

In the case of SDA there is a cryptographic check value (CCV which is not really a digital signature but which can provide the necessary authentication and integrity properties) created using a secret key stored in the card. The cryptographic algorithm used is symmetric which means the same secret key needs to be used to check this CCV.

It is very difficult to manage secret keys in a large terminal population so this CCV can only be checked by the card issuer who knows the unique secret key for each card in his population. If the transaction is allowed to complete off-line then the terminal cannot be assured that the card is genuine. In an on-line mode the issuer does of course check this CCV.

For DDA the chip and PIN card has the capability to create a digital signature for the transaction which as for the account data can be checked by the appropriate public key in the terminal. In this case it is not necessary for the terminal to go on-line to check the authenticity of the card.

So what can the hacker actually do (we are going to ignore the specialist reverse engineering laboratories for this conversation)? Well the EMV specifications are freely available on the internet. Any programmer could build an EMV card or you could buy one in the open market place. If you have captured the account data from a genuine card and remember you do need access to the card to do this then you could produce an SDA card that to an off-line terminal would appear correct because it can't check the CCV referred to previously.

The PIN is irrelevant here because you could choose your own and set the value in the counterfeit card. The security anchor is the secret key which creates the CCV and which is not available to the hacker. If the counterfeit card is used in an on-line mode then it would be detected immediately because of the false CCV generated by some key randomly chosen by the hacker. It is clear that the hacker would have the same problem for creating the DDA card; he wouldn't know the secret key used to generate the digital signature but in this case it would be spotted immediately by an off-line terminal.

So now the whole problem comes down to one of risk management. In the case of the magnetic stripe counterfeit card there is a real problem because the issuing bank has no way of knowing whether a genuine card was used. In this case the customer's account really is on risk. That's why we have chip and PIN. For DDA and SDA in an on-line mode the transaction would be declined at the terminal. So the risk which is to the issuing bank is under what conditions to allow an off-line transaction for an SDA card. But this is just a small part of the story. The cost of DDA cards is now rapidly approaching the original cost of SDA cards, on-line communications is becoming more readily available, and in the overall risk model the issuer needs to know there are available funds or that the customer in a post paid scenario is actually going to meet his commitments and then you have all the other controls on an EMV card to help you minimise risk. More importantly the real risk to the consumer is from magnetic stripe cards and terminals not chip and PIN when implemented and operated correctly.

[By David Everett]