**基于虚拟化技术的入侵容忍系统**

**一、基本概念**

**（一）虚拟化技术**

虚拟化（Virtualization）是一种资源管理技术，是将计算机的各种实体资源，如服务器、网络、内存及存储等，予以抽象、转换后呈现出现，打破实体结构间的不可分割的障碍，使用户可以比原本的组态更好的方式来应用这些资源。这些资源的新虚拟部分是不受现有资源的架设方式，地域或物理组件所限制。一般所指的虚拟化资源包括计算能力和资源存储。

**虚拟化的历史**

1. 硬件虚拟化

使用VMM（Virtual Machine Monitor）对所有的硬件接口进行虚拟化。

1. 处理器虚拟化

处理器虚拟化的意思是对处理器进行仿真。现代编译器所使用的模型为将编译器移植到新目标体系结构上提供了很大的灵活性（通过一种中间语言将前后端分隔开来）。

1. 指令集虚拟化

虚拟化的最新发展称为指令集虚拟化，或者二进制转换。在这种模型中，虚拟指令集被转换成底层硬件的物理指令集，这个过程通常是动态的。当代码执行时，就会对代码的某个段进行转换。如果出现分支情况，就会倒入新代码集并进行转换。这使它与缓存操作非常类似，后者是将指令块从内存移动到本地快速缓存中执行。

（二）入侵容忍系统

**二、问题**