Brief Contributions

Remote Password Extraction from RFID Tags

Yossef Oren and Adi Shamir

Abstract—Side-channel attacks are used by cryptanalysts to compromise the implementation of secure systems. One very powerful class of side-channel attacks is power analysis, which tries to extract cryptographic keys and passwords by examining the power consumption of a device. We examine the applicability of this threat to electromagnetically coupled RFID tags. Compared to standard power analysis attacks, our attack is unique in that it requires no physical contact with the device under attack. Power analysis can be carried out even if both the tag and the attacker are passive and transmit no data, making the attack very hard to detect. As a proof of concept, we describe a password extraction attack on Class 1 Generation 1 EPC tags. We also show how the privacy of Class 1 Generation 2 tags can be compromised by this attack. Finally, we examine possible modifications to the tag and its RF front end which help protect against power analysis attacks.

Index Terms—RFID, cryptanalysis, power analysis, side-channel attacks.

1 Introduction

Passive RFID tags have recently been making gains both in their capabilities and in their planned applications. The regulatory bodies behind the tag standards are aware of security and privacy issues and urge tag makers to make their tags as secure as possible [15]. There are indications that RFID tags will soon implement full-fledged cryptographic functionality. The threat model under which RFID tags are designed to be secure is based on an adversary who is able to listen to communications between tag and reader but does not have physical access to the tag. Security countermeasures such as cover coding and even secret key encryption [13] have been planned and deployed to address this scenario.

We present a new attack on RFID tags which we call the *parasitic backscatter attack*. Our attack is basically a power analysis attack, comprising a method of measuring the power consumed by a tag as it performs a computation. It is unique when compared to classical power analysis attacks in that it does not require either tag or reader to be physically touched by the attacker. By making use of the fact that the tag is powered by the reader's electromagnetic field, we are able to measure the tag's power consumption unintrusively and at a distance. We show how this attack compromises both the security and privacy aspects of RFID tags, and discuss how it can be prevented.

The paper will start with a short description of the electrical characteristics of UHF tags, which are the ones attacked in this paper. We will follow with the theoretical and practical framework of our attack. The paper will then present our results and conclude with a discussion of several countermeasures chip designers can use to protect their tags.

• *The authors are with the Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel 76100. E-mail: {yossi.oren, adi.shamir}@weizmann.ac.il.*

Manuscript received 4 July 2006; revised 14 Dec. 2006; accepted 20 Dec. 2006; published online 3 Apr. 2007.
Recommended for acceptance by V. Gligor.
For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number TC-0262-0706.
Digital Object Identifier no. 10.1109/TC.2007.1050.

1.1 Properties of the UHF Backscatter Channel

As described in [3], UHF readers send data to tags by pulse amplitude modulation of their carrier signal. This signal also provides the tags with power. The tags send data back to the reader via *modulated backscatter*, a technique in which the *backscatter aperture* of a tag is modulated in time, by means of a *switched impedance* connected in parallel to the tag's circuitry, thus changing the amount of power it reflects. As shown in this paper, the tag also *unintentionally* modulates its backscatter in a measurable way via the power consumed by its internal computations.

The relation between the tag's power consumption and the strength of its reflected field can be derived by observing the equivalent circuit of the tag-reader system. As shown in Fig. 1 [4, p. 131], the tag-reader system can be viewed from the point of view of the tag as an alternating voltage source U_0 representing the electromagnetic field falling across the tag's antenna, a complex impedance Z_{E} representing the tag's effective internal loading (consisting of the tag's circuitry in parallel to the aforementioned switched impedance), and another complex impedance Z_{S} representing the signal radiated from the tag antenna. Assuming a *matched circuit*, we can replace the impedances with Ohmic loads marked R_{E} and R_{S}. While R_{S} is generally a constant depending on factors such as the shape of the antenna and the wavelength of the incident signal, R_{E} is a time-varying quantity affected by both the tag's RF front end and by the tag's internal calculations. U_0 is determined by the strength and wavelength of the reader's field and by the properties of the tag's antenna. It is independent of the tag's power consumption (see [4, p. 125] and [3]).

The relation between P_{E} and P_{S} (the power consumption of R_{E} and R_{S}, respectively) is calculated using the standard voltage divider equation:

$$P_{\mathrm{S}}(t) = I(t)^2 R_{\mathrm{S}} = \left(\frac{U_0}{R_{\mathrm{S}} + R_{\mathrm{E}}(t)}\right)^2 \cdot R_{\mathrm{S}}. \quad (1)$$

Solving (1) for R_E, we obtain:

$$R_E(t) = U_0 \sqrt{\frac{R_{\mathrm{S}}}{P_{\mathrm{S}}(t)}} - R_{\mathrm{S}}. \quad (2)$$

Thus, knowing R_{S} and U_0 and measuring P_{S} allows explicit calculation of R_{E}. Assuming U_0 is known and R_s is constant, this gives us a direct way of obtaining the power consumption of the tag by measuring its reflected power.

There are several simplifications that have to be noted at this point. First, we assumed the tag's load is purely Ohmic. This may not be true, but it is certainly a good enough approximation of the *instantaneous* resistance of the tag. Second, we assume U_0 is well known. In fact, U_0 is the time-varying field generated by the reader and may contain noise or undesirable artifacts. Finally, it assumes that we can accurately measure the power reflected from the tag in the presence of the much stronger signal generated by the reader itself. As we will see, these simplifications do not prevent our attack.

The tag's intentional modulation does not disturb our measurements of its unintentional modulation because the tag and reader operate in a half-duplex line regime. Even in the case of a potential full-duplex regime, the tag's intentional backscatter can generally be predicted and eliminated from the traces.

1.2 The Power Analysis Side-Channel Attack

Side channel attacks attempt to compromise secure systems by observing outside information about the way these systems work.

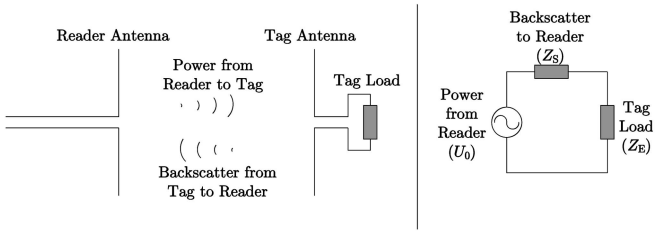

Fig. 1. The reader-tag channel and its equivalent circuit.

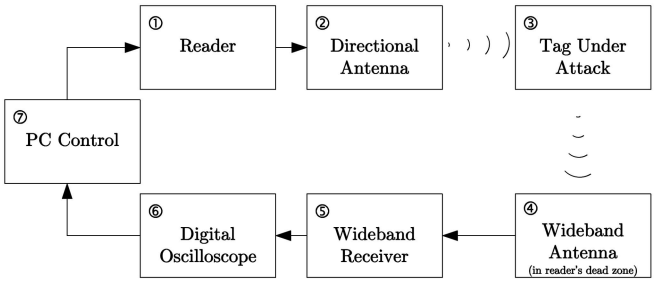

Fig. 2. Block diagram of lab setup.

Even cryptosystems which use provably secure functions may be broken by careful analysis of the auxiliary information they generate, such as instruction timing or EM radiation. Power analysis attacks rely on the fact that registers in modern ICs require more power to transition between states than to remain in the same state. To use this property to discover a password which is sent in bit-serial mode, we note that the first wrong bit decoded by a tag will cause it to perform some additional computations (moving to an error state, resetting its correct bit counter, etc.) and, thus, consume more power. This lets us discover a password in linear time, bit by bit, instead of in exponential time.[1] Power analysis has also been used to attack strong cryptosystems such as RSA and AES. Note that the significance of our attack is not that it can discover the kill password—the limited key space of an EPC tag can easily be covered using exhaustive search.[2] We chose to attack the kill password because it is one of the few secrets kept by today's RFID tags and because power analysis lends itself naturally to this type of attack. In the future, we expect higher-security tags to store more sensitive secrets, such as cryptographic keys, and it will be essential to protect them from this type of attack.

1.3 Previous Work

The capabilities of power analytic attacks were first demonstrated in an academic setting in [7]. There have been many follow-up works exploring both the capabilities of power analysis and the costs involved in preventing them. For a survey of power analysis attacks and some of their countermeasures, see [14]. In [15], the authors suggested that RFID tags may be vulnerable to power analysis and fault attacks, but did not test this prediction.

In [12] and [2], the authors demonstrated a remote attack on cryptographic smart cards using electromagnetic emanations. Our attack is different from the attack in [12] in that it does not monitor the internal electromagnetic emanations of the device under attack, but, rather, presents an indirect way of monitoring its actual power consumption. Our method of attack apparently has better range and more resistance to noise than the attack in [12]. There are also different countermeasures to be employed against these two attacks. On one hand, our attack can be prevented by using modified chips with constant power consumption, while the authors of [12] argue that certain types of power analysis countermeasures will not help against their attack. On the other hand, surrounding the chip at the heart of the tag with EM shielding (without, of course, shielding the antenna) will protect against standard EM attacks but will not protect against our attack.

1. This efficient method of password guessing has its roots in folklore. The first documented use of this attack as a way of guessing passwords in a computing environment was documented in [11, Section 2.1]

2. This assertion is clear in the case of the 8-bit key space of Generation 1 tag, but marginal in the case of Generation 2's 32-bit passwords. Assuming 10 milliseconds per failed kill command, an adversary trying random kill passwords is expected to succeed after only 8 months of attacks. If a group of tags is known to share a kill password, this attack can be carried in parallel using multiple tags and readers, reducing the time it should take to run.

2 Our Attack in Practice

This section will discuss the physical aspects of our attack.

2.1 Lab Setup

The logical view of our lab setup is shown in Fig. 2. A single experiment consisted of sending a kill command (with an incorrect password) from the reader, demodulating the response of the tag using the wideband receiver, capturing the baseband signal using the digital oscilloscope, and, finally, transferring the capture to the PC. The scope was triggered by a specific wave shape rather than by a signal from the PC to better emulate an actual attacker who does not control the reader. Each attack consisted of about 200 experiments and each experiment took about 30 seconds, most of which was spent transferring data from the scope to the PC through a slow RS-232 serial port. This gave us a total time of two hours per attack. Considering the fact that a kill command takes about 10 milliseconds to execute, the net time of each attack (which could be easily achieved with a more integrated attacking device) was only a few seconds.

The digital oscilloscope we used was a Lecroy 9402C, the wideband receiver was an HP 4011B-AYX spectrum analyzer with baseband output, and the RFID reader was a WJ Communications MPR-6000, installed in the PC's PCMCIA slot.

The tags under attack were EPC Class 1 Generation 1 and 2 tags from several vendors [1], [5]. We chose not to name the brands of the RFID tags we attacked since our attack is not vendor specific, and seems to apply to most brands.

After the data has been transferred to the PC, we loaded the samples into Matlab, normalized and aligned them, and, finally, analyzed them both visually and via a suitable program.

2.2 Attack Modes

We attempted several different modes of attack, as described below. In all attacks, we used a cooperating reader to send a series of kill commands with incorrect passwords to the tag under attack. We then used a directional antenna to collect the power reflected over time from the tag, minimizing the effect of power emitted by the reader on our traces by locating the attacker in the reader antenna's null zone.

The most straightforward attack is by **direct observation** of the intercepted signal. The main problem with this attack is an instrumentation problem—the reflected signal has a very large amplitude range, while the digital oscilloscope introduces a measurement error of up to 1 percent of the selected vertical scale. This means that we had to choose between capturing the whole gamut with a high measurement noise or limiting the measurement to part of the vertical scale and risking losing meaningful data. For our attack, it sufficed to look only at the top of the peaks of the original signal.

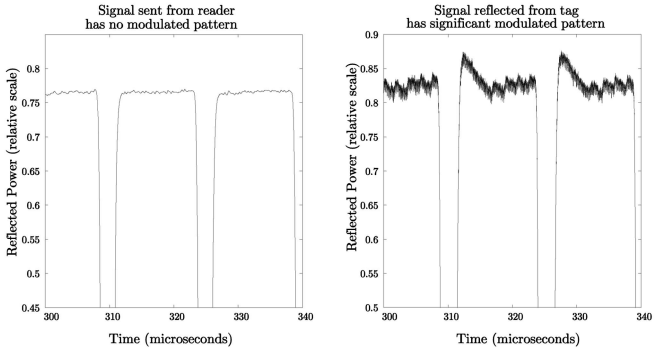

Fig. 3. Generation 1 reader signal versus tag signal.

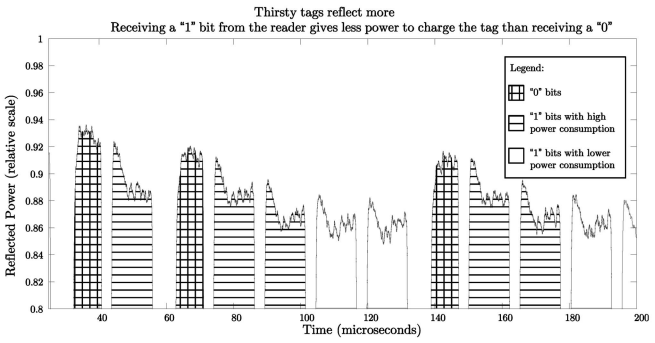

Fig. 4. "Thirsty" tags reflect more.

An alternative setup can use a pair of antennas, one of which is in the reader's field and the other in the reader's null zone. By combining the two signals, we can minimize the effect of the reader's signal. The price to be paid is a multiplicative increase in the amount of measured noise in areas with low reader power. This differential approach can also be emulated using an antenna array and DSP beamforming techniques.

A more advanced attack is the **pulse power attack**. This attack is based on the observation that significant decisions about the correctness of the password are made once per reader bit. The EPC air interface uses pulses of differing widths to differentiate between 1 and 0 symbols and the decoder decision regarding the value of the bit is made at the falling edge, which incidentally comes at a time when the tag is the most charged up. It is reasonable to assume that the computations are then performed at the trough between two consecutive pulses, at which time the tag receives very little power from the reader. We can assume, then, that the tag will attempt to replenish itself during the next pulse it receives and that it would be "thirstier" if it had to flip the values of many bits during the previous trough. Integrating the power consumed by a tag over the period of an entire pulse will then give us an indication of how hard it worked after the previous falling edge. Because it measures over a relatively long period of time, this attack is less sensitive to noise, again at the risk of losing some data. We believe this form of attack is the most easily adaptable to low-cost attack devices.

The final mode of attack is called the **probing attack.** For the probing attack, the setup was augmented with an HP 8530 swept signal generator, configured to send out a sine wave of constant amplitude at 900 MHz. We illuminated the tag with this *probe signal* while performing a normal transaction with a reader tuned to another frequency. If the reader and probe frequencies are set far enough apart, the amplitude of the bounced probe signal will only indicate the power consumption of the tag without including residual data from the reader. This allows us to get a lower dynamic range and thus capture the entire reflected waveform at high vertical accuracy. This attack has the disadvantage of requiring additional equipment and of announcing the presence of the adversary. Our results in this paper do not make use of the added power offered by this attack, although it seems to have practical advantages, especially when looking into time segments with low or unstable reader power.

3 An Attack against Generation 1 Tags

This attack was performed on a major brand Generation 1 tag. The tag was programmed with an ID of $10\cdots0$ and with different kill passwords. To minimize the variability in the experiment, we programmed the reader to always send a kill password of $00_h = 0000000_b$ and an odd parity bit of "1." In all cases shown below, we used the exact same tag in the same physical location, each time programming the tag in a different way. The attacker's antenna was placed in one of the reader's null zones, giving a 27 dB preference to the tag signal as compared to the reader signal. In all of the figures, the X axis represents time while the Y axis represents the relative field strength at the attacker's antenna.

First, Fig. 3 shows the power of the signal sent from the reader, compared to the signal reflected from the tag. Each pulse in this trace represents a single "0" bit, which is detected at the falling edge of the pulse. It is easy to see that, even though it is not supposed to be transmitting anything, the tag is adding unintentional information to the relatively clean signal sent by the reader. We discuss this fact further in Section 4.

Fig. 4 shows the strength of the field reflected by a Generation 1 tag while the reader is sending it "1" and "0" bits. Compared with a "0" bit (shown plain or with light horizontal hatching), a "1" bit (shown with cross-hatching) has a wider gap followed by a narrower pulse [1, p. 12].

Now, examine the wider gap before a "1" bit. As mentioned before, the tag's internal power storage is depleted during these low-power gaps. At the end of the long gap which forms the beginning of the "1" bit, the tag's power supply is relatively low. This makes it draw more power from the next pulse it receives. As the tag consumes more power, it radiates a stronger reflected field, as shown in the cross-hatched pulses. As the tag receives more "0" bits, it slowly charges up, causing the tag to reflect less power, as witnessed in the plain areas.

Finally, Fig. 5 shows a close-up view of the last 2 bits of a kill password being sent to a tag, followed by the first parity bit following them. These bits are located near the end of the VALUE parameter of the kill command. The exact format of a generation 1 kill command is defined in [1, Sections 4.1 and 4.2.2].

In the experiment shown on the top of Fig. 5, the tag expects a kill password of $FF_h = 11111111_b$, while, on the bottom, it expects a password of $01_h = 00000001_b$. In both cases, the password supplied by the reader is $00_h = 0000000_b$. This means the top tag already knows the kill command will fail, having previously received many wrong bits. The bottom tag, however, only learns that the kill password is wrong after the falling edge identifying the last "0" bit. The increased power consumption of the tag in the lower tag can be seen by the spike it exhibits as it starts receiving the parity bit as compared to the gentler slope on the top figure, as indicated by the hatched area. This demonstrates how a single password bit can be extracted from the reflected signal. We must note again that, while extracting a 8-bit password is far from impressive, it takes only a linearly larger effort to extract a larger password, be it 32 bit, 256 bit, or 1,024 bit.

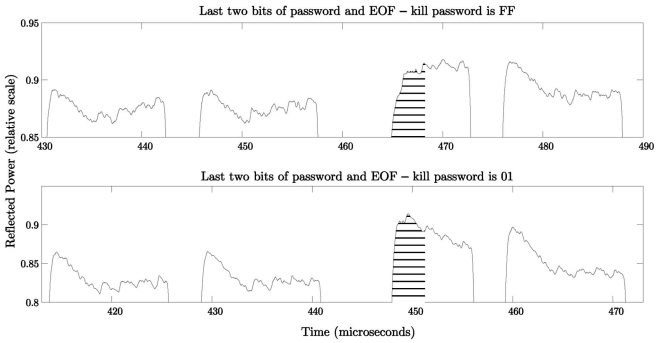

Fig. 5. Killing FF versus killing 01.

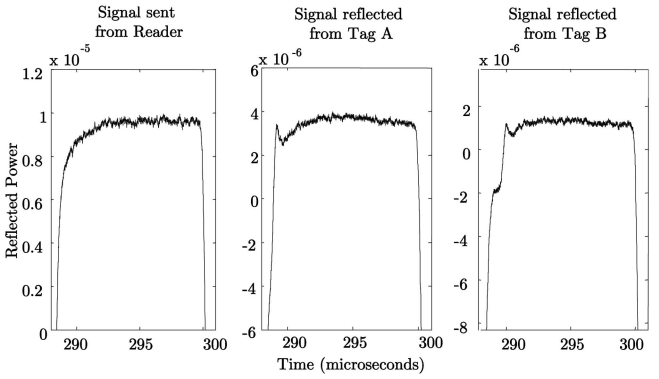

Fig. 6. Generation 2 reader signal versus tag signal.

4 An Attack against Generation 2 Tags

Generation 2 tags contain several functional enhancements which make the password extraction attack more difficult. In a future paper, we will demonstrate how Generation 2 passwords can also be extracted by a somewhat more complicated version of the parasitic backscatter attack. We show here how the privacy of Generation 2 tag users is compromised using the same attack.

Fig. 6 shows a figure similar to Fig. 3, comparing the signal transmitted by the reader and the signal reflected by the tag. The noticeable addition of the cusp shows that the tag is modulating its reflected signal. It is also evident that tags from different vendors have different RF signatures.

In our experiments, we noted that a dead tag (i.e., a tag which has received a kill command with the correct kill password) presents essentially the same backscatter signature as a live tag. Dead tags do not participate in EPC inventory commands and, as such, are considered invisible. However, a killed tag's RF front end is still functional and, thus, a dead tag modulates its reflected field in practically the same way that it does when the tag is active. This means that the *existence* of a killed tag can be detected by an adversary using an attack technique similar to ours, even though the tag's payload has been erased as part of the kill command. The different design choices made by tag vendors in implementing their RF front ends cause each brand of tag to modulate the reader's signal in a slightly different way. Thus, not only is it possible to tell a dead (or privacy-enhanced) tag from a reflecting surface which does not modulate the incident signal, such as a short segment of wire, but it is even possible to discover the brand of a specific dead tag simply by observing this tag's backscatter. By sweeping a directed beam with changing polarization over a person, an adversary can thus learn about the type and orientation of the various tags carried by this person, even if the tags are dead and cannot be interrogated. This calls into question the entire concept of application-layer privacy and gives credence to the opinion that only physical manipulation of a tag can silence it [6].

5 Discussion

5.1 Current and Future Threats

Special care should be taken when implementing cryptographic functions on passive tags. Hardware designers wishing to add cryptographic functionality (such as AES) to passive tags aim to minimize the power consumption and cost of their modules at the price of increased processing time. In [13], for example, the authors implement only a single S-box module and pass data through it 8 bits at a time. This makes the implementation even more susceptible to power analysis.

5.2 Protection against This Attack

This paper concentrates on attacks rather than on defenses. Nevertheless, we will review some common countermeasures and explain why they are problematic for RFID chip designers to implement. The interested reader is invited to look at the introduction to [16] or at [14] for a more detailed survey.

In general, power analysis countermeasures fall into one of two categories: *mitigation* and *prevention*. Mitigation countermeasures try to reduce the signal to noise ratio (SNR) of the secret information located in the power consumption trace, either by attenuating it or by hiding it in noise. Prevention countermeasures try to completely remove secret information from the trace.

A common type of mitigation countermeasure involves the addition of *random noise* to the power consumption of a device [8]. Since power is supplied to tags by the reader, it sounds tempting to add a noise source to the reader's signal and not to the tag, thus saving a redesign of the tags and keeping their costs low. However, this approach is unlikely to work. First, the attacker can point one directional antenna at the tag, point another one at the reader, and, finally, perform the attack on the difference signal. Second, the reader can only add very limited narrowband noise to the signal because of the strict regulatory constraints placed on its high-powered output.

An example of a prevention countermeasure is the introduction of *balanced logic*—designing the circuit such that the same number of gates switches between states every clock cycle [9], [10]. The unintuitiveness of this requirement can be eased by using prefabricated HDL components with this behavior (see, for example, [17]). The main drawback of this approach is in the price designers have to pay—the added gate count raises the cost of the device, while the larger number of transitions per cycle translates into a higher power consumption and, thus, a lower read range. It may be tempting to isolate the circuit into secure and nonsecure components and apply balancing only to the secure components. However, care must be taken when deciding which parts need protection and which do not. For example, a chip designer may try to protect the password function of a chip by balancing only the one-bit register containing the result of the comparison of the stored password bit and the received bit. However, if the tag's data bus is not balanced, it is still possible to detect individual bytes of the password as they are read from memory and learn about their Hamming weights.

A feasible solution, which is perhaps the most compatible with modern RF front ends, would be the separation of power supply from power consumption by use of a *double-buffering power supply* mechanism consisting of a pair of capacitors switched by power transistors [16]. At any stage in time, one capacitor is charged by the reader while the other is being discharged by the circuit. With proper design, this approach can almost eliminate the power

consumption information. Moreover, it involves changes only to the RF front end of the tag, making it the quickest to roll out. To make this countermeasure more effective, large flat capacitors can be attached to the inlay next to the printed antenna. Tag vendors can easily produce two versions of their ICs—a protected version for secure applications and an insecure version for cost-conscious applications—while sharing the internal logic and only dropping in different RF front ends. To further reduce costs, vendors can create a single IC with redundant contact points. Such an IC will offer power analysis resistance when fixed to inlays with the extra capacitor and degrade to insecure operation when fixed to inlays without such a capacitor. Tags using this protective mechanism still have to take care that power consumption does not leak out through the intentional backscatter modulation mechanism, which has to come out of the circuit proper and connect to the antenna. RFID tags consume very low amounts of power (on the order of tens of microwatts), several orders of magnitudes less than newer smart card chips with security coprocessors. This property means a moderately sized capacitor can power the tag for many hundreds of clock cycles, making the countermeasure particularly effective. In addition, the main threat against this countermeasure—removal of the external capacitors or a direct measurement of the current flow between the capacitors and the logic itself—is less relevant when considering the attack model in which the attacker does not have physical access to the tag.

6 Conclusion

We have described the parasitic backscatter attack and demonstrated its effect on the security and privacy aspects of RFID tags. We have also described several effective countermeasures against this attack.

7 Further Reading

The companion Web site for this paper can be found at http://www.wisdom.weizmann.ac.il/~yossio/rfid-ieee. It includes more traces and a hyperlinked version of the reference section.

Acknowledgments

The authors wish to thank Mickey Cohen, Ari Juels, Simon Krausz, Oded Smikt, Eran Tromer, Amir Yacoby, Oren Zarchin, and the many other people who shared their knowledge, time and equipment and helped this research take shape.

References

[1] Auto-ID Center, "860MHz-930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation," version 1.0.1, Nov. 2002.

[2] J.R. Rao, D. Agrawal, B. Archambeault, and P. Rohatgi, "The EM Side-Channel(s)," *Proc. Fourth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '02)*, J. Hartmanis, G. Goos, and J. van Leeuwen, eds., pp. 29-45, Aug. 2002.

[3] D. Dobkin, "The RF in RFID," http://www.enigmatic-consultng.com/Communications_articles/RFID/RF_in_RFID_index.html, Oct. 2005.

[4] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.* John Wiley & Sons, 2003.

[5] EPCglobal Inc., "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz," version 1.0.9, Sept. 2005.

[6] G. Karjoth and P. Moskowitz, "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced," *Proc. Workshop Privacy in the Electronic Society (WPES)*, Nov. 2005.

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Lecture Notes in Computer Science*, vol. 1666, pp. 388-397, 1999.

[8] P. Kocher, J. Jaffe, and B. Jun, "US Patent 6,327,661: Using Unpredictable Information to Minimize Leakage from Smartcards and Other Cryptosystems," 2001.

[9] P. Kocher, J. Jaffe, and B. Jun, "US Patent 6,510,518: Balanced Cryptographic Computational Method and Apparatus for Leak Minimizational in Smartcards and Other Cryptosystems," 2003.

[10] M. Akmal, K. Tiri, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," *Proc. Eighth European Solid-State Circuits Conf. (ESSCIRC '02)*, pp. 403-406, Sept. 2002.

[11] B.W. Lampson, "Hints for Computer System Design," *Operating Systems Rev.*, vol. 15, no. 5, pp. 33-48, Oct. 1983.

[12] S. Mangard, "Exploiting Radiated Emissions—EM Attacks on Cryptographic ICs," *Proc. Austrochip '03*, 2003.

[13] S. Dominikus, M. Feldhofer, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," *Proc. Sixth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '04)*, J.-J. Quisquater and M. Joye, eds., pp. 357-370, July 2004.

[14] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," *IEEE Trans. Computers*, vol. 51, no. 5, pp. 541-552, May 2002.

[15] S.E. Sarma, S.A. Weis, and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Proc. First Int'l Conf. Security in Pervasive Computing*, 2003.

[16] A. Shamir, "US Patent 6,507,913: Protecting Smart Cards from Power Analysis with Detachable Power Supplies," 2003.

[17] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Design and Analysis of Dual-Rail Circuits for Security Applications," *IEEE Trans. Computers*, vol. 54, no. 4, pp. 449-460, Apr. 2005.