

26 February 2008

New fears over contactless chip cards raised

Fresh concerns have been raised over the security of radio frequency identification (RFID) technology used for contactless payments after a hacking demonstration by security expert Adam Laurie at the Black Hat 2008 conference.

At the conference earlier this month Laurie used his new EMV Chip And PIN credit card reading script, called ChAP.py, to pull the name, account number and expiration date from an audience member's RFID enabled American Express card - without removing the plastic from the victims wallet.

American Express uses RIFD technology to support its contactless payments ExpressPay cards. The firm insists it is confident in the security of ExpressPay and says the account number extracted by Laurie cannot be used for online transactions.

ExpressPay cards have two account numbers - one for contactless payments and one for the debit or credit card feature. American Express says by only transmitting the 'alias' number for contactless payments it protects the credit or debit card number.

In a statement, the card scheme says: "As the payment host, American Express would not verify an online transaction using just the alias account number. There are several other security mechanisms that would be required in order for payment authorisation to take place."

The company says it has also stopped storing the cardholder's name on the ExpressPay chip.

Laurie, a non-executive director of data security firm The Bunker, has added ChAP.py, which uses the Python script language, to his RFIDIOT online library for people to download free of charge. The site also sells hardware to read and write RFID devices.

Concerns over the security of RFID are not new. In 2006 a group calling itself the RFID Consortium for Security and Privacy claimed to have uncovered lapses in the security and privacy features of several types of RFID payment cards.

The researchers tested around 20 contactless credit cards and found that RFID cards transmit cardholder names and so any device capable of scanning a card can learn the name imprinted on it - with or without the owner's consent

Secondly, the RFID credit cards are vulnerable to skimming. An attacker with an RFID reader can harvest information from a card, create an inexpensive clone

device, and make charges against the legitimate card, says the group. Alternatively, a fraudster may be able to perform online transactions with harvested credit-card information.

However the Smart Card Association rebutted the claims, suggesting that nothing in the report supports the conclusion that a criminal could complete a fraudulent contactless payment transaction in the real world.