



Le GIE des Cartes Bancaires « CB »

## Chip cards : the most secure and practical payment instrument

Paris, 21<sup>st</sup> January 2010

Scientific researchers from the University of Cambridge (UK), of which the most well known is Professor Ross Anderson, have announced that they have tested a scenario which attacks the EMV chip card.

The attack scenario in question has already been analysed by several teams of independent specialists, as well as CB's own experts, with the conclusion that neither the chip in itself, nor the importance and the advantages of the chip in terms of security have been put into question.

What is more, at this stage, the observations are the result of scientific research whose transposition outside laboratory conditions is complex since it would necessitate the use of highly sophisticated material.

### **It is a form of attack on chip cards which is highly complex to implement**

Without going into the technical details which are extremely complicated, the proposed scenario would modify the information exchanged between the terminal and the card.

It is also based on the use of a genuine card which has been stolen (and not a copy of a genuine card).

The scenario does not allow a card to be either cloned or reproduced in number, and is not in any way comparable with the "Yes Card" phenomenon which was encountered in the past, and which has been eliminated successfully since 2 years.

In fact, the scenario proposed by the researchers is based on the following premises and is subject to important limits in terms of its use :

1. the use of cumbersome equipment which has not been miniaturised,
2. the use of a stolen card,
3. based on the proposed scenario, it is impossible to use a stolen card in ATMs for cash withdrawal,
4. such a scenario could only be used for offline transactions, i.e. in essence those transactions which are for small amounts and which have not been subject to an authorisation

The conjunction of all these practical constraints greatly limits the interest which fraudsters might find in transposing such research into everyday life, especially since the principle target for fraudsters is to obtain cash.

As explained earlier the attack scenario in question cannot be used to obtain cash from an ATM.

### **CB Cardholders are, as always, protected against fraudulent debits**

It is important to note that CB Cardholders would not suffer any prejudice and would still be protected against fraudulent debits to the accounts should the above scenario occur.

The CB systems are able to clearly identify the type of attack described by the research, and the banks also have the capability to unambiguously determine the nature and origin of fraudulent card transactions therefore to clear the cardholder acting in good faith of any responsibility.

The fact that security of a system is continually being challenged is an excellent stimulus to identify potential residual vulnerabilities, and as a result to reinforce its robustness.

The publication of this research is an opportunity for the Groupement des Cartes Bancaires CB to confirm its close cooperation with the scientific and University communities. CB has always taken into account avant-garde work from these sectors which could contribute to the improvement in the quality and the security of the CB System.

The CB card remains both the most secure and the most practical means of payment today, whilst ensuring that Consumers are reimbursed for any fraudulent debits, and that Merchants are guaranteed payment for CB card transactions.

Press Contact :

Françoise Fanari – 01 40 15 58 57 – [francoise-fanari@cartes-bancaires.com](mailto:francoise-fanari@cartes-bancaires.com)