基于攻击源激发和攻击原子筛选的攻击图构建方法

焦 波，黄赪东，黄 飞，李 伟
（中国人民解放军 63880 部队，河南 洛阳 471003）

摘 要：针对现有攻击图在大规模网络应用中存在的时间复杂性高和图形化展示凌乱等不足，提出一种新的构建方法：在目标网络模型和攻击者模型的基础上，以攻击源为起点广度遍历网络主机，针对主机间的网络连接，通过攻击模式实例化和信任关系获取攻击原子集，并根据攻击者贪婪原则和攻击原子发生概率计算尺度筛选攻击原子，同时更新攻击原子作用对象状态。通过实验分析，该方法面向网络主机实现一次遍历，筛选关键攻击原子，快速生成攻击图，不仅具有较高的时间效率，而且为安全事件分析提供客观的攻击路径信息。该方法能够满足大规模网络环境下的攻击辅助决策、入侵检测和网络安全评估等应用需求。

关键词：攻击图；网络安全；攻击原子；攻击源；贪婪原则
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2013)03-0891-03
doi:10.3969/j.issn.1001-3695.2013.03.064

Attack graph generation method based on attack source excitation and attack atom filter

JIAO Bo, HUANG Cheng-dong, HUANG Fei, LI Wei
(*Unit of* 63880 *of PLA*, *Luoyang Henan* 471003, *China*)

Abstract: With the shortcoming of high time complexity and messy graphical presentation in large scale network application for attack graphs, this paper proposed a new generation method. The method visited network hosts using breadth-first traversing algorithm from attack sources based on target network model and attacker model, acquired attack atoms with attack patterns instantiation and confidential relationship for network connections between two hosts, filtered attack atoms through greedy principle and probability metric for attack atoms, and updated effect states of attack atoms. The experimental results show that the method can traverse once among hosts and filter attack atoms, not only has higher time efficiency, but also provides objective attack paths information for security events analyzing. The proposed method can meet the needs of attacking auxiliary decision, intrusion detection and network security evaluation in large scale network environment.

Key words: attack graph; network security; attack atom; attack source; greedy principle

0 引言

攻击图是一种网络脆弱性分析方法，它以成熟的脆弱性发现技术为基础，把攻击者可能的攻击路径组合成图的形式展现出来，便于网络安全人员了解各个脆弱性之间的关系，有针对性地进行安全防护。攻击图构建方法经历了从手工构建到自动构建的阶段，当前正在从面向小型网络的自动构建到面向大规模网络的自动构建的方向发展。Swiler 等人[1]提出了攻击图的概念，但仅给出了手工构建攻击图的方法。Sheyner[2]采用模型检测技术自动构建攻击图，但此类方法枚举所有可能的攻击路径，存在不可避免的状态爆炸问题。Ammann 等人[3]提出了攻击者能力的单调性假设，并给出了时间复杂性为 $O(N^5)$ 的攻击图构建方法（N 为网络主机数目）。Ou 等人[4]基于推理机提出了时间复杂性近似为 $O(N^3)$ 的攻击图构建方法。Pamula[5]基于主机提出了时间复杂性为 $O(X\times Y\times N^2+N^3)$ 的攻击图构建方法（X 为攻击原子总数，Y 为网络脆弱点总数），其中 $O(X\times Y\times N^2)$ 用于主机之间权限的提升，$O(N^3)$ 用于获取间接攻击路径。朱明等人[6]基于贪心策略提出了时间复杂性为 $O(M\times N^3+N^4)$ 的攻击图构建方法（M 为节点关联关系数目）。

针对大规模网络攻击图的自动构建，基于主机的构建方法[5]采用最小状态空间有效地降低了时间复杂性，但仍存在以下不足：a）根据攻击者贪婪原则在主机对间筛选能够获取最大权限的攻击原子，没有考虑能够获取相同权限的不同攻击原子之间的差异性（发生概率）；b）采用类似最短路径的算法添加间接攻击路径，不仅增加了时间复杂性，而且导致大规模网络攻击图表现的凌乱性；c）未考虑不同攻击源可能在同一主机上获得不同的权限；d）未考虑攻击原子和脆弱点在不同主机的重复出现，增加了时间复杂性。通用脆弱点评价系统（common vulnerability scoring system，CVSS）是目前计算攻击原子发生概率的常用尺度[6,7]，但其仅考虑了脆弱点易用性，未与目标网络安全防护水平和网络管理人员响应程度相结合，综合考虑攻击原子发生概率。攻击模式[8]是攻击原子和脆弱点的抽象模板，通过模板中变量的赋值，可以实现不同主机对间攻击原子的实例化。采用有限规模的攻击模式知识库可以有

收稿日期：2012-05-03；**修回日期**：2012-06-20

作者简介：焦波（1981-），男，湖北老河口人，助理研究员，博士，主要研究方向为网络安全评估（jiaobonudt116@163.com）；黄赪东（1978-），男，工程师，硕士研究生，主要研究方向为网络安全评估；黄飞（1985-），男，硕士，主要研究方向为网络安全评估；李伟（1981-），男，工程师，主要研究方向为网络安全评估.

效避免攻击原子和脆弱点总数随主机个数线性增加的问题。

本文在现有研究成果的基础上,给出目标网络模型和攻击者模型的形式化描述,从脆弱点易用性、目标网络安全防护水平和网络管理人员响应程度三个方面综合考虑攻击原子发生概率,采用主机和攻击者权限构造最小状态空间,并站在攻击者角度,从不同攻击源出发,结合攻击者心理和目标网络状态,给出时间复杂性为 $O(N^2)$ 的攻击图构建方法。

1 目标网络模型与攻击者模型

目标网络模型可以划分为网络、攻击源主机和被攻击主机三个层次。网络模型主要包含网络主机(攻击源主机/被攻击主机)之间的逻辑连接关系和信任关系;攻击源主机模型主要描述初始状态下攻击者在攻击源主机上拥有的权限;被攻击主机模型主要描述被攻击主机开放的通信协议/端口和服务上存在的脆弱点。表 1 给出了目标网络模型的属性描述方法。

攻击者模型主要是对攻击者的攻击能力进行建模,其可采用攻击模式知识库构建。如表 2 所示,攻击模式可以采用 {Nam,Vul,Pre,Eff} 四元组表示。其中:Nam 为攻击模式名称;Vul 为攻击模式针对脆弱点的 CVE_ID 编号集;Pre 为脆弱点被利用的前提条件;Eff 为脆弱点被成功利用后可能对网络和攻击者属性产生的后果。攻击模式可以通过 CVE 等脆弱点知识库获取,其通过变量和 CVE_ID 编号的实例化,可以获得不同具体的攻击原子。

表 1 目标网络模型的属性描述

	属性描述
网络	conn(h_s:host, h_t:host, p_r:protocol,p_o:port): 源主机 h_s 可以通过协议 p_r 访问目的主机 h_t 的端口 p_o trust(h_s:host,p_{rs}:privilege, h_t:host, p_{rt}:privilege): 若在源主机 h_s 上拥有 p_{rs}权限,则可以通过信任关系以 p_{rt}权限访问目的主机 h_t
攻击源主机	privilege(h:host, root): 攻击者在主机 h 上获取管理员级访问权限 privilege(h:host, user): 攻击者在主机 h 上获取用户级访问权限 privilege(h:host, DoS): 攻击者在主机 h 上获取实施拒绝服务攻击的权限 privilege(h:host, access): 攻击者在主机 h 上获取基本访问权限
被攻击主机	hostService(h:host,s_e:service,p_r:protocol,p_o:port): 主机 h 通过协议 p_r 和端口 p_o 提供服务 s_e vulnerability(h:host,s_e:service,c:CVE_ID): 主机 h 上的服务 s_e 存在 CVE 编号为 c 的脆弱点

表 2 “缓冲区溢出获取 root 权限”攻击模式描述

Nam	Attack_Mode1
Vul	CVE 2003-0352, CVE 2004-0840, CVE 2002-0695
Pre	hostService(h_t,s_e,p_r,p_o);vulnerability(h_t,s_e, $c\in$Vul);conn(h_s,h_t,p_r,p_o);Privilege(h_s,root)
Eff	privilege(h_t,root)

2 攻击原子发生概率

攻击者具有贪婪性的特征,即最大可能地增强自身的攻击能力和扩大其对目标网络的控制能力。因此,攻击者将选取能够获得最大权限且发生概率最大的攻击原子实施攻击。攻击原子包含两类:a)利用主机对间的信任关系提升权限;b)利用目的主机脆弱点提升权限。前者攻击原子发生概率可视为 1.0,后者攻击原子发生概率从脆弱点易用尺度、安全防护尺度和网管关注尺度三个方面计算。

1)脆弱点易用尺度[7] CVSS 评价系统中 access complexity属性值 L,表征攻击者渗透该脆弱点的难易程度;按照 CVSS 推荐,针对 L 的不同取值{“高”,“中”,“低”,“不定”},脆弱点 v 对应攻击原子的发生概率 $P_1(v)$ 的取值分别为 {0.35,0.61,0.71,0.71}。

2)安全防护尺度 防火墙能够有效降低攻击原子的发生概率;针对目标网络中部署防火墙的关键联络,在模拟正常背景业务流量的情况下,采取模拟攻击流量[9]进行多次测试,根据防火墙的拦截率计算攻击原子发生概率 $P_2(v)$;针对未部署防火墙的链路,令 $P_2(v)=1.0$。

3)网管关注尺度 IDS(入侵检测系统)会记录历史上的网络攻击行为;网络管理人员根据这些历史记录,通常会增强对此类网络攻击行为的警觉;采用 $N_{\mathrm{IDS}}(v)$ 表示 IDS 在一定历史时间段内检测出脆弱点 v 对应攻击原子的发生次数,计算攻击原子发生概率 $P_3(v)=\exp(-\lambda\times N_{\mathrm{IDS}}(v))$。其中 λ 是控制发生概率衰减速度的参数,也是网络管理人员的决策偏好;针对未部署 IDS 的链路,令 $P_3(v)=1.0$。

脆弱点易用尺度、安全防护尺度和网管关注尺度分别从脆弱点易用性、目标网络安全防护水平和网络管理人员响应程度三个方面,衡量攻击原子发生概率。为了综合考虑三个尺度,可以采用判断矩阵的群决策方法[10]给出合理的权值分配,并通过层次分析法(AHP)实现攻击原子发生概率三个下级指标的聚合。

3 攻击图构建方法

定义 1 攻击图 $AG=(V_s,V_e,V_u,E)$,其中 V_s 为攻击源状态节点集,V_e 为攻击效果状态节点集,V_u 为不可达状态节点集,E 为有向弧集。状态节点采用二元组 (h,p_r) 表示,其中 h 为主机名,p_r 为攻击者在 h 上获取的权限;将权限按递增次序划分为 none、access、DoS、user、root 五个等级(见表 1,其中 none 表示攻击者在目标主机上无权限);设 V_s、V_e 和 V_u 的属性 h 互不相交且并集构成网络全部主机;V_s 和 V_e 的属性 $p_r\in$ {access,DoS,user,root},V_u 的属性 $p_r\in$ {none};有向弧采用三元组 (h_s,h_t,l) 表示,其中 h_s 为攻击源主机名,h_t 为目的攻击主机名,l 为目的攻击主机上存在的脆弱点(或信任关系)。

目标网络模型、攻击模式知识库、CVSS 评价系统(脆弱点易用尺度)、防火墙攻击拦截测试报告(安全防护尺度)、IDS 攻击行为日志(网管关注尺度)和安全防护需求分析报告等,为攻击图构建方法的输入数据。如图 1 所示,本文从攻击者角度出发,根据贪婪性原则[5,6],给出攻击图构建方法 attack-graph-generation。其中输出的攻击原子集 AS 与有向弧集 E 一一对应,$|\cdot|$ 表示集合包含元素的个数,Prob(a) 表示攻击原子 a 的发生概率。

攻击图构建方法 attack-graph-generation

//输入:a)攻击源状态节点集 V_s,$(h,p_r)\in V_s$ 由“攻击源主机”中 privilege 函数组成(表 1);b)逻辑连接关系集 LS,由“网络”中的 conn 函数组成(表 1);c)信任关系集 TS,由“网络”中 trust 函数组成(表 1);d)网络主机集 HS,被攻击主机集 $HS\subseteq HS$,设 $|HS|=N$,$|\overline{HS}|=\overline{N}$;e)被攻击主机属性集 $\{HI(h^i)\}_{i=1}^{N}$,$HI(h^i)$ 由“被攻击主机” h^i 的 hostService/vulnerability 函数组成(表 1);f)攻击模式知识库 AMR;g)概率阈值 Th。

//输出:攻击原子集 AS、攻击效果状态节点集 V_e 和不可达状态节点集 V_u。

a)设集合 $\{NC(h^i)\}_{i=1}^{N}$ 记录攻击者从当前攻击源出发,在网络主机 $h^i(i=1,2,\cdots,N)$ 上获取的权限;令 $AS:=\varnothing$,集合 $V:=V_s$,$V_e:=\varnothing$;转 b);

b)若 $V=\varnothing$,则令集合 $KS:=\{h\in HS\mid h$ 不为 V_s 和 V_e 中任意元素的属性值$\}$,令 $V_u:=\{(h,p_r)\mid h\in KS,\ p_r=\text{none}\}$,算法结束;若$V\neq\varnothing$,则选取$(h^*,\ p_r^*)\in V$,令 $V:=V-\{(h^*,\ p_r^*)\}$,初始化$\{NC(h_i)\}_{i=1}^{N}$为 none,令 $NC(h^*):=p_r^*$,令集合 $FS:=\{h^*\}$,集合 $RS:=\varnothing$,转 c);

c)若 $FS=\varnothing$,则转 d),否则选取一个主机 $h_s\in FS$,令 $FS:=FS-\{h_s\}$,转 e);

d)若 $RS=\varnothing$,则转 b),否则令 $FS:=RS$,$RS:=\varnothing$,转 c);

e)令集合 $CS:=\{h_t\in HS\mid \exists\,\text{conn}(h_s,h_t,*,*)\in LS\vee\exists\,\text{trust}(h_s,*,h_t,*)\in TS\}$,对$\forall h_t\in CS$:

(a)依据 $NC(h_s)$、$\text{conn}(h_s,h_t,*,*)$、$HI(h_t)$和 AMR 实现攻击模式实例化,并结合信任关系 $\text{trust}(h_s,*,h_t,*)$,获取源主机 h_s 至目的主机 h_t 的攻击原子集 $AS_{s,t}$;(b)根据攻击原子发生概率,利用阈值 Th 剔除 $AS_{s,t}$中发生概率较小的攻击原子,将剩余攻击原子按其在 h_t 上获取的权限等级,划分为四个子集 $AS_{s,t}^{\text{access}}$、$AS_{s,t}^{\text{DoS}}$、$AS_{s,t}^{\text{user}}$和 $AS_{s,t}^{\text{root}}$,设 $AS(s,t)$为这四个子集中权限等级最高且不为空的子集;(c)根据贪婪原则,令 $a^*=\arg_a\{\max_{a\in AS(s,t)}\text{prob}(a)\}$,令 $AS:=AS+\{a^*\}$,利用 a^*更新 $NC(h_t)$;(d)若$(h_t,NC(h_t))\notin V_e$,则令 $RS:=RS+\{h_t\}$,$V_e:=V_e+\{(h_t,NC(h_t))\}$;

处理完 CS 中的元素,转 c)。

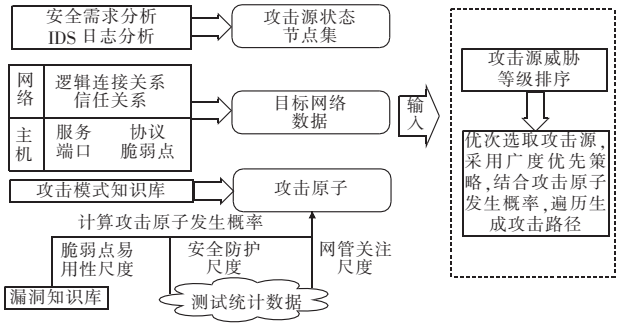

图 1　攻击图构建方法示意图

4　时间复杂性分析

设网络主机数目为 N,攻击模式知识库中攻击模式的数目为 W,攻击模式中 Pre 和 Eff 属性包含元素数目的上界为 U,CVSS 评价系统包含脆弱点的数目为 C。由定义 1 知 attack-graph-generation 生成状态节点的个数不大于 $5N$,因此状态节点对的数目不大于 $25N^2$。针对每对状态节点,$\text{trust}(h_s,*,h_t,*)$仅一个且 $\text{conn}(h_s,h_t,*,*)$包含于攻击模式的 Pre 或 Eff 属性。因此 attack-graph-generation 对应攻击图构建方法步骤 e)中攻击模式实例化步骤不大于 $U\times W$,信任关系步骤不大于 1。网络部署防火墙和 IDS 种类的有界性,使得攻击原子发生概率的计算复杂性为 $O(C)$。因此 attack-graph-generation 的时间复杂性为 $O(25N^2\times(U\times W+1)\times C)$。因为攻击模式知识库和 CVSS 评价系统的有界性(U、W 和 C 有界),所以 attack-graph-generation 的时间复杂性为 $O(N^2)$。

5　实验结果与分析

图 2 给出了 attack-graph-generation 应用的实验网络部署图,其中 IP 为 192.168.1.254 的 Mail 服务器提供邮件传输服务,IP 为 192.168.0.253 的 SQL 服务器提供数据库服务。

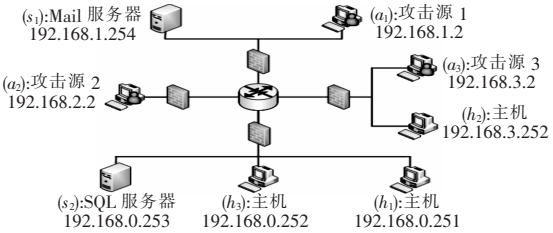

图 2　实验网络部署图

表 3 给出了实验网络部署图的网络模型、攻击源主机模型和被攻击主机模型属性描述。表 2、4 和 5 给出了实验网络部署图涉及的攻击模式。

表 3　目标网络属性描述

	属性描述		
网络	$\text{conn}(a_2,s_1,\text{TCP},25)$;$\text{conn}(a_1,s_1,\text{TCP},25)$ $\text{conn}(s_1,s_2,\text{TCP},1433)$;$\text{conn}(a_1,h_3,\text{TCP/UDP},*)$ $\text{conn}(h_3,s_2,\text{TCP},1433)$;$\text{conn}(h_1,s_2,\text{TCP},1433)$ $\text{trust}(a_3,\text{root},h_2,\text{root})$;$\text{conn}(h_2,h_1,\text{TCP/UDP},*)$		
攻击源主机	192.168.1.2 (a_1): Privilege(a_1,root);	192.168.2.2 (a_2): privilege(a_2, root)	192.168.3.2 (a_3) privilege(a_3, root)
被攻击主机	192.168.0.251(h_1)	$\text{hostService}(h_1,\text{UNIX},\text{TCP/UDP},*)$ $\text{vulnerability}(h_1,\text{UNIX},\text{CVE 2001-0439})$	
	192.168.3.252(h_2)	$\text{hostService}(h_2,\text{WinXP},\text{TCP/UDP},*)$ $\text{vulnerability}(h_2,\text{WinXP},\text{CVE 2003-0352})$	
	192.168.0.252(h_3)	$\text{hostService}(h_3,\text{WinXP},\text{TCP/UDP},*)$ $\text{vulnerability}(h_3,\text{WinXP},\text{CVE 2003-0352})$	
	192.168.1.254(s_1)	$\text{hostService}(s_1,\text{Mail},\text{TCP},1433)$ $\text{vulnerability}(s_1,\text{Mail},\text{CVE 2004-0840})$ $\text{vulnerability}(s_1,\text{Mail},\text{CVE 2010-0024})$	
	192.168.0.253(s_2)	$\text{hostService}(s_2,\text{SQL},\text{TCP},1433)$ $\text{vulnerability}(s_2,\text{SQL},\text{CVE 2002-0695})$ $\text{vulnerability}(s_2,\text{SQL},\text{CVE 2001-0498})$	

表 4　“缓冲区溢出获取 user 权限”攻击模式描述

Nam	Attack_Mode2
Vul	CVE 2001-0439
Pre	$\text{hostService}(h_t,s_e,p_r,p_o)$;$\text{vulnerability}(h_t,s_e,c\in\text{Vul})$ $\text{conn}(h_s,h_t,p_r,p_o)$;$\text{privilege}(h_s,\text{root})$
Eff	$\text{privilege}(h_t,\text{user})$

表 5　“DOS”攻击模式描述

Nam	Attack_Mode3
Vul	CVE 2010-0024, CVE 2001-0498
Pre	$\text{hostService}(h_t,s_e,p_r,p_o)$;$\text{vulnerability}(h_t,s_e,c\in\text{Vul})$ $\text{conn}(h_s,h_t,p_r,p_o)$;$\text{privilege}(h_s,\text{user})$
Eff	$\text{privilege}(h_t,\text{DoS})$

针对图 2 的实验网络部署图,利用 attack-graph-generation 可以获取图 3 对应的攻击图。Attack-graph-generation 是一种基于主机的攻击图构建方法,其采用二元组的最小状态空间,使攻击图包含的信息量相对降低(不足),但其符合攻击者以主机为攻击对象的直观意愿和力争在主机上获取最高权限的贪婪性特征。其正确性体现在:通过目标网络数据采集、防火墙测试、IDS 日志统计等策略,增强攻击图构建方法的定量数据支撑;通过攻击者贪婪性的模拟,使得攻击路径的生成符合网络攻击行为的实施过程;通过基于主机的广度优先遍历,使得攻击图全面体现攻击者针对网络主机的最大攻击能力。

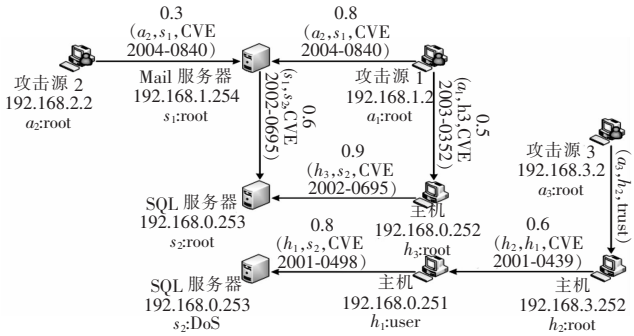

图 3　实验网络的攻击图

Attack-graph-generation 在保持原有方法[5] 低时间复杂性优势的前提下,其以攻击源为起点(根据贪婪原则)搜索攻击路径,删除攻击图中的冗余信息,使攻击图的展示更加清晰;采用脆弱点易用尺度、安全防护尺度和网管关注尺度综合考虑攻击原子发生概率,增强概率计算的客观性;借鉴(下转第 896 页)

衡的。当$1\leqslant W_H(\omega)\leqslant t$时,由条件b)知$P_1^{-1}(\beta)$和$P_2^{-1}(\beta)$均不存在,可得$S_f(\omega)=0$。由引理3得,$f(x)$是$t$阶相关免疫平衡函数。

定理5 $f(x,z,y)$满足严格雪崩准则,且一定条件下满足n次扩散准则。

证明 令$s=(\alpha,\gamma,\beta)\in F_2^n,\alpha\in F_2^k,\beta\in F_2^{k+1},\gamma\in F_2$,则有$f$的自相关函数为

$$2^n r_f(s)=\sum_{\tau\in F_2^n}(-1)^{f(\tau+s)+f(\tau)}=$$
$$\sum_{(x,z,y)\in F_2^n}(-1)^{[(1+z+\gamma)P_1(x+\alpha)+(z+\gamma)P_2(x+\alpha)]\times(y+\beta)+[(1+z)P_1(x)+zP_2(x)]\times y}=$$
$$\sum_{(x,y)\in F_2^{n-1}}(-1)^{[\gamma P_1(x+\alpha)+(1+\gamma)P_2(x+\alpha)]\times(y+\beta)+P_2(x)\times y}+$$
$$\sum_{(x,y)\in F_2^{n-1}}(-1)^{[(1+\gamma)P_1(x+\alpha)+\gamma P_2(x+\alpha)]\times(y+\beta)+P_1(x)\times y}$$

讨论:a)当$\gamma=0$时,

$$2^n r_f(s)=\sum_{(x,y)\in F_2^{n-1}}(-1)^{P_2(x+\alpha)\times(y+\beta)+P_2(x)\times y}+$$
$$\sum_{(x,y)\in F_2^{n-1}}(-1)^{P_1(x+\alpha)\times(y+\beta)+P_1(x)\times y}$$

(a)当$\alpha\neq 0$时,$P_1(x+\alpha)\neq P_1(x)$,$P_2(x+\alpha)\neq P_2(x)$,所以$r_f(s)=0$。

(b)当$\alpha=0$时,$2^n r_f(s)=2^{k+1}(\sum_{\beta\in F_2^{k+1}}(-1)^{P_2(x)\times\beta}+\sum_{\beta\in F_2^{k+1}}(-1)^{P_1(x)\times\beta})$,由条件c)知,当$W_H(\beta)=1$时,$\sum_{\beta\in F_2^{k+1}}(-1)^{P_1(x)\times\beta}=0$且$\sum_{\beta\in F_2^{k+1}}(-1)^{P_2(x)\times\beta}=0$,显然当$\alpha=0,\gamma=0$时,$W_H(s)=W_H(\beta)$。故$W_H(s)=1$时,$r_f(s)=0$,满足严格雪崩准则。

另外,若$\alpha=0$且$W_H(\beta)$是奇数时,$r_f(s)\equiv 0$。

b)当$\gamma=1$时,$r_f(s)=0$;当$\alpha=0,\beta=0$时,$W_H(s)=1$。故函数满足严格雪崩准则。在此条件下,当$1\leqslant W_H(\alpha)\leqslant n$时,总有$r_f(s)=0$,满足$n$次扩散准则。

定理6 $f(x,z,y)$不含非零线性结构。

证明 反证法。假设存在一个非零向量$u\in F_2^n$,使$\varphi(u,v)=f(0)+f(u)+f(v)+f(u+v)=0(v\in F_2^n)$,则$|r_f(s)|=1$成立。此时$\alpha=0,\gamma=0$且$|\sum_{\beta\in F_2^{k+1}}(-1)^{P_1(x)\times\beta}+\sum_{\beta\in F_2^{k+1}}(-1)^{P_2(x)\times\beta}|=2^k$。由定理5知$W_H(\beta)$是偶数。因此,当$y_1\in U_1,y_2\in U_2$时,$\#\{\beta\in F_2^{k+1}\mid y_1\times\beta=y_2\times\beta=b\}=2^{k-1},b\in\{0,1\}$为常数。其中$y_1\times\beta$是常数,因为$|U_1|=2^{k-1}$,所以当$y_1\notin U_1$时,$y_1\times\beta$亦是常数。由条件c)知存在$W_H(y_1')=1,y_1'\notin U_1$,使$y_1'\times\beta=1$。然而$0\notin U_1$,此时$y_1'\times\beta=0$。即$y_1'\times\beta$不是常数。同理可证$y_2'\notin U_2,y_2'\times\beta$不是常数。出现矛盾,故不存在非零线性结构。证毕。

4 结束语

本文利用部分Bent函数中的线性维数作为这些性质的统一变量,定量刻画了部分Bent函数的性质;结果表明,部分Bent函数能同时满足多种密码学性质,但函数中存在一定的线性结构,使得其非线性度达不到理想的程度。本文以排除函数中的线性空间为目的,构造了一种不含非零线性结构的函数。构造的函数具有高的非线性度,满足平衡性、相关免疫性及严格雪崩准则,且不具有像半Bent函数那样的退化性。

参考文献:

[1] CARLET C. Partially-bent functions[C]//Advance in Cryptoloy-CRYPT'92. Berlin:Springer-Verglag,1993:280-291.

[2] ZHOU Yu, XIE Min, XIAO Guo-zhen. On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity[J]. Information Science, 2010,180(2): 256-265.

[3] ZHANG Wei-guo. Construction of plateaued functions satisfying multiple criteria[J]. High Technology Letters,2005,11(4):364-366.

[4] 张卫明,李世取. 带1比特记忆组合生成器的条件相关性[J]. 信息工程大学学报,2002,3(2):13-16.

[5] 秦静,赵亚群. 半Bent函数的密码学性质[J]. 山东大学学报:理学版,2002,37(6):480-483.

[6] ZHANG Wei-guo, XIAO Guo-zhen. Construction of almost optimal resilient functions via concatenating Maiorana-McFarland functions [J]. Science China Information Science,2011,54(4): 909-912.

[7] ZHUO Ze-peng, ZHANG Wei-guo, XIAO Guo-zhen. Constructions of cheating immune secret sharing functions[J]. High Technology Letters, 2011,17(1):102-105.

[8] GAO Sheng, MA Wen-ping, ZHUO Ze-peng, *et al*. Walsh spectrum of cryptographically concatenating functions and its applications in constructing resilient Boolean functions[J]. Journal of Computational Information Systems,2011,7(4):1074-1081.

[9] 赵亚群,冯登国,李世取. 部分Bent函数的密码学性质[J]. 通信学报,2002,23(5):113-118.

(上接第893页)攻击模式知识库概念,在此基础上给出目标网络模型和攻击者模型的形式化描述方法,为数据的采集、存储以及攻击图构建的数据来源提供支撑;针对每个攻击源,采用步骤e)中的d)的状态$(h_t,\mathrm{NC}(h_t))$解决不同攻击源可能在同一主机上获得不同权限的问题,同时避免对同一状态节点的重复遍历,实现时间复杂性为$O(N^2)$的攻击图构建方法。

6 结束语

本文从攻击者角度,根据攻击者贪婪原则和攻击原子发生概率计算尺度,通过网络主机的近似一次遍历,筛选关键攻击原子,设计时间复杂性为$O(N^2)$的攻击图构建方法,不仅具有较高的时间效率(符合大规模网络攻击图的自动构建需求),而且为安全事件分析提供客观的攻击路径信息。

参考文献:

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

[2] SHEYNER O. Scenario graphs and attack graphs[D]. Pittsburgh:Carnegie Mellon University,2004.

[3] AMMANN P,WIJESEKERA D,KAUSHIK S. Scalable, graph-based network vulnerability analysis[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press, 2002:217-224.

[4] OU Xin-ming,BOYER W F,MCQUEEN M A. A scalable approach to attack graph generation [C]//Proc of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006:336-345.

[5] PAMULA J. Attack graph: scalable construction and analysis[D]. Fairfax:George Mason University,2007.

[6] 朱明,殷建平,程杰仁,等. 基于贪心策略的多目标攻击图生成方法[J]. 计算机工程与科学, 2010,32(6):22-25.

[7] 叶云,徐锡山,贾焰,等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报,2010,33(10):1987-1996.

[8] 毛捍东, 陈峰, 张维明, 等. 网络组合攻击建模方法研究进展[J]. 计算机科学,2007,34(11):50-61.

[9] 百度文库. 抗拒绝服务攻击设备测试方案[EB/OL]. [2010-12-26]. http:// wenku. baidu. com/view/5f7faef8aef8941ea76e057f. html.

[10] 徐泽水. 基于残缺互补判断矩阵的交互式群决策方法[J]. 控制与决策,2005,20(8):913-916.