Covert and Side Channels due to Processor Architecture*

Zhenghong Wang and Ruby B. Lee
Department of Electrical Engineering, Princeton University
{zhenghon,rblee}@princeton.edu

Abstract

Information leakage through covert channels and side channels is becoming a serious problem, especially when these are enhanced by modern processor architecture features. We show how processor architecture features such as simultaneous multithreading, control speculation and shared caches can inadvertently accelerate such covert channels or enable new covert channels and side channels. We first illustrate the reality and severity of this problem by describing concrete attacks. We identify two new covert channels. We show orders of magnitude increases in covert channel capacities. We then present two solutions, Selective Partitioning and the novel Random Permutation Cache (RPCache). The RPCache can thwart most cache-based software side channel attacks, with minimal hardware costs and negligible performance impact.

1. Introduction

Covert channels and side channels are two types of information leakage channels. A covert channel uses mechanisms that are not intended for communications, e.g., writing and checking if a file is locked to convey a "1" or "0". In a covert channel [1], an insider process leaks information to an outsider process not normally allowed to access that information. The insider (sending) process could be a Trojan horse program previously inserted stealthily into the computer. An outsider (receiving) process need only be an unprivileged process.

In a physical side channel attack, unconventional techniques are used to deduce secret information. Typically, the device has been stolen or captured by the adversary who then has physical access to it for launching a physical side-channel attack. Traditional side channel attacks involved differential power analysis [2-5] and timing analysis [6-10]. Different amounts of power (or time) used by the device in performing an encryption can be measured and analyzed to deduce some or all of the key bits. The number of trials needed in a power or timing side channel attack could be much less than that needed in mathematical cryptanalysis.

In this paper, we consider software side channel attacks. In these attacks, a victim process inadvertently assumes the role of the sending process, and a listening (attacker) process assumes the role of the receiving process. If the victim process is performing an encryption using a secret key, a software side channel attack allows the listening process to get information that leads to partial or full recovery of the key. The main contributions of this paper are:

- Identification of two new covert channels due to processor architecture features, like simultaneous multi-threading (SMT) and speculation.
- Showing that covert channel capacities have increased by orders of magnitude.
- Analysis of cache-based side channel attacks.
- Insufficiency of software isolation approaches for mitigating information leakage through processor-based covert and side channels.
- Selective partitioning solution for SMT-based covert channels.
- Novel Random Permutation Cache (RPCache) solution that can thwart cache-based software side channel attacks.

Section 2 describes the threat model. Section 3 illustrates the problem with real attacks and analysis of newly identified cache side channels. Section 4 shows the insufficiency of software solutions, motivating the need for hardware solutions to a hardware-induced problem. Section 5 provides our Selective Partitioning solution. Section 6 presents our novel Random Permutation Cache solution, and experimental results on its performance and security. Section 7 reviews related work and section 8 presents our conclusions.

* This work was supported in part by DARPA and NSF Cybertrust 0430487, and NSF ITR 0326372.

Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06)
0-7695-2716-7/06 $20.00 © 2006 IEEE