Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:1

Mr Geoff Swan
XTec Inc. (Australia)
Level 9, 123 Epping Road
NORTH RYDE NSW 2113
☎02 8875 7861 02 8875 7777
E-mail: gswan@xtec.com

XTec Incorporated (Australia)
Level 9, 123 Epping Road
North Ryde
NSW 2113
Australia

Tel: +61 2 8875 7861
Fax: +61 2 8875 7777
Cell: 0412 887 322

www.xtec.com

PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

CYBERCRIME INQUIRY

SUBMISSION FROM XTEC INC (AUSTRALIA)

Author: Geoff Swan (General Manager – XTec (Australia))
Authorisation Level: CEO, XTec Inc, Miami, FL, USA

BACKGROUND: XTEC INC

XTec Inc head office is located in Miami, Florida, USA with offices in Reston, Virginia and Sydney, Australia. XTec is involved in many areas of security with the US Government. XTec also develops of tools and techniques, in conjunction with the United States Secret Service-Financial Crimes Division, for the generation of evidence from confiscated skimmers and other electronic fraud devices. One such tool is the Skimmer Downloader, capable of downloading the skimmed credit card information from recovered skimmers.

Whilst the technology is assisting card issuers and law enforcement bodies with the capturing and presentation of evidence required to prosecute, XTec is aware that the level of sophistication of skimmer devices will eventually increase to the point where the extraction of evidential data from the confiscated device will be too time consuming and costly. To counter this eventuality, whose timeframe may be as short as 12-24 months, XTec is recommending the protection of the card base in use by the various issuers. XTec is one of several providers of technologies to accomplish this.

CARD SKIMMING DEVICES

(images courtesy of USSS eLibrary)

Hand-Held Skimmers

These types of devices are appearing in a multitude of different forms across the globe. Whilst many of these devices are relatively crudely hand-assembled (ie small volume manufacture) several have recently appeared which are obviously mass produced (ie batches of 100 or more at a time). This type of battery-operated device typically has a magnetic stripe reader together with some form of electronic processing, storage and communication mechanism. A user swipes a card through the reader and the card details are captured. The information is later downloaded or extracted using other hardware/software for this purpose.

Miniature hand-held skimmer (Japan)

Hand-held skimmer (Canada)

ATM Skimmers

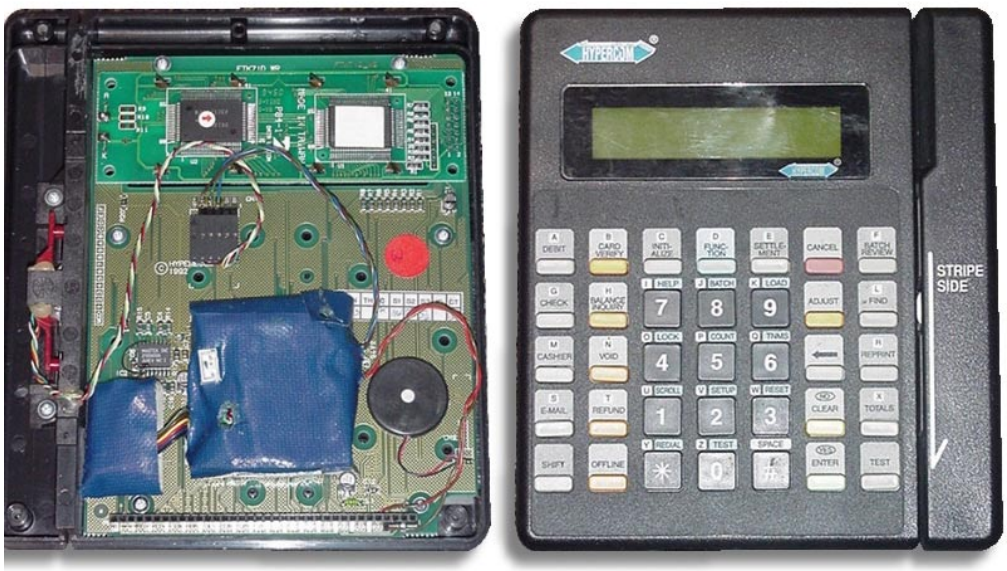
These types of devices are attached to the face of an ATM, either capturing or relaying the card data (wireless transmitter) as it passes through the card slot of the machine.

The cardholder's PIN is captured using techniques ranging from miniature wireless cameras mounted on or near the machine, long-range video cameras, over-the shoulder viewing to the attachment of a thin membrane keypad over the top of the existing PIN pad to directly capture the PIN as it is entered.

ATM skimmer (UK)
Inset shows card skimmer attached in front of machine card slot.

Modified POS Skimmers

The modified-POS skimmer incorporates the electronics or software required to capture and download card details and PIN numbers within an ordinary-looking POS terminal. This type of fraud can range from genuine merchants capturing the card/PIN data to shop fronts set up specifically for this purpose. Several modified-POS skimmers have been captured and data successfully extracted from it.



Modified POS skimmer (Japan). Captures data internally for later retrieval

SECURING THE EXISTING CARD BASE

It is our opinion that magnetic stripe cards will continue to be in use in the financial transaction markets for at least another 10-20 years. Reasons for this include the very

low cost (relative to other cards such as smart cards and contactless cards) and the huge amount of infrastructure in place to accommodate them. The card base is re-issued approximately every 2-3 years and the card reader/terminal base approximately every 5-10 years. One effective mechanism to dramatically reduce the instances of fraud currently being experienced in Australia and other countries is to secure the secure the cards themselves against duplication and alteration.

Duplicate (Counterfeit) Cards

XTec produces technology (Mediametrics) that enables the entire existing and future magnetic stripe card base to be secured against duplication or alteration. This does, however, require that the card reader/terminal base be upgraded gradually to be able to recognise and reject counterfeit cards. When included in terminals that handle the new smart cards and contactless tokens this will be a formidable step in dramatically reducing the instance of fraud involving duplicate cards.

Card Not Present Fraud

In the instance when the card is used remotely from the merchant, a mechanism for authenticating the card (and in some cases the card holder) is required. Several online mechanisms have been developed for use with Internet transactions, however they do not protect the remote offline transaction (eg telephone payments). One possible solution is a small hand-held swipe reader (looks like a skimmer with a display) that produces a series of numbers when the card holder swipes their card through it. These numbers can be entered (via keyboard for Internet transactions or telephone keypad for remote offline transactions) and are used at the host end to authenticate the card. XTec has developed these for use with its Mediametrics protected magnetic card system. It is possible to protect the existing magnetic stripe card base in this manner.

SECURING THE FUTURE CARD BASE

Given the widespread proliferation of magnetic stripe card systems, the introduction of smart cards for financial transactions will need to support access to the legacy system. In most cases this involves the inclusion of a magnetic stripe on the back of the smart card. Unless this magnetic stripe is secured against duplication, the fraud issues will remain similar. When the chip on the smart card is damaged the system commonly reverts to using the magnetic stripe, which could easily be a counterfeit.

It is likely that those card issuers that cannot justify the relatively large increase in card cost between magnetic stripe and smart cards will remain with a magnetic stripe card base. It is important that a mechanism to prevent fraud be available to the smaller issuers using magnetic stripe technology.