一种抵御中间人攻击的可信网络连接协议

赵 波[1),2)] 向 程[1),2),3)] 张焕国[1),2)]

[1)](武汉大学国家网络安全学院 武汉 430072)

[2)](空天信息安全与可信计算教育部重点实验室 武汉 430072)

[3)](96833 部队 湖南 怀化 418000)

摘 要 可信计算组织 TCG 提出的可信网络连接 TNC 可以很好地解决网络接入过程中的安全威胁.但由于 TNC 网络访问层和完整性评估层之间没有绑定关系,平台完整性信息可以被冒用,容易遭受中间人攻击,导致不合法的终端接入网络.为解决这一问题,我们设计了一种抵御中间人攻击的可信网络连接协议 S-TNC(Safe-TNC),在完整性评估层基于 TPM 协商一个秘密密钥,将其与平台完整性报告绑定,再由这个秘密密钥直接导出会话密钥,用于通信对端之间数据通信的保护,实现认证对端和通信对端的密码学绑定,抵御中间人攻击.经 BAN 逻辑形式化分析和实验测试,该协议本身没有发现安全缺陷,可以抵御中间人攻击.与现有方案相比,该协议不额外增加实体和证书,密钥受 TPM 保护,具有简单安全的特点.

关键词 可信计算;可信网络;可信网络连接;中间人攻击;平台信息冒用;秘密密钥生成

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.01137

A Trusted Network Connect Protocol for Resisting Man-in-the-Middle Attack

ZHAO Bo[1),2)] XIANG Cheng[1),2),3)] ZHANG Huan-Guo[1),2)]

[1)](*School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072)

[2)](*Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Wuhan* 430072)

[3)](96833 *Troops, Huaihua, Hunan* 418000)

Abstract Trusted Computing Organization (TCG) proposes the Trusted Network Connection (TNC) to solve the threats and problems in network access. However, due to the TNC architecture design features, it is vulnerable to man-in-the-middle attack, which can lead to illegal access, service interruption, sensitive information leakage and other security issues. By in-depth study of the attack process, the crux of the problem is found. Because there is no binding relationship between the network access layer and the integrity evaluation layer, valid authentication between the Access Requestor (AR) and the Policy Decision Point (PDP) is lacking. Attacker can use a legal terminal's platform integrity information by passing the TNC request and reply message in the middle. It impersonates a legal terminal to get access to network illegally. To solve this problem, this paper designs an improved protocol S-TNC (Safe TNC). According to S-TNC, a secret is negotiated in integrity evaluation layer between AR and PDP. Firstly, AR generates a pair of Bind Key (BK) based on Trusted Platform Module (TPM) and signs it with Attestation Identity Key (AIK) to prove that the BK belongs to AR's platform. Secondly, PDP generates a secret and send it to AR protected by BK. Thirdly, AR uses the secret as the externalData parameter of TPM_Quote command to generate the platform integrity report, so it is bound with the platform

收稿日期:2017-06-07;在线出版日期:2019-02-18.本课题得到国家"九七三"重点基础研究发展规划项目(2014CB340600)、国家"八六三"高技术研究发展计划项目(2015AA016002)、国家自然科学基金重点项目(61332019)、武汉市应用基础前沿项目(2018010401011295)资助.**赵 波**,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为信息安全、嵌入式系统、可信计算.E-mail:zhaobowhu@163.com.**向 程**,硕士研究生,主要研究领域为可信计算.**张焕国**,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为信息安全、密码学、可信计算.

integrity report. Finally, after verifying the integrity of AR's platform, PDP and AR both believe that the secret is only known to them, and they derive a session key using the same key generation algorithm based on the secret to protect the subsequent communication. So a cryptography bound between the authentication peers and the communication peers is achieved to resist man-in-the-middle attack. For S-TNC, the secret is the key thing to resist man-in-the-middle. The secret is generated based on AIK authentication and protected by TPM. It has a natural binding relationship with the platform. Any middleman can not acquire and forge the secret. Therefore, it is not possible to generate a valid session key, and illegal access is denied. S-TNC is implemented in the integrity evaluation layer, transparent to the network access layer and integrity collection layer. S-TNC does not change the original architecture of TNC and inherits the security features described in the TNC standard. BAN logic is a widely used formal analysis method for authentication protocols. It is used to analyze S-TNC to reveal some defects that are hard to find. After strict reasoning, S-TNC is proved to be safe and correct. An experimental system is built to test the feasibility, resistance to man-in-the-middle attack and system performance of the S-TNC. The tests prove that the S-TNC has reached the intended safety target. Compared with the existing methods, S-TNC does not increase the complexity of the system for no additional entities and certificates are added. Security is enhanced for the keys are protected by TPM hardware. It is simple and safe.

Keywords trusted computing; trusted network; trusted network connect; man-in-the-middle attack; fraudulent use of platform information; secret key generation

1 引 言

随着计算机网络的不断发展,网络安全问题愈演愈烈,传统防御手段显示出了局限和劣势.现在人们已经意识到,在面对网络安全威胁时,不仅要分别考虑终端和网络的安全,而且要将二者联动考虑,将终端的安全状态延伸到网络,让整个网络变得安全可信.可信计算[1-3]技术的出现和发展,为解决现有问题开辟了新的道路.它基于可信平台模块 TPM(Trusted Platform Module)[4]从底层硬件到操作系统和应用软件建立起一个可信的终端计算环境,再利用可信网络连接技术 TNC(Trusted Network Connect)[5-6]将可信的终端接入网络,从而保证整个网络的可信.

2004 年 5 月可信计算组织 TCG(Trusted Computing Group)成立了可信网络连接分组 TNC-SG(Trusted Network Connect Sub Group),现在是可信网络连接工作组(TNC-WG).他们主要研究可信网络连接 TNC 框架、制定标准规范.经过多年的发展,形成了比较完善的体系架构.可信网络连接旨在将终端的可信延伸到网络,从而确保网络连接的可信.TNC 把终端平台身份检查和平台完整性状态校验引入传统网络接入控制技术,终端只有用户身份和平台身份的认证都通过,而且完整性状态符合网络安全策略要求时,才能接入网络,否则将终端连接到指定的隔离区域,对其进行安全修补和升级.TNC 以可信计算理论为支撑,以可信平台模块 TPM 及信任链技术构建的可信终端平台环境为基础,以远程证明技术为桥梁,将终端的可信扩展到网络,很好地解决了网络接入过程中存在的安全威胁和问题.可信网络连接 TNC 架构包括 3 个实体:访问请求者 AR(Access Requestor),申请接入网络;策略执行点 PEP(Policy Enforcement Point),传递接入请求和认证信息并执行访问控制;策略决定点 PDP(Policy Decision Point),对 AR 进行可信评估并做出是否准许接入的决定.TNC 架构从下到上分为 3 个层次:网络访问层,与传统网络结合并对上层数据提供安全保护;完整性评估层,根据安全策略评估 AR 平台的真实性和整体的完整性;完整性度量层,收集和校验 AR 完整性信息.

TNC 采用完整性报告协议[7-8]对终端的平台身份和完整性进行校验.本文通过对 TNC 架构和完整性报告协议进行分析研究后发现,完整性报告协

议只设计了网络对终端的单向可信评估，而且网络访问层与完整性评估层没有绑定关系，这样就存在一个安全缺陷，即终端的平台身份和完整性信息可能被不法者冒用，发动中间人攻击[9-10]. 攻击者冒用合法终端的信息非法接入网络，给网络造成危害. 为解决这个问题，本文提出一种改进的可信网络连接协议 S-TNC(Safe TNC，安全 TNC)，将认证的对端和通信的对端进行密码学绑定，防止终端的平台身份和完整性信息被冒用的情况发生，抵御中间人攻击.

本文第 2 节对国内外研究现状以及本文研究的目的意义进行介绍；第 3 节介绍针对 TNC 的中间人攻击模型，分析中间人攻击产生的原因；第 4 节提出一种抵御中间人攻击的可信网络连接协议 S-TNC，介绍协议流程，并对其安全性进行形式化证明；第 5 节对 S-TNC 的有效性和性能进行测试和分析；第 6 节对全文进行总结和展望.

2　相关工作

围绕可信网络连接的安全问题，国内外学者进行了许多研究，可以归纳为 3 个方面：一是可信网络连接架构研究；二是远程证明方法研究；三是协议安全研究.

可信网络连接架构方面. TCG 提出的 TNC 是基于可信计算技术，侧重终端的身份认证与完整性校验，是可信平台模块 TPM 在网络中的应用拓展，标准开放，支持不同网络环境和厂商. 我国信息安全标准委员会在深入分析 TNC 架构和技术路线的基础上，也提出了具有国家自主知识产权的可信连接架构 TCA(Trusted Connection Architecture)[11-13]. 它基于三元对等架构，利用可信权威中心进行可信评估，它的平台鉴别协议具有国家自主知识产权，具有统一完备的访问控制协议和接口支持. TCA 虽然安全性高，但其架构和协议过于复杂，还处于理论研究阶段，没有实际的产品.

远程证明方面. 远程证明是可信网络连接的核心技术，包括平台身份证明和平台完整性证明. 它要求计算机平台创建关于平台身份和完整性状态的报告，该报告基于可信平台模块 TPM 产生，能被验证方所信赖. 远程证明问题受到国内外学者和机构的关注，取得了许多成果[14-18]. TCG 的完整性报告协议实现了终端平台向远端网络证明自身平台身份和完整性，这是一种基于二制数来表示平台的可信状态的方法，简单易行，但容易泄露平台身份和配置信息，而且限制了平台多样性. 为保护平台身份隐私，有学者提出了直接匿名证明 DAA(Direct Anonymous Attestation)[19-22]，这种证明方式既可以认证对方平台身份，又保证了平台身份隐私信息的安全，然而 DAA 协议存在效率低、实现复杂的缺点. 为保证平台配置信息安全，有学者提出了基于属性的远程证明[23-29]，这种证明方式把平台的某些状态信息或配置映射为属性，验证者不需知道平台具体的配置信息，而只需平台证明它具有某些属性就可以说明平台的完整性. 基于属性的远程证明本质上是将平台配置信息的验证交由第三方进行，虽然保护了平台配置信息隐私，但增加了实体、协议实现复杂.

协议安全方面. 文献[30]为防止平台替换攻击，利用 CK 模型分析推导出一种可信接入协议模型 TNC-PS，并证明了其安全性. 文献[31]对 TNC 的各层接口协议采用安全量化分析的方法，发现了安全威胁和漏洞并进行了改进. 文献[32]对网络访问层采用安全传输层协议(Transport Layer Security，TLS)和可扩展认证协议(Extensible Authentication Protocol，EAP)方法的 TNC IF-T 协议进行了安全分析和改进. 文献[33]基于扩展的串空间模型对远程证明协议的安全属性进行了抽象和分析，发现了可能的攻击并给出了防范方法.

对于 TNC 协议容易遭受中间人攻击的问题，也有许多研究成果. 文献[9]对基于隧道的认证协议可能存在的中间人攻击进行了分析，并给出了解决思路. TNC 面临的中间人攻击正是这种类型，目前，解决这个问题比较有代表性的方案有 3 种：一是基于 D-H 协议(Diffie-Hellman key exchange)的方法. 文献[34]基于 D-H 协议提出了一种健壮的完整性报告协议，认证双方基于 D-H 协议在平台认证阶段协商了与平台完整性报告绑定的共享密钥，再利用这个共享密钥加密后续所有通信，保证通信的两端与认证的两端的一致，防止平台信息冒用. 但该方案的密钥不受 TPM 保护，私钥存在泄露威胁. 文献[35]指出了其协议漏洞并进行了改进. 二是基于主题密钥认证证据(Subject Key Attestation Evidence，SKAE)证书的方法[36-37]. 基于 SKAE 证书的方案，是在用户证书中附带了包含身份证明密钥(Attestation Identity Key，AIK)索引的 SKAE 扩展项，本质上是基于 AIK 将用户身份与平台身份进行了绑定，那么，基于该用户证书协商的安全信道与平台认证协议是绑定的，可防止平台信息冒用. 但是 AR 在接入认证时，除了要申请 AIK 证书还要申请 SKAE 证书，还需要一个权威 CA 专门颁发用户证书. 采用

这种方法虽然可以抵御中间人攻击,但会增加系统和管理的复杂性;其次,如果实时申请绑定 TPM 的 SKAE 证书,也会降低系统的性能. 三是基于 tls-unique的方法[30,36-37]. 基于 tls-unique 的信道绑定的方案,是在 TLS 安全隧道中承载上层认证协议,将 tls-unique 值与完整性报告绑定,实现外层信道和内层认证协议的绑定,防止平台信息冒用. 但文献[38]指出,攻击者可以通过与非法用户合谋,使得合法终端与攻击者之间以及攻击者与认证者之间协商出相同的信道保护密钥,达成攻击的效果.

综上所述,为了提高可信网络连接的安全性,有的方案改变了 TNC 的架构,有的提出了新的远程证明的协议,虽然安全性增加了,但也增加了实体和协议的复杂度,违背了 TNC 设计的初衷. 有的学者用形式化的方法对 TNC 的协议进行分析,发现 TNC 的协议并不是尽善尽美. 对于中间人攻击的问题,目前具有代表性的三种方式或者引入了新的安全威胁,或者增加了系统和管理的复杂性,或者在某些特殊情况下不能达成抵御中间人攻击的目的. 针对上述问题,本文提出一种改进的可信网络连接协议 S-TNC,在完整性评估层利用 TPM 在认证协议中协商一个秘密密钥,将其与平台完整性信息绑定,再由这个秘密密钥直接导出会话密钥用于通信对端之间数据通信的保护,实现认证对端和通信对端的密码学绑定,防止终端平台身份和完整性信息被冒用,以抵御中间人攻击. S-TNC 不改变 TNC 的架构,不额外增加新的实体和协议的复杂性,密钥受 TPM 硬件保护,既达到抵御中间人攻击,提高 TNC 协议安全性的目的,又符合 TNC 架构设计的初衷.

3 针对 TNC 的中间人攻击分析

3.1 攻击模型

TNC 架构实际上是在用户认证的基础上增加对接入者的平台身份认证和平台完整性校验,完整性度量与报告是 TNC 的核心技术. TNC 架构采用了完整性度量报告协议来进行平台身份认证和平台完整性校验,该协议容易遭受中间人攻击,这一攻击可能导致不符合安全要求的终端接入网络,造成可信网络连接的安全目标不能达成.

图 1 是一个典型的针对 TNC 的中间人攻击模型. AR 是合法请求端,它拥有合法的用户和可信的平台;中间人攻击者(Man in the Middle,MitM)是攻击者,它拥有合法的用户,但它的平台不可信;PDP 是认证服务端. MitM 企图通过 PDP 的认证,接入网络.

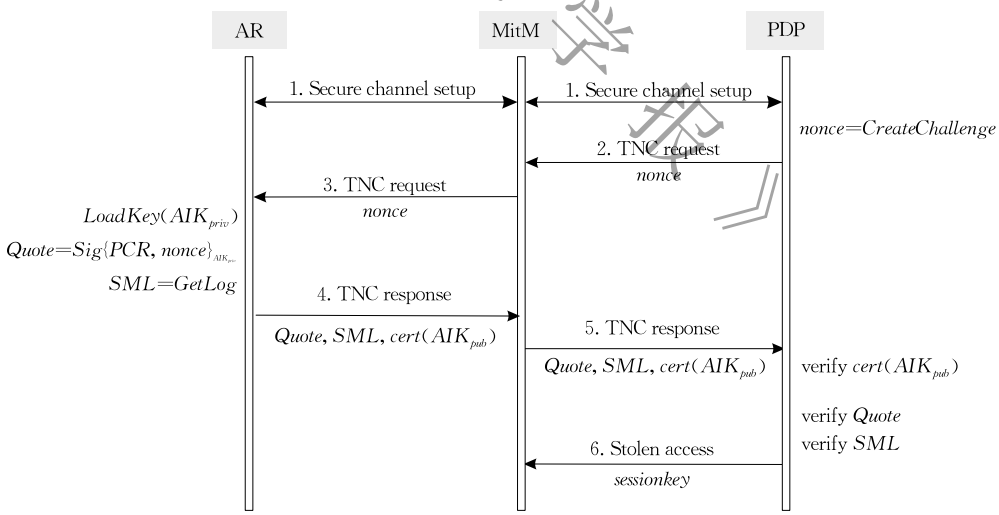

图 1 针对 TNC 的中间人攻击流程

图 1 中 *nonce* 是 PDP 向 AR 发出的认证挑战,(AIK_{priv}, AIK_{pub})是身份证明密钥对,$cert(AIK_{pub})$是 Privacy CA[39]向平台颁发的身份证明证书,*SML*(Storage Measurement Log)是存储度量日志,*Quote* 是 TPM 执行 *TPM_Quote* 操作对平台配置寄存器(Platform Configuration Register,*PCR*)和 *nonce* 的签名值.

第 2 步中 MitM 收到认证挑战 TNC request 后,并没有收集本地完整性信息,而是将其转发给 AR,AR 不能判别 TNC request 的真实来源,它生成完整性报告 TNC response 发送给 MitM,第 5 步中 MitM 将 TNC response 转发给 PDP. PDP 不能判定 TNC response 真实来源,如果它验证 $cert(AIK_{pub})$正确,则认为 TNC response 来自一个合法平台,进而如果验证 *Quote* 正确,且验证 *SML* 符合安全策略的话,则认为平台可信,并准许 MitM 接

入，于是中间人攻击达成了.

攻击结果是 PDP 认为 MitM 是一个可信平台并准许其接入，AR 也认为它与 PDP 进行了一次认证交互. 但实际上 MitM 利用了可信平台 AR 的平台完整性信息通过了 PDP 的认证.

3.2　原因分析

从上文的分析我们可以看到，针对 TNC 的中间人攻击之所以发生，主要原因是 AR 与 PDP 之间没有有效的认证，从而攻击者可以在二者之间传递 TNC request 和 TNC response，达到攻击的目的. 这是由 TNC 架构的固有局限导致的.

(1) 单向认证

TNC 只规定了 PDP 对 AR 单向的平台身份认证和完整性校验，而没有 AR 对 PDP 的认证，所以 AR 并不能判断与自己进行认证交互的是不是合法的 PDP. 所以，在攻击中 MitM 可以让 AR 对挑战信息进行签名.

(2) 完整性报告协议不能防止完整性信息被冒用

完整性报告协议的缺点是由 AIK 密钥的受限使用引起的. 根据 TPM 规范[23]，AIK 专门用于证明平台的真实性，它既不能直接用于建立安全通道，也不能认证通信的对端. AIK 对 PCR 的签名只能说明消息来自一个含有真实 TPM 芯片的平台，攻击者可以居中传递 AIK 证书和完整性信息的签名，而 PDP 不能察觉.

(3) 网络访问层与完整性评估层无绑定关系

TNC 的上层认证协议的安全依赖于底层的安全信道，但底层信道不提供平台的认证性. 网络访问层建立的安全信道是基于用户的，而上层的认证则是基于平台的，用户身份与平台身份没有绑定关系，所以进行通信的对端不一定是进行平台身份和完整性认证的对端.

4　抵御中间人攻击的可信网络连接协议 S-TNC

针对上述问题 1，可以采用双向认证的方法增强协议的认证性，但这改变了 TNC 的架构. 针对问题 2 和 3，行之有效的方法是通过一定的机制保证通信的对端就是进行平台认证的对端，对二者进行密码学绑定，防止信息的冒用，同时也解决了问题 1.

基于这样的想法，本文提出了一种改进的可信网络连接协议 S-TNC，在完整性评估层基于 TPM 协商一个秘密密钥，将其与平台完整性信息绑定，再由这个秘密密钥直接导出会话密钥用于通信对端之间数据通信的保护，实现认证对端和通信对端的密码学绑定，抵御中间人攻击.

4.1　协议流程

S-TNC 协议流程如图 2 所示.

图 2 中 *secret* 是 AR 和 PDP 协商出来的与平台绑定的秘密密钥，*sessionkey* 是基于 *secret* 导出的会话密钥. 其它符号意义同图 1.

步骤 0：AR 和 PDP 基于用户认证协商安全信道，对后续认证数据进行保护，通信密钥为 K_0.

步骤 1：AR 基于 TPM 生成一对绑定密钥 BK (Bind Key)，即 $CreateKey(BK_{priv}, BK_{pub})$，该密钥可以用于加解密，不可复制和迁移，AR 用自己 AIK 的私钥对 BK_{pub} 进行签名得到 $sig = CertifyKey(BK_{pub})_{AIK_{priv}}$. AR 将公钥 BK_{pub}、签名 sig 以及平台身份证书 $cert(AIK_{pub})$ 发送给 PDP.

步骤 2：PDP 验证 AR 的平台身份执行 $VerifyCert(cert_{AIK})$，并得到 AIK 公钥 AIK_{pub}；然后利用 AIK_{pub} 验证 sig 的真伪 $VertifyKey(sig)_{AIK_{pub}}$，从而确认 BK_{pub} 确实是平台 AR 的公钥. 任何一个验证结果非真，则终止协议，接入失败.

步骤 3：PDP 随机生成一个秘密密钥 *secret*，将其用 BK_{pub} 加密得密文 $c = Enc(secret)_{BK_{pub}}$；随机生成完整性认证挑战信息 *nonce*. PDP 将 c 和 *nonce* 发送给 AR.

步骤 4：AR 对 c 进行解密得到 $secret = Dec(c)_{BK_{priv}}$. AR收集完整性信息，计算 $H = Hash(secret|nonce)$，将 H 作为 *TPM_Quote* 命令的 *externalData* 参数交 TPM 计算 $Quote = Sign\{PCR, H\}_{AIK_{priv}}$，将 Quote 和 SML 发送给 *PDP*.

步骤 5：PDP 收到完整性报告后，也计算 $H = Hash(secret|nonce)$，利用 H、*PCR* 值、AR 的公钥 AIK_{pub} 对 *Quote* 进行验证，再对 *SML* 进行验证，如果验证通过，则认为 PDP 的平台是可信的. 若验证结果非真，则终止协议，接入失败.

步骤 6：PDP 通知 AR 接入成功. AR 和 PDP 基于 *secret* 采用相同的密钥生成算法生成会话密钥 *sessionkey*，后续的通信使用 *sessionkey* 进行保护. 在协议实现中，PDP 要将这个 *sessionkey* 发送给 PEP，AR 和 PEP 通过握手确认双方是否拥有相同的 *sessionkey*，然后用这个 *sessionkey* 加密通信数据，这样就将认证的对端与通信的对端进行了绑定.

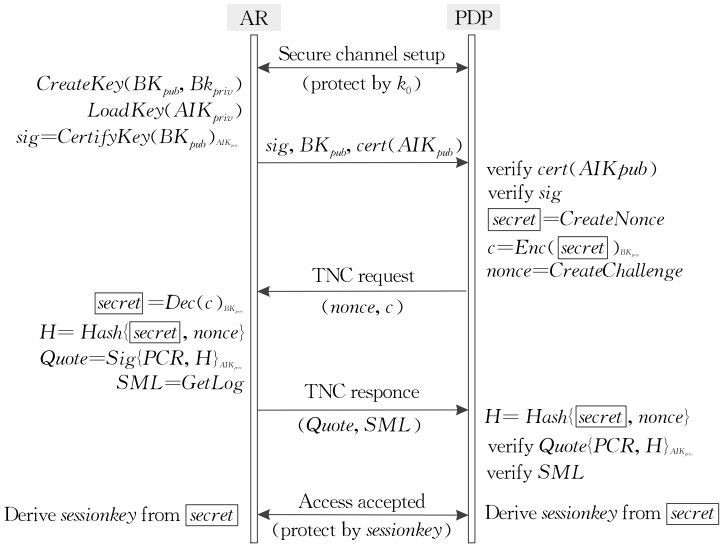

图 2 S-TNC 协议流程

S-TNC 协议能抵御中间人攻击的关键在于秘密密钥 *secret*. *secret* 基于 AIK 认证生成，由 TPM 密钥保护. 它与平台具有天然的绑定关系，攻击者无法获取或伪造这个秘密信息，因而无法生成有效的 *sessionkey*. 只有经过 PDP 认证并掌握 *secret* 的 AR 才能接入网络，这就实现了认证对端和通信对端的密码学绑定，达到抵御中间人攻击的目的. 本协议在完整性评估层实现，对网络访问层和完整性度量层透明，不改变 TNC 原有架构，继承了 TNC 标准所述安全特性，具有实现简单、增强安全性的特点.

4.2 协议证明

秘密密钥 *secret* 的协商是 S-TNC 协议达成安全目标的关键，本节使用 BAN 逻辑[40-41]来证明其安全性. BAN 逻辑是广泛使用的认证协议形式化分析方法，采用 BAN 逻辑来分析安全协议，可以提示一些非形式化方法很难发现的缺陷，通过严格的推理，可以很好地解决协议的认证性问题.

BAN 逻辑中常用的逻辑符号如下：

$P|\equiv X$：实体 P 相信 X 是真实的；

$P|\sim X$：实体 P 曾经发送消息 X；

$P\lhd X$：实体 P 收到消息 X；

$P|\Rightarrow X$：实体 P 对 X 有管辖权；

$\sharp(X)$：X 是新鲜的；

$K\mapsto P, K_P$：K 是实体 P 的公钥；

K_P^{-1}：K 是实体 P 的私钥；

$\{X\}_K$：用密钥 K 加密 X 的结果；

$P\overset{K}{\leftrightarrow}Q$：K 是实体 P 和实体 Q 之间的共享密钥；

BAN 逻辑共有 8 类规则，与本文相关的有：

消息含义规则

$$\frac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\lhd\{X\}_K}{P|\equiv Q|\sim X},$$

接收消息规则

$$\frac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\lhd\{X\}_K}{P\lhd X},$$

新鲜性规则

$$\frac{P|\equiv\sharp(X)}{P|\equiv\sharp(X,Y)},$$

临时值校验规则

$$\frac{P|\equiv\sharp(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X},$$

信任规则

$$\frac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}.$$

消息含义规则和接收消息规则还有公私钥的相关变形形式类似，此处不再赘述.

BAN 逻辑的推理步骤如下：

(1) 协议理想化，将协议的实际消息转换成 BAN 逻辑所能识别的形式，去除对协议分析没有影响的部分.

(2) 确定初始化假设，用逻辑语言对系统的初始状态进行描述，建立初始假设集合.

(3) 确定协议安全目标，用逻辑语言说明协议应满足什么目标公式才说明协议安全.

(4) 逻辑推理，应用推理规则对协议进行形式化推理，推导出目标公式.

为便于分析，将 S-TNC 形式化描述如下：

(1) $AR\rightarrow PDP$：

$CertifyKey(BK_{pub})_{AIK_{priv}}, BK_{pub}, cert(AIK_{pub})$

(2) $PDP\rightarrow AR$：$TNC\ request$

$(Enc(secret)_{BK_{pub}}, nonce)$

(3) $AR \rightarrow PDP$: $TNC\ response$

$Sign\{PCR, hash(secret, nonce)\}_{AIK_{priv}}$, SML

(4) $PDP \rightarrow AR$: $Enc(data)_{sessionkey}$

(5) $AR \rightarrow PDP$: $Enc(data)_{sessionkey}$

网络访问层保护密钥 K_0 只能保证通信的机密性，不能保证通信的认证性，对本协议分析没有影响，故不考滤.

为便于描述，本节用 C 代表 AR，S 代表 PDP，K_C 代表 AR 生成的绑定密钥 BK 的公钥 BK_{pub}，N_S 代表 PDP 生成的随机数 $nonce$，K_{CS} 代表 AR 与 PDP 之间共享的秘密密钥 $secret$，N_C 表示 AR 生成的随机数.

将协议理想化如下：

$$C \rightarrow S: \{K_C\}_{AIK_C^{-1}} \tag{1}$$

$$S \rightarrow C: N_S, \{C \overset{K_{CS}}{\leftrightarrow} S\}_{K_C} \tag{2}$$

$$C \rightarrow S: \{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}_{AIK_C^{-1}}, \{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}_{K_{CS}} \tag{3}$$

$$S \rightarrow C: \{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}_{K_{CS}} \tag{4}$$

以上四式抽象出与协议分析有关的交互数据，形式进行了改变但不影响原意，式(3)和(4)中 $\{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}_{K_{CS}}$ 表示 AR 和 PDP 用基于 K_{CS} 生成的会话密钥进行保密通信.

初始化假设如下：

$$S \mid\equiv AIK_C \mapsto C \tag{5}$$

$$S \mid\equiv \#(N_S) \tag{6}$$

$$C \mid\equiv \#(N_C) \tag{7}$$

在可信环境下，S 基于 AIK 证书进行平台身份认证，协议运行时要验证权威机构 Privacy CA 的签名，AIK 证书中包含公钥信息，故假设式(5)是可行的. S 随机生成 N_S，它是新鲜的，所以假设式(6)可行. C 随机生成 N_C，它是新鲜的，所以假设式(7)可行.

目标公式如下：

$$S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S,\ S \mid\equiv C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$$

$$C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S,\ C \mid\equiv S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S$$

如果目标公式成立，则说明 AR 与 PDP 都与对方协商并确认了秘密密钥，并且秘密密钥与 AR 的平台完整性报告及通信信道绑定.

逻辑推理如下：

由式(1)、(5)应用消息含义规则知：

$$\frac{S \mid\equiv AIK_C \mapsto C, S \lhd \{K_C\}_{AIK_C^{-1}}}{S \mid\equiv C \mid\sim K_C} \tag{8}$$

这说明 S 相信 K_C 来自 C. 由 TPM 密钥管理规范知：

$$S \mid\equiv K_C \mapsto C \tag{9}$$

S 在式(2)中用 K_C 加密 K_{CS}，只有 C 才能解密，S 把 K_{CS} 作为 S 和 C 之间共享的秘密密钥，那么应有：

$$S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S \tag{10}$$

由式(2)应用接收消息规则知

$$\frac{C \mid\equiv K_C \mapsto C, C \lhd \{C \overset{K_{CS}}{\leftrightarrow} S\}_{K_C}}{C \lhd C \overset{K_{CS}}{\leftrightarrow} S} \tag{11}$$

式(2)在 S 向 C 保密传递 K_{CS}，TNC 协议本身 AR 不对 PDP 进行验证，所以在 TNC 协议规定下应有：

$$C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S \tag{12}$$

由式(3)、(5)应用接收消息规则知

$$\frac{S \mid\equiv AIK_C \mapsto C, S \lhd \{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}_{AIK_C^{-1}}}{S \mid\equiv C \mid\sim \{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}} \tag{13}$$

由式(6)应用新鲜性规则知

$$\frac{S \mid\equiv \#(N_S)}{S \mid\equiv \#\{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}} \tag{14}$$

由式(13)和(14)应用临时值校验规则知

$$\frac{S \mid\equiv \#\{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}, S \mid\equiv C \mid\sim \{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}}{S \mid\equiv C \mid\equiv \{N_S, PCR, C \overset{K_{CS}}{\leftrightarrow} S\}} \tag{15}$$

由信任规则知

$$S \mid\equiv C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S \tag{16}$$

由消息(4)、(12)应用消息含义规则可得

$$\frac{C \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S, C \lhd \{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}_{K_{CS}}}{C \mid\equiv S \mid\sim \{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}} \tag{17}$$

由式(7)应用新鲜性规则知

$$\frac{C \mid\equiv \#(N_C)}{C \mid\equiv \#(N_C, C \overset{K_{CS}}{\leftrightarrow} S)} \tag{18}$$

由式(17)、(18)应用临时值校验规则可得

$$\frac{C \mid\equiv \#(N_C, C \overset{K_{CS}}{\leftrightarrow} S), C \mid\equiv S \mid\sim \{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}}{C \mid\equiv S \mid\equiv \{N_C, C \overset{K_{CS}}{\leftrightarrow} S\}} \tag{19}$$

由式(19)应用信任规则知

$$C \mid\equiv S \mid\equiv C \overset{K_{CS}}{\leftrightarrow} S \tag{20}$$

由式(10)、(12)、(16)、(20)可知目标公式可以

达到，说明协议是安全的. 上述证明说明 S-TNC 实现 AR 和 PDP 双方安全地协商和确认秘密密钥，实现秘密密钥与 AR 平台绑定、通信信道绑定的过程是正确的.

4.3 方案比较

国内外学者提出的各种抵御针对 TNC 的中间人攻击的方案中，比较有代表性的方案有 3 种，其它的方案大多是基于这 3 种方案的改进和变形，这 3 种方案分别是基于 D-H 协议的方案[34]、基于 SKAE 证书的方案[36-37]、基于 tls-unique 的方案[30,36-37]，和这些方案相比，本文提出的 S-TNC 方案具有一定优势，这几种方案比较如表 1 所示.

表 1 抵御 TNC 中间人攻击的方案比较

方案	安全目标实现	性能影响	特点
基于 D-H 协议	密钥由软件生成，密钥不受保护，存在私钥泄露的威胁	不增加管理复杂性，对协议性能影响不大	基于现有成熟协议，简单易行
基于 SKAE 证书	通过证书将用户身份与平台身份进行了绑定，从根本上杜绝平台信息冒用，可以抵御中间人攻击，安全性高	额外增加一个权威机构颁发带 SKAE 扩展项的用户证书，增大系统复杂性和证书管理复杂性； 实时绑定 TPM 与 SKAE 证书降低系统性能	协议复杂，但安全性高，适用多种网络访问层协议
基于 tls-unique	绑定外层通信信道与内层平台认证协议，但特殊情况下仍不能抵御中间人攻击	不增加管理复杂性，对协议性能影响不大	基于现有成熟协议，适用于网络访问层是基于 TLS 实现的情况
S-TNC	密钥由 TPM 硬件保护，绑定认证平台与通信对端，可以抵御中间人攻击	使用运行速度较低的 TPM 硬件执行密码相关操作，一定程度降低了系统性能	充分发挥 TPM 的特性优势，协议简单，安全性高，符合 TNC 设计初衷

通过上述对比可知，本文设计的 S-TNC 没有增加任何实体和证书，管理简单. S-TNC 在运行过程中，即便网络访问层保护密钥被攻破，由于 AIK、BK 均受 TPM 保护，攻击者仍然无法获取认证协议协商的秘密密钥 *secret*，而 *sessionkey* 是由 *secret* 产生的，故可以抵御中间人攻击. S-TNC 中使用的绑定密钥 BK 由 TPM 产生和保护，密钥不存在泄露威胁，会话密钥与平台具有绑定关系，充分发挥了可信计算模块 TPM 的特性优势，自身安全性高.

5 实验测试与分析

5.1 有效性测试与分析

本文基于开源项目 TNC@FHH 构建了实验环境. TNC@FHH 遵循 TCG 规范，实现了 TNC 架构的大部分组件和接口. 本文在不改变 TNC@FHH 系统的总体流程和架构的前提下，对其作了修改，实现了 S-TNC 协议.

本文按照 3.1 节所述中间人攻击流程，构建了如图 3 所示的验证环境.

系统软硬件配置如表 2 所示.

经测试，S-TNC 可以正常工作，PDP1 能够对接入终端 AR1 的用户身份、平台身份、平台完整性进行认证，并根据认证结果控制 AR1 的接入.

现在假定 AR1 已经被攻陷，它的完整性状态已经不能通过 PDP1 的验证，攻击者企图控制 AR1 来访问敏感资源网络. AR2 是一个合法的终端，它的状态符合完整性要求. 攻击者要利用 AR2 的完整性

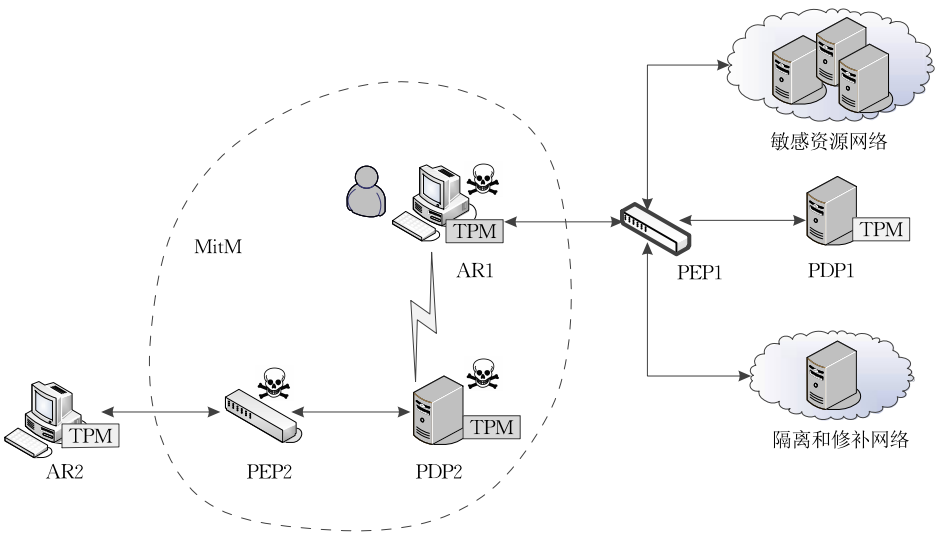

图 3 实验环境

表 2　软硬件配置

实体	硬件	软件
AR	Intel NUC DC 53427HYE 迷你电脑，Intel i5-3427U CPU，4 GB 内存，TPM2.0	SUSE Linux Enterprise Server 11 SP3，wpa_supplicant，TNC Client(由 TNC@FHH 编译)，openssl0.9.8，TSS，PTS
PEP	H3C S2626 交换机	
PDP	Intel NUC DC 53427HYE 迷你电脑，Intel i5-3427U CPU，4 GB 内存，TPM2.0	SUSE Linux Enterprise Server 11 SP3，FreeRADIUS，TNC Server(由 TNC@FHH 编译)，openssl0.9.8，TSS，PTS

信息代替 AR1 的完整性信息，来接受 PDP1 的验证. 攻击者设置 PEP2、PDP2，用来获取 AR2 的完整性信息. 对于未改进的 TNC，攻击者可以利用 AR1 接入敏感资源网络.

对于 S-TNC，本文针对攻击者可能进行的几种攻击手段设计了几个场景进行试验，结果如表 3 所示.

表 3　运行 S-TNC 时的中间人攻击结果

场景	攻击手段	攻击结果
1	利用 AR1、PEP2、PDP2 居中传递 AR2、PDP1 之间平台和完整性认证请求和应答.	1. AR1 通过用户身份认证； 2. AR1 通过平台身份认证； 3. AR1 通过平台完整性校验； 4. AR1 与 PEP1 通信失败，AR1 接入敏感资源网络失败.
2	1. AR1 使用自己的平台身份与 PDP1 进行平台认证； 2. 利用 AR1、PEP2、PDP2 居中传递 AR2、PDP1 之间完整性认证请求和应答.	1. AR1 通过用户身份认证； 2. AR1 通过平台身份认证； 3. 完整性校验失败，认证失败.
3	1. 伪造 BK 密钥； 2. 利用 AR1、PEP2、PDP2 居中传递 AR2、PDP1 之间平台认证请求和应答.	1. AR1 通过用户身份认证； 2. AR1 通过平台身份认证； 3. PDP1 验证 BK 签名失败，认证失败.

场景 1 中的攻击之所以会失败，是因为 *secret* 的产生和传递受到 TPM 密钥保护，只有 AR2 和 PDP1 才掌握，不可伪造，AR1 无法获取，故无法生成 *sessionkey*，所以认证完成后 AR1 与 PEP1 通信失败. 场景 2、场景 3 是模拟攻击者为获取 *secret* 而设置的，虽然 AR1 可以通过平台身份认证，能与 PDP1 协商出一个假的 *secret*，但 AR1 无法伪造 AR2 的 *Quote* 签名或 AIK 对 BK 的签名，所以最终认证失败.

AR1 要想通过 PDP1 的认证接入网络，则必须冒用 AR2 的平台状态信息，而 AR2 的平台状态又与 *secret* 绑定，*secret* 导出 *sessionkey* 后与信道绑定. 攻击者不可知晓又不可伪造 *secret*，使得改进的协议 S-TNC 可以有效抵御针对 TNC 的中间人攻击.

5.2　性能测试与分析

相比传统 TNC，S-TNC 增加了一些计算量，部分计算须由运算速度较低的 TPM 硬件来完成，如生成绑定密钥 *CreateKey*、对绑定密钥签名 *CertifyKey*、验证密钥签名 *VerifyKey*、非对称密钥加解密 *Encrypt*/*Decrypt*、摘要 *Hash* 以及生成随机数 *CreateNonce* 等. 为解决这些耗时操作带来的认证时延问题，本文采取以下三种措施对 S-TNC 进行优化：

(1) 通用操作尽量使用软件运算来代替 TPM 计算，提高计算速度；

(2) 优化流程，AR 和 PDP 同步执行必要的耗时操作；

(3) 一些操作可预先完成，如 *CreateKey*、*CertifyKey* 等可在系统启动后运行.

本文对运行 TNC 和运行 S-TNC 的系统各进行了 10 次测试，统计各个认证阶段平均耗时，结果如表 4 所示.

从表 4 可以看出，S-TNC 由于在平台身份认证时增加了秘密密钥协商的过程，所以增加了双方交互的次数和 TPM 私钥解密操作、会话密钥分发和确认等操作，造成了时间消耗增加的问题，但是这个时延是在可接受的范围内.

表 4　性能测试结果　　/s

方案	用户身份认证及建立安全信道	平台身份认证	平台完整性校验	成功接入总耗时
TNC	4.242	1.122	6.152	11.552
S-TNC	4.238	3.445	6.184	14.531

6　结束语

本文通过对 TNC 架构、协议和面临安全威胁的深入分析，设计实现了一种抵御中间人攻击的可信网络连接协议 S-TNC. 本文设计的方法基于 TPM 协商一个秘密密钥，实现平台认证对端和数据通信对端的密码学绑定，能防止攻击者冒用合法终

端的信息进行中间人攻击.本文对该协议进行了证明和讨论,对其有效性和性能进行了测试分析.本文设计的方法不改变 TNC 的架构,具有简单安全的特点.

目前,配备了可信平台模块 TPM 的 PC 和服务器越来越普及,这为 TNC 的进一步推广使用提供了良好的条件.TNC 非常适用于企业私有网、私有云、军队、政府涉密网等高安全需求场景的接入控制.它不仅仅具有用户身份认证、通信保密等常规手段,还可以与入侵检测、权限控制等方法进行联动[3],最重要的是,它要对终端的平台身份和可信状态进行验证,这无疑大大提高了保护能力.本文设计的 S-TNC,在安全性和复杂性之间找到了很好的平衡,为 TNC 中间人攻击的解决提供了新的思路,很好地解决了 TNC 面临的中间人攻击的威胁,可有效防止不安全的终端冒用可信终端的平台信息接入网络而给网络造成危害的情况发生,提高了 TNC 的安全性.

致 谢 匿名审稿专家对本文提出了宝贵的修改意见,在此对审稿专家表示由衷的感谢!

参 考 文 献

[1] Zhang Huan-Guo, Zhao Bo. Trusted computing. Wuhan: Wuhan University Press, 2011(in Chinese)
(张焕国, 赵波. 可信计算. 武汉: 武汉大学出版社, 2011)

[2] Shen Chang-Xiang, Zhang Huan-Guo, Wang Huai-Ming, et al. Research and development of Trusted Computing. Scientia Sinica: Informationis, 2010, 40(2): 139-166 (in Chinese)
(沈昌祥, 张焕国, 王怀民等. 可信计算的研究与发展. 中国科学: 信息科学, 2010, 40(2): 139-166)

[3] Zhao Bo, Zhang Huan-Guo, Li Jing, et al. The system architecture and security structure of Trusted PDA. Chinese Journal of Computers, 2010, 33(1): 82-92(in Chinese)
(赵波, 张焕国, 李晶等. 可信 PDA 计算平台系统结构与安全机制. 计算机学报, 2010, 33(1): 82-92)

[4] Trusted Computing Group. Trusted Platform Module Library, Part 1: Architecture, Part 2: Structures, Part 3: Commands, Family 2.0, Revision 1.16. 2014

[5] Zhang Huan-Guo, Chen Lu, Zhang Li-Qiang. Research on trusted network connection. Chinese Journal of Computers, 2010, 33(4): 706-717(in Chinese)
(张焕国, 陈璐, 张立强. 可信网络连接研究. 计算机学报, 2010, 33(4): 706-717)

[6] Trusted Computing Group. Trusted Network Communications TNC Architecture for interoperability. Specification Version 1.5, Revision 4. 2012

[7] Jaeger T, Sailer R, Shankar U. PRIMA: Policy-reduced integrity measurement architecture//Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. California, USA, 2006: 19-28

[8] Sailer R, Zhang X, Jaeger T, et al. Design and implementation of a TCG-based integrity measurement architecture//Proceedings of the 13th USENIX Security Symposium. San Diego, USA, 2004: 16-32

[9] Asokan N. Man-in-the-middle in tunnelled authentication protocols//Proceedings of the 11th International Conference on Security Protocols. Cambridge, UK, 2003: 42-48

[10] Conti M, Dragoni N, Lesyk V. A survey of Man-in-The-Middle attacks. IEEE Communications Surveys and Tutorials, 2016, 18(3): 2027-2051

[11] GB/T 29828-2013. Trusted connection architecture. Information Security Management Working Group, 2013(in Chinese)
(GB/T 29828-2013. 可信连接架构. 信息安全管理工作组, 2013)

[12] China Iwncomm Co, Ltd. Trusted network connection implementing method based on tri-element peer authentication, USA, 2015

[13] Li Ming, Li Qin, Zhang Guo-Qiang, et al. The implementation and application of Trusted Connect Architecture. Journal of Information Security Research, 2017, 3(4): 332-338(in Chinese)
(李明, 李琴, 张国强等. 可信网络连接架构 TCA 的实现及其应用. 信息安全研究, 2017, 3(4): 332-338)

[14] Tan Liang, Liu Zhen, Zhou Ming-Tian. Development of attestation in TCG. Acta Electronica Sinica, 2010, 38(5): 1105-1112 (in Chinese)
(谭良, 刘震, 周明天. TCG 架构下的证明问题研究及进展. 电子学报, 2010, 38(5): 1105-1112)

[15] Tan Liang, Chen Ju. Remote attestation project of the running environment of the trusted terminal. Journal of Software, 2014, 25(6): 1273-1290(in Chinese)
(谭良, 陈菊. 一种可信终端运行环境远程证明方案. 软件学报, 2014, 25(6): 1273-1290)

[16] Yu Yue, Wang Huai-Min, Liu Bo, et al. A trusted remote attestation model based on Trusted Computing//Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Melbourne, Australia, 2013: 1504-1509

[17] Zhao Bao-Hua, Guo Hao. Dynamic remote attestation on Trusted Computing. Applied Mechanics and Materials, 2015, 696: 167-172

[18] Hu Ling-Bi, Tan Liang. Research on the trusted virtual platform remote attestation method in cloud computing. Journal of Software, 2018, 29(9): 2874-2895(in Chinese)
(胡玲碧, 谭良. 云环境中可信虚拟平台的远程证明方案研究. 软件学报, 2018, 29(9): 2874-2895)

[19] Brickell E. Direct anonymous attestation//Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington, USA, 2004: 132-145

[20] Chen Xiao-Feng, Feng Deng-Guo. A direct anonymous attestation scheme in multi-doma environment. Chinese Journal of Computers, 2008, 31(7): 1122-1130(in Chinese)
(陈小峰，冯登国. 一种多信任域内的直接匿名证明方案. 计算机学报，2008，31(7)：1122-1130)

[21] Zhang Da-Wei, Han Zhen, Jiang Yi-Chen, et al. Anonymous remote attestation protocol based on DAA and TLS. Journal of Huazhong University of Science and Technology(Natural Science Edition), 2014, 42(11): 28-33(in Chinese)
(张大伟，韩臻，蒋逸尘等. 基于DAA和TLS的匿名远程证明协议. 华中科技大学学报(自然科学版)，2014，42(11)：28-33)

[22] Yang Bo, Feng Deng-Guo, Qin Yu, et al. Research on direct anonymous attestation scheme based on trusted mobile platform. Journal of Computer Research and Development, 2014, 51(7): 1436-1445(in Chinese)
(杨波，冯登国，秦宇等. 基于可信移动平台的直接匿名证明方案研究. 计算机研究与发展，2014，51(7)：1436-1445)

[23] Sadeghi A R, Stüble C. Property-based attestation for computing platforms: Caring about properties, not mechanisms//Proceedings of the 2004 Workshop on New Security Paradigms. Nova Scotia, Canada, 2004: 67-77

[24] Chen L, Landfermann R, Hr H, et al. A protocol for property-based attestation//Proceedings of the 1st ACM Workshop on Scalable Trusted Computing. Alexandria, USA, 2006: 7-16

[25] Li Jian-Jun, Li Ying-Jia, Hu Ya-Jun, et al. An improved protocol for property-based attestation//Proceedings of the 32nd Chinese Control Conference. Xi′an, China, 2013: 6343-6348

[26] Awad A, Kadry S, Lee B, et al. Property based attestation for a secure cloud monitoring system//Proceedings of the 7th International Conference on Utility and Cloud Computing. Washington, USA, 2015: 934-940

[27] Chen Xun, Liu Ji-Qiang, Shi Yang-Feng, et al. An enhanced authentication scheme for virtual private network access based on platform attributes of multi-level classification//Proceedings of the International Conference on Applications and Techniques in Information Security. Beijing, China, 2015: 52-64

[28] Zhang Xin, Yang Xiao-Yuan, Zhu Shuai-Shuai. A ring-signature based remote attestation scheme for the property of configurations. Journal of Wuhan University(Natural Science Edition), 2016, 62(2): 117-121(in Chinese)
(张鑫，杨晓元，朱率率. 一种基于环签名的属性配置远程证明方案. 武汉大学学报(理学版)，2016，62(2)：117-121)

[29] Zhao Shi-Jun, Feng Deng-Guo. A TNC Trusted Network Connection schema based on property attestation. Journal of Wuhan University(Natural Science Edition), 2012, 58(6): 519-525(in Chinese)
(赵世军，冯登国. 基于属性证明的可信网络接入方案. 武汉大学学报(理学版)，2012，58(6)：519-525)

[30] Ma Zhuo, Ma Jian-Feng, Li Xing-Hua, et al. Provable security model for Trusted Network Connect protocol. Chinese Journal of Computers, 2011, 34(9): 1669-1678(in Chinese)
(马卓，马建峰，李兴华等. 可证明安全的可信网络连接协议模型. 计算机学报，2011，34(9)：1669-1678)

[31] Luo An-An, Lin Chuang, Wang Yuan-Zhuo. Security quantifying method and enhanced mechanisms of TNC. Chinese Journal of Computers, 2009, 32(5): 887-898(in Chinese)
(罗安安，林闯，王元卓等. 可信网络连接的安全量化分析与协议改进. 计算机学报，2009，32(5)：887-898)

[32] Xiao Yue-Lei. Research on key technologies of Trusted Network Connect and their application [Ph. D. dissertation]. Xi′an: Xi′an Xidian University, 2013(in Chinese)
(肖跃雷. 可信网络连接关键技术研究及其应用[博士学位论文]. 西安：西安电子科技大学，2013)

[33] Feng Wei, Feng Deng-Guo. Analyzing trusted computing protocol based on the strand spaces model. Chinese Journal of Computers, 2015, 38(4): 701-716(in Chinese)
(冯伟，冯登国. 基于串空间的可信计算协议分析. 计算机学报，2015，38(4)：701-716)

[34] Stumpf F, Tafreschi O, Roder P, et al. A robust intergrity reporting protocol for remote attestation//Proceedings of the 2nd Workshop on Advances in Trusted Computing. Tokyo, Japan, 2006: 308-317

[35] Zhu Lie-Huang, Zhang Zi-Jian, Liao Le-Lian, et al. A secure robust integrity reporting protocol of Trusted Computing for remote attestation under fully adaptive party corruptions//Proceedings of the International Conference on Future Wireless Networks and Information Systems. Macao, China, 2011: 211-217

[36] Trusted Computing Group. Trusted Network Communications TNC IF-T: Protocol Bindings for Tunneled EAP Methods. Specification Version 2.0. 2014

[37] Trusted Computing Group. Trusted Network Communications TNC IF-T: Binding to TLS. Specification Version 2.0. 2013

[38] Zhang Jun-Wei, Ma Jian-Feng, Wen Xiang-Zai. Generalized composable trusted network connection model and EAP-TNC protocol in IF-T. Scientia Sinica Informationis, 2010(2): 200-215(in Chinese)
(张俊伟，马建峰，文相在. 通用可组合的可信网络连接模型和IF-T中的EAP-TNC协议. 中国科学：信息科学，2010(2)：200-215)

[39] Chen L, Warinschi B. Security of the TCG Privacy-CA solution//Proceedings of the 8th International Conference on Embedded and Ubiquitous Computing. Hong Kong, China, 2010: 609-616

[40] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18-36

[41] Abadi M, Tuttle M R. A semantics for a logic of authentication//Proceedings of the 10th ACM Symposium on Principles of Distributed Computing. Montreal, Canada, 1991: 201-216

ZHAO Bo, professor, Ph. D. supervisor. His research interests include information security, embedded systems, trusted computing, etc.

XIANG Cheng, master candidate. His research interest is trusted computing.

ZHANG Huan-Guo, professor, Ph. D. supervisor. His research interests include information security, cryptography, trusted computing, etc.

Background

With the development and popularization of trusted computing technology, people now realize that in the face of existing computer network security threats, we should not only consider the safety of terminals or networks separately, but also consider the linkage between them. It is necessary not only to ensure the trust of the terminal computing environment, but also to extend the trust of the terminal computing environment to the network, making the network into a trusted computing environment. Trusted Network Connection Sub Group (TNC-SG) has developed trusted network connect (TNC) architecture based on the trusted computing technology. TNC is a combination of trusted computing technology and network access control mechanism, which aims to extend the trusted state of the terminal to the network and extend the trust chain from the terminal to the network. However, due to the TNC architecture design features and the compromise on compatibility, it has some flaws. In view of the TNC security problem, the researchers have made many researches on architecture, platform attestation, protocol security and so on. Their achievements are published in many papers. One of these problems is man-in-the-middle attack, which allows an attacker to access a network illegally by impersonating other's platform information. By in-depth study of the process and causes of the TNC man-in-the-middle attack, this paper proposes a new trusted network connect protocol S-TNC to resist man-in-the-middle attacks. S-TNC binds the authentication peers and the communication peers, to prevent the fraudulent use of platform information, so it can resist man-in-the-middle attack.

This work is supported in part by the National Program on Key Basic Research Project (973 Program) of China (No. 2014CB340600), National High Technology Research and Development Program (863 Program) of China (No. 2015AA016002), National Natural Science Foundation of China (No. 6133209) and Frontier Projects of Applied Foundation in Wuhan City (No. 2018010401011295).