软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(7):1880−1898 [doi: 10.3724/SP.J.1001.2012.04112]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种给定脆弱性环境下的安全措施效用评估模型*

吴 迪[1,2,4+], 冯登国[1], 连一峰[1,3], 陈 恺[1]

[1](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

[2](中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

[3](信息安全共性技术国家工程研究中心,北京 100190)

[4](信息网络安全公安部重点实验室(公安部第三研究所),上海 201204)

Efficiency Evaluation Model of System Security Measures in the Given Vulnerabilities Set

WU Di[1,2,4+], FENG Deng-Guo[1], LIAN Yi-Feng[1,3], CHEN Kai[1]

[1](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](State Key Laboratory of Information Security, Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

[3](National Engineering Research Center for Information Security, Beijing 100190, China)

[4](Key Laboratory of Information Network Security of Ministry of Public Security (The Third Research Institute of Ministry of Public Security), Shanghai 201204, China)

+ Corresponding author: E-mail: wudi_dizi@163.com, http://www.isacs.ac.cn

Wu D, Feng DG, Lian YF, Chen K. Efficiency evaluation model of system security measures in the given vulnerabilities set. *Journal of Software*, 2012,23(7):1880−1898 (in Chinese). http://www.jos.org.cn/1000-9825/4112.htm

Abstract: The efficiency evaluation of information system's security measures is important to improve the information system security. Conventional evaluation methods did not consider the interactivity and inter-influence of the business dataflow, attack flow, and security measures factors when evaluating system's security measures. Thus, they can not ensure the effectiveness of the evaluation process and results. An efficiency evaluating approach for information system's security measures under the given vulnerability set is presented in this paper. It employs colored Petri-Net tools to uniform modeling and simulates the interaction among the system's workflow, attack flow, and security measures. Based on this modeling method, the paper proposes an inter-nodes vulnerabilities exploiting graph generation algorithm and improves Dijkstra algorithm to identify shortest-attack-paths, which can cause damage to the information system's security attributes. Next, it constructs a hierarchical model to evaluate the effectiveness of the security measures and employs a gray multiple attributes decision-making algorithm to choose the best effectiveness-improving alternatives. By using this approach, the dependency on evaluators' subjectivity in the process of the evaluation of information system's security measures can be alleviated. Also, it helps to ensure the consistency and traceability of the evaluation results. Finally, a practical Web business system is taken as a case study to validate the correctness and effectiveness of the evaluation model.

* 基金项目: 国家自然科学基金(61100226); 国家高技术研究发展计划(863)(2009AA01Z439, 2011AA01A203); 北京市自然科学基金(4122085); 信息网络安全公安部重点实验室(公安部第三研究所)开放基金(C10606)

收稿时间: 2010-11-17; 修改时间: 2011-04-28; 定稿时间: 2011-09-01

Key words: information security measures; efficiency evaluation; colored Petri net; shortest-attack-path; multiple attributes decision-making

摘 要: 评估信息系统安全措施效用是改进系统信息安全绩效的一条重要途径.传统方法在评估安全措施效用时并没有考虑业务数据流、攻击流和安全措施要素之间的相互作用和影响,无法保证评估过程和结果的有效性.提出了一种给定脆弱性环境下的信息系统安全措施效用评估方法,应用颜色 Petri 网为系统业务数据流、攻击流和安全措施要素进行统一建模.通过设计节点间脆弱性利用图生成算法和改进的 Dijkstra 算法识别所有可能破坏信息系统安全属性的最短攻击路径,使用层次评价模型评估系统安全措施的效用.给出了一种基于多属性决策的系统最优信息安全效用提升方案选择算法.改善评估过程对人员主观经验的依赖问题,有助于保证评估结果的一致性和可追溯性.以一个具体的 Web 业务系统为例进行实验,验证了所提出的模型和方法的正确性和有效性.

关键词: 信息安全措施;效用评估;颜色 Petri 网;最短攻击路径;多属性决策

中图法分类号: TP309 **文献标识码**: A

信息系统承载着组织等重要业务功能,为保障信息系统安全性,组织往往会在系统中应用各种安全措施.但如何验证所实施的安全措施是否依据安全要求正确地执行了其保护功能?如何评估所实施的安全措施抵御信息系统中各种攻击(包括脆弱性利用攻击)的效果?这些都是评估系统安全性时需要解决的重要问题,也是影响安全绩效和决策的重要因素[1].因此,如何评估信息安全措施的效用(efficiency of information system's security measures,简称安全措施效用)已引起国内外研究人员的关注,正成为网络安全领域的研究热点.

安全措施效用表示系统运营环境中控制措施的实施、运行和获取结果与系统安全要求的符合程度[2].评估安全措施效用的重点是评估系统安全措施抵御攻击的安全功能强度,需要确定在已知或发现的脆弱性条件下,分析系统是否能被诱发产生或利用安全脆弱性的行为,以评估系统安全措施在攻击状态下有效保障业务系统安全的能力[1].继承传统评估过程的性质,安全措施效用评估的有效性同样依赖于:1) 数据源是否基于系统安全要求且便于获取、可测量;2) 测量方法的客观性和可重复性;3) 评估结果的一致性和是否对安全管理活动有指导作用等方面[3,4].众所周知,一个业务系统的安全并不是由单个安全措施来保障的,而是由部署在业务系统中的多种安全措施的有效协作来保障.在当前日益复杂的、分布式和异构网络环境中,对部署在信息系统中各种安全措施的整体安全保障效果进行安全措施效用评估,已成为评估系统安全性亟待解决的问题.

建模是保证安全措施效用评估过程规范性和评估结果一致性的重要途径,但信息系统本身的复杂性和动态性难以全面抽象描述,而且模型层次与实际应用的矛盾使安全措施效用评估建模难度加剧.抽象层次越高,建模越简单,但模型分析结果与实际应用差距越大;反之,则建模越复杂.因此,需要均衡二者的矛盾来确定建模的抽象层次.目前,根据模型的不同抽象层次和粒度,可以通过分析系统安全策略、设计部署机制和管理应用措施等方面的信息来评估安全措施效用.文献[5,6]建模分析了安全策略的正确性和一致性,但无法验证安全措施是否正确实施了策略以及验证安全措施的实际效果.文献[7]基于安全要求评估系统风险并选择安全措施,建模过程关注系统脆弱性与安全要求的关系,但由于依赖系统的具体功能实现,不便应用且结果复杂.文献[8–11]基于系统设计中的脆弱性,分析系统可能面临的威胁,评价系统安全措施的收益与效果.文献[12]提出综合系统运营的安全需求和安全工程的生命周期思想的概念测试结构,为评估安全措施效用提出一种研究思路.文献[13]基于系统风险评估信息,给出了计算安全措施成本-收益的过程.文献[14]中给出的安全控制措施有效性分析测量模型,综合考虑了系统的安全管理信息,但缺少方法的支撑.

降低评估人员主观因素影响,以保证安全措施效用评估过程的规范性和结果一致性,是信息安全评估领域的研究难点.文献[5]应用颜色 Petri 网对系统访问控制数据流的处理功能建模,关注系统措施执行安全策略的正确性,但未考虑系统脆弱性和攻击对安全措施效用的影响.文献[6,8–11]基于攻击图生成技术,分别结合逻辑编程、多属性决策或动态 Bayesian 网络等分析方法,缓解攻击图方法自身局限性导致的分析过程和结果复杂问题.文献[7]综合运用元模型、脆弱性分析和风险评估方法建模,根据系统安全要求建立评估安全措施对抗脆弱性利

用效果的框架,但在进行安全措施分析、典型攻击模板建立和脆弱性传播规则分析时过于依赖于评估人员的主观经验.文献[11−13]集成信息安全风险评估理念给出结构化评估过程和模型,可操作性方面还有待完善.根据信息安全风险管理思想,为保障美国联邦政府信息系统的安全性,文献[1]用于指导系统安全绩效评估的实施,量化评价安全措施的正确性和有效性,但缺乏有效的评价和分析模型.文献[2]对选择安全控制措施提供指导,但并没有给出评价安全控制措施效用的方法.

以往的研究表明,基于系统脆弱性分析安全措施抵御脆弱性利用攻击的能力是评估安全措施效用的一种可行思路.系统业务、脆弱性、攻击和安全措施是进行安全措施效用评估的重要因素,它们相互作用、相互影响,导致安全措施效用分析过程复杂.以往的研究方法仍存在以下问题:1) 对安全措施的实际应用情况分析不足.安全策略为实现业务系统安全目标而设计,安全策略由业务系统中的各种安全措施来实施,安全措施效用不仅表现在正常业务应用过程中对身份认证和访问控制等安全策略的执行能力上,同时还表现在业务系统由于自身脆弱性问题受到攻击时抵御各种攻击的能力上.目前的研究工作无法验证安全措施在业务系统遭受攻击时是否仍然能够正确实现其安全目标;2) 以往的研究工作从系统脆弱性角度来评估安全措施效用,采用传统攻击图模型来对攻击者能力建模,缺乏对影响安全措施效用的各要素的相互作用和影响分析,所采用的评估方法存在可扩展性差、结果不易分析和理解等局限性;3) 安全措施效用评估过程中,在数据分析、参数设置、规则分析和结果应用等方面对评估人员主观经验的依赖性较高,影响了评估过程的规范性和结果一致性.

本文提出了一种安全措施效用评估框架和评估模型,通过分析业务系统由于自身脆弱性问题受到攻击时安全措施抵御各种攻击的能力,以定性定量相结合的方法来评估安全措施效用.综合考虑影响系统安全措施效用的各要素,提出了对系统业务、安全措施、脆弱性和攻击流进行统一建模的层次化 CPN(颜色 Petri 网)模型,实现各要素相互作用的影响分析;基于分析结果构建节点间脆弱性利用图,基于攻击成功率识别出攻击者获取某种可能危害到业务系统安全属性的攻击能力节点的最短攻击路径.通过安全措施效用层次评价模型评估这些穿透系统安全措施的最短攻击路径对系统安全属性的影响程度,计算安全措施效用.文中的评估框架和模型简化了安全措施效用分析过程,一定程度上减少了评估过程中人为主观因素的影响.最后,基于多属性决策的系统安全效用提升最优方案选择方法,指导系统安全管理活动.

1 安全措施效用评估框架与相关定义

组织在系统中应用安全措施的目的是抵御攻击,降低风险,为系统业务提供安全保障.所以,系统安全措施效用具体表现在以下两方面:1) 降低攻击者利用脆弱性非授权访问系统资源的成功率;2) 维护系统对象安全属性以满足安全要求.根据容侵的网络安全保障思想,安全管理员可以根据业务系统安全要求,重点考虑支撑业务系统安全运行的关键对象的安全.即,业务系统是安全的,当且仅当攻击者无法获取所有可能影响到业务系统私密性、完整性和可用性安全属性的关键对象权限.

图 1 为系统安全措施效用评估总体框架图.基于给定的系统脆弱性信息,以确保所有可能影响到业务系统安全属性的关键对象权限的安全(未被攻击者获取)来表示被评估系统的安全要求,并建立安全措施效用评价基准;同时,根据被评估系统的拓扑结构、业务流和配置信息等系统信息,应用 CPN 建模工具对系统业务、脆弱性、攻击和安全措施等要素进行统一定义和建模,建立攻击者能力分析模型,实现对各要素之间的相互作用分析,得到所有可能成功穿透系统安全措施的脆弱性利用攻击数据.根据攻击者能力分析模型仿真输出的脆弱性利用结果,构建节点间脆弱性利用图,利用改进的最短路径识别算法 Dijkstra 识别攻击者获取各种攻击能力的最短攻击路径,并计算各最短攻击路径的利用成功率,作为攻击者实施攻击所需的最小代价.根据系统分析过程得出的效用评价基准,利用层次评价模型综合评估系统安全措施效用.结合系统安全措施效用结果,针对不同的效用提升备选方案,应用基于多属性的最优方案选择算法评价各备选方案的安全措施效用,指导选取最优方案以改进系统安全措施效用.

业务系统数据流是刻画系统业务应用、安全措施和攻击之间相互作用的基本要素,基于业务系统数据流不仅可以分析业务应用对资源的访问控制是否符合安全要求,也可以分析系统中安全措施对抗脆弱性利用攻击

的能力.因此,文中以数据流为粒度,对系统业务、攻击实施和安全措施的数据流处理功能进行统一建模,建立攻击者能力分析模型.基于系统脆弱性环境信息,对实际攻击流,自动分析系统业务流、安全措施和攻击流之间的相互作用进行建模分析.

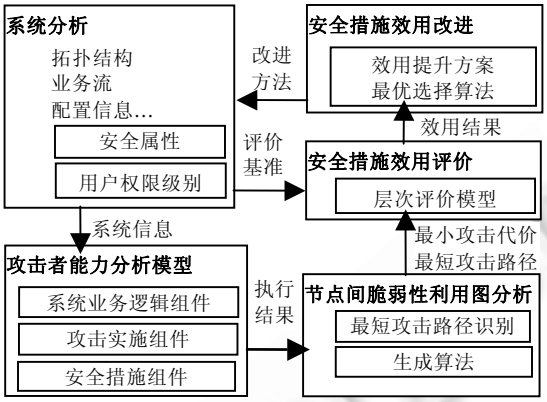


Fig.1 Efficiency evaluation framework for the information system's security measures

图 1 信息系统安全措施效用评估框架

在实际攻击过程中,攻击者能力体现为利用业务系统中存在的脆弱性非法获取系统访问权限.而且这种攻击能力会在攻击过程中逐渐增长,表现为如下两个方面:1) 攻击者在获取某一主机的普通用户权限后,可利用本地权限提升脆弱性,将攻击者权限提升为超级用户权限;2) 攻击者在获得某一主机用户权限后,可利用其他主机的脆弱性,进一步获取其他主机的用户权限.攻击能力不仅能为攻击者实施进一步攻击提供准备条件,更重要的是,它能让攻击者具备对支撑业务系统的关键节点实施破坏的能力.通过分析攻击过程中攻击者所获得的攻击能力是否影响到业务系统安全运行,可以验证系统安全措施是否发挥预期的安全保障作用.通过评估攻击者能力对业务系统安全的影响程度,是评价安全措施效用的一条有效途径.为了在建模中准确描述攻击者的攻击能力增长过程,给出攻击者能力定义如下.

定义 1(攻击者能力). 攻击者能力是指攻击者当前在系统各终端上所获取的用户权限的集合:

$$AttackCapability=\{\langle Hostname,Priv\rangle\},Hostname\in HOSTS,Priv\in PRIVILEGES,$$

其中,$\langle Hostname,Priv\rangle$表示攻击者在终端 *Hostname* 上获得了 *Priv* 级别的用户权限,*HOSTS* 为被评估系统所有终端的集合,*PRIVILEGES* 是被评估系统用户权限级别集合,可以取 *NONE*,*USER* 和 *ROOT* 这 3 个值.当攻击者在攻击过程中攻击能力逐渐增长时,相应的$\langle Hostname,Priv\rangle$值将得到及时更新.

攻击图是一种常用的基于脆弱性信息分析系统可能遭受的攻击和系统安全状态变化的方法.传统攻击图用有向边表示某单一攻击行为引起系统的状态转换,可以显式表示攻击者从初始状态开始,不断利用目标系统脆弱性实施攻击的所有可能攻击路径.但其中的攻击路径随目标系统中主机规模与脆弱性数目的乘积呈指数增长,可扩展性较差、分析过程复杂[15].为了解决传统攻击图的组合爆炸问题,在分析模型中引入攻击者能力单调递增假设,基于属性方法提出属性攻击图,以节点表示脆弱性利用条件(系统属性)和原子攻击,有向边表示节点间因果关系,明确了攻击过程中的推理分析,隐式描述系统所有可能的攻击路径[16].虽然属性攻击图克服了分析过程中的组合空间爆炸问题,但其节点数量和有向边数量随主机规模呈多项式增长,分析攻击者的攻击能力,即成功攻击应获取的终端特定用户权限,计算所需最小代价的过程仍较为复杂.文中提出一种节点间脆弱性利用图,节点表示攻击者在某终端(主机)上可能获取的权限级别,有向边表示攻击者为获取末端点对应终端权限级别所应实施的一次脆弱性利用动作.与属性攻击图不同,节点间脆弱性利用图中一对有序节点之间可能存在多条有向边,这表示攻击者在获得首节点对应终端权限级别后,任意选取从该首节点发出的一条有向边就能够获得末节点对应终端相应的权限级别.从攻击者所获得的攻击能力角度来看,有序节点对之间的多条有向边是

等价的,因此,在分析攻击者获取攻击能力的最小代价时,可以将等价的有向边进行归并进而简化属性攻击图.这使得节点间脆弱性利用图中的节点数量和有向边数量随主机规模呈线性增长,具有比属性攻击图更好的可扩展性.而且,简化后的节点间脆弱性利用图可以利用图论中的最短路径算法计算攻击者获取攻击能力所需的最小代价,有效降低安全措施效用评估的计算复杂度.下面给出节点间脆弱性利用图及相关定义.

定义 2(节点间脆弱性利用图). 节点间脆弱性利用图是一个有向图,记为 $G=\{V,E,A,L,s\}$,各元素含义分别为:V 是顶点集合,其中每个顶点 v 由主机标识和用户权限级别二元组表示,记为$\langle h,p\rangle$,p 可取值为 1(*USER*)或 2(*ROOT*);E 是有向边 e 的集合,有向边 e 表示攻击者成功利用脆弱性的一次攻击,它由四元组(s,d,vid,pr),$s,d\in V$,$vid\in VID$,$pr\in[0,1]$表示.其中,s,d 分别表示攻击者实施本次脆弱性利用所应具有的最小权限和利用成功后所获得的权限,vid 表示本次被利用的脆弱性编号,pr 表示该脆弱性的利用成功率;A 为攻击者执行的脆弱性利用动作集合,其中所包含的每个元素 a 由标识所利用脆弱性的编号和利用成功率的二元组表示,记为$\langle vid,pr\rangle$;L 是从 E 到 A 的映射函数,记为 $L:E\to A$,用于标识 e 相关的脆弱性利用动作;$s\in V$ 为攻击者的初始攻击节点.

节点间脆弱性利用图 G 中的有序点对(v,w)间可能存在多条等价的有向边 e,表示在攻击者获得节点 v 对应的用户权限级别之后,任选一条表示一次脆弱性利用攻击的有向边 e,可获得节点 w 对应的用户权限级别.为便于描述,对 G 中任一有向边 e 的起点和终点分别记为 $e.s$ 和 $e.d$,相应地,被利用的脆弱性编号为 $e.vid$,利用成功率为 $e.pr$.

节点间脆弱性利用图可以显式刻画系统所有可能的攻击路径,明确节点与攻击者获取用户权限的对应关系,便于分析和计算攻击者获取相应攻击能力的最小代价.为了识别最短攻击路径,将节点间脆弱性利用图转换为标准有向图,再利用标准有向图中的最短路径分析算法计算最短攻击路径.通过分析攻击流穿透安全措施的可能攻击路径和相应利用成功率,识别成功实施攻击的最短攻击路径对应的攻击流,计算攻击路径利用成功率表示攻击者成功实施攻击的最小代价,以便评价安全措施效用.相关定义如下:

定义 3(独立脆弱性利用成功率). 独立脆弱性利用成功率用于评估系统中某一脆弱性被攻击者成功利用,以实施攻击的难易程度.记为 pr.

独立脆弱性利用成功率受多种因素的影响,包括弱点信息、攻击方法和攻击工具.并且,这些要素的公布详细程度也影响到脆弱性利用成功率.鉴于目前国内外对独立脆弱性的分析和评分的研究相对成熟,本文基于国内外研究成果,参考通用弱点评价体系[17]和文献[18,19],给出脆弱性利用成功率赋值公式:

$$Pr=(E+M+T),$$

其中,$E\in[0,0.1]$,表示弱点信息发布情况,当没有发布的弱点信息时取值为 0,有已发布的弱点信息时取值为 0.1;$M\in[0,0.4]$为攻击方法公布情况,当没有公布的攻击方法时取0,有公布的粗略攻击方法时取值为0.2,有公布的详细攻击方法时取值为 0.4;$T\in[0,0.4]$表示攻击工具发布情况,当脆弱性成果利用需要攻击工具但未有相关发布信息时取值为 0,当有可用攻击工具时取值为 0.2,如脆弱性利用不需要攻击工具时取值为 0.4.相应的脆弱性利用成功率赋值基准见表 1.

Table1 An assignment for the attacking success probability

表 1 攻击成功率赋值标准

等级	*pr*	描述
1	0.9	不需要攻击工具,有详细的攻击方法
2	0.7	有可用的攻击工具和详细的攻击方法
3	0.5	无攻击工具但有详细的攻击方法
4	0.3	弱点信息发布,粗略说明攻击方法
5	0.1	弱点信息发布,未给出攻击方法

定义 4(攻击路径). 攻击路径是 G 中开始于 sn 和终止于 dn 的一个有向边序列 $e_0,e_1,e_2,\ldots,e_{n-1}$,即有 $e_0.s=sn$,$e_i.d=e_{i+1}.s$ 且 $0\leqslant i\leqslant n-2$,$e_{n-1}.d=dn$.

定义 5(攻击路径利用成功率). G 中某一攻击路径 $L=(e_0,e_1,e_2,\ldots,e_{n-1})$,$e_i=(vid_i,pr_i)$,$0\leqslant i\leqslant n-1$ 的利用成功率

Pr 为 $Pr=\prod_{i=0}^{n-1} pr_i$, 记为 $L.Pr$.

定义 6(最短攻击路径). 如果 G 中从 st 到 dt 存在 n 条攻击路径 $l_1,l_2,\ldots,l_n$,各攻击路径的利用成功率分别为 $Pr_1,Pr_2,\ldots,Pr_n$,则取 Pr 值最大的那条路径为从 st 到 dt 的最短攻击路径,记为 $sl=\arg\max_{1\leqslant i\leqslant n}\{pr_{l_i}\}$.

在实施攻击的过程中,攻击者通常利用脆弱性来提升攻击能力.表现为获取某些可能影响关键对象安全性的用户权限进行非授权访问,破坏业务系统的安全属性.如果系统中存在这样的攻击路径,说明系统现有安全措施无法满足安全要求.组织应用安全措施的根本目的是阻止攻击者利用脆弱性,防止攻击者非授权获取影响关键对象安全性的用户权限,维护系统安全属性以满足安全要求.从攻防双方视角来看,业务系统中安全措施效用体现在是否有能力合理维护系统用户权限,保证所有系统关键对象安全性;攻击者攻击能力的高低体现在它是否可能获取到相应的用户权限,达到破坏系统关键对象安全性的目的.因此,文中通过攻击者能力是否影响到关键对象安全性来刻画业务系统的安全属性,并基于关键对象用户权限建立安全措施效用层次评价模型.

下面给出了层次评价模型中所应用的安全属性定义.其中,$ObjS$ 为涉及业务系统安全的所有关键对象集合,$ObjS_C$ 为涉及业务系统机密性的关键对象集合,$ObjS_I$ 为涉及业务系统完整性的关键对象集合,$ObjS_A$ 为涉及到业务系统可用性的关键对象集合.

定义 7(机密性). 防止未授权的信息泄露,即要求攻击者通过脆弱性利用所获取到的攻击能力集合 $AtkCap$ 与影响业务系统机密性的关键对象权限集合 $PrivSet_C$ 的交集为空.

$PrivSet_c=\{p|\forall O\in ObjS_C,\forall p\in RdPrivs(O)\}, AtkCap=\{p|\forall O\in ObjS,\forall p\in AtkPrivs(O)\}\Rightarrow PrivSet_C\cap AtkCap=\varnothing$.

定义 8(完整性). 禁止未授权实体对客体的更改或破坏,即要求攻击者通过脆弱性利用所获得的攻击能力集合 $AtkCap$ 与影响到业务系统完整性的关键对象权限集合 $PrivSet_I$ 的交集为空.

$PrivSet_I=\{p|\forall O\in ObjS_I,\forall p\in MdPrivs(O)\}, AtkCap=\{p|\forall O\in ObjS,\forall p\in AtkPrivs(O)\}\Rightarrow PrivSet_I\cap AtkCap=\varnothing$.

定义 9(可用性). 保证所有服务必须对相关授权实体是可访问和使用的,即要求攻击者通过脆弱性利用所获得的攻击能力集合 $AtkCap$ 与影响业务系统可用性的关键对象权限集合 $PrivSet_A$ 的交集为空.

$PrivSet_A=\{p|\forall O\in ObjS_A,\forall p\in CPPrivs(O)\}, AtkCap=\{p|\forall O\in ObjS,\forall p\in AtkPrivs(O)\}\Rightarrow PrivSet_A\cap AtkCap=\varnothing$.

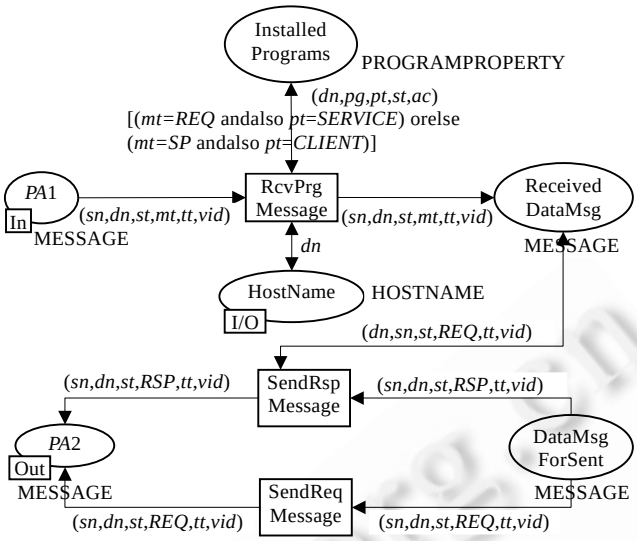
2 攻击者能力分析模型

Petri 网是 1962 年由德国科学家 Carl Adam Petri 提出的一种系统模型,具有严格的形式化定义和直观的图形表示,便于描述动态系统结构和并发行为.CPN 定义的模型可以采用标准方法进行分析(包括可达图分析和仿真执行),而无需设计专用分析方法,这能有效简化原型系统的建模和分析过程.同时,CPN 的分层描述方式易于表现信息系统层次化设计思想[20].攻击者能力分析模型需要分析系统业务流、攻击流和安全措施三者之间的并发行为和相互作用,因此选用 CPN 作为建模工具.将被评估系统抽象为 3 类通用 CPN 模型组件,包括:1) 业务逻辑组件;2) 攻击实施组件;3) 安全措施组件.利用 CPN 工具整合这 3 种组件建立攻击者能力分析模型,实现攻击者能力分析过程中各安全要素之间影响的分析,获取系统安全措施效用评估所需分析数据.

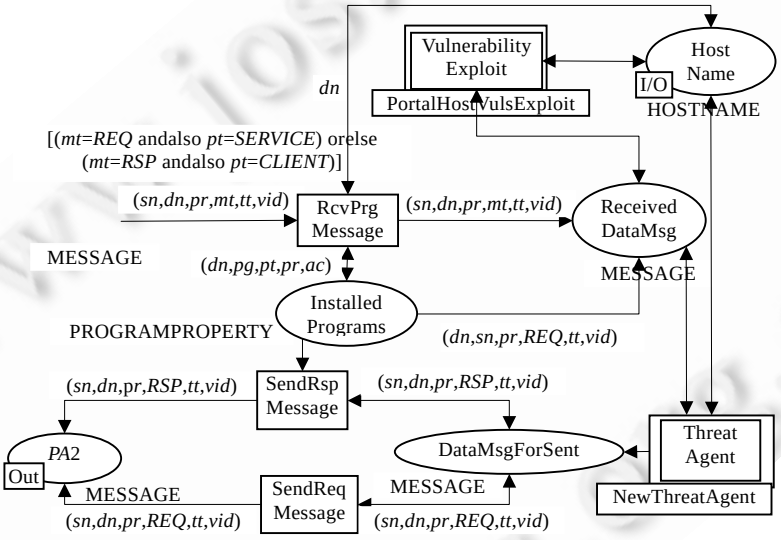
针对安全措施组件建模,主要借鉴文献[5]的方法建立了通信子网、过滤和转换安全机制的 CPN 模型,并扩展实现了安全分析机能模型.受篇幅所限,这里不再赘述.下面分别介绍针对业务逻辑组件和攻击实施组件的建模方法.

2.1 系统业务逻辑组件建模

系统业务逻辑组件建模包括网络架构和终端建模两部分.本文采用自顶向下方式建立业务系统网络架构,逐步细化子网结构和终端节点,得到最终的攻击者能力分析模型.终端建模方法独立于具体业务数据流处理功能,可以对不同服务模式(主动、被动或二者兼具)下的业务终端实现统一描述,相应的 CPN 模型如图 2(a)所示.



(a) 无脆弱性的基本终端 CPN 模型



(b) 具有脆弱性的扩展终端 CPN 模型

Fig.2 A CPN model for a basic end-entity without a vulnerability and an extended CPN model for an end-entity with vulnerabilities

图 2 无脆弱性的基本终端 CPN 模型和具有脆弱性的扩展终端 CPN 模型

在实际网络环境中,系统业务数据流和攻击流报文格式相同,二者的区别在于报文载荷内容:前者为正常的业务访问数据,后者为脆弱性利用攻击数据.因此,攻击者能力分析模型统一应用颜色集 *Message* 抽象表示由终端产生、发送以及在各终端间交互的数据流和攻击流,颜色集 *Message* 定义为六元组⟨*sn*,*dn*,*st*,*mt*,*tt*,*vid*⟩,其中,各颜色域的定义描述如下:

- *sn*,*dn*,分别标识发送方和接收方的终端,如 PC、工作站等;
- *st*,应用的服务类型,如 HTTP,FTP,MAIL,SSH 等;

- *mt*,消息类型,可取值为 *REQ*(请求数据流)和 *RSP*(响应数据流);
- *tt*,编码状态,*EF* 为未经数据加密等数据形式转换处理的数据(或攻击)流,*TR* 表示经转换处理的数据(或攻击)流;
- *vid*,载荷类型,取值为 0 时,表示该数据流是正常业务数据流;取值非 0 时,则表示当前数据流为攻击流,且对应的 *vid* 值是该攻击流所利用脆弱性的唯一标识.

如图 2 所示,基本终端 CPN 模型对业务系统终端接收和发送数据流的行为进行建模.其中,库所 *DatamsgforSent* 存储本终端需要发送的数据,变迁 *RcvPrgMessage* 根据业务系统配置情况接收进入终端的网络数据,变迁 *SendReqMessage* 和 *SendRspMessage* 分别实现终端请求和响应数据流的发送,前者不设定限制条件,表示业务请求可以随时发出;后者以 *ReceivedDataMsg* 作为输入库所,表示基本终端只有在收到对应请求数据流之后才允许发送相应的响应数据流.

2.2 攻击实施组件建模

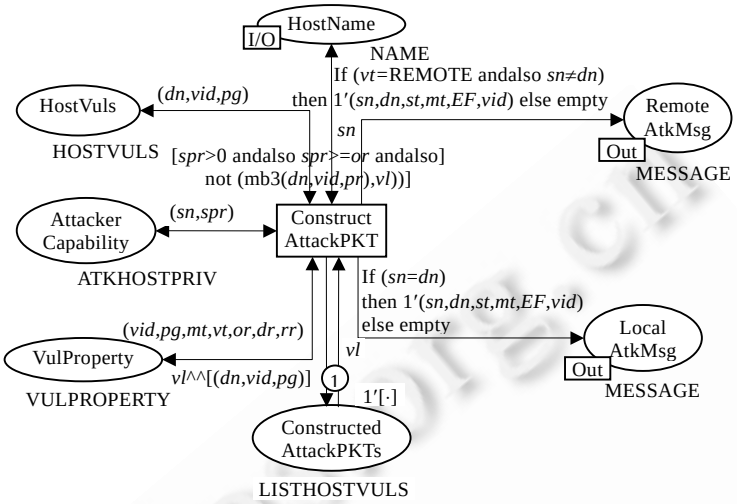
威胁是可能导致业务系统受损的不期望事件发生的潜在原因[21].攻击者在实施攻击时,需要不断尝试利用系统脆弱性,以非法获取业务资源访问权限的方式.本文基于攻击者能力的 3 个假设,实现对系统面临的威胁建模:1) 攻击者能够获取脆弱性、网络拓扑等可利用的系统信息;2) 攻击者掌握相关脆弱性的攻击利用方法;3) 攻击者是贪婪的,会基于已有攻击资源扩大攻击影响,破坏安全目标.攻击者能够成功利用对象 $O_i(i\in N)$上脆弱性 v 的前提条件包括:1) v 必须在 O_i 上存在;2) 攻击者能从所控制的攻击源访问到 O_i 所在的目标终端,即存在从攻击源到目标终端之间的访问通路;3) 攻击者在源和目标终端上的权限满足 v 被成功利用所须具备的最小权限要求.成功利用 v 的结果表现为攻击者已获得可对 O_i 施加影响的能力:直接影响是对 O_i 安全属性的破坏;间接影响是攻击者基于在 O_i 上获取的用户权限,尝试利用其他业务对象的脆弱性,以扩大攻击成果.实际应用中,攻击、威胁和系统脆弱性之间存在依赖关系,因此,文中把威胁和脆弱性利用建模集成到终端建模过程中:当终端不存在脆弱性时,将这种只对处理正常业务数据流的终端建模为基本终端(如图 2(a)所示);如果终端除了处理正常的业务数据流外还需根据已知脆弱性和攻击者能力对系统面临的安全威胁进行建模,得到的终端模型为扩展终端(如图 2(b)所示).相应地,攻击实施组件的 CPN 模型分为攻击流构造建模和脆弱性利用建模两部分.文中把终端上可被攻击者用来生成攻击流的功能抽象为威胁代理,威胁代理能否被激活取决于攻击者的能力,被激活的威胁代理会生成对业务系统内各脆弱性进行利用的攻击流.由于威胁代理模型可分布于不同终端,并且可能同时处于激活状态,因此可实现协同攻击场景建模.

威胁代理子模块 CPN 模型如图 3(a)所示,其中,*HostVuls* 库所存储了与各终端相关的脆弱性信息,*VulProperty* 库所存储各脆弱性相关的利用条件、脆弱性利用所产生的影响等信息,*AttackerCapabilities* 库所记录攻击者当前获取的攻击能力信息,库所 *ConstructedAttackPKTs* 记录了威胁代理生成的所有攻击流.变迁 *ConstructAttackPKT* 根据其 GUARD 函数定义的脆弱性利用条件,尝试为每个满足利用条件的系统脆弱性生成攻击流.库所 *LocalAtkMsg* 和 *RemoteAtkMsg* 分别为脆弱性利用攻击流的本地和远程输出接口.

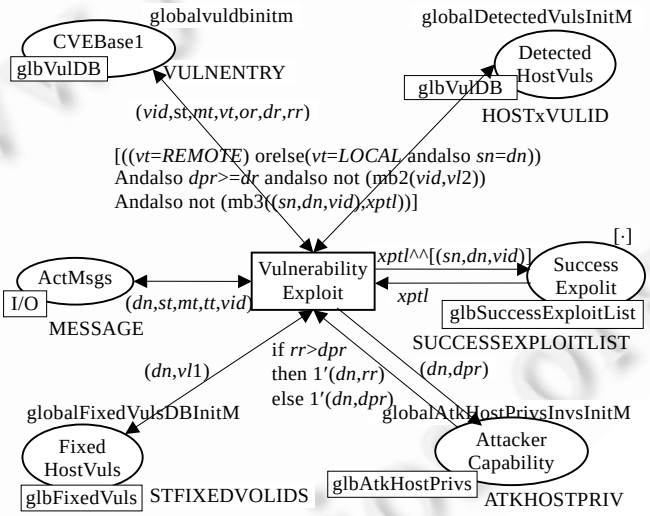
在攻击实施组件 CPN 模型中,用颜色集 *VulProperty* 表示系统的脆弱性及其利用的前提条件和后果,属于该颜色集的 token 记为八元组⟨*VulID*,*Program*,*MsgType*,*VulType*,*SrcPriv*,*DstPriv*,*RstPriv*,*CIAEffect*⟩,各颜色域含义依次为:

- *VulID*,脆弱性唯一标识,取值与 CVE(common vulnerabilities exposure)定义一致;
- *Program*,脆弱性所依附的应用程序名;
- *MsgType*,标识可利用该脆弱型的数据流类型,包括请求数据流或响应数据流;
- *VulType*,标识脆弱性被利用的方式,分为本地和远程利用;
- *SrcPriv*,*DstPriv*,说明攻击者要成功利用该脆弱性分别在源终端和目标终端上所必须拥有的最小用户权限;
- *RstPriv*,攻击者成功利用该脆弱性后在目标终端上获得的最大用户权限;
- *CIAEffect*,该脆弱性被利用后对目标终端安全属性所造成的影响.

脆弱性利用子模块 CPN 模型如图 3(b)所示,其中,变迁 *VulnerabilityExploit* 模拟脆弱性利用行为,依附于它的 GURAD 函数定义了成功利用脆弱性的前提条件.当脆弱性利用成功时,会更新记录攻击者能力的融合库所 *AttackerCapabilities*.融合库所 *SuccessExploitList* 记录了攻击者成功利用脆弱性的所有行为,评估人员可根据其中的输出结果构造节点间脆弱性利用图.



(a) 威胁代理 CPN 模型图



(b) 脆弱性利用 CPN 模型

Fig.3 A CPN model for a threat agent and the vulnerabilities exploited

图 3 威胁代理 CPN 模型图和脆弱性利用 CPN 模型

库所 *SuccessExploitList* 中的每个成功执行的脆弱性利用动作 *a* 由元组⟨*sn*,*dn*,*spr*,*dpr*,*vid*,*pr*,*rr*⟩表示,其中,

- *sn* 和 *dn* 分别表示 *a* 发起的源和目标节点;
- *spr* 和 *dpr* 为攻击者发起本次 *a* 时在源和目标节点上须具有的最小权限;
- *vid* 为 *a* 所利用的脆弱性编号;
- *pr* 表示 *a* 利用脆弱性的成功率;

- *rr* 为本次实施 *a* 成功后攻击者获得的目标节点权限.

在建立系统攻击者能力分析模型过程中,以层次化设计方式把上述脆弱性利用和威胁代理子模块集成于终端 CPN 模型(如图 2(b)所示),分别记为置换变迁 *VulnerabilityExploit* 和 *ThreatAgent*.攻击过程中,脆弱性利用模型中的变迁 *VulnerabilityExploit* 从库所 *ReceivedDataMsg* 中接收攻击流,被激活的威胁代理 *ThreatAgent* 产生远程或本地攻击流,前者直接注入终端模型中的 *DataMsgForSent* 库所,经过通信子网组件建模的传输网络抵达攻击目标,模拟远程脆弱性利用;本地攻击流直接注入 *ReceivedDataMsg* 库所,由本地终端的脆弱性利用模块接收,实现本地脆弱性利用的模拟.

2.3 攻击者能力分析模型复杂度分析

传统的 CPN 模型常采用可达图分析方法,因为可达图分析方法可以穷尽所有可能的状态,但可达图分析方法存在组合状态爆炸问题.下面的定理证明,由上述方法所构建的攻击者能力分析模型在有限步仿真后一定进入死状态,并且有且仅有一个死状态,且在死状态时攻击者所获得的攻击能力最大.由于在评估安全措施效应时只需知道攻击者所能够获得的最大攻击能力,而无需知晓其攻击能力变化过程,因此可以采用 CPN 仿真方法代替 CPN 可达图分析方法,从而避免了可达图分析中的组合状态爆炸问题.

定理 1. 由上述方法所构建的攻击者能力分析 CPN 模型在有限步仿真后一定进入死状态,并且有且仅有一个死状态,且在死状态时攻击者所获得的攻击能力最大.

证明:在攻击者能力分析模型中,攻击者在整个攻击过程中的攻击能力是单调递增的,即攻击者不会在攻击深入过程中失去已经获得的攻击能力.这一点可以从图 3(b)所示的脆弱性利用 CPN 模型的库所 *AttackerCapabilities* 看出,即只有当攻击者利用该脆弱性利用所获得的本机权限大于攻击者先前在该主机上所获得的权限时,脆弱性利用 CPN 模型才会更新库所 *AttackerCapabilities* 的 token 值.下面证明该 CPN 模型在有限步仿真后一定进入死状态.

由上面所述的攻击者能力分析模型建模过程可知,应用此方法建立的 CPN 模型中任一库所有界.因此,该模型所对应的可达图的节点数量有限,可以采用可达图分析方法穷尽所有可能状态.假设业务系统中的终端数量为 n,存在于各终端的脆弱性平均数量为 k,则每个终端的威胁代理能生成的攻击流 token 最多为 $k\times n$.假设各终端生成的业务数据流 token 的平均数量为 p,则每个终端至多能生成$(k\times n+p)$个攻击流.由于攻击者能力分析 CPN 模型不存在环路,所以由任何扩展终端生成的攻击流最终都会流入某扩展终端 *DataMsgReceived* 库所,或者被系统中相关安全控制措施(如过滤)拦截、丢弃.假设攻击者能力分析 CPN 模型中攻击流从源到目标终端需经历的变迁数最多为 m,则由任一终端威胁代理生成的攻击流在经历最多$(k\times n+p)\times m$ 个变迁后必然被另一个终端所接收.同理可知,由 n 个终端生成的攻击流在经历最多$(k\times n+p)\times m\times n$ 个变迁后最终被其他终端接收.由于在由上述方法所创建的任一攻击者能力分析 CPN 模型中,k,p,m 和 n 都为常数,因此本文所建立的攻击者能力分析 CPN 模型能在有限步仿真后进入死状态,其计算复杂度为 $O(n^2)$.

在攻击者能力分析 CPN 模型中,由于所有由扩展终端发出的数据流和攻击流最终都会被某一扩展终端所消耗掉或者被中间安全设备所拦截,此外,在所创建的攻击者能力分析 CPN 模型中并不存在可能导致多个变迁形成竞争的库所,并且在各存储攻击流(数据流)历史的库所中,列表中各元素是按序存储的,因此,可达图有且仅有一个死状态.当到达死状态时,攻击者一定已经尝试了所有可能的脆弱性利用攻击,因此在死状态攻击者所获得的攻击能力最大. □

依据定理 1 可知,可以用计算复杂度非常小的 CPN 仿真来代替传统的 CPN 可达图分析,并且 CPN 仿真结束后,CPN 所对应的可达图将进入死状态.此时,融合库所 *AttackerCapabilities* 中的 token 值就是攻击者所获得的最大攻击能力,融合库所 *SuccessExploitList* 中的 token 则记录了所有成功的脆弱性利用攻击结果.因此,可以基于融合库所 *SuccessExploitList* 中的 token 值来构建节点间脆弱性利用图.

3 安全措施效用评估算法

3.1 节点间脆弱性利用图生成算法

基于融合库所 *SuccessExploitList*(简称 *SEL*)记录的仿真结果,给出节点间脆弱性利用图生成算法(ExploitGraphGenerate,简称 EGG).EGG 的伪码描述如图 4 所示:第 1 行首先置 G 为空,然后创建攻击者初始节点 *ss*,并加入到顶点集合 V 中.第 2 行~第 17 行根据 *SEL* 融合库所中记录的脆弱性成功利用动作列表构造节点间脆弱性利用图 G,其中,第 4 行对读取的每个脆弱性利用动作进行数据分解;第 5 行~第 7 行创建首节点 *sv*;第 8 行~第 10 行创建末节点 *dv*;第 11 行基于首节点 *sv* 和末节点 *dv* 构造有向边 *e*,并以⟨*vid*,*pr*⟩标识有向边 *e*;第 12 行~第 16 行则在 *spr* 值为 1 的情况下创建以⟨*st*,2⟩为值的顶点 *tv*,并创建一条从 *tv* 到 *dv* 的边 e_2,同时以二元组⟨*vid*,*pr*⟩对其进行标识.第 18 行返回所构造的节点间脆弱性利用图 G,即为相应被评估系统的节点间脆弱性利用图.

```
Input: SEL, the given array of successful vulnerability exploits recorded by place SEL of
       the CPN simulation model; hh, the initial attacker node from where attack begins;
Output: G, an inter-nodes vulnerabilities exploiting graph constructed from result of
        the CPN simulation model.
Steps:
1.    V=Φ, E=Φ, A=Φ, G=⟨V,E,A⟩, ss=⟨hh,2⟩, AddVertice(G,ss), V=V+{ss};
2.    for each a in SEL
3.    begin
4.        ⟨st,dt,spr,dpr,vid,pr,rr⟩=a;
5.        sv=⟨st,spr⟩;
6.        if (not (sv∈V))
7.            AddVertice(G,sv); V=V+{sv}
8.        dv=⟨dt,rr⟩;
9.        if (not (dv∈V)))
10.           AddVertice(G,dv), V=V+{dv};
11.       e1=⟨sv,dv,vid,pr⟩, AddEdge(G,e1); LabelEdge(e1,vid,pr); E=E+{e1};
12.       if (spr==1)
13.           tv=⟨st,2⟩;
14.           if (not (tv∈V))
15.               AddVertice(G,tv), V=V+{tv};
16.           e2=⟨tv,dv,vid,pr⟩, AddEdge(G,e2), LabelEdge(e2,vid,pr), E=E+{e2};
17.   end
18.   return G;
```

Fig.4 Description for the algorithm EGG

图 4 节点间脆弱性利用图的生成算法描述

3.2 最短攻击路径分析算法

当针对某一攻击目标存在多条攻击路径时,攻击者往往会选择攻击成功率较大的攻击路径.同理,在节点间脆弱性利用图中,当攻击者从初始节点到目标节点存在多条攻击路径时,决定该目标节点安全性的应该是具有最大利用成功率的攻击路径,即最短攻击路径.

基于改进 Dijkstra 算法[22]的最短攻击路径分析算法伪码描述如图 5 所示.该算法由节点间脆弱性利用图求出从初始攻击节点 *ss* 到目标节点集合 O 中各目标节点 O_i 的最短攻击路径,它以 G 和 O 为输入,输出为一个只包括到达各 O_i 的最短攻击路径的节点间脆弱性利用图 $\overline{G}$.其中,第 1 行~第 6 行是对节点间脆弱性利用图中任意有序顶点对(v,w)之间等价的有向边进行归并,保留攻击成功率最大的有向边,归并后的节点间脆弱性利用图为标准有向图 $\hat{G}$;第 7 行~第 10 行采用改进 Dijkstra 最短路径算法,从 $\hat{G}$ 中求取从初始攻击节点 *ss* 到目标节点集合中各目标 O_i 的最短攻击路径;第 11 行~第 13 行在图 $\hat{G}$ 中创建从初始节点 *ss* 到各目标节点 O_i 的最短攻击路径.第 14 行返回只包含最短攻击路径的节点间脆弱性利用图 $\overline{G}$. 由于 G 中从 s 到各 O_i 的最短攻击路径是已知的,对于存在多条有向边的某一有序点对(v,w)存在如下两种情况:

1) (v,w)并不位于任意一条最短攻击路径中,这时,对(v,w)之间有向边的删除操作不会影响到各最短攻击

路径;

2) (v,w)位于某一最短攻击路径中,此时,通过反证法易知,所述最短攻击路径必然会选择(v,w)之间攻击成功率最大的有向边 es.

因此,步骤 1 中所述的 G 的简化操作并不会影响最终求取的从攻击初始节点到目标节点的最短攻击路径.

Input: G, an inter-nodes vulnerabilities exploiting graph constructed from result of the CPN simulation model; hh, the initial attack node; O, the given set of nodes from G;
Output: $\hat{G}$, the reduced inter-nodes vulnerabilities exploiting graph which only comprises shortest paths from initial node to each nodes in O.
Steps
1. for each sorted-binary (v,w) in G
2. $\{e_i\}$=*GetEquiventEdges*(v,w);
3. if (size of $\{e_i\}$>1)
4. $j = \arg\max_{e_i.pr}\{e_i\}$
5. for each e in $\{e_i\}$
6. if $(e \neq e_j)$ *RemoveEdge*(G,e);
7. *SPSet*=Φ;
8. for each o in O
9. *shortestpath*=*Dijkstra*(G,ss,o);
10. *SPSet*=*SPSet*+{*shortestpath*};
11. $V=\Phi, E=\Phi, A=\Phi$, $\hat{G}=\langle V,E,A\rangle$, $ss=\langle hh,2\rangle$, *AddVertice*$(\hat{G},ss)$;
12. for each *sp* in *SPSet*
13. *DrawPath*$(\hat{G},sp)$;
14. return $\hat{G}$;

Fig.5 Description for the algorithm the shortest-attack-paths analysis

图 5 最短攻击路径分析算法描述

3.3 安全措施效用评价算法

根据标准定义,机密性(C)、完整性(I)和可用性(A)是信息安全的基本属性[12,13,21],因此文中基于这 3 个基本安全属性建立系统安全措施效用评估准则,反映系统安全要求,并归纳具体评价指标.图 6 为本文所创建的安全措施效用层次评价模型(以下简称评价模型),其顶层为评价目标,即被评估系统的安全措施效用;中间层为准则层;底层为指标层,它是与维护系统对象安全属性相关的合法用户权限集合.

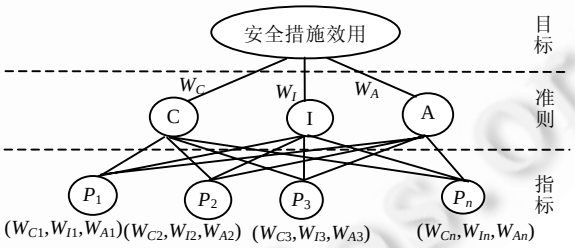


Fig.6 Hierarchical evaluation model of a security measures

图 6 安全措施效用层次评价模型

信息系统安全保障的核心是,通过在系统中应用安全措施来保障系统所支持的业务安全.由于信息系统承载业务的差异,不同系统的安全需求对安全属性的关注程度不同,相应的安全属性取值也不同.如,教育招生系统最为关注的是考生和成绩信息的完整性,国防军工系统最为关注的是信息的机密性,而电力电信等业务系统最为关注的则是系统的可用性.为体现这种差别,在评价模型的准则层中,评估人员根据系统业务应用的安全要求以及用户安全需求,为安全措施效用评价模型中的各安全属性分配相应权重,分别记为 W_C,W_I,W_A,且 $W_C+W_I+W_A=1$.此外,由于拥有不同对象的权限会对业务系统安全属性造成的影响程度有所不同,因此,评价模型为不同的对象权限分配相应的权重系数以示区别.各用户权限 P_i 对业务系统 C,I,A 安全属性的影响因子分别记

为 W_{Ci},W_{Ii},W_{Ai},并且 $\sum_{i=1}^{n}W_{Ci}=1,\sum_{i=1}^{n}W_{Ii}=1,\sum_{i=1}^{n}W_{Ai}=1$.对于某一对象权限 P_i,如果存在一条或多条攻击路径,且其中最短攻击路径的脆弱性利用成功率为 Pr_i,则现有安全措施只能以$(1-Pr_i)$的概率确保该对象权限 P_i 的安全.因此,当前系统安全措施效用 E 可由如下公式计算:

$$E=W_C\sum_{i=1}^{n}W_{Ci}(1-Pr_i)+W_I\sum_{i=1}^{n}W_{Ii}(1-Pr_i)+W_A\sum_{i=1}^{n}W_{Ai}(1-Pr_i) \tag{1}$$

理想情况下,安全措施能有效抵御各种脆弱性利用攻击,不存在从初始攻击节点 ss 到达各 P_i 的攻击路径,即从 ss 到 P_i 的最短攻击路径利用成功率 Pr 等于 0,因此有 $E=W_C\sum_{i=1}^{n}W_{Ci}+W_I\sum_{i=1}^{n}W_{Ii}+W_A\sum_{i=1}^{n}W_{Ai}=W_C+W_I+W_A=1$ 成立.

3.4 基于多属性决策安全措施效用提升方案的选择方法

当存在多种提升安全措施效用的解决方案时,如何综合各方面因素选择最优方案,是安全管理人员普遍面临的问题.文中采用多属性决策来实现最优效用提升方案的选择.算法实现步骤为:

第 1 步,构造被评估系统安全措施效用提升方案属性矩阵 X:

$$X=\begin{pmatrix}ap_1\\ap_2\\ap_3\end{pmatrix}\times(Act_1,Act_2,...,Act_n)=\begin{pmatrix}X_{11}&X_{12}&...&X_{13}\\X_{21}&X_{22}&...&X_{23}\\X_{31}&X_{32}&...&X_{3n}\end{pmatrix}_{(3\times n)},$$

其中,ap_i 为备选方案的决策属性,这里选择的决策属性包括方案投资成本(ap_1)、实施代价(ap_2)和安全措施效用值(ap_3);Act 表示备选的效用提升方案.以每一备选方案 Act_j 对应的 ap_i 取值为 x_{ij} 构建矩阵 X;

第 2 步,确定理想的效用提升方案 Act_o.本算法中理想方案应具有最小投资成本和实施代价,并产生最大的效用,因此,Act_o 对应的属性向量 ap^*有:$ap^*=(\min\{x_{1i}\},\min\{x_{2i}\},\max\{x_{3i}\})$;

第 3 步,构建多属性决策矩阵 D.对每个 ap_i,计算各备选方案与理想方案的灰色关联系数 r_{ij}($1\leqslant i\leqslant 3$,$1\leqslant j\leqslant n$),并由 r_{ij} 构造多属性决策矩阵 $D=[r_{ij}]_{3\times n}$.r_{ij} 反映 Act_j 在 ap_i 下的取值 x_{ij} 与最佳属性值 x_i^* 的相关性,其值越大,代表 Act_j 在 ap_i 下的效果越好.对于属性 ap_1 和 ap_2,确定 $r_{ij}=x_i^*/x_{ij}$;对于 ap_3,确定 $r_{ij}=x_{ii}/x_i^*$;

第 4 步,确定各决策属性权重.对 ap_i 权重有 $W=(w_1,w_2,w_3)$,其中,$\sum_{i=1}^{3}w_i=1$,各决策属性权重可采用人工经验赋值、DELPHI 方法或者熵权法得到;

第 5 步,选取效用提升最优方案.计算 Act_j 在所有决策属性上的综合评分结果 $R_j=\sum_{i=1}^{3}w_{ij}r_{ij}$, 得到 $R=(r_1,r_2,\ldots,r_n)$.综合评分结果,根据 $r_j^*=\max\{r_j\}$ 确定最优效用提升方案.

4 评估实验

本文参照普遍性的 Web 应用业务系统建立实验环境(如图 7 所示),并配置相应的安全策略:部署在网络信任域边界处的防火墙将网络分成了互联网、内网和 DMZ 区这 3 个安全域.DMZ 区部署的 Web 服务器为用户提供 Web 服务.内网的内部用户不允许与外网直接连接,防止外部蠕虫病毒等攻击直接进入内网传播,保证 Web 服务器对外提供服务.各安全域之间具体访问控制策略如下:1) 只允许互联网用户访问 DMZ 区 H_2 上的 IIS Web 服务和 H_3 上的 DNS 域名服务;2) DMZ 区的 H_2 允许访问 H_3 上的 Sendmail 服务和内网 H_4 上的 MYSQL 服务;3) 禁止 H_2 和 H_3 直接访问内网中的管理主机 H_5;4) H_5 允许直接访问 DMZ 的 H_2 和 H_3 及内网的 H_4.各应用终端的软件配置和脆弱性信息见表 2.

通过对 Web 业务系统进行数据流分析和业务支撑分析,得到所有可能影响业务系统安全属性的关键对象用户权限.根据 Web 业务系统安全要求,给出与 Web 业务系统安全属性相关的关键对象权限集合 $PrivSet$ 分别

设置如下:

$PrivSet_C$={[H_3,1],[H_4,2],[H_5,2]};$PrivSet_I$={[H_2,2],[H_3,2],[H_4,2],[H_5,2]};$PrivSet_A$={[H_2,1],[H_3,2],[H_4,2]}.

$PrivSet_C$集合表明,只要攻击者获取 H_3的普通用户权限、H_4的超级用户权限或 H_5超级用户权限中的一种,就获得了对被评估系统相关业务机密性的破坏能力.类似地,可知集合 $PrivSet_i$和 $PrivSet_a$的含义.由于所承载系统功能和安全要求的不同,$PrivSet_C$集合中各元素对整个被评估系统机密性的影响程度不同.因此,根据系统安全要求,基于第 3.3 节给出的安全措施效用层次评价模型,为各元素影响权重赋值,得到影响权重向量为(0.3,0.5,0.2).同理,$PrivSet_I$和 $PrivSet_A$集合的影响权重向量分别为(0.3,0.3,0,3,0.1)和(0.4,0.2,0.4).

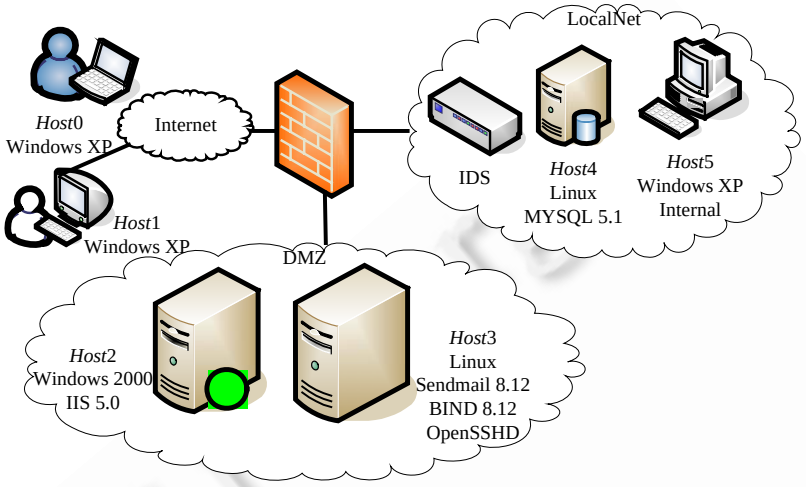


Fig.7 Topology of the Web system

图 7 Web 系统拓扑图

Table 2 Information of software configuration and vulnerabilities on the end entities in the Web system

表 2 Web 系统应用终端软件配置及脆弱性信息

主机	所在网段	提供服务	CVE 编号 (内部编号)	脆弱性利用条件 (*type*,*spr*,*dpr*)	脆弱性利用 结果权限	利用 成功率
H_0	互联网	攻击工具	无	无	无	0
H_1	互联网	移动办公软件	无	无	无	0
H_2	DMZ	IIS 5.0(HTTP)	CVE-2002-0364(1)	(*remote*,1,0)	2	0.70
H_3	DMZ	BIND8.x (DNS) Sendmail (Mail) OpenSSHD(SSH)	CVE-2001-0010(2) CVE-2002-1337(5)	(*remote*,1,0) (*remote*,1,0)	1 1	0.60 0.7
H_4	内网	OpenSSHD(SSH) MySQL 5.0.18 (SQL)	CVE-2002-0004(4) CVE-2006-1518(7)	(*local*,1,1) (*remote*,1,0)	2 1	0.8 0.7
H_5	内网	IE 6.0 (HTTP) Outlook (Mail)	CVE-2002-0193(6) CVE-2003-0352(8) CVE2010-0816(3)	(*remote*,2,0) (*remote*,1,0) (*remote*,2,0)	1 2 2	0.3 0.6 0.2

应用本文第 2 节给出的攻击者能力建模方法构造此 Web 系统的攻击者能力分析模型,根据系统中安全措施部署情况和脆弱性信息,使用系统业务逻辑(详见第 2.1 节)、攻击实施(详见第 2.2 节)、通信子网和安全措施(见第 2 节)等组件置换模型框架中相应功能组件,逐层细化子网结构和应用终端节点;并根据系统安全设备或措施配置规则定义、终端脆弱性信息和业务数据流信息对相应库所赋值,从而得到最终的攻击者能力分析模型.如图 8 所示,置换变迁 *Host*0 利用图 2(b)中的扩展终端 CPN 模型实现对攻击者所控制主机的建模;置换变迁 *Host*1,*Host*2,*Host*3,*Host*4 和 *Host*5 利用图 2(b)中的扩展终端 CPN 模型分别实现对业务系统中 H_1,H_2,H_3,H_4和 H_5主机终端的建模;置换变迁 Internet,EdgeRouter,DMZ 和 PrivateNetwork 利用文献[5]中的通信子网 CPN 模块分别实现对互联网、整个 Web 系统边界、DMZ 和内部网络的建模;置换变迁 *TF*1 和 *Tr*1 利用文献[5]中的转换

CPN 模块分别实现 VPN 端点的加解密功能;置换变迁 *EFW*1,*EFW*2 和 *FW*3 利用文献[5]中的过滤 CPN 模块分别实现边界防火墙、DMZ 防火墙和内网防火墙的建模,并依据安全策略分别配置相应过滤规则.

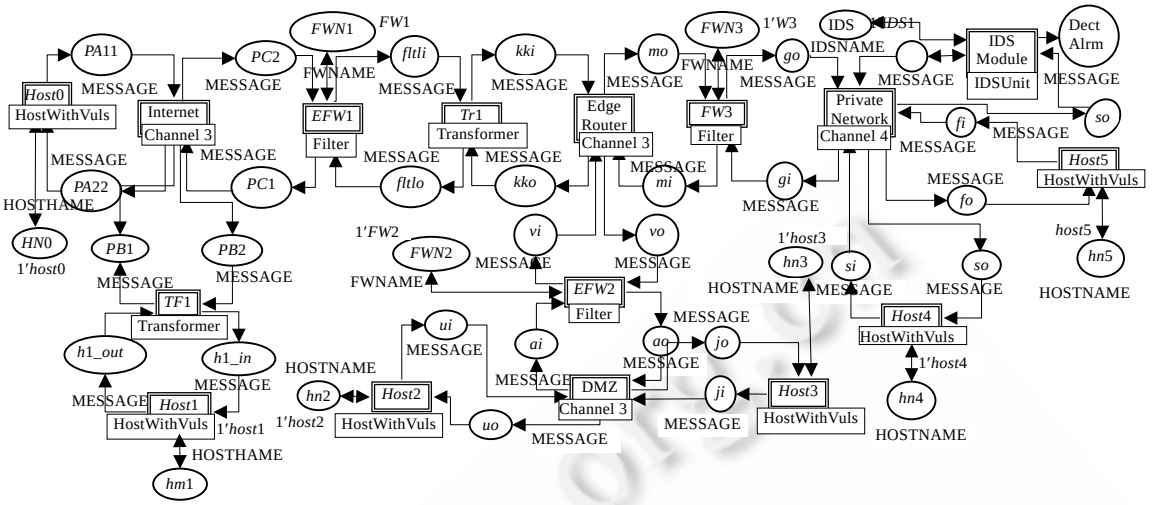


Fig.8 Attacker capability analysis CPN model for the Web system

图 8 Web 系统的攻击者能力分析模型

利用 CPN 工具[23]仿真攻击者能力分析模型,仿真过程在有限步内结束.仿真结束后,融合库所 *AttackerCapabilities* 中记录了攻击者脆弱性利用后在各应用终端上最终所获取的用户权限级别,其 Mark 值为

$$Mark(AttackerCapabilities)=1'(H_2,2)++1'(H_3,2)++1'(H_4,2)++1'(H_5,2).$$

将库所 *AttackerCapabilities* 值分别与 $PrivSet_C$,$PrivSet_I$ 和 $PrivSet_A$ 求交集,识别被评估系统面临的威胁.得到如下结果:

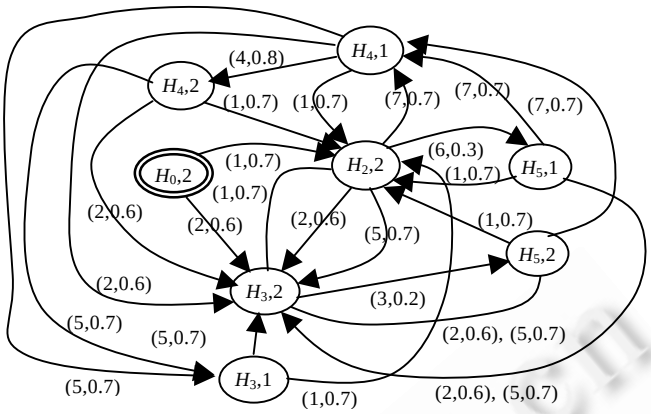
- $AttackerCapabilities \cap PrivSet_C=\{[H_3,1]^*,[H_4,2],[H_5,2]\}$
- $AttackerCapabilities \cap PrivSet_I=\{[H_2,2],[H_3,2],[H_4,2],[H_5,2]\}$
- $AttackerCapabilities \cap PrivSet_A=\{[H_2,1]^*,[H_3,2],[H_4,2]\}$

AttackerCapabilities 与 $PrivSet_C$ 的交集结果说明,此 Web 系统面临两个可能破坏机密性的威胁,即攻击者可非法获取 H_3 普通用户权限或 H_4 超级用户权限.同理,从 *AttackerCapabilities* 分别与 $PrivSet_I$ 和 $PrivSet_A$ 的交集结果可知:此 Web 系统面临破坏完整性的威胁有 4 个,即攻击者可以非法获得 H_2,H_3,H_4,H_5 上超级用户权限;破坏可用性的威胁有 3 个,即攻击者可能非法获得 H_2 的普通用户权限、H_3 或 H_4 上的超级用户权限.

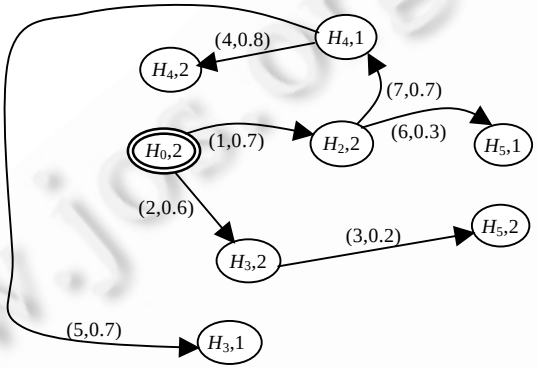
此 Web 系统的攻击者能力分析模型执行结束后,融合库所 *SuccessExploitList* 的 Token 为

1′[(H_0,H_2,1,0,1,70,2),(H_0,H_3,1,0,2,60,2),(H_2,H_3,1,0,2,60,2),(H_2,H_3,1,0,5,70,2),(H_2,H_5,2,0,6,30,1),(H_3,H_3,1,0,5,70,2),(H_2,H_4,1,0,7,70,1),(H_3,H_5,2,0,3,20,2),(H_5,H_4,1,0,7,70,1),(H_4,H_4,1,1,4,80,2),(H_4,H_3,1,0,2,60,2),(H_3,H_2,1,0,1,70,2),(H_4,H_3,1,0,5,7 0,1),(H_5,H_2,1,0,1,70,2),(H_5,H_3,1,0,2,60,2),(H_5,H_3,1,0,5,70,2),(H_4,H_2,1,0,1,70,2)].

应用第 3.1 节给出的节点间脆弱性利用图生成算法构造节点间脆弱性利用图,如图 9(a)所示.应用第 3.2 节的最短攻击路径识别算法对图 9(a)中的节点间脆弱性利用图进行处理,得到图 9(b)所示的简化后的节点间脆弱性利用图.从图 9(b)可以看出,位于 H_0 的攻击者可首先利用 H_2 上 IIS 服务器编号为 1 的缓冲区溢出漏洞,获得 H_2 的超级用户权限;然后以 H_2 为攻击跳板,利用 H_4 上编号为 7 的脆弱性,获取其普通用户权限;再利用 H_4 编号为 4 的本地权限提升脆弱性获取 H_4 的超级用户权限,从而获得对 Web 系统中数据库对象的完全控制,破坏系统安全属性.根据攻击路径利用成功率定义,计算与攻击者获取的最终权限相对应的最短攻击路径的利用成功率,计算结果见表 3.



(a) 节点间脆弱性利用图



(b) 简化后的节点间脆弱性利用图

Fig.9 An inter-nodes vulnerabilities exploiting graph and simplified inter-nodes vulnerabilities

图 9 节点间脆弱性利用图和简化后的节点间脆弱性利用图

Table 3 Success probability for the shortest attacking path destroying security attributes of the Web system

表 3 破坏 Web 系统安全属性的最短攻击路径成功率

最终权限	最短攻击路径	最短攻击路径利用成功率
[H_2,2]	(h0,h2,1)	0.7
[H_3,1]	(h0,h2,1),(h2,h4,7),(h4,h3,5)	0.343
[H_3,2]	(h0,h3,2)	0.6
[H_4,1]	(h0,h2,1),(h2,h4,7)	0.49
[H_4,2]	(h0,h2,1),(h2,h4,7),(h4,h4,4)	0.392
[H_5,1]	(h0,h2,1),(h2,h5,6)	0.21
[H_5,2]	(h0,h3,2),(h3,h5,3)	0.12

基于第 3.4 节给出的安全措施效用评价方法计算 Web 系统中安全措施效用 E.设 W_C=0.2,W_I=0.3,W_A=0.5,则有

$$E=0.2\times\{0.3\times(1-0.6)+0.5\times(1-0.392)+0.2\times(1-0.12)\}+$$
$$0.3\times\{0.3\times(1-0.7)+0.3\times(1-0.6)+0.3\times(1-0.392)+0.1\times(1-0.12)\}+$$
$$0.5\times\{0.4\times(1-0.7)+0.2\times(1-0.6)+0.4\times(1-0.392)\}=0.486.$$

上述 E 值表明,该 Web 系统现有安全控制措施抵御攻击的效果为 0.486,与理想值 1 之间还存在很大差距.因此,有必要改善系统安全措施,以满足系统安全要求.可采用的安全措施效用提升方法有两种:1) 修补 Web 系

统关键主机上的脆弱性,使攻击者无法以原有的脆弱性利用路径利用该脆弱性;2) 采用防火墙等安全设备加强主机节点间的访问控制,从而禁止攻击者通过该网络路径利用脆弱性实施攻击.表 4 给出了 3 种提升安全措施效用的备选方案以及每个方案的投资成本、实施代价和效用值 3 个属性上的赋值.其中,方案投资成本和实施代价采用相对成本运算法则,成本最大为 10,最小为 0;而方案效用值为经过安全措施效用评估所得效用值.

Table 4 Security efficiency improving acts for the Web system and the valued decision properties

表 4 Web 系统安全效用提升备选方案描述及决策属性赋值说明

备选方案 / 评估属性	方案 1	方案 2	方案 3	理想方案
	修补 H_2 的脆弱性 1	修补 H_3 的脆弱性 2	修补 H_4 的脆弱性 7	
投资成本	6	4	5	4
实施代价	7	5	6	5
效用值	0.813	0.514	0.639	0.813

采用第 3.4 节给出的基于多属性决策的最优方案选择算法,从中选择最优的安全措施效用提升方案.首先,将表 4 中的矩阵转换为决策矩阵:

$$D=\begin{pmatrix}0.667 & 1 & 0.8\\ 0.714 & 1 & 0.83\\ 1 & 0.632 & 0.786\end{pmatrix},$$

其中,3 个评估属性权重为 W=(0.2,0.2,0.6),则计算出各备选方案的综合评估结果 $R=W\times D$=(0.876,0.771,0.797).从各备选方案的综合评分可以看出,第 1 种效用提升方案为最优,即修补 H_2 的脆弱性 1 的效用提升方案.实际上,优先修补此脆弱性确实更具有合理性,这验证了基于多属性决策理论在选择最优效用提升方案时的有效性.

5 小 结

以往研究在评估系统安全措施效用的研究思路和实现方式上进行了有益的尝试,但仍存在对安全措施的实际应用情况分析不足、缺乏对安全措施效用评估各要素之间相互作用的分析、评估过程中对评估人员主观经验的依赖性较高等方面的局限性.文中提出了一种在给定脆弱性环境下的系统信息安全措施效用评估模型,该模型能适应信息系统复杂性、动态性特点,从系统数据流处理功能视角,应用 CPN 建模工具对系统业务流、安全措施和攻击流进行统一建模,并实现三者相互作用和影响的自动分析,为评估安全措施效用提供分析数据.文中提出节点间脆弱性利用图,给出生成算法和最短攻击路径识别算法,降低了分析攻击者获取攻击能力所需最小代价的计算复杂度,以及分析过程中对评估人员主观经验的依赖性.同时还剖析了安全措施效用与安全要求之间的关系,并基于系统安全属性所依赖的各关键对象用户权限建立安全措施效用层次评价模型,以定性与定量相结合的方法评估安全措施效用.文中还提供基于多属性决策的系统安全措施效用提升最优方案选择方法,为有效实施系统安全管理提供决策支持.以一个具体 Web 业务系统为例对所述安全措施效用评估方法进行验证,实验结果表明,文中的安全措施效用评估模型可以对业务系统中具体部署的安全措施对抗脆弱性利用攻击的效用进行有效评估,并可以减轻评估过程中对人员主观因素的严重依赖,可保证评估过程的规范性和评估结果的一致性和可追溯性,为实际网络环境中的安全管理活动提供指导.

进一步的后续研究工作包括:1) 加强攻击者能力分析模型在安全措施建模方面的可扩展性及对实际应用中安全措施抵御协同攻击的建模和能力评价;2) 进一步细化安全措施效用评价模型中合法用户权限粒度,使评估结果更接近实际应用;3) 针对系统安全措施效用提升最优方案的选择问题,通过增加决策属性进一步提高决策支持的合理性.

致谢 真诚感谢审稿人给本文提出的宝贵意见.

References:

[1] Chew E, Swanson M, Stine K, Bartol N, Brown A, Robinson W. Performance measurement guide for information security. NIST Special Publications 800-55, 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

[2] Joint Task Force Transformation Initiative. Recommended security controls for federal information systems (revision 3). National Institute of Standards and Technology (NIST) SP800-53, 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/SP800-53-rev3-finalupdate-errata_05-01-2010.pdf

[3] Jansen W. Directions in security metrics research. Technical Report, NISTIT 7564, NIST, 2009. http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

[4] Jaquith A, Wrote; Li DD, Wei R, Trans. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Beijing: Publishing House of Electronics Industry, 2007 (Chinese simplified language edition).

[5] Laborde R, Nasser B, Grasset F, Barr`ere F, Benzekri A. A formal approach for the evaluation of network security mechanisms based on RBAC policies. Electronic Notes in Theoretical Computer Science, 2005,121(2005):117−142. [doi: 10.1016/J.ENTCS.2004.10.011]

[6] Rieke R. Modelling and analysing network security policies in a given vulnerability setting. In: Lopez J, ed. Proc. of the Int'l Workshop on Critical Information Infrastructures Security 2006. Berlin, Heidelberg: Springer-Verlag, 2006. 67−78. [doi: 10.1007/11962977_6]

[7] Elahi G, Yu E, Zannone N. A vulnerability-centric requirements engineering framework: Analyzing security attacks, countermeasures, and requirements based on vulnerabilities. Requirements Engineering, 2010,15(1):41−62. [doi: 10.1007/s00766-009-0090-z]

[8] Chen Y, Boehm B, Sheppard L. Measuring security investment benefit for COTS based systems—A stakeholder value driven approach. CSSE Technical Reports, 2006-609, University of Southern California Center for Systems and Software Engineering, 2006.

[9] Dewri R, Poolsappasit N, Ray I, Whitley D. Optimal security hardening using multi-objective optimization on attack tree models of networks. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 204−213. http://www.cs.colostate.edu/~cs656/reading/2007ACMCCS.pdf [doi: 10.1145/1315245.1315272]

[10] Frigault M, Wang LY, Singhal A, Jajodia S. Measuring network security using dynamic Bayesian network. In: Proc. of the 4th ACM Workshop on Quality of Protection. New York: ACM Press, 2008. 23−30. http://csrc.nist.gov/staff/Singhal/qop2008_DBN_paper.pdf [doi: 10.1145/1456362.1456368]

[11] Wang LY, Noel S, Jajodia S. Minimum-Cost network hardening using attack graphs. Computer Communications, 2006,29(2006):3812−3824. [doi: 10.1016/j.comcom.2006.06.018]

[12] Practical Software and Systems Measurement (PSM) Safety & Security TWG. Security measurements. PSM White Paper, University of York, 2005. http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf

[13] Butler SA. Security attribute evaluation method: A cost-benefit approach. In: Proc. of the 24th Int'l Conf. on Software Engineering. New York: ACM Press, 2002. 232−240. http://www.cs.cmu.edu/~shawnb/SAEM-ICSE2002.pdf [doi: 10.1145/581339.581370]

[14] ISO/IEC. Information technology-security techniques-information security management-measurements. Int'l Standard ISO/IEC 27004: 2009. Switzerland: ISO, 2009. http://www.iso.org

[15] Chen F, Zhang Y, Su JS, Han WB. Two formal analyses of attack graphs. Journal of Software, 2010,21(4):838−848 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3584.htm [doi: 10.3724/ SP.J.1001.2010.03584]

[16] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2002. 217−224. http://mason.gmu.edu/~skaushik/index_files/p160-ammann.pdf [doi: 10.1145/586110.586140]

[17] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system (CVSS). version 2.0. Forum of Incident Response and Security Teams, FIRST.org Inc., 2007. http://www.first.org/cvss/cvss-guide.pdf

[18] Zhang YZ, Yun CX, Hu MZ. Research on privilege-escalating based vulnerability taxonomy with multidimensional quatitative attribute. Journal of China Institute of Communications, 2004,25(7):107−114 (in Chinese with English abstract).

[19] Stoneburner G, Goguen A, Feringa A. Risk management guide for IT systems. NIST Special Publication 800-30, 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[20] Wu ZH. PetriNet Guide. Beijing: China Machine Press, 2006 (in Chinese).

[21] ISO/IEC. Information technology-security techniques-code of practice for information security management. ISO/IEC 27002: 2005. Switzerland: ISO, 2005. http://www.iso.org

[22] Weiss MA, Wrote; Feng SX, Trans. Data Structures and Algorithm Analysis in C. 2nd ed., Beijing: China Machine Press, 2004 (Chinese simplified language edition).

[23] CPN tools homepage. http://cpntools.org/

附中文参考文献:

[4] Jaquith A,著;李冬冬,韦荣,译.安全度量-量化、分析与确定企业信息安全效能.北京:电子工业出版社,2007.

[15] 陈峰,张怡,苏金树,韩文报.攻击图的两种形式化分析.软件学报,2010,21(4):838−848. http://www.jos.org.cn/1000-9825/3584.htm [doi: 10.3724/SP.J.1001.2010.03584]

[18] 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.通信学报,2004,25(7):107−114.

[20] 吴哲辉.Petri 网导论.北京:机械工业出版社,2006.

[22] Weiss MA,著;冯舜玺,译.数据结构与算法分析-C 语言描述.第 2 版,北京:机械工业出版社,2004.

吴迪(1977－),女,辽宁葫芦岛人,博士生,讲师,主要研究领域为信息安全,安全测评.

连一峰(1974－),男,博士,副研究员,主要研究领域为网络与信息安全.

冯登国(1965－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为网络与系统安全.

陈恺(1982－),男,博士,助理研究员,主要研究领域为信息安全,软件漏洞分析与检测,恶意代码分析与防范.