

可信网络连接的安全量化分析与协议改进

罗安安 林 闯 王元卓 邓法超 陈 震

(清华大学计算机科学与技术系 北京 100084)

摘 要 可信网络连接(TNC)被认为是可信的网络体系结构的重要部分,随着 TNC 研究和应用的不断深入,TNC 架构自身的安全性问题变得更加至关重要.文中重点研究 TNC 协议架构的安全性问题,首先提出了一种针对 TNC 协议的基于半马尔可夫过程的安全性量化分析方法;其次针对 TNC 完整性验证和访问授权过程中存在的安全威胁和漏洞,提出了一套安全性增强机制,并通过安全量化分析方法进行了验证.最后利用 Intel IXP2400 网络处理器搭建了 TNC 原型系统,为文中提出的改进机制和系统框架提供了安全量化验证的实际平台.

关键词 可信网络连接;随机模型;认证性;机密性;完整性

中图法分类号 TP393

DOI号: 10.3724/SP.J.1016.2009.00887

Security Quantifying Method and Enhanced Mechanisms of TNC

LUO An-An LIN Chuang WANG Yuan-Zhuo DENG Fa-Chao CHEN Zhen

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084)

Abstract Trusted Network Connect (TNC) is considered as an important part of trusted network architecture, and with its deeper research and application development, whether it is enough trustworthy during TNC platform authentication and access control becomes a key problem. In the paper, we mainly focus on the trustworthy problem of TNC. First, we proposed a novel security quantifying method which is based on semi-Markov processes. And then, according to the potential threat and security holes during typical message flow and access authorization process in TNC specification, we proposed a set of trustworthy enhanced mechanisms, which is verified by our security quantifying method. Finally a TNC prototype system framework based on IXP2400 network processor is built to be a performance evaluation and trustworthy verification platform.

Keywords trusted network connect; stochastic model; authenticity; integrity; confidentiality

1 引 言

随着计算机网络技术的迅猛发展,由于互联网协议设计的开放性和简洁性,各种网络安全问题不断出现,而当前普通计算机用户采用以系统补丁、防

火墙、杀毒软件、入侵检测软件等组成的传统防护手段,功能上孤立单一,大多只能对抗已知攻击,难以及时发现系统自身漏洞、防范不断变种的计算机病毒,而网络传播时延小和相似的脆弱性又导致病毒极易从一台或多台计算机快速扩散到整个网络,造成大面积的网络瘫痪,最终造成无法估量的损失.

收稿日期:2008-09-22;最终修改稿收到日期:2009-03-19. 本课题得到国家自然科学基金(90718040,60673187,60673054,60673160,60803123)资助. 罗安安,男,1984年生,博士研究生,主要研究方向为网络体系结构、网络安全. E-mail: laa@mails. tsinghua. edu. cn. 林 闯,男,1948年生,教授,博士生导师,主要研究领域为计算机网络、系统性能评价、随机 Petri 网、可信网络与可信计算. 王元卓,男,1978年生,博士,助理研究员,主要研究方向为可信网络、系统性能评价、网络安全等. 邓法超,男,1985年生,硕士研究生,主要研究方向为网络访问控制、网络安全. 陈 震,男,1976年生,博士,讲师,主要研究方向为可信网络与可信计算、P2P 系统和高速网络安全.

另一方面,尽管大多数局域网安装了各类防火墙和安全网关,一定程度上可以抵御来自外部网络的各种恶意攻击和病毒感染,却无法阻止来自内部的攻击或破坏,如果在网络内部有未经授权的或者自身存在安全漏洞的主机接入网络,不仅容易诱发诸如蠕虫病毒、木马病毒、拒绝服务攻击等恶意的破坏行为,而且感染了病毒的终端主机一旦没有及时发现并被允许访问其它主机,很可能导致病毒肆意传播,扩散到整个网络.所以不能保证终端接入安全,会对网络带来严重的安全隐患.

为了增加当前网络抵御各类攻击和破坏行为的能力,必须加强网络访问控制机制以及终端主机接入网络的安全性保证和完整性保护.边缘网络中每一台终端主机都必须通过严格的身份认证和平台完整性检查,通过严格的网络访问控制策略,才授权允许其访问网络.只有这样才能真正有效地降低感染网络病毒或遭受恶意攻击的可能性.

可信网络连接(TNC)概念正是为了解决上述平台认证和终端完整性保护问题,由可信计算工作组(TCG)最早在 2004 年提出,并得到了企业界的大力推广.TNC 体系结构的规范文档和标准协议正在逐步制定和完善中,最新的 TNC 体系结构规范文档^①已在 2008 年 4 月发布.TNC 是网络访问控制的开放解决方案,向终端提供安全性保证和完整性认证,最终实现终端主机安全接入网络.

TNC 架构不仅得到工业界的大力推广与支持,也引起了学术界的关注.在文献[1]中,作者采用 TNC 终端验证机制提高 P2P 网络中数据真实性和完整性,在文献[2]中作者建立了基于可信网络连接的数据采集系统访问控制模型,而在文献[3]中,作者将 TNC 架构应用到 Ad-Hoc 网络中解决节点缺乏网络保护的问题,如上大部分研究都是针对 TNC 架构在不同网络环境下的应用和扩展,而作为采用 Server-Client 通信模式的可信网络连接要真正发挥作用,系统自身就必须保证可信,特别是要保证平台认证过程和访问控制机制足够可信,因此可信网络连接的体系结构与各层通信协议的安全性研究就更显重要.

本文研究的重点在于可信网络连接自身的安全性问题.首先,根据最新的 TNC 体系结构规范和协议描述,提出了一种基于半马尔可夫过程(SMP)的安全量化分析方法,主要从认证性、机密性和完整性三方面评价指标来针对 TNC 实体进行安全性量化分析.该量化方法为 TNC 协议建立随机状态模型,

考虑协议交互过程中不同状态之间的转移变迁和驻留时间,通过 SMP 过程中安全状态和不安全状态的稳态概率来计算相关安全评价指标.

其次,通过分析发现,TNC 仍然存在安全隐患和威胁,主要表现为终端与服务器之间通信的认证性、机密性和完整性得不到足够的保护,容易给网络攻击者提供安全漏洞,因此本文针对 TNC 规范中不同层的接口协议,增加了可信认证和安全保护的增强机制,使得 TNC 系统本身具有较强的安全性,并通过安全量化分析方法进行验证.

最后,本文创造性地利用网络处理器 IXP2400 搭建了一套符合上述协议和机制的 TNC 原型系统,为 TNC 协议改进和安全分析提供了实际验证平台.

本文第 2 节介绍 TNC 架构的基本知识;第 3 节详细介绍 TNC 协议的安全性分析;第 4 节提出一种基于半马尔可夫过程的量化分析方法;第 5 节提出一套改进 TNC 的安全性增强机制;第 6 节介绍安全性指标计算和分析验证;第 7 节介绍 TNC 原型系统;最后对我们的工作进行总结和展望.

2 TNC 体系结构

可信网络连接(TNC)的思想是向终端接入网络之前提供安全性保证和完整性认证.通过认证服务器收集和评估终端主机的安全状态和可信信息,对请求访问网络的节点进行安全性和完整性认证,确定网络节点的安全级别和访问权限的判定,并依据判定结果执行访问策略,最终实现可信的网络访问控制机制,防止不安全终端接入和破坏网络.

图 1 完整地描述了 TNC 体系结构,作为一个开放解决方案,TNC 体系结构结合了目前已有的网络访问控制机制,比如 802.1X 等^[4].采取 Server-Client 模型,主要包括 3 类实体:访问请求点 AR、策略执行点 PEP 和策略决断点 PDP,其中 AR 是请求访问网络的实体,PDP 是进行访问控制策略判决的实体,而 PEP 是执行 PDP 所判决的控制策略的实体.具体细节参考 TNC 体系结构的规范文档^[5].

TNC 的完整性认证和访问策略授权的过程如下:当终端有网络连接请求时,AR 实体与 PDP 实体建立连接,开始完整性验证过程,AR 端的 IMC

① TCG Trusted Network Connect Architecture for Interoperability Specification Version 1.3 R6, published on 28 April, 2008

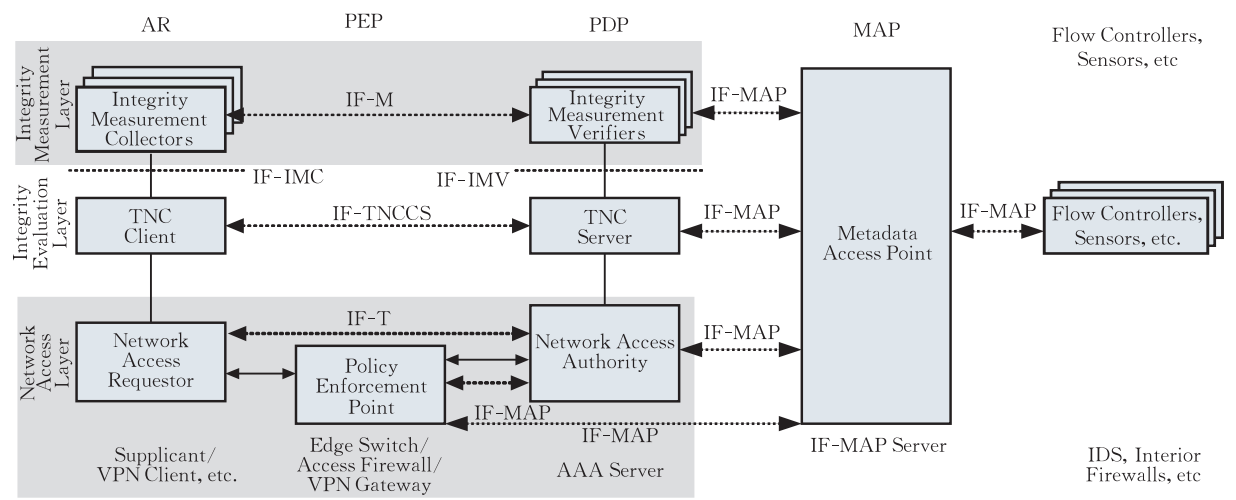


图 1 TNC 体系结构

开始进行完整性信息的收集,完整性信息包括终端主机的反病毒信息、防火墙信息、系统补丁更新信息等;然后 AR 将完整性信息通过 PEP 传递给服务器端的认证者 PDP;PDP 将获得的包含有完整性信息的 IMC 消息报告给 IMV 进行完整性验证,并进行安全评估,判决适当的访问控制策略和补救措施;随后 PDP 将访问控制策略的判决发送到 PEP 执行,并将补救隔离措施发送给 AR 端执行,直到满足完整性验证,才被授权接入网络。

TNC 的目标是保证终端用户的可信网络连接的建立和访问策略的授权,这是通过可信的平台认证的方法实现的,可信平台认证包括平台身份证明和完整性检查^[6]。其核心技术采用的是可信平台模块(TPM),这是含有密码运算部件和存储部件的芯片,可以提供可信的度量、存储和证明^[5]。作为一个工业界规范,TNC 体系结构并不是一个完全不同于以往设计的创新,而是整合了已有的访问控制机制和平台框架,所以没有必要重新为各实体间交互设计接口协议,这得到了越来越多的 IT 著名企业的支持和推广,包括 HP、Microsoft、Intel、IBM、Juniper、Symantec 等等,其中有的已经开发出了支持 TNC 规范的网络安全设备。

3 TNC 协议安全性分析

TNC 采用 Server-Client 通信模式,要保持 TNC 平台认证和访问控制的安全可靠,就必须首先保证 TNC 交互协议自身有足够的安全性,下面我们将依据相关的协议安全性评价指标,基于随机模型的分析方法,对各层接口协议中采取的安全机制

和可能存在的安全隐患进行安全性分析。首先,需要定义协议安全性的评价指标。

3.1 协议安全性评价指标

网络安全性通常被理解为在受到恶意攻击时计算机网络性能指标的反应,是一个综合性的概念,包含多种不同的属性,用以描述系统不同侧面的特性^[7],包括可靠性、可用性、可行性、机密性和完整性等等。部分属性指标在近几十年的研究中,已经有了一些广为接受的量化计算方法。而在本文中,针对 TNC 协议的安全性分析,主要考虑认证性、完整性和机密性三方面,定义如下:

协议安全性(protocol security)。它是指网络实体在网络交互过程中受到网络威胁或网络攻击时,抵御攻击和破坏,完成正常协议交互的能力,主要包括 3 种属性:认证性、完整性和机密性。

认证性(authenticity)。协议交互过程中,双方相互认可和证明身份合法,避免对合法用户的错误拒绝或者是对不合法用户的错误接受;

完整性(integrity)。协议交互过程中,不出现错误的系统变化或者被篡改的信息;

机密性(confidentiality)。协议交互过程中,交互信息不被未授权的用户获知。

构建协议安全性的系统分析和评价方法,需要从实际问题中抽象并建立对应的状态随机模型。当网络系统受到某种确定攻击的影响时,如果可以明确区分哪些系统状态满足认证性、机密性或完整性的话,我们就可以量化网络协议的各种指标。假定在所有的系统状态中, S_A 、 S_C 、 S_I 分别为满足认证性、机密性和完整性的 3 个不同状态集合,而系统稳定状态概率向量为 $\pi=(\pi_1,\pi_2,\pi_3,\cdots)$,其中 π_i 表示系

统处于 i 状态的稳定状态概率,则认证性 A 、机密性 C 和完整性 I 分别表示为

$$\begin{aligned} A &= \sum_{i \in S_A} \pi_i; \\ C &= \sum_{i \in S_C} \pi_i; \\ I &= \sum_{i \in S_I} \pi_i \end{aligned} \tag{1}$$

在定义了相关评价指标后,需要针对 TNC 各层接口协议中采取的安全机制和可能存在的安全隐患、面临的安全威胁进行分析总结。

3.2 针对各层接口协议的安全分析

3.2.1 IMC/IMV 协议层分析

在 AR 发起网络连接请求之前, TNCC/TNCS 要对 IMC/IMV 分别进行完整性验证, TNCC/TNCS 只与授权的 IMC/IMV 通信. 该认证过程在 AR 和 PDP 实体内部, 不涉及实体间通信, 通过基于硬件设备 (TPM) 的平台信任服务 (PTS) 保证其安全性。

3.2.2 TNCC/TNCS 协议层分析

TNCC/TNCS 在完整性验证握手之前会使用由 TPM 提供的身份证明密钥 AIK, 向对方提供平台的身份证明, 保证自身认证性. 但是 TNC 规范中提到关键假设: TNCC 和 TNCS 之间完整性信息和平台信任状认证信息的传递并没有自保护措施, 而是假定底层提供了两端通信的可靠性保护措施^[5]. 可见 TNCC 和 TNCS 之间通信的机密性和完整性完全依靠下层 IF-T 协议提供加密数据通道和认证机制来保证^[8]. 因此 TNCCS 接口存在的安全威胁主要来自于下层传输通道的机密性和完整性缺失, 并可能遭受针对 IF-T 协议攻击的后续攻击, 包括主动网络攻击 (导致完整性测量信息的暴露) 和被动网络攻击 (篡改完整性信息)。

另一方面, IF-TNCCS 协议用于承载 IMC-IMV 层消息, 当 IF-M 采取 CMS 加密协议之后, 保证了 IMC-IMV 层消息不被破解, 并不需要提供另外的保护机制, 但 IMC-IMV 层消息并不一定都采用 IF-M CMS 加密协议, IF-TNCCS 也有自己额外的信息 (比如维护 IMC-IMV 层消息的 Type, 进行消息的分发), 这些额外的信息缺乏有效的加密保护。

3.2.3 IF-T 协议层分析

根据图 1, IF-T 接口协议完成 NAA 和 NAR 之间的用户认证 (基于用户名/密码), 还提供了 NAR 和 NAA 之间 IF-TNCCS 层消息传递的通道安全保护. 根据 IF-T 规范文档中指出必须绑定隧道模式的

扩展认证协议 (Tunneled-EAP)^[9], 基于 EAP 的密码保护隧道来保证 NAA 和 NAR 之间的消息的完整性和机密性, 防止信息被篡改和偷听。

但是基于 EAP-TNC 初始请求进行协商的机制可能遭到恶意节点的中间人攻击^[10], 恶意节点通过控制 AR 成功通过 EAP 认证并捕获 IF-T 传递的消息, 破坏机密性和完整性, 并更进一步采取其它攻击手段破坏终端主机或者服务器. 具体的攻击方式见图 2, 攻击者植入木马成功控制 AR 后, 通过 AR 来成功套取 PDP 对于终端的 EAP-TNC 验证。

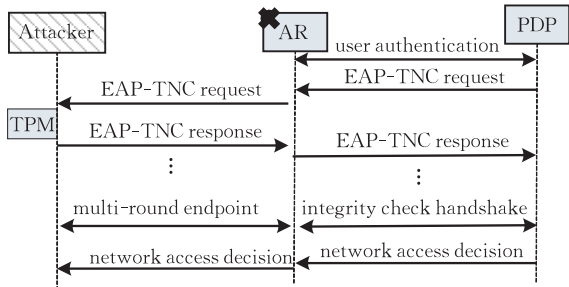


图 2 基于 EAP-TNC 的中间人攻击方式

3.2.4 IF-PEP 协议层分析

PEP 和 NAA 之间通信涉及到最终的网络访问策略, 也必须被认证和提供完整性保护. 根据 TNC-IF-PEP 规范^[11], TNC 是基于 AAA 认证框架的, 所以 IF-PEP 协议的安全威胁, 主要是 AAA 典型协议的漏洞造成, 以 RADIUS 为例, 伪装 NAA 采取针对 PEP 的 DOS 攻击以及中间人攻击, 而 IF-PEP 隐患的危害会导致关键决策信息的完整性和正确性无法得到保证。

3.2.5 NAR/PEP 之间分析

除了上述之外, TNC 还存在安全漏洞, 在完整性验证过程后 NAR 与 PEP 间缺乏安全保护机制. PEP 将网络访问策略判决发送给 NAR 之后, AR 访问网络的数据包发送到作为网关的 PEP 却并没有机密性和完整性保护, 恶意节点可以利用伪造 IP 方式冒充合法的 AR 发送数据包, 也可以在中间截取并篡改数据包内容, 加入恶意代码破坏网络. 尽管这一威胁在 TCG 发布的规范文档中并没有考虑, 但 TNC 作为一个网络访问控制平台, 确保终端安全地接入和访问网络是其最终目标, 所以如果不能确保 PEP 和 AR 之间的安全, 会影响整个系统的可信性。

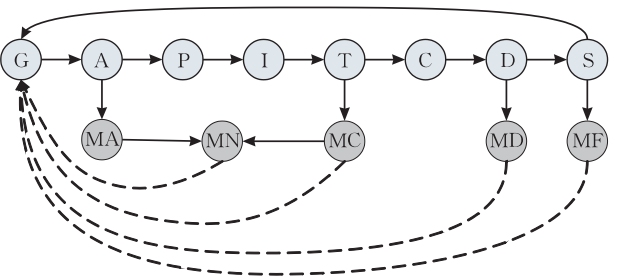
综上所述如表 1, 通过针对 TNC 各层接口协议的安全性分析, 发现 TNC 作为完整性认证和网络访问控制的平台框架, 其接口协议规范中尽管已经充分考虑了认证机制和安全协议, 但仍然可能存在着安全威胁和漏洞。

表 1 TNC 各层协议安全性分析

协议层	缺陷或漏洞	可能攻击方式	破坏安全属性
IF_TNCCS	针对 IF_T 协议攻击的后续攻击	主动网络攻击(导致完整性测量信息的暴露)和被动网络攻击(篡改完整性信息)	完整性、机密性
	当不采用 IF_M CMS 加密协议时无法保护 IMC/IMV 层消息	截取非 IF_M CMS 加密消息或 Type 消息	机密性
IF_T	基于 EAP_TNC 初始请求进行协商的机制可能遭到恶意节点的中间人攻击	中间人攻击	认证性、完整性、机密性
IF_PEP	AAA 典型协议的漏洞	DoS 攻击以及中间人攻击	完整性
NAR 与 PEP 之间	在完整性验证完成后 NAR 与 PEP 之间缺乏有效安全保护机制	恶意节点伪造 IP 方式冒充合法 AR 截取并篡改数据包内容	完整性、机密性

3.3 TNC 状态变迁模型

基于 TNC 体系结构(图 1)和各层协议安全性分析(表 1),可以得到 TNC 系统在完整性验证过程中带有网络攻击行为的状态变迁模型,如图 3.



- G: 网络连接请求发起
- A: NAA与NAR间用户认证(基于IF_T)
- P: TNCC与TNCs间平台认证(基于IF_TNCCS)
- I: IMC收集主机终端完整性信息
- T: AR和PDP间完整性信息传递(基于IF_TNCCS)
- C: IMV验证AR端完整性信息
- D: PDP确定AR访问策略并传递给PEP执行(基于IF_PEP)
- S: Ar完成可信连接并成功访问网络
- MA: 初始请求协商时的中间人攻击(针对IF_T)
- MN: IF_T攻击成功后的后续攻击(针对IF_TNCCS)
- MC: 破解非IF_M CMS加密的IMC/IMV层消息(针对IF_TNCCS)
- MD: 利用AAA典型协议漏洞的攻击(针对IF_PEP)
- MF: 伪造IP冒充合法AR截取数据包(针对NAR和PEP之间)

图 3 TNC 系统带有攻击行为的状态变迁模型

图 3 所示的状态变迁模型描述了 TNC 系统在正常完整性验证过程以及遭受网络攻击时的动态行为,共包括 8 个安全状态 {G,A,P,I,T,C,D,S} 和 5 个不安全状态 {MA,MC,MD,MF,MN}.

在网络实体正常交互过程中,由终端用户首先发起网络连接请求,进入状态 G;基于 TNC 协议架构,NAA 和 NAR 之间会首先基于 IF_T 接口协议进行用户身份认证(状态 A)以及基于 IF_TNCCS 的平台认证(状态 P);随后 IMC 开始收集主机终端完整性信息(状态 I),传递给 PDP(状态 T),由 PDP 对应 IMV 进行完整性验证(状态 C),然后 PDP 确认 AR 访问策略,由 PEP 执行(状态 D),最后 AR 完成可信连接后成功访问网络(状态 S).

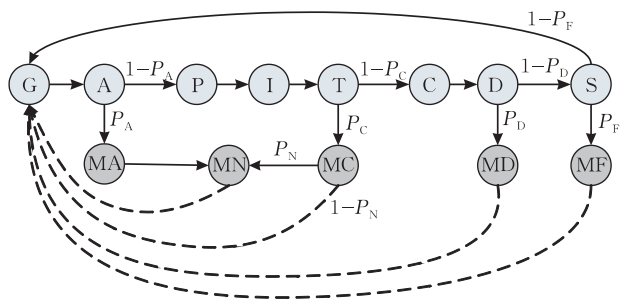
另外图 3 中 5 个不安全状态分别为:由状态 A 可能引起的初始请求协商时针对 IF_T 的中间人攻击过程(状态 MA);在状态 T 时被破解非 IF_M CMS 加密的 IMC/IMV 层消息(状态 MC);在状态 D 时针对 IF_PEP 的利用 AAA 典型协议漏洞的攻击(状态 MD);在状态 S 完成验证后,伪造 IP 冒充合法 AR 截取数据包(状态 MF);以及状态 MA 在 IF_T 攻击成功后针对 IF_TNCCS 的后续攻击,或者是 MC 状态的后续攻击(状态 MN).图中的虚线表示攻击成功后导致可信网络连接失败,重新开始请求连接,回到正常状态 G.

在建立 TNC 系统的协议安全随机模型之后,需要通过求解模型的定量分析方法来刻画协议安全性的指标特性以及网络攻击对安全性的影响.

4 基于半马尔可夫过程的安全量化分析

文献[7]指出,随机模型方法更易于网络系统状态进行全面有效的描述,精确刻画网络系统随机行为,便于计算各种安全性能指标.本文采取基于半马尔可夫过程(SMP)的安全量化分析方法.在 SMP 过程中,状态的驻留时间可以是任意分布;且它们的 PDF 可以依赖于当前状态和下一状态^[12],这符合 TNC 协议和安全攻击行为的状态变迁特征.图 3 所描述的系统 SMP 模型对应于图 4 所描述的嵌入式离散时间马尔可夫链(DTMC),首先计算 DTMC 过程的稳定状态概率,以及每个状态的平均驻留时间,来得到 SMP 模型的稳态概率,从而计算与安全性相关的 3 个量化评价指标.

TNC 完整性验证过程被认为是在离散状态空间 $X_s = \{G, A, P, I, T, C, D, S, MA, MC, MD, MF, MN\}$ 上的随机过程 $\{X(t): t \geq 0\}$,为了分析 SMP 稳态概率,需知道两类参数:(1) X_s 中每个状态 i 的平均驻留时间 h_i ;(2) 不同状态 ij 之间的变迁概率



P_A : 初始请求协商时的中间人攻击成功的概率
 P_C : 破解非 IF_MCMS 加密的 IMC/IMV 消息成功的概率
 P_D : 利用 AAA 典型协议漏洞的攻击成功的概率
 P_F : 伪造 IP 冒充合法 AR 截取数据包成功的概率
 P_N : IF_T 攻击成功后的后续攻击成功的概率

图 4 TNC 完整性验证的 DTMC 过程

p_{ij} , 主要是安全状态转移到不安全状态的变迁概率。

SMP 模型具体求解算法如下:

第 1 步. 基于图 4 的 TNC 完整性验证过程的 DTMC 过程, 通过式(2)、(3)计算 DTMC 稳态概率 ν .

$$\mathbf{v} = \mathbf{v} \cdot \mathbf{P} \quad (2)$$

$$\sum_i \nu_i = 1 \quad (3)$$

其中 \mathbf{P} 为图 4 中 DTMC 过程状态变迁概率矩阵, $\mathbf{v} = [\nu_G, \nu_A, \nu_P, \nu_I, \nu_T, \nu_C, \nu_D, \nu_S, \nu_{MA}, \nu_{MC}, \nu_{MD}, \nu_{MF}, \nu_{MN}]$, $i \in X_S = \{G, A, P, I, T, C, D, S, MA, MC, MD, MF, MN\}$.

通过式(2)计算出稳态概率之间的关系:

$$\begin{aligned} \nu_G &= (1-P_F)\nu_G + \nu_{MC} + \nu_{MD} + \nu_{MF} + \nu_{MN}, \\ \nu_A &= \nu_G, \quad \nu_P = (1-P_A)\nu_A, \quad \nu_I = \nu_P = \nu_T, \\ \nu_C &= (1-P_C)\nu_T, \quad \nu_D = \nu_C, \quad \nu_S = (1-P_D)\nu_D, \\ \nu_{MA} &= P_A\nu_A, \quad \nu_{MC} = P_C\nu_T, \quad \nu_{MD} = P_D\nu_D, \\ \nu_{MF} &= P_F\nu_S, \quad \nu_{MN} = \nu_{MA} + P_N\nu_{MC} \end{aligned} \quad (4)$$

将式(4)代入式(3), 可解得 DTMC 过程中 G 状态的稳态概率如式(5):

$$\nu_G = 1 / (4 + (1-P_A)(2 + P_N P_C) + (1-P_A)(1-P_C)[2 + P_F(1-P_D)]) \quad (5)$$

其它状态的稳态概率可以通过式(4)、(5)得到。

第 2 步. 通过半马尔可夫模型计算 SMP 过程的稳态概率 π , 为此必须确定每个状态 i 的平均驻留时间 h_i , h_i 是由状态 i 按照协议完成对应交互流程的随机时间所决定的。在本文的 SMP 模型中, 不失一般性, 我们假设正常 8 个状态的平均驻留时间 h 满足指数分布, 如 $h_G = 1/\lambda_G$, $h_A = 1/\lambda_A$ 等; 而对于攻击行为所导致的 5 个危险状态, h 与正常状态的平均驻留时间由于存在攻击者的攻击行为而有所不同, 参考文献[13], 满足 $HypoEXP(\lambda_1, \lambda_2)$ 或者

Weibull(λ, α), 如状态 h_{MA} 和 h_{MN} 可以表示为式(6):

$$h_{MA} = \left(\frac{1}{\lambda_{MA1}} + \frac{1}{\lambda_{MA2}} \right); \quad h_{MN} = \left(\frac{1}{\lambda_{MN}} \right)^{1/\alpha_{MN}} \Gamma \left(1 + \frac{1}{\alpha_{MN}} \right) \quad (6)$$

而 SMP 模型的稳态概率可以通过 DTMC 稳态概率和平均驻留时间通过如下公式计算而得^[14]:

$$\pi_i = \frac{\nu_i h_i}{\sum_j \nu_j h_j}, \quad i, j \in X_S \quad (7)$$

根据式(4)、(5)、(7)可以得到基于半马尔可夫模型所描述的 TNC 完整性验证和访问策略授权过程的每个状态的稳定概率, 表示如下:

$$\begin{aligned} \pi_G &= h_G / (\{h_G + h_A + P_A(h_{MA} + h_{MN}) + (1-P_A) \times \\ &\quad [h_P + h_I + h_T + P_C h_{MC} + P_N P_C h_{MN} + (1-P_C) \times \\ &\quad [h_C + h_D + P_D h_{MD} + (1-P_D) \times [h_S + P_F h_{MF}]]\}]), \\ \pi_A &= \frac{h_A}{h_G} \pi_G, \quad \pi_P = \frac{(1-P_A)h_P}{h_G} \pi_G, \quad \pi_I = \frac{(1-P_A)h_I}{h_G} \pi_G, \\ \pi_T &= \frac{(1-P_A)h_T}{h_G} \pi_G, \quad \pi_C = \frac{(1-P_C)h_C}{h_T} \pi_T, \\ \pi_D &= \frac{(1-P_C)h_D}{h_T} \pi_T, \quad \pi_S = \frac{(1-P_D)h_S}{h_D} \pi_D, \\ \pi_{MA} &= \frac{P_A h_{MA}}{h_A} \pi_A, \quad \pi_{MC} = \frac{P_C h_{MC}}{h_T} \pi_T, \quad \pi_{MD} = \frac{P_D h_{MD}}{h_D} \pi_D, \\ \pi_{MF} &= \frac{P_F h_{MF}}{h_S} \pi_S, \quad \pi_{MN} = \frac{h_{MN}}{h_{MA}} \pi_{MA} + \frac{P_N h_{MN}}{h_{MC}} \pi_{MC} \end{aligned} \quad (8)$$

第 3 步. 根据 SMP 模型的稳定状态概率向量, 计算相关安全属性的量化指标。根据表 1 的归纳以及式(1)的定义, 则本文 TNC 系统所考虑的认证性 A_{TNC} 、机密性 C_{TNC} 和完整性 I_{TNC} 分别表示为

$$\begin{aligned} A_{TNC} &= \sum_{i \in S_A} \pi_i = 1 - \pi_{MA} \\ C_{TNC} &= \sum_{i \in S_C} \pi_i = 1 - (\pi_{MA} + \pi_{MC} + \pi_{MF} + \pi_{MN}), \\ I_{TNC} &= \sum_{i \in S_I} \pi_i = 1 - (\pi_{MA} + \pi_{MD} + \pi_{MF} + \pi_{MN}). \end{aligned}$$

上述公式主要参考表 1, 将对应的不安全状态中所引入的攻击行为和安全属性相关联。例如, 不安全状态 MA 是因为初始协商阶段的中间人攻击而引入的, 可能会降低系统的认证性、机密性和完整性, 所以在 3 个安全量化指标中应该全部剔除 MA 的状态, 而状态 MC 是因为针对未 CMS 加密的 IMC/IMV 消息的破解行为, 会降低系统的机密性, C_{TNC} 将不包括 MC 状态。总之, 按照本文所介绍的安全量化计算方法, 通过采用 SMP 模型分析方法而得的公式组(8)、(9), 可以精确量化 TNC 系统在协议安全性 3 种评价指标, 进而完成安全量化分析。

5 TNC 协议改进机制

为了弥补 TNC 各层接口协议存在的安全威胁,避免可能的攻击,增加数据完整性和机密性保护、认证机制,从而增强协议安全性,在符合 TNC 设计规范的前提下,本文提出了安全性增强的改进机制.

5.1 IF-TNCCS 协议层

IF-TNCCS 层不仅负责完整性验证,由底层的 IF-T 保证足够安全的传输通道,同时负责承载 IMC-IMV 消息,由于不同类型 IMC 可能对应单个或多个 IMV,所以在不采用 IF-M CMS 加密消息时,需要在 IF-TNCCS 层进行消息加密,保证上层完整性验证实体的安全通信.

5.2 IF-T 协议层

IF-T 接口协议可能存在的安全威胁,主要包括进行解密攻击来暴露 TNC 数据和在初始访问请求时针对隧道 EAP 协议的中间人攻击,前者必须要使用不同的传输密钥以及更安全的加密算法来保证不被攻击者破解;后者抵御中间人攻击,需要在用户和平台认证过程中将 TPM 和证书相关联,建立信任链和检查证书的可信签名.为此,建立 NAR 和 NAA 之间相互平台认证.

因为在 NAR 发送初始访问请求时,容易发生针对隧道 EAP 协议的中间人攻击,必须在这之前建立 NAR 和 NAA 之间的平台认证机制,用 TPM 提供 AIKNAR,为客户端发送的平台认证密钥增加可信的证书签名,使得 AR 端 TPM 的可信与证书相关联,并将密钥证书在 CA 注册时提供.这样当服务器端进行验证时,将从签名的客户认证密钥中得到的 AIK_{NAR}和 CA 提供的 AIK_{NAR}比较,就可以保证该客户身份的真实性,抵御中间人攻击.同理 NAA 端也采用 AIK_{NAA}进行可信证书签名,让 NAR 认证 NAA 的合法身份.除此之外,为了更加有效地抵御中间人攻击,最好定期更换双方传输的加密密钥,即使数据包被恶意节点截获也无法截取或篡改.

5.3 IF-PEP 协议层

对于 IF-PEP 接口,由于 RADIUS 协议可能存在的漏洞较多,以 DOS 攻击和中间人攻击最典型,需要加强 NAA 发送的策略判决上数字签名的验证.同时,建立 PEP 端网络访问数据包的增强验证机制.

当 TNC 完成完整性认证,PEP 将访问策略发

送给 AR 后,AR 开始访问网络,通过网关 PEP 发送数据包给外网.由于 TCG 规范文档中并没有针对终端在完整性验证后访问网络时 AR 和 PEP 之间的保护机制,如不能保证 AR 数据包机密性和完整性,恶意节点可以利用伪造 IP 方式冒充合法的 AR,发送含有病毒的数据包或者攻击其它主机;也可以在截取并篡改数据包内容,加入恶意代码破坏网络.

为了在 PEP 端增强对网络访问数据包的验证机制,保证其完整性和机密性,首先在 NAA 发送访问决策判定时建立访问控制列表(ACL),列表项包括对于 AR 的 IP 地址、连接 ID、传输加密密钥 Traffic Key(由 IPSec SA 生成)、访问策略(3 种:允许、拒绝、隔离)等,见图 5.

Access Control List				
IP Addr	ID _{AR}	Traffic Key	Access Policy	Optional
⋮				

图 5 访问控制列表项

参考 IPSec 协议,AR 端数据包采用 IPSec AH+ESP 头部封装,参见图 6,数据包加密密钥使用 ACL 表中的传输加密密钥,除了在 AH 头部和 ESP 头部对整个数据包进行认证外,还在 payload 里加入 ID_{AR}用于 AR 端身份认证,当 PEP 接收到封装后的数据包,首先进行包头部(AH)和整体(ESP)的完整性验证,然后通过 IP 地址查找对应的访问控制列表,找到对应的传输加密密钥(Traffic Key)用于解密数据包有效载荷,通过解密后获取的 ID_{AR}和 ACL 中查找到的 ID_{AR}进行对比,进行身份认证.以此保证 AR 端网络访问数据包的完整性、机密性.

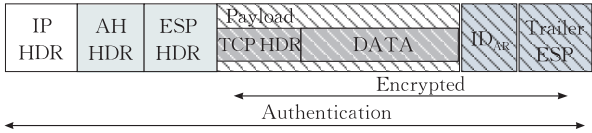


图 6 AR 端数据包封装格式

5.4 NAR-PEP 协议层

针对 NAR 和 PEP 之间以及 PEP 和 NAA 之间数据传输的机密性和完整性验证,还必须建立可靠连接的安全联盟.为此,建立 NAR 与 PEP 之间、PEP 与 NAA 之间的 IPSec 安全联盟(IPSec SAs).

为了保证完整性认证握手过程在底层消息传输的机密性和完整性,需要得到安全可靠的传输加密密钥,建立可靠的 IPSec 安全联盟连接.而在 NAR 与 PEP、PEP 和 NAA 之间建立 IPSec SA,既可以

保证 NAR 和 PEP、PEP 和 NAA 之间消息传输过程的机密性和完整性,也可以抵御欺诈、偷听、伪造等攻击,定期的 SA 更新,可以防止中间人攻击. 另外在 PEP 和 NAA 之间建立的 SA 可以为 IF-PEP 过程提供安全保证. 本文采取 IKE 协议,在 NAR 和 NAA 相互认证结束后,保证没有中间人攻击的前提下(IKE 第 1 阶段交互可能遭受中间人攻击),分别增加 NAR 与 PEP 和 NAA 和 PEP 之间的 IKE 交互,采用主动模式^[15]建立 IKE 安全联盟. 以 NAR 和 PEP 为例,消息流程见图 7,采用 Diffie-Hellman 密钥交换,获取双方的共享密钥,在 NAR 和 PEP 之间建立 IKE SA,提供两端之间数据加密、认证和数据完整性,同样在 PEP 和 NAA 之间也建立 IKE SA,注意在 IKE SA 建立之后,DH 密钥不再使用.

在 IKE SA 建立后可以生成多种密钥用于下面不同阶段的数据加解密过程和签名认证过程. 为了保证传输的安全,在 IKE SA 的保护之下,IKE 第 2 阶段交互建立 IPSec SA. 这一过程由 IKE SA 生成 Traffic Key 密钥,提供数据传输的加密保证(见图 7)、NAR 和 PEP 之间协会 IPSec 的认证和加密算法以及各自的身份、IP 地址和连接 ID,最终建立两个单向的 IPSec SA,为经过身份和地址验证通过的数据流进行 IPSec 加密和完整性保护,算法可以采用 ESP 3DES/SHA1 或者 AH/SHA1 等等. IPSec

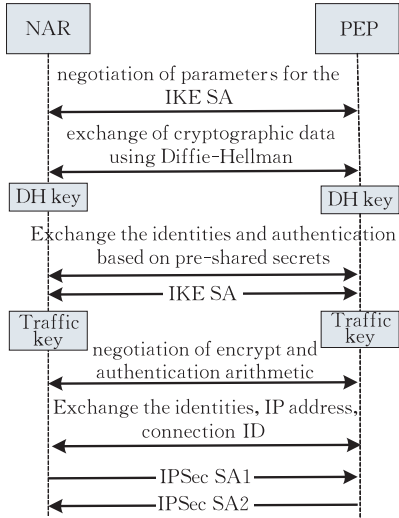


图 7 NAR 与 PEP 之间 IPSec SA 建立消息流程

SA 都需要定期更新,保证 SA 的有效性. 如果 IKE SA 有效,只需要重新进行第 2 阶段即可,否则将重新开始图 7 的交互过程建立新的 IPSec SA.

总结 TNC 安全性增强的改进机制,得到如图 8 所示的 TNC 各实体间典型消息流程与接口协议. 通过建立 NAR 和 NAA 之间相互平台认证,将 AR 端 TPM 的可信与证书相关联,保证 NAR 和 NAA 合法身份,抵御针对隧道 EAP 协议的中间人攻击;分别建立 NAR、NAA 与 PEP 之间的 IPSec SA,保证完整性认证握手过程在底层消息传输的机密性和

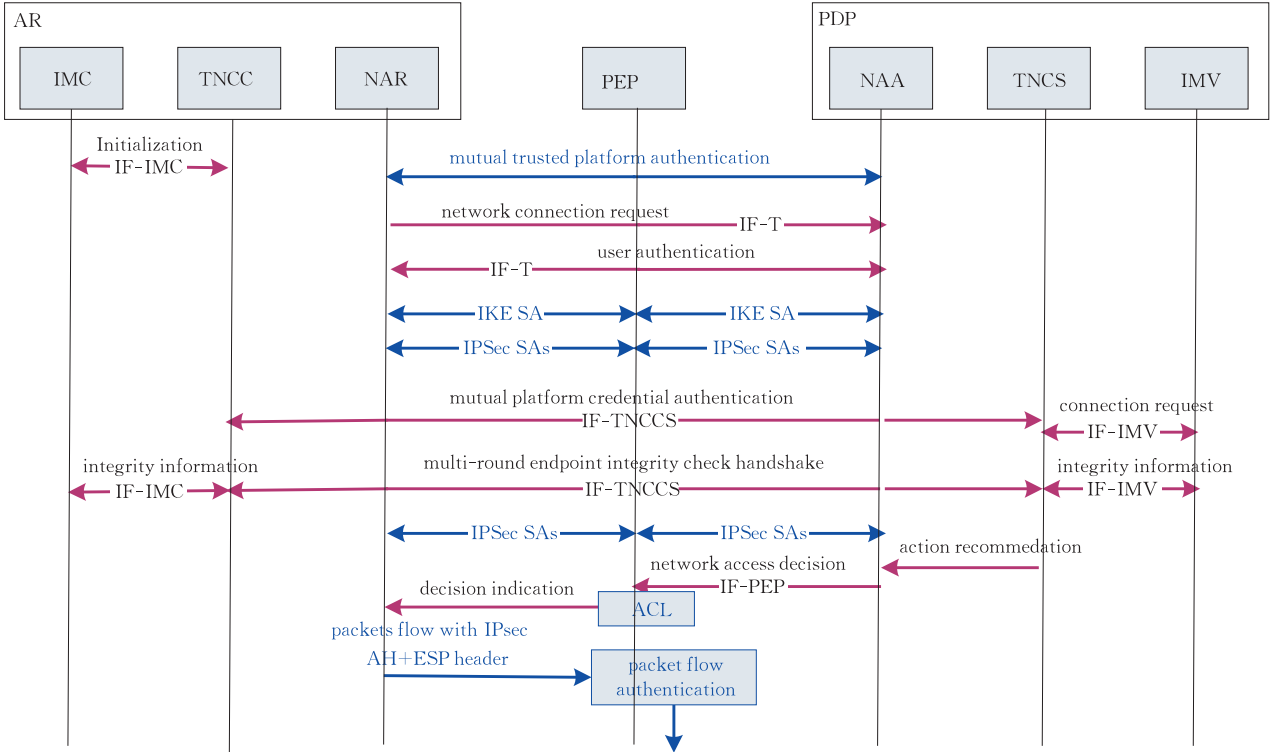


图 8 采用安全性增强机制后典型消息流程与接口协议

完整性,并为 IF-T 和 IF-PEP 协议提供安全可靠的加密密钥;建立 PEP 端网络访问数据包的增强验证机制,保证 AR 端网络访问数据包的完整性、机密性和认证性,防止数据包被篡改或伪造 IP。通过以上机制,在遵循 TNC 整体架构设计规范的前提下,加强 TNC 体系结构在底层传输的完整性和机密性保护,增强各实体之间相互认证的可靠性,从整体上增强了 TNC 架构的协议安全性。

6 安全性指标计算和评价

本节中,首先进行 TNC 协议安全性指标的数值计算分析,下面进行模型参数值初始化。

变迁转移概率 P : P_A 表示状态 A 到状态 MA 的转移概率,也是初始请求协商时的中间人攻击成功的概率,在没有建立 NAR 和 NAA 之间相互平台认证机制的情况下,设 $P_A=0.1$;而 P_C 是状态 C 破解非 CMS 加密的 IMC/IMV 层消息成功的概率,设 $P_C=0.12$; P_D 是利用 AAA 典型协议漏洞的攻击成功的概率,设 $P_D=0.1$; P_F 是伪造 IP 冒充合法 AR 截取数据包成功的概率,设 $P_F=0.1$; P_N 是 IF_T 攻击成功后的后续攻击成功的概率,设 $P_N=0.2$ 。

平均驻留时间 h_i : 根据第 4 节的分析, h_i 是由状态 i 按照协议完成交互流程的随机时间所决定的,正常 8 个状态的驻留时间满足指数分布,假设单位时间为 1 的话,平均驻留时间 $h_G=h_A=h_P=h_T=h_D=h_S=0.5$,完整性信息收集和验证过程需要驻留更多的时间,所以 $h_I=h_C=1$ 。而对于攻击行为所导致的 5 个危险状态, h 与正常状态的平均驻留时间由于存在攻击者的攻击行为而有所不同。对于 MA 和 MD 状态,针对 IF_T 和 IF-PEP 漏洞的中间人攻击成功的时间会偏长 $h_{MA}=h_{MD}=3$,而破解非 CMS 加密的 IMC/IMV 层消息耗费的平均时间 $h_{MC}=2$,MF 和 MN 状态平均驻留时间为 $h_{MF}=1.5$, $h_{MN}=1.5$ 。

根据上面参数以及式(8)可得结果如下:

$$\begin{aligned} \pi_G &= \pi_A = 0.0928, \pi_P = 0.0835, \pi_I = 0.1671, \\ \pi_T &= 0.0835, \pi_C = 0.1470, \pi_D = 0.0735, \\ \pi_S &= 0.0662, \pi_{MA} = 0.0557, \pi_{MC} = 0.0401, \\ \pi_{MD} &= 0.0441, \pi_{MF} = 0.0198, \pi_{MN} = 0.0339. \end{aligned}$$

根据式(9)计算安全性 3 种量化指标可得,认证性 $A_{TNC} = 0.9443$,机密性 $C_{TNC} = 0.8505$,完整性 $I_{TNC} = 0.8465$ 。

下面,为了更好地验证安全性增强协议的有效性和必要性,针对改进型 TNC 协议进行安全量化

分析和比较。在采用了安全性增强机制后,会改变 SMP 模型中不安全状态的变迁概率,例如建立 NAR 和 NAA 之间相互平台认证,将降低初始请求协商时的中间人攻击成功的概率, $P_A=0.05$;由于 PEP 端和 NAA 建立安全联盟,降低了利用 AAA 典型漏洞的攻击成功概率, $P_D=0.05$,降低了 AAA 建立 PEP 端网络访问数据包的增强验证机制降低伪造 IP 冒充合法 AR 截取数据包成功的概率, $P_F=0.05$;而平均驻留时间参数保持不变。

根据上面参数以及式(8)可得结果如下:

$$\begin{aligned} \pi_G &= \pi_A = 0.0957, \pi_P = 0.0909, \pi_I = 0.1819, \\ \pi_T &= 0.0909, \pi_C = 0.1601, \pi_D = 0.0800, \\ \pi_S &= 0.0760, \pi_{MA} = 0.0287, \pi_{MC} = 0.0437, \\ \pi_{MD} &= 0.0240, \pi_{MF} = 0.0114, \pi_{MN} = 0.0209. \end{aligned}$$

根据式(9)计算安全性 3 种量化指标可得,认证性 $A_{TNC} = 0.9713$,机密性 $C_{TNC} = 0.8953$,完整性 $I_{TNC} = 0.9150$ 。

由图 9 可以看出采取安全性增强机制后的 TNC 协议比原始 TNC 在 3 个安全性评价指标方面均有所提高,特别是机密性和完整性指标提高显著。由此也证明了安全性增强机制的必要性和有效性。

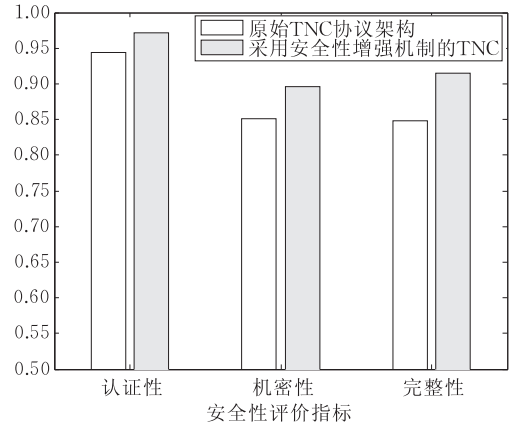


图9 原始和改进型 TNC 3 种安全性评价指标比较

接下来我们分析了不同参数变量对于安全性评价指标的影响。由于可变参数太多,对于不同状态的稳态概率影响不同。不失一般性,考虑不安全状态 MA 作为范例,与之相关的参数是初始请求协商时的中间人攻击成功的概率,即到达 MA 状态的变迁概率 P_A 和状态 MA 的驻留时间 h_{MA} 。

如图 10 所示,认证性指标和 P_A 、 h_{MA} 的函数变化关系紧密,由于 MA 状态是唯一影响认证性的不安全状态,而随着 P_A 、 h_{MA} 的增加,不安全状态的稳态概率是明显增加的,也使得认证性急剧降低。所以为了保证 TNC 协议的高认证性,必须尽可能降低

初始请求协商时的中间人攻击成功的概率 P_A , 或者及时发现攻击, 减少状态 MA 的驻留时间。

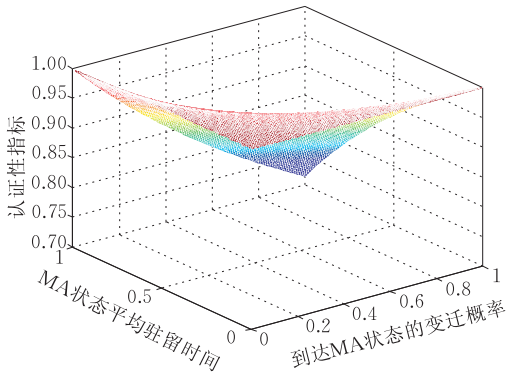


图 10 认证性指标与 P_A 、 h_{MA} 的函数变化图

图 11 和图 12 描述了机密性和完整性指标和 P_A 、 h_{MA} 的函数变化关系图, 从图可知, 机密性、完整性随 MA 状态的平均驻留时间变化较明显, 而 P_A 变化影响不大, 所以仅仅防范协商时的中间人攻击还无法显著提高 TNC 协议的机密性、完整性, 需要其它措施来保证。

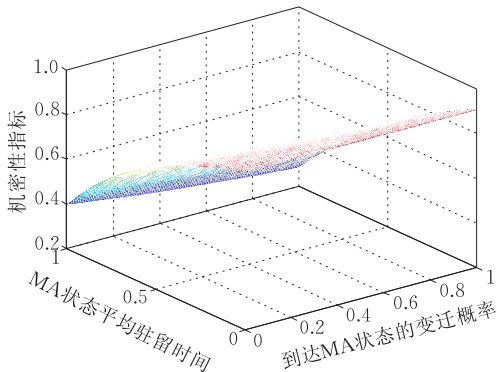


图 11 机密性指标与 P_A 、 h_{MA} 的函数变化图

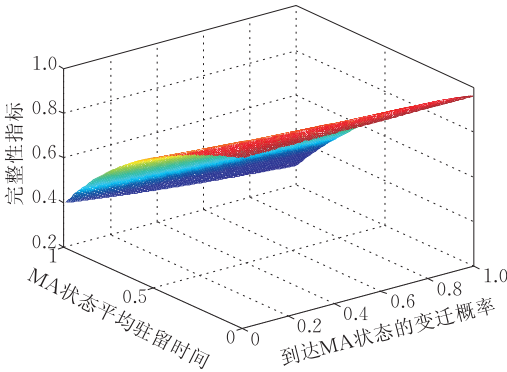


图 12 完整性指标与 P_A 、 h_{MA} 的函数变化图

7 协议改进后的 TNC 系统实现

在上述对 TNC 架构的安全量化分析以及安全

性增强机制的基础上, 本文提出并搭建了一个实际的基于网络处理器的改进后 TNC 原型系统, 为进一步研究 TNC 架构在实际工作条件下安全性的保证以及安全性增强机制对于 TNC 整体性能的影响等问题提供了验证平台。

该原型系统设计方案是基于网络处理器平台, 图 13 为基于 IXP2400 的 TNC 原型系统, 各实体件接口协议采用 TCG 发布的 TNC 库函数实现. 利用 IXP2400 含有 8 个多线程微引擎 (MicroEngines) 作为数据通道以及一个 XScale 通用处理器的特点, 采用基于服务器的 PEP 设计方法, 将 TNC 的 PEP 和 PDP 实体分别实现在微引擎和 XScale 上, 这样 IXP2400 的控制平面 XScale 完成认证服务器功能, 而数据平面的微引擎完成代理网关的功能。

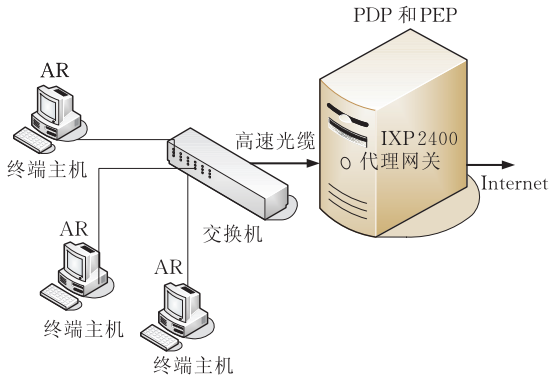


图 13 基于 IXP2400 的 TNC 原型系统架构

8 总结与展望

可信网络连接着眼于解决终端接入网络的安全性问题, 利用可信平台模块的硬件设备提供安全服务, 构建基于平台认证和终端完整性保护的访问控制平台, 为每一个终端提供安全可靠的访问策略. 为了 TNC 能提供安全可靠的访问控制策略, TNC 系统自身必须具有足够的安全性, 特别是要保证平台认证过程和访问控制机制足够可信。

本文突出贡献在于, 针对 TNC 体系结构和协议规范, 提出了一种基于半马尔可夫过程 (SMP) 的安全量化分析方法, 主要从认证性、机密性和完整性三方面评价指标来, 针对 TNC 实体进行安全性量化分析. 该量化方法为 TNC 协议建立随机状态模型, 考虑协议交互过程中不同状态之间的转移变迁和驻留时间, 通过 SMP 过程中安全状态和不安全状态的稳态概率来计算相关安全评价指标。

此外, 本文根据目前最新的 TNC 体系结构规

范和协议描述进行安全性分析,并根据 TNC 存在的安全威胁和漏洞,提出了一套增强安全性的机制,在遵循 TCG 关于 TNC 体系结构整体架构设计规范的前提下,加强 TNC 体系结构在底层传输的完整性和机密性保护,增强各实体之间相互认证的可靠性,提高 TNC 抵御各类恶意攻击的能力,从整体上增强 TNC 架构的安全性.

最后本文还提出了基于 IXP2400 网络处理器的 TNC 原型系统,搭建了 TNC 的可信验证平台.

未来将结合不断完善的 TNC 规范文档,深入研究 TNC 安全性问题,包括在完整性验证和保护的过程中不仅考虑终端,还考虑对于网络相关设备的完整性测量的问题,以及由于 IF-TNCCS 协议的通信效率要求,IF-MAP 接口的安全性保证,如何整合 PDP 和其它网络监控设备(IDS, IPS, Firewalls 等)联动实施动态访问控制等等问题. 同时还将在本文的研究工作的基础上,进一步分析 TNC 可能面对的安全威胁,并通过 TNC 的可信验证平台分析安全性增强机制对于 TNC 框架整体的安全与性能影响.

参 考 文 献

[1] Zhang Xin-Wen, Chen Song-Qing, Ravi Sandhu. Enhancing data authenticity and integrity in P2P systems. *IEEE Internet Computing*, 2005, 9(6): 42-49

[2] Xiang Dong, Wang Run-Xiao, Shi Cheng-Ji, Jiang Xiao-Peng. Trusted network connect based on access control model for data acquisition system. *Application Research of Computers*, 2006, 23(12): 157-158(in Chinese)

(向冬, 王润孝, 石乘齐, 姜晓鹏. 基于可信网络连接的数据采集系统访问控制模型. *计算机应用研究*, 2006, 23(12): 157-158)

[3] Xu Gang, Borcea Cristian, Iftode Liviu. Trusted application-centric Ad-Hoc networks//*Proceedings of the MASS07*. Pisa,

Italy, 2007

[4] IEEE802. Port-based network access control. *IEEE Std 802.1X-2001*, June 2001

[5] Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability Specification Version 1.3. Release 6 TCG Published, April, 2008: 7-35

[6] Trusted Computing Group. TCG 1.1b Specification Architecture Overview. Revision 0.14, March, 2004

[7] Lin Chuang, Wang Yang, Li Quan-Lin. Stochastic modeling and evaluation for network security. *Chinese Journal of Computers*, 2005, 28(12): 1943-1956(in Chinese)

(林闯, 汪洋, 李泉林. 网络安全的随机模型方法与评价技术. *计算机学报*, 2005, 28(12): 1943-1956)

[8] Trusted Computing Group. TCG Trusted Network Connect TNC IF-TNCCS Specification Version 1.1 Revision 1.0, TCG published, February, 2007: 20

[9] Trusted Computing Group. TCG Trusted Network Connect TNC IF-T: Protocol Bindings for Tunneled EAP Methods Specification Version 1.0 Revision 3, TCG published, May, 2006: 9-30

[10] Asokan N, Niemi Valtteri, Nyberg Kaisa. Man in the middle attacks in tunneled authentication protocols. *Nokia Research Center, Finland*, 2002

[11] Trusted Computing Group. TCG Trusted Network Connect TNC IF-PEP: Protocol Bindings for RADIUS Specification Version 1.1 Revision 0.7, TCG published, February, 2007

[12] Lin Chuang. *Stochastic Petri Nets and Performance Evaluation*. 2nd Edition. Beijing: Tsinghua University Press, 2005 (in Chinese)

(林闯. *随机 Petri 网和系统性能评价*. 第 2 版. 北京:清华大学出版社, 2005)

[13] Bharat B M, Katerina G. A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation*, 2004, 56(1-4): 167-186

[14] Trivedi K S. *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*. 2nd Edition. New York: Wiley, 2001

[15] RFC2409. The Internet Key Exchange (IKE). November, 1998



LIN Chuang, born in 1948, Ph. D., professor, Ph. D. supervisor. His current research interests include computer networks, performance evaluation, network security, Petri net

LUO An-An, born in 1984, Ph. D. candidate. His research interests include network architecture, network security, trust management.

theory, trustworthy networks and trustworthy computing.

WANG Yuan-Zhuo, born in 1978, Ph. D., assistant researcher. His research interests include trusted network, grid computing, network QoS, and security evaluation.

DENG Fa-Chao, born in 1985, M. S. candidate. His research interests include network access control, network security.

CHEN Zhen, born in 1976, Ph. D., lecturer. His research interests include peer-to-peer system, trusted computing and high-speed network security.

Background

Trusted Network Connect (TNC) is defined and promoted by TCG lately in 2004, which emphasizes endpoint security for network access; TNC uses Trusted Platform Module (TPM) to construct an open solution for endpoint connection to corporate network depending on platform authentication and endpoint integrity measurement and protection. Being an important part of trusted network architecture, TNC gets more and more focused by industry companies, such as Microsoft, Cisco, Intel, some of them have already promoted network products which support TNC specification. And in April 2008, TCG published latest TNC protocol 1.3 with IF-MAP on conference of Interop 2008.

With its deeper research and application development, whether it is enough trustworthy during TNC platform authentication and access control becomes a key problem. In the

paper, we mainly focus on the trustworthy problem of TNC. First, we proposed a novel security quantifying method which is based on semi-Markov processes. And then, according to the potential threat and security holes during typical message flow and access authorization process in TNC specification, we proposed a set of trustworthy enhanced mechanisms, which is verified by our security quantifying method. Finally a TNC prototype system framework based on IXP2400 network processor is built to be a performance evaluation and trustworthy verification platform.

This work is supported in part by several National Natural Science Foundation of China Project (90718040, 60673187, 60673054, 60673160, 60803123). Currently, the author is doing research on trusted computing and computing trustworthy.