持久化内存文件系统的磨损攻击与防御机制

- 1 研究动机
  - 持久化内存文件系统
    - 元数据
      - (1) 超级块.保存文件系统的全局信息,如 NVM的空闲页数和空闲索引节点数等
      - (2) 索引节点.保存文件的基本信息,如文件大小、文件数据的最后访问时间(atime)等
      - (3) 文件索引结构
    - 文件数据
    - 日志
- 2 针对 NVM的磨损攻击
  - 攻击方式 1:利用创建文件和删除文件操作执行磨损攻击
    - 创建文件
      - (1) 申请索引节点
      - (2) 申请物理页,创建文件索引结构
      - (3) 在父目录插入一条目录项
      - (4) 修改超级块的空闲页数和空闲索引节点数
    - 删除文件
      - (1) 释放文件索引结构的物理页
      - (2) 在父目录删除文件的目录项
      - (3) 释放索引节点
      - (4) 修改超级块的空闲页数和空闲索引节 点数
  - 攻击方式 2:利用创建硬链接和删除硬链接操作执行磨损攻击
    - 创建硬链接
      - 1) 在目标文件的父目录增加一条目录项
      - 2) 源文件索引节点的链接数加一
    - 删除硬链接
      - 1) 在目标文件父目录删除一条目录项
      - 2) 源文件索引节点的链接 数减一
  - 攻击方式 3:利用创建软链接和删除软链接操作执行磨损攻击
    - 创建软链接
      - 1) 申请目标文件的索引节点
      - 2) 在目标文件父目录增加目录项
      - 3) 申请物理页保存源文件的位置信息
      - 4) 修改超级块的空闲页数和空闲索引节点数
    - 删除软链接
      - 1) 释放保存源文件位置信息的物理页
      - 2) 在目标文件父目录删除目标文件的目录项
      - 3) 释放目标文件的索引节点
      - 4) 修改超级块的空闲页数和空闲索引节点数
  - 攻击方式 4:利用文件覆盖写操作执行磨损攻击
    - 采用预写日志机制实现数据一致性
      - 1) 把更新内容写入日志
      - 2) 把更新内容写入文件
      - 3) 修改索引节点
    - 采用写时复制机制实现数据一致性
      - 1) 把更新内容写入新申请的物理页
      - 2) 修改文件索引结构
      - 3) 修改索引节点
      - 4) 释放被替换的文件数据页
      - 5) 修改超级块的空闲页数
  - 攻击方式 5:利用文件重命名操作执行磨损攻击
    - 1) 在目标文件的父目录增加一条目录项
    - 2) 在源文件父目录删除该文件的目录项
    - 3) 修改索引节点
- 3 磨损防御机制 PFWD
  - 3.1 概 述
  - 3.2 索引节点元数据虚拟化技术
    - 每次更新索引节点, 需要增加该索引节点对应的 vInode 的写计数器.如果 vInode 的写次数达到设定的迁移阈值 Wp,则查找 vInode 写计数器,把该索引节点数据拷贝到一个空闲的索引节点的 Inode slot;然后把该索引节点对应的 vInode 的计数 器清零;最后,在索引节点映射表修改偏移量,实现索引节点的动态迁移
  - 3.3 超级块迁移技术
    - 设置一个超级块指针,即把 NVM 物理空间的前 8 个字节作为超级块指针,用来保存超级块存储区的首地址,超级块可以迁移,当超级块存储区的写次数达到迁移阈值Wq,则把超级块迁移到磨损低的物理页
  - 3.4 文件数据页磨损均衡技术
    - 使用日志文件数据页替换文件被修改数据页.每次数据写入日志文件数据页,都判断其写次数是否达到迁移阈值,达到则做 数据迁移.对文件执行数据追加操作,都是从空间管理模块申请磨损低的物理页来保存追加数据
  - 3.5 文件索引结构迁移技术
    - 每次更新文件索引结构的索引项,都判断该索引项所在物理页的写次数是否达到迁移阈值Wq:如果 没有达到迁移阈值,则直接修改索引项;如果达到迁移阈值,则拷贝该索引项所在物理页的所有索引项到空闲且 磨损低的物理页,修改索引项.然后修改上一级索引项,再判断上一级索引项所在的物理页的写次数是否达到迁 移阈值 Wq:如果没有达到迁移阈值,则本次文件索引结构迁移完成;如果达到迁移阈值,则对上一级文件索引结 构做迁移.按此迭代操作
- 4 实验结果与分析
  - 4.1 实验配置
  - 4.2 NVM磨损分析
  - 4.3 性能实验对比
- 5 结 论