Meltdown和Spectre攻击的危害性分析

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

龚晓锐

gongxiaorui@iie.ac.cn

提纲

- 漏洞攻击场景
- Cache攻击的危害性
- 内存攻防中的猫鼠游戏
- 影响公众的重量级漏洞

Meltdown的攻击面

- **影响范围**

主要影响Intel CPU。

对于AMD和ARM CPU而言，尽管也会出现乱序执行，但由于其无序执行的规则以及执行效率等多方面的因素，导致目前公布的poc在非Intel的处理器上很难通过侧信道的手段来泄露内存数据。因此，目前已有的Meltdown攻击想要泄露移动终端上的内存数据尚存在困难。

- **威胁模型**

通过在本地低权限进程中执行恶意代码，攻击者可以获取包括内核空间在内的整个进程地址空间中的数据，造成数据泄露。

Meltdown的攻击场景

- **针对个人电脑**——Meltdown需要攻击者获取本地代码执行的机会。这可以通过在目标终端上安装一个恶意软件或者利用其它远程代码执行的漏洞来实现，在此基础上：

1. 低权限的恶意应用可以获取完整的内核内存。这意味着被攻击者其他进程（例如浏览器）中的敏感数据，泄露用户隐私信息。
2. 恶意进程获取到的内核信息，可能配合其他提权漏洞，帮助攻击者进行权限提升，造成信息泄露之外的危害。

Meltdown的攻击场景

- **针对数据中心——**Meltdown攻击需要获取本地代码执行的机会才能触发。对于数据中心而言，由于一台物理服务器上可能管理着不同用户的多个虚拟节点，因此可能带来额外的攻击面：

1. 攻击者可以通过在云端申请虚拟机的方式，在申请的节点上执行Meltdown攻击，获取云端虚拟机的内核数据。在共享内核的容器（例如docker,LXC,OpenVZ）中，攻击者能通过获取整个物理内存映射的方式，进一步获取该物理服务器上其他客户机中的的数据。

2. 攻击者获取到的物理内存映射信息，可以帮助其获得关键的内存数据。这意味着Meltdown可能帮助攻击者利用一些原本无法利用或很难稳定利用的漏洞，造成信息泄露之外的影响（例如虚拟机逃逸、本地提权等）。

Spectre的攻击面

- **影响范围**

影响具有分支预测功能的部分Intel,AMD,ARM处理器

- **威胁模型**

攻击者可以通过在本地执行Spectre攻击，获取本地其他进程中的内存信息。

由于Spectre攻击可以使用JavaScript实现，因此利用一个恶意页面远程攻击也是可行的。

Spectre的攻击场景

- **针对个人电脑**：

Spectre可以通过安装恶意程序的形式，在目标设备上执行，获取其他进程中的敏感数据，例如浏览器进程中的用户隐私信息。

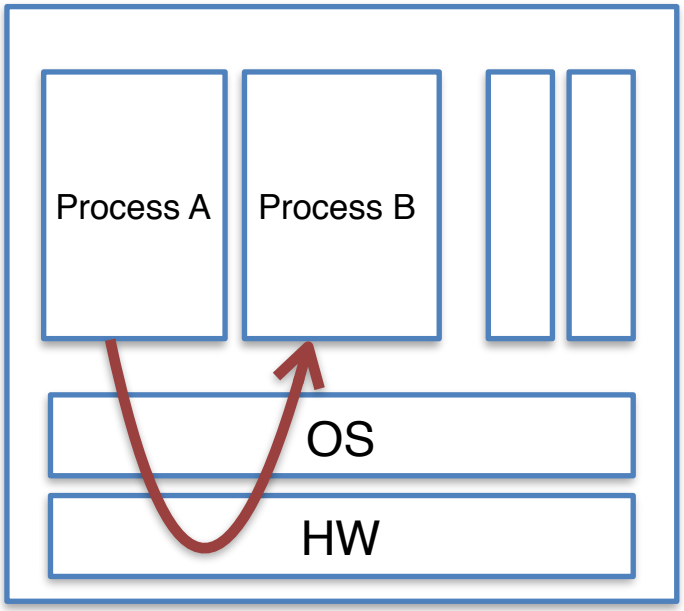
Spectre也可以使用Javascript编写，这意味着攻击者可以诱导目标设备访问一个恶意的web页面，从而获得远程执行的机会。一旦页面被浏览器加载，攻击者可以突破浏览器的进程沙箱，获取目标设备上其他进程的信息。

Spectre的攻击场景

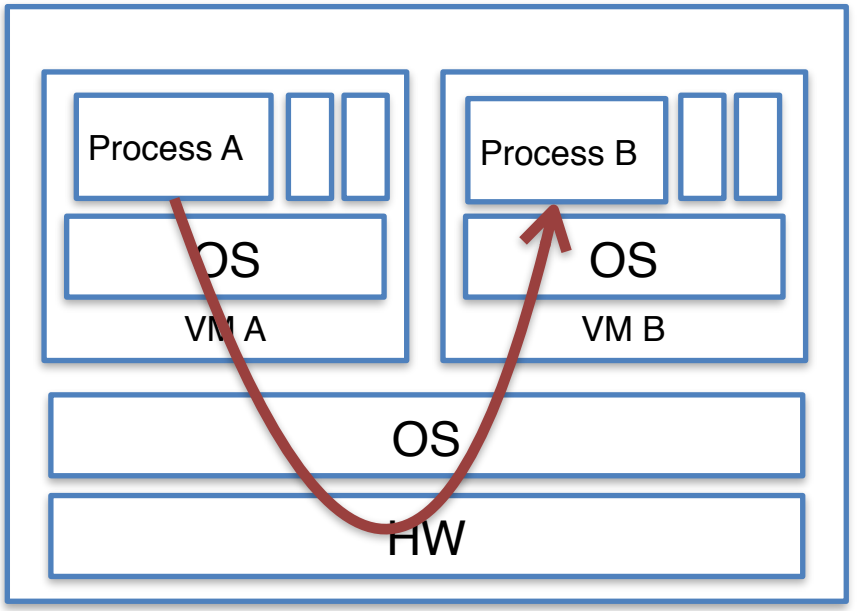
- **针对移动设备**

根据目前的测试情况，Spectre在三星及高通的几款主流处理器上可以成功利用。因此，上述针对个人终端的攻击场景，在一些移动设备上依旧可行。

攻击场景小结



同一台物理主机的进程间攻击



同一台物理服务器上不同虚拟机/Docker中的进程间攻击

针对Cache攻击的早期研究

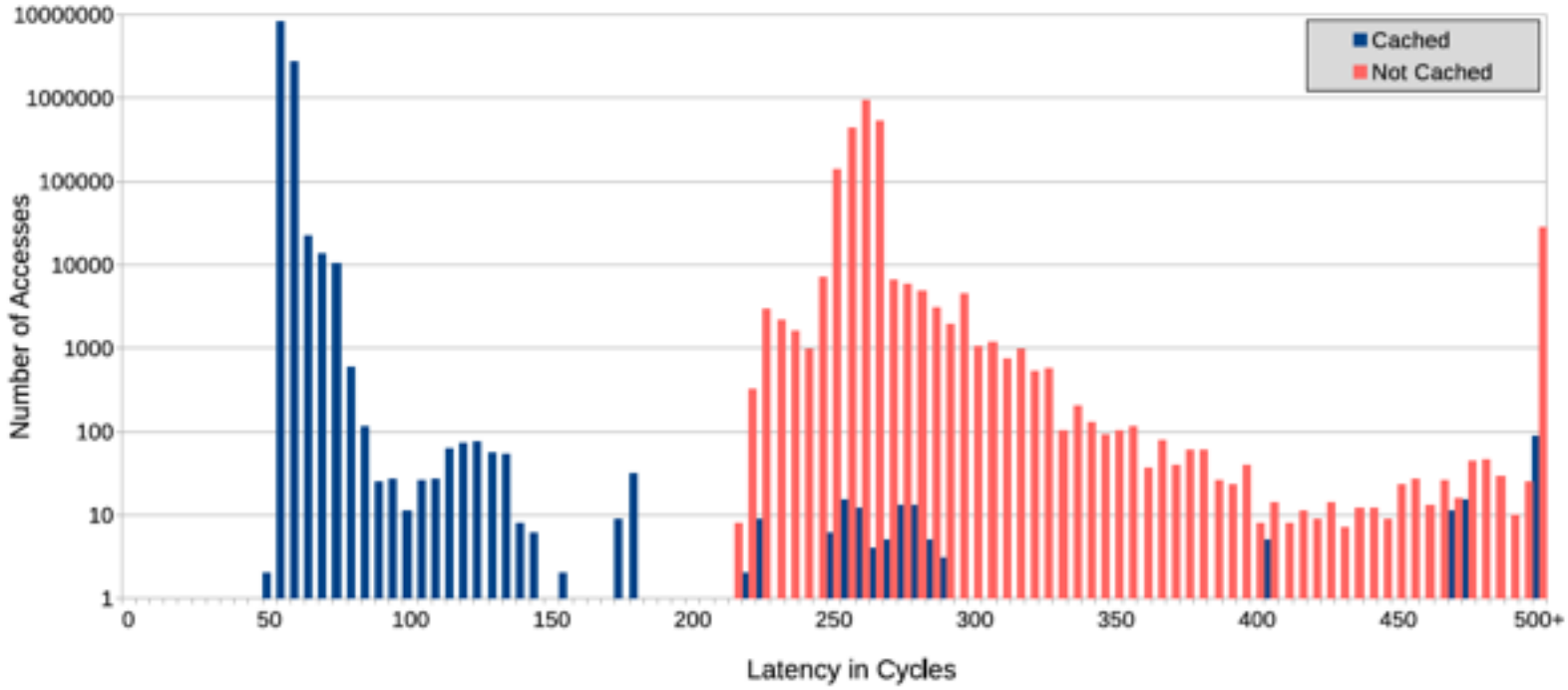
- PERCIVAL, C. Cache missing for fun and profit. In BSDCan (2005).
- BERNSTEIN, D. J. Cache-timing attacks on AES. https://cr.yp.to/antiforgery/cachetiming-20050414.pdf, 2005.
- BONNEAU, J., AND MIRONOV, I. Cache-collision timing attacksagainst AES. In Cryptographic Hardware and Embedded Systems- CHES 2006, L. Goubin and M. Matsui, Eds., vol. 4249 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, pp. 201–215.
- OSVIK, D. A., SHAMIR, A., AND TROMER, E. Cache attacks and countermeasures: the case of AES. Topics in Cryptology– CT-RSA 2006 (Jan. 2006), 1–20
- ACIICMEZ, O., AND SEIFERT, J.-P. Cheap hardware parallelism implies cheap security. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography (2007), pp. 80–91
- RISTENPART, T., TROMER, E., SHACHAM, H., AND SAVAGE, S. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security (2009), CCS ’ 09, pp. 199–212.
- TROMER, E., OSVIK, D., AND SHAMIR, A. Efficient cache attacks on AES, and countermeasures. Journal of Cryptology 23, 1 (2010), 37–71

针对Cache攻击的近期研究

- Yarom, Y., & Falkner, K. (2014, August). FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. In USENIX Security Symposium (pp. 719-732).
- YAROM, Y., AND BENGER, N. Recovering OpenSSL ECDSA nonces using the flush+reload cache side-channel attack. Cryptology ePrint Archive, Report 2014/140, 2014
- Oren, Y., Kemerlis, V. P., Sethumadhavan, S., & Keromytis, A. D. (2015, October). The spy in the sandbox: Practical cache attacks in javascript and their implications. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1406-1418). ACM.
- Liu, F., Yarom, Y., Ge, Q., Heiser, G., & Lee, R. B. (2015, May). Last-level cache side-channel attacks are practical. In Security and Privacy (SP), 2015 IEEE Symposium on (pp. 605-622). IEEE.
- Irazoqui, G., Eisenbarth, T., & Sunar, B. (2015, May). S $ A: a shared cache attack that works across cores and defies VM sandboxing--and its application to AES. In Security and Privacy (SP), 2015 IEEE Symposium on (pp. 591-604). IEEE.
- Daniel Gruss, Raphael Spreitzer, and Stefan Mangard, Cache Template Attacks: Automating Attacks on Inclusive Last-Level Caches, In 24th USENIX Security Symposium, 2015
- Moritz Lipp, Daniel Gruss, Raphael Spreitzer, Clémentine Maurice, and Stefan Mangard, ARMageddon: Cache Attacks on Mobile Devices, In 25th USENIX Security Symposium, 2016
- Disselkoen, C., Kohlbrenner, D., Porter, L., & Tullsen, D. (2017). Prime+ Abort: A Timer-Free High-Precision L3 Cache Attack using Intel TSX.

访问时延是Cache攻击的根源

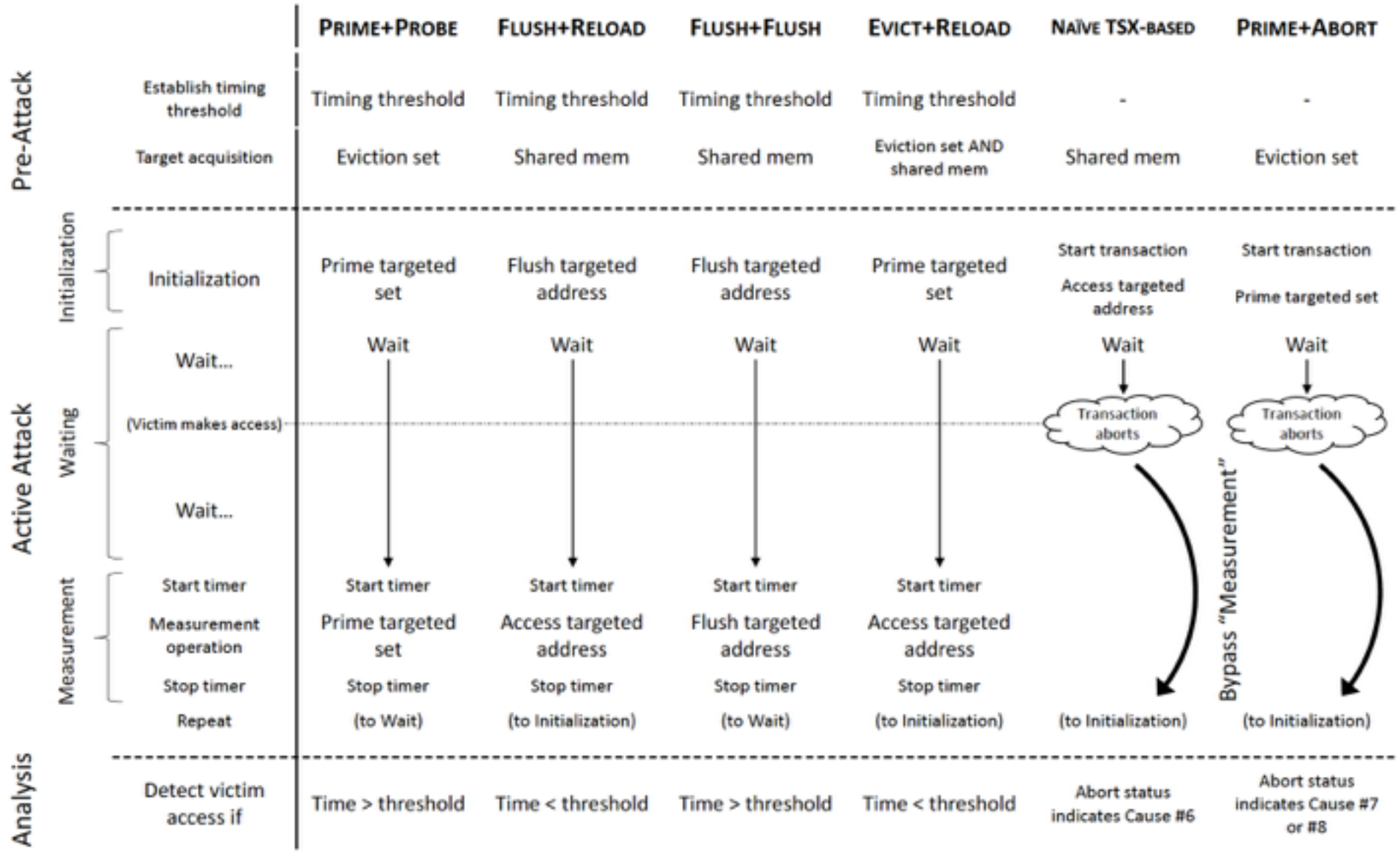
只要能测量数据从内存和Cache访问的时间差异，就有机会区分页面数据差异，从而猜测数据内容。



关键指令

- RDTSC
  - 通过CPU指令周期计数获取高精度计时，测量数据加载时间判断是否命中Cache
- CLFLUSH
  - 清除CPU缓存线，使反复测量成为可能

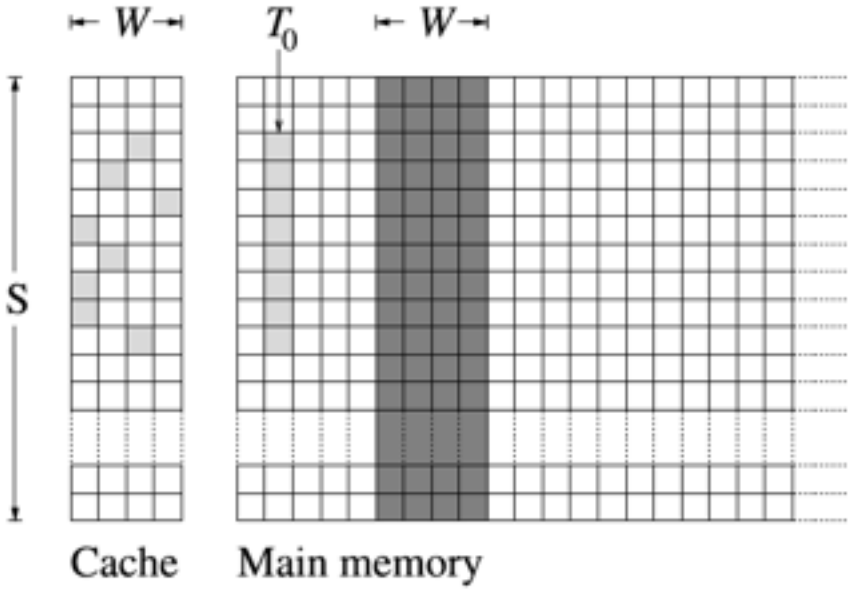
当前各类Cache攻击技术对比



Prime + Probe 攻击

- 允许一个进程在没有特殊权限的条件下攻击相同CPU上运行的其他进程
- 能够绕过内存隔离、沙箱保护、虚拟化隔离
- 能够破解AES、OpenSSL、DM-Crypt

- 攻击者用自己的内存覆盖Cache，在受害者执行敏感指令后测量被替换的页面

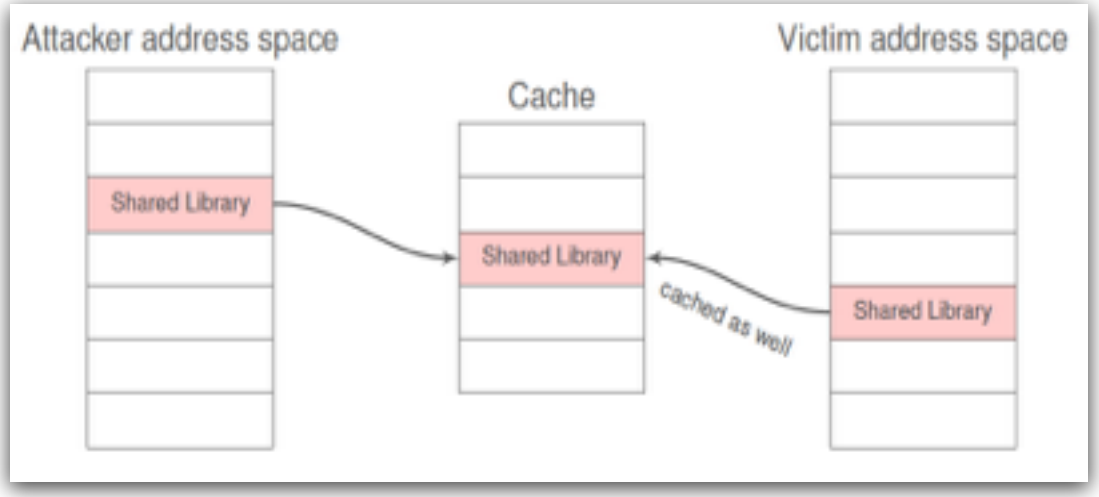


FLUSH + RELOAD 攻击

- 通过L3 Cache进行攻击
- 实现跨进程、跨虚拟机攻击
- 在攻击加密算法时，能够窃取像GnuPG私钥这样的高敏感数据

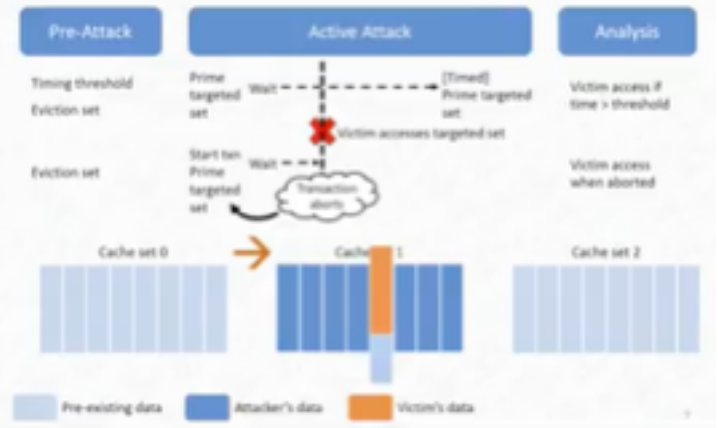
基础原理：Cache有可能与内存不一致，所以系统提供了Flush操作，以便下次把正确的内存数据加载到Cache中。

通过频繁的Flush和Reload操作匹配受害虚拟机/进程中的内存内容
变种：如果没有CLFLUSH则采用Evict方法



Cache攻击的发展

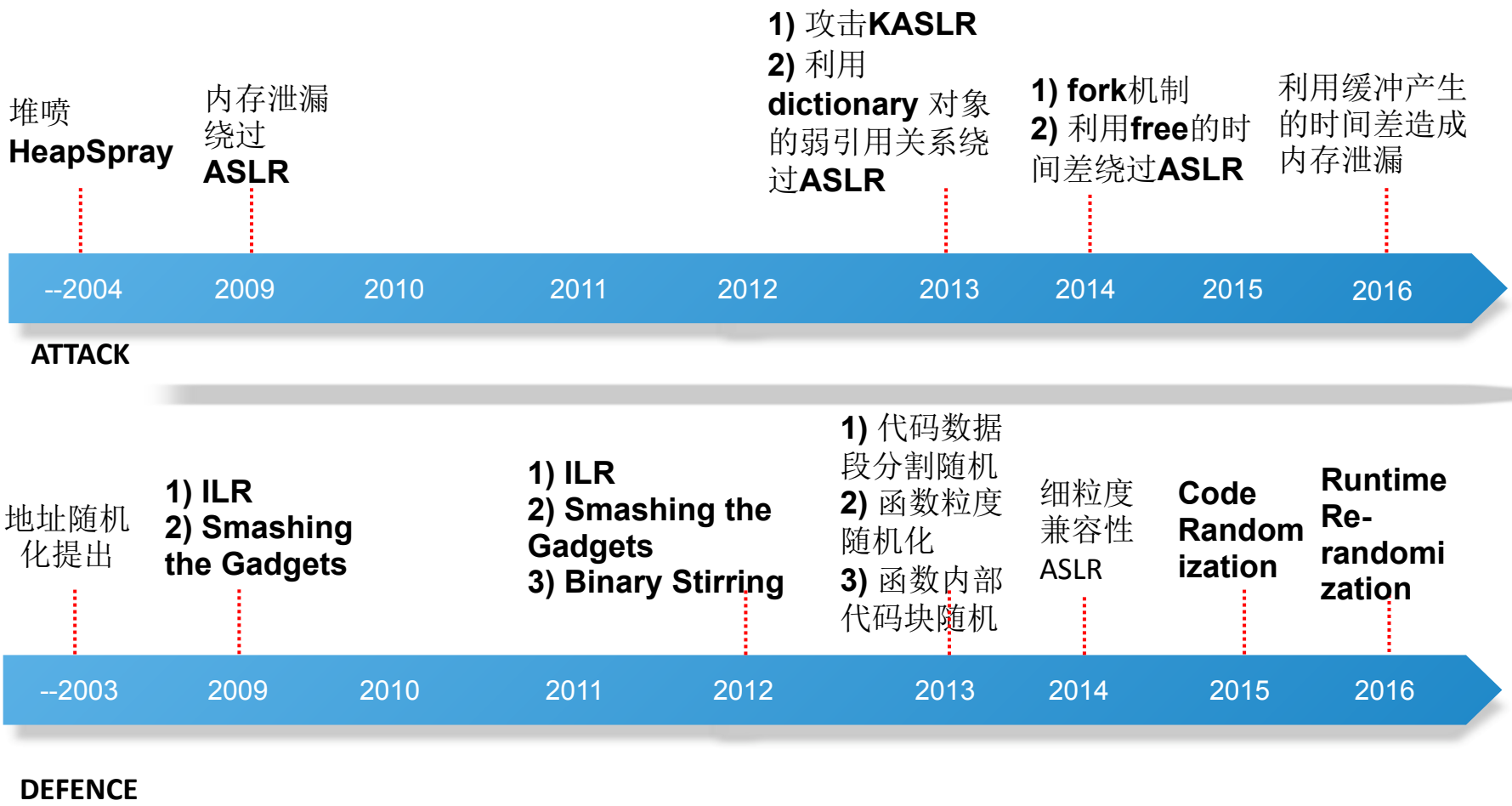
- ARMageddon攻击 -> 把攻击引入移动端
- Cache Template攻击 -> 提高普适性和自动化
- PRIME + ABORT
  - 不采用计时的方式判断Cache内容，而是通过TSX提供的机制，根据是否Abort来判断



内存攻防中的猫鼠游戏

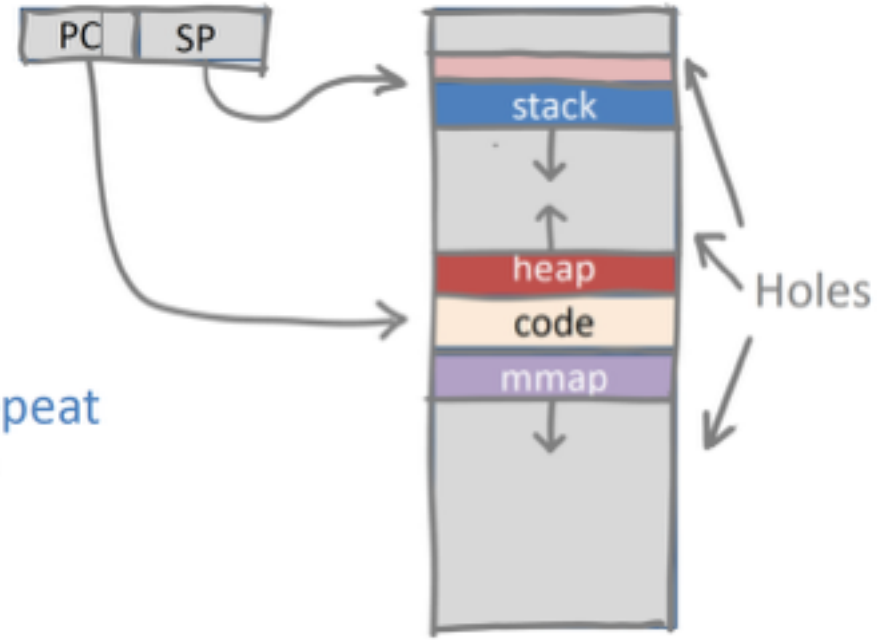
- 从内存中找信息一直是攻击者的一个重点关注
- DEP让攻击者学会了找代码
- ASLR迫使攻击者学会在恶劣的条件下找代码
- 随着对抗的升级，攻击者的脑洞也越来越大

地址随机化的对抗与反对抗演进

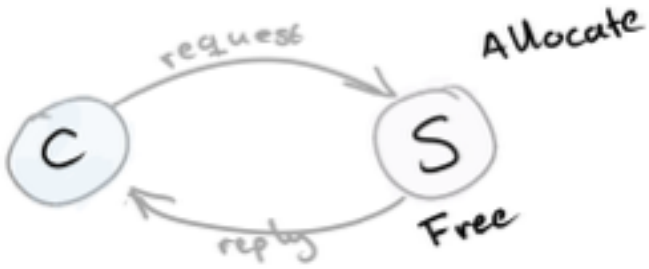


在内存中定位敏感信息

- Angelos Oikonomopoulos, Elias Athanasopoulos, Herbert Bos, and Cristiano Giuffrida,, Poking Holes in Information Hiding, in the Proceedings of the 25th USENIX Security Symposium August 10–12, 2016

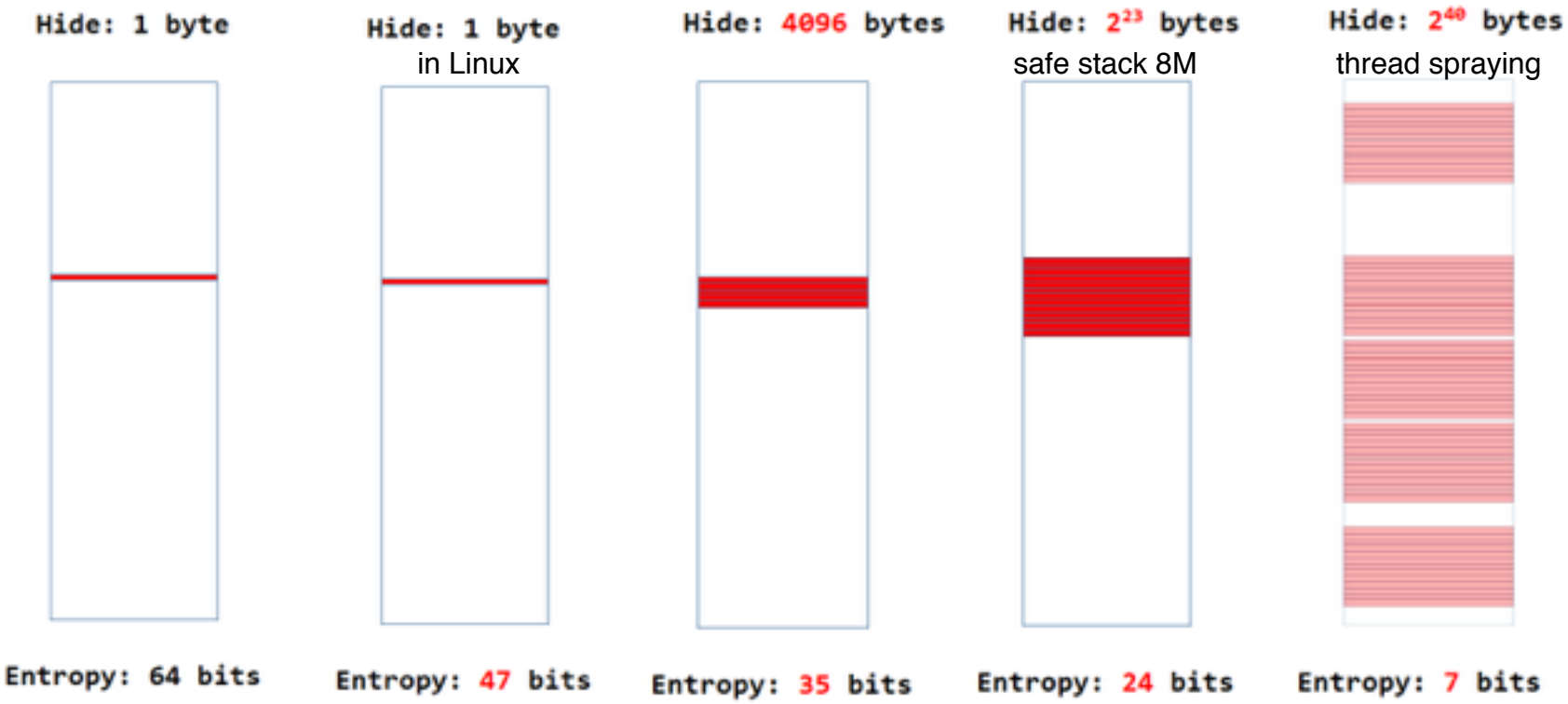


Strategy: allocation+deallocation, repeat



降低信息隐藏空间的熵

- Enes Göktaş, Robert Gawlik, Benjamin Kollenda, Elias Athanasopoulos, Georgios Portokalidis, Cristiano Giuffrida , Herbert Bos, Undermining Information Hiding, in the Proceedings of the 25th USENIX Security Symposium August 10–12, 2016



针对微软CFI的绕过

操作系统在创建支持 CFG 的进程时，将 CFG Bitmap 映射到其地址空间中，并将其基 址保存在ntdll!LdrSystemDllInitBlock+0x60 中。

CFG的实现中存在一个隐患，校验函数ntdll!LdrpValidateUserCallTarget 是通过函数指针 _guard_check_icall_fptr 来调用的。如果我们修改 _guard_check_icall_fptr，将其指向一个合适的函数，就可以使任意目标地址通过校验，从而全面的绕过 CFG。

通过堆溢出修改 CustomHeap::Heap 对象，将一个只读页面变成可读写的，从而改写函数指针 _guard_check_icall_fptr 的值

新近提出的一些解决方案

- SGX - Intel Software Guard Extensions
- ORAM - Oblivious RAMs
- TSX - Intel Transactional Synchronisation Extensions

- Dark-ROP攻击
  - 通过寻找pop指令间接定位ret指令
  - 实现对Enclave中隐藏代码的调用，构造ROP

如果站在历史的长河里看，
这个漏洞有多严重呢?

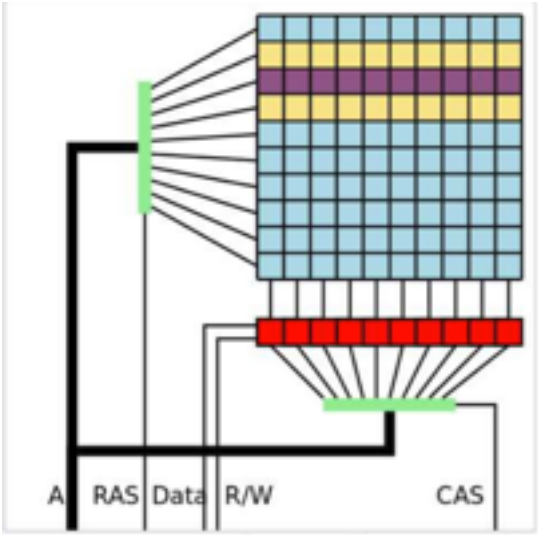
HeartBleed心脏滴血漏洞

简介：
是一个出现在加密程序库OpenSSL的程序错误，首次于2014年4月披露。该程序库广泛用于实现互联网的传输层安全（TLS）协议。只要使用的是存在缺陷的OpenSSL实例，无论是服务器还是客户端，都可能因此而受到攻击。

影响：
经由心脏出血漏洞发动攻击，获得的数据可能包括TLS双方将要交换、但尚未加密的机密内容，包括在用户请求中各种格式的post数据。此外，泄漏的数据还可能含有身份验证密令，如会话cookie及密码，可使攻击者向该服务冒充此用户。攻击还可能泄漏受攻击双方的私钥，这将使攻击者能解密通信内容（将来或是之前通过被动窃听捕获而存储的通信，除非使用完全正向保密，而在这种情况下，只能解密将来通过中间人攻击截获的通信）。

RowHammer漏洞

简介：
Rowhammer比特翻转攻击是指利用临近内存单元之间电子的互相影响，在足够多的访问次数后让某个单元的值从1变成0，反之亦然。这种攻击可以在不访问目标内存区域的前提下使其产生数据错误。



Rapid row activations (yellow rows) may change the values of bits stored in victim row (purple row). [12]:2

具体影响
1. 服务器平台，攻击公钥认证过程，伪造签名
2. 移动平台，利用RowHammer Root安卓手机
3. 桌面平台， RowHammer.js 通过浏览器执行js代码
利用rowhammer漏洞绕过沙盒

Kaveh Razavi, Ben Gras, Erik Bosman, et al, Flip Feng Shui: Hammering a Needle in the Software Stack, In 25th USENIX Security Symposium, 2016

SMB系列漏洞

简介：
NSA武器库，由Shadow Brokers公开披露，wannaCry蠕虫式勒索病毒软件的弹药

工具名称	主要用途
ETERNALROMANCE	SMB 和NBT漏洞，对应MS17-010漏洞，针对139和445端口发起攻击，影响范围Windows XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2
EMERALDTHREAD	SMB和NETBIOS漏洞，对应MS10-061漏洞，针对139和445端口，影响范围：Windows XP、Windows 2003
EDUCATEDSCHOLAR	SMB服务漏洞，对应MS09-050漏洞，针对445端口
ERRATICGOPHER	SMBv1服务漏洞，针对445端口，影响范围：Windows XP、 Windows server 2003，不影响windows Vista及之后的操作系统
ETERNALBLUE	SMBv1、SMBv2漏洞，对应MS17-010，针对445端口,影响范围：较广，从WindowsXP到Windows 2012
ETERNALSYNERGY	SMBv3漏洞，对应MS17-010，针对445端口，影响范围：Windows8、Server2012
ETERNALCHAMPION	SMB v2漏洞，针对445端口

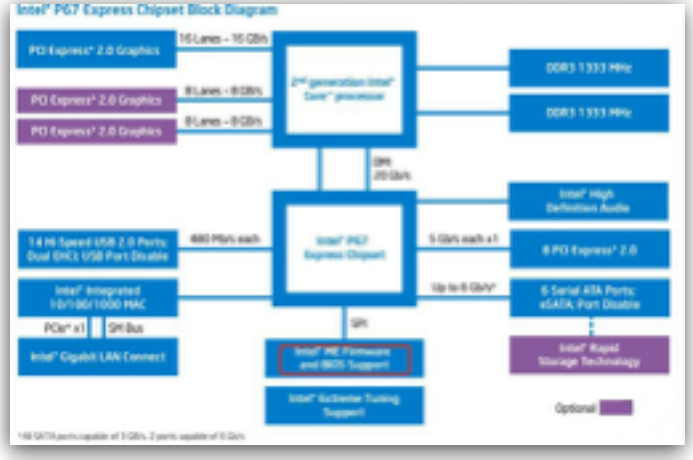
具体影响:
在0day状态时，可在内网下全版本的windows主机上执行任意代码。
被该勒索软件入侵后，用户主机系统内的照片、图片、文档、音频、视频等几乎所有类型的文件都将被加密。
至少150个国家、30万名用户中招，造成损失达80亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。中国部分Windows操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

Intel CPU管理引擎ME漏洞

简介
在现代Intel CPU中运行着Minix操作系统，充当ME管理引擎，用来协调内部诸多模块。其上下文拥有ring -3的至高无上权限，即使在关机状态下也运行。

2017年5月，intel修复ME组件中的一个可导致提权的严重漏洞（INTEL-SA-00075）
2017年11月，Intel再次对此组件上的8个漏洞进行修补 (Intel-SA-00086)。
2017年12月，BlackHat Europe展示了如何利用这些漏洞权限提升到ring -3

漏洞影响：
Ring -3 Rootkit
重装系统也抹不去，关机状态也能运行



危害性总结

- 由于内存空间中围绕敏感信息的隐藏和窃取已经进入精细化时代，每一个小小的缺陷都能被充分放大，导致大家非常重视本次发现漏洞

- 实际环境中的漏洞利用门槛决定了其真正危害性
  - “研究型”漏洞 vs “野战型”漏洞
  - 在低门槛利用代码研发出来之前，Meltdown和Spectre还只算是研究型漏洞

Good Enough is Good Enough !

谢谢！

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS