Zacks Kernel-News

Neue Rootkit-Generation

Die Tatsache, dass der 2.6-Kernel die Systemcall-Tabelle nicht mehr unterstützt, hat manchen Rootkit-Autor kurzfristig aus der Bahn geworfen. Viele Rootkits nutzten die Tabelle, um Systemcalls abzufangen und damit Root-Privilegien zu erobern.

Es gibt aber keinen Grund sich jetzt sicher zu fühlen, da weiterhin einige Möglichkeiten bestehen, Root auf einer Linux-Maschine zu werden. Es ist zum Beispiel möglich, weiterhin Systemcalls abzufangen, auch ohne auf eine exportierte Systemcall-Tabelle angewiesen zu sein. In einem solchen Szenario sucht das Rootkit nach einem beliebigen exportierten Symbol. Ist es fündig geworden, durchsucht es anschließend den Speicher in der Nähe des Symbols nach etwas Nützlichem. Es gibt jetzt schon Rootkits wie beispielsweise »adore-ng« die mit allen bekannten Funktionen auf Linux 2.6 portiert sind.

Im Fall von »adore-ng« hatte der Rootkit-Autor die Systemcall-Tabelle bereits als Eintrittspunkt aufgegeben und den Angriff auf ungeschützte Systeme über das virtuelle Dateisystem fortgesetzt. ■

Fibrechannel-Treiber als Open Source

Die Firma Emulex veröffentlicht Treiber für die Light-Pulse-Fibre-Channel-Adapter als Open Source und hat ein entsprechendes Sourceforge-Projekt ins Leben gerufen. Der veröffentlichte Code stammt von dem ehemals proprietären Treiber. Emulex hofft, dass sich zahlreiche Entwickler am Projekt beteiligen werden und dass der Treiber den Weg in den 2.6-Kerneltree findet.

Tatsächlich haben wichtige Kernelhacker wie Jeff Garzik den Code bereits unter die Lupe genommen und die Emulex-Entwickler mit Feedback geradezu überschüttet. Die Kernelentwickler sind sich einig, dass der Treiber zwar viel hässlichen Code enthält, Emulex aber auf dem richtigen Weg ist.

Die Entscheidung, den Treiber offen zu legen, hat das Unternehmen übrigens von sich aus getroffen, öffentlichen Druck durch die Entwicklergemeinschaft gab es in diesem Fall nicht. Bei Emulex ist man der Auffassung, dass sich der Treiber als Open-Source-Projekt besser entwickeln kann, als es bei rein internen Abläufen der Fall wäre. ■

Treiber für Intels Pro/Wireless-Adapter

Intel hat ein Free-Software-Projekt ins Leben gerufen, um den MiniPCI-Netzwerkadapter Intel Pro/Wireless 2100 für Centrino zu unterstützen. Dabei wurden ein Sourceforge-Projekt und eine Mailingliste aufgelegt sowie der Support für die 2.4- und 2.6-Kernelserien implementiert. Im Sinne der Open-Source-Philosophie stellte Intel den Code in einem frühen Betastadium bereit, um die Entwicklung und laufende Bugreports aus der Community zu fördern.

Der Treiber enthält zwar eine Closed-Source-Firmware, laut Projektleiter James Ketrenos wird diese aber ausschließlich auf der Hardware geladen und ausgeführt. Zu keinem Zeitpunkt greift die Firmware in den Linux-Kernel ein.

Closed-Source-Firmware ist ein rotes Tuch für die Linux-Community, aber beide Seiten scheinen einen Kompromiss zu suchen, was anhand des Intel-Projekts zu erkennen ist. Intel ist zwar dazu bereit, manche Open-Source-Treiber auf kooperative Art und Weise zu entwickeln, dennoch gelten etliche Einzelheiten der Hardware als Betriebsgeheimnis, das unbedingt zu schützen ist. ■

Sicheres Linux für Handhelds

Umbrella ist ein neues Sicherheitsprojekt für Linux auf Handhelds. Es benutzt die Linux Security Modules (LSM), die als API für solche Ansätze im 2.6er Kernel standardmäßig vorgesehen sind. Umbrella ähnelt älteren Projekten wie LIDS oder SE-Linux. Deshalb wartet es mit zentralen Funktionen für die Zugriffsteuerung, signierten Dateien sowie einfachen und klaren Konfigurationsoptionen auf. Die Einschränkungen, mit denen ein Prozess unter Umbrella läuft, sind dabei an die entsprechenden signierten Dateien im Filesystem gebunden.

Projektleiter Kristian Soerensen geht davon aus, dass sich das grundlegende Setup eines Handheld-Device nach der Einrichtung kaum noch ändert. Zudem nimmt er an, dass die knappen Hardwareressourcen typischer Handheld-Devices zu einer klar abgegrenzten Reihe von Anwendungen wie etwa E-Mail, Adressbuch, Spiele und Terminplanung führen werden. Diese Begrenzungen sollen es den Umbrella-Entwicklern und Software-Integratoren erlauben, sicherheitsrelevante Features des Projekts mit einem vertretbaren Aufwand zu nutzen. ■

Coding Style: Alles bleibt beim Alten

Seit vielen Jahren dient die Datei »CodingStyle«, die zum Lieferumfang der Kernelquellen gehört, als Richtlinie für das Organisieren und Formatieren von Kernelcode. Doch nicht jeder hält sich daran. Im Gegenteil: Viele Entwickler beschweren sich über die stilistischen Prinzipien, die ihren eigenen Vorstellungen widersprechen.

Dennoch tauchen von Zeit zu Zeit Clean-up-Patches in der Kernel-Mailingliste auf, mit dem Zweck, verschiedene Abschnitte des Kernels mit dem aktuellen Stand des Codingstyle-Dokuments besser in Einklang zu bringen. Bei einem neuerlichen Optimierungsversuch wurde Entwicklern nahe gelegt, in Code-Kommentaren auf den Apostroph bei Wörtern wie „don't" und „can't" zu verzichten und dafür „dont" und „cant" zu schreiben, weil der Apostroph häufig auch als Trennzeichen dient. Bei der Auswertung von Codezeilen kann es deshalb leicht Verwirrung geben.

Aber grammatisch richtiges Englisch hat sich letztlich durchgesetzt und die Vorschläge wurden zurückgenommen. »CodingStyle« rät den Programmierer jetzt, entweder den Apostroph zu nutzen oder solche Abkürzungen zu vermeiden.

Außerdem gab es Diskussionen darüber, ob das Limit von 80 Zeichen pro Zeile für die Kernelquellen zu eng gesetzt ist, weil viele Entwickler mit Xterms arbeiten, die weitaus mehr als 80 Zeichen unterstützen. Andrew Morton hat sich an dieser Diskussion beteiligt und gegen die Bemühungen um eine Erweiterung des Limits gestemmt. An einem Punkt sagte er: „Ja sicher sind 80 Zeichen Unsinn und in einer perfekteren Welt hätte »CodingStyle« schon vor fünf Jahren 96 Spalten genehmigt. Nur ist das nicht passiert."

Wie sich herausstellt, gibt es tatsächlich noch konservative Entwickler – unter anderen David Weinehall, den Maintainer von Kernel 2.0 –, die mit 80-Zeichen-Bildschirmen arbeiten. Obwohl das 80-Spalten-Limit eines Tages vielleicht gekippt wird, kann man im 2.6-Tree nicht damit rechnen. ■

Kernel 2.6.5

Linus Torvalds hat Anfang April Version 2.6.5 des Linux-Kernels freigegeben. Sie folgt nur etwa vier Wochen nach dem Vorgänger 2.6.4. Die neue Release behebt hauptsächlich Fehler, vor allem bei der Unterstützung von PowerPC-Architekturen wie PPC32 und PPC64, optimiert wurde auch der Support für auf PowerPC basierende I-Series von IBM.

Die größten Änderungen betreffen die Sound-Erzeugung mit den Alsa-Treibern, die seit 2.6 zum Standardkernel gehören. Hier haben die Kernelentwickler die neueste CVS-Version des Alsa-Projekts integriert, weitgehend identisch mit Alsa 1.0.4. Außerdem kamen Treiber für neue USB-Geräte hinzu. ■

Großoffensive für Kernel-Debugger

Unter der wohl wollenden Beobachtung von Maintainer Andrew Morton sind groß angelegte und abgestimmte Bemühungen im Gang, den Kernel-Debugger KGDB in den 2.6-Tree zu integrieren. Linus Torvalds hat sich in der Vergangenheit immer dagegen gestemmt, da dies nach seiner Meinung nur zu schlechten Gewohnheiten der Entwickler beim Debugging führt. Andere Entwickler sind nicht so streng, allen voran Andrew Morton, der offizielle 2.6-Maintainer.

Ein Problem stellen die vielen unabhängigen KGDB-Patches dar, die teilweise kollidieren und manchmal schlicht überflüssig sind. Schon Ende Januar hat Tom Rini deshalb ein Bitkeeper-Repository für die Arbeiten an KGDB eingerichtet, um die Bemühungen zu konzentrieren und die redundanten Beiträge zu entfernen. Etwas später hat Amit S. Kale ein ähnliches Projekt auf Sourceforge eingerichtet, wobei er den Bitkeeper-Tree durch CVS ersetzte.

In der Folge arbeiteten Tom, Amit und ein paar andere Entwickler wie Pavel Machek zusammen, um den Code weiter zu perfektionieren. Andrew Morton hat gelegentlich nachgesehen, ob die Arbeiten bereit für die Integration in 2.6 waren.

Zum damaligen Zeitpunkt war das Projekt wohl noch nicht so weit, aber schon Anfang März hatten Amit und die anderen die KGDB-Patches in mehrere kleinere Gruppen aufgeteilt und sich Gedanken gemacht, wie sie am besten einzureichen seien, um eine Integration zu ermöglichen. Für einige Patches wurde zu diesem Zeitpunkt ein Feature Freeze vereinbart, andere blieben in Entwicklung. Die eingefrorenen Patches bildeten ein KGDB-Lite-Patchset mit den Grundfunktionen.

Weitere Features sollten nach dessen Integration hinzukommen. Außerdem veröffentlichte Amit eine Dokumentationsreihe. Darin beschrieb er, wie man einen Kernel mit KGDB-Support kompiliert und nutzt. Danach – schon Mitte März – hielt er die Zeit für gekommen, eine erste Gruppe von Patches einzureichen. Wie sich herausstellte, musste Andrew gar nicht überzeugt werden, er war längst gewillt, mehr als die Lite-Patches zu integrieren. Er bestand förmlich auf Features, von denen die KGDB-Entwickler glaubten, dass sie zur Ablehnung von KGDB führen würden.

Einige der auch von ihm gewünschten Features hätten aber die Eleganz des Codes in Mitleidenschaft gezogen. Die Arbeiten werden also im Moment noch fortgesetzt, aber es scheint schon jetzt klar zu sein, dass 2.6 früher oder später eine komplette KGDB-Implementierung enthalten wird. *(Zack Brown/uwo)* ■