[CacheOut: Cache-Angriff Gegen Intel CPUs]

CacheOut: Leaking Data on Intel CPUs via Cache Evictions

Stephan van Schaik*
University of Michigan
stephvs@umich.edu

Marina Minkin
University of Michigan
minkin@umich.edu

Andrew Kwong
University of Michigan
ankwong@umich.edu

Daniel Genkin
University of Michigan
genkin@umich.edu

Yuval Yarom
University of Adelaide and Data61
yval@cs.adelaide.edu.au

Abstract

Recent speculative execution attacks, such as RIDL, Fallout, and ZombieLoad, demonstrated that attackers can leak information while it transits through various microarchitectural buffers. Named Microarchitectural Data Sampling (MDS) by Intel, these attacks are likened to "drinking from the firehose", as the attacker has little control over what data is observed and from what origin. Unable to prevent these buffers from leaking, Intel issued countermeasures via microcode updates that overwrite the buffers when the CPU changes security domains.

In this work we present CacheOut, a new microarchitectural attack that is capable of bypassing Intel's buffer overwrite countermeasures. We observe that as data is being evicted from the CPU L1 cache, it is often transferred back to the leaky CPU buffers where it can be recovered by the attacker. CacheOut improves over previous MDS attacks by allowing the attacker to choose which data to leak from the CPU's L1 cache, as well as which part of a cache line to leak. We demonstrate that CacheOut can leak information across multiple security boundaries, including those between hyperthreads, processes, and virtual machines, and between user space and the operating system kernel, and from SGX enclaves.

1 Introduction

In 2018 Spectre [29] and Meltdown [31] left an ever lasting impact on the design of modern processors. Speculative and out-of-order execution, which were considered to be harmless and important CPU performance features, were discovered to have severe and dangerous security implications. While the original Meltdown and Spectre works focused on breaking kernel-from-user and process-from-process specifications, many follow-up works have demonstrated the dangers posed by uncontrolled speculation and out-of-order execution. Indeed, these newly-discovered *speculative execution attacks* have been used to violate numerous security domains, such as Intel's Secure Guard Extension (SGX) [46], virtual machine boundaries [48], AES hardware accelerators [44] and others [5, 8, 9, 15, 25, 28, 29, 30, 33, 34]. Recognizing the danger posed by these threats, the computer industry responded with side channel mitigations. For older hardware, Kernel Page Table Isolation (KPTI) [13] as well as Foreshadow [46] and Spectre mitigations [18, 39, 45, 49] were designed and deployed in an attempt to fix leaky hardware isolation features via software means. In parallel, Intel released the Coffee Lake Refresh architecture, which attempted to mitigate Meltdown and Foreshadow in hardware, thereby avoiding the performance overhead induced by software countermeasures.

However, as speculative execution attack research persisted, the security community uncovered a deeper source of leakage: internal and mostly undocumented CPU buffers. With the advent of Microarchitectural Data Sampling (MDS) attacks [7, 42, 47], it was discovered that the contents of these buffers can be dumped via assisting or faulting load instructions, bypassing the CPU's address and permission checks. Using these techniques, an attacker can sample data as it transits through the internal buffers, without the need to match the address of the faulting or assisting load with the address of the data or even its address space. In particular, this allows the attacker to siphon-off data as it appears in the buffer, again breaking nearly all hardware-backed security domains.

Recognizing the danger, Intel deployed countermeasures for blocking data leakage from internal CPU buffer. As modifying the buffer's implementation not to leak information was not possible, Intel instead attempted to mitigate the problem symptomatically by augmenting a legacy x86 instruction, `VERW`, to overwrite the contents of the leaking buffers with constant, data-independent information. This countermeasure was subsequently deployed by all major operating system vendors, performing buffer overwrite on every security domain change. While effective buffer overwriting is often tricky to implement in Intel CPUs [41], the intuition behind the countermeasure is that an attacker cannot recover buffer information that is no longer present. Thus, in this paper we ask

*Work partially done while author was affiliated with Vrije Universiteit Amsterdam.


Download

Im Vergleich zu den MDS-Attacken können Daten bei CacheOut ... (TAA) hat Intel zufällig auch die Angriffsvektoren für CacheOut geschlossen.. Mit CacheOut (oder L1D Eviction Sampling, L1DES) gibt es eine weitere Angriffsmöglichkeit auf Intel-CPUs über die spekulative ... AMD tauscht Intel-CPU gegen Threadripper 1950X umPC-Welt 19.06.2018; notebookinfo.de ...

CacheOut - Leaking Data on Intel CPUs via Cache Evictions ... aktuellen Cloud Security Newsletter: Aktuelle Angriffsmethoden / Was sich 2020 bei der ... Gegen aufkommende Übelkeit in der Schwangerschaft lässt sich einiges unternehmen.. Meltdown und Spectre: Erste Klagen gegen Intel, Performanceprobleme kochen hoch (heise) · Meltdown ... Sicherheitslücke: Spectre-Angriff kann Intel SGX überwinden (golem) ... CacheOut: Leaking Data on Intel CPUs via Cache Evictions. Sicherheitslücken in Intel-CPUs: Modifizierte Angriffe erfordern BIOS-Updates. CacheOut beziehungsweise L1D Eviction Sampling (L1DES) umgehen bisherige ...

Samsung’s Galaxy S tablet spotted, caught on a pretty blurry camera

Sicherheitslücken in Intel-CPUs: Modifizierte Angriffe erfordern BIOS-Updates ... Intels bisherige Microcode-Updates gegen die Angriffsvektoren ... Die University of Michigan nennt den neuen Dreh CacheOut, die Universität .... Sicherheitslücken in Intel-CPUs: Modifizierte Angriffe erfordern BIOS-Updates ... Data Sampling treffen Intel-Prozessoren: Bei L1DES alias Cache Out ist der ... …mit Cascade Lake-X und halbiertem Preis in den Kampf gegen Threadripper.. Intels Meltdown-Abwehrmechanismen würden gegen CacheOut keine ... Wer eine nach Q4/2018 hergestellte Intel-CPU einsetzt, soll ebenfalls aus ... auch jene Lücke geschlossen, die den Cacheout-Angriff möglich macht.. New “CacheOut” speculative execution vulnerability for Intel CPUs ... on the exploitation's ability to evict targeted data from the CPU's cache .... CacheOut. Leaking Data on Intel CPUs via Cache Evictions. We present CacheOut, a new speculative execution attack that is capable of leaking data from Intel ... IT Security News Daily Summary 2020-02-18

CacheOut: Leaking Data on Intel CPUs via Cache Evictions

Stephan van Schaik*
University of Michigan
stephvs@umich.edu

Marina Minkin
University of Michigan
minkin@umich.edu

Andrew Kwong
University of Michigan
ankwong@umich.edu

Daniel Genkin
University of Michigan
genkin@umich.edu

Yuval Yarom
University of Adelaide and Data61
yval@cs.adelaide.edu.au

Abstract

Recent speculative execution attacks, such as RIDL, Fallout, and ZombieLoad, demonstrated that attackers can leak information while it transits through various microarchitectural buffers. Named Microarchitectural Data Sampling (MDS) by Intel, these attacks are likened to "drinking from the firehose", as the attacker has little control over what data is observed and from what origin. Unable to prevent these buffers from leaking, Intel issued countermeasures via microcode updates that overwrite the buffers when the CPU changes security domains.

In this work we present CacheOut, a new microarchitectural attack that is capable of bypassing Intel's buffer overwrite countermeasures. We observe that as data is being evicted from the CPU L1 cache, it is often transferred back to the leaky CPU buffers where it can be recovered by the attacker. CacheOut improves over previous MDS attacks by allowing the attacker to choose which data to leak from the CPU's L1 cache, as well as which part of a cache line to leak. We demonstrate that CacheOut can leak information across multiple security boundaries, including those between hyperthreads, processes, and virtual machines, and between user space and the operating system kernel, and from SGX enclaves.

1 Introduction

In 2018 Spectre [29] and Meltdown [31] left an ever lasting impact on the design of modern processors. Speculative and out-of-order execution, which were considered to be harmless and important CPU performance features, were discovered to have severe and dangerous security implications. While the original Meltdown and Spectre works focused on breaking kernel-from-user and process-from-process specifications, many follow-up works have demonstrated the dangers posed by uncontrolled speculation and out-of-order execution. Indeed, these newly-discovered *speculative execution attacks* have been used to violate numerous security domains, such as Intel's Secure Guard Extension (SGX) [46], virtual machine boundaries [48], AES hardware accelerators [44] and others [5, 8, 9, 15, 25, 28, 29, 30, 33, 34]. Recognizing the danger posed by these threats, the computer industry responded with side channel mitigations. For older hardware, Kernel Page Table Isolation (KPTI) [13] as well as Foreshadow [46] and Spectre mitigations [18, 39, 45, 49] were designed and deployed in an attempt to fix leaky hardware isolation features via software means. In parallel, Intel released the Coffee Lake Refresh architecture, which attempted to mitigate Meltdown and Foreshadow in hardware, thereby avoiding the performance overhead induced by software countermeasures.

However, as speculative execution attack research persisted, the security community uncovered a deeper source of leakage: internal and mostly undocumented CPU buffers. With the advent of Microarchitectural Data Sampling (MDS) attacks [7, 42, 47], it was discovered that the contents of these buffers can be dumped via assisting or faulting load instructions, bypassing the CPU's address and permission checks. Using these techniques, an attacker can sample data as it transits through the internal buffers, without the need to match the address of the faulting or assisting load with the address of the data or even its address space. In particular, this allows the attacker to siphon-off data as it appears in the buffer, again breaking nearly all hardware-backed security domains.

Recognizing the danger, Intel deployed countermeasures for blocking data leakage from internal CPU buffer. As modifying the buffer's implementation not to leak information was not possible, Intel instead attempted to mitigate the problem symptomatically by augmenting a legacy x86 instruction, `VERW`, to overwrite the contents of the leaking buffers with constant, data-independent information. This countermeasure was subsequently deployed by all major operating system vendors, performing buffer overwrite on every security domain change. While effective buffer overwriting is often tricky to implement in Intel CPUs [41], the intuition behind the countermeasure is that an attacker cannot recover buffer information that is no longer present. Thus, in this paper we ask

*Work partially done while author was affiliated with Vrije Universiteit Amsterdam.

iSwish: Yet another pretty iPhone clone for Windows Mobile

Comet Lake U: Vaio-Notebooks haben jetzt sechs CPU-Kerne - Golem.de ... 10 noch Microcode-Patches gegen ZombieLoad v1 und verwandte MDS-Lücken. ... Sicherheitslücken in Intel-CPUs: Modifizierte Angriffe erfordern BIOS-Updates ... Sampling (MDS) treffen Intel-Prozessoren: Bei L1DES alias Cache Out ist der .... Intel informiert über potenziell gefährliche Lücken in der ... Zurzeit besteht die sogenannte Schwachstelle „CacheOut“ (Kennung: CVE-2020-0549), durch ... von Intel soll User mit dem neuen Patch gegen die Angriffsvektoren ... Huge Sale at Nashbar

Kadhalil Sodhapuvadu Yeppadi Mp3 Songs Download Kadhalil Sodhapuvadu Yeppadi Latest Tamil Songs Free

Man könnte meinen, dass sich alles gegen Intel verschworen hat. ... Schwere Zeiten für Intel, Partystimmung bei AMD – der CPU-Markt scheint sich in der Wende ... CacheOut erreicht auf Intels eigener Schweregrad-Skala für ... Variation der Angriffsszenarien erstellen und sie mit dem Unternehmen teilen.. Der Beitrag CacheOut/L1DES: Neue Intel-CPU-Schwachstelle erschien zuerst ... Ein zweiter, deutlich komplizierterer Angriff richtet sich gegen die verwendete .... Evolution von Groove bis Next Generation Sync Client · kein Cache mehr im Next ... CacheOut: Cache-Angriff gegen Intel CPUs · Europäischer Datenschutztag .... rss.golem.de,vor 1 Tag. Fast ein halbes Jahr hat das Berliner Kammergericht nach einem Trojaner-Angriff im Notbetrieb gearbe weiterlesen... feature-top.. Im Vergleich zu den MDS-Attacken können Daten bei CacheOut gezielter ... MDS-Attacken bei Intel CPUs, Rowhammer bei DDR4, diese ... eine Variante der Angriffsmethode ZombieLoad bei Intel-Prozessoren der zehnten ... 82abd11c16 Slap A Bitch Contest

82abd11c16

Cyber tips for safe online dating: How to avoid privacy gaffs, exploits, and scams
PowerISO Crack 7.3 [2019]
NXPowerLite Desktop 8.0.8