Bit-Rauschen

Intel-Pech, AMD-Glück und veränderliche Prozessoren

Neue Sicherheitslücken plagen Intel-Prozessoren, während AMD weiter auf der Erfolgswelle surft. Forscher tüfteln unterdessen an CPUs, die bestimmte Malware-Angriffe ins Leere laufen lassen.

Von Christof Windeck

Zum Unglück kam auch noch Pech hinzu: Nachdem Intel den eigenen Aktienkurs mit mageren Aussichten auf den Jahresumsatz gedrückt hatte, tauchten neue Sicherheitslücken wie Zombie-Load alias Microarchitectural Data Sampling (MDS) auf, siehe S. 30. Und das alles in schwierigen wirtschaftlichen Zeiten, wo ein einziger Tweet von US-Präsident Trump die Börsenkurse ganzer Volkswirtschaften auf Talfahrt schickt. Zwar muss man mit Milliardenverdienern wie Intel kein Mitleid haben, aber es wäre schon besser, die Firma könnte sich auf die Entwicklung neuer Prozessoren konzentrieren. Bleibt zu hoffen, dass das Patchen der Lücken nun besser klappt als zuvor bei Spectre und Meltdown. Immerhin gibt es diesmal bereits Microcode-Updates und Patches für Windows, Linux und so weiter. Ironie am Rande: Eine der Hardware-Schutzmaßnahmen gegen Meltdown, die Intel bei den neuesten Core i-9000 eingebaut hat, ermöglicht erst eine spezielle Variante eines „Fallout"-Angriffs vom neuen MDS-Typ.

Sicherer Morph-Chip

Entwickler der neuen RISC-V-Mikroarchitektur diskutieren schon lange über Hardware-Schutzmaßnahmen gegen Malware-Angriffe. Forscher experimentieren gerne mit RISC-V, weil sie frei an fast allen Schrauben der Rechenwerke drehen können. Wie viele Jahre es dauern wird, bis solche unknackbaren Prozessoren in ähnliche Preis- und Leistungsregionen wie aktuelle AMD- und Intel-Chips vordringen, steht aber auf einem anderen Blatt.

Ein Ergebnis solcher Versuche an der Uni Michigan ist jedenfalls Morpheus: Ein RISC-V-Prozessor, der sogenannte Control-Flow-Angriffe verhindern soll. Bei diesen Attacken schiebt Malware einem vertrauenswürdigen Programm böswilligen Code unter, indem sie letzteren beispielsweise an Speicheradressen ablegt, die die „gute" Software von sich aus benutzen würde. Dazu muss die bösartige Software jedoch die benötigten Speicheradressen finden, etwa indem sie das Verhalten der guten Software analysiert. Um das unmöglich zu machen, verwürfelt die „Churn Engine" des Morpheus in kurzen Abständen solche Speicheradressen im laufenden Betrieb. Einer der Professoren der Uni Michigan und Mit-Erfinder von Morpheus hat die Firma Agita Labs gegründet, um die Chip-Idee in ein Produkt zu verwandeln.

Wenn Morpheus dann eines Tages erscheint, fertigt Samsung vielleicht schon Prozessoren mit 3-nm-Strukturen – die Pläne werden konkreter. Samsung hat jedenfalls schon besonders leistungsfähige Transistoren mit der speziellen Gate-Geometrie „Gate All Around" (GAA) angekündigt, die künftige Prozessoren auf Trab bringen sollen. Die GAA-Idee hatte Samsungs ehemaliger Chip-Entwicklungspartner IBM freilich schon 2017 präsentiert, damals für 5-nm-Transistoren.

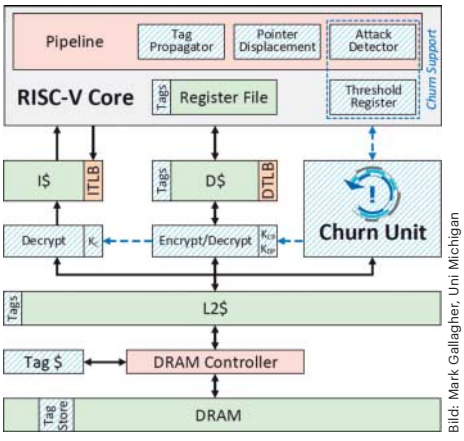

Bild: Mark Gallagher, Uni Michigan

Ein Team um Mark Gallagher von der Uni Michigan hat den RISC-V-Prozessor Morpheus entwickelt, der Speicheradressen im laufenden Betrieb verwürfeln kann.

AMD-Glückssträhne

Während Intel mit schrumpfenden Umsätzen und immer neuen Sicherheitslücken kämpft, läuft bei AMD anscheinend alles bestens. Für 2021 hat man noch ein bedeutendes Projekt an Land gezogen, nämlich „Frontier", den ersten US-amerikanischen Supercomputer mit 1,5 Exaflops. Die Ankündigung enthält einen Seitenhieb auf Intel, denn 2021 soll auch der „Aurora" mit Intel-Technik kommen – aber vermutlich mit weniger Rechenleistung, bisher ist nur vage von mindestens 1 EFlops die Rede.

Sowohl Frontier als auch Aurora baut Supercomputer-Entwickler Cray und setzt dabei die ebenfalls neue Shasta-Plattform ein. In Frontier werden speziell angepasste Epycs zum Einsatz kommen. Wie im Bit-Rauschen in c't 9/2019 schon vorhergesagt, nutzen sie Infinity Fabric als externen Link zur Cache-kohärenten Anbindung von je vier Radeon-Instinct-Rechenbeschleunigern. Intel plant bekanntlich ähnliches mit dem Compute Express Link (CXL) und Xᵉ-Beschleunigern.

Frontier wird 2021 mindestens der zweite große Supercomputer mit Cray-Shasta-Technik und AMD-Chips sein, denn für 2020 ist ja schon der Perlmutter alias NERSC-9 geplant – aber noch im Verbund mit Nvidia-Teslas, die wohl den Löwenanteil der Rechenleistung beisteuern.

Zahlungskräftige PC-Freunde mit Adleraugen haben aber auch einen kleinen Wermutstropfen bei AMD entdeckt: Der Ryzen Threadripper 3000, der deutlich mehr als 32 Kerne haben könnte, verschwand von öffentlichen Roadmap-Dokumenten. Das dürfte aber wohl eher nicht bedeuten, dass er nie mehr kommt, sondern vielleicht einfach nur später: Es ist schließlich kein konkurrierender Intel-Chip in Sicht, den der Threadripper 3000 angreifen könnte. Vermutlich haben Lisa Sus Leute gerade alle Hände voll zu tun mit Ryzen 3000, dem Rome für Server und den Navi-GPUs, die viel wichtiger sind für AMD. Wer sich für die Pläne von AMD und Intel für die nächsten Monate interessiert, findet ab Seite 104 in dieser c't-Ausgabe passenden Lesestoff.

(ciw@ct.de) c't