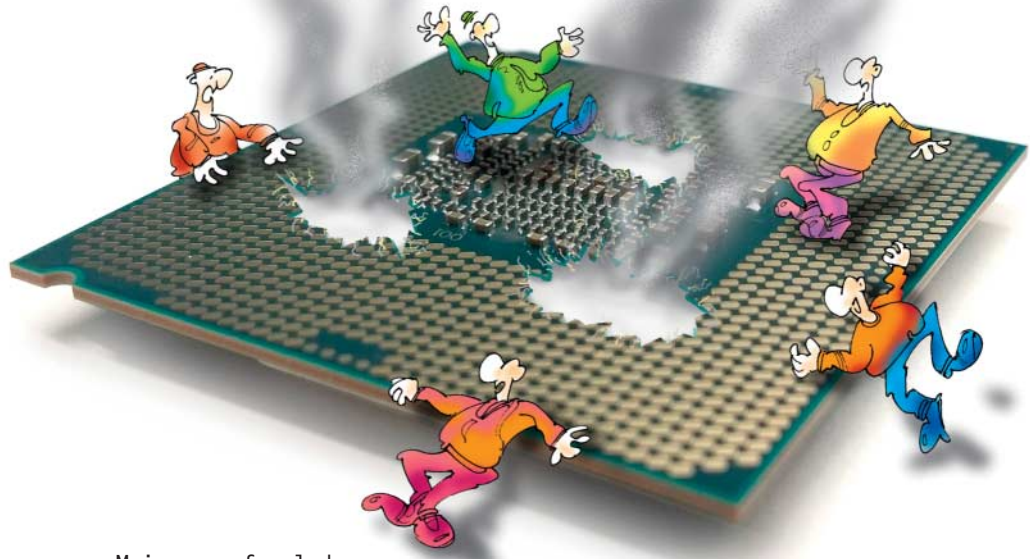




Wandern übers Minenfeld

Kaum ist man mal im Ruhestand - und schon ist nix mehr mit Ruhe. So viel Hektik querebeet in den Reihen der Prozessor-, Betriebssystem-, Browser-, Treiber-, System- und BIOS-Hersteller habe ich, soweit ich mich erinnere, noch nie erlebt, nicht einmal beim berühmten FDIV-Bug 1994. Damals war auch bloß ein einziger Prozessor betroffen, der sich zudem nur manchmal ein kleines bisschen verrechnete - lächerlich. Intel hat völlig recht, jetzt ist es kein Bug - nein, es ist schlimmer: Jetzt ist gleich eine ganze Architekturidee tief im Mark ge- und betroffen, die Intel, AMD, ARM, IBM und andere aufgegriffen haben.

Ein kurzer Blick auf die paar Zeilen Code im Kernbereich der Meltdown-Attacke reicht, um das Dilemma aufzuzeigen - jedenfalls, wenn man noch Assembler versteht, was ja immer seltener wird. Der weitere Trick, spekulativ einen Sprung der Sprungvorhersage unterzuschieben (Branch Target Injection), war demgegenüber schon etwas schwieriger auszutüfteln - genial! Doch warum ist das alles keinem früher aufgefallen?

Über 20 Jahre, seit dem Pentium Pro, gibt es schon Prozessoren mit komplexer Out-of-Order-Technik und mit weitreichenden Spekulationen - und niemand hat das Risikopotenzial bislang erkannt oder gar genutzt? Wirklich? Weiß Snowden vielleicht mehr? Die Technik zum "Morsen" von Informationen über die Caches oder über andere geheime Kanäle kennt man ja auch schon seit vielen Jahren.

Okay, ich habs auch nicht gesehen und komme mir nun so vor wie zahlreiche Wissenschaftler im Jahre 1958. Wers nicht mehr weiß: Damals ging ein eigentlich äußerst simples Experiment zur

Kernresonanzabsorption mit Hilfe des Doppler-Effekts um die Welt, überall war ein lautes Sich-an-den-Kopf-Schlagen zu vernehmen und so konnte der damals erst 32-jährige Doktorand Rudolf Mößbauer 1961 seinen wohlverdienten Nobelpreis entgegennehmen.

Folglich plädiere ich dafür, den Forschern von Google und von den beteiligten Universitäten den "Nobelpreis der Informatik" zu verleihen, den Alan-Turing-Preis. Dessen nach ihm benannte Maschine arbeitete indes ohne Spekulationen streng in Order. Soll man also nun zurück zu Turing-Maschinen - oder zu etwas moderneren In-Order-Nachfolgern wie dem Itanium? Da freuen sich die Altvorderen, die diesen Oldtimer noch einsetzen. Vielleicht überlegt sich Intel den Abschied vom Itanium jetzt doch noch ...

Nein, die Out-of-Order-Technik ist trotz der bekannt gewordenen Schwachstellen nicht out of Order. Man muss auch gar nicht ihre Spekulationen allzu sehr einschränken, sondern vielmehr dafür sorgen, dass keine verdeckten Kanäle mehr aus der Innenwelt des Prozessors nach draußen möglich sind. Ideen, wie man die Innereien in Zukunft hardwaremäßig ohne größeren Performanceverlust gegen die Cache-Morsetechnik schützen kann, hätte ich schon - aber da kommen Intel, AMD und Co. sicherlich selber drauf. Ansonsten bin ich ja über die Redaktion noch erreichbar ...

Mit ungeruhsamen Grüßen

Andreas Stiller

Andreas Stiller