论文选自《第二十次全国计算机安全学术交流会论文集》

可信计算与系统安全芯片

总参谋部第五十一研究所　王新成

一、可信计算及其发展

可信计算的研究从Anderson首次提出可信系统（Trusted System）到TCG的可信计算（Trusted Computing）已有30余年的历史，其研究重点也从早期的容错计算，故障检测和冗余备份技术发展到今天的可信硬件平台、可信软件系统、可信网络接入。随着全球信息化时代的到来，网格计算与WEB服务等分布式计算将成为未来的主流计算模式，同时，无线网络的迅速发展与广泛应用使得其必将成为今后的主流网络形式。因此，未来的可信计算研究将面向在分布式与无线网络环境下的安全与可信。

按照ISO/IEC 15408标准，所谓可信计算是：参与计算的组件，操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰。根据此定义，可信计算将成为无限可信的概念。事实上完全的、绝对的可信是不可能实现的，也是没有必要的。因此，计算中的可信标准，可信等级，可信区间及可信度的定义将成为可信计算工程实现的关键内容。

在TCG的可信计算平台标准实施规范中，可信计算包括以下三个属性与功能：

(1)确保用户身份的惟一性,用户工作空间的完整性与私有性；

(2)确保硬件环境配置、OS内核、服务及应用程序的完整性；

(3)确保存储、处理、传输的信息的机密性/完整性。

微软的可信计算（Trustworthy Computing）白皮书，从目标、策略、手段和实施四个层面对可信计算进行了概要性的阐述，其目标与TCG的功能定义一致，包括安全性、私密性、可靠性与完整性。同时，微软对可信计算策略的定义则包含了以下原则：

(1)安全开发原则 在可信计算产品开发的每个阶段（设计，仿真，调试，发布与维护）确保数据与系统的私密性，可靠性与完整性；

(2)信息平等原则 未经授权，不得收集或共享他人信息；

(3)可用性原则 在任何情况下系统都能立即响应用户的需求；

(4)可管理性原则 系统要易于安装与管理,同时在设计时须考虑到扩展性，效率与性价比；

(5)准确性原则 系统应能正确执行其功能,保证计算结果无差错，数据无丢失和损坏；

(6)实用性原则 系统易于使用，便于维护；

(7)责任追究原则 对系统出现的问题建立责任追究制度，并采取措施来解决，且为用户提供计算、安装和操作帮助；

(8)透明性原则 在与用户交互过程中应使其正确了解系统采取各项措施的目的。

二、可信计算终端平台

1、终端平台可信安全的重要性

提起信息系统安全问题，人们往往会想到防火墙、入侵检测和防病毒等。而面对不断发生的恶意攻击和病毒，人们只能把防火墙、入侵检测、病毒防范做得越来越复杂，但随着维护与管理复杂度的提高，使得整个信息系统变得更加复杂和难以实施，也使得信息系统的使用效率大大降低。如果从服务器、网络、终端三个组成信息系统层面上来看，现有的保护手段是逐层递减的，这说明人们往往把过多的注意力放在对服务器和网络的保护上，而忽略了对终端的保护，这显然是不合理的。主要原因有三：

（1）终端往往是创建和存放重要数据的源头；

（2）绝大多数的攻击事件都是从终端发起的；

（3）数据泄密和蠕虫病毒感染都由终端脆弱性引起。

这三个方面恰恰说明人们对信息安全问题仍然存在着一个大盲区。究其根源，都是终端保护不足所引起的。如果我们在信息安全建设中，能够将不安全因素从终端源头进行控制，使得系统中每一个使用者都是经过认证和授权的，其操作也都是符合规定的，那么再配合其他安全设施，就不会产生攻击性的事故，从而能够更加完善的保证整个信息系统的安全。由此不

难得出，从终端安全入手才能更好地解决整个信息系统的安全问题。

2、可信计算系统平台体系结构

可信计算系统平台是在通用计算系统平台基础上构架一种全新的安全体系结构而形成的（如图1所示），并围绕该安全体系结构形成计算机系统的安全解决方案。

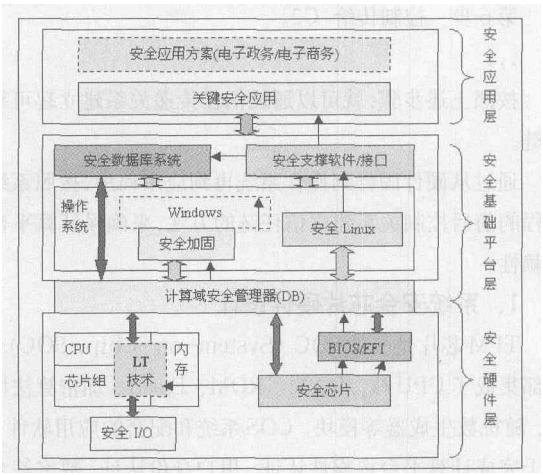

图1 可信计算系统平台安全体系结构

由图1可以看出，可信计算系统平台体系结构由三大部分构成;安全硬件层、安全基础平台层和安全应用层。也就是说，可信计算系统平台涵盖了基础硬件、基础软件平台以及各种丰富的安全应用。

从可信计算平台安全体系结构的模块构成来看，安全硬件层主要由安全芯片(TPM)、可信赖BIOS、LT技术模块和安全I/O构成;安全基础平台层主要包括计算域安全管理器、Windows安全加固、安全Linux、安全支撑软件与接口、安全数据库系统;安全应用层则包括关键安全应用。通过各层次安全模块的相互支撑构建统一的可信计算系统平台安全体系结构，其中LT是Intel在CPU/芯片组设置的安全模块，通过接口开放，建立与安全芯片、计算域安全管理器的支撑关系。

可信计算系统平台体系结构的安全功能主要体现在以下三条安全功能主线上：

第一条安全功能主线：在安全芯片(TPM)支撑下，由LT、计算域安全管理器和OS安全机制建立安全可信计算域，其中LT是一种CPU/芯片组/内存之间设置的安全技术，实现目标程序进程的物理计算空间的安全性(安全隔离)，OS安全机制实现目标程序进程的逻辑计算空间的安全性，而计算域安全管理器(DM)是程序进程的逻辑计算空间和物理计算空间之间安全转换的管理程序。

通过安全可信计算域，可以使每一个安全应用程序进程能在一个安全私有的空间中进行计算，可以非常有效地防止现今各种恶意代码(病毒、蠕虫、木马、间谍程序)和缓冲区溢出攻击，以确保应用程序运行过程中的可信赖性和数据安全性。

第二条安全功能主线：主板建有唯一一个CRTM(Core Root of Trust Measurement)，除厂商外，任何主体无法更改CRTM。系统每次启动时，以CRTM为起点(或称核心根)，由JY_TPM支撑建立系统平台的信任链，即在TPM的支持下，由CRTM度量BIOS/EFI(Extended Firmware Interface)的完整性，并将度量结果存放于TPM中，若度量结果经比较是可信赖的，则由BIOS/EFI度量OS Loader的完整性，之后由OS Loader度量OS Kernel的完整性，再由OS Kernel度量本地应用程序或远程应用程序的完整性，从而建立一条信任链。通过信任链确保计算平台和应用程序的可信赖性。

建立信任链过程中所有度量将构成系统平台的度量，这些度量将构成平台可信赖性判断依据，也是建立平台之间的可信网络连接(TNC--Trusted Network Connecting)的重要依据。

第三条安全功能主线：TPM作为硬件密码模块，通过TPM软件中间件，向系统平台和应用程序提供可信赖的密码学服务。其中，密钥管理、数据安全封装/解封装和数字签名运算具有高安全性，是未来开展电子政务的基础保障。

三、安全主板与可信计算域设计

安全主板设计主要体现TBB(可信赖性构件模块)的建立与实现，以及平台与用户可信赖关系的绑定上，如图2所示。

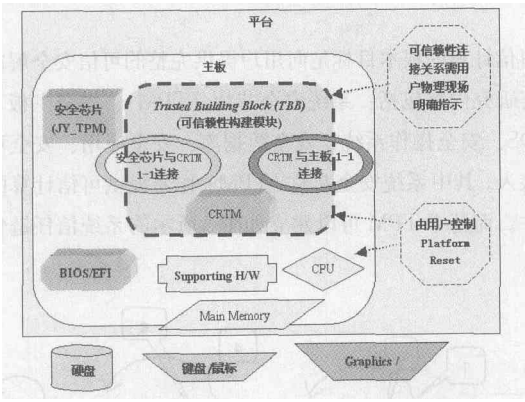

图2 安全主板

主板的可信赖性构建基础模块(TBB)是由建立信赖性(提供完整性度量)和提供CRTM、安全芯片(TPM)、主板、Platform Reset以及物理现场信号(physical presence signal)的软硬件组成。

TBB应能提供下列安全功能：

(1) 确保CRTM Code是平台重启(platform reset)时第一个执行的代码；

(2) 确保一旦安全芯片重启，TBB也重启，反之亦然；

(3) 如果发现安全芯片连接错误，仍然能够保持安全状态；

(4) 提供检测对安全芯片连接的物理攻击手段；

(5) 提供一个信任度量根(CTRM)，由CTRM度量确定的平台特征。

计算域安全管理器是位于操作系统与硬件层之间运行的软件模块，计算域安全管理器在LT模块的功能支撑下，为操作系统和应用程序提供运行环境安全隔离服务，以控制应用程序通过驱动程序直接获取另一应用程序的资源访问权限。

计算域安全管理器可以在操作系统启动之后另行启动，在启动过程中需先清理域管理器驻留的内存区域，并校验自身的完整性，只有当完整性未被破坏时才能启动工作。计算域安全管理器的完整性度量数据存储于安全芯片的平台寄存器中。系统休眠时，域管理器对所有受保护的内存区域的数据进行加密后再退出，系统恢复时，则对加密后的内存数据进行解密。处于受保护模式下的应用程序之间通过域管理程序来传递数据。

计算域安全管理器模块的功能实现依赖硬件层的LT技术支撑，而LT模块是集合了CPU和芯片组的功能模块，利用安全芯片提供的安全服务来实现安全的硬件运算环境。LT将是未来CPU/芯片组的主流技术。

四、可信系统安全芯片设计

可信计算的根本目标是向用户提供完整的可信安全解决方案，其研究内容包括：系统安全芯片（TPM）、安全主板、安全BIOS、安全操作系统、安全数据库、安全应用、安全可信网络接入，其中系统安全芯片（TPM）作为提供可信计算的核心部件。而基于TPM可以建立如图3所示的系统信任链传递方法。

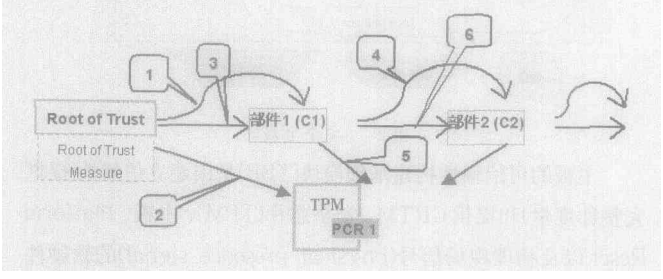

图3 信任传递原理

首先，在计算系统平台的主板CRTM(固件启始运行模块，软件攻击者无法修改)中设置一个信任的源头(Root of Trust)，然后按如下方法建立信任传递：

第1步 RTM(信任度量根) 度量部件1；

第2步 RTM 把度量值提供给JY_TPM芯片中PCR(平台配置寄存器)；

第3步 控制传给C1；

第4步 C1 度量部件2；

第5步 C1 把度量值提供给PCR；

第6步 控制传给 C2。

...

按照上述步骤，就可以通过信任传递关系建立起可靠的信任链。

通过从硬件固件到操作系统再到应用程序，按照系统启动过程的前后控制关系建立信任链的方法，来确保计算平台的可信赖性。

1、系统安全芯片硬件设计

TPM芯片是一款SOC（System-on-Chip，SOC）芯片，内部集成了CPU核、RAM、ROM、Flash、加密算法协处理器、随机数生成器等模块。COS系统和配套的应用软件，主要用于完成计算平台可靠性认证、用户身份认证、数字签名等功能。其硬件结构描述如图4所示。

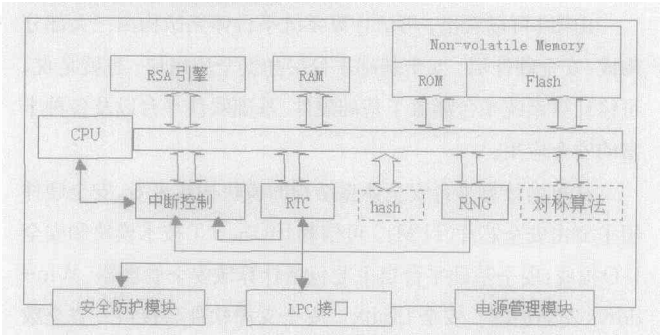

图 4 TPM芯片硬件总体结构图

HASH（散列算法模块）：硬件实现散列算法、SHA-1、及散列消息鉴别码HMAC。

RSA（非对称密码协处理器模块）：协处理器作为硬件算法加速器，主要完成模幂、模乘、模加运算。协处理器以改进的蒙格马利算法为基础，以位加法器和位乘法器为核心，通过使用总线仲裁、总线冻结及流水线等设计手段和设计技术完成算法的硬件加速功能。

RNG（随机数产生模块）：随机数产生器，快速生成各种安全运算所需的随机数。

安全防护模块：采用电流平衡分布设计技术防止能量攻击，采用硬件访问控制技术和存储加密技术来保护片上敏感信息。

LPC接口模块:LPC总线接口模块，符合Low pin count总线协议，是TPM芯片与外部交换数据的窗口。

中断控制模块：中断控制器IP软核。

CPU：32位RISC CPU硬核。

RAM：主要用作核心软件模块的运行和高速结果暂存。

Flash：用于COS系统静态存储，升级及保存密钥 、证书及标志。

时钟管理模块：按照ACPI协议的电源管理要求，实现动态时钟管理，当总线和总线上的模块在不选中的时候，以及安全芯片在一段时间内没有使用时，将时钟频率降低，以降低功耗。

2、TPM-COS与文件系统设计

TPM COS通过下列模块共同完成系统功能：初始化模块、精简的OS、对外提供命令接口以及自身安全防护。初始化模块负责内核的引导和加载。精简的OS模块是基于嵌入式OS原型开发的微型OS，包含以下几个模块：内存管理——负责为提交的任务动态分配内存以及回收内存碎片；任务调度模块——提供最简单的任务状态的切换；核心内核——负责各个子模块之间的调度；文件系统模块——负责Flash文件系统的维护，并提供掉电保护。最后还需要在内核中提供调试接口，对外命令接口负责向上层TSS提供标准TPM命令。自身安全保护模块使用加密和压缩机制使得内核在静态情况下，外界无法得到内核的二进制代码。此外，由于TPM主规范已经提供了完善的安全机制保护外界不可信的TSS提交的非法指令，因此自身的保护部分不涉及指令的保护。

其中的初始化部分包括的初始化自检和系统加载模块一般由CPU内核厂家提供。命令处理模块需要COS核心模块的支持，由于其主要功能是实现75个TPM主规范的命令，而安全保护模块提供对整个COS核心的保护，其功能架构如图5。

图5 TPM-COS功能架构

3、文件系统的组织结构

文件系统是TPM-COS的核心。TPM-COS根据层次化的文件系统进行设计，具体的层次结构如图6所示。

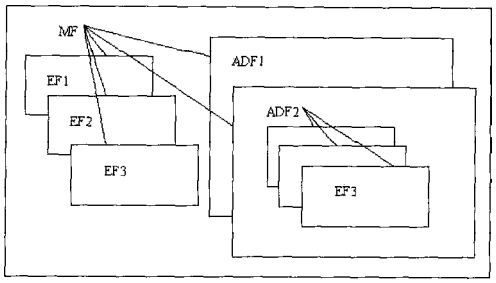

图6 文件系统的层次结构

(1)TPM主控文件(Master File，MF)

主控文件是整个TPM芯片文件系统的根（可看作根目录），每个TPM芯片有且只有一个主控文件。它是在芯片的个性化过程中首先被建立起来的，在芯片的整个生命周期内一直存在并保持有效，可存储芯片的公共数据信息并为各种应用服务。由个性化建立起来的主控文件包括文件控制参数以及文件安全属性等信息。在物理上，主控文件占有的存储空间包括MF文件头的大小以及MF所管理的EF和DF的存储空间。

(2)TPM专用文件(Dedicated File,DF)

在MF下针对不同的应用建立起来的一种文件，是位于MF之下的含有EF的一种文件结构（可看作文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据。

DF由创立文件命令建立。对DF的建立操作由MF下建立文件的安全属性控制。在DF下面不可再建立子DF，只能建立EF。为了保证各个DF的相互独立，只能从文件系统的MF层次选择一个DF，对DF下的数据进行的操作由各当前系统的状态机控制。

(3)TPM 基本文件(Elementary File,EF)

基本文件存储了各种应用的数据和管理信息，它存在于MF和DF下。EF从存储内容上分为两类：安全基本文件和工作基本文件。

安全基本文件(Secret Elementary File,SEF)的内容包含用于用户识别和与加密有关的保密数据(个人识别码、密钥等)，芯片将利用这些数据进行安全管理。SEF要在MF或DF建立后才能建立。建立后每个KEY都可以定义不同的修改权限。安全基本文件的内容不可被读出，但可使用专门的指令来写入和修改。在MF和每个DF下只能建立1个安全基本文件，但每个文件中的KEY和PIN的类型由用户指定。

工作基本文件(Working Elementary File，WEF)包含了应用的实际数据，其内容不被芯片解释。在符合WEF的读、修改安全属性时，可对其内容进行读取、修改。工作文件的个数和大小受到MF或DF所拥有空间的限制。

整个文件系统的空间在MF、DF和EF建立时被分配和确定，以后在物理上不会发生变化。当访问EF时，必须先选择

相应的MF或DF。可以从文件系统的任何位置选择MF。

（4）文件系统状态机

TPM状态机又称TPM安全状态，是指TPM芯片在当前所处的一种安全级别。TPM芯片的主控目录和当前应用目录分别具有多种不同的安全状态。用TPM芯片内一个寄存器存储主控目录的安全状态，即整个TPM芯片所处的安全级别。主控目录的安全状态复位后为0，应用目录的改变不改变主控目录的安全状态。只有主控目录下的口令核对或外部认证才能改变主控目录的安全状态。

（5）安全属性和状态机的关系

安全属性是指对某个文件进行某种操作时必须达到的状态机，又称其为访问权限。某个文件的访问权限是在建立该文件时指定的。TPM-COS的访问权限具有其独特性，是用一个状态机区间来描述一种权限的。如描述一个文件的读权限为AB，则其访问权限为：当前的状态机M必须满足A≤M≤B。

因此，若要定义一种永远不能获得的权限，则定义该权限为AB（B>A)。如果要定义一种可自动获得的权限，则定义该权限为 A=0，原因是复位后的主控文件和成功选择后的应用的安全状态都为0。0是一种自动获得的状态机。

（6）状态机跳变机制

TPM-COS通过核对口令和外部认证两种方法来实现状态机的转变。核对口令只在DF下有效。特别指出的是状态机不存在级别高低，同样的操作可定义为任意的状态机，即可以用一种改变状态机的手段来实现从任一种状态机到另外任一种状态机的转变。

五、可信计算目前存在的几个问题

1、TPM与CPU

可信平台模块把PKI、数字证书和安全协处理器纳入每台PC。按照微软设想，可信计算将使网络链路的每一端清楚另一端的配置情况，从而终结病毒、垃圾邮件及网络入侵。可信计算机的核心就是可信平台模块（TPM)。CPU生产的两大巨头Intel和AMD及竞争对手计划把该密码协处理器纳入每台PC。目前TPM是独立的系统安全芯片，基于可信计算组织（TCG）制订的规范，从技术的角度很容易与CPU融为一体。一旦出现这种所谓的“安全CPU”，和基于“安全CPU”之上的“安全操作系统”，我们的计算环境与计算终端将如何保证可信与安全。

2、TPM与BIOS

在TCG规范中把BIOS FLASH 与TMP芯片两个模块分别挂在CPU芯片组南桥的LPC总线上，在系统启动的过程中，由TPM模块来完成对FLASH 中BIOS的各模块进行完整性验证和各种密码与安全运算，进而控制可信安全终端从启动到运行的全过程。在这种安全机制中，TPM模块本身并不能防止FLASH中的BIOS被窜改，只能被动的对可能的攻击行为进行应付。如果把BIOS FLASH 与TMP模块集成在同一个芯片BIOS-TPM上，则可以利用芯片本身的各种防护措施主动防止对BIOS的各种攻击，同时又可以完成TPM模块在可信安全终端后续运行过程中的安全认证与机密信息加密功能。因此目前TCG中TPM模块与BIOS FLASH的分离设置，并不利于可信平台的安全。同时这也将使得以后TPM与可信主板需要重新设计。

3、可信计算的有效管理

如果说基于TPM上的安全技术是可信计算的“根”，那么有效管理就是其“本”。所有的安全技术，包括安全模型、安全策略、密码算法和协议都与信任相关，都有预先假定的信任前提。因此如何在网络环境中建立有效的信任关系，如何对这种信任关系进行有效的管理，就成为目前亟待解决的关键与基础问题。

4、可信计算标准

我国的无线局域网安全标准WAPI 在遭到联合绞杀而被判“无期”成为一种“不能忘却的纪念”。WAPI没有成功，很多人将其归咎于标准过于封闭，以“闭门造车”的心态去制定标准，自然遭到国际厂商的“联合封杀”。但这似乎不是真正的原因，我国可信计算标准会重蹈WAPI的覆辙吗？我国的可信计算标准能否“浮出水面”，将再一次验证我国信息安全产业相关政策的权威及国际地位，关系到我国可信计算技术与产品的前途与命运。

Check Point 安全解决方案荣获Windows IT Pro“2005年度读者之选”大奖

日前，Check Point软件技术有限公司宣布，它的两项解决方案在Windows IT Pro杂志最近举办的2005年度读者评选中夺魁，Check Point VPN-1®Pro™被评为“最佳服务器/单独使用防火墙”，而ZoneAlarm®Pro则被评为“最佳桌面电脑防火墙”。这项评奖的结果详情在9月出版的Windows IT Pro杂志中刊出。

Check Point VPN-1 Pro是一个整合防火墙及VPN网关的方案，能为企业应用及网络资源提供全面的安全保护及远程连接。ZoneAlarm Pro是互联网安全产品中最值得信赖的品牌之一，它保护数以百万计的个人电脑抵御黑客、间谍软件及数据盗窃的威胁。

Windows IT Pro杂志的读者中有超过1700人参与了评选，他们在12项技术类别中的750项产品和服务中投票选出最佳的解决方案。