Kernel-Log

Linux 4.7: RX-480-Support und Sicherheitsverbesserungen

Der Kernel soll das Stromsparpotenzial moderner Prozessoren in Zukunft stärker ausschöpfen. Linux 4.7 bringt Treiber für AMDs neue Radeon-Grafikchips mit und unterstützt rund 500 weitere Hardware-Komponenten.

Von Thorsten Leemhuis

Parallel zum Erscheinen dieser c't dürfte Linus Torvalds den Linux-Kernel 4.7 freigeben. Eine der größten Neuerungen: Der Amdgpu-Treiber unterstützt jetzt die Polaris-Grafikprozessoren, die AMD auf einer neuen Generation von Grafikkarten verbaut, die kürzlich mit der Radeon RX 480 gestartet ist (siehe S. 28). Einen dazu passenden und quelloffenen OpenGL/3D-Treiber bringt Mesa 12.0 (siehe S. 52) mit. Diese neuen Versionen dürften alle im Herbst erscheinenden Distributionen integrieren, um die neuen AMD-Grafikkarten von Haus aus ordentlich zu unterstützen.

BIOS-Selbst-Update

Über eine neue Kernel-Funktion können BIOS-Update-Programme eine aktualisierte Firmware an einem speziellen Ort des EFI-Speicherbereichs hinterlegen. Beim nächsten Start findet die Firmware die Update-Datei und kann sie nach einer Signaturprüfung automatisch einspielen. Solche Updates mit Hilfe von „UEFI Capsules“ sollen das Aktualisieren der Firmware erleichtern; die BIOSe der derzeit gängigen PCs, Notebooks und Server beherrschen diese Funktion allerdings nicht.

Gangschaltung

Durch den neuen Cpufreq-Governor Schedutil soll der Kernel in Zukunft besser entscheiden können, ob es gerade angebracht ist, den Prozessor in einen schnelleren oder sparsameren Betriebsmodus zu schalten. Dazu nutzt Schedutil Daten, die er über jüngst eingeführte Schnittstellen vom Prozess-Scheduler bekommt. Das Ganze gilt als wichtiger Meilenstein, der auch Grundlagen für besseres Power-Management für Smartphone- und Tablet-Prozessoren schafft; die neue Herangehensweise steckt aber noch in den Kinderschuhen und ist bislang allenfalls eingeschränkt alltagstauglich.

Schlange stehen vermeiden

Linux 4.7 soll kurze und sporadisch auftretende Wartezeiten vermeiden, die bislang häufiger auftreten, wenn der Kernel eine sehr große Zahl von Netzwerkpaketen verarbeitet. Diese Latenzspitzenvermeidung ist einigen Änderungen am TCP-Code zu verdanken. Der Kernel kann dadurch jetzt die Verarbeitung von Netzwerkpaketen an mehr Stellen unterbrechen, um sich vorübergehend anderen Arbeiten zu widmen. Neu ist auch „Partial Segmentation Offload“, das ein Tunneln des Netzwerkverkehrs beschleunigen kann; bei Tests des zuständigen Entwicklers mit einer 40-Gigabit-Ethernetchip von Intel steigerte die Technik den Durchsatz von 12 auf 20 GBit/s.

Sicherheit

Die Kernel-Quellen erläutern in Documentation/security/self-protection.txt jetzt Selbstschutztechniken, die der Kernel bereits bietet oder auf der To-do-Liste des „Kernel Self Protection Project“ stehen. Dort arbeiten einige Entwickler seit einigen Monaten verstärkt darauf hin, den Kernel robuster gegen Angriffe zu machen: Angreifer sollen Systeme nicht übernehmen können, selbst wenn sie über irgendeine Kernel-Lücke an beliebige Stellen des Arbeitsspeichers schreiben können.

Um Angriffe zu erschweren, haben die Entwickler in 4.7 die „SLAB freelist randomization“ integriert, die mit Heap Overflows arbeitende Angriffe erschwert. Die Build-Infrastruktur kann die Angriffsfläche jetzt reduzieren, indem sie alle externen Einsprungpunkte (Exported Symbols) aus dem kompilierten Kernel-Image entfernt, die beim Kernel-Bau übersetzte Module nicht verwenden; sollten Distributionen diese Funktion aufgreifen, könnte das den Einsatz selbst kompilierter Kernel-Module erschweren. Das neue LSM (Linux Security Module) LoadPin kann sicherstellen, dass vom Kernel geladene Dateien (Module, Firmware, ...) von einem vertrauenswürdigen, gegen ungewollte Modifikationen geschützten Datenträger kommen. Um Angriffe über den Interpreter für den Berkeley Packet Filter (BPF) zu erschweren, verwürfelt „Constant Blinding“ jetzt die in BPF-Programmen verwendeten Konstanten.

Entfernte Kopie

Der im Kernel enthaltene Code zum Zugriff auf NFS-Server kann Kopiervorgänge jetzt erheblich beschleunigen. Der NFS-Client kann einem NFS-4.2-Server nämlich jetzt mitteilen, welche Daten kopiert werden sollen; der macht das dann autark, was den Vorgang enorm beschleunigt, weil die kopierten Daten nicht vom Server zum Client und wieder zurück fließen müssen.

Auf nichtflüchtige Speichermedien wie NV-DIMMs kann man jetzt direkt über Gerätedateien (/dev/dax) zugreifen. Das vermeidet den Overhead von Dateisystemen, die bislang für den Zugriff auf Persistent Memory (Pmem) erforderlich waren.

Analysetechniken

Über den Berkeley Packet Filter (BPF) des Kernels ausgeführte Programme können nun Messdaten vorverarbeiten, die durch Prüfpunkte (Tracepoints) im Kernel-Code erzeugt wurden. Solch eine frei programmierbare und Kernel-interne Vorverarbeitung von Messwerten kann Overhead vermeiden und bietet so endlich eine leicht verwendbare dynamische Tracing-Funktion, wie sie Anwender von Dtrace oder Systemtap schätzen.

Die Event-Tracing-Infrastruktur von Ftrace kann durch die neuen Histogram Trigger (kurz: Hist Trigger) jetzt autonom

Analysedaten akkumulieren. Darüber kann der Kernel beispielsweise selbst ein via Sysfs abrufbares Histogram erstellen, das zeigt, welche Kernel-Funktion wie viel Arbeitsspeicher per `kmalloc()` angefordert hat. Die Hist Trigger erleichtern so Analysen und vermeiden Overhead, der das System verlangsamt und die Messung verfälscht.

Der Kernel soll Speicherknappheit (Out-of Memory/OOM) jetzt verlässlicher erkennen und zuverlässiger reagieren, wenn er in solch einer Situation einen Prozess abschießt, damit sich das System nicht komplett festfährt. Die Kernel-Entwickler haben zudem erste Schritte unternommen, um zukünftig reStructuredText (RST) als Hauptformat für die Kernel-Dokumentation zu nutzen, für die bislang zahlreiche verschiedene Formate zum Einsatz kommen.

Ausgabefähigkeiten

Im Treiber für Intels moderne Grafikprozessoren steckt jetzt ein Color Manager, um zusammen mit passenden Userland-Programmen eine möglichst realistische Farbwiedergabe zu gewährleisten. Der Kernel-Treiber beherrscht das Farbmanagement aber nur bei GPUs von Broadwell- und Skylake-Prozessoren, zu denen die Core-i-Modelle der 5000- und 6000er-Serie gehören.

Der Nouveau-Treiber kann jetzt auch den Nvidia GeForce 830M ansprechen, der in einigen Lenovo-Notebooks steckt. Der VC4-Treiber, der für die Grafikkerne der verschiedenen Raspberry-Pi-Modelle zuständig ist, unterstützt jetzt per Display Parallel Interface (DPI) angebundene Bildschirme. Das schafft zugleich Grundlagen, mit denen der Treiber bald per Display Serial Interface (DSI) angesteuerte Panels unterstützen soll.

Hardware-Tauglichkeit

Linux 4.7 bringt eine ganze Reihe neuer und um Hardware-Support erweiterte Treiber mit. Darunter befindet sich einer zur Unterstützung der Thunderbolt-Controller, die Apple bei einigen 2011 und 2012 gebauten Modellen von iMac, Mac Mini und MacBook Pro verbaut hat. Neu ist auch Support für den Xbox One Elite Controller von Microsoft oder Intels WLAN-Chip 9260. Ferner weiß der Kernel jetzt auch die auf PC- und Notebook-Mainboards verbauten HD-Audio-Codecs von Realtek anzusprechen.

Laut den Skripten der Linux Kernel Driver Database (LKDDb) enthalten die Kernel-Quellen jetzt Treiber für 26 300 verschiedene Geräte oder Geräteklassen, die der Kernel über Bezeichner wie ACPI-, PCI- und USB-IDs erkennt. Damit unterstützt Linux 4.7 rund 500 Hardware-Komponenten mehr als 4.6; zirka 180 davon sind PCIe/PCI- oder USB-Geräte.

(thl@ct.de) c't