入侵检测系统中告警相关部件的设计与实现*)

秦 拯[1] 沈亚敏[2] 李 娜[2] 张大方[1]
(湖南大学软件学院 长沙 410082)[1] (湖南大学计算机与通信学院 长沙 410082)[2]

摘 要 随着网络的迅猛发展,管理入侵检测系统产生的大量告警变得越来越重要。本文基于因果相关的思想,设计并实现了一个入侵检测系统中的告警相关部件。实验表明,该部件能有效减少告警数量,其告警减少率达到83.26%。

关键词 入侵检测,告警相关,因果相关

Design and Realization of Alert Correlation Component on IDS

QIN Zheng[1] SHEN Ya-Min[2] LI Na[2] ZHANG Da-Fang[1]
(Software College of Hunan University, Changsha 410082)[1]
(Computer and Communication College of Hunan University, Changsha 410082)[2]

Abstract With the rapid development of network, managing the alerts from IDSs becomes more and more important. In this paper, an alert correlation component of IDS is designed and realized based on causal correlation method. Experiments show that the alert correlation component is effective in reducing the number of alerts and the reduction rate can reach 83.26%.

Keywords Intrusion detection, Alert correlation, Causal correlation

1 引言

入侵检测系统(Intrusion Detection System,简称 IDS)通过从计算机网络中的若干关键点收集信息并加以分析,检查网络中是否有违反安全策略的行为和遭到袭击的迹象,从而提供对内部攻击、外部攻击和误操作的实时保护。大部分IDS,尤其是基于网络的 IDS,针对的往往是初级事件或攻击[1],这造成了入侵检测系统两个缺陷:(1)告警量大,难以有效管理;(2)单个告警包含的信息较少,难以做出合适且快速的响应。

为解决上述问题,入侵检测领域引入了告警相关(Alert Correlation)的概念。目前已有的告警相关方法很多,大致分为以下几类:过程相关,比较典型的有 Benjamin Morin 提出的编年史法[2];因果相关,包括有 Ning Peng 提出的因果相关(Causal Correlation)方法[3]和 Templeton 的 JIGSAW 模型[4],它们假设告警之间是有因果关系的,并用各个告警之间存在的因果关系进行攻击事件分析并相关告警;统计相关,如 Wenke Lee 提出的 GTC 方法[5]。因果相关方法,相对于统计相关方法,利用的是预先定义的知识进行相关,实现简单;而相对于过程相关方法,又具有一定的灵活性,即使改变固有攻击过程或只进行攻击过程的一部分,也能对告警进行相关性分析。

本文基于因果相关方法设计并实现了一个高效的告警相关部件。同时,本文在告警相关之前还考虑了相关关系的过滤,进一步缩短了相关时间。实验表明,该部件既能有效减少告警数量,提高单个告警的信息量,相关性分析所需时间也较少,进一步加快了管理员对入侵的响应,减少了管理员处理告警信息时的繁重负担。

2 告警相关部件简介

本文涉及的几种告警定义如下:初级告警(Original Alert):入侵检测系统产生的告警信息;全局告警(Global Alert)[6]:初级告警经合并和聚类之后,用一个全局告警代表一类初级告警;超级告警(Hyper-Alert)[7]:根据专家知识对全局告警分析后的结果,它由一个三元组(fact, prerequisite, consequence)表示,其中,fact 对应告警属性值,prerequisite 是告警对应的入侵动作所必须满足的最小逻辑条件集合,consequence 是告警对应的入侵动作成功实施后所得到结果的最小逻辑集合,prerequisite 和 consequence 都用全局告警及知识库的信息进行实例化。

告警相关可定义为:合并重复告警信息,将相互之间有逻辑关系的多个初始告警转换成一个有更多信息量的超级告警,以减少告警数量,并通过超级告警确定攻击过程及其所处阶段,对攻击做出准确而快速的响应[8]。

本文根据 Ning Peng 因果相关思想,设计并实现了一个入侵检测系统中的告警相关部件,从而减少告警的数量,便于管理员更快查找告警原因。

2.1 部件功能

图 1 为告警相关部件结构图。该部件处于入侵检测系统后端,即图中虚线所示部分。它采用集中式处理:将网络中各

*)本课题得到国家自然科学基金(60273070);湖南省科技攻关项目(04GK3022);东莞市科研发展基金的资助。秦 拯 博士后,研究方向为计算机网络安全与通信。沈亚敏 硕士生,研究方向为网络安全。李 娜 硕士生,研究方向为网络安全。张大方 博士生导师,研究方向为可信系统与网络。

个探测器(每个探测器为一个 IDS 引擎)产生的告警数据由一台机器统一处理。其功能如下:(1)集中管理收集到的告警。(2)聚合(Clustering)具有相同特征的重复告警。(3)聚类(Aggregation)相同 IP 地址和端口号的告警。(4)删除不相关告警之间的逻辑关系。(5)根据专家知识生成超级告警。(6)利用告警前提和后果对告警进行相关性分析,并将告警相关图显示出来。(7)根据用户的额外要求进行相关性分析。

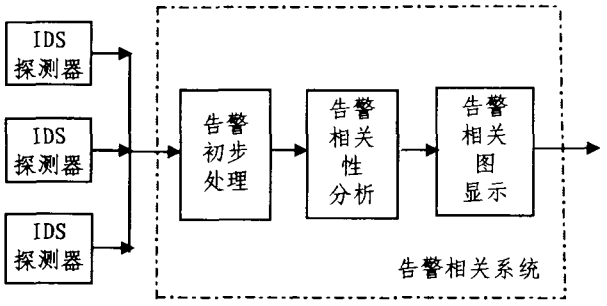

图 1 部件结构图

2.2 部件构成

部件的数据流图如图 2 所示。部件主要由 4 个模块组成(分为 4 个模块而不是部件结构图的 3 个,是由于前两个模块涉及的告警类型差别较大):①初级告警的归并:将初级告警用统一的告警格式 IDMEF(Intrusion Detection Message Exchange Format)[9]存放,再用聚合、聚类方法将初级告警归并为全局告警的形式;②全局告警的处理:过滤不可能相关的相关关系,将全局告警用超级告警表示;③告警相关性分析:实现告警相关,包括告警的相关分析;④控制台及相关图的形成:提供配置界面,相关图的显示输出。

四个模块的处理都围绕关系型数据库和知识库展开。关系型数据库系统存放初级告警、全局告警、超级告警及最终的相关结果。知识库存储已知超级告警的前提和隐含后果,以及超级告警之间的相关关系。

其数据处理步骤如下:

(1)各 IDS 探测器产生的初级告警经收集、聚合、聚类,形成全局告警并存入数据库。

(2)过滤和预处理全局告警,利用知识库中的专家知识将全局告警用超级告警表示,存入数据库。

(3)用知识库中的专家知识判断超级告警之间的相关关系,且用图形化的形式显示。

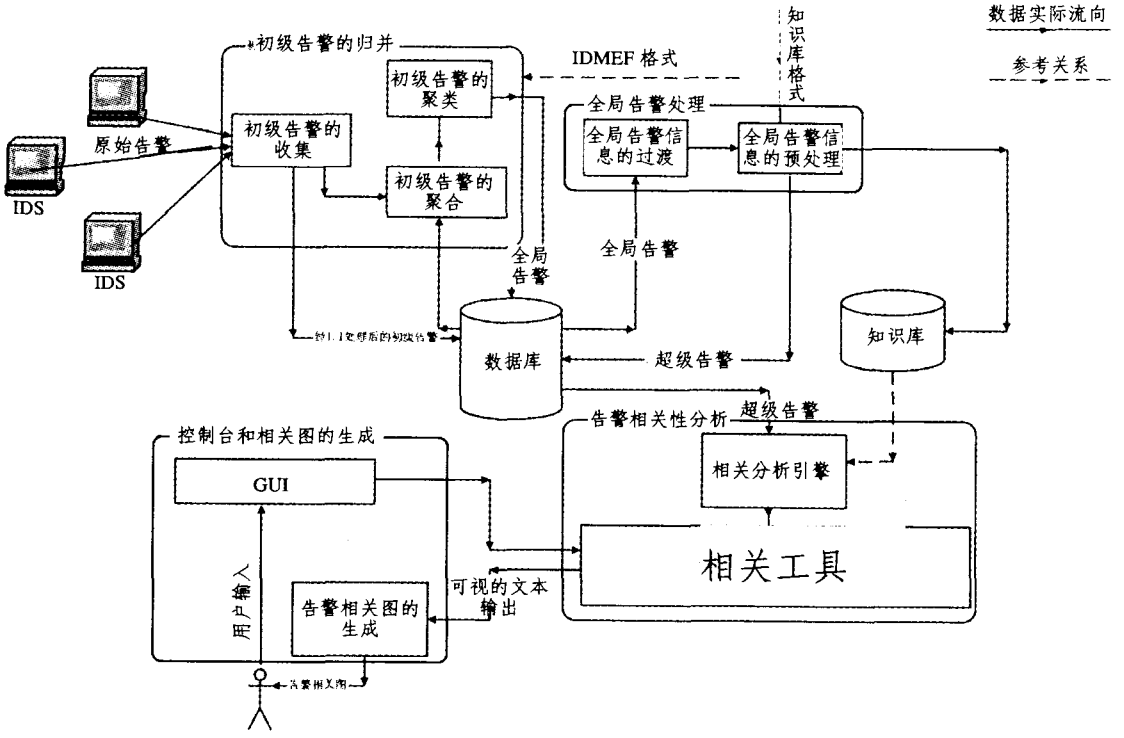

图 2 告警相关部件流程图

3 告警相关部件的设计和实现

该部件采用面向对象编程语言 Java 编写;数据库使用目前流行的 SQL server 关系型数据库系统;采用 XML(eXtensible Markup Language)语言存放知识库的内容。相关图的显示和实现利用 Graphviz 程序,该程序能将简单的图形文件转化为可视化的图形。

3.1 初级告警归并的设计

如图 2 中的"初级告警的归并"子模块。在分布式入侵检测系统中,为了更好地检测入侵,通常采用不同类型的 IDS,但这使得对同一种攻击,可能产生不同格式的告警,且由于 IDS 本身方法上的缺陷(都是针对初级信息),同一个 IDS 也会生成大量的重复告警信息。因此,本文使用该模块收集初级告警信息,统一信息格式,祛除其中的重复告警,形成全局告警,并将其存入数据库,步骤如下:(1)初级告警的收集。将不同的告警格式转化为统一的 IDMEF 格式,使每个告警都有 7 个属性,分别为时间(time)、类型(name)、传感器 ID 号(sensorID)、源/目的 IP 地址和源/目的端口号,其属性值用 IDMEF 规定的格式表示。(2)初级告警的聚合。比较告警中除时间和传感器 ID 之外的 5 个属性,如果完全相同,则用一个告警代替其他告警。(3)初级告警的聚类。利用源/目的 IP 地址和源/目的端口号、告警类型和时间等属性将相同攻

击产生的告警进行聚类分析，将一类告警用一个全局告警表示。

3.2 全局告警处理的设计

该部分的设计见图2中的“全局告警处理”模块。该模块将全局告警转化成为三元组形式的超级告警，包括两个过程：全局告警的过滤和相关的预处理。过滤是将全局告警中完全不可能相关的告警信息去掉，以减少相关总时间，提高效率；相关预处理是利用知识库中已有的知识分析得到超级告警：将全局告警的类型属性与知识库中的告警类型比较，得出其对应的前提集和结果集，填充三元组作为超级告警。

3.3 告警相关性分析的设计

如图2中的“告警相关性分析”模块。根据因果相关思想，如果后一个告警的前提和前一个告警的结果一样，这两个告警就可视为相关的告警。因此，该模块通过判断以下两个条件进行相关性分析：(1)超级告警的前提集和结果集中是否有相同的元素；(2)根据前提对应告警的时间是否晚于结果集对应告警的时间，来判断两个超级告警是否相关。最后将相关结果作为相关表保存到数据库，为相关图显示做准备。

3.4 控制台和相关图生成的设计

见图2中的“告警相关性分析”模块。该模块设计上主要完成两个任务：(1)和用户交互，用户输入知识库路径，数据库名称，用户名及密码，结果存放路径等信息；(2)读取“告警相关性分析”模块的相关表，生成文本文件，再利用graphviz程序显示告警相关图。

4 性能分析

本文对告警相关部件进行了相关测试，硬件环境CPU：2.4G，内存：512M，硬盘：40G；软件环境：windows 2000 professional，SQL server 2000数据库系统。

测试主要针对两个方面：相关速度和相关效果。考虑到影响相关速度的因素主要是告警到达后的预处理和相关分析的时间，为了做到告警连续不断地到达，本文在测试时先用入侵检测系统snort对DARPA 2000数据集进行检测，在收集到一定数量的告警后再用该部件处理。测试时，将告警按数量分为大小不等的几个部分，每部分的相关速度做3次平均值。结论如下：相关时间随告警数量的增长呈线性增长；用30多个超级告警(包括端口扫描、FTP、扫描等攻击类型)及其对应前提、结果作为专家知识进行判断时，平均每秒处理的告警数量为83.78。

此次测试中，相关效果主要通过告警减少率(经告警相关部件处理后减少的告警数量与入侵检测系统产生的初级告警数量的比值)来判断，snort生成的3,112个初级告警经上述测试平台处理后，最终有522个超级告警，告警减少率达到83.26%。这是由于大部分入侵检测系统都采用低级的检测方法，一个攻击(如DOS攻击)往往能产生很多初级告警，该部件处理后能大大减少告警数量，且生成的告警信息内容更加丰富，便于管理员快速对入侵进行响应。

结论 本文针对目前入侵检测系统中告警数目过多、难以处理的问题，基于Ning Peng的因果相关思想，设计并实现了告警相关部件。实验表明，该部件可以大大减少告警数量，并能有效快速地对告警信息进行相关性分析，且能以图形的形式将告警相关结果显示出来。

但现在仍有一些问题急需解决：(1)告警相关部件的数据源是入侵检测系统产生的告警，因此相关效果一定程度上受入侵检测系统本身性能限制，如果可以利用相关方法判断告警的准确性和可能的漏警，将既可以减少告警相关对入侵检测系统的依赖型，也可以提高入侵检测系统的性能；(2)因果相关本身还是一种基于已有知识的相关方法，对全新的攻击过程仍然无法正确识别，因此可以将因果相关与其他相关方法相结合，以识别新的相关关系；(3)测试中相关效果部分只测试了告警减少率，相关准确度、相关冗余度等都没有判断。这将是下一步的研究工作。

参考文献

1 Ning P, Reeves D, Cui Y. Correlating alerts using prerequisites of intrusions: [Technical Report TR-2001-13]. North Carolina State University, Department of Computer Science, Dec. 2001

2 Morin B, Debar H. Correlation of Intrusion Symptoms: an Application of Chronicles. In: Proc. of the 6th symposium on Recent Advances in Intrusion Detection (RAID 2003)

3 Ning P, Cui Y, Reeves D S. Analyzing intensive intrusion alerts via correlation. In: Proc. of the 5th Intl. Symposium on Recent Advances in Intrusion Detection (RAID 2002)

4 Templeton S, Levitt K. A requires/provides model for computer attacks. In: Proc. of New Security Paradigms Workshop. ACM Press, 31～38

5 Qin X, Lee W. Statistical Causality Analysis of INFOSEC Alert Data. In: Proc. of the 6th Intl. Symposium on Recent Advances in Intrusion Detection (RAID 2003)

6 Cuppens F. Managing alerts in a multi-intrusion detection environment. In: 17th Annual Computer Security Applications Conf. (ACSAC), 2001. 22～31

7 Ning P, Cui Y, Reeves D S, Xu D. Techniques and Tools for Analyzing Intrusion Alerts. ACM Transactions on Information and System Security (TISSEC 2004)

8 Cuppens F, Miege A. Alert Correlation in a Cooperative Intrusion Detection Framework. In: Proc. of the 2002 IEEE Symposium on Security and Privacy, May 2002. 202

9 Curry D, Debar H. Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition. draft-itetf-idwg-idmef-xml-03. txt, Feb. 2001