第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0160—03 文献标识码：A 中图分类号：TP309

基于TNC的安全认证协议的设计与实现

颜 菲，任江春，戴 葵，王志英
(国防科学技术大学计算机学院，长沙 410073)

摘 要：安全协议是保证网络安全的基础，现有安全协议为服务器和网络提供了很好的保护，但对客户终端缺乏保护。该文以可信网络连接(TNC)的终端完整性度量思想为基础，提出了一种基于TNC结构的安全认证协议。该协议在可信计算环境下将终端完整性度量技术与公钥基础设施(PKI)相结合使用，确保了终端平台的可信性。

关键词：安全认证协议；TNC结构；平台完整性认证；用户身份认证；终端完整性

Design and Implementation of Secure Authenticated Protocol Based on TNC

YAN Fei, REN Jiangchun, DAI Kui, WANG Zhiying
(School of Computer Science, National University of Defense Technology, Changsha 410073)

【Abstract】 Network security is based on secure protocols. Secure protocols in existence have offered a favorable protection for servers and network, but there's no protection for endpoint. A TNC (trusted network connection) based authenticated protocol, which focus on endpoint integrity, is proposed. The secure protocol, which integrates endpoint integrity measurement and PKI (public key infrastructure) under trusted computing environment, can assure the trustworthiness of endpoint.

【Key words】 Secure authenticated protocol; TNC architecture; Platform integrity authentication; User identity authentication; Endpoint integrity

1 概述

随着计算机网络的不断发展，全球信息化已成为人类发展的一大趋势。但由于计算机网络开放性、互连性等特征，致使网络易受黑客、恶意软件等不轨行为的攻击，因此，网络必须全方位地针对各种不同的威胁提供足够强的安全措施，以确保网络信息的机密性、完整性和可用性。

安全协议是保证网络安全的基础。近年来，SSL/TSL和SSH等安全协议的产生为服务器和网络提供了很好的保护作用，却忽略了对终端的保护，为黑客们提供了可乘之机。终端往往是创建和存放重要数据的源头。如图1所示，恶意代码可能寄生在客户终端，在客户端请求网络连接以前就已经篡改了数据或是在连接建立以后冒充用户与服务器端进行通信。在这种情况下，确保终端的可信性显得更为重要。因此，必须在原有安全协议的基础上增加更多的关于终端安全检测的细节。

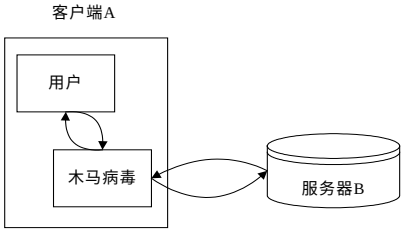

图1 木马攻击实例

TCG(trusted computing group)的可信网络连接(trusted network connection, TNC)小组提出了“终端完整性度量”的思想：即使用一系列由客户所在组织的IT部门制定的策略和预定的平台配置，对尝试连接网络的客户终端的可信性进行评估，未满足预定的类似补丁级别、杀毒软件或操作系统配置等策略的客户，都将被隔离起来以备修复[1]，从而防止不可信终端设备连接到网络实施破坏行动，解决了网络环境下的终端安全问题。

TNC能解决网络环境下的终端安全问题，而公钥基础设施PKI[2]则是比较完整的用户身份认证和网络安全解决方案，因此，本文将两者相结合提出了一种基于TNC规范的安全认证协议框架。在该框架下既能保证网络和服务器端的安全，又能确保终端安全，消除了现有协议忽略终端保护的弊端。

2 基于TNC的安全协议框架

如图2，TNC由访问请求方(access requestor, AR)、策略执行点(policy enforcement point, PEP)和决策点(policy decision point, Pdp)3部分组成。

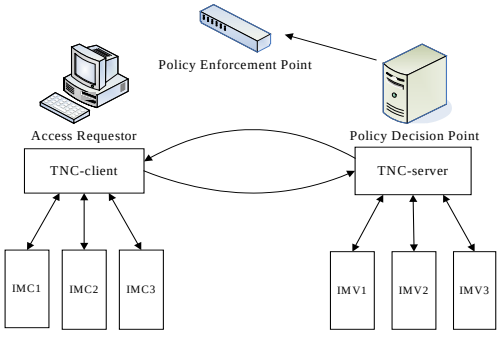

图2 TNC工作原理图

作者简介：颜 菲(1982－)，女，硕士生，主研方向：网络安全；任江春，博士生；戴 葵，副教授；王志英，教授、博导
收稿日期：2006-07-30 **E-mail：**yanfei8209@21cn.com

PEP负责监视网络连接，并在客户端AR发出网络连接请求后，将该请求传递给PDP；PDP接收到连接请求后，则发起对客户端的 3 步认证，即用户身份认证、平台身份认证和平台完整性度量(在不同环境下，认证顺序可以不同)。若 3 步认证均顺利通过，PDP认为终端可信，并通知PEP准许此次网络连接；否则将客户终端隔离起来以备修复[1]。

2.1 协议设计原理

基于 TNC 安全认证协议汲取了 TNC 的 3 步认证的思想来解决终端安全和网络安全问题。每个用户都是工作在特定平台上的，平台可信是用户可信的前提。因此，该协议的第 1 步就是搜集终端完整性数据，进行平台认证(平台身份认证和终端完整性度量)，完整性数据主要包括以下几个方面：

(1)操作系统版本以及其补丁级别；

(2)是否安装有TPM[3]核心芯片；

(3)终端是否安装有防火墙或是其他防病毒软件；

(4)杀毒软件签名库的最近更新日期；

(5)杀毒软件是否处于开启状态等。

若平台认证顺利通过，则进行用户身份认证。在众多的身份认证技术[4]中，本文采用了PKI数字证书技术，依靠非对称加密算法中密钥对匹配的唯一性，来确保用户的合法身份。使得每个终端用户都经过认证和授权，其操作都是符合规定的。

由于使用对称密钥加解密速度快，通常比非对称密钥算法快 10～100 倍。因此，本文在协议中还加入了一个协商共享密钥的步骤。平台认证通过后，采取公钥加密传输的方式为通信双方协商一对称密钥对，双方用户共享该密钥对进行通信，而其他用户对该密钥不得而知，这样能有效防止第三方密码猜测攻击。

综上所述，本文将TNC规范思想和PKI技术融合在一起，形成了一套安全高效的认证协议。该认证协议也包括 3 个步骤：平台认证(平台身份认证和终端完整性度量)，共享密钥协商和用户身份认证。

2.2 协议设计流程

下面以实体 A 和 B 之间的共享操作为例，给出了该协议的的具体设计流程，步骤如下：

(1)A 向 B 发送服务请求后，B 搜集自己的平台认证信息，连同平台认证请求一起发送给 A。逻辑表达方式为

B→ A：{ CertB, Sig(M_K, Sk_B), T, M_K}Pk_A

其中，CertB为平台B的公钥证书；M为平台B的完整性信息，采用单向散列函数计算其散列值，记为M_K；Sig(M_K, Sk_B) 表示用平台B的签名私钥Sk_B对M_K进行签名；T为当前时间戳。将以上信息打包后，用对方平台A的公钥Pk_A进行加密传送；

(2)A收到平台认证请求包后，首先用自己的私钥SK_A解密接收到的数据包，从中提取出对方平台的证书CertB，完整性数据签名值Sig(M_K, Sk_B)，以及完整性数据M_K，并从CertB中提取公钥Pk_B，验证签名值Sig(M_K, Sk_B)，若验证没有通过，A认为接收到的完整性数据已被篡改，停止协议并通知B；否则，向B发送A对M_K的签名Sig(M_K, Sk_A)、T+1 以及A的证书CertA；逻辑表达方式为

A→ B：{ Sig(M_K, Sk_A), T+1, CertA} Pk_B

(3)A收到密钥协商请求后，生成对称密钥K，并用私钥Sk_A进行签名后发送给可信第三方TTP，然后通知B一定时间内到TTP去取密钥K。逻辑表达式为

A→ TTP：{K, Sig(K, Sk_A), T+2} Pk_B

(4)B在规定时间内连接TTP收取密钥K，并用平台私钥Sk_B解密得到密钥K，签名值Sig(K, Sk_A)。最后，用Pk_A解密签名值验证密钥的完整性。逻辑表达方式为

TTP→ B：{K, Sig(K, Sk_A), T+2} Pk_B

(5)密钥协商成功后，B 向 A 发送用户身份认证请求；

(6)A 收到用户身份认证请求后，用对称密钥加密用户公钥证书以及其他与身份相关的信息传送给 B，逻辑表达式为

A→ B：{ CertUA }K

其中，CertUA 为用户公钥证书；

(7)用户认证通过后，B 给 A 回复确认信息。认证过程至此结束。

图 3 为协议的详细流程，在该认证流程的第(1)步和第(2)步，实现了 A、B 双方平台的相互认证，克服了以往单向认证所带来的安全问题，确保了服务器端的可信性。

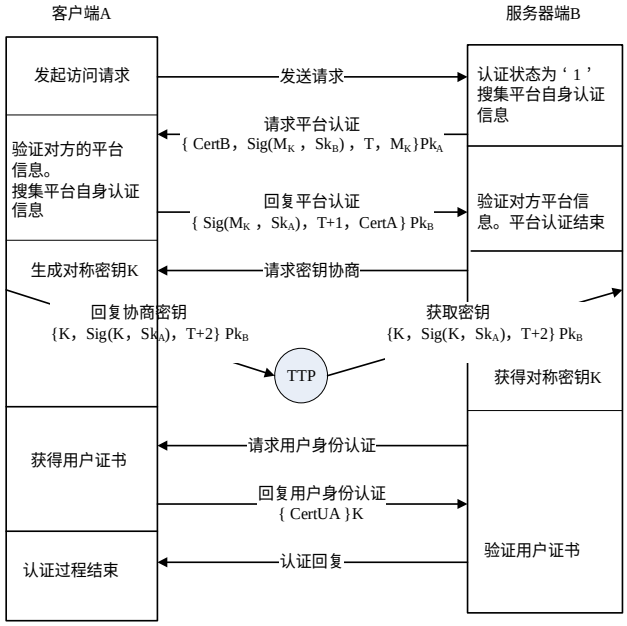

图 3 基于 TNC 安全认证协议的详细流程

3 安全认证协议的实现

协议在用户态和核心态下均可以实现。在用户态下进行数据包拦截最致命的缺点就是只能在Winsock层次上进行，而对于网络协议栈中底层协议的数据包无法进行处理。对于一些木马和病毒来说很容易避开这个层次的拦截。因此，本文选择了功能强大的NDIS[5]中间层驱动程序来截获网络数据包。

Passthru[5]是工作在网络层和媒体接入控制层之间的一个中间层驱动源代码范例，它实现了对网络数据包的底层截获。只要在Passthru基础上进行适当的修改，就可以实现本文提出的安全认证协议。

基于 TNC 安全认证协议的基本实现原理如下：自定义一个数据包，图 4 是自定义的认证协议报文格式。

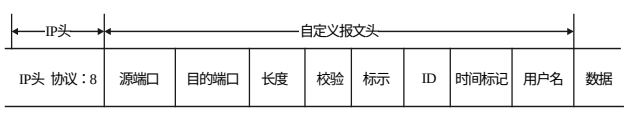

图 4 认证协议报文格式

其中，ID 为命令类型标志位。当 ID 为平台认证请求时，回复平台认证请求；当 ID 为平台认证返回时，发出密钥协商请求；当 ID 为密钥协商请求时，返回协商密钥；当 ID 为密钥

协商返回时，发出用户身份认证请求；当 ID 为用户身份认证请求时，回复用户身份信息；当 ID 为用户身份认证返回时，回复确认信息；当 ID 为用户身份信息确认时，认证过程结束。

接到数据时，根据包头信息进行判断：若不是自定义的数据包，则将该包缓存，并向对方平台发送平台认证请求；如果为自定义的数据包，则根据 ID 位回复相应的信息。认证顺利通过则转发缓存的数据包；否则，将该包丢弃。

4 协议的安全性分析

本文提出的安全认证协议主要是为了达到 3 个目的：(1)验证用户所在终端的完整性；(2)确认信息发送者的身份；(3)验证信息的完整性。该协议综合运用了数字摘要、数字信封、数字签名、数字时间戳和数字证书等多种安全认证技术[6]，下面以文件传送为例，分析该认证协议的安全性：

(1)终端的完整性

在请求方 A 试图接入网络进行文件传送前，接收方 B 对平台 A 的安全状态进行检测，从而决定是否允许 A 接入网络执行相应的权限。这个过程保证了终端的完整性，确保了终端在接入网络之前未受木马或是病毒攻击。

(2)不可否认性

不可否认性涉及到两个方面：

1)平台身份的不可否认性：平台认证过程中接收方B保留发送方A对完整性消息密文M_K的签名$Sig(M_K, sK_A)$能够证明平台A的真实身份；同样，发送方A保留签名值$Sig(M_K, sK_B)$以证明平台B的真实身份。

2)文件传送的不可否认性：协议中使用了可信第三方(trusted third party，TTP)，TTP内的日志文件可以防止接收方B取走密钥后却谎称自己没有收到密钥；接收方B称密钥K错误，解不开加密文件时，如果真是密钥错误，则由接收方B提供加密文件M_K、A对M_K 的签名、密钥K以及A对K的签名给TTP，由TTP裁定；如果是接收方B已经看到文件明文却谎称密钥K错误，则由发送方A提供文件密文M_K 、B对M_K 的签名给TTP，然后由TTP用存在其自身内的密钥K能否正确解密来裁定。

(3)消息的机密性和完整性

在文件传输前，协议通过终端完整性度量防止木马程序替换或篡改文件，保证了传输前文件的完整性；文件传输过程中，采用散列算法[6]从大块文件中提取一个摘要，并用私钥对该摘要进行签名操作后用进行加密传送；接收方B通过验证签名值可以确认消息是否从A发出以及消息是否被修改过，因为消息被插入、篡改或重排之后其散列值将会发生改变，从而保证传输过程中消息的机密性和完整性。

5 实验结果分析

根据上述协议，选用 3 台可信计算机[7]进行试验测试，可信计算机硬件环境为P4 2.4GHz、512MB内存，安装TPM芯片[3]。随机数密钥的产生、平台私钥以及平台证书的存储、文件的加密解密、签名以及认证都由可信计算机的TPM核心芯片完成。这 3 台机器分别用A、B、C标示，其中机器A和B均安装基于TNC的安全认证协议，而机器C不安装。将这 3 台机器两两连通进行测试。

5.1 连通性测试

机器 A、B 的认证状态置为“1”，两两运行 ping 命令后测试结果如图 5 所示。在平台可信的前提下，机器 A、B 能互相 ping 通，因为双方都装有基于 TNC 的安全认证协议，能自动完成完整性认证过程；由于 C 没有安装该协议，因此，A、B 分别能 ping 通 C，但是 C 无法 ping 通 A 和 B。

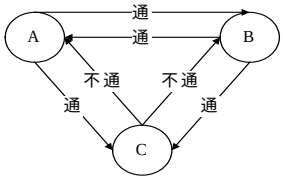

图 5 连通性测试结果

以上测试结果表明，终端顺利接入服务器端的条件是：终端安装有基于 TNC 的安全认证协议，且终端处于安全状态。不可信终端以及没安装该协议的终端均无法接入网络实施破坏行动。

5.2 完整性数据敏感性测试

测试结果见表 1。

表 1 数据敏感性测试结果

配置参数变动 \ 重认证情况	是否需重认证
安装 QQ 软件	不需要
更换操作系统版本	需要
更换硬盘	需要
增加内存条容量	不需要
卸载杀毒软件	需要

从以上测试结果体现了终端完整性认证的灵活性。在平台完整性认证过程中，只要终端不改变关键配置数据(在 2.1 节中提出)，其他对软硬件的升级以及容量扩充都不会影响终端完整性，避免终端频繁地陷入隔离状态，从而方便了用户操作。

5.3 用户独立性测试

现将实验条件改为 A、B、C 这 3 台机器均安装基于 TNC 的安全认证协议。并设定访问规则：终端 A 上两用户 a 和 b，a 只允许访问服务器 B，b 只允许访问服务器 C。测试结果如表 2 所示。

表 2 用户独立性测试结果

终端 A \ 服务器	服务器 B	服务器 C
用户 a	**通**	不通
用户 b	不通	通

从表 2 可以看出，通过采用终端完整性认证机制，基于 TNC 的安全认证协议能保证终端用户行为的合法性，使得每种用户操作都经过严格认证和授权，从而实现了多用户之间的相互独立性。

综合以上 3 项测试结果可以看出：基于 TNC 的安全认证协议通过采用 TNC 终端完整性度量的思想，确保了终端在接入网络之前的数据完整性和用户行为的合法性，避免了不可信终端接入网络实施破坏行动，这是保证网络安全和服务器安全的前提，也是跟现有安全协议相比的优点所在。

6 结束语

本文基于 TNC 规范提出了一套安全的网络认证协议，该认证协议将终端完整性度量技术与 PKI 技术相结合使用，提供了对通信双方的平台完整性验证以及信息发送方的用户身份认证，保证了终端、网络以及服务器端的安全。

(下转第 165 页)