一种面向任务的网络风险评估模型

孙 奥，殷肖川，李小青
（空军工程大学信息与导航学院，西安，710077）

摘要 针对网络业务安全风险评估问题，提出了一种基于STRIDE威胁建模和隐式马尔科夫模型理论的STRIDE-HMM风险评测方法，该方法以网络业务为切入点，给出了任务描述模型、任务资产模型、任务风险评估模型的构建方法及其联系。任务描述模型给出了任务阶段划分及相应的资产集、漏洞集和威胁集；任务资产模型给出了任务各阶段所依赖的资产集合，在此基础上采用隐式马尔科夫模型方法给出了资产安全状态量化计算方法；任务风险评估模型按照资产分类集合的结果，采用聚合分析方法给出了任务风险值计算方法，进而实现面向网络业务的风险评测。为了验证提出方法的有效性，采用TMT威胁建模工具典型web应用给出的资产、漏洞、威胁示例，利用提出的模型和方法对该示例进行了仿真验证，实验结果表明：该方法可为面向任务的安全计划制定和调度提供决策支持。

关键词 面向任务；风险评估；威胁建模；风险预测
DOI 10.3969/j.issn.1009-3516.2019.05.017
中图分类号 TP393.08 **文献标志码** A **文章编号** 1009-3516(2019)05-105-06

A Network Risk Assessment Model Geared to the Needs of Tasks

SUN Ao, YIN Xiaochuan, LI Xiaoqing
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract: In view of network business security risk assessment problems, a STRIDE-HMM network risk assessment and prediction method based on STRIDE threat modeling and HMM theory is proposed. Taking the network service as an entry point, the construction method of the task description model, the task asset model and the task risk assessment model and the relationship are given among them. The task description model gives the task phase partitioning and corresponding asset sets, vulnerability sets, and threat sets; The task asset model gives a set of assets depended on each stage of the task. On the basis of this, HMM is used to give the quantitative calculation method of asset security status. The task risk assessment model realizes the risk assessment for network business by using aggregation analysis method to achieve the task risk value calculation method according to the results of the asset classification set. To verify the effectiveness of the proposed method, a typical web application example of assets, vulnerabilities and threats combined with threat modeling tool TMT is given. The result proves that the proposed method can provide decision support for the security planning and scheduling oriented to the needs of tasks.

Key words: task-oriented; risk assessment; threat modeling; risk prediction

收稿日期：2019-05-09
基金项目：国家自然科学基金(71503260)
作者简介：孙 奥(1996—)，女，内蒙古通辽人，硕士生，主要从事网络空间安全研究。E-mail:AFsunao@163.com

引用格式：*孙奥，殷肖川，李小青. 一种面向任务的网络风险评估模型[J]. 空军工程大学学报(自然科学版)，2019，20(5)：105-110. SUN Ao，YIN Xiaochuan，LI Xiaoqing. A Network Risk Assess ment Model Geared to the Needs of Tasks[J]. Journal of Air Force Engineering University (Natural Science Edition)，2019，20(5)：105-110.*

目前,针对复杂网络进行态势评估预测和安全防护十分困难,传统的静态被动防护已不能适应当前的安全形势,动态的主动防御是当今网络安全防护的趋势[1-3]。针对态势预测,本文将任务与资产、风险相关联,针对面向任务的网络风险评估进行了关键技术理论研究,并提出了一种风险预测模型。该模型将网络的风险等级定义为任务推进过程中需要调用的各资产风险的组合结果,分别对任务、资产及威胁进行建模分析,得到动态风险评估预测结果,为管理员制定安全计划提供支持。

1 相关技术分析

1.1 风险评估方法研究现状

目前,国内外有很多网络风险评估的模型和方法。文献[4]中应用了 ANP 网络层次分析法,其广泛应用于风险评价指标的权重计算。ANP 可以弥补 AHP 等其他主观赋权方法不能考虑各指标之间的相关性而忽略各因素之间相互作用的缺陷。然而,在 ANP 方法中,专家决策容易出现不一致和判断矩阵数据库缺失等问题,只反映了各因素之间关系判断比的直接影响。相对而言,专家很难对间接因素之间的关系做出比较判断。文献[5]应用灰色理论评估方法,基于灰度的白化权重函数生成,根据某一类灰度描述的类别对具体数据进行分类,判断统计指标的灰度等级。灰色理论具有样本要求小、不需要固定分布、计算量小、定量与定性分析结果一致等优点。然而,灰色理论主要适合解决的是样本小、信息建模能力差的问题,而针对有较大规模和可变因素的系统建模灵活性稍差。文献[6]首次提出了隐式马尔科夫模型在网络安全中的使用,隐式马尔科夫模型可以用来建模包含隐含参数的马尔科夫过程,并根据隐含的内部状态进行相关的其他分析。该模型的一个主要特征是可以建模观察中的假阳性和假阴性,排除误差观测信息给评估结果带来的影响。

现阶段网络安全多以网络总体为中心进行研究[7-10],结合具体任务对象的研究较少,与传统的风险评估量化方法相比,本文提出的模型以任务目标为核心,排除与任务无关的资产、漏洞、威胁的影响,减少无关威胁及漏洞对评估结果的误导,更加贴近客观实际。

1.2 威胁建模基本理论

威胁建模通过对目标漏洞的识别来进行系统安全优化,定义防范方法或缓解系统威胁对策的过程。威胁建模是用来研究系统可用性的一种结构化方法。能够识别、量化和解决应用程序中相关的安全风险,是对安全代码审查过程的补充,能够使其更加的完善。威胁建模过程包括攻击面识别和威胁枚举,识别过程可应用 UML(Unified Modeling Language,UML)工具来进行。STRIDE 方法是一种典型的威胁枚举方法,可将全部威胁分成 6 类进行遍历,完成识别[11]。在系统生命周期中进行威胁建模可以确保开发者从一开始就以内置的安全性来开发应用程序。这与作为威胁建模过程中一部分的文档相结合,可以使开发者更好地理解系统[12]。这也使得审阅者可以看到应用程序中的每个节点的威胁。

现代威胁建模者大多从攻击者的角度来看待系统,而不是站在被攻击者的立场。当在系统生命周期之外执行源代码分析时(例如现有的应用程序上),威胁建模的结果通过推广宽度优先与深度优先来帮助降低源代码分析的复杂性,可以不用等重点地关注所有源代码,而是将安全代码评估放在优先级上,这些组件的威胁建模已经属于高风险威胁。

1.3 风险理论

网络风险评估的原理见图 1。

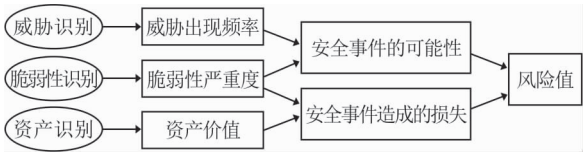


图 1 网络风险评估原理

风险可以由风险事件发生的可能性及其后果来进行定性或定量的衡量[13]。风险是指某些特定的威胁利用资产的漏洞,对其造成负面影响的潜在可能性,是该威胁发生的可能性与其影响后果综合作用的结果;资产是指被所有者保护的有价值的信息或资源,如硬软件平台、数据、信息等;威胁是指资产中可被威胁、利用的弱点,也可称之为漏洞。

2 任务资产分析

确保任务的可靠运行是网络安全的重要目标,本文以任务为切入点,通过分析任务各阶段所依托的资产及其安全性,进而实现对任务风险的预测。任务资产分析主要研究任务与资产、资产与漏洞、漏洞和威胁间的关系。

任务是将被监测网络各项资产集中起来并加以利用的基本目标[14]。一旦当前阶段任务的风险值超出一定范围就需要由安全管理员进行安全策略调整,故任务的完成依托于各项资产间的交互关联,任务推进过程中某一阶段所涉及资产带来的威胁可能会影响下一阶段任务的进行,进而导致整个任务进程的瘫痪[15]。任务目标的关键性同时也决定了资产的重要性。在任务模型中,需要评价每一项资产在完成特定任务时的重要性,故任务模型由以下 3

部分定义[16]：①对任务完成最关键的数据、硬件、软件和服务等资产；②资产自身的漏洞信息；③管理员最关心的入侵事件类别。该过程需要对任务的动态情况进行掌握，即对每个阶段调用资产的风险状态进行实时评估。

将任务记为 $M=\{M_1,M_2,\cdots,M_n\}$，$M_i\in M$，表示保证任务能够成功完成的各个阶段，每个任务阶段下面是该阶段调用的资产子集 $A_i\in A$，该资产子集对应一个漏洞集 V_i 和威胁集 T_i，该阶段任务模型可表示为 $M_i=(A_i,V_i,T_i)$。其中，任务阶段 M_i 与资产 A_i 是一对多的映射关系，资产 A_i 与漏洞 V_i 是一对多的映射关系，漏洞 V_i 与威胁 T_i 是多对多的映射关系。

3　资产模型构建

资产的安全是任务安全的基础，任务资产会随着任务的推进而变化，因此需要研究构建资产模型进行资产描述和安全状态评估。

3.1　资产模型分析

任务的风险状态可以通过对应资产的风险状态聚合得到[17]，所以本文将网络的风险视为任务推进阶段中涉及到的每个资产风险的组合，并使用隐式马尔科夫模型来表示安全状态之间转移的可能性。

由于网络的风险安全状态难以直接观测得到，根据该特点可以应用隐式马尔可夫模型对资产建模。每个资产的隐式马尔科夫模型[18]可以表示为 $\lambda=(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{\pi})$，包括一个状态转移概率矩阵 $\boldsymbol{P}$，一个观测概率矩阵 $\boldsymbol{Q}$ 和一个初始状态分布向量 $\boldsymbol{\pi}$。

假定每个资产 a 有 N 种不同的安全状态：

$$S=\{s_1,s_2,\cdots,s_N\} \tag{1}$$

每项资产的安全状态随时间变化，资产的状态序列表示为：

$$X=x_1,x_2,\cdots,x_t,x_t\in S \tag{2}$$

每个资产都被防火墙、入侵检测系统等多个传感器监视，$K_k^a,(k=1,2,\cdots,L)$是监控资产 a 的 L 个传感器。每个传感器生成的观测信息组成观测信号集 $V^k=\{v_1^k,v_2^k,\cdots,v_M^k\}$，其中 M 是传感器 k 生成的信息条数。观测信息序列表示为：

$$Y=y_1,y_2,\cdots,y_t,y_t\in V \tag{3}$$

式中：Y 表示 t 时刻接收到的观测信息。

状态转换概率矩阵 $\boldsymbol{P}$ 表示各安全状态间转换的概率。每个元素 p_{ij} 代表模型在 t 时刻处于状态 s_i 的情况下向 $t+1$ 时刻状态 s_j 的转移概率：

$$p_{ij}=\boldsymbol{P}(x_{t+1}=s_j\mid x_t=s_i),1\leqslant i,j\leqslant N \tag{4}$$

观测概率矩阵 $\boldsymbol{Q}$ 表示资产在某一特定状态下接收到不同观测结果的概率，即观测信息与安全状态的概率关系。每个元素 $q_n(m)$表示在 t 时刻资产处于状态 s_n 时接收到观测信号 v_m^k 的概率：

$$q_n(m)=\boldsymbol{P}(y_t^k=v_m^k\mid x_t=s_n),1\leqslant n\leqslant N,1\leqslant k\leqslant K,1\leqslant m\leqslant M \tag{5}$$

初始时刻资产处于各个安全状态的概率分布记为 $\boldsymbol{\pi}=\{\pi_i\}$。其中 $\pi_i=\boldsymbol{P}(x_1=s_i)$，即资产的初始状态为 s_i 的概率。

每项资产的隐式马尔科夫模型示意图见图 2。

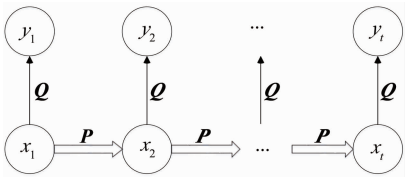


图 2　隐式马尔科夫模型示意图

图中 $x_1,x_2,\cdots,x_t$ 表示在各时刻资产的状态，且它们均属于集合 S，且 x 间的关系由 $\boldsymbol{P}$ 体现；$y_1,y_2,\cdots,y_t$ 表示在各时刻资产的观测信息，且它们均属于集合 V，y_t 仅与 x_t 有关，由 $\boldsymbol{Q}$ 体现。

3.2　资产状态及转换

在任务推进过程中，资产的安全状态也在变化，为了能够对资产进行动态风险评估，资产的状态概率 $\gamma_t=\{\gamma_t(i)\}$必须进行动态地更新。给定一个观察数据 y_t 和资产的隐式马尔科夫模型 λ 就可以使用前向算法来更新该资产的状态概率 γ_t，该算法的复杂度为 $O(N^2)$，算法如下：

已知资产的初始观测信息 y_1 和隐式马尔科夫模型 λ，初始状态分布 $\gamma_1(i)$可以通过式(6)得到：

$$\gamma_1(i)=\boldsymbol{P}(x_1=s_i\mid y_1,\lambda)=\frac{\boldsymbol{P}(y_1,x_1=s_i\mid\lambda)}{\boldsymbol{P}(y_1\mid\lambda)}=\frac{\boldsymbol{P}(y_1\mid x_1=s_i,\lambda)\boldsymbol{P}(x_1=s_i\mid\lambda)}{\boldsymbol{P}(y_1\mid\lambda)} \tag{6}$$

分母的计算可以通过对初次观测到的状态进行条件化，然后对所有可能的状态进行求和得到：

$$\boldsymbol{P}(y_1\mid\lambda)=\sum_{j=1}^{N}\boldsymbol{P}(y_1\mid x_1=s_j,\lambda)\boldsymbol{P}(x_1=s_j\mid\lambda)=\sum_{j=1}^{N}q_j(y_1)\pi_j \tag{7}$$

整合式(6)、(7)可得 $\gamma_1(i)$的最终表达式为：

$$\gamma_1(i)=\frac{q_i(y_1)\pi_i}{\sum_{j=1}^{N}q_j(y_1)\pi_j} \tag{8}$$

式中：$q_j(y_1)$是资产在状态 s_j 下观测信息为 y_1 的概率；π 是初始状态概率。为了简化状态分布计算，在接收 t 个观测信息后，定义一个前向变量：

$$\alpha_t(i)=\boldsymbol{P}(y_1y_2\cdots y_t,x_t=s_i\mid\lambda) \tag{9}$$

通过递归可得该变量也可以通过式(10)计算得到：

$$\alpha_t(i)=q_i(y_t)\sum_{j=1}^{N}\alpha_{t-1}(j)p_{ij},t>1 \tag{10}$$

推导 $\alpha_t(i)$时可以根据马尔科夫性质假设 y_t 只

取决于 x_t,通过式(6)、式(8)可得:

$$\gamma_1(i)=\frac{q_i(y_1)\pi_i}{\sum_{j=1}^{N}q_j(y_1)\pi_j} \tag{11}$$

因为本文研究的重点是计算多次观测之后的资产状态分布,所以在计算的处理上不考虑 t 时刻之后发生的观测结果。

因此利用前向变量 $\alpha_t(i)$ 和新的观测信息可以通过式(12)对任务阶段中涉及的资产的状态概率分布进行更新:

$$\begin{cases}\gamma_t(i)=\boldsymbol{P}(x_t=s_i\mid y_1y_2\cdots y_t,\lambda)=\\ \dfrac{\boldsymbol{P}(y_1y_2\cdots y_t,x_t=s_j\mid\lambda)}{\boldsymbol{P}(y_1y_2\cdots y_t\mid\lambda)}=\\ \dfrac{\boldsymbol{P}(y_1y_2\cdots y_t,x_t=s_i\mid\lambda)}{\sum_{j=1}^{N}\boldsymbol{P}(y_1y_2\cdots y_t,x_t=s_j\mid\lambda)}=\dfrac{\alpha_t(i)}{\sum_{j=1}^{N}\alpha_t(j)}\end{cases} \tag{12}$$

本文研究的重点是风险预测,即风险水平的表达,该资产模型旨在作为风险预测的工具。文中提出的隐式马尔科夫模型允许风险逐渐降低,即使涉及到的资产已被评为高危状态,如果风险值结果表明安全等级较之前水平高,那么资产的风险水平也会降低。这样做是为了避免越来越多的资产被评为高风险水平而导致整个任务的瘫痪。

4 风险预测模型

风险预测模型需要解决任务不同阶段的安全评估及安全预测问题,通过构建任务与资产及其漏洞和威胁的关联关系进而计算预测值,为任务风险进行预测。

4.1 模型要素分析

任务随时间推进分为不同阶段,每个阶段任务的依赖特定的资产集合,即每个阶段对应一个资产子集,而每一项资产本身都可能存在若干可被利用的安全漏洞[19],这些漏洞是导致任务风险的潜在威胁。风险预测模型的构成要素见图 3。

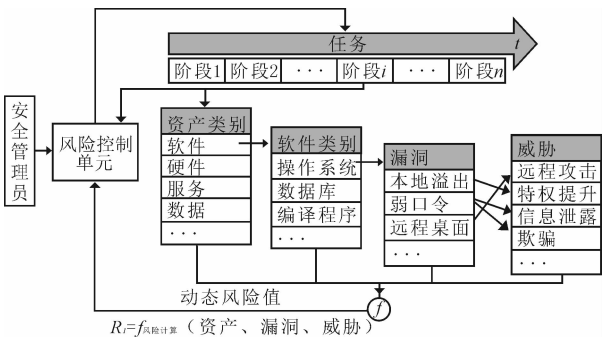


图 3 面向任务的网络安全风险的构成要素

根据当前时刻任务阶段调用的资产和资产具有的漏洞以及来自不同威胁源的威胁,可以生成该任务阶段情况下的动态风险值。在风险控制单元中,安全管理员结合任务需求,应用当前状态下该任务阶段的风险值制定相应的安全决策,减少风险对任务推进的影响,保障任务的顺利进行。

4.2 模型构建

任务的风险预测需要将任务模型与资产模型进行关联,通过资产的安全状态可以预测任务的风险。为了得到量化的资产状态风险值,需要用映射:$\boldsymbol{C}:S\rightarrow R$ 描述每个资产的预期代价。假设一个资产的每种状态对应一个代价向量 $\boldsymbol{C}$ 表示该安全状态下的潜在后果,则 t 时刻资产 a 的总风险 $R_{a,t}$ 表示为:

$$R_{a,t}=\sum_{i=1}^{N}\gamma_t(i)\boldsymbol{C}(i) \tag{13}$$

式中:$\gamma_t(i)$ 是资产在 t 时刻处于状态 s_i 的概率;N 是安全状态的总数;$\boldsymbol{C}(i)$ 是状态 s_i 下的代价值。不同资产在任务阶段中的代价向量 $\boldsymbol{C}$ 和影响因子 δ,$\left(\sum_{i=1}^{N}\delta_i=1\right)$ 可以由安全管理员通过漏洞集 V_i 和威胁集 T_i 并结合任务需求进行赋值,如 $\boldsymbol{C}(i)=(1,10,20,50)$,$\delta_i=0.2$。

将任务模型和资产模型关联分析可得,t 时刻子任务 M_i 的风险为:

$$R_{M_i,t}=\sum_{a=1}^{A_i}\delta_iR_{a,t} \tag{14}$$

任务 M 的 t 时刻的总风险可以表达为:

$$R_{mn,t}=\sum_{i=1}^{N}R_{M_i,t} \tag{15}$$

式中:N 代表网络中任务阶段的总数。

这种定义下的任务风险属性只涉及几个资产的安全事件,并不会将任务的风险值影响到一个较高水平。为了衡量任务的平均风险水平,可表达为:

$$\overline{R}_{mw,t}=R_{mw,t}/N \tag{16}$$

式中:$\overline{R}_{mw,t}$ 的值依赖于任务,因为不同资产的隐式马尔科夫模型和代价向量不同。与式(15)相反,任务的平均风险是给定的一个归一化的值。如果任务中大部分资产都受到入侵事件的影响,网络的平均风险值可能会随着时间的推移而显著变化。

4.3 示例说明

为了说明任务风险预测模型的应用,下面对典型 Web 应用的安全预测问题进行分析,威胁事例利用微软威胁建模工具产生,给出的资产与威胁关系并结合本文给出的风险预测模型进行。

该 Microsoft Threat Modeling Tool 2016 工具可以很好地映射任务中各项资产之间的拓扑关系[20],数据流程见图 4。

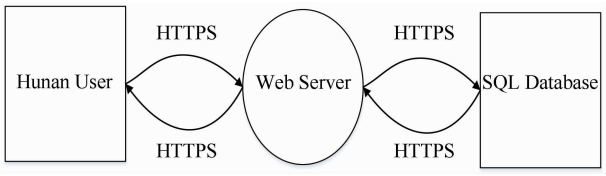
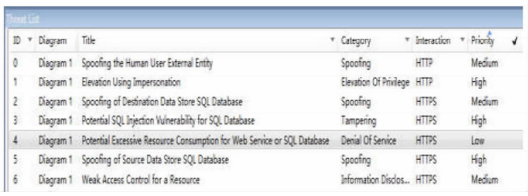


图 4　数据流程图

图中用户作为一个外部实体(由正方形表示)正在向 Web 服务器(圆形部分)发送命令，Web 服务器正在查询 SQL 数据库(2 条平行线)。通过应用 STRIDE 方法，该工具可以发现并生成基于默认模板的一系列威胁信息 T_i，见图 5。威胁列表显示了每条威胁信息的序号、图表来源、威胁标题、威胁种类、交互方式和优先级等信息。



ID	Diagram	Title	Category	Interaction	Priority
0	Diagram 1	Spoofing the Human User External Entity	Spoofing	HTTP	Medium
1	Diagram 1	Elevation Using Impersonation	Elevation Of Privilege	HTTP	High
2	Diagram 1	Spoofing of Destination Data Store SQL Database	Spoofing	HTTPS	Medium
3	Diagram 1	Potential SQL Injection Vulnerability for SQL Database	Tampering	HTTPS	High
4	Diagram 1	Potential Excessive Resource Consumption for Web Service or SQL Database	Denial Of Service	HTTPS	Low
5	Diagram 1	Spoofing of Source Data Store SQL Database	Spoofing	HTTPS	High
6	Diagram 1	Weak Access Control for a Resource	Information Disclos...	HTTPS	Medium

图 5　威胁信息列表图

图 6 中，ID 为 0 和 1 的威胁信息针对用户向 Web 服务器发送命令这一阶段任务生成，如下图加粗部分所示：

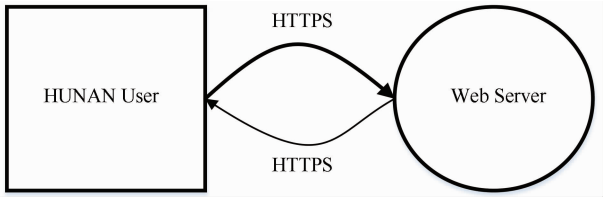


图 6　任务阶段示例 1

ID 序号为 0 的威胁信息具体见图 7。

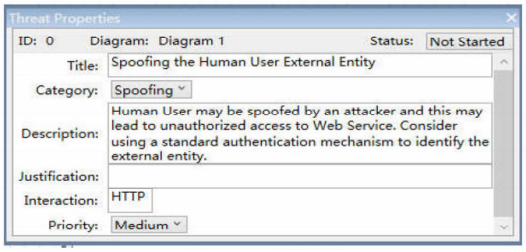


图 7　ID0 威胁信息

表中的描述“用户可能受到攻击者的欺骗，导致对 Web 服务的未经授权的访问”表明了针对用户的漏洞。以用户为例可以建模如下：

$$\boldsymbol{P}_{\text{user}}=\begin{pmatrix}0.6 & 0.3 & 0.09 & 0.01\\ 0.3 & 0.4 & 0.25 & 0.05\\ 0.1 & 0.2 & 0.6 & 0.1\\ 0.01 & 0.09 & 0.1 & 0.8\end{pmatrix}$$

$$\boldsymbol{Q}_{\text{user}}=\begin{pmatrix}0.05 & 0.000\,1 & 0.02 & 0.01 & 0.02 & 0.899\,9\\ 0.05 & 0.000\,1 & 0.25 & 0.01 & 0.02 & 0.669\,9\\ 0.1 & 0.005 & 0.1 & 0.03 & 0.03 & 0.735\\ 0.02 & 0.05 & 0.04 & 0.04 & 0.05 & 0.8\end{pmatrix}$$

$$\boldsymbol{\pi}_{\text{user}}=(0.8,0.1,0.05,0.05)$$

$$\boldsymbol{C}_{\text{user}}=(0.1,0.4,0.7,1)$$

$$\delta_{\text{user}}=0.2$$

为了简化计算令 Web 服务器与用户具有相同的 HMM 模型，并赋值其代价向量为 $\boldsymbol{C}_{\text{Web}}=(0.2,0.4,0.8,1)$，影响因子 $\delta_{\text{Web1}}=0.8$，则可得当前阶段任务的风险预测值为 0.385 2。

针对 Web 服务与数据库交互这一阶段任务如图 8 所示生成的威胁信息有：①SQL 数据库可能被攻击者欺骗，导致数据被写入攻击者的目标而不是 SQL 数据库；②SQL 数据库潜在 SQL 注入攻击；③Web服务或 SQL 数据库潜在的过度资源消耗；④SQL数据库被攻击者欺骗，导致不正确的数据传递到 Web 服务；⑤不正确的 SQL 数据库数据保护允许攻击者读取不打算公开的信息。

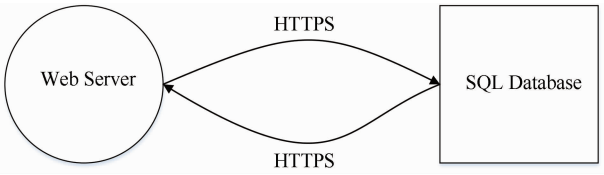


图 8　任务阶段示例 2

在此任务阶段中，令 Web 服务和 SQL 数据库与任务第一阶段中的用户这项资产具有相同的 HMM 模型，并根据威胁信息分别对 Web 服务和 SQL 数据库赋值如下：

$$\boldsymbol{C}_{\text{Web}}=(0.2,0.4,0.8,1),\quad \delta_{\text{Web2}}=0.4$$

$$\boldsymbol{C}_{\text{SQL}}=(0.3,0.5,0.8,1),\quad \delta_{\text{SQL}}=0.6$$

计算可得该阶段任务的风险预测值为 0.439 6，结合对上一阶段风险的计算可得任务的预测风险值为 0.824 8。通过结果可以看出 Web 服务和 SQL 数据库交互这一阶段对任务风险影响较大，其中针对 SQL 数据库的威胁信息最多，对任务风险贡献最大，管理员在制定安全计划时需要对这项资产严格配置。

5　结语

本文研究了一种网络风险预测评估方法，以任务为核心，并且将网络风险水平确定为任务推进中各阶段调用的所有资产风险值的聚合函数，为风险评估提供了一个可行的精确的细粒度模型。本文提出的方法的主要优点是隐式马尔科夫模型为状态估计提供了一个现有框架，既可以建模进入特定状态的概率，也可以建模在每个状态接收不同观测信息的概率，状态建模和转移概率也与传统的风险评估方法有关。一旦任务的风险值达到一定高度就需要安全管理员即使进行安全策略调整，加固网络安全。这种风险评估预测方法可为面向任务的安全调度和

管控提供决策依据,从而构建安全可靠的防御,在主动防御方面具有重要意义。

参考文献(References):

[1] 宋述贵.大型国有企业信息系统建设过程中的风险控制研究[D].北京:华北电力大学,2017.
SONG S G. Research on Risk Control in the Construction of Large State-Owned Enterprises' Information System[D]. Beijing: North China Electric Power University, 2017. (in Chinese)

[2] 何骞.网络安全态势评估若干关键技术研究[J].中国新通信,2016,18(14):42.
HE Q. Research on Key Techniques in Network Security Situation Assessment [J]. China New Telecommunications,2016,18(14):42. (in Chinese)

[3] 孟锦. 网络安全态势评估与预测关键技术研究[D].南京:南京理工大学,2012.
MENG J. Research on Key Techniques in Network Security Situation Assessment and Prediction [D]. Nanjing: Nanjing University of Science and Technology, 2012. (in Chinese)

[4] YUAN Z C. Network Efficacy Evaluation Based on AHP for Network Security Situation Assessment[C]//Proceedings of 2016 6th International Conference on Machinery, Materials, Environment, Biotechnology and Computer. [S. l.]: Computer Science and Electronic Technology International Society, 2016.

[5] 兰芳. 基于 FISM-ANP-灰色聚类的软件项目开发风险评价研究[D]成都:电子科技大学,2018.
LAN F. Risk Evaluation of Software Project Development Based on FISM-ANP-Grey Clustering [D]. Chengdu: University of Electronic Science and Technology of China, 2018. (in Chinese)

[6] RABINER L R . A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition [J]. Proceedings of the IEEE, 1989,77(2):257-286.

[7] 王巍. 面向对象贝叶斯网络及其在风险评估中的应用[D].南京:南京航空航天大学,2016.
WANG W. Object-Oriented Bayesian Networks and Its Application in Risk Assessment [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2016. (in Chinese)

[8] JIN Y H . The Model of Network Security Situation Assessment Based on Random Forest[C]//Proceedings of 2016 IEEE 7th International Conference on Software Engineering and Service Science (ICSESS 2016). Beijing:IEEE, 2016:4-20.

[9] LIU Q , PÉRÈS, F, TCHANGANI A . Object Oriented Bayesian Network for Complex System Risk Assessment[J]. IFAC-PapersOnLine, 2016, 49(28): 31-36.

[10] GRZEGORZ K, JOLANTA M P . Security Framework for Dynamic Service-Oriented IT Systems[J]. Journal of Information Systems and Telecommunication, 2018:1-21.

[11] 刘佳杰, 伍宇波, 张煜, 等.威胁建模在安全态势感知中的应用研究[J].中国金融电脑,2018(11):81-85.
LIU J J, WU Y B, ZHANG Y, et al. Application of Threat Modeling in Security Situation Awareness [J]. Financial Computer of China, 2018(11): 81-85. (in Chinese)

[12] HE K,LI X H, FENG Z Y. Approach to Object Oriented Threat Modeling [J]. Computer Engineering, 2011, 37(4):21-20.

[13] 贾承安.网络安全风险评估关键技术研究[J].网络安全技术与应用,2018,18(10):12-13.
JIA C A. Research on Key Technology in Network Security Risk Assessment [J]. Network Security Technology & Application, 2018,18(10):12-13. (in Chinese)

[14] PORRAS P A, FONG M W, VALDES A. A Mission-Impact-Based Approach to INFOSEC Alarm Correlation. [C]// International Conference on Recent Advances in Intrusion Detection. Zurich, Switzerland: Springer-Verlag, 2002.

[15] 马琳茹,杨林,何俊,等.面向任务的量化风险评估方法[J].计算机工程与应用,2007,43(6):136-139.
MA L R, YANG L, HE J, et al. A Method Basedon Mission Model for Quantitative Risk Assessment[J]. Computer Engineering and Applications, 2007,43(6): 136-139. (in Chinese)

[16] NAKHLA N , PERRETT K, MCKENZIE C . Automated Computer Network Defence Using ARMOUR: Mission-Oriented Decision Support and Vulnerability Mitigation[C]// International Conference on Cyber Situational Awareness. London, UK: IEEE, 2017: 1-8.

[17] LAHON M, SINGH Y J, LAHON M, et al. Task Oriented Risk Assessment (TORA)[J]. International Journal of Computer Applications, 2013, 66(7): 28-31.

[18] LI X , ZHAO H. Network Security Situation Assessment Based on HMM-MPGA[C]// 2016 the 2nd International Conference on Information Management. London, UK: IEEE, 2016.

[19] 陈建莉. 基于未确知数学的网络安全风险评估模型[J]空军工程大学学报(自然科学版),2014,15(2): 91-94.
CHEN J L. A Network Security Risk Assessment Model Based on the Unascertained Mathematics[J]. Journal of Air Force Engineering University(Natural Science Edition),2014,15(2):91-94. (in Chinese)

[20] SCANDARIATO R, WUYTS K, JOOSEN W . A Descriptive Study of Microsoft's Threat Modeling Technique [J]. Requirements Engineering, 2015, 20(2):163-180.

(编辑:徐楠楠)