Chapter 6
Design Time Engineering of Side Channel Resistant Cipher Implementations

Alessandro Barenghi
Politecnico di Milano, Italy

Luca Breveglieri
Politecnico di Milano, Italy

Fabrizio De Santis
Technische Universität München, Germany

Filippo Melzani
STMicroelectronics, Italy

Andrea Palomba
Politecnico di Milano, Italy

Gerardo Pelosi
Politecnico di Milano, Italy

ABSTRACT

Dependable and trustworthy security solutions have emerged as a crucial requirement in the specification of the applications and protocols employed in modern Information Systems (IS). Threats to the security of embedded devices, such as smart phones and PDAs, have been growing since several techniques exploiting side-channel information leakage have proven successful in recovering secret keys even from complex mobile systems. This chapter summarizes the side-channel techniques based on power consumption and elaborates the issue of the design time engineering of a secure system, through the employment of the current hardware design tools. The results of the analysis show how these tools can be effectively used to understand possible vulnerabilities to power consumption side-channel attacks, thus providing a sound conservative margin on the security level. The possible extension of this methodology to the case of fault attacks is also sketched.

INTRODUCTION

Recent advances in the complexity of modern information systems lead to their employment for treating a variety of security sensitive data. This has a direct impact on the everyday's life of the layperson, since quite a few secure devices are commonly employed to perform payments (e.g., credit cards and e-ticketing) and to regulate the access to infrastructures and automotive systems (e.g., remote access control systems). Another key area where the security and privacy of personal

DOI: 10.4018/978-1-4666-4030-6.ch006

data should be guaranteed is the one of mobile and embedded devices: voice and data communications have their confidentiality guarded by a plethora of crypto-schemes. These infrastructures have created the need to design mathematically secure cryptographic primitives and to engineer effective implementations thereof. Indeed, even if the security margin warranted by the mathematical properties of the cipher is adequate, the security of the system can be undermined by the information leakage via environmental parameters (i.e., by side-channel leakage).

One of the first official notes related to this concept dates back to 1956, when P. Wright reported that MI5 (the British intelligence agency) were stuck in their efforts to break an encryption machine employed by the Egyptian Embassy in London (Wright & Greengrass, 1988). The hand-operated, mechanical encryption machine was a rotor-based device including a number of wheels, each of which was associated to an alphabet letter in order to set the secret key employed to encipher a "plaintext" message. The enciphered message was printed on a paper ribbon, while the wheel-pins were set each day according to a "key sheet" shared only with the intended receiver. In order to sidestep the statistical cryptanalysis of the system, Wright suggested to place a microphone for eavesdropping on the tones (clicks) produced by the encryption machine during its usage. Indeed, Wright discovered that the click frequency could enable to determine the position of some rotors and, consequently, to reduce the computational effort needed to break the cipher.

Nowadays, Side-Channel Attacks (SCA) are a widespread and well recognized threat to digital embedded systems, which rely on gathering information on the cipher key from the observation of environmental parameters (Kocher, 1996; Kocher et al., 1999; Messerges et al., 1999a, 1999b; Brier et al., 2004; Mangard et al., 2007) despite the fact that such a secret is stored in a protected memory. Commonly observed parameters are represented by the power consumption of the device (Kocher et al., 1999; Mangard et al., 2007; Eisenbarth et al., 2008) or the electromagnetic emissions during the computation (Gandolfi & Mourtel, 2001; Quisquater & Samyde, 2001; Agrawal et al., 2002; Peeters et al., 2007; Gebotys & White, 2008; Barenghi et al., 2011c; Enev et al., 2011). Since these observed parameters depend on the switching activity of the circuit, which in turn depends on the values employed in the computation, it is possible to correlate the actual measurements on a real-world device with hypothetical values of the parameter predicted using a model depending on a part of the secret key. If the secret key portion is small enough, it is possible to examine exhaustively the correlation for all the possible values taken by the secret key portion and to detect which one is actually correlated with the exhibited device behavior. In this way, an attacker can recover the whole key one part at a time, with a limited computing effort (Mangard et al., 2007).

Until recently, both Differential Power Attacks (DPA) and Differential Electromagnetic Attacks (DEMA) have proven very successful in retrieving the embedded secret key even in very large, commercial grade devices such as FPGA (Moradi et al., 2011), through dealing with measurements issued with proper digital signal processing techniques (Barenghi et al., 2010b). A different approach from the passive observation of an environmental parameter during the regular functioning of a device, is to induce a device misbehavior, in such a way to cause errors during the execution of cryptographic primitives (Boneh et al., 2001; Joye & Tunstall, 2012). In this case, an attacker is said to mount a fault attack, by means of some injection technique such as focusing a laser beam on the chip, micro-carving it with a Focused Ion Beam, or inducing temporary alterations of the power supply or clock signals. An analysis of the results of the faulted computations, together with a suitable model of the fault injection technique (Differential Fault Attack, DFA), helps the attacker recover the secret key with a computational effort drastically reduced compared to the one needed