基于威胁度的动态报警管理研究*)

石 进 陆 音 谢 立
(南京大学计算机软件新技术国家重点实验室 南京 210093)
(南京大学计算机科学与技术系 南京 210093)

摘 要 IDS目前的主要问题之一是过高的误报率,这一方面给管理员增加了繁重的工作负担,从而使其可能忽视了系统中真正需要处理的关键攻击事件;另一方面,过高的误报率使得自动入侵响应,比如与防火墙联动,不能很好地执行下去。针对这个问题,提出了基于威胁度的动态报警管理TDAM模型,它通过对系统环境的感知分析报警信息,确定其威胁度。通过实验,可以得出TDAM框架能够比较好地进行报警评价、管理。

关键词 入侵检测,报警管理,博弈理论

Research on Threat-based Dynamic Alerts Management

SHI Jin LU Yin XIE Li
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract One of the primary issues of IDSes is excessive false positives. This adds heavy burden to the system manager, which may lead the essential attacks to be ignored, and lead the automated intrusion response, e.g. cooperating with firewalls, can't carry out well. To resolve these issue, this paper presents a TDAM (Threat-based Dynamic Alerts Management) model. It analyzes alerts by apperceiving the system environment to specify the alerts' threat. A conclusion can be drawn from the experiment that the TDAM model can well apply in alerts evaluation and management.

Keywords Intrusion detection, Alerts management, Game theory

1 引言

自从20世纪80年代James Anderson[1]首先提出入侵检测概念以来,入侵检测系统作为网络安全的一个组件获得了极大的发展。许多研发机构和安全厂商都在进行这方面的研究和开发,推出了很多相应的产品。虽然功能越来越强,但它们目前都存在着一个重要问题:过高的误报率[2]。这一方面给管理员增加了繁重的工作负担,从而使其可能忽视了系统中真正需要处理的关键攻击事件;另一方面,过高的误报率使得自动入侵响应,比如与防火墙联动,不能很好地执行下去。

本文从IDS自身的特点出发,提出了一个能感知IDS所处系统环境的基于威胁度的报警管理TDAM(Threat-based Dynamic Alerts Management)模型,该模型较之以前的一些报警评价研究[3,4]在评价标准上进行了改进,使用了威胁度的概念,即在通常使用的可信度评价标准的基础上,增加了对危险度的评价,并增加了节点、服务的价值和节点安全度等概念,使得评价模型更加全面、科学和合理。在报警威胁度的计算上,本文使用了改进了的基于模糊数学的多层模糊模型识别的方法,并且我们在评判矩阵、权值的确定方面进行了改进和简化,降低了参数的不确定性。这种算法较之以前的研究[3,4]在算法原理上更加贴近于报警评价的原理,并且在计算中,减少了计算的步骤和复杂度,减少了需要人工确定或学习的参数,因此报警评价计算的准确度得到了提高。

本文的第2部分将介绍TDAM模型的分析过程、原理和主要算法,第3部分给出了DAMR框架原型的实现和实验,最后是结论。

2 基于报警威胁度的动态报警管理TDAM模型

如何对IDS报警信息进行评价和管理一直是入侵检测研究领域的重要课题,一方面它能让系统管理员从海量的报警信息中发现较为可信的关键的报警信息,另一方面对系统的进一步响应包括自动响应也起着促进的作用。但是目前已有的一些报警评价和管理机制往往不够明确,其评价因素也不够全面。本文TDAM模型提出了一个新的报警评价体系:报警威胁度,它将报警可信度和危险度结合在一起,全面地考虑了报警信息评价的各个因素并明确了评价标准。

根据IETF入侵检测工作组IDWG(Intrusion Detection Working Group)起草的入侵检测信息交换格式IDMEF(Intrusion Detection Message Exchange Format)[5],一般的IDS报警信息包含的属性主要包括时间戳、源IP、目的IP、端口号、攻击类型和探测器ID等。如果要对IDS报警信息的威胁度进行评价,仅凭IDS报警提供的这些信息是不够的,为此还要确定以下一些基本元素。

2.1 基本元素

2.1.1 节点、服务

在这里使用的节点概念和网络系统中使用的节点概念是

*)本文得到国家自然科学基金(No. 60373064)、国家863计算(No. 2003AA144010)和江苏省高技术研究计划(BG2005029)资助。石 进 博士研究生,研究方向为网络安全、系统安全;陆 音 博士研究生,研究方向为网络安全、下一代互联网;谢 立 教授,博导,研究方向为系统安全、网络安全。

相同的，它指的是网络中一个特殊的机器和设备，而服务指的是一个节点所提供的基于局域网或 Internet 的网络服务。节点和服务对进入系统的连接来说是目的地。

2.1.2 节点价值和服务价值

节点价值是一个用来表示节点重要性的量化的一个值。我们设节点价值度量的范围从 1 到 10，其中 1 表示的是最低的重要性，而 10 表示最高的重要性。一些诸如不重要的匿名 FTP 服务器或者密罐(Honey pot)系统等节点的节点价值可能被赋予 1；相反，像生产服务器这样非常关键的节点可能被赋予一个比较高的节点价值比如 9。像节点一样，每一个服务都要赋予一个表示服务重要性的服务价值，其范围也是从 1 到 10。节点价值、服务价值的度量范围和取值是根据整个系统的具体情况由系统管理员指定的。

如果在一个有很多节点、服务的网络，特别是一些大型的企业网络，要在整个网络里对每台主机和服务逐一分配或修改节点价值和服务价值将是一件非常繁琐且困难的事。为了减少节点管理的复杂性以及便于对节点和服务的价值进行分配，这时可以引入了角色的概念。这儿的角色借鉴了 RBAC (Role-Based Access Control)[6] 中的角色某些特征，它与 RBAC 中的角色最大的不同在于对角色赋予的是价值属性而不是授权。

2.1.3 节点安全度

和节点价值与服务价值标示的是节点与服务的重要性相似，节点的安全度标示的是节点的安全性。节点的安全度也是一个量化的值，它由节点安装的操作系统及版本，应用程序，开放的服务、端口，使用的安全措施以及它在网络中的位置等来确定。它的值在一个范围之间，同节点价值一样，设为 1 到 10，其中 1 表示最低的安全度，10 表示最高安全度。一台安装了 Windows98 并且没有加装安全补丁，而且其大部分端口都开放的节点可以评估它的安全度为 1，另一台安装 RedHat AS3 且安装当前所有补丁，安装单机防火墙，关闭了大多数服务的节点，可以评估它的安全度为 9。节点安全度是由报警管理系统或系统管理员针对每一个节点的情况进行评估得到的。

2.2 报警信息的威胁度

对报警信息的评价，我们确定评价出来的等级为 10 个：0.1，0.2，0.3，…，1，值越大其威胁程度越高，而管理员也可以考虑根据其实际需要，对报警威胁度的等级分类成诸如高度威胁、中度威胁、轻度威胁和无威胁等。如上文所述，报警信息的威胁度包括两个方面：报警可信度与报警危险度。

2.2.1 报警可信度

报警可信度指的是报警信息所报攻击真实发生的可能性。首先，一般一种攻击要达到目的只能针对某种系统或服务程序的漏洞，因此可以通过将攻击所需的环境与目的地系统真实的环境进行对比来确定报警信息的可信度。本文将系统的环境归结到 5 个属性：操作系统的类型与版本、硬件类型、服务及使用的程序和版本、网络端口、应用。

同时，报警信息的可信度还与报警信息所报攻击的特征有很大的关系，如有的攻击的特征是一串字符，或某个特殊端口，当只检测到这一个特征时，其可信度较低；另外一些攻击，由一系列特殊操作组成，正常活动不会进行这套操作，这些类型的可信度相对较高。在本文中，根据攻击特征的不同将攻击分成扫描攻击，拒绝服务攻击，缓冲区溢出攻击，基于 Web 代码的攻击和其它攻击等几种类型并分配不同的可信程度。

其次报警信息所报攻击的相关攻击信息也影响其可信程度，其中相关攻击信息指系统中近段时间里是否存在和该攻击相关的辅助攻击；或类似的攻击是否已多次发生过。相关攻击信息对每一个报警需要建立一个强相关和弱相关攻击的列表。

最后，目的地的节点安全度，也影响着报警信息可信度，安全度高的系统势必会增加攻击成功的难度。综上所述，报警信息的威胁度与目的地系统的环境、攻击类型、相关攻击信息以及目的地系统节点安全度有关。

2.2.2 报警危险度

报警危险度指的是报警信息所报攻击如果真实发生时对系统的危险程度。对不同节点价值和服务价值的目的地发起同样的攻击，如果都成功的话，对系统造成的危害是不同的。同时，报警信息所报攻击自身，由于攻击目的和攻击方式的不同，导致攻击成功后对系统的影响，即危害程度也会不同，实际上一般的 IDS 也都有一个报警自身危险程度的评估。因此，报警危险度与报警目的地的节点价值、服务价值以及报警信息本身的危险度是直接相关的。

2.2.3 报警威胁度计算

由于报警威胁度实际上是个模糊概念，经过细致地分析和比较，本文采用多层模糊模型识别的方法进行报警威胁度评价。模型识别用于识别某个具体对象属于何种类别，而模糊模型识别是在标准模型和待识别对象可能是模糊的情况下的识别，这与我们前面分析的报警威胁度评价原理是非常吻合的。当然，由于本文报警威胁度的评价要先对报警可信度和报警危险度进行评价，报警可信度的评价还需要先对报警信息的环境匹配度进行评价，因此其算法还是多层传递的。具体如下：

设因素集为 $U=\{U_1,U_2\}$，其中 U_1 为报警可信度，U_2 为报警危险度；

评判集为 $V=\{V_1,V_2,\cdots,V_n\}$，其中从 V_1 到 V_n 表示从低到高报警威胁度的 n 个评价等级，本文中 $n=10$。而因素 U_1 和 U_2 又分别由以下因素决定：

$U_1=\{u_{11},u_{12},u_{13},u_{14}\}$，其中 u_{11}、u_{12}、u_{13}、u_{14} 分别指的是环境匹配度、攻击类型可信度、相关攻击情况、节点安全度诸因素。

$U_2=\{u_{21},u_{22},u_{23}\}$，其中 u_{21}、u_{22}、u_{23} 分别指的是报警自身危险度、节点价值、服务价值。最后 $u_{11}=\{w_1,w_2,w_3,w_4,w_5\}$，其中 w_1、w_2、w_3、w_4、w_5 分别指的是操作系统、硬件、服务、端口、应用诸因素。

具体计算过程如下：

1. 根据已知各环境因素的匹配度计算环境匹配度 u_{11}。

先确定 u_{11} 的评判集 $p=\{0.1,0.2,\cdots,1\}$，表示环境匹配的从低到高的 10 个等级，然后确定 w_1、w_2、w_3、w_4、w_5 对各个评判等级的标准匹配度，建立匹配度矩阵 $R=\{R_{ij}\}$，可由专家确定或通过学习获得。本文的实验使用一种简便方法，即设 $R_{ij}=p_i$，表示在评价等级是 p_i 时因素 w_j 的匹配度，例如 $R_{34}=0.3$ 表示环境匹配等级为 0.3 时，报警所需端口和节点端口的匹配度应为 0.3。而对操作系统等因素的实际匹配情况，只确定三种，即匹配、不匹配和未知，匹配度取值分别为 1、0 和 0.5。这样，就能进行各因素实际匹配度和每一评判等级的标准匹配度进行贴近度计算来评判匹配等级。而由于各个因素的匹配情况对报警匹配情况影响的不同，因此在进行

对比时还要设定各自的权值 $a_1,\cdots,a_5$，其中 $\sum_{i=1}^{5}a_i=1$。贴近度的计算，我们使用比较容易理解的 *Euclid* 贴近度来进行计算，即计算 $\delta(r,R_j)=1-\sqrt{\frac{1}{5}\sum_{i=1}^{5}a_i(\xi-R_{ij})^2}$，其中 $r=(r_1,r_2,r_3,r_4,r_5)$ 表示报警 r 的实际匹配度，计算出来 $\delta(r,R_j)$ 值最大的表示报警 r 的实际环境匹配度等级为 j。

2. 使用和计算环境匹配度一样的方法来逐级计算可信度和危险度以及最后的报警威胁度。

类似步骤 1，可信度和危险度以及危险度的计算都是先确定相应的评判集，然后建立各自的标准匹配度矩阵，本文实验中其建立过程类似于环境匹配度矩阵。而报警的攻击类型等因素的实际匹配度取值，定义如下：攻击类型可信度的状态分为高、中、低三种，取值分别为 1、0.6、0.2，相关攻击的状态分别设为强相关、弱相关和无相关三种，取值分别为 1，0.7 和 0.4，自身危险度按通常 IDS 的风险等级设为高、中、低三种状态，取值分别为 1、0.6 和 0.2。节点安全度、节点价值、服务价值的状态见本文 2.1 节，计算时的取值要乘上 0.1，环境匹配度、可信度和危险度的取值为下层因素评判出来的等级。贴近度的计算依然使用 Euclid 贴近度来进行计算，最终计算出报警威胁度的等级。由于篇幅的关系，具体算法从略。

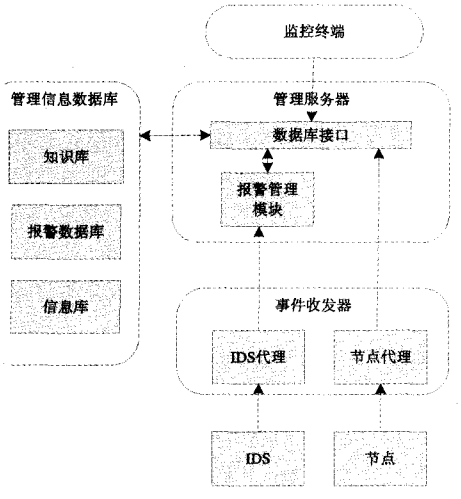

图 1　TDAM 实现框架图

以上算法中的环境匹配度、可信度、危险度以及威胁度的贴近度计算时的权值，首先由专家或管理员根据经验知识提出几种可能的权值方案，然后选用一些有代表性的报警，经贴近度计算与事先确定的评判值最相近的即为选用的权值方案。

3　TDAM 模型的实现和实验

3.1　TDAM 模型的实现

本文对基于威胁度的动态报警管理 TDAM 模型在南京大学主持开发的“网络安全管理平台”上进行了原型的实现。“网络安全管理平台”的主要功能是收集系统中节点、防火墙、IDS 等各部件的状态、日志、报警等相关信息并进行分析、评估和响应。TDAM 原型的实现如图 1，图中的管理信息数据库包括知识库、报警数据库和信息库。管理服务器包括数据库接口和报警管理模块。报警管理模块接收从 IDS 代理处传送过来的报警信息，经过评价通过数据库接口存放到报警数据库中。事件收发器包括 IDS 代理和节点代理，其中 IDS 代理和节点代理的功能是向管理服务器传送报警信息和节点主机的 OS、服务、应用等相关信息，并通过数据库接口存入信息库中。其中除报警管理模块以及知识库和信息库外其余部分均使用“网络安全管理平台”已有的模块。

3.2　实验环境

我们按图 2 建立了实验环境，其中模拟外网主机 10 台，内网主机 6 台，其中一台为管理平台 Mplat 并兼作管理信息数据库服务器，另外还有一台生产服务器 PrS，一台公共服务器 PuS，一台 DNS，还有两台是普通用户节点 Node1 和 Node2，其中 PuS 和 DNS 在 Firewall 的 DMZ 区。

为了更好地体现实验的仿真性，内网主机上安装的操作系统、开启的服务和配置的安全机制都是有差别的，这些状态信息都由各主机的节点代理收集并定时向管理平台汇报，由管理平台将它们转存到管理信息库中。内网的 6 台主机相应的节点价值、节点安全度和服务价值见表 1。

表 1　节点、服务价值及节点安全度信息表

	节点安全度	节点价值	服务价值				
			dns	ftp	http	telnet	smtp
Mplat	8	9	0	6	3	10	0
Pus	6	7	3	6	10	5	6
DNS	6	7	10	0	0	6	0
Node1	5	3	0	3	0	5	0
Node2	2	1	0	4	0	3	0
Prs	9	8	0	9	9	9	8

实验在外网主机和内网主机间共建立连接 13227 条，其中含有 150 次外网对内网的攻击，其余都是合法连接。

3.3　报警威胁度实验

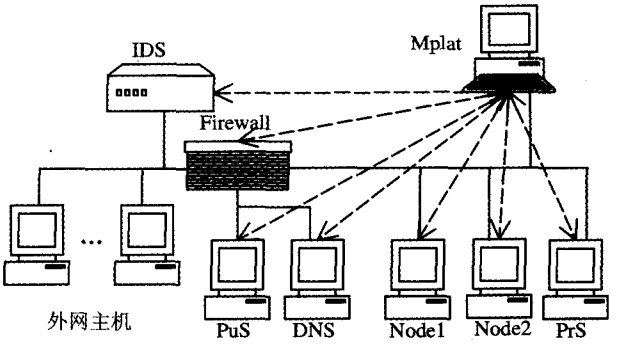

图 2　实验拓扑图

IDS 共发出了 693 次报警，其中针对 150 次攻击报警 163 次，在这 163 次报警中重复报警 41 次，有 28 次攻击未检测到。经过 TDAM 模型报警威胁度评估，结果如表 2 所示。

从表中可以看出，一方面，当报警威胁度比较低时，如不大于 0.2，IDS 报警误报率很高，达到了((348+152)−(3+5))/(348+152) * 100%=98.4%；而当报警威胁度比较高时，如不小于 0.9，IDS 报警误报率较低，仅为((11+3)−(9+2))/(11+3) * 100%=21.43%。如果我们将威胁度不大于 0.2 的报警过滤掉，则报警数量将会减少(348+152)/693 * 100% =72.15%，而此时被过滤掉的正确报警数仅为 3+5=8，占正确报警数的 8/163 * 100%= 4.91%，同时整体误报率却从(693−163)/693 * 100%=76.48%降低到了((693−348−152) −(163−3−5))/(693 − 348 − 152) * 100% = 19.68%。因此利用本文 TDAM 模型对报警信息进行管理可

（下转第 111 页）

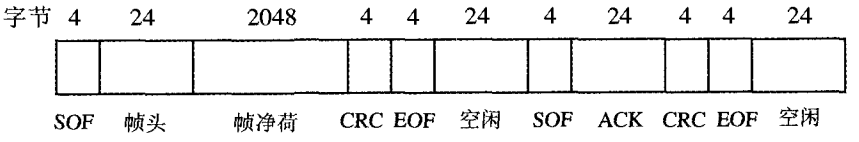

图5 带宽计算中的取样数据帧和ACK传送

SOF为帧头定界符;帧头表示源点、目标点、序列号和其它帧信息;CRC用于检验传送错误;EOF为帧尾界定符;空闲字节用于检错、同步和嵌入低层确认帧信息;ACK为确认信息。

光纤通道数据传输的基本时钟频率为1.0625GHz,2G的链路采用的是2倍频,考虑FC的0层使用8B/10B编码,则最大有效数据传输率为

$$S_{max}=2\times1.0625(\text{Gbit})\times2048(\text{B})\ /\ [(2048+120)(\text{B})\times10]=200.7\text{MByte/s}$$

尽管光纤通道的帧净荷长度可变,但传输帧需要的开销却是相同的。因此,随着净荷长度的缩短,有效数据传输率也会有所降低;另外,上述计算中没有考虑差错后的重传对性能的影响,由于光纤传输系统的误码率很低(如10^{-13}),因此,正常情况下差错重传的概率很低,重传对性能的影响很小。

结束语 本文利用FC的组播服务提出了一种基新的远程数据复制方法,该方法属于SAN层次的数据复制,能满足SHARE78[7]标准中第6级对数据进行实时备份的要求。该方法具有下列优点:

1)高度的灵活性。不仅与存储设备和应用服务平台无关,而且还可以根据应用的需要,建立多个组播域,实现不用类别信息的分类备份。

2)高性能。组播数据在交换结构层次而不是端口层次进行复制能大大提高带宽的利用率;另外,采用CWDM不仅可以提供存储设备与FC交换机之间的高带宽连接,还大大简化了数据复制的协议处理流程,提高了系统的效率。

3)高可用。可根据应用的需要,建立多个数据备份,提高系统数据的可用性。

随着4G和8G FC的普及,基于FC组播的数据复制方法的优点将更为明显,本文的研究结果将为城域网范围内的容灾提供一种高性能、高可靠的数据复制方法。

参考文献

1 2004 - FC-FS-2 Draft Standard. http://www.t11.org/ftp/t11/pub/fc/fs-2/04-045v0.pdf

2 Fibre Channel Generic Services - 5(FC-GS-5). http://www.t11.org/ftp/t11/pub/fc/ gs-5/06-192 v2.pdf

3 Qin Leihua, Zeng Dong, Liu Gang, et al. Network architecure of strage extension next generation SONET/SDH-based and GFP interface design of SONET/SDH with FPGA. In: Proceedings of SPIE, Network Architectures Management and Applications III, Shanghai, 2005. 965～973

4 Iannone P P, Reichmanna K C, Spiekman L H. Amplified CWDM systems. IEEE, 2003. 678～679

5 Qin Leihua, Yu Shengsheng, Zhou Jingli. Analysis and amendment of flow control credit-based in SAN extension. In: Proceedings of SPIE, Network Architectures Management and Applications III, Shanghai, 2005. 8595～973

6 Benner A F. 存储区域网光纤通路技术. 胡先志,胡佳妮,等译. 北京:人民邮电出版社,2003

7 IBM容灾白皮书. http://www-900.ibm.com/cn/ support/download/ Disaster-recovery.pdf

(上接第96页)

以从很大程度上减少报警数量和降低误报率,并且由于报警威胁度是基于可信度和危险度两方面的综合评价,这对管理员或其它工具进行进一步的分析和响应提供了相当坚实的依据。

表2 报警威胁度表

类别 / 威胁度	IDS报警数	正确报警数
0.1	348	3
0.2	152	5
0.3	55	31
0.4	33	37
0.5	38	38
0.6	30	17
0.7	16	14
0.8	7	7
0.9	11	9
1	3	2
合计	693	163

结论 本文针对当前入侵检测和响应领域的重要问题:过高的IDS误报率,提出了一种基于威胁度的动态报警管理TDAM模型。TDAM模型利用对所防护系统环境的感知,不仅对报警信息可信度而且对其危险度进行了评价,并将二者结合提出了报警威胁度。报警威胁度能更贴切地体现报警信息对系统的重要程度,对系统管理员来说有很高的参考价值,可以根据报警威胁度对报警信息进行统计、分类等管理。本文的实验进一步验证了TDAM模型在报警评价管理方面是有效而可行的。

参考文献

1 Anderson J P. Computer security threat monitoring and surveillance [R]. Fort Washington: James P. Anderson Company, 1980

2 Biermann E, Cloete E, Venter L M. A Comparison of Intrusion Detection Systems. Computers&Security, 2001, 20: 676～683

3 Phillip A P, Martin W F, Alfonso V. A mission-impact-based approach to INFOSEC alarm correlation [A]. In: Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID)2002[C]. Zurich Switzerland: Springer Verlag, 2002. 95～115

4 Qin X. A Probabilistic-Based Framework for INFOSEC Alert Correlation:[Ph. D. Dissertation]. College of Computing, Georgia Institute of Technology, USA, 2005

5 IETF Intrusion Detection Working Group. Intrusion detection message exchange format. http//www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-09.txt, 2002

6 Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based access control models. IEEE Computer, 1996,29(2):38～47