文章编号:1001 - 9081(2009)09 - 2315 - 04

网络安全组件协同操作研究

杨宏宇,邓 强,谢丽霞
(中国民航大学 计算机科学与技术学院,天津 300300)
(yhyxlx@ hotmail. com)

摘 要:当前网络环境中安全组件难以实施统一的安全策略,无法充分发挥网络安全防护的整体优势。提出一种基于安全域分层思想的协同操作模型,采用三层结构、两级管理模式,以安全域作为实现功能的最小单元实现安全组件间的协同和管理。采用基于可扩展块交换协议(BEEP)框架的入侵检测交换协议(IDXP)实现对入侵检测消息交换格式(IDMEF)消息的传递。仿真实验结果表明,提出的安全协同操作模型和 IDXP 可以有效实现网络安全组件间的信息传输和协同操作。

关键词:网络安全;协同操作;组件;协同响应;安全域
中图分类号: TP393.08; TP309.2 **文献标志码**:A

Research on collaborative operation of network security components

YANG Hong-yu, DENG Qiang, XIE Li-xia
(*School of Computer Science and Technology, Civil Aviation University of China, Tianjin* 300300, *China*)

Abstract: Nowadays, it is very difficult for various network security components to adopt unified security policy in one network environment, which results in not fully taking advantage of the whole network protection. The authors presented a cooperative model based on security domain layer with three-layer structure and two-class management. The security domain was used as the fundamental unit to implement collaboration and management, and an Intrusion Detection Exchange Protocol (IDXP) protocol based on Blocks Extensible Exchange Protocol (BEEP) frame was implemented to transmit Intrusion Detection Message Exchange Format (IDMEF) messages. The experimental results demonstrate that this model and IDXP can effectively implement message transmission and collaborative operation.

Key words: network security; collaborative operation; component; cooperative response; security domain

0 引言

随着网络安全技术的发展,网络安全系统的种类越来越多,先后出现了防火墙、入侵检测、漏洞扫描等多种软、硬件网络安全设备与系统。但是这些网络安全系统一般只侧重于网络防护的某一方面,它们之间缺少协同操作机制,难以实施统一的安全策略,无法发挥整体优势,降低了网络的整体防御能力。因此,如何充分利用网络安全系统和组件,提高防御体系的整体防御能力,构建有效的协同式安全防御机制是信息安全领域的研究热点。

美国加州大学 Davis 分校计算机科学实验室提出了一种通用入侵检测框架(Common Intrusion Detection Framework, CIDF)。CIDF 讨论了有关入侵检测系统协同的问题,包括场景和通用入侵说明语言(Common Intrusion Specification Language, CISL)。前者是对入侵检测系统组件间可能协同方式的划分,后者则提供了系统事件、分析结果及响应指示的通用表示[1-2]。

在网络安全防护系统中,协同操作就是指在防火墙、入侵检测系统、防病毒系统、VPN 安全网关、网络安全评估系统等安全组件之间建立一种关联和互动机制。通过这种机制,它们之间可以自由交换信息,相互作用和相互影响[3-4]。

入侵检测交换协议(Intrusion Detection Exchange Protocol, IDXP)是一个用于入侵检测实体之间交换数据的应用层协议,能够实现入侵检测消息交换格式(Intrusion Detection Message Exchange Format, IDMEF)消息、非结构文本和二进制数据之间的交换,并提供面向连接协议之上的双方认证、完整性和保密性等安全特征,可以作为安全组件协同操作模型的通信协议。

本文提出了一种基于安全域分层思想的协同操作模型,并在该模型中采用基于可扩展块交换协议(Blocks Extensible Exchange Protocol, BEEP)框架的 IDXP 传输协议实现对 IDMEF 消息的传递。

1 协同操作模型设计

1.1 协同操作模型体系结构

为了解决网络安全组件的协同操作问题,设计了网络安全组件的协同操作模型(如图 1 所示)。该模型采用三层结构、两级管理模式,以安全域作为实现功能的最小单元,将网络中的安全组件按照一定的规则划分到多个安全域[5-6],[7]107-108中,其中安全组件的数量和种类在每个安全域中都不尽相同。在安全域内设立域管理中心对安全组件进行管理。系统管理中心是协同操作模型的核心,负责对各个域

收稿日期:2009 - 03 - 30;**修回日期**:2009 - 05 - 14。 **基金项目**:国家自然科学基金资助项目(60776807);国家 863 计划项目重点课题(2006AA12A106);天津市科技支撑计划重点项目(07ZCKFGX01700);民航科技基金资助项目(RKXZY0814);中国民航大学科技基金重点项目。

作者简介:杨宏宇(1969 -),男,吉林长春人,教授,博士,主要研究方向:网络与信息安全、民航信息系统分析与设计; 邓强(1982 -),男,山西平遥人,硕士研究生,主要研究方向:信息与网络安全; 谢丽霞(1974 -),女,重庆人,副教授,硕士,主要研究方向:信息与网络安全。

管理中心的管理。

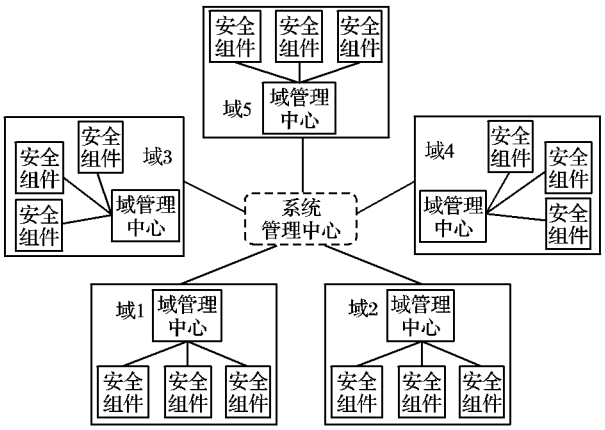

图1 安全组件协同操作模型结构

系统管理中心是模型的管理核心，负责对各个域管理中心的报告进行收集、分析，形成整个网络的安全态势[7]109-110，做出预警与响应。

域管理中心是安全组件协同框架中的重要组件，是每个域的核心。负责接收、汇总、分析其范围内安全组件的报告，做出响应决策[7]112-117，并向系统管理中心报告情况。

安全组件是各种网络安全设备，如：防火墙、入侵检测系统、防病毒系统、漏洞扫描系统或审计系统等，它可以是一个系统中的进程，也可能是一个硬件设备。安全组件负责监控所在网络的安全状态，当检测到入侵或信息安全事件时，在域管理中心的指导下做出恰当的响应。

1.2 安全域内部结构

一个典型的安全域内安全组件部署方案如图2所示。用户和工作系统包括个人PC、邮件服务器、数据库和其他信息系统，是被保护的对象。在协同操作模型中，安全组件在域管理中心管理下工作，根据防御、检测机制对用户和工作系统进行保护，在协同操作机制的指导下进行相互协作。

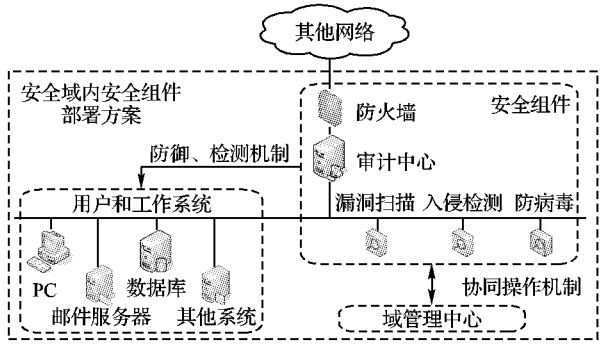

图2 安全域内安全组件部署方案

1.3 域管理中心

在协同操作模型中，域管理中心是安全组件的直接管理机构。本文设计的域管理中心结构如图3所示。域管理中心包括若干功能模块，按照功能的不同，将其分成三层：服务层、控制层、数据存储层。服务层包括通信模块、日志模块、组件管理模块、协同模块、数据分析模块和响应模块；控制层包括消息解析引擎、服务匹配模块；数据存储层由目录服务器、知识库和安全策略库等组成，负责各种信息的存储。其中控制层是管理中心的核心，控制服务层提供服务，控制数据存储层进行数据访问、存储。

2 协同操作模型中的信息传输

2.1 IDXP框架

因特网工程任务组(Internet Engineering Task Force，IETF)的入侵检测交互格式工作组(Intrusion Detection Workgroup，IDWG)提出了IDMEF和IDXP[8]，IDMEF描述了用来表示入侵检测系统输出信息的一个数据模型；IDXP则描述了入侵检测实体间的交互协议，该协议提供了基于面向连接协议双向鉴别，完整性和机密性并支持IDMEF消息、非格式化文本和二进制数据的交换[9]。

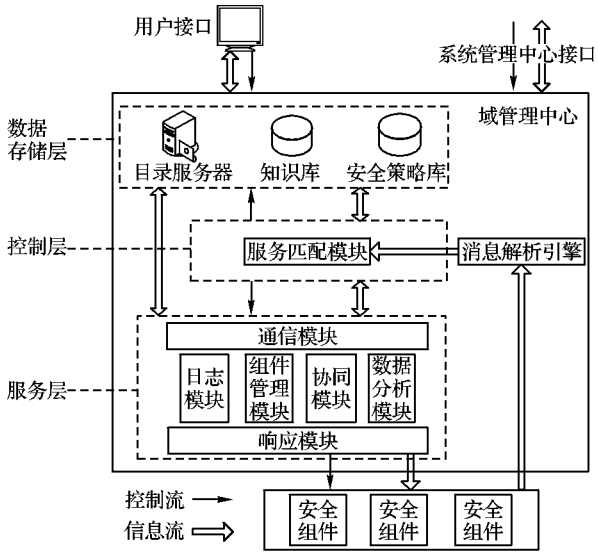

图3 域管理中心结构

IDXP框架提供了一种可以在对等体间交换信息的机制。BEEP协议可以根据框架定义产生一个应用层的隧道，继而在隧道中传送数据。IDXP也必须提供一个框架定义给BEEP协议，使BEEP协议可以控制IDXP隧道的产生[10-11]。

2.2 IDMEF消息传输的实现

在本文提出的协同操作模型中，IDXP主要负责IDMEF消息的传递，其中，报警消息由安全组件发送给域管理中心，而响应消息由域管理中心发送给执行响应的组件，故安全组件和域管理中心均有可能是通信的发起者，安全组件和域管理中心都需要设置监听端，以实现协同操作。

以两个安全组件和域管理中心的IDXP连接为例，IDXP实现信息传输过程如下。

1)安全组件A检测到安全事件，形成IDMEF报警，向域管理中心请求IDXP连接。

2)域管理中心接收到连接请求，同A建立连接，并接收IDMEF报警。

3)收到报警后，域管理中心对其进行解析，并进行策略匹配。

4)根据匹配的策略，需要将响应信息发送给安全组件B，域管理中心开始作为连接的发起端，同B建立新的IDXP通道。

5)安全组件B的监听端口收到连接请求，建立IDXP连接，接收IDMEF响应消息。

6)安全组件B对收到的响应消息进行解析，执行其中的命令。

本文设计的协同操作模型的 IDMEF 消息传输流程如图 4 所示。

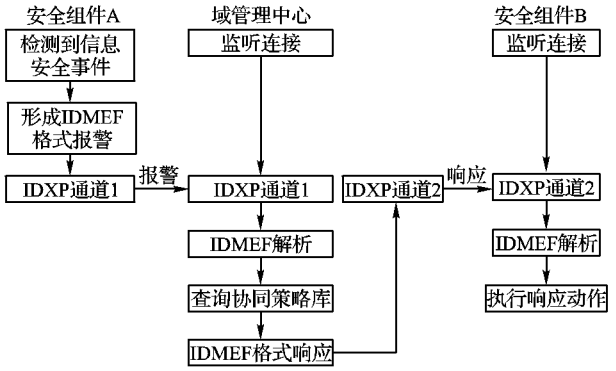

图 4　IDMEF 消息传输流程

3　仿真实验

在 BEEP-JAVA 的基础上,采用 Java 语言对 IDXP 协议进行编程实现,并实现了 IDXP 通道建立过程。

3.1　仿真实验系统结构

在实验室的局域网环境下进行仿真实验,使用一台 DELL 服务器模拟管理中心,三台 DELL PC 机模拟安全组件。仿真系统结构如图 5 所示。

A1 模拟域管理中心,负责接收安全组件发送的报警信息,进行策略匹配,将响应信息发送给相应的安全组件。A1 上部署的模块包括 IDXP 通信模块、协同操作模块和策略库(用 MySQL 数据库模拟)。B1、B2 和 B3 模拟安全组件向 A1 发送 IDMEF 报警消息,并接收来自 A1 的响应消息,部署 IDXP 通信模块。仿真系统部署说明如表 1 所示。

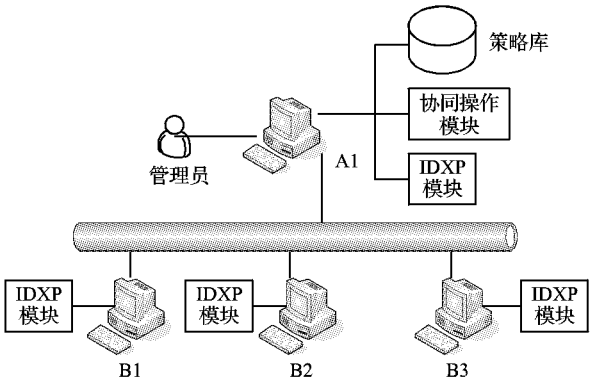

图 5　仿真实验系统结构

表 1　仿真系统部署情况

设备名称	IP	部署说明	功能说明
A1	10.6.233.158	MySQL 数据库, IDXP 通信模块、协同操作模块	模拟域管理中心, 接收安全组件报警, 进行协同操作响应
B1	10.6.233.51	IDXP 通信模块	模拟入侵检测系统
B2	10.6.233.22	IDXP 通信模块	模拟入侵检测系统
B3	10.6.233.53	IDXP 通信模块	模拟防火墙

在 MySQL 数据库中创建两张表:协同策略表和组件注册表。协同策略表用来存储协同策略,组件注册表用来记录安全域中注册的组件。

使用 IDMEF-JAVA 开源包中的标准 IDMEF 报警示例作为安全组件发送的报警消息。根据常见的报警类型,设计了常见报警类型及响应方式等协同策略,并将协同策略添加到数据库中的 Policy 表中。

3.2　仿真实验测试过程

1)开始监听。

管理中心运行协同操作模块与 IDXP 通信模块,开始在 3000端口监听客户端的连接。各客户端运行 IDXP 通信模块,在 3000 端口监听管理中心的连接请求。在 Eclipse 控制台中查看日志信息,各通信模块均开始监听。

2)安全组件发送报警消息。

B1 客户端向服务器请求 IDXP 连接,建立连接后,读取本地存储的“idmef_example_pingofdeath. xml”报警信息文件,并发送至域管理中心 A1。报警信息文件内容如下:

```
<IDMEF-Message version = "1. 0" xmlns = " urn: iana: xml: ns: idmef" >
  <Alert messageid = "abc123456789" >                    //消息类型
    <Analyzer analyzerid = "B1" >                        //分析器 ID
    </Analyzer >
    <CreateTime >
      2008 - 12 - 09T10: 01: 25. 93464
    </CreateTime >                                       //报警信息创建时间
    <Source ident = "a1a2" spoofed = "yes" >             //攻击者 IP
      <Node ident = "a1a2-1" >
        <Address ident = "a1a2-2" category = "IPv4-addr" >
          <address > 10. 6. 233. 22 </address >
        </Address >
      </Node >
    </Source >
    <Target ident = "b3b4" >                             //攻击目标 IP
      <Node >
        <Address ident = "b3b4-1" category = "IPv4-addr" >
          <address > 10. 6. 233. 51 </address >
        </Address >
      </Node >
    </Target >
    <Classification text = "Ping-of-death detected" >
                                                         //攻击类型判断
      <Reference origin = "cve" >
        <name > CVE-1999-128 </name >
        < url > http: //www. cve. mitre. org/cgi-bin/cvename. cgi?name = CVE-1999-128 </url >
      </Reference >
    </Classification >
  </Alert >
</IDMEF-Message >
```

安全组件发送报警消息过程的主要代码如图 6 所示。

安全管理中心 A1 收到该报警后,根据 < Classification > 标识的攻击类型匹配协同策略,并根据报警信息中的其他信息(如:攻击者的 IP 地址)产生响应策略实例,发送给需要执行响应的安全组件。

3.3　仿真实验结果及分析

模拟管理中心的 A1 和 B1 建立了 IDXP 连接,并收到了安全组件 B1 发送的报警信息,使用 XMLUtils 类在控制台输

出A1收到的IDMEF报警消息(如图7所示)。

经过比较,管理中心A1收到的报警消息与安全组件B1发送的报警消息内容一致,证明了IDXP传输协议的有效性。

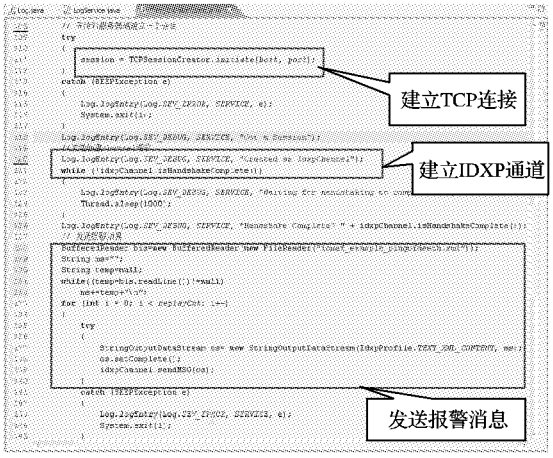

图6 客户端IDXP连接及发送IDMEF消息过程

图7 管理中心收到的报警信息

在数据库策略表,“Ping-of-death detected”报警信息对应的响应策略是:对报警信息<Source>标签中的IP采取屏蔽措施,时间为10 min,响应组件为该安全域中的防火墙组件。

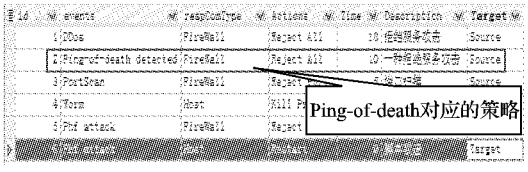

图8 Ping-of-death报警对应的策略

模拟网络防火墙的B3客户机收到了管理中心发送的响应消息,其内容如图9所示。

在响应消息中显示了如下信息:消息来自A1,响应目标为IP地址为10.6.233.53的防火墙,响应动作为屏蔽(Reject All)10.6.233.22的连接请求10 min。这些信息和策略库中“Ping-of-death”报警消息应采取的策略相吻合,证明了本文实现的协同机制的有效性。

4 结语

为了适应网络技术的发展,提高网络的整体防御能力,本文在分析网络安全组件协同技术研究现状的基础上,提出了一种基于分层思想的网络安全组件分层协同操作模型,采用Java语言对IDXP传输协议在该模型中进行了系统实现,采用关键字匹配的方法实现了基于策略的协同响应机制,并进行了仿真实验。结果表明该模型具有配置灵活、易于管理、主动性强等特点,IDXP协议在网络多安全组件的协同操作中是可行的。

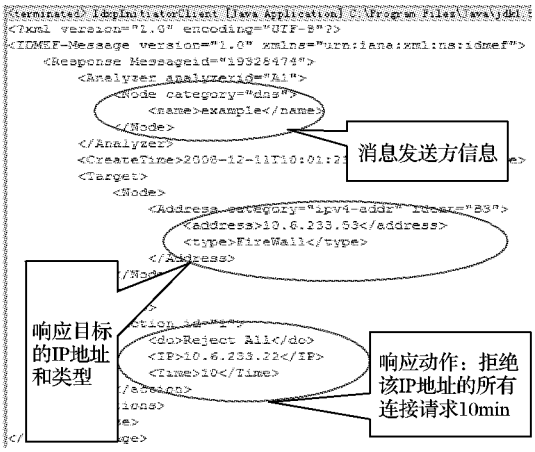

图9 响应消息界面

现实生活中,网络规模巨大,如何对不同的入侵检测系统之间报警信息进行聚合,如何有效减少重复和虚假警报[12],是下一步研究的重点。

参考文献:

[1] KAHN B, SCHNACKENBERG D. Communication in the common intrusion detection framework [EB/OL]. [2009 - 01 - 05]. http://www.isi.edu/brian/cidf/drafts/communi-cation.txt.

[2] FRICKE D, TOBIN D, MCCONNELL J. A framework for cooperative intrusion detection [C]// Proceedings of the 21st National Information Systems Security Conference. Arlington, Virginia, USA: [s.n.], 1998: 361 - 373.

[3] 段倩,周华春,刘颖,等.一种资源协同的分布式网络安全审计体系[J].北京交通大学学报:自然科学版,2007,31(5):39 - 43.

[4] 周慧芳,张亚玲,王尚平,等.协议分析与模式匹配相结合的IDS的设计研究[J].信息技术,2008,32(8):14 - 17.

[5] 韩宗芬,陶智飞,杨思睿,等.一种基于自治域的协同入侵检测与防御机制[J].华中科技大学学报:自然科学版,2006,34(12):53 - 55.

[6] 张亚平.基于分布智能代理的自保护系统研究[D].天津:天津大学,2005.

[7] KIM D, JUNG Y, CHUNG T. PRISM: A preventive and risk reducing integrated security management model using security label [J]. Journal of Super Computing, 2005, 33(1): 103 - 121.

[8] FEINSTEIN B, MATTHEWS G. The intrusion detection exchange protocol (IDXP), RFC4767 [EB/OL]. [2009 - 01 - 07]. http://www.ietf.org/rfc/rfc4767.txt.

[9] 杨莘,刘振华.入侵检测系统的比较[J].计算机工程,2004,30(6):137 - 138.

[10] ROSE M. The blocks extensible exchange protocol core [EB/OL]. [2009 - 01 - 05]. http://www.rfc - editor.org/rfc/rfc3080.txt.

[11] 汪晓东,朱淼良.基于IDXP的网络安全防卫系统[J].计算机工程,2005,31(7):151 - 154.

[12] 郭帆,叶继华,徐敏.基于IDMEF和分类的报警聚合[J].计算机应用,2008,28(1):250 - 253.