Quantifying the Potential for Side-Channel Leakage

Rohith Prakash

Abstract

In this paper, we study the problem of determining and measuring the probability of side-channel leakage being present on a system. We discuss the shortcomings of commonly used information theoretic metrics such as channel capacity and mutual information, specifically how they have been misapplied and why they fail to truly determine if side-channel leakage is possible or if potential leakage is due to sensitive inputs. To accurately quantify leakage probabilities, we propose a *distribution-based leakage* metric which measures the probability that an adversary may infer sensitive inputs as a result of the system processing the input.

1 Introduction

Side channel exploitation, anomaly detection, and covert channel communication are problems of detecting or exploiting leakage over information channels. Side and covert channels exists when observable differences in system behavior occur as the result of actions performed by a *victim* or sending process. These attacks typically involve an adversary learning secret information over the channel, based on the behavior of a victim process. Anomaly detection, on the other hand, involves detectors running on a system analyzing and categorizing observed behavior in real time. In this setting, a malicious program leaks information about its behavior through an observed channel.

2 Information Leakage

We first formalize the concept of side channel leakage.

Definition 1 (Side channel leakage)**:** Consider a system S performing computation f on a set of inputs X. Fix a method O of observing the behavior of S. A **side channel** leak occurs if $O(f(x_i))$ is *statistically distinguishable* from $O(f(x_j))$ for any $x_i \neq x_j \in X$.

What 1 describes is that, given a method of observing the behavior of a system, side channel leaks may occur if there are observable differences in system behavior as a result of processing two different inputs. *Observation methods* of a system may describe

Our primary observation with regards to such leakage is that information may only be learned from system observations if the underlying distributions which affect these observations are distinguishable.

Theorem 1 (Distribution-based leakage)**:** *Fix a method O of observing behavior on a system S. Consider two distinct program behaviors x and y on S, with output distributions D_x and D_y respectively. Observing $O(x)$ and $O(y)$ drawn from D_x and D_y respectively can only leak information about x and y if D_x, D_y are statistically distinguishable.*

We note that output distributions D_i are defined with respect to observation method O on S.

Corollary 1.1 (Privacy-preserving computations)**:** *A computation f with input set $X = \{x_1, \cdots, x_n\}$ and output distributions $D = \{d_1 = f(x_1), \cdots, d_n = f(x_n)\}$ (w.r.t. observation method O) is privacy preserving if and only if $d_1 = d_i \ \forall \ d_i \in D$.*

References