Linux 5.4内核的新特性

武彦整理 2020-02-11

**Linux 5.4主要新特性：**

* 内核锁定（Kernel Lockdown）

通过以Linux Security Module模块部署，来限制某些应用程序访问内核。5.4中添加了新的保护层，以使其能够按其创建者的意图运行软件，从而阻止了恶意行为者。

锁定功能旨在通过限制对内核功能的访问来进一步增强Linux安全性，这些功能可能允许通过用户域进程提供的代码执行任意代码。

简而言之，即使root帐户也无法修改内核代码，如果root帐户遭到入侵，此操作将大打折扣，而系统的其余部分将很难在内核级别进行入侵，简而言之，它增强了Linux的安全性。

有两种锁定模式：完整性和机密性。

在完整性锁定模式下，将禁用允许用户态修改正在运行的内核的内核功能。

在机密性模式下，允许用户态从内核中提取机密信息的内核功能也被禁用。

此锁定功能适用于设备制造商和Linux发行版（特别是面向企业的发行版），默认情况下，锁定模块将关闭。

* exFAT支持

Microsoft的FAT文件系统不允许传输大于4GB的文件，为了克服此限制，Microsoft创建了exFAT文件系统。Microsoft最近开放了exFAT文件系统的源代码，Linux 5.4内核现在将为Linux提供原生的exFAT支持，以便用户在连接exFAT格式磁盘时能够获得out-of-the-box体验。

* haltpoll CPU调节器
* iocost（以前为io.weight） I/O 控制器
* 华为EROFS 文件系统
* fs-verity 文件完整性机制

用于检测文件是否被篡改

* dm-clone 设备映射器对象

用于Live克隆块设备

* virtiofs 文件系统

在Android上引入了名为virtio-fs的应用程序内存管理机制，这是在主机和来宾之间分享文件的高性能virtio驱动程序。可在使用虚拟机时在主机和来宾操作系统之间共享文件/文件夹。

* Faster large directory modifications on XFS
* 围绕现有文件系统（例如Btrfs）和硬件有一些修复和改进

Improvements to the way cryptographic keys are added, removed and/or derived in fscrypt, the encryption API used in ext4/f2fs/ubifs file system encryption help improve security.

Also on the file system front, there’s optional case-insensitive file and folder handling available in f2fs.

* 对BPF的支持：一次编译、到处运行
* dm-clone设备映射器目标
* 内核符号名称空间
* 新的随机数生成器，旨在解决早期的引导熵问题
* Sound Open Firmware improvements
* 对新设备的支持
  + Intel Tiger Lake CPU
  + Qualcomm Snapdragon 855 SoC
  + Intel Lightning Mountain SoC
  + 部分新型AMD和Intel GPU
  + Intel Icelake Thunderbolt
* 其他
  + 能够在Arm消费者笔记本电脑上运行主线内核
  + 支持FlySky FS-iA6B无人机接收器
  + 通过Wine/Photon修复Windows游戏

**参考资料：**

<https://geeknous.com/linux-5-4-kernel-release-features/>