Server mit Xeon-D-SoC

Das Open-Compute-Mikroserver-Chassis Yosemite nimmt vier Xeon-D-Karten auf.

Die nagelneue SoC-Familie Xeon D-1500 (siehe S. 70) kommt schon in einigen Mikroservern und auf (Mini-ITX-)Serverboards zum Einsatz. Mainboards haben Asrock Rack (D1540D4X) und Supermicro (X10SDV-F und X10SDV-TLN4F) auf der CeBIT gezeigt, Preise sind noch unbekannt. In der Intel-Preisliste steht der Quad-Core Xeon D-1520 mit 199 US-Dollar, der Octo-Core Xeon D-1540 mit 581 US-Dollar. Supermicro baut das X10SDV auch in ein kompaktes Gehäuse mit vier Schnellwechselrahmen für 3,5-Zoll-Festplatten ein und bietet das SYS-5028D-TN4T als Server-Barebone an. Das Server-SoC sitzt auch auf Modulen für das MicroBlade-System von Supermicro, das 56 Xeon-D-Maschinchen in einem Rack-Chassis mit sechs Einheiten Bauhöhe vereint – inklusive 10-Gigabit-Ethernet-Switches und Netzteilen mit bis zu 96 Prozent Wirkungsgrad (80 Plus Titan).

Gemeinsam mit Facebook hat Intel Xeon-D-1500-Steckkarten namens Mono Lake für das Open Compute Project (OCP) entwickelt. Vier davon passen in Facebooks ebenfalls neues „Yosemite"-Chassis für Mikroserver. (ciw@ct.de)

HP-Server für Hyperscale-Rechenzentren

Auf dem Open Compute Summit hat HP die ersten fünf „Cloudline"-Server für große Rechenzentren und Internet-Dienstleister vorgestellt. HP Cloudline CL1100, CL2100 und CL2200 sind die erste Produkt-„Welle" aus einer Kooperation mit dem Auftragsfertiger Foxconn. Sie sind billiger, aber auch einfacher ausgestattet als ProLiant-Server. Die 1- und 2-HE-Einschübe besitzen das normale 19-Zoll-Format.

Später im Jahr sollen Cloudline CL7100 und CL7300 in Open-Compute-(OCP-)kompatiblen Bauformen erscheinen; der CL7300 entspricht der Microsoft-Spezifikation für „Open Cloud Server". (ciw@ct.de)

Außer ProLiant- und Apollo-Servern verkauft HP nun auch die von Foxconn gefertigte Cloudline-Serie, hier der CL7100.

Intels „Boot Guard" blockiert BIOS-Alternative Coreboot

Entwickler quelloffener Firmware kritisieren Intels Funktion „Boot Guard". Sie verhindert bei einigen PCs und Notebooks das Laden von (UEFI-)BIOS-Code, der nicht vom jeweiligen PC-Hersteller digital signiert wurde. Das soll vor Malware schützen, etwa vor „Evil Maid"-Attacken, um die Eingabe von Passwörtern mit einem manipulierten BIOS zu belauschen. Boot Guard blockiert aber auch alternative Firmware wie Coreboot, sofern sie nicht signiert ist.

Wenn ein PC-Hersteller den Coreboot-Code signiert, lässt ihn Boot Guard zu, Coreboot kommt etwa in Chromebooks und einigen Embedded Systems zum Einsatz. Freiwillige pflegen Coreboot aber auch zum nachträglichen Installieren auf bestimmten ThinkPad-Notebooks von Lenovo. Für deren jüngste Vertreter mit Broadwell-Prozessoren wie Core M oder Core i5-5000U klappt das wegen Boot Guard nicht mehr.

Boot Guard verwendet einige der von Intel unter dem Namen Trusted Execution Technology (TXT) vermarkteten Verfahren, um einen sogenannten „Verified Boot" zu ermöglichen, der ohne Trusted Platform Module (TPM) auskommt. Mit TPM ist ein „Measured Boot" möglich, bei dem Software auch später durch Abfrage bestimmter TPM-Register prüfen kann, ob zuvor ausgeführte Firmware, geladene Treiber und Bootloader signiert waren.

Boot Guard lässt sich nicht nachträglich abschalten. Der PC-Hersteller „brennt" einen SHA-256-Hash seiner kryptografischen Signatur als sogenannten OEM-Key unveränderlich in den Chipsatz. Anhand dessen prüft die im Chipsatz eingebaute Management Engine (ME) die Integrität des Firmware-Codes, bevor sie dessen Ausführung erlaubt. Für die Speicherung des OEM-Key stellt die ME sogenannte E-Fuses bereit.

Anders als es der Name der Management Engine erwarten lässt, dient sie nur bei manchen Systemen der Fernwartung. Trotzdem ist sie bei allen aktuellen Intel-Plattformen unverzichtbar, weil sie wichtige Funktionen bei der Initialisierung der Systeme ausführt. Bei den meisten steckt sie im einzigen verbliebenen Chipsatz-Baustein namens Platform Controller Hub (PCH), bei einigen Systems-on-Chip wie den Atoms aber direkt im Prozessor. Mobilprozessoren wie Core M sowie die U- und Y-Typen vereinen CPU und PCH in einem Chipgehäuse. Die ME-Firmware stellt Intel als verschlüsselte Binärdatei zur Verfügung; sie wird nur ausgeführt, wenn ihre Signatur zu einem in der Hardware hinterlegten Hash passt.

In den meisten aktuellen AMD-Prozessoren steckt ebenfalls ein 32-Bit-Mikrocontroller als System Management Unit (SMU). Die AMD-SMU führt bisher keine Funktionen ähnlich wie Intels Boot Guard aus. Die SMU-Firmware ist Teil des sogenannten AGESA-Code zur Initialisierung der CPU, den etwa auch Coreboot verwendet. In Zukunft wird AMD AGESA wohl ebenfalls als binären „Blob" ausliefern. Jüngere AMD-APUs enthalten einen ARM Cortex-A5 mit TrustZone-Erweiterung, die sich für ein Trusted Execution Environment der Firma Trustonic nutzen lässt.

Die Coreboot-Entwickler wünschen sich von der PC-Industrie, statt proprietärer Verified-Boot-Mechanismen lieber Measured Boot mithilfe von TPMs zu implementieren. (ciw@ct.de)

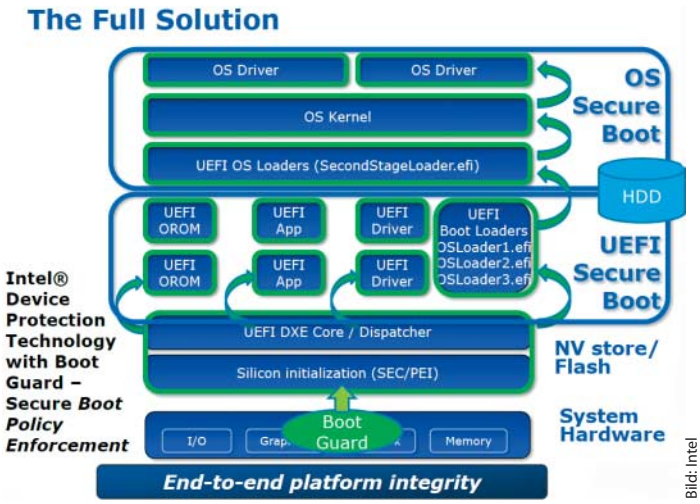

Bild: Intel

Boot Guard (grün) ist eine jener Funktionen, die sicherstellen sollen, dass der PC nicht schon beim Start Schadcode ausführt.

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover