ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.7, July 2006, pp.1633−1640
DOI: 10.1360/jos171633
© 2006 by of *Journal of Software*. All rights reserved.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于可靠性理论的分布式系统脆弱性模型*

冯萍慧+, 连一峰, 戴英侠, 鲍旭华

(信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

A Vulnerability Model of Distributed Systems Based on Reliability Theory

FENG Ping-Hui+, LIAN Yi-Feng, DAI Ying-Xia, BAO Xu-Hua

(State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88258551, Fax: +86-10-88258093, E-mail: phfeng@vip.sina.com, http://home.is.ac.cn

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. http://www.jos.org.cn/1000-9825/17/1633.htm

Abstract: After the analysis and comparison of the existing vulnerability analysis methods, a new vulnerability model of distributed systems based on reliability theory is proposed. First, it models vulnerabilities of distributed systems from the aspects of security-related factors. Then it utilizes the model checking method to build Vulnerability State Graph (VSG) of distributed systems to depict the complete process of exploitation of vulnerabilities. Finally, it introduces reliability theory to perform analysis and quantitative evaluation of vulnerabilities of distributed systems, which provides a theoretical evidence for security enhancement.
Key words: distributed system; vulnerability model; vulnerability state graph; reliability; reliability function

摘 要: 对现有的脆弱性分析方法进行分析和比较,提出基于可靠性理论的分布式系统脆弱性模型.针对影响分布式系统安全性的各项因素进行脆弱性建模,利用模型检验方法构造系统的脆弱性状态图,描述系统脆弱性的完整利用过程,引入可靠性理论对分布式系统的脆弱性进行分析和量化评估,从而为增强分布式系统的安全性提供理论依据.
关键词: 分布式系统;脆弱性模型;脆弱性状态图;可靠性;可靠度函数
中图法分类号: TP393 文献标识码: A

随着网络规模的不断扩大、用户需求的不断膨胀和新服务的不断增加,分布式系统得到了广泛的应用.分布式系统的特点是资源分布化、用户分布化、计算分布化和管理分布化,这给系统的设计、实现、评估、操作和安全维护都带来了不利因素.如何确保分布式系统的安全性,成为当前亟待解决的一个问题.

传统上,人们使用防火墙、IDS 和扫描器等工具来保护网络安全.防火墙通过执行访问控制规则来限制网络连接,但通常缺乏应用级保护能力;IDS 通过检测攻击特征和异常行为来发现安全问题,但普遍缺乏检测隐秘攻击的能力;扫描器通常针对单台主机进行扫描,而忽略了网络拓扑,不能识别更具危害性的复合攻击和协同攻击.另外,由于缺乏统一的安全策略和对脆弱性的全面分析,这些工具不能在保护网络资产安全性的同时确保网

* Supported by the National Natural Science Foundation of China under Grant No.60403006 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035801 (国家重点基础研究发展规划(973))

Received 2005-02-22; Accepted 2005-08-15

络的正常运行.因此,为了进一步提高分布式系统的安全性,必须有完整的脆弱性模型和分析方法,只有在充分理解分布式系统脆弱性的基础上,才能为分布式系统安全模型的设计和优化提供保证.

针对分布式计算环境,目前尚没有完整的脆弱性模型的研究成果.国内外研究工作主要集中在安全模型和分布式处理方面.近年来,研究人员开始关注脆弱性分析和安全量化评估等领域,主要研究方法如下:

Dacier[1]和 Ortalo[2,3]等人利用特权图描述入侵者权限提升的过程,将通往攻击目标的不同路径代表入侵者实施攻击的不同过程,并采用经验算法计算入侵行为的平均攻击代价.易见,这种方法是"以攻击为中心"的,其平均攻击代价的计算方法源于经验,缺乏理论基础,因此量化结果不能很好地反映系统的安全性.

Phillips 和 Swiler[4]使用攻击图描述入侵过程,根据攻击者的特征、网络配置和攻击模板,从目标状态出发,反向匹配攻击模板.如果找到通往起始状态的路径,则表明存在隐患,并利用最短路径算法计算最大入侵成功概率.其攻击图采用手工绘制,且最短路径算法成立的前提是入侵者事先了解攻击图的结构,这有悖于常理.

Sheyner 和 Jha 等人[5−7]使用改进的模型检验器 NuSMV[8]来构建攻击图,并在攻击图的基础上,利用平稳状态分布和 Markov 决策过程来计算攻击者成功完成攻击目标的最大平均概率.易见,该方法也是"以攻击为中心"的,而且对平稳状态分布的适用性缺乏论证,当攻击图中有大量转移概率未知时,用 Markov 决策过程所得的结果将会远远偏离正确值.

国内主要是清华大学在研究基于 Petri 网的模型检测的相关基础理论[9],并利用 Petri 网的模型检测技术来分析主机或网络系统脆弱性的可行性,相关研究工作仍在进行中.

通观上述方法,除了"以攻击为中心"、缺乏对其他安全威胁源(例如用户误操作、系统故障等)的充分考虑以及量化评估方法存在缺陷之外,还有一个共同的缺点就是不能表示分布式系统所特有的一些攻击,如需要获得不同主机的不同权限才能完成的攻击,包括分布式拒绝服务攻击、网络蠕虫和协同攻击等.

针对上述问题,本文提出一种新的分布式系统脆弱性模型,对影响分布式系统安全性的各项因素进行脆弱性建模,利用模型检验方法构造系统的脆弱性状态图,描述系统脆弱性的完整利用过程,并引入可靠性理论,对分布式系统的脆弱性进行分析和量化评估,从而为增强分布式系统的安全性提供理论依据.

本文给出该脆弱性模型的详细阐述.第 1 节介绍分布式系统的脆弱性建模.第 2 节描述脆弱性状态图的构造过程及其特点.第 3 节在脆弱性状态图的基础上引入可靠性理论进行脆弱性量化分析.第 4 节给出脆弱性模型的一个应用实例.最后是全文的总结.

1 分布式系统的脆弱性建模

大型的分布式系统通常包含多个节点、平台和应用,并通过多种模式连接.在对分布式系统进行脆弱性建模时,除了考虑每台主机的脆弱性之外,还必须了解整个分布式系统的网络拓扑信息,找出由于相互连接和不合理的信任关系所引入的关联漏洞.对整个分布式系统而言,这种漏洞往往比单个漏洞更具威胁性.

系统的脆弱性利用过程可分解为系统状态的一系列转移步骤.导致这些状态转移的原因可能是黑客利用漏洞进行攻击、后门程序被触发运行、用户的正常操作或系统本身硬件损坏等.这些行为得以实施有其一定的主体条件、客体条件和环境条件.行为的主体和客体可能是入侵者、普通用户或后门程序等,主体条件和客体条件分别是行为主体和行为客体所应满足的条件;环境条件主要包括主机间的连接关系、信任关系和入侵检测系统(IDS)的设置等.因此,在对分布式系统进行脆弱性建模时,主要考虑以下因素:

- H:分布式系统的主机集合.分布式系统中的任何一台主机 $h\in H$,都用一个五元组(id,usr,$svcs$,sw,$vuls$)来表示,其中 id 是主机的唯一标识符,可以是主机名或主机地址;usr 是主机设置的用户类型,如来宾、普通用户、特权用户、管理员等;$svcs$ 是主机上运行的应用服务;sw 是主机上安装的软件,例如操作系统类型和版本号;$vuls$ 是主机上存在的漏洞,包括软硬件漏洞、错误配置、管理缺陷等.
- I:入侵者模型,这里只简单考虑入侵者的权限,函数 $plvl_i(h)\rightarrow\{none,user,root\}$ 给出了入侵者 i 在主机 h 上的权限级别,它满足全序关系: $none<user<root$.有时,$plvl_i(h)$简写成 $plvl(h)$.
- R:主机间的连接关系,用三重关系来描述:$R\subseteq Host\times Host\times Port$,例如 $R(h_1,h_2,p)$表示主机 h_1 可以访问到

主机 h_2 的端口 p.

- T:主机间的信任关系,用二元关系来描述:$RshTrust \subseteq Host \times Host$.例如,$RshTrust(h_1,h_2)$表示用户可以从主机 h_1 登录到主机 h_2 上,而无须认证(即主机 h_2“信任”主机 h_1).
- IDS:入侵检测系统模型,用函数 $ids: Host \times Host \times Action \to \{d,s,b\}$来表示,如果源主机 h_1 与目标主机 h_2 之间的行为 a 是可检测的,则 $ids(h_1,h_2,a)=d$;如果 a 是隐秘的,则 $ids(h_1,h_2,a)=s$;如果 a 既有可检测部分又有隐秘部分,则 $ids(h_1,h_2,a)=b$.
- S:分布式系统的状态集合,该集合中的任一状态都表示为 $s=(sub,obj,env)$,其中,sub 为主体条件;obj 为客体条件;env 为环境条件.它们是下一个行为得以执行的前提条件.
- A:行为集合,该集合中的每个行为由一个六元组来描述:$a=(ID,Name,VulID,s_s,s_d,\lambda)$,其中,$ID$ 为该行为的唯一编号;$Name$ 为该行为的名称;$VulID$ 为该行为对应的漏洞编号,若无相应的漏洞,则该值设为 0;s_s 为行为的源状态;s_d 为行为的目标状态;λ为衡量该行为难易程度的代价参数.行为的执行将使系统脆弱性进入下一个状态,而下一个状态则可能是再下一个行为得以执行的前提.这里,我们建立了一个行为规则库用来保存各个行为的相关信息.
- G:系统的安全属性集合,即分布式系统所要达到的安全防护目标,这里采用系统断言语言 CTL(computational tree logic)来描述.例如,某个分布式系统的安全属性为:入侵者i在主机h上的权限级别应始终低于根用户权限,则该属性可表示为$AG(plvl_i[h]<root)$.

2 脆弱性状态图(VSG)

2.1 脆弱性状态图的构造

完成分布式系统的脆弱性建模之后,我们利用符号模型检验器 NuSMV[8]来构造反例.所谓反例,就是违背安全属性的状态转移过程.NuSMV 所使用的模型检验是一项用于检验系统的形式模型 M 是否满足给定属性 p 的方法.这里,M 是有限的转移系统;p 是由 CTL 语言描述的安全属性,其形式为 $p=AGf$,其中 f 为原子逻辑中的公式,如$-unsafe$ 表示不会出现不安全的状态.如果模型 M 满足属性 p,则 NuSMV 报告“true”;反之,则给出违背属性 p 的反例.

脆弱性状态图(VSG)描述的是系统到达不安全状态的各种可能的路径.我们把系统不会到达不安全状态的属性表示为 $AG(-unsafe)$.当该属性为“false”时,则存在从初始状态出发可到达的不安全状态,不安全的确切含义依赖于具体应用.下面简要描述违背安全属性 $AG(-unsafe)$的脆弱性状态图的构建算法:

- 建立状态集合S,初始状态集合$S_0 \subseteq S$,状态转移关系$R \subseteq S \times S((s,s') \in R$表示存在从$s$到$s'$的转移);
- 建立从某状态出发可用的原子行为集合$L: S \to 2^A$ (A是所有原子行为的集合),设定系统的安全属性$p=AG(-unsafe)$;
- 利用AG算子的定点特性,使用模型检验迭代算法搜索通往不安全状态的路径中所有状态的集合S_{unsafe};
- 将状态转移关系R限制在S_{unsafe}包含的状态集范围内,得到转移关系$R^p=R \cap (S_{unsafe} \times S_{unsafe})$;
- 生成脆弱性状态图$V_p = \left(S_{unsafe}, R^p, S_0^p, S_s^p, L\right)$,$S_{unsafe}$和$R^p$代表节点集合和边集合,$S_0^p = S_0 \cap S_{unsafe}$ 为可到达不安全状态的初始状态集合,$S_s^p = \left\{s \mid s \in S_{unsafe} \wedge s \models unsafe\right\}$为违背安全属性的不安全状态集合;
- 采用图形化工具Graphviz[10]将NuSMV输出的上述结果转化为状态转移图的形式.

2.2 脆弱性状态图的特点

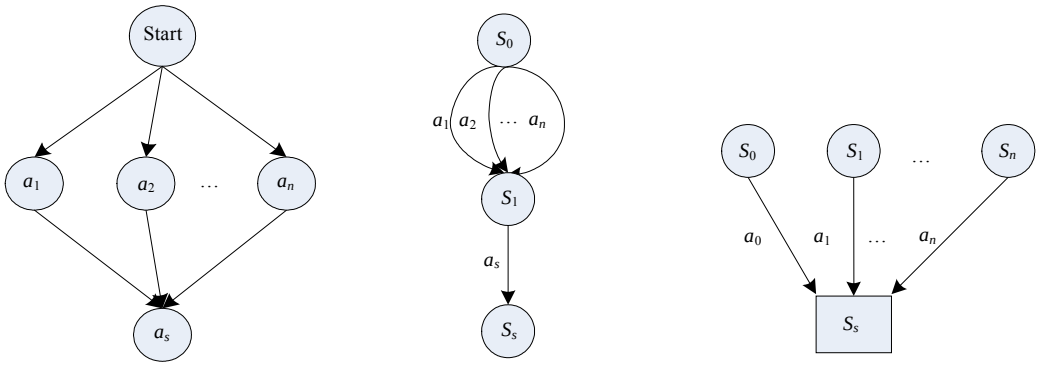
采用脆弱性状态图描述分布式系统的脆弱性,相比特权图和攻击图来说有以下 3 个优点:

(1) 采用系统状态作为节点比“以攻击为中心”的攻击图和特权图更具有普适性,因为一个系统的脆弱性并不仅仅源于攻击,也有可能是由系统本身的错误配置、用户误操作和硬件损坏等问题导致的.

(2) 与攻击图相比,更能节省状态空间.如图 1(a)所示的攻击图表示原子行为 $a_1,a_2,\ldots,a_n$ 的执行效果是一样

的,它们中任何一个行为的执行结果都可以使行为 a_s 继续执行,这里需要用 n+2 个节点来表示.如果采用脆弱性状态图来描述(如图 1(b)所示)只需要 3 个节点,比攻击图少了 n–1 个节点.因此,对大型分布式系统采用脆弱性状态图进行描述,将会大大节省状态存储空间,提高脆弱性状态图的构建效率.

(3) 引入多条件组合模型来满足分布式系统的需要.例如,对于分布式拒绝服务攻击,需要首先获得多台主机的控制权限,然后分别安装攻击代理程序才能控制这些主机对目标主机实施攻击.如图 1(c)所示,若想达到状态 S_s,需要执行从状态 S_0 出发的行为 a_0、从状态 S_1 出发的行为 a_1、…从状态 S_n 出发的行为 a_n.多条件组合模型在分布式系统中是很常见的.多条件组合节点 S_s 用矩形框来表示.



(a) An attack graph (a) 攻击图 (b) A vulnerability state graph (b) 脆弱性状态图 (c) A multi-condition combination model (c) 多条件组合模型

Fig.1 Advantages of vulnerability state graph

图 1 脆弱性状态图的优点

3 基于可靠性理论的脆弱性分析

在脆弱性状态图的基础上,我们引入可靠性理论,对分布式系统的脆弱性进行量化分析.

3.1 可靠性基本概念

表 1 给出了传统元器件产品的可靠性参数[11]和分布式系统脆弱性状态图中可靠性参数的对应关系.

Table 1 Comparison between reliability parameters of products and those of distributed systems

表 **1** 元器件产品与分布式系统的可靠性参数对比

Reliability parameters of components	Reliability parameters of distributed systems
A product (composed of several components) fails	A system goes to an unsafe state
A component fails	An atomic action is executed
A component's life indicates the duration from its first working to failure, noted as T	An atomic action's cost includes the time, resources, knowledge level and rights needed to execute the action, noted as C
Life T obeys the exponential distribution function: $F(t)=P\{T\le t\}=1-e^{-\lambda t}$	Cost C obeys the exponential distribution function: $F(t)=P\{C\le c\}=1-e^{-\lambda c}$
λ is the failing rate of a component, $\frac{1}{\lambda}=E(T)$ is the mean of the component's life	λ is the succeeding rate of an atomic action, $\frac{1}{\lambda}=E(C)$ is the mean of the action's cost
A component's reliability function $R(t)$ indicates the probability of accomplishing a prescriptive operation under a given condition during the time t: $R(t)=P\{T>t\}=1-F(t)=e^{-\lambda t}$	An atomic action's reliability function $R(c)$ indicates the unexecuted probability under a given condition with the expense of cost c: $R(c)=P\{C>c\}=1-F(c)=e^{-\lambda c}$
The reliability of a product means the ability to complete a prescriptive operation under a given condition during a given time	The reliability of a distributed system means the ability to maintain security under a given condition with expense of a given attacking cost. This value reflects the vulnerable extent of the distributed system
Let $R_s(t)$ be the reliability function of a product, then $E_s(T)=\int_0^{+\infty}R_s(t)dt$ shall be the mean of the product's life	Let $R_s(c)$ be the reliability function of a distributed system, then $E_s(C)=\int_0^{+\infty}R_s(c)dc$ shall be the mean of the attack cost of the system

表 1 中,原子行为的成功速率λ也称为行为代价参数,其取值依据该原子行为所要求的知识水平、所耗费的计算资源、人力资源、时间等因素而定.目前,我们采用等价攻击时间的方法来进行选取,即假定攻击者具有相同的知识水平、资源和对目标网络的了解程度.

这里参考了可靠性理论的方法,采用指数分布函数来计算代价分布情况,其原因在于:

- 如果通往目标节点的路径存在,而且攻击者付出了足够的代价即 $c\to\infty$,则有 $F(c)|_{c\to\infty}=1$,表示攻击者最终总可以达到攻击目标;
- 当 $c=0$ 时,$F(c)|_{c=0}=0$.即攻击者不进行任何攻击行为,则无法完成任何攻击目标;
- 相对于其他有类似性质的分布函数(如正态分布、对数正态分布和威布尔分布)来说,指数分布具有单参数的特性,有更好的适用性.

3.2 脆弱性状态图的可靠性分析

系统可靠度函数 $R_s(c)$为该系统在规定条件、规定代价 c 下维持安全状态的概率,$R_s(c)$值越大说明该系统的脆弱性越差.我们把脆弱性状态图分为如下 4 种模型,分别计算这 4 种模型所对应的可靠度函数.

3.2.1 串联模型

对于如图 2 所示的串联模型,设 C_i 和λ_i 分别为第 i 步原子行为的代价和成功速率,系统可靠度函数为

$$R_s(c)=1-P(C_1+C_2+\ldots+C_n\le c)=\sum_{i=1}^{n}\frac{\prod_{\substack{j=1\\ j\ne i}}^{n}\lambda_j e^{-\lambda_j c}}{\prod_{\substack{j=1\\ j\ne i}}^{n}(\lambda_j-\lambda_i)},\text{假定 }\forall i\ne j\to\lambda_i\ne\lambda_j,n\ge 2\ .$$

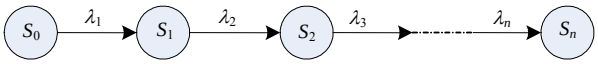


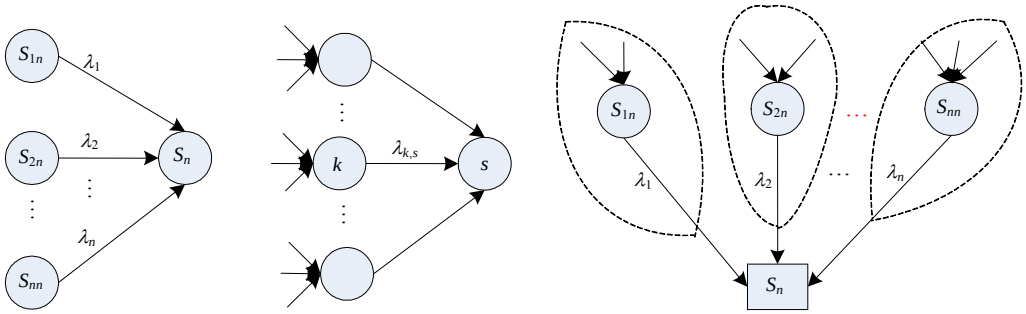
Fig.2 Serial model

图 2 串联模型

3.2.2 并联模型

对于如图 3(a)所示的并联模型,设 C_i 和λ_i 分别为第 i 步原子行为的代价和成功速率,系统可靠度函数为

$$R_s(c)=P(\min C_i>c)=\prod_{i=1}^{n}P(C_i>c)=e^{-\sum_{i=1}^{n}\lambda_i c}\ .$$



(a) A parallel model (a) 并联模型

(b) A composite model (b) 串并联复合模型

(c) A multi-condition combination model (c) 多条件组合模型

Fig.3 Parallel model, composite model and multi-condition combination model

图 3 并联模型、串并联复合模型和多条件组合模型

3.2.3 串并联复合模型

对于如图 3(b)所示的串并联复合模型,利用递归方法计算对应的可靠度函数.设状态 s 为脆弱性状态图的目标节点,则该系统的可靠度函数为

$$R_s(c)=\prod_{k\in in(s)}\left(R_k(c),\lambda_{k,s}\right).$$

其中,集合 $in(s)$为节点 s 的所有输入节点集合;$\lambda_{k,s}$是指从输入节点 k 到目标节点 s 的有向边所对应的原子行为的成功速率;$R_k(c)$为输入节点 k 对应的可靠度函数;$(R_k(c),\lambda_{k,s})$为沿着输入节点 k 到目标节点 s 这条路径所对应的可靠度函数.设 $R_k(c)=\sum_{i=1}^{n}a_i e^{-\lambda_i}$ ($\forall i\neq j\rightarrow\lambda_i\neq\lambda_j$),则有

$$\left(R_k(c),\lambda_{k,s}\right)=e^{-\lambda_{k,s}c}+\lambda_{k,s}\sum_{i=1}^{n}a_i e^{-\lambda_{k,s}c}\int_0^c e^{-(\lambda_{k,s}-\lambda_i)u}du=\sum_{i=1}^{n}a_i\frac{\lambda_{k,s}}{\lambda_{k,s}-\lambda_i}e^{-\lambda_i c}+\left(1-\sum_{i=1}^{n}a_i\frac{\lambda_{k,s}}{\lambda_{k,s}-\lambda_i}\right)e^{-\lambda_{k,s}c}.$$

3.2.4 多条件组合模型

对于如图 3(c)所示的多条件组合模型,如果组合节点的各输入节点相互独立,则先计算各输入节点的可靠度函数,再按串联模型计算;若其各输入节点具有相关性,则其计算方法需视各节点的条件相关性而定.

针对所分析的分布式系统,应综合利用以上模型,对表征系统脆弱性的可靠度函数进行计算.

3.3 系统的平均攻击代价

得到系统的可靠度函数 $R_s(c)$后,可以通过如下公式计算系统攻击(损坏)代价的期望值 $E(C)$:

$$E(C)=\int_0^{+\infty}cf_s(c)\,dc=-\int_0^{+\infty}cR_s'(c)\,dc=-\left(cR_s(c)\big|_0^{\infty}-\int_0^{+\infty}R_s(c)\,dc\right)=\int_0^{+\infty}R_s(c)\,dc.$$

期望值 $E(C)$越大,说明该系统的脆弱性越差,攻击者要完成攻击目标平均所要花费的代价也就越大.

4 实例分析

图 4 是实验网络拓扑图,由 DMZ 和内部局域网两个子网构成.DMZ 包含两台主机:主机 1 为 SSH 服务器,存在 sshd 缓冲区溢出漏洞;主机 2 为 IIS Web 服务器,存在 IIS 缓冲区溢出漏洞.内部局域网中,主机 3 运行关键数据库,我们的安全目标是保证该数据库的正常运行,防止出现拒绝服务.防火墙负责网络隔离,外部主机只能访问 DMZ 区域的主机,不能直接访问内部局域网;而 DMZ 区域的主机可以访问内部局域网.

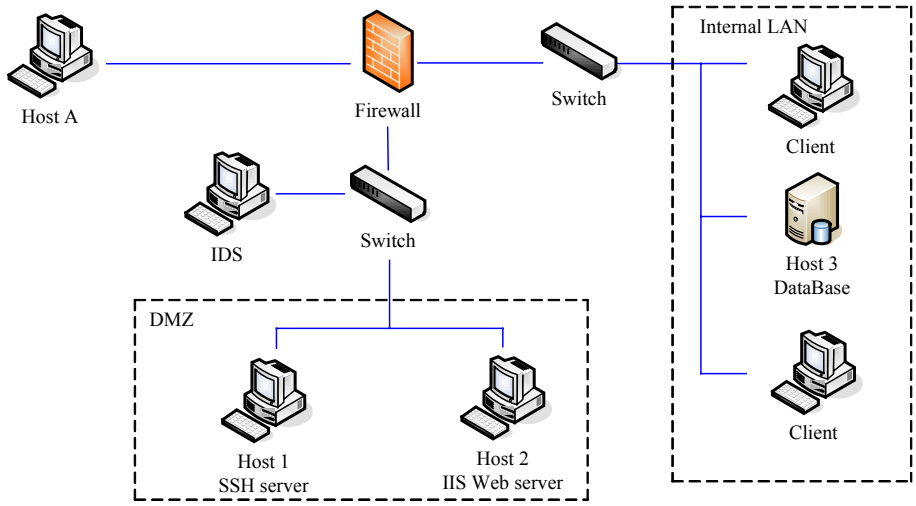


Fig.4 An experimental network instance of distributed system

图 4 分布式系统的实验网络实例

假定外部攻击者必须控制两台傀儡机,才能对数据库实施有效的分布式拒绝服务攻击,因此主机 A 上的攻击者必须先控制主机 1 和主机 2.由于对 DMZ 区域设置了 IDS 进行监控,攻击者如果直接攻击主机 2 的 IIS 缓冲区溢出漏洞,HTTP 明文数据流中包含的攻击特征将被 IDS 检测到;但如果攻击者利用主机 1 的 sshd 缓冲区溢出漏洞获取 root 权限,则双方交换的数据流是经过加密的,IDS 无法检测到这种隐秘攻击.因此,为了对数据库

实施有效且隐秘的拒绝服务攻击,攻击者采取如下的攻击过程:首先,利用 sshd 缓冲区溢出漏洞,获取主机 1 的 root 权限;然后,从主机 1 发起针对主机 2 的 IIS 溢出攻击,获取主机 2 的管理员权限;分别在主机 1 和主机 2 上安装代理,并控制它们同时向主机 3 的数据库发送大量数据包,致使数据库出现拒绝服务.

根据第 1 节介绍的脆弱性建模方法,表 2 给出了攻击者实施分布式拒绝服务攻击的各个行为的详细描述.其中,ip_0,ip_1,ip_2 和 ip_3 分别为主机 A、主机 1、主机 2 和主机 3 的 IP 地址,s_k 表示主机 h 上运行 s(s 为某个服务或程序).

Table 2 The set of actions of distributed denial-of-service attack

表 2 分布式拒绝服务攻击的行为集合

Action ID	Action name	Source state			Destination state	Cost Parameter λ
		Subject condition (sub)	Object condition (*obj*)	Environment condition (*env*)		
a_1	Sshd buffer overflow	$Plvl(ip_0)\geq user$	ssh_{ip}	$R(ip_0,ip_1,22)$	$Plvl(ip_1)=root$	λ_1
a_2	IIS buffer overflow	$Plvl(ip_1)\geq user$	IIS_{ip_2}	$R(ip_1,ip_2,80)$	$Plvl(ip_2)=root$	λ_2
a_3	Install an agent on host1	$Plvl(ip_1)=root$	$\varnothing$	$\varnothing$	$agent_{ip_1}$	λ_3
a_4	Install an agent on host2	$Plvl(ip_2)=root$	$\varnothing$	$\varnothing$	$agent_{ip_2}$	λ_4
a_5	Direct host1 and host2 to simultaneously send an enormous data to host3	$Plvl(ip_1)=root$ $Plvl(ip_2)=root$	$agent_{ip_1}$ $agent_{ip_2}$	$R(S,ip_3)$ $S=ip_1,ip_2$	$\neg database$ (database deny to work)	λ_5

利用第 2 节描述的脆弱性状态图构建流程,我们来绘制该实例所对应的脆弱性状态图,如图 5 所示.

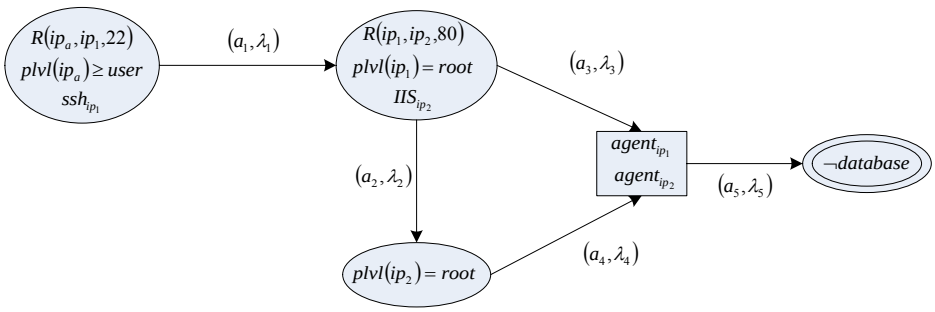


Fig.5 Vulnerability state graph of the experimental network instance

图 5 实验网络实例的脆弱性状态图

利用第 3 节介绍的基于可靠性理论的脆弱性分析方法,并根据上述脆弱性状态图,可以计算得到数据库系统的可靠度函数为 $R_s(c)=\sum_{i=1}^{5}\frac{\prod_{j\neq i}\lambda_j}{\prod_{j\neq i}(\lambda_j-\lambda_i)}\mathrm{e}^{-\lambda_i c}$,对应的平均攻击代价为 $E(C)=\int_0^{+\infty}R_s(c)\,\mathrm{d}c=\sum_{i=1}^{5}\frac{1}{\lambda_i}$.

5 小 结

对近几年国内外相关工作内容的调查研究后我们发现,针对分布式系统,目前缺乏完整的、具有普适性的脆弱性建模和评估方法.本文首次提出分布式系统的脆弱性模型,针对影响分布式系统安全性的各项因素进行脆弱性建模;引入系统状态作为脆弱性节点以缩小状态空间,与现有的攻击图或特权图方法相比,更具代表性和普适性,同时也为分布式系统所特有的多条件组合的脆弱性状态提供了合适的表示方法;采用模型检验方法,以脆弱性状态图的形式描绘分布式系统在遭受攻击或出现故障时的完整漏洞利用过程;在此基础上引入可靠性理论,对分布式系统的脆弱性进行量化分析,为系统的安全增强提供理论依据.针对网络实例的分析进一步验证了本文提出的脆弱性模型及相关计算方法.

今后的研究工作包括进一步完善脆弱性建模和脆弱性状态图的构建方法,研究系统配置、网络参数、攻击代价等因素对分布式系统脆弱性及可靠度函数的影响,研究原子行为的平均代价,依据原子行为所要求的知识水平、攻击资源和时间等因素,判定原子行为实施的难易程度,以实现准确的脆弱性量化评估.

致谢 在此谨向为本文工作提供支持和建议的老师和同学表示感谢.

References:

[1] Dacier M, Deswarte Y, Kaaniche M. Quantitative assessment of operational security models and tools. Technical Report, 96493, LAAS, 1996.

[2] Ortalo R, Deswarte Y. Information systems security: Specification and quantitative evaluation. Technical Report, DeVa ESPRIT Long Term Research Project No.20072, the 2nd Year Report, LAAS-CNRS & INRIA, 1997. 561−584.

[3] Ortalo R, Deswarte Y, Kaâniche M. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Trans. on Software Engineering, 1999,25(5):633−650.

[4] Swiler LP, Phillips C, Gaylor T. A graph-based network-vulnerability analysis system. Technical Report, SANDIA Report No. SAND 97-3010/1, 1998.

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

[6] Sheyner O, Haines J, Jha S, Lippmann R, Wing JM. Automated generation and analysis of attack graphs. In: Hinton H, Blakley B, Abadi M, Bellovin S, eds. Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 2002. 273−284.

[7] Jha S, Sheyner O, Wing JM. Minimization and reliability analyses of attack graphs. Technical Report, CMU-CS-02-109, Carnegie Mellon University, 2002.

[8] Cimatti A, Clarke E, Giunchiglia F, Roveri M. NuSMV: A new symbolic model verifier. In: Halbwachs N, Peled D, eds. Proc. of the 11th Conf. on Computer-Aided Verification (CAV'99). LNCS 1633, Trento: Springer-Verlag, 1999. 495−499.

[9] Jiang YX, Lin C, Qu Y, Yin H. Research on model-checking based on Petri nets. Journal of Software, 2004,15(9):1265−1276 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1265.htm

[10] Gansner ER, North SC. An open graph visualization system and its applications to software engineering. Software—Practice and Experience, 1999,30(11):1203−1233.

[11] Zeng SK, Zhao TD, Zhang JG, Kang R, Shi JY. A Design and Analysis. Tutorial of System Reliability. Beijing: Beijing University of Aeronautics & Astronautics Press, 2001 (in Chinese).

附中文参考文献:

[9] 蒋屹新,林闯,曲扬,尹浩.基于 Petri 网的模型检测研究.软件学报,2004,15(9):1265−1276. http://www.jos.org.cn/1000-9825/15/1265.htm

[11] 曾声奎,赵廷弟,康锐,石君友.系统可靠性设计分析教程.北京:北京航空航天大学出版社,2001.

冯萍慧(1979－),女,浙江临海人,博士生,主要研究领域为脆弱性分析.

戴英侠(1942－),女,教授,博士生导师,主要研究领域为信息安全.

连一峰(1974－),男,博士,副研究员,主要研究领域为网络安全.

鲍旭华(1977－),男,博士生,主要研究领域为入侵检测.