攻击图技术研究进展

陈 锋[1,2] 毛捍东[1] 张维明[2] 雷长海[1]
(第二军医大学网络信息中心 上海 200433)[1] (国防科学技术大学信息系统与管理学院 长沙 410073)[2]

摘 要 目前网络攻击技术逐步多样化和智能化,攻击者对目标网络内存在的脆弱性会采取多步骤的组合攻击方式进行逐步渗透。攻击图是一种新型的网络脆弱性分析技术,它在对目标网络和攻击者建模的基础上,根据二者之间的相互作用关系计算产生攻击图,展示攻击者利用目标网络脆弱性实施网络攻击的各种可能攻击路径。该技术能够自动发现未知的系统脆弱性以及脆弱性之间的关系,因此是目前研究的热点之一。攻击图技术经历了从面向小型网络的手工分析到自动分析的发展,目前正在向面向大规模网络的自动分析发展。总结了攻击图技术的发展现状,阐述了它的巨大应用前景,最后分析了该技术目前所面临的主要挑战。

关键词 脆弱性分析,攻击图,网络建模,攻击者建模
中图法分类号 TP393.08 **文献标识码** A

Survey of Attack Graph Technique

CHEN Feng[1,2] MAO Han-dong[1] ZHANG Wei-ming[2] LEI Chang-hai[1]
(Network Information Center, The Second Military Medical University, Shanghai 200433, China)[1]
(School of Information System and Management, National University of Defense Technology, Changsha 410073, China)[2]

Abstract The network attack techniques are being more diversified, and intelligent, an attacker can often infiltrate a seemingly well-guarded network system using multi-step attacks by exploiting sequences of related vulnerabilities. As the novel vulnerability assessment technique, the attack graph technique analyzes the interaction between the target network and the attacker through the models of these two agents, generates attack graph to show possible attack paths. Because this technology has the capacity to automatically discover the unknown system vulnerabilities and the relationship between vulnerabilities, it is currently a hot subject of research. The attack graph technique has experienced the stage of manual analysis and the stage of the automatic analysis of small-scale network, and is currently in the way of the automatic analysis of large-scale network. In this paper, the development of attack graph technique was summarized and challenges arising from the current research were discussed and some suggestions for the future research work were put forward.

Keywords Vulnerability assessment, Attack graphs, Modeling networks, Modeling attackers

1 引言

近年来,企业网络的安全性受到了越来越多人的关注。众所周知,网络中存在的脆弱性是导致网络安全事件发生的根本原因之一。随着网络攻击技术逐步多样化和智能化,攻击者在实施网络非法活动时会针对其存在的脆弱性采取多步骤的组合攻击方式进行逐步渗透。虽然有诸多成熟的脆弱性扫描工具如 Nessus[1]、X-scan[2]等,能够自动发现目标网络中已知的脆弱性,但是这些工具孤立地研究各个脆弱性,不能分析它们之间的相互作用关系和由此产生的潜在威胁。攻击图技术把研究对象抽象为两个目标主体:目标网络和攻击者。它认为目标网络和攻击者之间存在博弈的关系,即目标网络努力保持自己在正常的状态空间转化,而攻击者总是试图使目标网络向"不期望"的状态转化。它首先以面向攻击的方式分别对目标网络建模和攻击者建模,然后根据二者之间的相互作用关系产生攻击图。由于该技术能够自动发现未知的系统脆弱性以及脆弱性之间的关系,从攻击的角度展示了攻击者利用网络内存在的脆弱性进行逐步入侵的过程,因此它作为一种新的脆弱性分析技术正成为越来越多研究者关注的焦点之一。

对于攻击图技术,目前研究者的研究内容主要包括3个部分:目标模型构建、攻击图构建和攻击图分析。目标模型构建研究主要着眼于以面向攻击方式对目标网络和攻击者建立科学合理的模型,它正经历从手工建模到自动建模的发展过程。攻击图构建研究主要着眼于根据目标网络和攻击者模型构建攻击图,展示攻击者可能的入侵过程,它经历了从面向小

到稿日期:2010-12-02 返修日期:2010-03-08 本文受国家自然科学基金(912024006)资助。
陈 锋(1979—),男,博士,讲师,主要研究方向为网络与信息安全、密码学,E-mail:chenfeng@nudt.edu.cn;毛捍东(1980—),男,博士,讲师,主要研究方向为安全评估、内网安全;张维明(1963—),男,博士,教授,博士生导师,主要研究方向为信息安全、信息决策;雷长海(1974—),男,博士,副教授,主要研究方向为信息安全、医学图像处理。

型网络手工构建攻击图发展到自动构建攻击图，目前正在向面向大规模网络自动构建攻击图发展。攻击图分析研究主要着眼于基于攻击图来分析和解决目标网络面临的安全问题，目前它在网络安全定量评估、网络安全弥补措施分析以及IDS预警关联分析等多个不同安全问题中逐渐展开，取得了很好的效果，展示了其强大的应用前景，从而进一步有力推动了攻击图技术的发展。

2 攻击图技术研究进展

目前企业网络规模越来越大，网络攻击技术日新月异，导致企业网络中存在的脆弱性间关系也日趋复杂。攻击图技术的研究者期望该技术能够实现对大规模企业网络中脆弱性之间的复杂关系进行自动化分析。这对攻击图技术所涉及的主要研究内容，即目标模型构建、攻击图构建和攻击图分析，提出了巨大挑战。为了实现该目标，研究者对上述研究内容所涉及的5个主要关键点展开了深入的研究，见图1。

图1 攻击图技术研究中的主要关键点

在目标模型构建研究中，目标网络建模研究关注如何从攻击的角度对复杂目标网络进行合理抽象建模和自动从该网络中收集该模型的具体参数；攻击者建模研究，主要研究如何对攻击者攻击能力建模以及选取或设计有效语言描述该模型。

在攻击图构建研究中，攻击图构建算法研究的焦点在于其算法的可扩展性，即针对不同规模的目标网络和攻击者模型能够自动快速构建攻击图。由于大规模企业网络所对应的攻击图所包含的节点和边数目庞大，关系结构复杂，故研究者对攻击图的数据结构进行了研究，希望能够采取更加有效的图结构来简洁和直观地展示攻击者逐步利用各脆弱性进行网络组合攻击的过程。

攻击图分析研究主要着眼于基于攻击图来分析和解决目标网络面临的安全问题，目前它在网络安全定量评估、网络安全弥补措施分析以及IDS预警关联分析等多个不同安全问题中逐渐展开。

下面分别就其各关键点的研究进展进行介绍。

2.1 目标模型构建研究

目标模型构建涉及对目标网络建模和对攻击者的网络攻击能力建模，对它们的研究正经历从手工建模到自动建模的发展过程。

2.1.1 目标网络建模研究

在早期的攻击图技术研究中，有的目标网络模型引入了过多的元素，导致模型过于复杂，从而使攻击图构建困难且只能手工产生[4,5]；有的模型过于简单，不能表现一些复杂的网络攻击行为[6]。为此，Sheyner在深入研究后首次提出了以五元组$\langle H,C,T,I,ids\rangle$来描述目标网络[3,8]：

对于网络中的任何一台主机，$h\in H$是一个四元组$\langle id, svcs, sw, vuls\rangle$，其中

id：主机的唯一标识，如网络地址；

$svcs$：主机上运行的网络应用服务名和对应的侦听端口列表；

sw：其他软件列表，包括操作系统的类型和版本；

$vuls$：主机上存在的脆弱性，包括软件脆弱性、错误配置脆弱性等；

$C\subseteq H\times H\times P$表示主机之间的可达关系，如$C(h_1,h_2,p)$表示主机$h_1$通过端口$p$可达$h_2$，这里隐含了防火墙的信息；

$T\subseteq H\times H$表示主机之间的信任关系，如$T(h_1,h_2)$表示主机h_1可以无需授权可以直接远程登入h_2；

I表示攻击者对目标网络的初始能力，包含的信息主要有攻击者所知道的一些主机上的用户名和密码，以及他在各个主机上的访问权限等；

ids表示入侵检测系统模型，描述入侵检测系统可以发现哪些行为。

该模型对目标网络进行了合理的抽象且支持自动构建攻击图，诸多研究者采用了该模型[9,13-16]，或者在该模型的基础上进行了改进[10-12]。如Ritchey等人扩展了主机的连接模型，他们将主机连接性按照TCP/IP栈的多层结构细分成网络层、传输层、应用层的连接性。这样，该模型可以描述原模型无法描述的网络攻击行为[11]。

为了支持网络建模过程自动化，从目标网络中自动地获取其网络模型参数显得尤为重要。在MIT的原型系统TVA[26]中，目标网络中的脆弱性通过成熟的扫描工具Nessuss[1]获得。但是，由于网络中存在防火墙的限制，自动扫描工具无法获得完整的脆弱性信息。为此，Ou等人开发了MulVAL scanner，它作为代理程序在各个主机上并行运行，负责自动收集主机运行的软件和服务等相关信息[15,16]。该代理程序与扫描工具都只能获得由软件缺陷引起的脆弱性，很难获得其他类型的脆弱性，如软件配置错误引起的脆弱性。

在研究网络建模过程自动化中，自动获取网络中主机间的可达关系信息是至关重要的网络参数。由于复杂的网络拓扑结构和各种防火墙的限制为该信息的自动获得产生了很大困难，大多数方法研究都假设这些信息已经获得。Lippmann等人在原型系统NetSPA中对该问题进行了有意义的探索[17]，首次采取了可达矩阵来描述网络的拓扑、路由以及防火墙的过滤策略。对于大规模网络，可达矩阵中包含了大量的可达信息，他们又提出了两种压缩技术，从而大大减少了从可达矩阵中提取网络可达信息的计算量。

2.1.2 攻击者建模研究

对攻击者的建模主要是对其攻击能力的建模，一般采取规则库来描述其能力，本文将之称为攻击模板知识库。每个攻击模板一般与单个脆弱性关联且由两部分构成，即该脆弱性被攻击者成功利用实施攻击的前提条件和攻击者成功实施攻击后产生的后果。

根据网络脆弱性的分类，常见的攻击模板可以分为针对软件缺陷类脆弱性的攻击模板（例如远程内存溢出攻击模板[15]，见图1）和针对网络配置错误类脆弱性的攻击模板（例如关于.rhosts的攻击模板[3]，见图2）。研究者在不断的深入研究中发现，虽然攻击者的攻击行为主要是针对网络中的脆弱性的，但是攻击者可能在入侵目标网络后利用正常的网络访问行为继续扩大自身的攻击能力，如利用目标主机上的sshd服务进行远程登入控制主机，该行为本身是正常的网络

访问行为，但由于它可以被攻击者利用，因此研究者也将之归结为攻击模板[3,8]。

在早期研究中，研究者采用自然语言描述攻击模板，见文献[4]。自然语言描述虽然具有很强的描述能力，但是具有很大的不准确性，不支持攻击图自动构建。为此，研究者提出了多种形式化语言来描述攻击模板。例如，为了使用模型检测技术自动构建攻击图，Jha 等使用谓词逻辑创建了攻击模板[3,8,14]。对于知识库中的攻击模版，他们以 4 要素分别对其进行描述：攻击者所需前提条件、网络所需前提条件、对攻击者的影响、对网络的影响。图 2 是关于. rhosts 的攻击模板的描述[3]。同样地，为了能够使用推理机自动创建攻击图，Ou 等人采用了 Horn 逻辑描述攻击模板[15]。图 1 是对远程溢出攻击模板的描述。它的含义是如果主机 Host 上网络程序 Program 包含可被远程内存溢出提升权限的脆弱性 VulID，它在侦听 Protocol 和 Port，并且攻击者可以通过网络访问该进程，那么攻击者可以在主机 Host 上以 Priv 权限运行任意程序。需要注意的是，使用 Horn 语言描述的攻击模板，其后果只有一个：当攻击模板有多个后果时，需要把它拆分成多个等价的单后果攻击模板。

```
execCode(Attacker,Host,Priv) :-
  vulExists(Host,VulID,Program),
  vulProperty(VulID,remoteExploit,
  privEscalation),
  networkService(Host,Program,
  Protocol,Port,Priv),
  netAccess(Attacker,Host,Protocol,Port),
  malicious(Attacker).
```

图 1　Horn 语言描述远程内存溢出攻击模板

```
attack ftp. rhosts is
  intruder preconditions
    Plvl_A(S)≥user/ * 在源主机 S 上有 user 访问权 * /
  network preconditions
    ftp_T/ * 在目标机 T 上运行 ftp * /
    C(S,T,fp) / * 源主机 S 通过端口 fp 访问目标机 T * /
    wdir_T/ * ftp 用户在主机 T 上有合法的 shell * /
    ∃X. ¬RshTrust(X,T) / * T 和所有主机不存在 Rsh 信任 * /
  intruder effects
    none
  network effects
    ∃X. RshTrust(X,T)/ * 所有主机都和 T 有 Rsh 信任 * /
End
```

图 2　谓词逻辑语言描述关于. rhosts 的攻击模板

此外研究者还尝试了使用描述逻辑[19]、JIGSAW[20]、LAMBDA[21]、CAML[22]等形式化语言描述攻击模板。它们虽然都具有很强的描述能力且对不同的攻击模板描述各有优势，但是由于描述语言复杂，并不利于攻击图的自动构建。

为了获取攻击模板，安全专家需要从攻击的角度分析各个脆弱性被利用的前提条件以及可能产生的后果。该过程复杂且非常耗时。为了减小该过程的难度，Li Wei 进行了比较深入的有意义的研究。首先他提出了一个较为通用的攻击模板模型[18]，该模型由 3 部分组成：脆弱性实体、前提集和结果集，详细描述见表 1。同时，他通过研究开放的脆弱性数据 CVE，认为其中每条脆弱性描述可以分成存在特征、利用特征和后果特征 3 部分，它们可以分别映射到攻击模板模型的 3 部分。这样为知识库的构建者提供了实际可操作的途径。

表 1　前提集和结果集的详细描述

条件	类别	
脆弱性实体	操作系统	名字
		版本
		体系构架
		内核
	应用程序	名字
		版本
前提集	访问要求	源访问权限
		目标访问权限
	网络连接协议要求	
	脆弱性复杂度	
	附加	开放端口
		运行程序
		其他
后果集	CIA 属性	机密性
		完整性
		可用性
	网络连通关系	
	权限提升	

研究者在研究中发现，攻击模板的描述是否准确、知识库收集的攻击模板是否完备，是准确构建攻击图的基础；但并不等于攻击模板的描述字段越丰富，就越有利于攻击图的构建。因为攻击模板描述依赖于目标网络模型的抽象程度，同时攻击模板的复杂度也会影响到攻击图自动构建算法的效率。

2.2　目标模型构建研究

攻击图构建根据目标网络和攻击者模型来构建攻击图，一般以图结构来展示攻击者利用目标网络脆弱性实施网络攻击的可能的攻击路径。对它的研究经历了从面向小型网络的手工构建攻击图向自动构建攻击图发展，目前正在向面向大规模网络的自动构建攻击图发展。

2.2.1　攻击图构建算法研究

早期的攻击图大多为手工构建，如 Swiler[4]方法。为了能够为大规模目标网络自动构建攻击图，研究者所提的方法可以归为两类：采取定制的搜索算法，即重新编写程序构建攻击图；另外一类是采用成熟工具和技术构建攻击图，如模型检测技术、逻辑推理、智能规划技术和关系数据库查询技术。

定制的搜索算法也可分为两类：前向搜索算法和后向搜索算法。前向搜索算法从攻击者的初始能力出发，寻找攻击者所有可以使用的原子攻击，直到不能继续攻击为止。研究者发现攻击者一般的攻击步骤不会超过一定数目，因此前向搜索算法可以通过宽度优先搜索策略产生一种部分攻击图，它只包括小于给定攻击步骤数的可达攻击目标和攻击路径[10]。后向搜索算法是从攻击目标向攻击者初始能力反向搜索可达路径。这种搜索算法的主要优点在于与攻击目标无关的攻击模板不会被搜索，从而可以节省搜索空间。但是该类算法在运行前需要指定攻击目标，一般来说，该攻击目标是安全管理员所关注的保障其不被攻击者破坏的网络的安全属性。

从构建算法的输入看，攻击图构建算法可以分为单目标构建算法和多目标构建算法。单目标构建算法需要指定一个假设的攻击目标作为输入，产生的攻击图只包含从攻击者初始攻击能力出发到达该目标的所有攻击路径；多目标构建算法不需要指定攻击目标，产生的攻击图包含了从攻击者初始

攻击能力出发可以到达的所有攻击目标以及对应的所有攻击路径。

从构建算法的输出看，这些方法可以分为完全攻击图构建算法和部分攻击图构建算法。完全攻击图构建算法产生的攻击图包含了从攻击者初始攻击能力出发可以到达的所有攻击目标以及对应的所有攻击路径；部分攻击图构建算法产生的攻击图仅包含与指定目标相关的攻击路径或者从攻击者初始攻击能力出发经过指定的攻击步骤数目可以到达的攻击目标和攻击路径。

根据分析攻击者和目标网络两个主体间的相互作用关系的方式不同，可以分为没有基于单调性假设的和基于单调性假设的攻击图构建算法。前者能够分析拒绝服务攻击，但需以全局状态分析两个主体间的相互作用关系，算法可扩展性较差；后者不能分析拒绝服务攻击，但通过分析两个主体属性变化的依赖关系来产生攻击图，算法可扩展性较好。

表 2 对各种典型攻击图构建算法进行了总结和比较，其中 N 为企业网络中主机的个数。从表中可以看出，目前 Ingols 算法可扩展性最好，其算法的时间复杂度与企业网络中主机个数 N 线性增长。但该算法的局限性在于其只是针对远程内存溢出攻击模板，不能适用于一般的攻击模板。虽然 Ou 算法的时间复杂度约为 $O(N^3)$，但该算法可应用于一般的攻击模板，具有一定的普适性。模拟实验表明，该方法可对具有 1 千台以上主机规模的目标网络自动构建攻击图。

表 2　攻击图构建方法比较

方法	完全/部分	可扩展性	定制/工具	单调性	目标数
Swiler[4]	部分	手工	定制	否	单
Ortalo[23]	部分	较差	定制	否	多
Ritchey[6]	部分	较差	模型检测	否	单
Sheyner[3,8,14]	部分	较差	模型检测	否	单
Ou[15,16]	部分	$<O(N^3)$	逻辑推理	是	单
Ammann[9]	完全	$>O(N^6)$	定制	是	多
Berry[11]	完全	$>O(N^6)$	定制	是	多
Jajodia[26]	完全	$>O(N^6)$	定制	是	多
Feng[10]	部分	—	定制	是	多
Lingyu[7]	部分	较好	关系查询	否	单
Somak[24]	部分	较差	智能规划	否	单
Ingols[25]	完全	O(N)	定制	是	多

2.2.2　攻击图数据结构研究

研究者在对大规模企业网络构建攻击图时发现，其所对应的攻击图不仅包含的节点和边数目庞大，而且关系结构复杂，对理解和分析攻击图造成了非常大的困难。为了简洁和直观地展示攻击者逐步利用各脆弱点进行网络组合攻击的过程，研究者提出了多种攻击图的数据结构，本文将之总结为以下几种。

Sheyner 等在文献[3,8,14]中提出了一种攻击图，该攻击图的节点代表目标网络和攻击者的全局状态，节点内容通常包括主机名、用户权限、攻击的影响等。每条弧代表原子攻击，它被执行后将会引起全局状态的变迁，本文称该类攻击图为状态攻击图。状态攻击图需具有完整性，即攻击图包含所有的可以到达攻击目标的攻击路径；具有简洁性，即攻击图只包含到达攻击目标的状态。图 3 是一个状态攻击图的例子。为了便于理解，图中节点以原子攻击名称表示该原子攻击成功实施后的全局状态，其中虚线椭圆节点是初始状态节点。状态图是非常有效的攻击图数据结构，它显式地反映了攻击者所有的攻击轨迹，便于理解；但是并不是非常高效。原因在于状态节点代表系统全局状态，而网络模型是非常复杂的，这样在攻击图构建过程中需要遍历大量的与攻击无关的状态，影响了算法性能。并且显式的攻击路径描述造成攻击图节点数随主机数呈指数增长，不适用于大规模目标网络。

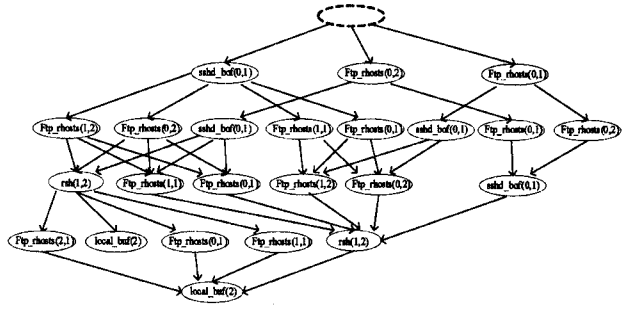

图 3　状态攻击图例子

Lingyu 等在文献[7]中提出了另外一种攻击图，它有两类节点：一类节点表示原子攻击；另一类节点为属性节点，它表示这些原子攻击的每个前提或后果，本文称该类攻击图为属性攻击图。原子攻击节点与属性节点间存在前提边和后果边。所有通过前提边与原子攻击节点相连的属性节点都满足时，该原子攻击才可被执行，从而使通过结果边与该原子攻击相连的属性都被满足。图 4 是属性攻击图例子，图中文字表示属性，椭圆表示原子攻击，它与图 3 的状态攻击图是同一个目标网络。通过比较可以发现，属性攻击图比状态攻击图更加简洁。属性攻击图隐式地反映了攻击者所有的攻击轨迹，便于分析攻击产生的原因，但是由于其攻击路径可能含圈，不便理解。

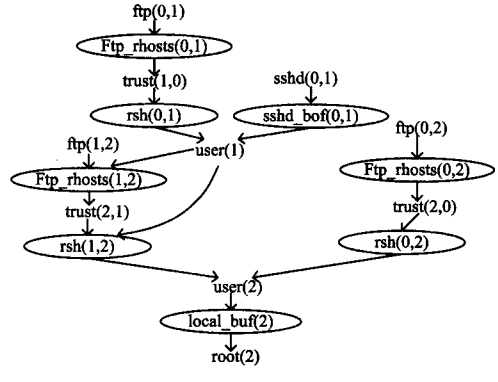

图 4　属性攻击图例子

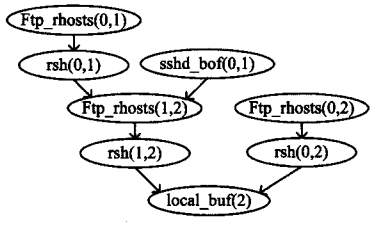

图 5　渗透依赖攻击图

Li wei 和 Ritchey 等在文献[11,18,41-43]中提出了一种只包含渗透节点的攻击图，它本质上是把属性攻击图中的所有属性转化为边，从而使该图中只包含原子攻击节点，它可以清晰地显示原子攻击（渗透）之间的依赖关系，本文称该类攻击图为渗透依赖攻击图。图 5 是图 3 属性攻击图例子对应的渗透依赖攻击图。但是，渗透依赖攻击图只是以“或”关系表示原子攻击之间的依赖关系，如图 5 中原子攻击 rsh(0,1)和

sshd_bof(0,1)是“或”关系，它不能表示原子攻击之间的“与”关系。如属性攻击图中原子攻击 τ_3 依赖于原子攻击 τ_1 和 τ_2 同时实施成功，则该属性攻击图无法转化为渗透依赖攻击图。因此渗透依赖攻击图存在局限性。

Ammann 在文献[9]中提出了一种只包含属性节点的攻击图，它本质上是把属性攻击图中的所有原子攻击转化为边，从而使该图中只包含属性节点，它可以清晰地显示目标网络在遭受攻击者实施原子攻击入侵后，其属性转换前后的依赖关系，本文称该类攻击图为属性依赖攻击图。图 6 是图 4 属性攻击图例子对应的属性依赖攻击图。

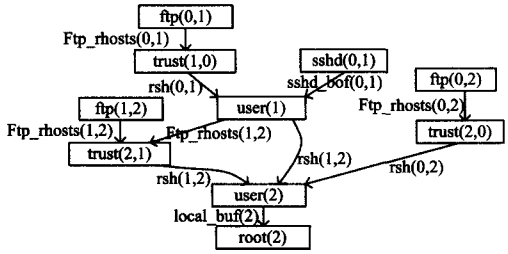

图 6　属性依赖攻击图

Ou 在文献[15,16]中了提出了逻辑攻击图。它包含推导规则、推导事实和原始事实 3 类节点。推导事实由推导规则根据已获取的推导事实和原始事实产生，且推导规则表示原子攻击。图 7 是逻辑攻击图的例子。图中，空心圆圈表示推导事实节点，方框表示推导规则节点，实心黑圈表示原始事实节点。逻辑攻击图以逻辑关系图隐式地表示了原子攻击之间的依赖关系，但是该图比较复杂，不便于直观理解。

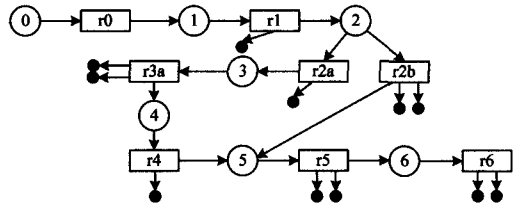

图 7　逻辑攻击图

目前的研究表明，即使对于只有 20 台主机规模的网络，它所对应的攻击图不仅节点数非常庞大而且关系非常复杂[11,28]。为此，研究者提出了多种攻击图复杂性管理技术。

针对属性攻击图，Noel 等提出了层次化聚合技术，用以管理其复杂性。图 8 是聚合攻击图例子。他的主要思想是提出了多个聚合规则，如对源主机和目标主机相同的原子攻击聚合成原子攻击集（椭圆表示）、对与相同原子攻击关联的属性聚合成主机（主机表示）、对多个主机聚合成保护域（矩形框表示）等，然后利用这些规则对攻击图以不同的粒度进行抽象聚合和展示[29]。这些聚合规则对攻击图的复杂性管理具有很大的指导意义，但是他没有提出具体的聚合算法，缺乏可操作性。在进一步的研究中，他们还提出了以邻接矩阵方法来描述大型的攻击图，以及通过过滤技术使攻击图只展示感兴趣的重要原子攻击，从而减少攻击图的复杂性和规模[44]。

文献[45,46]提出了空间分组和颜色标记方法来分层展示攻击图，并通过聚合相同层次主机的方法来降低整个攻击图的复杂性。他采用树型结构来展示各个子网中的主机，每个树形结构中的主机根据其可达性、攻击者拥有的访问权限以及所需前提分成各个组。

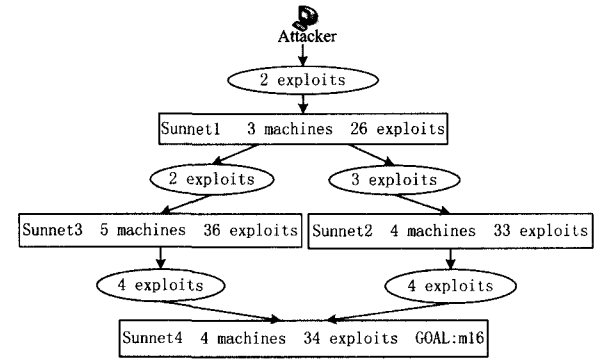

图 8　聚合攻击图例子

Homer 等认为逻辑攻击图中存在一些“冗余”的原子攻击，这些原子攻击增加了人们理解“核心”安全问题的困难，因而可以消除它。同时他提出了把一些相似原子攻击以虚拟节点聚合替换的方法，从而有效降低了逻辑攻击图的复杂性[47-49]。

2.3　攻击图分析研究

攻击图展示了攻击者利用目标网络内不同脆弱性逐步实施网络攻击行为的可能的攻击路径。基于攻击图，人们对网络安全分析和管理中所面临的相关问题展开了一系列深入研究，尤其是在网络安全测评、网络安全措施优化和网络入侵预警关联 3 方面上取得了比较显著的研究成果。

2.3.1　在网络安全定量评估中的应用研究

对目标网络进行科学的安全测评所面临的主要挑战之一是识别网络中攻击者利用各脆弱性间的相互关系产生的潜在威胁。攻击图是解决该问题的良好途径之一。

Jha 等认为状态攻击图中各个状态具有平稳分布特征，可以为每个原子攻击指派成功发生的概率值，并利用马尔科夫决策过程模型计算攻击目标被攻击者成功入侵的最大概率值[14]。但是他对平稳分布特征缺乏论证。如果状态攻击图中有大量转移概率未知，用马尔科夫决策过程所得的结果将会远远偏离正确值[10]。

Lingyu 等基于属性攻击图考虑了攻击的难度、重配置网络的代价以及网络中关键信息资产的价值等，提出了网络安全度量方法[31,32]。

冯萍慧等人认为攻击者利用网络中的脆弱性需要一定的成本，故可以通过计算攻击者沿着攻击路径到达攻击目标所需的攻击成本来测量目标网络的安全性。张海霞等利用状态攻击图在考虑了相似攻击的基础上对各条路径的攻击代价进行计算，从而以最小攻击代价来度量目标网络的安全性[50]。

Mehta 和 Sawilla 等考虑攻击图中各个节点由于在攻击路径中所处位置的不同而具有不同的重要性，如某些原子攻击是多条攻击路径中的关键点等，基于 google 的页分级思想来计算各个节点的重要度[35,36,51,52]。

2.3.2　在网络安全措施优化问题中的应用研究

攻击图能够识别目标网路中脆弱性之间的关系以及它们产生的潜在威胁。为了保证目标网络中的关键资产不被攻击者破坏，达到“适度安全”，需要采取有效的网络安全措施。由于这些安全措施的实施需要一定的成本，因此研究者基于攻击图对网络安全措施优化问题进行了研究。

2002 年，Jha 等认为每一步原子攻击可以通过安全措施来阻止，他们基于状态攻击图寻找保障目标网络中关键信息资产安全的最小安全措施集[14]。

2003年,Noel等研究认为阻止原子攻击的最好方式是从源头上把引起这些原子攻击发生的前提条件消除掉,并且每个安全弥补措施需要一定的成本。他们基于属性攻击图提出了最小成本的安全弥补措施集[34],但是该方法不能应用于大型的具有含圈攻击路径的攻击图。

2006年,Lingyu提出基于逻辑推理的方法[33]。首先把该问题转化为布尔表达式,然后通过求该表达式的析取范式计算出所有的弥补措施集合,并在此基础上求最优弥补集。该方法在最坏情况下具有不可避免的指数时间复杂度,无法应用于大规模目标网络。

2008年,Homer等人认为采取安全弥补措施提高网络的安全性受到多种条件的约束,如重要服务的可用性需求、潜在威胁的代价以及安全弥补措施的成本,于是基于逻辑攻击图提出了一种自动化网络配置管理方法,用以迭代地寻找权衡各种约束的网络配置方案[49]。但是该方法在最坏情况下具有不可避免的指数时间复杂度,仍然无法应用于大规模目标网络。

2.3.3 在网络入侵预警关联问题中的应用研究

对IDS的预警事件进行关联分析,能够有效检测多步骤组合攻击想定,减少IDS的误报率和漏报率。但是传统的预警关联研究都仅从攻击者的角度考虑各个原子攻击产生的预警事件之间的依赖关系,而忽略了目标网络的具体环境,从而产生了许多预警事件的关联和攻击意图预测与真实攻击想定不符的现象。例如,若目标网络不存在某种脆弱点,那么攻击者针对该脆弱点产生的预警事件并不会对目标网络产生实质的安全影响,因此在分析过程中,这些预警事件可以被过滤掉,从而提高预警关联和攻击意图预测的准确性。Noel,Lingyu和石进等利用攻击图确定目标网络中脆弱性之间的关系,然后将预警事件映射到攻击图中来进行预警关联分析,取得了很好的效果[38,39,53]。

2.4 展望

经过多年研究,攻击图研究取得了初步的研究成果,实现了多个原型,如TVA[26]、MulVAL[15,16]和NetSPA[25]等。但是为了能够自动地为大规模目标网络产生和分析攻击图,辅助管理员进行有效的网络安全分析和管理,我们认为研究者面临着下面4个方面的挑战。

(1)自动获取目标网络模型的参数。脆弱性自动扫描工具可以获取软件错误类型的脆弱性,但是很难获取软件配置错误类型的脆弱性,并且由于网络中存在防火墙的限制,自动扫描工具无法获得全部的脆弱性信息。而以在大规模网络中使用客户端代理工具收集脆弱性,存在非常大的管理和技术困难。再则,虽然网络扫描技术和防火墙建模技术可以获取简单网络中的连接信息,但是复杂网络中存在各种网络组件如路由器、防火墙、NAT、虚拟专网等,它们相互影响,决定着网络中的连接关系,自动获取这些信息需要更加有效的方法。此外,目前的方法在构建攻击图时,攻击者的初始能力都是由管理员假设的,这并不能反映真实的网络威胁状况,在攻击者真实初始能力基础上产生的攻击图对网络安全分析才更具有指导意义,例如,我们可以考虑利于入侵检测系统产生的预警信息来确定攻击者对目标网络的初始攻击能力。

(2)建立完备的攻击模板知识库。攻击模板知识库是对攻击者攻击能力的建模,它越完备越能反映攻击者的真实能力。目前攻击模板都是用手工完成的,这是一项非常耗时的工作,有的攻击模板可能需要专家花费十多分钟到一个小时才能确定它的前提条件和影响[40]。虽然目前有一些开放的脆弱性数据库,如CVE、CERT等,但是攻击建模必需的细节信息并不能自动产生。

(3)提高攻击图构建算法的可扩展性。目前关于攻击图构建算法的可扩展研究取得了很大的进展,尤其是Ingols算法的复杂度与目标网络的主机规模呈线性增长,但是这些算法研究都只是针对远程内存溢出攻击模板的,不能适用于一般的攻击模板。事实上,攻击图构建算法的复杂度不仅仅与网络中的主机数目有关,还与脆弱性数目、连接关系等因素有关。目前我们没有发现文献表明可以产生真实网络规模超过200台主机50台以上的攻击图[25]。为了能够为大型真实网络构建攻击图,我们认为一种可能的方法是为大型网络的各个子网分别并发构建攻击图,然后将这些子攻击图融合成完整的攻击图。

(4)丰富攻击图的实际应用研究。攻击图展示了攻击者利用目标网络脆弱性实施网络攻击理论上可能的各种攻击路径。但是在实际应用中还有诸多实际问题需要解决。例如,在网络安全测评研究中,研究者大多忽视了如何科学获取攻击路径上的基础数据,如原子攻击发生概率等的研究,从而制约了这些方法的实用性。在网络安全措施优化研究中,当前的方法大多不具有良好的可扩展性,从而无法应用于真实目标网络所对应的大规模攻击图中。在网络入侵预警关联研究中,研究者虽然进行了初步的研究,取得了一定的研究成果,但是要应用到真实的目标网络中还有许多问题需要做进一步的深入研究。

参考文献

[1] Beale J, Meer H, Temmingh R, et al. Nessus Network Auditing [M]. Rockland: Syngress Publisher, 1998

[2] xfocus team. xfocus[EB/OL]. http://www.xfocus.net/tools/200507/1057.html, 2009

[3] Sheyner O, Jha S, Wing J M, et al. Automated Generation and Analysis of Attack Graphs[C]// Proc. of the IEEE Symp. on Security and Privacy. NJ: IEEE, 2002: 273-284

[4] Swiler L P, Phillips C, Gaylor T. A Graph-based Network-vulnerability Analysis System[R]. California: National Laboratories, 1998

[5] Swiler L P, Phillips C, Ellis D, et al.. Computer-attack Graph Generation Tool[C]// DISCEX11. NJ: IEEE, 2001: 307-321

[6] Ritchey R W, Ammann P. Using Model Checking to Analyze Network Vulnerabilities[C]// S&P 2000. NJ: IEEE, 2000: 156-165

[7] Wang L, Yao C, Singhal A, et al. Interactive analysis of attack graphs using relational queries[C]// DBSec 2006. NJ: IEEE, 2006: 119-132

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

[9] Ammann P, Wijesekera D, Kaushik S. Scalable, Graph-based Network Vulnerability Analysis[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. New York: ACM, 2002: 217-224

[10] Feng Ping-hui, Lian Yi-feng, Dai Ying-xia, et al. A vulnerability model of distributed systems based on reliability theory[J]. Journal of Software, 2006, 17(7): 1633-1640

[11] Ritchey R, O'Berry B, Noel S. Representing TCP/IP Connectivity for Topological Analysis of Network Security[C]// Procee-

dings of the 18th Annual Computer Security Applications Conference. NJ:IEEE,2002

[12] Jalili Z R, Shahriari R, et al. Using Description Logics for Network Vulnerability Analysis[C]// Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies. NJ: IEEE, 2006: 78-78

[13] Zhang Hai-xia, Su Pu-rui, Feng Deng-guo. A Network Security Analysis Model Based on the Increase in Attack Ability[J]. Journal of Computer Research and Development, 2007, 44(12): 2012-2019

[14] Jha S, Sheyner O, Wing J. Two Formal Analyses of Attack Graphs[C]//CSFW'15. NJ:IEEE, 2002: 49-63

[15] Ou Xin-ming, Boyer W F, McQueen M A. A Scalable Approach to Attack Graph Generation[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 336-345

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

[17] Ingols L R P, Scott K W, et al. Evaluating and Strengthening Enterprise Network Security Using Attack Graphs[EB/OL]. http://citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.92.3063, 2005

[18] Li Wei. An Approach to Graph-based Modeling of Network Exploitations[D]. Mississippi: Mississippi State University, 2005

[19] Jalili Z R, Shahriari R, et al. Using Description Logics for Network Vulnerability Analysis[C]// MCL-2006. NJ: IEEE, 2006: 78-78

[20] Templeton S, Levitt K. A Requires / Provides Model for Computer Attacks[C]//Proceedings of the 2000 Workshop on New Security Paradigms. New York: ACM, 2001

[21] Cuppens F, Ortalo R. LAMBDA: A Language to Model a Database for Detection of Attacks[C]//RAID 2000. Berlin: Springer Verlag, 2001

[22] Cheung S, Lindqvist U, Fong M. Modeling Multistep Cyber Attacks for Scenario Recognition[C]// DISCEXIII. NJ: IEEE, 2003: 284-292

[23] Ortalo R, Dewarte Y, Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operation Security[J]. IEEE Transactions on Software Engineering, 1999(25): 633-650

[24] Bhattacharya S, Ghosh S K. An Artificial Intelligence-based Approach for Risk Management Using Attack Graph[C]//International Conference on Computational Intelligence and Security. NJ: IEEE, 2007: 794-798

[25] Ingols K, Lippmann R, Piwowarski K. Practical Attack Graph Generation for Network Defense[C]// ACSAC06. NJ: IEEE, 2006: 121-130

[26] Jajodia S, Noel S, O'Beny B. Topological Analysis of Network Attack Vulnerability[M]. Kumar V, Srivastava J, Lazarevic A, eds. Managing Cyber Threats: Issues, Approaches and Challenges. Dordrecht, Netherlands: Kluwer Academic Publisher, 2003

[27] Lippmann R P, et al. Validating and restoring defense in depth using attack graphs[C]// Proceedings of MILCOM2006. NJ: IEEE, 2006

[28] Artz M, NETspa. A Network Security Planning Architecture [D]. Cambridge: Massachusetts Institute of Technology, 2002

[29] Noel S, Jajodia S. Managing Attack Graph Complexity Through Visual Hierarchical Aggregation[C]//Proc. ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM, 2004

[30] Jacobs N S, Kalapa M P, Jajodia S. Multiple coordinated views for network attack graphs[C]//VizSEC 05. NJ: IEEE, 2005: 99-106

[31] Wang Ling-yu, Singhal A, Jajodia S. Measuring the overall security of network configurations using attack graphs[C]//DBSec 2007. Berlin: Springer Verlag, 2007: 98-112

[32] Wang Ling-yu, Singhal A, Jajodia S. Toward Measuring Network Security Using Attack Graphs[C]//QoP 2007. NJ: IEEE, 2007: 49-54

[33] Wang L, Noel S, Jajodia S. Minimum-cost network hardening using attack graphs[J]. Computer Communications, 2006, 29(18): 3812-3824

[34] Noel S, Jajodia S, O'Berry B, et al. Efficient minimum-cost network hardening via exploit dependency graphs[C]// ACSAC'03. NJ: IEEE, 2003

[35] Mehta V, Bartzis C, Zhu Hai-feng, et al. Ranking Attack Graphs [C]//RAID 2006. NJ: IEEE, 2006: 127-144

[36] Sawilla R, Ou Xin-ming. Googling attack graphs[R]. Defence R & D Canada, 2007

[37] Homer J, Ou Xin-ming, McQueen M A. From Attack Graphs to Automated Configuration Management- An Iterative Approach [EB/OL]. http://en.scientificcommons.org/42600212, 2008

[38] Noel S, Jajodia S. Correlating intrusion events and building attack scenarios through attack graph distance[C]// ACSAC'04. New York: ACM, 2004

[39] Wang Ling-yu, Liu A, Jajodia S. Using attack graphs for correlating, hypothesizing, and predicting network intrusion alerts[J]. Computer Communications, 2006, 29(15): 2917-2933

[40] Bilar D. Quantitative Risk Analysis of Computer Networks[R]. Hanover, New Hampshire: Thayer School of Engineering, Dartmouth College, 2003

[41] Li W, Vaughn R. Building Compact Exploitation Graphs for a Cluster Computing Environment[C]// Smc'05. NJ: IEEE, 2005: 50-57

[42] Li W, Vaughn R. Using Exploitation Graphs to Model Network Exploitations[C]//RMCI'05. NJ: IEEE, 2005: 404-409

[43] Li W, Vaughn R. An Approach to Model Network Exploitations Using Exploitation Graphs[C]//SMC'05. NJ: IEEE, 2005: 237-244

[44] Noel S, Jacobs M, Kalapa P, et al. Multiple coordinated views for network attack graphs[C]//VizSEC'2005. NJ: IEEE, 2005

[45] Williams L, Lippmann R, Ingols K. An interactive attack graph cascade and reachability display[C]//VizSEC'2007. NJ: IEEE, 2007

[46] Williams L, Lippmann R, Garnet I K. A graphical attack graph and reachability network evaluation tool[C]// VizSEC'2008. NJ: IEEE, 2008

[47] Homer J, Ou X. SAT-solving approaches to context-aware enterprise network security management[C]// JSAC'09. NJ: IEEE, 2009

[48] Homer J, Varikuti A, Ou X, et al. Improving attack graph visualization through data reduction and attack grouping[C]// VizSEC'08. NJ: IEEE, 2008

[49] Homer J. A comprehensive approach to enterprise network security managment[D]. Kansas: Kansas State University, 2008

[50] 张海霞,苏璞睿,冯登国. 基于攻击能力增长的网络安全分析模型[J]. 计算机研究与发展, 2007, 44(12): 1225-1227

[51] Saha D. Extending logical attack graphs for efficient vulnerability analysis[C]// Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS). New York: ACM, 2008

[52] Salim M, Al-Shaer E, Khan L. A novel quantitative approach for measuring network security[C]// INFOCOM 2008 Mini Conference. New York: ACM, 2008

[53] 石进,郭山清,陆音,等. 一种基于攻击图的入侵响应方法[J]. 软件学报, 2008, 19(10): 2746-2753