Digital Investigation 11 (2014) 154–159

Contents lists available at ScienceDirect

Digital Investigation

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

Case study: From embedded system analysis to embedded system based investigator tools

T. Souvignet [a, b, *], T. Prüfer [c], J. Frinken [c], R. Kricsanowits [c]

[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] Kriminaltechnisches Institut (KTI) des Bundeskriminalamtes (BKA), Äppelallee 45, 65173 Wiesbaden, Germany

ARTICLE INFO

Article history:
Received 21 February 2014
Received in revised form 7 June 2014
Accepted 13 June 2014
Available online 5 July 2014

Keywords:
Skimming
Embedded systems
Payment card fraud
Forensic tools
Bluetooth forensics
Arduino
Android

ABSTRACT

Since mid-2012, France and Germany have had to deal with a new form of payment card skimming. This fraud consists of adding a wireless embedded system into a point-of-sale payment terminal with the fraudulent goal of collecting payment card data and personal identification numbers (PIN).

This case study details the strategy adopted to conduct the digital forensic examination of these skimmers. Advanced technologies and analyses were necessary to reveal the skimmed data and provide useful information to investigators for their cross-case analysis.

To go further than a typical digital forensic examination, developments based on embedded systems were made to help investigators find compromised payment terminals and identify criminals.

Finally, this case study provides possible reactive and proactive new roles for forensic experts in combating payment card fraud.

Introduction

Europol estimates payment card fraud proceeds of approximately 1.5 billion euros per year (Europol, 2012). This fraud is thus a profitable means for organised crime groups that invest in technical skills to enhance their modus operandi and increase their rewards.

One of the types of payment card fraud is skimming, with the aim of collecting payment card data contained in the magnetic stripe and PIN codes despite cardholder vigilance. Technically speaking, skimming is based on purpose built embedded systems, called skimmers, which are designed to collect several analog signals from the standard magnetic read head, as well as video record PIN entry surreptitiously.

Over the last few years, experts in France and Germany have seen the evolution of skimmer internals from raw signal storage to state-of-the art encryption usage (Souvignet and Frinken, 2013). Forensic analysis techniques have had to follow that evolution, resulting in advanced analysis methods that are currently in place.

In order to fully demonstrate the complexity of a basic embedded system analysis, this case study first describes the strategy adopted to analyse a new type of skimming fraud based on manipulated point-of-sale (POS) payment terminals. Further efforts by police researchers to develop embedded systems to counter the criminal efforts are explained, with the goal of assisting investigators in detecting fraudulent activities to help tackle this lucrative fraud.

* 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.net, thomas.souvignet@gendarmerie.interieur.gouv.fr (T. Souvignet), thomas.pruefer@bka.bund.de (T. Prüfer), juergen.frinken@bka.bund.de (J. Frinken), ralf.kricsanowits@bka.bund.de (R. Kricsanowits).

http://dx.doi.org/10.1016/j.diin.2014.06.004
1742-2876/

As some investigations and court trials may still be ongoing, only the minimal information necessary to illustrate the case study will be disclosed, with some data anonymised for confidentiality.

Context

In mid-2012, French investigators had to face a new form of skimming as POS payment terminals were manipulated by inserting an electronic system (Le Parisien, 2013). It was believed that Germany was also targeted by this fraud; however, German investigators had already faced a similar type of fraud in the past (NDR 1, 2013).

Differences in POS terminal fraud between countries can easily be explained by comparing national payment scheme regulations. In France, all payment acquirers must comply with Anti Fishing-Anti Skimming (AFAS) standards imposed by Cartes Bancaires, the French national system. Cartes Bancaires requires POS terminals to use separate insertion slots for magnetic stripe and smartcard chip payments. Combined with the requirement to prevent full insertion of the card while managing chip payments, the French standard tends to prevent skimming involving an illegitimate magnetic reading head on POS terminals. Such requirements seem to not be in place in Germany where all-in-one slot POS terminals are widespread.

The fraud involved modifying POS terminals of various models to add an internal integrated circuit (IC) and installing them in stores by eluding the vigilance of the cashier vigilance. This skimmer circuitry consisted of an additional magnetic read head, the IC connectors, the genuine magnetic read head and some data lines of the terminal, all powered by the terminal power supply itself. Finally, as shown in Fig. 1, the French version of the skimming device required an extension of the legitimate insertion slot to bypass the aforementioned AFAS security mechanisms.

Both French Gendarmerie Nationale Forensic Laboratory (IRCGN) and German Forensic Science Institute (BKA/KT) were asked to conduct the forensic analysis of these fraud related exhibits.

Strategy

The strategy adopted by both agencies was quite traditional. Fully developed in Souvignet and Frinken (2013), it consisted of three stages: black box analysis, white box analysis, and stored data analysis based on the two previous results.

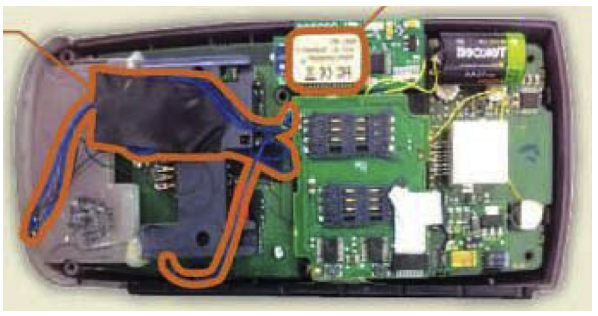

Fig. 1. Skimmer within the manipulated payment terminal (source: Le Parisien, 2013).

Black box analysis

First, the skimmer board was analysed to understand its design and the data stored in the flash memory was checked to determine if it was stored in plaintext or encoded/encrypted.

Visual analysis of the printed circuit board indicated that the skimmer was designed using the following components:

- magnetic read heads,
- double frequency phase coherence (F/2F)[1] application specific intergrated circuit (ASIC) decoder,
- microcontroller (Atmel ATMega640),
- flash memory,
- Bluetooth module (Roving Networks RN41).

This design implied that data storage would be in 7-bit (track 1) or 5-bit (track 2) ISO format and data collection would be completed wirelessly. The researchers were able to collect data wirelessly by providing the default PIN of 1234, as well as read the flash memory directly. Both datasets were found to be identical, indicating that no data manipulation was performed prior to transmitting over the Bluetooth serial interface.

Stored data analysis, however, did not reveal 7-bit or 5-bit ISO formatted data. Further statistical analysis indicated that the data was equally distributed, indicating that encryption was used. Deeper analysis of the encrypted data, particularly redundant areas, indicated that 128-bit electronic codebook encryption (EBC) was used.

White box analysis

Using the process described in (Souvignet and Frinken, 2013), the ATMega640 microcontroller was deprotected using focused ion beam (FIB) (Fig. 2) in order to gain access to the protected assembly program code in the exhibit.

The Atmel AVR assembly code was examined using IDA Pro, ultimately allowing for the identification of the encryption routine. It was found that the encryption used some AES-like substitution and mix columns subroutines, but no known AES constants were found and only three rounds were processed.

The encryption algorithm was then reproduced with a custom Python script and checked with plaintext/ciphertext samples that were produced by simulating the assembly code running within the AVR Studio Simulator. Once the encryption algorithm was verified, it was then possible to successfully design the decryption algorithm and the necessary Python script.

In order to retrieve the last paired Bluetooth devices, the Roving Networks RN41 Bluetooth Module was also

[1] Encoding used for storing data within magnetic tracks.