# Windows 的缺陷

尽管支持抢先式多任务处理，但进程生成却很昂贵——虽然比不上 VMS，但是（平均生成一个进程需要0.1秒左右）要比现在的 Unix 高出一个数量级。脚本功能薄弱，操作系统广泛使用二进制文件格式。除了此前我们总结过的，还有这些后果：

大多数程序都不能用脚本调用。程序间依赖复杂脆弱的远程过程调用（RPC）来通信，这是滋生 bug 的温床。

……

Unix 的系统配置和用户配置数据分散存放在众多的 dotfiles(名字以“.”开头的文件)和系统数据文件中，而 NT 则集中存放在注册表中。以下后果贯穿于设计中：

- 注册表使得整个系统完全不具备正交性。应用程序的单点故障就会损毁注册表，经常使得整个操作系统无法使用、必须重装。
- 注册表蠕变( registry creep ) 现象：随着注册表的膨胀，越来越大的存取开销拖慢了所有程序的运行。

互联网上的 NT 系统因易受各种蠕虫、病毒、损毁程序以及破解（crack）的攻击而臭名昭著。原因很多，但有一些是根本性的，最根本的就是：NT 的内部边界漏洞太多。

NT 有访问控制列表，可用于实现用户权限组管理，但许多遗留代码对此视而不见，而操作系统为了不破坏向后兼容性又允许这种现象的存在。在各个 GUI 客户端之间的消息通讯机制也没有安全控制，如果加上的话，也会破坏向后兼容性。

虽然 NT 将要使用 MMU，出于性能方面的考虑，NT 3.5后的版本将系统 GUI 和优先内核一起塞进了同一个地址空间。为了获得和 Unix 相近的速度，最新版本的 NT 甚至将 Web 服务器也塞进了内核空间。

由于这些内部边界漏洞产生的协合效应，要在 NT 上达到真正的安全实际上是不可能的。如果入侵者随便作为什么用户把一段代码运行起来（例如，通过 Outlook email 宏功能），这段代码就可以通过窗口系统向其它任何运行的应用程序发送虚假信息。只要利用缓存溢出或 GUI 及 Web 服务器的缺口就可以控制整个系统。