Detecting Fraud at the ATM

Significant losses resulting from fraudulent activity at ATMs due to manipulation of the device are a problem for banks and ATM operators worldwide. Apart from the direct financial losses incurred by the organization there are also operational and even reputational issues to address. While Wincor Nixdorf continues to develop new tools and add-ons to ATMs and Self-Service devices to enable the detection and/or prevention of such attacks, fraudsters are constantly changing their methods of attack to exploit any weaknesses in existing systems and of course attacking devices that do not have security protection devices implemented.

We have featured our IRIS fraud monitoring and prevention product in this magazine before in its deployment for identifying fraudulent use of cards but we are now looking at deploying the product for identifying misuse at ATMs. We are now taking the functionality from the product used to detect card fraud from the patterns of card usage and applying it to detecting fraudulent activity at ATMs by looking at the behavior of the device.

The way it detects fraudulent activity at ATMs is based on monitoring event and transaction messages from the device and identifying fraud from known sequences, patterns or data values of these messages. This is done by sending transaction and event messages along with related data to IRIS online, in real time. IRIS is configured to process new attributes related to ATM device processing (event and status data) and to establish multiple rules that will be designed to identify specific fraud attacks based on the sequence of messages, type of message and data values. On identifying a fraudulent event, IRIS will respond to the originating system with an action such as to decline the transaction or maybe capture the card and to raise an alert to allow an active response to the threat to be initiated.

So what type of fraudulent activity are we looking to detect using IRIS? There are basically two categories that we are targeting; the first is associated with device manipulation and the second looking at suspicious activity associated with card transaction activity.

**ATM Manipulation**

In the first case, significant losses are due to ”Transaction Reversal Fraud” (TRF) which has been a problem for many years. This type of fraud involves the manipulation of the device to sense that due to a blockage that cash has not been dispensed at a point in the withdrawal process where the cash can be physically accessed by the criminal. As the device has been unable to complete the withdrawal the transaction request amount is reversed (and thereby the available limit is not changed), allowing the criminal to repeat this deception.

In addition to TRF, other cases include card and cash trapping, where a device is inserted into the card reader that prevents the card from being returned to the customer. When the customer leaves the ATM to get help then the criminal will remove the trapping device (e.g. Lebanese Loop) and retrieve the card. Often the PIN number has been acquired in the attack (shoulder surfed or maybe a camera on the ATM), allowing the criminal to use this stolen card (with valid EMV data) at other ATMs or at POS.

Again, the ATM detects the problem and reports this through sensor events. It would be possible for the card to be blocked by IRIS for subsequent usage at the banks ATMs and blocked generally for on-us cards to prevent further usage of the card.
KYC – Know Your Cash-point

The second category of defense is designed to monitor activity at devices and detect suspicious transaction patterns. Examples of these types of fraud are out of hour’s attack where a criminal will have a pack of skimmed and stolen cards and will use these, one after another to see what cards can be used to withdraw cash. Typically this type of attack is made at a time and/or location where the unusual behavior of a criminal making multiple transactions would not normally be noticed and reported.

So why use IRIS for this type of device monitoring and fraud detection? It is of course possible to identify the pattern of transactions and events associated with any of the above cases and provide a suitable response in the device control system. In fact all ATM vendors do address these issues to resolve these problems but the problem is that fraud attacks have one common characteristic; they change all the time. Typically as soon as one attack is solved by the ATM vendor, then the method of attack is changed. As the method of the attacks can typically be identified by the sequence of events reported by the ATM, an approach allowing the setting of online rules to identify sequences of events (and customer transactions) has been adopted.

As the type and sequence of these events can vary according to various parameters – such as ATM vendor, ATM model, attack type etc., and all of these will vary over time, the solution must be based on a product that allows the setting of these rules based on a flexible configuration which can be changed easily and rapidly in the event of change. The solution must also be able to generate different responses and alerts according to the type of fraud attack detected. The detection of these attacks through the analysis of events must be made online to enable these losses to be stopped. Finally it should be considered that the monitoring of large ATM networks may require the solution to be able to process high volumes of these event messages in real time.

For further information, please click here or send an email to: utrecht.hq@wincor-nixdorf.com

Wincor Nixdorf is acknowledged as one of the world’s leading providers of IT solutions and services for retail banks and retailers. Providing hardware, software, and IT services, we assist both industries in managing changes to their business processes, particularly those that interface with the consumer.