分布式联动系统中的多级委托策略研究

朱丽娜[1,2] 孙潮义[2] 张 焕[2]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1] (武汉数字工程研究所 武汉 430074)[2]

摘 要 目前已有的集中式安全联动防御机制对大规模复杂攻击很难做到协同防范,且容易造成单点服务失效等问题。针对上述不足,在分布式体系结构的基础上提出了一种包含安全联动策略(SRP)和委托管理策略(DAP)的多级委托机制,该机制由联动权限的动态委托和可信委托链的构造方法组成。用XACML Admin规范语言描述了上述两种策略,用形式化的方法描述了委托链的结构组成和委托过程,给出了委托联动算法的伪代码实现。构造可信委托链不仅实现了协同安全联动防御,而且在一定程度上克服了单点失效等问题。提出的安全策略多级委托机制将为构建动态的、分布式的、协作的网络安全防护系统奠定良好的理论基础。

关键词 分布式联动,联动代理,委托,XACML Admin
中图法分类号 TP309 **文献标识码** A

Research on Multilevel Delegation Policy in Distributed Response System

ZHU Li-na[1,2] SUN Chao-yi[2] ZHANG Huan[2]
(School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[1]
(Wuhan Digital Engineering Institute, Wuhan 430074, China)[2]

Abstract Centralized Security Response System has many shortcomings, such as local response, single service invalidation, lack of cooperative response to large-scale complex attack, etc. In order to enhance the robustness of response system and realize cooperation, based on distributed architecture, this paper introduced multilevel delegation mechanism to response policy: Security Response Policy (SRP) and Delegation Administration Policy (DAP). This mechanism was composed of dynamic delegation of response privilege and construction of credible delegation chain. SRP and DAP were described by XACML Admin criterion language; the structure of delegation chain and the process of delegation were described in formal method; the delegation response algorithm was presented in pseudocode. Constructing credible delegation chain did not only realize cooperation response, but also solved single point invalidation, etc. Multilevel delegation mechanism will establish favorable theory base for constructing dynamic distributed cooperative network security defense system.

Keywords Distributed response, Response agent, Delegation, XACML Admin

1 概述

随着网络规模和复杂程度日益增加,网络攻击手段也在朝着组合式、分布式方向发展,网络安全问题愈演愈烈。大量安全设备广泛地部署在网络中,传统的网络安全联动系统对各种异构的安全设备采用分离操作、各自管理的模式,不仅浪费了资源,无法对安全策略进行统一管理,而且安全设备之间缺乏协作,对安全事件的响应能力低下,难以做到及时、准确的整体防卫。集中式网络安全联动系统存在若干缺陷,主要包括:本地检测本地响应,安全事件之间得不到关联,无法或很难响应复杂攻击,不能在网络层产生协作的安全联动;单点服务的安全性差,过分依赖中心控制台,容易造成流量瓶颈。此外,联动系统缺乏规范的安全策略描述,各种安全设备的联动策略无法互通,不能动态适应网络环境的变化。

网络安全体系的发展趋势是分布的、联动的、协作的。为了保证大型网络的安全,增强联动系统的健壮性,对大规模安全事件在一定范围内做出协同响应,需要在整个网络空间引入委托的思想,统一配置安全策略,改变以往各自为战、势单力薄的状况。本文提出的安全联动系统采用分布式体系结构,由分布在各级子网中的联动代理执行策略,基于XACML Admin规范语言[1,2]描述安全联动策略(SRP, Security Response Policy)和委托管理策略(DAP, Delegation Administration Policy),将多级委托机制引入到策略管理中:通过委托联动传递联动权限,生成相应的DAP;根据DAP的密钥判断权限的委托者是否可信,若不可信则委托终止,若可信且联动的安全设备有效,则生成SRP并执行,否则联动委托被继续传

到稿日期:2008-07-24 返修日期:2008-10-22 本文受国防"十一五"预研计划(No. C0820061362-06, No. A1420080183),国家"863"高新技术计划信息安全主题(No. 2007AA01Z464),船舶工业国防科技预研基金项目(No. 08J3. 7. 8)资助。
朱丽娜(1981—),女,博士研究生,主要研究方向为入侵检测与网络安全,E-mail:zhulina81@gmail.com;孙潮义(1956—),男,研究员,博士生导师,主要研究方向为指控系统软件工程;张 焕(1982—),男,硕士研究生,主要研究方向为软件工程与网络安全。

递。

2 分布式多级委托联动

2.1 委托机制的相关研究

委托是一种重要的安全策略，其基本思想是系统中的主动实体将自己的部分或全部权限传授给其他主动实体，让后者以前者的名义完成一些工作[3]。其中，发出授权的主动实体称为委托者，接收授权的主动实体称为被委托者。

委托的思想最早出现在访问控制模型中。研究人员在RBAC的基础上引入委托的概念，提出了基于角色的委托模型[4-6](RBDM，role-based delegation model)，支持委托者自主地委托角色或权限。最具有代表性的是Barka和Sandhu在2000年提出的RBDM[7]，该模型首先总结出委托的8个特性，即时效性、变化性、部分性、委托管理、委托协商、委托撤销、委托广度和深度，然后通过系统的方法分析得出相关联的特性结构，并提出了相应的委托模型框架，最后以永久委托、临时委托两个模型为出发点分析了各个特性的意义及内容。文献[8]提出了PBDM角色委托模型，其最大特点是支持部分委托和角色到角色的委托。

此外，人们对委托限制进行了大量的研究[9-12]，但成果相对较少。其中，Bandmann提出了一个受限的委托模型[12]，实现了对委托树的结构限制，该模型用正则表达式描述委托约束，不仅能分离权限的委托和使用，而且可以有效地限制被委托权限的传播。

2.2 联动系统中的委托机制

2.2.1 相关定义

引入多级委托机制的分布式安全联动系统中的策略分为两种：安全联动策略和委托管理策略。

定义1 安全联动策略是指可以直接联动安全设备的策略，记为SRP；委托管理策略指联动权限被委托传递的消息，记为DAP。

定义2 联动代理指分布在各个级别的子网中，产生并执行SRP或产生DAP传递委托消息的实体。每个代理有一对密钥(私钥和公钥)，私钥用于加密DAP以保证委托消息的可靠性和完整性，公钥在系统初始化时被广播。

在分布式联动系统中，一般存在两种情况可能发生委托联动：(1) 某联动代理需要联动的安全设备出现故障时，该代理委托其他联动代理代替其完成任务。(2) 若干个联动代理为了抵御某一有组织的复杂攻击而需要相互协作时，联动代理之间相互赋予协作方一定的权限，以防患于未然。

定义3 委托联动是指在上述两种情况下，当前联动代理把特定的联动权限委托给其他代理并实现联动的过程。其中，委托消息传递过程生成若干条DAP，权限到达联动服务器(即真正执行联动的代理)时生成一条SRP。

定义4 “安全设备树”是指将整个网络中的安全联动设备根据其作用范围按照树状结构划分等级，树中的每个节点记录相应的联动代理。

2.2.2 基于XACML Admin的联动策略描述

XACML提供了一种描述访问控制策略及其实现过程的规范。XACML核心规范[2]认为所有的策略都是可信的，同时不考虑委托的情况，XACML Admin[1]扩展了〈Policy〉定义，加入〈Issuer〉和〈Delegates〉，使其能够表示委托。扩展后的访问策略表达的语义从原来“在给定条件下，某主体可以(或不可以)以某种方式访问某资源”扩展为“某主体宣称‘在给定条件下，某主体可以(或不可以)以某种方式访问某资源’”，同时可以表达形式为“某主体宣称‘在给定条件下，某主体可以管理某些主体、资源、访问方式’”的委托策略，此处的“管理”指授权主体可以在其管理范围内设定访问策略，或进行进一步委托。

为了实现联动策略标准化，本文基于XACML Admin规范语言描述策略。分布式安全联动系统中的SRP和DAP，分别对应XACML Admin中的访问策略和委托策略。策略的〈Subject〉表示发生安全事件的子网所拥有的联动代理；策略中的〈Action〉表示对安全设备执行的动作，如阻断、重定向、修复等；〈Resource〉表示不同的安全设备，如防火墙、IDS、审计系统等。

约定：S表示联动代理集合，A表示联动方式集合，R表示安全设备集合，T表示有效时间区间集合。

SRP记为四元组$acc(s,a,r,t)$，表示联动代理s在时间区间t内能以方式a联动安全设备r；t可以取值∞，表示s能一直以方式a联动r。其中，$s\in S, a\in A, r\in R, t\in T$。

DAP记为五元组$adm(d,a,r,i,t)$，表示联动代理i宣称“在时间区间t内，联动代理d可以管理‘以方式a联动安全设备r’”。其中$d\in S$表示被委托者，同时也是联动的执行者；$a\in A$表示被委托的联动方式；$r\in R$表示被委托的安全设备；$i\in S$表示委托者；$t\in T$表示被委托权限的有效期限。

$adm'(d,K_i(a),K_i(r),i,K_i(t))$表示用第$i$个联动代理的私钥对委托管理策略中的动作、资源、时间属性加密。

2.2.3 委托联动

分布式安全联动系统由中心联动控制台(Console)和分布在各级域中的联动代理(Agent)组成，每个安全设备对应一个联动代理，联动代理负责监视安全设备的健康状态、生成/传递DAP、执行SRP。中心联动控制台是管理员制定、管理所有公钥、“安全设备树”和所有初始策略的接口，初始策略均为SRP。整个系统初始化时，中心联动控制台向各个联动代理下发公钥列表、“安全设备树”和特定的SRP。初始化完成后，中心联动控制台退出。

委托联动系统的部署如图1所示。

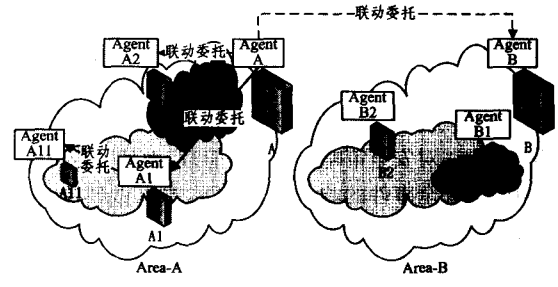

图1 委托联动系统部署图

域Area-A和Area-B的级别相同：Area-A拥有安全设备A，Area-A被细分为两个子域，分别对应安全设备A_1和A_2，其中，安全设备A_1所在的域被继续细分，对应安全设备A_{11}；Area-B拥有安全设备B，Area-B被细分为两个子域，分别对应安全设备B_1和B_2。

按照消息传递的方向划分，安全联动系统中的委托有两种：纵向委托和横向委托。纵向委托是在上级安全设备失效

的情况下，委托下一级安全设备响应；横向委托是指一个域中发生安全威胁时，提前委托同级域中的安全设备进行响应，防患于未然，适合协同抵御大规模的蠕虫传播。

假设在域 Area-A 中发现 Code Red 蠕虫，通过查找联动策略，安全设备 A 应该执行“阻断对 TCP 80 端口访问”的响应，然而 Agent A 发现设备 A 出现故障，无法实施响应，于是委托 Agent A_1 和 Agent A_2，让安全设备 A_1 和 A_2 执行相同的响应，不幸的是，设备 A_1 也出现故障，于是 Agent A_1 委托 Agent A_{11}，通知安全设备 A_{11} 响应。由于域 Area-B 中的机器与 Area-A 中的配置相同，即存在相同的漏洞，因此 Code Red 下一步感染的目标很可能是 Area-B，为了提前阻断蠕虫传播，Agent A 委托 Agent B 执行“阻断对 TCP 80 端口访问”的响应。图 1 中的有向实线表示纵向联动委托，虚线表示横向联动委托。在上述实例中，产生两条纵向委托链 $A\rightarrow A_1\rightarrow A_{11}$ 和 $A\rightarrow A_2$，一条横向委托链 $A\rightarrow B$。

联动委托链的形式化描述如下：

假设一组联动代理记为 $A_1, A_2, \cdots, A_n, Ser$，$A_1$ 产生联动请求，但是委托 A_2 实施请求，A_2 又委托 A_3，以此类推，联动代理 A_n 委托联动服务器 Ser 完成请求。委托标记以一种简单的次序被组织。用 T_{A_i} 表示从 A_i 到 A_{i+1} 的委托标记，req 表示联动请求，那么，从 A_1 到联动服务器 Ser 之间的消息传递表示如下

$$req, T_{A_n}, T_{A_{n-1}}, \cdots, T_{A_2}, T_{A_1}$$

该委托链由 $n+1$ 步组成，前 n 步是委托消息，最后一步是真正的联动请求。委托标记是一个五元组

$$T_{A_i}: \langle A_i, A_{i+1}, act_{A_i}, res_{A_i}, t_i \rangle$$

含义是 A_i 委托 A_{i+1} 在时间 t_i 内对安全设备 res_{A_i} 执行动作 act_{A_i}。加密后的委托标记为

$$T_{A_i}': \langle A_i, A_{i+1}, K_{A_i}(act_{A_i}, res_{A_i}, t_i) \rangle$$

通常，第 i 步委托消息为

$$A_i\rightarrow A_{i+1}: \langle A_i, T_{A_i}' \rangle (i<n)$$

当委托可信，即 A_{i+1} 从公钥列表中找到 A_i 的公钥并能够解密 T_{A_i}'，但因安全设备 res_{A_i} 出现故障而无法实施联动时，需要由 A_{i+1} 根据 T_{A_i} 继续构造 $T_{A_{i+1}}$ 并加密，同时生成一条 DAP。

当 $i=n$ 时，$A_n\rightarrow Ser: \langle A_n, T_{A_n}' \rangle$；

当 $i=n+1$ 时，Ser 能够联动 res_{A_n}，对应联动请求 req：$\langle Ser, act_{A_n}, res_{A_n}, t_n \rangle$，同时生成一条 SRP。

由 A_1 产生联动请求的过程表示如下

$$A_1\rightarrow Ser: \langle Ser, req \rangle \langle A_n, T_{A_n}' \rangle \langle A_{n-1}, T_{A_{n-1}}' \rangle \cdots \langle A_2, T_{A_2}' \rangle \langle A_1, T_{A_1}' \rangle$$

前 n 个委托标记中安全设备之间的关系为

$$rank(res_{A_1}) \geqslant rank(res_{A_2}) \geqslant \cdots \geqslant rank(res_{A_n})$$

表示前一步标记中的设备级别高于后一步标记中的设备或者两者平级（协同联动）。通过查询“安全设备树”找到将要被委托联动的安全设备及相应的联动代理。

由加密后的委托标记 $T_{A_i}': \langle A_i, A_{i+1}, K_{A_i}(act_{A_i}, res_{A_i}, t_i) \rangle (i=1,2,\cdots,n)$ 生成的 DAP 为 $adm'(A_{i+1}, K_{A_i}(act_{A_i}), K_{A_i}(res_{A_i}), A_i, K_{A_i}(t_i))$；由 req 生成的 SRP 为 $acc(Ser, act_{A_n}, res_{A_n}, t_n)$。

2.2.4 算法描述

假设：x 是联动代理，Attack(x, i) 表示 x 所在的域发生安全事件 i；Valid(res) 表示安全设备 res 是否发生故障，返回值为真表示没发生故障；Search(i, x, $Policy$) 表示针对安全事件 i 在 x 的子策略库中寻找合适的策略 $Policy$，由于采用 XACML Admin 规范语言描述策略，因此 $Policy.a$ 和 $Policy.r$ 对应将要执行的动作和被联动的资源；Delegate(x, y, Pr) 表示 x 委托联动代理 y 执行权限 Pr，其中，Pr 是二元组 (act, res)；Junior(res, sub) 返回安全设备 res 的下一级安全设备个数，数组 sub 存放各设备名称；Coequal(res, bro) 返回安全设备 res 的同级安全设备个数，数组 bro 存放各设备名称；Execute(x, $Policy$) 表示 x 执行安全联动策略 $Policy$；Produce ($Policy$) 表示生成策略 $Policy$，若是 DAP，则需要用委托者的私钥加密；Add(x, $Policy$) 表示向 x 的子策略库中添加 $Policy$；Credible ($DAPolicy$) 利用 $DAPolicy.i$ 的公钥解密 $DAPolicy$，若解密成功，说明 $DAPolicy$ 可信，否则不可信。

说明：函数 Delegate(x, y, Pr) 包含了生成相应的 DAP，但在下述伪代码中，为了表述清晰，用函数 Produce($Policy$) 又描述了一遍。

在分布式联动系统中存在两种发生委托的情况，规定：对于情况一，当联动代理 x 无法执行联动时，通过委托其安全设备的下一级设备完成联动，为了保证响应及时，需要限制委托深度 depth，即在“安全设备树”中向下寻找有效设备的深度；对于情况二，x 协同联动的同一级安全设备对应的代理，若设备出现故障则放弃联动。委托联动的伪代码描述如下：

```
(委托情况一)
Attack(x,i);
Search(i,x,req); //确定将要执行的动作和联动的设备
if(Valid(req.r)){ //联动代理 x 对应的安全设备有效
    Execute(x,req);
}
else{ //联动代理 x 需要委托联动
    n = Junior(req.r,sub); //寻找故障设备的下一级设备
    for(i=0; i<n; i++){
        Delegate(x,sub[i].agent,Pr); //Pr.act=req.a,Pr.res=
sub[i]
        Produce(adm); //生成 DAP 并加密,其中,adm.i = x,
              //adm.d = sub[i].agent,adm.a = Pr.act,adm.r
= Pr.res
        while((depth>0)&&(Credible(adm))){
        //未达到最大委托深度且当前委托可信
          if(Valid(sub[i])){ //安全设备 sub[i]有效
            Produce(acc); //由 DAP 生成 SRP,其中,
              //acc.s = sub[i].agent,acc.a= adm.a,acc.r =
adm.r
            Add(sub[i].agent,acc);
            Execute(sub[i].agent,acc);
            break;
          }
          else{ //安全设备 sub[i]无效,需要继续委托;
            m = Junior(sub[i],re);
            执行上述 for 循环,迭代委托;
            depth--;
            }
      }//while
    }//for
```

```
}//else
    (委托情况二)
Attack(x,i);
Search(i,x,req);
Execute(x,req);
n = Coequal(req.r,bro); //与设备 req.r 同级的安全设备共 n 个
for(i=0; i<n; i++){
    Delegate(x,bro[i].agent,Pr); //Pr.act=req.a,Pr.res=bro[i]
    Produce(adm); //生成 DAP 并加密
    if((Credible(adm))&&(Valid(bro[i]))){
        Produce(acc); //由 DAP 生成 SRP
        Add(bro[i].agent,acc);
        Execute(bro[i].agent,acc);
    }
}
```

结束语 本文基于 XACML Admin 规范语言描述了 SRP 和 DAP，将多级委托机制引入分布式安全联动系统中：在两种可能出现委托的情况下，通过委托联动有效地解决了单点服务失效的问题，同时初步实现了针对复杂攻击的协同响应；寻找更高级联动代理的多级委托机制大大提高了完成联动响应的成功机率，增强了联动系统的健壮性；非对称加密技术大大简化了委托是否可信的判断过程，不需要通过回溯寻找可信的消息发布者[13]。文中用形式化的方法描述了委托链的组成和委托过程，并以伪代码的形式给出了委托联动算法。

委托机制涵盖的内容较多，例如，委托深度、主体的可信度、权限的有效时间等等。为了突出多级委托机制应用于分布式联动系统的原理，本文没有涉及或者简化上述问题，在今后的工作中，需要进一步从深度和广度上展开更加细致的研究。

参 考 文 献

[1] Rissanen E, Lockhart H, Moses T. XACML 3.0 administrative policy [OL]. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, 2005

[2] Moses T. Extensible Access Control Markup Language (XACML) Version 2.0 [S]. OASIS Standard, 2005

[3] 张宏，贺也平，石志国. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报，2006，29(8)：1427-1437

[4] Barka E, Sandhu R. A role-based delegation model and some extensions[A]// Proceedings of 23rd National Information Systems Security Conference[C]. Baltimore, USA, 2000：168-177

[5] 徐震，李斓，冯登国. 基于角色的受限委托模型[J]. 软件学报，2005，16(5)：970-978

[6] Ye C X, Wu Z F, Ff Y Q. An attribute-based delegation model and its extension[J]. Journal of Research and Practice in Information Technology, 2006, 38(1)：3-16

[7] Barka E, Sandhu R. Framework for role-based delegation models [C]// Proc. of the 16th Annual Computer Security Application Conf. IEEE Computer Society Press, 2000：168-176

[8] Zhang X W, Oh S, Sandhu RS. PBDM：A flexible delegation model in RBAC[C]// Ferrari E, Ferraiolo D, eds. Proc. of the 8th ACM Symp. on Access Control Models and Technologies. New York：ACM Press, 2003：149-157

[9] Faulkner S, Dehousse S, Kolp M, et al. Delegation Mechanisms for Agent Architectural Design[C]// Proc. of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'05). Washington, DC, USA, IEEE Computer Society, 2005：503-507

[10] Seitz L, Rissanen E, Sandholm T, et al. Policy administration control and delegation using XACML and delegent [C]// The 6th IEEE/ACM International Workshop on Grid Computing. Washington, 2005

[11] 叶春晓，吴中福，符云清，等. 基于属性的扩展委托模型[J]. 计算机研究与发展，2006，43(6)：1050-1057

[12] Bandmann O, Dam M, Firozabadi BS. Constrained delegation[C]// Proc. of the 23rd Annual IEEE Symp. on Security and Privacy. Oakland：IEEE Computer Society Press, 2002：131-143

[13] 李晓峰，冯登国，何永忠. XACML Admin 中的策略预处理研究[J]. 计算机研究与发展，2007，44(5)：729-736

(上接第 40 页)

站点数量对站点响应时间的影响如图 7 所示。由图可见：子网 A 从属站、A 网主站 E_1、主网主控站的响应时间受站点数量的影响较大，且随着站点数量的增加而变大。原因是上述 3 个站点转发消息时，均是从属站，其消息的发送受主控站点的控制。随着站点数量的增加，被轮询到的周期也逐渐变大，使得响应时间变大。而主控站由于可以自主控制数据的发送，其响应时间较小且基本不受站点数量的影响。

结束语 战术数据链系统时延指标受系统资源分配、服务规则、网络容量、消息传输方式以及所传输消息的特点等多种因素影响，可以说时延指标在一定程度上反映了战术数据链系统的整体性能。作战单元通过战术数据链系统传输消息时，过大的时延会影响基于这些消息的特定应用。以现代空战为例，飞机飞行速度达到音速或亚音速时，如作战单元之间传输定位信息的延迟为 1s，则由此引起的定位误差可能达到数百米。因此，作战过程中应依据作战需求合理确定站点数量，选择合适的消息传输方式，使消息具有较好的时效性。

参 考 文 献

[1] 任培，周经伦，罗鹏程，等. 美军数据链发展概况与启示[J]. 装备指挥技术学院学报，2008，19(1)：43-47

[2] 王文政，周经伦，罗鹏程，等. 战术数据链仿真综述[J]. 系统仿真学报，2008，20(14)

[3] 陈敏. OPNET 网络仿真[M]. 北京：清华大学出版社，2004

[4] 孙义明，杨丽萍. 信息化战争中的战术数据链[M]. 北京：北京邮电大学出版社，2005

[5] 崔昊，匡镜明，何遵文. Link16 与 VHF 数据链互连建模与仿真研究[J]. 计算机工程与设计，2007，28(5)：1119-1122

[6] 梅文华，蔡善法. JTIDS/Link16 数据链[M]. 北京：国防工业出版社，2007

[7] 任培，周经伦，罗鹏程，等. 基于排队论的数据链系统信息传输时间延迟分析[J]. 计算机科学，2008，35(8)：93-94

[8] 田斌鹏. 战术数据链实时性研究[D]. 成都：西南交通大学，2007