**论文综述**

**(Dune: Safe User-level Access to Privileged CPU Features，**

**IX: A Protected Dataplane Operating System for**

**High Throughput and Low Latency)**

**朴东奎**

**2015280404**

目前计算机技术已达经到了可以虚拟化硬件的程度，有各种各样的虚拟化软件，他们不仅提供和现有的炒作系统一模一样的界面，并提供还不错的性能。本人要简单介绍一下两边论文提到的两种虚拟化系统系统

第一个论文中的Dune是一个提供应用软件的系统，它直接而安全地访问硬件功能如环保护、页表和标记的TLB，同时为进城保存现有的操作系统界面。它为提供进程使用在现代进程里的虚拟化硬件，而不是机器抽象。

它由一个初始化虚拟硬件、内核与用户级库之间介导的相互作用的内核模块，其用户级库帮助应用程序管理特权硬件特性。

文中他们以64-bit x86 Linux实验了Dune。他们使用Dune执行了三种用户端应用软件，其软件可以访问特权硬件的好处：一个不受信任的代码的sandbox、特权分离装置和一个垃圾收集器。

文中使用Dune简化了这些应用程序的实施，并提供了显着的性能优势。

第二个论文提出了一个数据层操作系统称为IX，它提供高的输入输出性能，同时保持强大地保护现有内核提供的关键优势。

IX通过硬件虚拟化分开地管理并安排从网络处理（dataplane）的内核（控制平面）函数。

dataplane架构建立在本地、zero-copy API，为了dataplane实例、处理有界批包来完成、通过消除相干交通和多核同步。

它通过硬件线程和网络队列优化带宽和延迟。

文中表明IX性能胜于Linux和state-of-the-art、用户空间网络栈。

除此之外，IX提高了广泛部署的吞吐量，高达3.6的键值存储并减少了尾部潜伏期两倍。

对于信息安全方面来讲，开发高性能的虚拟化软件是很重要的，几年前一家公司开发了通过虚拟化隔离系统防止传染病毒的软件，它格力的功能倒是不错但主要是它的性能不够高跟不上现有的操作系统，如果当时它们具有高性能的虚拟化技术，肯定会有更好的结果（当时那个软件项目因性能不够高而撤退了）。除此之外，虚拟化软件经常用于分析恶意代码，在分析恶意代码的时候，由于有可能本地系统被恶意代码受影响，因此基本上用虚拟化软件分析恶意代码，如VMware、virtualbox，这种强狂下这些也被称为sandbox。

最近有些韩国企业采用了虚拟化硬件，使用它上班，因此服务器不被工作人员受影响，但是还是有性能上的问题，本人期待将会有和现有的系统类似性能的虚拟化软件。