Linux下一种ELF文件的代码签名验证机制（1） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022_Linux_E4_B8_8B_E4_B8_c103_144521.htm 当入侵者在系统取得一定权限后，他们通常会在系统中植入恶意代码，并利用这些代码为日后的入侵提供方便。增加或修改 ELF 文件正是入侵者植入恶意代码的常用途径。本文将描述一种 Linux 下 ELF 文件的代码签名及验证机制的设计与实现，这种机制能有效防止基于 ELF 文件的恶意代码的入侵，并同时提供了灵活的分级验证机制，使系统在安全性与效率方面取得最佳平衡。 1 引言 随着 Linux 的不断发展，已有越来越多的人开始推广和使用 Linux，其安全性也受到越来越多的挑战。ELF（Executable and Linkable Format）[1] 作为 Linux 下最主要的可执行二进制文件格式，自然成了病毒及各种恶意代码的攻击目标。事实证明，有不少 Linux 下的病毒程序就是通过直接修改 ELF 文件的方法来实现入侵的 [10]。传统的 Unix 系统（包括 Linux）并不会对执行的代码进行完整性和合法性检测，因而让很多病毒程序以及木马程序有机可乘。 代码签名验证是一种能够有效的防止病毒以及其他恶意代码入侵的方法。对于 Linux 下的代码签名验证机制，早几年就已经有人研究。文[2]提出了在安装时进行签名验证的方法，并通过修改 chmod 系统调用控制文件的可执行属性，但这种方法无法检测程序安装后对代码的任何修改，有一定的局限性。文 [3] [4] [5] 描述的都是在执行时进行签名验证的方法，其中 [4] [5] 采用了缓存已验证文件的策略，使效率较 [3] 有很大提高。但是，它们将所有 ELF 文件 "一视同仁"，没有主次轻重之分，缺少灵活性。

本文提出了一种改进的基于 ELF 文件格式的代码签名验证机制，通过提供更加灵活的分级验证方式，进一步提高验证效率，并且使系统在安全性与效率方面取得平衡。 2 签名验证原理 我们采用完全符合 PKCS [8] 系列标准的签名验证算法，并兼容所有符合 X509 格式的证书，以 RSA [6 ][7] 非对称密钥体制为基础来完成对 ELF 文件代码的签名验证。 