其他地方，在这一观点下，惟一的解决办法是回复到上一个已知干净的完整备份。如果没有可用的备份，就要求从原始CD-ROM/DVD进行新的安装。

3. Sony rootKit

在2005年，Sony BMG公司发行了一些包含rootkit的音乐CD。这被Mark Russinovich（Windows管理工具网站www.sysinternals.com的共同创始人之一）发现，那时他正在开发一个rootkit检测工具并惊奇地在自己的系统中找到了一个rootkit。他在自己的blog中写下了这件事，这很快传遍了各大媒体和互联网。一些科技论文与此相关（Arnab和Hutchison, 2006; Bishop和Frincke, 2006; Felten和Halderman, 2006; Halderman和Felten, 2006;Levine et al.,2006）。这件事导致的轰动直到好几年以后才逐渐停止。以下我们对此事件做简单的描述。

当用户插入CD到一个Windows系统计算机的驱动器中时，Windows查找一个名为autorun.inf的文件，其中包含了一系列要执行的动作，通常包括打开一些CD上的程序（如安装向导）。正常情况下，音乐CD没有这些文件因为即便它们存在也会被单机CD播放器忽略。显然Sony的某个天才认为他可以聪明地通过放置一个autorun.inf文件在一些CD上来防止音乐盗版。当这些CD插入计算机时，就会立即安静地安装一个12MB大小的rootkit。然后一个许可协议被显示，其中没有提到任何关于软件被安装的信息。在显示许可的同时，Sony的软件检查是否有200种已知的复制软件中的任一种正在运行，如果有的话就命令用户停止这些复制软件。如果用户同意许可协议并关闭了所有的复制软件，音乐将可以播放，否则音乐就不能播放。即使用户拒绝协议，rootkit仍然被安装。

这个rootkit的工作方法如下。它向Windows内核插入一系列文件名由“sys”起始的文件。这些文件之一是一个过滤器，这个过滤器截取所有向CD-ROM驱动器的系统调用并禁止除Sony的音乐播放器之外的所有程序读取CD。这一动作使得复制CD到硬盘（这是合法的）变得不可能。另一个过滤器截取所有读取文件、进程和注册表列表的调用，并删除所有由“sys”起始的项（即便这些项是由与Sony和音乐都完全无关的程序而来的），目的是为了掩盖rootkit。这一方法对于rootkit设计新手来说非常标准。

在Russinovich发现这一rootkit之前，它已经被广泛地安装，这完全不令人惊讶，因为在超过2000万张CD上包含此rootkit。Dan Kaminsky（2006）研究了其广度并发现全世界超过50万个网络中的计算机已经被感染。

当消息传出时，Sony的第一回应是它有权保护其知识产权。在National Public Radio的一次采访中，Sony BMG的全球数字业务主席Thomas Hesse说：“我认为绝大多数人甚至不知道什么是rootkit，那么他们何必那么在意它？”当这一回应激起了公众怒火时，Sony让步并发行了一个补丁来移除对“sys”文件的掩盖，但仍保留rootkit。随着压力的增加，Sony最终在其网站上发布了一个卸载程序，但作为获得卸载程序的条件，用户必须提供一个E-mail地址并同意Sony可以在以后向他们发送宣传材料（这些可以被大多数人过滤掉）。

随着故事的终结，人们发现Sony的卸载程序存在技术缺陷，使得被感染的计算机非常容易遭受互联网上的攻击。人们还发现该rootkit包含了从开源项目而来的代码，这违反了这些开源项目的著作权（这些开源项目的著作权要求对其软件的免费使用也发布源代码）。

除了空前的公众关系灾难之外，Sony也面临着法律危机。德克萨斯州控告Sony违反了其反间谍软件法以及欺诈性贸易惯例法（因为即使许可被拒绝rootkit仍然会被安装）。此后在39个州都提起了公诉。在2006年12月，在Sony同意支付425万美元、同意停止在其未来的CD中放入rootkit并授权每位受害者可以下载一个有限的音乐目录下的三张专辑之后，这些诉讼得以解决。在2007年1月，Sony承认其软件秘密监视用户的收听习惯并将其报告回Sony也违反了美国法律。在与公平贸易委员会（FTC）的协议中，Sony同意支付那些计算机遭到其软件破坏的用户150美元的补偿。

关于Sony的rootkit的故事已经为每一位曾经认为rootkit只是学术上的稀奇事物而与现实世界无关的读者提供了实例。在互联网上搜索“Sony rootkit”会发现大量补充信息。

9.8 防御

面对危机四伏的状况，那么还有确保系统安全的可能吗？当然，是有的，下面的小节要介绍一下几种设计和实现系统的方法来提高它们的安全性。一个最重要的概念就是全面防御（defense in depth）。