基于权限变更规则的网络脆弱性分析方法①

莫秋妹, 陈启买

(华南师范大学 计算机学院, 广州 510631)

摘 要：网络脆弱点有导致访问者权限变更的隐患。从攻击者如何利用脆弱点获取目标实体未授予访问权限的角度出发，本文通过对拥有权限变更特征的脆弱点统一建模，引入 take 权限变更规则和脆弱点权限变更规则的概念，在构建权限变更图基础上利用脆弱性权限变更算法进行权限变更路径的分析，得到网络权限变更闭包图及相应的权限获取路径。最后通过构建相应的网络实例分析并证明该方法的有效性。

关键词：网络安全；脆弱点；脆弱性分析；权限变更

Right-Variation Rule Based Network Vulnerability Analysis

MO Qiu-Mei, CHEN Qi-Mai

(School of Computer, South China Normal University, Guangzhou 510631, China)

Abstract: Network vulnerability can lead to right-variation. From the view of how an attacker uses the vulnerabilities to achieve the unauthorized right of the destination entity, this paper models the vulnerabilities which lead to right-variation and introduces the concept of take rule and vulnerability right-variation rule. Based on the constructed right-variation model and the rules, the right-variation road closure can be achieved by using the vulnerability right-variation algorithm. A vulnerable network is modeled as the study case and it shows the effectiveness of the approach.

Key words: network security; vulnerability; vulnerability analysis; right-variation

1 脆弱点研究概述

当今网络安全面临各种威胁，如网络服务异常或不可用，根本原因在于网络本身存在脆弱点[1-6]。传统有关脆弱性的网络安全分析方法主要包括模型检测[12]和基于图论[9]技术，不少学者进行脆弱点的关联性研究[3]，相关算法经过不断改良而具有较好的时间和空间复杂性，但仍存在过多人工输入工作或与实际应用不符等问题。本文从攻击者角度出发，收集网络关键配置及相关脆弱点信息进行权限变更模型图的构建，同时对网络脆弱点进行统一规则建模，提出一种有效的网络脆弱性权限变更分析算法，并证明该算法能够在多项式时间内获取权限变更模型图的全部权限变更路径。

2 脆弱点权限变更模型VRV

从攻击者角度出发，研究脆弱点产生的环境及规则，引入权限变更规则，利用网络配置及脆弱点信息描述脆弱性环境，定义权限变更模型图，并给出相关的形式化描述。

2.1 网络脆弱点相关定义

学者们根据自身的不同理解对脆弱点进行了定义，目前接受较为广泛的是 Bishop 和 Baiey(1996)[1,15]对脆弱点的定义，描述如下：

定义 1. 计算系统 Computing System。简称 SC，计算系统是一种状态机 SYS = (S, S_0, t, S_A, S_U)，其中 S 为所有状态的集合，S0⊆S，为系统的初始状态集，t⊆S×S，是状态集的转化过程，S_A⊆S 和 S_U⊆S 分别代表可授权状态集和未授权状态集，其中 $S_A \cap S_U = \Phi$, $S_A \cup S_U$= S。

定义 2. 脆弱状态 Vulnerable State。简称 SV，状态 s (s∈SV)是脆弱的当且仅当 s 是一个授权状态，有未授权状态 s’(s’∈S_U)，s 经过若干个转化过程 $t_1, t_2, \cdots$ 最终到达状态 s’，即 $S \xrightarrow{t_1} \cdots\cdots \xrightarrow{t_i} S'$，i=1,2,…。

① 基金项目:广东省科技计划项目(2009B090300326)
收稿时间:2011-09-15;收到修改稿时间:2011-11-06

脆弱点定义为区别于所有脆弱性状态的若干属性或特征。

网络中普遍的脆弱点利用(Vulnerability Exploitation)会导致访问权限的变更，攻击者利用脆弱点获取非授权的权限集。

2.2 脆弱点权限变更模型 VRV

在对网络脆弱性的机理研究前提下，提出脆弱点权限变更模型 Vulnerability Right-Variation Model (VRVM)，参考网络攻击图[9]和 Take-Grant 安全模型[13](Jones, 1976)的构建思想对模型图进行扩展。

定义 3. 脆弱点权限变更模型 VREM。VRE= (V, R, L, A),V 为模型图的结点，表示网络实体，R、L 均作为模型图的边，R 为源实体对目标实体所拥有的访问权限集，L 是关联关系集，A 为关键脆弱点属性的集合。

定义 4. 访问权限 Access Right。简称 RC， RC = {(u, v, S_R)| u, v∈E, $S_R \subseteq R$ }，即实体 u 对实体 v 拥有访问权限集 S_R。

访问权限包括执行权限 execution，读权限 read 和写权限 write，分别用 x, r, w 表示，引入获取权限 take，用 t 表示，因此，R={ x, r, w, t }。

定义 5. 实体关联关系 Relationship。简称 L， L= {(u, v, S_L)| u, v∈E, $S_L \subseteq L$ }，即实体 u 和实体 v 存在关联关系集 S_L。

不失一般性，实体间的关联关系集定义为 L={h, o }， h 表示主体对实体的主控关系 hosting，如(c_1, f_1, h)表示主机 c_1 对文件 f_1 有 h 关系；o 为主体对客体的拥有关系 ownership，如最高管理者 root 拥有传输服务 http，表示成(root, http, o)。

模型中的数据收集可通过有效的主机和网络脆弱性扫描工具获得，如 OVAL Scanner 和 Nessus Scanner，并参考通用脆弱点数据库如 NVD[7]有关脆弱点信息的描述。

3 权限变更规则

参照 take-grant 安全模型的相关定义，进行 take 获取权限变更规则的建模，并简称为 take 规则；基于 take 规则的可循性，进行典型网络脆弱点的分组建模，得出通用脆弱点权限变更规则(Common Vulnerability Right-Variation Rule, CVRV)。

3.1 take 规则

take 规则的基本思想如下：

Take-rule: x, y 和 z 为模型图中三个不同结点，x 作为主体。从 x 到 y 的权限边标识为 α，其中 t∈ α ⊆R，对从 y 到 z 的权限边 β 有 α ⊆ β ⊆R，利用 take 规则增加一条自 x 到 z 的权限边 β 。(如图 1)

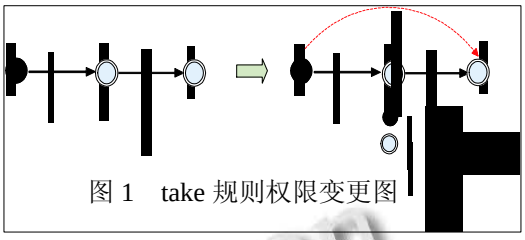


图 1 take 规则权限变更图

3.2 通用脆弱点权限变更规则

对同类型的脆弱点建模，得到通用脆弱点权限变更规则，反映脆弱点信息对访问权限的影响过程。

定义 6. 通用脆弱点权限变更规则 Common Vulnerability Right-Variation Rule。简称 CVRV 规则，CVRV = (G_{pre}, M, u)，Gpre 是脆弱点利用的前置条件图；M 为规则映射，把前置条件图映射为后置条件图 G_{pos}；u 是脆弱点利用的攻击主体。

下面通过对常见的三种脆弱点进行规则建模(如图 3，图 4 和图 5)。

BOF 规则。针对 BOF 脆弱点(Buffer Overflow Vulnerabilities，缓冲区溢出脆弱点)：带有 BOF 的进程 p 在主机 c 上以帐户 a 的身份运行，攻击者 A 对 p 有执行权限 x。则 A 能利用脆弱点 BOF 在帐户 a 下执行任意代码。可见，BOF 前置条件是攻击者对进程有执行权限 x 以及存在脆弱点 BOF，图中标识为{BOF}。

WPW 规则。涉及弱密码脆弱点 WPW(Weak Password Vulnerability)。当用户 a 在主机 c 上定义了一个强度不高的密码，主机 c 对访问用户提供登录服务(login service)，攻击者 A 通过猜测帐户 a 的密码而获取 a 的所有权限。弱密码脆弱点标识为{WPW}，同时把登录服务也看作脆弱点标识为{Login}。

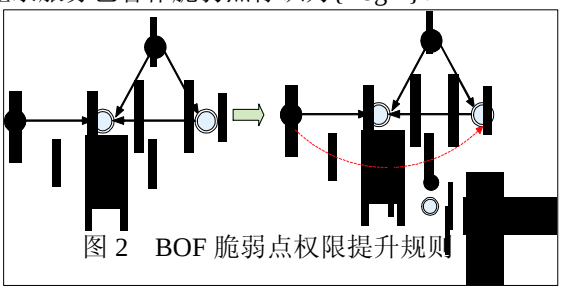


图 2 BOF 脆弱点权限提升规则

TRS 规则。可信关系脆弱点 TRS(Trust Relationship Vulnerability)使得用户 a1 与其它用户 a2 成为信任关系而允许 a2 访问其内部资源。因为攻击者不必运行任何

程序或恶意代码就能利用此脆弱点（图中标识为{ TRS }），在构建模型图时可以直接添加 “信任”边。典型的可信关系脆弱点有Unix 操作系统的.rhost 文件。

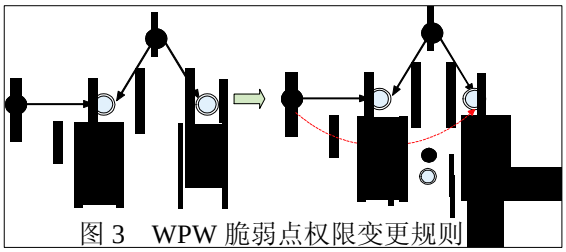
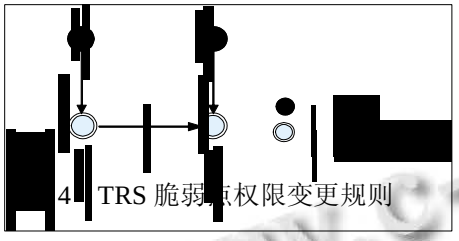


图 3　WPW 脆弱点权限变更规则



4　TRS 脆弱点权限变更规则

由上可知，脆弱点利用实为脆弱点权限变更规则应用在当前网络状态下的一个实例。

定义 7.　脆弱点利用 Vulnerability Exploitation。简称 Vexp，定义为三元组形式 Vexp = (G, CVRV, u_A)，CVRV 是应用在图 G 下的脆弱点权限变更规则，uA 对应于 CVRV 规则中的攻击主体。

3.3 权限变更规则实例

脆弱点利用会导致网络状态的变化，权限变更规则的利用反映了攻击者的攻击意图。现根据上述的规则举例进行简单说明。如下图 2-6 所示：

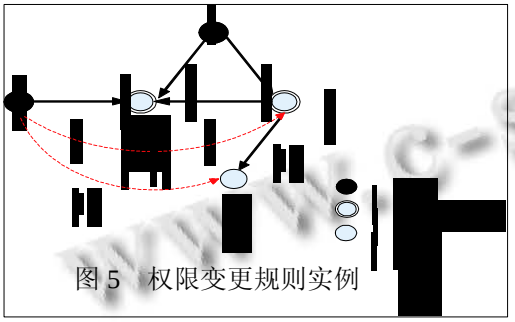


图 5　权限变更规则实例

可执行的权限变更规则是 take 规则和 BOF 规则，形式化表示如下：

$CVRV_{BOF}$ = (G_{pre}, M, v_A)，其中

G_{pre}=(V, R, L, A)

=({(A, B, P, c)}, {(A, P, x)}, {(c, P, h), (c, B, h), (B, P, o)}, {(P, {BOF}) }),

M =(V, R{(A, B, t)}, L, v_A)

=(V, G’ , L, v_A)，其中 v_A = A

对 G’再次采用 take 规则，有

$TGRV_{take}$ = (G’ pre, M, v_A)，其中

G’ $_{pre}$=(V, R, L, A)

=({(A, B, File)}, {(A, B, t), (B, File, {r,w})}, ϕ , vA),

M =(V, R{(A, File, t)}, ϕ , v_A)，其中 vA = A

4　VRV模型分析算法

从单点脆弱性利用方式[14]出发进行算法的设计和分析。

函数 1.　权限获取路径算法 AcquireRightRoad (α , x, y, G_0)。对于权限 α 和攻击实体 x 和网络实体 y，有限的利用 take 规则和 CVRV 规则，使当前网络状态 G_0 经过多个状态 G_1, G_2, …, G_n 的转化，记为 $G_0 \rightarrow {}^*G_n$。在最终状态 G_n 中存在从 x 到 y 访问权限为 α 的边，称$^*G_n$ 为权限变更图的闭包，$^*G_n$ 包括了从 x 到 y 的所有脆弱点利用成功的路径。

函数 2.　权限变更闭包图获取算法 GetComplete Graph(G_0)。获取，$^*G_n$ 是攻击者利用网络配置信息和脆弱点对网络发动攻击的所有可能路径，表示为权限变更图的闭包$^*G_n$。影响脆弱点权限变更分析算法的规则有 take 规则和 CVRV 规则，分别用$^*G^{take}$，$^*G^{CVRV}$ 表示采用 take 规则后的闭包图和采用 CVRV 规则后的闭包图。

算法说明如下。

算法 3.1.　AcquireRightRoad (α , x, y, G_0)

输入：初始脆弱性权限变更图 VRV_0，用 G_0 表示

输出：x 到 y 获取权限为 α 的权限变更路径 r_R。

(1)　$^*G_n \leftarrow$ GetCompleteGraph (G0)

(2)　遍历$^*VRV_n$所有的权限变更路径

(3)　　$W_R \leftarrow$ x 到 y 的可达路径

(4)　　for all w_R

(5)　　if　$x \xrightarrow{\alpha} y$

(6)　　标识并输出该路径 r_R

算法 3.2.　GetCompleteGraph (G_0)

输入：　G_0

输出：　$^*G_n$

(1)　F $\leftarrow$ all order pair (e, r) in (E, R) //E 是所有标识为 t 权限的边，R 为对应 E 的权限集合

(2)　While(!IsEmpty(F))　// 执行 take 规则

(3)　While(!IsEmpty(F))

(4)　(e, r) = head(F)

(5) take-rule available for e

//满足 take 规则的所有前置条件图 G_{pre}

(6) apply take-rule toG, generate new order pair(e', r'), add (e', r') to F

(7) Delete(e, r) //删除原来的边及权限序列对

(8) for all rule∈CVRV // 执行 CVRV 规则

(9) for all G_{pre} in G_i

// G_i 为第 i 遍循环后所得图

(10) Vexp = (G, CVRV, u_A), generate new order pair(e', r'),add (e', r') to F

(11) goto(2)

下面对算法 3.2 的正确性进行证明。

定理 1. 算法 3.2 能够利用 take 规则及 CVRV 规则分别成功构造$*G^{take}$和$*G^{CVRV}$。

证明:首先证明算法中(2)—(7)中 take 规则的应用:闭包图上新增的边及权限全部由算法生成。用序列表 S 表示算法采用的 take 规则顺序, $S=\{(T_1,R_1), (T_2,R_2), \cdots (T_n, R_n)\}$, R 为对应 take 规则所获取的权限。假设 S 出现不经过算法生成而存在权限 R_i, i=1,2,…n,对其首例(T_i,R_i),已知 T_i 的基本权限 t_i 由 $T_1, T_2, \cdots$ 或 T_{i-1} 应用所生成(否则为原图存在的权限),如此一来,T_i 的基本权限 t_i 已经被规则生成并添加到 F,t_i 作为新规则基本权限而被采用,再一次生成权限 R_i,与原假设矛盾,原命题得证。同时算法中(6)保证了 F 中不会产生重复的边和权限。

现针对 CVRV 规则进行证明。算法中(8)—(12)考虑满足条件的所有的 CVRV 规则,把新增的权限添加到 F 中。每一遍算法的运行对于存在脆弱点的结点只检索一次,对于可行的 CVRV 规则也只运行一遍,并在 VRV 图中产生权限为 t 的边,边的添加不会产生 CVRV 规则的前置条件图,因为标识为 t 的权限边并不作为前置条件的一部分。证毕。

定理 2. 算法 3.2 得到权限变更规则的闭包图*Gn 在多项式时间内完成。

证明:现令 n 为图 G 的结点数,令 m 为脆弱点的最大数量,k 为 CVRV 规则前置条件图 G_{pre} 最大结点数。首先计算外循环的时间复杂度。因为攻击者 uA 只参与一次脆弱点利用,即 Vexp = (G, CVRV, u_A),就可以通过 CVRV 规则在图 G 完成脆弱点利用,最坏情况下,每次外循环产生的闭包图中只有一条规则可行时,不超过 $nC_{n-1}^{k-1}(k-1)!m$ 时间就可以完成所有可行的权限变更规则,此时(8)—(12)的运行不再对闭包图产生任何改变。

现来考虑算法的两个内循环的时间复杂度。(2)—(7)考察序列表 F 使用满足前置条件的 take 规则, F 中有序对数目最多为 $O(n^2)$,而执行(5)的时间复杂度为 $O(n)$,执行(6)时,只需在构建的模型图检索相连的边,时间复杂度为 $O(1)$,故算法中第一个内循环的时间复杂度为 $O(n^3)$;考虑到脆弱点数量 m 和应用了权限变更规则图结点数 k 均为常数,第二个内循环(8)-(12)的时间复杂度为 $O(n^k)$。综上,算法的时间复杂度为 $O(n^k(n^k+n^3))$,化简为 $O(n^{2k}+n^{k+3})$。证毕。

5 实例分析

通过构造一个典型的脆弱性网络环境,利用本文所提出的脆弱点权限变更模型 VRVM 进行实例说明。

图 6 展示了一个本地网络拓扑结构,网络信息描述如下:攻击者以远程方式入侵网络,代理服务器 Agent 允许 Devil 用户访问 web 和 mail 服务,Agent 以 PowerUser 和 Root 权限身份利用 HTTP 和 SMTP 服务监听所有相连端口;在文件服务器 FileServer 上,root 角色运行着 SSH 和 RPC 服务;Danny 主机上 root 运行着 SMB 服务。同时 Danny 主机上的 SMB 服务及 Agent 上的 HTTP 有 BOF 脆弱点,FileServer 上的 root 用户有 WPW 脆弱点;root 用户是 Danny 主机上 Adam 用户的信任成员。

现假设 Devil 想访问 Danny 上的 File 文件,利用算法 3.1 得到攻击者 Devil 的权限变更闭包图,如果该闭包图中包含从 Devil 到 File 的权限变更路径,那么 Devil 就能达到目标。以上的攻击场景及结果展示如图 7 和图 8。

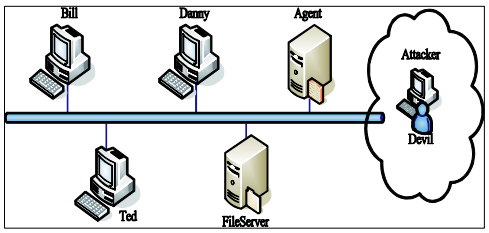


图 6 网络实例的拓扑图

分析可得,Devil 可以利用了 Agent 上的 BOF 脆弱点而获取 SuperUser 用户的访问权限,由于 Super User 用户能访问 FileServer 上的 SSH 服务,Devil 用户利用 root 用户上的 WPW 脆弱点破解管理员密码,当

成功获取密码时就可以通过信任关系获取 Adam 的访问权限，最终 Devil 用户成功入侵 Danny 主机的 File 文件，对其进行读写操作。

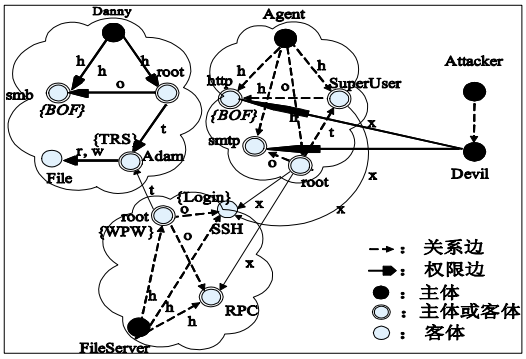


图 7　网络实例的部分 VRE 模型图

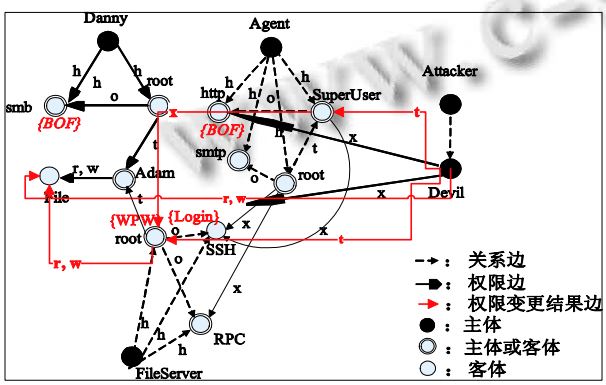


图 8　攻击者 Devil 的部分权限变更路径

6　结语

本文通过研究网络脆弱点的机理，提出了一种新型的基于权限变更规则的网络脆弱性分析方法。对常见的网络脆弱点进行统一建模，得到脆弱点权限变更规则；通过收集网络脆弱点信息和配置信息进行权限变更模型的构建；设计权限获取路径算法求得权限变更路径的闭包图，进一步得到攻击者的权限获取路径。我们可以对闭包图或权限获取路径作进一步挖掘，获取更多有效的网络安全信息，如求概率最高的权限变更路径，难度最低的权限获取路径等，为网络脆弱性的研究提供更多的参考价值。

参考文献

1 Hamid R. S, Rasoool Jalili. Vulnerability Take Grant(VTG): An efficient approach to analyze network vulnerabilities. Computers & Security, 2007,26:349–360.

2 Gerhard Eschelbeck. The Laws of Vulnerabilities: Which security vulnerabilities really matter. Information Security Technical Report, 2005,10(4):213–219.

3 Hai L. Vu, Kenneth K. Khaw,TY Chen,Fei-Ching Kuo. A New Approach for Network Vulnerability Analysis. IEEE Conf. on Local and Computer Networks(LCN). 2008:387– 394.

4 Igor Mishkovskia, Mario Bieya, Ljupco Kocarevb,c. Vulnerability of Complex Networks. Commun Nonlinear Sci Numer Simulat, 2011,16:341–349.

5 Yeu-Pong Lai, Po-Lun Hsia. Using the Vulnerability Information of Computer Systems. Computer Communications, 2007,30:2032–2047.

6 Anshu Tripathi, Umesh Kumar Singh. Towards Standardization of Vulnerability Taxonomy. 2010 2nd International Conference on Computer Technology and Development (lCCTD 2010). 2010:379–384.

7 Shuguang Huang, Heping Tang, Min Zhang, Jie Tian. Text Clustering on National Vulnerability Database. 2010 Second International Conference on Computer Engineering and Applications, 2010:295–299.

8 David Brumley, Umesh Kumar Singh. Towards Automatic Generation of Vulnerability-Based Signatures. Proc. of the 2006 IEEE Symposium on Security and Privacy, 2006.

9 Cynthia P, Laura PS. A Graph-based System for Network-Vulnerability Analysis. Proc. of the New Security Paradigms Workshop, Charlottesville, VA, 1998,71–79.

10 Erik Jenelius,Tom Petersen, Lars-Go¨ran Mattsson. Importance and Exposure in Road Network Vulnerability Analysis. Transportation Research Part A 40, 2006:537–560.

11 Xiangrong Wang, Hang Shi, Tze-Yau William Huang, Frank C. Lin. Integrated Software Vulnerability and Security Functionality Assessment. 18th IEEE International Symposium on Software Reliability Engineering, 2007:103–108.

12 Ritchey RW, Ammann P. Using Model Checking to Analyze Network Vulnerabilities. Proc. of the IEEE Sympo- sium on Security and Privacy. 2000.156–165.

13 Messaoud Benantar. The Take-Grant Protection Model. Access Control Systems, 2006.168–179.

14 王玉龙,杨放春.一种新型的脆弱性评估方法及其在 IMS 中应用的研究[博士学位论文].北京邮电大学,2009.

15 刘炜,杨武.网络系统脆弱性评估与分析技术研究[硕士学学位论文].哈尔滨工程大学,2009.