PAPER:

DIVING INTO MAGNETIC STRIPE CARD SKIMMING DEVICES

By **Johnny Bengtsson**

This paper provides an introduction to the technology in respect of magnetic stripe cards, magnetic stripe card readers, skimming devices and personal identification number (PIN) keypads.[1] The author proposes four main categories of magnetic stripe skimmers, based on observations and electronic device examinations at the Swedish National Laboratory of Forensic Science – SKL.

Background

Magnetic stripe cards, or magstripe cards, have been a part of our everyday lives for decades; prepaid cards, membership cards, loyalty cards, identification cards, library cards, time cards, key cards and access control cards are only a few examples. The physical possession of a magstripe card is not necessary. The true value lies in the specific data stored on the magnetic strip of the card. This becomes extraordinarily clear when considering fuel cards or financial transaction cards, and probably explains the existence of magnetic stripe card skimming devices, more known as skimmers.

Designing magstripe skimmers is not traditionally a field of research, more a peripheral phenomenon. There are innumerable articles and web pages that describes magnetic stripe card frauds and different types of skimmers, but no publications that provides a high quality forensic examination. Masters and Turner generally describe a case where a MSR500M (Mini123) magnetic stripe reader from Escan Technologies Corporation is repacked to a skimmer,[2] Ramsbrock attacks an access control system at University of Maryland[3] and Drimer attacks Ingenico i3300 and Dione Xtreme PIN entry devices and point out the vulnerabilities.[4]

The magnetic stripe card

The physical card size, embossment, recording techniques, magnetic stripe coercivity, recording capacity and density, data formats and encoding of magnetic stripe (or magstripe) cards are some of the properties defined by the standards ISO/IEC 7810 to 7813. Briefly, the magnetic stripe is an analogue data carrier – similar to the audio cassette tape. The magstripe can hold up to three separate audio tracks, where each track has its own data storage format and predefined maximum data length. Cards meeting the ISO/IEC 7811 standard are encoded in the two-frequency coherent-phase encoding (F/2F) technique, also known as Aiken Biphase. This encoding embeds the magstripe card data with the mandatory clock pulse used as a timing signal for the synchronisation of data as the card is swiped. Briefly, a logic '1' has a frequency doubled to a logic 'o', hence the name 'F/2F'.

The specifications for the track data differs for each track, which in turn effects storage capacity. Track 1 (IATA) has a recording density of 210 bits per inch, and uses a character set of 7 bits (6 bits plus one parity bit), and stores up to 79 alphanumeric characters. Track 2 (ABA), 75 bits per inch, 4+1 bits per character and 40 numeric characters. Track 3 (Thrift) is defined to keep 210 bits per inch. Historically, the ISO/IEC 4909 track 3 banking card specific standard defined an encoding of 4+1 bits per character and 107 numeric characters. Today, the ISO/IEC 7811 standard is also used for track 3 (6+1 bits characters).

Most financial transactions only need the card information on track 2. This has the following structure: a number of leading zeroes before the start sentinel (SS), the primary account number (PAN), a field separator (FS), additional data followed by discretionary data, an end sentinel (ES), a longitudinal redundancy

[1] *For a list of other types of attack and cases before courts across the world, see Stephen Mason, general editor, Electronic Evidence: Disclosure, Discovery & Admissibility, (LexisNexis Butterworths, 2007), 4.04 – 4.15.*

[2] *Gerry Masters and Philip Turner, 'Forensic data recovery and examination of magnetic swipe card cloning devices', Digital Investigation, Volume 4S (2007), S16 – S22 and http://www.dfrws.org/2007/proceedings/p16-masters.pdf.*

[3] *Daniel Ramsbrock, Stepan Moskovochenko and Cristopher Conroy, University of Maryland, College Park, 'Magnetic Swipe Card System Security', 2006, http://www.cs.umd.edu/~jkatz/THESES/ramsbrock.pdf.*

[4] *Saar Drimer, Steven J. Murdoch and Ross Anderson, 'Thinking inside the box: system-level failures of tamper proofing', Technical Report, UCAM-CL-TR-711, February 2008, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf.*

check (LRC) character used as a control checksum and finally a series of ending zeroes. Track 1 is similar to track 2, but has an addition field containing the name of the card holder.

Magnetic stripe card readers

The magnetic stripe card reader (MSR) is used for reading magstripe cards, or more specifically, to decode and transfer the analogue content recorded on the stripe into a digital representation. MSRs with writing capability are also able to alter information on a specific track by overwriting previously stored data. Adequate software is often required for interpretation or for editing the data.

Reading the data

Several steps are carried out when a magstripe card is swiped through a card reader. The magnetic head reads a specific track and registers its magnetic flux, which induces a proportional voltage signal, representing the F/2F encoded data stored on the magstripe. The voltage signal is passed into an amplifier to boost the signal; waveform adjustments and noise filtering might also be performed to make a better distinction between a logic '0' and logic '1'. The data in analogue format is converted into digital format by an analogue to digital converter (A/D converter or ADC), where the output data is clocked into a F/2F decoder for clock pulse signal and the separation of the data to be held on the card. The decoded magstripe data can now be utilised, in that it can be transferred to another function or interpreted into a meaningful representation.

The F/2F decoder chip

The steps described in the reading process are almost always carried out by a dedicated magnetic stripe decoder chip, or F/2F decoder IC (an integrated circuit), designed for amplifying the signal, adjusting the waveform, A/D conversion and F/2F decoding. The output signals from most F/2F decoder ICs are similar or the same: a card load signal for swiping the card, and the stream of extracted binary data and a clock pulse or strobe signal for stream synchronisation. Some of the output signals might be active low, which practically means that the signals must be inverted before utilising them.

Multitrack F/2F decoders are integrated circuits with an ability to decode two or three tracks in parallel. These decoders are often used together with multitrack magnetic heads, where each head has its own pair of signal lines to register track specific positive and negative induced voltage levels, but share a common ground signal.

Other magnetic stripe card reader features

The programmable microprocessor control unit, or microchip, are found in most magnetic stripe card readers. The integrated microprocessor control unit functions are developed to coordinate the data flow between the F/2F decoder and any peripheral hardware, such as physical connectors or non-volatile memory, and may also have functions to interpret the F/2F output, bidirectional reading, timekeeping, encryption, and such like. Some MSRs may use a PIN to prevent the unauthorised retrieval of data.

A non-volatile memory, for example an electrically erasable programmable read-only memory (EEPROM) or a flash memory, is often used in systems where synchronisation of data is needed, such as monetary transactions. The memory organises the magstripe card data in slots or posts, often with additional information such as time stamps or the amount of payment. The non-volatile memory is either integrated into the microprocessor control unit, or in memory integrated circuit, and soldered on to the printed circuit board. Some magnetic stripe card readers may also use a separate real time clock circuit to provide accurate timestamps.

Magnetic stripe card reader products

Many magnetic stripe card reader products only act as portable or handheld standalone magstripe readers, but the majority of the MSRs are integrated into or embedded in some sort of system, such as point-of-sale terminals, automated teller machines (ATM) or petrol pumps. All of these require a permanent or a temporary communication link between the host, such as the computer, transaction system or a database query server, and the specific magnetic stripe card reader integrated system for the synchronisation of electronic monetary transactions, to validate the card holder, or for controlling access.

Online, semi-online and offline

Many MSR integrated systems have the capability to interact against an on-line host for real-time operations, such as key card access system or ATMs. If the host accidentally disconnects, the magnetic stripe card reader has the capability to retain unprocessed card data in a non-volatile memory for synchronisation at a

later time. Card access systems are probably excluded, because of the need for instant verification. Semi-online MSR integrated systems connect to a host when appropriate; via a GSM modem, land based telephone line, low-frequency RF, Bluetooth or on any other communication product. Many point of sale terminals, car park ticket machines, and self-service kiosk systems are examples of semi-online MSR systems. Offline or standalone magnetic stripe card readers are portable or handheld devices, commonly used by retailers, merchants, restaurants, and taxi companies, with little or no possibility of interacting regularly online. These MSRs are equipped with a non-volatile memory for the purpose of storing the data from a card temporarily. The retrieval of the data is carried out via a data communication interface, and often protected by a PIN.

Other features

Most magnetic stripe card reader integrated systems have their own method of security to prevent tampering, such as alarm triggers or intrusion detection functions. The security mechanism is often integrated on the printed circuit board. To increase the security and to protect the data stored on the magstripe card from unauthorised use, a PIN is often required for the purposes of verification of the card holder. This is entered on a PIN keypad device or on a PIN entry device. The latter is used together with or integrated in the point of sale terminal.

Magnetic stripe card skimming devices

A magnetic stripe card skimming device – a magstripe skimmer, in short, a skimmer – can technically be described as a device with a concealed circuitry or mechanism engineered in such a way as to duplicate the data on the magstripe card.

Four skimming device categories

Based on experiences and observations at SKL, skimming devices can roughly be divided into four main categories, which are proposed as follows: unmodified commercial or commodity off-the-shelf (COTS) MSRs, modified COTS MSRs, COTS MSR hardware based skimmers and uniquely engineered skimmers.

1. Unmodified COTS magnetic stripe card readers are plain MSRs with the ability to store the data from the card. An unmodified COTS MSR is not really a skimmer, but can be used in the same way.
2. Modified COTS magnetic stripe card readers are devices that have been tampered with in some way. Some extra electronics is added to skim data. Common targets are point of sale terminals and petrol pumps, where employees or technical designs unintentionally allow the unauthorised opening of cabinets or the interception of terminal housings. In such cases, security switches and alarm triggers have been bypassed or disabled.
3. COTS magnetic stripe card reader hardware based skimmers consist of electronic parts from one or more dismantled COTS MSRs. In simpler cases, all the parts originate from the same source. The attacker does not necessarily need to understand how the architecture of the MSR, providing the electronic components are put together in the correct order. In more complicated cases, parts are taken from different magnetic stripe card reader products and integrated within its circuitry. Making these types of skimmers saves time, compared to skimmers that are uniquely engineered.
4. Uniquely engineered skimmers are designed and built individually. There is a great difference in quality between poorly constructed devices to pure masterpieces. Generally, the smaller design, the harder it is to reverse engineer it.

General technical description of skimmers

Some of the earliest skimming devices observed in Sweden were COTS MSR hardware based skimmers, encapsulated in fake slot-in readers and attached onto ATMs. The more advanced contained recordable MP3 players embedded in homemade ATM panels. Each time a magstripe card was put into the slot, the MP3 player recorded the analogue data on the magnetic stripe – typically track 2. In the most likely scenario, after the skimmer was removed, the audio file was decoded in the same way as for regular magnetic stripe card readers.

The majority of skimmers seen at the time of writing are equipped with a microprocessor control unit and a physical interface for retrieving the data stored on the magstripe. A number of significant features are integrated into the microprocessor control unit or represented by discrete components, such as a memory integrated circuit for storing data, a battery or battery pack for running the skimming device circuitry, a separate magnetic head for parallel magstripe reading, a F/2F decoder, a clock and date function or a real time clock for the purpose of providing synchronisation between the data skimmed from the card and retrieved, or the PIN obtained surreptitiously in some way, and perhaps an oscillator or a crystal to act as an external

drive for the microprocessor control unit.

Radio frequency communication devices

In some cases, the attacker does not include a non-volatile memory to store the data swiped from the card. Instead, the analogue data signal skimmed from the magnetic head is obtained, and then transferred to a standard commodity off-the-shelf radio frequency transmitter module. A corresponding radio frequency receiver module A/D converts the analogue radio signals and puts the resulting digital data stream into a microprocessor control unit for further processing. It is not possible to secure the card data that has been skimmed if only the transmitting part of the skimming equipment is seized from a crime scene.

There are also skimming devices where a memory to store the data on the magstripe is combined with a frequency receiver transceiver, which listens for polling devices. When a link is established between the skimmer and the polling device, the card data is transmitted to the receiving unit. After completion, the memory is emptied or overwritten by new card data. The COTS radio frequency modules normally operate on one of the unlicensed industrial, scientific and medical radio bands, where the most common centre frequencies are 433, 868, 915 and 2400 MHz. The higher the frequency, the shorter the range. Different COTS transmitters and receivers use different modulation techniques, such as frequency modulation (FM), amplitude modulation (AM) or on-off keying (OOK) modulation.

Skimmers with a Bluetooth radio frequency module using the serial universal asynchronous receiver/transmitter (UART) communication standard have also been examined at SKL. Bluetooth devices do not necessarily require specialised hardware for obtaining card data that is skimmed or stored; a mobile telephone or a laptop equipped with a Bluetooth module and a program for serial communication is sufficient.

Retrieving the PIN

Many magnetic stripe reader integrated systems require a PIN code to validate or confirm the card holder. There are two major technical methods of obtaining the PIN: externally or internally. Concealed pinhole cameras that film the PIN keypad have been found on apparatus such as ATMs and petrol pumps. These cameras send the images of the use of the keypad by wire or wirelessly to a video recording unit, such as a portable multimedia player or a cheap video camera.

External interception between a separate magnetic stripe reader unit and the system is theoretically possible. However, the traffic though the cable may be encrypted, which is often the case for point of sale terminal systems. Such interception has not yet been observed at SKL.

There are internal methods to obtain a PIN where the PIN keypad encapsulation or housing is opened, any possible alarm triggers are disabled, bypassed or removed and the keypad pressings are recorded. Separate wires are soldered on to the original keypad printed circuit board switches, and connected to a recording circuitry. A second method of attack that has been observed is when a separate overlay keypad printed circuit board or keypad membrane is placed in between the original keypad printed circuit board and the rubber keypad.

Discussion

There is no central coordination of magnetic skimming device in Sweden, hence there are no statistics or numbers available about such cases. However, the local police authorities are very aware of skimmers and are, in some situations, also able to retrieve magnetic stripe card data. SKL is specialised in forensic examinations and has a better opportunity to make qualified analyses to extract skimmed data and to reverse engineer electronic devices. One of the most frequent difficulties is the interpretation of raw binary data extracted from non-volatile memories. There is no standard way to define skimmed card data, which in many cases only result in a binary data dump.

Conclusions

Based on the observations and electronic examinations at the Swedish National Laboratory of Forensic Science – SKL, the four main skimming device categories demonstrate the complexity of the methods that can be employed to attach a magnetic stripe card and obtain the PIN.

Johnny Bengtsson is a member of the Computer Forensic group at the Swedish National Laboratory of Forensic Science – SKL. His primary roles are to initiate Research and Development projects within the field of computer forensics, and to examine seized electronic devices.

johnny.bengtsson@skl.police.se

Further references

Asian Identification System Limited, 'AIS-2101/2/3, Single/Dual/Triple Channel F2F Decoder ASIC', http://www.ais-hk.com/en/ and http://www.kiko-s.com/product/catalog/AIS-210x_v1_5_5.pdf

Bradley Dale Brown and Shamir Nizar, 'Magnetic stripe reader', U.S. Patent 6476743, 5 November 2002, http://www.freepatentsonline.com/6476743.pdf

DGA Houston, 'Mag Stripe Encoding', http://www.dgahouston.com/msrdata2.htm

Koninklijke Philips Electronics N.V., Philips Semiconductors, 'AN10307, UART to Bluetooth interfacing', 11 August 2004, http://www.nxp.com/acrobat_download/applicationnotes/AN10307_2.pdf

MagTek, Inc., 'I/O Interface for TTL Magnetic Stripe Readers, Technical Reference Manual (P/N 99875148 Rev-6)', December 2003, http://www.magtek.com/documentation/public/99875148-6.pdf

MagTek, Inc., 'Magnetic Stripe Cards Standards (P/N 99800004 Rev. 1 06/03)', June 2003, http://www.magtek.com/documentation/public/99800004-1.pdf

Renesas Technology Corp., 'M56710FP, F2F Magnetic Stripe Encoding Card Reader' (Rev.2.01), 31 March 2008 http://documentation.renesas.com/eng/products/assp/rej03f0175_m56710fpds.pdf

Helmut Scherzer, IBM, 'Method and apparatus for decoding F2F signals read from a magnetic data carrier', U.S. Patent 5434400, 18 July 1995, http://www.freepatentsonline.com/5434400.pdf

George. R. Steele, 'Decoder for magnetic stripe recording', U.S. Patent 5204513, 20 April 1993, http://www.freepatentsonline.com/5204513.pdf

Swedish National Laboratory of Forensic Science – SKL, 'SKL in English', 2007, http://www.polisen.se/inter/nodeid=12348750&pageversion=1.jsp

Uniform Industrial Corp., 'Specification for MRD531B, Triple Channel F2F Decoder IC' (Revision A), 5 June 2002, http://www.unitone.com.br/arquivos/f2f.pdf