一种基于攻防图的网络安全防御策略生成方法

戚 湧 莫 璇 李千目
(南京理工大学计算机科学与工程学院 南京 210094)

摘 要 复杂的网络多步攻击是当前典型的强目的性网络攻击方式,状态攻防图技术是对其进行建模分析的一种有效方案。但是,当前主流的状态攻防图技术在实施过程中存在众多局限性,如原子攻击成功概率的计算、攻击危害指数定义,使得在实际应用中如果实施人员的经验不足,则很难反映出真实网络安全态势。分析现有基于状态攻防图的网络安全防御策略生成方法的不足,改进脆弱点危害评分标准,引入攻击累计成功概率及主机信息资产值的概念,重新定义原子攻击危害指数与攻击路径危害指数的计算方式,对安全策略生成所需考虑的因素进行扩充,对安全策略的生成方法进行优化,实现攻击场景建模和攻击意图挖掘。最后通过算例分析验证了改进的方法更加易于实施和客观分析,为管理人员做出合理的防御决策提供了有效的辅助。

关键词 攻防图,CVSS,网络安全,防御策略
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.024

Improved Network Security Defense Strategy Generation Method Based on Attack-Defense Graph

QI Yong MO Xuan LI Qian-mu
(School of Computer Science and Engineering, Nanjing University of Science & Technology, Nanjing 210094, China)

Abstract Complex multi-step cyber-attack is a typical network attack method with strong purpose, and state attack-defense graph is an effective method for modeling and analyzing this problem. But it still has some limitation in practice, for example, the computation of the success probability of atomic attack and the definition of attack severity index are not so reasonable. When the operator is not experienced enough, it is very likely that the result can hardly reflect the real security situation of the network. By analyzing the shortages of existing security defense strategy generation method, the attack severity index of atomic attack and attack path were redefined by improving the vulnerability scoring standard and introducing the concepts like accumulated attack success probability and value of information asset. In this way, the considerations for security defense strategy generation is enlarged and the generation method is optimized, to realize the attack scene modeling and the attack intention mining. At last, a case study is made to prove the feasibility and the objectivity of the improved method, which can provide the network managers with effective assistant.

Keywords Attack-defense graph, CVSS, Network security, Defense strategy

1 引言

随着泛在网络、移动互联网等网络信息化技术的不断推进,网络规模和各类应用日益广泛,信息安全问题也层出不穷。据2015年6月的IDC统计,目前网络系统受到的强目的性攻击方式有5大类72小类,其中32.8%属于多步攻击。多步攻击主要是利用网络中脆弱点间的联系,对关键资产进行越权访问、窃取甚至损毁[1]。现有的脆弱性扫描软件还不具备分析潜在多步攻击可能性的能力,采用人侵检测、防火墙、防毒墙及防毒软件等基于规则的传统安全防御技术也很难对脆弱点间的相互作用进行全面评估,其防御方式具有片面性和被动性。

攻击图(Attack Graph)是解决多步攻击问题普遍采用的一种方法,对此专家学者开展了大量研究工作。Dantu等[2]提出了一种对攻击图中节点进行概率建模的方案,利用贝叶斯方法进行网络风险分析。Poolsappasit等提出了一种称为贝叶斯攻击图的风险评估模型[3],通过计算贝叶斯攻击图中每个属性的期望损益值进行风险评估。Albanese等基于攻防图技术从防御措施存在相互依赖的事实出发,建立了防御成本模型,提出了一种高时效、低成本的网络安全防御方法[4]。Wang等结合攻击图和隐马尔可夫模型提出了一种网络安全状态评估方法用于探索安全事件与安全状态间的概率关系[5]。罗智勇等[6]提出了一种简化的攻击图算法,并将其应用于防御系统中,但是该算法中的脆弱性危害评分是主观确定的,也无法针对确定的目标主机给出防御策略。刘刚等[7]结合攻击图和防御图的思想,提出了一种状态攻防图模型,同时从攻防双方的角度出发,设计了安全防御策略的生成算法,该模型采用通用脆弱点评估系统(CVSS)的默认评分标准计算原子攻击成功发生的概率和危害指数。但CVSS默认标准产生的分值通常不具有高多样性,不能有效区分各脆弱点的

到稿日期:2015-08-31 返修日期:2015-12-14 本文受国家自然科学基金项目(61272419)资助。
戚 湧(1970-),男,博士后,教授,博士生导师,CCF高级会员,主要研究方向为网络安全,E-mail:790815561@qq.com;莫 璇(1992-),男,硕士生,主要研究方向为网络安全;李千目(1979-),男,博士后,教授,博士生导师,主要研究方向为网络安全。

实际危害情况[8,9]。其次文献[7]在计算原子攻击危害指数时，仅考虑了当前原子攻击自身成功的可能性，忽视了攻击路径上父原子攻击的作用，也忽视主机信息资产价值不同时同样原子攻击造成危害的差异性。

针对上述问题，本文对 Spanos[10] 提出的加权脆弱点危害评分系统(WIVSS)进行改进，设计了原子攻击危害和原子攻击成功概率的计算方式，引入了攻击累计成功概率及主机信息资产值的概念，重新定义了原子攻击危害指数与攻击路径危害指数的计算方式，以期使状态攻防图更好地反映真实网络安全态势，并据此生成防御策略，为管理人员做出合理的防御决策提供有力辅助。

2 状态攻防图模型

定义 1(状态攻防图) 状态攻防图为一个状态转换系统图 $SADG=(S,T,s_0,S_G)$。其中，S 为图中安全状态节点构成的集合，反映网络中节点的安全状态；T 为边集，表示目标网络中安全状态的跃迁；s_0 是网络初始安全状态；S_G 是攻击者目标状态集合。

定义 2(安全状态节点) 在状态攻防图中，安全状态节点用二元组(*hostid*, *privilege*)表示。其中 *hostid* 是该网络安全状态下安全要素发生变化的主机节点名，*privilege* 是到达该安全状态时攻击者获得主机节点 *hostid* 上的权限。

定义 3(安全状态变迁) 在状态攻防图中，安全状态变迁用五元组(tid, vid, $harm$, p, d)表示。其中，tid 是安全状态变迁编号，vid 是该原子攻击所利用的脆弱点编号，$harm$ 是原子攻击危害指数，反映该次原子攻击成功后给目标主机信息资产造成的损害，p 是原子攻击成功概率，d 是防御该原子攻击的措施。

定义 4(攻击路径) 攻击路径用三元组(*src_host*, *dst_host*, *sequence*)表示，其中 *src_host* 是发起攻击的主机节点标识，*dst_host* 是遭受攻击的主机节点标识，*sequence* 是此次攻击的攻击序列。$sequence=(\perp\rightarrow\tau_1\rightarrow\tau_2\rightarrow\cdots\rightarrow\tau_l\rightarrow\diamondsuit)$。其中，"$\perp$"是该序列的起始标识符，"$\diamondsuit$"是该序列的结束标识符，$\tau_i\in T(1\leqslant i\leqslant l)$是原子攻击，$\tau_i$ 是 τ_{i+1} 的直接前驱，τ_{i+1} 是 τ_i 的直接后继。

定义 5(防御策略) 防御策略用 *defense* 表示。若一条攻击路径对应的攻击序列为 $sequence=(\perp\rightarrow\tau_1\rightarrow\tau_2\rightarrow\cdots\rightarrow\tau_l\rightarrow\diamondsuit)$，其对应的防御策略 $defense=(d_1,d_2,\cdots,d_l)$，其中 d_i 为 τ_i 原子攻击对应的防御措施。

3 网络安全防御策略生成方法

攻击者在实施攻击时会考虑攻击实施的难易程度和攻击危害大小两个因素，防御者在选取防御策略时认识到这一点才能给系统带来最大化的安全保障。本文通过寻找最易攻击路径和攻击危害指数最大的攻击路径来预测攻击者可能采取的攻击措施，进而确定防御者应当采取的防御策略。确定攻击危害指数最大的攻击路径需要计算攻击路径上原子攻击的成功概率，以及成功的原子攻击给目标主机造成的危害。一条攻击路径被成功实施的概率即为该路径上各原子攻击成功概率的乘积，一条攻击路径的攻击危害指数即为该路径上各原子攻击危害指数的和值。

网络安全防御策略生成方法的流程如图 1 所示。

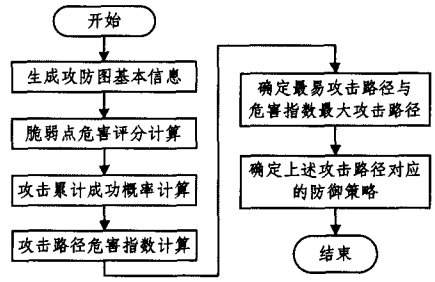

图 1 网络安全防御策略生成流程

攻防图基本信息的生成参考文献[7]，下面主要从脆弱点危害评分方法、攻击累计成功概率计算以及攻击路径危害指数计算 3 个方面对网络安全防御策略生成方法进行介绍。

3.1 脆弱点危害评分方法

近年来，国内外研究者提出了一些漏洞评级和评分系统。根据评价方法的不同，其可以分为定性的评级系统和定量的评分系统。代表性的脆弱点定性评级系统有 Symantec 的安全响应中心威胁严重性评估系统(SRTSAS)以及微软的安全公告严重性评级系统等。脆弱点定量评分系统主要以通用安全脆弱点评估系统 CVSS 为代表，它是目前较为通用的脆弱点评估系统，美国国家漏洞数据库(NVD)就是采用 CVSS 作为其评估标准，目前被普遍采用的版本是 CVSS v2[9]。但是，众多研究人员陆续发现 CVSS 的默认标准并不能产生高多样性分值，不能有效区分各脆弱点实际的危害情况[8,9]。高多样性非常重要，脆弱性本身就具有特征高多样性和影响高多样性的特点。鉴于此，有效的评分方法必须能反映这种复杂性和多样性。高多样性评分系统给脆弱性评级时有明显优势，能最大限度地避免给不同的脆弱性评以相同的分数。

为解决上述问题，Spanos 等人提出了 WIVSS 评分系统[10]。与 CVSS 对脆弱性的基本评分标准相同，WIVSS 的评分标准包括以下 6 项。

(1)*AccessVector*：反映脆弱点被利用的方式。其可能取值为 *Network*，*AdjacentNetwork* 和 *Local*。

(2)*AccessComplexity*：反映攻击者利用脆弱点的攻击复杂程度。其可能取值为：*Low*，*Medium* 和 *High*。

(3)*Authentication*：反映攻击者利用脆弱点所需身份认证次数。其可能取值为：*None*，*Single* 和 *Multiple*。

(4)*ConfImpact*：反映脆弱点被利用后对系统造成的机密性损害。其可能取值为：*Complete*，*Partial* 和 *None*。

(5)*IntegImpact*：反映脆弱点被利用后对系统造成的完整性损害。其可能取值为：*Complete*，*Partial* 和 *None*。

(6)*AvailImpact*：反映脆弱点被利用后对系统造成的可用性损害。其可能取值为：*Complete*，*Partial* 和 *None*。

WIVSS 默认在实际应用中机密性损害(*AvailImpact*)大于完整性损害(*IntegImpact*)，因为机密性损害最难被检测，且该种损害常常要等攻击者发布所窃数据时才会被系统管理员和用户意识到。完整性损害比可用性损害(*AvailImpact*)更严重，因为完整性损害常导致可用性损害同时也更容易被忽视。然而，随着各类 OTT 应用的日益增长，很多攻击的根本目的已经不是窃取数据，而是破坏网络系统的服务性和可用性，因此，有时数据的完整性损害会比较严重，有时数据的可用性损害会比较重要，这取决于信息资产所有者与使用者自身对其的评价。基于此，本文令损害值变量 *ImpactX*，*Im-*

pactY, *ImpactZ* 分别对应 *ConfImpact*, *AvailImpact*, *IntegImpact* 中的一个标准，提出如下规则。

规则 1 *Weight of ImpactX*>*Weight of ImapctY*>*Weight of ImpactZ*。

规则 2 "*None*" *ImpactX*="*None*" *ImpactY*="*None*" *ImpactZ*=0.0。

规则 3 *Partial Impact*=0.5 * *Complete Impact*。

规则 4 *Impact Score* 的范围为 0.0 到 7.0。

规则 5 3 项损害评分标准可能的 3^3 种和值必须不同。

规则 6 *Weight of Complete ImpactY*>*Weight of Partial ImpactX*。

规则 7 *Weight of Complete ImpactZ*>*Weight of Partial ImpactY*。

令评分最后结果保留一位小数，根据规则 3 有 *Complete Impact* 最小的取值为 0.2，此时 *Partial Impact* 取最小值 0.1，否则 *Partial Impact* 的值即小于 0.1，最后得到的评分值可能为两位小数，又因 *Step* 为对 *Complete Impact* 的搜索步长，应为其可取得的最小值，所以 *Step* 的值为 0.2。

根据规则 4 有：

$$W_{ImpactX}+W_{ImpactY}+W_{ImpactZ}=7 \tag{1}$$

另外根据规则 3、规则 6、规则 7 有：

$$2*W_{ImpactZ}>W_{ImpactY} \tag{2}$$

$$2*W_{ImpactY}>W_{ImpactX} \tag{3}$$

根据式(1)－式(3)，消元得式(4)：

$$7*W_{ImpactZ}>7\Rightarrow W_{ImpactZ}>1 \tag{4}$$

又 *Step*=0.2，故 $W_{ImpactZ}$ 的初始值可设为 1.2。

根据规则 1 和搜索步长 *Step* 的值有：

$$W_{ImpactZ}\leqslant W_{ImpactY}-0.2 \tag{5}$$

$$W_{ImpactY}\leqslant W_{ImpactX}-0.2 \tag{6}$$

联立式(1)、式(5)、式(6)可得：

$$3*W_{ImpactZ}\leqslant 7-0.6 \tag{7}$$

根据式(7)有 $W_{ImpactZ}\leqslant 2.13$，又 *Step*=0.2，评分权重值应为 0.2 的倍数，可得 $W_{ImpactZ}\leqslant 2.0$。

上述规则和公式转为如下的最优脆弱性评分权值组合穷举搜索算法，该算法中的各条件由上述规则或公式得到。

```
Start
W_ImpactZ=1.2
Step=0.2
While W_ImpactZ≤2
  W_ImpactY=W_ImpactZ+step
  W_ImpactX=7-(W_ImpactY+W_ImpactZ)
    While W_ImpactY≤W_ImpactX
    If 2 * W_ImpactZ> W_ImpactY AND 2 * W_ImpactY>W_ImpactX
          Compute the 3^3 Possible Sums for this combination of
          Weights
          If the 3^3 Possible Sums have different values Save this
          Combination of Weights
          EndIf
    EndIf
        W_ImpactY=W_ImpactY+Step
        W_ImpactX=W_ImpactX-Step
  EndWhile
  W_ImpactZ=W_ImpactZ+Step
EndWhile
Output of the algorithm the Final Combination of Weights
End
```

算法以 $W_{ImpactZ}$ 为自变量在 1.2 到 2.0 的区间上以 *Step* 为 0.2 的步长遍历。$W_{ImpactX}$ 与 $W_{ImpactY}$ 为因变量。对于符合上述规则和公式的取值组合予以保留，否则舍弃。算法执行后产生了关于 *ImpactX*, *ImpactY*, *ImpactZ* 的 14 个可能的脆弱性权值组合。根据实际情况的不同，可以任选三者与 *ConfImpact*, *AvailImpact*, *IntegImpact* 的对应关系。例如，若当前网络中 *IntegImpact* 最严重，*AvailImpact* 次严重，*ConfImpact* 最不严重，那么可以将 *ImpactX* 的值赋给 *IntegImpact*，将 *ImpactY* 的值赋给 *AvailImpact*，将 *ImpactZ* 的值赋给 *ConfImpact*。在对应关系确定后，可将上述 14 组权值应用于目标网络漏洞集上进行分析，选择产生最多分值的组合作为最终的评分标准。但在下文中，仍将遵循 *ConfImpact* 最严重，*IntegImpact* 次严重，*AvailImpact* 较不严重这一假设进行分析，根据文献[10]，相应的具体权重值会在下一节给出。

3.2 攻击累计成功概率的计算

定义 6(原子攻击成功概率) 原子攻击成功的概率用 p 表示，描述一次安全状态变迁所代表原子攻击成功的可能性。

结合上一节给出的评分系统，本文基于脆弱点利用难易程度 *Exploitability* 的修正值来表示原子攻击成功概率。其计算公式为：

$$\begin{aligned} p&=Exploitability\\ &=2*AccessVector*AccessComplexity*Authentication \end{aligned} \tag{8}$$

根据 3.1 节中评分搜索算法得到的结果，相应量化值如下。

$$AccessVector=\begin{cases}0.395, & Local\\ 0.646, & Adjacent\ Network\\ 1, & Network\end{cases}$$

$$AccessComplexity=\begin{cases}0.35, & High\\ 0.61, & Medium\\ 0.71, & Low\end{cases}$$

$$Authentication=\begin{cases}0.45, & Multiple\\ 0.56, & Single\\ 0.704, & None\end{cases}$$

参考文献[11]，给出状态攻防图中原子攻击的攻击累计成功概率的定义。

定义 7(攻击累计成功概率) 攻击累计成功概率用 P 表示，反映一条攻击路径上进行原子攻击时攻击成功的概率累计值。对于一条完整的攻击路径($\tau_1,\tau_2,\perp\rightarrow\tau_1\rightarrow\tau_2\rightarrow\cdots\rightarrow\tau_l\rightarrow\diamond$)，若 $\tau_k\in\{\tau_1,\tau_2,\cdots,\tau_l\}$ 有：

$$P(\tau_k)=\begin{cases}p_k\prod_{i=1}^{k-1}p_i, & k>1\\ p_1, & k=1\end{cases} \tag{9}$$

3.3 攻击路径危害指数的计算

定义 8(主机信息资产值) 主机信息资产值用 R 表示，代表主机上信息资产的价值 $R=r(C)+r(I)+r(A)$，其中，$r(C)$ 代表主机信息资产在机密性方面的价值，$r(I)$ 代表主机信息资产在完整性方面的价值，$r(A)$ 代表主机信息资产在可用性方面的价值，三者的取值范围均为 0 到 100。

根据定义 3，原子攻击危害指数用 *harm* 表示。结合 3.1

节评分系统得出的漏洞危害标准权重值，计算公式如下：

$$harm=(ConfImpact*r(C)+IntegImpact*r(I)+AvailImpact*r(A))*P \tag{10}$$

其中，P 为攻击累计成功概率。

根据上一节中评分搜索算法得到的结果，相应量化值如下 。

$$ConfImpact=\begin{cases}0.0, & None\\ 1.8, & Partial\\ 3.6, & Complete\end{cases}$$

$$IntegImpact=\begin{cases}0.0, & None\\ 1.1, & Partial\\ 2.2, & Complete\end{cases}$$

$$AvailImpact=\begin{cases}0.0, & None\\ 0.6, & Partial\\ 1.2, & Complete\end{cases}$$

定义 9(攻击路径危害指数) 攻击路径损害用 $Harm$ 表示，设一条攻击路径为$\{\tau_1,\tau_2,\cdots,\tau_n\}$，则：

$$Harm=\sum_{\tau_i\in\{\tau_1,\tau_2,\cdots,\tau_n\}}^{n}harm_i \tag{11}$$

其中，$harm_i$ 代表本条攻击路径上某单个原子攻击造成的损害，即该原子攻击的原子攻击危害指数。

根据式(9)可以找出攻击成功概率最大的路径，而根据式(11)可找出攻击危害指数最大的攻击路径，两条路径对应的防御策略即为两种情况下所求防御策略。

4 算例分析

为验证本文方法的有效性，设计如图 2 所示的网络拓扑来说明本文方法的具体应用过程。如图 2 所示的网络中，有一台公共 Web 服务器(server1)、一台 FTP 服务器(server2)、一台数据库服务器(server3)和一台邮件服务器(server4)。防火墙的设置保证能让外部用户直接访问的服务器仅有 Web 服务器(server1)，对其他服务器的访问都会被阻止。攻击者 Attacker 在其攻击主机节点上有 Root 权限，从此处发起攻击，通过 Internet 依次获取内网里其他主机节点的访问权限。

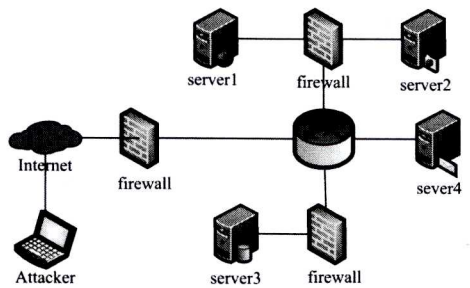

图 2 网络拓扑结构图

利用 Nessus[12] 脆弱点扫描器扫描网络中所有主机节点的脆弱点分布如表 1 所列，假设各主机中的信息资产价值构成如表 2 所列。从表 2 可以看出，Web 服务器的信息资产价值较其余服务器较低，其并不存储关键数据；FTP 服务器的价值较 Web 服务器略高，因为其存储了一些公开的数据资源，需要保证一定的数据完整性；数据库服务器的价值最高，其存储了不容丢失的数据资源，且对完整性和可用性要求很高；邮件服务器涉及通信，所以拥有较高的机密性价值。

表 1 脆弱点分布

主机名	脆弱点
server1	CVE-2015-1635
server2	CVE-2007-2318
server3	CVE-2008-5416,CVE-2011-1878
server4	CVE-2007-3791

表 2 主机信息资产价值构成

主机名	机密性价值	完整性价值	可用性价值
server1	30	30	60
server2	30	60	70
server3	60	90	80
server4	70	40	30

根据上述信息，利用前两节中的公式和规则对图 2 所示的网络拓扑进行分析，生成如图 3 所示的状态攻防图。

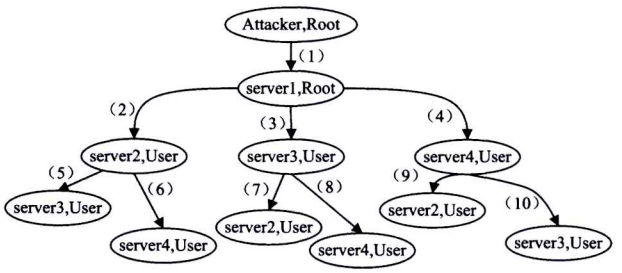

图 3 状态攻防图

(1)CVE-2015-1635，245.92128，0.99968，执行 Windows 更新 3042553。

(2)CVE-2007-2318，278.18964，0.85888，升级 FileZilla。

(3)CVE-2008-5416，405.42450，0.79520，执行 Windows 数据库更新 59420。

(4)CVE-2007-3791，187.87968，0.99968，升级至 Debian GNU/Linux 4.0 alias etch。

(5)CVE-2008-5416，348.21270，0.79520，执行 Windows 数据库更新 59420。

(6)CVE-2007-3791，161.36792，0.99968，升级至 Debian GNU/Linux 4.0 alias etch。

(7)CVE-2007-2318，221.21748，0.85888，升级 FileZilla。

(8)CVE-2007-3791，149.40360，0.99968，升级至 Debian GNU/Linux 4.0 alias etch。

(9)CVE-2007-2318，278.09892，0.85888，升级 FileZilla。

(10) CVE-2008-5416，405.29190，0.79520，执行 Windows 数据库更新 59420。

从图 3 可以看出，攻击者可采取的各条攻击路径及防御者可采取的防御策略如表 3 所列。以 server2 为例，如果考虑攻击易行性，攻击者可以采取路径 1-2 进行攻击。而防御者应优先在 server1 上执行 Windows 更新 3042553，并升级 server2 上的 FileZilla。如果考虑攻击损害最大化，那么攻击者可以采取路径 1-3-7。防御者应优先在 server1 上执行 Windows 更新 3042553，在 server3 上执行 Windows 数据库更新 59420，并升级 server2 上的 FileZilla，说明本文改进后的方法是切实有效的。类似地，server3 的最易攻击路径为 1-3，损害最大攻击路径为 1-2-5；server4 的最易攻击路径为 1-4，损害最大攻击路径为 1-3-8。另外，从上述结果可以发现，攻击路径越深意味着损害越大，而攻击路径越浅意味着攻击成功的概率越大，这一点应引起网络管理人员的注意。

表 4 反映了部分原子攻击危害指数和成功概率相关的信息。其中，原子攻击危害指数(不考虑概率因素)是指 *Conf-*

$Impact * r(C) + IntegImpact * r(I) + AvailImpact * r(A)$，是利用式(10)计算原子攻击危害指数时的中间值，故不再独立定义。以原子攻击编号 1,2 为例，它们所利用的脆弱点具有相同的机密性损害、完整性损害与可用性损害评分，但因为目标主机信息资产值的不同，其产生的原子攻击危害就不同，说明引入主机信息资产值是有必要的。以原子攻击 3,5 为例，二者利用的脆弱点相同，它们具有完全相同的原子攻击危害指数(不考虑概率因素)，但是引入攻击累计成功概率后，其所对应的原子攻击危害指数产生了差别。其中原子攻击 3 的原子攻击危害指数为 405.42450，原子攻击 5 的原子攻击危害指数为 348.21270，这是因为原子攻击 3 的攻击累计成功概率大于原子攻击 5 的攻击累计成功概率。通过上文的分析可知，引入攻击累计成功概率而不是如文献[7]中将原子攻击自身的成功概率作为攻击危害指数的计算参数是必要的，这里的差别成功验证了这一点。

以 server4 为例，采用文献[6]与文献[7]中的方法对其攻击路径和防御策略进行分析，如表 5 所列。对比表 5 和表 3 可知，用文献[6]或文献[7]中的方法时，server4 攻击损害最大路径均为 1-2-6。用本文计算方法，则路径 1-2-6 的攻击路径危害指数为 685.47884，小于路径 1-3-8 的攻击路径危害指数 800.74938，1-3-8 成为新的攻击损害最大路径。说明本文引入的评估因素如主机信息资产值等概念在攻击路径和防御策略的确定中起到了实际作用，若采用文献[6]或文献[7]中的路径对应的防御策略，将不能针对攻击危害最大的攻击路径进行防御。

与文献[6]相比，本文脆弱性评分方法更为客观且具有良好的多样性，同时可以根据给定的目标主机制定防御策略，综合考虑了攻击成功概率与攻击危害两个因素。与文献[7]的方法相比，本文漏洞评分算法具有更好的多样性，考虑了主机信息资产价值且通过分别计算各种危害提高了攻击路径判定的准确性。本文方法与文献[6,7]中方法的对比结果如表 6 所列。

表 3　攻击路径与防御策略

攻击目标	攻击路径	攻击序列	获取权限	成功概率	攻击路径危害指数	最易攻击路径防御策略	攻击损害最大路径防御策略
server1	1	1	Root	0.99968	245.92128	执行 Windows 更新 3042553	执行 Windows 更新 3042553
server2	1	1-2	User	0.85861	524.11092	执行 Windows 更新 3042553，升级 FileZilla	执行 Windows 更新 3042553，执行 Windows 数据库更新 59420，升级 FileZilla
	2	1-3-7	User	0.68277	872.56326		
	3	1-4-9	User	0.85833	711.89988		
server3	1	1-2-5	User	0.68277	872.32362	执行 Windows 更新 3042553，执行 Windows 数据库更新 59420	执行 Windows 更新 3042553，升级 FileZilla，执行 Windows 数据库更新 59420
	2	1-3	User	0.79495	651.34578		
	3	1-4-10	User	0.79469	839.09286		
server4	1	1-2-6	User	0.85834	685.47884	执行 Windows 更新 3042553，升级至 Debian GNU/Linux 4.0	执行 Windows 更新 3042553，执行 Windows 数据库更新 59420，升级至 Debian GNU/Linux 4.0
	2	1-3-8	User	0.79470	800.74938		
	3	1-4	User	0.99936	433.80096		

表 4　原子攻击危害指数及成功概率相关信息

原子攻击编号	利用脆弱点编号	脆弱点机密性危害	脆弱点完整性危害	脆弱点可用性危害	原子攻击危害指数(不考虑概率因素)	原子攻击成功概率	攻击累计成功概率	原子攻击危害指数
1	CVE-2015-1635	3.6	2.2	1.2	246	0.99968	0.99968	245.92128
2	CVE-2007-2318	3.6	2.2	1.2	324	0.85888	0.85861	278.18964
3	CVE-2008-5416	3.6	2.2	1.2	510	0.79520	0.79495	405.42450
5	CVE-2008-5416	3.6	2.2	1.2	510	0.79520	0.68277	348.21270

表 5　文献[6]与文献[7]方法下 server4 的攻击路径和防御策略分析

文献	攻击目标	攻击路径	攻击序列	获取权限	成功概率	攻击路径危害指数	最易攻击路径防御策略	攻击危害最大路径防御策略
文献[6]	server4	1	1-2-6	User	0.0016	1.6904	执行 Windows 更新 3042553，升级至 Debian GNU/Linux 4.0	执行 Windows 更新 3042553，升级 FileZilla，升级至 Debian GNU/Linux 4.0
		2	1-3-8	User	0.0003	1.2769		
		3	1-4	User	0.032	1.3296		
文献[7]	server4	1	1-2-6	User	0.85833	25.02809	执行 Windows 更新 3042553，升级至 Debian GNU/Linux 4.0	执行 Windows 更新 3042553，升级 FileZilla，升级至 Debian GNU/Linux 4.0
		2	1-3-8	User	0.79469	24.39123		
		3	1-4	User	0.99936	16.43856		

表 6　各文献防御策略生成方法对比

文献	脆弱性危害评分方法	主机信息资产值	危害细分	攻击成功概率计算方式	对确定的目标主机给出防御策略	是否综合考虑攻击成功概率与攻击危害
文献[6]	主观，较差多样性	考虑	有细分	主观，不精确	不能	否
文献[7]	客观，一般多样性	未考虑	无细分	客观，不精确	可以	是
本文	客观，良好多样性	考虑	有细分	客观，精确	可以	是

结束语　本文分析了现有基于状态攻防图的网络安全防御策略生成方法的不足，在其基础上改进脆弱点危害评分标准，引入攻击累计成功概率及主机信息资产值的概念，重新定义原子攻击危害指数的计算方式与攻击路径危害指数的计算方式，对安全策略生成所需考虑的因素进行扩充，对安全策略的生成方法进行优化。最后，通过算例分析验证了本文所提方法的有效性。

参 考 文 献

[1] Yigit B, Gur G, Alagoz F. Cost-Aware Network Hardening with Limited Budget Using Compact Attack Graphs[C]//2014 IEEE Military Communications Conference (MILCOM). IEEE, 2014: 152-157

(下转第 149 页)

精度的取值都不理想。ROC曲线下的面积AUC的值越接近1,表明分类器的分类效果越好。从图3可以看出,8维属性集的AUC值最高。综合考虑训练时间和检测时间,选取8维属性集作为分类器的属性集取得了较好的分类效果。

结束语 特征选择问题是欺诈检测的核心问题之一,而有效的特征提取对于提高欺诈检测的检测率、降低欺诈检测的误报率、提高欺诈检测的实时性有着重要影响。文中提出的检测方法首先对用户点击广告的日志数据特征利用Fisher分度量其特征重要性,然后选择相对重要的属性利用SVM二分类方法对用户最终分类。文中基于用户行为的欺诈点击检测算法经过了真实数据集训练,实验证明,通过去除冗余的特征属性,采用最能反映欺诈用户行为的重要特征进行检测欺诈,分类器的精度与未去除冗余特征所构建的分类器精度相当,但是训练和测试时间有所降低,且能够保证在精度基本不改变的情况下,更快速和有效地检测欺诈用户。

参 考 文 献

[1] Chen Shi-guo, Zhang Dao-qiang. Experimental Comparisons of Semi-Supervised Dimensional Reduction Methods[J]. Journal of Software, 2011, 22(1): 28-43(in Chinese)
陈诗国,张道强. 半监督降维方法的实验比较[J]. 软件学报, 2011, 22(1): 28-43

[2] Haddadi H. Fighting online click-fraud using bluff ads[J]. ACM SIGCOMM Computer Communication Review, 2010, 40(2): 21-25

[3] Tuzhilin A. The Lane's Gifts v. Google Report[EB/OL]. 2006 [2013-03-01]. http://googleblog. blogspot. com/pdf/Tuzh-ilin-Report. pdf

[4] Qin Chao. Visitor action analyzing system for electronic business website[D]. Shanghai: Shanghai Jiao Tong University, 2006(in Chinese)
秦超. 电子商务网站访客行为分析系统[D]. 上海:上海交通大学, 2006

[5] Perera K S, Neupane B, Faisal M A, et al. A Novel Ensemble Learning-Based Approach for Click Fraud Detection in Mobile Advertising[M]// Mining Intelligence and Knowledge Exploration. Springer International Publishing, 2013: 370-382

[6] Immorlica N, Jain K, Mahdian M, et al. Click Fraud Resistant Methods for Learning Click-Through Rates[C]// Proceedings of the Workshop on Internet and Network Economics. Berlin Heidelberg: Springer, 2005: 34-45

[7] Oentaryo R, Lim E P, Finegold M, et al. Detecting Click Fraud in Online Advertising: A Data Mining Approach[J]. Journal of Machine Learning Research, 2014, 14(1): 99-140

[8] Hager M, Landergren T. Implementing best practices for fraud detection on an online advertising platform [D]. Gothenburg: Chalmers University of Technology, 2010

[9] Sergios T, Konstantinos K. Pattern recognition(2nd ed)[M]. Salt Lake City: Elsevier Academic Press, 1999

[10] Chang C C, Lin C J. LIBSVM: A library for support vector machines[C] // ACM Transactions on Intelligent Systems and Technology. 2011: 389-396

[11] Ravisankar P, Ravi V, Raghava Rao G, et al. Detection of financial statement fraud and feature selection using data mining techniques[J]. Decision Support Systems, 2011, 50(2): 491-500

[12] Cortes C, Vapnik V. Support vector networks [J]. Machine Learning, 1995, 20(3): 273-297

[13] Zhang Yi-rong, Xian Ming, Xiao Shun-ping, et al. An Anomaly Intrusion Detection Technique of Support Vector Machine Based on Rough Set Attribute Reduction[J]. Computer Science, 2006, 33(6): 64-68(in Chinese)
张义荣,鲜明,肖顺平,等. 一种基于粗糙集属性约简的支持向量异常入侵检测方法[J]. 计算机科学, 2006, 33(6): 64-68

[14] Chang C C, Lin C J. LIBSVM: a library for support vector machines[J]. ACM Transactions on Intelligent & Technology, 2011, 2(3): 389-396

(上接第134页)

[2] Dantu R, Loper K, Kolan P. Risk management using behavior based attack graphs[C]// International Conference on Information Technology: Coding and Computing(ITCC 2004). Las Vegas: IEEE, 2004: 445-449

[3] Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1): 61-74

[4] Albanese M, Jajodia S, Noel S. Time-efficient and cost-effective network hardening using attack graphs[C]// 2012 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2012: 1-12

[5] Wang S, Zhang Z, Kadobayashi Y. Exploring attack graph for cost-benefit security hardening: A probabilistic approach[J]. Computers & Security, 2013, 32: 158-169

[6] Luo Zhi-yong, Sun Guang-lu, Liu Jia-hui, et al. Application of attack graphs algorithms in intrution prevention system[J]. Journal of Yunnan University, 2012, 34(3): 271-275(in Chinese)
罗智勇,孙广路,刘嘉辉,等. 攻击图算法在入侵防御系统中的应用[J]. 云南大学学报(自然科学版), 2012, 34(3): 271-275

[7] Liu Gang, Li Qian-mu, Zhang Hong. Defense strategy generation method for network security based on state attack-defense graph [J]. Journal of Computer Applications, 2013, 33(S1): 121-125 (in Chinese)
刘刚,李千目,张宏. 基于状态攻防图模型的网络安全防御策略生成方法[J]. 计算机应用, 2013, 33(S1): 121-125

[8] Mell P, Scarfone K. Improving the common vulnerability scoring system[J]. IET Information Security, 2007, 1(3): 119-127

[9] Wang Yu-long, Yi Yang. PVL: A Novel Metric for Single Vulnerability Rating and Its Application in IMS[J]. Journal of Computational Information Systems, 2012, 8(2): 579-590

[10] Spanos G, Angelis L. Impact Metrics of Security Vulnerabilities: Analysis and Weighing [J]. Information Security Journal A Global Perspective, 2015, 24(1-3): 1-15

[11] Ye Yun, Xu Xi-shan, Jia Yan, et al. An Attack Graph Based Probabilistics Computing Approach of Network Security[J]. Chinese Journal of Computers, 2010, 33(10): 1987-1996(in Chinese)
叶云,徐锡山,贾焰,等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报, 2010, 33(10): 1987-1996

[12] Li Qing-peng, Wang Bu-hong, Wang Xiao-dong, et al. Network security assessment based on probabilities of attack graph nodes [J]. Application Research of Computers, 2013, 30(3): 906-908 (in Chinese)
李庆朋,王布宏,王晓东,等. 基于攻击图节点概率的网络安全度量方法[J]. 计算机应用研究, 2013, 30(3): 906-908