

文章编号:1001-9081(2006)03-0567-02

一种基于协同调度的入侵检测框架

黄 亮,唐文忠

(北京航空航天大学 计算机学院,北京 100083)

(huangjinzi@sohu.com)

摘 要:分析了现有入侵检测系统的不足,讨论了协作的必要性,介绍了一种多主体协同入侵检测框架。本框架采用分布检测和集中处理的结构、通用的警报格式和安全通信协议,由控制中心的调度引擎对协同请求、关联数据收集、警报和新规则的分发进行统一的调度管理。经过测试和应用,能够很好地实现多主体间的信息共享,完成协同检测。

关键词:入侵检测;协同调度机制;入侵检测消息交换格式;包装器

中图分类号: TP393.08 **文献标识码:** A

Intrusion detection system framework based on collaborative dispatch mechanism

HUANG Liang, TANG Wen-zhong

(School of Computer Science & Engineering, Beijing University of Aeronautics & Astronautics, Beijing 100083, China)

Abstract: The shortages of current intrusion detection systems were analyzed, and the necessity of collaboration was discussed. A multiagent collaborative intrusion detection framework was put forward. It adopted distributed detection and centralized analysis architecture, generic alert form and secure transfer protocol in this system, unified dispatch by coordinate engine to manage cooperative request, collect relative data and distribute alerts and new rules. This system can well implement information sharing among multiagents and achieve collaborative detection after test and application.

Key words: intrusion detection; collaborative dispatch mechanism; IDMEF (Intrusion Detection Message Exchange Format); wrapper

0 引言

典型的入侵检测系统(Intrusion Detection System, IDS),无论是基于主机的还是基于网络的,都是针对一个管理域的。在这种环境下,对网络攻击模式的全局状态信息自然就没有检测到。而全局的信息对分类和定位攻击来说都是至关重要的。目前大多数的 IDS 都没有充分重视受攻击系统间的信息交换和各主体间的协作。

例如一个机关的内部网通常是部署多个检测引擎来分别监测不同的主机和网络资源。这种策略的不足如下:1)结构设计上缺少统一的标准,也就限制了扩展性和互操作性;2)每种检测引擎只关注于它本身检测机制所能覆盖范围的事件,对新的协同攻击显得无能为力;3)即使是一个检测引擎发现了攻击,其他的受保护资源可能还面临着同样的威胁。

针对这些实际问题,我们研究了开放式多主体协同入侵监控平台(Open Multiagent Collaborative Monitoring, OMCM),该系统通过对检测模型的改进及有效的协同调度机制实现了对现有的不同入侵检测系统有机地集成、管理和部署;并在一体化管理、控制和调度机制下,使不同产品间协同完成安全防护,建立安全管理防护链,提高了安全防护强度。

1 系统的平台构架

开放式多主体协同入侵监控平台如图 1 所示,它可以有效、方便地集成现有的入侵检测平台,通过增加一个包装器

(Wrapper)并连接到综合检测的控制中心(Control Center)来实现对复杂入侵的协同检测。整个系统的体系是 Client/Server 结构。首先,这种 Client/Server 结构使信息共享具有很强的灵活性,使得系统具有集中式系统的简单、易于实现的优点;Control Center 还可以用层次结构实现,使系统具有分布式系统的健壮性,便于系统扩充。

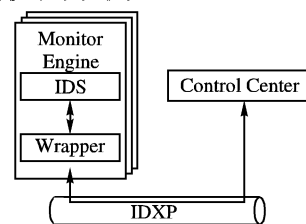


图 1 系统框架结构

1.1 监控引擎

监控引擎(Monitor Engine)是多主体入侵检测系统中“主体”的又一称呼。它由 IDS 和 Wrapper 组成。

IDS 可以是基于网络、主机等的典型入侵检测系统,它们可以单独部署于系统中,对网络流量、主机系统日志、数据库日志、电子邮件等数据进行分析,完成特定的检测功能。Wrapper 在将现有的 IDS 集成到本协同检测平台中起着关键的作用,它主要有以下几个功能:

1) 通过 IDMEF_XML_Plugin 将 IDS 生成的告警信息转换成统一的标准格式 IDMEF,并加上一个属性标识其为已知入侵还是可疑信息;

收稿日期:2005-09-28 修订日期:2005-12-05 基金项目:国家 863 计划项目(2004AA113040)

作者简介:黄亮(1977-),男(满族),辽宁丹东人,硕士研究生,主要研究方向:入侵检测、网络安全;唐文忠(1968-),男,河北涿鹿人,副教授,高级工程师,博士研究生,主要研究方向:计算机软件、信息安全。

2) 当 Control Center 分发由其他监控引擎发现的告警信息时,负责根据告警信息类别,采用一定的算法来提高其在引擎的警戒级别;

3) 当 Control Center 分发新的入侵规则时,负责将接收到的规则转换为本地规则,存入规则库中;

4) 当 Control Center 发送收集关联数据的命令时,负责进行解析并执行协同动作。

1.2 IDMEF 和 IDXP 的应用

在分布式 IDS 中,多个主体分别监控不同的主机和网络资源,可能运行于不同的平台上,并具有不同的数据格式,这就增加了协作的复杂性。

为解决上述问题,我们使用 IDMEF 提供的标准数据格式对可疑事件发出告警,以提高系统之间的互操作性,由于 IDMEF 由通用的 XML 语言进行描述,所以控制中心可以正确解析识别不同类型 IDS 发送来的告警信息,具有实施更复杂交叉分析和相互验证的计算条件;并且单个的图形界面就能够显示来自不同的入侵检测产品的报警,使用户从一个显示屏就能够监视许多产品的运行状况。

在通信协议的选择上,使用 BEEP 协议构造的入侵检测交换协议(Intrusion Detection Exchange Protocol, IDXP)在入侵检测实体之间交换数据。该协议能够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性。在一次 BEEP 会话中,使用多个 BEEP 信道,这样可以对在 IDXP 对等体之间的数据进行分类和优先权设置。

1.3 控制中心

以往的控制中心只是起到管理的作用,完成对系统的一些配置和查看告警信息,没有协同分析检测的功能。

本系统中的 Control Center 是协同检测的核心所在,它能够对整个系统的运作情况进行管理,包括开启和停止子监控引擎、配置协同的规则、管理告警信息等。并能够实现单一 IDS 无法胜任的工作,对分布式协同入侵进行检测。通过其内置的协同引擎,对告警信息和自动生成的新规则进行分发,还可以针对某条告警信息,向其他监控引擎发送请求,收集关联数据,构造协同事件来检测。

2 控制中心协同模型

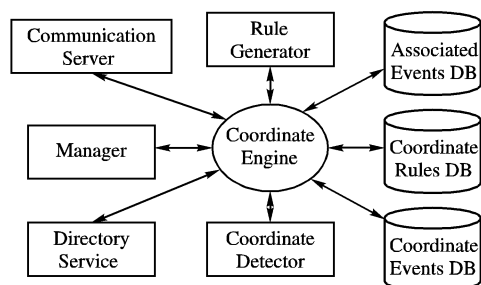


图2 调度引擎协作机制

控制中心内部的组织如图2所示,以一个协同引擎(Coordinate Engine)为核心,负责协调整个体系的运作。

2.1 目录服务

目录服务模块(Directory Service)利用 CIDF 提供的目录服务,使构件可以定位自己需要的服务构件以获取共享信息,或者注册自己以向其他构件提供信息共享,并且为通信双方构建安全的通信信道提供支持,比如管理和发布密钥。

当有新的检测引擎部署进来后,通过该模块向中心注册,存储在管理器的服务列表文件中;当有告警数据或新规则通过中心分发时,由管理器读取服务列表文件,向所有注册的检测引擎分发消息。对不确定的告警信息进行事件关联也需通

过该模块来收集相应的信息。

2.2 管理器

管理器(Manager)实现管理人员与系统的人机协同,通过该部分管理人员可以对系统的分析结果进行统一的过滤、分析,以最大化地利用分析结果信息;同时,通过配置调度模块,可以对整个系统的运行策略和不同功能模块进行配置,调整系统的运行行为。

2.3 协同检测器

对于已知的攻击,由中心直接分发告警信息,使其他相关的检测引擎提高警戒级别;对于未知的攻击,进行协同检测来发现分布式的攻击,以实现更精确的检测。

协同检测器(Coordinate Detector)是将关联数据所构造的协同事件和协同入侵规则库逐一匹配,判断是否有协同入侵行为发生。

对于关联数据,我们有基于主体和客体的两种关联机制。主体是指在相关检测引擎中收集和该事件的源 IP 一样或在同一子网中的某一时间段内的事件;客体是指在相关检测引擎中收集同一源 IP,目标 IP 不同的在某一时间段内的事件。这两种机制都是在事先设定好的一个时间窗内收集事件,所以时间窗大小的设定很重要,大了相应的通信开销会增加,小了可能收集不到某些慢攻击的相关事件。

2.4 规则生成器

规则生成器(Rule Generator)是利用数据挖掘方法,在协同入侵事件库中提取新的协同入侵规则,一旦生成新的规则,随即分发给已注册的监控引擎。这样就可以使系统具有自适应性,检测出未知模式攻击的协同入侵。

2.5 通信服务器

通信服务器(Communication Server)可以为消息提供路由服务,识别并接受本系统中使用的定向包和组播包,同时负责解析监控引擎传送过来的 XML 格式 IDMEF 告警数据。告警数据经过解析后,存入相应的数据库以备提取分析。作为专门的数据接收平台,通信服务器可以在连接多个监控引擎的情况下,保障大容量数据传输的可靠性。

2.6 存储模块

存储模块包括三个数据库,分别是协同入侵事件库(Coordinate Events DB)、协同入侵规则库(Coordinate Rules DB)和关联事件数据库(Associated Events DB)。协同入侵事件库存放发生过的协同安全事件,它是一组相关联的普通事件。协同入侵规则库存放描述协同入侵的规则,它由一组相关联的普通规则来描述。协同关联数据库是为收集未确定告警信息相关联的数据特别设定的,因为要将所有检测引擎的事件都存入一个综合的知识库有如下缺点:一是所需的存储容量太大;二是所需的网络通信量过重。

2.7 协同调度流程

协同调度的具体流程描述如下:

- 1) 调度引擎通过通信服务器模块接收告警数据;
- 2) 告警数据如果是明确的入侵,调度引擎就将其分发到已注册的监控引擎,后者验证接收到的告警信息的完整性,并采取相应的措施抵制类似的攻击;
- 3) 如果是未知的攻击,调度引擎随即设定收集关联数据的协同条件,发送协同请求;
- 4) 在和监控引擎协商并建立连接后,监控引擎的包装器负责解析命令,执行收集关联数据的动作;
- 5) 控制中心接收关联数据并构造协同安全事件,启动检测引擎和规则生成器,进行检测和分析;

(下转第 576 页)

安全的比率; R_{cal} 代表计算能力的比率; R_{wei} 代表该节点的权重所占的比率。

假设 t 时刻系统中有 8 个节点, 每个节点都维护这一张记录系统中其他节点的 *capability* 的表, 这张表在每个密钥刷新未更新。系统初始化时选取 *capability* 最大的节点产生 0 的密钥分量(w_1, w_2, \dots, w_n) 并安全的按节点的权重分发该系统内节点, 新的密钥分量 $s'_i = s_i + w_i$ 。如果在系统运行期间该节点被占领或改节点的 *capability* 下降到指定门限值则用欺负算法的思想重新选取一个可信节点来产生 0 的密钥分量(w_1, w_2, \dots, w_n), 以拥有 *capability* = 7 的节点变得不可用时新节点选取情况为例。

当拥有 *capability* = 7 的节点被攻破的情况: 拥有 *capability* = 4 的节点首先发现拥有 *capability* = 7 的节点被攻破, 则它发起选举请求, 系统中各节点重新计算各自的 *capability* 并广播给其他节点, 收到消息的节点会根据消息的内容更新 *capability* 表, 并查找出最大的 *capability* 值的节点, 则拥有当前最大 *capability* 值的节点为选举出的下一轮产生 0 的密钥分量(w_1, w_2, \dots, w_n) 的节点。

当拥有 *capability* = 7 的 *capability* 下降到指定门限值的节点的情况和上述情况类似, 只是发起选举的节点为它本身。

通过这种密钥刷新技术刷新系统密钥, 可以减少节点的计算量, 同时进一步保证密钥刷新计算过程的高效性, 每次选取的可信节点如果在密钥刷新时间被攻破, 则通过下一次的密钥刷新过程来刷新系统密钥。

4 结语

目前, 针对移动自组网中的信任模型问题, 国际上主要有

Shamir 提出的门限秘密分享方案; Feldman 提出的可验证秘密分享方案(VSS); Canetti 提出的主动秘密分量更新方案以及可变门限秘密分享和分布式产生秘密的秘密分享方案等。在国内, 中国科学院、上海交通大学、武汉大学、华中科技大学、解放军理工大学及西安电子科技大学 ISN 国家重点实验室等诸多研究机构就移动自组网中的信任模型、密钥协商、密钥分发和密钥托管等进行研究, 提出了各自的方案。但已有的方案都假设移动自组网系统中节点都是平等的, 而在实际应用中节点有可能是不平等的。

本文针对网络中节点不平等的 MANET 提出了一种基于权限的门限信任模型, 该模型在可信节点剩余很少时仍能完成网络中节点的认证, 同时在已有的密钥刷新技术的基础上提出了一种新的密钥刷新思想。

参考文献:

- [1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612 - 613.
- [2] ZHOU L, HASS ZJ. Securing Ad Hoc Networks[J]. IEEE Network, 1999, 13(6): 24 - 29.
- [3] FRANKEL Y, GEMEL P, MACKENZIE P, et al. Optimal resilience proactive public-key cryptosystems[A]. Proceedings of the 38th Symposium on Foundations of Computer Science[C]. Miami Beach, FL USA, 1997. 384 - 393.
- [4] ZHOU L. Towards Fault-Tolerant and Secure On-Line Services[D]. Cornell University, 2001.
- [5] ZHOU L, SCHNEIDER FB, van RENESSE R. Technical Report 2000-1828, COCA: A secure distributed on-line certification authority[R]. Department of Computer Science, Cornell University, Ithaca, NY USA, 2000.

(上接第 568 页)

6) 如发现协同入侵事件, 则分发到已注册的监控引擎, 同时将该事件存入协同入侵事件库中;

7) 当挖掘出新规则时, 调度引擎负责调用目录服务模块进行规则分发;

8) 各监控引擎接收到新的规则时, 将其转化为本地规则, 添加到规则库中。

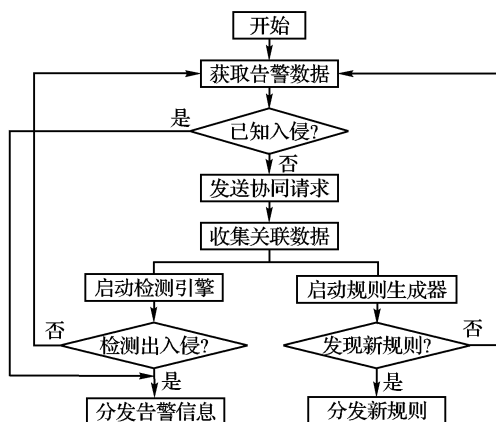


图3 协同调度流程

2.8 协同机制的优点

单个入侵检测系统无法检测到的复杂攻击, 可以通过协作, 获取其相关事件, 提供更全面丰富的数据支持, 从而得出结论, 这使得整个系统的检测能力获得提升。

告警信息的分发, 是把在一处发现的攻击提前通知给其他监控引擎, 使得能在入侵攻击的实施过程中检测到它, 并采

取相应的措施进行防御。

在控制中心, 由基于数据挖掘的协同入侵检测模块所生成的新规则能及时地分发给所有监控引擎, 快速地使系统抵御新的攻击。

3 结语

本文所讨论的开放式多主体协同入侵监控平台在传统检测引擎的基础上提出了包装器的概念和引擎间的协同机制, 可以有效、方便地集成现有的入侵检测系统, 也容易进行扩充。通过协同调度机制, 使系统能实现对新的分布式攻击的检测, 并能够快速地在整个系统内共享信息, 使整个系统在检测性能、准确性、完备性和及时性等方面都有很大提升。

参考文献:

- [1] PARK S - K, KIM K - Y, JANG J - S. Supporting Interoperability to Heterogeneous IDS in Secure Networking Framework [Z]. IEEE, 2003.
- [2] WU J-S. The Neuron Security of Joint Defense for Network Intrusion Detection[Z]. IEEE, 2003.
- [3] FEIERTAG R, RHO S, BENZINGER L. Intrusion Detection Inter-component Adaptive Negotiation[J]. Computer Networks, 2000, 34 (4): 605 - 621.
- [4] The Intrusion Detection Message Exchange Format draft-ietf-idwg-idmef-xml-12[S/OL]. <http://www.ietf.org>, 2005 - 04.
- [5] The Intrusion Detection Exchange Protocol (IDXP) draft-ietf-idwg-beep-idxp-07[S/OL]. <http://www.ietf.org>, 2005 - 04.