【科技】CPU的大毛病

2018-01-04 21:12:00

原文网址：http://blog.udn.com/MengyuanWang/109880988

一方面我不是做Computer專業的，另一方面這種消費者類的話題與這個博客的主旨（亦即幫助臺灣的知識分子認清世界大局）無關，所以我一直都避免討論Computer的技術細節。其實我從高一開始就對Personal Computing很有興趣，自買了Apple II以後，每隔幾年都要換新機。大學的時候還當了清華PC社的社長，花了不少時間來寫6502和8088的Assembly。成年後才覺得寫程式是一種必須鑽牛角尖的技藝，和我追求的大局觀有抵觸，於是就放棄了這個嗜好，只有在有需要的時候才會去用。

近日爆出來的CPU Bug，卻是歷史性地嚴重，值得我破例寫專文報導。這最早是The Register（這是一個著名的科技新聞網站，我還在金融界時，因爲必須管理IT人員，曾經有十幾年每日追讀）在2018年一月2日披露（參見https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ ），原本該作者以爲只有Intel的CPU才有問題，後來（參見最新文章https://www.theregister.co.uk/2018/01/04/intel_amd_arm_cpu_vulnerability/ ）額外的細節逐漸浮現，目前已知Intel、AMD和ARM（ARM的CPU核被用在現今幾乎所有的手機上）的產品基本都不能幸免，但是還是以Intel CPU的問題最糟糕。這是因爲Bug的來源是Intel在1995年的Pentium Pro領先推出的一個加速方法，叫做Speculative Execution；它的功能包括讓CPU在執行下一個指令之前，就先把那個指令會需要的資料從記憶體提出來，放在近處（也就是CPU自己的短暫記憶體，叫做Cache）；如此一來，CPU的執行單元就不必停下來等資料。

但是Intel的CPU自從80年代的80386之後，就有了另一個更遠為重要的功能，叫做Protected Mode。基本上它給予每個程序（Process，不是Program，程式；一個程式可以有好幾個程序）一個固定的記憶範圍，然後由CPU負責保證程序只能讀寫自己的資料。Protected Mode不但禁止一個程序侵犯其他程序，避免引起當機，而且是現代Computer Security的基石，否則在隨便一個網頁都可以啓動程式語言（最常見的是JavaScript）的背景下，它們就可以去搜索用戶在其他應用軟件打入的資料，包括密碼等等。

Intel的工程師在20多年前落實Speculative Execution這個功能的時候，就粗心沒有想清楚。Protected Mode必須檢查每一個指令所用的資料在合法範圍之內，但是這個檢查是在執行的時候才做的。前面提到，Speculative Execution就正是在執行之前先把資料提到Cache裏面；結果Intel的CPU遇到非法的指令，固然會依照規則予以拒絕，但是那些不屬於這個程序的資料還是已經被提出來了，可以另行設法讀取。

這麼糟糕的毛病，一直到2017年六月，才有“白帽子”（“White Hat”，指負責Computer Security的從業人員；至於是否有“黑帽子”如NSA早於他們發現，我們不得而知）注意到，立即通知了Intel。但是這個缺陷是內建在芯片上，Intel要改也只能改以後出廠的芯片（事實上這也很花時間，半年多了，改版的CPU還沒有定型），世界上現有的幾十億台用Intel CPU的計算機怎麼辦呢？白帽子們商議之後，把問題分爲兩類：第一類是惡意軟件（Malware）利用這個缺陷直接攻擊作業系統（OS），他們取名叫做“Meltdown”；第二類是攻擊其他的應用軟件，叫做“Spectre”。

Meltdown是最嚴重的，因爲作業系統的機密最多；但是解決起來卻容易些。這是因爲Intel的指令集對記憶體的定址是分頁（Page）的，如果作業系統把自己放在應用軟件看不到的頁上，就可以避免Meltdown（但是這會導致整個Computer變慢，所以以前沒有作業系統會故意這麼做）。Mac OS已經改了，Windows和Android應該在本月也會推出改版。

Spectre就麻煩得多，因爲記憶體是有限的，而同時在運行的應用軟件卻成百上千，不可能完全分頁。更可怕的是像瀏覽器這樣的程式一次可以開很多網頁，只要有一個惡性網頁啓動JavaScript，其他網頁上的密碼一般都算是同一個程序的資料，不能用分頁法來保護。所以Spectre的細節一公開，我馬上啓動了Chrome（這是我常用的瀏覽器）的“Site Isolation”功能（參見https://support.google.com/chrome/answer/7623121?hl=en ）。這個選項强迫Chrome把每一個網頁都當作獨立的程序來處理。如此一來，Chrome會占用更多的記憶體，並且可能會妨礙打印，但是至少會給惡意軟件製造一些困難。

The Register其實應該等到作業系統的改版都出來才報導這個問題，但是話說回來，再怎麼等，Spectre也是沒有完全解的。就算Intel現在就把所有現有的產品都改好了，也不可能很快替換掉過去20多年賣出去的CPU。Intel的CEO，Brian Krzanich顯然也瞭解這一點；他在十一月急急忙忙地把手裏的50萬股Intel股票以低於市場價賣掉一半（Intel的契約規定CEO必須至少持有25萬股）。他說賣股票的決定和Meltdown/Spectre無關，讀者你們覺得呢？

---

4 条留言

大陆读者 2018-01-05 01:32:00

我暂时还没有那么悲观。虽然不知道具体的技术细节，但大概率需要按特定的顺序执行特定的机器代码。所以想要利用漏洞，直接用Assembler会比较容易。而现代浏览器上运行的脚本插件都是在虚拟机上运行，浏览器做好补丁应该就可以。 Windows现在已经放出补丁了（http://support.microsoft.com/help/4056892），注意最后一条Security updates to Windows SMB Server, the Windows Subsystem for Linux, Windows Kernel, Windows Datacenter Networking, Windows Graphics, Microsoft Edge, Internet Explorer, and the Microsoft Scripting Engine.包含了浏览器的部分，似乎可以印证我的想法。

> 沒有錯，JavaScript和Java應該不容易搞出惡意軟件，不過小心總是好的。 那些黑帽子的天分不能低估。

syg 2018-01-05 10:16:00

Firefox不久前也釋出補丁：https://www.mozilla.org/en-US/firefox/57.0.4/releasenotes/

> 這個Bug的問題在於它來自CPU，所以不可能用軟件完全修補。

游客 越雷 2018-03-27 21:22:00

王先生，像台积电（代工），苹果（手机品牌），高通（芯片设计）LG（手机配件）这些到底哪个是大陆最落后？哪个最重要（符合中国制造2025）？发展这些产业，会不会真的像西方的那些人说的一样:西方对科技的垄断被打破，再也不能收专利费或者靠某个高科技卡中国的脖子了？(xzy1997128@163.com)

> 中國和歐美不一樣，不只是想要賺錢多的，而是所有高級的產業通通都要，所以無所謂哪個最重要。 產業升級的正道，是先做整機，有了營銷收入和額份之後，就可以慢慢地用國產部件替換外來的，手機是如此，大飛機也是如此。

南山臥蟲 2018-03-29 16:49:00

//中國和歐美不一樣，不只是想要賺錢多的，而是所有高級的產業通通都要，所以無所謂哪個最重要。// 一語道破！人本和資本之別，盡在其中矣。建議有空時王兄再深入談談這個，先謝。

> 其實説得更精確一點，資本主義在乎的是ROI（Return On Investment），人本主義重視的則是Value Added Per Capita。

返回索引页