Cache timing attacks have been known for a long time, however since the rise of cloud computing and shared hardware resources, such attacks found new potentially devastating applications. One prominent example is SSA (presented by Irazoqui et al at S&P 2015) which is a cache timing attack against AES or similar algorithms in virtualized environments. This paper applies variants of this cache timing attack to Intel's latest generation of microprocessors. It enables a spy-process to recover cryptographic keys, interacting with the victim processes only over TCP. The threat model is a logically separated but CPU co-located attacker with root privileges. We report successful and practically verified applications of this attack against a wide range of microarchitectures, from a two-core Nehalem processor (i5-650) to two-core Haswell (i7-4600M) and four-core Skylake processors (i7-6700). The attack results in full key recovery. Compared to earlier processor generations, the attacks are more involved, but still of practical complexity, requiring between $2^{19}$ and $2^{21}$ encryptions. For the last two processors, the cache slice selection algorithm (CSSA) was not known before and had to be reverse engineered as part of this work. This is the first time CSSAs for the Skylake architecture are reported. Our attacks demonstrate that cryptographic applications in cloud computing environments using key-dependent tables for acceleration are still vulnerable even on recent architectures, including Skylake. Our reverse engineering of the CSSAs of these processors will also be beneficial for developers in many other contexts, for instance for implementing page colouring in modern operating systems.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Andreou, A., Bogdanov, A., Tischhauser, E. W.
Pages: 155-155
Publication date: 2017

Host publication information
Title of host publication: Proceedings of 2017 IEEE International Symposium on Hardware Oriented Security and Trust
Publisher: IEEE
ISBN (Print): 9781538639290
(2017 Ieee International Symposium on Hardware Oriented Security and Trust (host)).
Keywords: Timing, Cryptography, Microarchitecture, Cloud computing, Computer architecture, Hardware, Microprocessors
DOIs: 10.1109/HST.2017.7951819
Source: FindIt
Source-ID: 2371671235
Research output: Research - peer-review › Article in proceedings – Annual report year: 2017