UNDERSTANDING TERMINAL MANIPULATION AT THE POINT OF SALE

One of the best places to obtain unnoticed access to card data plus PIN and ultimately access to clean money can be at the point of sale (POS). Whether acting independently, or in collusion with a merchant, criminals are developing an in-depth understanding of the function and vulnerabilities of many of the terminals deployed today — and they're working around the clock to exploit that knowledge and commit fraud.

In 2008, more than 280 million account details were compromised. This resulted in the re-sale price of account data falling dramatically. However, when track 2 data including the PIN was compromised, the price remained high.

Terminal Fraud – Defeating the Security of Terminals

The one thing you can be certain of is that criminals are focused on exploiting the weakest link in any layer of the transaction environment. They almost invariably seek out the least challenging route to easy money. Unfortunately, they are also very clever, or they have access to people who are very clever.

Indeed, history proves that the criminal will target the terminal that is easiest to get into. For example, in the United States, fuel pumps are among the easiest and most attractive targets because of their location — they sit in the open often unattended and typically have very high transaction volume. Generally, there is only one key which will unlock every pump and grant access to the payment terminal hardware, and the physical security surrounding the pay at the pump is poor at best.

Once a criminal has access, investigators familiar with this type of attack report that it only takes crooks about 30 seconds to remove the entire card device from a gas pump and replace it with an identical one fitted with electronic skimmers.

Given the potential for obtaining large amounts of cash through an effective terminal manipulation scheme, organized crime is attracting some very clever minds with the lure of easy money. Individuals capable of understanding the operation and hardening of a payment terminal can identify vulnerabilities and develop effective, low-cost attack methods for use in the field by a criminal network. Once the best means of exploitation is developed, the criminal in many instances has the network and resources to very quickly and efficiently deploy this attack on a very large scale across regions and around the world.

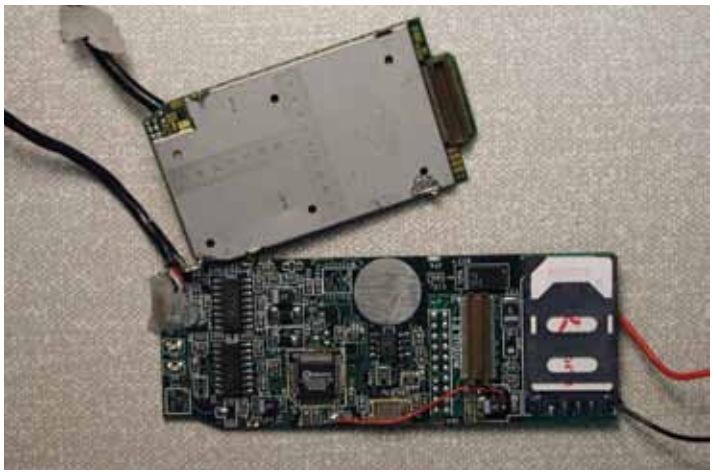
In recent times, there has been an increasing trend for criminals to target the dominant terminal in a particular marketplace. Recent mergers in the terminal manufacturing industry, where there are now significantly fewer companies offering only a limited number of terminals, have made attacks of this nature even more dangerous. If the criminals can learn to defeat the security of a particular terminal, then they will be able to use this information to attack many terminals, regardless of where it is located around the world.

Types of Attacks

MasterCard's experience investigating compromised terminals has shown that the most common method of attack is to obtain a single terminal and use this terminal to learn about all of its security features. The terminal can either be stolen or obtained through legal means such as online auction sites. On any given day, there are over 5,000 terminals available for auction online.

Once the criminal has learned how to defeat the security mechanisms of a particular terminal, they will move on to target terminals installed at a merchant location. Stealing a live terminal, compromising that terminal, and then returning it to the merchant location, or even another location (experience has shown that in some regions, poor controls mean that terminals will often work in different locations, and even different merchants) is a very effective means of obtaining card data. Of course, adherence to accepted terminal management best practices should prevent a device from functioning anywhere but at the location from which it was removed.

The type of skimmer used has also been evolving over the years, with the current skimming devices using wireless networking technology, such as Bluetooth or GSM, to transmit the data from the terminal to the criminal. Some criminals are even encrypting stolen data and sending it outside the merchant network to servers located in countries where it is difficult, if not impossible, to trace.



GSM Skimmer

MasterCard's Role

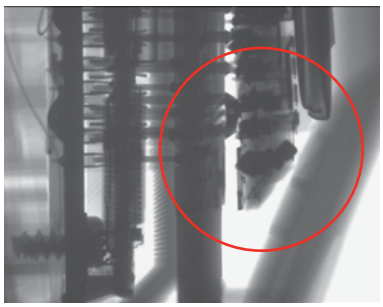
The MasterCard Analysis Laboratory was established more than 10 years ago to investigate card security. In recent years, it has also focused on identifying and understanding attacks against terminals. Working with police forces throughout the world and using a wide range of state-of-the-art equipment along with extensive engineering expertise, MasterCard's laboratory has successfully analyzed many compromised terminals.

A critical starting point for any evaluation is the real-time x-ray which allows images of the inside of the terminal to be taken without even needing to remove the terminal from the evidence bag, thus ensuring the integrity of any DNA evidence. This allows MasterCard to see if the terminal contains a skimming device or not.

From there, MasterCard will work to determine if the skimmer contains any actual card data, essential for any prosecution, and what methods were used to transmit the data. It will also investigate to the greatest extent possible where the data was transmitted to allow investigators to target additional entities involved in the illegal distribution and receipt of stolen payment card data.

Much of this information is provided to specialist police crime units for ongoing investigations.

MasterCard Analysis Laboratory regularly conducts forensic analysis of manipulated terminals



Added circuit board identified via x-ray analysis

Moneris SOLUTIONS

Case Study

Mitigating POS PIN Pad tampering and skimming attacks at Quick Service Restaurants (QSRs)

Author

Moneris Solutions | **www.moneris.com**

Background

The QSR sector has become a prime target for POS terminal tampering and skimming based on the following factors:

- National QSR chains have virtually identical payment configurations in each location
- Franchises in metropolitan areas typically have high payment card volumes
- Most establishments have multiple service lanes and POS devices are left unattended during non-peak periods
- Extended hours of operation usually coincide with reduced staffing levels
- New employees are not aware of the indicators associated with tampering or skimming activities

Solution

After conducting a comprehensive review of skimming and tampering techniques that fraudsters used against a Moneris QSR client, Moneris recommended a layered device security approach that encompassed both physical security solutions and process-related best practices. Per Moneris' recommended mitigation strategies, its QSR client implemented the following actions:

- Strategic replacement of stands with tethers and the storage of POS devices when they are not being used
- A security seal applied to POS devices to indicate possible tampering
- Management training on how to perform POS device integrity checks and serial number verifications
- An incentive-based education program for front-line employees that teaches them how to identify both common POS device skimming activities and if a POS terminal has been tampered with or is a decoy

Outcome

Following the implementation POS fraud mitigation strategies, the QSR customer determined:

- Device theft dropped 42 percent in one year
- Tampering losses decreased 26 percent in one year, with an estimated savings of more than $2 million
- Employees identified multiple decoy devices following the launch of the incentive program

POS Tampering is Everyone's Problem

MasterCard, as a member of the Payment Card Industry Security Standards Council (PCI SSC), is working hard at tackling this problem. From a terminal security perspective, this is through the PIN Transaction Security Requirements (PCI PTS).

This standard, which impacts new POS terminals, was updated in 2009 such that it is not only difficult to defeat the security of the PIN entry Point of Interaction (POI) device the first time, but each and every time. The standard also provides the opportunity for fuel pump and other unattended terminal manufacturers to submit their devices for evaluation.

Terminal manufacturers must continually improve the security of their terminals, but merchants also must realize that they have an important role to play.

To help, the PCI SSC has also released Skimming Prevention-Best Practices for Merchants, a guide on how to prevent skimming attacks against their terminals in merchant locations.

Issuing banks can help by continuing to implement a comprehensive set of fraud fighting tools that enable the early detection of fraud with effective transaction monitoring techniques. For those regions that have migrated or are migrating to chip and PIN authentication, issuers should ensure that they utilize the latest secure chips being offered by the industry and by adopting the use of Combined Dynamic Data Authentication which not only ensures that the PIN is never handled in clear text, but also prevents man-in-the-middle wedge attacks.

Acquirers can help by ensuring that their merchants use terminals certified to meet the requirements of the latest version of the PCI PTS program. In addition, they should develop programs to provide support and training on how to protect terminals at the merchant location, and how to identify signs of tampering or the addition of skimmers.

This is a never-ending race, yet by working together and adopting the above best practices we can ensure that terminal manipulation becomes a much less inviting target for organized criminals.