文章编号: 1673- 0062(2009) 02- 0074- 04

自适应的网络安全策略框架

胡义香, 饶 婕, 任 辉

(南华大学 计算机科学与技术学院, 湖南 衡阳 421001)

摘 要: 本文研究了现有的网络管理方式及形势, 提出一种自适应的网络安全策略框架. 通过引入认知情况、核心存在论、策略的分类和检测等相关元素, 使得该安全策略框架能够明确并执行动态的、灵活多变的网络环境里的安全策略, 实现网络管理的自动化.

关键词: 认知情况; 安全策略; 适应性; 安全框架

中图分类号: TP393 文献标识码: A

An Adaptable Network Security Policy Framework

HU Yi-xiang, RAO Jie, REN Hui

(School of Computer Science and Technology, University of South China, Hengyang, Hunan 421001, China)

Abstract: This paper studies the ways and situations of existing network management, and presents an adaptable network security policy framework. Due to the situation- awareness, the core ontology, the policy classification and detection, this framework can specify and enforce dynamic and flexible security policies in a dynamic environment, so the automatization of network management will come true.

Key words: Situation- awareness; Security Policies; Adaptability; Security Framework

0 引言

随着 Internet的迅猛发展, 网络规模、复杂性、异构性呈指数形式扩张, 应用服务的复杂度和人们对网络信息安全的要求也在不断增加, 网络管理随之变得越来越复杂. 在大规模的分布式系统中, 由于基于服务的系统无需考虑编程语言及平台的差异, 就能组合大量的可利用的服务去完成一个巨大的任务, 因此它的应用越来越广. 随着基于服务的系统成倍的增长, 这就迫切的需要一种有效的技术来保证只有授权的用户才能获得这个开放的动态系统中的资源及服务, 而现有的安全技术[1- 2]很难解决这个问题. 我们提出了一种自适应的安全策略框架来系统的分类和执行基于服务的系统中的安全策略.

1 基于策略的网络管理系统结构

IETF提出的基于策略的管理框架包括四个

收稿日期: 2008- 12- 16

作者简介: 胡义香 (1981-), 女, 湖南衡阳人, 南华大学计算机科学与技术学院助教, 硕士. 主要研究方向: 计算机网络与信息安全.

部分: 策略管理工具、策略决策点、策略执行点和策略仓库, 如图 1所示.

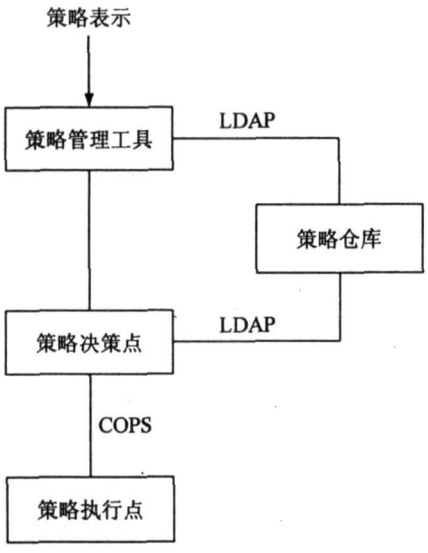

图 1　基于策略的网络管理系统结构

Fig 1　Network management system based on policy

供管理员编辑策略和监控策略的应用系统是策略管理工具 (Management Tools). 它可以为管理员提供一个易于使用的编辑界面 (如 GUI) 来编辑策略, 并将编辑好的策略转成一定格式, 存于策略仓库中. 同时它还可以对策略进行检查和确认, 以确保在整合策略的构成时不会发生冲突.

策略仓库 (Repository) 用于存储策略信息, 能对系统中的策略进行汇总. 它可以是目录服务器或数据库服务器, 除了储存管理员已经编辑好的策略信息, 还可以存储其它的网络信息和系统参数.

策略决策点 (Policy Decision Point) 通常也被称为策略服务器, 是整个系统的决策中心. 它负责存取策略仓库中的策略, 并根据策略信息做出决策, 然后将相应的策略分配至策略执行点. 策略决策点还能检测策略的变化和冲突, 从而采取应对措施.

接受策略管理的网络实体是策略执行点 (Policy Enforcement Point), 通常也被称作策略客户端. 它可以是路由器、交换机、防火墙等网络设备, 负责执行由策略决策点分配来的策略. 同时它还向策略决策点发送信息, 使策略决策点知道网络的变化以及策略的执行情况.

以上各个模块都是一个独立的子系统, 为了实现模块间的策略信息交换, IETF定义了一些协议来实现模块间的通信. LDAP (Light weight Directory Access Protocol) 协议用于策略数据库和其它子系统之间策略信息的传输; 在 PDP和 PEP之间可用 COPS (Common Open Policy Service) 协议、SNMP、CLI来进行策略信息的传输. 也可以使用其他的传输协议, 例如 HTTP, FTP或者 SNMP. 但是, 对于策略管理工具和 PDP之间以及多个 PDP之间的传输协议还没有明确.

2　自适应的网络安全策略框架

自适应的网络安全策略框架主要用于大规模的基于服务的系统, 这些大系统包括很多自治管理域, 却没有一个集中的管理权力中心. 在这个系统中, 很多成员 (如: 服务提供商和服务使用者) 都可以创建自己的安全策略, 并且采用不同的鉴定机制 (如 X. 509证书). 而每个成员的安全要求就体现在他们各自的安全策略中. 这个安全策略框架由以下主要部分组成, 如图 2所示.

1) 核心存在论: 用来描述基于服务的系统中的安全策略.

2) 合理的编程语言: 用来表达形式安全策略.

3) 分类算法: 用来分解和区分形式化的安全策略, 并将它们归于不同的策略集.

4) 冲突检测算法: 用来检测安全策略的一致性, 完整性和冗余性等.

5) 分布式安全策略执行点的工具和时间, 包括:

①编译器: 用来从分解的策略集中产生安全代理.

②平台: 用来配置安全代理.

③代理发现协议: 为了可靠地发现相关安全代理, 从而根据服务请求执行安全策略.

④授权安全技术: 如加密算法和鉴定机制.

⑤认知情况代理: 用来提供安全策略评估所需的情况信息.

从上可以看出, 可适应安全策略框架弥补了英国帝国大学的策略框架中语法结构过于复杂和 OASIS组织的策略框架中没有提供策略冲突的处理机制的不足, 结合了前两种安全策略的优点. 可适应安全策略框架, 通过一种将认知情况[3]和安全策略相结合的合理方法, 来系统地指明和执行分布式系统中的安全策略. 这种方法可以提供明确的合理的策略规范, 从而使得策略的确认和检验变得容易. 尽管逻辑语言提供了高级别的抽象, 但它对用户来说可能很难理解, 我们用一个基于

存在论的技术,可以很容易的用自然语言做出明确的策略.认知情况就是系统的行为能适应系统情况变化的性能.情况被认为是先前的设备行为或一段时间内在设备上运行的与应用软件相关的一组上下文的变化.一个上下文就是环境或设备的一个瞬间的可发觉的相关条件,如:时间、地点、可用带宽等.在安全策略的执行过程中,通过结合认知情况,系统能评估系统中各个部分之间动态信任关系,从而保护各种情况下的关联设备.

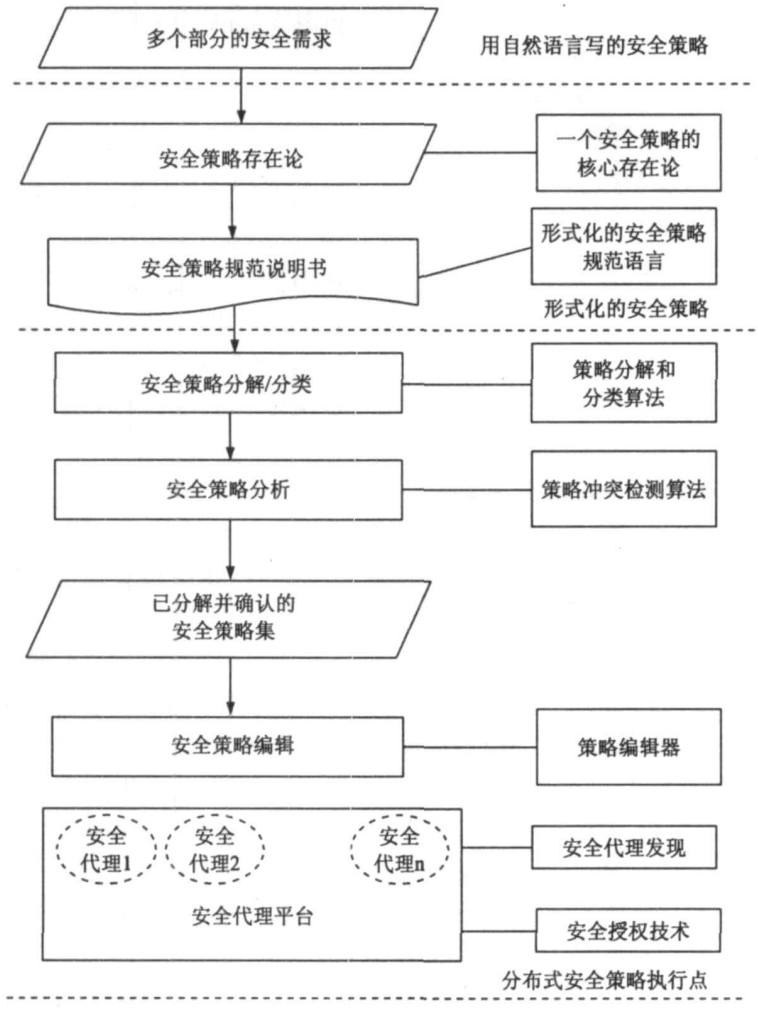

图 2 可适应安全策略框架

Fig. 2 an adaptable network security policy framework

3 明确基于服务的系统中的自适应安全策略

3.1 安全策略的定义

安全策略就是一些定义安全要求的规则,很明显,在基于服务的系统中,安全策略必需满足以下三个要求:

1)客户和服务提供商必需经过鉴定.

2)必需保护客户和服务提供商之间的通信机密.

3)服务访问行为必需授权.服务提供商要能控制他们的服务,并根据不同的形势采取不同的安全策略,同时他们还有授与第三方访问服务的权力.

为了比较容易地描述安全策略,在核心存在论里,定义了一个基类 A,这样就可以为上面的三个安全要求建模.基类 A 的具体内容如下:

$A = \{$实体,行为,安全机制,授权,属性$\}$

从上可以看出基类 A 由实体、行为、安全机制、授权和属性五个方面构成.

3.2 安全策略分类及自动检测

在安全策略中,规则 R_x 中 I 域和规则 R_y 中的相应域之间的关系可能是相等关系、子集关系、父集关系或无关,我们形式化描述如下:

域与域之间的关系: ①相等, $A = B$; ②包含, $A \subset B$; ③相交, $A \cap B \neq \emptyset$ 相交; ④无关, $A \cap B = \emptyset$. 在此基础上, 在我们先前的研究工作中, 将规则分为以下五类: (1)完全匹配规则 (记为 $R_X = R_y$); (2)包含匹配规则 (记为 $R_x = R_y$); (3)关联规则 (记为 $R_x \subset R_y$); (4)部分分离规则或部分匹配规则 (记为 $R_x R_y$); (5)完全分离规则 (记为 $Rx\ Ry$). 并在此基础上, 将网络安全策略比较全面的进行了分类, 如图 3所示.

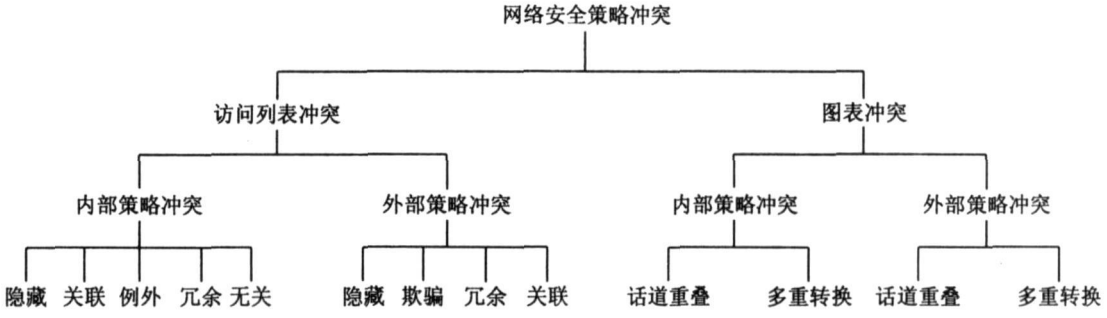

图 3　网络安全策略冲突分类

Fig 3　Classification of network security policy conflicts

实践中常用的五种策略执行优先权方案: ①反向策略优先; ②新加载策略优先; ③本地策略优先; ④指定优先权; ⑤属主级别优先. 将这五种方案, 引入有向图中, 提出了一种基于有向图的网络安全策略分类及检测方法, 并在校园网中进行模拟实验, 取得了较好的效果.

4　结束语

传统的基于 SNMP方法是以设备为中心的, 为了适应网络发展的需要, 人们提出了基于策略的网络管理, 将管理和执行分开, 管理员只要对策略进行定义, 而不必关心实现该策略的具体细节和相关设备的情况, 实现网络管理的自动化. 但是在大规模的基于服务的系统中包括很多自治管理域, 却没有一个集中的管理权力中心, 因此迫切需要一个统一的框架, 来协调这个系统中成员各自的采用不同的鉴定机制的安全策略.

本文提出的可适应网络安全策略框架中的核心存在论使安全需求的表达变得容易, 并且也易于理解. 同时由于认识情况的引入, 从而使得该安全策略框架能够明确并执行动态的、灵活多变的网络环境里的安全策略. 最后, 我们还将致力于提高运行时间, 及如何在合适的位置放置安全代理的研究.

参考文献:

[1] Nakamur Y, Hada S, Neyama R. Towards the integration of Web services security on enterprise environments[J]. Proc Symp on Applications and the Internet (SAINT) Workshops (2002), 2002, 8(7): 166-175.

[2] Naedele M. Standards for XML and Web services security[J]. IEEE Computer, 2003, 36(4): 96-98

[3] Yau S S, Karim F, Huang D, et al. Situation-aware contract specification language for middleware for pervasive computing[J]. IEEE Pervasive Computing, 2003, 30(28): 93-99.

[4] RFC3460 Policy Core Information Model (PCIM) extensions[S]. United States: RFC Editor, 2003.

[5] 姚　键, 茅　兵, 谢　立. 一种基于有向图模型的安全策略冲突检测方法[J]. 计算机研究与发展, 2005, 42(7): 1108-1114.

[6] 刘云玲, 杨　璐. IPsec体系结构及其策略管理机制的研究[J]. 网络安全技术与应用, 2006(2): 17-19.