基于网络安全风险评估的攻防博弈模型*

黄 鹏,张 娜
(西昌学院 汽车与电子工程学院,四川 西昌 615013)

【摘 要】如何量化网络安全风险评估的威胁概率是一个亟需解决的重要问题。网络安全攻防对抗的本质可以抽象为攻防双方的策略的相互影响。防御者所采取的防御策略是否有效,不应该只取决于其自身的行为,还应取决于攻击者和防御系统的策略。执行攻击的决定是在攻击收益和被检测可能带来的后果之间进行权衡,防御者的安全策略主要取决于对攻击者意图的了解程度。本文提出一种博弈攻防模型,量化了威胁的可能性,构建了一个风险评估框架。根据成本效益分析,笔者定义了制定支付矩阵的方法并分析该模型的平衡性。

【关键词】博弈论;网络安全;风险评估
【中图分类号】TP393.08 【文献标识码】A 【文章编号】1673-1891(2014)04-0071-04

1 引言

计算机网络风险评估是信息安全风险评估的重要组成部分,它是网络安全研究方向的热点问题之一。各国学者都对网络风险评估开展了积极的研究,不同的研究方法和框架层出不穷,如马尔可夫链[1]和不确定性推理[2]。在信息安全风险评估中最重要的问题是如何量化的威胁概率。一方面,人们只能靠一些间接信息,猜测,直觉或其他主观因素来确定的概率,从而导致不适当的主观决策。另一方面,在网络空间的"威胁"是指系统可能承受的攻击。威胁概率是攻击者决定和意志的反映,因此有可能通过客观的分析得到。从信息安全博弈理论角度看,与实现系统防御产生一定的成本相同,对于网络的任何攻击手段都要付出一定的代价,因此可以利用博弈论来研究攻防矛盾及其最优防御决策等信息安全攻防对抗难题[3]。

博弈论模型是对各种现实生活状况抽象概括,可为探讨信息安全攻防中的可行性提供理论基础。这一理论已被用于许多学科并取得了丰硕的研究成果。在计算机网络安全领域中,攻击方和防御方的互动过程是一个博弈过程。因此,博弈论可以用来预测攻击的行为,并支持策略制定[4]。

本文运用博弈论对基于网络安全风险评估的攻防博弈模型进行了研究与分析。

2 风险评估框架

网络安全风险评估的过程是由系统识别,威胁识别,脆弱性识别,测定的可能性,影响分析和风险计算等[6]。结合文献[6],本文提出一个如图1所示的风险评估框架,在该框架中,威胁概率计算方法起着重要的作用。

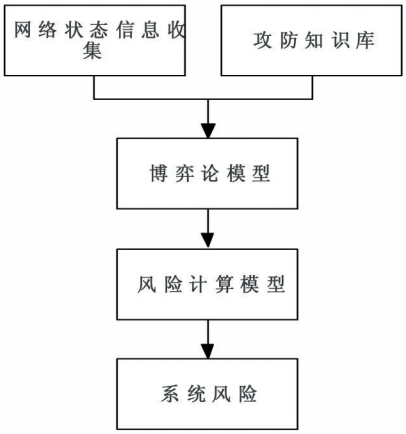

图1 风险评估框架

从图1看出,一个系统的资产和漏洞是由当前的网络状态来确定的。结合攻防知识库,可以确定漏洞所受到的威胁和检测措施。然后就可以为每个威胁设置一个博弈模型及其效用函数。这个框架的重点是计算博弈的平衡点和攻击的概率。最后,使用该攻击概率,可以计算出节点和系统的风险值。

网络状态信息采集:从当前的网络状态收集到的信息,确定威胁。与系统的逻辑连接相结合,就可以发现系统的漏洞[7]。

攻防知识库:它主要是存储漏洞,攻击行动和恢复措施之间的关系:

规则1:漏洞信息和攻击之间的关系,决定双方的策略空间。

规则2:攻击动作和其类型,其中包括攻击的成本信息之间的关系。

收稿日期:2014-10-15
*基金项目:西昌学院自然科学基金(项目编号:XA1201);四川省青年基金(项目编号:11zb115)。
作者简介:黄鹏(1982-),男,讲师,博士,研究方向:无线传感器网络。

规则3：攻击类型和恢复措施，其中包括措施的成本之间的关系。

博弈理论模型：攻击概率根据双方的成本效益计算。

风险计算模型：计算每个威胁可能带来的攻击概率的风险。然后计算节点和系统的风险。

3. 攻防博弈模型

3.1 模型细节

为了应用博弈理论模型来计算在风险评估领域的最重要问题之一的威胁概率，需要引入两个基本假设：

*攻击者的能力均等。假设攻击者的能力是相等的，这意味着对于一个典型的攻击动作，每一个攻击者具有相同攻击的概率，这同样意味着对于给定目标的每一个威胁，有明确的风险。有了这个假设，在风险评估框架计算出的概率才是有效的。

*最终用户的最小能力。作为攻防博弈模型的参与者之一的防御方显然不能存在这样的侥幸心理，即：在没有任何防御动作的情况下，攻击行为会失败。因此，在本文中，笔者假设的概率是攻击行动将没有防御的动作成功是100%。

显然，双方不能达成一项协议，因为他们没有合作的动机，因此该博弈是非合作的。无论是攻击方或防御方所采取的行动都有一定的成本，所以，博弈的效用函数不仅仅只通过收益来描述，因此博弈是非零和的。模型的主要目标是在风险评估领域中计算威胁的概率。攻击方和防御方采取的决策相互独立，因而他们的决策顺序不影响博弈的结果，因此博弈是静态的。作为评估者，知道攻击者和防御者所能采取的所有策略以及各种困难策略组合下给对手带来的得益，因此，该博弈过程属于完全信息博弈。综上所述，攻防博弈模型是一个完全信息的非合作且非零和的静态博弈。

定义1：攻防博弈模型定义为：

$$G::=\{P^1,P^2,S^1,S^2,U^1,U^2\} \quad (1)$$

$P^k(k=1,2)$ 表示博弈双方，p^1表示攻击方，p^2表示防御方。S^1，S^2分别是攻击方和防御方的策略空间。对每一个威胁$att_i(o)$，攻击方可以选择攻击$att_i(o)$或不攻击$(\neg att_i(o))$，则，$S^1::=\{att_i(o),\neg att_i(o)\}$。

面对典型攻击，防御方如果有相应的防御策略则定义为$S^2::=\{D_{(att_i(o))},\neg D_{(att_i(o))}\}$，否则定义为$S^2::=\{\neg D_{(att_i(o))}\}$。

U^1，U^2分别表示攻击方和防御方的效用。$Att\_Utility_{ij}$，$Att_Benefit_{ij}$和Att_Cost_{ij}分别表示攻击方采用攻击策略i，防御方采用防御策略j的效用函数，收益和代价。$Def\_Utility_{ij}$，$Def_Benefit_{ij}$和Def_Cost_{ij}分别表示当攻击方采用策略i进行攻击防御方采用策略j进行防御的效用函数，收益和代价。

定义2：博弈双方的支付（效用）定义为$Benefit_{ij}-Cost_{ij}$。

因此，攻击方的效用函数为：$Att\_Utility_{ij}::Att\_Benefit_{ij}-Att\_Cost_{ij}$，防御者的效用函数为：$Def\_Utility_{ij}::Def\_Benefit_{ij}-Def\_Cost_{ij}$。若$S^2::\{D_{(atti(o))},\ {}_{-1}D_{(atti(o))}\}$，那么支付矩阵如表1所示：

表1 支付矩阵

攻击策略 \ 防御策略	$D_{(atti(o))}$	${}_{-1}D_{(atti(o))}$
$att_i(o)$	$\begin{bmatrix}(Att\_Benefit_{11}-Att\_Cost_{11}),\\(Def\_Benefit_{11}-Def\_Cost_{11})\end{bmatrix}$	$\begin{bmatrix}(Att\_Benefit_{12}-Att\_Cost_{12}),\\(Def\_Benefit_{12}-Def\_Cost_{12})\end{bmatrix}$
${}_{-1}att_i(o)$	$\begin{bmatrix}(Att\_Benefit_{21}-Att\_Cost_{21}),\\(Def\_Benefit_{21}-Def\_Cost_{21})\end{bmatrix}$	$\begin{bmatrix}(Att\_Benefit_{22}-Att\_Cost_{22}),\\(Def\_Benefit_{22}-Def\_Cost_{22})\end{bmatrix}$

3.2 成本收益分析

根据文献[8-10]笔者定义本文中攻防博弈模型的攻防成本和收益如图2所示：

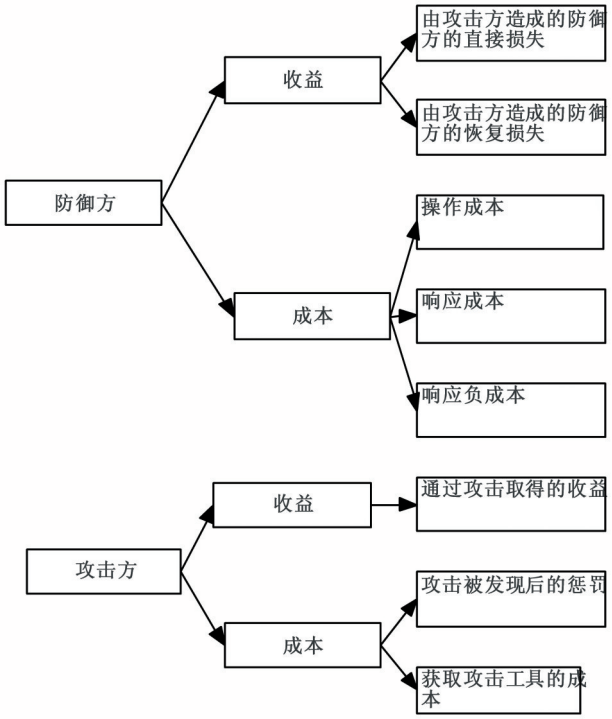

图2 成本和收益的组成

3.2.1 防御方的收益

当攻击成功（防御方未检测到攻击，或者攻击行动是入侵检测系统（IDS）检测不到的动作），定义防御方的损失为：

$$s\_Damage(att_i(o))::=Con_p*Con_v+Int_p*Int_v+Ava_p*Ava_v \quad (2)$$

Con_p、Int_p和$Ava_p\in[0,1]$分别是攻击i导致的目标在保密性，完整性和可用性的损伤度。Con_p、Int_p、

和Ava_v分别表示目标资产的保密性、完整性和可用性。

当攻击行为被检到时的损失定义为:

$$F\_Damage(att_i(o)) ::= (Con_p * Con_v + Int_p * Int_v + Ava_p * Ava_v) - Restore \quad (3)$$

恢复(*Restore*)是攻击行动后采取防御措施恢复一定的损失,定义为:

$$Restore ::= Con_p^r * Con_v + Int_p^r * Int_v + Ava_p^r * Ava_v \quad (4)$$

防御者的收益是*S_Damage*与*F_Damage*的组合。定义p为入侵检测系统的正确检测的概率,则攻防策略和*Def_Benefit*如表2所示:

表2　攻防策略与*Def_Benefit*之间的关系

攻防策略	*Def_Benefit*
$(att_i(o), D_{(att_i(o))})$	$Def\_Benefit_{11} = -(Con_p * Con_v + Int_p * Int_v + Ava_p * Ava_v) * (1-p) - ((Con_p * Con_v + Int_p * Int_v + Ava_p * Ava_v) - Restore) * p$
$(att_i(o), \neg D_{(att_i(o))})$	$Def\_Benefit_{12} = -(Con_p * Con_v + \mathrm{int}_p * Int_v + Ava_p * Ava_v)$
$(\neg att_i(o), D_{(att_i(o))})$	$Def\_Benefit_{21} = 0$
$(\neg att_i(o), \neg D_{(att_i(o))})$	$Def\_Benefit_{22} = 0$

3.2.2攻击方的收益

文献[10]指出,攻击方的收益取决于防御系统。因此,笔者定义转化率$k \in [0,1]$将防御方的损失转换为攻击方的收益。为简单起见,笔者假设$k=1$,则攻击方的收益为:$Att\_Benefit = -Def\_Benefit$。因此,攻击方的攻防策略和收益如表3所示:

表3　攻防策略与*Att_Benefit*之间的关系

攻防策略	*Att_Benefit*
$(att_i(o), D_{(att_i(o))})$	$Def\_Benefit_{11} = -(Con_p * Con_v + Int_p * Int_v + Ava_p * Ava_v) * (1-p) - ((Con_p * Con_v + Int_p * Int_v + Ava_p * Ava_v) - Restore) * p$
$(att_i(o), \neg D_{(att_i(o))})$	$Att\_Benefit_{12} = (Con_p * Con_v + \mathrm{int}_p * Int_v + Ava_p * Ava_v)$
$(\neg att_i(o), D_{(att_i(o))})$	$Att\_Benefit_{21} = 0$
$(\neg att_i(o), \neg D_{(att_i(o))})$	$Att\_Benefit_{22} = 0$

3.2.3 防御方的成本

防御方的成本由操作成本,响应成本和响应负成本构成。文献[8]指出,操作成本与其他两种成本相比可以忽略不计。响应成本与恢复策略有关,它可以从风险评估框架中的攻防知识库得到。一些响应行为可能会影响到系统的可用性,所以定义响应负成本$A_Cost ::= -P_a * Ava_v$。其中,P_a是响应行为导致的系统可用性的损坏度,它也可以从攻防知识库的得到,$P_a \in [0,1]$。

定义p^m为入侵检测系统的误检测率,因此,攻防策略和*Def_Cost*之间的关系如表4所示。

表4　攻防策略与*Def_Cost*之间的关系

攻防策略	*Def_Cost*
$(att_i(o), D_{(att_i(o))})$	$Def\_Cost_{11} = -(R\_Cost + P_a * Ava_v) * p$
$(att_i(o), \neg D_{(att_i(o))})$	$Def\_Cost_{12} = 0$
$(\neg att_i(o), D_{(att_i(o))})$	$Def\_Cost_{21} = -(R\_Cost + P_a * Ava_v) * p^m$
$(\neg att_i(o), \neg D_{(att_i(o))})$	$Def\_Cost_{22} = 0$

3.2.4 攻击方的成本

定义攻击者的成本时,需要考虑发动攻击 的成本以及当攻击行为被检测时攻击者受到的相应处罚。处罚是由防御方通过法律手段向攻击方收回的由攻击者所发起攻击行动导致的防御方的损失。为简单起见,笔者只考虑前者。因此, 和攻防策略之间关系如表5所示。

表5　攻防策略与 之间的关系

攻防策略	*Act_Cost*
$(att_i(o), D_{(att_i(o))})$	$Att\_Cost_{11} = Act\_Cost + p * Att\_pum$
$(att_i(o), \neg D_{(att_i(o))})$	$Att\_Cost_{12} = Act\_Cost$
$(\neg att_i(o), D_{(att_i(o))})$	$Att\_Cost_{21} = 0$
$(\neg att_i(o), \neg D_{(att_i(o))})$	$Att\_Cost_{22} = 0$

基于以上分析,表1可以细化为:

表6　支付矩阵

攻击策略	防御策略 $D_{(att_i(o))}$	防御策略 $\neg D_{(att_i(o))}$
$att_i(o)$	$\begin{bmatrix} \begin{bmatrix} S\_Damage(att_i(o)) * (1-p) \\ +(S\_Damage(att_i(o)) - Restore) * p \\ -p * Att\_Pun \end{bmatrix}, \\ \begin{bmatrix} -S\_Damage(att_i(o)) * (1-p) \\ -(S\_Damage(att_i(o)) - Restore) * p \\ -(R\_Cost + P_a * Ava_v) * p \end{bmatrix} \end{bmatrix}$	$\begin{bmatrix} S\_Damage(att_i(o)), \\ -S\_Damage(att_i(o)) \end{bmatrix}$
$\neg att_i(o)$	$(0, -(R\_Cost + P_a * Ava_v) * p^m)$	$(0,0)$

3.2.5均衡

假设攻击方选择攻击的概率为θ,那么不攻击的概率为(1-θ);防御方选择防御的概率为γ,那么选择不防御的概率为(1-γ),通过求解期望收益函数和微分方程,得到防御方采取防御行为$D_{att_i(o)}$的概率为:

$$\gamma^* = \frac{(Con_p * Con_v + Int_p * Int_v + Ava_p * Ava_v)}{(Restore + Att\_Pun) * p} \quad (5)$$

由公式(5)可以看出,当p为常量,防御方采取防御行为的动机与攻击造成的损失成正比,与防御方的恢复(*Restore*)和对攻击者的惩罚成反比。

攻击方采取攻击行为$att_i(o)$的概率为:

$$\theta^* = \frac{(R\_Cost + P_a * Ava_v) * p^m}{(R\_Cost + P_a * Ava_v) * (p^m - p) + Restore * p} = \frac{1}{1 + \frac{p}{p^m}} * \frac{(Restore - R\_Cost - P_a * Ava_v)}{(R\_Cost + P_a * Ava_v)} \quad (6)$$

从公式(6)可以看出,当响应损失和恢复(*Restore*)为常量,攻击概率随着正确检测率p值升

高而减小,同时,随着误检测率升高而增大。

4 风险计算模型

结合前文所述攻防博弈模型,构建如图3所示的分层风险计算模型:

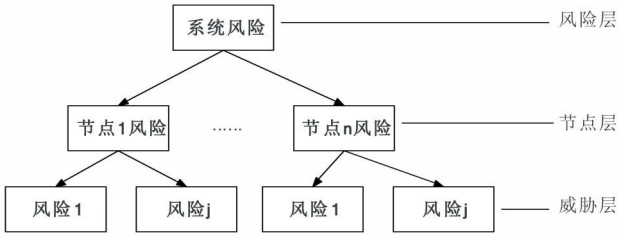

图3 风险计算模型

基于攻防博弈模型,使用图3所示的风险计算模型自下而上计算风险。首先,可以得到当攻击方发现系统的脆弱性的威胁概率($P_{(att_i(o))} \in [0,1]$),结合防御策略,可以计算出系统损失的期望($ED_{(att_i(o))}$)。进一步,可以得到攻击的风险为:

$$Risk_{(att_i(o))} = P_{(att_i(o))} * ED_{(att_i(o))} \quad (7)$$

其中,$ED_{(att_i(o))}=Def\_Benefit$。$Def\_Benefit$ 由系统防御方选择的 $D_{(att_i(o))}$ 或 $\neg D_{(att_i(o))}$ 确定。因此,节点 O 的风险定义为:

$$Risk_{(o)} = \sum_{i=1}^{n_0} Risk_{(att_i(o))} \quad (8)$$

n_0 表示节点 O 的总威胁,即一个节点的风险值是节点的威胁值的总和。因此,该系统的风险为:

$$Risk_{system} = \sum_{i=1}^{n} Risk_{(i)} \quad (9)$$

代表是脆弱的节点的数量。

5 结束语

针对目前的网络安全风险评估的威胁概率量化,本文介绍博弈论模型的攻击防御行为;本文分析了在攻防双方决策基础上的成本和效益因素,计算了均衡点找到量化的威胁概率。

注释及参考文献:

[1]Haslum, K. and Arnes, A., Multisensor real-time risk assessment using continuous-time hidden markov models[C]. Computational Intelligence and Security, 2006 International Conference on.2006, 2: 1536-1540.

[2]Gao, H., Zhu, J. and Li, C., The analysis of uncertainty of network security risk assessment using Dempster-Shafer theory [C]. Computer Supported Cooperative Work in Design, 2008. CSCWD 2008. 12th International Conference on.2008: 754-759.

[3]姜伟,方滨兴,田志宏,等.基于攻防博弈模型的网络安全测评和最优主动防御[J].计算机学报,2009, 32(4): 817-827.

[4]Sallhammar, K., Stochastic models for combined security and dependability evaluation[D].Norwegian University of Science and Technology:2007.

[5]谢识予.经济博弈论[M].复旦大学出版社,2002.

[6]Stoneburner, G., Goguen, A. and Feringa, A., Risk management guide for information technology systems[J]. Nist special publication.2002, 800(30): 800-30.

[7]Ritchey, R., O'Berry, B. and Noel, S., Representing TCP/IP connectivity for topological analysis of network security[C]. Computer Security Applications Conference, 2002. Proceedings. 18th Annual.2002: 25-31.

[8]Lee, W., Fan, W., Miller, M., Stolfo, S.J. and Zadok, E., Toward cost-sensitive modeling for intrusion detection and response [J]. Journal of Computer Security.2002, 10(1): 5-22.

[9]Jiang, W., Zhang, H.-L., Tian, Z.-H. and Song, X.-F., A game theoretic method for decision and analysis of the optimal active defense strategy[C]. Computational Intelligence and Security, 2007 International Conference on.2007: 819-823.

[10]Jin, S., Yin, L. and Li, X., Dynamic Intrusion Response Based on Game Theory [J]. Journal of Computer Research and Development.2008, 5: 001.

Attack and Defensive Game Model Based on Network Security Risk Assessment

HUANG Peng, ZHANG Na

(School of Automotive and Electronic Engineering, Xichang College, Xichang, Sichuan 615013)

Abstract: How to quantify the threat probability of network security risk is an important problem to be solved. The nature of attack and defense against network security can be abstracted as mutual influence of both strategies. Whether the defense strategy adopted by defenders is valid not only depend on their own behavior, but also depend on the strategy of the attacker and the defense system. The decision to implement the attack of an attack is a

(下转第86页)

The Application of CDIO in Program Design Courses of Non-computer Professionals

——Taking Universities in Ethnic Areas as an Example

WEI Lai-ke

(Xichang College, Xichang, Sichuan 615013)

Abstract: The article discusses the current situation and the drawbacks of teaching programming courses, and analyzes the CDIO concept and idea, CDIO thought in the course of the program design can improve the shortcomings in courses now and promote students to master the programming courses .

Key words: CDIO; program design courses; applicaiton

（上接第74页）

trade-off between income and the potential consequences. The defender's security strategy depends on understanding of the intent of the attacker. This paper presents the possibility of an offensive and defensive game model to quantify the threat to construct a risk assessment framework. Based on cost-benefit analysis, we define the payoff matrix method developed and analyzed the balance of the model.

Key words: game theory; network security; risk assessment