

# 可信网络的发展及其面对的技术挑战

## Development of Trustworthy Network and Facing Scientific Challenges

中图分类号: TP393 文献标识码: A 文章编号: 1009-6868 (2008) 01-0013-04

**摘要:** 随着信息网络的基础性、全局性作用日益增强,传统的网络理论与技术,尤其是网络安全,已经不能满足网络发展的需要,提供系统的安全可信的服务已经成为网络研究的新趋势。本文认为可信网络应该是网络和用户的行为及其结果总是可预期与可管理的。网络可信主要包括服务提供者的可信、网络信息传输的可信性和终端用户的可信等3个方面的内容。从网络与用户行为的可信模型、可信网络的体系结构、服务的可生存性、网络的可管理性4个方面进行研究,以便为解决可信网络面临的科学问题提供思路。

**关键词:** 可信网络;安全性;可生存性;可管理性

**Abstract:** While the information network's basic and global effect is gradually becoming more and more significant, traditional network theories, especially the network security theory, are not good enough to support the network's development. Supplying systematic and trustworthy services is the trend of the network study. In this paper, the trustworthy network is a kind of network whose behaviors and results can be predicted and managed by users. The trustworthy network has three components, namely, network service provider, network transmission and end user. The model, architecture, manageability and survival problem of the trustworthy network are discussed here to give guidance in solving scientific issues met in the research of trustworthy network.

**Key words:** trustworthy networks; security; survivability; manageability

随着网络技术和应用的飞速发展,互联网日益呈现出复杂、异构等特点,当前的网络体系已经暴露出严重的不足,网络正面临着严峻的安全和服务质量(QoS)保证等重大挑战,保障网络的可信成为网络进一步发展的迫切需求。最初网络应用的绝对自由主义理念和管理的无政府状态,已不适应当前实际的网络发展,需要建立网络可信行为的新秩序。在网络领域里,“高可信网络”的创意来自中国,旨在以高可信网络满足

“高可信”质量水准的应用服务需要。如今,“高可信网络”已被正式写进中国国务院公布的《国家中长期科学和技术发展规划纲要(2006—2020年)》(以下简称《纲要》)。《纲要》明确指出:“以发展高可信网络为重点,开发网络信息安全技术及相关产品,建立信息安全技术保障体系,防范各种信息安全突发事件”。

### 1 可信计算的发展

可信计算只提供了计算机平台的可信,不能提供网络可信,需要进一步将可信扩展到整个网络。1999年,由康柏、惠普、IBM、Intel和微软牵

林闯/LIN Chuang<sup>1</sup>  
王元卓/WANG Yuan-zhuo<sup>1,2</sup>

田立勤/TIAN Li-qin<sup>1,3</sup>

(1.清华大学计算机系,北京 100084;

2.北京科技大学信息学院,北京 100083;

3.华北科技学院计算机系,北京 101601)

(1. Department of Computer Science and

Technology, Tsinghua University, Beijing

100084, China;

2. Information Engineering School, University of

Science and Technology Beijing, Beijing

100083, China;

3. North China Institute of Science and

Technology, Beijing 101601, China)

头组织了可信计算平台联盟(TCPA),致力于在计算平台体系结构上增强其安全性。2001年1月,TCPA发布了标准规范;2003年改组为可信计算组织(TCG),成员扩大到200家;2003年10月发布了TPM规范。2002年底IBM发布了带有嵌入式安全子系统(ESS)的笔记本电脑,2003年9月,Intel推出了LaGrande技术。作为可信计算最积极的倡导者,微软公司宣称将其操作系统建立在“高可信计算”的基础上。中国目前包括联想在内也有8家企业加入了TCG。TCG进一步划分成更详细的研究组,包括体系组、无线移动组、PC客户机组、服务器组、软件堆栈组、存储组、可信网络连接组、可信平台模块组<sup>[1-3]</sup>等。

可信计算首先检查用户身份是否可信,如它是不是合法的一员、是不是认可的设备;再检查用户状态,如它的防御措施是否到位、是不是有安全合格的防病毒软件、终端防病毒软件数据是否及时更新等。为了提高美国的信息安全和信息信任,美国国家自然科学基金在2006年支持信息空间信任的研究项目<sup>[4]</sup>,美国国家研究委员会也提出信息空间信任研究

**基金项目:** 国家自然科学基金资助项目  
(90412012; 60673187)

建议<sup>[5]</sup>。中国在上述领域也进行了多年的研究,一些公司已经开始在可信计算终端和网络安全方面开展工作,但较多地处于跟踪国外研究动态的阶段。可信计算被列入“十一五”规划,中国国家信息中心、北京工业大学等正在进行可信计算终端的研究。清华大学国家信息实验室的网络控制研究组先后在可控可信可扩展的新一代互联网体系<sup>[6]</sup>、可信网络<sup>[7-8]</sup>、网络安全的随机模型方法与评价技术<sup>[9]</sup>等相关方面进行了大量的前瞻性的研究。

## 2 可信网络的含义

目前,网络安全技术多、杂、零散,实现代价越来越大,对网络性能的影响越来越大、越来越复杂,其臃肿的弊端逐渐显示出来,业界需要新的理念和思路来解决网络的安全与性能问题,可信网络在这种背景下被提出。目前业界虽然对可信网络有不同理解,有的认为是基于认证的可信、有的认为是基于现有安全技术的整合、有的认为是网络的内容可信、有的认为是网络本身的可信、有的认为是网络上提供服务的可信等,然而对可信网络的目的都又统一的认识:提高网络和服务的安全性,使整个人类在信息社会中收益。可信网络可以提高网络的性能,简化因不信任带来的监控、防范等系统的开销,提高系统的整体性能。同时,动态行为的信任可以提供比身份信任更细粒度的安全保障。

我们认为一个可信的网络应该是网络和用户的行为及其结果总是可预期与可管理的,能够做到行为状态可监测、行为结果可评估、异常行为可管理。具体而言,网络的可信性应该包括一组属性,从用户的角度需要保障服务的安全性和可生存性,从设计的角度则需要提供网络的可管理性。不同于安全性、可生存性和可管理性在传统意义上分散、孤立的概念内涵,可信网络将在网络可信的目

标下融合这3个基本属性,围绕网络组件间信任的维护和行为管理形成一个有机整体。

## 3 网络可信技术研究的主要内容

网络可信技术是在原有网络安全技术的基础上增加行为可信的安全新思想,强化对网络状态的动态处理,为实施智能自适应的网络安全和服务质量控制提供策略基础。网络可信主要包括3方面的内容: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。

### 3.1 服务提供者的可信

服务提供者的可信包括两个方面的内容:服务提供者的身份可信和行为可信。服务提供者身份可信是指服务提供者的身份可以被准确鉴定、不被他人冒充,即身份真实有效。服务提供者行为可信是指服务提供者的行为真实可靠、不带有欺骗性,不会给用户终端带来安全危险。

传统的安全机制提供授权和认证,解决了服务提供者的身份信任问题,但并不能处理服务提供者的行为信任问题。服务提供者的行为信任包括两个方面,基本行为信任和高级行为信任。

基本行为信任是指服务提供者的行为真实可靠、不欺骗、不随意中断服务、按契约的规定提供服务等。如在学校数字资源的使用方面,服务提供者按规定及时提供可靠的数字资源,提供的内容与规定的契约相符合、不虚假不欺骗、并随时可用。

高级行为信任是指服务提供者在提供服务的过程中没有破坏用户安全的行为,包括不提供带有恶意程序的内容、不将用户的私有信息透漏给第三方、不为了商业利益对用户进行其他破坏行为等。如在学校数字资源的使用方面,服务提供者的内容不携带蠕虫和木马等可能影响用户安全的恶意程序,不将用户的私有信

息如电子邮件等有意无意透漏给第三方、使用户收不到垃圾邮件从而消除用户安全隐患以及不提供不安全的超链接等。

### 3.2 网络信息传输的可信

网络信息传输的可信是指网络各节点在传输信息的过程中忠实、不删不改不夹带,在传输信息时可以根据用户的要求在指定的路径上传输信息,其核心是保证信息在传输过程的保密性、完整性和可用性。网络信息传输的可信一方面要防止第三方对网路传输信息的破坏,另一方面也要防止网络本身可能给传输的信息带来破坏。在制定的策略方面,一方面要在接收方和发送方从技术上保证传输信息的可信性,另一方面也要从法律制度、管理和技术等方面保证网络信息不被网络本身和第三方破坏的可信性。

### 3.3 终端用户的可信

如果从可信网络的服务器、网络本身和网络用户3个组成信息系统层面上来看,现有的保护措施是逐层递减的,这说明人们往往把过多的注意力放在对服务器和网络的保护上,而忽略了对用户端的保护,这显然是不合理的。因为用户端不仅能创建和存放重要的数据,也可能由于其脆弱性引发攻击事件,例如数据泄密和蠕虫病毒感染等。如果我们能从用户端源头开始控制不安全因素,使其符合安全的行为规范,就可以更加完善地保证整个网络的安全。因此加强用户端的可信是整个网络可信的重要内容之一。

终端用户可信又包括两个方面的内容——终端用户的身份可信和行为可信。终端用户身份可信是指终端用户的身份可以被准确鉴定、不被他人冒充,即终端用户的身份真实有效。终端用户的行为可信是指终端用户的行为可评估、可预期、可管理,不会破坏网络设备和数据。传统的安全

机制可以提供用户的授权和认证,能解决用户的身份信任问题,但并不能处理用户的行为信任问题。例如在数字化电子资源的订购方面,大学生可以通过可信的身份(一般是学校的IP地址)登录到学校定购的数字资源服务器上,但他的行为却有可能是不可信的,如使用网络下载工具大批量地下载学校购买的电子资源或者私设代理服务器牟取私利等。

#### 4 可信网络需要解决的科学问题

可信网络的研究将面临着4个重要的科学挑战:第一,由于网络攻击、破坏行为的多样性、随机性、隐蔽性和传播性,使用现有的网络模型理论已经难以对其进行描述分析;第二,网络尤其是互联网络的体系结构中,“边缘论”和面向非连接的设计思想保障了高效的互通,但控制手段相对薄弱,难以解决现实网络的安全问题;第三,网络固有的脆弱性、人为的操作失误和管理漏洞、以及网络攻击和破坏的存在,使得网络在保障服务的可生存性方面面临很大的挑战;第四,复杂的网络结构和高负荷网络负载使网络行为难以协调管理。

##### 4.1 网络与用户行为的可信模型

相比传统的网络安全概念,可信的内涵更深:安全是一种外在表现的断言,可信则是经过行为过程分析得到的一种可度量的属性。这是网络安全研究领域近来取得的一个新共识。如何建立能够有效分析刻画网络和用户行为的可信模型是认识和研究可信网络的关键问题。

建立网络与用户的行为可信模型的重要性主要体现在:它抽象而准确地描述了系统的可信需求而不涉及到其实现细节,便于通过数学模型的分析方法找到系统在安全上的漏洞。其次,可信模型是系统开发过程中的关键步骤,在美国国防部的“可信计算机系统的评价标准(TCSEC)”中,从B

级开始就要求对安全模型进行形式化描述和验证,以及形式化的隐通道分析等。再次,可信模型的形式化描述、验证和利用能够提高网络系统安全的可信度。最后,建立包括网络的脆弱性评估以及用户攻击行为描述等内容的可信评估理论,是实现系统可信监测、预测和干预的前提,是整个可信网络研究的理论基础。

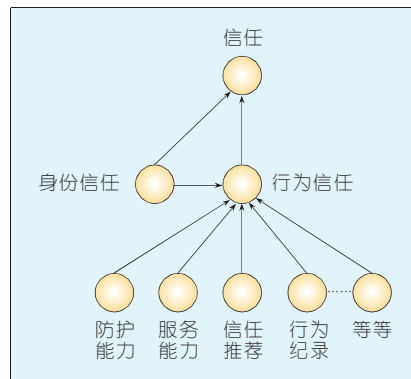
由于不可能存在完全安全的网络系统,所以网络脆弱性评估的最终目的不是完全消除脆弱性,而是提供解决方案,帮助系统管理员在“提供服务”和“保证安全”之间找到平衡,是攻击发生前的主动检测。例如建立攻击行为的描述机制,从大量正常用户行为中区分出存在攻击企图的行为,在可信评估基础上实施主机的接入控制。

传统的基于规则的方法一般只用于局部检测,对整体检测有些力不从心。现有的脆弱性评估工具,绝大多数都是基于规则的,最多也只是能够对单一的主机的多种服务进行简单的相关检查,对多台主机构成的网络进行有效评估还只能依靠人力。基于模型的方法为整个系统建立模型,通过模型可获得系统所有可能的行为和状态,利用模型分析工具测试,对系统整体的可信性进行评估。

图1描述了可信性分析的元素。网络行为的信任评估包括行为和身份的信任,而行为可信又建立在对防护能力、服务能力、信任推荐、行为记录等内容信任的基础之上。

##### 4.2 可信网络的体系结构

互联网在设计之初对安全问题考虑不足,是产生当前网络脆弱性的一个重要因素。然而目前的许多网络安全设计很少触及网络体系的核心内容,大多是单一的防御、单一的信息安全和补丁附加的机制,遵从“堵漏洞、作高墙、防外攻”的建设样式,以共享信息资源为中心在外围对非法用户和越权访问进行封堵,以达到



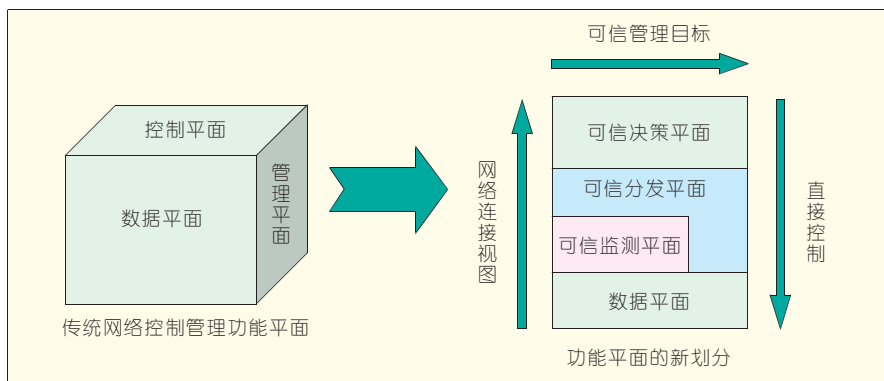
▲图1 可信模型的一种分析模式

防止外部攻击的目的。

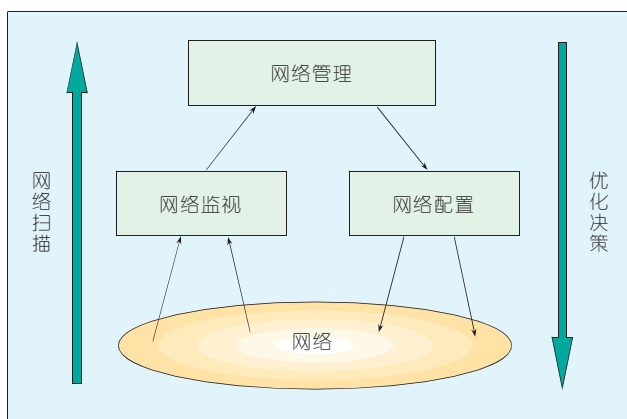
在攻击方式复合交织的趋势下,当前安全系统变得越来越臃肿,严重地降低了网络性能,甚至破坏了系统设计开放性、简单性的原则。因此基于这些附加的、被动防御的安全机制上的网络安全是不可信的,从体系结构设计角度减少系统脆弱性并提供系统的安全服务尤为重要。尽管在开放式系统互连参考模型的扩展部分增加了有关安全体系结构的描述,但那只是概念性的框架,很不完善。

网络安全已不再仅局限于信息的可用性、完整性和机密性,服务的安全将被作为一个整体属性为用户所感知的趋势日益明显,这就促使研究人员重新设计网络体系,整合多种安全技术并使其在多个层面上相互协同运作。一方面,作为补丁而附加到网络系统上的传统安全机制,由于单个安全技术或者安全产品的功能和性能都有其局限性,只能满足特定的安全需求,且安全系统自身在设计、实施和管理等各个环节上也不可避免地存在着脆弱性,严重威胁这些防御设施功效的发挥。如入侵检测不能对抗蠕虫病毒,防病毒软件不能对抗拒绝服务攻击,而防火墙对病毒攻击和木马攻击也无能为力。另一方面,网络安全研究的理念已经从被动防御转向了积极防御,不再局限于在共享信息外围部署安全防御,而需要从访问源端的开始进行安全分析,尽可能地将不信任的访问操作控制在





▲图2 可信网络的体系结构示意图



◀图3 网络管理示意图

源端。因此,十分需要为网络提供可信的体系结构,避免出现类似传统附加性安全机制的弊端。可信网络体系结构研究必须充分认识到网络的复杂异构性,从系统的角度保障安全服务的一致性。

新体系结构如图2所示,监控信息(监测和分发)和业务数据的传输通过相同的物理链路,控制信息路径和数据路径相互独立,这就使得监控信息路径的管理不再依赖于数据平面对路径的配置管理,从而可以建立高可靠的控制路径。与此形成强烈对比的是,现有网络的控制和管理信息的传输则必须依赖由路由协议事先成功设置的传输路径。

#### 4.3 服务的可生存性

可生存性在某种程度上可以理解为资源调度问题,即为同某个服务关联的冗余资源设计合理的调度策略,借助实时监测机制,调控这些资

源对服务请求做出响应。在网络系统遭受攻击和破坏时,应该通过可生存性设计,尽可能地减少关键服务的失效时间和失效频度。可生存性是网络研究的一个基本目标,需要为系统提供自测试、自诊断、自修复和自组织能力,维持关键服务的关键属性,如完整性、机密性、性能等。由于网络系统固有的脆弱性、人为的管理漏洞和操作失误、以及客观存在的攻击和破坏行为,在网络系统基础性作用日益增强的今天,保障网络关键服务的可生存性具有重要的现实意义。

几乎所有的网络系统都存在着可以造成攻击的渗透变迁,亦即存在着脆弱性。通常这些脆弱性并不是系统设计者刻意留下的,而是由于一些意外的原因造成的,表现在设计、实现、运行管理的各个环节。网络上的计算机总要提供某些服务才能够与其他计算机相互通信,然而如此复杂的系统不可能没有瑕疵。除了某些特

定网络服务程序编写的错误,网络系统的脆弱性还可能包括某个网络节点的服务和软件的不正确配置和部署,以及网络协议本身的缺陷。协议定义了网络上计算机会话和通信的规则,如果在协议设计时存在瑕疵,那么无论实现该协议的方法多么完美,它都存在漏洞。

安全服务作为网络系统的关键服务,某种程度的失效就可能会造成整个系统遭受更大范围的攻击,导致更多服务的失效甚至是系统瘫痪。因此必须将这些关键服务的失效控制在用户许可的范围内。可生存性的研究必须在理论上深入剖析独立于具体攻击行为的可生存性的本质特征,通过容错设计尽可能地隐藏脆弱性,避免出现错误的系统状态变迁,通过容侵设计使脆弱性被攻击者利用时,尽可能地减少攻击所造成的影响,为服务的可恢复创造条件。

#### 4.4 网络的可管理性

互联网络发展至今,已成为一个庞大复杂的非线性系统,具有规模大、用户数量不断增长、协议体系庞杂、业务种类繁多、异质网络融合发展等特点。这远远超过了当初设计时的考虑,使得网络越来越难于管理。网络的可管理性是指在网络环境受到内外干扰的情况下,不仅对网络状态还对用户行为进行持续的监测、分析和决策,进而对设备、协议和机制的控制参数进行自适应优化配置,使网络的数据传输、资源分配和用户服务可以达到预期的程度。

当前网络的体系结构和管理协议不支持可管理性设计,仅仅是在现有网络体系结构的基础上添加网络管理功能,无法实现网络的有效管理。可信网络应该是一个充分可管理的网络,网络的可管理性对于网络的其他本资属性,如安全性、鲁棒性、普适性等也具有重要的支撑作用。“网络管理”主要是对网络状态进行持

►下转第41页