基于攻击图的网络安全评估方法研究 *

马俊春[1,2], 王勇军[1], 孙继银[2], 陈 珊[3]
(1. 国防科学技术大学 计算机学院, 长沙 410073; 2. 第二炮兵工程学院 402 教研室, 西安 710025; 3. 中国人民解放军 96337 部队, 成都 610000)

摘 要: 为了提高网络的整体安全性,提出了基于攻击图的网络安全评估方法。首先,在攻击图的基础上提出了脆弱点依赖图的定义;其次,将影响评估的因素分为脆弱性自身特点、网络环境因素和脆弱性关联关系三部分;最后,按照网络拓扑的规模,采用自下向上、先局部后整体的思想,直观地给出了漏洞、主机和整个网络系统三个层次的脆弱性指数评估值。通过大量反复的实验测试,该方法可以对网络系统存在的脆弱性进行定期的、全面的量化评估,及时发现并弥补网络系统中存在的安全隐患,有效地提升网络系统的生存能力,从而提高网络系统应对各种突发攻击事件的能力,具有重大的理论价值、经济效益和社会意义。

关键词: 网络安全; 攻击图; 脆弱点依赖图; 网络脆弱性指数评估
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)03-1100-04
doi:10.3969/j.issn.1001-3695.2012.03.082

Novel method of evaluating network security based on attack graphs

MA Jun-chun[1,2], WANG Yong-jun[1], SUN Ji-yin[2], CHEN Shan[3]
(1. *School of Computer Science, National University of Defense Technology, Changsha* 410073, *China*; 2. 402 *Staff, The Second Artillery Engineering Institute, Xi'an* 710025, *China*; 3. *The* 96337 *Troop of PLA, Chengdu* 610000, *China*)

Abstract: In order to improve networks' total security, this paper presented a novel method of assessing network security based on attack graphs. Firstly, it proposed a definition of vulnerability dependence graph based on attack graphs. Secondly, it divided the factors which impact network vulnerability assessment into three parts: the vulnerability character by itself, the network environment and the relationship between vulnerabilities. Finally, according to the size of network topology, using the evaluation policy from bottom to top and from local to global, it gave the vulnerability assessment intuitively in three levels: the vulnerability, the host and the network. Through a large number of repeated laboratory tests, the experimental results show that this method can assess network security efficiently, help network security managers guard the network, which improves networks viability, and improves the ability of responding to sudden attacks. So it has great theoretical value, economic value and social significance.

Key words: network security; attack graphs; vulnerability dependence graph; network vulnerability assessment

0 引言

随着计算机网络技术的快速发展,全球信息化已成为世界发展的大趋势,人们对计算机网络的依赖性大大加强,但与此同时,网络信息系统存在的安全漏洞和隐患层出不穷,地下黑客产业不断发展,网络攻击的种类和数量成倍增长,基础网络和重要信息系统面临着严峻的安全威胁。攻击图是一种基于模型的脆弱性评估方法,它从攻击者的角度出发,在综合分析多种网络配置和脆弱性信息的基础上,枚举出所有可能的攻击路径,从而帮助攻击者或防御者直观地理解目标网络内各个脆弱性之间的关系、脆弱性与网络安全配置之间的关系以及由此产生的潜在威胁。虽然攻击图可以使网络安全管理人员更好地理解网络受到攻击的步骤,但是随着网络规模的增大,生成的攻击图已经严重超出人们的理解能力。因此,在此背景下研究针对大规模复杂网络的安全评估方法具有重要的现实意义。

1 相关工作

攻击图的构建方法经历了从手工分析到自动分析,从分析小型企业网络到大规模复杂网络的发展过程。Swiler 等人[1,2]首次提出了攻击图模型,根据已有的攻击模板,从目标状态开始,采用深度优先的搜索策略构建攻击图。由于该方法完全依靠手工完成,因此这种方法不能适用于大规模复杂网络的分析,但为后来的研究者对攻击图的自动产生、自动分析奠定了坚实的基础。目前,美国、英国、俄罗斯、以色列等都在该方面投入了大量的科研力量,取得了显著的成果。尤其是美国麻省理工大学、卡内基梅隆大学和林肯实验室等研发出了 TVA[3]、MulVAL[4]、NetSPA[5]原型系统。

US-CERT (United States Computer Emergency Readiness

收稿日期: 2011-08-03; **修回日期**: 2011-09-12 **基金项目**: 国家"863"高技术研究发展计划资助项目(2009AA01Z432);国家自然科学基金资助项目(60873215)

作者简介:马俊春(1983-),女,山东菏泽人,博士研究生,主要研究方向为信息安全;王勇军(1971-),男,教授,博导,主要研究方向为高性能网络隔离技术、网络脆弱性分析技术、网络安全态势分析评估技术、网络生存性技术等;孙继银(1952-),男,山东单县人,教授,博导,中国计算机学会高级会员,中国计算机用户协会理事,主要研究方向为指挥自动化工程、计算机应用技术;陈珊(1981-),男,浙江丽水人,博士,主要研究方向为计算机应用技术(chenshan1223@126.com).

Team)是由美国国家安全部门与公私营部门所创立的位于华盛顿特区的一家合作公司。其使用脆弱性指标来评价某一漏洞的严重程度,该指标是一个 0 ~ 180 的数值,其不足之处在于划分过细,从而造成应用繁琐。而且该评估方法的评估结果不公开,仅在 US-CERT 内部使用,用于确定哪些脆弱性足够严重,以致需要发布安全公告。

SANS 提出一个脆弱性评估系统,用它为特定脆弱性进行严重等级赋值,但提供的评估结果仅仅是 critical、high、moderate 和 low 四级,与 US-CERT 评估系统一样,用于产生分数和等级的公式未公开。

张海霞等人[6]提出了一种基于安全状态域的网络安全评估模型,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,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。其不足之处在于安全状态域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。

由于大多数脆弱性评估方法都是定性评估,而且对脆弱性的等级定义标准各有不同,给评估、应急响应等带来了不确定性。基于此,美国基础设施顾问委员会提出了通用脆弱性评估系统(common vulnerability scoring system, CVSS)[7,8]。CVSS 是对单个脆弱性进行量化评估的方法,但是在网络安全分析中,由于网络中的主机和网络组件之间是交互的,因此孤立地分析某个脆弱性存在极大的局限性,只有把网络中的脆弱性关联起来分析,才能更好地把握网络可能受到的潜在攻击。另外,由于 CVSS 的度量标准具有很大的主观性,即对于同一个脆弱性,不同的人选择的属性值可能不同,因此评价分数也会不同,这必然给补丁优先级的确定带来很大的麻烦。

目前已涌现出了多种评估方法,通过对现有方法进行总结分析发现,其不足是:网络脆弱性评估系统比较简单,主要针对单个脆弱性进行量化评估,但是在实际的网络安全分析中,由于网络中的主机和网络组件之间是交互的,因此孤立地分析某个脆弱性存在极大的局限性,从而造成评估结果不全面、不准确。

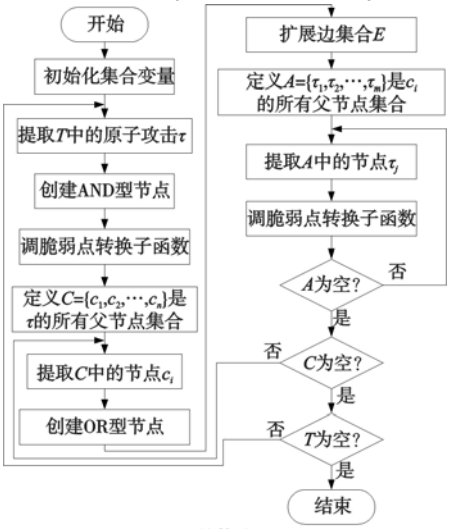
为了解决上述问题,本文在生成的攻击图基础上,提出了网络脆弱点依赖图的定义,将影响网络脆弱性指数评估的因素分为脆弱性自身特点、网络环境因素和脆弱性关联关系三部分;最后,按照网络拓扑的规模,采用自下向上、先局部后整体的思想,逐层逐级对目标网络进行评估。

2　基于攻击图的网络安全评估方法

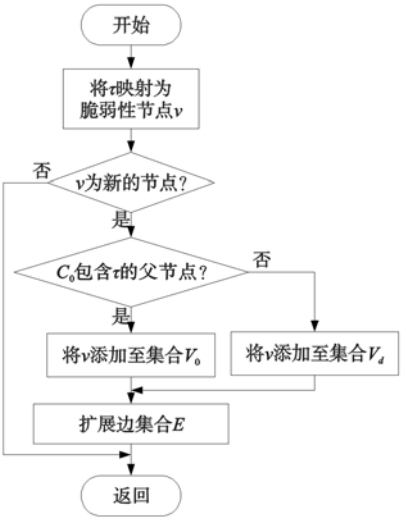
2.1　脆弱点依赖图

攻击图作为一种新兴的基于模型的网络安全评估技术,从攻击者的角度出发,在综合分析多种网络配置和脆弱性信息的基础上,自动枚举出所有可能的攻击路径,展示了原子攻击之间的关系,但它不能简洁地反映攻击者在攻击过程中所利用的不同脆弱点之间的依赖关系。为此,本文在攻击图的基础上提出了脆弱点依赖图的概念。安全管理员可以利用它确定目标网络内各种脆弱点的重要性并以此为依据确定为各脆弱点打补丁的优先级。

为了自动地将攻击图转换为脆弱点依赖图,本文提出了 VDG 算法。它将攻击图中的原子攻击节点映射为对应的脆弱性,并结合攻击图中原子攻击及属性节点之间的“或”和“且”关系,完成脆弱点依赖图。图 1 为程序流程。



(a)总体流程



(b)脆弱点转换子函数

图1　VDG算法流程

2.2　层次化网络脆弱性指数评估方法

针对大规模复杂网络,本文提出如图 2 所示的层次化网络脆弱性指数评估模型,从上到下分为网络、主机和漏洞三个层次。以 Nessus 扫描器获取的漏洞信息为原始数据,采取从下至上、先局部后整体的评估策略,首先评估漏洞的脆弱性指数,进而评估各主机的脆弱性指数,最后根据网络系统结构评估整个网络的脆弱性。

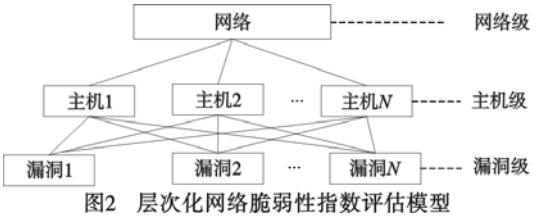


图2　层次化网络脆弱性指数评估模型

2.2.1　参数选取

为了评估漏洞的脆弱性,将影响漏洞脆弱性指数评估的因素分为脆弱性自身特点、网络环境因素和脆弱性关联关系三部分,如图 3 所示。

由于攻击者是利用网络中存在的漏洞实施攻击,有的漏洞只有极个别的攻击者掌握其攻击方法,而有的漏洞在网络上可以获得利用它的代码。同时,如果针对某漏洞存在补丁程序,或者有针对该漏洞的安全配置步骤,则说明该漏洞可以进行防

护,危害性比较小。因此,脆弱性自身特点考虑了利用代码和弥补措施两个因素,从漏洞自身的角度描述了攻击者利用漏洞进行攻击的难易程度,其值的大小反映了漏洞被攻击者利用的可能性大小。

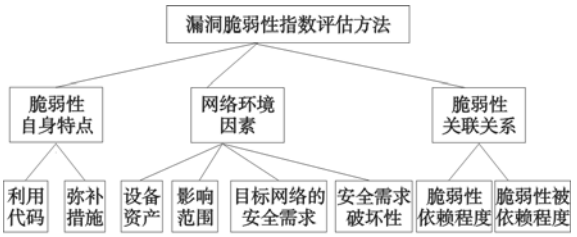


图3　漏洞脆弱性指数评估方法

在目标网络中,一方面,对于关键性的主机、服务器和路由器等设备,一旦遭到攻击,其造成的影响和损失将会是巨大的,因此漏洞所依赖的资产越关键,表示该漏洞潜在的影响范围越大,危害越大。同时,漏洞在目标网络内分布越广泛,对目标网络造成的危害也越大。另一方面,针对实际的目标网络,有的目标网络对机密性要求会高一些,而有的目标网络会对可用性要求高一些。比如主要从事网络服务提供的网络系统,其偏向可用性要多些;机要部门的网络系统对机密性偏向多一些;而电子商务类的网络系统几乎在完整性、可用性、机密性上是同等重要的,等等。因此,目标网络的安全需求及漏洞被利用后对安全需求造成的破坏成为考虑的因素。总之,为了描述漏洞被利用后对网络造成的影响,即攻击对网络造成破坏的严重程度,网络环境因素综合考虑了设备资产、影响范围、目标网络的安全需求和安全需求的破坏性四个因素,其值的大小反映了漏洞被利用后造成后果的严重程度。

由于目标网络中的脆弱点不是孤立存在的,只评估单个脆弱性忽略了脆弱性之间的关系,不全面。因此本文把网络中的脆弱性关联起来进行分析,利用 VDG 算法生成能够反映脆弱点之间依赖关系、脆弱性被利用先后顺序的脆弱点依赖图。在脆弱点依赖图中,$pre(V)$ 为脆弱点 V 的父节点集合,当 $pre(V)$ 中的一个脆弱点被利用后,V 就有被攻击者利用的可能性,所以 $pre(V)$ 中的脆弱点数目越多,V 被攻击者利用的可能性就越大,危害性就越大。同理,$post(V)$ 为脆弱点 V 的子节点集合,V 被利用后,$post(V)$ 中的一个或多个脆弱点就有被攻击者利用的可能性,所以 $post(V)$ 中的脆弱点数目越多,V 被依赖的程度就越大,危害性就越大。为此,脆弱性关联关系考虑了脆弱性依赖程度和被依赖程度两个因素。

2.2.2　参数取值

CVSS 是目前公认的脆弱性评估系统,其相关脆弱性评分因素的值在 CVE 中可以查到,因此本文采用了 CVSS 中的部分评分因素,如利用代码、弥补措施、目标网络的安全需求及安全需求的破坏性。

针对设备资产、影响范围因素的取值,目前尚无比较权威的专家或机构提出具有影响力和说服力的评估值。为了使评估结果更客观,本文采用专家赋值法,根据十位专家主观上对各评价指标的打分确定其取值。通过总结分析,设备资产有以下四种可选值:不重要,该漏洞被利用后对网络造成的损失微乎其微;不太重要,该漏洞被利用后对网络造成较低的损失;重要,该漏洞被利用后对网络造成中等程度的损失;非常重要,该漏洞被利用后对网络造成严重的损失。相应的评分值为 0、0.5、0.75、1.00。同样,影响范围有以下四种可选值:该漏洞在目标网络中分布范围很少,占网络中设备的 0% ~9%;该漏洞较小范围地存在于目标网络中,占网络中设备的 10% ~30%;该漏洞中等规模地存在于目标网络中,占网络中设备的 31% ~69%;该漏洞较大规模地存在于目标网络中,占网络中设备的 70% 以上。相应的评分值为 0、0.25、0.75、1.00。

针对脆弱性关联关系的取值,令目标网络中漏洞总数为 n,且脆弱性依赖程度用 dependence 表示。当脆弱点的依赖度为 $n-1$ 时,dependence = 1.00;当 $(n-1)/2 \leqslant$ 脆弱点的依赖度 $< (n-1)$ 时,dependence = 0.75,否则 dependence = 0.25。与脆弱性依赖程度相似,令目标网络中脆弱点总数为 n,且脆弱性被依赖程度用 $dependence_1$ 表示。当脆弱点的被依赖度为 $n-1$ 时,$dependence_1 = 1.00$;当 $(n-1)/2 \leqslant$ 脆弱点的被依赖度 $< (n-1)$ 时,$dependence_1 = 0.75$,否则 $dependence_1 = 0.25$。

在具体的实现过程中,首先使用 Nessus 扫描器获取目标网络中的漏洞信息,然后确定影响漏洞脆弱性评估的各个因素值,最后计算漏洞脆弱性指数评估值(vulasset),计算公式如下:

脆弱性自身特点评估值 = f(利用代码,弥补措施)

网络环境因素评估值 = f(设备资产,影响范围,目标网络的安全需求,安全需求破坏性)

脆弱性关联分析评估值 = f(脆弱性依赖程度,脆弱性被依赖程度)

vulasset = f(脆弱性自身特点评估值,网络环境因素评估值,脆弱性关联分析评估值)

其中:f 表示对影响脆弱性指数评估值的各个要素进行自下向上的聚合。本文采用直观易理解的加权平均法聚合函数,v_i 表示 x_i 的权重,则有

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n} v_i \cdot x_i, \sum_{i=1}^{n} v_i = 1 \quad (1)$$

主机脆弱性指数评估值(hostasset)的计算:按照 BS7799 的资产确定思想,主机由系统软件、应用软件及主机上运行的服务等组成,在计算出 vulasset 后,按照脆弱性所依赖的主机进行聚合,可以计算出 hostasset。

$$hostasset = f(vulasset_1, vulasset_2, \cdots, vulasset_n)$$

网络脆弱性指数评估值(netasset)的计算:网络系统本身包括网络拓扑、路由器(自治系统)互联关系、路由策略等,在计算出 hostasset 后,按照主机所依赖的路由器进行聚合,可以计算出 netasset。

$$netasset = f(hostasset_1, hostasset_2, \cdots, hostasset_n)$$

2.3　网络安全评估等级

为了便于国家计算机网络应急技术处理协调中心及相关网络安全管理人员对网络脆弱性指数的理解,按照网络脆弱性指数的计算结果,本文将网络安全评估分为“优、良、中、差、危”五个等级,各等级的具体含义参见表 1。

表 1　网络脆弱性指数定性描述

指数范围	级别	描述
(0.9,1]	优	网络安全状况优秀。网络中存在的漏洞造成的资产损失可以忽略不计
(0.7,0.9]	良	网络安全状况良好。网络中存在的漏洞造成的损失比较小,仅对网络的正常运行造成较小的影响
(0.3,0.7]	中	网络安全状况中等。网络中存在的漏洞造成的损失比较大,会对网络的正常运行造成比较大的影响
(0.1,0.3]	差	网络安全状况差。网络中存在的漏洞造成的损失很大,会对网络的正常运行造成很大的影响
(0,0.1]	危	网络安全状况高危。网络中存在的漏洞造成的损失特别大,会对网络的正常运行造成特别严重的影响

3　实验结果及分析

为了测试本文所提的网络安全评估方法,从不同角度分别

做了大量实验。

3.1　可行性、有效性

为验证该方法的可行性、有效性,搭建了如下简单的网络环境,如图 4 所示。其中服务器开放了 e-mail 和 FTP 两种服务,并存在 CVE-2004-0159 (remote-to-user)、CVE-2004- 0148 (remote-to-root)两个漏洞。由于服务器和外部主机之间设置了防火墙,因此这两种服务允许不同的内部主机访问,其中防火墙 1 只允许局域网 1 中的主机以 root 权限访问 FTP 服务,防火墙 2 只允许局域网 2 中的主机以 root 权限访问 e-mail 服务。攻击者通过 Internet 可以与内部网的主机相连。局域网 1 和 2 中的主机之间可以互相通信,而且局域网 1 中的每台主机存在 CVE-2002-0836 (remote-to-user)、CVE-2002-0838 (local-to-root)两个漏洞,局域网 2 中的每台主机存在一个 CVE-2002-0083 (remote-to-root)漏洞。通过执行 VDG 算法,其脆弱点依赖图如图 5 所示。

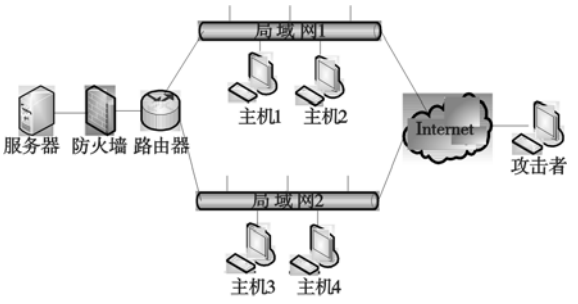


图4　实验网络环境

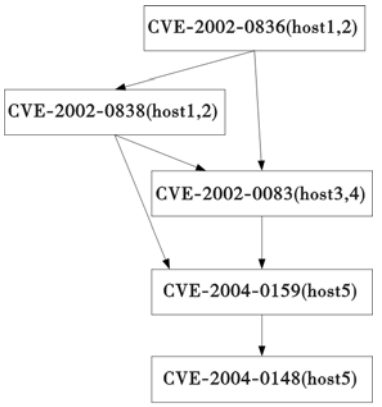


图5　实验环境的脆弱点依赖图

a)分析该网络中存在的漏洞,如表 2 所示。

表 2　网络中存在的漏洞

Hostname	Vulnerability
attacker	——
server	CVE-2004-0159,CVE-2004-0148
host1, host2	CVE-2002-0836,CVE-2002-0838
host3, host4	CVE-2002-0083
host3, host4	CVE-2002-0083

b)依次分析漏洞各个要素的取值,如表 3 所示。

表 3　漏洞各个要素的取值

CVE 编号	利用代码	弥补措施	设备资产	影响范围	目标网络安全需求	安全需求破坏性	脆弱性依赖程度	脆弱性被依赖程度
CVE-2004-0159	1.00	0.85	1.00	0.25	(0.33,0.33,0.33)	(0.00,0.00,0.00)	0.75	0.25
CVE-2004-0148	1.00	0.85	1.00	0.25	(0.33,0.33,0.33)	(1.00,0.00,1.00)	0.25	0.25
CVE-2002-0836	1.00	0.85	0.75	0.75	(0.33,0.33,0.33)	(0.00,0.00,0.00)	0.25	0.75
CVE-2002-0838	1.00	0.85	0.75	0.75	(0.33,0.33,0.33)	(0.00,0.00,0.00)	0.25	0.75
CVE-2002-0083	1.00	0.85	0.75	0.75	(0.33,0.33,0.33)	(0.00,0.00,0.00)	0.75	0.25

c)采用加权平均法聚合函数对表 3 中的各个要素进行自下向上的聚合,得到漏洞脆弱性指数评估值 vulasset,如表 4 所示。

表 4　漏洞脆弱性指数评估值(vulasset)

CVE 编号	vulasset
CVE-2004-0159	0.58
CVE-2004-0148	0.55
CVE-2002-0836	0.6
CVE-2002-0838	0.6
CVE-2002-0083	0.56

表 5　主机脆弱性指数评估值(hostasset)

主机 1	主机 2	主机 3	主机 4	服务器
0.6	0.6	0.56	0.56	0.57

d)采用加权平均法聚合函数对主机上所存在的脆弱性进行聚合,得到主机脆弱性指数评估值 hostasset,如表 5 所示。

e)采用加权平均法聚合函数对网络中所有主机进行聚合,得到网络脆弱性指数评估值 netasset = 0.58。

对照表 1 可得出:该目标网络的安全状况中等。网络中存在严重的漏洞,这些漏洞造成的损失可能比较大,会对网络的正常运行造成比较大的影响,应引起网络安全管理人员的注意,查找原因,并采取有效的安全措施确保网络的正常运行。

3.2　扩展性

为验证该方法的扩展性,能够适用于大规模复杂网络,图 6 给出实验的模拟网络拓扑图。模拟网络内子网的数目、每个子网内主机的数目、每台主机上存在的脆弱点个数的最大值都由用户输入,且主机上存在的脆弱点是随机分配的。因此,对于该模拟网络,可以通过增大网络内的主机数来改变目标网络的规模。

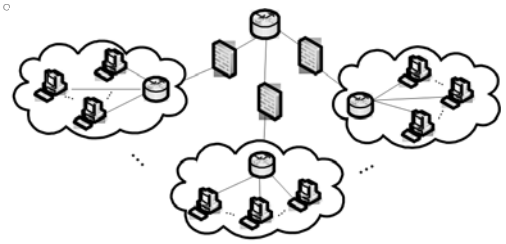


图6　模拟网络的拓扑图

本实验模拟了具有复杂拓扑结构的目标网络,该网络由 10 个子网构成,每个子网都有防火墙对其进行安全防护;每个子网内没有防火墙,因此子网内的主机之间可以互相通信;每台主机上最多有 5 个脆弱点。图 7 展示了该方法在不同的网络规模下评估所花费的 CPU 时间。从图 7 中可以看出,随着网络规模的扩大,CPU 消耗时间也不断增大,但增加的幅度在可以接受的范围内,当主机数目达到 1 000 台时,网络安全评估的时间也不过 13 min。

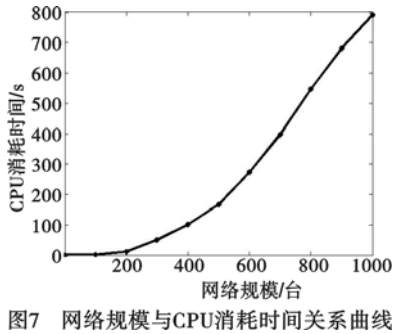


图7　网络规模与CPU消耗时间关系曲线

(下转第 1106 页)

$b_{2^{m+1}-1}^{(m+1)}$)。则 $L(\underline{b}^{(t)}) \neq R(\underline{b}^{(t)}), m+2 \leqslant t \leqslant r-1, L(\underline{b}^{(m+1)}) = R(\underline{b}^{(m+1)})$,且 $LC(L(\underline{b}^{(m+1)})) = 2^m - 1$。

由于 $\underline{b}^{(r)}$ 是 $L(\underline{a}^{(r+1)})$ 在位置 $u_1, u_2, \cdots, u_b$ 改变得到的。此时 $R(\underline{s}^{(r+1)})$ 作相应的变化可使得 $\underline{s}^{(r)}$ 变成 0。当 $b=4$ 时,因为 $W(\underline{s}^{(i)}) = 4, m+1 \leqslant i \leqslant r$,且 $\underline{s}^{(m)} = \varphi_{m+1} \cdots \varphi_r(\underline{s}^{(r)}) = 0$,则 $u_1 \equiv u_3 + 2^m \bmod 2^{m+1}, u_2 \equiv u_4 + 2^m \bmod 2^{m+1}$(当然还有其他的表示形式,此处只列出这一种形式,其他形式结果相同)。

$b_{u_1 \bmod 2^{m+1}}^{(m+1)}$, $b_{u_2 \bmod 2^{m+1}}^{(m+1)}$ 与 $b_{u_3 \bmod 2^{m+1}}^{(m+1)}$, $b_{u_4 \bmod 2^{m+1}}^{(m+1)}$ 分别属于 $L(\underline{b}^{(m+1)})$ 与 $R(\underline{b}^{(m+1)})$。因此适当改变 $b_{u_1 \bmod 2^{m+1}}^{(m+1)}, b_{u_2 \bmod 2^{m+1}}^{(m+1)}, b_{u_3 \bmod 2^{m+1}}^{(m+1)}, b_{u_4 \bmod 2^{m+1}}^{(m+1)}$ 来保证 $\begin{cases} b_{u_1 \bmod 2^{m+1}}^{(m+1)} + b_{u_3 \bmod 2^{m+1}}^{(m+1)} = 0 \\ b_{u_2 \bmod 2^{m+1}}^{(m+1)} + b_{u_4 \bmod 2^{m+1}}^{(m+1)} = 0 \end{cases}$,同时使得 $\begin{cases} b_0^{(m+1)} + b_2^{(m+1)} + \cdots + b_{2^m-2}^{(m+1)} = 0 \\ b_1^{(m+1)} + b_3^{(m+1)} + \cdots + b_{2^m-1}^{(m+1)} = 0 \end{cases}$,由引理 3 可知 $LC(L(\underline{b}^{(m+1)})) \leqslant 2^m - 2$ 与 $LC(L(\underline{b}^{(m+1)})) = 2^m - 1$ 矛盾,故 $c \neq 2^r - 2^m - 1$。当 $b=2$ 时,类似讨论也有 $c \neq 2^r - 2^m - 1$。

综上:当 $W_{2n}(\underline{s}) = W(\underline{s}^{(n)}) > 4, W(\underline{s}^{(m+1)}) \leqslant 4$ 时,$LC_{2^n,4}(\underline{s})$ 形如 $L'_{r,c} = 2^{n-1} + 2^{n-2} + \cdots + 2^{r+1} + c = 2^n - 2^{r+1} + c, 1 \leqslant c \leqslant 2^r - 2, c \neq 2^r - 2^m - 1$。

定理 2 设 $\underline{s} = (s_0, s_1, \cdots, s_{2^n-1})$,则满足线性复杂度为 $2^n - 2^m - 1$,且 $W_{2n}(\underline{s}) = W(\underline{s}^n) > 4, W(\underline{s}^{(m+1)}) > 4$ 的 2^n-周期二元序列的条数为 $2^{2^n - 2^m - 2^{r+1} + c + 2r - 1}$,其中 $2 \leqslant r \leqslant m-1, 1 \leqslant c \leqslant 2^r - 2$。

证明 由定理 1 情形 2 的证明过程可知,$LC(L(\underline{s}^{(m+1)})) = 2^m - 1, LC_{2n,2}(L(\underline{s}^{(m+1)})) = 2^m - 2^{r+1} + c, 2 \leqslant r \leqslant m-1, 1 \leqslant c \leqslant 2^r - 2$,由引理 4 可知满足该条件的序列的个数为 $2^{2^m - 2^{r+1} + c + 2r - 1}$。再由映射 φ_n 的性质 P3,满足 $LC(\underline{s}) = 2^n - 2^m - 1$ 且 $W_{2n}(\underline{s}) = W(\underline{s}^n) > 4, W(\underline{s}^{(m+1)}) > 4$ 的 2^n-周期二元序列的条数为 $2^{2^{n-1} + 2^{n-2} + \cdots + 2^{m+1} + 2^m - 2^{r+1} + c + 2r - 1} = 2^{2^n - 2^m - 2^{r+1} + c + 2r - 1}, 2 \leqslant r \leqslant m-1, 1 \leqslant c \leqslant 2^r - 2$。

例 1 设 $n=4, m=2$,求线性复杂度为 $2^n - 2^m - 1 = 11$ 的 2^n-周期二元序列 $s = (1,1,0,1,0,0,0,0,1,1,1,0,0,0,1,1)$ 的 4-错线性复杂度。

因 $W(\underline{s}) = W(\underline{s}^{(4)}) = 8 > 4$ 且 $W(\underline{s}^{(2)}) = 4$,利用定理 1 情形 3 的结论知 $1 \leqslant LC_4(\underline{s}) \leqslant 6, LC_4(\underline{s}) \neq 3$。计算得 $LC_4(\underline{s}) = 6$,与情形 3 的结论相符合。

3 结束语

本文给出了 F_2 上线性复杂度为 $2^n - 2^m - 1$ 的 2^n-周期二元序列 $\underline{s}$ 的 4-错或 5-错线性复杂度的表示形式,并在此基础上给出了特定重量下序列的条数。序列的期望和方差对流密码稳定性也起到了重要的作用,有待于进一步研究。

参考文献:

[1] DING Cun-sheng, XIAO Guo-zhen. The stability theory of stream ciphers [M]. Berlin: Springer-Verlag, 1991.

[2] STAMP M, MARTIN C F. An algorithm for the k-error linear complexity of binary sequences with period 2^n [J]. IEEE Trans on Information Theory, 1993, 39(4): 1398-1401.

[3] KUROSAWA K, SATO F, SAKATA T, *et al*. A relationship between linear complexity and k-error linear complexity [J]. IEEE Trans on Information Theory, 2000, 46(2): 694-698.

[4] MEIDL W. On the stability of 2^n-periodic binary sequences [J]. IEEE Trans on Information Theory, 2005, 51(3): 1151-1155.

[5] ZHU Feng-xiang, QI Wen-feng. The 2-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - 1$ [J]. Journal of Electronics, 2007, 24(3): 390-395.

[6] 谭林,戚文峰. F_2 上 2^n-周期序列的 k-错误序列[J]. 电子与信息学报, 2008, 30(11): 2592-2595.

[7] GAMES R A, CHAN A H. A fast algorithm for determining the complexity of a binary sequence with period 2^n [J]. IEEE Trans on Information Theory, 1983, 29(1): 144-146.

[8] FU Fang-wei, NIEDERREITER H, SU Ming. The characterization of 2^n-periodic binary sequences with fixed 1-error linear complexity [C]//Proc of SETA. Berlin: Springer, 2006: 88-103.

(上接第 1103 页)

4 结束语

本文的网络安全评估方法能定期地对网络系统进行安全扫描,分析扫描结果,帮助系统管理员更有效地管理整个网络系统。实验结果表明,该方法能够直观地给出漏洞、主机和整个网络系统三个层次的脆弱性指数评估值,使管理员及时地了解系统安全动态,查找安全变化的原因,调整安全策略,从而保证系统的安全。而且该方法具有很好的扩展性,可以适应对国家级公共基础网络或者运营商网络等大规模复杂网络脆弱性综合分析的需要。

参考文献:

[1] SWILER L P, PHILLIPS C, ELLIS D, *et al*. Computer-attack graph generation tool [C]//Proc of DARPA Information Survivability Conference and Exposition. [S.l.]: IEEE Computer Society, 2001: 1307-1321.

[2] SWILER L P, PHILLIPS C, GAYLOR T. A graph-based network-vulnerability analysis system, SAND97-3010/1 [R]. California: Sandia National Laboratories, 1998.

[3] JAJODIA S, NOEL S. Topological vulnerability analysis: a powerful new approach for network attack prevention, detection, and response [M]//Algorithm, Architectures and Information Systems Security. New Jersey: World Scientific, 2009: 285-305.

[4] OU Xin-ming. A logic-programming approach to network security analysis [D]. Princeton: Princeton University, 2005.

[5] LIPPMANN R P, INGOLS K W, SCOTT C, *et al*. Evaluating and strengthening enterprise network security using attack graphs, ESC-TR-2005-064 [R]. [S.l.]: Lincoln Laboratory, MIT, 2005.

[6] 张海霞,连一峰,苏璞睿,等. 基于安全状态域的网络评估模型[J]. 软件学报, 2009, 20(2): 451-461.

[7] CHAMBERS J T, THOMPSON J W. The common vulnerability scoring system: final report and recommendations by the council [R]. [S.l.]: National Infrastructured Advisory Council, 2004.

[8] MELL P. The common vulnerability scoring system (CVSS) and its applicability to federal agency systems [R]. [S.l.]: NIST, 2007.