Cryptology ePrint Archive: Report 2013/076

Design Space Exploration and Optimization of Path Oblivious RAM in Secure Processors

Ling Ren and Xiangyao Yu and Christopher Fletcher and Marten van Dijk and Srinivas Devadas

Abstract: Keeping user data private is a huge problem both in cloud computing and computation outsourcing. One paradigm to achieve data privacy in these settings is to use tamper-resistant processors. Users' private data is decrypted and computed upon in a secure compartment from which that data will not be revealed to an untrusted party. Since program working sets seldom fit within the on-chip storage of today's processor solutions, a secure and efficient way of transporting and storing data off-chip is required. A simple solution to this problem is to encrypt all data that leaves the chip. However, the address sequence that goes off-chip may still leak information. ORAM (Oblivious RAM) has been previously proposed to hide the address leakage of the program. However, ORAM has mainly been explored in server/file settings which assume a vastly different computation model than secure processors (e.g., accesses are for files not processor cache blocks). Not surprisingly, naively applying ORAM to a secure processor setting incurs large performance overheads.

In this paper, we demonstrate techniques to make ORAM practical in a secure processor setting. A particular ORAM proposed recently, called Path ORAM, is studied. For the first time, we thoroughly explore the design space of Path ORAM, and introduce a novel throughput-driven design space exploration approach based on ORAM background eviction schemes and super blocks. With our ORAM optimizations, ORAM latency drops by 45%, and SPEC benchmark execution time improves by 39% in relation to a baseline configuration. We also propose an efficient integrity verification scheme for Path ORAM. Our work can be used to improve the security level of previous secure processors.

Category / Keywords: implementation / Path Oblivious RAM, secure processor, integrity verification

Date: received 15 Feb 2013, last revised 15 Feb 2013

Contact author: renling at mit edu

Available formats: PDF | BibTeX Citation

Version: 20130220:094625 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]