# 可信计算

# 可信网络

可信计算/可信用计算（Trusted Computing，TC）是一项由可信计算组（Trusted Computing Group)，前称为TCPA）推动和开发的技术。这个术语来源于可信系统（Trusted system），并且有其特定含义。从技术角度来讲，“可信的”（Trusted）未必意味着对用户而言是“值得信赖的”（Trustworthy）。确切而言，它意味着可以充分相信其行为会更全面地遵循设计，而执行设计者和软件编写者所禁止的行为的概率很低。

这项技术的拥护者称它将会使计算机更加安全、更加不易被病毒和恶意软件侵害，因此从最终用户角度来看也更加可靠。此外，他们还宣称可信计算将会使计算机和服务器提供比现有更强的计算机安全性。而反对者认为可信计算背后的那些公司并不那么值得信任，这项技术给系统和软件设计者过多的权利和控制。他们还认为可信计算会潜在地迫使用户的在线交互过程失去匿名性，并强制推行一些不必要的技术。最后，它还被看作版权和版权保护的未来版本，这对于公司和其他市场的用户非常重要，同时这也引发了批评，引发了对不当审查（censorship）关注。

- 很多著名的安全专家已经表明了对可信计算技术的反对，因为他们相信它将给计算机制造商和软件作者更多限制用户使用自己的计算机的能力。有一些人关注的则是可信计算可能（或者本身就是要）起到限制自由软件市场、私有软件开发和更一般化的整个IT市场竞争的作用。有些人，如理查德·斯托曼，因此给它起了一个恶名——背叛的计算（Treacherous computing）。

- 不管这场争论以及可信计算最终产品的形式怎样，在计算机领域拥有重大影响的公司，如芯片制造商Intel、AMD和系统软件开发商Microsoft，都计划在下一代的产品中引入可信计算技术，如Windows Vista。

# 可信计算主要概念

可信计算包括5个关键技术概念，他们是完整可信系统所必须的，这个系统将遵从TCG（Trusted Computing Group可信计算组织）规范。

## 1.Endorsement key 签注密钥

**签注密钥是一个2048位的RSA公共和私有密钥对，它在芯片出厂时随机生成并且不能改变。这个私有密钥永远在芯片里，而公共密钥是用来认证及加密发送到该芯片的敏感数据。**

## 2.Secure input and output 安全输入输出

安全输入输出是指电脑用户和他们认为与之交互的软件间受保护的路径。当前，电脑系统上恶意软件有许多方式来拦截用户和软件进程间传送的数据。例如键盘监听和截屏。

## 3.Memory curtaining 储存器屏蔽

储存器屏蔽拓展了一般的储存保护技术，提供了完全独立的储存区域。例如，包含密钥的位置。即使操作系统自身也没有被屏蔽储存的完全访问权限，所以入侵者即便控制了操作系统，信息也是安全的。

## 4.Sealed storage 密封储存

密封存储通过把私有信息和使用的软硬件平台配置信息捆绑在一起来保护私有信息。意味着该数据只能在相同的软硬件组合环境下读取。例如，某个用户在他们的电脑上保存一首歌曲，而他们的电脑没有播放这首歌的许可证，他们就不能播放这首歌。

## 5.Remote attestation 远程认证

远程认证准许用户电脑上的改变被授权方感知。例如，软件公司可以避免用户干扰他们的软件以规避技术保护措施。它通过让硬件生成当前软件的证明书。随后电脑将这个证明书传送给远程被授权方来显示该软件公司的软件尚未被干扰（尝试破解）。

信息安全具有四个侧面：设备安全、数据安全、内容安全与行为安全。

可信计算为行为安全而生。据中国信息安全专家在《软件行为学》一书中描述，行为安全应该包括：行为的机密性、行为的完整性、行为的真实性等特征。

从概念上来说，可信计算（**Trusted Computing，TC**）并非由可信计算组织**Trusted Computing Group**（以前称为**TCPA**可信计算平台联盟）率先提出。可信这个概念早在彩虹系列的橘皮书就已经有提及，他的目标就是提出一种能够超越预设安全规则，执行特殊行为的运行实体。操作系统中将这个实体运行的环境称为可信计算基（**Trusted Computing Base，简称TCB**）。

为了实现这个目标，人们从**20**世纪**70**年代之后就在做着不懈的努力。包括从应用程序层面，从操作系统层面，从硬件层面来提出的**TCB**相当多。最为实用的是以硬件平台为基础的可信计算平台（**Trustec Computing Platform**），它包括安全协处理器、密码加速器、个人令牌、软件狗、可信平台模块（**Trusted Platform Modules，TPM**）以及增强型**CPU**、安全设备和多功能设备。

这些实例的目标是实现：数据的真实性、数据的机密性、数据保护以及代码的真实性、代码的机密性和代码的保护。

从广义的角度，可信计算平台为网络用户提供了一个更为宽广的安全环境，它从安全体系的角度来描述安全问题，确保用户的安全执行环境，突破被动防御打补丁方式。

# 可信计算的应用

## 1.数字版权管理

可信计算将使公司创建很难规避的数字版权管理系统，但也不是不可能（破解）。例子是下载的音乐文件，用远程认证可使音乐文件拒绝被播放，除非是在执行着唱片公司规则的特定音乐播放器上。密封储存防止用户使用其他的播放器或在另一台电脑上打开该文件。音乐在屏蔽储存里播放，这将阻止用户在播放该音乐文件时进行该文件的无限制复制。安全I/O阻止用户捕获发送到音响系统里的（流）。规避（破解）这样的系统需要操纵电脑硬件或者是用录音设备或麦克风获取模拟信号（这样可能产生信号衰减）或者破解加密算法。

## 2.身份盗用保护

可信计算可以用来帮助防止身份盗用。以网上银行为例，当用户接入到银行服务器时使用远程认证，之后如果服务器能产生正确的认证证书那么银行服务器就将只对该页面进行服务。随后用户通过该页面发送他的加密账号和PIN和一些对用户和银行都为私有的（不看见）保证信息。

## 3.防止在线游戏作弊

可信计算可以用来打击在线游戏作弊。一些玩家修改他们的游戏副本以在游戏中获得不公平的优势；远程认证，安全I/O以及储存器屏蔽用来核对所有接入游戏服务器的玩家（以确保）其正运行一个未修改的软件副本。尤其是设计用来增强玩家能力属性或自动执行某种任务的游戏修改器。例如，用户可能想要在射击游戏中安装一个自动瞄准BOT，在战略游戏中安装收获机器人。由于游戏服务器无法确定这些命令是由人还是程序发出的，推荐解决方案是验证玩家电脑上正在运行的代码。

## 4.保护系统不受病毒和间谍软件危害

软件的数字签名将使得用户识别出经过第三方修改可能加入间谍软件的应用程序。例如，一个网站提供一个修改过的流行即时通讯程序版本，该程序包含间谍软件。操作系统可以发现这些版本里缺失有效的签名并通知用户该程序已经被修改，然而这也带来一个问题：谁来决定签名是否有效。

## 5.保护生物识别身份验证数据

用于身份认证的生物鉴别设备可以使用可信计算技术（存储器屏蔽，安全I/O）来确保没有间谍软件安装在电脑上窃取敏感的生物识别信息。

# 可信网络简介

可信网络架构不是一个具体的安全产品或一套针对性的安全解决体系，而是一个有机的网络安全全方位的架构体系化解决方案，强调实现各厂商的安全产品横向关联和纵向管理。因此在实施可信网络过程中，必将涉及多个安全厂商的不同安全产品与体系。这需得到国家政府和各安全厂商的支持与协作。

鉴于可信计算技术的重要性，国际上一些著名的大学和公司，如卡内基梅隆大学、**AT&T**、微软公司等也在积极开展这方面的研究，并取得了一系列成果。随着研究日渐深入，可信网络开始走上台前。

当前，可信计算方兴未艾，可信网络呼之欲出。各企事业单位在信息化的过程中，根据各自面临的安全问题与应用需求，并根据针对性的安全性问题，逐步构建了基于信任管理、身份管理、脆弱性管理以及威胁管理等相应的安全管理子系统。但是这些针对性的安全产品和安全解决方案缺乏相互之间的协作和沟通，无法实现网络安全的整体防御。

因此，网络安全领域的发展已进入了综合安全系统建设的阶段。安全企业将面临用户从以往的安全系统建设转化为安全运行维护的新需求：如何发挥已有安全产品的整体效能；如何保 护已有的投资，避免重复投入与建设以节省资源；如何建立各安全子系统、各安全产品之间的关联，提高网络整体的安全防御能力成了网络安全发展的必然趋势。这些问题正受到企业的密切关注。

可信网络的推出旨在实现用户网络安全资源的有效整合、管理与监管，实现用户网络的可信扩展以及完善的信息安全保护；解决用户的现实需求，达到有效提升用户网络安全防御能力的目的。

## *可信网络特征：*

1、网络中的行为和行为中的结果总是可以预知与可控的；

2、网内的系统符合指定的安全策略，相对于安全策略是可信的、安全的；

3、随着端点系统的动态接入，具备动态扩展性。

## *架构网络安全模型*

可信网络架构的推出，可以有效地解决用户所面临的如下问题，如设备接入过程是否可信；设备的安全策略的执行过程是否可信；安全制度的执行过程是否可信；系统使用过程中操作人员的行为是否可信等。

可信网络的一般性架构主要包括可信安全管理系统、网关可信代理、网络可信代理和端点可信代理四部分组成，从而确保安全管理系统、安全产品、网络设备和端点用户等四个安全环节的安全性与可信性，最终通过对用户网络已有的安全资源的有效整合和管理，实现可信网络安全接入机制和可信网络的动态扩展；加强网内信息及信息系统的等级保护，防止用户敏感信息的泄漏。