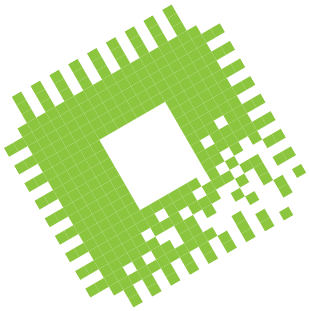
Bit-Rauschen

CPU-Seitenkanalattacke, Personalkarusselle und Switch-Chips



Angreifer enttarnen verschlüsselte Daten per „Undervolting“. Ein Start-up wirbt wichtige Mitarbeiter von Apple und Intel ab, Cisco und Broadcom bringen superschnelle Netzwerkprozessoren.

Von Christof Windeck

Bei Intel kehrt keine Ruhe ein: Ein weiterer Seitenkanalangriff wurde bekannt. Die Entdecker von „Plundervolt“ nutzen interne Register, um die Spannungsversorgung der CPU-Kerne abzusenken. Bei zu niedriger Spannung treten Rechenfehler auf, die Angreifer wiederum ausnutzen können, um an vermeintlich sicher geschützte Geheimwerte in einer verschlüsselten SGX-Enklave zu gelangen. Das hört sich jedoch spektakulärer an, als es letztlich ist: Bei Privatleuten und in Büro-PCs kommt SGX bisher kaum zum Einsatz und nur ein lokal angemeldeter Nutzer kann Plundervolt ausführen. Allerdings soll SGX eigentlich vor Angriffen böswilliger Administratoren oder Eindringlinge in Cloud-Rechenzentren schützen. Plundervolt zeigt zudem, wie Sicherheitslücken aufreißen, wenn die CPU anders arbeitet als vom Hersteller vorgesehen – das gilt auch fürs Übertakten.

Während sich Plundervolt relativ leicht mit Microcode-Updates beheben lässt, sieht es bei Intels Schwierigkeiten mit der Fertigungstechnik anders aus. Abermals gibt es Spekulationen, laut denen 2020 weitere Xeon-Verzögerungen drohen. Intel hat nun Dr. Gary Patton abgeworben, den bisherigen Chef-Techniker (CTO) des Auftragsfertigers Globalfoundries: Er soll dafür sorgen, dass aus Entwürfen rasch lieferbare Prozessoren werden. Zunächst sollen aber bekanntlich erst einmal weitere 14-Nanometer-Xeons kommen und im April dann wohl auch die ersten Zehnkerner für Desktop-PCs (Comet Lake-S) für Mainboards mit Serie-400-Chipsätzen und der neuen Fassung LGA1200.

AMD kann laut Server-Chef Forrest Norrod sein Glück gar nicht fassen: Er sagte in einem Gespräch mit Analysten, dass man vor vier Jahren eigentlich bloß gehofft hatte, mit der 7-Nanometer-Fertigungstechnik auf Augenhöhe mit Intels 10-Nanometer-Technik zu kommen. Er bezeichnete Intels jahrzehntelangen Vorsprung bei der Chip-Fertigungstechnik als das „vierte physikalische Gesetz der Halbleiterbranche“. Da mutet es schon wie ein Treppenwitz an, dass Intel ältere 22-Nanometer-Technik ausgerechnet für die futuristischste Computertechnik einsetzt: Der Controller namens „Horse Ridge“ ist zur Steuerung von Quantencomputern direkt in ihrem tiefgekühlten Kern gedacht. Laut Intel ist das ein wichtiger Schritt zu praktisch nutzbaren Quantenrechnern, weil die komplexe Steuerung damit schneller und einfacher wird.

Streit um Nuvia

Apple hat einen ehemaligen hochrangigen Mitarbeiter verklagt: Gerard Williams III war jahrelang für die Entwicklung der ARM-Chips für iPhones verantwortlich, verließ Anfang 2019 dann aber Apple und gründete Nuvia. Gemeinsam mit den ebenfalls erfahrenen Experten Manu Gulati und John Bruno entwickelt er dort neuartige Server-Prozessoren. Das schmeckt Apple offenbar nicht: Angeblich hat Williams seinen Arbeitsvertrag verletzt, unter anderem indem er andere Apple-Entwickler für Nuvia anheuerte. Eine solche Apple-Klage ist zwar einerseits bedrohlich, andererseits aber auch gute Werbung – immerhin hält Apple das Know-how für bedeutsam. An Nuvia verlor auch Intel eine Reihe von Marketing-Spezialisten, beispielsweise Jon Carvill, der einst für AMD und davor für ATI arbeitete. Auch Ex-ATI-Mann Chris Hook, der erst im April 2018 von AMD zu Intel wechselte, ist nun bei Nuvia. Was genau man dort plant, ist allerdings unklar; man will jedenfalls das Chip-Design „neu denken“ (reimagine silicon design).

Das klingt ähnlich wie bei der im vorletzten Bit-Rauschen erwähnten Firma Groq, deren KI-Chip seine Transistoren besser ausnutzen soll als bisherige Prozessoren. Dabei spielt der Compiler eine wichtige Rolle. An Spezial-Compilern für exotische Rechenwerke sind jedoch schon größere Firmen gescheitert.

Eine überraschende Neuerung gibt es beim Netzwerk-Hardware-Spezialisten Cisco, der bislang sehr viel Geld mit seinen proprietären Switches verdient. Der hauseigene Chip Silicon One Q100 soll nun nicht mehr nur eigene Hardware antreiben, sondern Cisco wird ihn auch an einige Betreiber von Hyperscale-Rechenzentren verkaufen, etwa Facebook und Microsoft. Der Q100 soll einen aggregierten Durchsatz von 10,8 Terabit/s verarbeiten, genug für 108 Ports mit je 100 GBit/s oder mehr als 24 Ports mit 400 GBit/s (400GE). Letzteres kommt in großen Rechenzentren zunehmend zum Einsatz, das sieht auch Broadcom so: Der StrataXGS Tomahawk 4 alias BCM56990 stellt sogar 25,6 TBit/s für 64 400GE-Ports bereit. Er vereint 31 Milliarden Transistoren, die TSMC mit 7-Nanometer-Strukturen fertigt. *(ciw@ct.de)* c't

Bild: Broadcom

Der Broadcom-Netzwerkprozessor Tomahawk 4 nutzt 31 Milliarden 7-Nanometer-Transistoren, um 64 Ethernet-Ports mit je 400 GBit/s zu verknüpfen.