NVLeak: Off-Chip Side-Channel Attacks via Non-Volatile Memory Systems[1]

Zixuan Wang[⋆] Mohammadkazem Taram[♯⋆] Daniel Moghimi[†⋆]
Steven Swanson[⋆] Dean Tullsen[⋆] Jishen Zhao[⋆]

[⋆]UC San Diego [♯]Purdue University [†]UT Austin

Abstract

We study microarchitectural side-channel attacks and defenses on non-volatile RAM (NVRAM) DIMMs. In this study, we first perform reverse-engineering of NVRAMs as implemented by the Intel Optane DIMM and reveal several of its previously undocumented microarchitectural details: on-DIMM cache structures (NVCache) and wear-leveling policies. Based on these findings, we first develop cross-core and cross-VM covert channels to establish the channel capacity of these shared hardware resources. Then, we devise NVCache-based side channels under the umbrella of NVLeak. We apply NVLeak to a series of attack case studies, including compromising the privacy of databases and key-value storage backed by NVRAM and spying on the execution path of code pages when NVRAM is used as a volatile runtime memory. Our results show that side-channel attacks exploiting NVRAM are practical and defeat previously-proposed defense that only focuses on on-chip hardware resources. To fill this gap in defense, we develop system-level mitigations based on cache partitioning to prevent side-channel leakage from NVCache. This paper is one of the first to study the architectural side-channel attacks in commercial NVRAM products, and the techniques and ideas can be applied to investigate future memory hardware designs.

1 Off-Chip Side-Channel Attacks

Microarchitectural side channels allow attackers to leak information from other users co-located on shared computing resources. Researchers have demonstrated such attacks by exploiting various hardware resources that are shared among untrusted users. For example, an attacker can construct a timing side channel based on the shared CPU cache and use this to break cryptography [3] and violate the privacy of encrypted databases [4]. These side channels are also the basic block to developing more advanced microarchitectural attacks that leak arbitrary data and undermine the confidentiality of several isolation domains on modern systems.

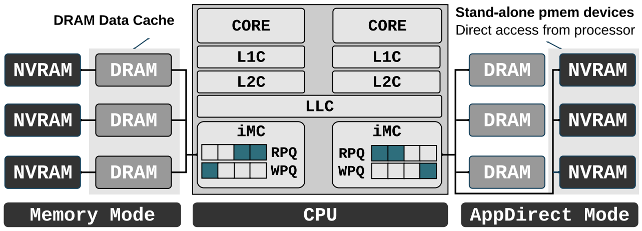

Figure 1: Memory hierarchy equipped with Optane DIMMs.

In this work, we study the security implications of scalable server-grade non-volatile RAM (NVRAM) DIMMs as implemented by Intel's Optane DIMM [2]. NVRAM DIMMs sit on memory bus (Figure 1) and support a larger memory capacity with data persistence which are long desired by server developers. Recent performance characterization studies [5] have shown that the Optane DIMM delivers its high levels of performance and scalability by employing various optimizations including multi-level buffers, internal address remapping schemes, and wear-leveling mechanisms. This combination leads to a discrepant performance behavior compared to what researchers expected before the product release [7]. Although previous studies [5] have investigated the microarchitecture of the Optane DIMM and analyzed its performance, its security implications remain largely unexplored. In this study, we investigate microarchitectural covert/side channels enabled by Optane DIMM, their impact on the security of real-world applications, and how we can improve system security against potential side channels.

2 NVLeak

In this work, we present NVLeak, a comprehensive collection of tools to reverse engineer off-chip memory architecture and perform side-channel attacks. With NVLeak, we make the following contributions:

1. Reverse-engineering. We perform reverse-engineering

[1] This work has been published at USENIX Security 2023 [6].

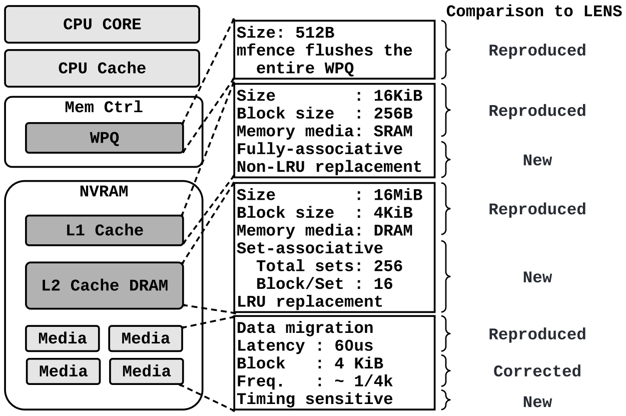

Figure 2: Overview of the NVRAM findings. *Reproduced* results are from LENS [5], *corrected* results are from NVLeak [6] and correct observations from LENS, and *new* results are from NVLeak and not discovered by LENS.

of the opaque design of NVRAMs, which helps us uncover new information leakage sources. Our goal is to detail the on-DIMM cache structures and configurations, control policies, and performance behaviors. We develop carefully crafted microbenchmarks that run in both kernel and user spaces to achieve this. These microbenchmarks trigger specific memory behaviors, which lead to detectable performance variances that reveal the corresponding hardware designs. As a result, we unveil a much more detailed picture of Optane DIMM microarchitecture compared to previous works [5]. Our findings, as shown in Figure 2, include the on-DIMM cache structures and wear-leveling policies, which we then exploit to develop new information leakage attacks.

2. Constructing covert channels. We develop and quantify new covert/side-channel attacks to empirically verify the existence of information leakage via the uncovered knowledge of Optane DIMM microarchitecture. First, we exploit the previously-undocumented on-DIMM cache structure to construct a cross-VM covert-channel attack. We show that cross-VM covert channels using the NVRAM cache are stable and achieve high channel capacity and low noise by solving several challenges. Second, we construct a covert channel that exploits the NVRAM wear-leveling mechanism to leak updates to a filesystem, which allows an attacker to monitor whether a victim updates its file without requiring elevated permission.

3. Side-channel attack case studies. Next, we show that our findings go beyond covert communication channels and affect the security of real-world applications. We demonstrate several side-channel attacks exploiting the NVRAM cache, under the umbrella of NVLeak attacks, applicable to everyday use cases of NVRAM:

First, we demonstrate several attacks in the scenario where NVRAM is used as persistent storage, compromising the privacy of databases. Although an attacker who shares the NVRAM with a victim does not have access to the victim's database/storage file and its queries, they can learn about its queries through NVRAM cache access patterns. Ultimately, an attacker can learn the details of queries and parameters, and previous work [1] shows that such information leakage is devastating for the privacy of encrypted databases.

Then, we demonstrate an NVLeak attack in the scenario where NVRAM is deployed like a volatile memory (like the DRAM). In this common scenario, to speed up workloads that don't require persistent storage, we show NVLeak can spy on code pages and detect which execution path is taken by a program whose code pages are stored in the NVRAM. Ultimately, we show that this has consequences for security-critical applications like cryptographic schemes.

4. Mitigations. We propose a set of mitigation mechanisms to defend against the NVCache-based side channels based on the reverse engineering results and side-channel attacks. We first propose a software-based L2 NVCache mitigation that allows a victim application to allocate memory blocks from isolated NVCache sets that are not shared with other applications, including the attackers, thus preventing information leakages. We develop this mitigation into a PMDK key-value store to make it resistant to NVCache-base side channels. The experimental results show that this mitigation's performance overhead is $< 4\%$. We then propose a software-based mitigation for L1 NVCache and WPQ, and a hardware-level mitigation for the entire NVRAM hierarchy.

5. Open source and responsible disclosure. We open source our code[2] in the hope of facilitating future off-chip memory security research. We have disclosed the vulnerabilities to Intel and received their acknowledgements.

References

[1] Paul Grubbs, Marie-Sarah Lacharité, Brice Minaud, and Kenneth G Paterson. Pump up the volume: Practical database reconstruction from volume leakage on range queries. In *CCS*, 2018.

[2] Intel. Intel Optane DC Persistent Memory, 2019.

[3] Cesar Pereida García, Billy Bob Brumley, and Yuval Yarom. Make sure DSA signing exponentiations really are constant-time. In *CCS*, 2016.

[4] Aria Shahverdi, Mahammad Shirinov, and Dana Dachman-Soled. Database reconstruction from noisy volumes: A cache Side-Channel attack on SQLite. In *USENIX Security*, 2021.

[5] Zixuan Wang, Xiao Liu, Jian Yang, Theodore Michailidis, Steven Swanson, and Jishen Zhao. Characterizing and modeling non-volatile memory systems. In *MICRO*, 2020.

[6] Zixuan Wang, Mohammadkazem Taram, Daniel Moghimi, Steven Swanson, Dean Tullsen, and Jishen Zhao. NVLeak: Off-chip side-channel attacks via non-volatile memory systems. In *USENIX Security*, 2023. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/wangzixuan.

[7] Jian Yang, Juno Kim, Morteza Hoseinzadeh, Joseph Izraelevitz, and Steve Swanson. An empirical guide to the behavior and use of scalable persistent memory. In *FAST*, 2020.

[2] https://github.com/TheNetAdmin/NVLeak