Bit-Rauschen

PC-Revolutionen, Kursschwankungen und Spionage-Chips

Wieder einmal nimmt HP den Mund zu voll. Der Aktienkurs von AMD fährt unterdessen Achterbahn. Intel versteckt einen x86-Kern im iPhone und das chinesische Militär angeblich Lausch-Chips in Servern.

Von Christof Windeck

Es wird zur Tradition: Alle zwei Jahre kündigt HP eine PC-Revolution an, die sich letztlich als mäßig spannende Idee entpuppt. Nach dem Sprout 2014 – einem All-in-One-PC mit 3D-Kamera – und dem Pavilion Wave 2016 – einem Desktop-PC im Lautsprecher-Gehäuse– kommt nun das 2-in-1-Notebook Spectre Folio (siehe S. 39). Es lässt sich wie ein Tablet verwenden und mit einem Stift bedienen, was nicht gerade revolutionär klingt. Anscheinend steckt die Revolution bei HP in einem neuartigen Klappmechanismus (Wahnsinn!) und im Gehäusematerial Leder (krass!). Da ist die Spannung kaum auszuhalten, was HP für 2020 plant.

Bei AMD reißt es den Aktienkurs derweil mal hoch, dann wieder rauscht er in die Tiefe. Hintergrund für den Aufschwung war die Spekulation, AMD könne bis 2020 seinen Marktanteil bei Prozessoren enorm steigern, weil Intel derzeit Lieferschwierigkeiten hat, wie in c't 21/18 berichtet. Doch dann hat wohl mal jemand nachgerechnet, wie viele Prozessor-Wafer AMD überhaupt von Globalfoundries und im Falle der kommenden 7-nm-Chips von TSMC kaufen kann. Dazu kam dann noch die Bekräftigung von Intel, 2019 wirklich endlich 10-nm-Chips zu liefern – und der AMD-Kurs sackte wieder ab.

x86 im iPhone

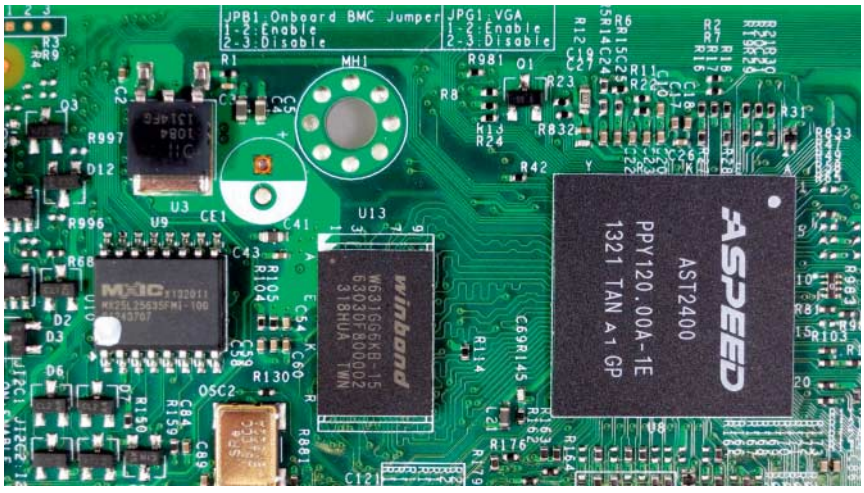
Eigentlich ist es nur eine Randnotiz, aber mit ironischem Witz: Ein Hacker hat bei der Analyse der Modem-Firmware für das neue iPhone XS Code für einen x86-Prozessor entdeckt. Möglicherweise – Intel hat das nicht offiziell bestätigt – steckt in dem von Intel zugelieferten LTE-Modem des iPhone XS ein abgespeckter x86-Kern als Mikrocontroller. Das könnte ein Kern aus der „Quark"-Familie sein, wie ihn Intel auch als Basis der Management Engine (ME) in Chipsätze einbaut. Apple lässt ins iPhone XS jedenfalls eine Variante des XMM 7560 löten, also von Intels erstem LTE-Modem aus der hauseigenen 14-nm-Fertigung. Die Vorgänger des XMM 7560 ließ Intel noch bei TSMC produzieren – schon möglich, dass man beim Umstieg auf die eigene Fertigungstechnik auch den steuernden ARM-Kern durch ein x86-Eigengewächs ersetzt hat. Relevante Auswirkungen auf das iPhone sind dadurch aber nicht zu erwarten. Ironie der Geschichte: Rund 10 Jahre nach Einführung des ersten Atom „Silverthorne", mit dem Intel bekanntlich erfolglos auf Smartphones zielte, ist x86 nun im iPhone angekommen – aber es spielt keine Rolle mehr.

Spionage mit und ohne Chips

Die schlimmsten Befürchtungen in Bezug auf die Sicherheit von Firmware und Hardware scheinen zwei Cyber-Attacken zu bestätigen. Experten von ESET melden, erstmals einen UEFI-BIOS-Schädling in freier Wildbahn gefunden zu haben: Lojax. Er wurde demnach unter anderem für gezielte Angriffe auf Notebooks von Regierungsmitarbeitern in Balkanstaaten verwendet. Dazu zweckentfremdeten die Angreifer die schon seit Jahren kritisierten Firmware-Funktionen, die einst Computrace (heute: Absolute) für den Diebstahlschutz eingebaut hat.

Umstritten ist ein Bericht von Bloomberg, laut dem US-Geheimdienste seit 2015 von Spionage-Chips auf manchen Server-Mainboards von Supermicro wissen. Dahinter steht angeblich eine Abteilung der chinesischen Volksbefreiungsarmee: Die habe Auftragsfertiger gezwungen, winzige Zusatzbauteile versteckt mit dem Fernwartungschip der Supermicro-Boards zu verbinden. Wie der Angriff im Detail funktioniert, verrät Bloomberg aber nicht. Die angeblich betroffenen Firmen Apple, Amazon und Supermicro dementieren die Behauptungen – hier steht Wort gegen Wort.

Spionage durch Chips befürchten jedenfalls alle Kontrahenten: Beim RISC-V-Kongress in Barcelona waren etwa Mitarbeiter russischer Militärzulieferer ebenso anwesend wie amerikanische Rüstungsfirmen. Bei der offenen Mikroarchitektur RISC-V muss man keine proprietäre Kröte mit zweifelhafter Füllung schlucken. RISC-V ist für viele Entwickler aber vor allem deshalb attraktiv, weil das Lizenzmodell viel einfacher ist als etwa bei ARM. Um solchen Ärger zu dämpfen, erlaubt ARM jetzt die kostenlose Nutzung des Cortex-M1 als Soft Core auf bestimmten Xilinx-FPGAs, bald soll der Cortex-M3 folgen. *(ciw@ct.de)* c't



Angeblich angezapft: Fernwartungschip Aspeed AST2400 auf Supermicro-Serverboard.