第34卷 第20期 计 算 机 工 程 2008年10月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0180—04 文献标识码：A 中图分类号：TP309.08

P2DR模型中策略部署模型的研究与设计

韩锐生，徐开勇，赵 彬
(解放军信息工程大学电子技术学院信息安全研究所，郑州 450004)

摘 要：分析动态自适应网络安全模型P2DR的缺陷，提出对P2DR模型的几点改进建议。针对模型中策略相关不足设计了一个策略部署模型，该部署模型实现了策略统一定制、自动分发、自适应管理等功能，同时在部署模型中引入了安全事件关联分析的思想，共享设备间安全信息以实现安全策略的联动操作，达到安全事故及时响应的目标。该部署模型实现了P2DR模型的动态性和自适应以及策略核心作用。
关键词：部署模型；自适应管理；策略联动；安全事件关联

Research and Design of Policy Deployment Model for P2DR Model

HAN Rui-sheng, XU Kai-yong, ZHAO Bin
(Information Security Institution, Electronic Technology Academy, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】This paper analyzes the insufficiency of dynamic adaptation network security model P2DR, and asserts some improved proposal for P2DR. A policy deployment model is designed on the insufficiency of policy for P2DR model. Deployment model provides the policy uniform defines, automatic distribution, self-adaptive management functions and so on. The security event coordination analysis is introduced in the deployment model. The model shares the security information between devices in order to realize cooperation of security policies, and achieves the goal of reposing security incident in time. The significance of deployment model is really realizing the dynamic and adaptive of P2DR model, and it makes the core effect of policy realized.
【Key words】deployment model; self-adaptive management; policy linkage; security event coordination

1 概述

以安全策略为中心的P2DR模型(如图1所示)是动态自适应网络安全模型的代表性模型，也是目前国内外在信息系统中应用最广泛的一个安全模型。根据P2DR模型(Policy, Protection, Detection, Response)构筑的网络安全体系，能够在统一安全策略(Policy)的控制和指导下，在综合运用防护工具(Protection，如防火墙、身份认证、访问控制等)的同时，利用检测工具(Detection，如漏洞评估、入侵检测系统)了解和判断网络系统的安全状态，并通过适当的响应(Response)措施将网络系统的安全性调整到风险最低的状态。防护、检测和响应组成了一个完整的动态安全循环。P2DR模型是一个动态性、过程性的抽象安全模型，体现了安全管理、按需安全的思想，但在实践指导中策略的核心作用并没有真正得以发挥，策略在模型中仅是以概念的形式存在，没有具体的部署管理体系。

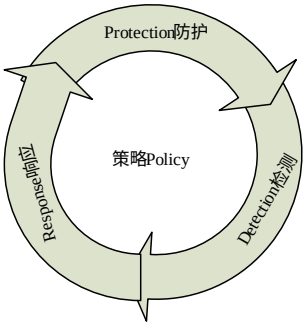

图1 P2DR动态自适应网络安全模型

2 P2DR模型的不足与改进

2.1 模型不足

按照P2DR的观点，一个良好完整的动态安全体系，不仅需要恰当的防护，而且需要动态的检测机制，在发现问题时还需要及时做出响应，这样的一个体系需要在统一、一致的安全策略的指导下进行实施，由此形成一个完备的、闭环的动态自适应安全体系。然而，在现实应用中P2DR模型并没有完成其应有的功能，模型中的安全策略没有实质的内涵，策略的真正指导作用存在缺陷。这导致P2DR动态安全模型中的各种安全组件仍然是相互独立的功能模块，只能依赖人为因素的参与来实现动态的安全循环。更深入地考虑P2DR动态安全模型的缺陷，可以总结出以下3点：

(1)策略核心没有相应的策略部署、实施平台给予支撑，无法实现真正意义上的基于策略的网络安全管理；

(2)对动态网络安全的支持不足，自动化程度很低，安全事件的响应过程总是需要人为参与，响应速度慢、效率低、准确度差；

(3)由于没有统一的管理平台，对大规模分布式系统的管理开销过高导致其可实现性很差，并且不能实现安全体系内部的信息共享和协作。

可见，策略核心的先天缺陷导致了P2DR动态安全模型

基金项目：国家部委预研基金资助项目
作者简介：韩锐生(1982－)，男，硕士研究生，主研方向：网络信息安全，安全策略系统；徐开勇，研究员；赵 彬，博士研究生
收稿日期：2007-11-06 **E-mail：**hrsgcxqq@sina.com

不能够满足当前安全信息系统的需求，需要对模型的策略核心进行改进，从而实现模型期望的目标。

2.2 模型改进

根据 2.1 节描述的 P2DR 动态安全模型缺陷，对模型进行了如下的改进：

(1)构建策略部署、管理体系结构；在结构中实现策略的自动分发、自动执行和运行时的自管理，使策略核心能够实现用户的操作行为和系统管理动作，满足用户意图及真正指导各安全组件的行为，实现基于策略的网络安全管理。

(2)引入策略自适应管理、策略联动和安全事件关联分析的思想，满足网络安全的动态性；这里的动态性主要表现在以下 3 个方面：1)依靠策略联动和安全事件关联分析的方法，实现由防护、检测和响应组成的动态安全循环，从而来保障网络安全；2)网络安全的目标是动态变化的，支持部分或者全网范围内安全级别的动态调整；3)安全目标实现所依赖的网络物理环境是动态可调整的，网络的安全策略要能够迅速、方便地做出调整以适应新环境下的安全需求。

(3)添加统一管理控制台，实现对分布的被管对象和安全策略进行管理，统一定制安全策略，统一收集各被管对象的安全事件信息，并引入“域”概念，有效地组织被管对象，实现被管系统的伸缩性，同时，实现了安全体系内部信息的高度共享和协作。

通过对模型的改进，设计了一个囊括以上建议的策略部署模型，改进的模型能够对整个网络中各种安全组件进行分布式、动态的、基于策略的管理，具有良好的可伸缩性，满足了动态网络安全的需求，提高了管理自动化的程度，同时还为各种安全组件提供了良好的信息共享和协作平台，具有较高的实用价值。

3 策略部署模型设计

3.1 部署模型逻辑结构

图 2 是本文设计的策略部署模型示意图。

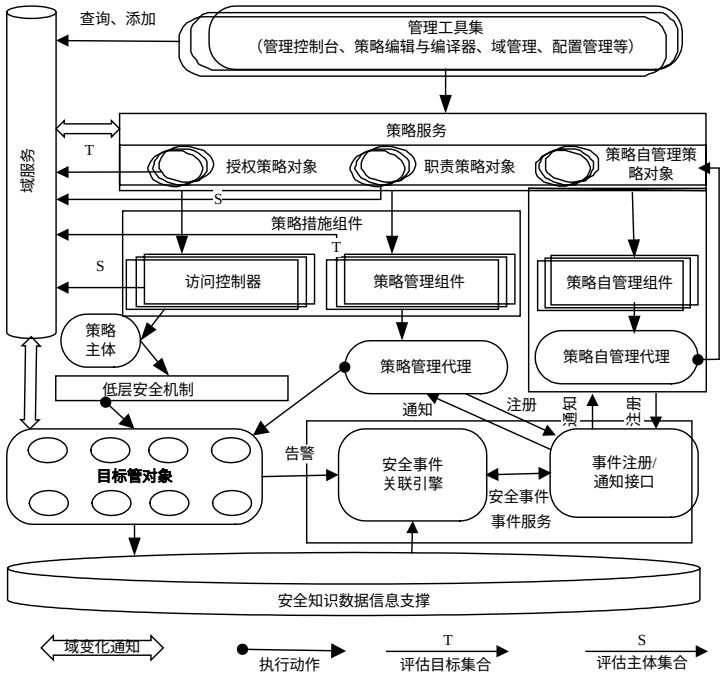

图 2 部署模型示意图

本策略部署模型借鉴了英国皇家学院Dulay等人提出的基于Ponder策略语言[1-2]的策略部署模型，在Ponder部署模型的基础上，引入了策略自管理[3]、策略联动和安全事件关联分析的思想。策略部署模型与底层的策略实施机制无关，能够应用在混合策略环境中。策略部署模型支持策略的实例化，支持策略对象的分发、启用、禁用、卸载以及删除，自动化地实施组件实施策略，能够根据域内成员关系的变化对策略实施做出相应的调整，为策略的动态自管理提供了更完善的支持。部署模型为P2DR 网络安全模型提供基于策略的安全事件处理和散发能力，提高了策略管理自动化的程度，使改进后网络安全模型具备了良好的可伸缩性和可扩展性以适应不同规模企业网络的需要。

3.2 模型的几点说明

(1)管理控制台：为用户提供图形化的管理界面，提供策略管理、配置管理功能，为系统管理员提供编辑、编译、浏览策略和安全事件查看等接口。

(2)策略服务：策略管理的接口，它存储编译好的策略类、创建并分发新的策略对象，在模型中提供了 3 种类型的策略对象，即授权策略对象(APO)、职责策略对象(OPO)和策略自管理策略对象(PSMPO)。策略服务为每个策略对象创建相应的策略控制对象，对策略对象进行运行的管理；同时策略服务器内存在一个策略自管理代理(PSMA)模块，PSMA 实现管理自管理。

(3)域服务：管理域对象的层次结构并支持运行时主体和目标集的有效性评估；域服务监控域变化并向策略控制对象进行及时通知；域服务通过 LDAP 目录服务实现。域这种管理对象的组织方式使一个策略可以应用于多个被管对象上，大大提高了被管系统的可伸缩性。

(4)事件服务：收集系统事件和系统中被管对象发布的事件，并将它们通知给已预定该事件的策略管理组件，以触发职责策略。在事件服务中，集成开发了一个安全事件关联引擎，引擎收集各安全设备的关键信息如 IDS 的告警信息、防火墙的日志信息等，利用关联方法对来不同设备、不同边界、不同时间段的日志信息进行关联分析，准确检测已知攻击，发现未知攻击；降低了误报，减小了漏报，从而缩短了响应时间。

(5)策略实施组件和代理：负责装入、卸载、启用、禁用执行对象，PMA 和 PSMA 通过通告/预定接口向事件服务注册事件。访问控制器 AC 通常负责保护它管辖范围内的所有目标，截获授权策略对目标采取的行为，检查行为是否允许；PMA 直接执行所有的义务和抑制策略。PSMA 实施策略自管理操作。

4 部署模型关键技术实现

4.1 策略自动分发

策略的分发是由策略服务发起的，首先，策略服务创建编译新的策略对象，并将其存储在域服务中；其次，从域浏览器中选择将要发布的策略对象，并生成相应的策略控制对象(PCO)，PCO 对该策略对象进行运行时的管理；最后，当管理员执行一个加载请求时，PCO 对策略应用的对象集和主体集进行避免策略和职责策略评估，对目标集进行授权策略评估，并将对应的策略对象分发给负责实施策略的所有实施组件。enable, disable and unload 操作同样被 PCO 转发给所有实施组件。除分发策略对象外，PCO 还将策

略与策略应用的域对象关联起来。这使得当域发生改变时，域服务能够通知 PCO，从而实现对新加入实施组件自动加载策略及自动从实施组件删除不再应用的策略。其详细流程如图 3 所示。

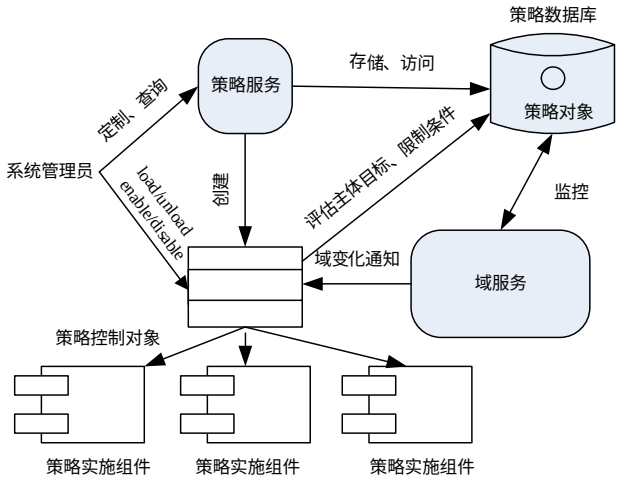

图 3　策略自动分发示意图

4.2　策略实施

根据策略的实施对象将策略分为主体策略和客体策略，部署模型中提到的授权策略属于客体策略，而职责策略和策略自管理策略属于主体策略。客体策略的策略主体是任何发起调用的对象，在该模型中，授权策略的实施组件称作访问控制器(AC)，访问控制器通常保护其所处位置上的所有目标，并实施所有与其相关的授权策略，执行访问控制的低层访问控制机制(如防火墙、操作系统或数据库管理系统等)接口，其实施细节如图 4 所示。对于主体策略而言，定义了职责策略和策略自管理策略，由于策略自管理策略与职责策略有实质的区别，因此本文仅介绍职责策略的实施，策略自管理策略的实施在 4.3 节将做详述。在该模型中，职责策略的实施组件称作策略管理代理(PMA)，PMA 解释并执行策略定义行为，其实施细节如图 5 所示。

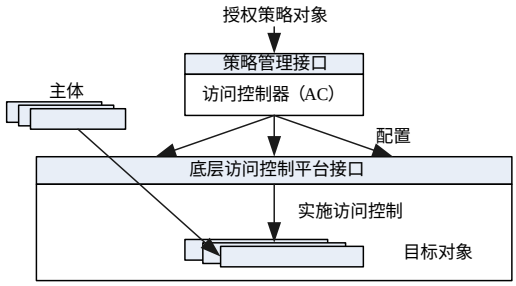

图 4　访问控制实施

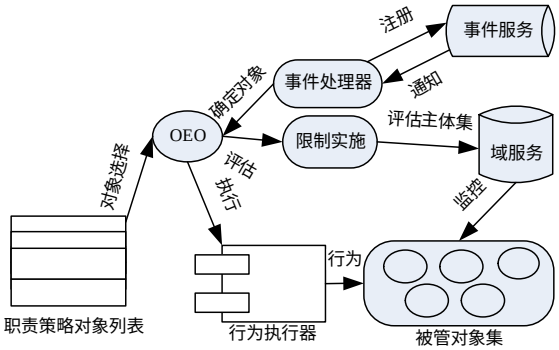

图 5　职责策略实施

4.3　策略自管理

针对大部分策略语言在动态自适应管理方面的不足，重新设计了策略自管理策略，策略自管理策略根据所作用的对象不同可分为：授权策略的自管理策略和职责策略的自管理策略，新类型策略的主客体都是策略服务，该类型策略从创建、分发到执行、停止都在策略服务内完成。在部署模型中，负责实现策略动态自管理的组件被称为策略自管理代理(PSMA)，PSMA 作为一个模块运行于策略服务器中，因此，策略自管理策略对象在实施之前是不需要分发的。PSMA 也要向事件服务注册关心的事件，并在接收到相应的事件之后执行策略自管理策略中规定的措施，但是 PSMA 所要执行的措施必须向策略服务提交。策略自管理措施执行的流程如图 6 所示。

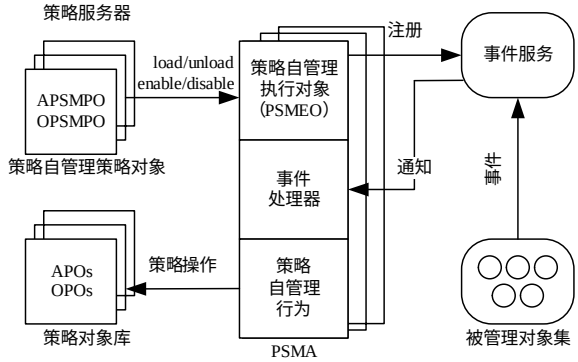

图 6　策略自管理措施执行的流程

策略自管理使部署模型具有了完善的动态自管理能力，是实现 P2DR 网络安全模型的动态性，使之具备自适应能力的关键部件。

4.4　策略联动

策略联动机制是部署模型实现自动响应的关键部件，一个策略成功实施能够实现多个策略的连续触发。当一个攻击事件发生，运用策略的联动机制可以同时实现报告管理员、关闭攻击源连接、配置部署在不同边界的防火墙等动作，尤其对于分布环境中，因为各安全产品部署在不同的边界，安全事件的及时响应很困难，这就要求必须采用高效自动的响应措施，使用联动机制可以满足以上要求，可见在大规模分布式系统基于策略的管理中策略的联动操作是很必要的。

在部署模型中，把攻击响应预案以策略模板的形式定义，当一个攻击发生时触发相应的策略模板，在策略模板中定义的各响应策略联动操作，实现安全事故的自动响应。策略模板的定制一方面根据的安全需求、常见攻击模式及防病毒措施等，另一方面根据安全事件关联模块的异常现象和复杂攻击。策略模板由策略服务维护，并根据需要分发给相应的实施代理。

当网络出现异常时，安全事件关联模块对告警信息进行关联分析，将多个来自不同安全设备的事件合并和过滤后形成一个准确的事件报告，事件服务接收安全事件触发并查找与之相应已注册的策略实施代理，如果没有与之相应的策略实施，将与策略服务进行交互得到或重新定制策略模板，利用安全事件参数将模板进行实例化，并自动分发到相应的策略实施代理上，策略实施代理处理事件响应，根据安全事件触发的限制策略或职责策略，执行策略定义的动作完成对事件的响应。

响应过程如图 7 所示。

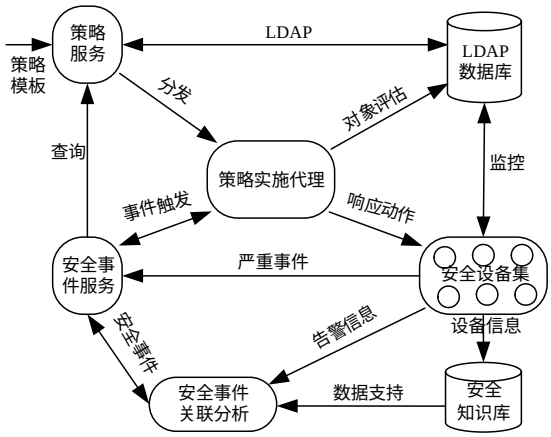

图 7　策略驱动响应过程

5　策略部署模型应用

根据改进的动态网络安全模型 P2DR，结合策略部署模型设计，实现了一个策略驱动的一体化网络安全管理系统，其逻辑示意图如图 8 所示。

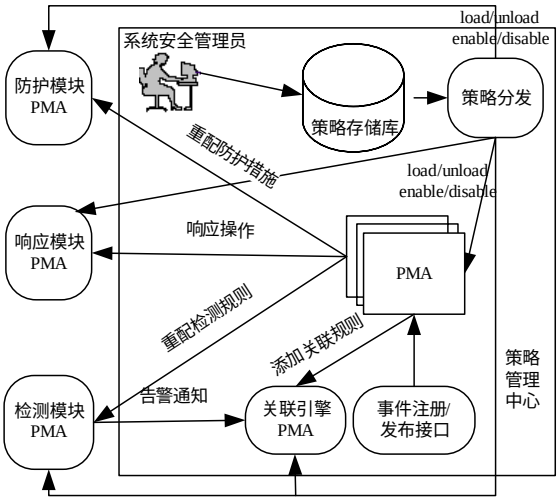

图 8　网络安全管理系统示意图

策略管理中心是该系统的核心，它分别与部署在防护模块、检测模块和响应模块的 PMA 进行通信，使用 Java RMI 机制实现远程通信和分布式操作。策略管理中心由系统安全管理员统一定制安全策略模板，自动分发给各相应模块的 PMA，当中心事件服务收到安全事件后，触发部署在 PMAs 上的策略模板，策略模板指导响应模块进行攻击响应和系统恢复，并对防护模块进行新安全措施的部署，同时对检测模块加强检测规则配置，如果相当一段时间内攻击现象不再发生，策略管理中心可停止策略模板的响应措施，并记录系统的当前的安全状态，向系统安全管理员进行报告。

以简单 Web 服务攻击防御为例来介绍系统的运行细节。当检测模块检测到一个 Web 攻击时，并向策略管理中心告警，告警信息进入安全事件关联引擎，计算告警的严重度与可能性，并重新配置信息收集器以获得更多的攻击特征，从而减少误报的机率。如果攻击的可能性和严重度很高，则事件服务通过事件通知接口通知响应模块的 PMA 触发相应的响应机制。针对 Web 服务攻击，有效的响应机制应该包括以下几个步骤：(1)向安全管理员报警，包括所影响的资产和资产安全状况；(2)关闭攻击源和受害对象的 TCP 连接，通过在 TCP 连接中加入 TCP FIN 或 RST 包实现；(3)重新配置防火墙规则，拒绝所有来自攻击源的连接请求；(4)重新配置检测模块的检测规则，挖掘告警的上下文信息，获得更多的攻击特征。

当检测到一个 Web 服务攻击且攻击的可信性大于预定义的攻击可信级别，将触发响应策略进行关闭 TCP 连接和重新配置防火墙规则，策略模板定制如下：

```
Inst oblig /SMPolices/signatureBasedAlert {
  on      WebAttack(attackSignature, confidence);
  subject          /PMA/SM;
  target       t=/PMA/DM;
  do      t.reConfigureDM(DecRules)->
  t.getContext(attackSignature);
  when  confidence <MIN_CONFIDENCE;}
Inst oblig /SMPolices/signatureBasedAlertRe {
  on      WebAttack(attackSignature, confidence);
  subject      /PMA/SM;
  do      getRisk(attackSignature)->
  alert(attackSignature)->
  generateEvent(AlertRespond,attackSignatue)->generateEvent
(reConfigFW,attackSignature);
  when  confidence >MIN_CONFIDENCE;}
Inst oblig /SMPolices/signatureBasedAlert SR{
  on          AlertRespond(attackSignature);
  subject          /PMA/RM;
  target       t=/PMA/SEVER
  do t.CloseConnection(attackSignature); }
Inst oblig /SMPolices/signatureBasedAlertFW
{ on          reConfigFW (attackSignature);
   subject          /PMA/PM;
   target          t=/PMA/FW;
   do          t.deny(attackSignature);}
```

在现实系统中已经实现了漏洞扫描工具 Nessus、入侵检测系统 Snort 和 NetScreen 防火墙的联动防御操作，利用 Nessus 扫描发现重要主机存在的漏洞信息，Snort 检测的告警信息与漏洞信息进行匹配，计算攻击的严重度，过滤到大部分误警，对严重事件进行阻击，在 NetScreen 上重新配置拒绝连接规则。运行结果表明，通过与漏洞信息等网络模型信息的关联，Snort 的误警率大大降低，过滤掉了 95%的告警信息，成功准确地防御了一些知名的漏洞相关攻击。

6　结束语

本文的策略部署模型对其他基于策略的系统有一定的借鉴意义。下一步的工作重点是利用策略自管理机制解决策略冲突，保障策略管理系统准确有效地运行。

参考文献

[1] Damianou N, Dulay N, Lupu E. Ponder: A Language for Specifying Security and Management Policies for Distributed Systems[D]. London, UK: Department of Computer, Imperial College of Science Technology and Medicine, 2000.

[2] Dulay N, Lupu E, Sloman M. A Policy Deployment Model for the Ponder Language[C]//Proc. of IFIP/IEEE International Symposium on Integrated Network Management. Seattle, USA: [s. n.], 2001: 529-543.

[3] 杨海松, 基于策略管理的分布式、动态网络安全模型[D]. 合肥: 中国科技大学, 2003.