·CTCIS 2016 推荐论文· DOI:10.15961/j.jsuese.201601046

基于攻防行为树的网络安全态势分析

付 钰,俞艺涵,陈永强,周学广
(海军工程大学 信息安全系,湖北 武汉 430033)

摘 要:现代网络面临遭受组合攻击的风险,通过构建基于攻防行为的安全态势分析模型来对每一个独立及组合攻击行为进行威胁分析十分必要。本文针对传统的攻击树模型没有考虑防御因素影响,防御树模型缺乏较好的可扩展性,故障树模型难以对外部攻击进行分析等问题,在攻击树模型中引入博弈论,以描述具体网络攻防事件场景。首先,分析网络中不同层次攻击行为的逻辑关系,整合不同层次攻击事件对应的攻防树,获得完整网络攻防行为树,进而构建网络攻防行为树模型。其次,从网络攻防行为、网络检测设备以及网络防御措施3方面对基本攻防行为树进行扩展,提出攻击目标成功率算法,计算其攻击概率。在此基础上,对攻击威胁进行评估,分析网络安全态势。最后,为验证网络攻防行为树模型的可行性和有效性,在BGP(border gateway protocol)攻击树的基础上构建攻防行为树模型,通过概率计算可知:攻击路径*PATH*1概率最大;且在没有防御措施的情况下,5条攻击路径的攻击成功率均得到增大,*PATH*2至*PATH*5概率增大倍数显著高于*PATH*1,与实际相符。本文所提的网络攻防行为树模型能很好地计算各种防御措施的效果,且能够在任意节点添加和删除攻防行为,具有较强的可扩展性,可为网络管理者与运营者提供科学的决策依据。

关键词:网络安全;态势分析;行为树;攻击行为树;防御行为树
中图分类号:TP393 **文献标志码**:A **文章编号**:2096-3246(2017)02-0115-06

Network Security Analysis on Attack-defense Behavior Tree

FU Yu, *YU Yihan*, *CHEN Yongqiang*, *ZHOU Xueguang*
(Dept. of Info. Security, Naval Univ. of Eng., Wuhan 430033, China)

Abstract: Modern network is subjected to the risk of combined attack. Therefore, a security situation analysis model based on attack and defense behavior is necessary to be build for analyzing the threat of each independent and combined attack behaviors. Aiming at the problems that the defense factors is not taken into account by the traditional attack tree, the defense tree model lacks good scalability and external attacks were hard to be analyzed by fault tree model, in this paper, the game theory was introduced into attack tree model to describe the specific network attack incident scene. Firstly, logical relationship between different levels of aggressive behavior was analyzed. Offensive and defensive attack trees corresponding to different attack levels are then integrated, and the complete network attack behavior tree was lately obtained. Based on the above steps, an algorithm on the network threat offensive behavior tree was proposed. By finding aggression combinations, analyzing its attack probability, and assessing the threat of attack, the network security situation was analyzed. In order to verify the feasibility and effectiveness of the attack behavior tree model, it was built on the basis of BGP(border gateway protocol) attack tree. By calculating the probability, the probability of *PATH*1 was largest. Meanwhile, the attack success rates of five attack paths were increased in the case of no defense measures. The probabilities of *PATH*2 to *PATH*5 were increased significantly higher than *PATH*1 which is consistent with facts. The experimental analysis showed that the model can calculate the effect of various defensive measures very well, which provides a theoretical basis of carrying out targeted network security defense.

Key words: network security; situation analysis; behavior tree; attack behavior tree; defense behavior tree

收稿日期:2016-06-28
基金项目:国家社会科学基金军事学资助项目(15G003-201);中国博士后基金资助项目(2014M552656);湖北省自然科学基金资助项目(2015CFC867)
作者简介:(1982—),女,副教授,博士. 研究方向:军事信息安全;系统建模与优化. E-mail:fuyu0219@163.com

网络的开放性、互联性和共享性等特点使其遭受网络入侵的风险日益增加,攻击手段的智能化、复杂化和多样化对传统的防护方法提出了严峻的挑战[1]。在网络中,针对某一特定目标,仅实施攻击事件所包含的单一或部分攻击行为不一定能构成威胁,攻击者为提高攻击成功率,其攻击事件往往由多个独立攻击行为所组成。例如,初期通过脆弱性扫描获得网络安全漏洞,实际上并不构成威胁,但如果通过掌握的安全漏洞展开进一步攻击,则其可能威胁网络安全。因此,分析网络面临的组合攻击形态,构建基于攻防行为的安全态势分析模型,对每一个独立及组合攻击行为进行威胁分析十分必要。

传统的攻击树模型[2-3]基于攻击行为进行建模,没有考虑防御因素影响。防御树模型[4-6]从防御的角度构建防御模型,但只能在叶节点添加防御措施,缺乏较好的可扩展性。故障树方法[7-8]通过分析目标事件发生的原因及彼此间的关系构建逻辑图,分析目标事件发生的原因和概率,但该方法适用于对系统内部产生的故障,难以对外部攻击进行分析。

针对以上问题,作者将攻击树和防御树进行整合进而构建网络攻防行为树,利用攻防树的特性描述具体的攻防行为场景,给出网络攻防树威胁算法,寻找可能存在的各种攻击行为组合,分析网络安全态势,对于发现网络关键脆弱性或链路,有效配置网络资源,优化网络系统等,具有重要理论意义。

1 网络攻防行为树模型

网络安全态势可从目标攻击成功率和攻击成功后对网络系统损害效果两个角度分析。不同攻防行为相关概率差异给网络安全造成了不同影响,本文从攻防行为及检测概率的角度对网络安全态势进行分析。首先,给出基于网络攻防行为树的安全态势分析架构,如图 1 所示。

将攻防行为树定义为一个三元组 $ADT = \{N, E, \psi\}$,其中:

1)节点集为:

$N = \{\forall k, n_k : n_k = n_0 \parallel n_k \in A_a \parallel n_k \in A_d \parallel n_k \in D\}$。其中,$n_0$ 表示根节点,代表攻击目标;D 表示入侵检测节点,代表入侵检测设备;A_a 和 A_d 分别表示攻击节点和防御节点,代表攻防双方可能采取的攻防行为。攻防行为树中的节点按照攻防性质可分为根结点(目标节点)、入侵检测节点、攻击节点以及防御节点 3 类。按照层次结构,可以分为根结点、中间节点和叶节点:最上层的根结点即为攻击目标(目标节点),要达到攻击目标的原子攻击行为和防御行为用叶节点表示,中间节点表示攻击的子目标。

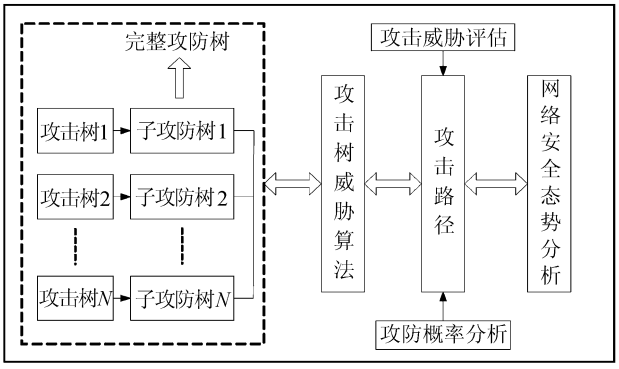


图 1 基于攻防行为树的网络安全分析架构

Fig. 1 Architecture for the network security analysis based on attack-defense tree

2)边集为:

$E = \{\forall k, e_k : e_k \in (n_i, \psi_j) \parallel e_k \in (\psi_i, \psi_j)\}$。

ADT 的边存在两种情况:一种表示节点和逻辑门间的连接关系 $e_k \in (n_i, \psi_j)$;一种表示两逻辑门间的连接关系 $e_k \in (\psi_i, \psi_j)$。

3)逻辑门集为:

$\psi = \{\forall n_k \in N, \psi(n_k) : \psi(n_k) \in \{\text{AND}, \text{OR}\}\}$。其中,$\psi(n_k)$ 反映了节点 n_k 与其子节点之间的逻辑关系。AND 逻辑门表示目标节点的所有子节点所对应的子目标均满足时才能达到该目标;OR 逻辑门表示满足任意节点即可。

攻防树模型利用树状结构描述网络可能遭受的攻击,一个简单的树形结构如图 2 所示。

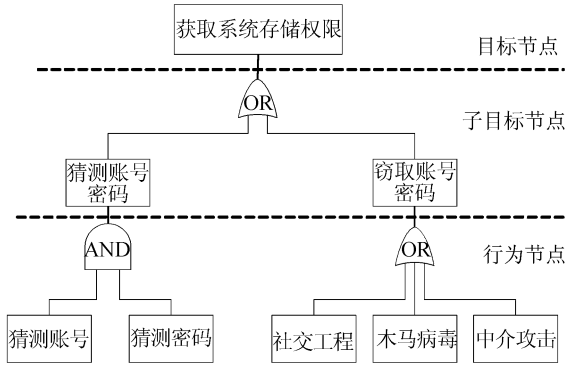


图 2 攻击树范例

Fig. 2 Basic attack-defense action tree

其中,最上层的根结点(获取系统存储权限)为目标节点,叶节点表示要获取系统存储权限所使用的方法。中间节点表示攻击子目标,按照逻辑关系而定,例如,窃取账号密码子目标的逻辑门为 OR,因此,只要社交工程、木马病毒或中介攻击任意一个原子攻击行为完成即可;猜测账号密码子目标的逻

辑门为 AND,猜账号和猜密码两个原子攻击行为必须同时满足才能获得系统存储权限,任缺其一则无法达到目标,可见独立或部分的攻击行为并不一定构成威胁。

2　目标攻击成功率算法

2.1　目标攻击成功率

目标攻击成功率从攻击与防御的角度出发,考虑存在的防御措施,从可被检测及防御两个方面来分析攻击事件的成功率, $p_{\text{goal}} = f(attack, defense, prodection)$。目标攻击成功率可以分为两部分;一是,攻击行为未被检测发现;二是,攻击行为被检测设备检测到但是未被防御措施成功阻止。网络攻防行为树的基本图形如图 3 所示,即只存在一种攻击行为、一种防御行为和一个检测设备。攻击者发起攻击行为 A_a 的概率为 p_{A_a},防御者通过入侵检测 D 获知攻击信息并采用防御措施 A_d,则攻击目标成功率 $p_{\text{goal}} = p_{A_a}(1 - p_D^a + p_D^a(1 - p_d^a))$,其中 P_{goal} 表示攻击目标成功率,p_D^a 为检测设备 D 成功检测到攻击行为 A_a 的概率,p_d^a 为防御措施 A_d 针对攻击行为 A_a 的防御有效率。

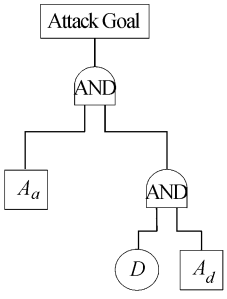


图 3　基本攻防行为树

Fig. 3　Basic attack-defense action tree

在基本攻防行为树的基础上从网络攻防行为、网络检测设备以及网络防御措施 3 方面对其进行扩展,如图 4 所示。

1)攻击行为扩展。攻击者发起攻击行为 $A_{a1}, A_{a2}, \cdots, A_{ak}$,攻击行为发生率为 $p_{A_{a1}}, p_{A_{a2}}, \cdots, p_{A_{ak}}$,检测设备 D 对 $A_{a1}, A_{a2}, \cdots, A_{ak}$ 的检测率分别为 $p_D^1, p_D^2, \cdots, p_D^k$,防御措施 A_d 针对攻击行为 $A_{a1}, A_{a2}, \cdots, A_{ak}$ 的防御有效率分别为 $p_d^{a1}, p_d^{a2}, \cdots, p_d^{ak}$,在此情形下,要求所有攻击行为均完成才能实现攻击目标。攻击行为 A_{ai} 的攻击成功率为 $p_{ai}^{\text{suc}} = p_{A_{ai}}(1 - p_D^i + p_D^i(1 - p_d^{ai}))$,总目标攻击成功率:

$$p_{\text{goal}} = \prod_{i=1}^{k} p_{ai}^{\text{suc}} = \prod_{i=1}^{k} p_{A_{ai}}(1 - p_D^i + p_D^i(1 - p_d^{ai}))。$$

如果逻辑节点为 OR,则只要有一种攻击完成即可实现攻击目标。因此,则目标攻击成功率:

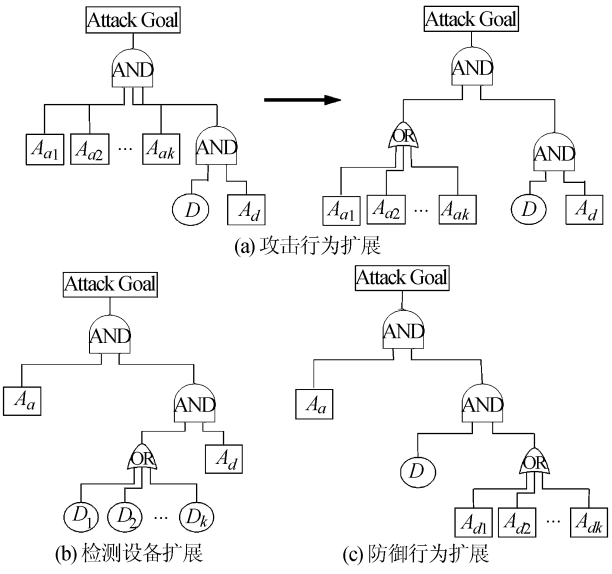


图 4　基本攻防行为树扩展

Fig. 4　Extend of basic attack-defense action tree

$$p_{\text{goal}} = \max_{1 \le i \le k} p_{ai}^{\text{suc}} = \max_{1 \le i \le k} p_{A_{ai}}(1 - p_D^i + p_D^i(1 - p_d^{ai}))。$$

2)检测设备扩展。攻击者发起攻击行为 A_a,网络中配置了检测设备 $D_1, D_2, \cdots, D_k$,检测设备对攻击行为的检测率分别为 $p_{D_1}^a, p_{D_2}^a, \cdots, p_{D_k}^a$,防御措施 A_d 针对攻击行为 A_a 的防御有效率为 p_d^a,则攻击行为未被检测到的概率 $p_{A_a}\prod_{i=1}^{k}(1 - p_{D_i}^a)$,被检测到但防御措施未成功的概率为 $p_{A_a}(1 - \prod_{i=1}^{k}(1 - p_{D_i}^a))(1 - p_d^a)$,因此攻击目标成功率:

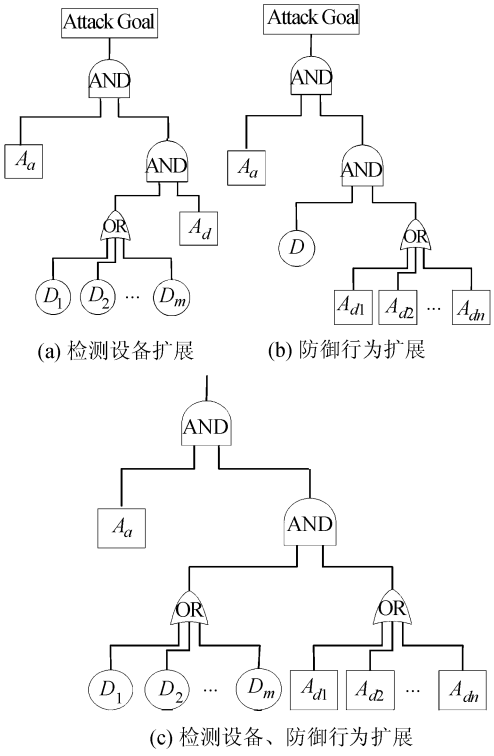
$$p_{\text{goal}} = p_{A_a} \times (\prod_{i=1}^{k}(1 - p_{D_i}^a) + (1 - \prod_{i=1}^{k}(1 - p_{D_i}^a))(1 - p_d^a)) = p_{A_a} \times (1 - (1 - \prod_{i=1}^{k}(1 - p_{D_i}^a)) \times p_d^a)。$$

3)防御措施扩展。攻击者发起攻击行为 A_a,检测设备 D 成功检测到攻击行为 A_a 的概率为 p_D^a,防御措施为 $A_{d1}, A_{d2}, \cdots, A_{dk}$,防御措施对攻击 A_a 的防御有效率分别为 $p_{d1}^a, p_{d2}^a, \cdots, p_{dk}^a$,攻击行为未被检测到的概率为 $p_{A_a}(1 - p_D^a)$,攻击行为被检测到但未有效实施防御概率为 $p_{A_a}p_D^a\prod_{i=1}^{k}(1 - p_{di}^a)$,攻击目标成功率:

$$p_{\text{goal}} = p_{A_a}((1 - p_D^a) + p_D^a\prod_{i=1}^{k}(1 - p_{di}^a)) = p_{A_a}(1 - p_D^a \times (1 - \prod_{i=1}^{k}(1 - p_{di}^a)))。$$

对图 4(b)和(c)进行整合,即同时对网络检测

设备和防御措施进行扩展,如图5所示。



(a) 检测设备扩展 (b) 防御行为扩展

(c) 检测设备、防御行为扩展

图5 攻防行为树扩展

Fig. 5 Extend of attack-defense action tree

攻击者发起攻击行为A_a,检测设备$D_1,D_2,\cdots,D_m$成功检测到攻击行为A_a的概率为$p^a_{D_1},p^a_{D_2},\cdots,p^a_{D_m}$,防御措施为$A_{d1},A_{d2},\cdots,A_{dn}$,防御措施对攻击$A_a$的防御有效率分别为$p^a_{d1},p^a_{d2},\cdots,p^a_{dn}$,攻击行为未被检测到的概率为$\prod_{i=1}^{m}(1-p^a_{Dj})$,攻击行为被检测到但未有效实施防御的概率为$\prod_{j=1}^{n}(1-p^a_{di})$,攻击目标成功率:

$$p_{\text{goal}} = p_{A_a}(1-(1-\prod_{i=1}^{m}(1-p^a_{Dj}) \times (1-\prod_{j=1}^{n}(1-p^a_{di})))) 。$$

2.2 攻击目标成功率算法

对于特定攻击目标常存在多条攻击路径,而不同的攻击路径达到目标的概率不同。通常情况下,理性攻击者会选择成功率最大的攻击路径,本文将攻击路径的最大成功率作为攻击目标成功率,即:

$P_{\text{goal}} = \max(P(PATHS_1),P(PATHS_2),\cdots,P(PATHS_n))$

给出如下攻击目标攻击成功率算法:

Algorithm: Computer_Attack_PATH(T_r) and P_{goal}

Input: An attack-defense tree T with r being the root, $P_{\text{goal}} = 0$

Output: attack-strategy, P_{goal}

1. If r is the only node of the tree T then
2. return path(r) = 1
3. else
4. let $v_1,v_2,\cdots,v_k$ be the k children nodes of r
5. for i = 1 to k do
6. Computer_Attack_PATHs (T_{vi}) and P_{goal}
7. end for i
8. do case
9. case 1: r is OR node
10. turn $PATH(r) = \sum_i PATH(v_i)$, and $P_{\text{goal}} = \max p^{\text{suc}}_{ai}$
11. case 2: r is AND node
12. return $PATH(r) = \prod_i PATH(v_i)$, and $P_{\text{goal}} = \prod_i p^{\text{suc}}_{ai}$
13. end case
14. end If

3 网络安全态势分析

依据风险定义,攻击事件的风险值R_{goal}等于攻击事件的成功概率P_{goal}乘以其对目标造成的损害U_{goal},即$R(A_a)_{\text{goal}} = U^{A_a}_{\text{goal}} \times P^{A_a}_{\text{goal}}$。网络系统根据其用途及防护目标不同,相应的安全属性指标也不相同。攻击行为对网络安全性造成的影响可以用网络系统安全度量指标的下降程度来描述,本文主要考虑机密性、完整性和可用性3个网络系统安全属性指标,应用多属性效用理论来度量目标节点的安全量化值:$U_{\text{goal}} = \lambda_C U(C) + \lambda_I U(I) + \lambda_A U(A)$,其中:$U_{\text{goal}}$为攻击目标达成对网络系统造成的损害,$\lambda_C$、$\lambda_I$、$\lambda_A$表示各安全指标的权重,反映各安全属性对网络影响程度,$U(C)$、$U(I)$、$U(A)$为各安全指标的效用性。

对于特定的攻击目标,最大的目标攻击成功概率与攻击对目标造成损害的乘积即是该目标的风险值,用R_{goal}表示:$R^{\text{without}A_d}_{\text{goal}} = U_{\text{goal}} \times \max P^{\text{without}A_d}_{\text{goal}}$,$R^{\text{with}A_d}_{\text{goal}} = U_{\text{goal}} \times \max P^{\text{with}A_d}_{\text{goal}}$。$R^{\text{without}A_d}_{\text{goal}}$、$R^{\text{with}A_d}_{\text{goal}}$分别为系统不采取防御措施和采取防御措施时的网络风险值,$P^{\text{without}A_d}_{\text{goal}}$、$P^{\text{with}A_d}_{\text{goal}}$分别为未采取防御策略和采取防御措施时攻击目标达成概率。防御措施的防御效果E_{A_d}可用损害的差值表示,亦可反映网络的安全性:

$$E_{A_d} = \Delta Risk_{\text{goal}} = Risk^{\text{without}A_d}_{\text{goal}} - Risk^{\text{with}A_d}_{\text{goal}} = U_{\text{goal}} \times \max P^{\text{goal}}_{\text{without}A_d} - U_{\text{goal}} \times \max P^{\text{goal}}_{\text{with}A_d} 。$$

4 实例分析

为验证网络攻防行为树模型的可行性和有效

性,在文献[9]中 BGP(border gateway protocol)攻击树的基础上构建攻防行为树模型,如图 6 所示。攻防行为信息如表 1 和 2 所示,检测信息如表 3 所示,对抗信息如表 4 所示。

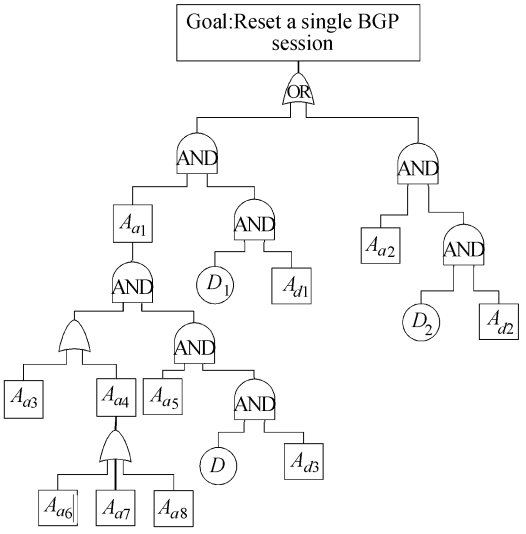


图 6　BGP 攻防行为树

Fig. 6　Attack-defense tree of BGP

表 1　攻击行为信息

Tab. 1　Information of network attack action

Symbol	Attack action description	p_{Aa}
A_{a1}	Send message to router causing reset	—
A_{a2}	Alter configuration via compromised router	0.4
A_{a3}	Send RST message to TCP stack	0.3
A_{a4}	Send BGP message	—
A_{a5}	TCP sequence number attack	0.7
A_{a6}	Notify	0.1
A_{a7}	Open	0.15
A_{a8}	Keep Alive	0.2

表 2　防御行为信息

Tab. 2　Information of network defense action

Symbol	Defense action description	p_d^a
d_1	Randomize sequence number	0.6
A_{d2}	Secure router	0.5
A_{d3}	MD5 authentication	0.5

表 3　检测信息

Tab. 3　Information of network detection

Symbol	Defense action	p_D^a
D_1	Trace route check	0.5
D_2	Router firewall alert	0.7
D_3	TCP sequence number check	0.8

表 4　攻防对抗信息

Tab. 4　Information of attack-defense action

	防御有效率			检测率		
	A_{d1}	A_{d2}	A_{d3}	D_1	D_2	D_3
A_{a1}	0.5	—	—	0.6	—	—
A_{a2}	—	0.5	—	—	0.7	—
A_{a3}	—	—	—	—	—	—
A_{a4}	—	—	—	—	—	—
A_{a5}	—	—	0.5	—	—	0.6

为达成目标 Reset a single BGP session,攻击者存在 5 条攻击路径可供选择,由攻击目标攻击成功率算法可计算每条攻击路径的成功概率:

$$PATH1: A_{a2}(D_2, A_{d2}) \rightarrow Goal;$$
$$P_{\text{goal}}^{\text{with}A_d}(PATH1) = 0.26。$$
$$PATH2: A_{a3} \times A_{a5}(D_3, A_{d3}) \rightarrow A_{a1}(D_1, A_{d1}) \rightarrow Goal;$$
$$P_{\text{goal}}^{\text{with}A_d}(PATH2) = 0.09。$$
$$PATH3: A_{a6} \rightarrow A_{a4} \times A_{a5}(D_3, A_{d3}) \rightarrow A_{a1}(D_1, A_{d1}) \rightarrow Goal;$$
$$P_{\text{goal}}^{\text{with}A_d}(PATH3) = 0.03。$$
$$PATH4: A_{a7} \rightarrow A_{a4} \times A_{a5}(D_3, A_{d3}) \rightarrow A_{a1}(D_1, A_{d1}) \rightarrow Goal;$$
$$P_{\text{goal}}^{\text{with}A_d}(PATH4) = 0.04。$$
$$PATH5: A_{a8} \rightarrow A_{a4} \times A_{a5}(D_3, A_{d3}) \rightarrow A_{a1}(D_1, A_{d1}) \rightarrow Goal;$$
$$P_{\text{goal}}^{\text{with}A_d}(PATH5) = 0.06。$$

由此可见,攻击路径 *PATH*1 概率最大,因为其攻击手段最为直接,且面临的检测和防御措施较少。当系统没有布置防御措施时,通过目标攻击成功率算法计算上述 5 条攻击路径的成功概率如下:

$$PATH1: A_{a2}(D_2) \rightarrow Goal,$$
$$P_{\text{goal}}^{\text{without}A_d}(PATH1) = 0.4。$$
$$PATH2: A_{a3} \times A_{a5}(D_3) \rightarrow A_{a1}(D_1) \rightarrow Goal,$$
$$P_{\text{goal}}^{\text{without}A_d}(PATH2) = 0.21。$$
$$PATH3: A_{a6} \rightarrow A_{a4} \times A_{a5}(D_3) \rightarrow A_{a1}(D_1) \rightarrow Goal,$$
$$P_{\text{goal}}^{\text{without}A_d}(PATH3) = 0.07。$$
$$PATH4: A_{a7} \rightarrow A_{a4} \times A_{a5}(D_3) \rightarrow A_{a1}(D_1) \rightarrow Goal,$$
$$P_{\text{goal}}^{\text{without}A_d}(PATH4) = 0.105。$$
$$PATH5: A_{a8} \rightarrow A_{a4} \times A_{a5}(D_3) \rightarrow A_{a1}(D_1) \rightarrow Goal,$$
$$P_{\text{goal}}^{\text{without}A_d}(PATH5) = 0.14。$$

在没有防御措施的情况下,5 条攻击路径的攻击成功率均得到增大,且 *PATH*2 至 *PATH*5 概率增大倍数显著高于 *PATH*1,因为后 4 条路径采取的多攻击行为组合,在没有防御措施的情况下,其成功概率会高于单攻击行为的成功概率,与实际情况相符。

假设攻击目标的网络安全属性向量为(200,

150,300),其影响权重向量为(0.35,0.25,0.4),各防御措施的防御效果:

$$\Delta Risk_{goal}(PATH1) = 31.85,$$
$$\Delta Risk_{goal}(PATH2) = 27.3,$$
$$\Delta Risk_{goal}(PATH3) = 9.1,$$
$$\Delta Risk_{goal}(PATH4) = 14.8,$$
$$\Delta Risk_{goal}(PATH5) = 18.2。$$

5 结 论

随着信息化的全面推进与网络的广泛应用,网络安全形势日益严峻,网络安全问题的研究成为热点。论文将原有攻击树模型进行扩展,构建了网络攻防行为树模型,利用博弈论和攻防树的特性描述具体的攻防事件场景,分析了不同层面攻击行为的逻辑关系,通过整合各种不同层次攻击事件对应的攻防树以获得完整网络攻防行为树,给出了的网络目标攻击成功率算法,从攻防行为概率的角度分析了网络安全态势。该方法能够在任意节点添加和删除攻防行为,具有较强的可扩展性,可为网络管理者与运营者提供科学的决策依据。

参考文献:

[1] Chen Yongqiang, Fu Yu, Wu Xiaoping. Security analysis of complex network based on system brittleness map[J]. Journal of Naval University of Engineering, 2013, 25(3): 30-33. [陈永强,付钰,吴晓平. 基于系统脆性图的复杂网络安全性分析[J]. 海军工程大学学报,2013,25(3):30-33.]

[2] Zhang Kailun, Jiang Quanyuan. Evaluating the weakness of WAMS communication system based on attack tree-model [J]. Protection and Control of Electronic System, 2013, 41(7): 116-122. [张凯伦,江全元. 基于攻击树模型的WAMS通信系统脆弱性评估[J]. 电力系统保护与控制,2013,41(7):116-122.]

[3] Niu Binru, Liu Peiyu, Duan Linshan. A improved attack tree-based trojan analysis and detection[J]. Computer Application and Software, 2014, 31(3): 277-280. [牛冰茹,刘培玉,段林珊. 一种改进的基于攻击树的木马分析与检测[J]. 计算机应用与软件,2014,31(3):277-280.]

[4] Bistarelli S, Dall'Aglio M D, Peretti P. Strategic games on defense trees[M]//Formal Aspects in Security and Trust. Heidelberg: Springer, 2007: 1-15.

[5] Bistarelli S, Fioravanti F, Peretti P. Defence trees for economic evaluation of security Investments[C]//Proceedings of the First International Conference on Availabibty Reliability and Security, 2006 (ARES'06). Vienna: IEEE, 2006: 416-423.

[6] Zhang Dehong. The research of attack-defense strategy and active defense in network security[J]. Natural Sciences Journal of Harbin Normal University, 2012, 28(2): 49-53. [张德洪. 网络安全中攻防策略与主动防御研究[J]. 哈尔滨师范大学(自然科学学报),2012,28(2):49-53.]

[7] Zhang Honglin, Zhang Chunyuan, Liu Dong, et al. A method of disjoint quantitative analysis for dynamic fault tree [J]. Journal of Computer Research and Development, 2012, 49(5): 983-995. [张红林,张春元,刘东,等. 动态故障树的不交化定量分析方法[J]. 计算机研究与发展,2012,49(5):983-995.]

[8] Xu Binfeng, Huang Zhiqiu, Hu Jun, et al. A method for quantitative analysis of state/event fault tree[J]. Acta Electronica sinica, 2013, 41(8): 1480-1486. [徐丙凤,黄志球,胡军,等. 一种状态事件故障树的定量分析方法[J]. 电子学报,2013,41(8):1480-1486.]

[9] Convery S, Cook D, Franz M. An attack tree for the border gateway protocol[R]. Washington DC: IETF, 2004.

(编辑 赵 婧)

引用格式: Fu Yu, Yu Yihan, Chen Yongqiang, et al. Network security analysis on attack-defense behavior tree[J]. Advanced Engineering Sciences, 2017, 49(2): 115-120. [付钰,俞艺涵,陈永强,等. 基于攻防行为树的网络安全态势分析[J]. 工程科学与技术,2017,49(2):115-120.]