Side Channel Attack using Machine Learning

Amina Amrouche[1,2], Larbi Boubchir[1] and Said Yahiaoui[2]

[1]*LIASD research Lab., University of Paris 8, France*
[2]*Research Center on Scientific and Technical Information (CERIST), Algiers, Algeria*
{amina_amrouche@outlook.fr, larbi.boubchir@univ-paris8.fr, syahiaoui@cerist.dz}

***Abstract*—The overwhelming majority of significant security threats are hardware-based, where the attackers attempt to steal information straight from the hardware that our secure and encrypted software operates on. Unquestionably, side-channel attacks are one of the most severe risks to hardware security. Rather than depending on bugs in the program itself, a side-channel attack exploits information leaked from the program implementation in order to exfiltrate sensitive secret information such as cryptographic keys. A side channel assault could manifest in different ways including electromagnetic radiation, power consumption, timing data, or even acoustic emanation. Ever since the side-channel attacks were introduced in the 1990s, a number of significant attacks on cryptographic implementations utilizing side-channel analysis have emerged, such as template attacks, and attacks based on power analysis and electromagnetic analysis. However, Artificial Intelligence has become more prevalent. Attackers are now more interested in machine learning and deep learning technologies that enable them to interpret the extracted raw data. The aim of this paper is to highlight the main methods of machine learning and deep learning that are used in the most recent studies that deal with different types of side-channel attacks.**

***Index Terms*—Side-channel attacks, Power analysis, Electromagnetic analysis, Machine learning, Deep learning.**

I. Introduction

Cryptanalysis refers to the process of decrypting ciphertext without the use of the actual key and to the process of analyzing cryptosystems to comprehend their functions. An alternative way to explain it : cryptanalysis is a method for getting at the plain text in transmission when you don't have access to the decryption key. A field in cryptanalysis that has grown in popularity recently is the Side-Channel Analysis (SC-Anal) [1]. The latter brings the issue of revealing secret information out of the domain of mathematics into the domain of physical implementation. Researchers have noticed that by focusing on the implementation of cryptosystems rather than their specifications, they can conduct attacks that are low-cost in terms of the time and resources needed, and extremely successful in obtaining valuable results. A side-channel attack (SCA) is a security vulnerability that relies on information obtained from the hardware implementation of a program instead of the programming errors. A SCA may include power consumption, electromagnetic emanations, and acoustic emissions, among other varieties. The security community has been very interested in physical attack vectors ever since P. Kocher released the first side channel attack back in 1996 [2]. Several side-channel attacks such as Simple (SPA), Differential power analysis (DPA), ElectroMagnetic analysis (EMA), and Template attacks, have long been the main subject of research. The idea of using machine learning techniques for side-channel analysis, however, became actively investigated as a result of recent advancements in machine learning (ML) and deep learning (DL) technologies.

This paper aims to review a number of new studies on side-channel attacks using ML and DL techniques. Each study will be briefly discussed to explain its main ideas and demonstrate how researchers approached each specific SCA class.

The structure of this article will be as follows: Section II will include background information on side-channel attacks, machine learning, and deep learning. The studies on ML and DL applications used in side-channel attacks are examined in Section III. In Section IV we wrap up our research with a brief review and outline of potential future work.

II. Background

A. Side-Channel Attacks

The vast majority of serious security threats are hardware-based, where the attacker can steal information directly from the hardware that our secure and encrypted software runs on. Side channel attacks are considered one of the most severe risks to hardware security.

a) Types of side-channel attacks: Malicious hackers can perform side-channel attacks in a number of ways, including the following:

- **Electromagnetic:** One of the earliest side-channel attacks, measures and analyzes the radio waves or electromagnetic radiation emitted from a target device in attempt to reconstruct the internal signals of that device. Van Eck phreaking [3] is an example of an EM attack.
- **Power:** Measures or influences the power consumption of a device or subsystem. In order to determine the input of the computation, a power-based SCA examines how power consumption changes during the course of the computation. An attacker can determine the activity of a system by watching the amount and timing of power used by that system or one of its components.
- **Acoustic:** Measures the sounds produced by a device. By listening to the sounds that electronic components generate, hackers can obtain information.
- **Timing:** Analyzes the time a system spends running cryptographic algorithms. The total time can provide data