

Kernel-Log

Linux 4.6: GeForce-900-Treiber und neue Sicherheitstechniken



Der dieser Tage erscheinende Linux-Kernel 4.6 kann auf das Cluster-Dateisystem Orangefs zugreifen. Eine ganze Palette neuer und überarbeiteter Treiber verbessert die Hardware-Unterstützung und den Support für moderne Stromspartechniken.

Von Thorsten Leemhuis

Linux-Distributionen werden bald besser mit GeForce-Grafikprozessoren der 900er-Reihe zurechtkommen, denn der Nouveau-Treiber von Linux 4.6 unterstützt diese deutlich besser. Die parallel mit Erscheinen dieser c't erwartete Kernel-Version bringt sogar Schnittstellen, durch die ein Mesa-Treiber die 3D-Beschleunigung dieser Grafikchips nutzen kann.

Bei diesen seit Herbst 2014 verkauften GPUs der Maxwell-v2-Generation war das zuvor nicht möglich: Nvidia hat bei ihnen eine Sicherheitstechnik eingeführt, bei der sich Funktionen wie die 3D-Beschleunigung nur mit einer von Nvidia signierten GPU-Firmware nutzen lassen. Eine solche hat Nvidia nach langem Warten im Februar unter einer Lizenz veröffentlicht, die eine Integration in Linux-Distributionen ermöglicht. Der Treiber kann die Grafikprozessoren allerdings nicht in ihre schnellsten Betriebsmodi schalten und liefert so nur einen Bruchteil der 3D-Performance, die Nvidias proprietäre Grafiktreiber erzielen.

Sicherheit

Um das Ausnutzen von Sicherheitslücken im Kernel-Code zu erschweren, markiert der Kernel jetzt auch seine eigenen Datenstrukturen als schreibgeschützt, die sich nach der Initialisierung nicht mehr verändern. Beim Ausführen von 32-Bit-x86-Programmen verwendet der Kernel die Möglichkeiten der Speicheradressen-Verwürfelung (ALSR/Address Space Lay-

out Randomization) jetzt deutlich stärker, um Schadsoftware den Angriff zu erschweren.

Um den Kernel robuster zu machen, wurde Kcov integriert. Dabei handelt es sich um eine Infrastruktur, die es Fehler-Suchwerkzeugen erleichtert, mehr Code-Pfade zu testen. Das nutzt das Fuzzing-Tool Syzkaller, ein eigens entwickeltes Programm zum Testen von Syscalls. Mit ihm haben die Entwickler in den vergangenen Monaten bereits über 170 Fehler im Kernel-Code aufgespürt, von denen sich einige als Sicherheitslücken entpuppten.

Dateisysteme

Linux 4.6 kann auf das Orange File System (Orangefs) zugreifen. Bei diesem Nachfolger des Parallel Virtual File System (PVFS) handelt es sich um ein Cluster-Dateisystem. Orangefs ist speziell für Umgebungen ausgelegt, bei denen der Rechnerverbund große Datenmengen verarbeitet und viele parallele Zugriffe auslöst; es kommt daher unter anderem in Wissenschaft und Forschung zum Einsatz.

Zum Einbinden eines Btrfs-Volumes mit beschädigtem Wurzelknoten ist jetzt die neue Mount-Option `usebackuproot` gedacht, die `recovery` ersetzt. Wie Ext4, XFS und einige andere Dateisysteme unterstützt Btrfs jetzt auch die Option `norecovery`, die eine automatische Fehlerreparatur beim schreibgeschützten Einbinden unterbindet; alternativ funktioniert auch `nologreplay`.

Um Strom zu sparen, kann Linux jetzt AHCI-Controller ausschalten, wenn alle von ihm versorgten SATA-Verbindungen gerade schlafen. Wie viele andere vom Kernel unterstützte Stromspartechniken muss man auch diese Möglichkeit manuell via Sysfs aktivieren, weil sie auf einigen Systemen womöglich nicht korrekt arbeitet.

Power-Management

Apropos Stromsparen: Die Kernel-Entwickler haben einige größere Umbauar-

beiten an der CpuFreq-Infrastruktur vorgenommen – dem Code also, der darüber entscheidet, mit welcher Geschwindigkeit der Hauptprozessor läuft. Dadurch ist der Prozess-Scheduler jetzt stärker involviert, was Overhead vermeidet. Diese Anbindung schafft zudem neue Schnittstellen; mit ihnen soll ein neuer, noch in Entwicklung befindlicher CpuFreq-Governor in Zukunft noch besser entscheiden können, wann sich der Wechsel in einem sparsameren oder schnelleren Betriebszustand lohnt.

Netzwerk

Damit der Kernel auch den Netzwerkverkehr von 40- und 100-Gigabit-Ethernet zeitnah verarbeiten kann, haben die Entwickler den Overhead bei der Speicher-verwaltung von Netzwerkpaketen reduziert. Dieser Verarbeitungsschritt sollte so nicht mehr so leicht zum Flaschenhals werden, der den Durchsatz schmälert oder Latenzen verlängert.

„Local Checksum Offload“ verspricht die Performance beim Tunneln des Netzwerkverkehrs zu verbessern, indem es Overhead bei der Prüfsummenerzeugung reduziert, wenn der Kernel die Pakete kapselt. Erstmals dabei ist auch der Kernel Connection Multiplexor (KCM), der es Anwendungsentwicklern erleichtern soll, Nachrichten per TCP zu verschicken. Ferner beherrscht der Kernel jetzt die in IEEE 802.1AE definierte MAC-level Encryption (MACsec). Dabei handelt es sich um eine Verschlüsselungstechnik zum Schutz vor Angreifern, die sich als Man in the Middle in die Netzwerkverkabelung einklinken.

Ablaufverfolgung

Neu ist auch die „Compile-time stack metadata verification“. Fürs Erste verbessert diese Infrastruktur lediglich die Fehleranalyse, denn durch sie zeigt ein Stacktrace jetzt die Funktions-Aufruffolge zuverlässig an, die zum Fehler geführt hat; bislang fehlten in Assembler geschriebe-

ne Funktionen dort häufiger, weil dazu eine explizite Auszeichnung im Code nötig ist, die Entwickler gelegentlich vergessen. Die Kernel-Hacker haben die neue Infrastruktur aber aus einem anderen Grund entwickelt: Sie schafft Grundlagen, über die sich in Zukunft mehr Kernel-Fehler via Kernel Live Patching (KLP) beheben lassen sollen, ohne das System neu starten zu müssen.

Container-Hosts nutzen typischerweise Control Groups (Cgroups), um den Ressourcenverbrauch eines Containers zu begrenzen, damit nicht einer sämtliche CPU-Zeit oder den ganzen Arbeitsspeicher an sich reißt. Durch die „Cgroup Namespaces“ kann der Container die ihm gewährten Ressourcen jetzt selbst mit Cgroups regeln. Das ist wichtig für Betriebssystem-Container, damit die Cgroup-Werkzeuge von Linux-Distributionen im Container genauso schalten und walten können wie beim direkten Betrieb auf der Hardware.

Ein per Hyper-V in einer virtuellen Maschine (VM) laufendes Linux 4.6 kann durch einen neuen Treiber auf PCI/PCIe-Geräte zugreifen, die Windows vom Host an das Gast-System durchreicht; Letzteres gelingt per „Discrete Device As-

signment“, das der Windows Server seit Version 2016 beherrscht.

Treiber

Bei Notebooks mit Intel-Prozessoren der Haswell- und Broadwell-Generation könnte der Akku mit Linux 4.6 ein wenig länger halten, denn bei deren GPUs aktiviert der zuständige Treiber nun Framebuffer Compression (FBC) und Panel Self Refresh (PSR). Parallel haben die Entwickler die Unterstützung für andere Stromspartechniken ein klein wenig verbessert, die gerade nicht benötigte GPU-Funktionsbereiche vorübergehend schlafen legen; weitere Änderungen dieser Art sollen bei den nächsten Kernel-Versionen folgen. Der Treiber unterstützt jetzt auch die Iris-550-Grafik, die aktuellen Linux-Distributionen größere Schwierigkeiten bereitet (siehe S. 60). Der Kernel erhielt zudem weitere Grundlagen, damit virtuelle Maschinen mittelfristig auf Teilfunktionen eines im Host verbauten Grafikprozessors von Intel zugreifen zu können, um so dessen 3D-Beschleunigung zu verwenden.

Der Grafiktreiber für die verschiedenen Raspberry-Pi-Modelle soll mit 4.6 „signifikant mehr 3D-Performance lie-

fern“. Bei MacBook-Pro-Modellen der Baujahre 2008 bis 2013 beherrscht der Kernel jetzt den Wechsel zwischen den beiden Grafikprozessoren. An Support für neuere Modelle – das sind jene mit Retina-Displays – wird noch gearbeitet.

Der Kernel bringt jetzt einen Treiber für den Audio-Prozessor mit, den AMD in einigen seiner SoCs verbaut. Neu dabei ist auch ein Treiber für die in manchen Notebooks verbauten Synaptics-Touchpads, die über das RMI4-Protokoll kommunizieren; er ersetzt einen Staging-Treiber, der Qualitätsmängel aufwies und in manchen Distributionen daher außen vor blieb.

Beim erst jüngst integrierten Netzwerktreiber Rtl8xxxu gab es eine Reihe von Detailverbesserungen, die auch die Zahl der unterstützten USB-WLAN-Chips von Realtek steigert. Mit Linux 4.6 lässt sich erstmals die Force-Feedback-Funktion des von Logitech vertriebenen Racing-Lenkrads G920 verwenden. Das sind nur einige Beispiele aus einer Reihe von Treibern, die neu sind oder für 4.6 verbessert wurden. Zusammen mit den eingangs erwähnten Verbesserungen für GeForce-GPUs werden Linux-Distributionen und Live-Linuxe so deutlich besser auf moderner Hardware laufen. (thl@ct.de) **ct**

Anzeige