Digital Investigation 11 (2014) 143–153

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Payment card forensic analysis: From concepts to desktop and mobile analysis tools

T. Souvignet [a], [b], *, J. Hatin [c], F. Maqua [a], D. Tesniere [c], P. Léger [c], R. Hormière [d]

[a] Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110, Rosny-Sous-Bois, France
[b] PRES Sorbonne Universités – Université Panthéon-Assas Paris II, 12 place de Panthéon, 75005, Paris Cedex 05, France
[c] ENSICAEN, 6 boulevard maréchal Juin, 14050, Caen Cedex 4, France
[d] INSA Lyon, 20 avenue Albert Einstein, 69100, Villeurbanne, France

ARTICLE INFO

Article history:
Received 21 February 2014
Received in revised form 26 June 2014
Accepted 27 June 2014
Available online 16 July 2014

Keywords:
Payment card fraud
Skimming
Carding
Forensic tool
Payment card analysis

ABSTRACT

While one would not even consider them alike, payment cards are one of the most valuable and widely used embedded systems. Payment card systems are probably the most attacked and counterfeited. In fact, even though the use of smart cards have introduced high security capabilities, criminal activity has not been deterred and payment card fraud remains a lucrative activity.

From low-tech (carding) to high-tech (man in the middle attack) fraud, all payment card based frauds require stealing or modifying card data and reusing it with a direct profit. Physical forms of fraud, such as Automated Teller Machine (ATM) withdrawals or in store payments, are mostly based on and associated with manipulated cards. Through their nefarious actions, that may include overwriting the magnetic strip data or injecting attacks on the embedded microcontroller, criminals are able to realise significant monetary gains. To effectively deal with these fraud cases, investigators have to quickly determine whether a card is authentic or a counterfeit. Currently no known easy forensic tool exists that provides a quick effective and accurate response.

In this article, after having conceptualised payment cards as multi-interface embedded systems, we propose simple and fast forensic analysis methods to finally provide investigators with associated desktop and mobile forensic tools.

Introduction

Payment cards represent the most used non-cash means of payment, surpassing wire transfers and bank cheques, due to the extra protections they afford (The UK Cards Association, 2014; Comité Consultatif du Secteur Financier, 2011). The total number of payment cards issued in the EU in 2011 reached 726906710 and the value of legitimate non-cash associated transactions within the region exceeded 3000 billion euros (Europol, 2012).

To support such a large volume and value, payment cards are no longer just a simple plastic card with an account number, nor a simple magnetic stripe card. Since the end of the 20th century, payment cards are smart cards, with an Integrated Circuit (IC) moulded in the card plastic. According to Eurosmart (Eurosmart, 2013), more than 1.5 billion payment smart cards will be shipped in 2014, which will make payment cards one of the most widely distributed embedded systems.

* Corresponding author. Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110, Rosny-Sous-Bois, France.

E-mail addresses: thomas.souvignet@gendarmerie.interieur.gouv.fr, thomas@souvignet.net (T. Souvignet), julien.hatin@ecole.ensicaen.fr (J. Hatin), fabrice.maqua@gendarmerie.interieur.gouv.fr (F. Maqua), damien.tesniere@ecole.ensicaen.fr (D. Tesniere), pierre.leger@ecole.ensicaen.fr (P. Léger), romain.hormiere@insa-lyon.fr (R. Hormière).

http://dx.doi.org/10.1016/j.diin.2014.06.006
1742-2876/© 2014 Elsevier Ltd. All rights reserved.

Due to the associated ease of use and fast money they represent, payment cards are attractive items for organised criminal groups. In response, Law Enforcement Agencies (LEA) have had to develop investigative and forensic analysis methods to fight payment card fraud. It is paramount that LEA continue these efforts to address the escalating threat to the global banking industry.

Payment card related fraud

According to Europol (Europol, 2012), payment card fraud reaches around 1.5 billion euros per year in Europe. It is also a profitable activity for organised criminal groups which develop and exploit every possible form of this crime. Essentially, all of the alleged and associated activities are based on a two step crime: first obtain the payment card data, and then use it.

Even if no serious studies have been conducted to provide a formal link between each form of data theft and each form of data usage, likely due to the complexity of this task, it is commonly admitted that payment card fraud can be classified into 2 main categories:

- Card Not Present (CNP) or online frauds, where data comes from payment card breaches, phishing, or malware;
- physical fraud, where data originates from lost and stolen cards, skimming, shimming,[1] man in the middle attacks, Automated Teller Machine (ATM) reverse engineering, etc.

Most of the complaints are due to skimming, that consists of stealing payment card details and Personal Identification Numbers (PIN) against cardholder vigilance. Stolen data is then reused to make counterfeit cards, known as carding. These cards are then used at ATMs to withdraw money or at shops to buy goods.

Investigating such complaints requires the investigators to fully understand payment card mechanisms and to be able to detect if a card is genuine or counterfeit.

Payment cards

In order to simplify payment card understanding and integrity analysis, we propose to consider payment cards as multi-interface embedded systems that contain both static and dynamic data.

Nowadays payment card characteristics, mostly based on ISO 7813 (International Organization for Standardization, 2006b) and EMV standards (EMV book 1, 2011; EMV book 2, 2011; EMV book 3, 2011; EMV book 4, 2011; EMV book D, 2013), can be defined by 4 interfaces:

- visual interface;
- magnetic stripe interface;
- IC contact interface;
- IC contactless interface.

Visual interface

The first and most obvious interface of every card is its visual one. The visual interface is much more standardised than might be expected. The following ISO standards define this interface:

- ISO 7810 defines the plastic card physical characteristics with ID1 dimensions;
- ISO 7811 defines location of “identification number line” and “name and address area”, and characteristics of readable characters (International Organization for Standardization, 2002a);
- ISO 7811 also defines location of magnetic stripes (International Organization for Standardization, 2002b, 2008a, 2008b);
- ISO 7812-1 defines the PAN format (International Organization for Standardization, 2006a);
- ISO 7816 defines location of the contacts (International Organization for Standardization, 2004).

Payment card visual interface is thus easily characterised and the following elements can be found on Fig. 1:

1. Primary Account Number (PAN)
2. Cardholder name
3. Expiration date
4. Payment authority logo
5. Card not present payment verification code (CVV/CVC)
6. Manufacturer serial number
7. Cardholder signature
8. Holograms and UV securities

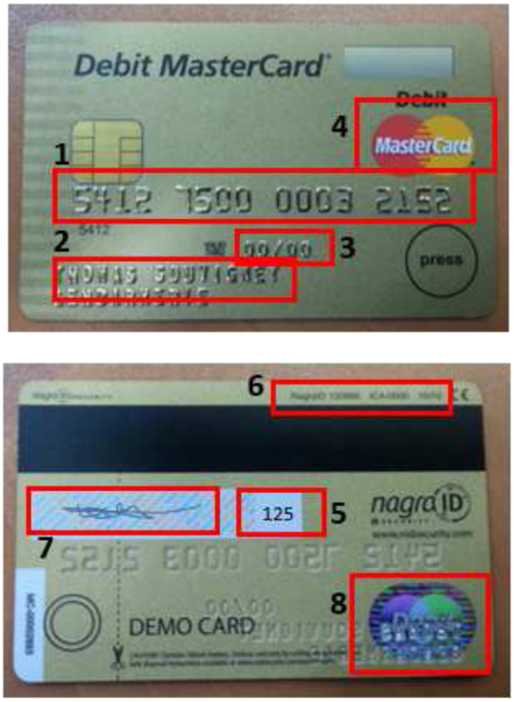

Fig. 1. Payment card visual interface.

[1] Skimming applied to chip-terminal transactions.