基于NVM的存储安全综述

李 月 王 芳
(武汉光电国家研究中心信息存储系统教育部重点实验室(华中科技大学计算机科学与技术学院) 武汉 430074)
(深圳华中科技大学研究院 广东 深圳 518000)

摘 要 大数据时代的来临为存储系统提供了新的机遇,同时也提出了新的挑战。传统的基于动态随机存储(DRAM)的内存架构面临着容量、能耗、可靠性等方面的问题;新型非易失存储器件(Non-Volatile Memory,NVM)具有非易失、字节寻址、空闲能耗低等优势,可以作为外存、内存或存储级内存(Storage Class Memory,SCM),为未来存储系统的变革提供了新选择,但同时也存在一些安全问题。NVM器件本身的耐久性有限,频繁对某一位置进行写操作时会造成该位置磨损,从而缩短设备的寿命;同时,由于具有非易失性,NVM被用作内存时,断电后数据不会丢失,攻击者可以通过窃取数据来提取敏感信息或对数据进行篡改;当NVM与DRAM构成混合内存时,可能会产生指针指向不明等问题;NVM作为SCM时,应用程序通过存取(load/store)接口直接对其进行访问,绕过了文件系统等权限管理和一致性管理机制。针对这些问题,文中总结了磨损均衡、减少写操作、减少写入量、内存加密、设计一致性机制、设计权限管理机制等解决办法;最后从硬件、操作系统以及编程模型层面探讨了仍须关注的NVM安全问题。

关键词 非易失性存储,安全,磨损均衡,加密,一致性

中图法分类号 TP333 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.07.008

Survey on Storage Security of Emerging Non-volatile Memory

LI Yue WANG Fang
(Wuhan National Laboratory for Optoelectronics,Key Laboratory of Information Storage System(School of Computer Science and Technology,Huazhong University of Science and Technology),Ministry of Education of China,Wuhan 430074,China)
(Shenzhen Huazhong University of Science and Technology Research Institute,Shenzhen,Guangdong 518000,China)

Abstract The age of big data provides new opportunities and challenges to the memory/storage system. Traditional main memory architecture based on DRAM faces the problems of capacity,energy consumption and reliability. The new non-volatile memory (NVM) devices are non-volatile and byte-addressable,and possess the feature of low idle consumption,so they can replace persistent storage,main memory or storage class memory (SCM). Though NVM devices provide new choices to the revolution of traditional memory/storage system,there are some security concerns as well. For NVM device itself,the endurance is limited. So writing frequently at one place can wear it out. The lifetime of the NVM devices can be seriously affected by that. When NVM devices work as memory,the non-volatile feature makes the data persistent in the NVM devices. The attackers can steal it and extract sensitive information or tamper the data. When NVM devices work with DRAM as heterogeneous memory,hard-to-find pointers may occur because of non-volatile feature of NVM. In addition,NVM device can work as SCM,because it's byte-addressable like DRAM. Applications can directly operate the NVM devices through load/store interface bypassing the file system. This paper surveyed some solutions about wear-leveling,reducing write operation,reducing write amount,encrypting main memory,designing consistent and right management mechanism. Finally,it explored some issues that need to be concerned from the aspects of hardware,OS and programming model.

Keywords Non-volatile memory,Safety,Wear-leveling,Encryption,Consistency

随着信息技术的不断发展,数据爆炸的时代悄然到来。各种电子设备(如手机、电脑、可穿戴智能设备、智能家居、车载设备、电子摄像等)充斥着人们的生活,每个人都与海量数据的产生息息相关。预计到2020年,全球数据总量将超过

到稿日期:2017-07-27 返修日期:2017-11-18 本文受武汉应用基础研究计划项目(2017010201010103),深圳市科技计划项目(JCYJ20170307172248636)资助。

李 月(1993-),女,博士生,主要研究方向为存储安全,E-mail:yueli@hust.edu.cn;王 芳 女,博士,教授,CCF会员,主要研究方向为海量存储系统、并行文件系统、非易失性存储、大规模图数据存储和处理,E-mail:wangfang@mail.hust.edu.cn(通信作者)。

40 ZB，大数据时代已经来临。海量数据向传统计算机存储系统提出了新的挑战。

传统以计算为中心的系统架构由于内外存之间的 I/O 性能不匹配，同时受限于容量、速度、功耗等因素，难以满足大数据的需求。新型非易失存储器件（NVM）的出现，推动了大数据处理模式的发展，使得新的内存和存储体系结构的产生变为可能。

目前，NVM 包括铁电随机存储器（Ferroelectric Random Access Memory，FRAM）、相变存储器（Phase Change Memory，PCM）、阻变随机存储器（Resistive Random Access Memory，RRAM）、自旋转移力矩随机存储器（Spin Transfer Torque Random Access Memory，STT-RAM）等。表 1[1] 列举了几种存储器件的属性信息。

表 1 几种存储器件的属性信息

Table 1 Comparison of properties of several storage devices

Attribute	DRAM	RRAM	STT-RAM	PCM	FeRAM
Capacity	～16 GB	～1 TB	～64 MB	～8 GB	～64 MB
Cell Area/F2	6～10	4～14	16～60	4～8	15～34
Read Latency/ns	＜10	10～50	2～20	10～100	20～80
Write Latency/ns	＜10	10～50	5～35	20～120	5～10
Write Energy/nJb^{-1}	～0.1	～0.1	1.6～5	＜1	＜1
Endurance	＞10^{15}	10^{8}～10^{10}	10^{12}～10^{15}	10^{8}～10^{12}	10^{12}～10^{14}
Idle Energy Consumption	high	low	low	low	low
Non-volatile	No	Yes	Yes	Yes	Yes

从表 1 可以看出，与传统动态随机存储器（Dynamic Random Access Memory，DRAM）相比，NVM 具有非易失、空闲功耗低等特性。目前，DRAM 的制作尺寸已经达到工艺极限，周期性刷新操作的开销也随着 DRAM 密度的增大变得越来越严重。以 DRAM 为代表的内存技术面临着容量、功耗、可靠性等方面的挑战，而 PCM 等非易失存储器件的出现，在一定程度上为计算机存储体系架构的发展提供了新的方向。不同的 NVM 各具优势：RRAM 容量大、工艺制程小；STT-RAM 读写速度快、数据保持力长；FeRAM 和 PCM 写操作功耗低；等。但是，想要解决目前面临的技术困境，单纯使用 NVM 替换 DRAM 或外存显然不是最佳方案。

尽管 NVM 非易失、字节寻址的特性存在着一定的优势（如节约了不断刷新需要的能耗，作为内存时可实现秒开机；应用程序直接操作 NVM，降低了延迟，提升了性能等），但也带来了一些安全问题。

NVM 作为外存时存在的安全问题与其他传统持久性存储介质基本一致，因此文中不讨论 NVM 单纯作为持久性存储介质时存在的问题，而主要针对 NVM 自身、作为内存以及存储级内存（SCM）时存在的安全问题进行探讨。

NVM 器件本身存在耐久性问题，易遭受磨损攻击。NVM 可以作为直接内存，也可以与 DRAM 构成混合内存。当 NVM 作为直接内存时，由于具有非易失的特性，数据存在被窃取的风险，因此需要设计数据保密与数据完整性保护方案；当 NVM 与 DRAM 构成混合内存时，由于两者存在不同，可能产生指针指向不明的问题。不论是作为直接内存还是混合内存，一致性问题始终存在。NVM 是有望实现 SCM 技术的新型器件，因此需要设计新的监督机制与一致性模型。NVM 作为内存时，一些常见的内存攻击手段（如冷启动攻击、侧信道攻击等）依然存在。

1）NVM 读写不对称、可靠性不高、耐久性不强等自身特性决定了其容易受到磨损攻击，若反复对某一位置进行写入，则会造成该存储单元因磨损而无法正常存储数据。恶意的用户或程序若采用重复暴力写入的手段进行攻击，则 NVM 的寿命会不正常缩短，对整个存储系统也会产生不利影响。

2）DRAM 依靠刷新保持数据，在电源关闭后，其上的数据消失。与此不同，NVM 作为内存时，其上的数据在电源关闭后依然保持，攻击者可以入侵系统并窃取或篡改数据，因此需要对内存中的数据进行加密和完整性保护。当 NVM 与 DRAM 组合构成混合内存时，由于指针所在位置和指针指向位置可能分别处于易失性介质或非易失性介质中，因此可能发生指针指向不明的问题。另外，当系统故障或突然断电时，DRAM 只需从持久性存储中读取数据重建并重新启动即可；而 NVM 由于非易失性，会产生一致性问题。

3）当 NVM 作为 SCM 时，其字节寻址特性使得应用程序可以绕过传统文件系统的管理权限而直接操作 NVM，增加了 NVM 被恶意攻击的风险，因此需要设计新的安全机制。

针对以上提出的问题，目前有磨损均衡、加密、添加新的保护机制等解决方案。下文将对 NVM 的存储安全问题进行介绍。

1 NVM 器件级安全问题

NVM 自身存在耐久性问题，其写寿命短，若恶意程序或攻击者对某一模块进行频繁写入，则会造成该位置损坏，从而缩短器件寿命。目前，研究人员提出了众多方法来延长 NVM 的使用寿命，其中包括磨损均衡算法、减少写入量、减少写入次数等。

较早的用于 NVM 的磨损均衡算法是由 Qureshi 等提出的 Start-Gap 算法[2]，其简单小巧且有效，仅使用两个寄存器：Start 和 Gap，其中 Start 记录所有的行被重定位的次数，Gap 记录被重定位的行数。另外，该算法还需一个内存行（memory line）Gapline，当写操作达到一定次数时，内存行用于移动数据，对存储块进行调整。Start-Gap 将内存分成几个独立的区域，结合简单的地址空间随机化技术，可以有效防止重复地址攻击，减少由于频繁写操作造成的失效问题。Start-Gap 是基于代数的磨损均衡办法，通过代数关系运算进行地址映射，同时通过移动物理行实现大量的行交换，开销低且安全性高。

Zhao 等[3] 认为磨损均衡可以以不同的粒度进行。使用不同粒度的均衡策略可以在不同的开销下实现不同的生命周期等级，更精细的粒度通常能实现更均衡的写入，但是成本相对较高。由于精确记录不同位的写入次数并利用计数值指导行内写入分布是不切实际的，因此很少有工作考虑位级别的磨损均衡工作。然而，程序特性可能引起内存行写入显著不平衡，这时位级磨损均衡就显得非常必要。本文首先探索磨损均衡的设计空间，分析并总结现有的磨损均衡策略，然后提出一个接近零成本的比特级磨损均衡方案，即行内翻转（ILF）。ILF 周期性地翻转内存行中的位映射，以交换热位和冷位上的写入；同时还兼容许多现有的粗粒度磨损平衡策略。

Huang 等[4]根据 PCM 写入时间不对称这一现象，提出了重新定时攻击：由于 PCM 设备写延迟不对称，且某些磨损均衡方案需要将逻辑地址重新映射到新的位置，因此可以精心设计写入序列并判断磨损均衡方案的映射变换方式。这一问题可使最先进的磨损方案快速失效，为此文献[4]提出了新的磨损均衡方案 Security Rbsg。Security Rbsg 是一个双层磨损均衡方案，通过外层映射增加密钥的复杂度，通过内层代数磨损均衡降低开销。

PV(Process Variation)和不均匀的写入强度可以使低耐久性的 PCM cell 在短时间内损耗。许多 PV 感知磨损均衡方案遵循一个共同的想法：基于写入强度分布预测强写入，并将其分配给具有强耐久性(即强单元)的单元。但这里要求写入分布在一定时间间隔内是一致的。该想法存在漏洞，即如果某恶意程序的写入强度是变化的，则以往的磨损均衡方案将不再适用。为了缓解强度变化的写入攻击，一种新型的 PV 感知损耗均衡即 TWL[5]被提出，它不依赖于写入强度的一致性分布，而是根据单元的耐久性随机地重新分配写入。将一个强大的页面(page-A)与一个弱页面(page-B)结合成一个“toss-up pair”，每次将写入分配给该对中的任何页面，具有强耐力的页面可能更频繁地被写入。文献[5]还进一步优化了 TWL 以提高鲁棒性、减少写入开销。

以上研究均是采用磨损均衡的方式来抵抗 NVM 磨损攻击，通过用不同的映射方式将不均衡的写操作均匀分布到各存储单元。除磨损均衡算法外，研究人员还采用了改变写操作的执行过程、减少写次数和写入量的方式来降低对 NVM 的写消耗，以延长其寿命。常见的方法有写截断策略、两阶段写策略、写前读策略、写操作去冗余、缓冲区重组和部分写策略[1]等。下文中的数据机密性涉及减少写操作和写入量的方式，通过减少因加密产生的大量写操作来延长设备的使用寿命，因此不再对减少写操作和写入量的相关方法做介绍。

2　基于 NVM 的内存安全问题

传统的基于 DRAM 的内存技术面临着严峻挑战，而 NVM 的出现为未来内存系统的发展提供了新的可能。NVM 可以作为直接内存，也可以与 DRAM 组合作为混合内存。NVM 与 DRAM 组成的存储体系架构有图 1 所示的几种形式。目前的存储架构如图 1(a)所示，以 DRAM 为内存，磁盘作为外存；图 1(b)所示的架构中，NVM 作为外存；图 1(c)所示的架构中，NVM 作为内存；图 1(d)所示架构为 NVM 与 DRAM 的混合内存。

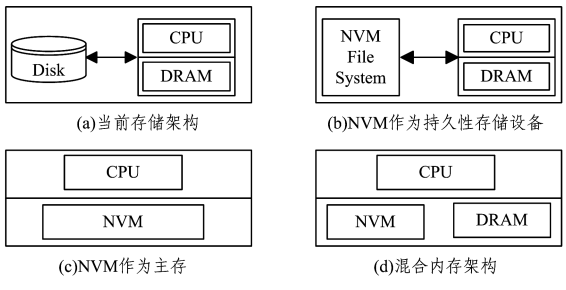

图 1　NVM 的 4 种存储体系架构[6]

Fig. 1　Four kinds of storage system architecture for NVM[6]

传统内存存在着许多安全问题：内存泄露、冷启动攻击、侧信道攻击以及其他常见的内存攻击(如代码破坏攻击、信息泄露、数据攻击、控制流劫持攻击[7]等)。传统内存存在的安全问题，在 NVM 环境下依然存在且会发生一定的改变。与传统内存一样，NVM 内存可能受到冷启动攻击、侧信道攻击等，但两者的攻击方法、攻击效果以及防御办法存在不同。

除了 NVM 特性带来的不同之外，图 1 中的 4 种存储体系架构也使内存环境变得更加复杂，如传统内存环境下的内存泄漏问题在新的存储体系架构下会演变为持久性内存泄漏问题。

下文将对 NVM 作为直接内存以及 NVM 与 DRAM 构成的混合内存存在的安全问题进行探究。

2.1　NVM 作为直接内存

NVM 的非易失性是一个卓越的特性，该特性使得计算机即启即用成为可能：数据被保存在 NVM 内存中，系统启动或从休眠状态唤醒时都能够及时恢复。当 NVM 作为直接内存时，非易失性可能导致数据机密性和完整性等问题。

2.1.1　数据机密性问题

传统内存在断电一段时间后，其中的数据会消失，这在一定程度上防止了内存中的敏感信息被攻击者窃取后提取其中的有效内容的问题。但对于 NVM，在断电或系统崩溃后，其中的数据依然存在，受到攻击的可能性比 DRAM 更大，同时除冷启动攻击外，可采取的攻击手段也更多。针对该问题的常见解决方法是利用加密的方法对 NVM 中的数据进行保护。

i-NVMM[8]是一个增量式加密方案，通过观察数据对处理器是否有效来识别处理器经常使用到的数据工作集(working set)，并对其他不常用的数据进行加密，这样就可以保持内存中的大部分数据一直处于加密状态而不需要加密整个内存，因此不会对应用的性能产生太大影响。i-NVMM 在内存模块内部，不依赖于其他额外的硬件和软件。该方案需要对数据是否加解密进行预测，会产生较大的开销。

Kong 等[9]提出的计数器模式内存加密方案的结构如图 2 所示。该方案提出了合适的加密方案，使得原先的负载均衡方案可用，降低了写负载；同时提出计数器加密的方式，设计了高效的 ECC 管理方案，将两者相结合后延长了 PCM 的寿命。

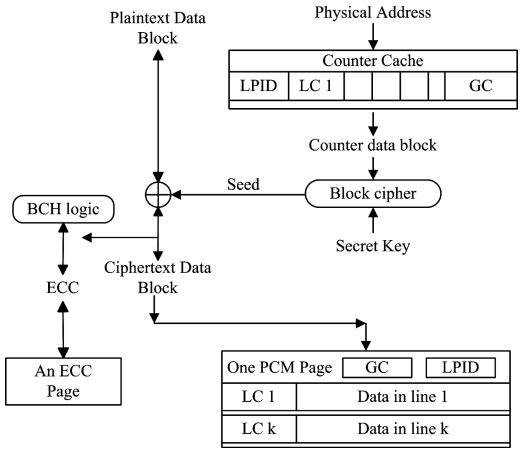

图 2　计数器的加密结构图

Fig. 2　Structure of counter encryption

i-NVMM 和 Kong 设计的内存加密模式是两种较为经典

的加密算法,但依然存在一些不足,目前有一些相应的改进方案。Huang 等[10]提出了重映射复位计数器 RCR 方案,以解决计数器加密模式存在的计数器溢出或需要重新加密整个内存的问题。RCR 的基本思想是利用磨损均衡重映射来重置计数器,降低计数器的存储开销,提高计数器的缓存命中率。COVERT[11]同样是基于计数器的加密方案,按需分配内存,降低重新加密的频率,同时保留了小型计数器的性能优势。

由于加密技术的扩散特性,即使只修改了明文中的部分数据,也可能导致密文产生雪崩式的变化,使需要写入的数据大量增加,因此出现了考虑磨损均衡的加密技术框架。

SEDURE[12]方法认为磨损均衡技术不仅可以缓解由加密引起的存储器寿命缩短的问题,还能向地址空间引入更多的随机性来提高安全级别;同时,由于加密和磨损均衡的某些执行步骤重合,因此将它们集成到一站式的解决方案中比独立并分开执行的开销更低。文中描述了两个不同层次的磨损均衡和加密过程,即页级别和块级别;同时提供了两种算法,即 SEDURE-enc 和 SEDURE-wl,供使用者根据数据的安全级别或内存使用寿命灵活运用。

与上文提升 NVM 耐久性的方案类似,除了通过磨损均衡的方法增加 NVM 的耐久性,还可以减少写入量和写入次数。

在内存加密的基础上,可以考虑通过减少写入量和写入次数的方式延长 NVM 的使用寿命。Yong 等提出的 DEUCE[13]方案正是利用了这一想法。实验观察发现,典型的写回操作平均修改 cacheline 中的 12 个比特位,加密导致写入位数几乎增加了 4 倍;而 DEUCE 仅对修改过的内容进行重新加密,有效减少了修改位数,以减少写入量的方式延长了 NVM 的使用寿命。

Silent Shredder[14]方案表明,大量的内存写入是由操作系统中的数据碎化(shredding)产生的。数据碎化是系统中最常见的操作之一,是指在每个物理内存页映射到进程之前将其初始化为零的过程。虚拟化和服务器的整合,使得 shredding 的频率进一步增加,影响了 NVM 的寿命及性能。文献[14]提出了 Silent Shredder 的方案,该方案对标准计数器模式进行改进,完全消除了 shredding 产生的写入(shredding write),而且能够加速读取 shreded cache line,降低能量消耗;此外,在减少写入量的基础上,还对读取进行了优化。

Jalili 等[15]认为,加密算法增加了数据块的信息密度,当时已有的 NVM 寿命增强方案不适用于加密场景。基于这一观点,他们提出了 CryptoComp:利用压缩后数据块减小的优势来延长内存系统寿命并提高其安全性。文中主要通过压缩和选择性加密来限制由加密算法引起的效应,减少了写操作和写入量。对于高可压缩数据块,遵循完全加密方式;对于不太可压缩数据块,依赖非确定性的选择加密机制。

目前针对 NVM 内存的加密方式有直接加密机制和计数器加密机制两种。i-NVMM 和 Kong 等设计的加密方案是其中的典型代表;且针对这些方案的不足,出现了相应的改进方案。内存加密会对 NVM 寿命产生消极影响,因此在设计内存加密模块时,减少对 NVM 寿命的损耗也是一个必须考虑的条件。

2.1.2 数据完整性问题

尽管目前已经有众多针对非易失内存数据机密性的研究,但针对数据完整性的研究内容相对较少。数据完整性可检测数据是否被攻击者篡改、丢失或发生错误。

目前的完整性认证方案除了传统的 Merkle Tree(MT)内存认证,还有 ASSURE 和 TREBIVE 方案。传统的 MT 内存认证可以有效阻止数据的篡改攻击,但大大增加了 NVM cell 的写入和内存访问,增加了 NVM 的使用能耗,缩短了 NVM 的使用寿命,整个系统的性能不佳。ASSURE[16]是一个低消耗、高效能的 NVM 认证方案,协同整合了智能消息认证码(SMAC),使用 MMTs(multi-root MTs)仅对修改后的内容进行 MAC 计算以消除多余的写操作;它保留了经典 MT 身份认证的安全属性,并与所有的 NVM 加密方案兼容。TREBIVE[17]是一个基于数据的完整性认证环境,为现有的 CTOS 提供了基于 VMM 的内存完整性和机密性保护。

除了保密性问题,NVM 内存环境下的数据完整性问题同样值得关注。数据遭到篡改、丢失或发生错误等会对生产和生活产生重要的影响,因此确保数据完整性是 NVM 内存安全性极为重要的一环。

2.2 NVM 与 DRAM 构成混合内存

当 NVM 与 DRAM 组合作为混合内存时,可能产生指针指向不明和非易失内存泄露问题。

1)指针指向不明问题,在 NVM 与 DRAM 组合作为混合内存时可能发生。例如,将某个指向易失区域的指针放置在非易失区域时,若系统突然发生故障或掉电,则该指针将指向不确定的内存地址,从而产生一定的安全风险。

NV-heaps[18]是一个轻量级、高性能的面向持久对象的系统,其架构如图 3 所示。该系统除了能避免常见的悬挂指针和锁错误(locking errors)等故障,还防止了指针指向不明的问题(hard-to-find pointer bugs)。

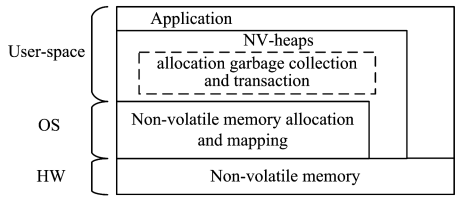

图 3 NV-heaps 结构图

Fig. 3 NV-heaps architecture

NV-heaps 将地址空间划分成了易失性区域和非易失性区域,从而可能产生 4 种新的指针类型,如表 2 所列。为保证程序的正常运行,须满足以下条件:①不能存在 NV-to-V 指针,即位于非易失性堆而指向易失性区域的指针,因为当程序结束时,指针即失效;②不能存在 inter-heap NV-to-NV 指针,即位于一个非易失性堆而指向另外一个非易失性堆。注意,inter-heap NV-to-NV 指针与 intra-heap NV-to-NV 不同,intra-heap NV-to-NV 指针表示位于非易失性堆,且指向该堆内部的指针[6]。

表 2 易失性与非易失性指针

Table 2 Volatile and non-volatile pointers

Allocated Apace Attribute	Target Apace Attribute	
	Volatile	Non-volatile
Volatile		V-to-NV pointers
Non-volatile	NV-to-V pointers	Intra-Heap/Inter-Heap NV-to-NV pointers

2）内存泄露指不再使用的内存由于疏忽或错误没有被释放，造成了内存的浪费。对于传统内存，内存泄露会导致程序崩溃，但可以通过重新启动程序解决[7]。对于 NVM 而言，由于重新启动不需要从外存中读取数据进行重建，因此内存泄露造成的问题不能通过重启程序解决，会产生严重的影响。这里，可以将持久化内存泄漏看作指针指向不明问题的一种特殊情况。

Mnemosyne[19]是一个轻量级的持久化存储系统，同时也是少数涉及非易失性内存泄露问题的系统，图 4 给出其结构图。Mnemosyne 提供了两种机制来防止泄漏：①在进行内存分配时，将持久性指针指向分配内存，避免了系统崩溃时丢失内存；②对 NVM 进行虚拟化，以确保一个程序的内存泄漏不会对其他程序产生影响，即使发生泄漏，程序也可以通过分配新的持久性内存区域将数据从现有区域复制到新内存区域进行恢复[6]。此外，还有各种各样的语言级技术能防止泄漏，包括垃圾回收、智能引用计数指针等。

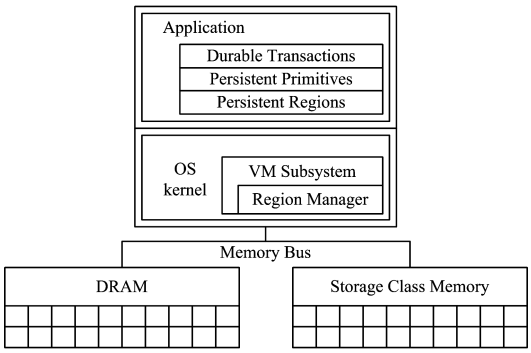

图 4　Mnemosyne 结构图

Fig. 4　Mnemosyne architecture

2.3　内存通用安全问题

对于需要原子操作的写流程，系统故障只写部分内容会导致内存的一致性问题；此外，对于基于 DRAM 的传统内存，数据保持依赖于不断的刷新，当发生系统故障或断电时，DRAM 中的数据丢失，通过重新启动从持久性存储中读取数据来重建内存，这时没有不一致现象。但对于 NVM，发生故障或断电后，数据依然保持在内存中。由于 CPU 输出到内存的数据是乱序的，DRAM 可直接重新运行程序；但对于 NVM，运行了一半的程序如何继续运行并确保获得正确的运行结果，值得研究。

当 NVM 作为内存时，不论是作为直接内存还是与 DRAM 构成混合内存，都会有一致性问题，且一致性问题可能造成严重的后果。

Chen 等[20]研究了持久性内存中的 B+-Trees，其被广泛应用于数据库和数据密集型系统。文献[20]提出了一种新型的内存 B+-Trees——wB+-Trees，旨在减少 NVM 写入和 CPU 缓存刷新操作产生的性能开销。wB+-Trees 利用节点中的原子写入或通过重做日志记录来实现节点的一致性。

Atlas[21]是一种基于锁代码（lock-based code）的持久性语义系统，可在 NVM 的上下文中自动提供基于锁的程序和有用的持久性语义，在系统存在故障的情况下自动保持全局一致性的状态。

ThyNVM[22]采用基于硬件的机制，提供 DRAM 和 NVM 混合内存的软件透明（software-transparent）的崩溃一致性保证。文献[22]提出了两种粒度的数据检查点，即高度缓存块（cache block）粒度和页（page）粒度，同时以协调的方式启用多个粒度的检查点，自动对内存状态进行定期检查，最大程度地减小对程序执行时间的影响。

3　基于 NVM 的 SCM 安全问题

NVM 作为 SCM 时，需要合适的字节寻址监管机制，以及持久性和一致性保证。

3.1　字节寻址监管机制

将 NVM 作为 SCM 时，使用 load/store 命令直接操作持久化数据，无需使用耗时的基于块的磁盘 IO。这种做法在带来高性能的同时也产生了一定的风险：直接使用 load/store 命令操作持久化数据，NVM 将直接暴露给进程和内核的虚拟地址空间，若应用或驱动程序存在缺陷，则可能导致杂散写入（stray writes）；此外，传统操作系统采用虚拟内存管理器对内存进行管理，持久性存储则采用文件系统和块驱动器进行管理，无需使用基于块的磁盘 I/O，使得传统文件系统的管理权限被绕过，因此需要设计新的权限监控机制。

Dullor 等[23]提出的 PMFS 是一个轻量级的 POSIX 文件系统，其利用 NVM 的字节寻址能力有效避免了面向块存储产生的开销，应用程序能够直接访问 NVM。PMFS 利用简单的硬件原语提供了一致性保护；同时，为实现较高的性能，PMFS 将整个 NVM 映射到内核虚拟地址空间；且提供了写保护机制，以防止操作系统或驱动程序中的错误导致的 stray writes 对设备产生损坏。

Chen 等[24]采用混合存储模型，通过将 NVM 集成到计算系统中，设计了 PMBD 块存储驱动程序。其利用以下几种保护机制来防止 stray writes 产生的不利影响：1）基于页面的保护，通过分页隔离进程的地址空间并共享有限的物理内存；2）基于私有映射（private mapping）的保护，将页面动态映射到内核空间，而不是通过控制每个页面的可访问性来提供写保护。因此，大多数时候 NVM 空间对操作系统的内核代码是不可见的，防止了 stray writes 可能造成的损害。

字节寻址特性除了使得 NVM 直接暴露给应用进程而可能产生 stray writes 外，还会旁路文件系统，新的权限监控机制因此产生。

Aerie[25]是一种灵活的文件系统架构，将 SCM 直接暴露给用户程序，在不与内核交互的情况下也能读写文件，降低了操作系统内核在文件访问中的参与度。为了减少因恶意用户访问元数据而导致的安全问题，Aerie 设计了分散的元数据访问架构：不可信的库（libFS）和可信的服务（TFS）。用户可以通过 libFS 访问 NVM 上的数据，而通过 TFS 进行元数据的更新或并发访问。

SCMFS[26]是专门为 SCM 设计的文件系统。对于传统的持久存储设备，I/O 延迟带来的开销远大于文件系统层本身；

而对于 SCM,因存储设备直接连接存储总线,故降低文件系统开销即可降低存储系统中的 CPU 开销,从而提升总体性能。SCM 在虚拟空间构建文件系统,并利用内存管理单元(MMU)将文件系统地址映射到 SCM 上的物理地址,物理和虚拟地址空间中的布局简单;且 SCMFS 中每个文件的空间连续,因此在文件系统中处理读/写请求的过程将被简化。SCM 简单易实现,性能表现良好。SCMFS 对小文件请求的性能提升较为明显,对大文件的效果相对较弱。

3.2 SCM 持久性和一致性保证

传统的内存一致性模型中,应用程序将数据顺序写入处理器核可见的共享区域,数据持久化由文件系统完成。使用 NVM 后,由于其既能够作为内存,又能够作为持久化存储,为了充分发挥其性能,通常旁路文件系统,应用程序将数据直接写入持久化内存[19]。由于文件系统不能正常完成数据的持久化工作,因此需要将内存一致性模型延伸到持久化存储系统中。

Heapo[27]继承了 Mnemosyne 的部分思想,有自己管理的堆空间,即一个预先分配的内存块;使用不连续分配的虚拟地址空间,采用静态地址映射,物理地址和虚拟地址对固定不变。Heapo 仅能保证其维护的几种数据结构(链表、哈希表和 B 树)的数据一致性,对于其他的数据结构,比如红黑树和 B+树,由于是用户自定义数据结构及相关操作,因此无法保证其数据的一致性。

对持久存储而言,一致性需要串行化写入操作,耐久性会降低写入速度。由于内存和持久化存储两者存在差异,直接利用 NVM 作为内存或持久化存储并不能得到最佳结果,反而会失去一些优化机会,无法利用 NVM 的最佳特性。NVM Duet[28]的设计目标是为持久存储提供所需的一致性和持久性保证,它采用跨层方式,当 NVM 作为内存时,则放松约束,以提高系统的性能。NVM Duet 采用智能刷新技术,利用 NVM 的设备特性来消除不必要的刷新开销。

4 其他通用安全问题

1)冷启动攻击利用了内存单元在断电后数据会保持一定的时间才会消失的特性,将断电后的内存单元置于低温环境下,这样内存单元中的数据会保存更长的时间,攻击者可以将内存上的数据转移到执行攻击的计算机上,获取内存快照,并从中提取密钥等重要信息。目前,针对冷启动攻击还没有较好的抵御办法,只有在一些特定限制条件下才可以抵御冷启动攻击,常用的方法有密码学方法和系统化方法[29]。冷启动的攻击条件是数据被保留更长的时间,与 NVM 的非易失特性易遭受断电后攻击相近。

2)侧信道攻击是指从密码系统的物理实现中获取时间、功率消耗和电磁泄露等信息,从而对系统进行破解,而非暴力破解或利用算法分析。针对 NVM 的侧信道攻击有:光学注入攻击、局部加热攻击、测量 EEPROM 存储单元电荷[30]等。

对于新型非易失存储器件,如 PCM,当保存在 cell 中的位被反复翻转时,其物理特性会发生变化,可能产生侧信道信息泄露。Xu 等[31]对 PCM 的调频效应(seasoning effect)进行了研究,提出了对 AES 的密钥恢复攻击。实验假设 AES 采用流水线的方式实现,且中间结果被存储在 PCM 存储阵列中,AES 加密密钥对攻击者来说是未知的,对于给定明文,攻击者可以知晓或控制其加密次数。当系统对给定的明文加密后,攻击者可以检查内存单元,预测密钥值。针对该攻击,文中提出内存位置混淆和内存重新使用两种解决方案。

Mao 等[32]发现,NVM 行缓冲区命中(row buffer hit)信息会泄露地址映射的详细信息,通过利用这些信息可以对设备进行磨损攻击,即使目前最先进的磨损均衡方案也只能抵御 137 s 的 NVM 磨损攻击。为了对抗该攻击,文献[32]提出了一种行内交换(IRS)的策略,以隐藏磨损细节。

冷启动攻击和侧信道攻击是常见的攻击方式,不限于 NVM,其他设备或环境下也可能发生。冷启动攻击的攻击方式多样,且目前没有合适的防御办法;对于侧信道攻击,针对相应的攻击办法应采用合适的抵御方式。

5 研究展望

5.1 硬件层面

1)降低当前耐久性方案的开销或设计新方案

目前的磨损均衡方案包括针对 NVM 器件的方案,以及 NVM 处于不同环境下的磨损均衡方案。各方案都有一定的适用场景,且需要一定的开销。怎样对现有方案进行更优的设计,以扩大其适用范围或降低开销,是研究人员可进一步思考和探究的。

除了对原有的方案进行改进之外,发现新的攻击方式,并针对该攻击方式设计新的磨损均衡方案,或发现新的减少写入量和写入次数的方法,也有助于抵抗攻击者有目的的写入攻击,延长 NVM 的使用寿命,降低开销。

2)应用冷启动攻击、侧信道攻击的新方式

尽管目前只有在特定条件下才能够抵抗冷启动攻击,但随着技术的发展,将特定环境下的抵御冷启动攻击的方案扩展到一般状态并应用到 NVM 领域,是值得期待的。

目前,侧信道攻击的相关已有研究内容依然较少,但侧信道攻击方式多样,且可能造成严重的损失。例如,利用时间频次等信息猜测磨损均衡映射方案,针对猜测方案的弱点进行写入攻击造成设备损坏等。新的侧信道攻击方式,将不断催生新的防御方案。

5.2 操作系统层面

1)设计新的加密方案

针对 NVM 持久性内存的数据机密性保护措施的研究主要集中在采用加密算法对内存进行加密;现有的加密机制有直接加密机制和计数器加密机制两种。然而,由于扩散等特性,直接加密在少量明文发生变化时会导致大量的密文变化,从而产生大量的写操作,对 NVM 的性能、寿命均产生影响。计数器加密模式是目前主流的内存加密技术,但仍然存在着计数器溢出、虚拟内存支持不足和全内存加密开销大的问题。

对于两种加密机制存在的不足,目前已经有学者展开研

究并获得了一定的成果。未来是否有其他新的更好的加密机制运用到 NVM 内存加密中,也是一个值得关注的研究方向。

2)完整性保证方案

NVM 加密确保了数据的机密性,但并不能保证数据的完整性。目前有较多针对 NVM 数据机密性的研究,但确保数据完整性的方案较少。MT 内存认证能够确保数据的完整性,但增加了单元写入和存储器访问量,造成 NVM 能耗和性能损失。ASSURE 为最新的安全节能 NVM 认证方案。数据完整性认证关系到用户数据是否遭到篡改、是否有丢失、是否存在错误等,因此需要针对数据完整性设计相应的保证方案。

3)NVM 环境下的常见内存攻击

NVM 环境下的内存安全问题,除了前文所述的冷启动攻击、侧信道攻击、内存泄露等,还有代码破坏攻击、信息泄露、数据攻击、控制流劫持攻击[7]等常见的内存攻击方式。由于非易失性和耐久性等特性,在磁盘下针对这些攻击的解决方式在 NVM 环境下的适用性降低,需要针对 NVM 的特性设计新的针对常见内存攻击方式的解决方案。

5.3　编程模型层面

1)延伸内存一致性模型

传统的内存一致性模型不再适用于 SCM 环境,需要设计新的编程模型。将内存一致性模型延伸到持久化存储中,解决因应用程序绕过文件系统,直接对 NVM 进行操作,而略过的持久化问题。

2)面向 SCM 的字节寻址监管机制

存储级内存 SCM 是利用 NVM 实现的新型存储技术,有望实现内外存的统一。当 SCM 作为内存和外存时,其控制单元和访问方式均不同。当作为内存时,由内存控制器管理;当作为外存时,采用文件系统等方式管理,因此需要设计新的权限保护机制,以更好地实现权限和保护机制。

5.4　其他

便携系统,如手机、便携式媒体播放器,通常都会使用 NVM 来保存数据与元数据。与在计算机系统上一样,在移动设备上,NVM 的非易失、字节寻址等特性依然存在,因此也存在着相似的安全问题。但移动设备与计算机系统又存在不同,如移动设备的能耗、空间等限制远比计算机系统严苛,因此 NVM 在移动设备端使用时存在的安全问题也值得关注。

目前已有学者针对 NVM 应用于移动设备时的相关问题展开了研究,相信未来会有更多的 NVM 移动设备安全相关技术问世。

结束语　大数据时代的来临,使得传统以计算为中心的处理模式转向以数据为中心的处理模式,即内存计算。这对传统系统架构提出了挑战,新型非易失存储器件的诞生为应对这些挑战提供了新的选择。非易失性、空闲低功耗、字节寻址等特点,使得新型非易失存储器件能够作为直接内存或与 DRAM 组合为混合内存,或作为持久性外存。

利用 NVM 构建新型存储体系的过程中也会存在各种问题。文中主要针对基于 NVM 的存储安全问题进行了讨论,从 NVM 特性的角度对各安全问题进行探讨:1)耐久性,由于耐久性不高,写入次数有限,NVM 易遭受磨损攻击;2)非易失性,当 NVM 作为内存时,断电后数据依然保留,则可能遭受攻击,也可能产生一致性、指针悬挂等问题;3)字节寻址,该特性使得应用程序能够绕过文件系统等权限机制而直接访问 NVM,存在安全隐患。针对以上问题,目前已有磨损均衡、内存加密、一致性保证等解决办法。

尽管 NVM 目前还在研究阶段,且应用到传统存储系统中时存在着各种问题,NVM 自身也存在着如读写不对称和写入次数有限等缺陷,但其优越的特性依然使其备受研究人员的关注。充分利用 NVM 的性能优势,构造新型的大容量、高性能的存储系统,未来整个计算机系统将充满希望!

参 考 文 献

[1] MAO W,LIU J N,TONG W,et al. A Review of Storage Technology Research Based on Phase Change Memory[J]. Chinese Journal of Computers,2015,38(5):944-960. (in Chinese)
冒伟,刘景宁,童薇,等. 基于相变存储器的存储技术研究综述[J]. 计算机学报,2015,38(5):944-960.

[2] QURESHI M K,KARIDIS J,FRANCESCHINI M,et al. Enhancing Lifetime and Security of Pcm-Based Main Memory with Start-Gap Wear Leveling[C]// Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture. New York:ACM,2009:14-23.

[3] ZHAO M,SHI L,YANG C,et al. Leveling to the Last Mile:Near-Zero-Cost Bit Level Wear Leveling for Pcm-Based Main Memory[C]// 32nd IEEE International Conference on Computer Design. Seoul:IEEE,2014:16-21.

[4] HUANG F,FENG D,XIA W,et al. Security Rbsg:Protecting Phase Change Memory with Security-Level Adjustable Dynamic Mapping[C]// 2016 IEEE International Parallel and Distributed Processing Symposium. Chicago:IEEE,2016:1081-1090.

[5] ZHANG X,SUN G. Toss-Up Wear Leveling:Protecting Phase-Change Memories From Inconsistent Write Patterns[C]// Proceedings of the 54th Annual Design Automation Conference. Austin:ACM,2017:3.

[6] XU Y C,YAN J F,WAN H,et al. A Survey on Security and Privacy of Emerging Non-volatile Memory[J]. Journal of Computer Research and Development,2016,53(9):1930-1942. (in Chinese)
徐远超,闫俊峰,万虎,等. 新型非易失存储的安全与隐私问题研究综述[J]. 计算机研究与发展,2016,53(9):1930-1942.

[7] SZEKERES L,PAYER M,WEI L T,et al. Eternal War in Memory[J]. IEEE Security & Privacy,2014,12(3):45-53.

[8] CHHABRA S,SOLIHIN Y. I-Nvmm:A Secure Non-Volatile Main Memory System with Incremental Encryption[C]// 2011 38th Annual International Symposium on Computer Architecture. San Jose:IEEE,2011:177-188.

[9] KONG J,ZHOU H. Improving Privacy and Lifetime of Pcm-

Based Main Memory[C]// Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks. Chicago:IEEE,2010:333-342.

[10] HUANG F,FENG D,HUA Y,et al. A Wear-Leveling-Aware Counter Mode for Data Encryption in Non-Volatile Memories [C]// 2017 Design,Automation & Test in Europe Conference & Exhibition. Lausanne:IEEE,2017:910-913.

[11] SWAMI S,MOHANRAM K. Covert:Counter Overflow Reduction for Efficient Encryption of Non-Volatlle Memories[C]// 2017 Design,Automation & Test in Europe Conference & Exhibition. Lausanne:IEEE,2017:906-909.

[12] LIU C,YANG C. Secure and Durable (Sedura):An Integrated Encryption and Wear-Leveling Framework for Pcm-Based Main Memory[C]// Proceedings of the 16th ACM SIGPLAN/SIGBED Conference on Languages,Compilers and Tools for Embedded Systems. Portland:ACM,2015:12.

[13] YOUNG V,NAIR P J,QURESHI M K. Deuce:Write-Efficient Encryption for Non-Volatile Memories[C]// Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems. Istanbul:ACM,2015:33-44.

[14] AWAD A,MANADHATA P,HABER S,et al. Silent Shredder:Zero-Cost Shredding for Secure Non-Volatile Main Memory Controllers[C]// Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems. Atlanta:ACM,2016:263-276.

[15] JALILI M,SARBAZI-AZAD H. Endurance-Aware Security Enhancement in Non-Volatile Memories Using Compression and Selective Encryption[J]. IEEE Transactions on Computers,2017,66(7):1132-1144.

[16] RAKSHIT J,MOHANRAM K. Assure:Authentication Scheme for Secure Energy Efficient Non-Volatile Memories[C]// Proceedings of the 54th Annual Design Automation Conference 2017. Austin:ACM,2017:11.

[17] HASHIMOTO M,YAMADA N,KANAI J. Trebivetm:A Tree Based Integrity Verification Environment for Non-Volatile Memory System[C]// 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing. Zhangjiajie:IEEE,2015:279-289.

[18] COBURN J,CAULFIELD A M,AKEL A,et al. Nv-Heaps:Making Persistent Objects Fast and Safe with Next-Generation,Non-Volatile Memories[J]. ACM SIGPLAN NOTICES,2011,46(3):105-118.

[19] VOLOS H,TACK A J,SWIFT M M. Mnemosyne:Lightweight Persistent Memory[C]// Proceedings of the 16th International Conference on Architectural Support for Programming Languages and Operating Systems. Newport Beach:ACM,2011:91-104.

[20] CHEN S,JIN Q. Persistent B+-Trees in Non-Volatile Main Memory[J]. Proceedings of the VLDB Endowment,2015,8(7):786-797.

[21] CHAKRABARTI D R,BOEHM H,BHANDARI K. Atlas:Leveraging Locks for Non-Volatile Memory Consistency[J]. ACM SIGPLAN NOTICES,2014,49(10):433-452.

[22] REN J,ZHAO J,KHAN S,et al. Thynvm:Enabling Software-Transparent Crash Consistency in Persistent Memory Systems [C]// Proceedings of the 48th International Symposium on Microarchitecture. Waikiki:IEEE,2015:672-685.

[23] DULLOOR S R,KUMAR S,KESHAVAMURTHY A,et al. System Software for Persistent Memory[C]// Proceedings of the Ninth European Conference on Computer Systems. Amsterdam:ACM,2014:15.

[24] CHEN F,MESNIER M P,HAHN S. A Protected Block Device for Persistent Memory[C]// 2014 30th Symposium on Mass Storage Systems and Technologies. Santa Clara:IEEE,2014:1-12.

[25] VOLOS H,NALLI S,PANNEERSELVAM S,et al. Aerie:Flexible File-System Interfaces to Storage-Class Memory[C]// Proceedings of the Ninth European Conference on Computer Systems. Amsterdam:ACM,2014:14.

[26] WU X,REDDY A L. Scmfs:A File System for Storage Class Memory[C]// Proceedings of 2011 International Conference for High Performance Computing,Networking,Storage and Analysis. Seattle:ACM,2011:39.

[27] HWANG T,JUNG J,WON Y. Heapo:Heap-Based Persistent Object Store[J]. ACM Transactions on Storage,2015,11(1):3.

[28] LIU R,SHEN D,YANG C,et al. Nvm Duet:Unified Working Memory and Persistent Store Architecture[J]. ACM SIGARCH Computer Architecture News,2014,42(1):455-470.

[29] YANG Y,GUAN Z,CHEN Z. Survey of cold boot attack [J]. Application Research of Computers,2015,32(10):2886-2890. (in Chinese)
杨阳,关志,陈钟.冷启动攻击研究综述[J].计算机应用研究,2015,32(10):2886-2890.

[30] DYKA Z,WALCZYK C,WALCZYK D,et al. Side Channel Attacks and the Non Volatile Memory of the Future[C]// Proceedings of the 2012 International Conference on Compilers,Architectures and Synthesis for Embedded Systems. Tampere:ACM,2012:13-16.

[31] XU L,SHI W,DESALVO N. Seasoning Effect Based Side Channel Attacks to Aes Implementation with Phase Change Memory [C]// Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy. Minneapolis:ACM,2014:5.

[32] MAO H,ZHANG X,SUN G,et al. Protect Non-Volatile Memory From Wear-Out Attack Based on Timing Difference of Row Buffer Hit/Miss[C]// 2017 Design,Automation & Test in Europe Conference & Exhibition. Lausanne:IEEE,2017:1623-1626.