Merchant Terminals Provide New Method For Stealing Customer's Credit Cards

March 4 2008, by Mary Anne Simpson

UK based Timesonline reports a flurry of credit card fraud in the first half of 2007. Researchers at Cambridge found chip and PIN merchant terminals lack necessary security encryption. The merchant terminal can be programmed to capture pin and card numbers in order to produce a clone card. The programming takes only 10 minutes.

As reported by Timesonline recently, the popular use of chip and PIN cards has a fraudster in the mix. A merchant can program a chip and PIN terminal to capture all the information needed to create a clone card including the PIN number. Researchers from the Computer Laboratory at Cambridge who conducted the investigation found the vulnerability in the device. There are several reported instances, including an incident at a Shell garage.

The apparent vulnerability of the merchant terminals involves the manufacturer´s failure to build in the necessary encryption technology into the device. The specific encryption required is absent from the present terminal model. Thus, the card runs through the device unproteced.

APACS, the UK payment association in charge of the introduction of the chip and PIN technology acknowledged the possibility cited by the Cambridge researchers. An APACS spokesman stated, "We´re not denying this type of fraud is achievable, but there are easier ways of achieving the same type of fraud, including skimming cards and capturing the PIN using a pin-hole camera." This type of fraud is the

current focus of APACS.

In January, 2008 Visa announced that all new cards issued would include a new chip-based technology called "ICVV". The technology is designed to alert banks and merchants when a clone card is being used for products or services. Unfortunately, not all banks have made the new cards available to customers.

According to the Cambridge researchers, the problem with the chip and PIN cards is systemic. According to Saar Drimer, one of the Cambridge researchers part of the problem is that lack of an independent evaluation device´s security technology. In fact, GCHQ a govenmental and industry comprised security group confirmed it had not certified the card system technology.

ASPACS says it tested the security of the device utilizing internationally accepted standards called the "Common Criteria." Further stating that other secure devices are tested using these same standards.

The manufacturer of the terminal device, Ingenico disputed the ease in which the device can be manipulated. Stating in pertinent part, " the method ... requires specialist knowledge and has inherent technical difficulties ... and not reproducible on a large scale."

Be that as it may, ASPACS reports losses resulting from credit card fraud rose 26 percent in the first half of 2007. The monetary loss is 263.6 million GBP.