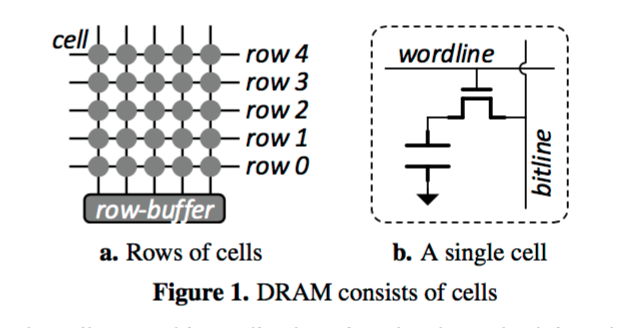
通杀所有系统的硬件漏洞? - 聊一聊Drammer，Android上的RowHammer攻击

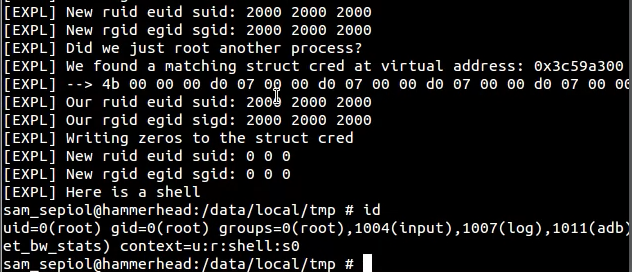
作者：蒸米@阿里移动安全

大家肯定知道前几天刚爆出来一个linux内核(Android也用的linux内核)的dirtycow漏洞。此洞可以说是个神洞，通过dirtycow，一个普通权限的app可以做到root权限的文件任意写，随后还可以转化为android上的通用root。就在大家纷纷埋头研究dirtycow的时候，Drammer横空出世，号称也可以root最新版的Android 6.0.1，同时还放出了论文（中了CCS：https://vvdveen.com/publications/drammer.pdf）和POC(https://github.com/vusec/drammer)。那么这个Drammer到底是什么东西呢？

Drammer可以说是一种针对android设备的攻击方式，利用的是内存芯片设计上的一个缺陷。然而，这个问题并不是只出现在Android系统上，而是所有使用内存的系统都会出现这个问题。最早提出这种攻击方式的人是卡内基梅隆大学的Yoongu Kim写的一篇paper -《Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors》(https://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf) 在这篇文章中，作者提到有个有趣的现象，如果不断的访问两个具有"侵略者"性质的虚拟地址会让一个具有"受害者"性质的内存数据进行位翻转，更神奇的是这个具有"受害者"性质的内存可能会在当前进程可访问的虚拟地址以外。为什么会有这种现象呢？原因是内存厂商为了能让内存芯片存储更多的数据，于是将内存中的DRAM（The Dynamic Random Access Memory）cell越做越小并且离的越来越近，从而导致相邻的cell在通电的过程中会受到影响。因此，如果我们不断的访问某个位置上的内存，就可能会造成相邻的内存进行位翻转。随后google project zero还通过PC上的linux提权，证明了这种现象的确存在并且可以用来进行攻击(https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html)并将这种攻击方式称为RowHammer。因此，这次出现的drammer是受之前研究的启发，从而实现了Android上的rowhammer攻击，所以drammer全称其实是DRoid and rowhAMMER。



在Android上，整个攻击的基本思路是：1. 先找到用户态可以flush内存的api，比如Android上的ION。2. 然后利用这个api配合上FLIP FENG SHUI技术进行rowhammer攻击。目的是位翻转Page Table Entry (PTE)并让其指向一个攻击者可以控制的内存上。3. 修改PTE从而控制整个物理内存。配合其他漏洞还可以做到远程攻击（DEMO：https://www.vusec.net/projects/drammer/）。



原来硬件上设计的缺陷还会出现这种问题，是不是感觉脑洞已经快要爆炸了。并且这次的攻击与操作系统和软件无关，纯粹是硬件上的漏洞导致的。因此，不光是linux和Android，Windows, OS X和iOS应该也是受影响的。唉，May god bless all electronic devices.