

基于可信计算技术的 P2P 网络连接方案

梁志宏¹, 胡朝辉¹, 谭一鸣², 刘文娟²

(1 广东电网公司电力科学研究院, 广东 广州 510080; 2 中标软件有限公司, 上海 200030)

摘 要: 提出了基于可信计算技术实现对接入 P2P 网络终端的可信验证, 以防止不可信的终端接入 P2P 网络. 结合 P2P 网络的特点, 同时还考虑了可靠性、可用性和安全性对终端可信性的影响, 另外, 还可实时的对终端的行为特征进行监控, 以保证终端在接入网络时刻和在连接网络期间的安全可靠. 实验证明, 设计的方案使对终端可信性的认证方面, 具有较高的准确度, 还使 P2P 具有更好的可靠性和稳定性.

关键词: P2P 网络; 可信计算; 可信网络连接; 行为度量

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2014)12-0038-05

P2P Network Connect Control Based on Trusted Computing

LIANG Zhi-hong¹, HU Zhao-hui¹, TAN Yi-ming², LIU Wen-juan²

(1 Electric Power Research Institute of Guangdong Power Grid Corporation, Guangzhou 510080, China;

2 China Standard Software Co., Ltd, Shanghai 200030, China)

Abstract: This paper proposes a P2P network connection method based on trusted computing technology to prevent the malicious terminal from accessing to the P2P network. We take into account the reliability, availability and security of a terminal, and the behavioral characteristics of the terminal which can protect the terminal is secure when it is running. The experiments prove that the method we presented is more accurate in trust certification of terminal, and the P2P has better reliability and stability.

Key words: P2P; trusted computing; TNC; behavior measurement

1 引言

为保证 P2P 网络的安全, 应该对申请加入 P2P 网络的终端的安全性进行验证. 对访问网络的终端进行身份验证和安全性评估, 确保只有安全可信的计算终端才能接入网络, 体现了终端安全与准入控制的结合, 大大提高了网络对来自于终端安全威胁的防御能力. 目前, 基于终端准入控制的思想, 国内外已提出了多种技术方案^[1-3].

思科提出了网络接入控制(network admission control, NAC)技术^[1], 微软提出了网络接入保护(network access protection, NAP)技术^[2], TCG (Trusted Computing Group)基于可信计算的思想, 提出了可信网络连接(Trusted Network Connec-

tion, TNC)技术^[3]. 文献[1-3]中的终端准入控制技术虽然各有特点, 但是其核心问题都是如何判断终端的安全可信. 它们都存在一些问题: 所述三个技术都只是考虑了终端的一些静态特性来判定其在接入网络那一时刻的可信性, 而对于终端运行时的动态特性, 例如用户进程的行为没有考虑, 因此, 没有全面地反映终端的实际可信性. 三个技术对终端可信性的度量是通过二值化的方式, 即要么可信, 要么不可信, 不能很好地反映客观事实, 因为在实际环境中, 不存在绝对不可信或可信的情况.

本文以 TNC 技术为基础^[3], 提出了一种基于可信计算技术的 P2P 网络连接方案, 其主要思想是: 当终端要申请加入 P2P 网络时, 从终端的静态特征和动态特征两方面来综合评价终端的可信性,

收稿日期: 2014-01-09; **修回日期:** 2014-03-01

基金项目: 国家高技术研究发展计划项目(2012AA050212)

并且终端的可信性以量化的方式进行度量. 通过对终端的综合量化度量, 可得到终端的可信度, 为终端是否可接入 P2P 网络提供了更加全面和完整的依据.

2 可信网络连接的相关概念及计算模型

2.1 可信的基本概念

可信是可信计算中的重要概念, 根据近年来学者对可信的研究^[4-7], 并结合本文研究的背景, 给出可信的相关定义如下所示.

定义 1 可信: 一个终端可信是指, 该终端的行为总是以预期的方式运作, 且执行结果也是可预期的. 一个高可信的终端, 应该具有高完整性、高可靠性、高可用性和高安全性.

定义 2 完整度: 完整度是指终端的平台配置信息、系统软件 and 用户数据等信息未被篡改和破坏的程度, 终端 c_i 的完整度可表示为 in_i , 且 $0 \leq in_i \leq 1$, 特别地, 当未被篡改或破坏时, $in_i = 1$.

定义 3 可靠度: 可靠度是指终端在规定环境、规定时间内和规定条件下无故障地完成其规定功能的概率. 假设终端的失效服从指数分布, 则终端 c_i 的可靠度可表示为 $de_i = e^{-\lambda t}$, 其中 λ 表示失效率, t 表示运行时间, 且 $0 \leq de_i \leq 1$. 特别地, 当终端 c_i 在一定时间段内没有出现失效时, 则 $de_i = 1$.

定义 4 可用度: 可用度是指终端在一定时间段内能够正常提供服务所占的时间比, 终端 c_i 的可用度可表示为 $av_i = \frac{MTBF_i}{MTTR_i}$, 且 $0 \leq av_i \leq 1$. 其中, $MTBF_i$ 表示终端 c_i 的平均失效间隔时间 (mean time between failure), $MTTR_i$ 表示终端 c_i 的平均恢复时间 (mean time to repair). 特别地, 当终端 c_i 在一定时间段内能够一直正常提供服务时, 则 $av_i = 1$.

定义 5 OS 安全级别: OS 安全级别是指终端上运行操作系统的安全等级, 终端 c_i 上操作系统的安全等级可表示为 se_i . 本文将操作系统的安全等级分为 5 级^[8], 5 级时 $se_i = 1$; 4 级时 $se_i = 0.75$; 3 级时 $se_i = 0.5$; 2 级时 $se_i = 0.25$; 特别地, 1 级时 $se_i = 0.1$.

定义 6 终端静态可信度: 静态可信度是指根据终端的一些静态属性, 反映终端 c_i 自身完整性、可靠性、可用性和安全性的程度, 可表示为 t'_i .

定义 7 主体: 终端系统中的主体是指用户或系统启动的进程, 是系统进行各种操作的发起者. 终

端系统中的主体可表示为集合 $O = \{o_1, o_2, \dots, o_M\}$, 其中 o_i 表示第 i 个主体.

定义 8 主体行为: 终端系统中主体的行为是指主体根据用户或系统的要求进行的各种操作. 主体行为可表示为集合 $B = \{r, w, e\}$, 分别表示读、写和执行.

定义 9 主体行为完整性: 主体行为完整性是指软件在实际运行过程中, 主体所产生的行为与主体预期的行为相一致, 或者主体行为不是被非法启动或终止^[9], 主体 o_i 行为的完整性可表示 $I_{o_i} = \begin{cases} 0, & \text{不完整} \\ 1, & \text{完整} \end{cases}$.

定义 10 终端状态: 终端状态是指对终端在当前时刻, 系统中处于活动状态的主体集合, 以及每个主体正在进行的各种行为的一个总体描述. 终端状态 $S = O \times B = \{s_1, s_2, \dots, s_N\}$, 即终端状态是主体和主体行为的笛卡尔积, 其中 s_i 表示第 i 个状态.

定义 11 终端行为可信度: 终端行为可信度是指根据终端当前状态 s_i 下各种主体行为的完整性, 来判定整个终端在当前时刻的动态可信度, 终端 c_i 的行为可信度可表示为: $t''_i(s_i)$.

定义 12 用户身份符合性: 用户身份符合性是指用户的身份与预先设定的身份认证策略是否符合, 终端 c_i 的身份符合性可表示 $d_i = \begin{cases} 0, & \text{不符合} \\ 1, & \text{符合} \end{cases}$, 例如安全策略规定只有管理员用户才能上网, 当访问网络的当前用户为普通用户时, 则说明身份符合性 $d_i = 0$, 即不允许当前用户接入网络.

定义 13 综合可信度: 综合可信度是指结合主体行为完整性和终端行为可信度对终端可信程度的评价, 终端 c_i 的综合可信度可表示为 t_i , 即 $t_i = f(t'_i, t''_i)$.

2.2 终端可信度的计算

一个终端的可信度受两方面影响, 是根据终端自己的静态属性进行可信度的评价, 即静态可信度; 二方面是根据终端在某一状态下的行为特征进行可信度的评价, 即行为可信度.

2.2.1 基于静态特征的可信度模型

由于终端 c_i 的静态可信度受该节点完整度、可靠度、可用度和安全级别四个因素的影响, 因此, 终端 c_i 的直接可信度可通过式 (1) 来计算,

$$t'_i = \alpha_1 in_i + \alpha_2 de_i + \alpha_3 av_i + \alpha_4 se_i \quad (1)$$

式中, $\alpha_i (i = 1, 2, 3, 4)$ 表示权重, 且 $\sum_{i=1}^4 \alpha_i = 1, 0 \leq t'_i$

≤ 1 .

2.2.2 基于行为特征的可信度模型

根据定义 11 可知,终端 c_i 在状态 s_j 时的行为可信度与该状态下所有主体的行为完整性有关,因此,终端 c_i 的行为可信度可通过式(2)来计算:

$$t_i(s_j) = \frac{1}{M} \cdot \sum_{k=1}^M I_{o_k} \quad (2)$$

式中, $0 \leq t_i(s_j) \leq 1$.

2.2.3 终端综合可信度的计算模型

根据定义 13 可知,终端 c_i 的综合可信度 t_i 是与终端静态可信度 t'_i 、终端行为可信度 t''_i 和用户身份符合性三个因素有关,则综合可信度 t_i 可通过式(3)来计算:

$$t_i = d_i \times [\alpha t'_i + (1 - \alpha) t''_i] \quad (3)$$

式中, $0 \leq t_i \leq 1$. d_i 为终端 c_i 的用户身份符合性,当不符合时, $d_i = 0$, 则综合可信度 $t_i = 0$; 当符合时, $d_i = 1$. $0 \leq \alpha \leq 1$, 称之为可信因子. 特别地, 当 $\alpha = 0$ 时, 表明终端 c_i 的可信度完全来自于对终端行为完整性的评价, 即不考虑终端 c_i 静态特征对可信的影响. 当 $\alpha = 1$ 时, 表明终端 c_i 的可信度完全来自于静态特征对可信度的影响, 不考虑终端行为的影响. 可信因子 α 的值可由每个终端根据自己的需求进行自行设定, 也可以由云平台统一进行设定.

3 基于终端可信性量化度量的可信网络连接控制方案

3.1 基于终端可信性量化度量的可信网络连接体系架构

TNC 的体系架构包括三个层次, 分别为网络访问层、完整性评估层和完整性度量层^[10].

(1) 网络访问层. 该层支持传统的网络连接技术, 从属于传统的网络互联和安全层, 支持现有的如 VPN 和 802.1X 等技术. 网络访问层包括网络访问请求者 (Network Access Requestor, NAR)、策略执行点 (Policy Enforcement Point, PEP) 和网络访问授权者 (Network Access Authority, NAA) 3 个组件.

(2) 完整性评估层. 该层主要进行终端的认证, 并评估访问请求者 (Access Requestor, AR) 的完整性. 完整性评估层包括 TNC 客户端 (TNC Client, TNCC) 和 TNC 服务器 (TNC Server, TNCS) 2 个组件.

(3) 完整性度量层. 该层主要收集和校验访问请求者 AR 的完整性相关信息. 完整性度量层包括完

整性度量收集器 (Integrity Measurement Collector, IMC) 和完整性度量验证器 (Integrity Measurement Verifier, IMV) 2 个组件.

由于本文对终端可信性的度量是在完整性度量的基础上, 增加了对终端可靠性、可用性和安全性的度量, 同时还对终端系统中主体的行为进行度量, 还考虑了终端用户的身份. 因此, 需要对 TNC 方案进行扩展. 主要是将完整性度量层扩展为可信性度量层.

可信性度量层主要收集和校验访问请求者 AR 的可信性相关信息, 包括终端的完整性、可用性、可靠性、安全性、行为完整性等信息. 可信性度量层包括除了完整性度量收集器 IMC 和完整性度量验证器 IMV, 又增加了以下几个方面:

(1) 可靠性度量收集器 (Dependability Measurement Collector, DMC);

(2) 可用性度量收集器 (Availability Measurement Collector, AMC);

(3) 安全性度量收集器 (Security Measurement Collector, SMC);

(4) 行为度量收集器 (Behavior Measurement Collector, BMC);

(5) 可靠性度量验证器 (Dependability Measurement Verifier, DMV);

(6) 可用性度量验证器 (Availability Measurement Verifier, AMV);

(7) 安全性度量验证器 (Security Measurement Verifier, SMV);

(8) 行为度量验证器 (Behavior Measurement Verifier, BMV).

本文设计的基于可信计算技术的 P2P 网络连接方案架构如图 1 所示.

3.2 基于可信计算技术的 P2P 网络连接控制流程

基于本文设计的可信网络连接方案, 当终端要进行网络访问时, 其内部的工作流程如下所示.

步骤 1: 当发现终端发起了建立网络连接的请求时, NAR 在网络访问层启动一个连接请求.

步骤 2: PEP 收到来自 NAR 的连接请求后, 将该请求发送到 NAA 进行决策.

步骤 3: 如果用户的身份和角色认证在 AR 和 NAA 之间成功实施, 则 NAA 将该连接请求通知 TNCS. 否则退出网络连接.

步骤 4: TNC 客户端和 TNC 服务器进行双向身份认证, 如果认证成功则转到步骤 5, 否则退出网

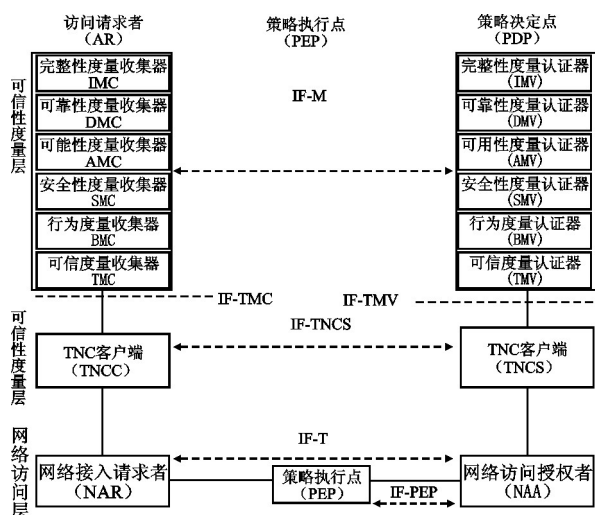


图1 基于可信计算技术的 P2P 网络连接方案体系架构
网络连接。

步骤 5: TNCC 和 TNCS 分别通知 TMC 和 TMV, 启动新的连接请求。同时, TNCC 和 TNCS 分别实现对 TMC 和 TMV 可信性检查握手, 在握手过程中, TNCC 和 TNCS 需要交换多次信息, 如果 TNCS 判定 AR 的可信状态符合要求, 则转步骤 6, 否则退出网络连接。

步骤 6: TNCC 向 TMC 发送请求, 收集对 AR 完整性、可靠性、可用性、安全性、行为完整性的度量结果, TMC 计算 AR 的综合可信度。同时, TNCS 通知 TMV 验证开始, TMV 完成策略的配置和初始化。

步骤 7: 当 TNCC 得到 TMC 计算的综合可信度后, 将该结果发送给 TNCS。

步骤 8: 当 TNCS 收到 AR 的综合可信度报告后, 将其传递给匹配的 TMV, 将其与事先制定的安全策略进行比对, 并将结果返回给 TNCS。

步骤 9: TNCS 将决策结果发送给 NAA。

步骤 10: NAA 又将决策结果发送给 PEP 进行执行, 同时 NAA 也把最后决策返回给 TNCS, 而 TNCS 又将其发送给 TNCC。

步骤 11: 如果 PEP 执行的结果是允许 AR 进行网络连接, 那么在网络连接建立后, TMC 将继续实时的监视并分析 AR 的可信度, 并周期性的将分析结果发送给 TNCS, TMV 一旦发现 AR 的可信度低于一定的阈值, 将及时通过 NAA 通知 PEP 执行操作, 断开 AR 的网络连接。

本方案是在可信计算技术的基础上, 通过对终端完整性、可靠性、可用性、安全性、行为完整性的度量机制来保证终端的可信, 不仅可用于对终端接入

网络那一时刻的可信度进行度量, 还可以用于实时地对终端的行为完整性进行监视。

4 实验与结果分析

为了说明本文提出的可信网络连接方案的有效性, 本文设计了可信度量和可信验证的原型系统。

实验环境: 32 台 PC 作为终端, 即访问请求者 AR, 在这些 PC 上部署了终端完整性、可用性、可靠性和安全性, 以及行为可信性度量模块, 对终端的可信状态进行监督和评价, 且 PC 上运行的操作系统为符合国家安全 4 级标准的安全操作系统, 另外设定一台 PC 作为策略执行点 PEP 和策略决策点 PDP。在实验中, 设定了 PC 之间已实现了平台认证和完整性认证工作, 以保证度量和验证模块能够正常运行。

验证本文设计方案有效性的方法是在访问请求者 AR 的 32 台 PC 端放置四个恶意代码, 分别是: 破坏系统完整性的恶意代码、可导致系统宕机的恶意代码、一个可关闭操作系统安全策略的恶意代码、一个可自我复制的病毒程序。当恶意代码运行时, 验证终端的综合可信度, 当可信度低于设定的可信阈值 0.9 时, 则断开该终端, 反之, 允许连接。

实验 1: 该实验设定 32 台 PC 相继申请加入 P2P 网络。同时, 将四个恶意代码置于每台 PC 上, 并且设置这些恶意代码的发作时间间隔服从负指数分布。为了验证本文提出的基于可信计算技术的 P2P 网络连接方案(方案 1)在可信验证方面的优越性, 将其和刘巍伟提出的基于终端行为的可信网络连接控制方案^[11](方案 2)进行对比, 实验结果如图 2 所示。

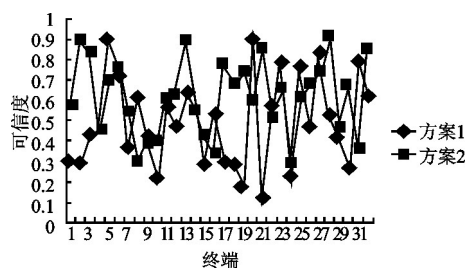


图2 方案效果在可信方面的对比

根据图 2 可知, 经过多次试验的结果, 本文设计的方案在对终端可信验证的准确率达到了 93.75%, 而方案 2 的准确率为 90.63%。

实验 2: 该实验设定 P2P 网络环境需要从 32 台 PC 中选择 16 台可信的 PC 进行五个大规模的计算任务, 分别是: 高斯消解 GE(矩阵规模为 $1024 \times$

1024), DES 算法(64 位), 求解 N-body 问题的 PP 算法(1024 粒子), 二维 FFT 算法(矩阵规模为 1024×1024), 矩阵相乘 MM(矩阵规模为 1024×1024). 为了验证提出的基于可信计算技术的 P2P 网络连接方案在性能方面的优越性, 将本文设计的方案将传统的基于完整性验证的 TNC 方案(简称方案 3)进行对比. 实验结果如图 3 所示.

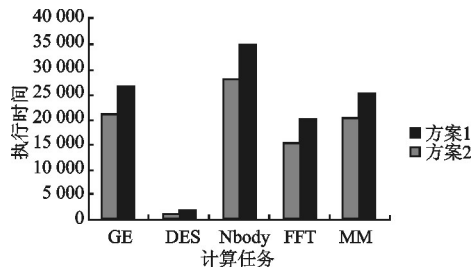


图 3 方案效果在性能方面的对比

根据图 3 可知, 经过多次试验的结果, 本文设计的方案对每个计算任务的执行时间较方案 2 平均提高了 20.99%.

通过对试验结果的分析得出以下两点发现.

(1) 本文提出的方案可较为准确地对终端的可信性进行验证, 避免了一些不可信终端接入 P2P 网络的可能性, 保护了网络的安全. 分析原因是: 因为对终端是否可信的验证上, 本文采用了恶意代码的静态特征分析的方法, 该方法首先需要对各种恶意代码的执行特征进行分析并形成特征库, 再将进程的行为与特征库进行对比, 因此, 有较高的准确性.

(2) 本文设计的方案在执行性能上也优于传统的 TNC 方案, 分析原因是: 由于本文提出的方案对终端可信性进行验证的时候, 考虑了终端的可靠性和可用性, 因此, 在选择终端的时候, 选择了一些可靠性和可用性较高的节点, 防止了节点失效对计算性能的影响. 但是传统的 TNC 方案只考虑了完整性, 没有考虑可靠性和可用性, 因此, 选择的终端在进行计算时, 失效的概率较大, 导致在传统可信网络连接方案下, P2P 网络的稳定可靠性和执行性能差于本文提出的方案.

5 结束语

本文提出了基于可信计算技术的 P2P 网络连接方案. 该方案在 TNC 技术的基础上, 不仅考虑了终端的完整性, 同时还考虑了终端的可靠性、可用性和安全性, 对计算节点进行可信性的量化度量. 另

外, 还考虑了终端的行为特征对可信性的影响. 结合终端基于静态属性的可信度和基于动态行为的可信度, 实现了对一个终端进行全面的、更加客观的可信评价. 根据该思想, 本文设计了基于可信计算技术的 P2P 可信网络连接体系架构和操作流程, 可实现对终端可信性的评价. 本文的不足之处是对终端行为的度量是基于静态特征库的方法, 不能检测出未知恶意代码的行为. 因此, 下一步的研究工作将考虑如何针对未知恶意代码的行为进行判定.

参考文献:

- [1] Cisco Company. Cisco network admission control [EB/OL]. [2014-01-10]. <http://www.cisco.com>.
- [2] Microsoft Corporation. Network access protection platform architecture [EB/OL]. [2014-01-03]. <http://www.microsoft.com>.
- [3] Trusted Computing Group. TCG trusted network connect TNC architecture for interoperability [EB/OL]. [2014-01-04]. <http://www.trustedcomputinggroup.org>.
- [4] 张焕国, 罗捷, 金刚, 等. 可信计算研究进展[J]. 武汉大学学报, 2006, 52(5): 513-518.
- [5] 赵佳, 沈昌祥, 刘吉强, 等. 基于无干扰理论的可信链模型[J]. 计算机研究与发展, 2008, 45(6): 578-584.
- [6] 冯登国, 秦宇. 可信计算环境证明方法研究[J]. 计算机学报, 2008, 31(9): 1640-1652.
- [7] 沈松, 邢剑锋, 王鹏飞, 等. 构建基于虚拟机的可信云计算平台[J]. 微电子学与计算机, 2011, 28(8): 191-194.
- [8] 中国国家标准化管理委员会. GB/T 20272-2006 信息安全技术操作系统安全技术要求[S]. 北京: 中国标准出版社, 2006.
- [9] 彭国军. 基于行为完整性的软件动态可信理论与技术研究[D]. 武汉: 武汉大学, 2008.
- [10] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学, 2007, 37(2): 129-155.
- [11] 刘巍伟, 韩臻, 沈昌祥. 基于终端行为的可信网络连接控制方案[J]. 通信学报, 2009, 30(11): 127-134.

作者简介:

梁志宏 男, (1984-), 硕士, 工程师. 研究方向为电力系统信息技术与信息安全.

胡朝辉 男, (1986-), 硕士. 研究方向为电力信息系统安全防护与等级保护.

谭一鸣(通讯作者) 男, (1982-), 博士. 研究方向为可信计算、云计算. E-mail: tanlming@126.com.

刘文娟 女, (1989-), 硕士. 研究方向为可信计算、云计算.