文章编号:1001 - 9081(2008)04 - 0843 - 03

一种分布式入侵检测系统的通信机制设计

黄文文,郭 帆,文 剑,余 敏
(江西师范大学 计算机信息工程学院, 南昌 330022)
(chinawenzi@gmail.com)

摘 要:基于关联和代理的分布式入侵检测模型,提出了一种分布式入侵检测系统的通信机制设计方案。其中通信 Agent 间的消息交换格式参照 IDMEF 标准,给出其消息内容详细设计,并根据需求扩充了警报数据 XML 描述;汇聚点通信 Agent 中使用基于 subscription 通信模式减少了系统的通信开销,具体描述了 subscription 的逻辑结构实现;还在通信机制中采用 SSL 技术较好解决了数据传输的安全问题。

关键词:分布式入侵检测;代理;通信机制;入侵检测消息交换格式;XML
中图分类号: TP393.08 **文献标志码**:A

Communication mechanism designed for distributed intrusion detection system

HUANG Wen-wen, GUO Fan, WEN Jian, YU Min
(*School of Computer and Information Engineering, Jiangxi Normal University, Nanchang Jiangxi* 330022, *China*)

Abstract: According to the distributed intrusion detection model based on correlation and Agent, a kind of communication mechanism was proposed. With reference to the Intrusion Detection Message Exchange Format (IDMEF), a detailed message system was described for communication Agent, and in accordance with demand expanded XML description. Using the subscription communications model in order to reduce the overhead of communication, subscription logic framework was described. Based on SSL, a security communication mechanism can meet the demand of the distributed intrusion detection system.

Key words: distributed intrusion detection; Agent; communication mechanism; Intrusion Detection Message Exchange Format (IDMEF); XML

0 引言

分布式入侵检测系统中,由多个检测 Agent 分别检测不同的主机和网络,各 Agent 间需要通过互相协作来完成较复杂的检测任务。然而,各检测 Agent 可能使用不同的检测办法,运行于不同的平台上,具有不同的数据表达格式,这就增加了 Agent 间进行协作的复杂性[1]。因此,在分布式入侵检测系统中,需要一种通用且高效的入侵检测通信机制。

互联网工程任务组(IETF)的入侵检测工作组(IDWG)制定的入侵检测消息交换格式(IDMEF)[2]和美国国防部研究局(DARPA)制定的公共入侵检测框架(CIDF)[3]等标准提供了一个入侵检测通用的体系结构、入侵消息和入侵对象的表达格式。借鉴以上标准化成果,基于郭帆等人提出的基于关联和代理的分布式入侵检测模型[4],提出了一种分布式入侵检测系统的通信机制方案。

本文中通信 Agent 间的消息交换格式参照 IDMEF 标准,给出了详细的消息内容设计方案,并根据需求扩充警报数据 XML 描述,给出了具体的消息实例;在汇聚点通信 Agent 中使用了基于 subscription 通信模式减少了系统的通信开销,具体描述了基于 subscription 模式中事件管理服务模块(Event Management Service, EMS)的实现;在通信机制中采用 SSL 技术,使其数据传输安全。因此通信机制总体上满足了分布式入侵检测模型中系统警报信息量大、Agent 间通信协作复杂、实时通信、安全性高的特点。

1 相关工作

郭帆等人提出的一种分布式入侵检测系统(Intrusion Detection System, IDS)模型,在文献[4]中详细描述了该模型的结构。其中该模型中的通信 Agent 分为本地通信 Agent 和网络通信 Agent,所有 Agent 逻辑上组成树结构。本地 Agent 处于树的末梢,负责收集网络中各集中式 IDS 采集的信息并传递给网络 Agent,它们之间的通信必须通过网络 Agent。汇聚节点之间的信息传播使用 Emerald 等人提出的基于订阅的方式来减少通信负载[5]。每个网络 Agent 存在一张订阅者列表,订阅者只能是该 Agent 的兄弟和儿子,所有 Agent 都必须向其父亲传递所有消息。订阅者信息的动态配置和修改由网络配置工具来专门实现。

通信机制中具体消息定义是基础,在分布式系统中具有重要意义[6]。本文中重点描述了通信 Agent 之间的交互消息的内容,具体给出了汇聚点通信 Agent 基于 subscription 通信方式的逻辑结构实现,解决其中数据安全传输问题。

2 通信机制的总体设计

通信机制中信息内容的设计主要基于 IDMEF 标准,并给出消息内容详细设计,描述了 XML 定义消息的实例;在汇聚点通信 Agent 中使用了基于 subscription 通信模式,对事件服务模块(EMS)进行具体的描述;最后在 Agent 通信安全机制中采用基于 SSL 的通信解决办法,满足数据传输的安全。整个通信机制方案符合分布式入侵检测系统模型中通信的需求。

收稿日期:2007 - 10 - 30;**修回日期**:2007 - 12 - 10。
基金项目:国家 973 面上项目(2006CB303006);国家 973 前期研究项目(2007CB316505);江西师范大学博士基金项目。
作者简介:黄文文(1983 -),男,湖北枝江人,硕士研究生,主要研究方向:信息安全、传感器网络; 郭帆(1977 -),男,江西于都人,副教授,博士,主要研究方向:信息安全、软件体系结构; 文剑(1980 -),男,湖北孝感人,硕士研究生,主要研究方向:信息安全; 余敏(1964 -),女,江西南昌人,教授,博士,主要研究方向:信息安全、网络计算技术。

2.1 信息交换格式的设计

2.1.1 IDMEF

IDMEF是IETF的入侵检测工作组制定的标准草案,其目标之一是满足报警之间的关联需求并用于检测分布式协同攻击,目前绝大部分IDS产品都支持IDMEF格式。IDMEF描述了入侵检测系统输出信息的数据模型,并解释使用此模型的基本原理。

IDMEF数据模型如图1所示。该模型用XML(Extensible-Markup Language)实现,并定义了标准的数据格式。IDMEF数据模型以面向对象形式表示告警信息,设计模型的目标就是为警报提供确定的标准表达式。所有信息均继承自IDMEF-Message类,每种类型的消息都是它的子类1。IDMEF目前定义了两种类型的消息:Alert和Heartbeat,这两种消息又由各自子类聚集而成,从而可以描述更详细的消息。

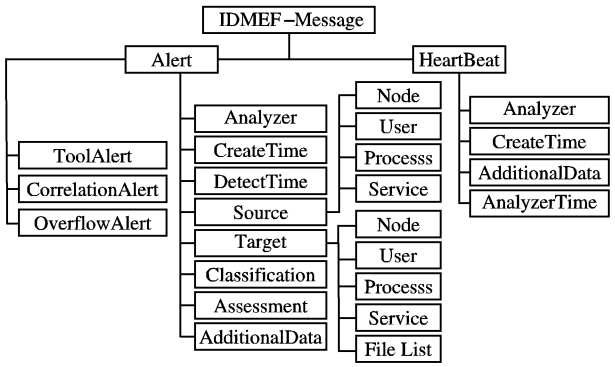

图1 IDMEF数据模型

2.1.2 消息内容详细设计

IDMEF关注的主要是Alert和HeartBeat消息。根据分布式入侵检测的特点,各个通信Agent之间要交互的信息比较多,对IDMEF进行了扩展,定义了订阅、通知、指令等消息,以支持系统中数据上报、响应指令、协作分析等要求。下面具体描述五种消息内容:

1)报告(Report)

报告是集中式IDS提交的消息,用于反映IDS的上报数据,主要包括Alert,HeartBeat,AuditData。Alert是在集中式IDS检测到入侵行为后,主动向本地汇聚Agent提交的报警信息,用于描述特定的攻击事件(Event)。HeartBeat是集中式IDS向分析器报告自身处于运行状态,需要定时发送。Alert和HeartBeat可以按照在IDMEF草案中给出的定义。AuditData是集中IDS提交用于挖掘检测规则和进行异常检测的安全审计数据。另外,Alert还有一个特征属性,用于标识该消息的id(ident)。

2)订阅(Subscription)

通信Agent通过订阅消息向其他组件发布请求,订阅可以是获取本地组件中提交的状态(HeartBeat)、安全审计记录、或协作请求消息(AssistReq)。当出现大范围的分布式攻击行为时,通信Agent向其他本地汇聚Agent组件发出AssistReq请求,订阅与此次攻击有关的所有信息。其他通信Agent通过对协作请求中包含的事件信息,结合自身监控范围内的安全事件,进行相关分析,发布相关信息,从而帮助确定攻击行为。AssistReq通知所包含的数据项包括:CreateTime,CurrentTime,Sender,Receiver,Event, AdditionalData。

3)通知(Notification)

通知是分布式入侵检测系统中最普遍应用的消息,检测组件之间通过通知交换攻击事件消息(Attack),本地汇聚Agent状态消息(Heartbeat)和网络Agent对请求协作消息的回复(AssistResp)。

Attack用于通信Agent之间的攻击事件通知,当网络关联和汇聚Agent最终确认一次攻击时,无论是由其集中式IDS检测到的攻击和网络IDS检测到的攻击,还是对警报数据的关联分析结果,该汇聚点通信Agent都可以使用Attack类型的通知消息向其他通信Agent通报,网络通信中Agent接收到通知消息后,可以根据自身的安全策略,转交网络汇聚Agent处理。AssistResp是AssistReq的回复消息,用于返回协作请求消息,与AssistReq数据项大致相同,增加Assessment项,表示发送方汇聚Agent对该事件的评估。

4)广告(Advertisement)

一旦确认攻击事件,通信Agent可使用广告消息向整个系统广播攻击事件。广告使用通知的Attack消息,但内容比通知简单,仅需要表示几个关键的信息,或者是攻击事件的摘要。

5)指令(Instruction)

指令是响应Agent向其控制的集中式IDS发送的消息,主要功能是控制数据收集组件的启动、停止和对网络入侵行为作出的响应。根据模型定义Operation和Response两种数据类型。

Operation是由响应Agent组件向集中IDS发出的操作指令,有启动(OPER_SRUN),停止(OPER_STOP),查询数据状态(OPER_STOR)等类型。Operation所包含的数据项如表1所示。

表1 Operation指令包含的内容

数据项	说明	允许个数
CreateTime	Operation指令的创建时间	1
Sender	Operation指令的发送者	1
Receiver	Operation指令的接收者	0...*
OperClass	Operation消息类型	1...*
AdditionalData	附加数据	0...*

Response是通信Agent根据分析结果对响应Agent发出的响应消息,可以是切断连接、阻塞IP或端口和杀死异常进程等类型,分别用RESP_RESET,RESP_BLOCK,RESP_KIL表示。Response所包含数据项与Operation相同,还包括响应的时间(Time)和消息类型数据(RespData)。

2.1.3 基于XML的消息定义

XML具有很好的可扩展性,即它允许用户自己定义标记,它是一种完全面向数据语义的标示语言,突出了数据的语义与元素结构描述能力[8]。越来越多的应用使用XML作为一种通用数据交换格式,在IDMEF规范中也推荐使用XML来实现入侵检测系统之间的数据交换[9]。为了正确建立基于XML格式的报警消息,定义了一个Schema来定义和约束XML消息,它是对IDMEF格式的扩展,因而满足了本地Agent和网络Agent间的相互协作性的通信需求。例如Report中的报警消息Alert包括:Analyzer, CreateTime, DetectTime, AnalyzerTime,Source,Target,Classification和AdditionalData等部分,可以写出消息的XML Schema文档如下:

```
<xs: Schema xmlns: xs =
  "http://www.w3.org/2001/XMLSchema" >
   <xs: element name = "Alert" type = "AlertType"/ >
   <xs: ComplexType name = "AlertType" >
   <xs: sequence >
   <xs: element name = "Analyzer" type = "AnalyzerType"/ >
   ...
</xs: Schema >
```

其他的消息可以类似基于XML Schema定义。需要传递的报警消息,都可以转换成XML格式进行传输。XML格式

的消息可以基于其堆栈结构进行存储[9]。限于篇幅,这里简要给出一条报警消息可能为:

```
<IDMEF>
<Alert id="abc" impact="unknown" suspect="6">
  <Analyzer id="4460">
    <Node Id="589" Category="unknown">
    <Location>202.112.231.122</Location>
    <name> badguy.example.net </name>
    <Address Id="232" Category="vm"
      Vlan-Name="instruction" Vlan-Num="4333">
    <Address>http://www.jxnu.edu.cn</Address>
      <netmask> 219.229.250.255 </netmask>
    </Address>
    ...
  </Analyzer>
</Alert> </IDMEF>
```

2.2　汇聚点通信 Agent 中的通信模式

在汇聚点通信 Agent 中采用基于 subscription(订阅)模式的通信模型来完成多个 Agent 的通信和协作。在这种模式中,事件管理服务模块相当于所有消息的管理机构,而订阅者(subscriber)相当于接收方,该模型中提供了一个事件管理服务(EMS)。subscriber 将感兴趣的事件向 EMS 申请注册,EMS 用一个注册/订阅信息表专门维护这些订阅的事件信息。EMS 在注册/订阅信息表里查找对该信息感兴趣的 subscriber,然后将消息发送给它们,所有订阅消息必需经过汇聚点通信 Agent。图 2 显示出了通信模式的逻辑结构。

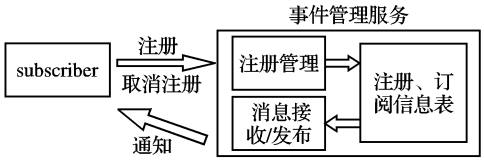

图 2　通信模式 subscription 逻辑结构

关键是 EMS 的实现,在通信 Agent 中对所有注册/订阅同一事件,通知每一个 subscriber。EMS 是不同 Agent 间通信和协作的基础。由于汇聚点通信 Agent 接收不同本地组件的警告消息还要将其转发给网络关联和汇聚 Agent,同时又要与其他汇聚点 Agent 相互协调,因此,事件的注册、订阅、发布需要遵循一定的协议来满足通用性要求。根据分布式入侵检测特点,EMS 要处理注册、发布、报告、通知、指令等消息:

注册　subscriber 需要提供自己的 IP 和注册/注销的事件,EMS 收到请求后,修改相应的注册服务信息表。

发布　EMS 需要注明发布的事件 ID、事件相关数据然后发送到通信 Agent。可以发布的事件有:特征库更新,策略更新,响应方式,更新,报警。

报告　主要接收本地组件和网络组件上报的告警消息。

通知　所有 subscriber 处于同一多播组,ES 在发布事件时,根据其订阅消息列表,即所有递交订阅的 subscriber 都可以接收到这一事件。接收到事件通知的 subscriber 向 EMS 发送反馈消息,相应汇聚点通信 Agent 由此修改 subscriber 的状态,将其对应的事件修改为已更新,记录更新时间,并且把指令信息发送到相应通信 Agent。

指令　响应 Agent 接受的消息,是由 EMS 先传送给到通信 Agent,最后到达响应 Agent。

在汇聚点通信 Agent 中,所有 Agent 逻辑上形成树结构,形成一片森林,本地 Agent 通信必须通过网络 Agent[4]。通信机制中采用基于订阅的通信模式,结合树形结构来达到快速高效传播告警信息、攻击意图和响应动作的目的。比起传统的分布式环境下的通信模式,如应答式、RPC 等,基于 subscription 的通信模式具有很好的时间、空间的松耦合性。这里只是给出了汇聚点通信 Agent 中 subscription 逻辑实现方式,下一步具体实现网络组件中的汇聚点通信 Agent,也包括本地组件中通信 Agent。

2.3　通信机制的安全

该模型采用基于代理的分布式体系结构,各个自治检测 Agent 的通信安全非常重要。这里只考虑本地组件中检测的有效消息能够安全传输到汇聚点通信 Agent 中,可以在系统中采用应用层协议中使用 SSL 终端服务器进行认证,还可选择对客户进行认证[7]。常规的是基于 X.509 标准定义的证书结构和身份认证协议来进行的,由于需要一个 CA 证书中心造成了不必要的开销,因此在本地组件到汇聚点通信 Agent 中采用 RSA 算法来进行身份认证,具体过程如下:1)建立安全能力。认证双方(Sever 和 Client)各有一对公钥和私钥,在认证前采用物理拷贝的形式交换密钥。2)身份确认和产生会话密钥。在 Sever 方先用自己的私钥 *ks* 加密一个随机数 *Eks*(*N*),然后用 Client 方的公钥 *kcp* 再次加密。这样能保证只有 Server 方公钥 *kp* 的 Client 方才能解密出这个随机数,就能对 Client 方的身份进行确认。3)握手过程完成。首先在一次连接的握手协商中确定所采用的加密算法并产生密钥,并保证不同连接中密钥也不同。

本地组件传送的是 XML 格式定义的消息格式报警消息,可以对其对称加密。汇聚点通信 Agent 中用多个子线程同时处理不同本地组件中的消息,经过身份认证和信息加密后就可以保证整个信息源的可靠性、信息传输过程的安全性。

3　结语

基于关联和代理的分布式入侵检测模型,提出了一种通信机制设计方案,满足了分布式入侵检测系统中诸多组件间的通信需求。下一步工作是根据该方案,具体实现汇聚点通信 Agent 中基于 subscription 的通信模式,而通信 Agent 中基于逻辑树组织结构需要用网络拓扑工具来进行划分和动态配置,然后根据预先设计的几种攻击场景,使响应 Agent 能够对分布式协同攻击发出指令消息并传递给集中式 IDS。

参考文献:

[1] LOCASTO M E, PAREKH J, STOLFO S. CUCS-012-04, Collaborative distributive intrusion detection[R]. New York: Columbia University, Computer Science Department, 2004.

[2] DEBAR H. The intrusion detection message exchange format [EB/OL]. [2006-03-16]. http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txt.

[3] PORRAS P. The common intrusion detection framework architecture [EB/OL]. [1999-09-10]. http://gost.isi.edu/cidf/drafts/architecture.txt.

[4] 郭帆,余敏,叶继华. 一种基于关联和代理的分布式入侵检测模型[J]. 计算机应用, 2007,27(5):1050-1053.

[5] PORRAS P, NEUMMAN P. EMERALD: event monitoring enabling response to anomalous live disturbances[C/OL]// The 20th National Information System Security Conference. Baltimore, Maryland, USA, 1997: 353-365[2007-10-01]. http://citeseer.ist.psu.edu/porras97emerald.html.

[6] SPAFFORD E, ZAMBONI D. Intrusion detection using autonomous agents[J]. Computer Networks, 2000, 34(4): 547-570.

[7] FREIER A, KARLTON P, KOCHER P. The SSL Protocol: Version3.0[S]. 1996.

[8] 单来祥,杨寿保. 分布式入侵检测系统的通信模块的设计[J]. 计算机应用, 2004,24(7):93-96.

[9] 丁捷,谭建龙,程学旗. 分布式入侵检测系统通讯协议的研究与实现[J]. 计算机工程与应用, 2004,40(8):157-159.