文章编号: 1001- 9081(2003) 08- 0001- 03

一种新的主动节点资源安全管理机制

黎忠文[1,2], 李乐民[1]
(1. 电子科技大学 通信学院, 四川 成都 610054; 2. 厦门大学 计算机与信息工程学院, 福建 厦门 361005)

摘 要: 较传统网络而言, 主动网络的高复杂性引起了更加严峻的资源安全问题, 特别在主动节点方面。尽管在主动网络原型系统中设计了一些安全措施, 但是它们都不具通用性。这在主动网络必须和传统网络相兼容的情况下, 阻碍了主动网络的发展。文中设计了主动节点资源控制核, 然后深入地研究了它与传统网络安全系统的接合问题, 提出了对后者的具体修改建议。

关键词: 主动网络; 安全; 资源控制核; 资源使用策略
中图分类号: TN915.01 文献标识码: A

A New Security & Safety Management Mechanism of Active Node Resources

LI Zhong-wen[1,2], LI Le-min[1]
(1. *Communication College, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*; 2. *School of Computer and Information Engineering, Xiamen University, Xiamen Fujian* 361005)

Abstract: Active Networks are obviously more complex than traditional networks and raise considerable security & safety (in short, we call them S&S later) problems, especially in active node. Although some S&S technologies are designed in most active networks, all of them cannot be used as a universal way. On condition that active networks must be compatible with traditional IP networks, this situation results in baffling active networks' development. Based on some concepts defined in this paper, such as negative error and positive error, this paper designs a resource controlling kernel for active node. In addition, this paper comprehensively studies the problem of tying this kernel in traditional network security system, and then, puts forth some suggestions of modifying traditional network security system in two aspects of security agent lay and security service lay in detail.

Key words: Active networks; security & safety; resource controlling kernel; resource usage policy

1 引言

主动网络[1,2]是一种新型的网络结构, 它具有高灵活性和高处理能力。其路由器可以通过执行包所携带的可执行代码(又叫主动代码) 定制处理用户数据, 还能改变自身的状态。

与传统网络相比, 主动网络更加复杂, 路由器处理用户包需要更多资源的参与和配合。令 $S_T = \{S_{T1}, S_{T2}, \cdots\}$, $S_A = \{S_{A1}, S_{A2}, \cdots\}$ 分别代表传统和主动网络每一跳所能提供服务的集合, 其中 S_{Ti}, S_{Ai}, $i = 1, 2, \cdots$ 是服务的类型。由于传统网络主要是被动传送数据, 网络用于终端系统之间数据的转发, 并不对数据内容进行调整和改动, 因此传统网络每一跳的通信服务集可简化为 $S_T = \{S_{T1}, S_{T2}, S_{T4}\}$, 其中:

S_{T1}: 用于包交换或调度的服务; S_{T2}: 用于包在网络节点上排队的服务; S_{T3}: 用于包在链路上传输的服务。

显然主动网络提供的服务丰富得多, 其每一跳的服务集 $S_A = \{S_{A1}, S_{A2}, S_{A3}, S_{A4}\}$,

其中: S_{A1} 至 S_{A3} 分别与 S_{T1} 至 S_{T3} 类似; S_{A4} 为主动节点执行可执行代码段对包数据或节点本身进行相应处理的服务类。

由此可见, 主动网络有着比传统网络更加复杂和突出的资源保护问题。

2 资源管理存在的问题

现有主动网络原型系统所采用的安全技术大致分为授权、鉴别、资源受限使用和编程语言四种。具体而言, 可应用于保护主动节点资源安全的技术有[3,4,5,6,7,12]:

对主动包认证: 即进入网络的主动包都携带认证证书, 以确保有人对主动包负责。

限制技术: 限制主动包可使用的节点的数量及节点资源量, 以阻止主动包独占节点资源。限制技术又分为时间限制(如允许执行主动信包的时间长短), 范围限制(如允许信包经过的节点总数) 和拷贝限制(如信包拷贝自己的次数)。

证明码: 主动包携带"证明码", 即把对可执行代码安全验证的规格说明和代码本身捆绑起来, 移动到目的执行环境, 由主动节点执行该码来确定该主动包的合法性。

编程语言: 主动代码的编程采用类型安全和具有垃圾收集机制的语言, 如 Java, PLAN 等, 以减少程序 bug 对主动节点造成的破坏。

这些安全技术虽然对节点资源的保护起到了较好的作用, 但是它们依赖于网络的具体基础设施, 没有通用性。这在

收稿日期: 2003- 03- 12; 修订日期: 2003- 05- 12 基金项目:"十五"国防基金项目(41001010106)
作者简介: 黎忠文(1970-), 女, 重庆人, 博士后, 主要研究方向: 大型系统的高可靠、高防危技术和主动网技术; 李乐民(1932-), 浙江吴兴人, 中国工程院院士, 博士后导师, 主要研究方向: 数字信息传输与宽带通信网.

目前主动网络必须与传统 IP 网络兼容[7]的情况下, 阻碍了主动网络的发展。

3 主动节点资源控制核的设计

3.1 资源控制核的原理

定义 1 消极型错误。当系统做了不希望让其做的事时, 称系统发生了消极型错误。如节点资源被非法占用。

定义 2 积极型错误。希望系统做的事情, 系统没有完成时, 称系统发生了积极型错误。如安装了防木马进攻的系统, 却没能挡住木马的进攻。

我们设计的资源控制核用于处理消极型错误[3], 其原理见图 1 所示:

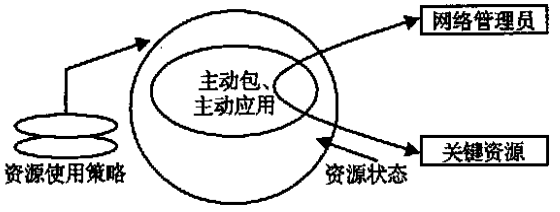

图 1 资源控制核的原理

每个主动节点上都设一个资源使用控制核, 它根据资源使用策略(如每个包可用的资源的最大限制等) 对节点的关键资源进行保护。凡是对关键资源的使用都必须遵循资源使用策略, 不合法者节点将采取相应出错处理, 维护节点的安全。这里的关键资源指主要的底层资源: CPU 占用时间、存贮器和带宽三种[8]。

资源控制核适于处理消极型错误: 无论核外其它系统组件如何工作, 它都通过维持资源使用策略的不变性来保证主动节点上不希望发生的事情发生。比如对于否定服务这种安全威胁而言, 造成资源非法占用的错误很多, 但资源控制核不会根据这些错误一一的设计安全措施, 而是只根据资源使用策略, 对于合理的请求给予资源分配, 不合理的就拒绝。因此只要资源使用策略设计得合理, 就不会造成否定服务的出现。

3.2 保证资源控制核有效实施的条件[9]

要保证资源控制核的有效性, 必须遵循下列的规则:

1) 资源控制核应短小精练

资源控制核尽可能小, 才易于正确性的检验。为此主动节点所有的资源使用策略均由资源控制核来实施是不现实的, 适于在资源控制核中实施的资源使用策略可归纳为下面两条:

• 这些资源使用策略中所包含的变量必须在资源使用控制核的控制之下, 否则对资源控制核来说这些资源使用策略本身就是可变的, 资源控制核就根本无法去维护它们。

• 无论主动节点其它组件(特别是主动应用) 如何访问被保护对象(即关键资源) , 资源控制核都要能保持资源使用策略的正确实施。

2) 完备性

完备性要求不通过资源控制核, 任何对被保护对象的访问都必须被禁止, 即采用了资源控制核的主动节点必须要保证该核对被保护对象的专一控制。

3.3 资源使用策略

资源使用策略至少要包括下面四种:

1) 被保护对象的控制策略

当可执行代码向主动节点的资源发出请求指令时, 该策略用以判断这个指令的执行是否使被保护对象保持在安全状态, 安全则允许执行操作, 否则出错处理。

2) 可执行代码的状态策略

与硬件相似, 在一个特殊的软件行为发生前, 必须要检测这种行为发生的合理性, 即严格控制软件的执行路径, 避免错误指令的产生。对于每一可执行代码段的行为都要为之设计可接受的命令序列及参数, 以备检测时使用。

3) 设备错误诊断策略

这类策略主要是检测主动节点设备的动作是否与指令动作一致。

4) 错误响应策略

错误出现后, 采取的补救措施。

3.4 资源控制核的实现问题

资源控制核的实现与节点操作系统密切相关, 可分为下列几种:

1) 库的方式: 生成. o 文件, 在编译时联入。

2) 扩展系统调用: 修改系统函数 API: 修改系统函数的 API, 在原 API 上加入类似于转向资源控制核功能。

3) 内核模块法: 这种方法用于类 Linux。把资源控制核做成一个核心模块加入到实时 Linux 的内核中去。

同时要对其支持环境进行修改:

出错处理 需要进一步增强操作系统的出错处理功能。传统的任务级出错处理方法(即操作系统返回错误代码, 然后由应用程序根据这个错误代码及当前操作的功能代码进行相应的出错处理) 在主动节点中不适合, 因为它存在错误被遗漏及非安全状态没有及时处理的危险。可以增加系统强制处理错误的手段, 比如一旦操作系统调用错误处理程序也无法处理错误时, 就进入系统级的错误处理, 即系统按有利于保障安全的方式采取措施, 比如关机或重新启动。

存贮器管理 存贮器的管理在主动节点中也是非常重要的。因为进程间通讯存在一定的安全隐患。在对存贮区进行管理时要加入 security 考虑, 制定一系列的管理措施。比如把存贮器分为几个不同级别的 security 区, 入驻存贮区的进程必须具有与存贮区相同的 security 级别。同一进程派生的子进程分配到 security 区的某一 security 段中。处于同一 security 段的进程可以读写对方的存贮区; 属于相同的 security 区, 但不是相同的 security 段的进程, 只有读的权力, 不能写, 因此它们之间进行通信时可以用指针的方式; 而不同 security 区的进程通信时, 只能通过可信中介进行拷贝。具体的存贮器管理措施与主动应用的应用特点有关。

处理器的调度方法 进行处理机调度时要充分的考虑进程的多样性, 应该设计新的调度策略, 比如在进行处理器调度前把进程的优先级和进程的资源使用情况按一定的比例进行折算等。

4 资源控制核与传统网络安全体系的结合

节点资源控制核与传统网络安全体系[10, 11]的最终结合, 并成为它的组成部份, 才能保证主动网络与传统网络的兼容性。要达到这个目标, 必须对传统网络的安全体系进行适当的修改, 本文集中于安全代理和安全服务两层。

4.1 对安全代理层的修改

设置下述几类安全代理:

主动包代理: 记录主动包的安全需求; 记录用户注入的“小程序”, 根据严格的规则来判断其合法性; 根据标准的安全信息, 审查报文安全需求的合理性, 并做出适当的响应。主动

包的主人除了用户外, 也可以是系统管理员, 他通过主动包更改主动节点的设置或更新软件系统。

主动应用代理: 记录进入的主动应用, 根据严格的规则来判断其合法性。

安全管理代理: 与监视代理和恢复代理协同工作; 与安全管理数据库代理协同工作, 完成对安全管理数据库的访问。

资源使用代理: 该代理是主动节点的中心控制和操作代理, 主要负责提供资源的合理分配和使用服务。

安全管理数据库代理: 凡是要访问安全管理数据库的代理均需通过安全管理数据库代理。

监视代理: 监视代理接收安全管理代理所收集的数据并通过安全管理数据库代理把它们记录在安全管理数据库中。

恢复代理: 恢复代理负责探测系统的安全性是否被破坏, 并在系统进入不安全状态时将系统恢复到安全状态。

环境代理: 对主动包、主动应用和管理信息进行初步的安全审查, 合格者交给相应的代理, 不合格者禁止访问本节点; 负责节点间网络安全, 确保数据的保密性和完整性。

EE 代理: 它根据收到的 EE 代码, 负责在主动节点上加载 EE。在主动网络中存在这样一种情况, 当某主动包/ 应用所需的 EE 不在主动节点上时, 需要向 EE 中心请求 EE 代码, 从而把 EE 加载在该节点上。

数据包代理: 它用来处理传统网络中的数据包。

各安全代理之间相互配合, 共同保障系统的安全。安全代理之间的相互关系见图 2 所示。

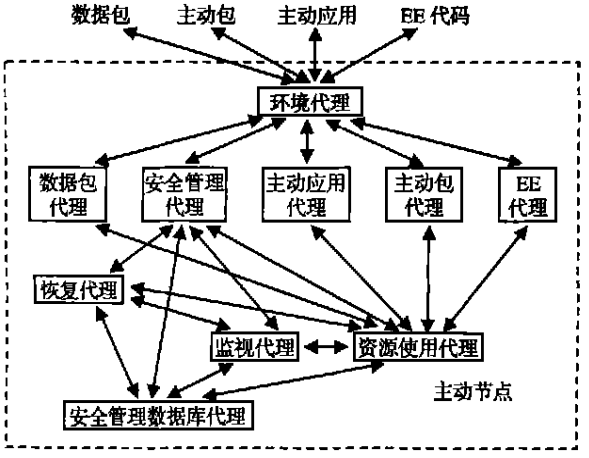

图 2　安全代理之间的关系

注意:

1) 环境代理要进行初步的安全(主要是 security) 审查, 凡是没有通过审查的应用、用户和其它数据不能进入主动节点内;

2) 环境代理把经过安全审查的应用、用户和其它数据分别交给相应的代理。

4.2　对安全服务的修改

安全服务是安全系统的功能, 这些功能针对系统中潜在的不安全因素提供有效防范措施。主动节点的安全服务分为三类:

1) 资源使用服务

资源使用服务分为四类, 分别用于维护资源使用策略、软件的状态策略、错误诊断策略和错误响应策略。

2) 数据库 security 服务

数据库 security 服务引用开放系统环境中的数据库 security 服务, 即除了 OSI 的访问控制、数据保密和数据完整 security 服务外, 还提供保持数据流安全一致性和防止推知数据两项 security 服务。

3) 管理安全服务

• 安全审核服务: 安全审核服务实现探测和调查与安全性有关的事件, 即记录、分析和报告与安全性有关的信息。

• 安全恢复服务: 在安全性破坏发生后, 安全恢复服务采取一定的措施将系统恢复到安全状态。

5　总结

主动网络资源管理主要涉及主动节点的自我保护, 防止对资源的非法占用等问题。基于现有主动网络安全技术不具通用性, 有碍主动网络的发展, 本文提出了主动节点资源控制核的观点。并从原理、安全策略和实现等方面对它进行了详细地设计。为了达到主动网络与传统网络相兼容的目标, 本文进一步研究了资源控制核与传统网络安全体系的嵌入问题。传统网络安全体系一般分为五层, 本文对其中较为重要的安全代理和安全服务两层进行了深入地研究, 提出了具体的修改建议。对另一较重要的基础层的修改, 将是我们下一步的任务。

参考文献

[1] DARPA. DARPA active network homepage[EB/OL]. http://www.darpa.mil/to/research/anets/index.html.

[2] Tennenhouse DL. A Survey of Active Networks Research [J]. IEEE Communications Magazine, 1997, 35(1): 80-86, 1997.

[3] Li Zhong-wen, Yu Shui, Li Le-min. A New Safety Mechanism of Active networks [A]. ICII2001 (International Conferences on Info-tech & Info-net), Proceedings of IEEE Network' 2001[C]. Bei Jing. China, 2001. 779-785.

[4] David J W. ANTS: A Toolkit for Building and Dynamically Deploying Network Protocols [A]. Proceedings of IEEE OPENARCH' 98[C]. San Francisco. USA, April 1998.

[5] Galtier V, Mills KL, Carlinet Y, *et al*. Expressing meaningful processing requirements among heterogeneous nodes in an active network [A]. Proceedings of the second international workshop on software and performance[C], 2000. 20-28.

[6] Moore J T, Hicks M, Nettles S. Practical programmable packets [A]. IEEE InfoCom 2001[C], 2001.

[7] Active Networks Working Group. Architectural framework for active networks (version 1.0) [DB/OL]. http://www.cc.gatech.edu/projects/acnes/arch/arch-1-0.ps, 2000-02-5.

[8] Yamamoto L, Leduc G. An agent-inspired active network resource trading model applied to congestion control [A]. MATA 2000[C], 2000. 151-169.

[9] 黎忠文. 分布式控制系统中新安全机制的研究——安全核[D]. 成都: 电子科技大学, 2001.

[10] 秦志光. 开放系统中全局安全性的研究[D]. 成都: 电子科技大学, 1996.

[11] Muftic S. Extended OSI Security Architecture — Second Stage of the CEC COST-11 Project [J]. Computer Networks and ISDN Systems, 1989, 17(1): 223-227.

[12] Konstantinos P. Active Networks: Applications, Security, Safety, and Architectures [DB/OL]. http://www.Comsoc.Org/pubs/surveys, 2001.