信息安全风险概率计算的贝叶斯网络模型

王桢珍[1],姜 欣[2],武小悦[1],谭 旭[3]
(1.国防科学技术大学信息系统与管理学院,湖南长沙 410073; 2.清华大学计算机科学与技术系,北京 100084;
3.深圳信息职业技术学院计算机应用系,广东深圳 510829)

摘 要: 构建了一个基于贝叶斯网络的信息安全风险概率计算模型,并保证其可扩展性、精确性和客观性.模型的网络结构以规划渗透图表现,模型网络参数由专家知识确定并利用贝叶斯学习对其进行更新.实例分析表明构建的模型可以正确量化评估信息安全风险概率.

关键词: 风险评估; 贝叶斯网络; 规划渗透图; 贝叶斯学习
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 2A-018-05

Planning Exploitation Graph-Bayesian networks Model for Information Security Risk Frequency Measurement

WANG Zhen-zhen[1], JIANG Xin[2], WU Xiao-yue[1], TAN Xu[3]
(1. *College of information System and Management, National University of Defense Technology, Changsha, Hunan* 410073, *China*;
2. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*;
3. *Department of Computer Application, Shenzhen Institute of Information Technology, Shenzhen, Guangdong* 518029, *China*)

Abstract: A planning exploitation graph-bayesian networks model that can be applied in measurement of information security risk frequency is proposed, and the model's scalability, accuracy and objectivity are achieved. The model graph structure is determined by Planning Exploitation Graph, the local conditional probability distributions are computed by combination of expertise knowledge and the maximum entropy prior probability distribution method, and the model parameters are updated with training data by Bayesian networks learning. The analysis of the example shows the model could evaluate the information security risk frequency successfully.

Key words: risk measurement; Bayesian networks; planning exploitation graph; Bayesian networks learning

1 引言

随着信息技术的飞速发展,网络系统的信息安全问题面临着巨大的挑战.首先,针对网络系统的恶意攻击趋于多样化和复杂化,特别是同时利用系统多个脆弱性(vulnerability)进行的多步骤复合攻击较之于以往的利用单个脆弱性进行的单一攻击更为常见.其次,除已知的多个脆弱性外,一些组织也在不断发掘和发布新的安全脆弱性.最后,在考虑系统可用性、病毒库更新时延、系统安全维护资金投入等客观因素的情况下,一些脆弱性即使被发现也无法及时、彻底地从系统中移除.因此,完全消除系统的脆弱性几乎是不可能的,从而断定一个网络系统是"绝对安全的"或者"绝对不安全的"并无意义.更为符合实际的做法是从脆弱性之间的相互关系出发,分析它们可能导致系统发生哪些安全事件及其可能性,从而给出系统的安全风险状态评价.研究者提出了众多信息安全风险分析方法[1~5],这些方法从不同角度分析了系统安全事件发生的可能性.已有的网络安全评估标准[1,2]大多侧重于单个脆弱性的危害程度,无法准确度量复合攻击对关键资产造成的潜在危害.例如,攻击图[3~5]分析了复合攻击中脆弱性之间的因果关系,可以直观地表现系统安全风险发展的过程,但攻击图仅仅定性地分析了系统的安全风险,并认为如果存在导致关键资产安全事件的复合攻击则系统是不安全的,反之则系统是安全的.这种缺乏定量分析的做法显然不能满足当前安全风险分析的实际需求.文献[5~8]将风险概率计算引入安全风险分析,在攻击图模型的基础上加入了脆弱性的危害度量,定量地评估了系统的整体安全水平,是比较符合实际的风险分析方法,但这些方法仍然存在一些不足.Yu Liu 和 Hong Man[6]首次提出利用贝叶

收稿日期:2009-04-15;修回日期:2009-06-18
基金项目:国家自然科学基金(No.70771109)

斯网络模型进行风险评估,但他们构建模型时考虑的是各主机间安全状态的变化概率,没有从脆弱性利用这一风险发生的本质原因上去度量系统安全风险水平,同时基于状态的攻击图建模方法可扩展性较差[3],很难应用于大规模网络系统. Lingyu Wang[7]等人利用TVA构建系统风险的贝叶斯网络模型,但是他们的方法仅仅提高了模型的构建速度,却没有解决如何确定模型中节点的条件概率分布的这个问题.文献[3,8]对风险概率的计算仅限于局部节点间相互依赖关系的讨论,没有对整个系统的风险进行计算,也没有对风险概率计算数值的准确性进行分析.本文在前人工作基础上构建了基于贝叶斯网络[9]的信息安全风险概率计算模型(Planning Exploitation Graph-Bayesian Networks, PEG-BN),其具体做法是将风险的概率因素引入规划渗透图[10](Planning Exploitation Graph, PEG),以规划渗透图表现模型的网络结构,模型网络参数由专家知识与最大熵验前分布方法联合计算得到,并利用贝叶斯学习进行网络参数的更新.随后,利用一个具有代表性的实例阐明了该模型在网络安全风险评估中的应用.与文献[6,7]的工作相比,该模型由于引入了贝叶斯网络学习机制,生成的模型参数更为准确,构建的模型更能真实地反映系统实际风险状况;与文献[6]的工作相比,该模型的生成时间较短,可扩展性较强.此外,本文从系统全局的角度出发进行系统风险预测及实时评估的处理方法较之已有工作更为符合实际情况.

2　基于信息安全风险概率计算模型

2.1　模型定义

定义 1　基于贝叶斯网络的信息安全风险概率计算模型 $PEG\text{-}BN = \{PEG, P\}$,其中:

(1) PEG 为规划渗透图,表现了原子风险渗透之间的因果关系,决定了 $PEG\text{-}BN$ 的网络结构.

(2) $P = \{P(ae_i \mid Pa(ae_i)), ae_i \in AE)\}$ 是 PEG 中原子风险渗透发生的条件概率的集合,其中 $Pa(ae_i) = Pre(ae_i)$ 是原子风险渗透 ae_i 在 PEG 中的父节点集合,即 ae_i 的前提条件. P 决定了 $PEG\text{-}BN$ 的网络参数.

如图 1 所示,对于一个特定的 $PEG\text{-}BN$,其网络结构由 PEG 确定,表现了对应网络环境下,威胁主体利用脆弱性之间的因果关系,逐步进行原子风险渗透,直至获取特定安全目标的风险过程.网络参数由 P 确定,表现了每个特定原子风险渗透 ae_i 被威胁主体执行的可能性大小,其数值大小取决于网络环境、脆弱性、威胁主体和安全措施等前提条件,因此, P 表现为一组条件概率. $PEG\text{-}BN$ 有以下特点:

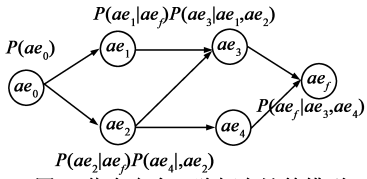

图1　信息安全风险概率计算模型

(1) PEG 是一有向无环图,其中 $s_i = ae_0$ 为根节点, $s_g = ae_f$ 为叶节点.任意原子风险渗透的父节点就是满足其发生前提条件的那些原子风险渗透,即 $\forall ae_i \in AE, Pa(ae_i) = Pre(ae_i)$.

(2)每个原子风险渗透的执行有执行成功(S)、执行失败(F)两种可能结果,各种可能的发生情况可以用条件概率 $P(ae_i) = P(ae_i \mid Pa(ae_i))$ 表示,它表达了该原子风险渗透与其父节点之间的相关关系.没有父节点的原子风险渗透的条件概率为其先验概率.

(3)所有的信息安全风险评估的贝叶斯网络中,定义 $P(ae_0) = 1$,即系统的初始状态.所有可能的安全目标都是从初始状态开始经渗透转变以一定概率到达的.

(4)所有信息安全风险评估的贝叶斯网络中,定义对所有 $ae_k \in \{Pa(ae_f)\}$,当且仅当其执行结果都为 F 时 $P(ae_f) = 0$,否则 $P(ae_f) = 1$.

2.2　模型构建

$PEG\text{-}BN$ 模型的构建包括了两部分:模型结构的定性构建和模型参数的定量构建,具体步骤如下:

步骤 1　确定模型的网络结构.

规划渗透图 PEG 表现了系统特定安全目标的风险过程中各原子风险渗透之间的因果关系,可作为构建 $PEG\text{-}BN$ 模型结构的基础,其转化算法如图 2 所示.

(1)对 PEG 模型的初始状态节点 $ae_0 = s_i$,在 $PEG\text{-}BN$ 模型中建立一个二态节点,并命名为 ae_0.

(2)对 PEG 模型的 ae_0 节点,寻找其所有直接后续的原子风险渗透 ae_i,在 $PEG\text{-}BN$ 模型中也相应建立的二态节点,将这些节点作为 ae_0 节点的子节点,并相应命名为 ae_i,显然 ae_i 为此时 $PEG\text{-}BN$ 模型的叶结点.

(3)对 2 中 $PEG\text{-}BN$ 模型的所有叶结点 ae_i,遍历其对应的 PEG 模型中的所有原子风险渗透 ae_i,寻找其所有直接后续的原子风险渗透节点 ae_j,在 $PEG\text{-}BN$ 模型中也相应建立的二态节点,并将这些节点作为 ae_i 节点的子节点,并相应命名为 ae_j.如果 PEG 模型中多个原子风渗透 ae_i 拥有同一个直接后续原子风险渗透节点 ae_j,则在 $PEG\text{-}BN$ 模型中也相应地对这多个 ae_i 节点建立一个子节点 ae_j.显然 ae_j 为此时 $PEG\text{-}BN$ 模型的叶结点.

(4)重复 3 的做法,直至遍历完 PEG 模型中的所有原子风险渗透.此时建立起的 $PEG\text{-}BN$ 模型只有一个叶结点 ae_f,此叶结点 ae_f 对应于 PEG 模型中的目标状态节点 $ae_f = s_g$.

图 2　$PEG\text{-}BN$ 模型结构的转化算法

步骤 2　确定模型的网络参数.

确定模型的网络参数就是计算网络节点的条件概率.经典的贝叶斯学习算法要求采用成败型试验确定网络节点的条件概率,但由于实际上通常很难有足够

的试验数据用于确定模型的网络参数,因此我们基于 *PEG* 模型的结构特点,采用多源验前信息获取融合验前分布[11]计算 *PEG-BN* 模型参数.

风险渗透之间的关系可以概括为如下三种:(1)一源一果,即一个 ae_j 可能导致一个 ae_k 的发生;(2)一源多果,即一个 ae_j 可能导致多个 $ae_{ki}(i=1,\cdots,n)$的发生,其中多个 ae_{ki}之间的逻辑关系为"或";(3)多源一果,即多个 $ae_{ji}(i=1,\cdots,n)$可能导致一个 ae_k 的发生,其中多个 ae_{ji}之间的逻辑关系为"或".图 3 展示了 *PEG-BN* 模型参数确定过程的中几种情况.

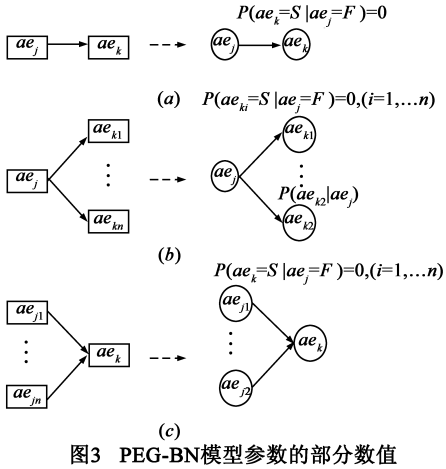

图3 PEG-BN模型参数的部分数值

我们采用多源验前信息融合计算 *PEG-BN* 模型中节点条件概率 θ 的验前分布.考虑 *PEG* 中各原子风险渗透的执行结果只有成功(S)或失败(F)两种情况,即节点事件状态均为二态,则可取"原子风险渗透成功执行"事件发生条件概率 θ 的验前分布服从 *Beta* 分布.咨询专家意见获取参数 θ 的验前均值 μ,综合 $Beta(\theta,a,b)$的极大熵,则可确定 $Beta(\theta,a,b)$的分布参数.

首先,在参考 *CVO* 中的脆弱性被成功利用的概率和网络系统体系结构的安全度两个属性的基础上[12],咨询专家意见获取参数 θ 的验前均值 μ,则

$$\mu=\frac{a}{a+b} \tag{1}$$

其次,计算 $Beta(\theta,a,b)$的极大熵,即

$$\begin{aligned}\varepsilon_N(\pi) &= -\int \pi(\theta)\log\left(\frac{\pi(\theta)}{\pi_0(\theta)}\right)\mathrm{d}\theta \\ &= -\int \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}\theta^{a-1}(1-\theta)^{b-1} \\ &\cdot\log\left(\frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}\theta^{a-1}(1-\theta)^{b-1}\right)\mathrm{d}\theta\end{aligned} \tag{2}$$

其中 θ 的自然无信息验前 $\pi_0(\theta)=1$.

联合式(1),(2),计算可使 $\varepsilon_N(\pi)$取值最大的 a 和 b,此 a 和 b 即为最大熵验前分布参数,则得到节点事件发生概率.

步骤 3 模型参数更新.

试验过程中,安全设备可以收集系统中原子风险渗透的执行情况,得到 *PEG* 模型中对应节点及其父节点的部分组合状态.此时可以根据贝叶斯学习[10,15],通过融合验前分布和样本信息来得到验后信息.具体做法为:

首先,对步骤 1 和步骤 2 建立得到的 *PEG-BN*,取其中第 i 个节点 x_i,在其父节点第 j 个组合状态下,该节点的验前概率分布为

$$\pi(\theta_{ij})=Beta(\theta_{ij}\mid a_{ij},b_{ij}) \tag{3}$$

其次,通过样本数据发现,在第 i 个节点的父节点的第j 个组合状态发生 n 次的条件下,该节点 x_i 发生了 m 次,则其似然函数为

$$P(D\mid\theta_{ij})=C_n^m\theta_{ij}^m(1-\theta_{ij})^{n-m} \tag{4}$$

又在设定获取的数据均是完备的前提下,记 $\pi(\theta)$为验前分布,$p(D\mid\theta)\pi(\theta)$为样本信息,$\pi(\theta\mid D)$是在给定样本 $D=(D_1,D_2,\cdots,D_n)$的条件下 θ 的验后分布,则

$$\pi(\theta\mid D)=\frac{p(D\mid\theta)\pi(\theta)}{\int_\theta p(D\mid\theta)\pi(\theta)\,d\theta} \tag{5}$$

将式(3)和式(4)代入式(5)可得到参数 θ_{ij}的验后分布为

$$\pi(\theta_{ij}\mid D)=Beta(\theta_{ij}\mid a_{ij}+m,b_{ij}+n-m) \tag{6}$$

综上,θ_{ij}的验后分布的均值就是在通过试验数据训练后该节点 x_i 在父节点的第 j 个组合状态下的条件概率.

2.3 基于 PEG-BN 的风险概率计算

在 *PEG-BN* 模型中,利用贝叶斯网络推理算法,不但可以将最大成功概率的计算扩展到预测和实时计算两个方面,还可以进行系统全局风险概率的计算,从而实现对系统安全状况进行多角度分析.

定义 2 系统全局风险概率是指,特定安全目标在系统当前安全配置情况下,所有脆弱性及威胁主体共同作用导致其风险发生的概率.

定义 3 安全目标的系统全局风险概率的预测,是指在没有探测到系统中原子风险渗透执行状态的前提下,对系统中特定安全目标被威胁主体成功渗透可能性进行的预测.其数值上等同于 *PEG-BN* 中目标节点 s_g 被成功渗透的概率,记为 $P(PEG)_{fore}$.

$$P(PEG)_{fore}=P(s_g=S\mid Pa(s_g)) \tag{7}$$

定义 4 安全目标的系统全局风险概率的实时计算,是指在收集了部分甚至全部原子风险渗透执行状态的前提下,对系统中特定安全目标被威胁主体成功渗透的可能性计算.其数值上等同于 *PEG-BN* 中目标节点 s_g 被成功渗透的概率,记为 $P(PEG)_{realtime}$.

$$P(PEG)_{realtime} = P(s_g = S \mid Pa(s_g), E) \quad (8)$$

其中 E 为证据数据.

在基于 *PEG-BN* 模型的风险概率计算中,可以分别对最大成功概率[1-3]进行没有证据数据时的预测及有证据数据时的实时计算.

最大成功概率的预测为

$$\begin{aligned} P_{MPE\text{-}fore} &= \max(P_{fore}(aep_1), \cdots, P_{fore}(aep_m)) \\ &= \prod_{ae_j \in aep_i} P_{fore}(ae_1 = S, \cdots, ae_f = S) \\ &= \prod_{ae_j \in aep_i} P_{fore}(ae_j = S \mid Pa(ae_j)) \end{aligned} \quad (9)$$

其中,$AE = \{ae_j \mid ae_j \in aep_i\}$, $aep_i \in AEP$, $j = |AE_i|$, $0 \leqslant P_{fore}(ae_j) \leqslant 1$.

类似地,最大成功概率的实时计算

$$\begin{aligned} P_{MPE\text{-}realtime} &= \max(P_{realtime}(aep_1), \cdots, P_{realtime}(aep_m) \mid E) \\ &= \prod_{ae_j \in aep_i} P_{realtime}(ae_1 = S, \cdots, ae_f = S, E) \\ &= \prod_{ae_j \in aep_i} P_{realtime}(ae_j = S \mid Pa(ae_j), E) \end{aligned} \quad (10)$$

其中,$AE = \{ae_j \mid ae_j \in aep_i\}$, $aep_i \in AEP$, $j = |AE_i|$, $0 \leqslant P_{realtime}(ae_j) \leqslant 1$.

3　实例分析

我们针对一个典型的网络信息系统环境[12],使用 3.2 中给出的方法构建如图 4 所示的风险概率计算 *PEG-BN* 模型,并对其进行风险概率的计算和分析.

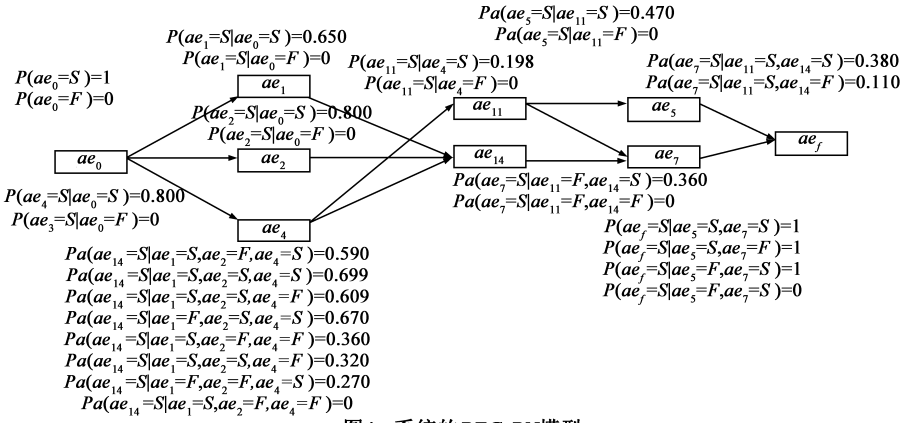

图4　系统的*PEG-BN*模型

利用建好的 *PEG-BN* 模型,对试验系统进行风险概率计算.

(1)分别计算系统安全目标的全局风险概率的预测和实时计算.得到

$$P(PEG)_{fore} = P(ae_f = S \mid Pa(ae_f)) = 0.278 \quad (11)$$

系统运行一段时间后收集系统各主机上的安全事件信息,计算在获得这些证据时系统安全目标风险概率的实时数值 $P(PEG)_{realtime}$:

$$P(s_g = S \mid Pa(s_g), ae_1 = F, ae_2 = F) = 0.175 \quad (12)$$

$$P(s_g = S \mid Pa(s_g), ae_1 = F) = 0.237 \quad (13)$$

$$P(s_g = S \mid Pa(s_g), ae_1 = S) = 0.300 \quad (14)$$

$$P(s_g = S \mid Pa(s_g), ae_1 = S, ae_2 = S) = 0.310 \quad (15)$$

$$P(s_g = S \mid Pa(s_g), ae_1 = S, ae_{18} = S) = 0.411 \quad (16)$$

式(11)表示在没有探测到系统任何原子风险渗透的执行情况时,我们依据历史经验和专家知识,认为系统的预测风险概率数值为 0.278,显然它的数值比任何一条单条风险渗透路径给安全目标带来的风险数值要大.式(12)~式(16)则表示在探测到一些原子风险渗透的执行情况时,我们综合当前观测结果、历史经验和专家知识,认为系统安全目标具有当前的风险概率数值.分别对上式进行比较,发现式(14)与式(15)之间的比较可以看出成功执行的原子风险渗透越多,我们就会认为系统的实时风险越大.同样,比较式(15)与式(16)可以看出,其它观测情况不变,当发现某条渗透路径上被成功执行的原子风险渗透越深入,我们就会认为系统安全目标的实时风险越大.显然,上述结果符合实际情况和常识经验.我们相信相较于文献[12~14]中的最大风险概率,本文中的 $P(PEG)_{fore}$ 和 $P(PEG)_{realtime}$ 概念更能贴切地反映出系统整体所面临的安全风险状况.

(2)计算系统安全目标最大成功概率的预测 $P_{MPE-fore}$,得到

$$P_{MPE-fore} = \max P_{fore}(aep_i) = P_{fore}(aep_1) = 0.105 \quad (17)$$

取 E 为"原子风险渗透 ae_2 被成功执行后实时计算数值",则

$$\begin{aligned} P_{MPE-realtime} &= \max P_{realtime}(aep_i, E) \\ &= P_{realtime}(aep_2, E) = 0.114 \end{aligned} \quad (18)$$

显然,没有获取任何证据数据时候,安全管理员预测安全目标的最大成功概率为 0.105,威胁主体最可能采取的风险渗透路径为 $aep_{MPE} = (ae_0, ae_1, ae_{14}, ae_7, ae_f)$.式(17)计算结果与文献[13]的评估结果相吻合,说明了本文所建立的 *PEG-BN* 模型的正确性.当探测到原子风险渗透 ae_2 被成功执行后,计算得到威胁主体最大成功概率为 0.114,如式(18)所示安全管理员认为威

胁主体最可能采取的实时风险渗透路径为:

$$aep_{MPE-realtime} = (ae_0, ae_2, ae_{14}, ae_7, ae_f)$$

4 结论

为评估网络系统的信息安全风险,本文构建了一个可以在定性及定量两个层次上体现脆弱性之间依赖关系的信息安全风险概率计算的贝叶斯网络模型,并以一个实例阐明了该模型在网络风险概率计算中的应用,验证了模型计算方法的正确性,与已有的风险概率计算方法相比,本文构建的贝叶斯网络模型具有以下优势:(1)模型构建速度快,同时基于贝叶斯学习的网络参数更新保障了本模型对系统描述的客观性和准确性;(2)评估结论适当反映系统风险的实际情况,即模型的计算方法更完善、更准确;(3)能够对系统进行安全事件探测之前的系统风险预测及安全事件探测过程中的系统风险实时评估,风险评估方法灵活多样.

参考文献:

[1] Swanson M, et al. Security Metrics Guide for Information Technology Systems: NIST Special Publication 800-55 [R]. NY USA: National Institute of Standards and Technology, 2003.

[2] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system[J]. IEEE Security & Privacy Magazine, 2006, 4(6): 85 – 89.

[3] Wang L, Tania Islam, Tao Long. An attack graph-based probabilistic security metric[A]. Proceedings of 22nd International Federation for Information Processing[C]. DAS USA: Springer Berlin/Heidelberg, 2008. 283 – 296.

[4] Sushil Jajodia. Topological analysis of network attack vulnerability[A]. Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security[C]. NY USA: ACM Press, 2007. 2 – 2.

[5] P Ammann, D Wijesekera, S Kaushik. Scalable, graph-based network vulnerability analysis [A]. Proceedings of the 9th ACM Conference on Computer and Communications Security [C]. Washington DC USA: ACM Press, 2002. 217 – 224.

[6] Y Liu, H Man. Network vulnerability assessment using bayesian networks[A]. SPIE′05[C]. Orlando FL USA: ACM Press, 2005. 61 – 71.

[7] Marcel Frigault, Wang L. Measuring network security using bayesian network-based attack graphs[A]. Annual IEEE International Computer Software and Applications Conference[C]. Washington USA: IEEE Computer Society, 2008. 698 – 703.

[8] Wang L, Jajodia S. Measuring the overall security of network configurations using attack graphs[A]. Proceedings of 21st IFIP WG 11.3 Working Conference on Data and Applications Security[C]. Montreal USA: Springer Berlin, 2007. 98 – 112.

[9] 张连文,郭海鹏. 贝叶斯网引论[M]. 北京:科学出版社, 2006.
Zhang Lianwen, Guo Haipeng. Introduction to Bayesian Networks[M]. Beijing: Science Publisher, 2006.

[10] 王桢珍,武小悦,刘忠. 一种基于智能规划的信息安全风险过程建模方法[J]. 电子学报, 2008, 36(12A): 76 – 80.
Wang Zhenzhen, Wu Xiaoyue, Liu Zhong. A planning-based method of risk process modeling for information security[J]. Acta Electronic Sinica, 2008, 36(12A): 76 – 80.

[11] 张金槐,刘琦,冯静. Bayes 试验分析方法[M]. 长沙:国防科大出版社, 2007.
Zhang Jinhuai, Liu Qi, Feng Jing. Bayes Method in Test Analysis[M]. Changsha: NUDT Publisher, 2007.

[12] 毛捍东. 基于逻辑渗透图模型的网络安全风险评估方法研究[D]. 长沙:国防科学技术大学研究生院, 2008.
Mao Handong. A Novel Assessment Approach Based on Logical Exploitation Graph Model for Network Security [D]. Changsha: National University of Defense Technology, 2008.

[13] Oleg Mikhail Sheyner. Scenarios Graphs and Attack Graphs [D]. Pittsburgh, Pennsylvania, USA: Department of Computer Science, Carnegie Mellon University, 2004.

[14] 陈光. 信息系统信息安全风险管理方法研究[D]. 长沙:国防科学技术大学研究生院, 2006.
Chen Guang. Research on Method of Information System Information Security Risk Management[D]. Changsha: National University of Defense Technology, 2006.

[15] 厉海涛. 基于贝叶斯网络的东两轮可靠性建模与分析[D]. 长沙:国防科学技术大学, 2008.
Li Haitao. Reliability Modeling and Analyzing of Momentum Wheel based on Bayesian Network[D]. ChangSha: National University of Defence Technology, 2008.

作者简介:

王桢珍 女,1980 年 4 月出生于安徽合肥. 国防科学技术大学信息系统与管理学院在读博士研究生. 从事信息安全及风险评估方面的有关研究.

E-mail: wangzhenzhen_2005@hotmail.com

武小悦 男,1963 年出生于山西平遥. 教授、博士生导师,研究领域包括装备系统论证与决策分析、系统工程.