From random block corruption to privilege escalatio：A filesystem attack vector for rowhammer-like attack

`MLC` `Flash` `Security` `FileSystem`

Kurmus A, Ioannou N, Papandreou N, et al. From random block corruption to privilege escalation: A filesystem attack vector for rowhammer-like attacks[J]. Usenix WOOT, 2017.

背景

研究者针对DRAM特性提出Rowhammer攻击，在非物理接触的基础上利用硬件漏洞实现攻击。Cai Yu2提出MLC NAND也存在这样的脆弱性和利用的可能。这篇文章利用Cai Yu的研究基础“通过闪存Cell干扰，实现随机的bit变化”，提出一种基于随机块破坏的攻击思路实现基于Ext3文件系统的提权攻击。需要说明的是，作者所展示的为非“full system”的攻击，重点说明文件系统层的一个攻击向量，并且假设底层闪存介质的脆弱性利用存在可能性。

MLC的脆弱性

- 闪存的介质特点
  - P/Es cycles的增加，使得MLC NAND的可靠性下降，即bit errors会增加。
  - Cell-to-Cell干扰。由于电容耦合效应，当对一个cell施加电压时会影响相邻的cell产生干扰造成电容上的电子变化。
  - 阈值电压的不稳定性（进行多次的加电）会造成的bit错误情况加重。
  - 对于正在写的MLC，大量的读操作会使还未完成写的页bit错误率增加。

使用CCI(Cell-to-cell interference)的方式，攻击者可以采用一种最大化干扰的数据写模式，实现对victim页的随机修改

- 一些闪存管理机制的绕过
  - ECC绕过**“较为困难”**。在纠错能力为T的前提下，有三种解码结果。一种情况下，解码成功，说明数据中出错的bit数不大于T;第二种情况是解码失败，出错bit数目大于T且出错后的码字没有落入另外一个码字的范围；第三种情况是，出错bit数目大于T，且出错后的码字落入了另外一个码字的范围，此时ECC不能检测到出错bit并且会返回成功。

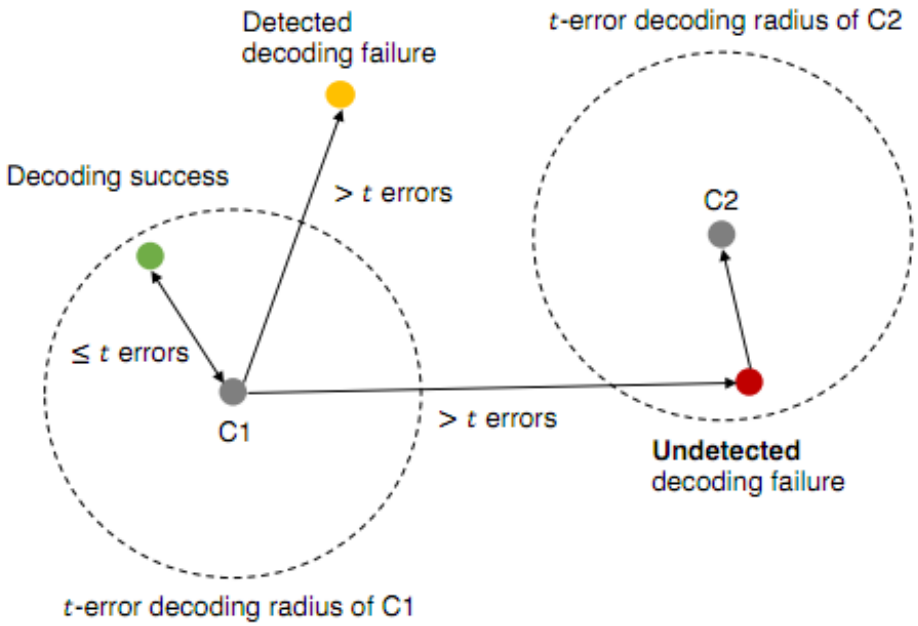
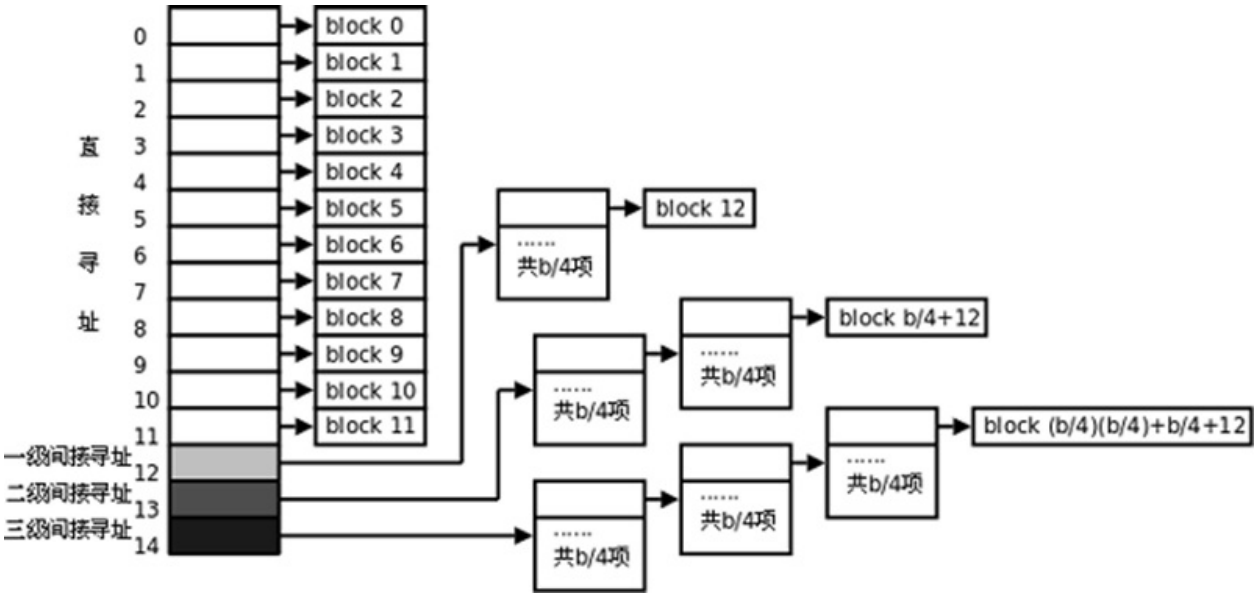


Figure 1: The three possible decoding events that can be induced by injecting errors into a Flash codeword (C1).

  - FTL管理机制的绕过。GC操作，等待GC完成。磨损均衡，与页的分配有关。文中的讨论不够深入和完善，比较牵强。

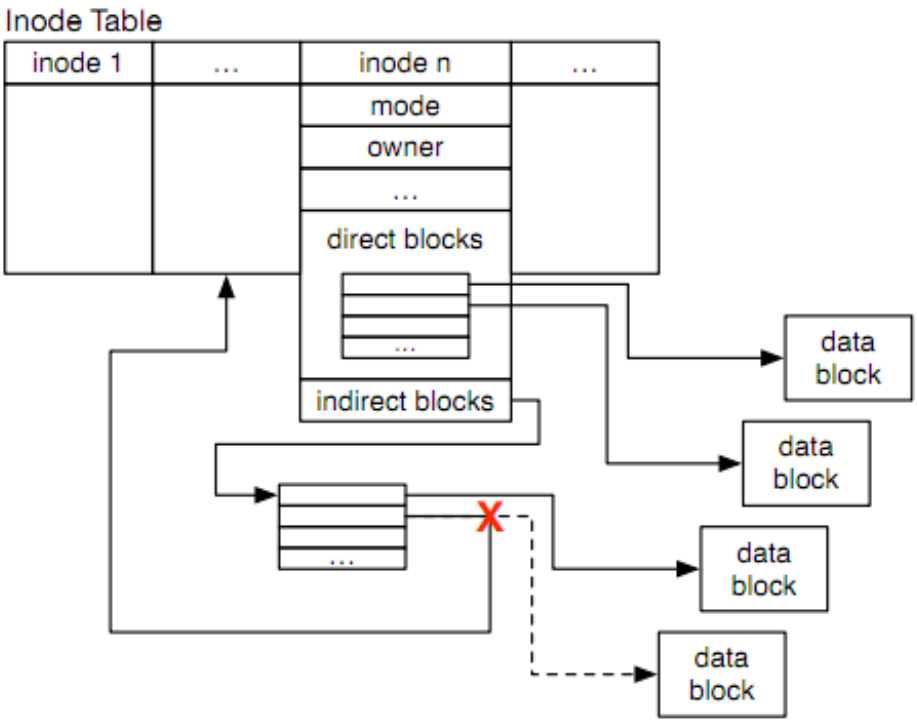
文件系统层的攻击向量

- EXT3的文件组织
  - 通过inode号查到inode数据地址，其中记录文件的数据和文件数据块地址。其中有12个指针为直接数据块地址，另外三个分别为多级的间接块地址。间接块中可能记录直接数据块地址也可能记录了下一级间接块的地址。由此也可以解释文件系统可支持的最大文件大小。



Block size:	1 KiB	2 KiB	4 KiB	8 KiB
max. file size:	16 GiB	256 GiB	2 TiB	2 TiB
max. filesystem size:	4 TiB	8 TiB	16 TiB	32 TiB

- 攻击利用方式
  - 通过闪存Cell-to-cell的目的，修改自己文件的某个间接块中的指针，使其指向inode table中的某个inode。从而将其他文件inode数据作为本文件的数据，达到随意修改的目的。进一步使次文件为一个shell文件，并实现setuid的目的，从而实现提权。概率计算上来讲有9%的成功率（不考虑ECC,FTL，仅考虑地址空间上能指向inode table的概率）。



视频网址

- https://www.youtube.com/watch?v=Mnzp1p9Nvw0

总结

这个工作首次提出rowhammer-like攻击在SSDs的一种攻击示例，并提出了一种基于文件系统的攻击向量，最后讨论了其局限性，即局限于EXT2/3文件系统，并且一些对元数据进行校验的文件系统如ZFS和一些进行数据加密的文件系统不受此攻击影响。
但是我感觉在闪存管理绕过的部分讨论的不太清楚，以及如何最大化cell-to-cell干扰部分很简略，再者找到文件对应的inode数据块位置（即victim）也是一个问题。