编号：CNIS-2007AA01Z4929-01

可信网络连接架构研究报告

西安电子科技大学计算机网络与信息安全教育部重点实验室

2007.3

前言

可信网络连接架构研究报告包括以下几部分：

1. 可信计算的发展、概念与本质
2. 可信计算平台架构与基本特征
3. TCG-TNC 规范研究
4. 国内外其他可信接入标准
5. 可证安全的网络连接模型
6. 可信接入标准制定的工作设想

该报告为 GB/T ××××—××××的预演报告。

起草单位：西安电子科技大学计算机网络与信息安全教育部重点实验室

起草人：马建峰，马卓，李兴华，张志勇，吴振强，杨力，杨超，邱罡，曾勇

近二十年来伴随着信息技术的迅猛发展，涌现出大量面向各种通信网络环境的应用如E-commence, E-business, E-government, 移动计算，普适计算，网格计算，音频视频等电子数据的共享，以及企事业基于业务的 Intranet 构建等等，使得整个互联通信网络得到了空前的广泛应用。由此而产生的计算环境的安全问题也面临着严峻的考验，嗅探、窃听、身份冒充、分布式拒绝服务攻击等手段以及 Trojan horse，蠕虫病毒、恶意程序的入侵，致使敏感的数据信息被窃取、篡改和滥用，系统安全遭受到严重的威胁。传统的安全解决方案如防火墙、入侵检测、防病毒软件等在一定程度上减少了上述不安全隐患，但并未从根本上解决系统安全问题。如何构建新一代适应信息发展需求的可信计算平台体系及通信环境已经成为信息科学技术领域最重要的课题之一。可信计算（Trusted Computing[1，4，5], 或称为 Trustworthy Computing [11]）技术作为全新的安全解决方案在资源共享与交换[3，13]、Digital Rights Management[17，27]、无线移动网络[16，19，20]和 Peer-to-Peer 网络、普适计算[6，12，28]等方面近年来得到了研究者的广泛关注和研究。

本文将首先简要介绍可信计算的发展历程、概念及其本质**（第 1 节）**，从而给出 TCG 的可信计算平台架构与基本特征**（第 2 节）**，然后着重介绍 TCG 的可信网络加入标准**（第 3 节）**，以及国内外其他相关的可信接入标准**（第 4 节）**，最后提出我们将在制定可信接入标准中的工作设想**（第 5 节）**。

1. 可信计算的发展、概念与本质

1.1 可信计算的发展

可信计算技术的发展可以追溯到上世纪七十年代早期开始的容错计算研究。从1975年开始，商业化的容错机便推向市场。到九十年代，软件容错的问题被提了出来，进而发展到网络容错[24，25]。同一时期，安德逊首次提出了可信系统(Trusted System)的概念。较早期学者对可信系统研究主要集中在硬件设备和运行于其上的软件的安全和可靠性。此时的可信计算实际上是一种可靠计算（Dependable Computing）的概念，与容错计算(Fault- Tolerant Computing)领域的研究密切相关。此外，还有八十年代作为可信计算机安全评价标准的TCSEC标准及TCB（Trusted Computing Base）概念，它们存在着一些局限性：（1）主要强调了信息的秘密性,而对完整性、真实性考虑较少； （2）强调了系统安全性的评价,却没有给出达到这种安全性的系统结构和技术路。虽然目前已不再采用，但对构建计算机安全体系仍具有指导意义。

2000 年 12 月美国卡内基梅隆大学(CMU)与美国国家宇航总署(NASA)的艾姆斯(Ames)研究中心牵头，十几家大公司和著名大学成立了高可信计算联盟 TCPA。该组织致力于发展新一代安全、可信的硬件运算平台。2002 年 1 月比尔·盖茨提出可信计算(Trustworthy Computing)的概念，此后微软、英特尔(Intel)，IBM 等 190 家公司参加的可信计算平台联盟（TCPA）都在致力于数据安全的可信计算，包括研制密码芯片、特殊的 CPU,主板或操作系统安全内核。2003 年 4 月，由于原有目的的改变，TCPA 被重组为“可信计算组织”(Trusted Computing Group, TCG)。TCG 在原 TCPA 强调安全硬件平台构建的宗旨之外，更进一步增加了对软件安全性的关注，旨在从跨平台和操作环境的硬件组件和软件接口两方面，促进不依赖特定厂商的可信计算平台工作标准的制定[2]。

TCG 的任务是通过平台、软件和技术的协作，定义、开发、推广一套开放的、系统的可信计算规范，提供一整套可信计算安全技术，规范硬件构建模块和通用的软件接口，设计多平台、多外设的可信计算环境。TCG 规范包括 TPM 规范,TCG 体系结构规范、可信软件堆栈规范、可信网络连接规范、可信客户端规范、可信服务器规范等[8]。

1.2可信计算的概念及本质

信任是一个复杂的概念，当某一事物为了达到某种目的总是按照人们所期望的方式运转，那么它就是可信任的。在ISO/IEC15408标准中给出了以下定义：一个可信的组件、操作或过程的行为在任意操作条件下是可预测的，并能很好地抵抗应用程序软件、病毒以及一定的物理干扰造成的破坏。闵应骅在文献[23]中提出，计算机系统的可信性应包括：可用性、可靠性、安全性、健壮性、可测试性、可维护性等。因此，一个可信的计算机系统所提供的服务可以认证其为可依赖的。系统所提供的服务是用户可感知的一种行为，而用户则是能与之交互的另一个系统(人或者物理的系统)。此外，TCG对“可信”的定义是：“一个实体在实现给定目标时，若其行为总是如同预期，则该实体是可信的”（An entity can be trusted if it always behaves in the expected manner for the intended purpose)[8]。这个定义将可信计算和当前的安全技术分开：可信强调行为结果可预期，但并不等于行为是安全的，这是两个不同的概念。

目前在计算机系统中已经采用了多种基于软件的安全技术用于实现系统及数据的安全，如X.509 数字证书、SSL、IPSEC、VPN以及各种访问控制机制等。但是Internet的发展在使得计算机系统成为灵活、开放、动态的系统同时，也带来了计算机系统安全问题的增多和可信度的下降。

可信计算的本质主要是通过增强现有的终端体系结构的安全性来保证整个系统的安全。其主要思路是在各种终端（包含PC,手机以及其它移动智能终端等）硬件平台上引入可信架构，通过其提供的安全特性来提高终端系统的安全性。终端可信的核心是TPM (Trusted Platform Module)芯片。

以TPM为基础的“可信计算”由几个方面构成：用户的身份认证是对使用者的信任；平台完整性，体现了使用者对平台运行环境的信任；应用程序的完整性，体现了应用程序运行的可信；平台之间的可验证性，体现了网络环境中终端之间的相互信任。

2. 可信计算平台架构与基本特征

可信计算框架主要是通过增强现有的终端体系结构的安全性来保证整个系统的安全。其主要思路是在各种终端（包含PC,手机以及其它移动智能终端等）硬件平台上引入可信架构，通过其提供的安全特性来提高终端系统的安全性。终端可信的核心是称为可信平台模块TPM（Trusted Platform Module）的可信芯片。针对PC的可信平台参考架构如图1所示。

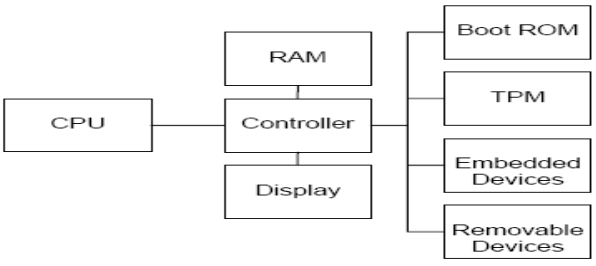


图1 PC可信计算平台参考架构

2.1 可信计算平台软件体系架构[8，9]

可信计算平台是以 TPM 芯片为核心，整个软件体系框架主要分为三层：低层 TPM 及其设备驱动、中间层可信软件堆栈 TSS（Trusted Software Stack）和上层提供本地应用的服务层。TSS 负责提供应用程序访问 TPM 的接口，同时进行对 TPM 的管理。其中核心服务层 TCS 提供一组标准平台服务的 API 接口。核心服务包括(1)上下文管理； (2)证书和密钥的管理；(3)度量事件管理； (4)参数块的产生等。在用户模式下的本地应用服务层中主要有服务提供层 TSP，它能够提供上下文管理和密码操作两种核心服务，可充分利用 TPM 芯片的功能。完整的 TCP 体系结构如图 2 所示。

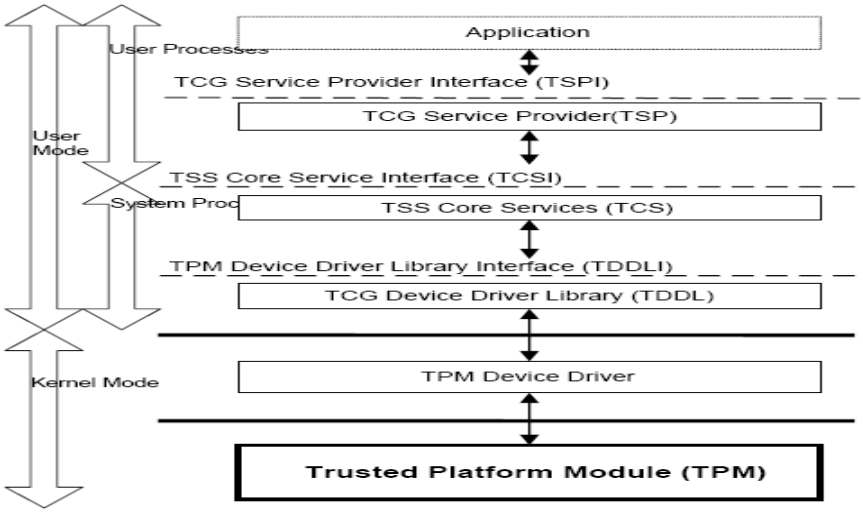


图 2 可信计算平台 TCP 软件体系架构

2.2 TCP 的基本特征

一个可信平台要达到可信的目标，最基本的原则就是必须真实报告系统的状态，同时决不暴露密钥和尽量不表露自己的身份阁。这就需要三个必要的基础特征：保护能力(Protected Capabilities)、证明（Attestation).完整性度量存储和报告（Integrity Measurement, Storage and Reporting)。

（1）保护能力

保护能力是唯一被许可访问保护区域（Shielded Locations）的一组命令，而保护区域是能够安全操作敏感数据的地方（比如内存，寄存器等)。TPM 通过实现保护能力和被保护区域来保护和报告完整性度量，平台配置寄存器 PCRs 位于 TPM 内部，仅仅用来装载对模块的度量值，大小为 160bits，对于 PC 平台共有 24 个 PCR。除此之外，。TPM 通过实现保护能力和被保护区域来保护和报告完整性度量. 这些功能使得系统的状态任何时候都处于可知，同时可以将系统的状态与数据绑定起来。由于 TPM 的物理防篡改性，这也就起到了保护系统敏感数据的功能。

（2）证明

证明是确认信息正确性的过程。通过这个过程，外部实体可以确认保护区域、保护能力和信任源，而本地调用则不需要证明。通过证明，可以完成网络通信中身份的认证，而且由于引入了 PCR 值，在身份认证的同时还鉴别了通讯对象的平台环境配置. 这大大提高了通信的安全性。

证明可以在不同层次进行：基于 TPM（by the TPM）的证明是一个提供 TPM 数据的校验的操作，这是通过使用 AIK，对 TPM 内部某个 PCR 值的数字签名来完成的，AIK 是通过唯一秘密私钥 EK 获得的，可以唯一地确认身份；针对平台（to the platform）的证明则是通过

使用平台相关的证书或这些证书的子集来提供证据，证明平台可以被信任并做出完整性度量报告；基于平台（of the platform）的证明通过在 TPM 中使用 AIK 对涉及平台环境状态的 PCR 值进行数字签名提供了平台完整性度量的证据。

（3）完整性的度量、存储和报告[26]

完整性的度量是一个过程，包括：获得一个关于平台的影响可信度的特征的值（Metrics），存储这些值，然后将这些值的摘要放入 PCRs 中。通过计算某个模块的摘要同期望值的比较，我们就可以维护这个模块的完整性。在 TCG 的体系中，所有模块（软件和硬件）都被纳入保护范围内，假如有任何模块被恶意感染，它的摘要值必然会发生改变，使我们可以知道它出现了问题，虽然还不能知道问题是什么。通过这种方式，就可以保护所有已经建立 PCR 保护的模块。

另外，平台 BIOS 及所有启动和操作系统模块的摘要值都将存入特定的 PCR,在进行网络通信时，可以通过对通行方 PCRs 值的校验确定对方系统是否可信（即是否感染了病毒、是否有木马、是否使用盗版软件等）。

度量必须有一个起点，这个起点必须是绝对可信的，它被叫做度量可信根 RTM（Root of Trust for Measurement）。一次度量叫做一个度量事件，每个度量事件由两类数据组成：(1)被度量的值：嵌入式数据或程序代码的特征值；　(2）度量摘要：这些值的散列。

完整性报告则是用来证明完整性存储的过程，展示保护区域中完整性度量值的存储，依靠可信平台的的鉴定能力证明存储值的正确性。TPM 本身并不知道什么是正确的值，它只是忠实地计算并把结果报告出来。这个值是否正确还需要执行度量的程序本身，通过度量存储日志 SML（Stored Measurement Log)来确定。此时的完整性报告使用 AIK 签名，以鉴别 PCR 的值。按照“可信”的定义，完整性度量、存储、报告的基本原则就是：许可平台进入任何可能状态（包括不期望的或不安全的），但是不允许平台提供虚假的状态。(也就是说必须忠实的度量)。

除了计算的散列值存在 PCR 里面，还需要存储期望值。SML 保存着有关系的被度量值的序列，每个序列公用一个通用摘要。这些被度量的值附加在通用摘要之后被再次散列，通常称之为摘要的扩展。扩展保证了不会忽视这些有关系的被度量值,同时可以保证操作的顺序。SML 可能会非常大，需要存在硬盘上，不过由于都是散列值，所以不需要 TPM 提供保护。

3 TCG-TNC 规范研究[10]

基于可信计算平台架构及可信任的根TPM芯片，终端系统里面建立可信链。此外，还能够通过保障终端的可信将信任链扩展到网络中去,即要构建可信的网络。在2004 年5 月, 可信计算组织TCG 成立了可信网络连接分组(TNC Sub Group, TNC-SG),主要负责研究及制定可信接入框架及相关的标准。

3.1 TNC 的研究背景及动机

随着信息化的发展，恶意软件(Malware,比如病毒、蠕虫等）的问题异常突出。现在已经出现了超过三万五千种的恶意软件，每年都有超过四千万的计算机被感染，而且这个数据还在逐年增大。

面对如此严峻的形势，传统的防御技术已经难有大的突破了，必须换一个角度来解决问题，不仅需要解决安全的传输和数据输入时的检查，还要从源头上，即从每一台连接到网络的终端开始，遏制住恶意攻击。

可信网络连接，本质上就是要从终端的完整性开始，建立安全的网络连接。首先，需要创建一套在可信网络内部系统运行状况的策略。然后只有遵守网络设定的策略的终端才能访问网络，网络将隔离和定位那些不遵守策略的设备。这些策略可以是：安装最新反病毒软件并正确的配置，经常运行全盘扫描，个人防火墙开启并正确配置，操作系统安装最新补丁，不运行未授权软件等。同时策略还可以禁止某些行为，如：端口扫描、发送垃圾邮件等等。

3.2 TNC 的研究目标

TNC 是基于完整性和认证性双重概念开发的。“完整性”是保证计算平台的安全启动和软硬件基本配置符合自定义的安全策略，是否被恶意软件所攻击或篡改，是否参与异常或恶意的行为等。“认证性”保证了系统通过认证只能被授权用户所使用。可信赖平台模块 TPM(Trusted Platform Module)基于 TCG 规范并安全储存密码、认证和数字密钥,平台用户可得到额外的安全性，因为能够将策略植入其中来判断平台的完整性和用户的认证性。TNC 构架的主要目的是通过提供一个由多种协议规范组成的框架来实现一套多元的网络标准，它提供如下功能:

（a）平台认证:用于验证网络访问请求者身份，以及平台的完整性状态。

（b）终端策略授权:为终端的状态建立一个可信级别，例如:确认应用程序的存在性、状态、升级情况，升级防病毒软件和 IDS 的规则库的版本，终端操作系统和应用程序的补丁级别等。从而使终端被给予一个可以登录网络的权限策略从而获得在一定权限控制下的网络访问权。

（c）访问策略:确认终端机器以及其用户的权限，并在其连接网络以前建立可信级别，平衡已存在的标准、产品及技术。

（d）评估、隔离及补救:确认不符合可信策略需求的终端机能被隔离在可信网络之外，如果可能执行适合的补救措施。

3.3 TNC 的基本架构及相关实体

TNC 的基本架构如图 3 所示，主要包括三个实体、三个层次和若干个接口组件等。该架构在传统的网络接入层次上增加了两层，可实现平台间的完整性验证，从而满足可信性、完整性和安全性。

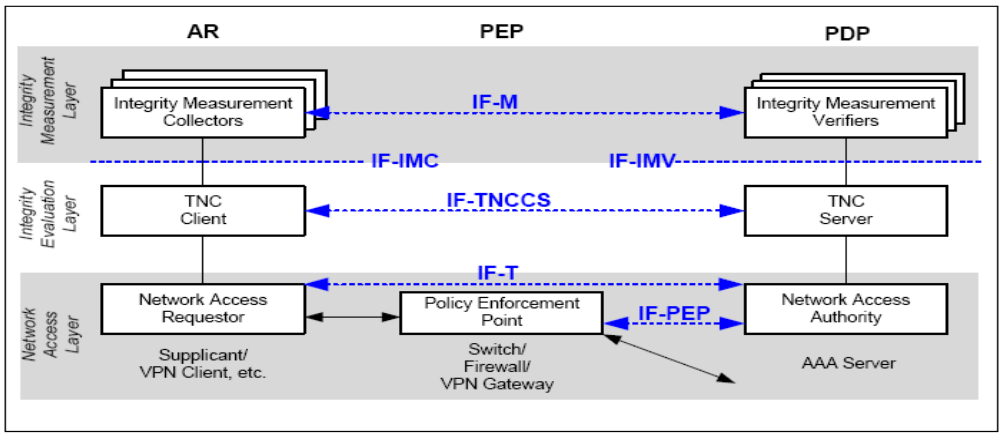


图 3 TNC 基本架构

（1）三类基本实体：

(a)请求访问者AR (the Access Requestor):功能为发出访问请求，收集平台完整性可信信息，发送给PDP，从而建立网络连接。该实体包括以下组件：网络访问请求者(NAR) 负责发出访问请求，建立网络连接。在一个AR上可以有几个不同的NAR，来建立同网络的不同连接；TNC客户(TNCC) 负责汇总来自IMC的完整性测量信息，同时测量和报告平台和IMC 自身的完整性信息；完整性测量收集器(IMC) 执行测量AR 的完整性属性。在一个AR 上可以有多个不同的IMC。

(b)策略执行者PEP (Policy Enforcement Point):该组件控制对被保护网络的访问。PEP 咨询PDP 来决定访问是否应该被执行。

(c)策略决策者 PDP (Policy Decision Point):功能为根据 TNCS 的推荐和本地安全策略对 AR 的访问请求进行决策判定，判定结果为允许/禁止/隔离。该实体包括以下三个组件：网络访问授权(NAA) 决定一个 AR 的访问请求是否被允许。NAA 可以咨询 TNCS 来决定 AR 的完整性状态是否同 NAA 的安全策略相一致，从而决定 AR 的访问请求是否被允许；TNC 服务器(TNCS) 负责控制 IMV 和 IMC 之间的信息流动，汇总来自 IMV 的访问决定，并形成一个全局的访问决定，传递给 NAA；完整性测量鉴别器(IMV) 负责对从 IMC 接收到的关于 AR 的完整性测量值进行鉴别，并做出访问决定。

（2）三个基本层次：

(a)网络访问层 (Network Access Layer)：这一层用于支持传统的网络连接技术，如802.1X,VPN,AAA Server 等机制。在这一层里面有三个实体：NAR、PEP 和 PDP。

(b)完整性评估层 (Integrity Evaluation Layer)：负责评估所有请求访问网络的实体的完整性。这一层和上层有两个重要的接口:IF-IMC(Integrity Measurement Collector Interface)和IF-IMV (Integrity Measurement Verifier Interface)。其中，IF-IMV是IMC同TNCC 之间的接口。该接口的主要功能是从IMC 收集完整性测量值，并支持IMC 同IMV 之间的信息流动；：IF-IMV是IMV和TNCS 之间的接口。该接口的主要功能是将从IMC 得到的完整性测量值传递给IMV，支持IMC 同IMV 之间的信息流动，将IMV 所做出的访问决定传递给TNCS。

(c)完整性度量层 (Integrity Measurement Layer)：收集和校验请求访问者的完整性相关信息的组件。

（3）其他重要的接口组件：

（a）IF-TNCCS 是TNCC 和TNCS 之间的接口。该接口定义了一个协议，该协议传递如下的信息：从IMC 到IMV 的信息(如完整性测量值) ；从IMV 到IMC 的信息(如要求额外的完整性测量值) ；会话管理信息和一些同步信息。

（b）IMC 和IMV 接口(IF-M) ：IF-M 是IMC 和IMV 之间的接口。在该接口上传输的信息主要是一些与提供商相关的信息。

（c）网络授权传输协议(IF-T) ：IF-T 维护在AR 实体和PDP 实体之间的信息传输。在这两个实体中维护该接口的组件为N A R 和N A A 。

（d）策略实施点接口(IF-PEP) ：IF-PEP为PDP和PEP之间的接口。该接口维护PDP 和PEP 之间的信息传输。通过它，PDP 可以指示PEP 对AR 进行某种程度的隔离，以对AR 进行修复。当修复完成之后，方可授予AR 访问网络的权利。

(3) 可信网络连接过程：

一次完整的可信网络连接交互过程如图 4 所示：

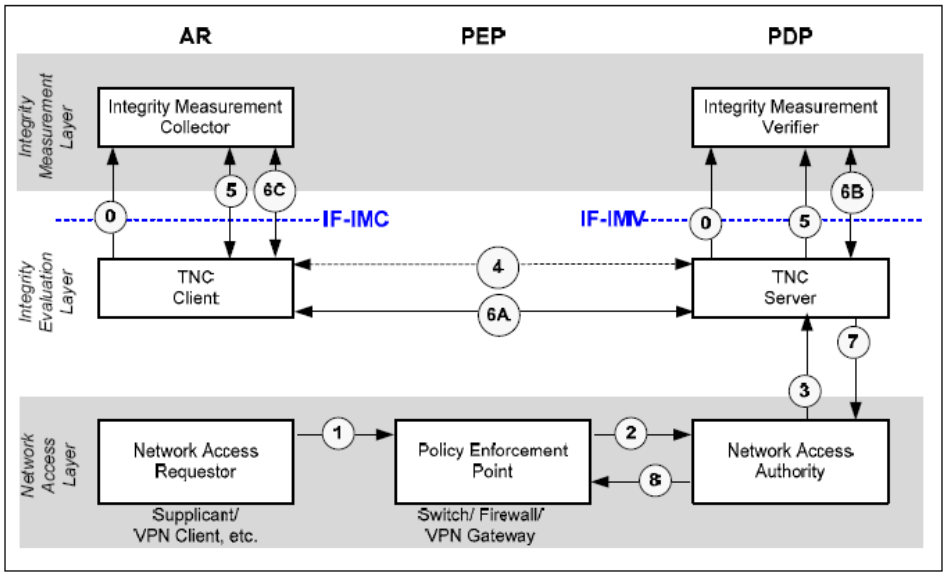


图 4 TNC 的可信连接过程

一次完整的可信连接具体过程为：

(0) 在开始网络连接和完整性检查握手协议之前，TNCC 必须将所需要的完整性信息，装载每一个相关的IMC。对于一个拥有TPM的可信终端，这也就是将网络策略所需信息经散列后存入PCRs,然后启动这些IMC，同时还要保证同这些IMC 连接的状态是不可破坏的。类似的，TNCS 也要装载并启动IMV，TNC服务端需要预先制定完整性的要求，并交给IMV。

(1)当有网络连接请求发生时，NAR 在网络层启动一个连接请求。这个策略执行者通常是防火墙、交换机或者VPN网关。

(2) 收到网络连接请求后，PEP 发送一个网络访问决定请求给NAA。这里，假定NAA 已经设置成按照用户认证、平台认证和完整性检查的顺序进行操作。如果有一个认证失败，则其后的认证将不会发生。用户认证可以发生在NAA 和AR 之间。平台认证和完整性检查发生在AR 和TNCS 之间。

(3)假定AR 和NAA 之间的用户认证成功完成，则NAA 通知TNCS 有一个网络连接请求到来。

(4) TNCS 和TNCC 进行双向的平台完整性验证。这个过程可能会交互多次才能完成。

(5)TNC客户端告诉IMC开始了一个新的网络连接，这个网络连接需要一个完整性握手协议。IMC通过IF-IMC返回所需信息. TNC服务端将这些信息通过IF-IMV交给IMV。

(6A)为了执行一个完整性检查握手,TNCS 和TNCC 开始交换同完整性检查相关的各种信息。这些信息将会被NAR、PEP 和NAA 转发，直到AR 的完整性状态满足TNCS 的要求。

(6B)TNCS 将每个IMC 信息发送给相应的IMV。IMV 对IMC 信息进行分析。如果IMV 需要更多的完整性信息，它将通过IF-IMV 接口向TNCS 发送信息。如果IMV 已经对IMC 的完整性信息做出判断，它将结果通过IF-IMV 接口发送给TNCS。

(6C)TNCC也要转发来自TNCS的信息给相应的IMC，并将来自IMC 的信息发给TNCS。

(7)当TNCS 完成和TNCC 的完整性检查握手之后，发送TNCS 动作推荐（Action Recommendation）给NAA。这里要注意的是，即使AR通过了TNCS 的完整性检查，如果它的某些安全属性不满足NAA 的要求，NAA 仍然可以拒绝AR 的网络访问请求。

(8) NAA发送网络访问决定给PEP来具体实施。NAA 也必须向TNCS说明它最后的网络访问决定，这个决定也将会发送给TNCC。通常，PEP会向NAR指示它对网络访问决定的执行情况。

3.4 TNC 的全面架构

在 TNC 的全面架构中除了基本框架中的三层结构，又引入了第四层，该层位于整个模型的最高层次。它包括两个组件：（1）供给与修补应用 PRA（Provisioning Remediation Application）负责当 AR 不能满足安全策略被隔离（Isolation）后,为其进行完整性修补。例如，AR 的病毒库版本、OS 补丁程序等已过期，则 PRA 为其更新相关配置。（2）供给与修补资源 PRR（Provisioning Remediation Resource）负责提供修补资源，如最新的病毒库数据，OS 补丁程序等。AR 在该层完成平台配置修补后，则重新开始尝试新的网络连接，PDP 对其重新进行完整性度量。完整的 TNC 的架构如图所示，其中 IF-PTS 为新增加的接口函数，实现对于具有可信计算平台（可信芯片+可信软件堆栈+可信平台服务）的访问请求者 AR，为其提供计算平台与 AR 组件间的接口界面。依据此界面，AR 的组件将可以使用可信平台所提供的基本功能，如密码生成，数据保护等。TNC 全面架构如图 5 所示。

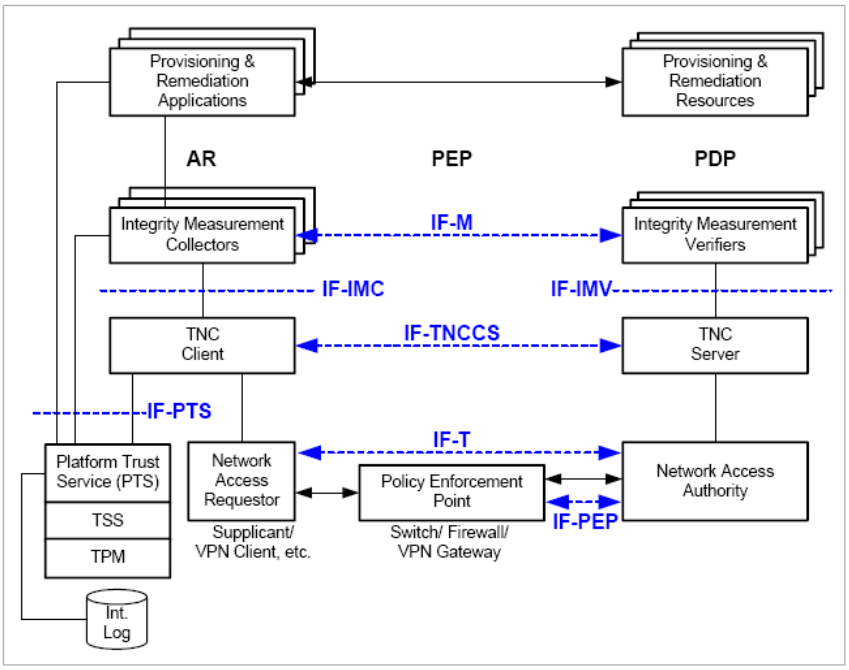


图 5　完整的 TNC 架构

3.5 TNC 实施的相关安全考虑[10]

在当前的结构中，主要是考虑到了AR 和PDP 之间信息流动的完整性。而在具体的实现中，以下的一些安全方面也是要考虑的：

（1）端点系统的完整性测量架构：如何在端点系统上构建一个有效的完整性测量架构，测量系统的各种完整性属性。这里的完整性属性不仅应该包括终端，还要包括网络相关的部分。

（2）AR 和PDP 之间的安全通道：为了在TNCC 和TNCS之间传输各种完整性信息，必须要建立一个安全通道。这个通道建立的可能位置是在NAR 和NAA 之间。这个通道应该是端到端的，PEP 不能访问这个通道中所传输的内容。这个通道的具体实现应该和具体的应用环境相结合。

（3）对TNCC/TNCS 和IMC/IMV 的授权：TNCC 和TNCS应该只能和得到授权的IMC和IMV通信，以防止非授权的IMC/IMV发送虚假的完整性信息。

（4）AR 和PDP 自身的完整性：要在AR 和PDP 之间正确的传输完整性信息，AR 和PDP 自身的完整性必须是得到保护的。

（5）对各种接口的保护：在具体的实施中，要保证通过各种接口的消息是完整的，不能被非法修改。

3.6 TNC 的相关支撑技术

（1）网络访问技术：

（a）IEEE 802.1X

（b）VPNs

（c）PPP

（2）消息传输技术：

（a）受保护的 EAP 机制

（b）TLS 和 HTTPS

（3）PDP 技术

（a）RADIUS

（b）Diameter

3.7 可信网络的相关实现机制[9]

（1）可信传输

传统的报文交换基于非对称加密，就是说只有一个人可以使用公钥加密。而通过使用私钥签字可以防止对报文的篡改。在这种传统传输中，不正确的管理密钥和终端不正确的配置都会导致安全上的风险。TPM 通过提供密钥管理和配置管理（保护存储、度量和报告）来增加传输的安全性。这些特性可以同封印组合到一起，使得终端配置更加清晰和强壮。TCG 定义了四种被保护的报文交换方式：绑定（Binding），签名（Signing）、封印绑定（Sealed-Binding）、封印签名（Sealed-Signing）。

绑定和签名同传统方法一样，-TCG. 体系中最有特色的也就是“封印”了。封印比绑定有着更进一步的安全性，封印报文就是一套由发送者定义的 PCR 值，平台 PCR 值描述了在解密之前必须存在的平台的配置值，封印帮助使用 PCR 值和不可移交的密钥去加密报文（事实上，使用对称密钥加密报文）。拥有非对称解密密钥的 TPM,只有在平台配置符合发送者规定的 PCRs 值时，才能对对称密钥进行解密，这是 TPM 的一个强有力的特性。

签名操作也可以和 PCR 值一起作为一种提高平台安全性的手段，要求平台签名的时候使用精确的配置信息。验证者要求签名必须包含一部分 PCR 值。签名者在签名的过程中，收集要求的 PCRs 值并把它们包含进报文中，作为计算摘要的一部分。验证者能够检查报文中的 PCR 值，作为确认签名平台在生成时的配置。

通过将 PCR 值加入到传输中，也就保证了不仅要经过身份认证，还要同时保证目标平台的环境配置也满足要求才能进行传输，这一方面可以加强安全性，同时也能够进行数字版权保护。

（2）身份认证

身份认证并不难，但一般希望在使用个人隐私来证明身份的时候，要尽可能少地暴露自己的身份信息，这与身份认证的要求正好矛盾。而在 TCG 的体系里，这个隐私就是 EK,我们不能使用 EK 来进行身份认证。所以，在 TCG 体系中，身份认证一般是是使用 AIK,作为 EK

的别名。这种方法类似传统的解决方案，首先需要生成一个 AIK，如图 6 所示。

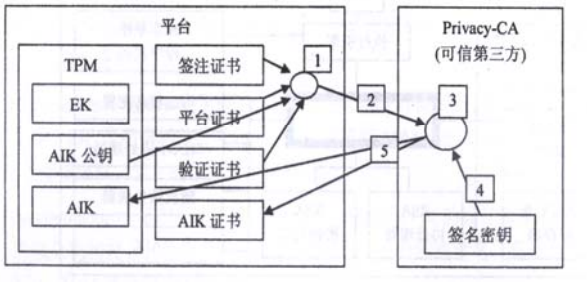


图 6 AIK 的获取

(1)所有者使用 RSA 密钥生成模块生成一对 AIK 密钥，然后将公钥和签注证书、平台证书和验证证书打包在一起；
(2)发送一个 AIK 的请求给 Privacy-CA；
(3)可信第三方通过验证证书的有效性来验证 AIK 请求的有效性；
(4)可信第三方使用自己的签名密钥对 AIK 证书签名；
(5)将签名后的 AIK 证书返回给 TPM。

此后，平台就可以使用 AIK 和 AIK 证书来证明自己的身份，基于 AIK 的平台间验证如图 7 所示。

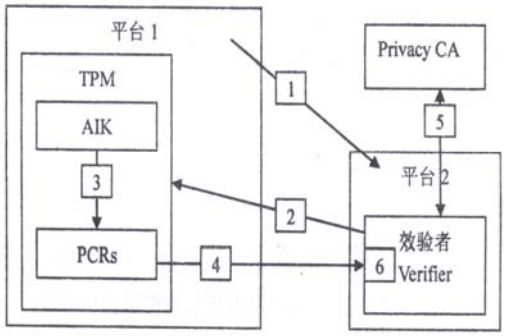


图 7 基于 AIK 的平台验证

(1)平台 1 所有者向平台 2 发送请求；
(2)平台 2 向平台 1 发送证明（attestation)的请求，同时说明需要那些 PCR 值；
(3)使用 AIK 对需要的 PCR 值签名；
(4)将签名后的 PCR 值发送给平台 2 的校验者；
(5)同 PrivacyCA 一起确认平台 1 的身份，评估平台 1 的可信程度；
(6)评估平台 1 的环境配置状态。

通过这两步，就可以完成通信时的身份认证了．而且因为加入了对环境配置的评估，能够确认通信双方的状态，增强对各种恶意软件的抵御能力。

由于一个用户理论上可以有无限多个 AIK，用户在进行通信的时候，只有可信第三方知道用户的真实身份，通信对象并不知道，这样，也就减少了隐私的暴露。尽管如此，还是暴露了 AIK 证书，而且需要可信第三方的参与，所以 TCG 架构 1.2 规范中还提供了一种认证方法一—直接匿名认证 DAA(Direct Anonymous Attestation)。直接匿名认证的基础，来自于贝尔实验室与剑桥大学在 1990 年代初所开发的零知识证明(Zero-Knowledge Proof)概念。

3.8 可信计算的相关应用情景

这个领域主要解决的是如何将可信性从可信的终端设备扩展到网络之中，以及在现有的计算平台和资源环境下，如何使用可信度较低的终端系统来构建可信的网络，则是目前工业界和学术界的主要研究方向。已有的解决方案有天融信公司的基于可信服务的可信网络架构研究，思科公司的网络准入控制机制以及TCG的可信网络接入标准。

（1） **可信网络及可信接入** 针对目前网络的脆弱性所导致的不可信或不完全可信问题，为了提高网络系统的安全性、可用性和可控性，林闯在文献[21,22]中首先回顾了互联网络的发展历程，预测地提出了新一代互联网络的研究内容，即网络的可信性、可控性和可扩展性；此外他在文献又给出了可信网络的基本定义，以及关键的科学问题，如网络与用户行为的可信模型，可信网络体系架构，服务的可生存性，网络的可控性等等。对于网络接入研究，TCG标准中[8]则涉及了可信网络的接入，如何增强可信网络的安全性、可用性，并将现有的多种访问控制技术和网络安全技术融入其中是目前网络接入的研究重点。

（2） **基于可信计算的无线移动网络安全** 无线移动网络的迅速发展和广泛应用使得它也面临着安全威胁，无线网络的特点决定了对它的攻击方式与有线网络有所不同，因此必须研究新的专门用于无线网络的安全技术；下一代网络将是有线网络和无线网络的结合体，研究有线网络和无线网络的安全技术，为下一代网络的安全技术研究奠定基础是非常有意义的。Zheng Yan在文献[16]中构建了一个处理可信移动环境问题的概念环状模型，从而依据该模型来研究可信移动环境下的通信、服务和应用的可信问题。该模型从里层向外依次为概念层、理论层、实现层和应用层，主要研究可信的概念、相关理论和构建方法、基于理论的模型和标准的构建以及支持可信的应用和系统的实现。最后并给出一个基于此概念模型的移动P2P应用。郑宇等在文献[20]中针对移动终端的安全性问题，首先讨论了现有解决方案存在的问题，如基于PIN的用户身份认证，基于生物特征和智能卡的身份认证等，以及TMP标准存在的缺陷，提出了结合USIM(Universal Subscriber Identity Module) 和TPM(可信平台模块) 的可信移动平台(TMP) ,并以智能手机主流处理器为基础,讨论了TMP 的设计案例以及TPM 在ME中的三种构建方法，给出了基于可信计算的移动终端认证方案，实现了用户和ME、用户和USIM 间的相互认证,强化了用户域的安全,并可满足TMP标准草案中安全等级3 对用户认证的要求。 该方案在不要求使用者与ME 预先协商信任关系的前提下,既可区分攻击者和合法用户,又可辨别ME 的主人和普通使用者,并能在认证过程中及早发现攻击行为,避免不必要的计算开销。最后所提方案和已有的方案作了安全性、通用性和执行效率上的比较。此外，他在文献[19]中提出了基于可信计算的4G移动网络的安全框架。Shane Balfe在文献[28]中根据普适网络中节点的若干特性，如动态性、上下文感知性、不可见性以及资源有限性，提出了保障普适网络中移动终端节点可信与安全,基于TPM芯片的移动节点的加入和验证架构，该结构分为被匿名认证访问一个安全设施、安全存储与机密信息的非泄露与秘密共享等三个步骤。最后以一个匿名投票的案例对所提架构加以应用和阐释。

（3） **基于可信计算的Peer-to-Peer安全** P2P网络回归了互联网络的本质，不存在集中的控制节点，每个Peer之间是对等的，它既可以作为服务器，也可以作为客户机，Peer之间相互共享资源和交换信息。但由于P2P网络中节点的匿名和身份不确定性，因此带来了Peer间相互信任问题，以及不可忽视的信息安全问题与隐私问题。近来Sandhu[9, 13]给出了P2P网络中基于可信计算实现资源共享的解决方案，他们的研究主要集中在OM-AM (Objective-Model-Architecture-Mechanism)[10]的架构层次，并未涉及到安全模型层，因此该解决方案对于选择何种策略模型具有一定的普遍意义。该解决方案在TPM基础上，添加了安全的OS内核与关键部件-Trusted Reference Monitor,实现了“服务器推”模式，基于可信计算的原理，在客户端保障资源访问控制策略的完整性实施。文中同时给出了基于TPM的相关的身份认证、策

略分发和策略实施协议等，是实现P2P网络中资源安全共享的访问控制策略。Shane Balfe在文献[12]中也基于P2P网络的安全性问题，采用TCG标准的DAA(Direct Anonymous Attestation)协议实现了Peer间的认证，减少了Peer的相关证书及隐私的暴露。关于DAA的详细介绍，可参考文献[15]，以及陈在06年提出的基于属性的远程证明协议方案[14]。

4 国内外其他可信接入标准

4.1 Cisco Network Admission Control (NAC)标准

Cisco NAC 使用网络基础设施对试图访问网络计算资源的所有设备执行安全策略检查，从而限制病毒、蠕虫和间谍软件等新兴安全威胁损害网络安全性。实施 NAC 的客户能够仅允许遵守安全策略的可信终端设备(PC、服务器及 PDA 等)访问网络，并控制不符合策略和不可管理的设备受限地访问网络或拒绝访问[29]。Cisco NAC 架构如图 8 所示。

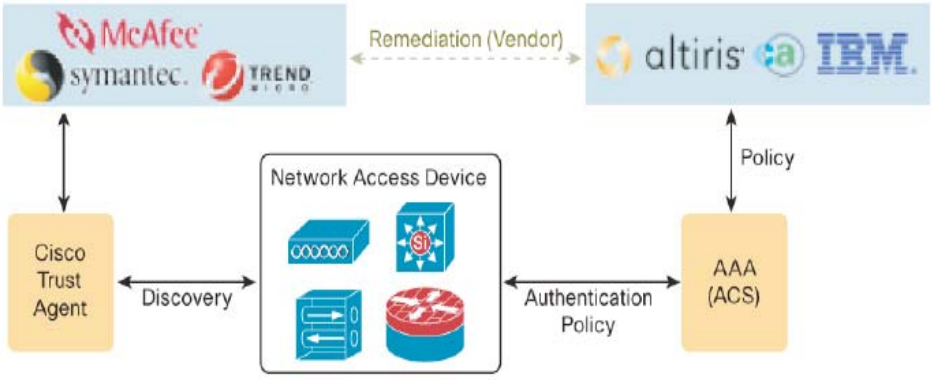


图 8 Cisco NAC 架构

通过运行 NAC，只要终端设备试图连接网络，网络访问设备(LAN、WAN、无线或远程访问设备)都将自动申请已安装的客户端或评估工具提供终端设备的安全资料。随后将这些资料信息与网络安全策略进行比较，并根据设备对这个策略的符合水平来决定如何处理网络访问请求。网络可以简单地准许或拒绝访问，也可通过将设备重新定向到某个网段来限制网络访问，从而避免暴露给潜在的安全漏洞。此外，网络还能隔离的设备，它将不符合策略的设备重新定向到修补服务器（Remediation Server）中，以便通过组件更新使设备达到策略符合水平。

NAC 设备 Cisco Clean Access 包含以下组件：

（a）Cisco Clean Access Server，评估设备并基于终端的策略符合情况授予访问权限。

（b）Cisco Clean Access Manager，集中管理 Cisco Clean Access 解决方案，包括执行策略和修补服务。

（c）Cisco Clean Access Agent，可选的免费软件，提供更严格的终端策略符合评估，并同时简化可管理与不可管理环境中的修补流程。

Cisco Clean Access 通过以下技术支持无线访问：所有的 802.11 Wi-Fi 接入点，包括 Cisco Aironet 接入点；以及提供支持 NAC 的 IEEE 802.1X 请求系统的所有 Wi-Fi 客户设备。

NAC 框架提供以下技术支持： 为园区 LAN、WAN、VPN 和无线接入点提供广泛的网络设备支持；连接第三方主机评估工具，用于评估无人值守的、“无代理的”和其他非响应型设

备，且能够对每个设备应用不同的策略；为 Cisco 可信代理提供广泛的平台支持 ，通过远远超越防病毒和基本操作系统补丁的应用和操作系统状态检查，来扩展多厂商集成功能。

4.2 Microsoft NAP（Network Access Protection）标准

微软 NAP 目前虽还尚未普遍，但已经有多达 60 多家厂商支持，Windows Server 系统自 Active Directory 架构以来，缺少良好的安全政策管理与政策执行能力，而 NAP 方案则要解决此问题。NAP 借助许多机制来执行安全政策，像是利用 IPSEC 主机认证、802.1X、VPN 或 DHCP 等，微软将把 NAP 开发成一套开放的安全架构标准[30]，如图 9 所示。

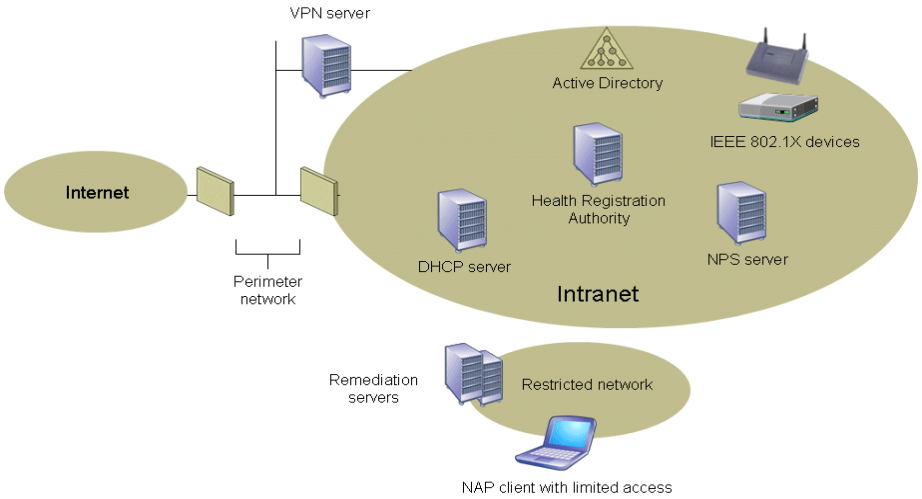


图 9 Microsoft NAP 架构

NAP 架构可利用客户端程序 Quarantine Agent，来将系统信息传送至 Microsoft 的 Network Policy Server，其作用跟 Cisco 的 ACS 一样，可与 Third-Party 政策服务器合作，检查是否符合政策。NAP 提供了 DHCP、IPSEC、VPN、802.1X 等方式来执行安全政策。

微软开发 NAP 是为了帮助企业控制内部网络设备，确保所有设备上网前都能得到安全检查。它整合了病毒扫描和连接策略控制系统，以阻止未获得安全许可的连接。很多开发 VPN 技术的企业也加入了微软的 NAP 联盟，包括 CheckPoint、北电、F5 和 Aventail。微软公司负责 Windows 服务器的高级市场官员 Steve Anderson 称：“将 VPN 企业纳入我们的合作联盟非常重要。如今，非常多的攻击是通过 VPN 隧道进入企业内网的，我们希望能让客户在不更换 VPN 设备供应商的前提下，获得更为安全的 VPN 连接服务。”

4.3 华为 EAD（Endpoint Admission Defense）标准

华为 3Com 端点准入防御 EAD 方案从网络终端入手，整合网络接入控制与终端安全产品，强制实施企业安全策略，从而加强网络终端的主动防御能力，防止“危险”、“易感”终端接入网络，控制病毒、蠕虫的蔓延。这种端到端的安全防护体系，可以在终端接入层面帮助管理员统一实施企业安全策略，大幅度提高网络的整体安全。

EAD 解决方案在用户接入网络前，强制检查用户终端的安全状态，并根据对用户终端安全状态的检查结果，强制实施用户接入控制策略，对不符合企业安全标准的用户进行“隔离”并强制用户进行病毒库升级、系统补丁安装等操作；在保证用户终端具备自防御能力并

安全接入的前提下，合理控制用户的网络行为，提升整网的安全防御能力。EAD 架构如图 10 所示。

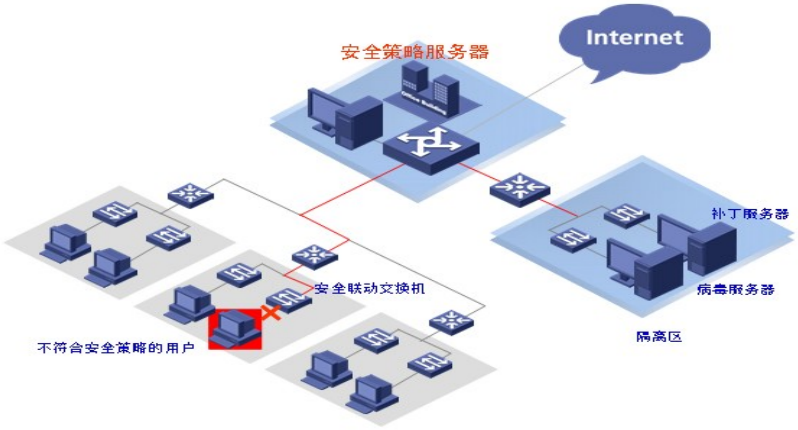


图 10 华为 3Com EAD 架构

（1）EAD 的功能特点

（a）完备的安全状态评估

用户终端的安全状态是指操作系统补丁、第三方软件版本、病毒库版本、是否感染病毒等反映终端防御能力的状态信息。EAD 通过对终端安全状态进行评估，使得只有符合企业安全标准的终端才能准许访问网络。

（b）实时的“危险”用户隔离

系统补丁、病毒库版本不及时更新或已感染病毒的用户终端，如果不符合管理员设定的企业安全策略，将被限制访问权限，只能访问病毒服务器、补丁服务器等用于系统修复的网络资源。用户上网过程中，如果终端发生感染病毒等安全事件，EAD 系统可实时隔离该“危险”终端。

（c）基于角色的网络服务

在用户终端在通过病毒、补丁等安全信息检查后，EAD 可基于终端用户的角色，向安全客户端下发系统配置的接入控制策略，按照用户角色权限规范用户的网络使用行为。终端用户的 ACL 访问策略、是否禁止使用代理、是否禁止使用双网卡等安全措施均可由管理员统一管理，并实时应用实施。

（d）可扩展的、开放的安全解决方案

EAD 是一个可扩展的安全解决方案，对现有网络设备和组网方式改造较小。在现有企业网中，只需对网络设备和第三方软件进行简单升级，即可实现接入控制和防病毒的联动，达到端点准入控制的目的，有效保护用户的网络投资。

EAD 也是一个开放的安全解决方案。EAD 系统中，安全策略服务器与网络设备的交互、与第三方服务器的交互都基于开放、标准的协议实现。在防病毒方面，目前 EAD 系统已与瑞星、金山、江民等多家主流防病毒厂商的产品实现联动。

（e）灵活、方便的部署与维护

EAD 方案部署灵活，维护方便，可以按照网络管理员的要求区别对待不同身份的用户，定制不同的安全检查和隔离级别。EAD 可以部署为监控模式（只记录不合格的用户终端，不进行修复提醒）、提醒模式（只做修复提醒，不进行网络隔离）和隔离模式，以适应用户对安全准入控制的不同要求。

（2）EAD 方案部件

（a）安全策略服务器

EAD 方案中的用户管理与策略控制中心，实现用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能，是 EAD 解决方案的核心部件。华为 3Com 公司的 CAMS 产品作为安全策略服务器，可以在全面管理网络用户信息的基础上，实现对网络用户的身份认证和接入终端的安全认证，并通过与网络设备的联动控制用户网络访问行为。同时，该系统详细记录了用户上网信息和安全事件信息，可以方便地跟踪审计用户上网行为和安全事件。

（b）安全客户端

安装在用户终端系统上的软件，是对用户终端进行身份认证、安全状态评估以及安全策略实施的代理。安全客户端可按照企业安全策略的要求，集成第三方厂商的安全产品插件，提供丰富的身份认证方式、实施基于角色的安全策略。

（c）安全联动设备

企业网络中安全策略的实施点，起到强制用户准入认证、隔离不合格终端、为合法用户提供差异化服务的作用。华为 3Com 系列交换机、路由器、安全网关等网络设备，可以通过标准的协议与 CAMS 安全策略服务器的联动，在不同的应用场景实现对用户的准入控制。

（d）第三方服务器

第三方服务器是指病毒服务器、补丁服务器等网络安全产品。通过安全客户端的代理插件以及安全策略服务器的策略控制，第三方安全产品可以集成至 EAD 解决方案中，实现不同层面安全功能的联动与融合。

4.4 天融信 TNA（Trusted Network Architecture）

TNA是北京天融信在2004年12月，基于行为与内容可信的信息安全新理念提出的一个面向用户业务的、体系化的安全解决方案[31]。TNA的主要目标如下：

（1）TNA将通过安全管理系统、可信网络接入认证系统、网络行为与内容的监管体系以及信息的可信交换平台等的协同与融合，有效地解决用户的安全新需求：

（a）管理和整合现有安全资源；

（b）构筑“可信网络”安全边界；

（c）有效监管网络中的行为与内容，强化对网络资源的保护；

（d）解决信息化业务的互联、互通、互操作；

（2）在实现用户网络的综合安全防御能力提升的同时，确保用户业务的正常运作。

TNA架构如图11所示，其中主要系统组件如下：

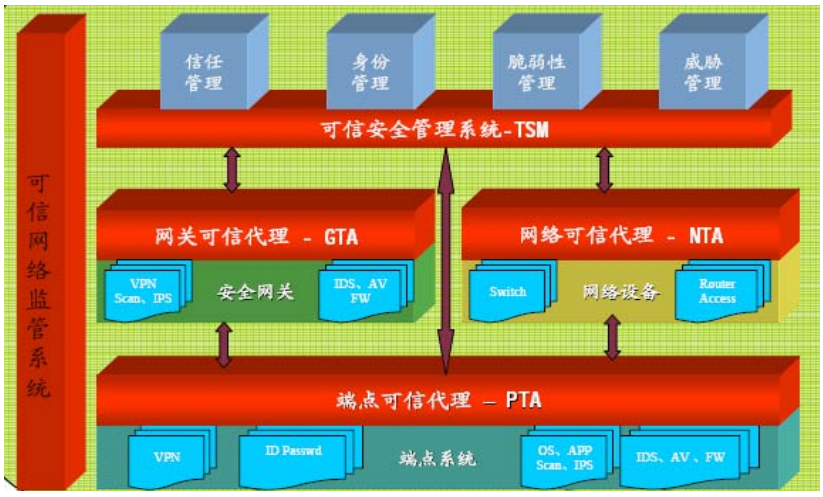


图 11　天融信 TNA 架构

（1）可信网络安全管理系统TSM（Trusted network Security Management system）：通过对网络中各种设备（包括路由设备、安全设备等）、安全机制、安全信息的综合管理与分析，对现有安全资源进行有效管理和整合；

（2）可信监管系统TMS（Trusetd network Monitor System）：主要实现对网络与业务应用中的行为与内容进行监测、审查、管理与控制；

（3）可信接入认证系统TAS（Trusted Access Authentication System）：它是实现可信网络动态扩展的基础，主要基于可信代理技术，结合认证、评估机制，对终端系统（用户）的安全状况进行评估、认证及接入控制管理；能够有效地避免因不可信终端系统接入网络所带来的潜在风险。

（4）面向用户业务进程的多代理体系：代理具有代理性、自治性、协同性、交互性和适应性等特性，网络环境内有组织群体的应用进程。TNA多代理体系在多系统、多应用的异构环境下，实现用户业务的安全保障、监管以及相关服务的基础，并且能够实现多个业务系统之间的连接与互联互通、互操作等。TNA的架构如图所示：

4.5 联想可信计算环境接入解决方案

联想的可信计算环境接入解决方案的本质和 TNC 及其它标准的架构类似，主要由请求接入计算机、策略执行设备和可信接入服务器组成，如图 12 所示[33]。请求接入计算机是基于可信芯片的，该芯片能够提供一系列的可信平台服务，包括系统的完整性检测、身份认证服务以及其它安全服务等；可信接入服务器在收到请求接入计算机终端设备的请求和各种系统完整性度量信息后，首先进行身份认证，然后判定度量信息是否符合安全策略，最后把决策信息发给策略执行设备来执行相应的操作，如通过、拒绝或升级计算机程序（修补）等。在企业计算环境中，策略执行设备也可以是防火墙、路由器、VPN 网关或应用服务器等。

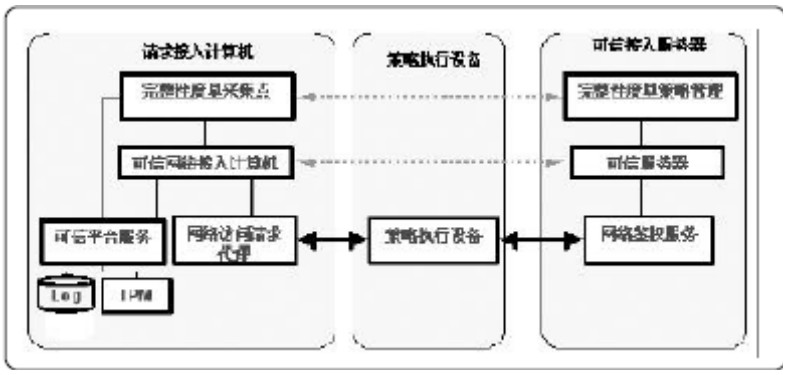


图 12 联想可信计算环境接入解决方案

随着计算机网络与信息化的不断发展，信息安全问题日趋复杂，系统安全问题，特别是计算机平台的开放框架所带来的威胁层出不穷。面对严峻的网络安全形势，传统的信息安全系统从架构和强度上已经难有大的突破。人们在信息安全的实践中逐渐认识到，大多数安全隐患来自于终端，因此必须确保源头的信息安全，即从每一台连接到网络的终端开始，遏制恶意攻击，由此产生出可信计算的基本思想[1-6]。可信计算本质上是要通过增强现有终端体系结构的安全性来保证整个系统的安全，其主要思路是基于安全硬件和安全操作系统来实现一个可信的平台。可信计算经过多年的发展，1999 年由 IBM、HP 等著名 IT 企业发起成立了可信计算平台联盟 TCPA (trusted computing platform alliance)，2003 年 TCPA 改组为可信计算组织 TCG (trusted computing group)。可信计算组织制定了关于可信平台模块[7]、可信存储[8]等一系列技术规范，在可信计算领域具有较大的影响力。其可信网络连接分组（TNC Sub

Group，TNC-SG）制定了一个基于可信计算技术的可信网络连接 TNC 架构[9]，它本质上就是要从终端的完整性开始，建立连接。在传统网络认证接入基础上，增加平台的身份认证和平台的完整性校验，终端用户只有在两层认证通过且平台完整性校验成功后才可以接入网络。研究人员对 TNC 架构以及基于 TNC 架构的可信网络连接协议进行了大量的研究[10-14].

IBM 公司在 TNC 架构基础上提出了一个完整性评估层协议——完整性报告协议[14]，该协议实现 TNC 架构中完整性评估层平台的身份认证和完整性校验。本文通过对 TNC 架构和完整性报告协议的分析，发现 TNC-SG 提出的可信网络连接（TNC）架构存在一个安全缺陷，即用户与平台之间没有安全绑定关系，这一安全缺陷直接造成基于 TNC 架构的完整性评估层协议漏洞。因此，可信网络连接协议的设计应避免这一漏洞。为使协议的设计和分析更具一般性和安全性，本文设计了一个可证明安全的可信网络连接协议模型，通过模型指导协议的设计和分析，从而解决了 TNC 架构的安全缺陷.

可信网络连接架构是在传统网络认证接入协议架构基础上提出的，两者有着密切的联系和本质的区别。因此本文基于当前非常流行的可证明安全形式化方法——CK 模型[15]的基本思想，结合 TNC 架构的具体规范[9]，设计了可证明安全的可信网络连接协议模型 TNC-PS。TNC-PS 模型为两层结构：网络访问层模型和完整性评估层模型。我们通过对网络访问层协议内部和外部攻击者，以及协议运行环境的分析，指出 CK 模型可以直接作为网络访问层协议的设计和分析模型。完整性评估层模型将协议的运行环境抽象为两类：可信链路模型（PTM）和非可信链路模型（PUM）。可信链路模型是一种理想化的链路模型，在这一模型中，网络访问层用户与完整性评估层平台之间存在安全绑定关系，完整性评估层协议的运行在网络访问层安全信道保护下进行；非可信链路模型 PUM 是现实协议的运行环境，其中不存在上述绑定关系。本文还提出了绑定器的概念，它是完整性评估层模型的核心，通过绑定器，可以将 PTM 中设计的安全协议简单的转化为 PUM 中具有同等安全性的协议，从而避免 TNC 架构的安全缺陷.

本文其余部分组织如下：第 1 节对背景知识进行介绍，包括可信网络连接 TNC、CK 模型；第 2 节给出针对完整性评估层协议的一种新的攻击——平台替换攻击，并指出 TNC 架构的安全缺陷；第 3 节给出了可证明安全的可信网络连接协议模型 TNC-PS，并形式化的定义了可信网络连接协议；第 4 节利用 TNC-PS 模型设计了一个满足可信网络连接安全目标的完整性评估层协议；最后一部分对全文进行了总结并给出下一步的工作.

5 可证安全的网络连接模型

5.1 可信网络连接

可信计算组织可信网络连接分组（TNC Sub Group，TNC-SG）制定了一个基于可信计算技术的网络连接规范，它本质上就是要从终端的完整性开始，建立连接。即在传统网络认证接入基础上，增加平台的身份认证和平台的完整性校验，终端用户只有在两层认证通过且平台完整性校验成功后才可以接入网络.

可信网络连接（TNC）[9]架构如图 13 所示，包含三类实体：访问请求者、策略执行者和策略决策者，这些都是逻辑实体，可以分布在任意位置.

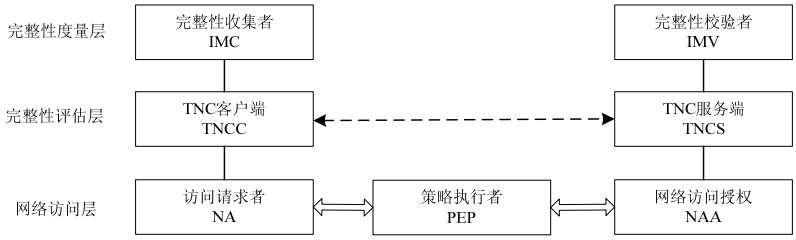


图 13 可信网络连接 TNC 架构

TNC 架构在纵向分为三个层次，从下到上为：

网络访问层：这一层用于支持传统的网络连接技术，进行用户身份认证和密钥协商并建立安全信道，完成后通知上层进行完整性评估层协议；

完整性评估层：负责评估所有请求访问网络的平台的完整性，这一层协议的运行受网络访问层安全信道的保护；

完整性度量层：收集和校验请求访问者的完整性相关信息的组件.

5.2 平台替换攻击及其分析

完整性报告协议[14]被用于实现平台身份认证和平台的完整性校验，它基于挑战-应答认证协议[18]。如图 14 所示，平台 PA 向平台 PB 证明自己的身份和完整性，其中 nonce 为不可预知的随机数，AIK_{priv} 和 AIK_{pub} 为证明身份密钥对[7]，$loadkey(AIK_{priv})$ 表示使用存储根密钥从可信平台模块 TPM 中读取证明身份密钥 AIK_{priv}，SML 为存储测量日志[9]，$cert(AIK_{pub})$ 为 Privacy CA 向平台签发的 AIK 证书，$Sig\{PCR,nonce\}_{AIK_{priv}}$ 表示以 AIK_{priv} 为私钥将选择的 PCR 值和收到的随机数 nonce 进行签名.

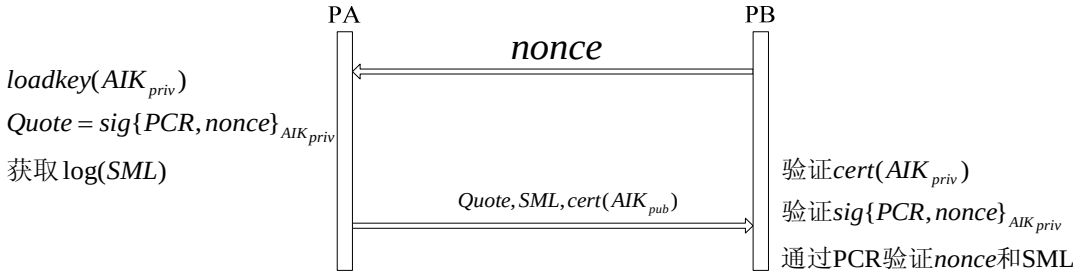


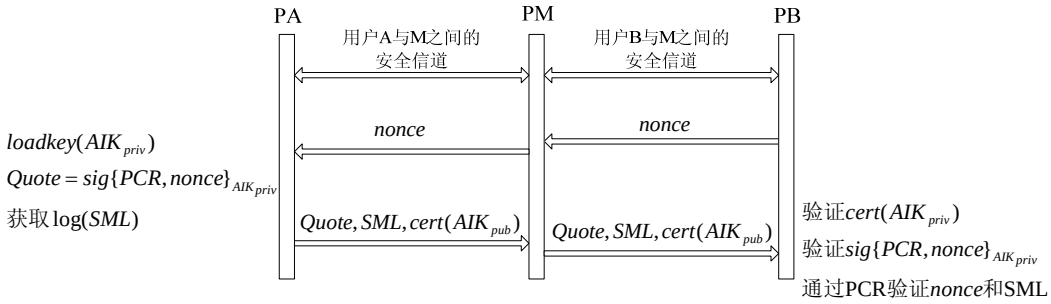
图 14 完整性报告协议

我们发现，上述协议容易遭受一种新的攻击——平台替换攻击。可信网络连接架构中完整性评估层的目的是验证接入平台的身份和平台完整性，这一攻击将导致平台身份认证的失败以及平台完整性校验错误，造成可信网络连接的安全目标不能达到.

合法用户 M 希望通过不可信的平台 PM 接入平台 PB，攻击过程如图 15 所示.

假定 用户 A、M 和 B 都是合法用户，且 A 与 M、M 与 B 之间分别建立了安全信道。用户 A、M 和 B 分别控制平台 PA、PM 和 PB，其中 PA、PB 是可信平台，PM 是不可信平台。

攻击结果 平台 PB 认为 PM 是一个可信平台并允许其接入，但实际上 PM 是一个不可信平台。



攻击过程

1) PB 生成随机数 nonce 并发送给 PM；
2) PM 收到 nonce 后，将其转发给 PA；
3) PA 接收到 PM 发来的挑战消息 nonce，按照 2.1 节协议规定，使用存储根密钥从 TPM 中读取证明身份密钥 AIK_{priv}，并以 AIK_{priv} 为私钥将选择的 PCR 值和收到的随机数 nonce 进行签名 $Sig\{PCR,nonce\}_{AIK_{priv}}$，然后将签名消息连同存储测量日志 SML 和 AIK 证书 $cert(AIK_{pub})$ 一同发给 PM；
4) PM 将 PA 发来的消息转发给 PB。
5) PB 的验证过程与 2.1 节协议中 PB 的验证过程相同。

图 15 平台替换攻击

攻击中，平台 PM 成功的说服平台 PA 对平台 PB 的一次性随机数进行签名，并进而允许平台 PM 成功的欺骗平台 PB。这是一次完美的攻击，因为平台 PA 和平台 PB 都不能够察觉到任何错误。攻击结束后，平台 PB 认为 PM 是可信平台并允许其接入，平台 PA 认为它与平台 PM 进行了一次协议交互。但实际上平台 PM 是一个不可信平台，它借助可信平台 PA 接入 PB.

可信网络连接框架中，完整性评估层协议是在网络访问层用户之间建立的安全信道基础上进行的。尽管有安全信道保护，但无法避免平台替换攻击，如图 3 所示。攻击发生的根本原因是：

一方面，按照 TPM 主规范[7]的规定，对于验证平台而言，AIK 签名只能说明消息来自一个含有真实 TPM 芯片的平台，不能证明签名消息的平台就是议定的通信平台，证明身份密钥 AIK 不能直接用于认证通信平台的身份。因此，验证平台 PB 不能确定接收到的消息属于协议议定的响应平台 PM，而只能确定消息来自一个可信的平台.

另一方面，在进行可信网络连接过程中，同一用户可以使用不同的计算平台，不同的用户也可以使用同一平台进行连接，这就使得用户与用户所使用的平台之间不存在一一对应的关系。网络访问层建立的安全信道只能保证网络访问层用户之间通信的认证性和保密性，不能保证用户所使用的平台之间的认证性。可信网络连接架构规定，网络访问层的安全信道能够保护完整性评估层协议的消息交互[9]，但实质上用户与平台之间没有绑定关系，不能将两者看作一个整体来处理，平台之间的身份认证和完整性校验不能完全依赖于用户之间的安全信道。这是造成平台替换攻击最主要的原因，同时它也是 TNC 架构的设计中没有考虑到的一个安全缺陷.

5.3 可证明安全的可信网络连接协议模型

由于 TNC 架构设计上的缺陷（网络访问层用户与完整性评估层平台之间不存在安全绑定关系），基于这一架构设计的协议容易遭受平台替换攻击。本文发现在保持 TNC 架构不变的前提下，通过协议的巧妙设计可以实现网络访问层用户与完整性评估层平台之间的动态绑定，从而避免了 TNC 架构安全缺陷造成的影响。但协议的设计和分析是一项十分复杂的工作，凭借经验进行协议的设计和分析，是非常容易出错的[19]，而且为了使协议的设计和分析更具一般性，需要有可证明安全或形式化的方法来指导。现有的可证明安全模型和形式化方法（如 CK 模型[15]、UC 模型[20]、PCL 模型[21]等）在网络认证接入协议方面只针对传统协议，而且这些模型和方法多是基于 Dolev-Yao 威胁模型[20]构造的.

可信网络连接协议与传统网络认证接入协议有着很大的差别：首先，网络连接设备有所不同，可信的网络连接设备具有 TPM 模块，由于 TPM 的物理防篡改特性，能够保护系统内部部分敏感数据；其次，可信网络连接架构在传统网络连接架构基础上，增加了完整性评估层，这一层协议的网络运行环境与传统网络访问层协议的运行环境有所不同（完整性评估层协议是在网络访问层安全信道上进行的）。这导致 Dolev-Yao 威胁模型在可信环境下不再完全适用，相应的基于这一模型构造的可证明安全模型和形式化方法也就不再适用。这就要求我们设计一种新的可信环境下的协议设计和分析模型.

通过对 TCG 可信网络连接架构的深入分析，我们提出了可信网络连接协议的安全目标，在此基础之上，结合可证明安全模型 CK 模型[15]的基本思想，给出了一种可证明安全的可信网络连接协议模型.

根据 TNC 的规定，可信网络连接架构底层网络访问层采用传统网络连接技术（如 VPN[23]，802.1x[24]等），完整性评估层协议在底层安全信道保护下进行。因此，可信网络连接的一个最基本要求是底层网络连接协议的安全性.

目标 1　网络访问层实现用户身份认证，协商出用户之间 SK 安全的会话密钥，在此基础之上，实现通信用户实体之间的安全信道.

在网络访问层协议安全基础上，可信网络连接架构提出了新的要求，即要求用户使用的平台之间进行平台身份认证和平台完整性校验。这是可信网络连接架构的又一安全目标.

目标 2　完整性评估层在网络访问层安全信道保护下，实现平台身份认证和平台完整性校验.

网络访问层的安全信道，是户实体之间的安全信道。TNC 架构指出用户间建立的安全信道可以直接用来保护平台间的消息交互。TNC 架构没有考虑到用户与平台之间并不是一种固定的绑定关系，同一用户可以使用任意平台进行网络连接，不同用户也可以使用同一平台，用户之间的每一次连接会话都可能使用不同的平台。TNC 架构的这一缺陷，直接导致了 2.2 节攻击的产生。所以需要在用户与平台之间建立一种动态的安全绑定关系.

定义 3 (用户与平台动态授权绑定)　对于每一次可信网络连接会话，网络访问层用户都与唯一的完整性评估层平台相对应.

目标 3　用户与平台动态授权绑定。在网络访问层用户之间建立安全信道基础上，通过用户对平台的动态授权，实现用户与平台之间的安全绑定，从而使平台可以安全的使用用户之间建立的安全信道.

可信网络连接架构包括相互关联的两个过程[9]：网络访问层的用户身份认证和密钥协商，以及完整性评估层的平台身份认证和平台完整性校验。完整性评估层协议是在网络访问层用户身份认证和密钥协商完成，建立了安全信道基础上进行的。因此，本文设计的可证明安全的可信网络连接协议模型是相互关联的两层：网络访问层模型和完整性评估层模型.

CK 模型是一种模块化的协议设计方法，它具有三类攻击者模型[15]：攻陷参与者、会

话密钥查询及会话状态暴露。这三类攻击模型是针对计算实体内部的攻击，不涉及对网络上传输消息的攻击。认证器[16,17]保证了协议消息在网络上传输时不会遭受攻击，从而保证了 AM 中安全的协议转化为现实环境（UM）中具有同等安全性的协议。从本质上来说，CK 模型将攻击分为两大类，针对计算实体内部的攻击以及网络上的攻击.

可信网络连接架构中的网络访问层协议与传统的网络认证接入协议相同，它们具有相同的协议参与者、相同的链路环境以及相同的安全目标.

对于可信网络连接架构中的网络访问层协议，CK 模型中的三类内部攻击同样存在.

对于会话密钥查询来说，协议会话密钥的泄漏可能是密钥拥有者处理不当被攻击者获取，或攻击者通过密码分析的手段也可能造成会话密钥的暴露.

会话状态暴露查询用来暴露会话的状态信息，网络访问层模型中协议的会话状态与 CK 模型中定义的会话状态相同（如在 DH 交换中用于计算 g^x 的指数 x）。由于会话状态信息需要在内存中进行处理，即使会话状态信息存放于 TPM 内部，但由于 TPM 不能直接对这些状态信息进行处理，因此需要将会话状态信息读入内存中。这就有可能造成会话状态信息的泄露.

对于攻陷实体攻击，除了能够获取上述两种攻击所能获取的信息外，还能够获取实体的长期密钥。用户的长期密钥有可能是证书权威 CA 或密钥管理中心 KMC 生成的长期私钥，也可能是预共享的主密钥，这一信息在未存入 TPM 之前、或从 TPM 读入内存进行处理的过程中以及用户的处理不当都有可能被攻击者获取.

对于可信网络连接架构中的网络访问层协议，CK 模型中的外部攻击同样存在.

可信网络连接架构网络访问层采用传统网络连接技术（如 VPN，802.1x 等），可信计算技术没有对网络访问层用户之间的消息交互提供更多的安全保障。因此传统网络认证接入协议的漏洞，在可信网络连接架构网络访问层协议中同样存在.

结论 1 CK 模型可以作为可信网络连接架构网络访问层协议的分析与设计模型.

完整性评估层模型是可证明安全的可信网络连接协议模型的核心.

根据 CK 模型的设计思想，完整性评估层模型中包括两类攻击：平台内部攻击和网络攻击。完整性评估层协议完成平台身份认证和平台完整性校验，协议需要交互的秘密信息，以及有关平台身份和平台完整性的信息（包括签注密钥 EK[7]、认证身份密钥 AIK[7]、平台完整性度量值[7]等信息）在平台内部是安全的。在平台内部，这些秘密信息存放在 TPM 中的受保护区域，TPM 的安全存储特性保证了攻击者（包括非授权用户）无法从 TPM 中直接获取这些秘密信息。所以攻陷实体攻击在这一层不存在.

完整性评估层协议交互过程中的状态信息存放在 TPM 内部，协议交互过程中这些状态信息不读入内存，而是直接在 TPM 内部进行签名等操作，然后通过网络传送给通信平台。完整性评估层协议中的会话状态信息受 TPM 保护。因此，会话状态暴露攻击在这一层不会发生.

完整性评估层协议的目的是进行平台身份认证和平台完整性校验，平台之间并不协商会话密钥，因此会话密钥查询攻击在这一层没有意义.

结论 2 完整性评估层模型中不存在平台内部攻击.

CK 模型定义了认证链路模型 AM 和非认证链路模型 UM，分别用来表示协议的不同运行环境[15]。完整性评估层协议的运行环境与网络访问层协议的运行环境有所不同。完整性评估层协议是在网络访问层用户身份认证和密钥协商结束，并建立安全信道的基础上进行的，完整性评估层协议的消息交互借助网络访问层的安全信道进行传输。协议运行环境的差异，导致 CK 模型中的链路模型与完整性评估层协议模型的链路模型有着很大的差别。因此，我们给出了完整性评估层的链路模型：平台不可信链路模型（PUM）和平台可信链路模型

(PTM).

平台不可信链路模型（PUM）

平台不可信链路模型PUM定义了攻击者能力以及攻击者与协议的交互。图16总结了在存在PUM敌手的情况下协议的执行情况。考虑存在n个平台的消息驱动协议，其中用 $P_1...P_n$ 表示不同的平台。每个平台 P_i 都有输入 x_i 和 r_i。在这一环境下，存在一个PUM敌手 U 。PUM环境下协议 π 的运行包括不同平台之间的一系列协议 π 的激活行为，这些激活行为被敌手 U 控制和安排.

PUM 模型中协议的执行

参与方：平台 $P_1,...,P_n$ 分别以 $x_1,...,x_n$ 为输入执行n方协议 π ，敌手 U .

1) 初始化：网络访问层用户之间安全信道建立后，完整性评估层协议开始。每个平台 P_i 以本地输入 x_i 、秘密参数 k 和随机输入 r_i 调用协议 π .

2) 若敌手 U 没有终止，则执行以下操作：

敌手 U 可以激活一些平台 P_i 之间的协议 π ，这一激活过程可以有两种形式：

ⅰ. 激活请求 q ：这一激活来自平台内部的程序调用;

ⅱ. 输入消息 m ：这一激活来自网络中的另一个平台.

如果一个激活发生，那么被激活平台 P_i 执行它的程序并将产生的输出消息和激活请求提交给敌手 U （敌手 U 能够完全控制激活的顺序以及决定输入消息的值）。协议产生的本地输出不会被敌手 U 获取.

3) 协议执行的全局输出是敌手 U 和平台 $P_1,...,P_n$ 输出的级联组合.

图 16 平台不可信链路模型下协议的运行

在PUM环境下，虽然完整性评估层协议是在网络访问层安全信道基础上进行的，但由于网络访问层的安全信道是网络用户实体之间建立起来的，用户实体与实体所使用的平台之间并没有一种安全绑定的关系，即使平台之间的消息交互受网络访问层用户之间的安全信道的保护，同样不能保证协议免受网络攻击。因此，平台没有得到用户的授权而使用用户之间建立的安全信道是不安全的.

这一链路模型中的网络攻击者能够决定何时发送什么样的消息，可以修改消息或者任意插入自己产生的消息。在这一链路模型中，由结论2可知不存在平台内部攻击.

全局输出：在PUM中运行的协议的全局输出是协议参与平台 P_i 和敌手 U 的本地输出的级联。$PUM-ADV_{\pi,U}(k,\vec{x},\vec{r})$ 表示敌手 U 与协议参与平台交互的本地输出，其中k表示秘密参数， $\vec{x}=x_1...x_n$ 表示输入， $\vec{r}=r_0...r_n$ 表示随机输入（ r_0 给敌手 U ）。

$UNPTRUST_{\pi,U}(k,\vec{x},\vec{r})_i$ 表示平台 P_i 的本地输出的级联.

定义4 (PUM中协议运行的全局输出)

$$UNPTRUST_{\pi,U}(k,\vec{x},\vec{r}) = PUM-ADV_{\pi,U}(k,\vec{x},\vec{r}), UNPTRUST_{\pi,U}(k,\vec{x},\vec{r})_1 ... UNPTRUST_{\pi,U}(k,\vec{x},\vec{r})_n$$

平台可信链路模型（PTM）

在这一链路模型中，平台可以安全的使用网络访问层建立的安全信道，也就是说，在这一链路模型中，用户与平台之间存在安全绑定。这一环境中存在PTM敌手 T，与PUM敌手 U 不同，敌手 T 只能通过协议中的其它平台产生的输入消息来激活平台。PTM中的网络攻击者，只能够传递由参与者产生的真实消息，而且不能够改变或增添消息的内容。在这一链路模型中，由结论2可知不存在平台内部攻击.

PTM模型下全局输出的定义 $PTRUST_{\pi,T}$ 与PUM模型下 $UNPTRUST_{\pi,U}$ 的定义类似.

绑定器(Binder)

绑定器与CK模型中的认证器相仿，是一种特殊的算法，其作用类似于一个自动的编译器，它能够将PTM中的协议转化为PUM中一个安全性相同的等价协议.

定义5 设 π 和 π' 是n方消息驱动协议，π 运行在PTM中，π' 运行在PUM中。我们称 π' 在PUM中仿真（emulates）π，如果对于任何PUM对手U，存在一个PTM对手T使得

$$PTRUST_{\pi,T} \cong UNPTRUST_{\pi',U}$$

$\cong$ 表示计算上是不可区分的.

定义6 (编译器compiler) 编译器C是一个算法，它的输入和输出都是协议的描述.

定义7 (绑定器binder) 若编译器B对于PTM中的任何协议 π，协议B(π)可以在PUM中仿真 π，则称这个编译器为绑定器.

绑定器的设计和构造是模块化的，当协议需要增加新的安全属性时，只需要针对这一安全属性设计一个新的绑定器并证明其安全性，那么经过这一绑定器编译的协议就能够保证要求的安全属性。我们将设计一个绑定器，它能够实现用户与平台动态授权绑定.

绑定器 λ_{bind}： λ_{bind} 的构造基于公钥签名。网络访问层用户实体之间已经协商出了SK安全的会话密钥 k_{ij}。初始函数 I 进行密钥分配，假设 AIK_{priv_i} 和 AIK_{pub_i} 分别表示参与者 p_i 的AIK签名和验证密钥，其中 $I_0 = AIK_{pub_1} ... AIK_{pub_n}$ 为公开信息，发送给每个参与方 p_i，$I_i = AIK_{priv_i}$ 为 p_i 的私有信息。当完整性评估层平台 p_i 发送消息*m*给平台 p_j 的请求激活时，λ_{bind} 激活一个双方通信协议 $\hat{\lambda}_{bind}$，$\hat{\lambda}_{bind}$ 过程如下（既然 $\hat{\lambda}_{bind}$ 仅涉及两个平台，我们使用 p_A、p_B 代替 p_i、p_j）：

1) p_A 把消息 m 发送给 p_B；

2) p_B 收到来自 p_A 的消息 m 后，选择一个随机数 $N_B \xleftarrow{R} \{0,1\}^k$，把挑战 $\{m, N_B\}$ 发送给 p_A；

3) p_A 收到 p_B 的挑战后，计算 SIGN=$\{m, N_B, k_{AB}\}_{AIK_{\mathrm{Priv}_A}}$，把响应 m,SIGN 发送给 p_B；

4) p_B 收到 p_A 的响应后，验证 SIGN 和 k_{AB}，通过后接受 m.

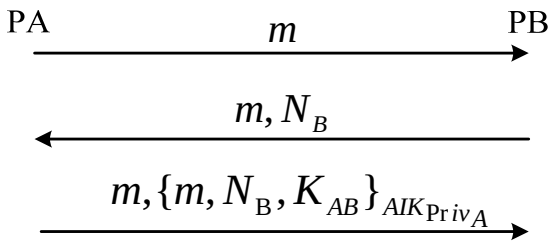


图 17 绑定器 λ_{bind}

定理1 若签名机制是选择消息攻击安全的，则协议 λ_{bind} 在PUM中仿真PTM中的消息传输协议.

证明：设U是一个和 λ_{bind} 交互的PUM对手，我们要构造一个PTM对手使 $PTRUST_{MT,T} \cong UNPTRUST_{\lambda_{bind},U}$，其中“≅”表示计算上是不可区分的.

运行U，U和n个运行 λ_{bind} 的参与者 $p_1', \cdots, p_n'$ 进行仿真的交互，T同时在PTM中和 $p_1, \cdots, p_n$ 交互（直观上，T在PTM中和 $p_1, \cdots, p_n$ 的交互作为 λ_{bind} 协议的上层协议），T按照以下规则进行：

1) 参与者 $p_1', \cdots, p_n'$ 拥有平台使用者之间的共享密钥；

2) 当 U 激活某个平台 p_i'，把消息 m 发送给参与者 p_j' 时，T 在 PTM 中激活 p_i 把消息 m 发送给 p_j；

3) U 继续与运行 λ_{bind} 的参与者 p_j' 交互；

4) 当 p_j' 输出 “p_j' received m from p_i'” 时，T 在 PTM 中用来自 p_i 的消息 m 激活 p_j；

5) U 所输出的就是 T 的输出.

从上面规则容易看出，除了第2条，T的行为是合法的PTM对手。在第2条规则中，(p_i, p_j, m) 可能没有在 p_i 的未送达消息队列中。当 p_j' 输出“p_j' received m from p_i'”，而 p_i 没有发送m给 p_j 或 p_j 以前已经收到过m，让 β 代表这个事件.

如果 β 没有出现，则A执行规则2时是合法的PTM对手行为。这时T在PTM中精确地模仿了U的运行，即 $PTRUST_{MT,T} = UNPTRUST_{\lambda_{bind},U}$，“＝”表示同一分布（identically distributed）.

如果 β 出现，我们说明其出现的概率是可忽略的，$PTRUST_{MT,T} \cong UNPTRUST_{\lambda_{bind},U}$。假设 β 出现的概率是 ε，ε 是不可忽略的，我们构造一个伪造器F以概率 ε / n 破坏签名机制.

构造 F：

如下定义F：F的输入是 N_B 和 K_{AB}。F可以访问SIGN Oracle S，它根据输入m，$N \neq N_B$ 且 $K \neq K_{AB}$ 计算输出 $\{m,N,K\}_{AIK_{\mathrm{Priv}_A}}$。若 $N = N_B$ 或 $K = K_{AB}$，$S(m,N,K) = \perp$.

F运行U，U和一组运行 λ_{bind} 的参与者进行如下仿真交互：

1) F 根据初始函数 I 给各个运行 λ_{bind} 的参与者分配密钥，除了随机选择的一对参与者 p_A、p_B，p_A 的验证密钥 AIK_{pub_i} 替换为 AIK_{pub^*} 发送给 p_B；
2) 对于不是 p_A 和 p_B 交互的消息，涉及的那些参与者按照 λ_{bind} 执行；
3) 设 L 是 p_B 从 p_A 收到的所有消息的集合，m^* 是在其中随机选择的一个消息；
4) 当 p_B 被来自 p_A 的消息 m 激活后,若 $m = m^*$，F 让 p_B 回应挑战 N_B；否则，随机选择 $N \xleftarrow{R} \{0,1\}^k$ 作为挑战；
5) 当 p_A 被来自 p_B 的挑战 N 激活时，若 $N \neq N_B$ 且 $K \neq K_{AB}$，计算输出 $\{m,N,K\}_{AIK_{\mathrm{Priv}_A}}$；若 $N = N_B$ 或 $K = K_{AB}$，F 询问它的 SIGN Oracle S 进行计算 $S(m,N,K) = \perp$，如果得到 $\perp$，仿真中止，F 失败.

从U看来，它和F的交互（在F没有中止仿真的情况下）与它和PUM中参与者的真实交互是没有区别的。假设 β^* 是指 β 出现在U和F的仿真交互的事件，这时参与者是 p_A，消息是 m^*。既然 p_A、p_B 和 m^* 都是随机选择的，若 β 出现的概率是 ε，则 β^* 出现的概率是 ε / n.

如果 β^* 出现，则 p_B 最后收到的消息是对（$\mathrm{m}^*, \mathrm{N_B}, K_{AB}$）的有效签名。从上述规则看出，$p_A$ 从来没有产生过这个签名。（若 p_A 没有被激活发送消息 m^*，很明显 p_A 不会产生这个签名；若 p_B 输出两次相同的值，但所有消息都应该是不同的，因此 p_A 只会发送消息 m^* 一次）。因此F不会访问他的 SIGN Oracle S进行这个签名。所以，F可以成功的攻破签名机制，这违反了签名机制的安全假设.

综上所述，β 出现的概率是可忽略的，因此 $PTRUST_{MT,T} \cong UNPTRUST_{\lambda_{bind},U}$.

定义8 如果协议能够满足下列三条性质，则我们称该协议是一个可信网络连接协议：

1) 网络访问层用户在 UM 环境下协商出 SK-Secure 的会话密钥，并建立用户之间的安全信道；
2) 网络访问层用户与完整性评估层平台之间存在动态授权绑定；

3) 完整性评估层平台之间的协议会话在 PUM 环境下是匹配会话.

5.4 一个可证明安全的可信网络连接协议

可信网络连接架构中网络访问层协议采用传统网络连接技术，文中不再考虑。我们通过本文提出的模型，将存在平台替换攻击的完整性报告协议[9]转换成安全的完整性评估层协议.

首先对完整性报告协议[9]进行形式化描述，将其转换成模型所能理解的形式并消除冗余的信息：

1) 通信用户双方预共享一个密钥 k_{ij}；

2) 发起方 p_i 收到建立会话 (p_i, p_j, s) 的请求后，选择随机数 $r_i \xleftarrow{R} \{0,1\}^k$，然后把消息 (p_i, s, r_i) 发送给 p_j；

3) 响应方 p_j 收到消息 (p_i, s, r_i) 后，计算 $t_j = sig\{PCR, nonce\}_{AIK\,priv}$，然后把消息 (p_j, s, t_j) 发送给 p_i；

4) p_i 收到消息 (p_j, s, t_j) 后，验证 t_j，验证通过做出接入判断.

显然，在平台可信链路模型（PTM）中，完整性报告协议[15]是一个安全协议。通过绑定器 λ_{bind}，我们将PTM中安全的完整性报告协议转变为PUM中安全性相同的等价协议。协议如图18所示.

1) 网络访问层用户之间共享 SK 安全的密钥 k_{ij}；

2) 发起方 p_j 收到建立会话 (p_j, p_i, s) 的请求后，选择随机数 $r_j \xleftarrow{R} \{0,1\}^k$，然后把消息 (p_j, s, r_j) 发送给 p_i；

3) 响应方 p_i 收到消息 (p_j, s, r_j) 后，选择随机数 $r_i \xleftarrow{R} \{0,1\}^k$，然后把消息 $(p_i, s, r_{j,} r_i)$ 发送给 p_j；

4) 发起方 p_j 收到消息 $(p_i, s, r_{j,} r_i)$ 后，计算 $t_j = sig\{PCR, nonce, k_{ij}\}_{AIK\,priv}$，然后把消息 (p_j, s, r_i, t_j) 发送给 p_i；

5) p_i 收到消息 (p_j, s, r_i, t_j) 后，验证 t_j，验证通过做出接入判断.

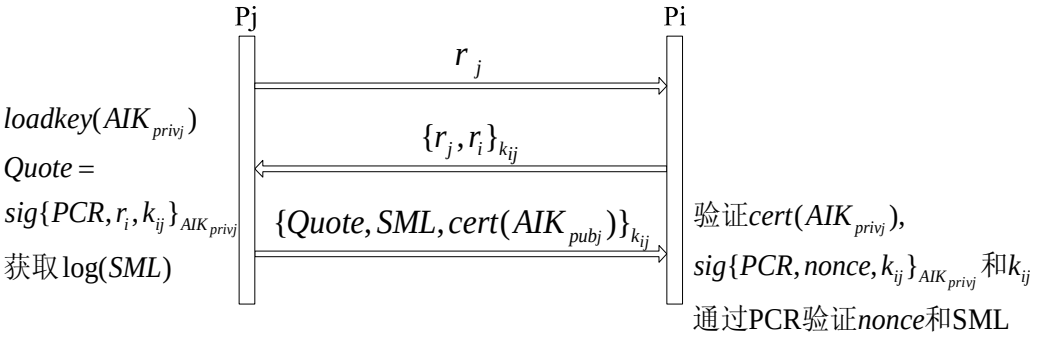


图 18 可证明安全的可信网络连接协议

5.5 结论与下一步工作

本文通过对TNC架构和完整性报告协议的深入分析，发现TNC架构存在安全缺陷，即网络访问层的用户和完整性评估层的平台之间不存在绑定关系，造成网络访问层建立的安全信道不能保护完整性评估层协议的交互。这一安全缺陷会引起一种新的攻击——平台替换攻击。为有效解决TNC架构安全缺陷造成的影响，我们形式化的提出了可信网络连接协议的安全目标。基于这一目标和CK模型的基本思想，本文对可信环境下的攻击者模型和链路模型进行了抽象，提出了一种可证明安全的可信网络连接协议模型TNC-PS。该模型在保持可信网络连接架构不变的前提下，通过其中的绑定器，可以建立用户与平台之间的动态绑定关系，使存在安全缺陷的完整性评估层协议转化为TNC-PS模型证明安全的协议，且协议能够达到可信网络连接协议的安全目标，有效解决了TNC架构的安全缺陷.

我们下一步的工作是：使绑定器带有隐私保护属性，以解决完整性评估层协议隐私保护的问题。另外，TNC-PS模型的设计基于CK模型的基本思想，并未考虑协议的并发组合情况。因此，我们将从协议组合理论角度出发，对模型进行进一步的完善，使它能够在更为复杂的并行环境下对可信网络连接协议进行设计和分析.

6 可信接入标准制定的工作设想

我国已经出台的国家“十一·五”规划和“863 计划”中，将把“可信计算”列入重点支持项目，并有较大规模的投入与扶植。2005 年 1 月全国信息安全标准化技术委员会在北京成立了 TC260 可信计算小组(WG1)。目前，国内兆日和联想已经生产出了符合 TCG 1.2 规范的 TPM 芯片，同时也已经开发出了相应的 PC 软硬件平台。同时瑞达等也开发了拥有自己独立知识产权的，类似 TCG 规范的可信计算产品。随着今后中国自己的可信计算标准的出台，可信计算技术将取得更大的发展[32]。

关于制定我国的可信计算标准应遵循的原则，沈院士[33]提到:“第一，要保障国家利益和安全，可信链是机器基于源头的第一道防御系统，密码体系以及认证体系应采用我国自己的标准；第二，从技术上来讲，密码技术在国内是完全独立自主的，必须遵循我国《商用密码管理条例》的有关规定，密码和认证保障体系要我们自己来建立；第三，要总结WAPI 的经验教训，不仅在技术上要自主创新，而且起步要早，并立足于国内首先执行，这样才能谈到与国际衔接问题。另外，可信计算平台的应用要满足各种层次的安全需求，也要实行产品分级。电子政务及一些敏感的关键行业，等级要求较高；面向个人、社会的可信计算标准则讲求通用性和自主性。当然，前提是必须使用国家主管部门批准的密码。”

今后我们在可信接入规范中的工作设想如下：

(1) TNC作为开放的、具有可伸缩性的可信接入安全体系架构，我们将以此为基础框架，融合现有的其他可信接入标准，制定自己的可信网络接入框架主规范，表述研究目标与动机、应用背景、基本架构与组件、接口与相关服务、其他安全与隐私问题等；

(2) 基于主规范，具体定义组件、接口和服务相应若干子规范，表述具体实现函数，参数定义、实现机制和支撑技术。

(3) 基于主规范，结合其他可信接入架构，给出和它们互操作的子规范，表述互操作的基本特征与意义、互操作基本架构和相关支撑技术。

(4) 制定可信网络接入的评估和认证规范。权威部门将依此来进行可信网络的测试、评估、认证和监管。

（5） 整个可信接入规范体系构成层次结构，从主规范制定入手，继而给出若干接口

和服务子规范、互操作子规范，最后制定评估与认证规范，作为完整规范体系的补充。

基于上述工作设想，我们将作以下工作计划安排：

第一阶段：全面深入地研究国内外现有的可信网络接入标准及规范（见第3、4节）。

第二阶段：融合现有的可信网络接入架构的本质特征，结合我实验室已有的研究工作背景和技术手段，提出自身的可信网络接入体系。

第三阶段：依据所提出的体系，从主规范入手，分期分批制定相关的全部可信接入体系标准。

第四阶段：利用该标准与已有的相关研究项目，研究具体的可信无线移动网络接入的实现机制和技术，并给出一个原形系统，进一步验证和测评标准的可行性和可操作性。

参考文献

[1] Stephen Mason. Trusted computing and forensic investigations. Digital Investigation [J].2005, 2, 189-192.

[2] Brian Berger.Trusted computing group history. Information Security Technical Report [J]. 2005, 10, 59-62.

[3] Ravi Sandhu, Kumar Ranganathan, Xinwen Zhang. Secure Information Sharing Enabled by Trusted Computing and PEI Model. Proc. of ASIACCS06, Mar., Taipei, Taiwan, 2006.

[4] Moti Yung. Trusted Computing Platforms: The Good, the Bad, and the Ugly. R.N. Wright (Ed.): FC 2003, LNCS 2742, pp. 250–254, 2003.

[5] Siani Pearson. Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy. P. Herrmann et al. (Eds.): iTrust 2005, LNCS 3477 pp. 305 – 320, 2005.

[6] Ravi Sandhu, Xinwen Zhang. Peer-to-Peer Access Control Architecture Using Trusted Computing Technology. Proc. of SACMAT05,Stockholm, Sweden, Jun,2005.

[7] Ravi Sandhu. Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way. In the Proc. of ACM Workshop on Role Based Access Control 2000, Berlin, Germany.

[8] TCG Specification Architecture Overview Revision 1.2, Trusted Computing Group, Apr, 2004, http://www.trustedcomputinggroup.org.

[9]张旻晋，桂文明，苏涤生等.从终端到网络的可信计算技术[R].中科院计算所信息技术快报（内刊），2006,4(2)：21-34。

[10] TCG Specification Trusted Network Connect TNC Architecture for Interoperability Revision 1.1, Trusted Computing Group, May, 2006, http://www.trustedcomputinggroup.org.

[11] Vijay Varadharajan. Trustworthy Computing. X. Zhou et al. (Eds.): WISE 2004, LNCS 3306, pp. 13–16, 2004.

[12] Shane Balfe, Amit D. Lakhani and Kenneth G. Paterson. Trusted Computing: Providing Security for Peer-to-Peer Networks. Proceedings of the Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05).

[13] Ravi Sandhu, Xinwen Zhang, Kumar Ranganatham,et.al. Client-side access control enforcement using trusted computing and PEI models.Journal of High Speed Network, 2006(15), pp. 229-245.

[14] Liqun Chen, Rainer Landfermann, Hans L¨ohr. A Protocol for Property-Based Attestation [C]. *STC'06,* November 3, 2006, Alexandria, Virginia, USA.

[15] Ernie Brickell, Jan Camenisch, Liqun Chen. Direct Anonymous Attestation[C]. *CCS'04*, October 2529, 2004, Washington, DC, USA.

[16] Zheng Yan. A Conceptual Architecture of a Trusted Mobile Environment. Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06)

[17] John S. Erickson. FAIR USE, DRM, AND TRUSTED COMPUTING [J]. COMMUNICATIONS OF THE ACM, 2003, 46 (4).
[26-18] Munindar P. Singh. Trustworthy Service Composition: Challenges and Research Questions. R. Falcone et al. (Eds.): AAMAS 2002 Ws Trust, Reputation..., LNAI 2631, pp. 39–52, 2003.
[19] *Yu Zheng, Dake He, Weichi Yu and Xiaohu Tang.* Trusted Computing-Based Security Architecture For 4G Mobile Networks. Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'05).
[20] 郑宇，何大可，何明星. 基于可信计算的移动终端用户认证方案[J]. 计算机学报，2006, 29(8):1255-1264.
[21] 林闯, 任丰原. 可控可信可扩展的新一代互联[J]. 软件学报，2004, 15(12): 1815-1821.
[22] 林闯, 彭雪海. 可信网络研究[J]. 计算机学报，2005，28（5）：751-758.
[23] 闵应骅. 可信系统与网络[J]. 计算机工程与科学, 2001, 23(5):21-23.
[24] 闵应骅. 容错计算二十五年[J]. 计算机学报, 1995, 18(12):930-943.
[25] 闵应骅. 网络容错与安全研究述评. 计算机学报，2003，26（9）：1035-1041.
[26] Boris Balacheff, Liqun Chen, Siani Pearson et.al. Trusted Computing Platforms: TCPA Technology in Context[M]. Prentice Hall Press, Jul, 2002.
[27] Trusted Computing and Digital Rights Management Principles & Policies. State Services Commission. 2006, 9.
[28] Shane Balfe, Liqun Shen. Pervasive Trusted Computing. Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06).
[29] Cisco Network Admission Control [S]. Cisco Company, 2006, http://www.cisco.com/en/US/netsol/ns617/
[30]Network Access Protection Platform Architecture[S], Microsoft Corporation, 2006, 12, *http://www.microsoft.com/technet/network/nap/*
[31]李鸿培.可信网络架构概述[R].北京天融信公司，2005, 11.
[32]冯登国.国内外信息安全技术研究现状及发展趋势[R].2005年中国计算机科学技术发展报告,2006.
[33]沈昌祥. 坚持自主创新, 加速发展可信计算[J]. 计算机安全，2006，6：1-4+17.