关于无线网络中分布式入侵检测系统的混合体系架构研究

李 焕

(咸阳职业技术学院 , 陕西 咸阳 712000)

摘 要 : 网络应用的快速增长 , 新型网络攻击层出不穷。因此 , 保护网络免受攻击和入侵检测技术的普及是至关重要的。因此 , 有必要从网络设计和部署开始就阐明这个安全问题。入侵检测技术是识别网络活动的过程 , 可以导致安全策略的妥协。在入侵侦测已经做了大量的工作 , 但解决方案并不令人满意。在本文中 , 我们提出了一种新的分布式入侵检测系统使用多代理 , 以减少误报和管理误用和异常检测。

关键词 : 入侵监测 ; 体系结构

中图分类号 :TP393 文献标识码 :A 文章编号 :1003-7241(2018)05-0052-05

Research On Hybrid Architecture for Distributed Intrusion Detection System in Wireless Network

LI Huan

(Xianyang Vocational Technical College, Xianyang 712000 China)

Abstract: With the rapid growth of the network application, new kinds of network attacks are emerging endlessly. So it is critical for the protection of networks from attacks and the popularity of intrusion detection technology. Therefore, it is necessary that this security concern must be articulate right from the beginning of the network design and deployment. The intrusion detection technology is the process of identifying network activity that can lead to a compromise of security policy. Lot of work has been done in detection of intruders. But the solutions are not satisfactory. In this paper, we propose a novel distributed intrusion detection system using multi agent, which can decrease false alarms and manage misuse and anomaly detects.

Key words: intrusion detection; architecture

1 引言

随着计算机网络的发展 , 计算机安全保护也抵制了巨型机在过去获得大规模无限计算机网络的安全。随着日常生活中信息技术的普及 , 对计算机安全的需求变得更加重要。威胁的本质已经由物理渗透和密码破解转变为计算机病毒 [1], 自我繁殖和自我复制的“蠕虫”病毒、秘密的软件、木马、脚本小子 , 计算机罪犯 , 恐怖分子名单很长。在计算机系统的可靠性和相应的风险和威胁的增加革命性的计算机安全技术 [5]。新的概念和样式正在被采用 , 新的工具正在被发明和安全意识的做法和政策正在实施。显然需要新的机制来处理这种新的复杂程度。

网络入侵检测系统 (NIDSs) 被认为是针对计算机系统的基于网络攻击的有效的第二道防线 [3][4], 而且 , 由于日益严重和此类攻击的可能性 - 采用几乎所有的大型 IT 基础设施 [2]。入侵检测系统 (IDS) 必须分析和关联从不同的关键网络接入点收集的大量数据。在本文中 , 我们提出了一种新的分布式入侵检测系统使用多代理 , 以减少误报和管理误用和异常检测。

2 系统结构

我们提出了新的架构建设 IDSs 采用代理作为他们的数据收集和分析的最低水平的因素和采用的结构允许的可扩展性。在一般情况下 , 主要有两种技术的入侵检

收稿日期 : 2017-01-13

测：误用基于签名的检测和异常基于行为的检测[6]。

在本文中，我们应用这两种技术。应用这两种技术的目的是试图检测系统中的任何攻击或入侵。如图 1 所示，提出的 IDS 架构包括七个模块 – 跟踪器，异常检测模块，误用检测模块，监视器，签名生成器，推理检测模块和对策模块结合三个检测模块的结果。

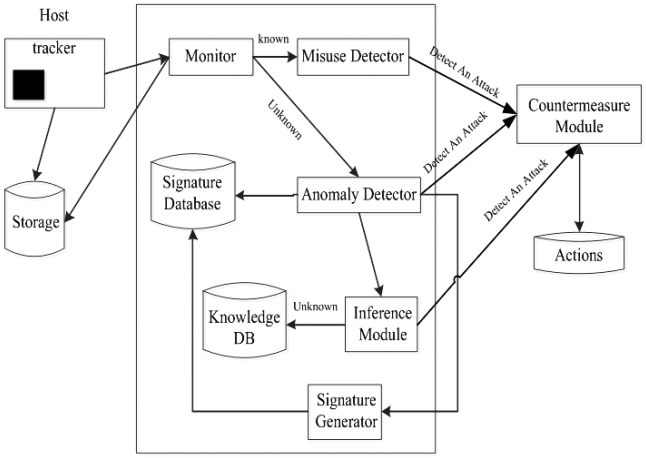

图 1 入侵检测系统的体系结构

跟踪器：跟踪器是一个独立运行的实体，监视主机的某些方面[7]。然后代理将生成一个报告，该报告被发送到适当的监视器，并存储在存储器中。代理没有权限直接生成告警。通常，对策模块将根据一个或多个代理／检测器接收到的信息生成告警。通过结合来自不同的代理的报告，监视器建立一个其主机图片的状态[8][10]。

监控：分析正在进行的过程，以确定其是否符合预期[11]。另一方面，通过使用模式匹配算法，将接收到的数据包与签名数据库中正常行为模式的签名或规则进行比较。如果监视器找到任何匹配，则向误用检测器模块发送已知攻击的适当消息[9]。它也在日志文件中输入关于引起警报的事件的条目。如果监视器没有找到任何匹配，然后将数据发送到异常检测器，使用模式挖掘技术发现异常。

误用检测器：误用检测代理像监视器一样工作，但它们之间的区别是详细的[12]。事实上，每个监视器作为独立的 IDS 和检测攻击本身只有不共享任何信息与另一 IDS 节点的系统，甚至不配合其他系统。因此，所有的入侵检测决策的基础上的信息提供给单个节点。它的效果太有限了。然而，每个节点运行自己的误用检测器，并最终他们合作，形成一个全球性的误用检测器。该代理是用来分析全球监测代理捕获的数据[13]。利用模式匹配算法检测网络中已知的攻击。如果数据库中接收到的报告与攻击签名之间存在相似性，则向对策模块报告以确定解决方案。

异常检测：使用异常检测代理，使用分类技术来检测新的或未知的攻击。分类与建立对象的正确类（或类别）有关[14]。分类是基于对象的特性[15]。异常检测代理收集数据从监视器分析数据来检测未知的攻击。然后进行分类，以检测新的攻击。分类模型的规范如图 3 所示。第一 while 循环生成候选解集。第二循环修剪这套新信息的获取。如果下列三个条件之一为真，则该方法将完成。

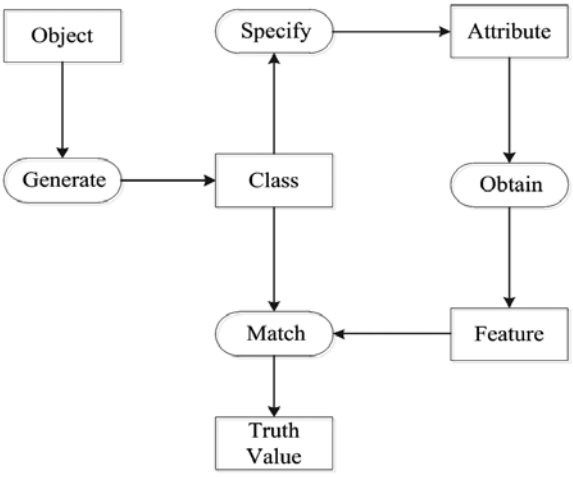

图 2 分类结构

```
While new-solution generate (object->candidate) do
Candiate-classes:=candidate Union candidate-classes;

While new-solution specify (candidate-classes->attribute)
And length candidate-classes > 1 do
Obtain(attribute->new-feature);
Current-feature-set:=new-feature union current-feature-set
For each candidate in candidate-classes do
Match(candidate+current-feature-set->truth-value);
If truth-value = false then
Candidate-classes:= candidate-classes subtract candidate;
```

图 3 分类模型的方法控制

图 2 显示了相应的推理结构。三个推论中使用的方法加上传递函数获得的属性值：

- 生成候选：在最简单的情况下，这一步只是在潜在候选解决方案的知识库中查找。
- 指定属性：有几种实现这种推理的方法。最简单的方法就是做随机选择。
- 获取特性：通常，允许用户输入一个“未知”值。此外，有时有域知识表明，某些属性应该始终同时得到。
- 匹配：每个候选执行此推理，并产生一个真值，指示候选类是否与所收集的信息一致。推理应该能够处

理某些属性的“未知”值。正常的做法是每个候选人都是一致的“未知”值。

分类后，如果异常检测器发现任何异常，然后发送适当的消息到推理模块进行更多的调查[16]。否则，它将报告发送给对策模块来决定解决方案，并与攻击进行对抗。

E. 推理模块：推理是知识模型的重要组成部分。推理作为推理过程的基石。在推理的知识，我们描述了如何将这些静态结构可以用来进行推理过程。该模块是在体系结构中最高水平的实体。它们还具有类似于异常检测器的控制和数据处理角色。推理模块和异常检测器之间的主要区别是，一个推理模块可以控制在几个不同的主机运行的实体，而异常检测器只控制本地代理[17]。本部分通过 KB 和签名的基本知识和规则决定。知识库包含与用户行为相关的知识类型的实例。该模块采用朴素贝叶斯分类器来检测新的攻击。基于知识数据库中可用的数据集它对数据进行分类[18]。如果传入的数据被检测为攻击手段，然后报告给签名生成器，这反过来又向警报代理报告有关攻击。它更新数据库中的检测到的攻击。

F. 签名生成器：签名生成器创建规则或签名，并在签名数据库中新建条目。然后它发送相应的消息来监控重新分析攻击。

G. 签名数据库记录使 IDS 具有一组签名、标准或规则，它们可以用来比较数据包像通过主机时的数据包一样。签名数据库需要与 IDS 软件和硬件本身一起安装。

H. 对策：对策模块接收模块时已知攻击的探测器的警报信息，它通知管理员有几种方式，管理员预先配置。例如该模块可能会显示一个弹出窗口或向指定的个人发送电子邮件。除了发送给管理员的自动响应外，此模块还可以在收到警报消息的同时进行操作配置[19]。典型的动作是：报警，其中警报发送给管理员；丢包，其中没有向发送计算机发送错误消息的数据包被删除；复位，指示 IDS 停止并重新启动网络流量，从而停止特别严重的攻击。此模块还由网络管理员使用，以评估警报消息，并采取适当的行动，如丢弃数据包或关闭连接。管理员可以预期要微调签名数据库，以考虑到 IDS 似乎是入侵的情况，但实际上是合法的流量[20]。例如，可能会进行调整，以启用可能被防火墙视为可疑的流量。例如由位于特定 IP 地址的扫描设备执行的漏洞扫描。IDS 可以被配置为添加一个规则，该规则改变 IDS 执行的操作，以响应从该 IP 地址到警报的流量[21]。

3 所提出的架构优异

3.1 架构的优点

以下是我们 IDS 的独特特性列表。

- 它将继续运行，以最少的人力监督。它将创建新攻击的签名。
- 这将是应用的分布式入侵检测系统。
- 这将是自适应的性质和适应用户和系统行为的变化。
- 它将提供才跟踪攻击者。
- 我们的 IDS 的设计使得它容错，以便它能够从崩溃中恢复过来。它可以得到它的前状态，并恢复其操作没有任何不利影响。
- 它将能够监视自己，并检测攻击。
- 这将是准确的，因此将有较少的误报和假阴性。

3.2 架构的缺点

我们已经确定了在建议的架构的几个缺点。入侵的推理模块的检测被推迟，直到从代理得到所有必要的信息。这是一个问题，常见的分布式入侵检测系统。体系结构没有指定访问控制机制，允许不同的用户对 IDS 有不同的访问级别。这是一个需要解决的问题。

在他们的控制作用下，推理模块是单点故障。如果推理模块停止工作，它所控制的异常检测器停止产生有用的信息。这是可以解决的，通过一个层次结构的失败的推理模块将注意到更高层次的显示器，并采取措施将开始一个新的推理和检查的情况下，导致原来的失败。另一种可能性是建立冗余监视器，检查同一组异常检测器，以便如果其中一个失败，则另一个可以在不中断其操作的情况下接管。如果使用重复的推理模块来提供冗余，则必须使用机制来保证冗余推理模块保持相同的信息，将得到相同的结果，并且不会干扰 IDS 的正常运行。

3.3 安全性

我们已经进行了分析性能比较，我们提出的方案与现有的计划。我们分析了他们的表现在两个主要因素，即安全性和效率。安全因素进一步分为三个参数，即内部的、外部和新的威胁。内部威胁是那些由网络内部的入侵者发起或注入的攻击。外部威胁来自外部攻击者。新的威胁是不寻常的或未确认的入侵形式，以前没有发生过。这些入侵所使用的三种可能的值是高、中、低，清楚地表示建议方案识别这些入侵。

我们给出了低值的所有计划，不提供防御的妥协节

点，攻击节点，内部攻击者，主密钥或密钥被捕获或节点的活动是依赖于邻居节点信息，信任关系节点等。所有建议的方案，确定入侵的中介价值，但不提供任何防御测量如何处理它们，产生大量的假阴性。高价值的所有这些计划，明确识别入侵以及提供针对这种入侵的对抗措施，一个节点的妥协不会使系统的整体安全性变得脆弱。

我们将效率因素划分为三个参数，即计算成本，网络带宽，节点资源利用率和消息的数量。在计算成本、网络带宽和节点资源利用率方面，采用了两种类型的值。我们已经给了高价值的所有方案，增加负担，网络资源即加密算法自然需要额外的计算和存储开销，节点之间的通信的步骤增加，同时传输增加碰撞影响带宽问题的速度，大量的假阴性消耗能量资源等。给出了利用受害资源，利用最小网络资源发现入侵的方案。包含整数值的消息数，即建议方案使用的附加步骤以识别入侵。

4 结束语

误用（基于签名）入侵检测技术的主要特点是在比较传入威胁对预定义的知识，为了决定是否威胁被认为是攻击或入侵，而异常检测技术涉及寻找任何意想不到的变化，对系统的行为被认为是正常的行为。误用和异常检测技术各有优缺点。在我们的 IDS 架构已经使用了入侵检测技术的特点。本文提出了一种正在进行的研究使用的入侵检测技术的特点，设计一个新的和有效的混合 IDS 的研究。IDS 建议的设计，目的是要更准确，它不需要更多的处理资源，从而提供速度和精度来检测入侵。

参考文献：

[1] EID M.A New Mobile Agent-Based Intrusion Detection System Using Distributed Sensors[J].Proceeding of Feasc,2004.

[2] ALLEN J,CHRISTIE A,FITHEN W,et al.State of the Practice of Intrusion Detection Technologies[J].State of the Practice of Intrusion Detection Technologies,2000.

[3] DEBAR H,DACIER M,WESPI A.A revised taxonomy for intrusion-detection systems[J].Annales Des Télé communications,2000,55(7-8):361-378.

[4] SCHULTZ E E.Intrusion Detection:Rebecca Bace Macmillan Technical Publishing,2000[J].Network Security,2000,2000(8):19.

[5] KARLOF C,WAGNER D.Secure routing in wireless sensor networks:attacks and countermeasures[C]//IEEE International Workshop on Sensor Network Protocols and Applications,2003.Proceedings of the First IEEE. IEEE,2003:113-127.

[6] AXELSSON S.Intrusion Detection Systems:A Survey and Taxonomy[J].Breast Cancer Research Bcr, 2000,17(1):1-10.

[7] LI Y,QIAN Z.Mobile Agents-Based Intrusion Detection System for Mobile Ad Hoc Networks[C]// International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering.IEEE Computer Society,2010:145-148.

[8] BRAHMI I,YAHIA S B,AOUADI H,et al. Towards a Multiagent-Based Distributed Intrusion Detection System Using Data Mining Approaches[M]// Agents and Data Mining Interaction.Springer Berlin Hei delberg,2011:173-194.

[9] JAISANKAR N,SARAVANAN R,SWAMY K D.Intelligent Detection System framework using Mobile agents[J].International Journal of Network Security&Its Applications,2009,1(2):72-88.

[10] JIN X,OSBORN S L.Architecture for Data Collection in Database Intrusion Detection Systems[C]// VLDB Conference on Secure Data Management.Springer-Verlag,2007:96-107.

[11] BOLZONI D,CRISPO B,ETALLE S.ATLANTIDES: An Architecture for Alert Verification in Network Intrusion Detection Systems[J].Usenix Association,2007:141-152.

[12] NISHIYAMA H,MINE Y,MIZOGUCHI F.The Design of a Secure Distributed Devices System Based on Immunity[J].Lecture Notes in Computer Science, 2004,(3233):330-344.

[13] WHITE G B,FISCH E A,POOCH U W.Coopera ting security managers:a peer-based intrusion detection system[J].IEEE Network,2002,10(1):20-23.

[14] DEPREN O,TOPALLAR M,ANARIM E,et al.An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks[J].Expert Systems with Applications,2005,29(4):713-722.

[15] SCHREIBER,MARTIN H M.Knowledge Enginee ring and Management[M]//Knowledge engineering and management:the CommonKADS methodology.MIT Press, 2000:39.

[16] SONI G,EZEIFE C I.An Automatic Email Management Approach Using Data Mining Techniques[C]// International Conference on Data Warehousing and Knowledge Discovery.Springer Berlin Heidelberg,2013:260-267.

[17] STOLFO S J,LEE W,CHAN P K,et al.Data mining-based intrusion detectors:an overview of the columbia IDS project[J].Acm Sigmod Record,2001,30

（下转第 60 页）

[5] 杜明 , 赵向军 . 改进 Retinex 的光照变化人脸图像增强算法 [J]. 计算机科学 ,2016,43(2):105-108.

[6] WANG Y,WANG H,YIN C,et al.Biologically inspired image enhancement based on Retinex[J].Neurocomputing,2016,(177):373-384.

[7] 赵华夏 , 禹晶 , 肖创柏 . 基于目的性优化及改进直方图均衡化的夜间彩色图像增强 [J]. 计算机研究与发展 ,2015,52(6):1424-1430.

[8] JIANG B,WOODELL G A,JOBSON D J.Novel multi-scale retinex with color restoration on graphics processing unit[J].Journal of Real-Time Image Processing,2015,10(2):239-253.

[9] TSAI C M.Adaptive Local Power-Law Transformation for Color Image Enhancement[J].Applied Mathematics&Information Sciences,2013,7(5):2019-2026.

[10] NNOLIM U A.Log-hybrid architecture for tonal correction combined with modified un-sharp masking filter algorithm for colour image enhancement[J].Integration the Vlsi Journal,2014,48(1):221-229.

作者简介 : 黄玉蕾 (1981-), 女 , 讲师 , 研究方向 : 数据挖掘 , 算法分析。

(上接第 51 页)

本文分析和总结了信息等级保护工作的定义与作用 , 综合考虑某高校办学层次与社会影响力 , 结合高校信息化建设中网络系统的特征与定级需求 , 对其进行定级描述、确定网络系统的业务信息安全保护等级、确定网络系统的服务安全保护等级 , 并结合安全保护定级与业务信息安全等级和系统服务安全等级的设定情况 , 将网络系统的定级确定为二级。

参考文献 :

[1] 范艳芳 . 重要信息系统强制访问控制模型研究 [D]. 北京 : 北京交通大学 ,2011.

[2] 黄勇 . 安全系统形式化设计与分析研究 [D]. 杭州 : 浙江大学 ,2009.

[3] 蔡鹏程 , 冯方回 . 等级保护与政务终端安全 [J]. 信息网络安全 ,2010,(8):64-66.

[4] 刘淑鹤 . 落实等级保护构筑安全“城堡” [J]. 信息安全与技术 ,2010,(6):5-8.

[5] 张宇 , 魏海 , 刘显傅 . 海洋环境观测数据传输网信息系统安全三级保护建设研究 [J]. 海洋信息 ,2013,(3):18-23.

[6] 马帅 . 等级保护设计要求下的移动业务系统安全防御体系 [J]. 保密科学技术 ,2012,(1):24-28.

作者简介 : 龚文涛 (1984-), 男 , 工程师 , 研究领域 : 访问控制和网络安全。

(上接第 55 页)

(4):5-14.

[18] LEE W,STOLFO S J.Data mining approaches for intrusion detection[C]//Conference on Usenix Security Symposium.USENIX Association,1998:6-6.

[19] KHANUM S,USMAN M,ALWABEL A.Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks[J].International Journal of Computer Science Issues,2012,9(1).

[20] JADIDOLESLAMY H.A HIERARCHICAL INTRUSION DETECTION ARCHITECTURE FOR WIRELESS SENSOR NETWORKS[J].International Journal of Network Security&Its Applications,2011,3(5):131-154.

[21] MAMUN M S I,KABIR A F M S.HIERARCHICAL DESIGN BASED INTRUSION DETECTION SYSTEM FOR WIRELESS AD HOC SENSOR NETWORK[J].International Journal of Network Security&Its Applications,2010,2(3):102-117.

作者简介 : 李焕 (1980-), 女 , 讲师 , 研究方向 : 计算机网络、计算机应用技术。