Contact-Based Fault Injections and Power Analysis on RFID Tags

Michael Hutter, Jörn-Marc Schmidt, and Thomas Plos
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
Email:{Michael.Hutter,Joern-Marc.Schmidt,Thomas.Plos}@iaik.tugraz.at

Abstract—**In the last decade, many articles have been published that demonstrate the susceptibility of cryptographic devices against implementation attacks. Usually, such devices draw their energy from a contact-based power supply. This power-supply connection is often exploited to extract the secret key by applying fault-injection methods and power-analysis attacks. In this article, we present implementation attacks on Radio Frequency Identification (RFID) tags which are usually powered contactlessly by an electromagnetic field. We describe a contact-based measurement setup that allows both injection of faults and measuring of the power consumption of passive RFID tags. Furthermore, we demonstrate the applicability of our setup by providing practical results of attacks on commercially available HF and UHF RFID tags. The results have led us to the conclusion that RFID tags are as susceptible to such attacks as contact-based powered devices. Appropriate countermeasures are needed to thwart these attacks.**

I. INTRODUCTION

Radio Frequency Identification (RFID) is an emerging technology that has gained much attention in the last few years. The possibility to read RFID tags contactlessly and without the need of a line of sight provides great potential for many applications such as supply-chain management, inventory control, electronic passports, and ticketing. In the year 2008, more than one billion of RFID tags have been shipped worldwide and they have been applied in many applications which actually become more and more security related. This article focuses on such security-related RFID tags and its susceptibility to implementation attacks.

RFID tags consist of a small microchip that is attached to an antenna. They are typically powered passively by an electromagnetic field that is generated by an RFID reader. In order to provide an acceptable reading range, tags have to be implemented to operate in low-power conditions. They also have to be designed for a small chip area to minimize the costs for a large scale production. Besides these requirements, further aspects have to be considered if RFID tags are deployed in security-related applications. Many of these objectives are indeed identical to those of embedded smart cards in the 1990s. Large effort has been made by the industry and also by the cryptographic community to meet all the requirements and to overcome several security threats that emerged during that time. One of the first articles in the field of practical attacks on smart cards were published by R. Anderson and M. Kuhn [1], [2] in the mid 1990s. They injected glitches in the clock signal and induced spikes in the power-supply line

of a smart card. They showed that these induced faults can manipulate the internal memory of the device. D. Boneh et al. [3] presented theoretical attacks on RSA and on different identification schemes using fault attacks in 1997. In the same year, E. Biham and A. Shamir presented a theoretical fault attack on the Data Encryption Standard (DES) [4]. Next to fault attacks, which manipulate the internal state of a device by active means, there exist powerful techniques that exploit the physical characteristics of cryptographic devices by passively measuring their power consumption. P. Kocher et al. [5] introduced differential power analysis (DPA) attacks in 1998 and showed how to extract secret information from a set of measured power-consumption traces of smart cards. Nowadays, smart cards are successfully employed in many security-related applications that need appropriate countermeasures to thwart these kind of attacks [6].

The same attacks that have been performed on smart cards in the mid 1990s, have also been conducted on RFID devices recently. Y. Oren and A. Shamir [7] have been the first who demonstrated the vulnerability of power-analysis attacks on ultra-high frequency (UHF) tags in 2006. The same susceptibility of UHF tags has been shown by T. Plos [8] in 2008. Hutter et al. [9], [10] performed successfully attacks on high-frequency (HF) RFID tags and showed that RFID tags are also vulnerable to various fault attacks. They induced optical and electromagnetic fault attacks and applied an antenna tearing technique that caused faults during the writing of data into the tag memory.

In this paper, we present a new fault attack on RFID tags by injecting over-voltage spikes into commercially available RFID tags. For this attack, we used a proper measurement setup that allows the tags to be powered over a contact-based connection with the reader. We present results of fault attacks causing the tags to write faulty values into the internal memory. Furthermore, we present first results of contact-based power analysis attacks on RFID tags. All attacks have been performed successfully. The results emphasize the need of appropriate countermeasures for RFID tags if they are applied in security-related applications.

The remainder of this article is structured as follows: Section II presents the contact-based measurement setup that is used for fault injections and power-analysis attacks. Section III describes the performed attacks on the HF and the UHF RFID tags. In Section IV, the results of our experiments are given
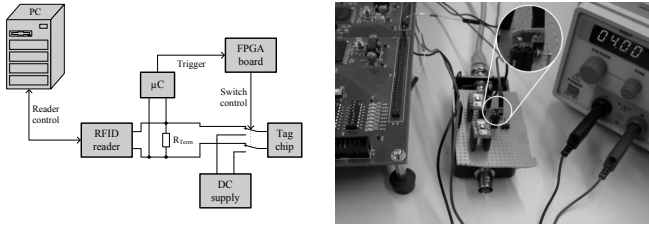
(a) Schematic view of the fault-injection setup

(b) The FPGA board (left), the tag chip (middle), and the DC power supply (right)

Fig. 1. Measurement setup for injecting over-voltage spikes in HF and UHF RFID tags.

(a) Schematic view of the DPA measurement setup

(b) The tag chip, the measurement resistor, and the differential probe that measures the power consumption

Fig. 2. Measurement setup for power-analysis attacks on HF and UHF RFID tags.

and discussed. Conclusions are drawn in Section V.

II. CONTACT-BASED MEASUREMENT SETUP

In order to perform fault injections and power-analysis attacks on RFID tags, we used a contact-based measurement setup. This setup is advantageous due to several reasons. First, tag and reader are directly connected by two wires and they are not coupled over an electromagnetic field. This allows contact-based fault injections like over-voltage spikes and power-consumption measurements by simply measuring the voltage drop across a resistor. Equipments such as electromagnetic probes and receivers are therefore not needed. This makes the setup more attractive in terms of costs. Second, the reproducibility of fault-injection techniques and side-channel measurements is increased in a contact-based setup compared to an electromagnetic-coupled measurement setup. Electromagnetic-coupled systems are often interfered by the proximity and the measured electromagnetic traces are expected to be more inhomogeneous than the results obtained from power measurements over a wire.

In the following, we first describe the measurement setup that has been used to perform fault attacks on RFID. Second, we describe the setup used for power-analysis attacks.

A. Fault-Injection Measurement Setup

The measurement setup for fault injections is composed of several components: a measurement PC, an RFID reader, an impedance-matching resistor, an HF or a UHF tag, a microcontroller with an analog front-end, an FPGA board, a DC power-supply, and two high-speed multiplexers. A schematic view of the measurement setup is shown in Figure 1(a).

Matlab, which runs on the PC, is used to control the overall measurement process. For HF tags, the PC is connected to a standard ISO 15693 compatible RFID reader. For UHF tags, an ISO 18000-6C compatible RFID reader is used. Both readers are connected to the PC over a serial interface. The reader is then connected to a 50 Ohm impedance-matching resistor that is used to match the impedance of the reader antenna-output. The tag is connected in parallel to the matching resistor over a two wire cable. For this, the tag has been separated from its antenna and the antenna pads of the tag have been soldered on a two-pin strip. The antenna output of the reader
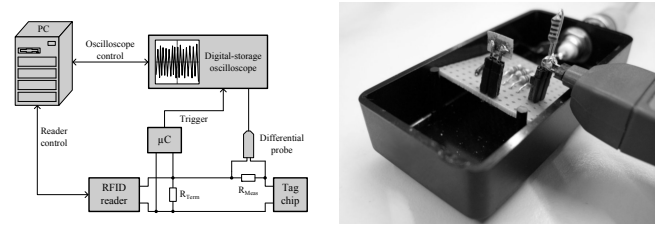
is further connected to an analog front-end that is connected to the microcontroller. The analog front-end consists of a fast envelope detector that is used to transform the analog signal of the reader into digital signals for the microcontroller. We have used an 8-bit ATmega128 microcontroller from Atmel. It provides 128 kB of Flash memory and allows easy interaction with other components by providing 53 customizable I/O pins. The microcontroller was programmed to set a dedicated output pin as soon as a write command is received. This signal is then fed into an FPGA board that is able to generate signals of very short duration. We have used the Side-Channel Attack Standard Evaluation Board (SASEBO) that features two Xilinx VirtexTM-II Pro devices. One FPGA device has been programmed to concurrently control two *ISL54200* high-speed multiplexers. The multiplexers are used to connect the tag to either the reader or the DC power supply. If the multiplexers are activated, the tag is no longer powered by the reader and an over-voltage spike is injected into the antenna-pad connections that causes the tag to perform faulty operations. A picture of the tag chip and the surrounding components such as the FPGA board and the DC power supply is depicted in Figure 1(b).

B. Power-Consumption Measurement Setup

A schematic of the measurement setup for contact-based power-analysis attacks on RFID tags is shown in Figure 2(a). It is composed of the following components: a PC, an RFID reader, an HF or a UHF tag, a microcontroller with an analog front-end, a digital oscilloscope, a differential probe, an impedance-matching resistor, and a measurement resistor. The reader is again connected to a 50 Ohm impedance-matching resistor like in the setup described before. Furthermore, the tag is connected in parallel to the matching resistor. For the HF tag, a 100 Ohm measurement resistor is placed between the tag and the matching resistor. The consumed power of the tag is then simply measured over this resistor using an active 1 GHz differential probe (AP034 from LeCroy). For the UHF tag, the resistor was removed so that the tag current flows over the internal 0.1 pF capacitor of the differential probe. This is because the capacitor becomes conductive at high frequencies. The voltage drop across the inputs of the differential probe is captured by an 8-bit digital oscilloscope which has a 1 GHz

bandwidth (LC584AM from LeCroy). The trigger signal has been generated by the same microcontroller that has been used in the fault-injection experiment. It sets an output pin to high when a write command has been received. The target of all attacks has been the writing of data into the internal memory of the tag. In Figure 2(b), a picture of the DPA measurement setup is given. It shows the tag chip, the measurement resistor, and the differential probe that is used to measure the voltage drop across the resistor which corresponds to the consumed power of the tag.
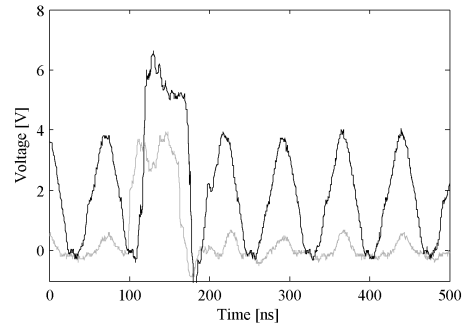

Fig. 3. Injection of an over-voltage spike during the writing of data into the tag memory. The injected spike is drawn in black, the trigger signal is drawn in gray.

III. DESCRIPTION OF THE ATTACKS

The fault-injection attack has been performed as follows. First, a Matlab script is started on the PC that initializes all components and sends a write command to the reader. The reader transmits the command to both the corresponding tag (HF or UHF) and the analog front-end that is connected to the microcontroller. After that, the microcontroller enables the FPGA that has been configured to activate the multiplexers after a certain period of time. This time constitutes the exact fault-injection time and can be controlled by the PC. The multiplexers are then activated for a fixed period of time (i.e. about 80 ns in our experiments). During this time, the tag is decoupled from the reader signal and an over-voltage spike is injected into the antenna connections of the tag. Therefore, a DC power supply is used that delivers a constant voltage of 4 V. After injection, the multiplexers are deactivated and the tag is again reconnected to the reader.

The FPGA is configured to run at 120 MHz, which allows us to produce spikes in steps of about 9 ns. The fault-injection occurrence can be varied by the PC and can go up to several microseconds.

The power-analysis attacks are conducted in the following way. A Matlab script, which runs on the PC, generates random input data. A write command sends the input data to both the tag and the analog front-end that is connected to the microcontroller. After that, the microcontroller generates a trigger signal which forces the oscilloscope to start the acquisition of data. For all experiments, we have used a sampling rate of 100 MS/s and measured the power consumption during the time between the occurrence of the trigger signal and the sending of the tag response. The measured power traces are than transferred to the PC and further processed using Matlab.

IV. RESULTS

In the following, we present results obtained from our experiments. First, we give results of the performed fault-injection attacks. Second, the results of power-analysis attacks are described.

A. Fault Attacks using Spikes

We injected an over-voltage spike during the writing of data into the internal memory of the tag. First, the tag receives the data from the reader and deletes the content of the current memory block. Second, it writes the new data. After each writing operation, the tag sends an acknowledge message to the reader or returns an error message if the writing has not succeeded. In our experiments, we focused therefore on the time between the last write-command sequence (end of frame) of the reader and the sending of the tag response. This time period takes some hundred microseconds depending on the tag manufacturer. By using the FPGA board, we have been able to sweep over this time and to accurately inject spikes in steps of 9 ns. In Figure 3, the injection of an over-voltage spike into an HF RFID tag is shown. The injected spike is drawn in black and the trigger signal of the FPGA board is drawn in gray. The trigger signal has been high for about 80 ns, which actually corresponds to the time of one clock period of a 13.56 MHz carrier signal. The black signal in the figure has been obtained by measuring the voltage on the tag connections using the differential probe. It can be seen that the signal, which effectively goes from about -4 to 4 V, is clipped by the two multiplexers resulting in a signal that contains only the positive component. After a trigger event (which starts in the figure at 100 ns), the DC voltage is injected which can be observed by a higher signal going up to about 7 V. The injected voltage causes the tag to perform a reset during the writing of data. Thus, the writing process got incomplete and an incorrect value is written into the memory of the tag. In our experiments, we analyzed several RFID tags that showed the same behavior, i.e. faulty values are written into the internal memory of the tags.

B. Power-Analysis Attacks

For the power-analysis attacks, we have taken both an HF and a UHF RFID tag and measured a set of power traces. Afterwards, we applied several post-processing techniques. First, we applied filtering techniques in order to remove the carrier of the reader signal. We calculated the envelope signal by taking the absolute values of the traces and by applying a 2 MHz low-pass filter afterwards. This largely removes the reader-signal component that interfered the measurement of the very weak side-channel signals of the tags. Second, we aligned all traces in vertical and horizontal orientation.

The target of the power-analysis attack has been an 8-bit value that was written into the internal memory of the tag.
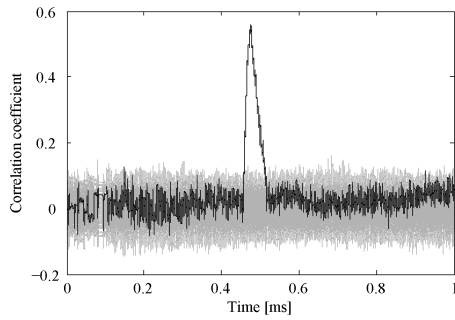
Fig. 4. Result of the DPA attack on a UHF RFID tag. The correct key hypothesis is drawn in black, incorrect hypotheses are drawn in gray.

The power consumption during the time when the value is processed and stored into the memory was measured using the oscilloscope. 1 000 power traces have been recorded for the HF and the UHF RFID tag. The attack was performed as follows. First, we measured the consumed power of the tag during the processing of the input value. Next to the measured power traces, we constructed a model that takes the same input values as they were written into the tag memory. For each possible input value (i.e. 256 possible values for an 8-bit input), the power consumption of the tag was estimated by using an appropriate power model. The output of this model is than correlated with the physically measured power traces using the Pearson correlation coefficient. The correct hypothesis shows a peak in time when the input value is processed by the tag. Incorrect hypotheses provide no peak [11].

All performed attacks have been successful and revealed the value that was written into the tag memory. The processed input value was successfully revealed for both HF and UHF RFID tags. In Figure 4, the result of a DPA attack that was performed on a UHF RFID tag is shown. The correct hypothesis is drawn in black. It leads to a correlation coefficient of 0.56. A peak can be clearly discerned after about 480 ns. The incorrect hypotheses are drawn in gray and show no significant correlation over the data-processing time of the tag.

V. CONCLUSION

This article presents first results of contact-based fault-injection techniques and power-analysis attacks on commercially available RFID tags. Both HF and UHF tags have been analyzed. A measurement setup was used that establishes a contact-based connection between the tag and the reader. Using this setup, we first injected over-voltage spikes into the tags during the writing of data. This caused tags to write faulty values into their internal memory. Second, we performed classical DPA attacks by measuring the power consumption of the tags over a simple resistor. All performed attacks have been successful and have been performed with low-cost equipment.

Future work will be to analyze the effectiveness of other contact-based fault-injection techniques like glitches. The setup also allows the combination of fault-injection techniques and power-analysis attacks on RFID devices.

The results of our practical investigations emphasize the need of appropriate countermeasures for RFID tags against fault and power-analysis attacks and demonstrate the effectiveness of such attacks on this emerging wireless technology.

REFERENCES

[1] R. J. Anderson and M. G. Kuhn, "Tamper Resistance - a Cautionary Note," in *Second Usenix Workshop on Electronic Commerce*, November 1996, pp. 1–11.

[2] ——, "Low Cost Attacks on Tamper Resistant Devices," in *Security Protocols, 5th International Workshop*, ser. Lecture Notes in Computer Science, M. L. et al. Ed., vol. 1361. Springer, 1997, pp. 125–136.

[3] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract)," in *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceedings*, ser. Lecture Notes in Computer Science, W. Fumy, Ed., vol. 1233. Springer, 1997, pp. 37–51.

[4] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, ser. Lecture Notes in Computer Science, B. S. K. Jr., Ed., vol. 1294. Springer, 1997, pp. 513–525.

[5] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, ser. Lecture Notes in Computer Science, M. Wiener, Ed., vol. 1666. Springer, 1999, pp. 388–397.

[6] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards," in *USENIX Workshop on Smartcard Technology (Smartcard '99)*, May 1999, pp. 151–162.

[7] Y. Oren and A. Shamir, "Remote Power Analysis of RFID Tags," Master's thesis, Weizmann Institute of Science, Rehovot, Israel, August 2006, further information on http://www.wisdom.weizmann.ac.il/~yossio/rfid/. [Online]. Available: http://eprint.iacr.org/2007/330.pdf

[8] T. Plos, "Susceptibility of UHF RFID Tags to Electromagnetic Analysis," in *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008, Proceedings*, ser. Lecture Notes in Computer Science, T. Malkin, Ed., vol. 4964. Springer, April 2008, pp. 288–300. [Online]. Available: http://www.springerlink.com/content/l5n71111404317t6/fulltext.pdf

[9] M. Hutter, S. Mangard, and M. Feldhofer, "Power and EM Attacks on Passive 13.56 MHz RFID Devices," in *Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, ser. Lecture Notes in Computer Science, P. Paillier and I. Verbauwhede, Eds., vol. 4727. Springer, September 2007, pp. 320–333. [Online]. Available: http://www.springerlink.com/content/n27q456qhr34818k/fulltext.pdf

[10] M. Hutter, J.-M. Schmidt, and T. Plos, "RFID and its Vulnerability to Faults," in *Cryptographic Hardware and Embedded Systems – CHES 2008, 10th International Workshop, Washington DC, USA, August 10-13, 2008, Proceedings*, ser. Lecture Notes in Computer Science, E. Oswald and P. Rohatgi, Eds., vol. 5154. Springer, August 2008, pp. 363–379. [Online]. Available: http://www.springerlink.com/content/rm23vg1071355423/

[11] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks – Revealing the Secrets of Smart Cards*. Springer, 2007, iSBN 978-0-387-30857-9. [Online]. Available: http://www.dpabook.org