一种在网络环境下实施多级安全策略的方法*)

张志文　周明天
(电子科技大学计算机学院　成都610054)

摘　要　本文提出了一种新颖的在网络环境下实施多级安全机制的方法,测试结果证明此方法对网络性能影响小,简单实用。

关键词　多级安全机制,计算机网络,Linux

A Method of Enforcing Multilevel Security Policy in Computer Networks

ZHANG Zhi-Wen　ZHOU Ming-Tian
(College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054)

Abstract　Due to the distributed nature of the network architecture, the high degree of openness of the network medium and the increased need for sharing resources within the network, the protection mechanism residing within the individual operating system becomes inadequate to ensure the security of inter-process communications across the network. Hence a security enforcement mechanism for the network is required in addition to the existing protection mechanisms within the individual computers. This paper proposes a novel method of enforcing multilevel security in computer networks. Experimental results show that the method has little effect on the network performance, which is simple and practical.

Keywords　Multilevel security, Computer networks, Linux

1　引言

由于计算机和网络的广泛使用,计算机之间的信息共享快速增长,计算机网络的安全问题一直是研究的热点。而目前操作系统的安全机制主要考虑单机系统的信息安全,忽视了网络环境下的信息安全。

过去对网络环境的信息安全的研究主要考虑信息在网络上传送时,其本身的安全问题(比如机密性、有效性),主要针对信息的非法窃听,而很少关心合法用户的信息泄露问题,这些问题可以通过加密技术来解决,例如,IPSEC 在 IP 层提供安全的通信[14~16];SSL/TLS[17,18]运行在 TCP 与高层应用协议(如 HTTP,FTP,TELNET)之间,通过双向认证,在 C/S 通信之间建立加密的连接。然而,当两个或两个以上独立自主的主机互联,构成计算机网络时,操作系统本身的保护机制已经不适合保护计算机网络的通信。由于网络的分布特性,高度开放性,网络信息的共享性,合法用户可以随便泄露自己所知道的信息。

作为事实标准的 TCP/IP 协议对网络通信的控制是脆弱的,通过网络,两个用户是很容易通信的,几乎不受任何限制。只需简单的 Socket 编程,简单的 C/S 程序,或者现成的网络应用,就可以将自己所知道的信息传送到世界的任何地方,只要允许用户使用网络。这对于处理多级安全信息的计算机系统来说是不可忍受的,要求有安全策略对网络间的通信,信息共享进行控制,防止"合法"用户随意泄漏敏感信息。

多级安全网络的研究开始主要针对局域网,文[4]利用可信接口单元(TIU),主机的安全级别由 TIU 决定,可以是单安全级或多安全级,通过修改链路层数据报头来发送安全级别,来提供主机之间的多级安全策略;文[5]在内部机构网络(ION)实施多级安全网络机制,将地理上分散的网络看成是一个个的逻辑网络,每个逻辑网络有 ION 网关,由 ION 网关来实施逻辑网络之间的多级安全机制;文[6]描述了在局域网实施多级安全策略的方法,局域网由网络接口设备,网络安全设备(NSD),网络安全员终端,网络安全中心组成。主机连接到 NSD,每个 NSD 具有微处理器,本地 RAM,ROM,加密硬件,以及以太网硬件,主机之间通过数据报通信,形成一个完全封闭的局域网。上述模型或方法要么需要专用的网络接口设备,要么是控制粒度较粗,甚至修改局域网的数据包格式,来提供网络的多级安全策略,因而牺牲了系统的兼容性,及广泛的可用性。文[12]是对文[13]的实现,其 TCP 和 UDP 报文都带了安全信息,降低了 TCP 的效率。

本文以应用广泛的 Interrnet 为基础,提出了一种新颖的在网络环境下实施多级安全机制的方法,区分 TCP 和 UDP 报文,对 TCP 进行特别处理,降低对网络性能的影响,兼容目前的网络应用,并对网络性能进行了分析。测试结果表明,此方法对网络性能的影响非常小,是简单实用的。

2　安全策略模型

2.1　基本概念

1) 实体(Entity):网络资源(如文件,进程,设备等)以及合法的用户;

2) 主体(Subject):主动实体,它对其他实体执行操作,这里的逐条是参与通信的主机(client / server),每个主机都有一个安全级别;

3) 客体(Object):被动实体,由主动实体操作,这里的客体是主机之间通信的数据,比如数据报,每个客体都有一个密级;

*)本文工作受到国家"863"高科技项目(合同号2001AA144020)的支持。张志文　博士生,主要研究领域为操作系统安全、网络安全。周明天　教授,博士生导师,主要研究方向为计算机网络,网络与信息安全,并行分布处理,分布对象技术。

4）安全级别(Security Class)：网络中实体的安全属性，安全级别由敏感级别和类别集合组成，安全级别用以决定是否允许主体对客体的访问；安全级别集合及其上所确定的级别之间信息流动的关系构成格；

5）密级(Classification)：分配给客体的安全信息，它反映了客体的重要程度。密级和安全级别一样，也是由敏感级别和类别组成的；

6）签证(Clearance)：反映相应主体的信任程度。其表示也和安全级别一样，用户的签证是根据对用户背景的调查来分配的，由网络安全员分配，进程的签证是由它代表执行的用户的签证决定的；

7）支配(Dominate)：若有两个安全级别 labelA 和 labelB，如果 labelA 的敏感级别大于等于 labelB 的敏感级别，且 labelA 的类别集合包含 labelB 的类比集合，则称 labelA 支配 labelB；

8）相等(Equal)：若有两个安全级别 labelA 和 labelB，如果 labelA 的敏感级别等于 labelB 的敏感级别，且 labelA 的类别集合等于 labelB 的类别集合，则称 labelA 与 labelB 相等；

9）不相交(Disjoint)：若有两个安全级别 labelA 和 labelB 是不可比的，则称 labelA 与 labelB 不相交；

10）操作(Operation)：主体对客体的作用，这里只有一个通信操作；

11）简单安全性(Simple security)：主体允许从客体读，当且仅当主体敏感标签支配客体的敏感标签；

12）*-特性(Star security)：主体允许向客体写，当且仅当主体的敏感标签受客体的敏感标签支配；

13）安全周界(Security perimeter)：是一个主机的集合，具有一致的安全策略。在同一安全周界的所有主机的安全级别是兼容的，换句话说，它们相互认识它们的安全级别。

2.2 策略模型

最著名的多级安全策略模型是 Bell &Lapadula 模型[1~3]，模型使用数学符号和集合理论定义了安全状态的概念、访问模式，及授予访问的规则。模型用主体、客体来描述一个访问。

网络多级安全策略模型可以看作是 Bell & Lapadula 模型在网络上的扩展。我们假设系统由运行独立操作系统的主机组成，模型的主体是网络主机，客体是网络主机间通信的数据，模型只有一个操作，即网络通信。网络通信可以用三元组表示(S_i,O_{ij},S_j)，这里 S_i 是发送主体，S_j 是接受主体，O_{ij}是通信的数据。

一个网络通信满足简单安全策略，当且仅当 S_j 的签证支配 O_{ij}的密级，即：

simple_security(S_i,O_{ij},S_j) iff
domainates(clearance(S_j),classification(O_{ij}))

一个网络通信满足 *-安全特性，当且仅当 O_{ij}的密级支配 S_i 的签证，即：

star_security(S_i,O_{ij},S_j) iff
domainates(classification(O_{ij}),clearance(S_i))

一个网络通信是安全的，当且仅当满足简单安全特性和 *-安全特性；即：

security(S_i,O_{ij},S_j) iff
simple_security(S_i,O_{ij},S_j) and
star_security(S_i,O_{ij},S_j)

一个网络系统是安全的，当且仅当当前系统所有的网络通信都是安全的。

3 策略实现

3.1 计算模型

在 Internet 上，网络计算模型的事实标准是 C/S 计算模型，将 C/S 的通信模型简化如图1。图中表示的是两个主体之间的点对点的信息交换模型。

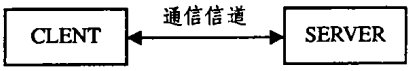

图1 C/S 通信模型

主体：C/S 进程；客体：通信信道上传送的数据。

其中主体是用户进入主机(Host)后启动的 C/S 进程，或者是由系统启动的，是通信的实体，我们将 C/S 进程之间的通信看作是其所在主机之间的通信，它们继承主机的安全级别；通信信道是由 C/S 进程创建的 SOCKET 通信，可以是 TCP/UDP；数据报是由主体生成的，通过通信信道发送，或从信道上接收。

3.2 假设条件

要实施网络多级安全策略，对底层网络的支持，我们有以下一些假设条件：

1）设有底层技术防止网络上传送数据被物理窃听；

2）系统中有一个网络安全员(NSO)是可信的，他负责分配网络主机的安全级别；

3）有相应的网络协议保证网络通信的可靠传送；

4）有相应的加密技术防止信息在网络上传送时被泄露，被修改。

3.3 实现

由于网络的分布式特性，首先要使得各个主机之间有一个一致的网络安全级别，即要相互认识；其次，还要建立实施多级访问控制的基础，即通信双方有一种机制给出各自的安全级别，策略机制以此判定是否允许它们之间的通信，有以下一些方法：

1）在数据链路层实施，通过数据报来传送主机的安全级别，需要修改数据链路层的协议，还要相应的硬件支持，这种方法只适用于局域网；

2）在 IP 层实施，这要求对每个 IP 包都要携带安全级别信息；

3）在传送层实施，需要对 TCP 和 UDP 分别对待。对 TCP 在建立连接时，交换主机的安全级别信息，对 UDP 则每个包均要携带安全级别信息；

4）在传送层之上实施，需要开发一个独立的协议来完成网络多级安全策略。

对于上述几种方法，由于1)、4)会带来协议或应用的不兼容性，是不可取的；2)是可以考虑的，不过每个 IP 包都要携带安全信息；3)的实施要复杂一些，但是效率上要高得多。因此，我们考虑在 TCP/UDP 程实施网络强制访问控制，目的是提供最大的对现有技术的兼容性。如果在 IP 程实施可能是最简单的办法了，但是 IP 层关系到网络的寻径问题，而且如果每个 IP 包都包含一个 MAC 信息，其效率是低下的，因此我们考虑在 TCP/UDP 层实现，几乎可以不影响效率，特别是对 TCP 通信，还会提高网络的效率，避免垃圾数据在网络上传送。

3.3.1 UDP 由于 UDP 是按数据报为单位进行通信

的，因此每个 UDP 数据报应包含安全信息，而进程又不知道对等进程的其他任何信息，因此需要将安全信息封装在 UDP 数据报中。具体做法是将安全信息封装在有效数据的头部，接着是有效数据，如图2所示。

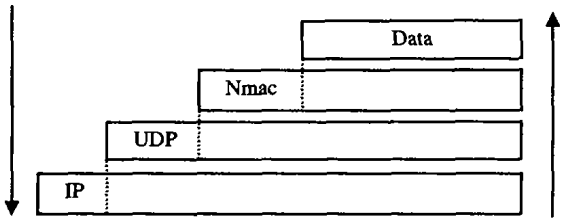

图2 UDP 数据报中安全信息的封装与解封

如图2所示，UDP 在发送数据时在用户数据前面封装上安全信息，再加上 UDP 头信息，交给 IP 层发送。

对等实体收到 UDP 数据报后，取得对方的安全信息，然后与自己的安全信息比较，根据安全策略，以确定是否可以接受此数据报。

3.3.2 TCP 根据 TCP 的通信过程，通信双方在通信之前，要先建立连接。安全信息的交换是在连接建立的三次握手过程中完成的。CLIENT 方首先将自己的安全信息发送给服务器进程(SERVER)，SERVER 在收到联接请求后，取得 CLIENT 的安全信息，在响应时向 CLIENT 发送自己的安全信息，当连接建立后，CLIENT/SERVER 已经完成了安全信息的交换了，建立了强制访问控制的基础，因此，可以实施多级安全策略了。其过程如图3所示。

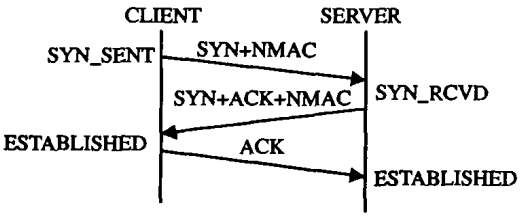

图3 C/S 之间的安全信息交换

4 性能分析

我们在 LINUX 核心 TCP/IP 协议栈实现了网络多级安全策略。下面对 TCP/IP 协议栈进行描述，并对协议性能的影响进行实验测试。

4.1 LINUX 核心 TCP/IP 结构

LINUX TCP/IP 协议栈是核心的一部分，可以分为五层，即：SOCKET 层，INET 层，TCP/UDP 层，IP 层，网络设备层，如图4。

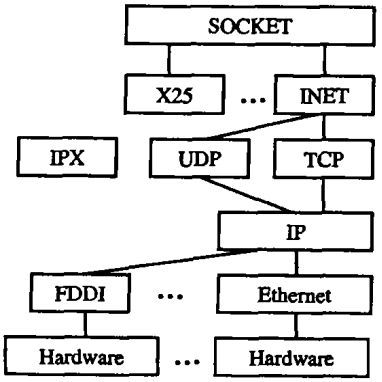

图4 LINUX 核心 TCP/IP 结构

4.2 TCP/IP 排队模型

TCP/IP 是一种存储转发协议，因此，在协议栈上会有队列存在。在协议栈的收发方都存在队列，对于 TCP 协议，发送方有两个队列，分别位于 TCP 层和网络设备层；UDP 层没有队列，因为它没有流控。网络设备的队列是为了缓冲 IP 层高速到达的数据包。接收方也有两个队列，即网络设备接收队列和 TCP(UDP 层等待接收的数据队列。其模型如图5。

4.3 测试方法

根据以上分析，我们采用文[19,20]的测试方法，在 TCP/IP 协议栈中加入探测代码，以记录所需信息。当然，探测代码的加入，会增加 CPU 开销，而我们的目的是分析网络多级安全策略的实现，对 TCP/IP 网络性能的影响，我们在原 TCP/IP 协议栈和修改后的 TCP/IP 协议栈的相应位置，插入相同的探测代码，因此，得出的结果是具有可比性的。我们主要记录数据经过 TCP/IP 协议栈不同位置的时间，以考察对 TCP/IP 各层的时间开销。探测代码的插入点如图5，其中，圆圈代表不同的探测代码位置。

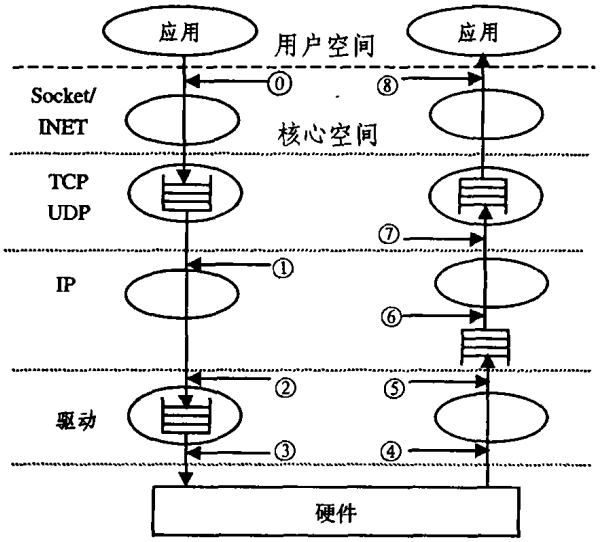

图5 TCP/IP 协议排队模型

4.4 测试环境

我们的测试环境是两台 PC 兼容机，其配置是 INTEL PIII 800MHZ，256MB 内存，20GB 7200转 IDE 硬盘，VIA-RHINE 100MBPS 网卡；以及 INTEL CELERON II 900MHZ，256MB 内存，40GB 7200转 IDE 硬盘，VIA-RHINE 100MBPS 网卡。通过一个10MBPS HUB 连接。核心版本是 2.4.4。

两台计算机都运行在多用户模式，没有启动 XWINDOW 系统，以确保最少的后台服务进程。

4.5 测试结果

我们通过在两台测试机上分别运行 CLIENT/SERVER 程序，测试发送不同的数据包长，记录数据经过协议栈不同位置的时刻，然后计算数据经过协议栈不同部件所需要的时间，下面是在上述环境下的测试结果。

4.5.1 UDP 对 UDP 修改后与修改前的测试对比结果，如图6所示。其中，横坐标表示所发送的字节数，单位是字节；纵坐标表示数据报通过 UDP 层的延时，单位是微秒(US)。

图6的结果表明，网络多级安全策略的实现，对网络的性能几乎没有影响，但是，根据我们的实现方法，特别是对

UDP，我们在用户数据前封装了 NMAC 头，降低了数据传输的效率。

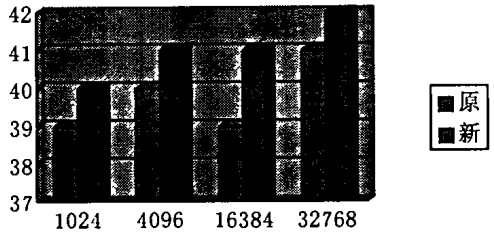

图6 UDP 层开销对比

假设，我们封装的 NMAC 头长度为 Ln，用户的有效数据长度为 Ld，那么引入 NMAC 头后，与未做修改的 UDP 相对传输效率为：$Ld/(Ld+Ln)$，其下降为：

$1-Ld/(Ld+Ln)=Ln/(Ld+Ln)$

由此式可以知道，当 UDP 报文长度与 NMAC 头的长度相差不大时，传输效率急剧降低，这是极端的情况。但是，从网络数据报的统计来看，NMAC 头长度相对于数据报的长度还是很小的，一般不会对 UDP 的传输效率带来较大损害。

4.5.2 TCP 对 TCP 修改后与原来的测试对比结果，如图7所示。

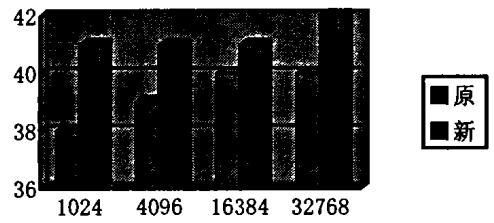

图7 TCP 层开销对比

对于 TCP 通信，在建立 TCP 连接的过程中，NMAC 数据与 SYN/ACK 请求/响应包一起发送，当通信双方建立连接后，就完成了双方 NMAC 信息的交换。测试结果表明，对 TCP 的传输性能几乎没有什么影响。所增加的时间延时是在进行多级安全策略判断时的 CPU 开销。

结语 我们感兴趣的是控制网络中主机保存的敏感信息传送，特别是合法用户之间的数据共享。许多协议需要发送双向确认信息，我们的方法不影响协议确认信息的传送，现成网络应用可以不加修改地运行，因而，极大地保证了网络应用的兼容性。能够灵活控制网络主机之间的信息按多级安全策略传送，保证信息的机密性，可以有效防止合法用户任意泄漏信息，支持复杂的信任关系，提高了网络的安全性。

参考文献

1 Bell D E, Laphadula L J. Secure computer systems: Mathematical foundations. Hanscom. AFB. Bedford. MA. Rep. ESD-TR-73-278, vol. 3, ESD/AFSC. 1973

2 Bell D E. Secure computer systems: A refinement of the mathematical model. Hanscom AFB. Bedford. MA. Rep. ESD-TR-73-278, vol. 3, ESD/AFSC, 1973

3 Bell D E, Lapadula L J. Secure computer systems: Unified exposition and Multic interpretation. Mitre Corp., Bedford. MA. Rep. Mtr-2997, 1975

4 Sidhn D P, Gasser M. A multilevel secure local area network. In: proc. of the 1982 symposium on security & privacy

5 Esterin D. Non-discretionary controls for Inter-organization Networks. In: proc. of the 1985 symposium on security & privacy

6 Mchugh J, Moore A P. A Security Policy and Formal Top Level Spicification for a Multi-level Secure Local Area Network. In: proc. of the 1986 symposium on security & privacy

7 Walker S T. Network security overview. In: proc. of the 1985 symposium on security & privacy

8 Anderson D P, Rangan P V. A basic for secure communication in large distributed systems. In: proc. of the 1987 symposium on security & privacy

9 Macewen G H, et al. Multi-level security based on physical distribution. In: Proc. of the 1984 symposium on security & privacy

10 Rushy J M, Randell B. A distributed secure system. In: Proc. of the 1983 symposium on security & privacy

11 Anderson J P. A unification of computer and network security concepts. In: proc. of the 1985 symposium on security & privacy

12 Chitturi A. Implementating Mandatory Network Security In a Policy-Flexible System: [Master Thesis]. Department of Computer Science, The University of Utah. June 1998

13 Smally S D. A network access control model for Flask: [Technical Report]. U. S. Department of Defense, July 1997

14 Atkinson R. Security architecture for the Internet Protocol. RFC 1825, Internet Engineering Task Force, Aug. 1995

15 Atkinson R. IP authentication header. RFC 1826, Internet Engineering Task Force, Aug. 1995

16 Atkinson R. IP encapsulating security payload(ESP). RFC 1827, Internet Engineering Task Force, Aug. 1995

17 Dierks T. The TLS Protocol Version 1.0. RFC 2246, Internet Engineering Task Force, Jan. 1999

18 Robinson P. Understanding Digital Certifications and Secure Sockets Layer(SSL). Securing Digital Idantifies & Information Jan. 2001

19 Papadopoulos C, Parulkar G M. Experimental evaluation of SUNOS IPC and TCP/IP protocol implementation. IEEE/ACM Trans. on Networking, 1993, 1(2)

20 Guo Chuanciong, Zheng Shaoren. Analysis and Evaluation of the TCP/IP Protocol Stack of LINUX. In: Proc. 16th Ifip world computer congress Beijing, China 2000

（上接第62页）

4 Hallapuro A, Karczewicz M, Malvar H. Low complexity transform and quantization. JVT of ISO/IEC MPEG and ITU-T VCEG, Docs. JVT-B038 and JVT-B039, Jan. 2002

5 Rao K R, Yip P. Discrete Cosine Transform: Algorithms, Advantages, Applications. Boston: Academic Press, 1990

6 Taubman D S, Marceline M W. JPEG2000 Image Compression. Boston: Kluwer, 2002

7 Malvar H, Hallapuro A. Low-complexity Transform and quantization with 16-BIT arithmetic for H. 26L. www. vcodex. com

8 Hallapuro A, Karczewicz M. Low complexity (I) DCT. ITU-T SG16 Doc. VCEG-N43, Sept. 2001

9 Cham W. Development of integer cosine transforms by the principle of dyadic symmetry. In: IEE Proc. Part 1, vol. 136, Aug. 1989. 276～282

10 Richardson E G. Transform and quantization. H. 264 / MPEG-4 Part 10 White Paper 19/03/03 Page 1 of 9

11 Malvar H S. Signal Processing with Lapped Transforms. Boston: Artech House, 1992

12 Kerofsky L, Lei S. Reduced bit-depth quantization. ITU-T SG16 Doc. VCEG-N20, Sept. 2001

13 Malvar H S. Low-Complexity length-4 transform and quantization with 16-Bit arithmetic. ITU-T SG16 Doc. VCEG-N44, Sept. 2001

14 Bjontegaard G. Calculation of average PSNR differences between RD curves. ITU-T SG 16 Doc. VCEG-M33, Mar. 2001