Side-Channel Monitoring of Contactless Java Cards

Janardan Kumar
Student(M.Tech) , CSC,
Gokul Group Of Institutions
Visakhapatnam, India.

K.R.Koteeswa Rao
Asst. Prof, CSC,
Gokul Group Of Institutions
Visakhapatnam, India.

Abstract:

Smart cards are small, portable, tamper-resistant computers used in security- sensitive applications ranging from identi_cation and access control to payment systems. Side-channel attacks, which use clues from timing, power consumption, or even electromagnetic (EM) signals, can compromise the security of these devices and have been an active research area since 1996. Newer contactless" cards communicate using radio frequency (RF), without physical contact.

These contactless smart cards are sometimes grouped with radio frequency identi_cation (RFID) devices in popular usage of the term. This thesis investigates devices that use the ISO 14443 (proximity card) protocol, a large class of contactless/RFID devices. Although contactless smart cards are increasingly common, very few repro- ducible practical attacks have been published. Presently, there are no known documented side-channel attacks against contactless Java Cards (open standard multi-application cards) using generic unmodi_ed hardware.

This thesis develops a research-friendly platform for investigating side-channel attacks on ISO 14443 contactless smart cards. New techniques for measurement and analysis, as well as the _rst fully documented EM side-channel monitoring pro- cedure, are presented for a contactless Java Card. These techniques use unmodi_ed, commercial o_-the-shelf hardware and are both practical and broadly applicable to a wide range of ISO 14443 devices, including many payment cards and electronic passports.

I. Introduction:

Smart cards are an embedded systems technology that are becoming entrenched in the security-conscious computing and business landscape. The smart card is a small plastic card containing an embedded computer system (low-power micropro- cessor, RAM, ROM, EEPROM, and limited I/O). Secure tamper-resistant memory often protects sensitive information on the card, such as private keys for use in cryptographic communications [31]. When used in a bank or credit card, these keys are _nancial in nature.

In GSM mobile phone Subscriber Identi_cation Modules (SIM cards), the card securely stores the subscriber's private identi_cation key used for authentication and identi_cation on the network. In both the bank and SIM cards, the private key is never transmitted outside the card but only used for internal operations. Smart cards are not necessarily required by design to encrypt or otherwise protect communications. However, in practice smart cards regularly use cryptographic algorithms such as DES, DSA, and RSA.

The new applications of contactless devices, notably in payment systems and passports, will undoubtedly attract attention from malicious parties of all kinds. For this reason, it is important to research the weaknesses of contactless systems so that vulnerabilities can be found and corrected. Unlike contactless cards, attacks against contact smart cards are not new. Since Kocher's early _ndings on practical timing [5] and later power analysis [6], a large number of practical attacks have been published against various smart card implementations and algorithms.

These \side-channel attacks" use extra information obtained through a side channel (time, power consumption, electromagnetic emissions), rather than the data channel. Among these attacks, the class of di_erential power analysis attacks [26] have proved to be particularly e_ective and di_cult to protect against, and continue to be a major research area. However, nearly all of these attacks have targeted smart cards with electrical contacts. When it comes to contactless smart cards, there has been surprisingly little published research on side-channel attacks. Even within current published research, there are few (if any) documented details on test and measurement procedures that can be used to repeat and con_rm _ndings.

The objective of this thesis is to develop research-friendly test techniques and contactless measurement methods that can be used with unmodi_ed, commercial o_-the-shelf equipment. The target device in this research is a commonly-used contactless Java Card which can be programmed according to an open speci_cation. It is hoped that this research will open the door for further research into contactless smart card attacks, with less proprietary hurdles than encountered up to now.

II. smart cards:

Smart cards are embedded systems built into a plastic card with a standard form factor, de_ned by ISO 7816 [20]. The smart card includes a low-power microprocessor, RAM, ROM, EEPROM and serial I/O (half-duplex) through either metal contacts or an antenna, in contactless operation.

Typically, smart cards do not include a power source and are powered either through contacts or an electromag- netic _eld. A smart card operates when connected to a card acceptance device, which in this thesis will be called a card reader or reader for short. Hardware implementations of smart cards vary considerably with vendor and microprocessor capabilities, as do programming models and software protocols.

To provide some interoperability, ISO 7816 standardizes some aspects of smart cards, such as the external physical/electrical characteristics and the application-level protocol for data exchange.Figure 2.1: Web server Java SQL architecture 2.3 ISO 14443 Type A ISO 14443 [21] de_nes speci_cations for a class of contactless integrated circuit cards (\proximity cards") which operate at a nominal distance of approximately 10 cm, as opposed to \close coupled" or \vicinity" cards which operate at di_erent distances. ISO 14443 compliant cards may be called RFID cards or contactless smart cards, depending on microprocessor capabilities.

Java Cards are a relatively new type of multi-application smart card that are growing in popularity due to the ease of application development and platform com- patibility. There have been some published attacks, such as using power analysis to reverse engineer applications [38] and theoretical fault attacks [7].

Some recent research describes methods that could be used to launch side-channel attacks [4]. There is ongoing research in our university lab relating to side-channel attacks and countermeasures.

This thesis extends some of the lab techniques introduced by Tiu in her embedded systems side-channel attacks [37]. Gebotys and White have also developed re_nements to DEMA that make the technique usable on more complex Java devices [10].

The devices investigated in this thesis are also Java-based and may share similar characteristics, from an EM attack perspective.

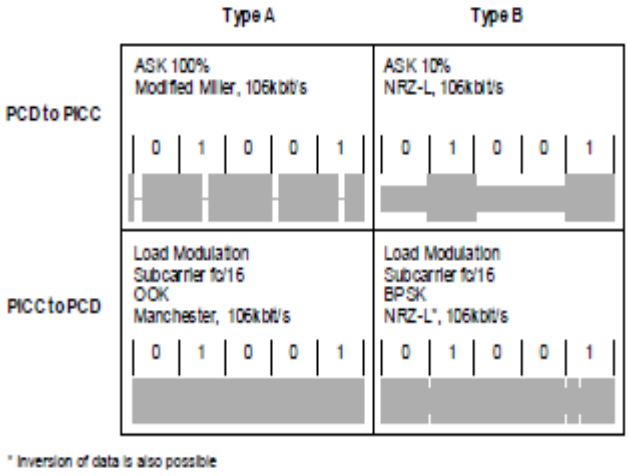

Figure 1: RF Modulated Data (From ISO 14443-2 [21])

The 100% ASK used in the reader-to-card communication is characterized by a pause in the carrier. Since the card is powered by this carrier, the pause must not be too long. Figure 2.4 shows the speci_cations for this pause.

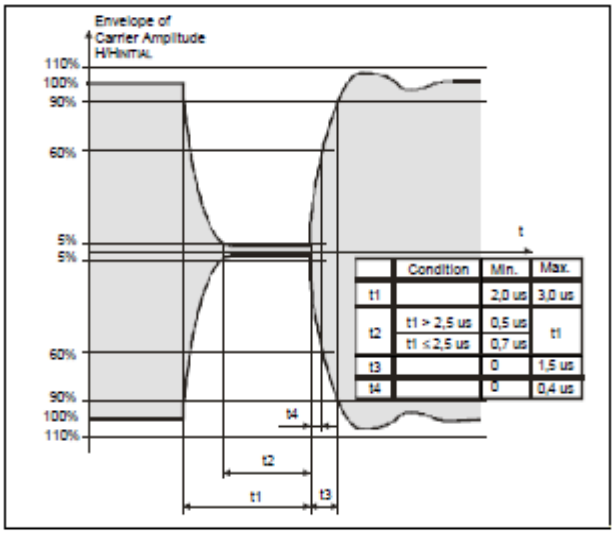

Figure 2 `Pause' in Reader-to-Card Communication

III. SOFTWARE ANALYSIS TOOLKIT (SAT):

3.1 Methodology:

This section introduces the methodology for the investigation into contactless Java Cards and the experiments in this thesis. A considerable amount of laboratory work is required to establish the basic methods and procedures for dealing with contactless Java Cards, since test and measurement procedures in this area have not previously been documented. The required preparations, such as probe con_guration and oscilloscope triggering, are described in the following sections.

The novel con_guration of this test equipment and method for observing the side-channel is it- self one of the thesis contributions. Section 4 then describes further experiments on the contactless Java Cards carried out after the test methods have been established. This thesis aims to investigate the execution of Java Card applets on contactless smart cards from a side-channel perspective.

See Section 2.4 for an introduction to these attacks. In this thesis, only unmodi_ed smart cards are studied so the power analysis (from direct current ow) is ignored as a potential side-channel. Contactless smart cards do not draw power from external wires, and any points which carry measurable current ow are buried beneath the card's surface.

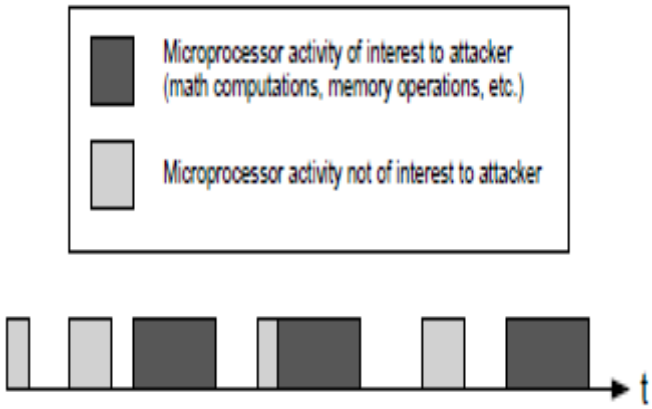

Figure 3 Activity of Microprocessor on Java Card

3.3 EM Probe:

Contactless smart cards are near _eld communication devices, and an antenna placed in the _eld measures the superposition of both the modulated communication and any side-channel emanating from the device's microprocessor(s).

This allows passive observation of the communication channel and any side-channel emanating from the microprocessors on the contactless device. A near _eld EM probe by Electro-Metrics Inc. (Model EM-6992) connected to a pre-ampli_er with typical gain of 22 dB provides the input signal to the digital oscilloscope.

The probe's 1 cm loop antenna is sensitive to H-_eld frequencies from below 100 kHz to 1 GHz.

Figure 3: EM Probe Position, Side

Finding Modulated Communications With the probe positioned for best e_ect and the oscilloscope con_gured appro- priately for viewing ISO 14443 [21] communications, it is now necessary to locate modulated data in order to re_ne the test and measurement techniques needed for further testing. As a starting point, the digital oscilloscope is con_gured for a simple rising edge trigger at 0 V with a 250 ms hold-o_ period before the next trigger. With the digital oscilloscope continually showing captured data (at 250 ms intervals), the contactless smart card is inserted into the card reader's _eld. The presence of the card causes a back and forth initialization communication as per ISO 14443-3. This communication includes both short command and response packets being sent over RF. Because no technique has yet been established to speci_cally capture these communications, the digital oscilloscope's \fast frame" acquisition mode is used as a search tool. Fast frame mode starts capturing many records into memory so that each record can be individually viewed later, as if it was a separate acquisition. Fast frame acquisition is started and then the contactless smart card is manually inserted into the card reader's _eld. Each captured frame (of 250 ms width) is then manually observed from oscilloscope memory, until something other than unmodulated 13.56 MHz carrier is observed.

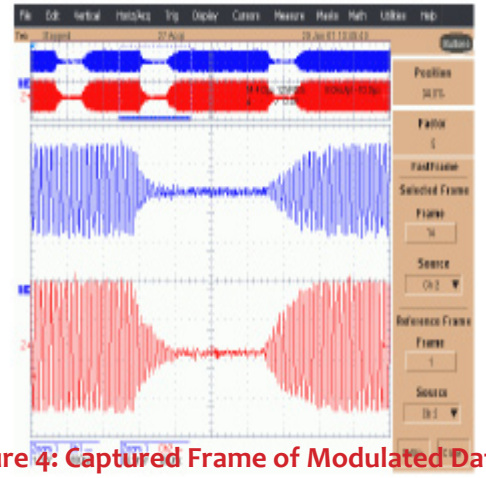

Figure 4: Captured Frame of Modulated Data

Timing Attack Implications Besides validating the EM side-channel observation techniques introduced in this thesis, some of the experiments also imply the feasibility of an EM-based time side- channel attack. In this kind of attack, the attacker measures the execution time 65 of software on the smart card under di_erent conditions and uses di_erences in run-time to draw conclusions about the system (such as a private key). This can be demonstrated using the results from the experiments which per- form di_erent iterations of a mathematical transformation. In the experiments, three di_erent applets perform one, two and three iterations of a simple mathematical transformation. The only di_erence between these applets is the termination condition in a for loop, which determines how many iterations to compute. The results of the experiments show that each additional iteration results in an additional 210 _s \gap" time delay, as described in Section 5.1. The relative processing times are depicted in Figure 5.1 from the perspective of the EM side- channel observation. The \gap" times as measured from di_erent experiments are marked above this timing diagram.

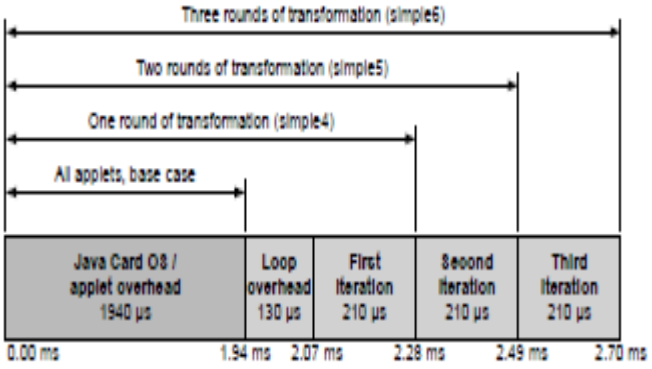

Figure 5.1: Possible Relative Processing Time of Java Card Routines.

Previous research on Java Card attacks ([4, 7, 38]) do not document the physical measurement techniques required to apply such attacks to contactless cards, or indicate whether such attacks are even relevant to the contactless case. In this thesis, contactless cards are speci_cally targeted. Leaving aside the Java Card technology, there is previous research on contact- less device attacks ([12, 16, 23, 24]) but all of these require some sort of custom hardware. The custom devices used in the experiments range from simple low cost electronics which replicate the behaviour of simple RFID tags to fully functional contactless prototypes manufactured with the help of commercial smart card makers. Some researchers describe generic tools that can be used for these kinds of contactless experiments [2]. There have however been practical attacks on contact- less smart cards carried out without custom hardware [3].

Still, such attacks target simpler, single-application smart cards that don't involve additional complications that exist with the Java Cards used in this thesis (see Section 3.2 for a description of these complications).

CONCLUSION:

This work succeeded in developing research-friendly test techniques that can be used with contactless Java Cards for EM-based side-channel analysis. The methods and procedures developed in Section 3 have proved to be usable in a practical environment, at least with the JCOP-type Java Cards used in this research. Throughout this investigation, only open standards were used and knowledge of proprietary hardware or software was not required.

To help monitor the EM side-channel of contactless Java Cards, a method to trigger a standard oscilloscope from an ISO 14443 [21] contactless signal was developed and tested on physical cards. Using this method, one can passively intercept data packets by observing EM signals while the smart card is processing input. For the _rst time, this research shows that it is possible to monitor the EM side-channel of a contactless Java Card using only a standard oscilloscope and unmodi_ed commercial o_-the-shelf equipment, without any card contact or custom hardware.

The timing and communication model introduced in Section 3.1 is believed to be applicable to all ISO 14443 contactless smart cards. The technique for measuring communications and triggering by EM is believed to be applicable to all ISO 14443 RFID devices, although this thesis only experimented with Type A cards.

While far more research is needed to investigate the extent of possible attacks, it is believed that the measurement techniques introduced in this thesis will be applicable to bank/payment cards and electronic passports which are ISO 14443 compliant.

REFERENCES:

[1] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi. The EM Side- Channel(s). In Proceedings of Workshop on Cryptographic Hardware and Em-bedded Systems (CHES 2002), LNCS 2523, pages 29{45. Springer-Verlag, 2002.17, 34, 73.

[2] D. Carluccio, T. Kasper, and C. Paar. Implementation Details of a Multi Purpose ISO 14443 RFID-Tool. In Proceedings of Workshop on RFID and Lightweight Crypto (RFIDSec06), 2006. 18, 68, 69.

[3] D. Carluccio, K. Lemke, and C. Paar. Electromagnetic side channel analysis of a contactless smart card: First results. In Proceedings of Workshop on RFID and Lightweight Crypto (RFIDSec05), 2005. 18, 31, 37, 38, 68, 69.

[4] S. Chaumette, D., and Sauveron. An e_cient and simple way to test the secu-rity of Java Cards. In WOSIS 2005, 3rd International Workshop on Security in Information Systems, April 2005. Miami, Fl., USA, April 2005. 18, 37, 68, 69.

{5] Z. Chen. Java Card Technology for Smart Cards: Architecture and Program- mer's Guide. Addison-Wesley, 2000. 2, 9, 10.

[6] Electro-Metrics Inc. Near Field Probe Set Broadband Response Model EM-6992 Instruction Manual, 2002. Available at http://www.electro-metrics.com/.30.