主动网络基于分散式角色激活管理的访问控制

陈 鸿, 黎忠文
(厦门大学 信息科学与技术学院, 福建 厦门 361005)

摘 要: 可编程性使主动网络面临更严重的安全威胁, 虽然已经提出了大量的安全策略和安全机制, 但它们的实现多以静态为主, 无法满足主动网络的动态需求。提出一种基于分散式角色激活管理的访问控制策略, 包括身份认证、授权和权限验证, 对动态约束提供了灵活有效的支持, 比传统的基于角色的访问控制更适应主动网络的动态特性。最后在此基础上设计了主动节点的安全机制。

关键词: 主动网络; 分散式角色激活; 访问控制
中图分类号: TP393.08 文献标识码: A 文章编号: 1673-629X(2007)09-0156-04

Access Control of Active Networks Based on Decentralized Role Activation Management

CHEN Hong, LI Zhong-wen
(College of Information Science and Engineering, Xiamen University, Xiamen 361005, China)

Abstract: Programmability makes active networks more vulnerable to security threads. Although many security policies and mechanisms are provided, most of them are implemented in static ways and can not meet the dynamic requirement of active networks. Proposes a decentralized role activation in RABC for active networks, which includes authentication, authorization and permission verification. The mechanism provides a flexible way to support dynamic constraints and is more suitable for the dynamic characteristic of active networks than the traditional RABC. Based on this work, a security mechanism of active node is brought forward in the end.

Key words: active network; decentralized role activation; access control

0 引 言

主动网络使网络节点的功能由传统的存储-转发演变为存储-计算-转发。主动数据包中携带了能对网络节点资源进行访问的程序, 它们在很大程度上可以对资源进行分配、修改等操作, 所有这些都可能使网络受到恶意程序和有缺陷代码的攻击或影响。因此, 众所周知如何构造一个安全的主动网络环境是主动网能够得以推广实用的前提保障。目前对主动网的安全性研究已经投入了大量精力, OPENSIG 和 IETF 组织专门成立了有关标准化小组负责规范主动网及其安全体系结构标准, 但该规范只提出了一个安全框架, 许多细节和实现在该规范中并没有具体地体现。现有的主动网络原型系统中采用的安全策略和安全机制仅仅以静态方式实现, 无法满足主动网络的动态需求, 例如无法确保动态约束被一致贯彻, 为网络节点资源的安全留下隐患。为了克服现有安全机制的缺陷, 文中研究基于授权的安全防护技术, 在我们以前所做工作[1]的基础上, 提出了主动网基于分散式角色激活管理的访问控制策略, 并以公钥加密体制及数字签名和证书机制作为认证机制, 实现对主动网络的安全防护。

1 主动网络基于授权的安全防护技术

目前主动网的安全防护技术可分为两类[2]: 基于系统授权的安全防护技术和基于编程语言的安全防护技术。基于语言的安全机制是一种事半功倍的方式, 很多执行环境(EE)的原型包括 ANTS 和 ASP 都选择了 Java 作为编程语言, 这在很大程度上仰赖于 Java 提供的强大的安全属性。但仅仅靠语言不可能完全排除代码中的 bug。当主动应用在主动网络中大量使用

收稿日期: 2006-12-08
基金项目: 福建省 2004 年自然科学基金(A0410004); 厦门大学院士基金资助(0630-E23011); 厦门大学新世纪优秀人才支持基金(0000-X07116); 广东省自然科学基金(06029667); 中山市科技项目(2006A157)
作者简介: 陈 鸿(1981-), 男, 福建福州人, 硕士研究生, 研究方向为系统安全; 黎忠文, 博士, 副教授, 研究方向为实时系统高安全和高可靠技术。

时, 会有越来越多 bug 的存在。因此, 基于授权的安全防护就显得十分必要。

基于授权的安全防护技术主要可以从两个层面上加以实现: 一是认证, 可靠的认证机制能正确辨别访问者的身份, 同时还能确认用户数据的合法性等等, 从而免遭非授权的攻击; 二是访问控制技术, 对所有的访问实施访问控制限制, 只有获得授权, 才能在允许范围内访问系统资源。根据访问授权方式的不同, 访问控制可以细分为自主访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制(RBAC), 其中 RBAC 的功能相当强大、灵活, 适用于网络系统。授权管理的基本单位为域, 可以将主动网中一组具有相似安全需求的节点组成抽象成一个域, 每个域建立一个授权中心, 并用互联表示数据通信设备和网络, 于是主动网可抽象为如图 1 所示。域与域之间的关系可分为对等和主从两种[1]。对等关系中, 域与域之间是完全平等的, 都有各自的安全策略。在主从关系中, 安全策略具有继承性, 即子域要继承祖先域的策略。此外, 子域还可以定义自己的策略。域之间通过上级授权中心相互鉴别身份。必须保证域间传递的信息具有保密性、完整性。域内安全包括用户数据的安全和执行环境的安全。

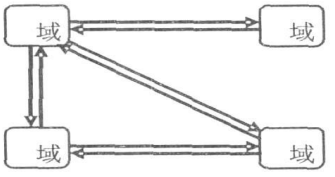

图 1　主动网的抽象表示

2　主动网络基于分散式角色激活管理的访问控制

基于角色的访问控制(RBAC, Role Based Access Control)策略将行为角色与访问权限关联起来, 非常适合于在一个组织环境中布署安全策略。RBAC 模型的基本组件包括用户、角色、对象、操作、权限和会话。用户与角色、角色与权限之间都是多对多的关系, 即多个角色可以赋予同一个用户, 多个用户也可以具有同一个角色; 角色与权限之间也是一样。每个合法用户进入系统得到自己的控制的时候, 就得到一个会话, 一个会话可以激活该用户全部角色的一个子集, 用户能够获得全部被激活角色的所有权限。可见, RBAC 的实施和管理非常简单, 使得用户能够容易地创建更复杂的策略定义。在这种体系中一个用户可以具有多个角色从而拥有不同的许可权限。

在主动网络中为了减轻移动代码的负担, 非常需要这种能以较简单的方式完成复杂管理配置的特征。然而, 传统的 RBAC 模型存在安全缺陷, 无法直接运用于主动网络中。传统的 RBAC 模型只考虑了用户、角色、权限及其关系而忽视了角色激活的重要性。在许多现有的 RBAC 系统中, 角色激活过程常以一种特殊的不协调的方式完成, 动态约束难以一致地贯彻。在一些系统中角色激活过程甚至被忽略, 用户自动获得所有被指派的角色所具有的权限, 而不需要角色激活。在主动网络中为了保护主动节点资源的安全, 在角色激活时赋予用户的角色必须满足动态约束条件。例如, 当主动代码到达某主动节点时, 将根据主动节点当前资源占用/预留情况以及该主动节点的服务类型(如尽力服务、QoS 协商等)等等条件, 动态地赋予用户角色, 从而动态限制用户对节点资源的访问, 这样既提高服务质量, 又能维护主动节点的安全, 还有一定的抗网络攻击能力。因此, 角色激活管理机制能保证动态约束得以一致的贯彻, 对主动网络的安全性至关重要。

文献[3]讨论了 RBAC 中角色激活管理的三种方式: 自主式、集中式、分散式, 分析了这三种方式的优缺点, 并提出一种访问控制模型和授权过程, 以支持分散式角色激活管理。文中在此基础上提出一种适合主动网络的分散式角色激活管理机制, 以弥补传统 RBAC 模型应用在主动网络中的不足。适合主动网络的角色激活管理机制必须满足服务质量(QoS)保证和主动策略控制的要求, 使主动网络可以控制对资源的分配, 对特定主体提供 QoS 保证服务, 也可以动态改变访问控制策略, 以适应用户或业务的动态需求, 还可以部署网络级的整体访问控制, 防止 DDoS 等分布式网络攻击。分散式角色激活管理具有以下优点:

(1) 允许安全策略的制定分散在各个子域中, 子域继承了祖先域的安全策略, 并可制定满足自身要求的安全策略, 使动态约束的制定更加灵活、切合实际。

(2) 在祖先域中已激活的角色, 在子域中无须重复激活, 避免不必要的时间开销, 提升性能。

(3) 具备容错性, 即使一些角色激活服务不可用(例如, 受到 DDoS 攻击), 用户仍然可以在其他角色激活服务中实施角色激活。

(4) 一旦在某个域中实施了角色激活, 相关域的动态约束就随之更新, 对动态约束提供了灵活有效的支持, 可以实施 QoS 服务保证和主动策略控制。

因此分散式角色激活管理非常适合于主动网络的动态特性。

2.1　分散式角色激活管理的访问控制模型

支持分散式角色激活管理的访问控制模型包括以

下几个实体:

用户集 U

客体集 OBS

操作集 OPS

权限集 P, $P = 2^{OBS \times OPS}$

角色集 R

策略域集 D

角色等级关系 $RH \in R \times R$, R 上的偏序

域等级关系 $DH \in D \times D$, D 上的偏序

用户到角色的多对多的指派 $UR \in U \times R$

权限到角色的多对多的指派 $PR \in P \times R$

对象到域的映射函数 $OD: O \rightarrow D$

用户到指定域 d 的已激活角色集的映射关系 $ARS_d: U \rightarrow 2^R$

用户到指定域的冲突角色集的映射关系 $CRS_d: U \rightarrow 2^R$

2.2 主动网络基于分散式角色激活管理的访问控制过程

主动节点通过包接受机制从本地网络接口接收用户发送的主动信包, 进行完备性检查和分类, 并发往相应的执行环境(EE)。主动节点查阅证书库对用户进行身分认证, 通过认证后根据主动信包可执行代码的资源使用策略对用户进行授权验证。授权验证过程如图 2 所示。5 至 7 行, 判断主动信包在可信任(所在域或其祖先域) 的角色激活服务(RAS) 中被激活的角色是否具备足够访问权限, 若是则授权验证通过, 允许主动信包访问节点资源; 否则需要进行角色激活。8 至 11 行, RAS 根据用户身份查找出所有满足权限要求且不违反已定义的角色激活策略(RAP)(例如, RAS 将验证该角色是否在冲突角色集中, 其等级是否高于 EE 的角色等等) 的角色, 将这些角色的集合记为 PORS。12 至 16 行, 若 PORS 不为空, 则 RAS 激活 PORS 中具有最小权限集合的角色, 更新所在域的 ARS, 同时更新所在域及其子域的 CRS; 17、18 行, 若 PORS 为空, 则授权验证失败。

```
Procedure authorization(u ∈ U,o ∈ OBS,opr ∈ OPS)
{
1.    d = OD(o) ∈ D; perm = (o,opr) ∈ P;
2.    PORS = ∅;
3.    Retrieve activated role set ⋃_{d'≥d} ARS_d'(u) as ACRS;
4.    Retrieve all assigned roles in UR as ASRS;
5.    foreach role r_i ∈ ACRS do
6.        if (perm, r_i) ∈ PR then
7.            return TRUE;
      /* if No role in ACRS satisfies the condition*/
8.    foreach role r_j in ASRS do
9.        if (perm, r_j) ∈ PR then
              /*check if r_j can be activated */
10.           if r_j can be added to ARS_d(u) then
11.               PORS = PORS∪{r_j};
      /* check if there is a role that can be activated */
12.   if (PORS = ∅) then
13.       find r_k ∈ PORS which has least privilege
14.       ARS_d(u) = ARS_d(u)∪{r_k};
15.       Update CRS_d'≤d(u);
16.       return TRUE;
17.   else
18.       return FALSE;
}
```

图 2 授权验证过程

主动节点可为每个角色设置相应的时限, 当超过这个时限角色就自动失效。也可在主动信包中设置时限, 在角色激活时所取的时限应为二者的较小值。

2.3 访问控制过程与认证过程的结合

在访问控制过程中必须对正确的用户赋予正确的权限(身份认证), 并确保正确的用户使用正确的权限对系统进行访问(授权验证), 这就需要将访问控制过程与认证过程相结合。在主动网环境中, 对分组报文的认证不仅会出现在信源和信宿端, 还可能出现在传输路径上的各个主动节点间。因此在逐跳安全的基础上, 必须进一步实施对主动报文主体的端到端安全认证以对主动网提供更强的安全保护。为了具有不可抵赖性和避免数字签名失效, 我们将整个主动分组划分为两部分[4,5]: 一部分为可变化的内容; 另一部分为不发生改变的静态内容(如图 3 所示)。这样, 在主动分组的静态部分设计主体标识(可考虑采用 X. 509v3 证书作为主体标志), 然后采用公钥密码体制的数字签名技术签名静态内容, 即可实现主动网中端到端的认证保护。而对于逐跳安全保护, 则可以采用对称密钥体制加密主动分组的可变化的内容, 并加入单向 HASH 函数计算数字摘要, 对主动网络及其分组的传输实施数据完整性、机密性或不可抵赖性认证保护。

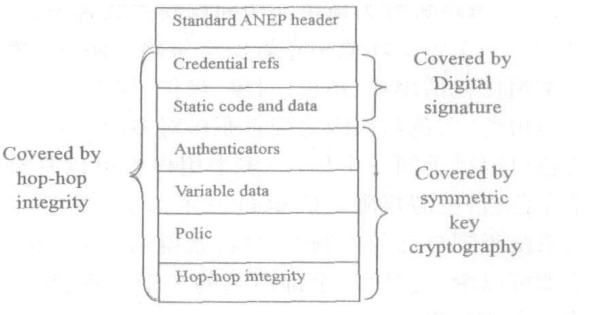

图 3 ANEP 包格式

2.4 主动节点的安全机制

在这一访问控制过程的基础上, 设计主动节点的安全机制如图 4 所示。部分尚未涉及的构件说明如

下:

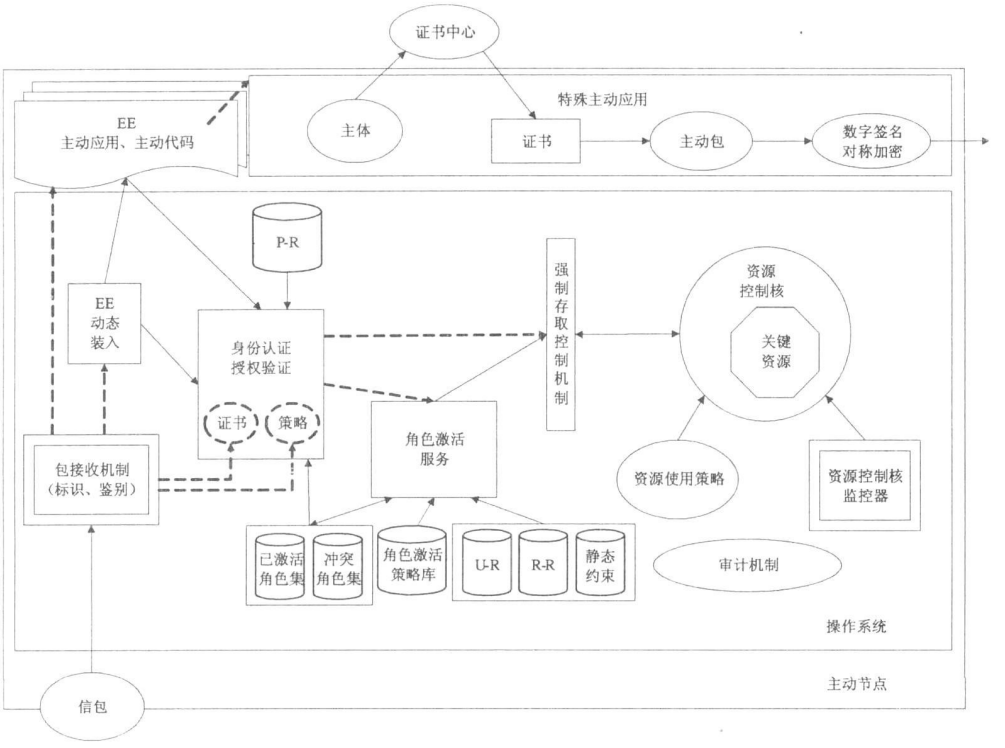

图 4　主动节点的安全机制

(1) EE 动态装入机制。负责在主动节点上装入新 EE, 它根据新 EE 的资源访问要求和节点资源管理策略计算该出该 EE 的最大特权集(指节点操作系统允许 EE 可访问的节点资源的最大限制) 并激活相应的角色。对于在 EE 上执行的用户代码的角色, 其等级不得高于 EE 的角色。

(2) 强制存取控制机制。其作用是对主动节点中的每个客体(进程、文件、设备、管道、IPC 客体) 都赋予了相应的安全级, 是操作系统固有的。

(3) 资源控制核监控器。它一方面用于监视资源控制核的工作, 另一方面当该控制或系统出错时进行处理, 尽量避免或减少损失。

(4) 资源控制核。资源控制核通过节点资源的安全使用策略对节点资源进行保护, 这里主要是实现对 CPU、内存及带宽的保护。该控制核动态地生成资源使用监控进程, 分别用于监视各 EE 对受保护资源的使用情况。一旦资源使用超过了 EE 的权限则进行相应的处理。

(5) 审计机制。审计作为一种事后追查的手段用来保护系统的安全。

(6) 特殊主动应用。每个 EE 中都有一个特殊主动应用, 它为 EE 生成的主动包向证书中心(在网络内) 申请证书, 并负责主动包的数字签名、对称加密和发送。

3　结束语

主动网的安全性是它能够得以推广实用的前提保障, 对资源的控制访问是主动网基础结构安全的基础, 它包括对用户进行授权, 对用户的权限进行验证, 保证授权的正确性和完整性等方面的内容。因此如何对合法用户进行授权以及防止用户对资源进行非授权攻击成为主动网络的重要研究课题。文中提出一种基于分散式角色激活管理的访问控制策略, 用对称密码体制以及数字签名和证书机制保证用户数据的合法性和完整性, 用分散式角色激活管理机制保证动态约束可以一致地贯彻, 比传统的基于角色的访问控制更适合主动网络的动态特性。

参考文献:

[1] 黎忠文, 李乐民, 李美蓉. 一种新的主动网络安全体系的设计[J]. 通信学报, 2004, 25(1): 119- 125.

[2] Psounis K. Active networks: application, security, safety, and architectures[J]. IEEE Comm Surveys, 1999, 2(1): 445- 457.

[3] Lui R W C, Chow S S M, Hui L C K, et al. Role Activation Management in Role Based Access Control[C]//ACISP. [s. l.]: [s. n.], 2005.

[4] 唐　寅. 基于授权的主动网络安全防护技术研究[D]. 成都: 电子科技大学, 2003.

[5] Xia Zheng- you, Zhang Shi- yong. Design of Secure System Architecture Model for Active Network[J]. Journal of Software, 2002, 13(8): 1352- 1360.

(上接第 155 页)

[4] Li S J, Mou X Q, Cai Y L. Improving security of a chaotic encryption approach[J]. Physics Letters A, 2001, 290: 127- 133.

[5] 求是科技. Visual FoxPro 数据库通用模块及典型系统开发[M]. 北京: 人民邮电出版社, 2006.