效用理论在信息安全投资优化中的应用

陈天平 张串绒 郭威武 郑连清
(空军工程大学电讯工程学院 西安 710077)

摘 要 为了解决组织预算过程中信息安全投资最优的问题,建立了安全投资与风险控制的关系模型,对安全投资的有效性进行了研究,提出了降低事件发生概率有效性及缓解损失有效性的新概念。采用效用理论作为组织财富、风险损失和安全投资的描述模型,指数效用函数作为组织投资收益的描述模型。分析了安全投资的边界,使用求偏导数取极值的方法对投资效用函数进行了研究,并求得最小投资的解。应用实例表明,基于效用的风险度量方法是科学的,损失效应越大的安全事件需要更大的安全投资。

关键词 网络安全,效用理论,风险控制,信息安全投资
中图法分类号 TP393.08 **文献标识码** A

Application of Utility Theory in Investment Optimizing of Information Security

CHEN Tian-ping ZHANG Chuan-rong GUO Wei-wu ZHENG Lian-qing
(Telecommunication Engineering Institute, Air Force Engineering Univ., Xi'an 710077, China)

Abstract The relation model between security investment and risk control was introduced to solve the problem of the optimal information security investment in corporation budget. The security investment efficiency was studied and the new concept of reducing the event probability and lost efficiency was presented. The utility theory was used to model system under the corporation wealth, risk lost and security investment, and the exponential utility function was used to model the yield of corporation, maximum security investment bound was analyzed. The method using differential coefficient to achieve extremum was applied for the utility function and derived the result of optimal investment. The case study demonstrated the risk measurement method based on the utility was scientific and the security events producing more loss effect need more security investment.

Keywords Network security, Utility theory, Risk control, Information security investment

计算机蠕虫和病毒、间谍软件、黑客攻击和非授权访问等安全事件频频发生,导致了全球范围内每年数以亿计的巨额损失[1]。依据CSI/FBI在2005年的调查,75%以上的被调查者反映曾经遭受过各种信息安全事件[2]。据估计,美国公司为解决信息安全问题人均每年花费196美元[3]。因此,适量投资于信息安全管理或技术,以降低安全事件的风险,是组织明智的选择。文献[4]基于图论分析网络安全的威胁态势,为安全投资调控提供决策支持,但缺少具体的投资优化方案[4];文献[5]给出了信息系统的最小安全投资额模型以及求解该模型的自适应遗传算法[5],但该算法所需的前提条件过于复杂,难以实现。

鉴于此,本文采用经济学中的效用理论分析信息安全投资问题,并应用指数型效用函数计算信息安全最优投资额。

1 效用理论

效用是一种主观感受,是一种主观愿望的满意程度。效用函数是对效用的一种数量表示,给出了综合满意程度的数值度量。效用理论是一个经典的经济学概念,在保险精算领域有广泛的应用[6,7]。

定义1 集合M上的实值函数$u(x)$,若满足条件:当$x\geqslant y$时,恒有$u(x)\geqslant u(y)$成立,称$u(x)$为集合M上的效用函数[6]。

效用值表示为u,组织的财富表示为w,则

$$u=u(w) \tag{1}$$

其中,$u(x)$为效用函数,反映了决策者对于一项投资所带来的收益的满意程度。

根据效用理论,效用函数应满足以下两个性质。

性质1 $u(w)$是w的单调增函数。

性质2 $\Delta u=u(w+\Delta w)-u(w)$是$w$的单调减函数,这一性质称为边际效用递减规律。

若$u(w)$具有2阶导数,则以上性质可表示为

$$u'(w)\geqslant 0, u''(w)\leqslant 0 \tag{2}$$

2 信息安全投资的有效性分析

2.1 安全投资与风险控制的关系

风险评估是在综合分析系统资产、威胁、弱点和控制措施

到稿日期:2009-01-07 返修日期:2009-04-30 本文受国家自然科学基金项目(60873233),陕西省科技攻关(2008-k04-21)资助。
陈天平(1979-),男,博士生,主要研究方向为信息安全风险管理,E-mail:chentianping1979@163.com;郑连清(1963-),男,教授,博士生导师,主要研究方向为信息网络管理与安全应用技术。

后，识别安全风险事件集合 E，并评价每个事件在当前信息系统状态下发生的概率 ρ 及造成的损失 L。风险控制是依据评估结果进行信息安全投资预算，并制订、执行相应的风险消减方案的过程。安全投资与风险控制的关系如图 1 所示。

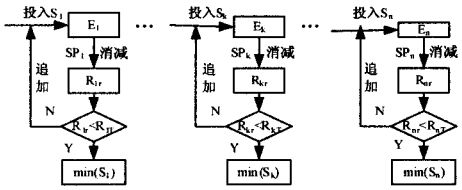

图 1　安全投资与风险控制关系模型

信息安全风险可表示为有序对的集合

$$R^n \triangleq \{(E_1,\rho_1,L_1),\cdots,(E_i,\rho_i,L_i),\cdots,(E_n,\rho_n,L_n)\} \quad (3)$$

其中，R^n 为组织面临的关键风险；E_i 为风险事件；ρ_i 为 E_i 的发生概率；L_i 为 E_i 可能造成的损失。

图 1 中 S_k 为控制 E_k 而进行的安全投资；SP_k 为消减风险的安全方案；R_{kr} 为实施 SP_k 后的残余风险；R_{kT} 为组织设定的风险阈值；$\min(S_k)$ 为最小投资额。

因此，组织的最小安全投资预算 $S_{\min}$ 可表示为

$$S_{\min}=\sum_{k=1}^{n}\min(S_k),k=(1,2,\cdots,n) \quad (4)$$

2.2　分析安全投资的有效性

信息安全事件的发生概率 ρ 可表示为威胁态势 t、脆弱性程度 v 和安全投资额 s 的函数，即

$$\rho=\rho(s,v,t)=\frac{f(v,t)}{k_\rho s+1} \quad (5)$$

且满足以下条件

①$0\leqslant\rho(s,v,t)\leqslant 1,\forall s,v,t$；

②$\rho(0,v,t)=f(v,t)=\rho_0,\forall v,t$；

③$\rho(s,v,t)=0\Leftrightarrow s=\infty,\forall v>0,t>0$。

损失 L 可表示为资产价值 a、脆弱性程度 v 和安全投资额 s 的函数，即

$$L=L(s,a,v)=\frac{l(a,v)}{k_l s+1} \quad (6)$$

且满足以下条件

①$0\leqslant L(s,a,v)\leqslant+\infty,\forall s,a,v$；

②$L(0,a,v)=l(a,v)=L_0,\forall a,v$；

③$L(s,a,v)=0\Leftrightarrow s=\infty,\forall a>0,v>0$。

定义 2(投资有效性)　投资单位金额 Δs，采用安全方案 sp_j 对风险的消减效果，简记为 $\xi(sp_j)$。

$\xi(sp_j)$ 可表示成数对形式：$\xi(sp_j\rightarrow\rho)$ 为 Δs 产生的降低事件发生概率有效性；$\xi(sp_j\rightarrow L)$ 为 Δs 产生的缓解事件损失有效性。$\xi(sp_j)$ 可表示为

$$\xi(sp_j)=\left(\frac{\partial\rho}{\partial s},\frac{\partial L}{\partial s}\right) \quad (7)$$

以式(5)为例，取初始概率 $\rho_0=0.6$，可变系数 k_ρ 分别取值 2，1 和 0.5 时，投资有效性 $\xi(sp_j\rightarrow\rho)$ 如图 2 所示。

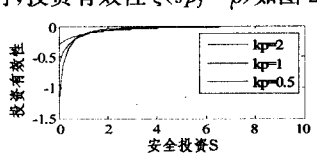

图 2　投资有效性分析

由图 2 可知，投资安全方案 SP 的有效性 $\xi(sp\rightarrow\rho)$ 随 k_ρ 取值的增大而增大，故 k_ρ 的取值能反映出投资有效性的大小。$L(s,a,v)$ 的情况类似，不再赘述。

3　基于效用函数优化安全投资的方法

效用理论的关键是效用函数，选取一个能真实度量人们满意程度(或不满意程度)的效用函数是关键所在。本文使用指数型效用函数，它是保费计算的基础，其表达式为

$$u(w)=\frac{1}{\alpha}(1-e^{-\alpha w}) \quad (8)$$

其中，$\alpha>0$ 为常数，α 表示决策者对风险的厌恶程度或承受能力；w 代表组织财富；$u(w)$ 是 w 的效用函数。

3.1　分析最大安全投资的边界

假设随机变量 X 表示某一信息安全事件 (E,ρ,L) 可能对组织造成的损失，则 X 符合以下分布律

X	L	0
P_X	ρ	$1-\rho$

根据指数型效用函数的性质，存在以下不等式关系[10]

$$E[u(w-X)]\leqslant u(E[w-X])=u(w-E(X)) \quad (9)$$

其中，$E(X)=\rho L$，表示 X 的期望损失。

如果组织进行安全投资后所产生的效用小于或等于不做任何投资时(即接受风险)的效用，那么该项投资是毫无意义的。若决策者进行安全投资的上限值为 $\hat{S}$，一旦超过 $\hat{S}$ 将导致投资失效，数学表达为

$$E(u(w-X))=u(w-\hat{S}) \quad (10)$$

联立式(8)和式(10)，可解得

$$\hat{S}=\frac{\ln(1-\rho+\rho e^{\alpha L})}{\alpha},L>0,\rho\in[0,1] \quad (11)$$

L 经过形式变换后与 $\hat{S}$ 进行比较，得

$$L=\frac{\ln(e^{\alpha L})}{\alpha}=\frac{\ln(\rho e^{\alpha L}+(1-\rho)e^{\alpha\cdot 0})}{\alpha}>\hat{S} \quad (12)$$

联立式(9)、式(10)、式(13)得 $\hat{S}$ 的上、下取值边界范围

$$\rho L<\hat{S}<L \quad (13)$$

3.2　求解最优安全投资额

当组织面临风险损失 X 时，如何确定安全投资 S 的大小使组织获得最大效用，是每个组织亟需解决的问题。

组织的期望效用为 $E[u(w-S-X)]$，其数学展开式[8]

$$\begin{aligned}E[u(w-S-X)]&=\rho u(w-S-L)+(1-\rho)u(w-S)\\&=\frac{\rho(1-e^{-\alpha(w-S-L)})+(1-\rho)(1-e^{-\alpha(w-S)})}{\alpha}\end{aligned} \quad (14)$$

求 $E[u(w-S-X)]$ 的 S 偏导数。假若在 $S=S^*$ 处，偏导数为 0，故 $E[u(w-S-X)]$ 取得极值，即 S^* 为最优的投资额。

$$\partial E[u(w-S-X)]/\partial S=-\frac{1}{\alpha}e^{-\alpha(w-S)}\left[\frac{\partial\rho}{\partial S}e^{\alpha L}+\alpha\rho\left(1+\frac{\partial L}{\partial S}\right)e^{\alpha L}-\frac{\partial\rho}{\partial S}+\alpha(1-\rho)\right]$$

要使得偏导数为 0，只有满足以下条件

$$\frac{\partial\rho}{\partial S}(e^{\alpha L}-1)+\alpha\rho(e^{\alpha L}-1)+\alpha\rho e^{\alpha L}\frac{\partial L}{\partial S}+\alpha=0 \quad (15)$$

投资有效性为

$$\zeta(sp_j)=(-\frac{k_\rho f(v,t)}{(k_\rho S+1)^2},-\frac{k_L l(a,v)}{(k_L S+1)^2}) \tag{16}$$

联立式(5)、式(6)、式(15)、式(16)，得

$$\frac{f(v,t)}{(k_\rho s+1)^2}(e^{\frac{\alpha(a,v)}{k_L s+1}}-1)-\frac{\alpha f(v,t)}{k_\rho s+1}(e^{\frac{\alpha(a,v)}{k_L s+1}}-1)+\frac{\alpha k_L f(v,t)l(a,v)}{(k_\rho s+1)(k_L s+1)^2}e^{\frac{\alpha(a,v)}{k_L s+1}}=\alpha \tag{17}$$

解方程(17)，可分两种情形讨论。

情形 1：不妨假设 $e^{\frac{\alpha(a,v)}{k_L s+1}}-1=c>0$ 为常数；$f(t,v)=\rho_0$，$l(a,v)=L_0$ 分别表示不做任何投资时事件的初始发生概率及损失；$k_\rho=k_L=k>0$。化简上式，可得

$$\alpha(ks^*+1)^3+\alpha\rho_0 c(ks^*+1)^2-c\rho_0 k(ks^*+1)=\alpha\rho_0 L_0 k(c+1) \tag{18}$$

求解此一元三次方程，可得 S^* 的解。

情形 2：假设所采用的安全方案 sp_k 对于缓解事件损失没有效果。譬如采用入侵检测类技术，则投资有效性可表示为 $\xi(sp_k)=(\xi(sp_k\to\rho),0)$，即事件造成的损失 L 为常量。

不妨取式(5)中 $f(v,t)=vt, v,t\in[0,1]$，则

$$\frac{\partial\rho}{\partial S}=-\frac{k_\rho vt}{(k_\rho S+1)^2} \tag{19}$$

联立式(5)、式(15)、式(19)，解得 S^* 为

$$S^*=\frac{-(2\alpha+\alpha(e^{\alpha L}-1)vt)+\sqrt{(\alpha(e^{\alpha L}-1)vt)^2+4\alpha k_\rho(e^{\alpha L}-1)}}{2\alpha k_\rho}vt \tag{20}$$

且必须满足条件

$$v\geqslant\frac{\alpha}{(k_\rho-\alpha)(e^{\alpha L}-1)t} \tag{21}$$

3.3 基于效用的安全风险度量方法

传统的风险度量方法采用期望损失的方法，将导致高损失、低概率事件与低损失、高概率事件不能区分。实际上，因为损失效应[6]，决策者对损失巨大的事件更加敏感，心理承受压力亦更大。

效用函数能够度量事件带来的不满意程度。但所得结果是损失越高，效用越小，这不符合人们的思维表达习惯。在此采用效用函数的反函数来度量风险，表示事件损失越高，效用也越大，使用该效用值来代表受损失效应影响的事件风险值。

取式(8)的反函数为 $\phi(x)$，则

$$\phi(x)=-\frac{1}{\alpha}\ln(1-\alpha x) \tag{22}$$

安全事件 (E_i,ρ_i,L_i)，考虑损失效应时的风险值为

$$\phi(E_i)=\phi(L_i)\rho_i+\phi(0)(1-\rho_i)=\phi(L_i)\rho_i \tag{23}$$

4 应用举例

4.1 实例计算步骤

以某信息系统作为风险评估对象。为了计算简便，假定风险评估结果有以下 3 项。

1)恶意代码和病毒，表示为(E_1，0.4，25 万)；

2)非授权访问，表示为(E_2，0.1，100 万)；

3)黑客非法篡改数据，表示为(E_3，0.05，200 万)。

步骤 1　根据风险评估结果，分别制订相应的风险控制安全方案 sp_j，$j=1,2,3$。

步骤 2　由专家分析 sp_j 的风险控制效果，以确定其投资有效性，以此作为选取系数 k_ρ 和 k_L 的依据。为了计算方便，不妨取 $k_\rho=k_L=0.5$。

步骤 3　基于效用度量安全事件的风险大小。由式(23)得 E_1，E_2 和 E_3 的风险为 $r'(E_1)=10.326$ 万；$r'(E_2)=11.507$ 万；$r'(E_3)=13.863$ 万(其中 $\alpha=0.0025$)。

步骤 4　计算信息安全最小投资额。由式(20)分别得到最小投资额 $S_1^*=2.65613$ 万，$S_2^*=3.69567$ 万，$S_3^*=5.68547$ 万；再由式(4)得最小投资预算 $S_{\min}=\sum_{i=1}^{3}S_i^*=12.03727$ 万。

4.2 结论分析与比较

1)针对 $E[u(w-S-X)]$，将式(5)、式(6)代入式(14)，以安全事件 E_1，E_2 和 E_3 为分析对象，从而得到安全投资 S 与效用之间的关系，如图 3 ($\alpha=0.01$，$k_\rho=k_L=0.5$)所示。

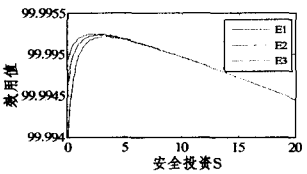

图 3　安全投资的效用

分析图 3 可知：①3 条效用曲线均在某个最优投资 S^* 处获得极大值；②仿真结果与式(20)所得结果相吻合，说明将风险事件损失当常量处理是科学的。

2)为了证明基于效用的安全风险度量方法的优势，与期望损失的度量方法相比，结果如图 4 所示。

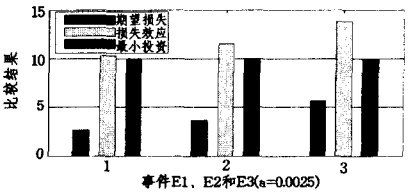

图 4　两种方法的结果比较图

分析图 4 可知：①基于效用的风险度量方法能反映损失效应带来的风险影响，而期望损失的度量方法却不能；②在期望损失相同的情况下，损失效应越大的风险事件所需的安全投资亦越大，即存在关系 $S_1^*<S_2^*<S_3^*$，该结论与上节中步骤 4 的结论完全一致。

3)本方法与文献[5]中的方法相比，其优势体现在：文献[5]提出的计算最小安全投资额的方法，是建立在信息系统的利用图模型完全清楚的前提下。然而，由于信息系统的漏洞数量及攻击方式极其复杂，因此准确获取利用图模型十分困难。本文所提的方法简洁明了，首先根据专家经验初步确定安全方案的投资有效性，然后以组织效用最大化作为评判准则来求解最小投资额。

结束语　本文应用效用理论解决信息安全最优投资的问题。本方法为合理的安全投资的风险控制提供了新的思路。文中初步提出投资有效性的概念，还需要结合具体安全措施做进一步分析研究；安全事件发生概率及造成损失的数学表达模型需要利用实验数据进行完善；最关键的是，如何利用有限的安全投资成本，选取适当的安全方案，使风险控制的效能最大化，这将是进一步研究的重点内容。

(下转第 123 页)

检测器库，以保证其它节点同样具有快速检测该蠕虫的能力。

本文所提出的蠕虫检测免疫模型与其它蠕虫检测方法相比在很多方面具有优势，下面对这些优势加以分析。

首先，本模型具有较好的开放度。相比传统反向选择、克隆选择算法中训练阶段是在受保护的环境中进行，本文模型由于在训练阶段记忆检测器模块关闭，该阶段可以在开放的环境中完成。

其次，本模型采用 DCs 检测抗原的系统和网络信息、T 细胞检测器识别抗原结构的双重识别方法降低了系统的错误检测率。在危险信号存在的情况下，如果成熟 T 细胞检测器和记忆 T 细胞检测器都不匹配与此危险信号相关的所谓的"危险"抗原，或者有匹配发生，但是在规定时间内二者之间匹配次数达不到检测器的激活阈值，都说明该危险信号不是真正的"危险"，该"危险"抗原有可能是"安全"抗原；如果安全信号存在且不成熟 DCs 提呈可能的安全抗原给 T 细胞检测器，即便有识别信号产生，不成熟 DCs 也不会将该抗原交给虚拟胸腺进行耐受处理。两种情况下系统都不会做出任何响应，降低了错误检测率。

此外该模型通过"危险与否"实现虚拟胸腺中"自我"集的更新，从而使模型具备了很好的自适应性。如果 DCs 的输出信号是"安全"的，则同期采集到的相应抗原是"安全"的，将其加入到虚拟胸腺中的"自我"集中，最终导致成熟 T 细胞检测器集的更新。

最后，由于记忆 T 细胞检测器的引入，记忆检测器激活阈值更低，可以保证模型对经历过的攻击进行快速响应，提高了系统的执行效率。

结束语 本文详细描述了危险理论中先天免疫系统(DCs)和适应性免疫系统(T cells)的协同，在此基础上提出用于蠕虫检测的人工免疫模型，并对主要功能模块的实施进行了详细的描述，最后从理论上对模型的性能进行了分析。在该模型中，以分析蠕虫引起的系统和网络资源的变化信息是否预示"危险"为中心，同时结合了适应性免疫中的反向选择、免疫记忆原理。本模型应具有如下优势：1)采用双重检测：在 DCs 处理模块完成对蠕虫引起的系统和网络"危险"的初步检测后，呈捕获的相应抗原由记忆 T 细胞检测器或者成熟 T 细胞检测器完成下一步检测，这样降低了错误检测率；2)同时，记忆 T 细胞检测器的引入，可以保证对感染过的蠕虫进行快速响应，提高时效性，阻止蠕虫进一步蔓延；3)由于采用双重识别，如果仅仅检测到危险，而相应的匹配没有发生，则说明不是真正的"危险"，可以忽略；4)由于模型以"危险"与否确定蠕虫身份，不再完全依赖于蠕虫特征码的提取，这样对于多态蠕虫具有较好的检测效果。这些都对建立一个更加健壮的蠕虫检测系统具有重要的意义。

接下来仍然有许多的工作要做。以下几点将是未来工作的重点：开发出实验系统，以更好地验证本文所提出模型所具备的种种优势；大量参数值的合理设置如何获取；将机体免疫学中的其它机理引入到本模型中，比如 T 细胞的克隆增殖等等。

参 考 文 献

[1] Lockwood J W, Moscola J, Kulig M. Internet worm and virus protection in dynamically reconfigurable hardware[J]. WORM, 2003

[2] Malan D J, Smith M D. Host-Based detection of worms through peer-to-peer cooperation[C]// Keromytis AD, ed. Proc. of the 2005 ACM Workshop on Rapid Malcode. 2005: 72-80

[3] Cheung S, Hoagland J, Levitt K. The Design of GrIDS: A graph-based intrusion detection system[R]. CSE- 99- 2, U. C. Davis Computer Science Department, 1999

[4] Bakos G, Berk V. Early detection of Internet worm activity by metering ICMP destination unreachable activity[C]// The SPIE conference on Sensors, and Command, Control, Communications and Intelligence. 2002

[5] 张运凯，王方伟，马建峰，等. 基于隔离策略的蠕虫传播模型及分析[J]. 计算机科学，2005，32(3)：62-65

[6] Aickelin U, Greensmith J, Twycross J. Immune system approaches to intrusion detection-a review[C]// Proceedings of ICARIS'04. September 2004: 316-329

[7] Kim J. Integrating Artificial Immune Algorithms for Intrusion Detection[D]. Department of Computer Science, University College London, 2002

[8] Tolerance M P. Danger and the Extended Family[J]. Annual Review in Immunology, 1994, 12: 991-1045

[9] Aickelin U, Cayzer S. The Danger Theory and Its Application to AIS[C]// 1st International Conference on AIS. 2002: 141-148

[10] Kim J, Wilson W, Aickelin U, et al. Cooperative Automated Worm Response and Detection Immune Algorithm (CARDINAL) inspired by T-cell Immunity and Tolerance[C]// The 3rd Int. Conf. on AIS (ICARIS-05). 2005: 168-181

[11] Twycross J. Integrated Innate and Adaptive Artificial Immune Systems Applied to Process Anomaly Detection[D]. University of Nottingham, 2007

(上接第 72 页)

参 考 文 献

[1] Denning D. Reflectons on cyberweapons controls[J]. Computer Security Journal, 2000, 16(4): 3-53

[2] Gordon L A, Loeb M P, Lucyshyn W, et al. CSI/FBI Computer Crime and Security Survey[M]. Computer Security Institute, 2005

[3] Geer D, Soo Hoo K, Jaquith A. Information security: Why the future belongs to the quants[J]. IEEE Security and Privacy, 2003, 1(4): 24-32

[4] 陈天平，乔向东，郑连清，等. 图论在网络安全威胁态势分析中的应用[J]. 北京邮电大学学报，2009，32(1)

[5] 陈光. 信息系统信息安全风险管理方法研究[D]. 长沙：国防科学技术大学，2006：146-153

[6] 彭俊好，徐国爱，杨义先，等. 基于效用的安全风险度量模型[J]. 北京邮电大学学报，2006，29(2)

[7] Menoncin F. Optimal portfolio and background risk: An exact and an approximate solution[J]. Insurance Mathematics and Economics, 2002, 31(2): 249-265

[8] Huang C D, et al. An economic analysis of the optimal information security investment in the case of a risk-averse firm[J]. Production Economics, 2008, 114: 793-804

[9] Kaas R, Gavaerts M, Phaene J, et al. Modern actuarial risk theory [M]. Boston, MA: Kluwer Academic Publishers, 2001