All You Ever Wanted to Know About Side-Channel Attacks and Protections

Sylvain Guilley[1,2] and **Olivier Rioul**[1]

[1] Télécom-Paris, 19 place Marguerite Perey, 91 120 Palaiseau,
[2] Secure-IC S.A.S., 104 boulevard du Montparnasse, 75 014 Paris.

Proposal for a "tutorial" presentation at FIC 2023

Introduction

Security applications have become pervasive. Cryptography ensures the basic foundations for security, namely the triad: *confidentiality*, *integrity* and *authenticity*. Of course, normalized cryptographic algorithms do exist and are widely deployed. Still, algorithms undergo a constant revision, as attested by the recent contests aiming at modernizing some fields. Typically, asymmetrical cryptography is currently challenged by emerging large-scale quantum computers, hence novel so-called "post-quantum cryptographic" algorithms are gaining some momentum.

In this talk, we focus on today's implemented algorithms, in particular block ciphers, which are not threatened by quantum computers. We tackle the question of their security when implemented in real devices. Namely, we address the question of protection of cryptographic algorithms against attacks which arise when the attacker has physical access to the devices which embed them. This topic is called "**side-channel analysis**". Clearly this family of threats has been around for a while, and is the reason for the existence of "AVA_VAN" rating (Vulnerability ANalysis) activity in Common Criteria (ISO/IEC 15408[1]) evaluations. Recently such attacks have been shown to be realizable practically from the remote, leveraging the internal power measurement capability of modern processors (consider for instance TPMfail – CVE-2019-11090 & CVE-2019-16863, Platypus – CVE-2020-8694 & CVE-2020-8694, Herzbleed – CVE-2022-23823). The goal of this talk is to give an overview of existing *attack* and *protection* techniques, including those which are involved in certification aspects.

[1] See also the Common Criteria web portal: https://www.commoncriteriaportal.org/.

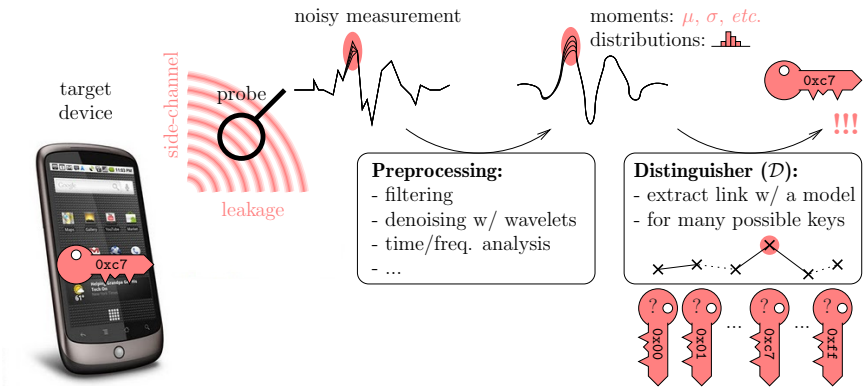

Figure 1: Illustration of the different steps involved in a side-channel analysis.

Context

Embedded devices conceal secrets that can be extracted by an attacker. The typical attacks consist in measuring the *power consumption*, the *radiated electromagnetic field*, or the *duration* of a target device. Those consist in a noisy source of information somehow correlated to the secret. Attacks leverage distinguishers that enable secret recoveries. In many cases, the attacker can purchase one (or several) blank device(s) of the same series and learn about their leakage, in particular how it relates to the targeted secret. Such information can also improve the hardware attacks deployed on another device.

Presentation Contents

In this presentation, we address the following topics.

Side-Channel Analysis Framework

We describe side-channel analysis setups, discuss leakage models, and compare existing attacks. Some possible options are depicted in Fig. 1.

Side-Channel Countermeasures

Then, we introduce countermeasures, including *masking*. We explain that it consists in achieving a cryptographic computation with different intermediate variables for each computation, even though, e.g., the same data is inputted several times. We also state that masking boils down to encoding an informative variable with artificially generated digital noise (independent from the information).

We detail the special case of "code-based masking" (CBM) which encompasses most of previously proposed masking schemes. In this framework, we study attacks on the one hand and evaluation of the amount of leakage on the other hand:

Attacks

We detail both *unprofiled* and *profiled* attacks. Unprofiled attacks can be carried out from scratch, whereas profiled attacks require a preliminary training before being perpetrated.

Unprofiled attacks have an advantage in terms of practicability, as they can be performed out-of-the-box. At the opposite, profiled attacks require the procurement of a clone device which is open, i.e., which can be provisioned with a chosen key. We first present unprofiled attacks such as "correlation", "mutual information", "collision", and "expectation minimization" attacks, and emphasize in which situation they are the most suitable. Interestingly enough, each one of them is provably optimal in different albeit real and representative contexts.

Profiled attacks have first be demonstrated on unprotected devices. However, those attacks have been extended to masked implementations as well. One key advantage of profiled attacks is that they can make the most of *multivariate* traces, such as those captured by oscilloscopes. The higher the acquisition signal-to-noise ratio, the faster the attack.

Evaluations

When designing countermeasures, it is important to be able to assess the added security brought by each and every countermeasure. Indeed, this allows to arbitrate some decisions, as countermeasures always incur some additional cost.

We first introduce an information-theoretic framework for side-channel evaluations. It requires techniques such as estimation of mutual information, and computation of (high-order) cumulants when tackling the question of attacks against (high-order) masking countermeasures. We also relate the question of security evaluation to underlying code-based structure of the masking scheme.

Key Takeaway Messages

In this presentation, we offer a comprehensive overview of side-channel analyses, and describe their power in various real-world scenarios. We introduce usual protections, and show their limits, both by discussing the most powerful attack or by showing evaluation methods.

The material of this talk consists in a formalization work carried out by the co-authors of this talk. It is the gist of a reference manual to be published as a book next year.