主动网络安全原型的设计

寇雅楠[1,2], 李增智[1], 廖志刚[1], 宋 涛[1], 周恒琳[1]
(1. 西安交通大学电子与信息工程学院, 陕西西安 710049; 2. 空军工程大学工程学院, 陕西西安 710038)

摘 要: 提出利用可插入模块方式设计主动网络动态可扩展的安全原型, 实现了加密与数字签名、授权、验证和代码撤消等方面的安全. 加密与数字签名解决了主动代码的完整性和机密性问题; 使用解码绑定方式, 实现了可扩展的系统加密方法. 系统采用基于证书的验证方式, 专门设计证书中心, 负责颁发 X.509 格式的证书, 使用目录服务器(LDAP)对证书进行管理. 用主动权来描述任何可以表示的授权策略, 系统既可以使用默认的某种策略, 也可以根据用户需要更换策略. 代码撤消部分的设计保证主动代码执行的有效性, 同时根据数据库对代码的跟踪记录, 进行安全预警.

关键词: 解码绑定; 主动代码; 访问权限控制; 可插入模块; 主动权能
中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2003) 11-1701-04

Study of Scalable Security for Active Network

KOU Ya-nan[1,2], LI Zeng-zhi[1], LIAO Zhi-gang[1], SONG Tao[1], ZHOU Heng-lin[1]
(1. School of Electronics and Information Engineering, Xi. an Jiaotong University, Xi. an, Shaanxi 710049, China;
2. School of Engineer, Air Force Engineer University, Xi. an, Shaanxi 710038, China)

Abstract: By the aid of pluggable module, a security prototype is designed in the active network, which facilitates the security in the aspects of encryption, digital signature, authorization, authentication and revocation. The encryption and digital signature ensure the integrity and confidentiality to the active code. The decode-binding realizes the expansion capacity of the encryption methods in the system. By means of the certificate-checking method, the whole system designs a certificate center that issues X.509 certificate and manages the certificate through light directory access protocol (LDAP). With the active capability adapted to describe any authorization policy, the system can either choose the permitted policy or change the policy according to the requirements of the users. The revocation designed for the active network ensures the validity in the operation of the active code. In the meantime, with the trace records in the database, the revocation can realize the security alarm in the whole system.

Key words: decoding binding; active code; access privilege control; pluggable module; active capability

1 引言

主动网络[1,2]作为一种新型的中间节点可编程的网络体系结构, 为网络协议和新服务的开发、验证和部署提供了很好的支持. 同时也为网络管理、服务质量控制(QoS)、可靠组播等提供了一条新的途径, 主动网络已经成为人们注意的焦点.

但是, 主动网络到目前还没有得到广泛地实施和应用, 其主要原因除需要对传统的中间节点进行改造而遇到阻力和困难之外, 其本身的安全性还没有得到较好的解决. 由于主动网络允许用户对网络的中间节点编程, 到达主动节点的主动代码在执行的过程中需要访问节点的资源, 使得主动网络的安全性面临更大的威胁. 十分清楚, 如果安全性得不到较好的解决, 该网络就不存在真正的实用价值. 主动网组已经提出了一个主动网络安全规范[7], 但该规范只提出了一个安全框架, 而许多具体细节和实现在该规范中并没有体现.

在国外, 如麻省理工学院、宾夕法尼亚大学、BBN 公司等的主动网络系统中虽然考虑了一些安全方面的问题, 但他们或者由于侧重点不同(如麻省理工学院的 ANTS[3], 侧重协议和主动服务的快速开发, BBN 的 SmartPacket[4] 侧重于网管) 而对安全性考虑得不周全, 或者虽然考虑了, 但采用了特殊的技术(如宾夕法尼亚大学的 Switchware[5] 使用硬件) 而不具通用性. 在国内, 目前对主动网络的研究还处于起步阶段, 而在主动网络安全方面的研究还几乎处于空白.

经过几年的研究, 我们已经取得了一些研究成果, 并开发了主动网络系统原型[8]. 本文旨在原型系统的基础上进行安全扩展, 主要是动态可扩展安全结构, 它采用可插入模块框架设计, 使得安全系统可以灵活配置.

收稿日期: 2002-04-05; 修回日期: 2003-03-24
基金项目: 国家自然科学基金项目(No. 60173059)

2 安全结构

主动网络安全原型的体系结构采用可插入模块(Pluggable Module)框架模式,其安全性是针对不可信任网络设计的,这样可以提高可信任网络的执行效率.网络的可信任性由用户定制.在可信任网络中,使用一般主动信包(Capsule);在不可信任网络中,使用安全主动信包(Secure Capsule).网络中的信包执行情况如图1所示.其中节点1、节点2和节点3均为主动节点.

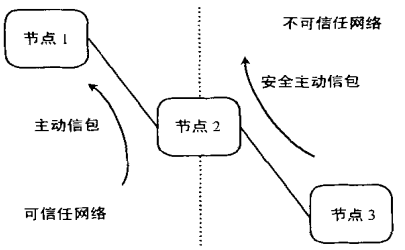

图1 信包执行示意

211 安全信包的设计

我们将安全控制在信包级,每个信包在执行前要经过安全检查.安全信包的设计是在主动网络封装协议ANEP[2]基础上增加了安全关联信息,其格式如图2所示.

版本号	安全模式	类型标识 ID
ANEP 头长度		ANEP 包长度
认证长度		数字签名长度
认 证	数字签名	
选 项		
有效负载		
解码绑定		

图2 安全信包格式

在安全信包格式中,ANEP原有内容:版本号、安全模式、类型标识ID、信包头的长度、信包的长度、选项和有效负载;安全信包加入的内容有:认证长度、认证、数字签名长度、数字签名和解码绑定.

212 安全结构

我们将每个主动节点设计成两个转换通道,一个通道传输一般主动信包,另一个通道传输安全信包.安全信包不能通过非安全通道传输,反之亦然.安全结构如图3所示.

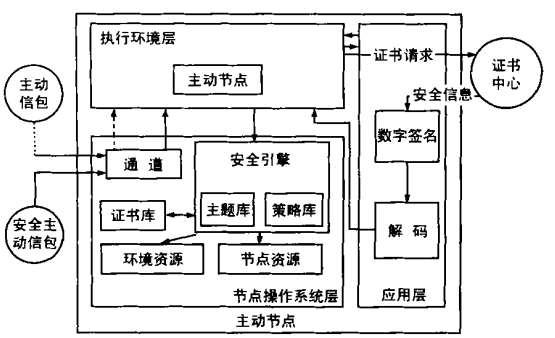

图3 主动网络安全结构

主动网络安全结构主要包括如下内容:

(1)节点操作系统层、执行环境层和应用层.这是主动网络的三层体系结构,最底层为节点操作系统层(NodeOS);中间层为执行环境层(Executing Environments);最上层为应用层(Active Applications);

(2)安全信包.它是为主动网专门设计的信包;

(3)主题(Subject).它表示有多个主体(principal)标识、一组公用证书(publicCredentials)和一组专用证书(privateCredentials).

原有的主动网原型是在Java环境下运行的,我们旨在该基础上进行安全扩展,以提高系统的安全性.Java扩展的安全包主要包括:加密/数字签名Java.Cryptix.*(DSA, RSA, DES);认证/授权JAAS(Java Authentication Authorization Service);生成证书(JCSI).

3 认证

为了防止主动网络环境遭到破坏,要对网络访问者进行认证和授权服务.认证是检查身份,授权是允许某个身份可以访问资源.本系统采用基于证书的认证方式.设计认证中心颁发X1509证书,利用目录服务器LDAP对证书进行管理.

JAAS认证围绕主题进行[10],认证决策根据认证主题制定.认证的具体步骤是:从LoginContext类开始运行,采用两阶段提交认证.JAAS用LoginContext和Configuration来创建LoginModule,再用CallbackHandlers和Callbacks来认证一个主题,如果都成功,JAAS就在当前的文件中增加一个主题,并允许检查这个合法的主题.

4 授权

411 访问控制策略

访问控制表示提供限制主体对重要资源访问的机制.主体标识可能与安全属性相关联,如分类级别、权力、权限角色,以便更好的制定访问控制决策.访问控制种类很多,包括强制的访问控制[6](MAC, Mandatory Access Control),自由的访问控制(DAC, Discretionary Access Control),基于角色的访问控制(RBAC, Role Based Access Control)等.

访问控制的最简单形式是自由访问控制DAC,它是基于主体访问的访问控制.这种访问控制方式通常在访问控制列表(ACL, Access Control List)中保存主体及相应权限清单.ACL可以存放在文件中或数据库中,帮助简化访问控制的管理工作.

强制的访问控制MAC基于主体所属的访问密级.密级指定主体相关的信任级(例如绝密、机密、秘密).密级指定主体隐含的信任级.如果主体密级高于或等于资源密级,则用户可以访问这个资源.

RBAC是最灵活的访问控制类型,其定义如下:

定义1 一个角色是一个2元组P=(u, p),其中u为用户名,p为用户口令.系统中所有的角色组成角色集合A={P_i| 0< i< n, n为角色数}.

定义2 假设系统的资源集合为S, R={R_i| i[n, i, nIN}为S的一个划分, R_i H R_j= U, i X j,其中R_i A S,则称R_i为S的等级资源,i为R_i的资源等级数.

定义3 P aI A,存在k, 0< k< i,使得角色a对资源集

$\sum_{j=1}^{k} GR_j$ 具有权限, 称为角色访问控制权限.

所有的 RBAC 客体都有其功能, 每个功能代表了一个特殊的主体以及在此基础上所允许的操作. RBAC 的主要好处是可以节省大量的空间, 而且管理起来比较容易. RBAC 允许用户自己生成比 DAC 和 MAC 更加复杂的策略. 一个用户可以有不同的角色, 以及在此基础上所特有的权力. 与角色和特权相关联的限制可以在 RBAC 中得到改善.

传统系统提供的是单一的静态访问控制, 如系统的安全策略不能自动的从 DAC 策略转换到 MAC 的策略, 而且带有不同访问控制的应用不能在一起共存. 如果没有得到访问控制的安全保证, 应用则不能在不同的系统中传送. 在我们设计的安全系统中, 安全策略可以根据用户需要动态调整, 实现动态扩展.

为了适用于用户的特殊安全策略, 提供一个面向对象的策略表示框架, 其类层次如图 4 所示.

框架底层的类是最抽象的, 用于表示数学概念. 这些对象形成更为专业的类描述层次的基础, 如标签和访问控制列表. 顶层的类用于表示各种普通的策略形式, 包括 MAC、DAC、RBAC 等.

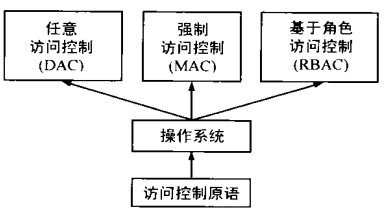

图 4　策略层次

4.2　可插入部件设计

对每个主动节点设计了可插入安全部件, 如图 5 所示.

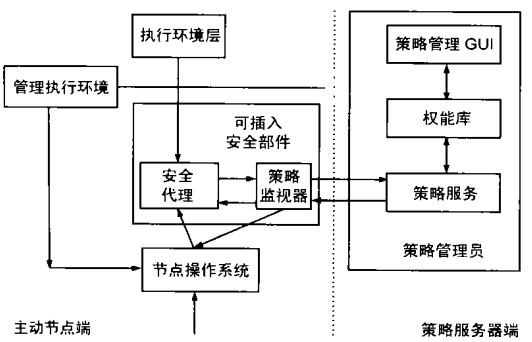

图 5　可插入安全部件

这个部分的主要功能是为了满足与 NodeOS 的扩展连接的需要, 它包括一个策略监听组件和安全代理. 通过可插入安全部件, 可以访问各个节点的资源信息. 策略框架则是监听组件的一部分. 这个策略是重定位的, 当外部有需求时, 可以从它的上面动态地下载策略. 应用或者管理员可以根据策略所提供的接口来生成用户化的代码, 这些代码是对访问控制协议和其他在访问控制决策进程中的策略进行编码, 且以主动权能的形式出现.

传统意义上的权能仅仅是指对规则, 以及与规则有关的命令进行编码的那些授权认证. 然而, 主动网的权能实际上则是一个 Java 的代码执行. 另外, 一个被数字签名保护的主动能力取决于用户的空间大小, 并且可以随意的传送. 在概念上, 主动权能主要是对在访问控制中所执行的策略进行编码的工作.

通过利用一个主动权能, 我们可以对由系统属性决定的各种策略进行编码. 例如, 通过编写一个检测目前时间并与一个固定的值进行比较的代码, 可以在一个时间期限后产生一个过期的策略. 相似的, 也可以实现基于其他属性, 例如限额的历史和信息等内容来生成加强的和改进的模型框架. 根据各种不同的应用需求, 这些框架模型在开放型的网络中是非常有用的. 一个应用可以用限额的基础来限制系统资源的访问控制, 这对进行拒绝服务攻击是非常有用的.

目前的策略框架支持下列公共类型的访问控制策略: MAC、DAC 和 RBAC. 更多的特定访问控制策略系统的应用能很容易地从这个面向对象的框架中得到扩展. 在我们的模型中, 不仅能指定3主体, 客体, 操作4 访问控制关系, 也包含使用上的资源限制, 如基于当前时间或当前角色的主题.

系统部署策略有以下三种方法:

(1)应用创建特定权能, 或从策略服务器获得权能, 然后沿主动信包发送. 权能可以嵌入主动信包, 或者它就是主动信包本身. 当主动信包到达远程节点, 多路输出到主动网 EE 层, 维护有关信包的状态, 而权能随同对节点操作系统资源的请求一起发往安全代理;

(2)如果应用信包没有权能, 通过 EE 在接收资源请求之上, 策略监视器直接接触主域策略服务器, 请求应用信包主体的权能;

(3)对于公共应用或经常性的用户, 在系统初始化时, 策略服务可以给策略监视器发放权能.

为了改善权能计算效率, 策略监视器使用高速缓存存储权能或权能计算结果. 依靠内容更新和权能的类型, 一个请求可以在快速缓存中查找得到满足, 而不需要重新进行权能计算. 另一方面, 对于权能的一些类型, 策略监视器能从策略服务器下载最新的权能.

另外, 可信任授权中心在任何时间都具有取消权能的能力. 可信任授权中心可以发送清除缓存信息去释放策略监视器, 并且在运行时安装新的权能. 一个应用能提供运行期间更新的权能来代替现有的权能.

5　解码绑定

目前广泛使用的加密/解密方法和数字签名/验证方法[6], 都涉及密钥(公钥, 私钥)管理. 在本系统中所使用方法是: 在对原节点加密的同时, 将解密方法与信息一同打包发出, 到达目的节点后解密执行, 而目的节点无需进行密钥管理. 这种解码绑定方式主要用于加密和数字签名, 其优点在于: 加密方式具有灵活性和可扩展性. 由于每次传输的信包随机使用加密方法, 甚至有时可以采用简单方法进行加密, 即使信包被截获, 也无法破获其他信包. 这种加密可以随时更新.

数字签名/验证方法在实际签名中有下列特性: ¹ 不可伪装性. 由于签名者使用私有密钥, 而私有密钥只有保密者自己才能使用; º 可验证性. 由于公开密钥是公开的, 任何能访问

消息和签名的人都可以验证消息; » 单一用途. 签名对特定消息是惟一的, 不可能将一个签名用于多个消息; ¼ 非否认性. 签名与信息一起发送, 签名者无法否认这个事实; ½ 密封性. 签名消息就是用数字密封, 无法改变.

系统实现双方双重非否认. 双方非否认就是发送方和接受方不能否认发送和接受消息, 双重非否认就是在数字签名和授权时两次验证.

6 代码撤消

主动网络安全要解决的另一个主要问题是代码撤销. 当发现了一个终止主动代码的原因, 这个主动代码已分布于系统, 则无论在那里发现, 一定要终止它.

参考移动代理系统的代码定位方式[9], 并使用全局数据库方式实现代码撤销, 其具体方法是: 在主动网络上分布式建立转发信包登记表, 记录每个转发信包的 ID 和下一个转发节点的地址. 当发送者请求代码撤消时, 采用递归方法确定代码位置, 执行代码撤消命令撤消代码. 代码定位方式如图 6 所示.

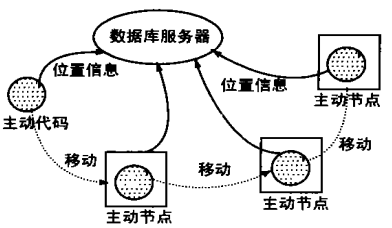

图 6 数据库定位方式

7 总结

我们在主动网原型上插入了安全扩展. 机器安装了 Jbuilder4l 0、Cryptix 包、JAAS 等, 并测试了网络延迟和网络吞吐率. 加入安全后, 对主动网的网络延迟和网络吞吐量略有影响. 安全性越完善, 对网络性能的影响就越大. 我们的系统最终将是无级安全的, 可以根据需要, 配置安全. 主动网络技术是为弥补现有网络技术的不足而开发的一种新型网络结构, 解决它的安全性问题, 使之得以广泛使用的关键. 相信克服安全困扰的主动网络将有着广阔的应用发展前景.

参考文献:

[1] Active Network Working Group. Architecture framework for active networks version 1[R]. USA: Active Network Working Group, 1999.

[2] Scott D A, Bob B, Carl A G, et al. ANEP: Active network encapsulation Protocol[R]. http://www.cis.edu/Switcg23 http://www.cis.upenn.edu/Switcg24 Ware/ANEP/P/docs/ANEP.txt. 1997207/2000203209.

[3] Wedtherall D, Guttag J, Tennenhouse D. ANTS. A toolkit for building and dynamically network protocols[A]. IEEE OPENARCH. 98[C]. San Francisco, CA, 1998.

[4] Alexander D S, Arbaugh W A. A secure active network environment architecture: Realization in SwitchWare[J]. IEEE Net, 1998, 12(3): 37 - 45.

[5] D Scott Alexander, William, Arbaugh, Michael, et al. The switchware active network architecture[J]. IEEE Network, 1998, 3: 29- 36.

[6] Roy H Campbell, Zhaoyu Liu, et al. Seraphim: Dynamic interoperale security architecture for active networks[A]. IEEE OPENARCH[C]. Tel Aviv, Israel, 2000.

[7] Active Network Working Group. Security Architecture for Active Nets [R]. USA: Active Network Working Group, May 30, 2001.

[8] 王建国. 主动网络关键技术研究[D]. 西安: 西安交通大学, 2002. 12.

[9] 李钢. 移动代理平台的设计与实现[D]. 西安: 西安交通大学, 2001. 12. 44- 53.

[10] [美] Jamie Jaworski. Java 安全手册[M]. 北京: 电子工业出版社, 2001. 58- 187, 222- 242.

作者简介:

寇雅楠 女, 1964 年 7 月生于北京, 博士研究生, 副教授, 研究方向: 主动网络安全, 网络管理, 软件工程.

李增智 男, 1938 年 3 月生于陕西, 教授, 博导, 研究方向: 网络管理及应用, 分布式系统, 电子数据交换. 国家 863 重点项目(863- 511- 946 - 008)、国家自然科学基金项目(60173059)第一负责人. 近年发表学术论文数百篇, 学术专著 3 本.