**CPK虚拟内核**

南湘浩 关志

**1引言**

虚拟软件网是从软件发行者到软件使用者的虚拟链接而成的网。在这个虚拟网中，CPK系统为发行者提供所需真实性证明，这些证明可以作为安全内核用。安全内核的概念是由计算机提出来的。计算机操作系统都有安全内核，在安全内核中设置了很多控制表，规定允许的操作和不允许的操作，以此保证计算机运行的安全。这种安全是基于行为的信任理论基础上的，是从计算机运行管理层面上的安全。关于行为学的研究，我国也有很深的造诣，集中体现在屈延文等人撰写的“银行行为监管和监管信息化”一书中。基于行为的信任理论，虽然具有重要的社会学意义，但是对操作系统安全内核来说，只能作为访问控制表的参考值，远没有满足计算机运行安全的真正需求，没有起到真正安全内核的作用。1990年代末又出现了新的情况，为了打破计算机操作系统的垄断，各国（包括中国、日本、台湾、苏联）相继提出并开发自己的操作系统，于是5个超级计算机操作系统厂家发起的联盟提出了“信托计算”（trusted computing)的概念，意思是把信任根都信托于你，不要再搞自己的操作系统了。这一着很管用，确实达到了预期的目的。尽管是被迫，但毕竟向自主可控概念的形成迈进了一大步，这是值得肯定的。于是各国掀起了信托计算的研究热潮。现在信托计算由简单对比MAC码的基础上，又增加了对MAC的签名，称代码签名。代码签名大大改善了信托计算，可作为操作系统安全内核的组成部分。

现在的软件世界可以说是三无世界，这就是恶意软件随意泛滥的主要原因。如果每一软件代码都有合法的商标，就能有序管理软件世界。软件的商标可以起到操作系统内核的作用，因此可构成双核操作系统，原有内核仍然控制软件运行安全，外加的CPK虚拟内核可控制软件的真伪。

**2虚拟化内核**

软件的商标可由发行者对软件名和对软加体的签名实现。因此商标化的软件可以起到管理的作用，可称虚拟内核。信托计算虽然增加了代码签名，起到了部分安全内核的作用，但还没有达到真正安全内核的水平，因为信托计算仍属于“事后证明”体制，在软件加载之后，可以做到执行之前的鉴别，但不能做软件加载之前进行可否加载的判别。

虚拟在英文中的意思很清楚，但在中文中容易与“虚设”，“虚无”搞混。按着虚拟的定义，虚拟是“不是A，但真正起A的作用的，称虚拟”。如虚拟专网VPN，它不是专用网，但起真正的专网作用。CPK不是安全内核，但是能起到真正安全内核的作用，因此称虚拟安全内核。

CPK 卡用芯片实现,内容包括CPK组合公钥体制和鉴别协议。鉴别协议执行真值逻辑，判别结果只是yes或no，没有二义性。真值逻辑将操作系统软件的真实性证明，分软件的下载、安装。启动三个独立过程进行。

**3软件下载和加载控制**

软件发行中的软件下载控制和软件调用中的软件加载，根据软件发行者的真实性和软件名的真实性来决定下载（加载）与否。其中，软件发行者的的真实性证据是发行者（issuer）对时间的签名，证明者被时间所验证，称标识签名：

SIG*issuer*(time)=(*s*1,*c*1)

VER*ISSUER*(*s*1,time)=*c*1’

软件名真实性证据是软件发行者对软件名（name）的签名，软件名被发行者所证明，称数据签名：

SIG*issuer*(name)=(*s*2,*c*2)

VER*ISSUER*(*s*1,name)=*c*2’

其中，*issuer*（小写）是发行者的私钥，*ISSUER*（大写）是发行者的公钥。

发行者可以分为三种：一是厂家，二是集团客户，三是个人。由厂家发行的软件由厂家负责签名，集团客户的专用软件由发行的软件的集团签名，个人用户对自己选定的的软件签名。

**4软件安装和执行控制**

软件发行中的安装控制和软件调用中的执行控制，由软件体（data）的真实性来决定安装（执行）与否。

软件体真实性证明是发行者对软件数据的签名与验证。软件数据可由数据的特征码代表，如压缩码mac或抽样码sam：

SIG*issuer*(mac)=(*s*3,*c*3,)

VER*ISSUER*(*s*3,mac)=*c*3’

**小结**

在虚拟化的安全内核和传统的安全内核之间，存在很多概念的不同：虚拟安全内核以可证系统替代了可信系统；在安全策略中以自主可控取代了强制控制；在鉴别逻辑中以真值逻辑替代了信任逻辑；在鉴别对象中以我方识别取代了对方识别；等等。

虚拟内核，对内可起到安全内核的作用，一原安全内核构成双安全内核；对外，对所有软件实行商标话管理。在代码运行中或在网络中，取证很方便的，由此可净化吵杂的计算环境和网络环境。可见，由此可启开了在网际安全时代，即自主可控的虚拟内核新时代。