一种基于可信计算的VPN接入认证方案

邱 罡[1] 王玉磊[2] 周利华[1]

(西安电子科技大学CNIS教育部重点实验室 西安 710071)[1] (南阳理工学院网络中心 南阳 473009)[2]

摘 要 平台安全性在远程访问企业资源显得越来越重要。目前VPN客户端认证在对终端用户身份和平台身份认证的同时,尚未很好地保证终端平台的安全性,使得终端平台成为入侵者获得非法访问权限的途径。通过采用智能卡和可信平台模块相结合的方案,提高了终端平台身份认证的安全性,确保网络接入和通信的安全可信。

关键词 虚拟专用网,可信计算,认证,智能卡

中图法分类号 TP393.08 **文献标识码** A

Novel VPN Authentication Scheme Based on Trusted Computing

QIU Gang[1] WANG Yu-lei[2] ZHOU Li-hua[1]

(The CNIS Key Laboratory of the Education Ministry, Xidian University, Xi'an 710071, China)[1]

(Network Information Center, Nanyang Institute of Technology, Nanyang 473009, China)[2]

Abstract Platform security is particularly important in the case of remote access to corporate resources. Today, Virtual Private Network(VPN) client authentication mostly focuses on the identity of end-user and platform without ensuring the trust properties of the platform the end-user is operating. An attacker could exploit it to gain unauthorized access. Scheme based on the combination of smart card and Trusted Platform Module(TPM) can secure the identity authentication of the end-user's platform and assure the security of network connections.

Keywords Virtual private network(VPN), Trusted computing, Authentication, Smart card

虚拟专用网(Virtual Private Network,VPN)利用公用互联网作为信息传输媒介,通过安全隧道,用户认证和访问控制等技术实现信息的安全传输。企业必须确保其VPN上传送的数据不被攻击者窥视和篡改,并且要防止非法用户对网络资源或私有信息的访问。但是,由于VPN仅能提供对客户身份的认证,不能有效地认证客户端主机的配置,作为网络终端的主机是攻击者发起对网络和网络中各类设备攻击的入口,若主机本身不安全,如不安全的网络连接或被病毒感染,就不能保证终端信息安全。可信平台模块(Trusted Platform Module,TPM)可以用来增强主机安全,同时可信网络连接针对网络的安全性和完整性设计,防止不安全设备接入和破坏网络的机制,确保了终端的安全防护。本文针对当前VPN的不足,运用可信计算技术和EAP认证协议,保证了信息在端点和传输过程中的安全。

1 VPN客户端认证

1.1 扩展认证协议

VPN网络中使用加密及其他安全机制确保只有经过认证的用户才可以访问网络,并保证数据的安全性。在VPN协议中,如PPP协议(Point-to-Point Protocol),客户端计算机通过向远程服务器发送客户证书来抵御重放和假冒攻击。大多数PPP协议提供有限的认证方法,如:简单的明文认证协议——口令认证协议(Password Authentication Protocol,PAP);用来避免传输实际口令的加密的认证协议——挑战握手认证协议(Challenge Handshake Authentication Protocol,CHAP)。此外,VPN所使用的IPsec协议通过扩展IP包头提供无连接的完整性和数据源认证。

上述VPN所采用的认证方案主要解决了客户端用户认证,但随着为满足客户端设备认证的要求而出现的扩展认证协议(Extensible Authentication Protocol,EAP)[1]提供了一种灵活的认证方法,可以结合各种成熟的认证方案如PKI及基于令牌的方案,来实施包括用户到平台的认证。

使用EAP,任意身份验证机制都可以对远程访问连接进行身份验证。通过远程VPN客户端和验证程序(ISA服务器或RADIUS服务器)协商要使用的确切身份验证方案。EAP允许远程VPN客户端和验证程序之间进行开端对话。对话由对身份验证信息的验证程序请求和远程VPN客户端的响应组成。EAP是一组以插件模块的形式为任何EAP类型提供结构支持的内部组件。为了成功进行身份验证,远程访问客户端和验证程序必须安装相同的EAP身份验证模块,其所支持的认证方法通常包括:基于PKI的EAP-TLS、基于GSM的EAP-SIM或者基于一次性口令的EAP-OTP。EAP通常与RADIUS服务器联系在一起,以便进行身份验证使用。EAP-RADIUS的优势在于不需要在每个远程访问服务器上

到稿日期:2009-01-06 返修日期:2009-03-11 本文受国家自然科学基金(60573036)资助。

邱 罡 博士生,讲师,主要研究领域为网络信息安全,E-mail:qiugang7780@163.com;王玉磊 硕士,讲师,主要研究领域为计算机网络安全;周利华 教授,博士生导师,主要研究领域为计算机网络安全理论与技术、多媒体技术等。

安装 EAP 类型，只需在 RADIUS 服务器上安装即可。

1.2 VPN 设备认证

在建立网络连接时，接入设备向认证服务器发送设备唯一的平台身份信息，如：网络接口卡的 MAC 地址以及机器序列号等，由认证服务器按照许可列表对照检查平台的身份信息。

为防止平台身份认证的窃取，可对平台身份采用加密机制，如：为设备分配与 IP 地址绑定的预共享密钥，并在设备和认证服务器之间采用加密认证协议；采用设备证书和公钥加密。设备证书是由设备生产厂家颁发的公钥证书，将设备身份信息与对应私钥绑定。但由于病毒、木马等恶意程序的存在，上述方法并不能保证平台身份的安全使用。存储证书、密钥等秘密信息的平台存在被攻破的可能，证书及密钥会被窃取。这就要求设备能够抵御篡改，私钥在保证安全存储的同时能够在不同的环境下很容易地使用。因此，理想的设备身份认证方案应满足以下特点：

(1)不可迁移。避免证书被安装到未经授权的平台上；基于硬件的实现机制应能提供防篡改的存储保护。

(2)加密能力。用户平台与网络接入服务器间使用的认证协议中使用加密算法可避免重放攻击和欺骗。

(3)报告能力。能够报告其软件环境的完整性并向认证服务器安全地传递可信报告。

2 可信计算技术

2.1 TCG 安全结构

TCG[2] 定义了一组使硬件和软件能够支持可信计算的工业标准的规范。TCG 的核心是一个称为 TPM[3] 且能防止篡改的硬件安全模块。另外，TPM 作为加密协处理器和保护密钥及秘密信息的保护存储装置，也被用来度量和报告平台的完整性信息，并且不会受到平台使用者或其上运行的软件的威胁。

2.1.1 平台完整性度量

平台完整性度量包括对构成平台的硬件和软件部分分阶段的度量和存储。完整性度量通常分为两种类型：TCG 的可信引导及在可信引导基础上的其它完整性度量。

当系统加电运行时，初始引导代码(如 BIOS 引导块)在将控制权传递给下一个组件之前对其进行度量，并将度量值存入 TPM。接下来的每个软件组件都要进行度量，并保存度量结果，直到整个操作系统被装入。BIOS 引导模块及 TPM 被称作核心根(Core Root of Trust for Measurement，CRTM)，可信计算平台的可信性建立在以 TPM 为信任根和从信任根开始的信任链之上。每一个度量都使用 SHA-1 哈希算法对组件的二进制映像进行度量，并将度量结果存入 TPM 中的平台配置寄存器(Platform Configuration Registers，PCR)。

2.1.2 平台完整性报告

TCG 标准中定义的平台完整性报告(或远程证明)机制，用于向挑战方报告存储在 PCR 中的完整性度量值是以可靠方式存储的。在证明过程中 TPM 对 PCR 值和附加的数据(如来自挑战方防止重放攻击的随机数)使用私钥签名，并传给挑战方。证明是一项受保护的原子操作，不能被恶意软件伪造。平台也可以在证明中发送附加信息如完整性度量日志，其中包括平台中加载并被 TPM 度量过的组件列表，以及这些组件是如何构成的。

远程挑战方通过验证带有 AIK 证书的签名，并将完整性度量值与本地收集的参照度量日志进行对比来验证证明。攻破的系统可以修改度量日志，但其不能改变受 TPM 保护的度量结果与修改过的日志匹配，因此通过和签过名的度量结果对照验证度量日志，伪造操作即可被发现。

2.2 身份管理

TCG 定义了几种类型的密钥和证书在证明 TPM 的真实性的同时保护其隐私。

签注密钥(Endorsement Key，EK)是一个不可迁移的解密密钥，它在平台的生产过程中生成，代表着每个平台的真实身份，每个平台都拥有唯一的一个 EK。EK 只能用来在建立平台所有者时解密用户的授权数据，还有解密与生成 AIK 相关的数据。它不能用于任何签名或加密。

身份证明密钥(Attestation Identities Key，AIK) 是不可迁移密钥，只用来对 TPM 生成的 PCR 值进行签名，用来证明平台的身份和平台的环境配置。每个用户可以拥有多个 AIK。

AIK 证书被用来鉴定对 PCR 值进行签名的 AIK 私钥，它包括 AIK 的公钥和其它发布者认为有用的信息。AIK 证书为发布信息的 TPM 提供真实性证明。

TCG 定义了一个被称为 Privacy CA 的证书中心来为 AIK 签发证书。在签发过程中，发出请求的 TPM 首先生成 AIK 密钥对，并将其公钥部分与 EK 证书和平台证书一起发送给 Privacy CA。Privacy CA 验证这些证书，并确认该请求来自于具有真实 TPM 的真实平台。Privacy CA 返回使用 EK 公钥加密的 AIK 证书，因此只有发出请求的 TPM 具备真实的 EK 才可以解密。Privacy CA 中保留了 AIK 与 EK 的对应关系，因此必须严格加以保护。

3 解决方案

本节描述一种基于智能卡的用户身份认证与基于 TPM 证明的平台认证相结合的 VPN 客户端认证方案。

图 1 所示的场景中，企业员工通过可信平台接入企业网络，使用用户名识别用户并利用口令认证其身份。登录之前用户先向系统管理员申请智能卡进行注册，用户的智能卡信息存储在服务器端注册用户身份鉴别信息表[4] 中，服务器采取保护措施保障信息表的安全性。

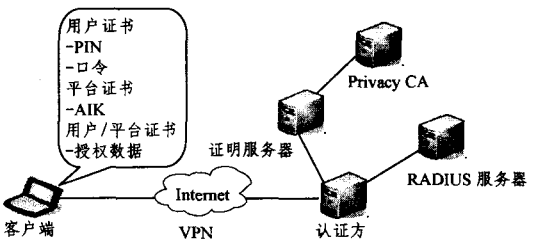

图 1 典型架构

在本方案中，用户使用与用户名关联的口令，用于 RADIUS 认证服务器实现通常的用户认证；与智能卡关联的 PIN，用于解锁 AIK 授权数据 AD。终端平台拥有一个由 Privacy CA 颁发的用于平台证明的 AIK 证书 $Cert_{CA}(AIK)$。

3.1 基本标识

本方案中使用的基本标识如图 2 所示。

U	平台用户
P	用户平台
S	认证服务器
U_{KEY}	智能卡
K_i	实体 i 的非对称密钥的公钥部分
K_i^{-1}	实体 i 的非对称密钥的私钥部分
$Cert_i(O)$	由实体 i 公钥对对象 O 签名的证书
$E_k(\cdot)$	使用公钥 K 的加密算法
$D_k(\cdot)$	使用公钥 K 的解密算法
$Sing_k(\cdot)$	使用密钥 K 的签名算法
$Verify_k(\cdot)$	使用密钥 K 的验证算法
$H(\cdot)$	采用 SHA1 算法的哈希函数
X‖Y	表示 X 和 Y 按照先后顺序的串联结果
X→Y:Z	表示消息 Z 是从 X 发送到 Y

图 2　基本标识

3.2　客户端用户平台使用授权

在要求使用 AIK 的任何操作之前，TPM 用户 U 必须要先进行认证[3]，证实用户知道共享秘密——授权数据(Authorization Data，AD)。授权数据是用户存储在平台 P 上或由口令作为外部种子计算得来的，经过 Hash 运算归一化处理后的 Hash 值，一般长度为 160 比特。知道对象的授权数据就能完全证明对 TPM 保护对象的所有权。因此，对于共享秘密的保护就显得尤为重要。基于智能卡的认证能够解决共享秘密的安全存储问题，在这种方案中 AD 不暴露于智能卡外部；智能卡为需要 AD 的协议提供计算能力。平台利用智能卡计算输入认证值 IAV(Input Authentication Value)，该值被返回到平台执行认证命令。

1) $U \rightarrow P$：平台使用请求

2) $P \rightarrow U$：请求输入 PIN

3) U：输入 PIN

4)U_{KEY}：验证 PIN，计算 IAV

5)$U_{KEY} \rightarrow$P：发送 IAV

6) $P \rightarrow TPM$：启动授权协议

3.3　客户端用户身份认证

基于智能卡的身份鉴别方案由初始化、注册、登录和身份鉴别 4 个阶段组成[5,6]。用户认证可使用其偏好的认证方法(本方案使用标准的登录/口令方式)；用户输入 PIN 向智能卡认证；认证方将用户名及口令传递给 RADIUS 认证服务器，进行用户身份的认证。本方案使用的用户认证协议采用文献[6]中提出的基于 Yang-Shieh 智能卡认证协议[5]的改进协议，能够更有效地对抗假冒攻击。由于篇幅所限，具体请参见文献[6]。

3.4　客户端平台认证

在客户端平台认证过程中，假定挑战方 S 和证明方 U 事先已约定有限域 F_p 和元素 $g \in F_p$，认证双方分别使用 Diffie-Hellman 协议[7]来产生非对称密钥对。

1) S：S 选择大素数 p 和高阶群 Z^* 的生成元素 $g(2 \leqslant g \leqslant p-2)$，$S$ 选择一个随机秘密数 $s(2 \leqslant s \leqslant p-2)$，并计算 $g^s \bmod p$；同时生成 160 位随机数 N_s。

2) $S \rightarrow U$：ChallengeRequest($g^s \bmod p, N_s$)

3a) U：U 选择一个随机秘密数 $u(2 \leqslant u \leqslant p-2)$，并计算 $g^u \bmod p$。计算 $K_{SU}=(g^s)^u \bmod p$ 得到会话密钥 K_{SU}。

3b) U：U 所在平台的 TPM 生成不可迁移密钥 K_{TS}。该密钥与一组特定 PCR 值绑定。TPM 使用 K_{AIK}^{-1} 为 K_{TS} 签发的证书 $Cert_{AIK}(K_{TS})$，其中说明与 K_{TS} 绑定 PCR 值。

3c) U：U 返回证明

$Quote=Sign_{K_{TS}^{-1}}\{PCR, SHA1(N_S, g^u \bmod p)\}$

3d) U：U 得到存储度量日志 SML(Stored Measurement Log)

4) $U \rightarrow S$：ChallengeResponse($Quote$, $g^u \bmod p$, SML), $Cert_{CA}(AIK)$, $Cert_{AIK}(K_{TS})$

5a) S：验证 $Cert_{CA}(AIK)$, $Cert_{AIK}(K_{TS})$

5b) S：验证 $Sign_{K_{TS}^{-1}}\{PCR, SHA1(N_S, g^u \bmod p)\}$

5c) S：使用 PCR 验证 N_s 和 SML

5d) S：计算 $K_{SU}=(g^u)^s \bmod p$ 得到会话密钥 K_{SU}

6) S：生成 160 位随机数 N_s'

7)$S \rightarrow U$：ChallengeRequest(N_s')

8) U：计算 $R=E_{K_{SU}}\{N_S'\}$

9) $U \rightarrow S$：ChallengeResponse(R)

10)S：验证 N_s'

在步骤 3a)中，证明方 U 生成公钥 $g^u \bmod p$，并将该公钥与 PCR 值和随机数 N_s 一起包含在平台证明消息 $Quote$ 中，然后使用 K_{TS} 对消息 $Quote$ 进行签名。公钥 $g^u \bmod p$ 是作为 external data(外部数据)插入 TPM_Quote 操作中的，但由于 TPM_Quote 仅允许 160 位的外部数据，因此必须使用 SHA1 算法进行数据压缩后才能达到 160 位的数据要求。在步骤 5d)中，挑战方 S 使用自己的私钥和 U 的公钥计算出会话密钥 K_{SU}，并通过步骤 6－步骤 10 的第二轮挑战-应答来验证证明方 U 是否拥有此会话密钥。

4　安全性分析

与传统的 VPN 认证方案相比，本方案具有以下优点。

(1)信息的安全性。与用户证明相关的信息保存在具有加密功能的智能卡中，有效防止信息泄露；与平台证明相关的证书等秘密信息保存在 TPM 中，防止了非法用户读取。

(2)信道的安全性。数据均未以明文方式在信道上传输，在远程证明过程中利用随机数使得传输的信息具有不规则性和不可预计性，可抵御重放攻击。

(3)认证的安全性。对于用户的认证采用低成本，保密程度高的智能卡可以保证用户认证的灵活性和安全性。智能卡利用其中保存的授权数据和 TPM 实现了双向认证，可防止攻击者伪装成其他用户参与通信。建立在可信平台度量基础上的终端用户和远程服务器间的认证，所有消息都是通过认证双方协商的会话密钥 K_{SU} 加密后传输的，避免攻击者通过隐藏其配置值实施延迟攻击[8]。会话密钥 K_{SU} 在 TPM 提供的环境下安全地存储，保证了信息的可靠性。挑战方可依据接收到的 SML 和 PCR 来验证证明方的平台配置是否可信。

结束语　当前 VPN 协议(如 IPsec)不能认证终端用户平台的配置，终端的安全不能保证，使之成为侵入者获取秘密信息的途径。采用智能卡和可信计算技术结合的认证方案提供了用户和平台的双重认证，有效地保证了 VPN 接入终端可信、网络接入和网络通信的安全，从而构成一个信息安全保障

(下转第 140 页)

见第 5.5 节。算法中所用到的交叉和变异操作见第 5.3 节。算法 1 的终止条件为进化代数。

VCA-GS 算法的时间复杂度主要取决于种群的规模和迭代次数。算法的每次迭代的时间主要取决于两个部分：个体分级排序和保持优良解。个体分级排序的时间复杂度为 $O(2(|F|+|C|+m+n)(2s)^2+2s\cdot\log(2s))$，保持优良解的时间复杂度为 $O((|F|+|C|)(2s)s^*)$，其中，s^* 为辅助种群的上限。因此，整个算法的时间复杂度为：$O(((|F|+|C|+m+n)s^2+ss^*)T)$。

6 实验分析

实验程序采用 Java 语言开发，算法运行微机的配置为 PentiumIV 1.73GHZ 处理器，0.99G 内存，操作系统为 Windows XP。我们假定依赖构件的数量等于绑定构件的数量，每个构件的请求接口的最大数量为 2，每个请求接口所依赖的构件的最大数量为 5。实验中每个功能的候选构件集，构件的接口以及接口之间的连接关系，每个构件的 QoS 以及 QoS 的约束条件均是随机生成的。在进行实验中，由于 QoS 约束的存在，因此有可能产生空解，在空解的情况下只要重新调整各个参数的随机值，必然最终会得到相应的解。

实验以 10 个功能为例，分别考虑每个功能的候选构件数量为 10，15 和 20，进化代数为 100，200，300 和 400 的情况下，利用 VGA-CS 算法求解满足约束的非劣组装方案的 CPU 时间开销。对于每一种情况，算法分别运行 10 次取平均值。图 3 描述了随着候选构件数量的增加，在不同进化代数下，执行算法的 CPU 开销。从该图可以看出，随着候选构件数量的增加，CPU 的执行时间并没有明显增加，CPU 的执行时间与进化代数有关，并随着进化代数的增加而呈线性增加。在功能数量为 10，每个功能的候选构件数量为 20 的情况下，执行时间为 10s 左右。这一求解规模可以满足构件组装方案选择问题的需求。

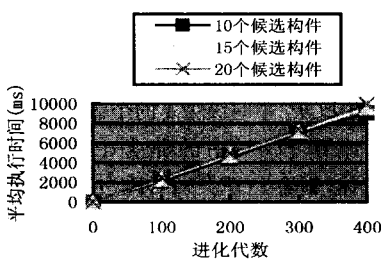

图 3 VGA-CS 的平均执行时间

结束语 为了提高应用系统的构件组装质量，提出了一个面向配置的构件组装模型，基于此模型给出了一个基于向量编码构件组装方案选择遗传算法（VGA-CS）以帮助用户选择最佳的构件组装方案。与目前所提出的面向全局构件选择算相比，VGA-CS 具有如下优点：

（1）能够有效地表示构件之间的依赖关系。目前大多数面向全局 QoS 优化的组装方案选择方法都是将构件看作是一个独立的单元，不考虑构件之间的依赖关系，从而限定了其适用范围，而本文所提出的构件组装模型既适用于独立构件的情况，也适用于构件之间具有复杂依赖关系的情况，因此能够适用于各种类型的体系结构。

（2）VGA-CS 是一个基于多目标优化的构件组装选择算法，其可以得到一组满足约束条件的非劣组装方案，与基于单目标优化得到一个优化解相比，可以更好地满足用户的需求。

参 考 文 献

[1] 杨芙清. 软件工程技术发展思索[J]. 软件学报，2005，16(01)：1-7

[2] Ruhe G. Intelligent Support for Selection of COTS Products[C]// Proceeding of the Net. ObjectDays 2002. Erfurt: Springer 2003

[3] Sheng Jinfang, Chen Songqiao, Wang Bin. COTS Evaluation and Selection Based on Requirements Decomposition[J]. Chinese Journal of Electronics, 2005(1): 62-67

[4] Cui Yi, Nahrstedt K. QoS-Aware Dependency Management for Component-Based Systems[C]// Proceedings of the 10th IEEE International Symposium on High Performance Distributed Computing. Washington, DC, USA, 2001

[5] 廖渊，唐磊，李明树. 一种基于 QoS 的服务构件组合方法[J]. 计算机学报，2005，29(4)：627-634

[6] 唐磊，廖渊，李明树，等. 面向普适计算的服务构件动态部署问题及算法[J]. 计算机研究与发展，2007，44(5)：815-822

[7] 战德臣，徐晓飞，李成严. 时间-成本双主线 ERP 管理体协研究[J]. 计算机集成制造系统，2002，8(8)：635-639

[8] 赵俊峰，王亚沙，谢冰，等. 一种支持构件服务质量的构件管理框架[J]. 电子学报，2004，32(a2A)：165-168

[9] Sedigh-Ali S, Ghafoor A. A graph-based method for component-based software development [C]// Proceeding 10th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems. Feb. 2005: 254 - 259

[10] 汪定伟，王俊峰，王洪峰，等. 智能优化方法[M]. 北京：高等教育传版社，2007：4

（上接第 78 页）

架构，更好地保证了企业信息的安全使用。

参 考 文 献

[1] Aboba B, Blunk L, Vollbrecht J, et al. Extensible Authentication Protocol(EAP) [S]. IETF RFC3748, June 2004

[2] Trusted Computing Group. TCG Specification Architecture Overview[EB/OL]. [2007-11-01]. https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf

[3] Trusted Computing Group. TPM Main Part 1 Design Principles [EB/OL]. [2007-11-01]. https://www.trustedcomputinggroup.org/specs/TPM/tpmwg-mainrev62_Part1_Design_Principles.pdf

[4] Shen J J, Lin C W, Hwang M S. A Modified Remote User Authentication Scheme Using Smart Cards[J]. IEEE Transactions on Consumer Electronics, 2003, 49(2): 414-416

[5] Yang W H, Shieh S P. Password authentication scheme with smartcards[J]. Computers & Security, 1999, 18(8): 727-733

[6] 杨照芳，程小平. 基于 Diff-Hellman 的改进 Yang-Shieh 智能卡认证协议[J]. 西南师范大学学报：自然科学版，2006，31(6)：110-113

[7] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22(6): 644-654

[8] Stumpf F, Tafreschi O, Roder P, et al. A Robust Integrity Reporting Protocol for Remote Attestation[C]// Second Workshop on Advances in Trusted Computing(WATC'06 Fall). Tokyo, Japan, November 2006