Bayesian 事件关联算法在分布式入侵检测系统中的应用

舒俊辉 杨 武 李 波
(重庆工学院 重庆400050)

摘 要 如何准确有效地检测分布式网络环境下多源可疑的入侵事件,并能进行关联分析和判定是入侵检测的核心问题。本文研究了一种面向分布式多源传感器实时事件数据采集及关联分析的方法,运用 Bayesian 算法进行事件分类处理。本文所提的模型已经在我们承担的教育部重点科技课题中得到实际应用,这种方法在复杂网络环境下能有效地分析攻击报警事件,帮助管理员从大量数据中找到有效的信息。

关键词 入侵检测系统(DIDS),关联,Bayesian

Application of Bayesian Correlation Arithmetic to Distributed Intrusion Detection System

SHU Jun-Hui YANG Wu LI Bo
(Chongqing Institute of Technology, Chongqing 400050)

Abstract On the basis of analyzing the Multiple-source events correlation in the Distributed Intrusion Detection, we introduce a framework of real-time events gathering and correlation analyzing, which is based on the Multiple Distributed Intrusion Detection's Sensors. Using Bayesian correlation arithmetic, we process the events such as filtering, reducing, and formatting them. At last, we provide the unified formatted evidences based on IDMEF to upper level model to deduce whether attack is true. The framework has been applied in our item projected by science and technology key project of National ministry of education.

Keywords DIDS, Correlation, Bayeian

1 引言

入侵检测系统(IDS)作为信息安全的第二道防线,通过对网络数据包及主机状态信息进行监控、检测进而判断企图破坏计算机资源的完整性、真实性和可用性的入侵行为,可以有效地保护计算机系统的安全。

分布式 IDS 针对传统 IDS 的缺陷,采用分布检测的方式,综合基于网络和基于主机的检测,从网络上不同的节点检测恶意的攻击行为,由分析器对报警信息进行分析和处理后,再提交给管理员或采取主动响应以保护计算机安全不受威胁。

目前,分布式入侵检测系统面临的主要问题之一是如何在大量数据中挖掘出潜在的关联事件,进行分类、归约,消除冗余事件,对事件进行时间、空间以及应用等不同角度的关联分析,找出相互之间的相关度以及关联关系,进而转化为入侵判定或推理的证据。本文在这方面做了一些有益的尝试。

2 相关工作

入侵检测系统发展至今,出现了许多原型系统和商业产品,一些公司和研究机构也在入侵事件的融合分析上做了大量工作。EMERALD 是 SRI 继 IDES、NIDES 之后提出的新一代入侵检测系统架构,它采用专家系统的方法对入侵事件做出推理判断。EMERALD 的专家系统技术称为 P-BEST (Production-Based Expert System Toolset),推理分析模块 eXpert 利用它来判断是否针对网络的恶意攻击行为。P-BEST 包含一个规则解析器,一个运行时程序库以及一组垃圾收集程序。规则解析器在系统初始化时翻译检测规则并将系统编译为可执行程序;当检测到报警事件后,系统调用运行期程序库将检测规则与报警事件进行模式匹配,确认攻击是否发生。P-BEST 的缺陷在于很难发现未知的攻击行为,而且只有当系统检测到的报警事件各种属性值完备且符合预定义的规则时,才能得出比较好的推理结果。

IBM Zurich 实验室的 Debar 等人向 RAID 2001 提交了一篇名为《Aggregation and Correlation of Intrusion- Detection Alerts》的论文,该文详细阐述了他们针对入侵报警事件所做的工作。Debar 提出利用现有的 IDS 产品收集入侵报警事件,然后在 IBM 的 Tivoli Enterprise Console (TEC) 中设计分析模块: Aggregation and Correlation Components (ACCS),在 Probe、Target、Source、Detailed target 四个层次上对多源入侵报警事件进行聚合和关联,将多 Sensor 检测到的事件处理后,提交给 TEC 的报告模块,实现网络域内报警信息的综合管理。这种方法能降低报警事件的数目,但不能识别复杂的网络攻击行为,也无法辨别报警事件的真伪,在实际应用中有一定局限性。

总体上,目前的 IDS 产品初步具备入侵推理的能力,但这些推理方法还存在着不足,只能应用于很小的范围。问题的关键在于能否对分布的入侵事件进行多层次、多角度的关联分析。随着黑客入侵行为的增长,各种入侵方式层出不穷,如何准确地对报警事件进行分析和处理,以降低 IDS 的误报率,从大量信息中识别黑客真正的攻击行动,是 IDS 研究和发展的重点。为此,我们提出了对可疑的入侵事件进行时间、空间以及应用等多层次、多角度的关联分析的思想,关联分析

*)基金项目:教育部科技重点项目(03115),重庆市科技公关项目((CSTC2004AC2018)。

的结果将提交给上层模块，采用各种融合推理算法，对入侵报警事件进行融合推理判定，识别真正的黑客攻击行为。分以下3个步骤来设计实现：

1）数据获取：支持多类IDS系统，收集多源异构的报警信息，并按标准的数据格式进行归一化处理，利于关联模块进行关联分析。

2）数据预处理：对入侵检测数据进行预处理，包括消除脏数据、归约重复性事件、进行数据转换等。

3）事件关联：对入侵报警事件进行链接，识别出同一事件的多次报警，消除语义二义性；而后对事件进行预测分类，为融合推理进行预分析处理。

4）融合推理：采用各种融合推理算法，对入侵报警事件进行融合推理判定，识别真正的黑客攻击行为。

3 分布式入侵事件关联

3.1 数据一致性描述

鉴于不同类型的Sensor具有不同格式的入侵事件描述，因此作为事件关联的第一步，需要采用标准的数据格式对事件进行描述。IDMEF是IDWG发起的一份建议草案，它通过定义IDS系统、组件及其他安全产品之间进行互操作的数据格式，实现信息共享。如图1所示，参考IDMEF的草案，我们建立了Alert_Object数据结构，包括Analyzer，Signature，Target，Source，Response等子类，分别描述了Sensor的地址和属性，攻击事件详细说明，被攻击者的地址和主机属性，攻击发起者的地址和主机属性，安全响应策略等信息。多源异构的Sensor采用Alert_Object存储报警事件Events，并向NSM发送，由NSM的预处理器进行统一处理。

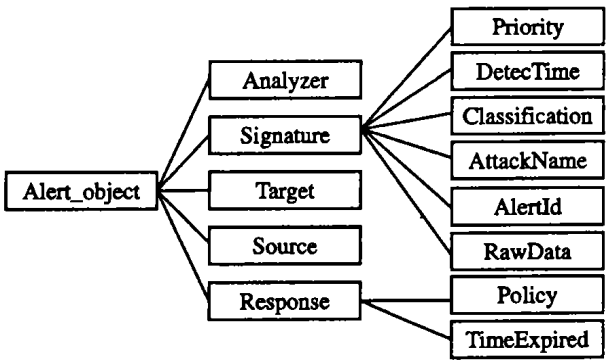

图1 入侵事件标准数据格式

3.2 事件预处理

原始的入侵事件常常是不正确、不完整、不一致的。检测数据异常、对待分析的数据进行归约，并将数据转换为符合内部推理机制的证据，将有助于提高以后关联和推理过程的精度与性能。

3.2.1 *事件过滤* 由于大规模网络的复杂性和黑客攻击的不确定性，多源异构的Sensor所产生的入侵报警可能存在某种错误，直接对这些包含错误信息的Events进行关联处理，将影响结果的精度和处理的效率。因此首先需要对Events进行事件过滤，消除脏数据和噪声数据。考查分布式入侵检测系统的工作环境，入侵报警事件的测量值有可能在下列方面产生随机错误或偏差：

·时间错误：在分布式系统中，硬件环境的差异或人为因素的干扰，各子系统时钟的不一致是正常现象，但这对关联分析及判断可能导致错误。因此，在事件过滤阶段中，将需要针对Events的时间值进行检测，若发现明显错误则需要进行纠正，统一到一致的时钟标准上。

·地址错误：许多黑客在进行DOS攻击时，为了掩饰自身的信息，往往采用伪造地址的方法，即填写错误的源地址或根本不存在的IP地址。大量伪造的地址将严重影响事件的关联分析，因此需要对Events中的IP地址进行检查，若发现地址错误则需进行统一标记，供上层模块分析。

·攻击错误：网络攻击总是针对特定的操作系统或漏洞进行的，若在Events报告中，攻击事件与目标系统实际情况不符，则可认为是Sensor的检测信息出现了错误。例如，当Events报告了Wu-Ftp攻击事件而目标主机并未开放Ftp时，可认为这是一个错误的事件报告。

3.2.2 *事件归约* 就是对原始报警事件进行评估，合并重复性事件，这样有利于提高关联分析过程的处理效率，同时帮助管理员从整体上把握网络的安全状况。文[4]阐述了一种利用后向搜索和前向推理进行归约的方法。在此基础上，我们提出一种实时事件归约算法，称为RTDRA (Real-Time Duplicate Reduction Algorithm)。

定义1 Duplicate是这样的两个或多个Events，它们包含相似的信息，具有固定的内在联系，描述同一个黑客攻击事件。它们可能被一个Sensor检测上报，也可能由多个异构Sensor检测出。

RTDRA算法需要对Events的以下4个属性进行考察，以确定待检测的多个Events是否确实属于Duplicate事件，第5个属性给出Duplicate事件的敏感度：

·Attack Name：入侵事件的攻击名称，该属性指明Sensor检测到发生了哪种攻击。

·Source IP Address：发起攻击者的IP地址。

·Target IP Address：遭受攻击者的IP地址。

·Detect Time：Sensor检测到攻击发生的时间戳。

·Severity：经过归约处理后的Events敏感度，指出了该事件对系统安全的威胁程度，它的值为0～1。若取值为0时，说明Duplicate事件对系统安全无影响，可以简单地丢弃该事件。

设系统接到新的报警事件Events B，采用RTDRA算法查找Duplicate事件，进行事件归约：

(1) 根据B的Attack Name进行分类，查找相应攻击类型的事件列表。

(2) 遍历该攻击的事件列表，按B→Source IP搜索，设找到Events A，如A具有与B相同的源地址，则继续按B→Target IP匹配，若匹配成功，转(4)；若匹配不成功，则转(2)重新按B源地址进行匹配。若事件列表已空，转(3)。

(3) 将B加入属于Attack Name攻击类型的事件列表，将Detect Time记入Start_Detect_Time字段并启动计时器。退出本函数，等待下一个Events的到来。

(4) 判断B与A是否Duplicate事件，若是A事件Duplicate计数加1，则A事件Count属性计数加1，调用Severity-Count()函数计算Severity值，并更新A中Severity属性的值，使用B→Detect Time更新End_Detect_Time字段，计时器重新计时。

(5) 计时器时间到，将Duplicate事件A输出，同时输出Count，Start_Detect_Time，End_Detect_Time，Severity等属性。清除事件列表中的过期事件A。

3.2.3 *事件转换* 归约处理后的入侵事件需要转换为

证据，供关联模块和推理模块进行处理。证据的形式使用元入侵事件(Meta Intrusion Event)来表述，从内容上分析，它定义了导致安全滥用事件发生的特征、条件、时序和关系等因素；从性能上要求，它具有以下的特征：(1)唯一性：每个元事件类型都是唯一的，相互之间不具有交集；(2)一致性：元事件之间不存在冲突，根据元事件推理得出的结论不会发生矛盾；(3)完备性：理论上，利用元事件定义的证据库，总能在推理模块中复合生成安全目标判定。

我们用一个 N 元组来描述元入侵事件：

Evidence ::= ⟨sensor_type, protocol, attack_name, start_time, end_time, sensor_ip, {[src_ip, src_port]* | [src_host, src_process]}, {[dst_ip, dst_port]* | [dst_host, dst_process]}, Count, Severity, data⟩

由于 Evidence 是经过归约处理后的证据，它的源地址和目的地址字段有可能包含多个地址，因此需要根据实际情况，使用多个元组记录所有的地址信息。而基于主机和基于网络的 Sensor 均采用统一的格式向 NSMS 发送 Events，因此元入侵事件的表述应该能够包含两种 Sensor 不同的报警信息，在描述地址信息时，可能使用 IP 地址，也可能使用主机系统名称。

3.3 事件关联

事件数据的关联是进行融合推理判定的关键之一，进行推理判断前，首先要针对大量 Evidence 进行关联分类，才能得到较好的推理效果。在大型网络环境中，分布式 IDS 通过数目众多的 Sensor 检测网络的安全状况，采用关联分析，来自每个 Sensor 的证据 Evidence 将不再孤立地显示在用户界面上，管理员可以从分类清晰、定义明确的一组证据中发现黑客有序的攻击行为。

在复杂的网络入侵攻击及检测中，黑客的攻击行为往往是多变的、分步骤的和综合的，因此在发现某一可疑事件后，不能只看当前获得的证据而判定是否发生了入侵，而应当从时间、空间、攻击等多个角度进行关联分析：

1) 证据的时间关联：将当前证据和历史证据进行关联分析，主要使用时间参数进行关联。

2) 证据的空间关联：将当前证据和涉及其他网络地址的证据进行关联，这在分布式入侵的情况下尤其重要。主要使用 Sensor 地址，源和目的地址以及网络端口进行关联。

3) 证据的攻击关联：各种攻击方式相互之间存在着一定的联系，例如扫描往往是一次入侵的前奏。主要使用攻击方式进行相互关联。

3.3.1 *简单贝叶斯分类算法* 我们采用简单贝叶斯的分类方法对证据进行关联，其工作原理如下：

1. 每个数据样本用一个7 维特征向量 $X=\{x_1,x_2,\cdots,x_7\}$ 表示，分别描述对7 个属性 $A_1,A_2,\cdots,A_7$ 的度量。A_1 到 A_7 分别对应 N 元组中的7 个属性 attack_name，time，sensor_ip，src_ip，src_port，dst_ip，dst_port。

2. 假定已有 M 个类 $C_1,C_2,\cdots,C_m$，给定一个未知分类号的数据样本 x，分类法将根据贝叶斯定理 $P(C_i|x)=\frac{P(x|C_i)P(C_i)}{P(x)}$ 计算 x 与现有的 m 个类的后验概率 $P(C_i|x)$，其中，$P(x|C_i)=\prod_{k=1}^{7}P(x_k|C_i)$。若 $P(C_i|x)\geqslant P$(P 是预先给定的概率阈值)，则预测 x 属于类 C_i。否则，创建新的类 C_{m+1}，预测 x 属于类 C_{m+1}。

3. $P(x)$是 x 的先验概率，即任意挑选的一个数据样本为 x 的概率。由于对所有类来说，$P(x)$为常数，因此 $P(C_i|x)\geqslant P$ 可变为 $P(x|C_i)P(C_i)\geqslant P(x)P$，假设给定阈值 $P(x)P$，首先计算 $P(x|C_i)$，可用样本进行估值 $P(x_k|C_i)=S_{ik}/S_i$，其中 s_k 是在属性 A_k 上具有值 x_k 的类 C_i 的样本数，而 S_i 是 C_i 中的样本数。

3.3.2 *采用特征相似度方法对贝叶斯算法进行修正* 由于每一个可能相关联的证据中，attack_name 属性是不一致的，例如一次 DDOS 攻击的序列为：扫描→漏洞分析→提升权限→安装后门→发起攻击；无法采用样本统计的方法来估算 $P(x_{attack\_name}|C_i)$，因此需要采用计算特征相似度的方法对朴素贝叶斯分类进行修正，使用特征相似度的计算值代替统计样本估值作为属性 attack_name 在分类 C_i 上的先验概率。

文[8]中阐述了通过计算特征相似度从而预测两个证据是否相互关联的方法。计算相似度的公式为：

$$SIM(X,C)=(\sum_j SIM(X,C_j)E_j)/\sum_j E_j$$

其中，X 为系统新接到的证据，C 为待计算相似度的分类，j 指出 C 中的样本编号，C_j是 C 中的第 j 号证据样本，若 X 与 C 关联成功时人们对样本 j 的期望相似度是 E_j，$SIM(X,C_j)$ 从给定的相似度矩阵得出，即关于攻击方式的相似度矩阵作为计算的先验知识已经给出。

结束语 本文所提的模型已经在我们承担的教育部重点科技课题中得到实际应用，这种方法在复杂网络环境下能有效地分析攻击报警事件，帮助管理员从大量数据中找到有效的信息。当然，本文所提的方法也存在不足和有待改进之处，表现为：1)这种方法需要预先提取黑客的攻击特征模式，具有足够的知识库和特征相似度矩阵；2)具有自适应的相似度计算能力，以适应复杂的分布式协同攻击判定；3)采用朴素贝叶斯算法可以定量地进行入侵事件的关联，初步实现了入侵事件的多角度分析，但其相对来说比较简单，对于复杂条件下的事件关联准确度不够，同时缺乏自学习的功能。因此需要找到更好的关联算法，同时要收集足够的训练数据，提高关联的准确度。

参 考 文 献

1 McHugh J, Christie A, Allen J. Defending Yourself :The Role of IntrusionDetection Systems. IEEE SOFTWARE September/October 2000

2 http://www.sdl.sri.com/projects/emerald/project.html

3 http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-06.txt

4 http://www.ietf.org/html.charters/idwg-charter.html

5 Han Jiawei, Kambr M. Data Mining: Concepts and Techniques . Copyright 2001 by Morgan Kaufmann Publishers, Inc.

6 Valdes A, Skinner K. Probabilistic Alert Correlation. RAID 2001, LNCS 2212, 2001. 54～68

7 Lindqvist U, Porras P A. Detecting Computer and Network Misuse Through theProduction-based Expert System Toolset (P-BEST). In: Proc. of the 1999 IEEE Symposium on Security and Privacy, Oakland, California, May 1999

8 Debar H, Wespi A. Aggregation and Correlation of Intrusion- Detection Alerts. RAID 2001, LNCS 2212, 2001. 85～103