文章编号:1001-9081(2010)06-1475-05

网络安全组件间协同响应机制研究

谢丽霞,李学菲,杨宏宇

(中国民航大学 计算机科学与技术学院,天津 300300)

(lxxie@126.com; lixuefei135@163.com; yhyxlx@hotmail.com)

摘要:为解决由于组件间缺乏协同机制而无法充分发挥网络安全系统整体优势的问题,提出了一种基于策略的协同响应机制。基于策略驱动模型设计安全组件间的协同响应过程,通过对入侵检测消息交换格式(IDMEF)的扩展实现协同消息,采用块可扩展交换协议(BEEP)框架实现用于组件通信的入侵检测交换协议(IDXP),编程实现协同模块实施协同操作。运用该机制对网络安全组件的协同响应进行评估实验,获得各个阶段的时间开销。实验结果表明该机制能有效地实现网络安全组件的协同响应。

关键词:网络安全组件;协同响应机制;策略;入侵检测消息交换格式;入侵检测交换协议

中图分类号: TP309;TP393.08 **文献标志码:** A

Research on collaborative response mechanism of network security components

XIE Li-xia, LI Xue-fei, YANG Hong-yu

(School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: To solve the problem that the network security systems cannot play overall advantages due to the lack of coordination mechanism among components, a policy-based collaborative response mechanism was proposed. The process of collaborative response was designed with the policy-driven model. The Intrusion Detection Message Exchange Format (IDMEF) was expanded to be the collaborative message format. A Blocks Extensible Exchange Protocol (BEEP)-based Intrusion Detection Exchange Protocol (IDXP) was implemented to communicate among security components. The collaboration module was programmed to implement the collaborative operations. An evaluation experiment on the collaborative response of security components was performed with this mechanism, and the time costs of each process were obtained. The experimental results demonstrate that the mechanism can implement the collaborative response of security components effectively.

Key words: network security component; collaborative response mechanism; policy; Intrusion Detection Message Exchange Format (IDMEF); Intrusion Detection Exchange Protocol (IDXP)

0 引言

当今世界是一个以网络为中心的信息时代,随着网络技术的飞速发展和开放性应用,安全防御成为信息化必须解决的重要问题。网络安全防御围绕着如何检测网络情况,解决安全问题展开,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,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。

入侵检测消息交换格式(Intrusion Detection Message Exchange Format, IDMEF)是一种安全事件警报的标准格式,描述了表示入侵检测系统输出信息的数据模型,具有高度的抽象性和很好的扩展性,可以作为组件间统一的通信信息格式^[1]。

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 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响应机制的通信协议^[2]。

本文提出了一种基于策略的安全组件间协同响应机制,依据协同响应的需求对 IDMEF 进行了扩展,实现了基于块可扩展交换协议(Blocks Extensible Exchange Protocol, BEEP)框架的 IDXP 传输协议,在此基础上实现了安全组件间的协同响应机制。

1 基于策略的协同响应机制

1.1 策略驱动模型

策略广义上就是对一组规则和方法的描述,用以动态调整控制系统的状态与行为^[3]。在网络安全管理中,策略定义了对发生的某个或某些安全事件系统应采取的行为。在各种安全模型中,包括形式化安全策略模型如 BLP、Biba、Clark-Wilson 和非形式化的安全风险模型如 PDCA、P2DR、PDRR 等,安全策略都处于核心地位^[4]。基于策略的协同响应机制将系统视为一个状态机,策略则作为调整系统状态的依据。

收稿日期:2009-12-02;修回日期:2010-01-20。

基金项目:国家 863 计划项目(2006AA12A106);国家自然科学基金资助项目(60776807);天津市科技支撑计划重点项目(07ZCKFGX01700);中国民航科技基金资助项目(RKXZY0814);中央高校基本科研业务费中国民航大学专项项目(ZXH2009A006;ZXH2010D009)。

作者简介:谢丽霞(1974-),女,重庆人,副教授,主要研究方向:网络与信息安全;李学菲(1988-),男,河南新安人,硕士研究生,主要研究方向:网络与信息安全;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。

策略驱动模型如图1所示。图1中的状态A是初始状态,状态B是安全状态, P_0 是任务策略。该策略包含各扫描任务的启动计划,以及各扫描任务的启动配置参数。

在 P_0 的驱动下,网络安全系统应建立各种扫描任务,形成各种安全机制,由初始的“裸机”状态A进入相对安全的状态B,表示为 $AP_0 \rightarrow B$;在此状态下,系统发生了某种安全事件,导致系统进入一种危险状态,称为事件触发,表示为 $B_{E_i} \rightarrow C_i$,其中B为安全状态, C_i 为危险状态, E_i 为安全事件。在此状态下,系统执行了某种策略,导致系统恢复到安全状态,称为策略驱动,表示为 $C_i P_i \rightarrow B$,其中 C_i 为危险状态, P_i 为策略或策略集合。

图1 策略驱动模型示意图

1.2 协同响应过程设计

本文的协同响应机制基于管理中心实现。管理中心由信息分析模块、协同模块、响应模块等组成。当安全组件检测到安全事件后,将报警消息以IDMEF发送至管理中心;管理中心的信息分析模块对报警信息进行分析处理,形成对安全事件的综合判断^[3],并将该数据发送到协同模块,由协同模块继续处理。协同模块根据对安全事件的综合判断结果查询策略库,根据协同策略、访问控制策略、组件注册信息库检索结果,生成针对该安全事件的策略实例,由响应模块将策略实例填充到IDMEF响应消息中,发送给安全组件,指导其做出响应。

安全组件还可以将策略执行效果反馈给管理中心,由管理中心的信息分析模块对策略实例的优劣做出分析判断,形成新的策略供决策模块选用^[5]。安全组件的协同过程如图2所示。

图2 协同响应过程示意图

1.3 策略格式设计

在本文提出的协调响应机制中,以XML格式描述策略信息^[5-6]。策略消息内容包括策略的ID、策略类型、策略描述、策略触发规则、安全等级、执行策略组件、策略响应动作等。以端口扫描事件的响应策略为例:

```
<policy>
  <policy-id>32</policy-id>           //策略ID
  <policy-type>
    协同响应策略、访问控制策略
  </policy-type>                       //策略类型
  <description>
    对端口扫描行为进行干扰
  </description>                       //策略描述
  <events>
```

端口被扫描

```
</events>                             //策略触发规则
<level>1</level>                       //安全等级
<target>防火墙</target>               //执行策略组件
<actions>                              //响应动作
  <action>屏蔽端口</action>
  <time>10000</time>                  //时间特性
</actions>
</policy>
```

其中:策略描述说明了该策略的功能;events为触发规则,明确了策略触发的条件;actions为执行的动作。当需要对现有策略进行更新或者扩充新策略时,在保证策略的不可冲突和有效性的前提下^[5],修改或添加events、level、target和actions中相应参数,可生成新的XML文件,保证了系统的健壮性和可扩充性。

2 协同响应机制的实现

2.1 IDMEF扩展

标准的IDMEF消息仅适用于入侵检测设备和管理器间信息安全事件的描述,它缺少对信息安全事件的响应信息等的描述。本文对IDMEF进行了扩展,设计了安全事件响应消息类Response、协同请求消息类CooperationRequest、策略更新消息类PolicyUpdate和策略消息类Policy。所扩展的消息类均作为IDMEF的子类^[6-7],并使用IDXP协议传输。

2.1.1 响应消息

响应消息类对响应目标、响应周期、响应方式,及其他信息进行了说明。一个响应消息包含以下内容:

响应目标 指定执行该响应的安全组件,可以是确定的某个组件,也可以是某一类组件。

时间 指定响应的时间特性。响应可以是一段时期的持续状态,也可以是无持续性性的一个动作。

动作 即响应方式,包括产生安全报告、锁定用户、隔离IP、杀死进程、关闭端口、断开连接、关闭主机等。

其他信息 响应消息中包含的其他必要信息。

由于不同安全组件的响应方式各不相同,本文在Response类基础上创建了IDS、Firewall和Host等Response子类,使响应消息更具有针对性。

2.1.2 协同请求消息

当安全组件不能确定某个安全事件时,将请求管理中心进行协同分析,以确认该安全事件。为此,本文设计了一种协同请求消息。协同请求消息包含以下内容:

请求组件ID 请求协同的组件的标识,每个组件都有唯一的标识来使自己的身份,以便

于进行身份验证与访问控制。

协同请求 需要的协同操作,如数据请求、对可疑安全事件确认或补充等。

疑似安全事件描述 相关安全事件的信息,可以用报警信息进行描述。一个协同请求可能包含多个相关疑似事件的描述,所以一个协同请求可能包含多个报警信息。

其他信息 其他需要提供给管理中心的信息。

2.1.3 策略和策略更新消息

在协同响应的过程中,协同模块针对不同的安全事件从策略库中检索出相应的策略,并将其中的响应方式填充到响应消息中;在策略更新时,将新创建的策略完整地发送给安全组件,使其能够应对不断变化的安全事件。

策略更新消息对策略消息进行封装,并对策略消息的其他信息进行补充,如:策略创建者(人工创建、自动生成)、策略创建时间、策略的更新方式(添加、替换等)。

2.2 IDXP 协议的实现

协同响应机制的实现需要安全组件和管理中心间进行通信,以传递报警和响应等多种消息。IDXP 协议是一个用于入

侵检测实体之间交换数据的应用层协议,能够实现 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的双方认证,可作为安全组件间协同响应机制的通信协议。

本文在 BEEP-JAVA 的基础上,采用 Java 语言实现了 IDXP 协议,设计并实现了 IDXP 通道建立机制。IDXP 协议的实现类如图 3 所示。

图3 IDXP UML 类图

IdxpProfile 实现了 BEEP-JAVA 包中的 Profile 接口和 StartChannelListener 接口,通信监听端在接收到连接发起端的 IDXP 连接请求后,在 StartChannel() 方法中调用 IdxpChannelFactory 创建一个 IdxpChannel 实例。

IdxpChannelFactory 采用工厂模式^[10]对 IdxpChannel 类的构造方法进行封装,其 createIdxpChannel() 方法调用 IdxpChannel 的构造方法返回 IdxpChannel 的一个实例。

IdxpChannel 代表一个 IDXP 隧道,聚合了 BEEP-JAVA 中的 ChannelImpl 类和本文实现的 IdxpMessageListener 和 IdxpReply 类。通道创建成功后,通过 sendMSG() 方法传输数据,IdxpMessageListener 对象负责接收并处理 MSG 类型数据,IdxpReply 对象负责返回数据接收状态。

协同响应机制主要传递的是 IDMEF 格式消息和建立 IDXP 通道时的 Greeting 消息,通过对这些消息的比较,可以按照首元素名称的不同,实现流程控制。

Greeting 消息首行内容如下:

```
<IDXP-Greeting role="server" uri="http://example/IdxpDaemon"/>
```

IDMEF 消息的前两个内容如下:

```
<IDMEF-Message version="1.0" xmlns="urn:iana:xml:ns:idmef">
  <Response Messageid="19328474">
    <IDMEF-Message version="1.0" xmlns="urn:iana:xml:ns:idmef">
      <Alert messageid="123456789">
```

在监听端和连接发起端均使用 IdxpChannel 和 ChannelImpl、IdxpMessageListener、IdxpReply 类,实现 IDXP 隧道的信息传输,该过程的 UML 协作关系图^[11]如图 4 所示。

图4 IDXP 通道信息传输协作图

2.3 协同模块的实现

实现协同模块的 Java 类包括实体类和操作类两部分。实体类包括报警消息类、策略描述类和响应消息类。操作类包括数据传输类、数据解析类、数据库访问类、策略实例创建类和日志记录类等。协同响应机制的主要实现类如图 5 所示。

数据传输类由 IDXP 实现,在 IdxpMessage-Listener 类中增

图5 协同响应实现类

加一个数据解析类的对象引用,可将 IDMEF 格式数据流传递给数据解析类。

数据解析类 dataParser 主要负责 XML 数据对象和报警对象的互相转换,并调用 responseCreateAction 类的成员 rca 获得创建好的响应消息。其主要代码如下:

```
public dataParser
{
    private responseCreateAction rca;

    //关联一个响应创建类对象

    //XML 转换成 IDMEF 对象
    public Idmef convertToIdmef (org.w3c.dom. document) {}
    //IDMEF 对象转换成 XML
    public org.w3c.dom. Document convertToXML (Idmef idmef) {}
    public void getResponse (Idmef idmef)
    {
        rca.createResponse (idmef); //创建 Response 对象
        ...
    }
}
```

响应生成类 responseCreateAction 创建一个 Response 对象,并委托数据库访问类进行策略和组件信息的查询,将查询结果集中的信息赋值给 Response 对象相应成员;将该 Response 对象传递给数据解析类。

数据库访问类由策略查询类 PolicyDAO 和组件信息查询类 ComponentsDAO 两个类构成,提供查询策略数据库和组件注册信息库的各种方法。根据 IDMEF 报警对象的类型,提取关键字段进行数据库查询操作。

日志记录类在其他类相关方法中增加监视代码,检测它们的方法调用,执行信息记录。

3 仿真实验

3.1 仿真系统设计

在局域网环境中进行仿真实验。在实验环境中,将模拟管理中心部署到一台 DELL 服务器 A1,将安全组件部署到 3 台 DELL PC 机 B1、B2 和 B3。管理中心负责接收报警信息,进行策略匹配并向安全组件发送响应信息。仿真系统结构如图 6 所示。

图 6 仿真系统结构

安全组件向管理中心发送 IDMEF 报警信息,并接收来自管理中心的响应消息。将本文实现的 IDXP 通信模块(包括 IDXP 协议和扩展后的 IDMEF)分别部署到 A1、B1、B2 和 B3 上,在 A1 上还部署了协同模块和策略库,其中策略库用 MySQL 数据库模拟。

根据常见的信息安全攻击和事件,设计了信息安全报警及消息响应方式(如表 1 所示)。在 MySQL 数据库中创建协同策略表存储协同策略,用组件注册表记录注册的组件,如图 7 所示。

id	name	type	ip	level	Description
1	B1	IDS	10.6.233.51	1	入侵检测设备
2	B2	IDS	10.6.233.52	2	入侵检测设备
3	B3	FireWall	10.6.233.53	1	防火墙设备

图 7 数据库安全组件注册表

表 1 常见报警类型及响应方式

安全事件类型	说明	响应组件类型	响应目标	协同策略
DDoS	拒绝服务攻击	防火墙	攻击源	屏蔽 IP
Ping-of-death	拒绝服务攻击	防火墙	攻击源	屏蔽 IP
PortScan	端口扫描	防火墙	攻击源	关闭端口
Worm	蠕虫病毒	受攻击主机	被攻击主机	杀死进程
Phf attack	浏览器脚本攻击	防火墙	攻击源	屏蔽 IP
		受攻击主机	被攻击主机	重启

3.2 实验过程

A1 运行协同操作模块和 IDXP 通信模块,监听客户端的连接,B1、B2、B3 运行 IDXP 通信模块,监听管理中心的连接请求。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。

安全组件协同响应的全过程包括 3 个阶段(见图 8):

第 1 阶段 安全组件发现安全事件,与管理中心建立 IDXP 连接,将报警信息发送给管理中心。

B1 向 A1 请求 IDXP 连接,连接建立后,读取“idmef_example_portscan.xml”报警信息文件,发送至管理中心 A1。

第 2 阶段 管理中心对报警信息进行解析,匹配合适的策略,并生成响应消息。

A1 收到报警后,根据类型标识的攻击类型匹配协同策略。在数据库的协同策略表中,“PortScan”报警信息对应的响应策略为:对报警信息中的端口采取关闭措施,响应组件为防火墙。在安全组件注册表中,防火墙组件为 B3,结合报警信息中的端口等其他信息,A1 生成发送给 B3 的响应消息实例。

第 3 阶段 管理中心同需要执行响应的组件建立 IDXP 连接,将响应消息发送给该组件。

A1 向 B3 请求 IDXP 连接,连接建立后,把上一阶段生成的响应消息发送给 B3。

图 8 安全组件协同响应过程三阶段

在表 1 中,PortScan、DDoS 等攻击只有防火墙予以响应,这样的协同策略属于单匹配策略;Phf attack 攻击则由防火墙和受攻击主机同时响应,这种协同策略是多匹配策略。

采用单匹配策略,对安全组件间协同响应过程的各个阶段的时间开销进行测试。

3.3 结果及分析

安全组件间协同响应过程的各个阶段的时间开销测试结果如表 2 所示,性能对比结果如图 9 所示。

表 2 安全组件协同响应过程性能测试数据

实验序号	T_1	T_2	T_3	T_4
1	1718	16	1737	3471
2	1704	15	1540	3259
3	1469	15	1619	3103
4	2078	16	1911	4005
5	1688	15	1648	3351
6	1766	15	1842	3623
7	1922	15	1779	3716
8	1718	16	1834	3568
9	1625	15	1615	3255
10	1547	15	1671	3233
累计时间	17235	153	17196	34584
平均时间	1723.5	15.3	1719.6	3458.4

注: T_1 为发送报警时间; T_2 为处理报警时间; T_3 为发送响应时间; $T_4 = T_1 + T_2 + T_3$ 。

从表2中的测试数据可以看出,从安全组件发出报警信息到响应安全组件收到响应信息,一般为3.4 s左右,其中建立1次IDXP连接的时间开销为1.7 s左右,安全中心处理报警消息生成响应消息的时间开销很少,一般为15 ms左右。

图9 安全组件协同响应过程性能测试结果

性能测试结果表明,本文提出的协同响应机制可以在较短的时间内对信息安全事件做出响应,性能比较稳定,能够满足安全组件协同操作的需求。

4 结语

为了充分利用网络安全系统,提高防御体系的整体防御能力,本文提出了一种基于策略的网络安全组件协同响应机制,设计了报警信息描述格式和信息传输方法,采用Java语言实现了协同响应机制。通过仿真实验证明了本文提出的基于策略的协同响应机制的可行性和有效性。

本文仅对基于策略的协同响应机制进行了设计实现,但未对协同策略的生成方式进行设计实现。为了应对不断变化的信息安全事件,在未来研究工作中将研究基于报警信息和知识库的协同策略自动生成算法。

参考文献:

- [1] DEBAR D. The intrusion detection message exchange format [EB/OL]. [2009-11-24]. <http://www.rfc-editor.org/rfc/rfc4765.txt>.
- [2] FEINSTEIN B, MATTHEWS G. The intrusion detection exchange protocol [EB/OL]. [2009-11-24]. <http://www.rfc-editor.org/rfc/rfc4767.txt>.
- [3] 张新跃, 邓炜春, 沈树群. 策略驱动的网络安全管理模型[J]. 计算机应用研究, 2005, 22(1): 226-231.
- [4] 朱乾林, 云晓春, 王永恒, 等. 一种基于策略驱动的联动平台设计与应用[J]. 计算机工程, 2007, 33(2): 283-285.
- [5] DEBAR H, THOMAS Y, CUPPENS F, et al. Enabling automated threat response through the use of a dynamic security policy [J]. Journal in Computer Virology, 2007, 3(3): 195-210.
- [6] 卢锦泉, 苏一丹. 网络管理中安全策略与安全信息共享模型研究[J]. 广西民族学院学报: 自然科学版, 2005, 11(2): 77-81.
- [7] 谢宁. 协同入侵检测技术的研究[D]. 西安: 西安理工大学, 2007.
- [8] DA SILVA P F, WESTPHALL C B. An intrusion answer model compatible with the alerts idwg model[C]//Network Operations and Management Symposium. New York: IEEE Communications Society, 2006: 1-4.
- [9] KOUTEPAS G, STAMATELOPOULOS F, MAGLARIS B. Distributed management architecture for cooperative detection and reaction to DDoS attacks[J]. Journal of Network and Systems Management, 2004, 12(1): 73-94.
- [10] 徐旭平, 李之棠. 基于BEEP-Java的IDXP Profile的实现[J]. 华中科技大学学报: 自然科学版, 2003, 31(增刊): 147-149.
- [11] 钱德沛, 张然. 一种基于UML的协同入侵检测系统分析方法[J]. 北京航空航天大学学报, 2004, 30(9): 803-807.

(上接第1465页)

图5 OFDM离散信号循环谱(SNR=0 dB)

6 结语

加循环前缀矩形脉冲成型的OFDM基带信号具有循环平稳性,其循环谱以 $\alpha = 1/T$ 进行切片,噪声仅影响 $\alpha = 0$ 的切面,检测切片间的距离,可以估计到基准循环频率,进而得到OFDM的符号周期 T 。仿真验证了理论分析的结论,并在低信噪比条件下,实现了OFDM信号符号周期的盲估计,本文的结果可以进一步用于OFDM认知无线电系统中。

参考文献:

- [1] SEIDEL S, BREINIG R. Autonomous dynamic spectrum access system behavior and performance [C]// 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN. Washington, DC: IEEE, 2005: 180-183.

- [2] MITOLA J, III, MAGUIRE G Q, Jr. Cognitive radio: Making software radios more personal [J]. IEEE Personal Communications, 1999, 6(4): 13-18.
- [3] MAHMOUD H, YÜCEK T, ARSLAN H. OFDM for cognitive radio: merits and challenges [J]. IEEE Wireless Communications, 2009, 16(2): 6-15.
- [4] BUDIARJO I, NIKOOKAR H, LIGHTHART L P. Cognitive radio modulation techniques [J]. IEEE Signal Processing Magazine, 2008, 25(6): 24-34.
- [5] HUANG ZHI-TAO, JIANG WEN-LI, WANG JIANG-XIN. Signals-based time-difference extraction of moving targets [J]. Journal of Electronic and Information Technology, 2002, 24(7): 887-89.
- [6] 黄知涛. 循环平稳信号处理及其应用研究[M]. 长沙: 国防科技大学出版社, 2007.
- [7] GARDNER W A. Cyclostationarity in communications and signal processing [M]. New York: IEEE, 1994: 329-454.
- [8] BÖLSKEI H. Blind estimation of symbol timing and carrier frequency offset in wireless OFDM systems [J]. IEEE Transactions on Communications, 2001, 49(6): 988-999.
- [9] VUCIC D, OBRADOVIC M. Spectral correlation evaluation of MSK and offset QPSK modulation [J]. Signal Processing, 1999, 78(3): 363-367.
- [10] GARDNER W A. Exploitation of spectral redundancy in cyclostationary signals [J]. IEEE Signal Processing Magazine, 1991, 8(2): 14-36.