

基于攻击图模型的网络可能入侵估计研究

王继钢

(呼伦贝尔学院 计算机科学与技术学院, 内蒙古 海拉尔 021008)

摘 要: 提出了一种基于攻击图模型的网络可能入侵估计方法. 该方法先将以往每次成功的网络入侵行为都当作一次网络状态的变迁, 并以此为依据定义网络攻击图、网络入侵路径、网络攻击行动, 并预测攻击者下一次入侵目标的可能性和选择入侵路径的可能性, 在此基础上融合已知和潜在的网络入侵威胁因素构建网络入侵的原子攻击库, 计算系统网络环境下入侵者所面临的攻击压力与收益期望, 对网络入侵者在决策时的攻击意愿进行量化, 以量化后的结果为基础建立网络可能入侵估计风险模型, 利用该模型给出网络可能入侵估计量化的风险值, 从而有效地完成对网络可能入侵的估计. 实验仿真证明, 基于攻击图模型的网络可能入侵估计方法具有良好的可行性和有效性, 可大幅减少不可信报警数量.

关键词: 网络攻击; 攻击图; 攻击模型

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2016)02-0116-04

Invade Estimation Research Based on Network Attack Graph Mode

WANG Ji-gang

(College of Computer Science and Technology, Hulunbuir University, Hailar 021008, China)

Abstract: This paper proposes a network based on attack graph model approach to estimate the possible intrusion. This method first before every successful network intrusion behavior as the change of network state at a time, and on this basis to define the network attack graph, the path of network intrusion, and network attacks, and to predict the likelihood of the attacker next invasion target and chose the path of the invasion of possibility, on the basis of the integration in the known and potential threat of network intrusion factors to build atomic attack library network intrusion, computing system under the network environment the invaders attack pressure and earnings expectations, facing the network invaders attack intend to quantify in decision-making, on the basis of the quantitative results after establishing network may be invaded to estimate risk model, by using the model given network intrusion estimates may be quantitative risk value, effectively completed the estimate of the network may be invaded. Experimental simulation show that based on network attack graph model approach to estimate the possible intrusion has good feasibility and effectiveness, and greatly reduce the amount of untrusted alarm.

Key words: network attack; attack graph; attack model

1 引言

目前, 在全世界对信息社会的依赖性不断增加的情况下, 网络与信息安全的重要性与日俱增^[1-3]. 与此同时网络攻击也正在向大规模、协同化和多层次的方向发展, 网络入侵的攻击行为多表现为无规律性、复杂性和多样性等特点^[4-6]. 在这种情况下,

如何客观地进行网络可能入侵估计成为该领域亟待解决的问题, 而网络可能入侵估计方法可以为整个系统建立网络攻击入侵评估模型, 通过模型可获得网络系统所有可能的入侵攻击行为和状态, 是解决上述问题的根本途径, 引起了很多专家与学者的重视^[7]. 由于网络可能入侵估计方法具有深远的发展意义, 因此也成为了业内人士研究的焦点课题, 受到

收稿日期: 2015-04-20; 修回日期: 2015-05-22

了广泛的关注,同时也出现了很多好的方法。

文献[8]提出了基于规则的网络可能入侵估计方法。该方法从历史的网络入侵攻击案例中提取网络入侵攻击的特征,将其形成一定的规律表述,将网络系统与已有的入侵攻击规律相融合,从而实现对网络可能入侵的估计。该方法较为简单,但是存在评估误差大的问题。文献[9]采用了基于粗糙图的网络可能入侵估计方法。该方法先建立网络的部件节点粗糙关联模型,依据该模型对网络攻击入侵风险最大流进行估计,有效地完成了对网络可能入侵的估计。该方法鲁棒性较强,但是存在计算量大、评估时间复杂度较高的问题。文献[10]重点讨论了基于多智能代理(Agent)的网络可能入侵估计方法。该方法以网络中主机上的组件为主要节点,运用多 Agent 协同工作的方式实现对网络可能入侵的估计。该方法网络入侵评估的时间效率较高,但是采用当前的算法对网络的可能入侵进行估计时,对入侵者的攻击意愿缺乏详细的分析,存在入侵估计误差大的不足。

针对上述问题的产生,提出了一种基于攻击图模型的网络可能入侵估计方法。该方法先对网络攻击图、网络入侵路径、网络攻击行动进行定义,再预测入侵者下一次入侵目标的可能性和选择入侵路径的可能性,计算系统网络环境下入侵者所面临的攻击压力与收益期望,对网络入侵者在决策时的攻击意愿进行量化,建立网络可能入侵估计风险模型,完成了对网络可能入侵的估计。

2 网络可能入侵估计优化原理

针对采用当前的算法进行网络可能入侵估计时,对入侵者的攻击意愿缺乏详细的分析,存在入侵估计误差大的问题,提出了一种基于攻击图模型的网络可能入侵估计方法。

2.1 网络入侵目标的可能性预测

在对网络可能入侵优化估计过程中,先将以往每次成功的网络入侵行为都当做一次网络状态的变迁,并以此为依据定义网络攻击图、网络入侵路径、网络攻击行动,并利用网络状态间的转移概率预测入侵者下一次入侵目标的可能性和选择入侵路径的可能性,计算网络入侵的成功概率。具体的步骤如下所示。

对网络攻击图、网络入侵路径、网络攻击行动作如下定义。

(1) 将网络攻击图描述为一个对网络状态转换的系统,利用下式表述为

$$T = (S, t, s_0, S_G) \quad (1)$$

式中, S 代表网络入侵状态的集合, t 代表网络入侵状态转换关系的集合, s_0 代表网络初始状态, S_G 代表入侵目标状态的集合, T 代表建立的网络攻击图。

(2) 假如由 $S_n \in S_G$ 代表一个网络入侵目标状态, 设从网络初始状态 S_0 开始就存在着一组 $S_1, S_2, \dots, S_{n-1}$ 代表的状态序列, 并可以满足于 $(S_i, S_{i+1}) \in t$ 的条件, 则将 $S_1, S_2, \dots, S_{n-1}$ 定义为一条网络入侵的路径, 利用下式表示。

$$\{S_1, S_2, \dots, S_{n-1}\} = \frac{\{S_n \in S_G\} \otimes T}{(S_i, S_{i+1}) \in t} \quad (2)$$

式中, (S_i, S_{i+1}) 代表攻击图中的任意状态集合。

(3) 对网络攻击行动可以利用下式进行表述。

$$v_{id} = \frac{(\text{Src_host}, \text{dst_host})}{\{S_1, S_2, \dots, S_{n-1}\}} \quad (3)$$

式中, Src_host 代表发动攻击的主机 ID, dst_host 代表遭受入侵攻击的主机 ID, v_{id} 代表此次攻击所利用的弱点号。

对于 S_i 代表的攻击图中的任意一种状态, 由 ac_i 表示相对应入侵复杂度, 假设入侵者到达 S_i 代表的状态后, 可以选取由 SUB_S 代表的网络入侵攻击子目标状态集合, 则利用下式可以预测由 $\lambda_{i,j}$ 代表下一步网络入侵目标的可能性。

$$\lambda_{i,j} = \frac{ac_i}{s_i} / \sum_{\text{SUB_S}} v_{id} \quad (4)$$

设 L 代表攻击图中能够到达某入侵目标状态的攻击路径集合, 由 l_i 代表 L 中的任意一条攻击路径, 则利用下式预测由 c_i 代表的入侵者选择该条路径进行入侵的可能性:

$$c_i = \prod_{j=0}^{l_i} \lambda_{i,j} \times L \quad (5)$$

综上所述, 在对网络可能入侵优化估计过程中, 先将以往每次成功的网络入侵行为都当作一次网络状态的变迁, 并以此为依据定义网络攻击图、网络入侵路径、网络攻击行动, 并预测入侵者下一次入侵目标的可能性和选择入侵路径的可能性, 为实现网络可能入侵优化估计奠定了基础。

2.2 网络可能入侵估计的实现

以式(5)预测的入侵者下一次入侵目标的可能性和选择入侵路径的可能性为基础,使用融合于已知和潜在的网络入侵威胁因素来构建网络入侵的原子攻击库,计算系统网络环境下攻击者所面临的攻击压力与收益期望,对网络入侵在决策时的攻击意愿进行量化,并以量化后的结果为基础建立网络可能入侵估计风险模型,利用该模型给出网络可能入侵估计量化的风险值,从而有效地完成了对网络可能入侵的估计. 具体的步骤如下所示.

将网络节点属性用来映射网络节点实时状态,假设由 A 代表网络中节点的当前状态,host 代表属性 A 所对应的实体网络主机,则 A_i 代表实体网络主机前驱节点的属性, A_j 代表实体网络主机后继节点的属性,将 $A_i \cdot \text{host} = A_j \cdot \text{host}$ 定义为已知入侵攻击威胁因素,将 $A_i \cdot \text{host} \neq A_j \cdot \text{host}$ 定义为潜在的网络入侵攻击威胁,以上式预测攻击者下一次入侵目标的可能性和选择入侵路径的可能性为基础,利用下式建立网络入侵的原子攻击库:

$$AP(E) = \frac{A}{(c_i, \lambda_{i,j})} \times \frac{A_i \cdot \text{host} \neq A_j \cdot \text{host}}{A_i \cdot \text{host} = A_j \cdot \text{host}} \quad (6)$$

式中, $AP(E)$ 代表网络入侵的原子攻击库.

在对网络可能入侵优化估计过程中,利用下式计算在系统的网络环境下入侵者所面临的攻击压力收益期望:

$$\lambda = \frac{AP(e) \times AP(E)}{p_{\text{sue}}(e) \cdot \text{Atkprofit_Actual}(e)} \quad (7)$$

式中, p_{sue} 代表网络入侵攻击策略(e)的攻击意愿, $AP(e)$ 代表(e)的成功率, $\text{Atkprofit_Actual}(e)$ 代表网络入侵攻击策略(e)的攻击收益, λ 代表网络入侵攻击策略的压力收益比,当满足于 $\lambda \geq 1$ 的条件时,入侵者的意愿为 0,则网络攻击的压力大于收益期望,即 $\text{Atkprofit_Actual}(e) \geq P_{\text{sus}}(e)$,可以说明,入侵者不会选取攻击策略(e),而满足于 $\lambda = 0$ 的条件时,攻击压力为 0,可以说明,在入侵者执行攻击策略(e)时不会对自身形成损失,但如果入侵者发现低风险攻击时,则会选取此项攻击策略.

在对网络可能入侵优化估计过程中,利用下式表述对网络入侵攻击压力的量化:

$$T' = \frac{[\text{roud_to} - \text{decimal}(\text{APVB}_{\text{ase}} \cdot \text{roud})]}{\lambda} \quad (8)$$

式中, APVB_{ase} 代表对网络攻击潜在价值的基础评分,roud 代表网络入侵攻击执行成本,decimal 代表实际攻击收益, T' 代表网络入侵攻击压力的量化值.

以量化后的结果为基础建立网络可能入侵估计风险模型,表述为

$$\text{pr}(A_j | p_a[A]) = \begin{cases} A_i \cdot \text{status} = 0 \\ (T' \cdot \text{otherwise}) \end{cases} \quad (9)$$

式中, $A_i \cdot \text{status}$ 代表估计的网络入侵量化的风险值, $\text{pr}(A_j | p_a[A])$ 代表建立的网络可能入侵估计风险模型.

综上所述可以说明网络可能入侵估计优化原理,从而有效地完成了对网络可能入侵的优化估计.

3 实验及仿真证明

为了证明基于攻击图模型的网络可能入侵估计方法有效性,需要进行实验. 设计了一个实验网络平台环境,其拓扑图如图 1 所示. 改进算法可能入侵估计整体性能见表 1.

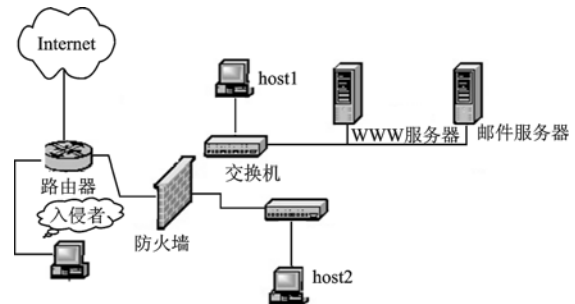


图 1 实验网络结构图

表 1 改进算法网络可能入侵估计整体性能

实验次数/次	改进算法入侵风险评估精确度/%	改进算法入侵风险评估可靠度/%	改进算法入侵风险评估误差率/%
15	96	98	0.01
25	97	97	0.01
35	96	97	0.02
45	96	98	0.01
55	96	98	0.02

改进算法进行网络可能入侵估计的有效性要优于传统算法,主要是因为改进算法先将以往每次成功的网络入侵行为都当做一次网络状态的变迁,并

以此为依据定义网络攻击图、网络入侵路径、网络攻击行动,并预测入侵者下一次入侵目标的可能性和选择入侵路径的可能性,从而保障了改进算法对网络入侵估计评估的精确性。

实验仿真证明,基于攻击图模型的网络可能入侵估计方法具有良好的可行性和有效性,可大幅减少不可信报警数量。

4 结束语

针对采用当前的算法进行网络可能入侵估计时,对入侵者的攻击意愿缺乏详细的分析,存在入侵估计误差大的问题,提出了一种基于攻击图模型的网络可能入侵估计方法。该方法先将以往每次成功的网络入侵行为都当做一次网络状态的变迁,并以此为依据定义网络攻击图、网络入侵路径、网络攻击行动,并预测入侵者下一次入侵目标的可能性和选择入侵路径的可能性,在此基础上融合已知和潜在的网络入侵威胁因素构建网络入侵的原子攻击库,计算系统网络环境下入侵者所面临的攻击压力与收益期望,对网络入侵者在决策时的攻击意愿进行量化,以量化后的结果和原子攻击本身的入侵性质为基础建立网络可能入侵估计风险模型,利用该模型给出网络可能入侵估计量化的风险值,从而有效地完成了对网络可能入侵的估计。实验仿真证明,基于攻击图模型的网络可能入侵估计方法具有良好的可行性和有效性,可大幅减少不可信报警数量。

参考文献:

- [1] 杨宏宇,江华. 基于攻击图的多 Agent 网络安全风险评估模型[J]. 计算机科学, 2013, 40(2):148-152.
- [2] 滕丽萍. 无线传感器网络中基于 Sinkhole 攻击的入侵检测系统研究[J]. 计算机应用与软件, 2013, 30(6):312-315.
- [3] 田志宏,王佰玲,张伟哲,等. 基于上下文验证的网络入侵检测模型[J]. 计算机研究与发展, 2013, 50(3):498-508.
- [4] 方明,徐开勇,杨天池,等. 基于攻击图的分布式网络风险评估方法[J]. 计算机科学, 2013, 40(2):139-144.
- [5] 陈靖,王冬海,彭武. 基于动态攻击图的网络安全实时评估[J]. 计算机科学, 2013, 39(2):133-138.
- [6] 陈小军,方滨兴,谭庆丰,等. 基于概率攻击图的内部攻击意图推断算法研究[J]. 计算机学报, 2014, 37(1):62-72.
- [7] 崔海鹏. 计算机数据库入侵检测技术的探讨[J]. 黑龙江科技信息, 2014, 29(6):96-96.
- [8] 李楠. 计算机网络安全漏洞检测与攻击图构建的研究[J]. 价值工程, 2014, 17(5):189-190.
- [9] 张辉. 自体集网络入侵检测中的高效寻优算法仿真[J]. 计算机仿真, 2013, 30(8):297-300.
- [10] 何保荣,李建荣,王超智. 基于分类算法的校园网络入侵检测系统研究[J]. 电子设计工程, 2013, 21(12):12-13.

作者简介:

王继钢 男,(1982-),硕士,讲师.研究方向为计算机网络、计算机硬件,信息处理、嵌入式技术.

E-mail:wjg26712092@sina.com