Chapter 17
Embedded Forensics: An Ongoing Research about SIM/USIM Cards

Antonio Savoldi
University of Brescia, Italy

Paolo Gubian
University of Brescia, Italy

ABSTRACT

This chapter is aimed at introducing SIM and USIM card forensics, which pertains to the Small Scale Digital Device Forensics (SSDDF) (Harril, & Mislan, 2007) field. Particularly, we would like to pinpoint what follows. First, we will introduce the smart card world, giving a sufficiently detailed description regarding the main physical and logical main building blocks. Then we will give a general overview on the extraction of the standard part of the file system. Moreover, we will present an effective methodology to acquire all the observable memory content, that is, the whole set of files which represent the full file system of such devices. Finally, we will discuss some potential cases of data hiding at the file system level, presenting at the same time a detailed and useful procedure used by forensics practitioners to deal with such a problem.

PHYSICAL AND LOGICAL DESCRIPTION OF A SIM/USIM CARD

The purpose of this section is to give an overview on smart cards used in the telecommunications field by detailing the main building blocks, their functions and how they are related to each other. Generally speaking, smart cards belong to the group of identification cards using a ID--1 format formally defined in ISO Standard 7810, *Identification Cards -- Physical Characteristics*. This standard specifies the physical properties, such as mechanical flexibility and temperature resistance, of four types of cards, namely ID--1, used for banking cards such as ATM (Automatic Teller Machine) cards, credit cards, and debit cards; ID--2, prevalently used for identity documents; ID--3, used worldwide for passports and

DOI: 10.4018/978-1-60566-836-9.ch017

Table 1. ISO 7810 specification

Type of Card	Size [mm]	Application field
ID--1	85.60 × 53.98	banking field
ID--2	105 × 74	identity documents
ID--3	125 × 88	passports and visas
ID--000	25 × 15	SIMs/USIMs

visas; and finally, ID--000 used for SIM/USIM cards. In Table 1, some technical details regarding these cards are shown.

As stated in the standard reference, a smart card is the youngest and cleverest member of the family of identification cards in the ID--1 format. Among its features there is an embedded integrated circuit within the card, which is aimed at transmitting, storing and processing data for a specific purpose. The central component for such a pervasive embedded system is undoubtedly the microcontroller, whose main purpose is to control and monitor all the card's activities. Usually, for functional security and reliability reasons, a smart card processor is based on a well known platform, which can be optimized in order to provide the right performance and the appropriate level of system security.

As it can be seen in Figure 1, there are several elements to consider in order to describe a smart card at the functional level. Current state-of-the-art microprocessors usually have a RISC (Reduced Instruction Set Computer) 32 bits architecture with emphasis on the security of the system. For instance, the Atmel AT91SC512384RCT microcontroller (Atmel, 2007) is based on the well known ARM SC 100 secure core (ARM, 2003), with a 32-bit instruction set, a Von Neumann Load/Store architecture, a 3-stage pipeline architecture and data types within the range 8--32 bits. From the memory point of view, it has a 512 Kbytes of ROM program memory, 384 Kbytes of EEPROM, including 256 bytes of *One Time Programming* (OTP) memory, and 24 Kbytes of RAM. Another common platform frequently used in the realm of smart cards is the SmartMIPS architecture (MIPS, 2005). It aims at improving the protection of the system by using cryptographic algorithms such as RSA, DES, AES, and Elliptic Curve.

All modern architectures have common modules. Usually, a OTP area is present in the EEPROM memory and it provides hardware-secured, tamper-proof storage for program memory and security information. Three types of memory are usually present: EEPROM, used for storing the file system and user data, ROM, used for the operating system, and RAM, used for dealing with temporary data. A *Firewall* is an important module whose role is, with the *Memory Management Unit* (MMU), to encapsulate an application in a manner that it cannot access memory areas forbidden to it. To perform calculations in the realm of symmetric and asymmetric cryptographic algorithms, such as RSA, elliptic-curve and DES/3DES, there is a special arithmetic unit capable of performing all the basic operations that are necessary for these types of algorithms, such as exponentiation and modulo calculation which makes use of large numbers, usually up to 2048 bits for the RSA case. A *Java accelerator* module is an hardware component which implements a Java Virtual Machine. This is useful to directly process Java bytecode, thus fastening the execution of Java applications which are becoming more and more used. *Cyclic Redundancy Check* (CRC) is a hardware module specifically used to secure data or programs by means of an error detection code. A *Random Number Generator* (RNG) module provides a safe way to produce truly random numbers used, for instance, for generating keys and authenticating smart cards and terminals. Another important module integrates the hardware for data transmission, which takes