一种基于攻击图的安全威胁识别和分析方法

吴 迪[1),2),4)] 连一峰[1),3)] 陈 恺[1)] 刘玉岭[1),2)]

[1)](中国科学院软件研究所 北京 100190)

[2)](中国科学院研究生院 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)

摘 要 业务系统安全管理需要网络攻击图来评估系统整体安全性或态势,同时又需要对那些可能严重危害系统安全的脆弱性利用威胁进行重点分析和优先处置.现有安全威胁识别和分析方法无法兼顾这两个方面,也无法处理脆弱性利用威胁分析过程中的不确定性问题.作者提出了一种安全威胁识别和分析方法.利用颜色Petri网(CPN)定义网络攻击图,并给出了网络攻击图生成NAGG算法,根据攻击模型分析结果生成网络攻击图;给出了基于CPN仿真的网络攻击图分解NAGD算法,可一次性分解出各脆弱性利用威胁对应的子攻击图,所述子攻击图不存在循环路径且最长攻击路径不超过预设值.并给出了一种脆弱性利用威胁度评估VETE算法,将子攻击图转换为不确定性推理规则集,采用D-S证据推理计算各子攻击图所对应安全威胁的威胁度,以确定安全威胁处置优先级.最后以一个典型Web应用系统为例,验证了所述安全威胁识别和分析方法的有效性.

关键词 攻击模型;网络攻击图;子攻击图;颜色Petri网;不确定性推理;D-S证据理论

中图法分类号 TP393 **DOI号**: 10.3724/SP.J.1016.2012.01938

A Security Threats Identification and Analysis Method Based on Attack Graph

WU Di[1),2),4)] LIAN Yi-Feng[1),3)] CHEN Kai[1)] LIU Yu-Ling[1),2)]

[1)](*Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[2)](*Graduate University of Chinese Academy of Sciences, Beijing* 100049)

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

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

Abstract Business system's security management needs to assess the system security situation by using network attack graph. It also needs to analyze the threats exploiting security vulnerabilities. Current security threat identification and analysis methods cannot handle the upper two problems very well at the same time. It cannot handle uncertainties occurred in the process of vulnerability exploiting threat analysis, either. A security threat identification and analysis method is proposed in this paper. The network attack graph is defined via Colored Petri Net (CPN) and an algorithm named NAGG is proposed to construct network attack graph based on the simulation results. We also give an algorithm named NAGD to simultaneously decompose network attack graph into several sub-attack-graphs, each corresponding to a specific vulnerability exploiting threat. The graph is loop-free and its longest attack path is limited to a certain predefined value. In order to prioritize all security threats for disposal, a vulnerability exploiting threat evaluating

收稿日期:2012-05-14;最终修改稿收到日期:2012-07-11.本课题得到国家"八六三"高技术研究发展计划项目基金(2009AA01Z439,2011AA01A203)、国家自然科学基金(61100226)、北京市自然科学基金(4122085)和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)资助.**吴 迪**,女,1977年生,博士研究生,讲师,主要研究方向为网络安全、信息安全测评.E-mail:wudi_dizi@163.com.**连一峰**,男,1974年生,博士,副研究员,主要研究方向为网络与信息安全.**陈 恺**,男,1982年生,博士,助理研究员,主要研究方向为信息安全、软件漏洞分析与检测、恶意代码分析与防范.**刘玉岭**,男,1982年生,博士研究生,主要研究方向为网络安全、绩效评估.

method named VETE is given to convert sub-attack graph into uncertain inference rule set. This method uses D-S evidence inference engine to calculate threat degree of each threat corresponding to the sub-attack-graph. At last, a typical Web application system is used as an example to validate the effectiveness of the proposed method.

Keywords　attack model; network attack graph; sub-attack-graph; Colored Petri Net (CPN); uncertainty reasoning; D-S theory

1　引　言

业务系统不可避免地存在脆弱性，因而使其面临各种脆弱性利用威胁. 从脆弱性利用角度剖析业务系统面临的安全威胁是一种有效的业务系统安全分析途径. 攻击图是一种广泛应用的脆弱性利用分析方法. 它从攻击者角度出发，基于系统网络配置和脆弱性信息，分析脆弱性利用之间的依赖关系，找出所有可能的攻击路径[1-3]，以便管理员采取必要措施抵御安全威胁，以降低安全风险. 因此，攻击图可为信息系统安全风险评估和绩效分析提供重要依据[4-5].

按攻击图中节点和边表示的含义不同，本文将攻击图分为状态攻击图和因果关系图. 状态攻击图[1,6]中的节点表示目标网络和攻击者的全局状态，有向边表示单一攻击行为引起的状态转换. 状态攻击图由于存在状态空间爆炸问题，不适用于大规模系统的安全性分析；因果关系图[7-9]中，节点表示系统条件(属性)和原子攻击，有向边表示节点间的因果关系. 因果关系图克服了状态攻击图的状态组合爆炸问题，具有更好的可扩展性，能用于大规模网络安全性分析. 目前的攻击图[7-10]大都属于因果关系图.

依据攻击图中攻击路径覆盖范围，本文将攻击图分为网络攻击图和子攻击图. 网络攻击图展示业务系统中所有可能攻击路径，子攻击图只展示与特定安全威胁相关的攻击路径. 网络攻击图适用于识别系统中各种可能影响到业务系统安全属性的脆弱性利用威胁，有助于评估业务系统整体安全性或态势，但网络攻击图[7,9]往往非常庞大，不适合对某一特定脆弱性利用威胁的分析；子攻击图[1,10]适于对特定脆弱性利用威胁进行有针对性的分析和处置. 在具体安全分析场景中，鉴于系统业务重要性的不同及资源有限和成本等因素影响，往往需要进一步分析所识别出的各种脆弱性利用威胁，生成各脆弱性利用威胁所对应的子攻击图，确定脆弱性利用威胁的优先处置顺序，以合理分配安全资源. 以往攻击图生成算法只能生成网络攻击图[7,9]或者子攻击图[1,10]. 但在实际的脆弱性利用威胁识别和分析过程中，通常需要基于网络攻击图和安全属性识别出所有影响业务系统安全性的脆弱性利用威胁，再基于子攻击图对所识别出的各脆弱性利用威胁进行深入分析.

近年来攻击图的研究工作主要集中在攻击图可视化[11]和基于攻击图的安全分析[4,12-14]上. 文献[11]利用数据归约和攻击组合方法改善攻击图可视化方法，更关注攻击图呈现问题，不是完备的攻击图分析方法. 文献[10]尝试基于网络攻击图裁剪出特定安全威胁所对应的子攻击图时，发现了网络攻击图中的循环攻击路径问题，但并未给出有效去除循环攻击路径的方法. 文献[12]给出从网络攻击图求取所有 n-有效路径的后向迭代算法，一次只能生成一个与特定安全威胁相关的子攻击图. 文献[15-16]给出了基于 Petri 网的组合攻击模型，但并未给出创建 Petri 网攻击模型的方法. 文献[17]应用贝叶斯网络评估网络脆弱性，提出了量化评估计算方法，但无法克服贝叶斯网计算过程中大量先验概率的获取问题. 文献[4]考虑攻击图中各个节点由于在攻击路径中所处位置不同而具有不同的重要性，基于 PageRank 思想将状态攻击图转换为 Markov 链，来计算攻击图中各个节点的重要度，但仍未解决状态攻击图组合爆炸问题.

在基于子攻击图分析特定脆弱性利用威胁的过程中，往往需要处理大量的不确定性信息，这些不确定性主要表现在模糊性和不一致性. 传统基于概率的信息系统安全分析方法无法有效解决模糊性问题[4,17-18]. 基于 D-S 证据理论的脆弱性利用威胁分析方法可以有效处理信息安全分析过程中的不确定性. 文献[19]使用 D-S 证据理论来处理网络风险评估中的不确定性，利用 D-S 组合方法对风险评估指标相关的安全因子进行融合. D-S 证据理论因其在不确定信息表达和合成方面的明显优势，近年来广泛应用于数据融合[14,19]，但在脆弱性利用威胁分析

方面的应用尚处于探索阶段.

本文旨在基于网络攻击图识别业务系统中各脆弱性利用威胁,并通过对网络攻击图进行分解以得到各脆弱性利用威胁所对应的子攻击图,并评估各脆弱性利用威胁度,以便对各脆弱性利用威胁进行优先级排序和处置.本文采用文献[20]中的攻击模型建模方法构建业务系统攻击模型,并基于攻击模型分析结果构建基于颜色 Petri 网(CPN)的网络攻击图,然后将网络攻击图进行分解,可一次性得到各脆弱性利用威胁所对应的子攻击图,并采用不确定性 D-S 证据推理方法,将安全威胁所对应的子攻击图转换为不确定性 D-S 推理规则集,采用 D-S 推理引擎计算各脆弱性利用威胁的威胁度.最后以一个典型 Web 系统为例,验证了本文所述安全威胁识别和分析方法的有效性.

2 安全威胁识别

2.1 网络攻击图定义和生成算法

为叙述方便,本文称单次脆弱性利用攻击为原子攻击.如图 1 所示,原子攻击包括三类要素,即原子攻击成功实施所依赖的前提条件、原子攻击动作本身以及攻击后果.其中,原子攻击前提条件包括攻击者权限、攻击可达性、服务活跃性和脆弱性存在性.攻击者权限指攻击者在源主机和目标主机上获得的权限级别,包括 None、User 和 Root 权限;攻击可达性指攻击者从源主机发起的原子攻击能否抵达目标主机;服务活跃性指原子攻击成功实施所依赖的服务是否在目标主机上运行;脆弱性存在性指攻击所利用的脆弱性在目标主机的服务中是否存在.在实际攻击中,只有满足这些前提条件的原子攻击才可能成功实施.原子攻击成功实施的结果主要表现为攻击者能力的提升,比如攻击者获得了目标主机上的 user 或 root 权限.

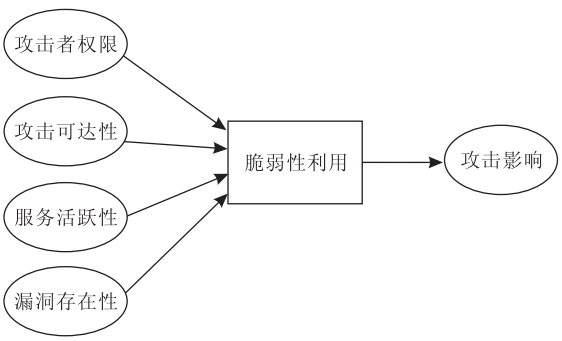


图 1 原子攻击

图 1 所述原子攻击其实是一个 CPN 网结构,其中,用来表示原子攻击前提条件和后果的椭圆形节点等同于 CPN 网结构中的库所;用来表示原子攻击动作本身的矩形节点等同于 CPN 网结构中的变迁.下面基于 CPN 给出原子攻击形式化定义.

定义 1. 原子攻击 AAG 是一个 CPN 网结构,记为 $AAG=\langle P_{Ao},t,P_{Ad}\rangle$,其中,$P_{Ao}$ 为所定义原子攻击的输入库所集合,每个库所代表一个攻击前提条件,它可定义为攻击者在源主机或目标主机上的初始权限、源主机到目标主机的攻击可达性、脆弱性所依赖服务的可用性及脆弱性存在性;t 为变迁,它表示原子攻击的一个脆弱性利用行为;P_{Ad} 为原子攻击的影响库所集合,其中每个库所记录该原子攻击成功实施后的效果.

图 2 为一个具体的原子攻击实例,假设攻击者要从其所控制的主机 1 利用主机 2 上的 IIS Web 服务中的一个缓冲区溢出漏洞(CVE-2002-0364),则必须满足以下 4 个条件:(1)攻击者在源主机 H_1 的权限至少为 User(记为椭圆 U_h1);(2)主机 1 可以访问主机 2 的 HTTP 服务(记为椭圆 http_h1_h2);(3)主机 2 上的 IIS5.0 Web 服务正在运行(记为椭圆 IIS_h2);(4)主机 2 上的 IIS5.0 服务存在一个编号为 CVE-2002-0364 的缓冲区溢出漏洞(记为椭圆 v364_h2).

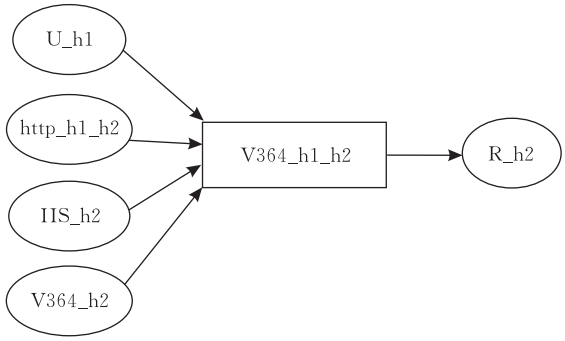


图 2 原子攻击实例

只有当以上 4 个条件都满足时,攻击者才可能成功的从 H_1 上发起对 H_2 上 IIS Web 服务的攻击(记为矩形 v364_h1_h2),攻击结果是,攻击者可能获得了 H_2 上的 Root 权限(记为椭圆 R_h2).

本文采用文献[20]中的攻击建模方法构建攻击模型,所创建的攻击模型为一个 CPN 系统.所述攻击模型基于攻击能力增长假设.定理证明:该攻击模型所对应 CPN 系统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 CPN 系统进入死状态时,SuccessExploitList 库所包含了攻击者成

功执行的所有脆弱性利用动作.由于可以采用 CPN 仿真方法代替复杂度较高的可达图分析方法,因此,所述攻击模型分析方法具有较好扩展性,非常适合大规模网络的攻击建模.

CPN 攻击模型仿真结束后,融合库所 SuccessExploitList 中保存有本次攻击过程中所有可能成功执行的脆弱性利用攻击动作.根据定义 1 可知,每个脆弱性利用动作可用原子攻击 CPN 模型表示.当各原子攻击建模结束后,可以根据各原子攻击之间依赖关系构建网络攻击图.下面给出网络攻击图的定义.

定义 2.　网络攻击图 AG 是一个 CPN 网结构,记为 $AG=\langle P_0\cup P_d, T_0\cup T_d, E\rangle$,其中,初始库所集合 P_0 中每个库所代表网络和攻击者的初始状态,表示原子攻击成功实施的前提条件;可达库所集合 P_d 中每个库所代表网络和攻击者的可达状态,它记录原子攻击成功实施后的效果;T_0 为独立型变迁集合,对于 T_0 中各变迁,其输入库所包含在初始库所集合 P_0 中,因此,T_0 中各变迁所代表的原子攻击的实施不依赖于其它原子攻击;T_d 为依赖型变迁集合,对于 T_d 中各变迁,其输入库所集合中至少有一个库所属于可达库所集合 P_d,因此,成功实施 T_d 中各变迁所代表的原子攻击必须依赖于其它原子攻击;E 为连接 CPN 攻击图中库所和变迁的有向弧.网络攻击图 AG 满足如下约束:① 攻击图 AG 中的有向弧只能连接库所和变迁,或者连接变迁和库所,即 $E\subset((P_0\cup P_d)\times(T_0\cup T_d))\cup((T_0\cup T_d)\times(P_0\cup P_d))$;② 对于独立型变迁集合 T_0 中任一元素 t,$pre(t)$ 表示该变迁的输入库所集合,$post(t)$ 表示该变迁的输出库所集合,则 $(pre(t)\subseteq P_0)\wedge(post(t)\subseteq P_d)$;③ 对于依赖型变迁集合 T_d 中任一元素 t,$pre(t)$ 表示该变迁的输入库所集合,$post(t)$ 表示该变迁的输出库所集合,则 $(\exists p\in pre(t): p\in P_d)\wedge(post(t)\subseteq P_d)$.

算法 1.　网络攻击图生成算法(NAGG).

输入:CPN 攻击模型中记录着所有成功的脆弱性利用动作列表的融合库所 SuccessExploitList 值;根据 CVE 定义的脆弱性利用信息数据库 CVEDB;攻击者在主机 host0 上所需拥有的初始权限 Root,记为 token "root(host0)"

输出:网络攻击图 $AG=\langle P_0\cup P_d, T_0\cup T_d, E\rangle$

1. $P_0=\{\text{Markeplace(root(host0))}\}$, $P_d=\varnothing$, $T_0=\varnothing$, $T_d=\varnothing$, $E=\varnothing$;
2. $AG=\langle P_0\cup P_d, T_0\cup T_d, E\rangle$
3. for each sel in SuccessExploitList
4. begin
5. sel(sn,dn,vid)=split(sel);
6. cveentry(vid,st,snm,mt,vt,or,dr,rr)=(searchCVEDB (CVEDB,vid));
7. atomic_model=ConstructAtomicExploitModule(sel,cveentry);
8. AG=AppendAtomicModuletoCPN(AG,atomic_ model);
9. end
10. return AG.

算法 1 给出了基于 CPN 攻击模型中融合库所 SuccessExploitList token 值的网络攻击图生成(NAGG)算法.算法第 1 行和第 2 行将初始攻击图 AG 置为空,调用 Makeplace 过程创建一个表示攻击者拥有 h_0 主机上 root 权限的库所,并加入到初始攻击图 AG 中.第 3 行到第 9 行为一个循环,它为 SuccessExploitList 中记录的每个脆弱性利用动作 sel 构造原子攻击 CPN 网结构,然后追加到当前攻击图 AG 中.其中,第 5 行对 sel 进行分解;第 6 行根据脆弱性利用漏洞编号检索 CVEDB 数据库,得到该脆弱性对应 CVE 条目 cveentry;第 7 行利用 sel 和 cveentry 输入数据,根据原子攻击的 CPN 网结构(如图 5 所示)构造相应的 CPN 模块;第 8 行将构造的原子攻击 CPN 模块追加到当前攻击图 AG 中;第 10 行返回生成的网络攻击图 AG.

为确保网络攻击图 AG 中脆弱性利用的前提条件和后果所对应库所及原子攻击所对应变迁的唯一性,NAGG 算法对脆弱性利用相关库所和变迁进行规范命名.NAGG 算法采用如下规范命名规则来命名各库所和变迁:

(1)前提条件"攻击者权限"(包括攻击者在源主机和目标主机上具有的权限),表示为"权限级别(主机编号)",其对应库所命名为"权限级别_主机".如,在构造攻击图时,攻击者在 h1 上具有的权限 User(h1)所对应的库所名为 U_h1.

(2)前提条件"攻击可达性",表示为"协议(源主机,目标主机)",此前提条件对应库所命名为"协议_源主机_目标主机".如,在构造攻击图时,主机 h1 和 h2 之间 http 协议的可达性 http(h1,h2)对应库所名为 http_h1_h2.

(3)前提条件"服务活跃性",表示为"服务名(主机名)",对应库所命名为"服务名_主机名".如,在构造攻击图时,主机 h1 上的 IIS 服务 IIS50(h1)所对应的库所名为 IIS50_h1.

(4)前提条件"漏洞存在性",表示为"漏洞编号(主机名)",相应库所命名为"漏洞编号_主机名".

(5)对于脆弱性利用后果,本文仅指攻击者获得的权限,因此,其命名方法和对应库所命名方法与

前提条件“攻击者权限”相同.

(6)某一脆弱性利用动作表示为“漏洞编号(源主机,目标主机)”,其相应变迁命名为“漏洞编号_源主机_目标主机”.如在构造攻击图时,脆弱性利用动作 CVE364(h1,h2)对应的变迁名称为 v364_h1_h2.

3 网络攻击图分解算法

算法 1 所示网络攻击图生成 NAGG 算法所构造的网络攻击图 AG 包含了系统所有可能的攻击路径,以及攻击者所有可能获得的攻击权限.为了对特定脆弱性利用威胁进行重点分析和优先处置,需要基于各脆弱性利用威胁,对网络攻击图进行分解,以获得各安全威胁对应的子攻击图.子攻击图包含了攻击者从初始节点出发抵达指定威胁目标的所有可能攻击路径.这里给出一个基于 CPN 的网络攻击图分解算法,可一次性分解出各脆弱性利用威胁所对应的子攻击图,所述子攻击图不存在循环路径且最长攻击路径不超过预设值.攻击图相关定义和网络攻击图分解算法如下.

3.1 网络攻击图分解算法和相关定义

定义 3. 攻击路径.设 $Path=t_1\rightarrow t_2\rightarrow\cdots\rightarrow t_n$ 是给定网络攻击图 AG 中的一个变迁序列,其中 $t_i(1\leq i\leq n)$ 为变迁,它代表一个原子攻击,则称满足下面约束条件的变迁序列为攻击路径:① 变迁 t_1 为独立型变迁;② 变迁 t_n 的输出库所集合 $Potst(t_n)$ 与关键节点集合 P 的交集不为空;③ 变迁序列中前驱变迁的输出库所为后继变迁的输入库所.攻击路径长度为攻击路径所对应的变迁序列长度.

定义 4. 脆弱性利用威胁定义为 $SR_i=\langle P_C^i\rangle$,其中 P_C^i 为攻击者在某关键节点上所获得的危害业务系统安全的权限集合,脆弱性利用威胁所对应的子攻击图只包含了从初始节点出发抵达集合 P_C^i 中各元素所示权限的攻击路径.本文所指威胁除特别说明外,均为脆弱性利用威胁.

网络攻击图分解需要解决两个问题:(1)循环攻击路径问题;(2)超长攻击路径问题.根据攻击者能力单调增长特性可知,实际攻击过程中攻击者没有必要重复获取已获得的攻击能力,因此循环攻击路径没有实际意义,并且循环攻击路径的存在会增加子攻击图分析复杂度.根据以往对黑客攻击事件的研究显示,实际网络攻击场景中,并不存在超长的攻击路径[12].这里首先给出子攻击图定义,然后给出一个可以消除循环攻击路径和限制攻击路径长度的网络攻击图分解(NAGD)算法.

定义 5. 子攻击图.某脆弱性利用威胁 $SR=\langle P_C\rangle$ 所对应的子攻击图为满足下述条件的网络攻击图 $AG=\langle P_0\cup P_d,T_0\cup T_d,E\rangle$,记 AG 的所有攻击路径集合为 $PATH_{AG}$:(1)不存在循环路径,即对 $\forall p(t_1,t_2,\cdots,t_l)\in PATH_{AG}$,有 $Post(t_i)\bigcap(\bigcup_{k=1}^{i-1}Pre(k))=\varnothing,2\leq i\leq l_k$;(2)任意攻击路径长度不超过指定常数 $N(N\geq 1)$,即 $\forall p(t_1,t_2,\cdots,t_l)\in PATH_{AG}$,$Len(p)\leq N$;(3)任一攻击路径抵达的目标必然为脆弱性利用威胁 SR 中的节点,即 $\forall p(t_1,t_2,\cdots,t_l)\in PATH_{AG},Len(p)\leq N,Post(t_l)\bigcap P_C\neq\varnothing$.

算法 2 为 NAGD 算法,其中,代码第 1 到第 7 行将网络攻击图所对应的 CPN 网结构转换为可仿真 CPN 系统;代码第 8 行对转换后的 CPN 系统进行仿真,仿真必然在有限步停止;代码第 9 到 15 行根据仿真结束后各脆弱性利用威胁相关库所记录的攻击路径列表对网络攻击图进行分解,得到各威胁对应的子攻击图.NAGD 算法可在只执行一次网络攻击图转换和 CPN 系统仿真前提下,一次性得到各脆弱性利用威胁所对应的子攻击图.

算法 2. 网络攻击图分解算法(NAGD).

输入:需分解的 CPN 网络攻击图 $AG=\langle P_0\cup P_d,T_0\cup T_d,E\rangle$;脆弱性利用威胁列表 $\{\langle P_c^i\rangle\}_{i=1..n}$;子攻击图中允许的最大攻击路径长度 N

输出:$\langle P_c^i\rangle$ 中各威胁相关子攻击图 $AGS_i=\langle P_0'\cup P_d',T_0'\cup T_d',E'\rangle$ 的列表 $\{AGS_i\}_{i=1..n}$,其中每条攻击路径长度不大于 N

```
1.  P0'=∅, Pd'=∅, T0'=∅, Td'=∅, E'=∅;
2.  AG'=⟨P0'∪Pd', T0'∪Td', E'⟩;
3.  for each t in T0∪Td do begin
4.      AAG=ObtainAAG(t);
5.      AAG'=AAGtoCPN(AAG, N);
6.      AG'=AppendCPNModel(AAG', AG');
7.  end
8.  CPNSimulate(AG');
9.  for i=1 to n do begin
10.     ValidTransSet=
            ObtaintransitionSetfromPc(AG', Pc^i);
11.     AGS_i=AG;
12.     for each t in T0∪Td do begin
13.         If (t∉ValidTransSet)
                then RemovetransitionfromCPN(AGS_i, t)
14.     end
15. end
16. return {AGS_i}_{i=1..n}.
```

在算法 2 所示的 NAGD 算法中,函数 AAGtoCPN 将原子攻击 $AAG=\langle P_{A0},t,P_{Ad}\rangle$ 转换为可仿真 CPN 子模块 AAG',它是 NAGD 算法实现的关

键步骤. 该函数所用到的颜色类型定义见表 1. 函数 AAGtoCPN 伪代码如算法 3 所示，其中，代码 1～4 行为 P_{A0} 中各输入库所指定颜色类型 APT，并为属于初始库所集合 P_0 的各输入库所建立一个攻击路径和攻击者能力列表都为空的 token；代码第 5 行为输出库所 P_{Ad} 中各库所指定颜色类型 APT；代码 6～8 行将($P_{A0}\times t$)中各输入弧改为双向弧，以避免变迁 t 与其它变迁在输入库所代表的攻击条件上形成竞争；同时为双向弧附上可将 APT 类型 token 分解为攻击路径和攻击能力列表的脚本表达式；代码第 9～11 行为($t\times P_{Ad}$)中各输出弧附上可将变迁 t 所代表的脆弱性利用行为追加到当前攻击路径中，以及将变迁 T 输出结果所代表的攻击者能力追加到当前攻击者能力列表中的弧表达式；代码第 12 行创建颜色类型为 APL 的库所 P_h，它记录了所有经过变迁 t 的攻击路径的列表，以防止仿真过程中变迁 t 的同一绑定被重复触发；代码第 14 行为变迁 t 添加 guard 函数，以去除攻击图中的循环路径和超长路径.

表 1　函数 AAGtoCPN 中用到的颜色类型定义说明列表

序号	颜色类型名称	定义	记录内容
1	AP	colset AP=list STRING	脆弱性利用过程中已经成功执行的原子攻击序列
2	AT	colset AT=list STRING	脆弱性利用过程中攻击者获得的能力或权限列表
3	APT	colset APT=product AP*AT	包括 AP 和 AT 两部分
4	APL	APL: colset APL=list AP	经过各变迁的攻击路径的列表

算法 3.　AAGtoCPN 函数伪代码.

输入：网络攻击图 $AG=\langle P_0\cup P_d, T_0\cup T_d, E\rangle$；需转化的原子攻击图 $AAG=\langle P_{A0}, t, P_{Ad}\rangle$

输出：AAG 相应的被转化的 CPN 子模块 AAG'

1. For each p in P_{Ao} do
2. AttachColorType(p,APT);
3. if $p\in P_0$ then AttachEmptyToken(p)
4. End for
5. For each p in P_{ad} do AttachColorT(p,APT); End for
6. For each e_i in ($P_{A0}\times t$) do
7. e_i=MakeDuralArc(e_i), $e_i\in(P_{A0}\times t)\hat{}e_i\in(t\times P_{A0})$; AttachSplitAPTExpr($e_i$)
8. End for
9. For each e_i in ($t\times P_{Ad}$)($t\times P_{Ad}$) do
10. AttachArcExpression(e_i, $MkExpr(Pre(e_i), Post(e_i))$)
11. End for
12. Ph=MakeHistoryPlace(APT);
13. AttachGurad(t);
14. return AAG.

图 3 为一个利用 AAGtoCPN 函数将与变迁 v2_0_3 相关的原子攻击网结构转换为可执行 CPN 子模块实例. 其中，设置输入库所 R_0，dns_0_3，bnd_h3 和 v2_h3 的颜色类型为 APT；设置输出库所 R_3 的颜色类型为 APT；分别为 4 个输入库所 R_0，dns_0_3，bnd_h3 和 v2_h3 附加初始 token 值“([],[])”；将从输入库所到变迁 v2_0_3 的 4 个输入弧设置为双向弧，并定义弧表达式为(p_i,t_i)；以表达式“(p1^^[“v2_0_3”],t1^^[“R_3”])”标识从变迁 v2_0_3 到库所 R_3 的输出弧(表达式中的^^为 CPN 语言中 list 元素追加运算符)，从而将变迁 v2_0_3 所代表的脆弱性利用行为追加到当前攻击路径中，同时将变迁 v2_0_3 成功执行后所获得的攻击权限(获得了 host3 上的 root 权限)追加到当前攻击者能力列表中；创建一个颜色类型为 APL 的历史库所 P_H，分别创建从 P_H 到 v2_0_3 和从 v2_0_3 到 P_H 的有向弧，并分别附加弧表达式“pl”和“pl^^[p1]”，以记录经过变迁 T 的所有攻击路径的列表.

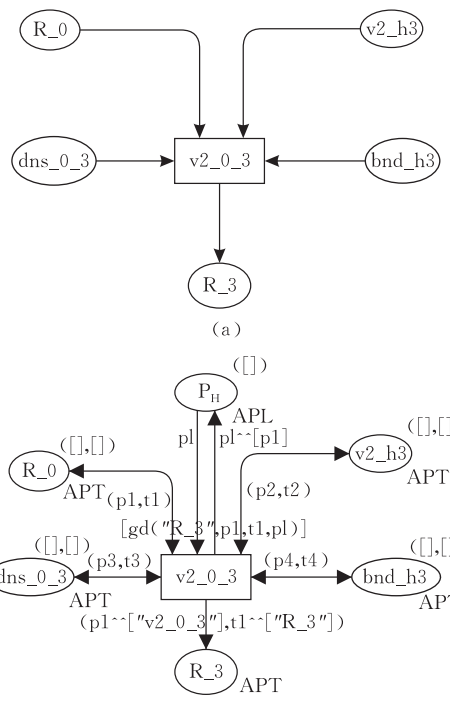


图 3　利用 AAGtoCPN 函数转换原子攻击例子

图 3 中，为变迁 v2_0_3 设置 guard 函数“gd(“R_3”,p1,t1,pl)”，以限定变迁 v2_0_3 所代表原子攻击的执行条件，限定条件为 3 个条件的与：① 该变迁的执行不会导致循环攻击路径；② 该变迁

的执行不会获取到重复的攻击权限；③ 该变迁所在攻击路径长度不超过指定值.

3.2 NAGD 算法复杂度分析

NAGD 算法包括转换、仿真和裁剪 3 个步骤，其算法复杂度主要由第 8 行的 CPN 系统仿真复杂度决定，因此，这里只分析 CPN 系统的仿真复杂度. 为说明 NAGD 算法的正确性和有效性，这里给出两个定理.

定理 1. NAGD 算法中，由网络攻击图转换而来的 CPN 系统仿真复杂度为 $O(m(k_{tout}k_{pout})^N)$，其中，m 为网络攻击图中的独立型变迁数量；k_{pout} 为库所最大输出度；k_{tout} 为变迁最大输出度；N 为子攻击图中允许的攻击路径最大长度.

证明. 采用数学归纳法证明. 假设网络攻击图所对应的 CPN 网结构中，各库所 a_i 输出度最大为 k_{pout}；各变迁 T_i 输出度最大为 k_{tout}；网络攻击图中存在 m 个独立型变迁. 假设子攻击图中允许出现的最大攻击路径长度为 1，则只有 m 个独立型变迁能被触发，因此，CPN 系统在 m 步仿真后停止，这 m 个独立型变迁将最多向 mk_{tout} 个库所输出 token；假设子攻击图中允许出现的最大攻击路径长度为 2，则由第 1 步攻击所得到的最多 mk_{tout} 个 token 将可能触发最多 $mk_{tout}k_{pout}$ 个变迁，这些变迁将向最多 $mk_{tout}^2k_{pout}$ 个库所输出 token；假设子攻击图中允许出现的最大攻击路径长度为 3，则第 3 步可能触发的变迁数最多为 $mk_{tout}^2k_{pout}^2$ 个；利用归纳法可知，在子攻击图中允许出现的最大攻击路径长度为 N 的情况下，第 N 步攻击可能触发的变迁数最多为 $mk_{tout}^{N-1}k_{pout}^{N-1}$ 个. 因此，在连续 N 步攻击中，CPN 系统仿真所触发的变迁数最多为 $(m+mk_{tout}k_{pout}+mk_{tout}^2k_{pout}^2+\cdots+mk_{tout}^{N-1}k_{pout}^{N-1})=m(k_{tout}^Nk_{pout}^N-1)/(k_{tout}k_{pout}-1)$. 因此，由网络攻击图转换而来的 CPN 系统仿真复杂度为 $O(m(k_{tout}k_{pout})^N)$. 证毕.

在网络攻击图中，独立型变迁数 m 一般为较小值，变迁最大输出度 k_{tout} 和库所最大输出度 k_{pout} 为较小常数；最大攻击路径 N 一般长度为 3 或 4. 综上所述，算法 2 所示的网络攻击图分解 NAGD 算法计算复杂度与文献[12]中求取 N-有效攻击路径计算方法相比复杂度更小，且本文所述 NAGD 算法可一次性求出各脆弱性利用威胁所对应的子攻击图，比文献[12]中所述一次只能求取一个关键节点集合的 N-有效攻击路径灵活性更好.

定理 2. NAGD 算法中，由网络攻击图所对应的 CPN 网结构转换而来的 CPN 系统在有限步仿真后一定进入死状态，且有且仅有一个死状态；在死状态时，各威胁节点对应库所 token 值包含了攻击者抵达脆弱性利用威胁节点的所有无环和最大长度不超过 N 的攻击路径集合.

定理 2 证明与文献[20]中的定理 1 证明类似，首先证明可采用 CPN 系统仿真代替 CPN 可达图分析法，然后基于本文定理 1 可得定理 2 结论. 由于篇幅所限，定理 2 证明过程从略.

4 脆弱性利用威胁度评估

本文采用 D-S 证据不确定性推理方法评估各脆弱性利用威胁的威胁度. 这里首先给出脆弱性利用威胁度和 D-S 证据推理相关定义，然后给出脆弱性利用威胁度评估 VETE 算法.

定义 6. 脆弱性利用威胁度为从指定脆弱性利用威胁的子攻击图 AAG 到区间[0,1]的映射 f：$AAG\rightarrow[0,1]$，用来综合评估攻击者达到脆弱性利用目标的成功率，攻击者达到脆弱性利用目标成功率越大，脆弱性利用威胁度越大，反之越小.

定义 7. 具有不确定性的推理规则可表示为 IF E then H, CF；其中 H 为假设，表示为 $H=\{a_1,a_2,\cdots,a_m\}$，$a_i\in\Omega$；E 为支持 H 成立的假设集，它们是命题的逻辑组合，CF 为可信度因子，$CF=\{c_1,c_2,\cdots,c_m\}$，$c_i$ 用来描述前提 E 成立时 a_i 的可信度，且 c_i 满足如下条件：(1) $c_i\geq0$，$1\leq i\leq m$；(2) $\sum_{i=1}^{m}c_i\leq1$.

定义 8. 不确定性传递. 对于不确定性规则 IF E then H, CF，定义 $m(\{a_i\})=f(E)c_i(a_i=1,2,\cdots,m)$，并规定：① $m(\Omega)=1-\sum_{i=1}^{m}m(\{a_i\})$；② 对于 Ω 的所有其它子集 H，均有 $m(H)=0$.

定义 9. 不确定性组合. 当规则的前提(证据) E 是多个命题的合取或析取时，定义：

$f(E_1\wedge E_2\wedge\cdots\wedge E_n)=\min(f(E_1),f(E_2),\cdots,f(E_n))$，

$f(E_1\vee E_2\vee\cdots\vee E_n)=\max(f(E_1),f(E_2),\cdots,f(E_n))$.

当有 n 条规则支持同一结论时，即如果 $H=\{a_1,a_2,\cdots,a_m\}$，则

IF E_i then H, $CF_i(CF_i=\{C_{i1},C_{i2},\cdots,C_{im}\})$, $1\leq i\leq n$.

如果这些规则相互独立的支持结论 H 成立，则可以先计算

$m_i(\{a_1\},\{a_2\},\cdots,\{a_m\})=$

$(f(E_i)C_{i1},f(E_i)C_{i2},\cdots,f(E_i)C_{im})$，$1\leq i\leq n$，

$m_i(\{a_1\},\{a_2\},\cdots,\{a_m\})=$

$(f(E_i)\cdot C_{i1}, f(E_i)\cdot C_{i2}, \cdots, f(E_i)\cdot C_{im})$, $1\leq i\leq n$.

然后根据证据合成法则对 m_i 进行证据合成，得到所有规则对结论 H 的支持.

算法 4 给出基于 D-S 证据推理的 VETE 算法，它包括 3 组步骤：(1)第 1 行至第 6 行将子攻击图转换为如定义 7 所示的 IF-then 规则集，其中，对于子攻击图中每个变迁，算法第 3 行抽取该变迁所对应的原子攻击，第 4 行将原子攻击分解为原子攻击前提条件、原子攻击动作和原子攻击后果，算法第 5 行根据原子攻击分解结果生成 IF-then 规则；(2)第 7 行至第 10 行根据 CVSS 发布的脆弱性利用难易程度评估经验值和初始证据可信度等知识，将 IF-then 规则转换为 D-S 证据推理规则；(3)第 11 行利用 D-S 证据理论推理引擎对所生成的 D-S证据推理规则集进行不确定性推理，最终得到脆弱性利用威胁度.

算法 4.　VETE 算法.

输入：脆弱性利用威胁相关子攻击图 $SAG=\langle P_0\cup P_d, T_0\cup T_d, E\rangle$；已知脆弱性利用和证据知识库 $DSVE$

输出：子攻击图相关脆弱性利用威胁的威胁度 VEI

1. For each t in $T_0\cup T_d$ do
2. Begin
3. $aag=$ObtainAAG(t);
4. $\langle P_{Ao}, t, P_{Ad}\rangle=$DecomposeAAG($aag$);
5. $R_i=$Convert2IF-Then-Rule(P_{Ao}, t, P_{Ad});
6. End
7. For each r in $\{R_i\}$ do
8. Begin
9. $R_i'=$Convert2DSRule(r, $DSVE$);
10. end
11. $VEI=$DSReasoning($\{R_i'\}$);
12. return(VEI).

5　实验分析

本文建立了一个典型 Web 应用业务系统实验环境，用于验证基于攻击图的安全威胁识别和分析方法的有效性. 实验系统拓扑结构如图 4 所示，部署在网络信任域边界处的防火墙将系统网络分成内网、DMZ 区和可访问互联网的外网 3 个安全域，各安全域之间的安全策略如下：(1)外网用户只允许访问 DMZ 区 H_2 上的 Apache 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 PostgreSQL 服务；(3)禁止 H_2 和 H_3 直接访问内网中其它主机；(4)内网中的管理主机 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.

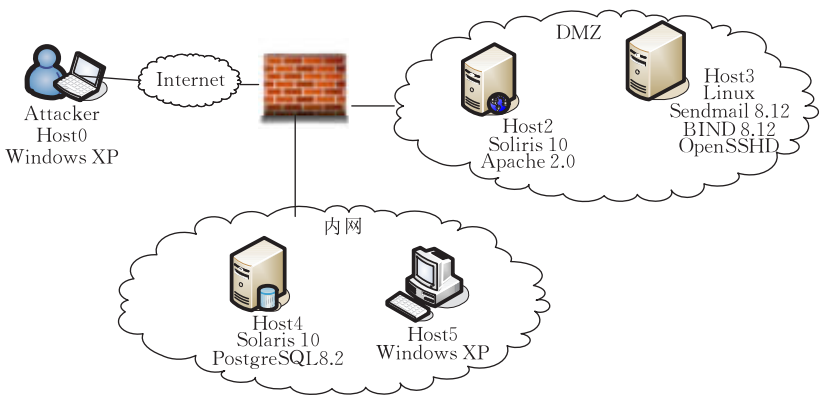


图 4　Web 系统拓扑图

表 2　Web 业务系统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	外网	攻击工具	无	无	无	0
H_2	DMZ	Apache2.0 (HTTP)	CVE-2011-3607(1)	(remote,1,0)	2	0.50
H_3	DMZ	BIND8.x (DNS) Sendmail (Mail) OpenSSHD (SSH)	CVE-2001-0010(2)	(remote,1,0)	1	0.40
			CVE-2002-1337(5)	(remote,1,0)	1	0.5
H_4	内网	OpenSSHD (SSH) PostgreSQL 8.2(SQL)	CVE-2002-0004(4)	(local,1,1)	2	0.4
			CVE-2010-4015(7)	(remote,1,0)	1	0.3
H_5	内网	IE 7.0 (HTTP) Outlook2007 (Mail)	CVE-2002-0193(6)	(remote,2,0)	1	0.3
			CVE-2008-0110(8)	(remote,1,0)	2	0.3
			CVE-2010-0816(3)	(remote,2,0)	2	0.2

应用文献[20]中给出的攻击建模方法为此Web业务系统建立攻击模型,然后利用标准工具CPN Tools[19]对该CPN攻击模型进行仿真.仿真结束后,融合库所SuccessExploitList的token数据为1′[(H_0,H_2,1),(H_0,H_3,2),(H_2,H_3,2),(H_2,H_3,5),(H_2,H_5,6),(H_2,H_4,7),(H_3,H_5,3),(H_5,H_4,7),(H_4,H_4,4),(H_4,H_3,2),(H_3,H_2,1),(H_4,H_3,5),(H_5,H_2,1),(H_5,H_3,2),(H_5,H_3,5),(H_4,H_2,1)].应用2.1节给出的NAGG算法构造基于CPN的网络攻击图如图5所示.从图5可以看出,攻击者在初始状态拥有主机H_0上的Root权限(用库所R_h0表示),它可以利用主机H_3上编号为2(CVE-2001-0010)的脆弱性,从而获得H_3上的Root权限,它由图5中名为v2_0_3的原子攻击表示;攻击者也可以利用主机H_2上编号为1(CVE-2011-3607)的脆弱性,从而获得H_2上的Root权限,它由图5中名为v1_0_2的原子攻击表示.

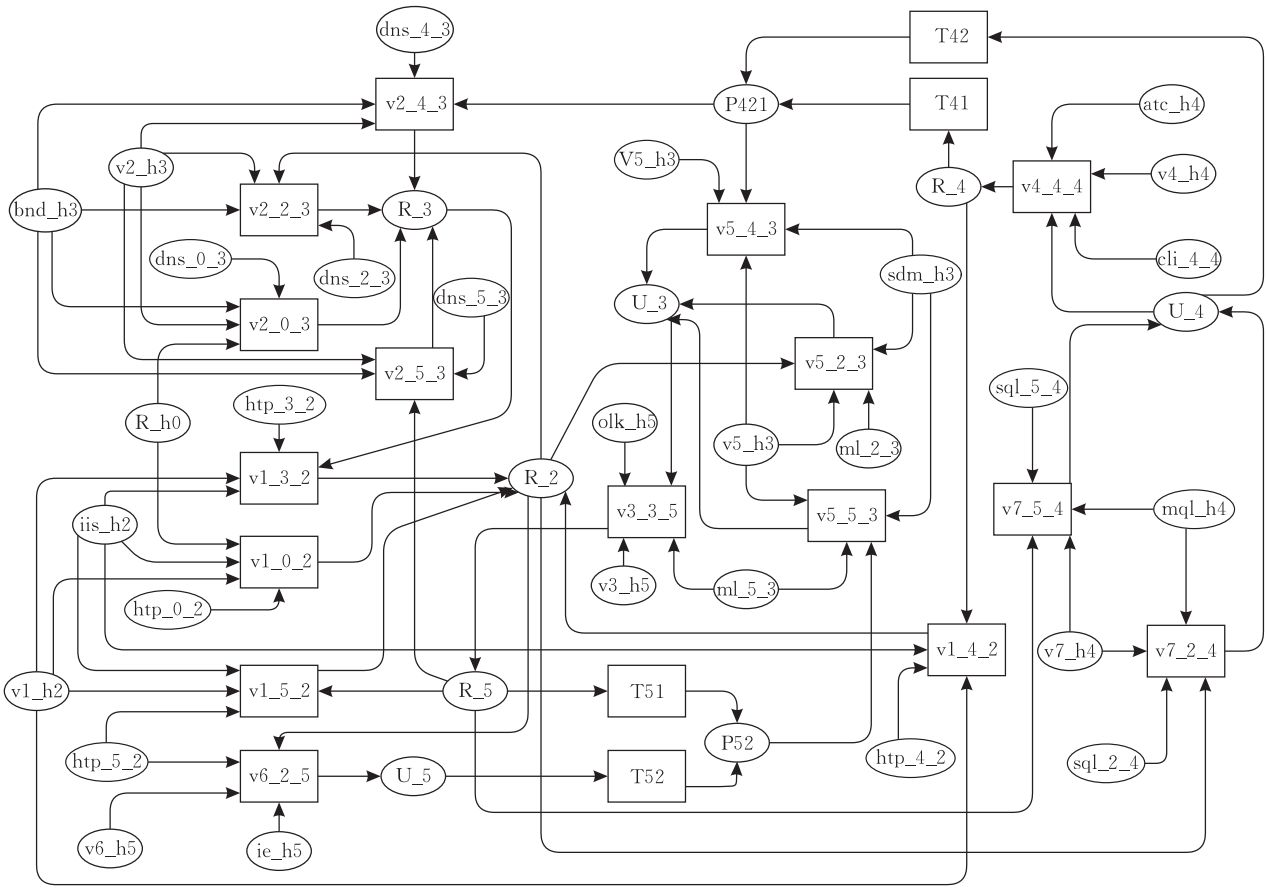


图5 由CPN攻击模型结果生成的网络攻击图

基于Web业务系统安全属性对图5所示的网络攻击图进行分析,可识别影响Web业务系统安全性的各种脆弱性利用安全威胁,即攻击者可能获得的影响业务系统网络节点安全属性的攻击权限.根据Web系统业务流和安全属性分析可知,影响到本业务系统安全的关键节点为H_2,H_3和H_4.容易从网络攻击图中识别出它们可能面临的脆弱性利用威胁分别为{R_2}、{R_3}、{U_4,R_4}和{U_5, R_5}.

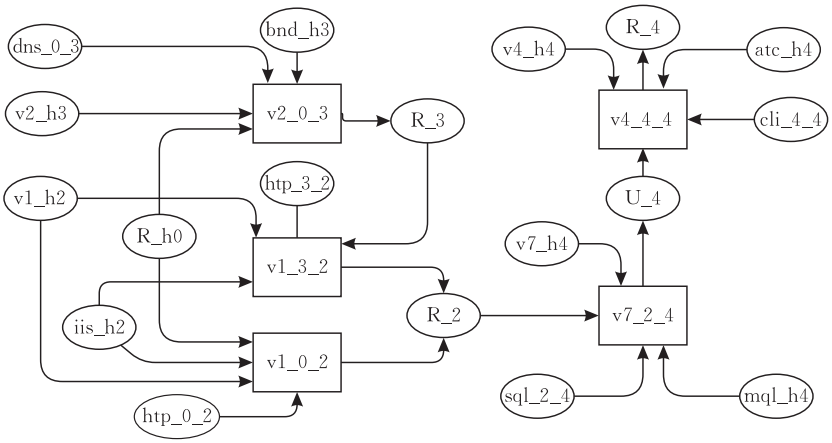
下面利用NAGD算法从网络攻击图分解出各脆弱性利用威胁所对应的子攻击图.这里假设在子攻击图中允许出现的最长攻击路径为3.NAGD算法第1阶段将图5所示的网络攻击图转换为可仿真CPN系统;第2阶段利用CPN Tools工具[21]对转换后的CPN系统进行仿真,仿真在有限步内结束后,各脆弱性利用威胁相关库所中包含了攻击者从初始节点出发抵达目标节点所有可能的步长不超过3的脆弱性利用攻击路径,因此,可以基于这些攻击路径信息对网络攻击图进行分解,一次性得到各种脆弱性利用威胁所对应的子攻击图.

这里以节点H_4和H_5面临的脆弱性利用威胁{U_4,R_4}和{U_5,R_5}为例,给出相应的子攻击图.网络攻击图仿真结束后,库所U_4的token值为1′([v1_0_2,v7_2_4],[R_2,U_4])++1′([v2_0_3, v1_3_2, v7_2_4], [R_3,R_2,U_4]),表明存在两条长度不超过3的攻击路径,使攻击者可以获得节点H_4上的User权限;库所R_4的token值为

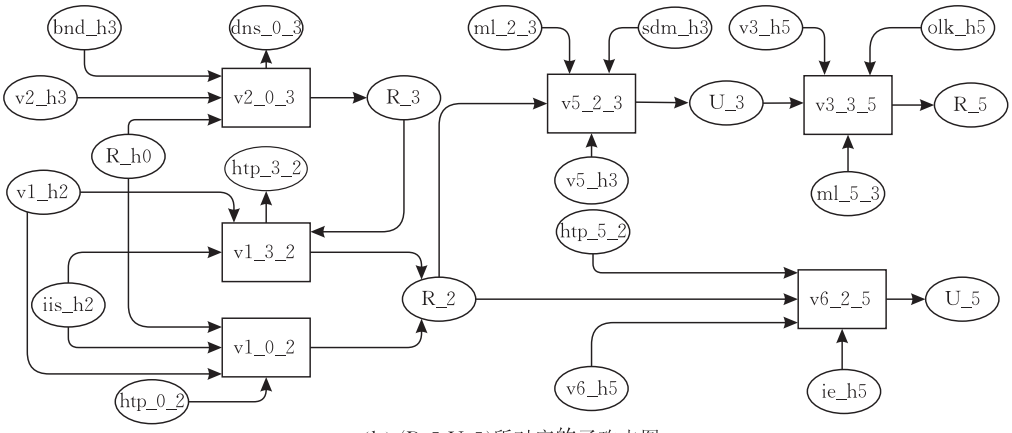
1′([v1_0_2,v7_2_4,v4_4_4],[R_2,U_4,R_4]),这表明存在一条长度不超过 3 的攻击路径,使得攻击者可以获得节点 H_4 上的 Root 权限.

脆弱性利用威胁{R_4,U_4}所对应的子攻击图如图 6(a)所示.类似地,对于脆弱性利用威胁{R_5,U_5},库所 R_5 的 token 值为 1′([v1_0_2,v5_2_3,v3_3_5],[R_2,U_3, R_5]),库所 U_5 的 token 值为 1′([v1_0_2,v6_2_5],[R_2,U_5])＋＋1′([v2_0_3,v1_3_2,v6_2_5],[R_3, R_2,U_5]),最后得到脆弱性利用威胁{R_5,U_5}对应的子攻击图如图 6(b)所示.由于篇幅问题,其余脆弱性利用威胁所对应的子攻击图说明从略.

在得到指定节点面临的各种脆弱性利用威胁所对应子攻击图后,下面根据 VETE 算法计算各脆弱性利用威胁度.由于篇幅问题,这里只给出脆弱性利用威胁{R_4,U_4}的脆弱性利用威胁度计算过程.首先,将图 6(a)所示的子攻击图转换为如图 7 所示的不确定性推理规则集;然后,根据初始证据可信度和脆弱性利用成功率经验值将不确定推理规则集转换为 D-S 不确定性推理规则集.这里假设各初始证据可信度为 1(即初始条件总成立),D-S 证据样本空间大小$|\Omega|=6$,基于 CVSS 知识库确定子攻击图中各脆弱性利用成功率和失败率(参见表 2 中利用成功率栏),从而确定对应推理规则的 CF 因子.



(a) {R_4,U_4}所对应的子攻击图



(b) {R_5,U_5}所对应的子攻击图

图 6　脆弱性利用威胁所对应的子攻击图实例

```
//v2_0_3脆弱性利用所对应的推理规则
r1: if (R_0^dns_0_3^bnd_h3^v2_h3) then R3={R_3}, CF1={0.4}
//v1_3_2脆弱性利用所对应的推理规则
r2: if (R_3^htp_3_2^iis_h2^v1_h2) then R2={R_2}, CF2={0.5}
//v1_0_2脆弱性利用所对应的推理规则
r3: if (R_0^htp_0_2^iis_h2^v1_h2) then R2={R_2}, CF3={0.5}
//v7_2_4脆弱性利用所对应的推理规则
r4: if (R_2^sql_2_4^mql_h4^v7_h4) then R4={U_4}, CF4={0.3}
//v4_4_4脆弱性利用所对应的推理规则
r5: if (U_4^cli_4_4^atc_h4^v4_h4) then R4={R_4}, CF4={0.4}
```

图 7　由图 6(a)转换而来的不确定性推理规则集

最后,根据 D-S 证据理论的不确定性推理算法求出脆弱性利用威胁{R_4,U_4}的威胁度.

(1) 根据 r1 求 R_3 的确定性

$$f(\text{R\_0}\hat{}\text{dns\_0\_3}\hat{}\text{bnd\_h3}\hat{}\text{v2\_h3})=\min(1.0,1.0,1.0,1.0)=1.0,$$

$$m_1(\{\text{R\_3}\})=(1.0\times 0.4)=(0.4),$$

$$Bel(\text{R\_3})=m_1(\{\text{R\_3}\})=0.4,$$

$$Pl(\text{R\_3})=1-Bel(\neg\text{R\_3})=1-0=1,$$

$$f(\text{R\_3})=Bel(\text{R\_3})+(|\{\text{R\_3}\}|/|\Omega|)\times$$

$$(Pl(\mathrm{R\_3})-Bel(\mathrm{R\_3}))$$
$$=0.4+1/6\times(1-0.4)$$
$$=0.5.$$

(2)求 R_2 确定性

根据规则 r2 和 r3,有

$$f(\mathrm{R\_3\hat{}htp\_3\_2\hat{}iis\_h2\hat{}v1\_h2})=\min(0.5,1.0,1.0,1.0)=0.5,$$
$$m_2(\{\mathrm{R\_2}\})=(0.5\times0.5)=(0.25),$$
$$f(\mathrm{R\_0\hat{}htp\_0\_2\hat{}iis\_h2\hat{}v1\_h2})=\min(1.0,1.0,1.0,1.0)=1.0,$$
$$m_3(\{\mathrm{R\_2}\})=(1.0\times0.5)=(0.5),$$
$$m_2(\Omega)=1-0.25=0.75,$$
$$m_3(\Omega)=1-0.5=0.5.$$

由 D-S 证据组合公式得到

$$K=\sum_{x\cap y\neq\varnothing}m_2(x)\times m_3(y)$$
$$=m_2(\Omega)m_3(\Omega)+m_2(\Omega)m_3(\mathrm{R\_2})+m_2(\mathrm{R\_2})m_3(\Omega)+m_2(\mathrm{R\_2})m_3(\mathrm{R\_2})$$
$$=0.75\times0.5+0.75\times0.5+0.25\times0.5+0.25\times0.5$$
$$=1.00,$$

则有

$$m_{23}(\{\mathrm{R\_2}\})=(m_2(\Omega)m_3(\{\mathrm{R\_2}\})+m_2(\{\mathrm{R\_2}\})m_3(\Omega)+m_2(\{\mathrm{R\_2}\})m_3(\mathrm{R\_2}))/K$$
$$=(0.75\times0.5+0.25\times0.5+0.25\times0.5)/1.0$$
$$=0.625,$$
$$Bel(\mathrm{R\_2})=m_{23}(\{\mathrm{R\_2}\})=0.625,$$
$$Pl(\mathrm{R\_2})=1-Bel(\neg\mathrm{R\_2})=1-0=1,$$
$$f(\mathrm{R\_2})=Bel(\mathrm{R\_2})+(|\{\mathrm{R\_2}\}|/|\Omega|)\times(Pl(\mathrm{R\_2})-Bel(\mathrm{R\_2}))$$
$$=0.625+(1/6)\times(1-0.625)$$
$$=0.687.$$

(3)求 U_4 确定性

$$f(\mathrm{R\_2\hat{}sql\_2\_4\hat{}mql\_h4\hat{}v7\_h4})=\min(0.688,1.0,1.0,1.0)=0.688,$$
$$m_4(\{\mathrm{U\_4}\})=(0.688\times0.5)=(0.344),$$
$$Bel(\mathrm{U\_4})=m_4(\{\mathrm{U\_4}\})=0.344=0.344,$$
$$Pl(\mathrm{U\_4})=1-Bel(\neg\mathrm{U\_4})=1-0=1,$$
$$f(\mathrm{U\_4})=Bel(\mathrm{U\_4})+(|\{\mathrm{U\_4}\}|/|\Omega|)\times(Pl(\mathrm{U\_4})-Bel(\mathrm{U\_4}))$$
$$=0.344+1/6\times(1-0.344)$$
$$=0.453.$$

(4)求 R_4 确定性

$$\mathrm{f(U\_4\hat{}cli\_4\_4\hat{}atc\_h4\hat{}v4\_h4})=\min(0.453,1.0,1.0,1.0)=0.453,$$
$$m_5(\{\mathrm{R\_4}\})=(0.453\times0.4)=(0.181),$$
$$Bel(\mathrm{R\_4})=m_5(\{\mathrm{R\_4}\})=0.181,$$
$$Pl(\mathrm{R\_4})=1-Bel(\neg\mathrm{R\_4})=1-0=1,$$
$$f(\mathrm{R\_4})=Bel(\mathrm{R\_4})+(|\{\mathrm{R\_4}\}|/|\Omega|)\times(Pl(\mathrm{R\_4})-Bel(\mathrm{R\_4}))$$
$$=0.181+1/6\times(1-0.181)=0.317.$$

通过 D-S 不确定性推理可知,在限定最长攻击路径为 3 的情形下,节点 H_4 面临的脆弱性利用威胁{R_4,U_4}的威胁度为 0.317.按照类似方法,可以求得其它节点面临的脆弱性利用威胁度,分别为{R_2}=0.665,{R_3}=0.413,{R_4,U_4}=0.317,{R_5,U_5}=0.215.最后,按照威胁度大小对各脆弱性利用威胁排序,得到影响 Web 业务系统安全性的各脆弱性利用威胁优先级排序:{R_2},{R_3},{R_4,U_4},{R_5,U_5},结果表明,脆弱性利用威胁{R_2}发生的可能性最大,脆弱性利用威胁{R_3}次之.

6 结论和进一步工作

本文提出了一种基于攻击图的安全威胁识别和分析方法,以分析和处置业务系统面临的各种脆弱性利用安全威胁;所述方法基于 CPN 攻击模型仿真分析结果构建基于 CPN 的网络攻击图,以分析业务系统整体安全性;与现有网络攻击图生成算法相比,本文所述方法可基于标准 CPN 分析工具实现,便于利用成熟 CPN 分析工具,且所构建的网络攻击图为一个 CPN 网结构,易于进一步分析.本文给出了一个可实现网络攻击图分解的 NAGD 算法,以获取各脆弱性利用威胁所对应的子攻击图;与现有子攻击图生成算法相比,本文所述算法在不增加算法复杂度情况下,可一次性得到各脆弱性利用威胁所对应的子攻击图.最后,本文给出了一种实现脆弱性利用威胁度评估的 VETE 算法,将子攻击图转换为不确定性 D-S 证据推理规则,利用 D-S 证据推理引擎计算脆弱性利用威胁度;与传统脆弱性利用分析方法相比,本方法选择 D-S 证据来描述系统中的不确定性,因而更具有合理性.本文最后以典型 Web 业务系统为例,验证了本文所述安全威胁和识别方法有效性.

进一步研究工作包括:(1)考虑在基于 CPN 的网络攻击图和子攻击图上实现更多的攻击图分析方法,包括基于子攻击图的攻击预测等;(2)寻找一种更合理的 D-S 初始证据的可信度赋值方法.

参 考 文 献

[1] Ritchey R, Ammann P. Using model checking to analyze network vulnerabilities//Proceedings of the 2000 IEEE Symposium on Research on Security and Privacy. Oakland, California, USA, 2000: 156-165

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

[3] Cheung S, Lindqvist U, Fong M W. Modeling multi-step cyber-attacks for scenario recognition//Proceedings of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX III). Washington, DC, USA, 2003: 284-292

[4] Mehta V, Bartzis C, Zhu H F. Ranking attack graphs//Zamboni D, Kruegel C eds. RAID 2006. Lecture Notes in Computer Science 4219. Berlin Heidelberg: Springer-Verlag, 2006: 127-144

[5] Wang LY, Noel S, Jajodia S. Minimum-cost network hardening using attack graphs. Computer Communications, 2006, 29(18): 3812-3824

[6] Sheyner O, Haines J, Jha S, Lippmann R, Wing J M. Automated generation and analysis of attack graphs//Proceedings of the 2002 IEEE Symposium on Security and Privacy. Berkeley, California, USA, 2002: 273-284

[7] Jajodia S, Noel S, O'Berry B. Topological analysis of network attack vulnerability//Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. Singapore, 2007: 2-2

[8] Ingols k, Lippmann R, Piwowarski K. Practical attack graph generation for network defense//Proceedings of the 22nd Annual Computer Security Applications Conference. Miami Beach, Florida, USA, 2006: 121-130

[9] Ingols K, Chu M, Lippmann R, Webster S, Boyer S. Modeling modern network attacks and countermeasures using attack graphs//Proceedings of the 25th Annual Computer Security Applications Conference. Honolulu, Hawaii, USA, 2009: 117-126

[10] Ou X M, Boyer W F, McQueen M A. A scalable approach to attack graph generation//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA, 2006: 336-345

[11] Homer J, Varikuti A, Ou X M, McQueen M A. Improving attack graph visualization through data reduction and attack grouping//Proceedings of the 5th International Workshop on Visualization for Computer Security (VizSec2008). Cambridge, MA, USA, 2008. Belin Heidelberg, Germany: Springer- Verlag, 2008: 68-79

[12] Chen Feng, Zhang Yi, Su Jin-Shu, Han Wen-Bao. Two formal analysis of attack graphs. Journal of Software, 2010, 21(4): 838-848(in Chinese)
(陈锋，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)

[13] Wang LY, Singhal A, Jajodia S. Toward measuring network security using attack graphs//Proceedings of the 2007 ACM Workshop on Quality of Protection. Alexandria, VA, USA, 2007: 49-54

[14] Zhang Shao-Jun. Research on key techniques in network security integrated management based on attack graphs [Ph.D. dissertation]. Shanghai Jiaotong University, Shanghai, 2010(in Chinese)
(张少俊. 基于攻击图的网络安全综合管理关键技术的研究[博士学位论文]. 上海交通大学，上海，2010)

[15] Steffan J, Schumacher M. Collaborative attack modeling//Proceedings of the 2002 ACM Symposium on Applied Computing(SAC). Madrid, Spain, 2002: 253-259

[16] Zhou S J, Qin Z G, Zhang F, Zhang X F,Chen W, Liu J D. Colored Petri net based attack modeling//Proceedings of the 9th International Conference Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing (RSFDGrC). Chongqing, China, 2003. Lecture Notes in Computer Science: Springer, 2003: 715-718

[17] Chen Si-Si, Lian Yi-Feng, Jia Wei. A network vulnerability evaluation method based on Bayesian networks. Journal of the Graduate School of the Chinese Academy of Sciences, 2008, 25(5): 639-648(in Chinese)
(陈思思，连一峰，贾炜. 基于贝叶斯网络的脆弱性状态评估方法. 中国科学院研究生院学报，2008，25(5)：639-648)

[18] Ye Yun, Xu Xi-Shan, Jia Yan, Qi Zhi-Chang. An attack graph-based probabilistic computing approach of network security. Chinese Journal of Computers, 2010, 33(10): 1987-1996(in Chinese)
(叶云，徐锡山，贾焰，齐治昌. 基于攻击图的网络安全概率计算方法. 计算机学报，2010，33(10)：1987-1996)

[19] Gao Hui-Sheng, Zhu Jing, Li Cong-Cong. The analysis of uncertainty of network security risk assessment using dempster-shafer theory//Proceedings of the 12th International Conference on the Computer Supported Cooperative Work in Design. Xian, China, 2008: 754-759

[20] Wu Di, Feng Deng-Guo, Lian Yi-Feng, Chen Kai. An efficiency evaluation model of system security measures in the given vulnerabilities set. Journal of Software, 2012, 23(7): 11880-11898(in Chinese)
(吴迪，冯登国，连一峰，陈恺. 一种给定脆弱性环境下的安全措施效用评估模型. 软件学报，2012，23(7)：11880-11898)

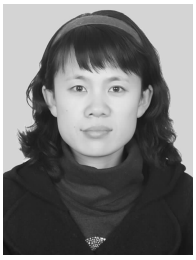
[21] Kijsanayothin P, Hewett R. Analytical approach to attack graph analysis for network security//Proceedings of the 2010 International Conference on Availability, Reliability and Security. Krakow, Poland, 2010. Washington, DC, USA: IEEE Computer Society Press, 2010: 25-32

[22] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis//Proceedings of the 9th ACM Conference on Computer and Communications Security. New York, USA, 2002: 217-224

[23] Noel S, Jajodia S. Managing attack graph complexity through visual hierarchical aggregation//Proceedings of the 2004 ACM CCS Workshop on Visualization and Data Mining for Computer Security. Fairfax, VA, USA, 2004: 109-118

[24] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs//Proceedings of the 15th IEEE Computer Security Foundations Workshop. Cape Breton, Nova Scotia, Canada, 2002: 49-63

[25] Laborde R, Nasser B, Grasset F, Barrère F, Benzekri A. A formal approach for the evaluation of network security mechanisms based on RBAC policies. Electronic Notes in Theoretical Computer Science (ENTCS), 2005, 121(4): 117-142



WU Di, born in 1977, Ph. D. candidate. Her research interests include network security, testing and evaluation of information security.

Lian Yi-Feng, born in 1974, Ph. D., associate professor. His research interests include network and information security.

CHEN Kai, born in 1982, Ph. D.. His research interests include information security, software vulnerability analysis and detection, malware analysis and prevention.

LIU Yu-Ling, born in 1982, Ph. D. candidate. His research interests include network security and performance assessment.

Background

Attack graph is an efficient method to analyze and evaluate vulnerability exploiting threats of information systems. The identification and analysis of each vulnerability exploiting path can help administrator to choose effective security measures to counter vulnerability exploiting threats and decrease security risk. In practical security administration scenario, we need both network attack graph to assess the security situation of the systems, and also need efficient method to dispose of the most harmful security vulnerability exploiting threats at the same time. Also, we need methods to handle uncertainties in the process of vulnerability exploiting threat analysis. Conventional methods use proprietary algorithms to construct network attack graph, which are complex and error-prone. Even when the network attack graph of the information system is constructed, there is still lack of effective method to generate sub-attack graphs for specific security threats, and also lack of assessment methods for specific security threats. This paper used CPN based attack model simulation results to generate network attack graph, which can leverage the efficiency of the current CPN analysis tools. Also a network attack graph decomposition algorithm is proposed to retrieve all the sub-attack-graphs corresponding to each attack threat at the same time with equivalent computation complexity. To assess the degree of a specific vulnerability exploiting threat, the sub-attack graph corresponding to a specific security threat is converted to inference rules with uncertainty, and the D-S evidence reasoning algorithm is used to calculate the degree of security threat. This topic is sponsored by the National High Technology Research and Development Program (863 Program) of China (Nos. 2009AA01Z439, 2011AA01A203), National Natural Science Foundation of China (No. 61100226), Beijing Natural Science Foundation (No. 4122085) and the Opening Project of Key Laboratory of Information Network Security of Ministry of Public Security (The Third Research Institute of Ministry of Public Security)(No. C10606). The funded projects are engaged in information security measure related research. This paper focuses on identification and analysis of the attack path and the assessment of system security threats. The author's main research fields are focused on evaluation of the network and information security.