文章编号:1001 - 9081(2011)03 - 0767 - 04
doi:10.3724/SP.J.1087.2011.00767

基于贝叶斯网络的可信平台控制模块风险评估模型

王 丹,周 涛,武 毅,赵文兵
(北京工业大学 计算机学院,北京 100022)
(wangdan@bjut.edu.cn)

摘 要:对可信平台控制模块(TPCM)的风险进行了分析,针对其特点和风险定量评估要求,提出了基于贝叶斯网络的 TPCM 风险评估模型。在对影响 TPCM 可信性的风险识别的基础上,根据风险之间的相关性,建立了贝叶斯风险评估网络模型;基于专家评价数据,进一步运用贝叶斯网络推理工具定量评估风险的发生概率及其影响,评估风险强度并对其进行排序,以确定整个 TPCM 中各风险的控制优先级。最后通过实例分析验证了该模型的有效性。

关键词:可信计算;可信平台控制模块;风险评估;贝叶斯网络
中图分类号:TP301.4 **文献标志码**:A

Risk assessment model for trusted platform control module based on Bayesian network

WANG Dan, ZHOU Tao, WU Yi, ZHAO Wen-bing
(*College of Computer Science, Beijing University of Technology, Beijing* 100124, *China*)

Abstract: A risk assessment model based on Bayesian network was proposed. In this model, each risk event influencing the Trusted Platform Control Module (TPCM)'s trust was analyzed. According to the relation among risks, the Bayesian network evaluation model was built. According to the evaluation from expert, Bayesian network inferring method was used to evaluate the risk probability and its influence. The whole system's risk value and risk priority were determined. An example was given to verify the model's correctness and validation.

Key words: trust computing; Trusted Platform Control Module (TPCM); risk evaluation; Bayesian network

0 引言

可信计算成为近几年信息安全领域的研究热点。与传统的安全体系不同,可信计算机是通过将可信平台模块(Trusted Platform Module, TPM),嵌入到计算机中,利用 TPM 的度量和信任传递机制来保证系统的可信。可信计算的基本思想是[1]:首先构建一个信任根,再建立一条信任链,从信任根开始到硬件平台,到操作系统,再到应用,一级认证一级,一级信任一级,把这种信任扩展到整个计算机系统,从而确保整个计算机系统的可信。信任根和信任链是可信计算平台的主要技术之一。信任链把信任关系从信任根扩展到整个计算机系统。在可信计算组织(Trusted Computing Group, TCG)的可信技术规范中,给出了可信计算机信任链的实现方法[2]。

针对 TCG 提出的可信平台模块度量起始点和信任链构建问题,我国可信计算联盟提出了可信平台控制模块(Trusted Platform Control Module, TPCM)方案,将可信度量根均设计在芯片内部,解决了可信度量根的保护问题和核心度量根的起始度量点问题。同时改进了启动模式,使得该模块作为主动设备,能够先于中央处理单元(Central Processing Unit, CPU)方案通过主动度量模式的信任链体现了可信平台控制模块作为整个平台信任根的控制特性[1-2]。

TPCM 功能的正确性是可信计算平台正确启动的核心和基础,而可信平台模块的功能测试和验证是保证可信平台模块的实现正确性以及规范一致性的重要手段,但是目前尚不存在一种有效、严格的可信平台模块测试和功能验证方法,同时可信计算组织给出的 TPM 规范是描述性的,不利于产品的开发和测试。目前,市场上已经有多个计算机厂家都在生产带有可信平台控制模块的可信计算机。为了验证这些可信计算机是否真正符合可信计算机设计规范的要求,应建立一套完整的测评指标,构建测评模型,用于对该类产品的标准符合性、功能特性和工作流程等进行测试、评估,保障其行为的可信性。

考虑到可信平台控制模块构造复杂,同时缺乏评估中所需要的实际原始数据和样本数据,这导致测评有很大难度和实际可操作性。本文以可信平台控制模块(TPCM)为研究对象,从风险分析的角度出发,将信息系统中安全风险评估的相关理论和方法应用于可信计算中,开展可信测评工作,为可信计算机的测评提供了一种新思路。目前关于开展基于风险评估理论的 TPCM 测评工作还鲜有报道。针对 TPCM 在启动和运行过程中面临风险的特点,在充分分析风险因素以及各风险因素间关联关系的基础上,构建了基于贝叶斯网络的风险网络模型,以此作为整个风险评估的基础。结合专家的知识和经验分析以及相应的计算,在得到影响系统风险的每一个因素的概率值的情况下,就可以有针对性地关注模块风险发生点,进而采取更有效的控制措施减少风险的发生。

1 相关工作

目前国内外尚没有完善的可信计算平台环境的安全测评理论,也没有相应的可信计算平台安全测评系统。如何依据产品规范中规定的目标、功能、流程、结构等方面的要求,借鉴

收稿日期:2010 - 08 - 30。 **基金项目**:国家 973 计划项目(2007CB311106)。
作者简介:王丹(1969 -),女,辽宁沈阳人,教授,博士,主要研究方向:分布式计算、可信软件; 周涛(1986 -),男,北京人,硕士研究生,主要研究方向:可信计算、可信测评; 武毅(1987 -),男,北京人,硕士研究生,主要研究方向:可信计算、可信测评。

可信计算的相关技术规范,以可信产品的可信特征测评为重点,展开研究是可信计算中可信测评亟须解决的问题之一。

国内外在可信计算平台测评方面,有关可信平台模块符合性测试[3-4]、可信平台模块形式化分析[5]等方面的研究已取得了一定的成果:文献[3-4]提出了基于状态机理论针对TPM进行的规范一致性测试研究,根据TPM规范提出测试目标,构造测试状态机,提出相应测试策略;文献[5]在分析可信平台模块目前存在的一些问题的基础上,以TPM密码子系统为例给出了该子系统的形式化规格说明,并且基于该规格说明,给出了扩展有限状态机模型。文献[6]在标准符合测试研究方面,对TPM进行了标准符合性测试,其工作中发现,目前国外主流的TPM在不同程度上都存在与标准不符合的问题,随之带来了一些相关的安全问题,如部分TPM的会话句柄和密钥句柄采用了固定值、部分TPM不能有效抵抗字典攻击、对TPM功能测试的返回码与规范定义不一致等问题。

这些研究促进了可信计算测评工作的开展。但目前尚缺少对可信计算平台进行风险评估的测评研究。信息安全的风险评估主要是针对信息、以及信息处理系统,从内因(资产、脆弱性)和外因(威胁、安全)两个方面综合判断其面临的风险[7]。风险评估是一种主动的安全防范技术。与入侵检测等技术相比,风险评估能够帮助用户更主动地识别系统所面临的潜在的安全威胁,提前评估其安全态势,从而根据需求来制定安全建议,最终避免危险事件的发生。通过利用适当的安全风险评估工具,包括定性和定量的模型和方法,确定信息资产的风险等级、风险出现的概率和风险控制的优先次序,以采取适当的安全措施减少损失。安全风险评估是信息系统安全风险管理的一个不可或缺的部分。

风险评估的主要内容包括[8]:分析平台中的资产的重要程度,评估平台面临的安全威胁、存在的脆弱性、计算威胁发生的可能等。只有通过合理的风险评估方法比较准确地对TPCM的风险进行评估,才能有针对性地控制其风险,以保证其功能的正确实现。

Pearl于1986年提出了贝叶斯网络概率模型,即使用概率理论来处理知识的不确定性,通过可视化的网络图来进行概率推理。贝叶斯网络具备很强的描述能力,能够有效地将专家经验、历史数据以及各种不完整、不确定性信息综合而提高建模效率和可信度,其在很多领域得到了广泛的应用。本文将贝叶斯网络与层次分析法相结合,提出基于贝叶斯网络的TPCM风险模糊综合评估方法,给出了模型的描述和应用。

2 基于贝叶斯网络的TPCM风险评估模型

2.1 贝叶斯网络理论

贝叶斯网络[9]是基于概率推理的数学模型,所谓概率推理,就是通过一些变量的信息来获得其他变量的概率信息的过程。假定有随机变量集合 $V=\{V_1,V_2,V_3,\cdots,V_n\}$,$v_i$ 表示 V_i 的取值。表达式 $P(v_1,v_2,\cdots,v_n)$ 表示一个联合概率,即变量 $V_1,V_2,V_3,\cdots,V_n$ 的值分别是 $v_1,v_2,\cdots,v_n$ 时的概率。可以按照一个条件概率链来表达一个联合概率,其一般形式为:

$$p(V_1,V_2,\cdots,V_k)=\prod_{i=1}^{k}p(V_i\mid V_{i-1},\cdots,V_1) \tag{1}$$

贝叶斯网络采用图形化的网络结构直观地表达变量的联合概率分布及其条件独立性,这对概率推理是非常有用的。贝叶斯网络主要由两部分组成。

1)一个具有 n 个节点的有向无环图 G。图中节点代表随机变量,节点间的有向边代表了节点间的相互关联关系。节点变量可以是任何问题的抽象。通常认为有向边表达了一种因果关系,有向图蕴含了条件独立性假设,贝叶斯网络规定图中的每个节点 V_i 条件独立于由 V_i 的父节点给定的非 V_i 后代节点构成的任何节点子集,即如果用 $A(V_i)$ 表示非 V_i 后代节点构成的任何节点子集,用 $Pa(V_i)$ 表示 V_i 的直接双亲节点,则:

$$p(V_i\mid A(V_i),Pa(V_i))=p(V_i\mid Pa(V_i)) \tag{2}$$

2)一个与每个节点相关的条件概率表(Conditional Probability Table, CPT)。条件概率表可以用 $p(V_i\mid Pa(V_i))$ 来描述,它表达了节点同其父节点的相关关系——条件概率。没有任何父节点的节点概率为其先验概率。因为有了节点及其相互关系、条件概率表,故贝叶斯网络可以表达网络中所有节点(变量)的联合概率:

$$p(V_1,V_2,\cdots,V_k)=\prod_{i=1}^{k}p(V_i\mid Pa(V_i)) \tag{3}$$

如果网络中任何一个节点状态确定,网络本身就可以利用贝叶斯公式进行正向或反向计算,从而得出网络中任意节点间的概率。图1是一个典型的贝叶斯网络,它的联合分布函数为:

$$\begin{aligned}P(V_1,V_2,V_3,V_4,V_5,V_6)=&P(V_6\mid V_5)P(V_5\mid V_3,V_2)\cdot\\&P(V_4\mid V_2)P(V_3\mid V_1)\cdot\\&P(V_2\mid V_1)P(V_1)\end{aligned} \tag{4}$$

由此可知,贝叶斯网络的推理实际上是进行概率计算,具体而言,在给定一个贝叶斯网络模型的情况下,根据已知条件,利用贝叶斯概率中条件概率的计算方法,计算出感兴趣的节点概率。

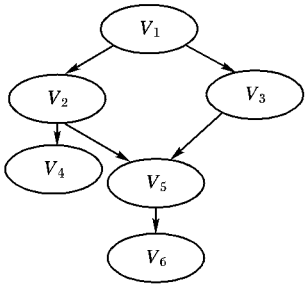

图1 贝叶斯网络

贝叶斯网络的特点在于根据观测的结果,可以很方便地对问题进行推断。一旦设计好贝叶斯网络的结构,只需要为每个节点指定其相对于给定父节点的条件概率就可以了。网络结构图和条件概率分布的结合足以指定所有变量的全联合概率分布。

2.2 TPCM风险因素的分析

为了使贝叶斯网络有更好的预测效力,模型评价指标的选择相当重要,评价指标可以看成是指标变量,每一变量都不同程度地反映了该类指标的信息,变量之间难免存在重叠、相关的关系。在测评要素体系建立的基础上,将测评要素经过分析转化为评估模型中的风险因素,作为贝叶斯网络的节点集。

通过分析TPCM功能及运行时相关流程要求,本文将以下因素作为对TPCM功能产生风险的10个影响因素,即:1)可信/异常/非可信工作模式运行阻塞;2)密码算法漏洞;3)自定义内容漏洞;4)指令接口漏洞;5)敏感数据泄露;6)硬件基本属性不符;7)日志安全漏洞;8)可信度量根(Root of Trust for Measurement, RTM)组成电路故障;9)完整性度量功能问题;10)命令包与应答包收发运行阻塞。

再经过分析得知这些风险因素之间存在一定程度上的依赖关系,分析结果如表 1 所示。

表 1　TPCM 风险因素分析

风险因素	将对其产生影响的因素
密码算法漏洞	敏感数据泄露、日志安全漏洞、完整性度量功能问题
自定义内容漏洞	敏感数据泄露、日志安全漏洞
指令接口漏洞	敏感数据泄露、日志安全漏洞、完整性度量功能问题
敏感数据泄露	命令包与应答包收发运行阻塞
硬件基本属性不符	可信/异常/非可信工作模式运行阻塞、RTM 组成电路故障
日志安全漏洞	可信/异常/非可信工作模式运行阻塞
RTM 组成电路故障	完整性度量功能问题

同时要确定节点的状态和取值范围,在大量的应用经验指导下,本文确定在对可信计算平台进行风险评估时,每个节点的状态为“prob”、和“not”,即“风险因素产生问题”和“风险因素不产生问题”;对于节点取值,为了适应模型应用于风险概率发生预测和每个节点产生问题的概率计算,确定取值区间为[0,1]。

2.3　贝叶斯网络模型构建

假设决定风险评估模型中的风险因素由 n 个因素组成,本文则建立一个 $n+1$ 个节点的贝叶斯网络,其中 n 个节点对应评估模型中的 n 个风险因素,另一个节点作为风险发生的概率输出。由于在实际应用过程中缺少 TPCM 使用的历史数据和经验数据的收集,因此采用专家评估的方法获得网络模型中节点间的因果关系和节点间的条件概率分布。根据已经确定的节点之间的因果关系或先验依赖关系确定网络结构,而大多数情况下由专家知识获得的贝叶斯网络结构是相对最优的贝叶斯网络结构。本文用同样的方法再确定条件概率表,其中没有父节点的节点给出其先验概率,有父节点的节点则给出其在父节点影响下的条件概率,概率取值均在区间[0,1]内。

由于本文定义的 TPCM 的风险因素由 10 个因素组成,因此需要建立一个有 11 个节点的贝叶斯网络,其中 10 个节点对应评估模型中的 10 个风险因素,另一个节点作为风险发生的概率输出,即 Problem 节点。风险因素表如表 2 所示。

表 2　贝叶斯网络各节点对应的风险因素

编号	风险因素
V_1	可信/异常/非可信工作模式运行阻塞
V_2	密码算法漏洞
V_3	自定义内容漏洞
V_4	指令接口漏洞
V_5	敏感数据泄露
V_6	硬件基本属性不符
V_7	日志安全漏洞
V_8	RTM 组成电路故障
V_9	完整性度量功能问题
V_{10}	命令包与应答包收发运行阻塞
Problem(V_{11})	TPCM 功能产生问题

通过上一步分析,得到的风险因素之间的关系如图 2 所示。

进一步,结合专家评估和经验分析等,给出风险因素的条件概率分布,假设各概率值如表 3 所示。

根据条件概率表和网络结构图,利用式(4)描述的方法即可计算出 TPCM 的风险概率:

$$p(V_1,V_2,\cdots,V_{11})=\prod_{i=1}^{11}p(V_i\mid Pa(V_i))=p(\text{Problem}\mid V_{10},V_9,V_1)p(V_{10}\mid V_5)p(V_9\mid V_8,V_4,V_2)p(V_1\mid V_7,V_6)p(V_5\mid V_4,V_3,V_2)p(V_7\mid V_4,V_3,V_2)p(V_8\mid V_6)p(V_4)p(V_3)p(V_2)p(V_6) \tag{5}$$

同时也可计算出每个节点的概率,能够确定影响系统风险的关键因素排序(具体过程略)。

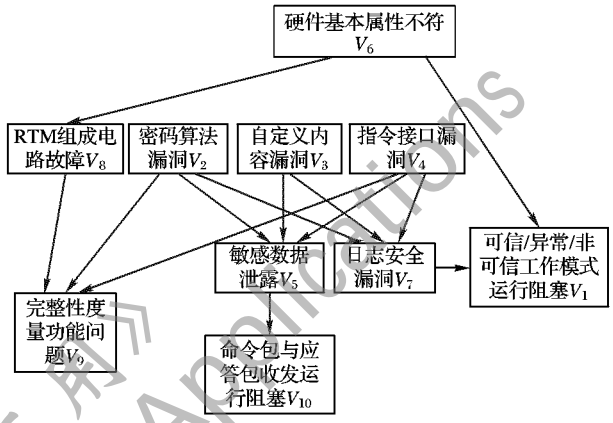

图 2　风险因素因果关系

3　实验验证和结果分析

Hugin Expert 是一款商业软件,它包括一系列产品并提供 C、C ++、Java、. Net 语言的应用程序开发接口(Application Program Interface, API)支持,也可作为单个工具使用,支持面向对象的贝叶斯网络展示。本文选取其免费版软件 Hugin Lite 来演示验证本文提出的基于贝叶斯网络的 TPCM 风险评估模型。依照以上分析结果建立贝叶斯网络,如图 3 所示。

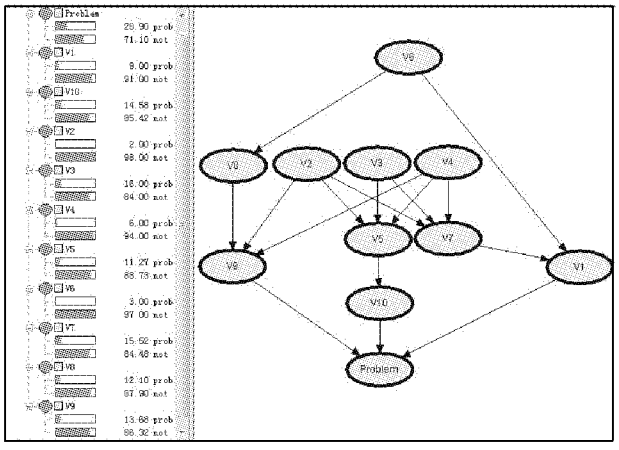

图 3　在 Hugin 软件中建立的网络拓扑图

以节点 V_7 为例,通过专家评估得出风险因素及其条件概率表输入,如图 4 所示。

V7

V4	prob				not			
V3	prob		not		prob		not	
V2	prob	not	prob	not	prob	not	prob	not
prob	0.55	0.4	0.45	0.2	0.5	0.4	0.2	0.1
not	0.45	0.6	0.55	0.8	0.5	0.6	0.8	0.9

图 4　V_7 的条件概率表输入

按照同样的方法,最后整个 TPCM 的各风险因素的结果分析如表 4 所示。

表 3 专家评估风险因素条件概率分布表

概率名称	概率值
P(硬件基本属性有不符)	0.03
P(密码算法有漏洞)	0.02
P(自定义内容有漏洞)	0.16
P(指令接口有漏洞)	0.06
P(RTM 组成电路产生故障|硬件基本属性有不符)	0.80
P(RTM 组成电路产生故障|硬件基本属性没有不符)	0.10
P(敏感数据有泄露|密码算法有漏洞,自定义内容有漏洞,指令接口有漏洞)	0.90
P(敏感数据有泄露|密码算法没有漏洞,自定义内容有漏洞,指令接口有漏洞)	0.70
P(敏感数据有泄露|密码算法有漏洞,自定义内容没有漏洞,指令接口有漏洞)	0.65
P(敏感数据有泄露|密码算法有漏洞,自定义内容有漏洞,指令接口没有漏洞)	0.40
P(敏感数据有泄露|密码算法没有漏洞,自定义内容没有漏洞,指令接口有漏洞)	0.20
P(敏感数据有泄露|密码算法没有漏洞,自定义内容有漏洞,指令接口没有漏洞)	0.35
P(敏感数据有泄露|密码算法有漏洞,自定义内容没有漏洞,指令接口没有漏洞)	0.25
P(敏感数据有泄露|密码算法没有漏洞,自定义内容没有漏洞,指令没接口有漏洞)	0.05
P(日志安全有漏洞|密码算法有漏洞,自定义内容有漏洞,指令接口有漏洞)	0.55
P(日志安全有漏洞|密码算法没有漏洞,自定义内容有漏洞,指令接口有漏洞)	0.40
P(日志安全有漏洞|密码算法有漏洞,自定义内容没有漏洞,指令接口有漏洞)	0.45
P(日志安全有漏洞|密码算法有漏洞,自定义内容有漏洞,指令接口没有漏洞)	0.50
P(日志安全有漏洞|密码算法没有漏洞,自定义内容没有漏洞,指令接口有漏洞)	0.20
P(日志安全有漏洞|密码算法没有漏洞,自定义内容有漏洞,指令接口没有漏洞)	0.40
P(日志安全有漏洞|密码算法有漏洞,自定义内容没有漏洞,指令接口没有漏洞)	0.20
P(日志安全有漏洞|密码算法没有漏洞,自定义内容没有漏洞,指令没接口有漏洞)	0.10
P(可信/异常/非可信工作模式运行有阻塞|硬件基本属性有不符,日志安全有漏洞)	0.90
P(可信/异常/非可信工作模式运行有阻塞|硬件基本属性没有不符,日志安全有漏洞)	0.15
P(可信/异常/非可信工作模式运行有阻塞|硬件基本属性有不符,日志安全没有漏洞)	0.88
P(可信/异常/非可信工作模式运行有阻塞|硬件基本属性没有不符,日志安全没有漏洞)	0.05
P(完整性度量功能有问题|密码算法有漏洞,指令接口有漏洞,RTM 组成电路有故障)	0.95
P(完整性度量功能有问题|密码算法没有漏洞,指令接口有漏洞,RTM 组成电路有故障)	0.90
P(完整性度量功能有问题|密码算法有漏洞,指令接口没有漏洞,RTM 组成电路有故障)	0.85
P(完整性度量功能有问题|密码算法有漏洞,指令接口有漏洞,RTM 组成电路没有故障)	0.60
P(完整性度量功能有问题|密码算法没有漏洞,指令接口没有漏洞,RTM 组成电路有故障)	0.80
P(完整性度量功能有问题|密码算法没有漏洞,指令接口有漏洞,RTM 组成电路没有故障)	0.40
P(完整性度量功能有问题|密码算法有漏洞,指令接口没有漏洞,RTM 组成电路没有故障)	0.10
P(完整性度量功能有问题|密码算法没有漏洞,指令接口没有漏洞,RTM 组成电路没有故障)	0.02
P(命令包与应答包收发运行有阻塞|敏感数据有泄露)	0.90
P(命令包与应答包收发运行有阻塞|敏感数据没有泄露)	0.05
P(系统发生风险|命令包与应答包收发运行有阻塞,完整性度量功能有问题,可信/异常/非可信工作模式运行有阻塞)	0.99
P(系统发生风险|命令包与应答包收发运行没有阻塞,完整性度量功能有问题,可信/异常/非可信工作模式运行有阻塞)	0.95
P(系统发生风险|命令包与应答包收发运行有阻塞,完整性度量功能没有问题,可信/异常/非可信工作模式运行有阻塞)	0.98
P(系统发生风险|命令包与应答包收发运行有阻塞,完整性度量功能有问题,可信/异常/非可信工作模式运行没有阻塞)	0.88
P(系统发生风险|命令包与应答包收发运行没有阻塞,完整性度量功能没有问题,可信/异常/非可信工作模式运行有阻塞)	0.90
P(系统发生风险|命令包与应答包收发运行没有阻塞,完整性度量功能有问题,可信/异常/非可信工作模式运行没有阻塞)	0.70
P(系统发生风险|命令包与应答包收发运行有阻塞,完整性度量功能没有问题,可信/异常/非可信工作模式运行没有阻塞)	0.80
P(系统发生风险|命令包与应答包收发运行没有阻塞,完整性度量功能没有问题,可信/异常/非可信工作模式运行没有阻塞)	0.05

由此得到模型中每一个节点的概率,同时也得到了节点概率的排列顺序,即模型中的风险因素对系统风险影响程度的排序。可以看出,其中影响最大的因素为“自定义内容漏洞”,其次是“日志安全漏洞”、“命令包与应答包收发运行阻塞”、“完整性度量功能问题”、“敏感数据泄露”、“可信/异常/非可信工作模式运行阻塞”,影响最小的为“RTM 组成电路故障”等。

在使用 Hugin 工具模拟过程中,双击左侧列表的“Problem”节点的“prob”项,即可计算整个系统发生风险的概率,为 0.289 024,即与“Problem”节点本身的概率相同。再点击该软件的按钮,计算得知风险产生时最有可能出现的组合为:V_8V_9,其概率为 0.032 434,即系统产生风险时,最有可能的组合为“RTM 组成电路故障”和“完整性度量功能问题”,同时还有较大可能存在的情况是“可信/异常/非可信工作模式运行阻塞”、“命令包与应答包收发运行阻塞”、“敏感数据泄露”和“自定义内容漏洞”。

如果某些节点的评估概率发生改变,只需要调整条件概率表中的相应数值,然后重新训练网络模型,而无需改变网络结构。

(下转第 789 页)

以概率 0.346 选择 $s_d^1(\delta_{1,1})$,以概率 0.291 选择 $s_d^6(\delta_{6,4})$,为最优防御策略。根据 3.3 节可得到实验网络的最大攻防策略集 *maxASS* 及 *maxDSS*。

$$\begin{aligned} maxASS = \{&\{O_0\cdot p_0, t_1, O_1\cdot p_1, t_9, O_7\cdot p_8, t_{17}, O_6\cdot p_6; \cdots; \\ &O_0\cdot p_0, t_1, O_1\cdot p_1, t_{10}, O_{57}\cdot p_{58}, t_{18}, O_6\cdot p_6;\}, \\ &\{O_0\cdot p_0, t_2, O_2\cdot p_2, t_{11}, O_6\cdot p_6; O_0\cdot p_0, t_3, \\ &O_2\cdot p_2, t_{11}, O_6\cdot p_6; O_0\cdot p_0, t_4, O_3\cdot p_3, t_{12}, \\ &O_6\cdot p_6; O_0\cdot p_0, t_5, O_3\cdot p_3, t_{12}, O_6\cdot p_6;\}, \\ &\{O_0\cdot p_0, t_6, O_4\cdot p_4, t_{13}, O_7\cdot p_8, t_{17}, O_6\cdot p_6; \cdots; \\ &O_0\cdot p_0, t_6, O_4\cdot p_4, t_{14}, O_{57}\cdot p_{58}, t_{18}, O_6\cdot p_6;\}, \\ &\{O_0\cdot p_0, t_7, O_4\cdot p_4, t_{13}, O_7\cdot p_8, t_{15}, O_5\cdot p_5, t_{19}, \\ &O_6\cdot p_7; \cdots; O_0\cdot p_0, t_7, O_4\cdot p_4, t_{14}, O_{57}\cdot p_{58}, t_{16}, \\ &O_5\cdot p_5, t_{19}, O_6\cdot p_7;\}\} \end{aligned}$$

$$maxDSS = \{s_d^1(\delta_{1,1}), s_d^6(\delta_{6,4}), \{s_d^7(\delta_{9,8}, \delta_{13,8}), s_d^8(\delta_{10,58}, \delta_{14,58}), \cdots\}\}$$

最大防御策略反映了防御者应首先考虑修复防火墙、FTP 服务器以及内部局域网中各用户机上存在的漏洞。

由上述分析可以看出,高水平更倾向于利用攻击复杂度较高的攻击方式,这是因为它们的阻止率较低,且某些漏洞尚未发布安全补丁(如 38115),更易于避免防御阻拦。同时高/低水平攻击者均偏爱于选择节点重要度和关联度高的节点进行攻击,以便获得更高的获益和更多的备用选择策略。由于通过内网用户集群对 DB 服务器的访问来窃取企业资料在整个策略空间中占主要地位,而限制主机访问权的防御负面成本较高,因此提前修复用户机上的漏洞为最佳策略,可有效阻止 98.3% 的攻击路径。防火墙的节点重要度高且通过更改其过滤设置可以直接攻击内网任意主机以及备份服务器,因此 $s_d^1(\delta_{1,1})$ 也具有高选择概率。由于 FTP 对内网用户集群具有访问权,通过 FTP 可以攻击选择任意一个用户机为跳板,因此它比 Web 服务器具有更多的攻击选择且攻击危害更大,则首先应考虑防御策略 $s_d^6(\delta_{6,4})$。

5　结语

针对复杂网络系统上攻防策略研究中的不足,本文提出了一种新的攻防模型结构——基于粗糙扩展对象 Petri 网的攻防对峙模型,在此基础上将粗糙集理论与传统贝叶斯博弈相结合,在攻防策略空间上划分等价类,通过从各等价类中提取特征攻击策略来去除复杂网络中的冗余信息,缩减策略空间规模,从而令博弈论在网络攻防研究中的应用更为广泛。

由于大型复杂网络中将有多个防御 Agent 协作防御的情形,因此下一步研究工作可放在多防御 Agent 合作博弈共同对抗攻击者行为上,将合作博弈与本文的竞争博弈相结合。

参考文献:

[1] LYE K-W, WING J. Game strategies in network security [R]. Pittsburgh: Carnegie Mellon University, 2002.

[2] BURKE D A. Towards a game theory model of information warfare [R]. Dayton, OH: Airforce Institute of Technology, 1999.

[3] STAKHANOVA N, BASU S, WONG J. A Taxonomy of intrusion response systems [J]. International Journal of Information and Computer Security, 2007, 1(1/2): 169 - 184.

[4] 石进,陆音,谢立. 基于博弈理论的动态入侵响应[J]. 计算机研究与发展,2008,45(5):747 - 757.

[5] 张少俊,李建华,陈秀真,等. 基于动态博弈理论的分布式拒绝服务攻击防御方法[J]. 上海交通大学学报,2008,42(2):198 - 201.

[6] 郭渊博,马建峰. 基于博弈论框架的自适应网络入侵检测与响应[J]. 系统工程与电子技术,2005,27(5):914 - 917.

[7] 姜伟,方滨兴,田志宏,等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,2009,32(4):817 - 825.

[8] 张永铮,云晓春,胡铭曾. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报,2004,25(7):107 - 114.

[9] 王纯子,黄光球. 基于脆弱性关联模型的网络威胁分析[J]. 计算机应用,2010,30(11):3046 - 3050.

(上接第 770 页)

表 4　风险因素(节点)概率表

编号	风险因素	风险概率
V_1	可信/异常/非可信工作模式运行阻塞	0.090 047 6
V_2	密码算法漏洞	0.02
V_3	自定义内容漏洞	0.16
V_4	指令接口漏洞	0.06
V_5	敏感数据泄露	0.112 721
V_6	硬件基本属性不符	0.03
V_7	日志安全漏洞	0.155 201
V_8	RTM 组成电路故障	0.121
V_9	完整性度量功能问题	0.136 801
V_{10}	命令包与应答包收发运行阻塞	0.145 813
Problem(V_{11})	TPCM 功能产生问题	0.289 024

4　结语

本文利用贝叶斯网络建立了 TPCM 的风险评估模型,其评估结果为风险管理决策者制定风险控制策略提供了科学的依据。该方法在考虑风险发生概率和风险影响两方面因素的同时,还考虑了风险之间的关系及其相互作用。在得知影响系统风险的每一个因素的概率值的情况下,就可以有针对性地关注模块风险发生点,进而采取更有效的控制措施或者更有把握地选择接受风险。

由于现有的贝叶斯网络没有考虑原因节点影响结果节点的滞后时间,从而只适用于静态分析。同时,随着对 TPCM 风险因素分析的深入,如何提高进一步结合专家评估和经验分析等,准确给出各风险因素的条件概率,不断调整、优化贝叶斯网络模型,得到更准确的评估结果也是需要进一步分析和研究的问题。

参考文献:

[1] 沈昌祥,张焕国,王怀民,等. 可信计算的研究与发展[J]. 中国科学 F 辑:信息科学,2010,40(2):139 - 166.

[2] 张焕国,严飞,徐明迪,等. 可信计算平台测评理论及其关键技术研究[J]. 中国科学 F 辑:信息科学,2010,40(2):167 - 188.

[3] 詹静,张焕国. 可信平台模块自动化测试研究[J]. 计算机研究与发展,2009,46(11):1839 - 1846.

[4] 詹静,张焕国,徐士伟,等. 基于状态机理论的可信平台模块测试研究[J]. 武汉大学学报:信息科学版,2008,33(10):1067 - 1069.

[5] 陈小峰. 可信平台模块的形式化分析和测试[J]. 计算机学报,2009,32(4):646 - 653.

[6] SADEGHI A, SELHORST M, STUEBLE C, *et al*. TCG inside? A note on TPM Specification compliance [C]// Proceedings of the First ACM Workshop on Scalable Trusted Computing. New York: Association for ComPuting Machinery, 2006: 47 - 56.

[7] 冯登国,张阳,张玉清. 信息安全风险评估综述[J]. 通信学报,2004,25(7):10 - 18.

[8] 吴亚飞,李新友,禄凯. 信息安全风险评估[M]. 北京:清华大学出版社,2007.

[9] 蒋国萍,陈英武. 基于面向对象贝叶斯网络的软件项目风险评估[J]. 系统工程与电子技术,2005,27(2):353 - 356.