The Rogue Capacitor Attack

Chee Lee
Department of Electrical & Computer Engineering,
Oregon State University, Corvallis, Oregon 97331 - USA.
E-mail: leech@engr.orst.edu

Abstract— **Side-channel attacks, attacks that target information that leaks from the physical device, are a real threat to smart cards. Although different countermeasures have been proposed and implemented to defend against these attacks, such methods do not make attacks impossible. In most cases, these countermeasures only serve as a stalling mechanism and not necessarily a prevention mechanism – the required resources to break the algorithm are increased, but the algorithm is not any stronger. As such, this paper examines the weakness of detached power supplies by presenting a method of defeating it or, at the very least, a method that will minimize its affect. The goal is to spur new interest and research in the design of secure smart cards by bringing into light the immediate danger of current smart card implementations and the false security that current countermeasures provide.**

Keywords— **Power attack, smart card, countermeasure, differential power attack, simple power attack, detached power supply.**

I. Introduction

Millions and millions of smart cards are used today in a wide variety of applications ranging from cellular telephones and computer access control to identification and credit cards. These smart cards are typically used for authentication and sensitive transactions by executing cryptographic computations based on secret keys embedded in their non-volatile memories.

Due to the large number of smart cards in use and the nature of the transactions involving those smart cards, there has been increased concern over the vulnerabilities of smart card cryptographic algorithms to side-channel attacks. These attacks exploit the fact that a hardware device can sometimes leak information when running a cryptographic algorithm. [1]

One source of leaked information is the time-varying power consumption of a device executing a cryptographic algorithm. An attacker using this information to extract the secret keys from a smart card would be considered as using a "power attack."

A power attack works by exploiting the fact that a cryptographic device will consume a varying amount of current as it executes an algorithm. By making observations, an attacker can attempt to deduce information about what is occurring and obtain the secret key. The two most common power attacks are the Simple Power Attack (SPA) and the Differential Power Attack (DPA). [2]

As a direct threat of power attacks, researchers and manufactures of smart cards have developed various techniques to make smart cards more secure. However, such countermeasures do not make attacks infeasible. They simply increase the attacker's experimental and computational workload beyond reasonable limits. [3].

This paper examines one such countermeasure, the detached power supply, and illustrates, using a rogue capacitor, how an attacker's workload can be brought back down to within reasonable limits. Section II describes the detached power supply countermeasure. Section III and IV examines the previous power attacks SPA and DPA and why they fail against the detached power supply countermeasure. Section V presents a new attack using a rogue capacitor that is effective against the detached power supply countermeasure. And Section VI summarizes my experimental results.

II. Detached Power Supply Countermeasure

In a standard smart card without a detached power supply, an attacker can obtain the secret key by measuring the power used by the card. Such measurements produce a plot similar to the one in Figure 1. With this information, the attacker can then use the SPA or DPA to actually analyze the plot and obtain the secret key of the smart card (See Section III and Section IV for an explanation on the SPA and DPA). Due to this vulnerability, researchers have developed a detached power supply countermeasure that reduces the usefulness of the power leakage information received.

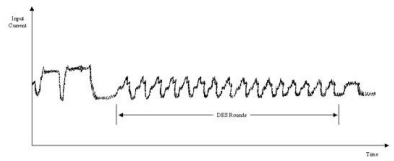

Figure 1: Power Trace of DES on a Standard Smart Card

In the detached power supply countermeasure, two capacitors are used to completely decorrelate the power supplied to the card from the power consumed by the card (See Figure 2). These capacitors serve as a power isolation unit. During half the time, capacitor 1 is regularly charged by the external power supply and capacitor 2 is irregularly discharged by the smart card. During the other half, the roles of the two capacitors are reversed. [4].

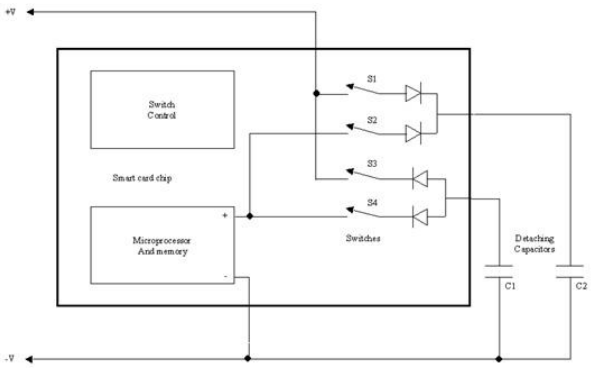

Figure 2: Schematic of a Smart Card with Detached Power Supplies

A simple switch control unit embedded in the smart card defines the behavior of the smart card. When the smart card is first connected to the external power supply, switch 1 is closed connecting capacitor 2 to the external power supply. After capacitor 2 is fully charged, switch 1 opens and switch 2 closes connecting capacitor 2 to the smart card providing the smart card with power. At the same time, switch 3 also closes connecting capacitor 1 to the external power supply charging and preparing it for use. Once capacitor 2 approaches the minimum voltage required to operate the smart card, switches 2 and 3 open and switches 1 and 4 close. The closed switch 4 connects capacitor 1 to the smart card providing the card with power. And the closed switch 1 connects capacitor 2 to the external supply charging and preparing it for use. This process repeats until the smart card has completed its communication.

If an attacker were to analyze the power leakage while the above process is taking place, the attacker would receive a plot similar to the one in Figure 3. The plot still provides power leakage information, specifically, the total charge consumed by all chip operations during the discharging period. At the standard smart card clock rate of 5 MHz, the chip performs about 100 instructions within this period. Thus, the attacker only knows the total power consumed by the chip during about 100 consecutive instructions. This is simply not enough information for an attacker using the SPA or DPA to obtain the secret key (See Section III and IV for an explanation.). [4]

Figure 3: Power Trace of a Smart Card with Detached Power Supplies

III. Simple Power Analysis (SPA)

The Simple Power Attack (SPA) is a technique that involves directly interpreting power consumption measurements collected during cryptographic operations. SPA can yield information about a device's operation as well as key material. An SPA trace refers to a set of power consumption measurements taken across a cryptographic operation. These traces, under close analysis, can reveal the structure of the cryptographic algorithm and reveal the sequence of instructions executed. This information can then be used to break cryptographic implementations in which the execution path depends on the data being processed. For example:

DES key schedule: The DES key schedule computation involves rotating 28-bit key registers. A conditional branch is commonly used to check the bit shifted off the end so that "1" bits can be wrapped around. The resulting power consumption traces for a "1" bit and a "0" bit will contain different SPA features if the execution paths take different branches for each.

DES permutations: DES implementations perform a variety of bit permutations. Conditional branching in software or microcode can cause significant power consumption differences for "0" and "1" bits.

Comparisons: String or memory comparison operations typically perform a conditional branch when a mismatch is found. This conditional branching causes large SPA characteristics.

Multipliers: Modular multiplication circuits tend to leak a great deal of information about the data they process. The leakage functions depend on the multiplier design, but are often strongly correlated to operand values and Hamming weights.

Exponentiators: A simple modular exponentiation function scans across the exponent, performing a squaring operation in every iteration with an additional multiplication operation for each exponent bit that is equal to "1". The exponent can be compromised if squaring and multiplication operations have different power consumption characteristics, take different amounts of time, or are separated by different code. Modular exponentiation functions that operate on two or more exponent bits at a time may have more complex leakage functions. [5]

A typical SPA on the DES algorithm would produce a trace similar to the one in Figure 1. Notice how the 16 rounds of DES can be distinguished in the plot. This and other information, upon closer inspection, can be used to find the DES key. The drawback of SPA is that it is susceptible to signal noise and the attacker must know implementation details of the cryptographic algorithm.

IV. Differential Power Analysis (DPA)

The Differential Power Analysis (DPA) is similar to the SPA. It is, essentially, a statistical analysis of the electric consumption records (traces) measured for a large number of computations with the same key. Each trace is similar to the trace in Figure 1.

The advantage that the DPA has over the SPA is that this attack does not require any knowledge about the individual electric consumption of each instruction, nor about the position in time of each of these instructions. Implementation details of the cryptographic algorithm do not need to be known and the signal noise is eliminated. The DPA only relies on the following fundamental hypothesis: There exists an intermediate variable, that appears during the computation of the algorithm, such that knowing a few key bits allows us to decide whether two inputs (respectively two outputs) give the same value or not for this variable. [6]

The above characteristics of the DPA give it an advantage over the SPA. However, there is still one drawback – compared to the SPA, an attacker using the DPA needs to make many more traces in order to implement a successful attack.

V. Rogue Capacitance Attack

The detached power supply countermeasure makes the SPA and DPA attacks extremely difficult to employ since now the only information we receive from a trace is the total power consumed during a large amount of consecutive instructions. So at first glance, this countermeasure is fairly effective. However, upon further inspection, this countermeasure provides a false sense of security because a modified measuring tool employing load matching can circumvent the detached power supply and make the SPA and DPA attacks applicable again.

The flaw with the detached power supply countermeasure is that it hides the structure of the cryptographic algorithm inside the discharging period of the capacitors. In other words, the decay of the current in the trace in Figure 3 depends on the time constant T, where T is the resistance multiplied by the capacitance ($T = R * C$). Proof of this comes from the fact that the detached power supply circuit is an RC circuit. And the natural response of an RC circuit is as follows:

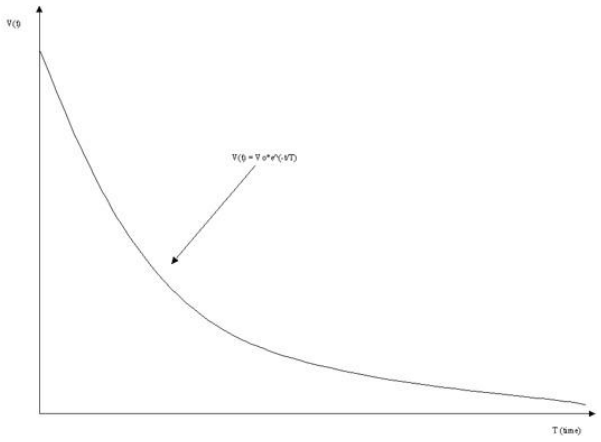

Figure 4: Natural response of an RC Circuit

The detached power supply circuit can be simplified to the RC circuit shown in Figure 5. From this circuit, we can easily find the voltage v(t) by thinking in terms of node voltages. Using the lower junction between R and C as the reference node and summing the currents away from the upper junction between R and C gives $C * (dv/dt) + v/R = 0$.

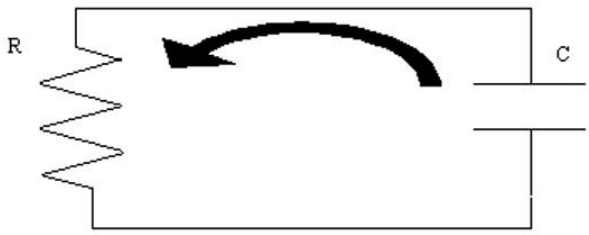

Figure 5: Standard RC Circuit

Solving this equation for v, we get $v(t) = v(0) * e^{-t/(R*C)}$, $t >= 0$. And from this equation we can easily find the expressions for current i and power p: $i(t) = v(t)/R = (Vo/R) * e^{-t/T}$, $t >= 0$ and $p = v * I = (Vo^2/R) * e^{(-2*t)/T}$. Graphing these equations (see Figure 4) will show that the decay is dependent on T, which is equal to R*C.

Since the detached power supply countermeasure relies on the time constant T, any attack would first need to neutralize this. Hence, a measuring tool with load matching could be used to neutralize the time constant and make the SPA or DPA useful again.

In order to neutralize the time constant T, we first recognize that $T = R * C$ and that the decay is determined by $e^{-t/T}$. The larger the time constant, the slower the decay, and the more instructions that can be executed during the discharging time. So as an attacker, we want to make the discharging time as small as possible. To do this, we need to reduce T. And to reduce T, we need to reduce the value of either R or C. Since the detached power supply circuit has no direct value of R for us to manipulate (the microprocessor and memory block have resistance, but we can't get to it), we have decided to reduce T by reducing the capacitance.

We do this by first simplifying the circuit in Figure 2 to the circuit in Figure 6. This simplification is made possible by recognizing that the microprocessor and memory block have resistive, capacitive, and inductive components giving it an impedance Z.

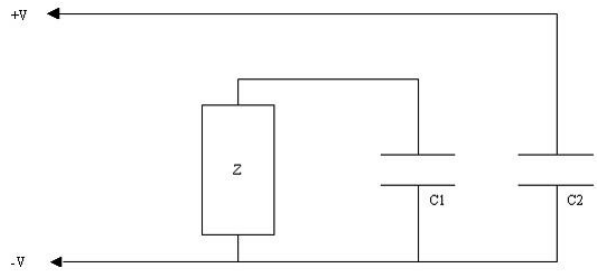

Figure 6: Simplified Schematic of a Smart Card with Detached Power Supplies

Next, we recall that two capacitors in series combine to make a single effective capacitor with a value closest to

the smaller of the two capacitor values. Therefore, we can add a small capacitor (labeled the "rogue capacitor" on the order of pico-farads) at the -V terminal as shown in Figure 7.

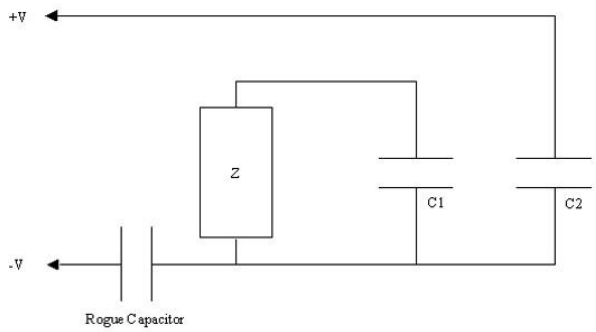

Figure 7: Rogue Capacitor Placement

The ideal spot to place this capacitor would be between the microprocessor and memory block connection to ground and the two capacitors as shown in Figure 8. However, this is not possible because we assume this path is internal to the smart card so that we cannot get to it. The idea is to develop a passive attack - one that does not destroy the card. If we were developing an active attack - one that destroys or changes the structure of the card - we could simply rip out the two detaching capacitors. And with them gone, we could go straight back to using either the SPA or DPA methods.

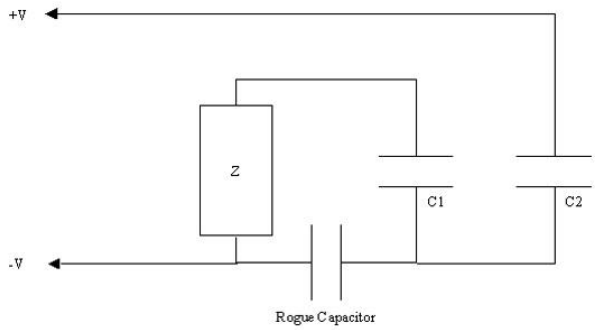

Figure 8: Ideal Rogue Capacitor Placement

With the rogue capacitor in place, we notice that C1 and the microprocessor and memory block are high impedance nodes and can be ignored simplifying the circuit in Figure 7 to the one in Figure 9. Now we have two capacitors in series and if the rogue capacitor is much smaller, we will receive a total effective capacitance that is smaller than either C1 or C2. The effective capacitance is determined by the following equation: $Ceff = (1/Ca + 1/Cb)^{-1}$ where Ca = either C1 or C2 and Cb = the rogue capacitor.

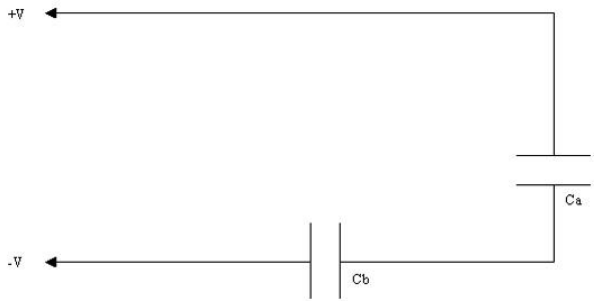

Figure 9: Changing the Effective Capacitance

With the effective capacitance reduced, we now have a smaller time constant T. Now when we make a trace of the power usage, we no longer receive a trace with long discharge times as in Figure 3. Instead, due to the shorter discharge times, we receive a trace that is essentially similar to the trace in Figure 1. Now we can again see the structure of the cryptographic algorithm. And thus, we can proceed with using the SPA and DPA attacks.

It is important to note that the shorter discharge time does, on occasion introduce a glitch in the power trace (see Figure 10). During this glitch, it is impossible to obtain any useful information about the cryptographic algorithm. However, if we know the implementation details of the cryptographic algorithm, then we can make an educated guess about what activity goes on during the glitch and still go back and use the SPA attack to determine the key. The idea here is that we know how long a certain instruction should take when it is processing a "0" bit or a "1" bit and what instruction should come next. So we can tell whether that instruction or small group of instructions is hidden under the glitch caused by the new smaller discharging cycle or not. And by analyzing whether they fit or not, we can determine what values are being processed and essentially determine the key. The DPA attack is unchanged. We continue to take multiple traces and from them we can analyze them together and determine the key. The glitch is not a factor with the DPA attack because it is averaged out.

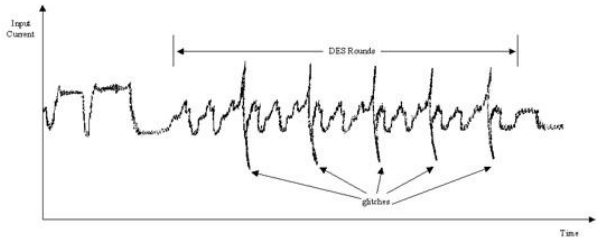

Figure 10: Glitches in the New Power Trace

VI. Conclusion

In our lab experiments, we were able to reduce the discharge cycle to the point where only approximately 5 glitches occurred in the trace of the 16 rounds of DES. This allowed us to use the SPA and DPA attacks to determine the key. However, we did notice that since the trace

had these 5 occurrences of glitches, the time it took for us to find the key was 1.25 times longer than normally possible using the SPA and DPA attacks on a card without a detached power supply countermeasure. Also, it took us a while to determine the optimal rogue capacitance. It is important to note that if the rogue capacitance is larger than either C1 or C2, then the discharge cycle has not been reduced at all. However, if the rogue capacitance is significantly smaller than either C1 or C2, then the smart card may not function properly because there may not be enough charge on C1 or C2 to provide power to the card. Hence finding the optimal rogue capacitance is a daunting and time consuming task.

Overall, our results show that the detached power supply countermeasure is only moderately secure. A determined attacker willing to spend the extra time to find the optimal value of the rogue capacitance can easily circumvent the detached power supply countermeasure and obtain the secret key with the same amount of resources and only a slight increase in time.

	Standard Method	Our Method
SPA	2 min	2.5 min
DPA	5 min	6.25 min

Table 1: Average Time for a Successful Power Attack

References

[1] Thomas S. Messerges, "Using second-order power analysis to attack dpa resistant software," *Cryptographic Hardware and Embedded Systems (CHES)*, , no. 1965, pp. 238–251, 2000.

[2] David Naccache and Michael Tunstall, "How to explain side-channel leakage to your kids," *Cryptographic Hardware and Embedded Systems (CHES)*, , no. 1965, pp. 229–230, 2000.

[3] Jean-Sebastien Coron Christophe Clavier and Nora Dabbous, "Differential power analysis in the presence of hardware countermeasures," *Cryptographic Hardware and Embedded Systems (CHES)*, , no. 1965, pp. 252–263, 2000.

[4] Adi Shamir, "Protecting smart cards from passive power analysis with detached power supplies," *Cryptographic Hardware and Embedded Systems (CHES)*, , no. 1965, pp. 71–77, 2000.

[5] Joshua Jaffe Paul Kocher and Benjamin Jun, "Differential power analysis," *White Paper*, pp. 1–10, http://www.cryptography.com.

[6] Louis Goubin and Jacques Patarin, "Des and differential power analysis," *Cryptographic Hardware and Embedded Systems (CHES)*, , no. 1717, pp. 158–172, 1999.