基于智能化状态转移以及权限改进的攻击图构建方法

马彦图 王联国
(甘肃农业大学信息科学技术学院 兰州 730070)

摘 要 针对当前攻击图在大范围网络应用中具有时间复杂度以及图形化描述不准确等缺陷,提出了一种基于智能化状态转移以及权限改进的攻击图构建方法:采用智能化状态转移途径构建攻击模型,依据该模型规划相应的攻击图,并在攻击图生成中引入了权限改进体制,该方法以主机间的连接分析为依据,根据网络攻击状态图中不同主机的原始权限,获取攻击权限的改进路径,能够针对网络变换情况调整主机的权限,进而确保相应网络的安全性,针对大规模复杂化网络攻击问题构建有效的攻击图,以确保整体网络的安全性和高效性。通过最终的仿真实验可得,该方法构建网络攻击图的时间较短,具备较低的时间复杂度和较高的扩展性,是一种高效的攻击图构建方法。

关键词 攻击图,网络安全,智能化状态转移,权限改进
中图法分类号 TP311 **文献标识码** A

Attack Graph Construction Method Based on Intelligent State Transition and Permission Improvement

MA Yan-tu WANG Lian-guo
(College of Information Science and Technology, Gansu Agricultural University, Lanzhou 730070, China)

Abstract In view of the current attack graph in a wide range of network applications with time complexity and not accurate graphical description, this paper put forward a attack graph construction method based on intelligent state transition as well as permission improvement, which adopts the intelligent state transition way to build attack model, based on the model of planning the corresponding attack graph generation algorithm, and introduces the permissions in the attack graph generation algorithm improvement system. The method based on host connections between analysis, based on network attack state graph and network of different host original permissions, access permissions attack improvement path, can adjust the host network transformation condition in the permissions, then ensure network security, corresponding to large-scale complicated network attacks effectively attack graph, to ensure the overall network security and high-efficiency. By the final simulation experiment, this method can decrease consumption of system CPU time to complete the construction of network attack graph, has lower time complexity and high scalability, is a highly efficient attack graph method.

Keywords Attack graph, Network security, Intelligent state transition, Permission improvement

1 引言

网络攻击是一个攻击者按照攻击条件以及目标,依据一定的规律进行信息采集以及权限提升的过程,相应的过程中,攻击效果同攻击者的性能、经验以及相关的环境具有一定的关联性。面向网络攻击方法进行模型描述的主要途径包括:描述语言、攻击树以及攻击图等。其中,攻击图[1]是一种重要的网络安全分析和评估工具,其广泛应用于网络安全规划、网络安全和漏洞控制、入侵检测系统以及入侵响应等领域。网络攻击图[2,3]不仅可用于普通的互联网络,还能够应用于无线网路、工业控制网络以及电力网络,具有较高的应用价值。当前,国外发达国家重视研究网络攻击图的构建方法,并投入了大量的科研力量,获取了较多的方法,如 Qu 分析的依据 Prolog 逻辑的模型构造算法——MulVAL 系统、Steven Noel 等分析出的依据 EDG 模型的 TVA 系统-sl 等。这些攻击图构建方法虽然能够针对相应的网络环境构建攻击图,但是存在一定的缺陷:(1)实际的应用过程中,网络管理员应了解攻击者可能采取的入侵路径,并且还应掌握可能受到攻击的主机情况,但是传统的网络攻击图构建方法通常只对单一的攻击目标进行分析,无法对多种目标进行准确的分析。(2)传统的攻击图构建方法[4-6]在构建攻击图时具有复杂度高、扩展性能弱、运算时间长、对使用者技能要求高等缺陷,使得产生攻击图的过程中消耗了大量的系统资源,不能对大规模复杂网络系统的网络攻击现象进行有效的分析,具有一定的局限性。

因而提高攻击图的扩展性、运行效率成为相关学者分析的重点问题。本文为了准确预测攻击者可能采用的攻击路径,提出了一种基于智能化状态转移以及权限改进的攻击图构建方法,力图解决这一问题。

到稿日期:2012-12-03 返修日期:2013-01-27 本文受国家自然科学基金 2011(61063028)资助。
马彦图(1979-),男,硕士,主要研究方向为计算机网络与安全技术、物联网技术、软件工程,E-mail:mayt@gsau.edu.cn;王联国(1968-),男,博士,教授,硕士生导师,主要研究方向为网络技术、智能信息处理。

2 基于智能化状态转移的网络攻击模型

模型的作用是将一次成功的网络攻击行为转换成网络状态的变化情况，设计出基于智能化状态转移的网络攻击模型，进而获取描述网络攻击路径的攻击图，详细的模型用图 1 描述。

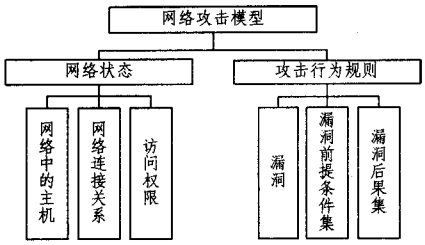

图 1 基于智能化状态转移的网络攻击模型

网络攻击模型包括网络状态以及攻击行为标准两个特征，本文构建的模型中的网络状态用 $ss(\{P\},\{Q\},\{(h_i,p_j)\})$ 描述。其中{P}用于描述主机集，网络中的主机是网络中的基层因素，用四元组 $P=$(hostid, os, svcs, vuls)描述。hostid 用于标识网络中的主机，通常采用 IP 地址进行描述；os 用于描述操作系统和相关版本的信息；svcs 用于描述同主机相关的服务列表，通常用端口号进行描述；vuls 用于描述主机中的弱势列表，主要包括操作系统的弱点、主机中软件的弱点以及其它的误差信息。{Q}用于描述网络连接关系集，通常用三元组 $Q=$(src, dst, protocol)描述网络连接。src 用于描述源主机，dst 用于描述目标主机，protocol 用于描述主机间连接的协议以及端口。如果二者间相互独立，则 protocol 是空集，如果二者是相同的主机，则 protocol={localhost}。$\{(h_i,p_j)\}$ 用于描述攻击者相对于网络中各主机的访问权限集，描述用户在主机 h_i 上的访问权限 p_j。

本文构建的智能化网络攻击模型将权限划分成 3 级：(1)系统关联员级 Root，其能够管理主机资源；(2)普通系统用户级 User，其开始于系统的初始阶段，并且通过系统管理员进行设置，用于独自管理的资源；(3)远程访问者级 Access，其能够访问网络服务，通过网络服务进行数据交流，并搜索相关的系统资源。该模型中的网络攻击行为规范标准采用四元组 $U=$(vul, preconditions, postconditions, cost)描述。可将攻击者的攻击行为看成是对弱点的一次应用，并且相应的结果能够增强相应的攻击行为以及网络连通关系的增加。vul 用于描述攻击采用的弱点，pre-conditions 用于描述使用该弱点的相关规范集，包括攻击者在攻击源主机上的最低访问权限、攻击者在目标主机上的最低访问权限、攻击源主机同目标主机间的连通标准。post-conditions 用于描述攻击行为产生的不良后果集，采用三元组(Rslt-access, Rslt-conn, Rslt-vuls)进行描述，其中 Rslt-acces 用于描述实施攻击后攻击者在主机上得到的访问权限，Rslt-conn 用于描述攻击后网络的连接关系的变化，Rslt-vuls 用于描述攻击后网络增加的弱点。cost 用于描述攻击行为消耗的代价，其包括攻击复杂度和攻击产生的几率。

3 基于权限改进的攻击图生成算法

网络攻击图通常用于描述网络中不同弱点的关联性，通过攻击图能够准确获取攻击者采用的攻击路径。攻击图中的节点用于描述攻击状态，节点主要指网络中的主机名称、用户权限以及攻击的影响等；攻击图中的各条边用于描述单一行为导致的网络状态改变。

本文分析的网络攻击图是入侵者依据相应的目标采取的攻击行为的集，也就是攻击事件关联图。攻击者采用相应的主机向网络中同其具有协议相关并且具有漏洞的主机发起攻击，如果攻击产生一定的效应，则攻击者会使用被攻击主机的访问权限，再次发动攻击，攻击行为特征是：

(1)具有单一性，攻击者在一台主机上的权限对后续的攻击行为无任何的干扰性。

(2)实际的攻击者可充分利用系统的一切漏洞发出攻击行为，并且攻击行为具有唯一性。

3.1 权限改进算法的描述

设置网络中存在一台主机到另一台主机间的权限使用关系，该种权限关系能够反映当前网络中性能上要求的主机间的信任访问，并且能够描述网络攻击产生的权限改进情况。本文主要按照主机间的连接分析网络主机间权限改进关系，具体的改进方法描述结构是 $Eacalation(WBS, KBS, U_{pre}, U_{post}, Q_{name}, Q)$。$WBS$ 用于描述权限改进的标识；KBS 用于描述改进相关的连接；对于网络攻击描述，U_{pre} 表示权限改进前攻击主机对目标主机的最低权限状态，U_{post} 表示改进权限后攻击主机对目标主机达到的最高权限，U_{name} 用于描述网络攻击行为，$Q=0$；U_{pre} 表示攻击主机达到相应信任的最低权限，U_{post} 表示攻击主机能够获取目标主机的最高权限，U_{post} 用于描述信任名，$Q=1$。

3.2 网络攻击状态图

设置一个连接为网络中任意两台主机间的连接关系，网络攻击行为都是依据连接关系进行的，网络中的权限改进过程也依据连接进行，本文用 Connection(KBS, AttackSrc, HostDst, K)描述连接结构，其中，KBS 用于描述连接标识，AttacSrc 表示攻击主机，HostDst 表示目标主机，K 用于描述状态值，用于分析攻击主机同目标主机的一致性，如果 $K=1$，表明攻击主机同目标主机是同一主机，否则 $K=0$，依据相应的网络连接关系可产生网络攻击状态图 A-K，算法如下。

算法 1 生成网络攻击状态图的算法

```
输入：主机间的连接状态 Connection
输出：网络连接状态结果并存入 A-K 中
过程：K=0;
    for(i=1;i<=size(Connection);i++)
    If Connection. K=0
    第 Connection. AttackSrc 行 i 列是-1;
    第 Connection. HostDst 行 i 列是 1;
    elseif Connection. K=1
    第 Connection. AttackSrc 行 i 列是 2
    end
```

3.3 构建网络攻击图

全局网络攻击图 Z 是有向无圈图，该图节点是主机名、用户权限以及攻击干扰，边是单一行为引起的网络状态改变的提升路径。网络攻击图的描述结构是：

$Z(RBS\_U_{pre} \rightarrow RBS\_U_{post})$

RBS_U_{pre} 用于描述 RBS 主机的 U_{pre} 状态，RBS_U_{post} 用于描述 RBS 主机的 U_{post} 状态，Z 表示两个主机间能够实现改进攻击路径的可行性。通过网络连通状态图和权限改进分析总

体网络的攻击图，具体的算法如下。

算法 2　构建总体网络攻击图的算法

输入：网络攻击状态图 H-c 网络中权限改进描述

输出：总体网络权限改进攻击图的过程：Z=0；

For every row in Q(t)

For every row in A-K(j)

If A-K(j,Q(i,2))>0 且 Escalation. Q=0

{A}={RBS 用于描述 i 的主机大于 Escalation. U_{pre}权限的状态集}

{B}={RBS 用于描述 i 的主机小于 Escalation. U_{post}权限的状态集}

Z 中用于描述集合 A 到集合 B 的权限改进攻击路径=1

elseif A-K(j,Q(i,2))<0 且 Escalation. Q

{C}={RBS 用于描述 i 的主机大于 Escalation. U_{pre}权限的状态集}

elseif A-K(j,Q(i,2))>0 且 Escalation. Q

{D}={RBS 用于描述 i 的主机小于 Escalation. U_{post}权限的状态集}

end

end

Z 中用于描述集合 C 到集合 D 的权限改进攻击路径=1

end

过滤图中的多余攻击路径

本文采用 SQL 数据库以及 C++确保攻击图生成算法的顺利运行。SQL 数据库具有简便性，能够保存大量的数据，并且搜索效率高，能够优化算法的性能。C++的模板库可以增强算法的运算效率，确保攻击图的完整性。上述分析的基于权限改进的攻击图生成算法的流程如图 2 所示。

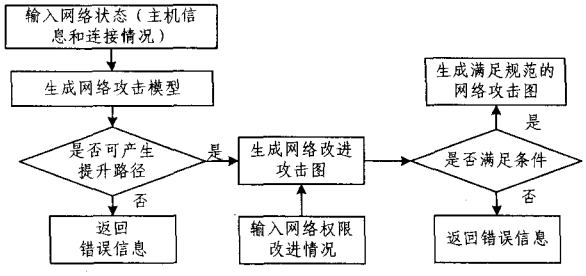

图 2　本文攻击图生成算法的流程

4　实验结果及分析

为了验证本文方法的有效性，应进行相应的实验。图 3 描述的是本文实验采用的网络拓扑图，该网络内子网的数量/各个子网内主机的数量和各台主机上的弱点数量的最大值都通过用户进行输入，并且主机上的弱点分布具有随机性。

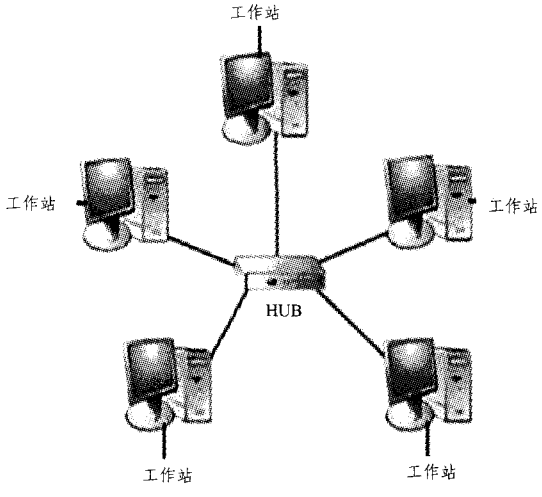

图 3　模拟网络的拓扑图

实验在 Linux 下采用 C 语言实现了本文设计的攻击图构建方法，从 CPU 耗时以及可扩展性两个方面验证本文方法的有效性和优越性，并对实验结果进行相应的分析。实验运行的环境是：服务器 Power Edge R710，操作系统 RetHat v5.4，内存 28G，CPU2.26GHz。

4.1　CPU 耗时实验

当前存在较多的攻击图构建方法，本文主要分析 Sheyner 和 Ou 攻击图构建方法，实验模拟了简单的目标网络，该网络中仅存在一个子网，网络中不存在防火墙器件，全部的主机间能够进行交流，各个主机中弱点数量不高于 5。实验分别使用 Sheyner、Xinming Ou 以及本文分析的攻击图构建算法，面向不同的网络规模构建相应的攻击图，3 种方法构建攻击图消耗的 CPU 时间用图 4 描述。

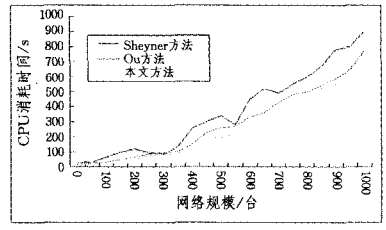

图 4　CPU 性能结果对比

分析图 4 可得，Sheyner 算法的时间复杂度较低，消耗的 CPU 时间会随着网络规模的扩大呈现大幅度的增加，本文分析的攻击图构建方法以及 Ou 方法消耗的 CPU 时间随着网络规模的扩大呈现小幅度的增加，具有较强的时间复杂度。并且本文方法的性能比 Ou 方法好，因为在实际的应用中，本文方法通过智能化状态变换方法以及权限改进体系完成对攻击行为的有效分析和处理，并且限制了网络攻击的步骤数，进而降低了攻击图消耗的 CPU 时间，极大提高了算法的运行效率。

4.2　可扩展性实验

本文实验模拟了具有复杂拓扑结构的目标网络，其中包含 10 个子网络，各子网络都采用防火墙进行安全防护，子网内主机间可进行信息交流，并且各主机中的脆弱点数应不高于 5 个。图 5 描述了本文方法在不同的网络规模下，构建攻击图消耗的 CPU 时间。分析图 5 可得，随着网络规模的不断增加，本文方法消耗的 CPU 时间也逐渐增加，但是增长的幅度满足相应的规范要求，并且当网络中主机的数量达到 1000 台时，网络构建攻击图的时间小于 11min，并且产生攻击图的时间是 22s。

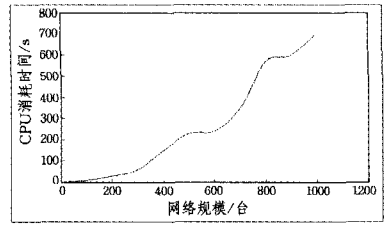

图 5　网络规模与 CPU 消耗时间关系曲线

分析上述实验结果可得，本文提出的攻击图构建方法具有较强的扩展性，能够对大规模复杂网络脆弱性进行综合性分析。主要是因为本文采用智能化状态变换方法分析相关的

（下转第 193 页）

能世界。文中指出可以通过区分各个实体的网络化特征将智能世界构建成相互关联的3个不同的子世界。其与统一地建模相比:①充分地考虑了不同类型实体的行为和连接特征,每个子世界由具有相同行为类型的实体和相同类型的连接构成,可以分别建立统一的推理机制;②各个子世界之间通过网络化连接进行通信,更有利于研究整个智能世界的通信安全问题;③可以通过将推理问题定位在某个(些)子世界的模型中,降低推理过程的复杂性;④抽象过程可以分别进行,并通过子世界之间的网络化连接进行各个抽象层之间的通信,降低抽象过程的复杂性。在未来,我们将继续对上面4部分内容进行扩展研究。

参 考 文 献

[1] The Internet of Things. Networked Objects and Smart Devices [R]. The hammersmith group research report. February 2010, http://thehammersmithgroup.com/images/reports/networked_objects.pdf

[2] Elson J, Estrin D. Sensor networks: a bridge to the physical world[M]. Wireless sensor networks. Kluwer Academic Publishers, Norwell, MA, 2004

[3] Barton J, Kindberg T. The Challenges and Opportunities of Integrating the Physical World and Networked Systems[R]. HPL Technical report HPL-2001-18. 2001

[4] Estrin D, Culler D, Pister D, et al. Connecting the Physical World with Pervasive Networks[J]. IEEE Pervasive Computing, 2000, 1(1): 59-69

[5] Joseph A D. Ubiquitous System Software[J]. IEEE Pervasive Computing, 2004, 3(3): 57-59

[6] Boone G. Reality Mining: Browsing Reality with Sensor Networks[OL]. Sensors Magazine Online. http://sensorsmag.com/articles/0904/14/main.shtml, 2004-09

[7] Coetzee L, Eksteen J. The Internet of Things-Promise for the Future? An Introduction[C]// IST-Africa 2011 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation. 2011

[8] 欧阳丹彤,姜云飞. 刻画基于模型的中心诊断[J]. 软件学报, 1999, 10(1): 74-77

[9] Reiter R. A Theory of diagnosis from first principles[J]. Artificial Intelligence, 1987, 32(1): 57-96

[10] 陈荣,姜云飞. 含约束的基于模型的诊断系统[J]. 计算机学报, 2001(2): 127-135

[11] 李占山,王涛,孙吉贵,等. 利用元件替换测试求诊断[J]. 软件学报, 2005, 16(9): 1599-1605

[12] Goldstone R, Barsalou L. Reuniting perception and conception [J]. Cognition, 1998, 65: 231-262

[13] Brooks R A. Elephants don't play chess [J]. Robot. Auton. Syst, 1990, 6: 3-15

[14] Choueiry B, Iwasaki Y, McIlraith S. Towards a practical theory for reformulation for reasoning about physical systems [Z]. Artif. Intell., 2003

[15] Mozetic I. Hierarchical model-based diagnosis[J]. Int J of Man-Machine Studies, 1991, 35(3): 329-362

[16] Chittaro L, Ranon R. Hierarchical model-based diagnosis based on structural abstraction[J]. Art. Intell, 2004, 155(1/2): 147-182

[17] Hou Ming-liang, Liu Yu-ran, Xing Shu-bin, et al. Study of Intelligent Diagnosis System for Photoelectric Tracking Devices Based on Multiple Knowledge Representation[J]. Advanced Materials Research, 2011(179/180): 602-607

[18] Chittaro L, Guida G, Tasso C, et al. Functional and teleological knowledge in the multimodeling approach for reasoning about physical system: a case study in diagnosis[J]. IEEE Trans. Syst. Man, Cybern., 1993, 23(6): 1718-1751

[19] 孙善武,王楠,欧阳丹彤. 广义KRA模型[J]. 吉林大学学报:理学版, 2009, 47(3): 537-542

[20] Barton J, Kindberg T. The Challenges and Opportunities of Integrating the Physical World and Networked Systems[R]. HPL Technical report HPL-2001-18. 2001

[21] Bodhuin T, Canfora G, Preziosi R, et al. Hiding complexity and heterogeneity of the physical world in smart living environments [C]// Proceedings of the 2006 ACM Symposium on Applied Computing, 2006. New York, US, 2006: 1921-1927

[21] Kotiadis K, Robinson S. Conceptual Modelling: Knowledge Acquisition and Model Abstraction[C]// Proceedings of the 2008 Winter Simulation Conference, 2008. 2008: 951-958

[22] Robinson S. Conceptual modelling for simulation part I: definition and requirements [J]. Journal of the Operational Research Society, 2008, 59(3): 278-290

(上接第158页)

网络环境,能够对大规模复杂网络的状态以及攻击行为进行准确的分析,构建合理的网络工具模型,并采用权限改进方法生成攻击图,最终实现对网络攻击行为的有效分析,为后续的处理工作提供可靠的依据。

结束语 本文提出了一种基于智能化状态转移以及权限改进的攻击图构建方法,即采用智能化状态转移途径构建攻击模型,依据该模型规划相应的攻击图生成算法,并在攻击图生成算法中引入权限改进体制,以对大规模复杂化网络攻击问题构建有效的攻击图,确保整体网络的安全性和高效性。通过最终的仿真实验可得,本文方法能够消耗较低的系统CPU时间完成网络攻击图的构建,具备较低的时间复杂度和较高的扩展性,是一种高效的攻击图构建方法。

参 考 文 献

[1] 王国玉,王会梅,陈志杰,等. 基于攻击图的计算机网络攻击建模方法[J]. 国防科技大学学报, 2009, 31(4): 74-80

[2] 陈春霞,黄皓. 攻击模型的分析与研究[J]. 计算机应用研究, 2005, 22(7): 115-118

[3] 司加全,张冰,尚大鹏,等. 基于攻击图的网络安全性能增强策略制定方法[J]. 通信学报, 2009, 30(2): 123-128

[4] 冯萍慧,连一峰,戴英侠,等. 面向网络系统的脆弱性利用成本估算模型[J]. 计算机学报, 2006, 8(29): 1375-382

[5] 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

[6] 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

[7] 黄志宏,巫莉莉,张波. 基于云计算的网络安全威胁及防范[J]. 重庆理工大学学报:自然科学版, 2012, 26(8): 85-90