ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.2, February 2009, pp.451−461
DOI: 10.3724/SP.J.1001.2009.03172

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

基于安全状态域的网络评估模型*

张海霞[1,2+], 连一峰[1,2,3], 苏璞睿[1,2], 冯登国[1,2]

[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 软件研究所,北京 100190)

[3](中国科学院 研究生院,北京 100049)

Security-State-Region-Based Model of Network Security Evaluation

ZHANG Hai-Xia[1,2+], LIAN Yi-Feng[1,2,3], SU Pu-Rui[1,2], FENG Deng-Guo[1,2]

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

[2](Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[3](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: zhanghx@is.iscas.ac.cn

Zhang HX, Lian YF, Su PR, Feng DG. Security-State-Region-Based model of network security evaluation. *Journal of Software*, 2009,20(2):451−461. http://www.jos.org.cn/1000-9825/3172.htm

Abstract: A security-state-region-based (SSR-based) model called security-state-region-based evaluation model (SSREM) is proposed, which integrates the assessment based on the attack graph and the evaluation according to criteria together. In the model, the attack result is divided into the change in the attack ability and environment. The cause and effect relationship among them lays a foundation for building mathematic equations. After that, the definition of SSR is proposed, and also curve and surface fitting recurring to Matlab is used to analyze the attack trend, the result of which provides a theoretical basis for the division of SSR and the network security assessment based on SSR. Experiments in the posterior part of the paper show that, the evaluation according to SSREM can reflect how difficult it is to enter into different states through SSR and the tendency coefficient of security state region (TC_SSR), which can be used for reference by quantitative evaluation of network security.

Key words: security state region (SSR); security-state-region-based evaluation model (SSREM); tendency coefficient of security state region (TC_SSR); attack graph; vulnerability

摘 要: 将基于攻击图的评估与依赖标准的评估相结合,提出了一种基于安全状态域(security state region,简称SSR)的网络安全评估模型(security-state-region-based evaluation model,简称 SSREM).该模型将攻击的影响分为攻击能力改变和环境改变,通过两者之间的因果关系建立数学模型,提出了安全状态域趋向指数的概念,借助Matlab进行攻击趋势的曲面拟合,进而进行安全状态域的划分和网络的安全性评估.实验结果表明,依据SSREM进行的评估能够通过安全状态域和安全状态域趋向指数反映网络进入不同状态的难易程度,对网络安全性量

* Supported by the National Natural Science Foundation of China under Grant No.60403006 (国家自然科学基金); the National Basic Research Program of China under Grant No.2007CB311202 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant Nos.2006AA01Z437, 2006AA01Z412, 2006AA01Z433 (国家高技术研究发展计划(863))

Received 2007-04-10; Accepted 2007-09-04

化评估具有借鉴意义.

关键词: 安全状态域;基于安全状态域的评估模型;安全状态域趋向指数;攻击图;脆弱性

中图法分类号: TP393 **文献标识码:** A

随着以计算机技术和通信技术为代表的信息技术的不断进步,网络在全球范围内迅速地发展壮大.与此同时,突出的网络安全问题日益成为人们关注的焦点.分散的资源分布、系统的分而治之、协同工作的特殊性以及网络的差异性都为网络安全防御和评估带来了难以估量的困难.如何确保网络的安全性成为当前亟待解决的一个问题.

防火墙、入侵检测和扫描器是网络安全领域发展较为成熟的几种技术.防火墙技术是一种通过执行访问控制策略来降低网络和系统被非法利用的风险的技术.它不能阻止合法用户发动的攻击,也不能阻止不经过防火墙的攻击.入侵检测技术通过特征检测和异常行为发现来保障网络安全,然而却不能有效地检测隐秘攻击.近年来出现的各种扫描器利用穿透测试的方式进行系统的脆弱性探测,虽然能够发现大多数的脆弱性,但却不具备检测复合攻击的能力.脆弱性分析评估技术是一种从模拟攻击角度对网络的脆弱性进行分析的技术.该技术从拓扑结构、信任关系、脆弱性信息等方面对目标网络进行模型化表示,通过攻击图的分析能够预测网络可能遭受的各种攻击,是上述安全技术的有力补充.目前脆弱性分析评估技术已经引起了国内外相关领域研究人员的广泛关注,逐步成为网络安全领域的研究热点.

Swiler 和 Phillips 在文献[1]中提出了基于图的网络安全分析模型,并在此基础上提出了最小攻击代价分析和最短路径分析.通过对攻击图的分析可以了解攻击者可能的攻击路径,从而通过改变网络配置达到网络防御的目的.他们的工作在相关领域是第一次,然而由于分析方法过于简单,其准确性有待进一步考察.

Sheyner 等人在文献[2,3]中提出了自动化生成攻击图的方法,并在此基础上提出了最小安全措施分析.文献[4,5]中详细证明了该方法在多项式时间内能够完成.Noel 等人在文献[6–8]中提出的最小代价分析将代价与安全措施相关联,对基于利用的攻击图进行分析.Ammann 等人[9]提出了基于主机的攻击链分析方法,通过“攻击图一个节点对应网络中的一台主机”来增强方法可扩展性的,并尝试利用攻击图来进行安全改进.Ou 等人[10−12]则主要着眼于网络的模型化表示以及攻击规则的简化,以达到降低复杂度的目的.Zakeri 在文献[13]中提出了利用描述逻辑进行网络脆弱性分析的方法.

陈秀真等人在文献[14]中提出的层次化网络安全态势评估方法是对入侵检测系统(IDS)警报的分析,虽然该评估方法并不基于攻击图,但全面考虑了攻击网络中各个环境因素的影响,这一点值得借鉴.冯萍慧等人在文献[15]中提出了并串联可靠性分析模型.该模型基于攻击图对网络可靠性进行了量化评价.

近年来,依赖标准的安全产品评估[16,17]受到业界的推崇,然而无论是侧重管理的 BS7799[16],还是侧重于技术测试的 CC[17]都是一种对信息系统和安全产品的验证性评估.当然,对安全产品各个组件细节上的模型化表示依然值得借鉴.

文献[1–9]关于攻击图的分析方法最终都是为了改进网络的安全性能,或根据最有可能的入侵路径,考虑最有效的安全措施进行安全增强.文献[14,15]两项工作则是在攻击图基础上对网络进行安全量化评估的代表.上述方法都只是对攻击图进行分析,能够单纯地从攻击角度反映网络的安全性.文献[10–13]则侧重于逻辑形式化表示在脆弱性分析中的利用,攻击图的分析较为简单.然而,网络安全受多方面因素的影响,例如物理安全、资产权重等.单纯依赖攻击图的评估方法显然不能满足全面评估的需要.网络的安全性评估工作需要我们建立起能够从多个层面反映网络安全性的评估模型.

本文将基于攻击图的安全评估与依赖标准的评估相结合,提出了一种通过攻击者进入不同的网络状态区间的难易程度来评估网络安全性的模型——基于安全状态域的评估模型(security-state-region-based evaluation model,简称 SSREM).该模型首先借鉴风险评估的资产分析过程,对环境破坏和攻击能力进行量化表示;然后使用环境破坏值和攻击能力威胁值的曲面拟合求解攻击过程中的安全状态值;随后,根据安全状态值划分安全状态域;最后,综合考虑攻击过程依赖系数、攻击代价和隐秘系数求解网络安全评估的指标——安全状态域趋向

指数(tendency coefficient of security state region,简称 C_SSR).SSREM 模型能够提供从多层面反映网络安全性的评估方法,也可以为网络安全状况的改进提供参考.

本文第 1 节给出安全状态域的定义,描述衡量安全状态域时需要考虑的因素.第 2 节介绍安全状态值的衡量方法和安全状态域的划分方法.反映不同层次网络安全状况的安全状态域趋向指数求解规则在第 3 节详细加以说明.第 4 节给出一个利用该模型进行网络安全评估的实例.第 5 节是全文的总结.

1 安全状态域

安全状态是对网络安全状况的瞬时反映,安全状态域则表示了安全状态的范围.定义如下:

定义 1. 安全状态域(security state region,简称 SSR)是安全状态的量化区间表示,是对网络破坏状况和网络面临威胁的量化衡量.

随着攻击过程的不断深入,一方面对网络造成了现实的破坏,另一方面则使得攻击者的能力随着攻击资源的逐步积累而不断增长,为网络带来了更大的安全威胁.因此,作为安全域划分重要依据的安全状态域衡量应该考虑网络环境破坏和攻击能力威胁这两方面因素的综合作用.本节将从这两个方面详细阐述安全状态域衡量的方法,作为 SSREM 模型的基础.

1.1 环境破坏值(destroy value of environment,简称DVE)

网络环境错综复杂,作为安全状态域衡量至关重要的一环,环境破坏值(DVE)的估算需要对网络环境进行准确的模型化.本文借鉴 BS7799 的资产确定思想[16]来确定 DVE 时需要考虑的因素,并将安全相关联的各个资产进行分类分层的衡量.借助加权平均的思想,通过自底向上的计算得到 DVE.

首先,对网络环境进行层次化表示.网络环境由各个不同的实体组件构成.实体组件可以是主机、路由器、防火墙等等.每一个实体组件由软件、硬件、数据和服务等一部分或多部分组成.这里的软件、硬件、数据和服务等与 BS7799 的资产分类相对应,不同之处在于剔除了 BS7799 中管理相关的要素.软件、硬件、数据和服务则由具体的资产来组成.例如,具体的软件资产可以是操作系统(如 Windows 2000),也可以是应用程序软件(如 Mysql),还可以是存在于组件上的源程序等.服务包括 FTP,RPC,HTTP,TELNET 等.

然后,为底层资产赋值.底层资产的破坏值由底层资产的属性破坏值和底层资产的属性权重决定.属性破坏值是指资产的(秘密性/完整性/可用性)遭受破坏时对系统造成的影响的量化衡量.各个属性破坏值视该属性遭受破坏时对系统造成的危害分 5 级进行赋值,分别是:可忽略、低、中等、高、极高,如图 1 所示.

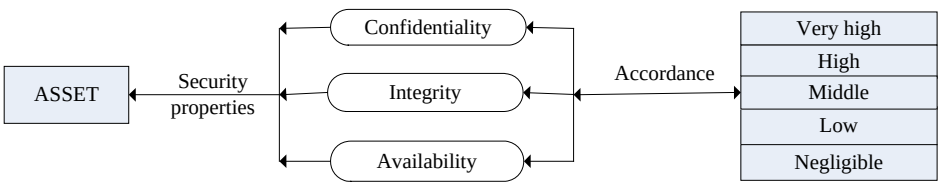


Fig.1 Criterion to set the asset destroy value

图 1 资产破坏值赋值准则

资产的属性破坏值可以用一维向量表示.

$$\overrightarrow{D\_ASSET\_Attr}=[D\_Secret,D\_Integret,D\_Available].$$

属性权重是各个安全属性在资产破坏值衡量中所占的比重,随资产的不同而不同.例如,对于 Mysql 数据库来说,如果其中存储的是敏感数据,则数据的秘密性所占的权重较大;而如果存储的是校验数据,则数据完整性的权重就需要优先保证.资产的属性权重也可以表示为一维向量:

$$\overrightarrow{W\_ASSET\_Attr}=[W\_Secret,W\_Integret,W\_Available].$$

资产的破坏值计算公式如下:

$$D\_ASSET = \overrightarrow{D\_ASSET\_Attr} \times \overrightarrow{W\_ASSET\_Attr} \quad (1)$$

最后,使用加权平均法计算组件构成元素的破坏值、组件的破坏值以及环境破坏值(DVE).计算过程中涉及的要素按照自底向上的顺序依次为资产→组件构成元素→组件→环境.加权平均法的公式如下:

$$DVE_{up} = \sum_{i=0}^{n} DVE_{next}[i] \times \omega[i] \quad (2)$$

即上层要素的破坏值为该要素所有子要素破坏值的加权平均,其中 $\omega[i]$ 表示上层元素的第 i 个子元素所占的权重.

1.2 攻击能力威胁值(threat value of attack,简称TVA)

攻击能力威胁值(TVA)是对攻击过程某特定时刻、攻击者拥有的攻击能力对安全造成的威胁的衡量.取决于攻击者已经获得的敏感数据、攻击者对目标网络的控制状况等.攻击能力威胁值(TVA)的计算重点是考虑敏感数据威胁和攻击者获得的权限威胁.攻击能力威胁值估算的层次为:攻击能力威胁值→实体组件威胁值→敏感数据威胁值/攻击能力威胁值→具体的数据资产/具体权限.

敏感数据的威胁值计算与第 1.1 节中资产的破坏值计算相同,通过对属性破坏值的加权平均得到.计算过程涉及的要素从下到上依次为资产属性→资产→敏感数据,计算公式如下:

$$TVA_{up} = \sum_{i=0}^{n} TVA_{next}[i] \times \omega[i] \quad (3)$$

即上层要素的威胁值等于其下层子元素威胁值的加权平均.其中,$\omega[i]$ 表示上层要素的第 i 个子要素所占的权重.

随着攻击过程的深入,攻击者对网络的控制体现在攻击者对网络中实体组件的掌控上,在攻击能力的获取上表现为攻击者对实体组件权限的获得.SSREM 模型将攻击者可能获得的实体组件权限进行了划分,如图 2 所示.图中实线箭头表示权限逐渐提升的过程,虚线则表示利用转化关系.例如,远程登录的攻击者通过一个可以在本地获得读权限的攻击转化为远程攻击者获得读权限.图中划分的 4 个层次分别为攻击者远程登录权限、攻击者获得读权限、攻击者获得写权限以及攻击者获得根权限.这 4 层与攻击者无任何操作权限一起构成了 5 个权限级别,与资产属性的 5 个级别相对应.对攻击能力威胁赋值是根据当前攻击者获得的权限层次来进行的.

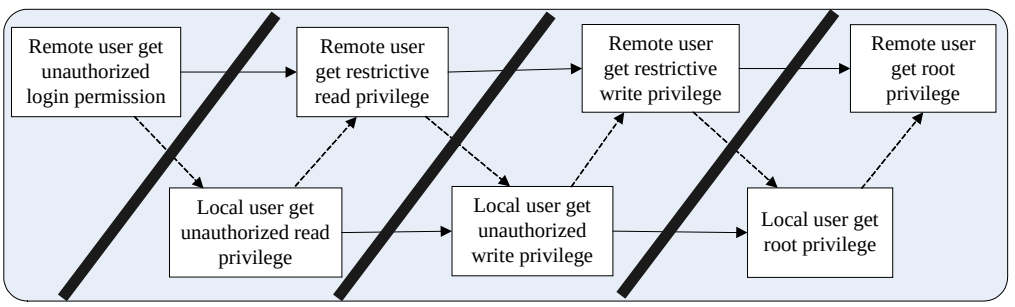


Fig.2 Criterion to set the privilege threat value

图 2 权限威胁值赋值准则

如果敏感数据和权限威胁没有交叉,则直接进行加权平均方法向上计算威胁值.如果有交叉,则通过公式 $T = T\_Pri + T\_S - T(Pri \cap S)$ 来计算,其中,T 表示影响攻击能力威胁值的实体因素集合;T_Pri 表示与攻击者获得网络控制权限相关的网络实体因素集合;T_S 表示与攻击者获得敏感数据相关的实体因素集合;而 $T(Pri \cap S)$ 则表示与攻击者获得网络控制权限以及敏感数据均相关的网络实体因素集合.计算的其他步骤仍遵循加权平均法.

2 状态域融合

基于安全状态域的网络安全评估模型使用了文献[3,4]中提出的算法来生成攻击图.为了方便后续表述,这

里使用如下定义界定攻击图的表示符号.

定义 2. 攻击者对网络发动单次攻击称为攻击者对网络脆弱性的单次利用,用 e 表示;不同的利用以 e_i 表示.攻击路径 AP 表示攻击者发动的一次完整的攻击过程,表示为攻击序列的有序组合$e_0e_1e_2...e_n$.攻击图 $GM(S_0,S_t,N,ES,MG)$是网络从初始状态出发到达目标状态的所有攻击路径组合,其中 N 表示攻击图的节点集,$node\in N$ 表示节点,对应网络的状态.ES 表示攻击图的边集,攻击图的边 $e\in ES$ 表示单次脆弱性利用或攻击者的单次攻击.MG 是攻击图的关系矩阵表示.

2.1 环境破坏值与攻击能力威胁值的融合

对一条特定攻击路径 AP 完成上述 3 步计算之后,得到一组环境破坏值和攻击能力增长的威胁值.根据攻击步骤之间的因果关系可知,得到的这组值满足式(4)所示的函数关系.

$$\left.\begin{array}{l} f(DVE_0,TVA_0,e_1)=\Delta DVE_1;\ g(DVE_0,TVA_0,e_1)=\Delta TVA_1;\ DVE_0\oplus\Delta DVE_1=DVE_1;\ TVA_0\oplus\Delta TVA_1=TVA_1 \\ f(DVE_1,TVA_1,e_2)=\Delta DVE_2;\ g(DVE_1,TVA_1,e_2)=\Delta TVA_2;\ DVE_1\oplus\Delta DVE_2=DVE_2;\ TVA_1\oplus\Delta TVA_2=TVA_1 \\ \cdots \\ f(DVE_{n-1},TVA_{n-1},e_n)=\Delta DVE_n;\ g(DVE_{n-1},TVA_{n-1},e_n)=\Delta TVA_n;\ DVE_{n-1}\oplus\Delta DVE_n=DVE_n;\ TVA_{n-1}\oplus\Delta TVA_n=TVA_n \end{array}\right\} \tag{4}$$

式(4)中 f 是单步攻击的环境变化函数,表示在环境破坏值为 DVE,攻击能力为 TVA,利用 e 进行攻击所带来的环境变化;g 是单步攻击的攻击能力变化函数,表示在环境值为 DVE,攻击能力为 TVA,利用 e 进行攻击所带来的攻击能力增长.式(4)罗列了攻击过程中各个量的变化.如果用 SSV 表示安全状态的衡量值,则各个攻击步骤之间的函数变化满足如式(5)所示的偏微分方程关系.

$$\begin{cases} \dfrac{\partial_{SSV}}{\partial_{DVE}}=f(DVE,TVA,e) \\ \dfrac{\partial_{SSV}}{\partial_{TVA}}=g(DVE,TVA,e) \end{cases} \tag{5}$$

需要说明的是,对于单步攻击的环境破坏值(DVE)变化和攻击能力威胁值(TVA)变化可能都不是连续的.为了计算的准确性,可以将各步攻击划分为无穷小的攻击增量,这种方法只是一种近似.我们采取的方法是将单个攻击步骤的环境破坏值变化和攻击能力威胁值变化首先模拟为一个连续的过程,然后取值重新组成环境破坏值、环境破坏增量、攻击能力威胁值和攻击能力威胁增量代入式(5).然后对这组值进行曲面拟合[18]得到一阶偏微分方程,通过偏微分方程与原函数之间的系数关系得到 SSV 与 DVE,TVA 之间的关系,并计算得到 SSV 的值.

2.2 安全状态域划分

在计算得到 SSV 之后可以根据各个节点对应的 SSV 进行安全状态域(SSR)的划分,依此来区分攻击过程的不同阶段和网络的不同状态区间.为了与前面的计算保持一致,这里将安全状态域划分为 5 级.首先计算出网络初始安全状态值与网络完全遭受破坏时的安全状态值组成的增量区间$SSV_0\sim SSV_{all}$,其中,SSV_0 表示网络的初始安全状态值,SSV_{all} 表示网络完全遭受破坏时的安全状态值,增量区间的大小$\Delta SSV=SSV_{all}-SSV_0$.然后,按照特定状态值 SSV_t-SSV_0 与ΔSSV 的比值进行安全域划分,其中, SSV_t 表示攻击过程具体时刻的安全状态值.划分规则见表 1.

目前为止,对于 $a1$,$a2$,$a3$,$a4$ 的取值主要依据经验进行.SSR 划分的标准化是下一步研究工作的重点.

Table 1 Division rule of SSR

表 1 SSR 划分规则

SSR (Level 1)	SSR (Level 2)	SSR (Level 3)	SSR (Level 4)	SSR (Level 5)
[0,$a1$)	[$a1$,$a2$)	[$a2$,$a3$)	[$a3$,$a4$)	[$a4$,1]

3 安全评估算法

3.1 安全状态域趋向指数定义

定义 3. 路径的节点趋向指数 *CP_Node*(tendency coefficient of path to node)是指攻击者沿某特定路径进入某节点所表示的网络状态需要付出的综合代价.*CP_Node* 越大,说明沿该路径进入特定状态越困难,可能性越小;反之则可能性越大.

定义 4. 路径的安全状态域趋向指数 *CP_SSR*(tendency coefficient of path to security state region)是指攻击者沿某特定路径进入某特定安全域所需付出的综合代价.*CP_SSR* 越大,说明沿该路径进入特定安全状态域越困难,该条路径被攻击者采用的可能性越小;反之则可能性越大.

定义 5. 安全状态域趋向指数 *C_SSR* 是指攻击者进入某安全域所需付出的平均综合代价.进入特定安全状态域趋向指数越大,说明进入该安全域需要付出的综合代价越大,网络在该级别上的安全性越好;反之则说明安全性越差.

路径的安全状态域趋向指数依赖于 3 个方面:(1) 攻击路径上攻击节点之间的依赖,主要是指后续节点对前面节点的依赖.由于攻击者沿某特定路径进入安全域的第 1 个节点所代表的安全目标不一定是攻击者最终的攻击目标,所以该节点之前的直接相邻的节点不一定是为该节点服务的.因此,要求解路径的安全域趋向指数需要考虑该节点对其前面所有节点的依赖.这里我们用依赖系数来表示.(2) 攻击经验的增加对攻击代价的影响.(3) 攻击过程的隐蔽程度.沿某一路径进行攻击的难易程度在一定程度上取决于攻击过程的隐蔽程度.因此,文中使用了组合入侵检测和用户干预因素在内的隐秘系数计算方法.接下来,文中首先给出了依赖系数、攻击代价以及隐秘系数的定义和求解方法,定义 3~5 给出的各个指数求解方法将在第 3.5 节详细说明.

3.2 依赖系数的定义

在情景攻击过程中,为了完成某一特定的攻击目标,攻击者往往需要进行多步努力.攻击者的每一步攻击都直接或间接地为攻击目标的完成服务,也可以说,攻击者的目标完成直接或间接地依赖于前面目标的完成.定义 6~定义 8 对各种依赖及依赖关系的表示进行了定义.

定义 6. 目标节点 N_G 直接依赖于攻击节点 N_M,是指 N_M 的完成直接为攻击目标 N_G 的完成提供了前提条件.目标节点 N_G 对攻击节点 N_M 的直接依赖程度使用直接依赖系数 $NC_{G\to M}$ 表示.攻击图的所有节点之间的直接依赖关系表示为一个矩阵 *MN*,矩阵元素 $MN[i,j,k]$表示第 i 条路径上的节点 N_j 对节点 N_k 的直接依赖系数,即 $MN[i,j,k]=NC_{j\to k}$.

定义 7. 目标节点 N_G 间接依赖于攻击节点 N_M,是指 N_M 的完成间接为攻击目标 N_G 的完成提供了前提条件,或者说攻击节点 N_M 的完成为攻击目标 N_G 的前提条件提供了前提条件.目标节点 N_G 对攻击节点 N_M 的间接依赖程度使用间接依赖系数 $IC_{G\to M}$ 表示.攻击图的所有节点之间的间接依赖关系表示为矩阵 *MI*,矩阵元素 $MI[i,j,k]$表示第 i 条路径上的节点 N_j 对节点 N_k 的间接依赖系数,即 $MI[i,j,k]=IC_{j\to k}$.

定义 8. 目标节点 N_G 对攻击节点 N_M 的依赖是目标节点 N_G 对攻击节点 N_M 所有依赖的总和.目标节点 N_G 对攻击节点 N_M 的依赖程度使用依赖系数 $DC_{G\to M}$ 表示.攻击图的所有节点之间的依赖关系表示为矩阵 *MD*,矩阵元素 $MD[i,j,k]$表示第 i 条攻击路径上的节点 N_j 对节点 N_k 的依赖系数,即 $MD[i,j,k]=DC_{j\to k}$.

一个攻击图所有节点之间的依赖可以用 3 个三维矩阵表示:$MN[i,j,k]$表示攻击图的直接依赖矩阵;$MI[i,j,k]$表示攻击图的间接依赖矩阵;$MD[i,j,k]$表示攻击者的依赖矩阵.这里,i 表示攻击路径序号,j 表示攻击路径上的目标节点序号,k 表示攻击路径上的攻击节点序号.依赖矩阵的求解由算法 1 完成.

算法 1.

Input: All nodes in every attack path and the cause and effect of each attack step.

Output: *MN*, the matrix of direct dependence corresponding to the attack graph of network; *MI*, the matrix of indirect dependence corresponding to the attack graph of network; *MD*, the matrix of dependence corresponding to the attack graph of network.

Steps:

1. For each attack path give path serial number i=(1,2,3,…,m)
2. For each node in the ith path, set node serial number j=(1,2,3,…,*length*)
3. For each node before j, set node serial number $k\geq 1$ and $k\leq j$
4. if ($j-1$.*precondition*==$k-1$.*consequence*)
5. $MN[i,j,k]=1$
6. Set i=(1,2,3,…,m)
7. Set j=(1,2,3,…,*length*)
8. Set k=(1,2,3,…,$j-1$)
9. Set l=(1,2,3,…,$k-1$)
10. if ($MN[i,j,l]$==1 and $MN[i,l,k]$==1)
11. $MI[i,j,k]=2$
12. if ($MN[i,j,l]$==1 and $MD[i,l,k]$!=0)
13. $MI[i,j,k]=MN[i,j,l]+MI[i,l,k]$
14. Standalize *MI* according to the second dimension
15. For each element which is not equal to 0, search for dependence tree reversely, solving *MI*
16. *MD*=*MI*+*MN*; Output *MN*, *MI* and *MD*

算法 1 的第 1~5 行是针对攻击过程为直接依赖矩阵赋值的过程;第 6~12 行是间接依赖矩阵的求解过程;13~15 行是标准化矩阵及输出的过程.其中,m 表示攻击路径的数目.由于得到的攻击图中的攻击路径较少且攻击路径的长度较短,矩阵 *MN* 和 *MD* 中针对每一条路径的矩阵又都是下三角稀疏矩阵,因此,求解依赖系数的算法复杂度比实际要低得多,在 $O(n^2)$与 $O(n^3)$之间.这里,n 表示攻击图中路径的平均长度.

3.3 攻击代价

攻击代价指的是攻击者为完成攻击所需付出的努力.每一步攻击的完成通常与以下 3 个方面相关:(1) 攻击者的经验.例如,攻击者利用主机 A 上的脆弱性 V_x 获得对目标主机 B 上的用户权限,然后再利用主机 B 上的脆弱性 V_x 获得对目标主机 D 上的用户权限.对攻击者而言,一旦进行了第 1 次攻击,第 2 次攻击尽管环境因素有所影响,但攻击变得更为容易.(2) 单步攻击对攻击者经验的依赖程度.例如,口令猜测、木马植入等攻击在很大程度上取决于攻击者的攻击经验和熟练程度,然而一些 Web 类服务的脆弱性的利用对攻击者经验的依赖程度相对要小得多.(3) 通常情况下,攻击者进行攻击所需付出的努力.因此,我们有如下计算公式:

$$Cost_i = d_i^{time-1} \times \cos t_i \tag{6}$$

d_i(d_i<1)表示攻击过程对攻击者经验的依赖系数,*time* 是指攻击过程相似子攻击的重复次数,$cost_i$ 表示第 i 步攻击通常情况下所需付出的努力.计算出的攻击代价越大,说明这一步攻击越艰难.

3.4 隐秘系数

攻击过程的隐秘性与如下 3 个方面相关:(1) 环境改变是否会引起入侵检测系统的警报;(2) 环境改变是否会引起网络用户的注意;(3) 环境改变可能引起警报或用户注意相对于整个攻击过程的位置.这里,我们借鉴 Sheyner 等人在文献[2,3]中的方法,将入侵检测系统进行如下模型化表示:

$$IDS:\{H,H,\Delta E\}\rightarrow\{s,d,b\},\ IDS:\{H,H,\Delta A\}\rightarrow\{s,d,b\}.$$

根据环境改变是否会引起入侵警报,对攻击过程的隐秘性进行放大.

$$ids_i=\begin{cases}1, & \text{不会引起警报}\\ a, & 1<a<2,\text{介于两者之间}\\ 2, & \text{较大可能引起警报}\end{cases} \tag{7}$$

另外,每一次子攻击对环境的改变不尽相同,过大的环境改变可能会引起用户的注意,从而使得用户采取措

施干扰入侵.因此,针对环境改变是否会引起用户的注意,我们定义如下函数:

$$h(\Delta E)=\begin{cases}a, & 0\le a<1,\text{不会引起用户注意或很小}\\ b, & b\ge 1,\text{会在较大程度上引起用户注意}\end{cases} \tag{8}$$

环境改变可能引起警报或用户注意相对于整个攻击过程的位置对于攻击者是否会采用该攻击过程来达到攻击目标十分重要.因此我们定义:

$$p\_pos=1-\frac{depth-1}{length} \tag{9}$$

p_pos 表示位置对环境改变的贡献系数;$depth$ 表示可能引起警报或用户注意的攻击深度;$length$ 表示攻击链的长度.综合各种因素的环境改变表示为

$$E\_Change_i=(ids_i+h(\Delta E_i))\times p\_pos_i \tag{10}$$

其中, ids_i 表示第 i 个子攻击的入侵检测放大系数;$h(\Delta E_i)$表示环境改变引起用户注意的系数;p_pos_i表示第 i 个子攻击的位置对环境改变的贡献系数.E_Change_i 越大,表示攻击的隐秘性越差,系统的安全性就越好.

3.5 安全状态域趋向指数求解

本节对定义 3~定义 5 给出的各个指数的求解方法进行详细描述.首先,节点趋向指数的求解公式如下:

$$TCP\_Node_{i,j}=\alpha(MD,COST,E\_Change,i,j)=\sum_{l=0}^{j-1}\sum_{k=0}^{l-1}MD[i,j,k]\times Cost_k/E\_Change_k \tag{11}$$

根据式(11)可以计算得到攻击者沿攻击路径 i 到达攻击节点 j 所需付出的综合代价.其中,$Cost_k$ 表示攻击路径 i 上第 k 步攻击的代价;E_Change_k 表示第 k 步攻击的隐秘系数.

当 j 表示沿路径 i 进入安全状态域 l 的首节点序号时,可以得到路径的安全状态域趋向指数求解公式:

$$TCP\_SSR_{i,l}=TCP\_Node_{i,j}=\sum_{l=0}^{j-1}\sum_{k=0}^{l-1}MD[i,j,k]\times Cost_k/E\_Change_k \tag{12}$$

由定义 5 可知,安全状态域趋向指数可以按照式(13)进行求解:

$$TC\_SSR=\frac{1}{n}\sum_{i=1}^{n}TCP\_SSR_{i,j} \tag{13}$$

其中,n 表示能够进入安全状态域的路径个数;j 表示攻击者沿路径 i 进入安全状态域所经过的首节点序号,对于不同的路径 i,j 值不同.

4 实例网络分析

如图 3 所示为实验网络环境.外部防火墙与内部防火墙将整个网络分为 3 个部分:攻击者所在的外部网络、Web 服务器所在的临界区域,以及包含 Linux 主机和 Windows 主机在内的内部网络.实验网络的可能的脆弱性见表 2.

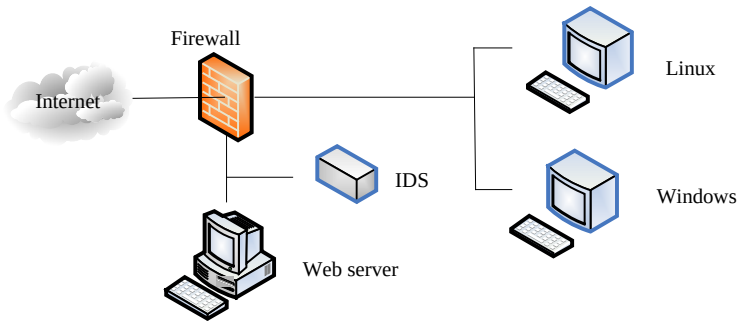


Fig.3 Topology of sample network

图 3 实例网络拓扑

Table 2 Vulnerability list of example network

表 2 实例网络的脆弱性列表

ID	Information of vulnerabilities			Exploited cost/ *E_Change*/ Detect or not
	Vulnerability name	Attack type	CVE	
V_1	Trust vulnerability	Remote user login		1/1/0.5/*n*
V_2	Buffer overflow in IIS	Remote user get root privilege	CVE-2002-0364	2/1/1/*n*
V_3	Remote code execute vulnerability in Microsoft Excel	Remote user get user privilege	CVE-2006-0031	2/1.5/0.5/*n*
V_4	Off-by-One error in Linux NFS	Remote user get privileges	CAN-2003-0252	2/1/1/*n*
V_5	SMB driver elevation of privilege vulnerability	Local privilege escalation	CVE-2006-2373	3/2/1/*d*

根据攻击图生成算法[2,3]生成的攻击图如图 4(a)所示,其中,节点上标示的数字代表网络的状态.

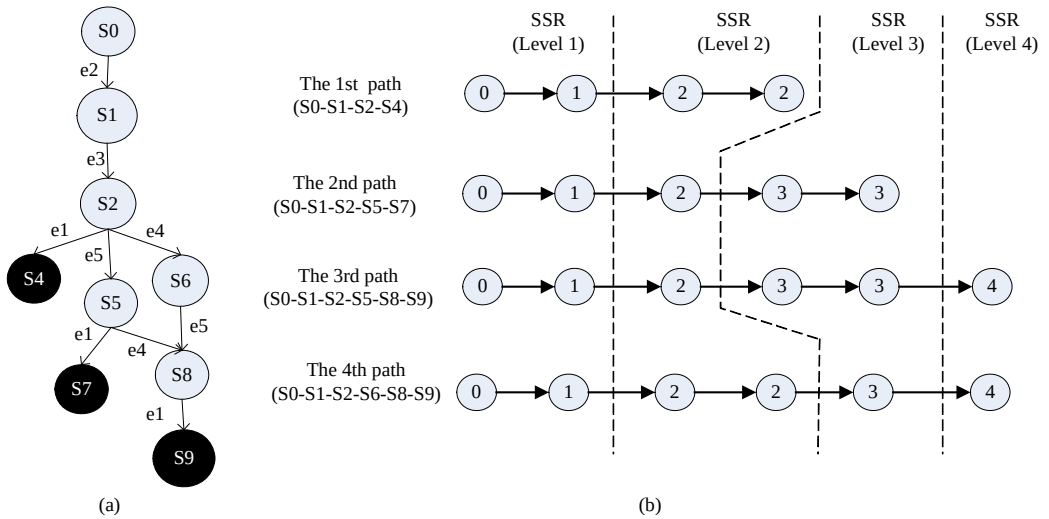


Fig.4 Attack gragh and analysis of attack path SSR of example network

图 4 实例网络的攻击图及攻击路径的安全状态域划分

由图 4(a)所示的攻击图可知,攻击者通过利用脆弱性 V_2 可以控制 Web 服务器;然后,通过利用脆弱性 V_3 可以获得 Windows 主机的普通用户权限;利用信任脆弱性可以访问 Mysql 数据,或者借助脆弱性 V_5 的权限提升获得 Windows 系统的根权限,再利用信任脆弱性访问 Mysql 数据.利用 SSREM 模型计算得到的结果见表 3,其中曲面拟合借助 Matlab[18]完成,结果给出的是多项式的系数.

由表 3 可知,沿攻击路径 4 进入 3 级安全状态域付出的代价比沿路径 3 进入 3 级安全状态域付出的代价要大.

根据以往网络评估和脆弱性分析的经验,表 1 中 $a1$=0.1,$a2$=0.25,$a3$=0.45,$a4$=0.70.实际上,SSR 划分规则可以视具体情况有所不同.对各个路径的 SSR 划分结果如图 4(b)所示,节点标示的数字表示当前节点代表的网络状态所处的安全域级别,0 表示起始点.根据式(13)计算得到的 *TC_SSR* 的结果见表 4.

表 4 的结果显示了实例网络进入不同的安全状态域的难易程度,是对网络安全性的一种量化反映.

Table 3 Evluation result of each attack path

表 3 各个攻击路径的评估结果

Path serial		Serial number of node in each path											
		0		1		2		3		4		5	
1	Environ&Attack	62.65	0	45.99	12	45.06	16.8	39.60	18				
	TCP_SSR	0		5		8.83		11.2025					
	Result of curve and surface fitting	{{0, −430.3055,2.1693},{−95.0461,15.4118, −0.134},{0.7479,0.1274,0.0009}}											
2	Environ&Attack	62.65	0	45.99	12	45.06	16.8	39.6	18	39.3	22.8		
	TCP_SSR	0		5		9		13		15.3125			
	Result of curve and surface fitting	{{0,13.9882,2.8170},{136.8889, −3.6354,0.1540},{−1.1044,0.0012,0.0028}}											
3	Environ&Attack	62.65	0	45.99	12	45.06	16.8	44.75	21.6	39.3	22.2	37.3	23.22
	TCP_SSR	0		5		7.9		9.125		12.425		13.03125	
	Result of curve and surface fitting	{{0,−105.5693,3.1348},{−20.1926,6.0706,−0.1869},{0.1511,−0.0652,0.00215}}											
4	Environ&Attack	62.65	0		12	45.06	16.8	44.75	21.6	42.78	22.02		
	TCP_SSR	0		5		7.9		10.7		13.425		15.15625	
	Result of curve and surface fitting	{{0,−74.1748,0.3181},{6.6136,4.5731,−0.1134},{−0.0623,0.0388,0.0018}}											

Table 4 Result of *TC_SSR* for example network

表 4 实例网络的 *TC_SSR* 结果

	Levels of SSR			
	1	2	3	4
TC_SSR	5	8.407 5	12.95	14.093 75

5 小 结

本文在前人工作的基础上提出了一种利用网络脆弱性分析得到的攻击图、基于安全状态域的网络安全评估模型(SSREM).与依赖 BS7799,CC 等标准的评估方法不同,该模型利用的是动态分析的结果.与已有攻击图的分析利用方法不同,本文提出的方法旨在从多个层次对网络安全性作出评价.本文的主要贡献在于,提出了将脆弱性分析结果与依据标准的评估相结合进行网络安全评估的方法,建立了基于网络状态域的网络评估模型,提出了安全状态域、安全状态域趋向指数的概念,给出了安全状态域的划分方法和趋向指数的求解算法.

文中实例给出的 SSR 的划分方法在很大程度上依赖于以往分析工作的经验,实际的网络安全评估需要根据情况进行调整.今后我们将进一步研究安全状态域划分的标准化,并在此基础上通过对不同网络的对比评估进一步验证 SSREM 模型的有效性和适用性.

致谢 在此,我们向对本文工作给予支持和建议的同行以及课题组的全体同学和老师表示感谢.

References:

[1] Phillips C, Swiler L. A graph-based system for network vulnerability analysis. In: Proc. of the New Security Paradigms Workshop. Charlottesville, 1998. 71−79.

[2] Sheyner O, Haines J, Jha S, Lippmann R, Wing J. Automated generation and analysis of attack graphs. In: Hinton H, Blackley B, Abadi M, Bellovin S, eds. Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 2002. 254−265.

[3] Sheyner O, Wing JM, Tools for generating and analyzing attack graphs. In: Proc. of the Workshop on Formal Methods for Components and Objects. Tehran, 2004. 344−371.

[4] Jha S, Sheyener O, Wing JM. Two formal analyses of attack graphs. In: Proc. of the 15th IEEE Workshop on Computer Security Foundations. Cape Breton: IEEE Computer Society, 2002. 49−63.

[5] Sheyner O. Scenario graphs and attack graphs [Ph.D. Thesis]. Pittsburgh: Carnegie Mellon University, 2004.

[6] Noel S, Jajodia S, O'Berry B, Jacobs M, Efficient minimum-cost network hardening via exploit dependency graphs. In: Proc. of the 19th Annual Computer Security Applications Conf. Las Vegas: IEEE Computer Society, 2003. 86−95.

[7] Noel S, Jacobs M, Kalapa P, Jajodia S. Multiple coordinated views for network attack graphs. In: Proc. of the Workshop on Visualization for Computer Security. Minneapolis: IEEE Computer Security, 2005. 99−106.

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

[9] Ammann P, Pamula J, Ritchey R, Street J. A host-based approach to network attack chaining analysis. In: Proc. of the 21st Annual Computer Security Application Conf. Tucson: IEEE Computer Society, 2005. 72−84.

[10] Ou XM, Govindavajhala S, Appel AW. Mulval: A logic-based network security analyzer. In: Proc. of the 14th USENIX Security Symp. Baltimore: USENIX Association, 2005. 113−128.

[11] Ou XM. A logic-programming approach to network security analysis [Ph.D. Thesis]. Princeton: Princeton University, 2005.

[12] Ou XM, Boyer WF, McQueen MA. A scalable approach to attack graph generation. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. Alexandria: ACM, 2006. 336−345.

[13] Zakeri R, Abolhassani H, Shahriari HR, Jalili R. Using description logics for network vulnerability analysis. In: Proc. of the 5th Int'l Conf. on Networking. Mauritius: IEEE Computer Society, 2006. 78−83.

[14] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. Journal of Software, 2006,17(4):885−897 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/885.htm

[15] Feng PH, Lian YF, Dai YX, Bao XH. A vulnerability model of distributed systems based on reliability theory. Journal of Software, 2006,17(7):1633−1640 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1633.htm

[16] ISO 27001. Information technology-security techniques-information security management systems-requirements. 2005. http://www.securitycn.net/img/uploadimg/20070924/183844756.pdf

[17] ISO/IEC 15408. Common criteria for information technology security evaluation. Version 3.1, 2006. http://www.commoncriteriaportal.org/

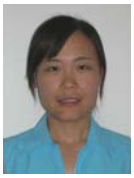
[18] Zeng QH, Lu DT. Curve and surface fitting based on moving least-squares methods. Journal of Engineering Graphics, 2004,25(1): 84−89 (in Chinese with English abstract).

附中文参考文献:

[14] 陈秀真,郑庆华,管晓宏,林晨光,层次化网络安全威胁态势量化评估方法.软件学报,2006,17(4):885−897. http://www.jos.org.cn/1000-9825/17/885.htm

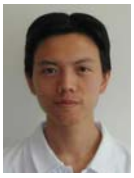
[15] 冯萍慧,连一峰,戴英侠,鲍旭华.基于可靠性理论的分布式系统脆弱性模型.软件学报,2006,17(7):1633−1640. http://www.jos.org.cn/1000-9825/17/1633.htm

[18] 曾清红,卢德唐.基于移动最小二乘法的曲线曲面拟合.工程图学学报,2004,25(1):84−89.



张海霞(1981－),女,河北元氏人,博士,主要研究领域为网络安全,脆弱性评估.

苏璞睿(1976－),男,博士,副研究员,主要研究领域为恶意代码分析与防范.



连一峰(1974－),男,博士,副研究员,主要研究领域为网络安全,脆弱性评估.

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.