基于攻击群模型的协同入侵的响应方法

吴姚睿,刘淑芬
(吉林大学计算机科学与技术学院,吉林长春 130012)

摘 要: 本文提出了一种通过关系图建立攻击群模型的方法,在时间特征及因果关系的约束条件下,判断攻击序列,重构协同入侵行为的攻击过程,在无须考虑攻击群中个体的响应成本与损失成本的比例的情况下,及时对攻击行为做出响应,从而达到最大程度地减少响应成本的目的.

关键词: 入侵响应; 协同入侵; 攻击群; 攻击关系图; 极小支配集
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2009) 11-2416-04

A Response Method for Cooperative Intrusions Based on the Attack Group Model

WU Yao-rui, LIU Shu-fen
(College of Computer Science and Technology, Jilin University., Changchun, Jilin 130021, China)

Abstract: A method for establishing the attack group model by means of the relationship graph of various attacks has been proposed. Under the constraints of time characteristics as well as the causality relation it can determine the attack sequence and reconstruct the attack sequence of the cooperative intrusion. Beside, make a timely response without considering the ratio of damage cost and response cost of the individual attack, so as to achieve the maximal reduction of the response cost.

Key words: intrusion response; cooperative intrusions; attack group; attack relationship graphs; Minimal dominating set

1 引言

随着计算机网络的不断发展和普及,网络攻击手段更加复杂化和多样化,相应的网络安全技术如防火墙、入侵检测[1~5]安全性分析[6,7]等应用也越来越广泛. 入侵响应是指针对入侵警告进行响应策略选择并执行响应的过程. 它的目的是为了抑止、评估和恢复入侵损失,甚至追踪和封堵入侵源[8]. 在入侵响应系统(IRS)的实际工作中,如果对所有的警报都做出响应会造成较大的不必要的资源浪费,因此越来越多的 IRS 将响应的成本问题放到了关键的位置,即使用最小的响应成本阻止最大的损失成本的发生. 为了这个目的,判断协同入侵就非常重要. 本文使用攻击关系图的方法呈现和分析攻击的分类、状态及攻击间的关系,建立攻击群模型,从而在多个攻击中找出协同入侵所属的攻击序列.

2 问题描述

2.1 问题一:协同入侵的判断

协同入侵是指一个或者多个入侵者采取各种攻击手段,根据事先协商的入侵策略和步骤,有组织地针对同一个目标系统进行联合攻击. 这样的攻击复杂度高,隐蔽性好,且破坏严重. 它的损失成本不是简单的几个入侵行为的累加,而是呈指数倍增长. 为了判断一个攻击行为是否是一系列协同攻击行为中的一个,我们提出了基于攻击群模型的方法来进行分析.

2.2 问题二:攻击关系图的生成及分析

网络攻击模型将攻击过程划分为攻击身份和位置隐藏、目标系统信息收集、弱点信息挖掘分析、目标使用权限获取、攻击行为隐蔽、攻击实施、开辟后门和攻击痕迹清除八个阶段[9]. 在实际的攻击过程中,我们可以发现一个攻击过程往往是由多个具有一定关系的攻击组成. 例如,使用端口扫描来获取目标信息,再通过获取到的信息非法获取 root 权限. 这一系列的攻击构成攻击序列,相辅相成形成协同入侵. 协同入侵的发起者或发起位置可以有多个,但是它们具有相同的攻击目标. 我们根据网络连通性及数据流时间特征获得攻击间关系,并使用求解极小支配集的方法来发现形成攻击群的攻击序列.

收稿日期:2008-09-25;修回日期:2009-03-02
基金项目:吉林省科技计划重大项目(No. 20076004)

3　攻击群的定义

3.1　响应原则

攻击是被实施的威胁(威胁行为),如果成功,将会导致不期望的安全侵害或威胁后果[10]. 攻击行为的三个要素是攻击者、攻击过程以及攻击目标[9]. 一般来说,一个攻击操作序列由攻击者发起,攻击者通过一定的攻击策略,形成具体的攻击过程,对攻击目标发起攻击并达到一定的攻击效果.

不同种类的攻击所造成的损失成本(Dc)和响应成本(Rc)是不同的. 损失成本是指攻击对目标系统造成危害导致的费用,响应成本是指对入侵行为做出正确响应所要付出的代价. 根据以最小的响应代价实现最大的安全目标的原则,当响应成本大于损失成本时,如扫描和嗅探类的攻击,它的损失成本为 2,而最低响应成本为 5[11],对于此类攻击所发出的入侵警报,可以不做入侵响应;反之,当响应成本小于损失成本时,如非法获取 root 权限类的攻击,它的损失成本为 100,而最高响应成本为 60[11],对于此类攻击所发出的入侵警报,则必须要及时响应.

但是,在实际的攻击中,攻击过程是由一系列的攻击策略和方法构成的,不能如上所述简单地定义响应成本和损失成本. 通常在实施真正的攻击目的之前,都需要对目标系统信息进行收集,扫描与嗅探类别的攻击正是收集目标系统信息的常用手段,此时它的目的是通过找出攻击目标的开放服务列表,将其作为攻击策略的第一步,以便进一步地获得目标系统的知识和进入目标系统的途径,为更严重的攻击做准备,此时的扫描攻击不能简单的将其损失成本定义为 2,而应将其视为协同入侵的攻击前兆. 我们可以通过判断几个攻击是否是一个协同入侵所形成的攻击序列,来确定攻击的危险程度,从而更合理地定义响应成本和损失成本. 例如,如果端口扫描和非法获得 root 权限属于同一个攻击序列,当端口扫描攻击发生时就做出响应,则最高响应成本为 7 时阻止了损失成本为 100 的攻击,从而最大可能的符合了最小响应代价实现最大安全目标的原则.

3.2　攻击的描述

使用五元组(Src,Des,Type, T_{begin}, Weight)描述一个攻击,其中 Src 表示攻击的来源,Des 表示攻击的目标,Type 表示攻击的类型, T_{begin} 表示攻击的开始时间,Weight 表示攻击对攻击目标的影响因子,

$$\text{Weight}(A_i) = \ln \frac{Dc}{2}$$

A_i 为攻击类型.

攻击类型[11]	成本值[11]	Weight
普通用户获得 Root 权限	$Dc = 100$ $\max(Rc) = 60, \min(Rc) = 40$	3.91
远程用户获得本地用户权限	$Dc = 50$ $\max(Rc) = 40, \min(Rc) = 20$	3.22
拒绝服务	$Dc = 30$ $\max(Rc) = 15, \min(Rc) = 10$	2.71
扫描与嗅探	$Dc = 2$ $\max(Rc) = 7, \min(Rc) = 5$	0

3.3　攻击群的定义

定义 1　假设 n 个攻击的目标均为同一个主机,且满足以下两个条件之一,则称这 n 个攻击构成一个攻击群.

条件 1　假设多个攻击行为,其攻击序列为$(a_1, a_2, \cdots, a_n)$,攻击出现的时间间隔序列为$(\eta_1, \eta_2, \cdots, \eta_{n-1})$,$\eta_{i-1} = t_i - t_{i-1} (1 < i \leq n)$,若 $\eta_i < t_T, t_T$ 为预定义的时间阈值,则称攻击序列$(a_1, a_2, \cdots, a_n)$为一个攻击群;

条件 2　若攻击间存在因果关系,即一个攻击发起前一定需要具备某些前提条件,发起后没有及时响应就会造成一定的后果,如果一个攻击 a_1 造成的后果是 a_2 的前提条件,a_2 造成的后果是 a_3 的前提条件,依此类推,则称$(a_1, a_2, \cdots, a_n)$构成一个攻击群.

4　攻击群模型

4.1　问题二的数学描述

假设 k 个攻击中最多存在 m 个攻击群(一个攻击群表示是一个协同入侵),求解每个协同入侵的攻击序列.

定义 2　问题二的数学模型是:以攻击为顶,仅当两个攻击间不满足条件 1 或条件 2 描述的关系时,相应的两顶间连线构成一个图 $G(V, E)$,如图 1 所示,此图的极小支配集即为所求. 其中

$V = \{v_u, 1 \leq u \leq k\}$,

$E = \{(v_u, v_v), 1 \leq u, v \leq k\}$.

V 是顶点集,每个顶点代表了一个攻击. E 是边集,不满足关系条件的两攻击间连线的集合.

图 1 由 6($k = 6$)个攻击构成,其中:

$V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$,

$E = \{(v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_4), (v_3, v_4), (v_4, v_5), (v_4, v_6), (v_5, v_6)\}$.

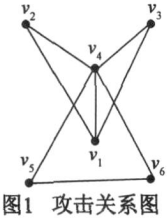

图1　攻击关系图

4.2　极小支配集的求解

对定义 2 形成的图的极小支配集求解,即可获得在 k 个攻击中可能存在的 m 个攻击群.

$$\prod_{u=1}^{k}\left(v_u+\sum_{l\in N(v_u)}l\right) \quad (1)$$

v_u:第 $u(1\le u\le k)$ 个顶点;

$N(v_u)$:v_u 的所有邻顶的集合.

式(1)的运算是逻辑运算.求解的描述如下:每个多项式看成一个"队列",其中每一项看成一个"链表".

步骤 1 将多项式转化为相应的队列,左、右队列各有一个指针指向队列的第一项;

步骤 2 判断左、右两项是否相等,如果相等,只将左项挂进结果队列;如果不相等,将两项的"下标编号"按顺序合并,由小到大,消掉重复项,并将生成的新项挂到结果队列中;向结果队列挂接新项时,应检查即将挂入的项是否与已有项相等,如果相等,则不挂载该项.

步骤 3 右队列的指针下移一位,当右队列的指针遍历一遍所有的元素后,左队列的指针下移一位,同时右队列的指针指向第一项,转到步骤 2.否则直接执行步骤 2.如此循环直到左队列的指针移动到队尾,循环结束,执行步骤 4;

步骤 4 从上到下遍历生成的队列中的每一个单项式,若发现元素 x 与 xy 同时存在,则删除 xy 项.当所有项目都遍历一次后,即可得到最终结果;

步骤 5 两个以上多项式相乘,重复以上步骤即可.

以图 1 为例,公式(1)可描述为:

$$(v_1+v_2+v_3+v_4)(v_2+v_1+v_4)(v_3+v_1+v_4)$$
$$\cdot(v_4+v_1+v_2+v_3+v_5+v_6)(v_5+v_4+v_6)(v_6+v_4+v_5)$$
$$=v_4+v_1v_5+v_1v_6+v_2v_3v_5+v_2v_3v_6$$

则所得极小支配集 $D_a(|D_a|\ge 2)$ 为

$D_1=\{v_1,v_5\}$; $D_2=\{v_1,v_6\}$;

$D_3=\{v_2,v_3,v_5\}$; $D_4=\{v_2,v_3,v_6\}$.

由此可见,在 6(即 $k=6$)个攻击中可能存在 4(即 $m=4$)个攻击群,分别是$\{v_1,v_5\}$,$\{v_1,v_6\}$,$\{v_2,v_3,v_5\}$,$\{v_2,v_3,v_6\}$.

4.3 协同入侵的响应

对图 1 求解极小支配集获得了 4 个协同入侵攻击序列(即攻击群),对每个攻击群分别执行:

(1)对攻击群中的每个攻击提取其 T_{begin} 属性,并按照 T_{begin} 值由前到后排序;

(2)对已经完成排序的攻击序列中的每个攻击提取其 Weight 属性,若攻击群中仅存在一个攻击的 Weight 值不等于 0,则选择攻击序列中初始项做出响应;若攻击群中存在多个攻击的 Weight 值不等于 0,则选择在攻击序列中 Weight 值最大的攻击前发生的具有最小 Weight 值的攻击做出入侵响应.

以图 1 为例,若按攻击发生的时间顺序排列为 v_1,v_2,v_3,v_4,v_5,v_6,且 $Weight_{v_1}=0$,$Weight_{v_2}=3.22$,$Weight_{v_3}=2.71$,$Weight_{v_5}=3.91$,$Weight_{v_6}=3.91$,则仅对 v_1 和 v_3 做出响应(尽管 v_1 的响应成本高于其损失成本),就可以避免协同入侵$\{v_1,v_5\}$,$\{v_1,v_6\}$,$\{v_2,v_3,v_5\}$,$\{v_2,v_3,v_6\}$造成的损失,从而达到减少响应成本的目的.

5 结论

面对越来越复杂的入侵行为,协同入侵的响应已经成为入侵响应中日益关注的焦点.本文用攻击关系图建立攻击群模型,在时间特征、因果关系的约束条件下,重构了攻击序列以判断协同入侵行为攻击过程,在无须考虑攻击行为的个体响应成本与损失成本的比例的情况下,及时做出响应,从而达到最大程度地减少响应成本的目的.应用本方法形成的入侵响应系统雏形在实验室的测试过程中显示对于攻击群的发现以及攻击行为的响应效果良好,但仍有一些问题需要进一步研究,下一步的工作主要是针对网络攻击与病毒程序结合后,病毒的复制传播特点使网络攻击更加复杂和智能,我们拟通过对病毒建立数学模型,结合本文提出的攻击关系图方法,进一步提高对协同入侵的判断与响应能力.

参考文献:

[1] 俞研,黄皓.基于小样本标记实例的数据流集成入侵检测模型[J].电子学报,2007,35(2):234 - 239.
YU Y,HUANG H. A streaming ensemble intrusion detection model based on small labeled data[J]. Acta Electronica Sinica,2007,35(2):234 - 239. (in Chinese)

[2] WANG W,DANIELS T. Network forensics analysis with evidence graphs[EB/OL]. Digital Forensic Research Workshop (DFRWS),2005.

[3] CUPPENS F,MIEGE A. Alert correlation in a cooperative intrusion detection framework[A]. Proceedings of the IEEE symposium on Security and Privacy[C]. Oakland:IEEE,2002. 202 - 215.

[4] 张相锋,孙玉芳,赵庆松.基于系统调用子集的入侵检测[J].电子学报,2004,32(8):1338 - 1341.
Zhang xiang-feng,et al. Intrusion detection based on sub-set of system calls[J]. Acta Electronica Sinica,2004,32(8):1338 - 1341. (in Chinese)

[5] DAIN O,CUNNINGHAM R. Building scenarios from a heterogeneous alert stream[A]. Proceedings of the IEEE SMC Information Assurance Workshop[C]. New York:IEEE,2001. 231 - 235.

[6] 张海霞,苏璞睿,冯登国.基于攻击能力增长的网络安全分析模型[J].计算机研究与发展,2007,44(12):2012 -

2019.
ZHANG HX, SU PR, FENG DG. A network security analysis model based on the increase in attack ability[J]. Journal of Computer Research and Development, 2007, 44(12): 2012 - 2019. (in Chinese)

[7] 张涛,胡铭曾,云晓春,张永铮. 计算机网络安全性分析建模研究[J]. 通信学报, 2005, 26(12): 100 - 109.
ZHANG T, HU MZ, YUN XC, ZHANG YZ. Research on computer network security analysis model[J]. Journal on Communications, 2005, 26(12): 100 - 109. (in Chinese)

[8] 张剑,龚俭. 可回卷的自动入侵响应系统[J]. 电子学报, 2004, 32(5): 769 - 773.
ZHANG J, GONG J. Rollbackable automated intrusion response system[J]. Acta Electronica Sinica, 2004, 32(5): 769 - 773. (in Chinese)

[9] 卿斯汉,蒋建春. 网络攻防技术原理与实战[M]. 北京:科学出版社, 2004.
QING SH, JIANG JC. Wang luo gong fang ji shu yuan li yu shi zhan[M]. Beijing: Science Press, 2004. (in Chinese)

[10] Stallings W, Brown L. Computer Security: Principles and Practice[M]. New Jersey: Prentice Hall, 2008.

[11] LEE W, FAN W, MILLER M. Toward cost-sensitive modeling for intrusion detection and response[EB/OL]. Workshop on Intrusion Detection and Prevention, 7th ACM Conference on Computer Security, 2000.

作者简介:

吴姚睿　女,博士,主要研究方向为计算机网络与安全,计算机取证.
E-mail: yrwu@jlu.edu.cn

刘淑芬　女,教授,博士生导师,研究方向:计算机支持协同工作、软件体系结构、基于模型驱动的软件编程方法、网络管理技术.
E-mail: liusf@jlu.edu.cn