Spekulatives Vertrauen

Kommt eine Instruktion in eine Bar. Nein, doch nicht. Ihr Portemonnaie wurde trotzdem dort geklaut.“ Derartige Witze brachten bis vor Kurzem nur eingefleischte CPU-Experten zum Lachen. Plötzlich will jeder außer der NSA gewusst haben, dass Angriffe auf Prozessoren ein heißes Thema sind.

Die letzten drei Wochen haben mir in Diskussionen mit Fachkollegen gezeigt, dass die Grenzen des Verständnisses bei vielen von uns ausgetestet werden. Ich musste mich tagelang einlesen in spekulative Blog-Posts und 4000-Seiten-Manuals. Eine Bar kann hier echt hilfreich sein. Als Metapher. Selbstverständlich.

Denn es geht noch anschaulicher: Ein Kunde kommt jeden Tag in eine Bar. Der Barmann bereitet immer schon den Lieblings-Latte zu, sobald er ihn sieht. Das geht manchmal schief, wenn der Kunde ausnahmsweise Kamillentee bestellt, aber unterm Strich spart es Zeit. Der Kunde ist eine Instruktion, die Bar ein Computer, der Barkeeper ein CPU-Thread – Speculative Execution in Aktion.

Da niemand wissen soll, was die anderen bestellen, darf man nur einzeln an die Bar. Inzwischen werden Kunden häufig außer der Reihe bedient, wenn eh jemand wartet. Dank Abstellflächen für häufig Gebrauchtes rennt man nicht ständig ins Lager.

Die Meltdown-Nummer: Durch geschicktes Bestellen und Zurückgeben in der Zeit, die der Barmann braucht, herausfinden, was das Personal selbst konsumiert. Geht nur bei Starbugz.

Etwas komplizierter der Spectre-Trick: Die Getränkekarte hoch und runter bestellen, bis der Barmann von alleine losläuft, um mir nach meinem Gin Tonic den Baileys zu holen. „Aber den guten aus dem Regal ganz oben!“, rufe ich ihm hinterher. Bis er gemerkt hat, dass er die Kiste mit den Geschenkgutscheinen geholt hat, habe ich mir bereits drei ausgefüllt. Oder ich behaupte, Geburtstag zu haben. Bis er meinen Ausweis prüft, habe ich längst abgefragt, dass den Moët schon mein Chef abgestaubt hat.

Meltdown lässt sich relativ einfach durch eine Anweisung an das Barpersonal (OS) reparieren: Immer alle Spuren der letzten Order wegräumen (KPTI)! In modernen Bars hängt man faul kleine Fähnchen an Wegzuräumendes (PCID). Spectre ist schwerer auszunutzen, weil man das Personal gut kennen muss. Gegen Variante 1 hilft nur eine Überarbeitung aller Dienstanweisungen: Wenn jemand etwas aus dem Lager bestellt, zuerst nachdenken (lfence) – aber bitte nicht zu oft.

Gegen Variante 2 hilft ein Trampolin: Barmann hüpft, bis er den Ausweis gesehen hat (retpoline). Dafür müssen alle Bars und Ausbildungen angepasst werden. So lange hat Starbugz verboten, Specials aus dem Lager zu holen, und der Kollege darf auch nichts mehr von dort mitbringen (IBRS und Co.). Letzteres macht die Sache allerdings schmerzlich langsam, vor allem in alten Bars und bei alten Servern, äh, Bedienpersonal.

Werden uns die Exploits das Genick brechen? Nein, auch wenn sie uns noch einige Zeit beschäftigen werden. Muss jeder sie bis in die Tiefe verstehen? Auf keinen Fall! Aber bitte immerhin so weit, dass wir die Ehrfurcht vor der „Hard“ware wieder verlieren, die sie in den letzten Jahren gegenüber der unsicheren „Soft“-ware angesammelt hat. Die Grenzen verschwimmen eh immer mehr: Der Turingmaschine war immer schon egal, ob sie auf Band oder FPGA läuft. Spätestens seit Microcode ist die CPU im Grunde so weich wie ein Smart Contract – und mit all ihrer *magic inside*™ mindestens ebenso komplex. In den Abstraktionsebenen warten noch viele Seitenkanäle auf Ausnutzung. Wenn wir den Kampf bei den Prozessoren nicht gewinnen können, wie wollen wir dann die Komplexität bei Software oder KI in den Griff kriegen?

DAVID FUHR

ist Head of Research beim IT-Sicherheitsberatungsunternehmen HiSolutions.

PS: Mehr zu Meltdown/Spectre finden Sie auf Seite 62.