

基于攻击图模型的网络安全风险评估研究

谢丽霞, 仇晓锐, 李学菲

(中国民航大学 计算机科学与技术学院, 天津 300300)

摘 要: 提出一种基于攻击图的多智能代理(Agent)的网络安全风险评估模型. 首先, 提出了基于多 Agent 的风险评估架构并给出了主 Agent 和子 Agent 的主要模块的功能设计, 以网络中主机上的组件为基本节点, 采用多 Agent 协同工作的方式构建攻击图. 其次, 定义五种风险指数并给出网络安全风险指数的计算方法. 最后, 基于 Java 的 Agent 开发框架(Java Agent Development Framework, JADE)实现了该评估模型, 通过对仿真网络的风险评估验证了此模型的可行性和有效性.

关键词: 风险评估; 分布式; 攻击路径; 攻击图; 多 Agent

中图分类号: TP309; TP393.08

文献标识码: A

文章编号: 1000-7180(2014)07-0077-07

Research on Network Security Risk Assessment Based on Attack Graph Model

XIE Li-xia, QIU Xiao-rui, LI Xue-fei

(School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: This paper proposes a multi-agent network security risk assessment model based on attack graph. Firstly, this paper proposes the architecture of multi-Agent risk assessment and gives the function design of main modules for main and subsidiary Agent. Multi-Agents are adopted to generate attack graph synergistically by using the components of network hosts as the basic nodes. Secondly, five risk indexes are defined and the method to compute the risk index of network security is given. Finally, the network security risk assessment model is performed based on the Java Agent Development Framework(JADE), and a risk assessment experiment with simulation network is conducted. The experimental results prove that our model is a feasible and effective approach to the network security risk assessment.

Key words: risk assessment; distribute; attack path; attack graph; multi-agent

1 引言

计算机网络的飞速发展促进了人类社会的进步, 与此同时, 网络攻击和破坏行为也日益普遍和多样. 如何保障计算机网络的安全, 对其实施安全风险的管理已成为人们关注的焦点. 而对网络信息系统进行客观有效的安全风险评估是进行安全风险管理的前提和基础. 当前网络安全评估的方法主要有 2 种,

分别为基于规则的方法和基于模型的方法^[1].

风险评估是对风险进行辨识和分析的过程, 主要包括对资产、威胁、脆弱性(漏洞)及三者发生的可能性^[2]. 网络攻击图能够准确地反映出存在于网络中的漏洞以及他们之间的相互关系, 在网络安全分析方面是一种比较有效的手段^[3]. 而多 Agent 系统由于其所拥有的社会性、自制性与协作性的特点, 在构建攻击图等方面具有优势.

收稿日期: 2013-09-07; **修回日期:** 2013-10-29

基金项目: 国家自然科学基金(61179045, 60776807); 国家科技重大专项(2012ZX03002002); 国家“八六三”计划重点课题(2006AA12A106); 天津市科技计划重点项目(09JCZDJC16800); 中国民航科技基金(MHRD201009, MHRD201205); 中央高校基本科研业务费专项(ZXH2009A006)

攻击图概念最早是在 1986 年由 Cunningham 等提出^[4]. 而在 1998 年, Phillips 和 Swiler 等人首次提出基于攻击图的网络安全分析方法^[5]. 该方法使用攻击行为模板描述相同的攻击行为, 然后根据攻击行为模板从攻击者预期网络的目标状态开始, 反向推测攻击者所有攻击行为序列和期间的网络状态, 最终生成状态攻击图^[4]. 在攻击图刚出现的时候, 研究者主要通过手工分析对攻击图进行研究分析, 但是随着网络的不断发展, 网络的拓扑结构越来越复杂以及安全漏洞的不断被发现, 通过手工来构造攻击图开始变得越发繁琐与低效, 因此通过模型检测器, 对其编写相应的算法使其能够自主的生成攻击图, 这种方式开始被研究者们所关注^[6-10].

研究人员发现随着主机和脆弱性数目的增加, 用模型检测方法生成攻击图的时间复杂度呈指数级增长, 出现状态空间爆炸问题, 并且用实验证明了这点^[9]. 因此 Ammann 等人在后来的研究中放弃了模型检测方法而使用一种基于图论的方法生成攻击图^[11].

目前攻击图的表示方式主要有 2 种, 一是用顶点和有向边来表示, 二是用邻接矩阵来表示^[12]. 而为避免状态空间爆炸, 本文以网络中主机上的组件为基本节点, 引入 Agent 技术, 采用多 Agent 协同方式分析可能存在的攻击路径为边构建攻击图, 在此基础上对整个网络进行安全风险评估.

2 基于多 Agent 的风险评估模型

2.1 评估模型的架构设计

本文设计的评估模型包含两类 Agent, 分别是子 Agent 和主 Agent, 子 Agent 有多个, 主 Agent 只有一个. 子 Agent 散布于网络的各个主机上, 重点评估其所在主机及主机上组件的安全风险; 主 Agent 协调整个风险评估过程, 构造攻击图, 并计算网络整体风险. 评估模型架构如图 1 所示.

2.2 Agent 的模块功能设计

(1) 风险评估模型子 Agent 的主要模块包括: 本地漏洞扫描、关联关系发现、攻击分析、通信等模块. 每个模块的具体功能设计如下:

①本地漏洞扫描模块. 子 Agent 扫描主机上的安全漏洞, 并向主 Agent 报告. 子 Agent 根据主 Agent 返回数据初始化本地漏洞库和攻击规则库.

②关联关系发现模块. 关联关系是安全风险评估的另一重要依据. 张永铮等人在文献^[13]中对关联关系的发现进行了探讨, 本文采用张永铮的研究

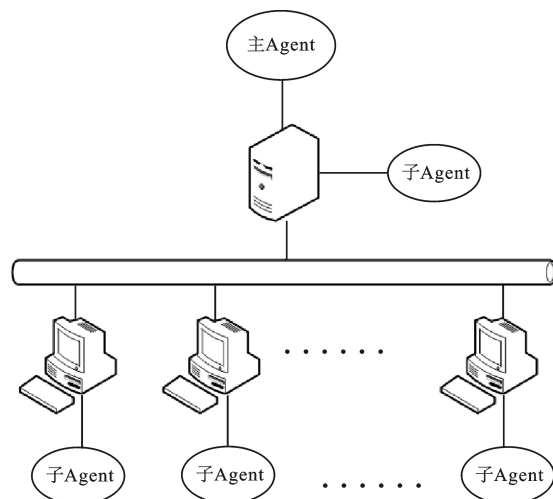


图 1 风险评估模型架构示意图

成果, 用工具自动探测和手动分析相结合的方式发现网络中的关联关系.

③攻击分析模块. 攻击过程分析是网络安全风险评估的核心步骤. 子 Agent 根据主机的漏洞和关联关系, 结合对应的攻击规则, 对可能发生的非法访问过程进行全面的分析. 由于关联关系的传递性, 攻击者成功攻击某一主机的组件后, 也获得了该组件对其他组件的访问权, 子 Agent 必须将这种变化了的关联关系通知对应的其他子 Agent, 以便其他子 Agent 进行更进一步的攻击分析. 攻击者成功攻击组件后还可能会植入新的漏洞, 因此攻击分析时还可能会有对本地漏洞库的更新.

④通信模块. 分布式评估模型中的所有 Agent 协同工作完成网络整体的安全风险评估. 子 Agent 与主 Agent 以及子 Agent 之间的协同通过相互发送协同消息实现, 这一功能由通信模块提供.

(2) 风险评估模型中的子 Agent 的主要模块包括: 攻击规则匹配、关联关系分析、风险计算、通信和协同消息等模块. 每个模块的具体功能设计如下:

①攻击规则匹配模块. 接收子 Agent 的攻击规则请求, 将与子 Agent 所在主机相关的攻击规则返回. 攻击规则匹配以漏洞为依据, 该模块根据子 Agent 发送的漏洞信息匹配攻击规则库中的攻击规则. 在向子 Agent 返回攻击规则的同时, 主 Agent 将与漏洞相关的量化指标一并返回, 以便在风险分析计算阶段量化评估网络的安全风险.

②关联关系分析模块. 汇总所有子 Agent 的关联关系报告, 将这些关联关系分析整理后向每个子 Agent 返回.

③风险计算模块. 接收子 Agent 的分析结果,

在此基础上计算网络中主机的组件、主机以及网络整体的安全风险. 风险计算模块还评估每个漏洞和每条关联关系给网络带来的风险, 并对其带来的风险指数大小排序, 给网络管理者采取安全防护措施提供参考.

④通信模块. 负责主 Agent 与子 Agent 的通信, 把接收到的子 Agent 消息进行分类并发送至主 Agent 相应模块, 处理完成后将结果向子 Agent 返回.

(3) 协同消息模块. 模型中的各 Agent 通过通信模块传递协同消息协同工作. 协同消息分为数据请求消息, 数据消息和通知消息.

当 Agent 需要通过其他 Agent 获取数据时, 就向对应的 Agent 发送数据请求消息. 数据消息有两种, 一种对应与数据请求消息, 可以认为是数据请求消息的响应消息; 另一种是包含风险计算结果、网络状态变化等信息的数据消息. 在评估过程中, Agent 需要将分析结果等信息通知其他 Agent, 此类信息通过数据消息传递. 在本文的评估模型中, 通知消息只有一种, 主 Agent 在攻击图构建完毕后发送通知消息通知各子 Agent 攻击图构建完成, 子 Agent 收到通知后结束监听状态, 转入风险计算阶段.

3 攻击图的生成

3.1 基于主从 Agent 的攻击图构建

攻击图构建由各子 Agent 和主 Agent 协同工作共同完成. 子 Agent 发现可能存在的攻击路径, 计算攻击成功概率并向主 Agent 报告; 主 Agent 根据子 Agent 报告的攻击路径构建攻击图.

在网络漏洞和攻击手段日益增多的今天, 需要时常对漏洞库和攻击规则库进行更新, 因此, 为了管理和维护的方便, 评估模型中由主 Agent 维护全局漏洞库和攻击规则库. 子 Agent 进行攻击路径分析时要向主 Agent 请求, 动态生成本地漏洞库和攻击规则库. 漏洞和攻击规则信息收集过程如图 2 所示.

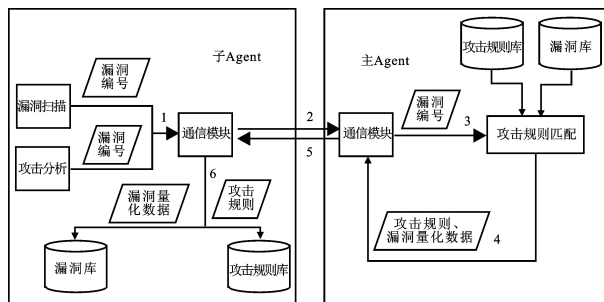


图 2 漏洞和攻击规则信息收集流程图

子 Agent 首先运行漏洞扫描模块, 扫描本地漏洞, 扫描结束后依据漏洞编号向主 Agent 发送数据请求消息请求漏洞量化数据和攻击规则. 主 Agent 根据漏洞编号检索全局漏洞库和攻击规则库, 返回漏洞的量化数据以及对应于漏洞的攻击规则, 子 Agent 接收数据并更新本地漏洞库和攻击规则库.

由于网络攻击后可能包括新漏洞的植入, 因此在攻击分析过程中也必须对本地漏洞库和攻击规则库进行更新.

3.2 关联关系的发现

首先由手动分析和各子 Agent 用工具自动探测相结合的方式寻找本地关联关系, 然后向主 Agent 报告. 主 Agent 对所有子 Agent 发送来的关联关系信息处理汇总之后, 将全网关联关系保存到关联关系库中, 然后对关系库中的数据进行分析, 向子 Agent 返回所有与其所在主机组件相关的关联关系. 简单来说就是主机用户都很清楚主机各组件对其他服务的访问关系, 但不能掌握网络全局信息, 所以需要主 Agent 对全网关联关系处理汇总之后把与每个子 Agent 所在主机组件里边相关的关联关系发送给子 Agent 供其分析攻击者可能将要发起的攻击过程.

随着子 Agent 对攻击过程的分析, 会产生由非授权入侵等攻击行为触发的关联关系的变化, 此时要根据攻击后果及时通知子 Agent 并更新主 Agent 关联关系库.

主 Agent 上的攻击图的构建算法如图 3 所示.

```

Input: 网络主机上存在的所有组件 components, 子 Agent
对攻击路径进行分析所得的结果
Output: 生成的攻击图
begin
  监听从子 Agent 所发来的消息;
  While(消息队列非空)
  {
    getMessage(); // 取出消息队列中的一条消息
    If(消息是子 Agent 分析所得的攻击路径的结果)
    {
      if(在节点  $A_i$  与  $B_j$  之间原本不存在边 || 新得出的
      风险指数比原来存在的边的风险指数大)
      将攻击图中的节点  $A_i$  与  $B_j$  之间的边的信息更新为  $E$ 
      ( $A_i, B_j, Attseq, P$ );
    }
    if(消息队列中没有剩余的消息 || 时间超时)
    将攻击图构建已经结束的消息发送给子 Agent;
  }
end
  
```

图 3 攻击图的构建算法

4 安全风险的计算

4.1 安全风险指数

网络风险指数评估采用自下而上的计算方法,依据攻击图中的攻击路径计算组件风险,在此基础上计算主机和网络安全风险.所以,本文提出的风险评估模型主要获取和计算五种风险指数:攻击路径的风险指数、组件安全风险指数、主机安全风险指数、网络安全风险指数、漏洞和关联关系风险指数.

(1) 攻击路径的风险指数

攻击路径是一条包含了攻击者从初始条件到达攻击目标所经历的节点和利用条件的序列,该序列即为一个非法的关联关系.利用条件包括漏洞和关联关系,在攻击路径中以“-”和节点分开.例如,攻击路径“A - NC_{AB}, B, v - B - NC_{BC} - C”表示攻击者从节点 A 出发,利用关联关系 NC_{AB} 和节点 B 上的漏洞 v,获得节点 B 的访问权限,然后利用关联 NC_{BC} 关系,到达攻击目标即节点 C.

攻击者攻击成功的概率为由式(1) 计算得出

$$P(\text{Attack}) = \prod_{i=1}^n v_i \cdot p \quad (1)$$

式中, $v_1, v_2, \dots, v_n$ 为攻击路径上被攻击者利用的一系列漏洞, p 为漏洞被攻击者成功利用的概率.

每条非法访问路径给组件带来的风险指数由式(2) 计算:

$$R(\text{AttSeq}) = P(\text{Attack}) \cdot C \cdot A \cdot W \quad (2)$$

式中, $C \cdot A$ 为被攻击节点的资产价值, W 为加权系数,表示攻击者攻击成功对组件的危害程度. W 按攻击者在组件上非法获得的权限对应于 root, user, access 分别赋初值为 3、2、1,如果非法访问者来自于网络内部,则 W 取值在初值基础上再乘以 0.3. 非法访问者的来源可由攻击序列的起始点分辨出.

攻击图由所有的攻击路径构成,本文所提出的网络风险评估的核心就是对攻击路径的分析.通过量化分析这些攻击可能发生的概率以及发生后对网络带来危害的严重程度,得到网络安全风险指数,向管理者提供建议,优先对可能给网络造成危害较大的漏洞和关联关系采取安全防护措施,尽可能降低网络的安全风险.

(2) 组件安全风险指数

主机上的组件可能被攻击者从多条路径进行不同程度的攻击,在这些攻击中,把给组件带来最大风险的攻击所造成的风险作为组件的安全风险指数.

$$R(\text{Component}) = \max(R(\text{AttSeq}_1), R(\text{AttSeq}_2), \dots, R(\text{AttSeq}_n)) \quad (3)$$

式中, $\text{AttSeq}_1, \text{AttSeq}_2, \dots, \text{AttSeq}_n$ 为攻击图中以该组件为目标的所有攻击路径.

(3) 主机安全风险指数

主机安全风险来源于主机上各组件的安全风险,计算方法如下:

$$R(\text{host}) = \text{host.Weight} \cdot \sum_{i=1}^n R(\text{Component}_i) \quad (4)$$

式中, host.Weight 为主机在网络中的重要性系数. $\text{Component}_1, \text{Component}_2, \dots, \text{Component}_n$ 是主机上的所有组件.

(4) 网络安全风险指数

网络的整体安全风险指数由网络中各主机的安全风险指数累加获得

$$R(\text{network}) = \sum_{i=1}^n R(\text{host}_i) \quad (5)$$

式中, $\text{host}_1, \text{host}_2, \dots, \text{host}_n$ 为网络上的所有主机.

(5) 漏洞和关联关系风险指数

对网络进行一定程度的安全风险评估只要是为了给网络的管理者在采取一定的措施来加强网络的安全性时能够提供一些有价值的建议.所以,在本文所给出的网络安全风险评估模型中增加了对网络的漏洞以及关联关系风险的考虑,网络管理者通过模型中计算出来的风险指数来决定对漏洞和关联关系的修补顺序.

攻击者的非法的访问权限主要是利用网络的漏洞和关联关系获得.不同的攻击路径所利用的漏洞或关联关系可能是同一种,该漏洞或关联关系被攻击路径所里用的次数越多表明它对网络安全造成的威胁的可能性越大.所以,用包含某一漏洞或关联关系的所有攻击路径给网络带来风险的累加值作为漏洞或关联关系风险指数能够准确反映其给网络带来的威胁的大小^[14].

$$R(\text{vul}) = \sum_{i=1}^n R(\text{AttSeq}_i) \quad (6)$$

$$R(\text{NC}) = \sum_{i=1}^n R(\text{AttSeq}_i) \quad (7)$$

式中, $\text{AttSeq}_1, \text{AttSeq}_2, \dots, \text{AttSeq}_n$ 为攻击图中包含 vul 或 NC 的所有攻击路径, $R(\text{AttSeq})$ 用式(2) 计算.

4.2 风险指数的计算方法

在网络安全风险指标的计算中,子 Agent 计算组件及主机的安全风险指数,主 Agent 汇总所有子 Agent 的计算结果计算网络的整体安全风险以及漏

洞和关联关系的风险指数.

攻击图生成完成后,主 Agent 将攻击图中的边,即攻击路径发送给子 Agent.子 Agent 分析攻击路径及其中漏洞和关联关系给网络带来的风险,进而计算组件和主机风险指数,并向主 Agent 汇报.主 Agent 根据子 Agent 的计算结果得出网络的整体风险指数.

主 Agent 的风险指数计算算法 GlobaleRisk Compute 如图 4 所示.

```

Input:攻击图
Output:网络整体风险指数,各漏洞和关联关系风险指数
begin
    netWorkRisk=0;
    foreach( 网络中的主机、漏洞库中的漏洞、关联关系库中的关联关系 )
        初始化其风险指数为 0;
    foreach(攻击图中的攻击路径 )
        解析出路径中攻击目标,将攻击路径发送给攻击目标组件所在子 Agent;
    While(存在主机 host, risk = 0 )
        {getMessage ( );
        If( 消息为漏洞风险指数 )
            计算漏洞风险指数;
        If ( 消息为关联关系风险指数)
            计算关联关系风险指数;
        If ( 消息为主机风险指数)
            更新主机安全风险指数;
        }
    foreach( host )
        netWorkRisk+=host, risk;
end

```

图 4 GlobaleRiskCompute 算法

在 GlobaleRiskCompute 算法中,主 Agent 首先将网络风险指数、各主机、漏洞及关联关系风险指数初始化为 0,然后将攻击图中攻击路径发送给子 Agent 由于子 Agent 对攻击路径进行分析.然后接收子 Agent 攻击分析结果,计算网络整体风险及各漏洞和关联关系的风险指数.

子 Agent 的风险计算算法 NativeRisk Compute 如图 5 所示.

在 NativeRiskCompute 算法中,子 Agent 分析接收到的攻击路径.首先将主机及各组件风险指数初始化为 0,计算每条攻击路径的风险指数,解析攻击路径中的漏洞和关联关系,向主 Agent 发送相应

的数据消息.根据式(3)和式(4)计算组件和主机风险指数,并向主 Agent 报告计算结果.

```

Input:攻击路径
Output:组件、主机安全风险指数,漏洞、关联关系数据消息
begin
    host, risk=0;
    foreach ( component )
        component, risk=0;
    foreach(攻击路径 )
        {计算攻击路径的安全风险指数;
        解析攻击路径中的漏洞和关联关系;
        向主 Agent 发送风险数据消息(漏洞,风险指数)、(关联关系,风险指数);
        If(风险指数>目标组件风险指数)
            更新目标组件风险指数为攻击路径风险指数;
        }
    计算主机安全风险;
    向主 Agent 发送主机安全风险数据消息;
end

```

图 5 NativeRiskCompute 算法

5 原型系统的实现与验证

在实际网络中各主机软件环境复杂,windows、unix、linux 系统都有应用,因此网络安全风险评估系统应具备跨平台性,以避免由于软件环境差异造成的不能对全网展开正确评估.Java 的 Agent 开发框架 (Java Agent Development Framework, JADE)是一个完全采用 JAVA 语言编写的多 Agent 系统开发框架,具有跨平台的优点^[15].基于 JADE 平台,对本文提出的评估模型和评估方法进行了仿真实现,并通过实验验证风险评估模型的有效性.

5.1 JADE 平台

JADE 为分布式主体平台,完全采用 JAVA 语言编写,并提供给 JAVA 程序员编写多 Agent 系统.其结构示例图如图 6 所示.

在该系统中,每台主机上运行一个容器,一个平台可包含多个容器,其中有一个主容器.每个容器中可运行一个或多个 Agent.

JADE 平台采用异步消息传输方式进行 Agent 间的信息交换,每个 Agent 有一个 Agent 消息队列,用来接收其他 Agent 传递的消息,当有信息传递到 Agent 消息队列中,该 Agent 即被唤醒,队列中的信息的处理时机是由开发人员指定的.

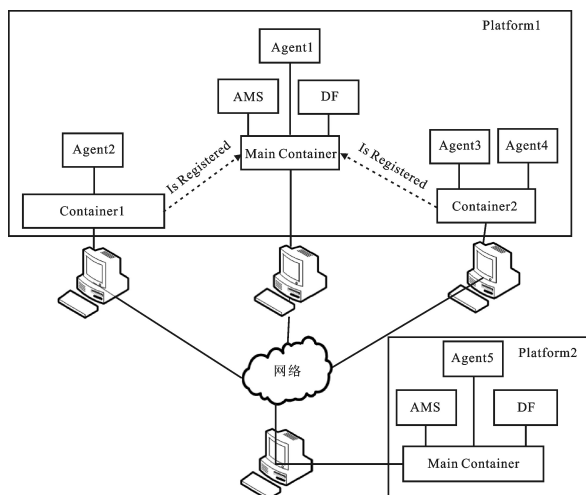


图 6 JADE 容器与平台结构图

5.2 仿真网络设计

通过一个网络环境验证本文提出的安全风险评估方法,仿真网络如图 7 所示。

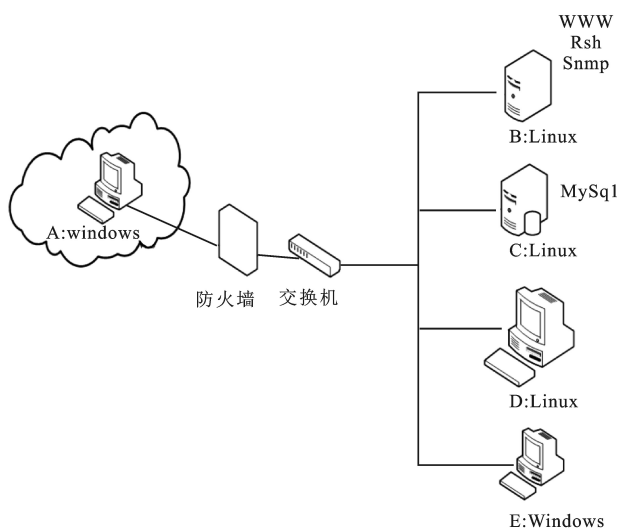


图 7 仿真网络组织结构图

图 7 中的节点 A 是外网中的一台 PC 机,代表目标网络外的访问用户,节点 B,C,D,E 分别是网络信息服务器、数据库、管理机和个人计算机,它们和防火墙组成内网。

5.3 系统测试与验证

在该系统中由主 Agent 构建攻击图,首先,主 Agent 将构成攻击图边的攻击路径发送给子 Agent,并由子 Agent 计算各主机和组件的安全风险指数,然后主 Agent 汇总由子 Agent 的计算机计算出的安全风险指数,最后通过汇总所得的安全风险指数计算得到网络的整体风险指数。最终的网络攻击图如图 8 所示。

图 8 只给出了与非法入侵相关的主机组件,B

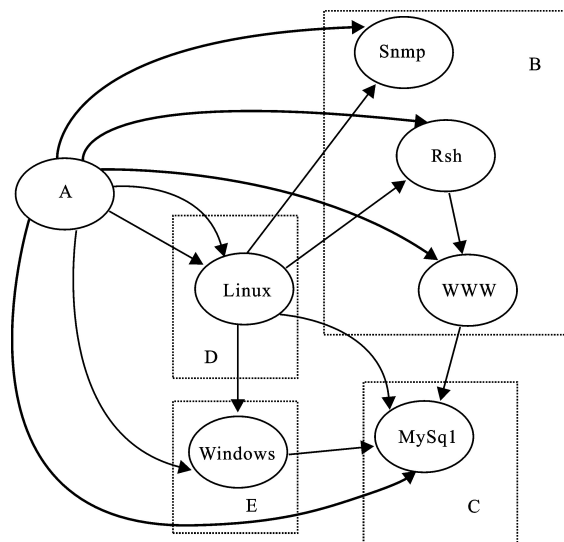


图 8 网络攻击图

和 C 的操作系统组件即 hB、CLinux 和 hC。CLinux 均未标出。图中较粗的曲线是非法的访问关系,代表一条攻击路径;直线表示被攻击者利用的合法的关联关系。通过攻击图可以看出,外部攻击者 A 通过主机 D 上 linux 组件的漏洞成功获取主机 B 的 Snmp 组件、Rsh 组件和 WWW 组件的访问权限,主机 C 的 MySQL 组件访问权限及主机 E 的 Windows 组件访问权限。

计算出的网络整体及各部分安全风险如表 1 所示。

表 1 网络安全风险指数

对象	风险指数
网络	38.4
主机 B	28.5
主机 C	12
主机 D	4.5
主机 E	10.5
组件 h _B . C _{WWW}	6
组件 h _B . C _{Rsh}	13.5
组件 h _B . C _{Snmp}	9
组件 h _C . C _{MySQL}	12
组件 h _D . C _{Linux}	4.5
组件 h _E . C _{Windows}	10.5

6 结束语

本文提出了基于攻击图的多 Agent 网络安全风险评估模型和风险评估方法。在此基础上,采用了攻击图的理论并引入 Agent 技术,使风险评估模型具有良好的扩展能力。另外还扩展了关联关系的概念,在攻击路径的分析中引入关联关系,并将攻击者

可能植入的漏洞纳入攻击规则进行分析,使攻击路径的分析更符合现实情况。

然而在实际环境中由于管理不善引发的网络安全风险也很常见,因此将管理因素纳入风险评估模型是下一步的工作目标。另外在风险评估中加入入侵检测器等网络安全防范措施对攻击者攻击的影响,将会使评估结果更加准确。

参考文献:

- [1] 李庆朋,王布宏,王晓东,等.基于安全状态约简的攻击图生成方法[J].计算机工程与设计,2013,34(5):1589-1592.
- [2] GB/T 20984-2007.信息安全技术 信息安全风险评估规范[S].中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会.2007.
- [3] 钟尚勤.基于主机攻击图的网络安全性研究[D].北京:北京邮电大学,2012.
- [4] 徐立.基于攻击图模型的网络安全分析方法研究[D].上海:上海交通大学,2010.
- [5] Phillips C, Swiler L P. A graph-based system for network vulnerability analysis [C]//Proceedings of the 1998 workshop on New security paradigms. Charlottesville, Virginia, United States, 1998:71-79.
- [6] Ramakrishnan C, Sekar R. Model-based vulnerability analysis of computer systems[C]//Proceedings of the 2nd International Workshop on Verification, Model Checking and Abstract Interpretation. Italy, Pisa, 1998: 1-8.
- [7] Ritchey R, Ammann P. Using model checking to analyze network vulnerabilities [C]//Proceedings of the IEEE Symposium on Security and Privacy. USA: Berkeley, 2001: 156-165.
- [8] Sheyner O. Scenario graphs and attack graphs [D]. Pittsburgh, USA. Carnegie Mellon University, School of Computer Science, 2004.
- [9] Sheyner O, Haines J, Jha S, et al. Automated generation and analysis of attack graphs [C]//Proceedings of 2002 IEEE Symposium on Security and Privacy. USA, Oakland, 2002:254-265.
- [10] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs [C]//Proceedings of the 15th Computer Security Foundations Workshop. Canada, Nova Scotia, 2002:49-63.
- [11] Ammann P, Pamula J, Ritchey R, et al. A host based approach to network attack chaining analysis [C]//AC-SAC 05: Proceedings of the 21st Annual Computer Security Applications Conference. USA: Tucson, IEEE Computer Society, 2005:72-84.
- [12] 叶云,徐锡山,贾焰,等.基于攻击图的风险邻接矩阵研究[J].通信学报,2011,32(5):112-120.
- [13] 张永铮,方滨兴,迟悦,等.网络风险评估中网络节点关联性的研究[J].计算机学报,2007,30(2):234-240.
- [14] 杨宏宇,江华.基于攻击图的多Agent网络安全风险评估模型[J].计算机科学,2013,40(2):148-152.
- [15] 李冠君.基于安全代理的网络自保护系统模型研究[D].天津:中国民航大学,2009.

作者简介:

谢丽霞 女,(1974-),硕士,副教授.研究方向为网络与信息安全.

仇晓锐 男,(1989-),硕士研究生.研究方向为网络与信息安全.

李雪菲 男,(1988-),硕士研究生.研究方向为网络与信息安全.

(上接第76页)

- [2] Jia Hao Cheong, Kok Lim Chan, Pradeep Basappa Khannur, et al. A 400-nW 19.5-fJ/conversion-step 8-ENOB 80-kS/s SAR-ADC in 0.18- μ m CMOS [J]. IEEE Transactions on circuits and systems—II: Express Briefs, 2011, 58(7):407-411.
- [3] Wenbo Liu, Pingli Huang, Yun Chiu. A 12b 22.5/45MS/s 3.0mW 0.059 mm² CMOS SAR-ADC achieving over 90dB SFDR [C]//2010 IEEE International Solid-State Circuits Conference. San Francisco, 2010: 380-382.
- [4] Ginetti B, Jespers P. Reliability of code density test for high resolution ADCs [J]. Electronics Letters, 1991, 27(24):2231-2233.

作者简介:

陈笑 男,(1990-),硕士研究生.研究方向为模拟与混合信号 VLSI 设计.