重新思考安全含义让Linux系统更安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E9_87_8D_E6_96_B0_E6_80_9D_E8_c103_260896.htm 安全的定义 安全是当今 IT 相关头条新闻的一个重要话题。经常出现的系统漏洞和安全补丁以及病毒和蠕虫是每个使用计算机的人都耳熟能详的名词。因为几乎每台计算机系统都连接到另外的计算机或者连接到 Internet，因此确保这些计算机的安全，对于减少入侵、数据窃取或丢失、误用甚至对第三方的责任而言是至关重要的。 确保安全即使对于没有连接到网络的独立的计算机也是很重要的。必须自可信赖的来源安装应用程序，比如经过验证的并检查过病毒的光盘。对应用程序数据也必须同样小心。例如，对于可以执行强大的宏语言或者引入非法数据的软件程序包（office 套件等等），其软件缺陷可能会被利用来执行任意的代码。因此，应用程序数据在拷贝到计算机之前必须经过完整性检查。可以通过将数据放置在一个安全的地方来控制对系统的访问（当然，不考虑来自已授权人员的攻击）。 当系统连接到网络并向其他计算机提供服务（有意地或无意地）时，事情会变得更为棘手。在那种情况下，数据可能不只是来自系统管理员，因为客户机程序要使用所提供的服务，而系统漏洞可能会让入侵者控制计算机。 这就是为什么安全是从开始计划直到拆除系统的整个系统生命周期中最基本的问题。但是，安全的确切含义是什么？ 通常，数据安全和系统安全可以分开来考虑。 数据安全 通常被认为是确保以下方面的所有努力： 机密性（Confidentiality）。 完整性（Integrity）。 可用性（Availability）。 综合起来，这些

被称作是存储在计算机上的数据的“ CIA ”。对 /etc/passwd 等配置数据的保护可以归类为数据安全。系统安全 指的是计算机平台本身。美国 National Information Systems Security Glossary（参阅 参考资料 以获得链接）对系统安全的定义如下： 系统安全。对信息系统的保护，防止未授权的访问及对信息（不论是存储中的、正在处理的还是正在传输的）的修改，并防止对授权用户服务的拒绝或对未授权用户服务的允许，包括那些检测、记录和反击此类威胁的措施。 重要的是要认识到系统安全强调的是一个反复的过程，这个过程包括应用安全补丁、经常审计、控制，同时最起码要有一个安全的系统配置。就此而言，不可能保证绝对的安全，也不可能提供百分之百安全的服务。目标更应该是在安全性、系统可用性和维护这个安全层级所需要的努力这三者之间找到一个折衷点。这个折衷取决于安全对于存储在计算机中的数据来说的重要性以及这些数据预期的使用情形（阅读 Bruce Schneier 的 Secrets and Lies，John Wiley &amp. Sons，2000；参阅 参考资料以获得链接）。 