网络入侵检测系统关联分析技术

李磊
(中国电信股份有限公司福建信息产业分公司 福建福州 350001)

摘要:随着计算机网络的飞速发展,信息安全越来越受到人们的重视。入侵检测技术作为保证计算机网络安全的核心技术在保护计算机安全方面起着越来越重要的作用。本文从入侵检测技术的基本概念和发展入手,以攻击事件的关联分析方法如何减少入侵检测系统的误报及漏报率进行了综述和研究,同时讨论了入侵检测系统面临的主要问题及今后的发展趋势。

关键词:入侵检测系统 关联分析预测 攻击脚本关联 元攻击行为建模
中图分类号:TK2513.4 **文献标识码:**A **文章编号:**1007-9416(2011)11-0237-02

1、前言

电脑网络的快速发展,产生了许多新型的应用及信息的沟通方式,但也产生了许多网络犯罪及入侵攻击事件,一方面是因为软硬件具有可被入侵的漏洞,另一方面网络及系统管理员希望能够安全地防护所管理的系统及敏感信息,所以信息加密技术、防火墙、杀毒软件等安全防护措施便应运而生。时间证明一直以来这些技术仍然无法杜绝攻击事件的发生,因此具有不同技术和特性的入侵检测系统(Intrusion Detection System,IDS)成为信息系统的第二层防护。入侵检测系统是由软件或硬件所组成,用来主动监测在信息系统和网络中所发生的安全事件。当主机被攻击时,入侵检测系统分析主机所遭受的入侵程度和损害程度,并依此发出报警,使管理员可以依据报警信息作出即时的反应和事后的修复工作。

2、研究问题

2.1 问题分析

目前入侵检测系统主要面临以下几个问题:

(1)因为不同入侵检测系统的特性及检测能力不尽相同,单一的入侵报警无法完整且正确的搜集系统所受的威胁及所面临的攻击事件信息。如网络型入侵检测系统,无法确认主机是否实际遭到入侵;而主机性入侵检测系统则无法得知入侵前攻击者所采取的攻击方式。

(2)入侵检测系统会产生的正确报警,可以提供报警的重要性级别,但是无法关联某项攻击的流程和顺序,造成管理员无法即时

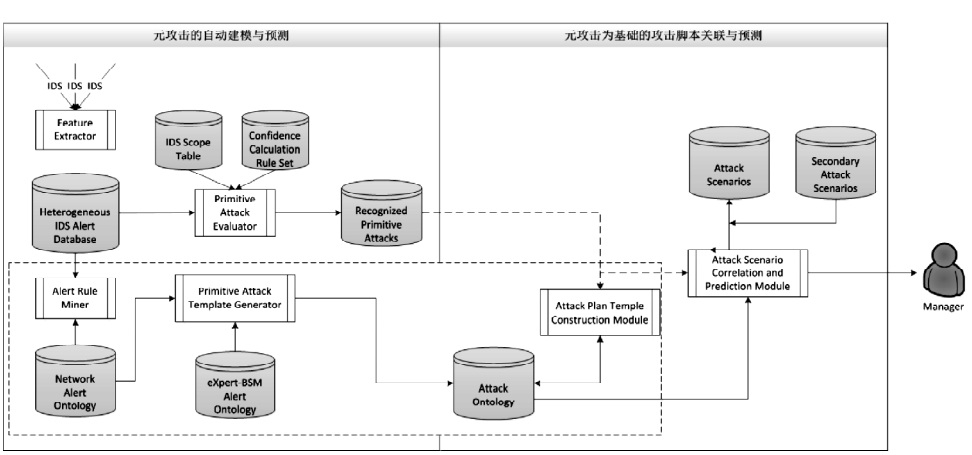

图1 元攻击为基础的入侵报警关联系统架构图

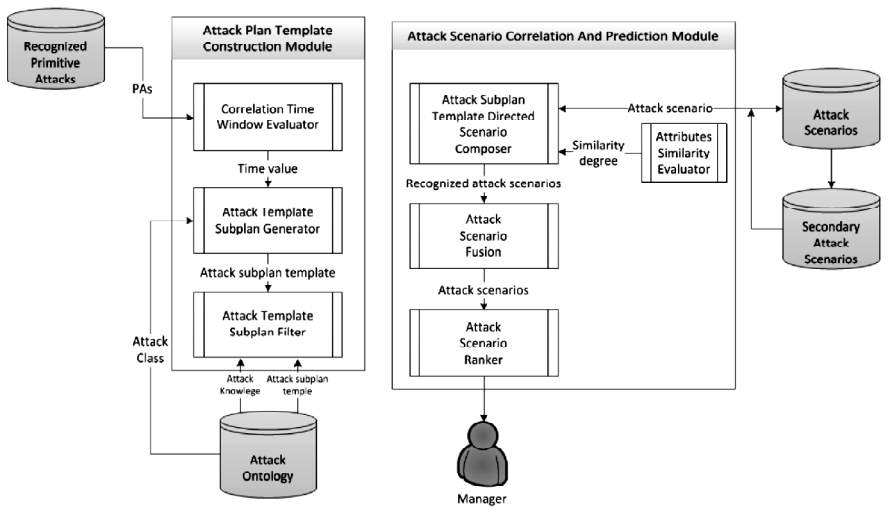

图2 以自动建立攻击计划模板为基础的攻击关联分析及预测系统

对攻击事件作出回应或修复系统的漏洞。

为了解决上述问题,若能研究出一套能有效处理不同入侵检测系统报警信息的方法,除了可以过滤误报并减少管理员负担之外,并可以借由高重要性攻击知识库描述机制的引入,来引导低重要性报警信息的整合,并提供足够的关联分析依据,用于从报警信息中迅速提取出完整的攻击脚本和攻击路径,最后提供优先顺序来帮助管理员判断处理攻击事件的发生。

2.2 研究方法

本研究的解决方法是引进元攻击(Primitive Attack)作为高级报警信息来整合不同入侵检测系统所发出的报警信息,并以元攻击信息为基础来关联出攻击脚本(Attack scenario),再以隐藏式马尔可夫模型(Hidden Markov Model, HMM)来判断攻击脚本的优先顺序。

(图1)是以元攻击为基础的入侵检测报警关联系统的架构图,大致分为左侧的元攻击的建模与检测子系统,以及右侧的以元攻击为基础的攻击脚本关联与检测子系统。左侧子系统主要负责建模与识别元攻击,基本概念是利用自动产生的原始攻击模板来整合不同入侵检测系统所发出的报警信息,使其统一格式为元攻击,一方面可以减少报警数量,另一方面可以提供更有实际意义的高级报警信息,以降低右侧的关联处理负担。右侧子系统则利用元攻击为基础来进行攻击脚本的识别,再通过攻击脚本的减少及删除,来过滤错误的攻击脚本,并经由HMM计算发生几率后加以排序。管理员可以根据排序后的攻击脚本所提供的攻击信息,针对目前的安全状况作出正确的评估与反应。

2.3 系统架构

本文以高级攻击计划为关联基础的概念发展出一套新系统,此系统能够自动建立攻击子计划(Attack Sub plan),并利用子计划的组合来进行脚本关联,关联后产生的攻击脚本再利用整合及几率的方式来找出最重要的攻击脚本并预测最有可能的攻击。

3、系统分析

3.1 元攻击(Primitive Attack)

所谓元攻击是依据元攻击模板(Template Primitive Attack)所制定的规则及限制条件,将异质入侵检测系统的入侵报警信息整合为高级报警信息。之所以需要元攻击来整合异质入侵检测系统的原因是,不同的入侵检测系统的特性和功能都有所差异,若以单一的报警进行攻击手段的分析往往会因为数据的正确性和依据的不足导致无法正确识别出攻击脚本。因此在本系统中使用元攻击作为组成攻击脚本的基本元素,并利用元攻击的特征相似度作为关联攻击脚本时的判断依据。

3.2 攻击知识实体(Attack ontology)

之前所提到的知识实体是一种将特定领域概念化的工具,并利用这些领域的正规化描述概念来达到知识分享以及再使用的目的。本文参照MIT Lincoln Lab Intrusion Detection Attacks Database的攻击分类方式,开发出攻击知识实体,本攻击知识实体用来确认元攻击所属的攻击类型,并提供知识来协助攻击脚本的关联。

这三大攻击分类下分别再衍生出各种子分类,用以描述更细化的攻击行为。每一个攻击分类除了继承父类别的属性外,也可以增加新的特征以及对应关系来增强描述高攻击分类所扮演的角色。在攻击知识实体的树状架构的最下层,描述了构建攻击知识实体的基本元素,即元攻击,这样借由元攻击所属的攻击分类可以协助理清元攻击之间的互相关系以及元攻击在攻击脚本中所扮演的角色。

3.3 关联时间窗口评估器(Correlation Time Window Evaluator)

在本系统中利用子计划模板来关联元攻击,但是在建立攻击子计划模板之前,需要先考虑时间因素对于关联操作的影响,因为关联时间窗口太小则无法进行有效的攻击关联,并导致无法找出攻击脚本;如果时间窗口太大则会产生过多的攻击脚本,导致影响系统的性能和攻击脚本的正确性。因此本文先将攻击资料库转换成为元攻击序列,再分析各元攻击序列的时间戳,以找出更适当的关联时间窗口。利用Mutual Information Method来分析元攻击序列。

$$MI(A,C,d)=\sum_{a\in A}\sum_{c\in C}p(a,c,d)I(a,c,d) \quad (1)$$

$$I(a,c,d)=\log\frac{p(a,c,d)}{p(a)p(c)} \quad (2)$$

式2中p(a)、p(c)表示元攻击a、c在元攻击序列中个别的发生几率,p(a,c,d)表示在时间长度为d的情况下,元攻击a发生在元攻击c之前或者之后的几率,I(a,c,d)表示元攻击a、c的关联度,式3中MI(a,c,d)表示元攻击序列在时间长度为d的状况下整体的关联强度。借由Mutual Information Method可以得到在不同关联时间d下,元攻击序列的关联度。无论在哪一个攻击信息库在某一特定时间后,元攻击之间的关系便会达到稳定的状况,即元攻击之间已经没有其他的关联发生。通过Mutual Information Method的分析,关联时间窗口评估器即可挑选出一个适当的时间窗口作为攻击子计划模板产生器的时间窗口变量及关联攻击的时间窗口依据。

3.4 攻击子计划导向的脚本组合器(Attack Sub plan Template Directed Scenario Composer)

攻击子计划导向的脚本组合其旨在利用攻击子计划模板来关联元攻击并产生对应的攻击脚本。首先在接受到元攻击后,根据攻击知识实体所记录的攻击子计划模板实体化元攻击对应的攻击子计划。若发现两个元攻击所对应的攻击子计划具有相同的攻击类别是,即可利用特征相似度评估器来判断两个元攻击之间的相似程度,若相似程度达到一定的标准则将两个元攻击所产生的攻击子计划进行整合以达到关联目的。以此可以循序建立出攻击脚本以供后续进行分析及预测,反之则表示两个元攻击虽然有关联的攻击类型,但是因为特征的相似度不足而被判断为独立的攻击事件。

3.5 特征相似度评估器(Attributes Similarity Evaluator)

特征相似度评估旨在通过两个元攻击间的特征值比对来决定其相似度。本系统中采用源IP地址、源端口、目标IP地址和目标端口作为比较的特征值,设计了相似程度关联表作为比较的依据。等级1表示元攻击A的源IP地址、源端口、目标IP地址和目标端口与元攻击B完全相同;或元攻击A的目标IP地址、目标端口相同于元攻击B的源IP地址、源端口且元攻击A的源IP地址、源端口相同于元攻击B的目标IP地址、目标端口。

元攻击之间的特征相似度的确认除了能够判断是否进行关联之外,还可以用来提供帮助预测攻击脚本发生几率的信息。

4、结语

本文在探讨以元攻击为基础的入侵报警关联系统的攻击脚本关联部分。首先在攻击计划模板建立模型中透过攻击信息库的元攻击序列的时间戳分析,建立攻击子计划模板与攻击脚本所需的关联时间窗口,之后在关联时间窗口下利用元攻击间的关联强度分析来建立对应的攻击子计划模板,再借由攻击知识实体所提供的攻击分类知识来进行攻击子计划模板的过滤和确认,最后再将合法的攻击子计划模板记录至攻击知识实体中,并提供后续元攻击的关联。在攻击脚本关联与预测模块中,通过攻击子计划模板为导向的攻击脚本组合器来进行元攻击的关联,并借由特征相似度的比较来元攻击间关联发生的可能性,并利用攻击脚本结合器来过滤单一行为所产生的攻击脚本和减少攻击脚本中所包含的错误元攻击,之后再以攻击脚本排序器计算出攻击脚本的优先顺序。

参考文献

[1]卿斯汉,蒋建春,马恒太等.入侵检测技术研究综述[J].通信学报,2004,25(7):19—29.

[2]lajinath B, Raghavan S V. 基于学习行为模式的入侵检测[J].计算机通信,2001,24:(12): 1202. 1212.(英文版).

[3]HU C,eng·ming, LIAO Jun—quo. 基于支持向量机的入侵检测研究[c]/ /第1届高级计算机理论与工程国际会议论文集.普吉岛(泰国): IEEE 计算机学会出版社,2008: 434—438.(英文版).

[4]李守鹏;信息安全及其模型与评估的几点新思路[D].四川大学,2002年.

[5]罗守山,陈亚娟,宋传恒,王自亮,钮心忻,杨义先.基于用户击键数据的异常入侵检测模型[J].北京邮电大学学报,2003年04期.