# 可证明安全的可信网络连接协议模型

马 卓[1) ] 马建峰[1),2)] 李兴华[1)] 姜 奇[1)]

[1)](西安电子科技大学计算机学院 西安 710071)

[2)](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 西安 710071)

**摘 要** 该文作者发现可信计算组织 TCG 提出的可信网络连接架构存在安全缺陷,攻击者利用这一缺陷可以发起一种平台替换攻击,攻击将导致可信网络连接过程中平台身份认证的失败和平台完整性校验错误.针对这一情况,文中形式化地给出了可信网络连接协议的安全目标.在此基础之上,为了使协议的设计和分析更具一般性和安全性,提出一种可证明安全的可信网络连接协议模型(TNC-PS),通过模型中的绑定器,可将理想环境下设计的完整性评估层协议,转化为实际环境下安全性相同的等价协议.从而在保持可信网络连接架构不变的基础上,避免其安全缺陷造成的影响.最后,利用 TNC-PS 模型设计了一个完整性评估层协议,该协议能够满足可信网络连接协议的安全目标.

**关键词** 可信网络连接;平台替换攻击;可证明安全模型;绑定器

**中图法分类号** TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01669

## Provable Security Model for Trusted Network Connect Protocol

MA Zhuo[1)] MA Jian-Feng[1),2)] LI Xing-Hua[1)] JIANG Qi[1)]

[1)](*School of Computer Science & Technology, Xidian University, Xi'an* 710071)

[2)](*Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an* 710071)

**Abstract** A platform substitution attack on the trusted network connect protocol is founded in this paper, which will cause the failure of platform authentication and the error of platform integrity verification. To solve this problem, this paper proposes the security objectives of the trusted network connect protocol formally, and a provable security model TNC-PS for the trusted network connect protocol. In particular, it is show that how to systematically transform protocols working in idealized communications into those which are secure in the realistic communication channels, by using the binder presented in the model. By the TNC-PS model, security flaw is avoided with the TNC architecture keeping unchanged. Finally, this paper proposes an integrity evaluation layer protocol designed by using the TNC-PS model, which satisfies the security objectives of the trusted network connect protocol.

**Keywords** trusted network connect; platform substitution attack; provable security model; binder

## 1 引 言

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

收稿日期:2008-08-20;最终修改稿收到日期:2011-03-15.本课题得到国家自然科学基金项目(60872041,61072066,61100233)、中央高校基本科研业务费专项资金项目(JY10000903001、K50510030010)资助.**马 卓**,男,1980 年生,博士,讲师,主要研究方向为网络与信息安全.E-mail: mazhuo@mail.xidian.edu.cn.**马建峰**,男,1963 年生,博士,教授,博士生导师,主要研究领域为计算机安全、密码学.**李兴华**,男,1978 年生,博士,副教授,主要研究方向为安全协议.**姜 奇**,男,1983 年生,博士,讲师,主要研究方向为无线网络安全等.

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[1-5]. 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[6]、可信存储[7]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[8]，它本质上就是要从终端的完整性开始，建立连接. 在传统网络接入认证基础上，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[9-13].

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[13]，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协议接入架构基础上提出的，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[14]的基本思想，结合 TNC 架构的具体规范[8]，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的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.

本文第 2 节对背景知识进行介绍，包括可信网络连接 TNC、CK 模型；第 3 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 4 节给出可证明安全的可信网络连接协议模型 TNC-PS，并形式化地定义可信网络连接协议；第 5 节利用 TNC-PS 模型设计一个满足可信网络连接安全目标的完整性评估层协议；最后一节对全文进行总结并给出下一步的工作.

## 2 预备知识

### 2.1 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. 即在传统网络接入认证基础上，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)[8]架构如图 1 所示，包含 3 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.

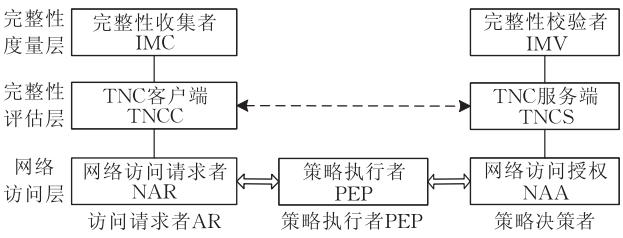



图 1 可信网络连接 TNC 架构

TNC 架构在纵向从下到上分为 3 个层次.

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.

### 2.2 Canetti-Krawczyk 模型

CK(Canetti-Krawczyk)模型是用于形式化分析密钥交换协议的工具[14]. 该模型给出了会话密钥安全的定义和利用该定义证明认证和密钥交换协议安全性的模块化方法. CK 模型的主要目标是，通过模块化的方法来设计和分析认证和密钥交换协议，以简化协议的安全设计与安全性分析. CK 模型有 3 个重要的组成部分：非认证链路模型(UM)、认证链路模型(AM)和认证器(authenticator).

(1) 非认证链路模型(UM)

非认证链路模型(UM)中的攻击者除了能够控制通信链路和协议事件的调度外，还能够通过明确的攻击手段得到协议参与者存储器中的秘密信息. 为了区分各种攻击，确保信息在被暴露情况下最大限度的安全，根据攻击者能够得到信息的实际情况，CK 模型将攻击分为 3 类：攻陷参与者(Party corruption)、会话密钥查询(Session-key query)和会话状态暴露(Session-state reveal).

(2) 认证链路模型(AM)

AM 的定义方式和 UM 的基本相同，一个根本不同之处在于，AM 中的攻击者只能够传递由参与者产生的真实消息，而不能够改变或增添消息的内容.

**定义 1**(认证器 authenticator)[15-16]. 认证器是一种特殊的算法，其作用类似于一个自动的编译器，它能够将 AM 中的协议转化为 UM 中一个安全性相同的等价协议.

(3) 会话密钥安全(*SK-secure*)

**定义 2**(测试会话查询 test-session query)[14]. 针对密钥交换协议的对手 $U$ 可以在它运行的任何时刻，从那些完成的、没过期的、没暴露的会话中选择一个测试会话(test-session). 设 $K$ 是测试会话的会话密钥，当 $U$ 对测试会话查询时，掷币 $b$，$b \xleftarrow{R} \{0,1\}$. 若 $b=0$，把 $K$ 给 $U$；否则，从协议产生的密钥的概率分布空间随机选择一个值 $r$ 给 $U$. 除了在测试会话过期前不允许使测试会话暴露外，$U$ 可以继续进行各种活动. 最后，$U$ 输出一个比特 $b_0$，作为 $b$ 的猜测.

**定义 3**(KE 对手)[14]. 被允许执行测试会话查询的密钥交换协议对手是 KE 对手.

**定义 4**(会话密钥安全 SK-secure)[14]. 如果对于 UM 中任何 KE 对手 $U$，协议能够满足下列两条性质，则我们称该协议在 UM 中是会话密钥安全的：

① 如果两个未被攻陷的参与者完成了匹配的会话. 它们将输出相同的会话密钥；

② $U$ 进行测试会话查询，它猜中 $b$ 的概率不超过 $0.5+\varepsilon$，其中 $\varepsilon$ 为安全参数下可忽略的概率.

如果上述性质对于任何 AM 中的 KE 对手是满足的，则协议在 AM 中是会话密钥安全的.

## 3 平台替换攻击及其分析

### 3.1 完整性报告协议

完整性报告协议[13]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[17]. 如图 2 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，$AIK_{\text{priv}}$ 和 $AIK_{\text{pub}}$ 为证明身份密钥对[6]，$loadkey(AIK_{\text{priv}})$ 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 $AIK_{\text{priv}}$，*SML* 为存储测量日志[8]，$cert(AIK_{\text{pub}})$ 为 Privacy CA 向平台签发的 AIK 证书，$Sig\{PCR,nonce\}_{AIK_{\text{priv}}}$ 表示以 $AIK_{\text{priv}}$ 为私钥将选择的 *PCR* 值和收到的随机数 *nonce* 进行签名.

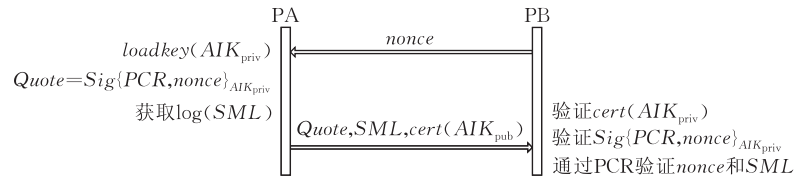



图 2　完整性报告协议

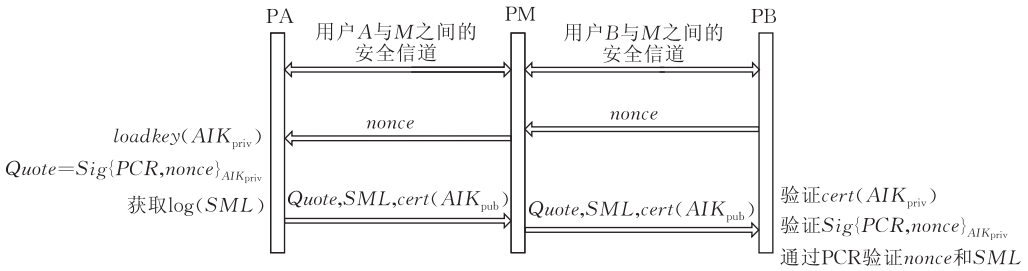
我们发现，上述协议容易遭受一种新的攻击——平台替换攻击. 可信网络连接架构中完整性评估层的目的是验证接入平台的身份和平台完整性，这一攻击将导致平台身份认证的失败以及平台完整性校验错误，造成可信网络连接的安全目标不能达到.

### 3.2 平台替换攻击

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 3 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 3.1 节协议规定，使用存储根密钥从 TPM 中读取证明身份密钥 $AIK_{\text{priv}}$，并以 $AIK_{\text{priv}}$ 为私钥将选择的 *PCR* 值和收到的随机数 *nonce* 进行签名 $Sig\{PCR,nonce\}_{AIK_{\text{priv}}}$，然后将签名消息连同存储测量日志 SML 和 AIK 证书 $cert(AIK_{\text{pub}})$ 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 3.1 节协议中 PB 的验证过程相同.

图 3 平台替换攻击

攻击中，平台 PM 成功地说服平台 PA 对平台 PB 的一次性随机数进行签名，并进而允许平台 PM 成功地欺骗平台 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.

### 3.3 平台替换攻击产生的原因及 TNC 架构的安全缺陷

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[6]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[8]，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.

## 4 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[18]，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[14]、UC 模型[19]、PCL 模型[20]等）在网络接入认证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[19]构造的.

可信网络连接协议与传统网络接入认证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 模型的基本思想，给出一种可证明安全的可信网络连接协议模型.

### 4.1　可信网络连接协议的安全目标

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[22]，802.1x[23]等），完整性评估层协议在底层安全信道保护下进行.因此，可信网络连接协议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，即要求用户所使用的平台之间进行平台身份认证和平台完整性校验.这是可信网络连接协议的又一安全目标.

**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.

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 3.2 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 5**（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.**　用户与平台之间存在动态授权绑定关系.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地使用用户之间建立的安全信道.

### 4.2　基于 CK 模型的可证明安全的可信网络连接协议模型

可信网络连接架构包括相互关联的两个过程[8]：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，并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.

#### 4.2.1　网络访问层模型

CK 模型是一种模块化的协议设计方法，它具有 3 类攻击者模型[14]：攻陷参与者、会话密钥查询及会话状态暴露.这 3 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[15-16]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接入认证协议相同，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 3 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.因此传统网络接入认证协议的漏洞,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.

4.2.2 完整性评估层模型

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[6]、认证身份密钥 AIK[6]、平台完整性度量值[6]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[14].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).

4.2.2.1 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 4 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 $P_1 \cdots P_n$ 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 $\pi$ 的运行包括不同平台之间的一系列协议 $\pi$ 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 $P_1 \cdots P_n$ 分别以 $x_1 \cdots x_n$ 为输入执行 $n$ 方协议 $\pi$,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 $\pi$.
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 $\pi$,这一激活过程可以有两种形式:

   i. 激活请求 $\boldsymbol{q}$:这一激活来自平台内部的程序调用;

   ii. 输入消息 $\boldsymbol{m}$: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 $P_1 \cdots P_n$ 输出的级联组合.

图 4 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.网络访问层用户之间的安全信道不能保护平台之间的消息交互,同样不能保证完整性评估层协议免受网络攻击.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.$PUM-ADV_{\pi,U}(k,\boldsymbol{x},\boldsymbol{r})$ 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,$\boldsymbol{x}=x_1 \cdots x_n$ 表示输入,$\boldsymbol{r}=r_0 \cdots r_n$ 表示随机输入($r_0$ 给敌手 $U$).$UNPTRUST_{\pi,U}(k,\boldsymbol{x},\boldsymbol{r})_i$ 表示平台 $P_i$ 的本地输出的级联.

**定义 6**(PUM 中协议运行的全局输出).

$UNPTRUST_{\pi,U}(k,\boldsymbol{x},\boldsymbol{r})=PUM-ADV_{\pi,U}(k,\boldsymbol{x},\boldsymbol{r})$,

$UNPTRUST_{\pi,U}(k,\boldsymbol{x},\boldsymbol{r})_1,\cdots,UNPTRUST_{\pi,U}(k,\boldsymbol{x},\boldsymbol{r})_n$.

4.2.2.2　平台可信链路模型(PTM)

在这一链路模型中，平台可以安全地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 7.**　设 $\pi$ 和 $\pi'$ 是 $n$ 方消息驱动协议，$\pi$ 运行在 PTM 中，$\pi'$ 运行在 PUM 中. 我们称 $\pi'$ 在 PUM 中仿真(emulates)$\pi$，如果对于任何 PUM 对手 $U$，存在一个 PTM 对手 $T$ 使得

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

式中$\cong$表示计算上是不可区分的.

**定义 8**(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 9**(绑定器 binder).　若编译器 $C$ 对于 PTM 中的任何协议 $\pi$，协议 $C(\pi)$ 可以在 PUM 中仿真 $\pi$，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 $\lambda_{\text{bind}}$.**

$\lambda_{\text{bind}}$ 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 $AIK_{\text{priv}i}$ 和 $AIK_{\text{pub}i}$ 分别表示参与者 $p_i$ 的 AIK 签名和验证密钥，其中 $I_0 = AIK_{\text{pub}1} \cdots AIK_{\text{pub}n}$ 为公开信息，发送给每个参与方 $p_i$，$I_i = AIK_{\text{priv}i}$ 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 $p_j$ 的请求被激活时，$\lambda_{\text{bind}}$ 激活一个双方通信协议 $\hat{\lambda}_{\text{bind}}$，$\hat{\lambda}_{\text{bind}}$ 过程如下(既然 $\hat{\lambda}_{\text{bind}}$ 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 $SIGN = \{m, N_B, k_{AB}\}_{AIK_{\text{priv}A}}$，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 $m$.

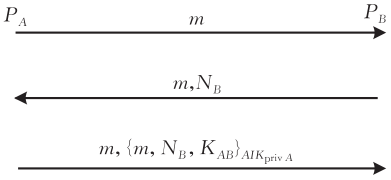



图 5　绑定器 $\lambda_{\text{bind}}$

**定理 1.**　如果签名算法可抵抗选择消息攻击，则完整性报告协议[13]在 PTM 中是安全的. 则协议 $\lambda_{\text{bind}}$ 在 PUM 中仿真 PTM 中的消息传输协议.

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

运行 $U$，$U$ 和 $n$ 个运行 $\lambda_{\text{bind}}$ 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 $\lambda_{\text{bind}}$ 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 $\lambda_{\text{bind}}$ 的参与者 $p'_j$ 交互；

(4) 当 $p'_j$ 输出“$p'_j$ 收到 $p'_i$ 发来的消息 $m$”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 条规则外，$T$ 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“$p'_j$ 收到 $p'_i$ 发来的消息 $m$”，而 $p_i$ 没有发送 $m$ 给 $p_j$ 或 $p_j$ 以前已经收到过 $m$，让 $\beta$ 代表这个事件.

如果 $\beta$ 没有出现，则 $T$ 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 $PTRUST_{MT,T} = UNPTRUST_{\lambda_{\text{bind}},U}$，“$=$”表示同一分布(identically distributed).

如果 $\beta$ 出现，我们可说明其出现的概率是可忽略的，$PTRUST_{MT,T} \cong UNPTRUST_{\lambda_{\text{bind}},U}$. 假设 $\beta$ 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$\varepsilon/n$破坏签名机制.

**伪造器 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$\{m,N,K\}_{AIK_{\text{priv}A}}$.若$N=N_B$或$K=K_{AB}$,$S(m,N,K)=\perp$.

F运行U,U和一组运行$\lambda_{\text{bind}}$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$\lambda_{\text{bind}}$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$AIK_{\text{pub}i}$替换为$AIK_{\text{pub}^*}$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$\lambda_{\text{bind}}$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$\{m,N,K\}_{AIK_{\text{priv}A}}$;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$\beta^*$是指$\beta$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$\beta$出现的概率是ε,则$\beta^*$出现的概率是$\varepsilon/n$.

如果$\beta^*$出现,则$p_B$最后收到的消息是对$(m^*,N_B,K_{AB})$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,$\beta$出现的概率是可忽略的,因此$PTRUST_{MT,T}\cong UNPTRUST_{\lambda_{\text{bind}},U}$. 证毕.

### 4.3 可信网络连接的定义

**定义 10.** 如果协议能够满足下列3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 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[13]转换成安全的完整性评估层协议.

首先对完整性报告协议进行形式化描述,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$t_j=sig\{PCR,r_i\}_{AIK_{\text{priv}j}}$,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.

通过绑定器$\lambda_{\text{bind}}$,将完整性报告协议编译为协议PSTNCP,如图6所示.与完整性报告协议不同,该协议通过两个随机数,保证协议参与双方的消息新鲜性,同时利用网络访问层协商的共享密钥,对完整性评估层协议消息进行加密,实现用户与平台之间的安全绑定.

(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$t_j=sig\{PCR,r_i,k_{ij}\}_{AIK_{\text{priv}j}}$,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.

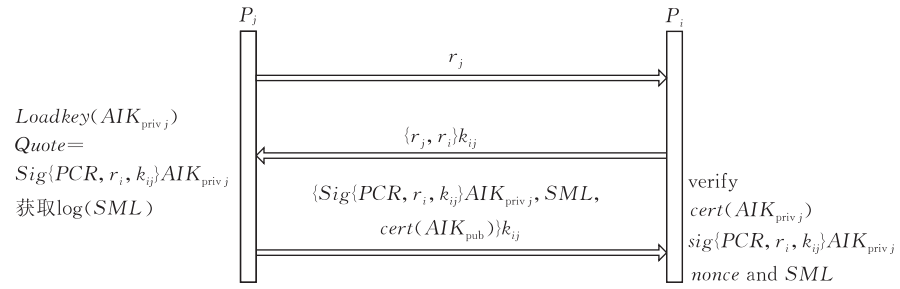



图 6　可证明安全的可信网络连接协议 PSTNCP

**定理 2.**　如果签名算法可抵抗选择消息攻击，则完整性报告协议[13]在 PTM 中是安全的.

证明.　在 PTM 环境下平台可以安全的使用网络访问层建立的安全信道，用户与平台之间存在安全绑定.因此，可抵抗选择消息攻击的 AIK 签名能够保证完整性报告协议在该环境下的安全性.　　证毕.

**定理 3.**　如果签名算法可抵抗选择消息攻击，则协议 PSTNCP 在 PUM 中是安全的.

证明.　由定义 7、定理 1 和定理 2，可直接推出结论.　　证毕.

## 6　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.

## 参　考　文　献

[1] Shen Chang-Xiang, Zhang Huan-Guo, Feng Deng-Guo et al. Survey of information security. Science in China Series F, 2007, 50(3): 273-298(in Chinese)
(沈昌祥，张焕国，冯登国等. 信息安全综述. 中国科学 E 辑，2007，37(2)：129-150)

[2] Zhang Huan-Guo, Luo Jie, Jin Gang et al. Development of trusted computing research. Journal of Wuhan University (Natural Science Edition), 2006, 52(5): 513-518(in Chinese)
(张焕国，罗捷，金刚等. 可信计算研究进展. 武汉大学学报(理学版)，2006，52(5)：513-518)

[3] Sailer R, Jaeger T, Zhang X L et al. Attestation-based policy enforcement for remote access//Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04). New York: ACM, 2004: 308-317

[4] Pearson S. Trusted computing: Strengths, weaknesses and further opportunities for enhancing privacy//Herrmann et al. eds. Proceedings of the iTrust' 2005. LNCS 3477. Berlin: Springer-Verlag, 2005: 305-320

[5] Hilley S. Trusted computing-path to security or road to servitude? Infosecurity Today, 2004, 1(4): 18-21

[6] Trusted Computing Group. Trusted Platform Module Main Specification, Part1: Design Principles, Part 2: TPM Structures, Part3: Commands, Specification Version 1.2, Revision 94. 2005

[7] Trusted Computing Group. TCG Storage Architecture Core Specification Version 1.2. 2007

[8] Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability Specification Version 1.2. 2007

[9] Shen Chang-Xiang. Network credit and public key authentication. Electronic Commerce, 2006, 3: 58-64(in Chinese)
(沈昌祥. 网络信任与公钥认证. 电子商务，2006，3：58-64)

[10] Zheng Yu, He Da-Ke, He Ming-Xing. Trusted computing based user authentication scheme for mobile equipment. Chinese Journal of Computers, 2006, 29(8): 1255-1264(in Chinese)
(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. 计算机学报，2006，29(8)：1255-1264)

[11] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-

758(in Chinese)
(林闯，彭雪海. 可信网络研究. 计算机学报，2005，28(5)：751-758)

[12] Goldman K，Perez R，Sailer R. Linking remote attestation to secure tunnel endpoints//Proceedings of the 1st ACM Workshop on Scalable Trusted Computing. Virginia，2006：21-24

[13] Sailer R，Zhang X L，Jaeger T et al. Design and implementation of a TCG-based integrity measurement architecture//Proceedings of the 13th Conference on USENIX Security Symposium(SSYM'04). California，2004：223-238

[14] Canetti R，Krawczyk H. Analysis of key exchange protocols and their use for building secure channels//Pfitzmann B ed. Advancesin Cryptology-Eurocrypt 2001. LNCS 2045. Berlin：Springer-Verlag，2001：453-474

[15] Bellare M，Canetti R，Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols//Proceedings of the 30th Annual Symposium on the Theory of Computing. New York，1998：419-428

[16] Bellare M，Rogaway P. Entity authentication and key distribution//Stinson D R eds. Proceedings of the Advances in Cryptology(Crypto'93). LNCS 773. Berlin：Springer-Verlag，1993：232-249

[17] Bellovin S M，Merritt M. Encrypted key exchange：Password-based protocols secure against dictionary attacks//Proceedings of the IEEE Symposium on Security and Privacy (SP'92). California，1992：72-84

[18] Mao W B. Modern Cryptography：Theory and Practice. NJ：Prentice-Hall PTR，2004

[19] Canetti R. Universally composable security：A new paradigm for cryptographic protocols//Proceedings of the 42nd IEEE Annual Symposium on Foundations of Computer Science. Oakland，2001：136-145

[20] Datta A，Derek A，Mitchell J C et al. Secure protocol composition//Proceedings of the 2003 ACM Workshop on Formal Methods in Security Engineering (FMSE'03). New York，2003：11-23

[21] Dolev D，YAO A C. On the security of public key protocols. IEEE Transactions on Information Theory，1983，29(2)：198-208

[22] Cohen R. On the establishment of an access VPN in broadband access networks. IEEE Communications Magazine，2003，41(2)：156-163

[23] IEEE. IEEE Standards for Local and metropolitan area networks. Port based Network Access Control. 802.1X-REV，Draft 11. 2004

**MA Zhuo**，born in 1980，Ph. D.，lecturer. His research interests include network and information security.

**MA Jian-Feng**，born in 1963，Ph. D.，professor，Ph. D. supervisor. His research interests include computer security and cryptography.

**LI Xing-Hua**，born in 1978，Ph. D.，associate professor. His research interest is security protocols.

**JIANG Qi**，born in 1983，Ph. D.，lecturer. His research interests include wireless network security.

**Background**

This research is supported by the National Natural Science Foundation of China under grant Nos. 60872041，61072066，61100233，the Fundamental Research Funds for the Central Universities under grant Nos. JY10000903001，K50510030010.

Through the practice of information security，people have realized that the causation of security troubles comes from network terminals. To ensure the source security of the network terminals，the solution must comprehensively consider chips，hardware architecture，and operating system，etc.，and the original idea of trusted computing comes into being. Trusted Network Connect Group (TNC-SG)，a TNC Sub Group，has developed trusted network connect (TNC) architecture based on the trusted computing technology，which，in essence，establishes connections from the terminal integrity. The researchers have carried out a great deal of researches on the TNC architecture and the protocols based on it. An integrity reporting protocol was proposed，running in the integrity evaluation layer of the TNC architecture. According to the protocol，the platform authentication and the platform integrity verification were realized in the integrity evaluation layer.

This paper analyzes the TNC architecture and integrity reporting protocol，and a platform substitution attack on the trusted network connect protocol is pointed out，which can cause the failure of platform authentication and platform integrity verification. That is，there is no security binding relationships between the user and their platform. The security flaw will result in the loophole of the integrity evaluation protocols based on the TNC architecture. Therefore，TNC protocols should be designed to avoid the loophole. For designing and analyzing the protocols more securely and universally，the security objectives of the trusted network connect protocol were formally specified，and a provable security model TNC-PS for the trusted network connect protocol was proposed. In particular，based on this model，we show how to systematically transform protocols working in the idealized communication channel into ones working in the realistic communication channel，by using the binder presented in the model. By the TNC-PS model，the security flaw is avoided while the TNC architecture keeping unchanged. An integrity evaluation layer protocol which satisfies the security objectives of the trusted network connect protocol was designed.