可信网络关键技术研究

周雁舟[1,2] 张焕国[1] 宋 扬[2]
(武汉大学计算机学院 武汉 430079)[1] (信息工程大学电子技术学院 郑州 450004)[2]

摘 要 分析研究了可信网络的关键技术,揭示了其基本属性,即安全性、可控性及可生存性。并从可信网络的架构与信任模型、安全接入控制及网络管理等方面对其进行了深入的研究探讨。

关键词 可信网络,信任模型,安全接入,网络管理
中图法分类号 TP309 **文献标识码** A

Research on the Critical Technologies of Trustworthy Networks

ZHOU Yan-zhou[1,2] ZHANG Huan-guo[1,2] SONG Yang[2]
(Computer School, Wuhan University, Wuhan 430079, China)[1]
(Scool of Electronic Technology, The PLA Information Engineering University, Zhengzhou 450004, China)[2]

Abstract The paper analysed some key technology of Trustworthy Networks, and in this paper, three essential properties were proposed and explained to interpret trustworthy of network, namely security, survivability and controllability. Then we went deep into the trustwortyhy networks respectively from the network architecture, trusted model, security access control and the network manager.

Keywords Trustworthy networks, Trusted model, Security access, Network manager

1 引言

计算机网络系统由网络协议将终端、服务器和各种网络设备连接在一起,构成了一个复杂的系统。随着技术的研究与发展,对该系统的信息安全防护由对网络中某一单元或某一元素的防护发展到对整个网络的体系的防护。在这个过程中,可信网络的概念被提了出来,对它的研究也逐渐成为人们关注的焦点。

由于对它的探索刚刚开始,目前业界内对它的定义还没有完全统一。本文认为一个可信的网络指网络和网络用户的行为与预期结果相一致,即可以被信任,它不是一个某个安全产品或安全解决方案的应用,而是一个有机的网络安全全方位的架构体系。具体而言它应该包括如下属性:安全性、可生存性和可控性[1]。安全性,指网络数据和网络服务的安全性,包括了数据的完整性、不可否认性和保密性等。可生存性,按照文献[1]的定义指网络在遭受到攻击、故障或意外事故时能及时完成其关键任务的能力。可控性,指网络在某种程度上可以被监控和管理,并对网络异常行为进行控制和预警。可信网络与传统网络安全意义上最大不同是这3个属性,围绕着可信这个总体目标,互相融合形成一个有机的整体,每个属性都不是孤立存在的。

具体到可信网络的研究内容则包括如下部分:网络服务提供者的可信、网络信息传输的可信和终端用户的可信[2]。本文从可信网络的信任模型与架构、网络可生存性模型、可信网络安全接入控制和网络管理等方面对可信网络进行研究。

2 可信网络的架构与信任模型

可信网络架构是一个通过对现有网络安全产品和网络安全子系统的有效整合和管理,并结合可信网络的接入控制机制、网络内部信息的保护和信息加密传输机制,实现全面提高网络整体安全防护能力的可信网络安全技术体系[3]。根据可信网络的架构的定义,可信网络应具有如图1所示的架构。

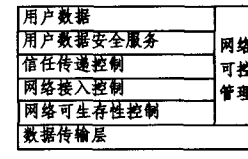

图1 可信网络架构

数据传输层负责网络数据的传输,并保障传输的可靠性。网络的可生存性控制保障了数据传输层遭到一定破坏后,还可以保证关键数据传递的可能性。网络接入控制,控制了网络申请者接入数据业务层的进出口。信任传递包括一组可信协议支持信任信息在可信用户间的共享,并驱动和协调具体的行为控制方式。网络数据安全服务保证了用户数据在安全特性方面的要求。网络的可控管理,使网络可管可控。

在上述架构中,如果能够构建出网络的信任模型,则可以解决可信网络中的一个核心问题,信任传递控制层的构建也可由此得到解决。然而现时的网络已经演变成为一个庞大的

到稿日期:2008-07-16 返修日期:2008-10-06 本文受863项目2008AA01Z404资助。
周雁舟(1971—),男,博士生,副研究员,主要研究方向为信息安全,E-mail:zyanzhou@163.com;张焕国(1945—),男,博士生导师,主要研究方向为信息安全;宋 扬(1981—),硕士生,研究方向为网络安全。

非线性复杂系统，网络节点间的协议交互以及用户之间的合作与竞争，使网络行为呈现出相当的复杂性、非线性，而且攻击和破坏行为也呈现出多样、随机、隐蔽和传播等特点，从而难以预测、分析和研究。另一方面，传统理论方法具有局限性，建立描述网络和用户行为的可信模型是比较困难的。这需要借助现有的基础理论和创建新的理论，开发新的研究方法，才能逐步解决[4]。本文对此做如下探讨。

信任在网络环境中具有非对称性、信任的可组合性和信任的传递性等特点。对信任度的计算方法有基于信任传递的简单迭代方法，该方法的计算基础是假定信任具有传递性；有基于原子传递的矩阵迭代法，该方法不仅考虑了信任的传递模型，同时将不信任的传递纳入到算法的模型中，并在计算中进行信任和不信任的有效组合；还有基于主观逻辑的迭代计算法，这种方法从主观逻辑的角度对可信网络进行简化和分析，借用结构化符号对可信传递与信任路径的组合进行了描述。上述的方法简单、有一定的可用性但都存在着假设条件与实际网络不符、信任传递算法与实际环境相差较远等问题。还需要在算法自适应设计、可信网络的初始数值的设计、可信度的进化计算等方面进行深入研究。

3 可信网络安全接入控制

3.1 IEEE802.1 协议的接入控制模式

对网络接入的安全控制研究在互联网发展的早期就已经开始了，其中有代表性的研究成果是 IEEE 802.1x 标准[5]。该标准提供了一种独立于网络服务类型的基于端口的接入控制标准，用于基于以太网、城域网和各种宽带接入手段的用户和用户设备的接入认证。它的认证流程如图 2 所示。

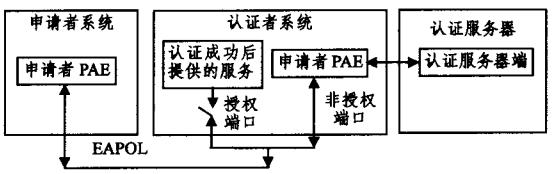

图 2 IEEE802.1 协议认证流程图

它的认证流程简述如下：

(1)申请者启动客户端程序，发出请求认证请求报文 EAPOL-Start，认证过程开始；

(2)认证者 PAE 收到消息后向申请者 PAE 发送 EAP-Request/Identity 消息，要求申请者 PAE 提供认证信息；

(3)申请者 PAE 响应认证者 PAE 发出的请求，通过数据帧 EAP-Request/Identity 将用户名信息送给认证者 PAE。认证者 PAE 将申请者 PAE 送上来的数据帧经过封包处理后通过 RADIUS Access-Request 数据帧送给认证服务器进行处理；

(4)认证服务器收到认证者 PAE 转发上来的用户名信息后，将该信息与数据库中的用户名表相比较，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时将此加密字通过 RADUIS Access-Challenge 帧传送给认证者 PAE，由认证者 PAE 通过 EAP-Request 帧传给申请者 PAE；

(5)申请者收到由认证者传来的加密字后，用该加密字对口令部分进行加密处理(此种加密算法通常是不可逆的)，并通过 EAP-Response 帧交给认证者 PAE，认证者 PAE 通过 RADIUS Access-Request 帧再传给认证服务器；

(6)认证服务器将送上来的加密后的口令信息和自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息 RADIUS Access-Accept，将其传给认证者 PAE，认证者 PAE 发出打开端口的指令，并通过 EAP-Success 帧告知用户的业务流可通过端口访问网络。否则，反馈认证失败的消息，并保持认证者 PAE 端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过；

(7)当用户要求下线或者是用户系统关机等需要断开网络连接时，请求方发送一个断网请求 EAP-Logoff 给认证者，然后认证者即把端口设为非授权状态(Unauthorized Port)，从而断开连接。

由以上流程可知 IEEE802.1 协议简单、实用，易于推广。但这种接入模式与目前可信网络的技术趋势不相吻合，因为一、认证协议的单项性不符合安全性的要求，二、该协议将业务流和认证数据的离，固然有对网络业务数据方便性的优点，但与可信网络对网络行为和用户行为的可信性要求不符，所以 IEEE802.1 协议不能作为可信网络的接入控制协议来使用。

3.2 TNC 网络接入控制

可信计算工作组(TCG)制定了一个基于可信计算技术的网络连接规范。TCG 体系的可信网络连接包括了开放的终端完整性(Integrity)架构和一套确保安全互操作(Interoperability)的标准[6]。它的连接结构如图 3 所示。

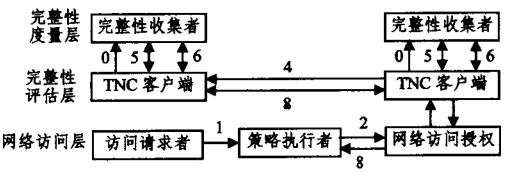

图 3 TNC 连接结构图

TNC 的架构分为 3 类实体：请求访问者(the Access Requestor，AR)、策略执行者(Policy Enforcement Point，PEP)、策略定义者(Policy Decision Point，PDP)，这些都是逻辑实体，可以分布在任意位置。TNC 体系架构在纵向分为 3 个层次，从下到上为：网络访问层，这一层用于支持传统的网络连接技术；完整性评估层，负责评估所有请求访问网络的实体的完整性；完整性度量层，收集和校验请求访问者的完整性相关信息的组件。

可信网络连接的建立过程如下：

在建立网络连接之前。TNC 客户端需要准备好所需要的完整性信息，交给完整性收集者(IMC)。在一个拥有 TPM 的终端里面，这也就是将网络策略所需信息经散列后存入 PCRs，TPM 服务端需要预先制定完整性的要求，并交给完整性验证者(IMV)。

1. 向 PEP 发起访问请求，这个策略执行者通常是一个网络接入网关。

2. PEP 将访问请求描述发往网络访问授权者。

3. 假设授权被允许了，网络访问授权者将请求发往 TNC 服务端。

4. TNC 服务端开始对客户端的授权验证。

(下转第 143 页)

on e-Commerce Technology. California, 2004:129-136
[14] Menascé D A. Composing Web Services: A QoS View[J]. IEEE Internet Computing, 2004, 8(6):88-95
[15] 刘书雷,刘云翔,张帆,等. 一种服务聚合中 QoS 全局最优服务动态选择算法[J]. 软件学报,2007,18(3):646-656
[16] Demian A D, Ananthanarayana V S. Quality Driven Web Service Selection and Ranking[C]//Fifth International Conference on Information Technology. New Generations, 2008
[17] Wan C, Wang H. Uncertainty-aware QoS Description and Selection Model for Web Services[C]//IEEE International Conference. 2007:154-161
[18] Cardoso J, Bussler C. Semantic Web Services and Processes: Semantic Composition and Quality of Service[C]//On the Move to Meaningful Internet Computing and Ubiquitous Computer. Irvine CA, 2002
[19] Jaeger M C, Rojec G, Muhl G. QoS aggregation for Web service composition using workflow patterns[C]//The 8th IEEE International Conference on Enterprise Distributed Object Computing. California, 2004:149-159
[20] Wang X, Tomas V, Mick K, et al. A QoS-aware Selection Model for Semantic Web Services[C]//ICSOC 2006, LNCS 4294. 2006:390-401

(上接第 113 页)

5. TNC 客户端告诉 IMC 开始了一个新的网络连接,这个网络连接需要一个完整性握手协议。IMC 返回所需信息。TNC 服务端将这些信息交给 IMV。

6. 在这个过程里面,TNC 客户端和 TNC 服务端需要交换一次或多次数据,直到 TNC 服务器端满意为止。

7. 当 TNC 服务器完成了对客户端的完整性握手,它将发送一个推荐信(Action Recommendation)给网络访问授权(NAA),要求允许访问。这里需要特别注意,如果还有另外的安全考虑,此时 NAA 仍旧可以不允许网络访问者(NA)的访问。

8. NAA 传递访问决定(final decision)给 PEP,PEP 将最终执行这个决定,来控制 NA 的访问。

TNC 的安全接入控制系统主要基于"可信代理"的安全机制,结合终端系统的认证、评估子系统来实现对接入可信网络的终端系统、用户进行认证/授权控制,能够有效地避免可信网络中因不可信终端系统接入所带来的潜在风险。但一些关键技术点:网络安全策略的定义,客户端完整性的度量值和网络传输协议的安全性和效率都是需要进一步的研究。

4 网络的可管、可控和生存性研究

互联网络发展至今,已成为一个庞大的非线性复杂系统,如系统规模和用户数量巨大且不断增长,协议体系庞杂,业务种类繁多,异质网络融合发展等等。这远远超过了当初设计的考虑,现有的一些控制手段相对显得很薄弱,产生了许多的安全隐患。"边缘论"和面向非连接的设计思想保障了网络的高效互通,逐跳存储转发的分组传送方式简单灵活,无需在中间节点维护过多的状态信息,核心网络的工作集中于路由转发。这些机制的优点是设计简单,可扩展性强等,然而却造成了分组传输路径的不可控,网络中间节点对传输数据包的来源不验证、不审计,导致地址假冒、垃圾信息泛滥,大量的入侵和攻击行为无法跟踪[7]。所以对网络可管和可控目前依然是一个研究难题。

可信网络的可控可管性主要是指网络具有对用户行为、网络运行状态和网络资源的有效控制和管理的能力[8]。为了实现真正的可信和安全,网络必须具有对用户行为高度的控制和管理能力。对用户行为的可控可以采用可信计算技术和密码技术进行管理和控制。对于网络状态的管理可以采用网络用户数据和管理数据分离开;将网络状态数据的管理功能纳入到核心路由器的处理中;将状态管理功能模块化和普适化。

可生存性(Survivability)是指网络在遭受攻击、失效或者意外后能够及时地完成任务的能力[9]。可生存性研究包括:定量评估问题,涉及建立包括网络的脆弱性分析、用户攻击行为描述在内的合理故障模型理论和定量评估的方法;保证可生存性的机制和策略问题,从单纯容错到同时考虑容错、容侵;从同构网络环境下的单种技术到异构网络下的层次化、协同可生存性技术。目前这些问题都是没有解决的热点问题。

结束语 可信网络是国际上将要出现的研究方向,借鉴了系统可信性的概念,将传统孤立的研究内容融合到网络可信这一目标下,面向用户提供系统的安全服务。本文对可信网络的几个关键问题进行了分析、总结和研究,包括它的架构、信任模型、接入控制、网络的可控可管和可生存性方面。

参 考 文 献

[1] 林闯,彭雪海. 可信网络研究[J]. 计算机学报,2005,28(5):751-758
[2] Forsberg D, Ohba Y, Patil B, et al. Protocol for Carrying Authentication for Network Access (PANA) [EB/OL]. [2007-12-03]. http://www.ietf.org/internet-drafts/draft-ietf-pana-pana-18.txt
[3] Casadcm, Garfinel T, Akellaa, et al. SANE: A protection architecture for enterprise networks[C]//Proceedings of 15th USENIX Security Symposium. July31-Aug. 4. 2006, Vancouver, Ganada, 2006:137-151
[4] Nicol D M, Sanders W H, Trivedi K S. Model-based evaluateon: From dependability to secureity[J]. IEEE Transactions on Depen-dable and Secure Computing, 2004, 1(1)
[5] IEEE. Std. 802. 1x IEEE Standard for Local and Metropolitan Area Network Port Based Network Access Control[s]. 2001
[6] TCG Trusted Network Connect TNCArchitecture for Interoperability[OL]. www.trustedcomputinggroup.org April 2008
[7] Lin Chang, Peng Xuehai. Research on network architecture with trustworthyness and controllability[J]. Journal of Computer Science and Technology, 2006, 21(5):732-739
[8] Shenker S, Allman M, Paxson V. Architectural support for network trouble-shooting [EB/OL]. NSF FING' 2006. http://www.nets-fing.net/Funded/ArchtSupportNet.php
[9] Ellison R, Fischer D, Linger R, et al. Survivable network systems: An emerging discipline [R]. CMU/SEI-2001-TN-001. Pittsburgh, PA, USA: Software Engineering Institute, Camegie Mellon University, 2001