文章编号: 1001- 2486(2009) 04- 0074- 07

基于攻击图的计算机网络攻击建模方法*

王国玉, 王会梅, 陈志杰, 鲜 明
(国防科技大学 电子科学与工程学院, 湖南 长沙 410073)

摘 要: 随着计算机网络入侵技术的不断发展, 网络攻击行为表现出不确定性、复杂性和多样性等特点, 攻击向大规模、协同化和多层次方向发展, 计算机网络攻击建模已成为当前研究的热点。综合论述计算机网络攻击建模的研究概况, 剖析网络攻击图的定义, 讨论现有的典型网络攻击图的主要生成方法并对其进行复杂性分析, 在此基础上归纳总结目前网络攻击图的应用。给出网络攻击图研究的若干热点问题与展望。

关键词: 网络攻击; 攻击图; 攻击建模
中图分类号: TP393. 08 文献标识码: A

Research on Computer Network Attack Modeling Based on Attack Graph

WANG Guo-yu, WANG Hui-mei, CHEN Zhi-jie, XIAN Ming
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: With the development of the intrusion technology and the uncertainty, complexity and diversity character of the network attack, the next direction will be characterized as large scale, collaboration and multilayered. As a result, modeling of network attack has been the focus of attention. In the current study, firstly, the research background of modeling of network attack and the concept of attack graph are presented. Then the represented network attack graph generating method and its algorithmic complexity are discussed. Finally, the application of network attack graph is given. In conclusion, some major problems and research trends in this area are addressed.

Key words: network attack; attack graph; attack modeling

随着全世界对信息社会的依赖性不断增加, 网络与信息安全的重要性不断凸现, 网络攻击向大规模、协同化和多层次方向发展, 攻击行为表现出不确定性、复杂性和多样性等特点, 网络攻击建模已成为当前研究的热点。通过对网络攻击进行建模, 发现网络攻击的特点和规律, 并对网络安全和网络攻击的效果进行评估和预测, 可以提高网络系统应对各种突发网络攻击事件的能力, 弥补信息安全基础建设方面的不足。

现有的网络攻击建模方法有很多, 主要集中于攻击语言、攻击树、攻击网、状态转移图和攻击图等。最早的攻击图由 Cunningham 等于 1985 年提出[1], 该方法认为网络由各种组件构成, 这些组件之间通过物理的或者逻辑的方式相连。攻击图中的边表示攻击者需要付出"费用", 攻击者通过攻击网络组件获取"收益"。Kuang 最早提出了生成完整攻击图的方法[2], 并扩展成网络环境——NetKuang 系统, 目前已被用来分析 UNIX 主机的网络配置脆弱性。1998 年 Swiler 等提出了一种攻击图方法[3], 目的是为了在安全分析中把网络拓扑信息也考虑在内。为了自动生成网络攻击图, Ritchey、Sheyner、Jha 等提出了采用模型检测器的方法[4-6]。虽然模型检测技术能够自动生成攻击图, 但为了获取所有的攻击场景, 模型必须包含所有的状态, 容易导致状态爆炸而无法处理大规模网络问题。为了获取简洁的攻击图, Sheyner 采用二分决策图(BDD) 技术来降低模型检测算法的复杂性, Ammann 提出了网络攻击的单调性假设, 对攻击图生成过程予以限制[7]。Tao Zhang 等提出了一种生成攻击图的有效的方法[8], 通过分析主机、链路关系和攻击特征, 构建网络安全状态模型, 然后通过前向搜索、广度优先、深度限制来生成攻击路径。

* 收稿日期: 2009- 01- 04
作者简介: 王国玉(1962—), 男, 研究员, 博士。

Melissa Danforth 研究了一种可测的攻击图生成算法[9], 通过抽象模型和聚类方法减少了原子攻击的数目和机器的数目。Kyle Ingols 提出了一种基于多前置条件的网络攻击图生成方法[10], 随着网络规模的增大, 攻击图成近似线性增加。Ronald W. Ritchey 提出了一种以主机为中心的模型[11], 该方法复杂性较好, 可用于大型网络。Dapeng Man 等提出了一种基于宽度优先搜索的全局攻击图生成算法, 通过限制攻击步骤和攻击路径的成功概率来减少攻击图的复杂性[12]。

本文首先综合论述计算机网络攻击建模的研究概况, 剖析网络攻击图的定义, 讨论现有的网络攻击图的主要生成方法并对其进行复杂性分析, 归纳总结目前网络攻击图的应用。最后给出网络攻击图研究的若干热点问题与展望。

1 计算机网络攻击建模方法

建模和仿真是指构造现实世界实际系统的模型和在计算机上进行仿真的有关复杂活动, 建模主要研究实际系统与模型之间的关系, 它通过对实际系统的观测和检测, 在忽略次要因素及不可检测变量的基础上, 用数学的方法进行描述, 从而获得实际系统的简化近似模型。

为了能够对各种复杂的网络攻击行为进行分析和形式化描述, 以便能够在网络安全防护系统中制定更好的防范措施, 已经提出了攻击语言、攻击树[13-14]、攻击网[15-16]、状态转移图和攻击图等攻击建模方法。这些建模方法各有特点。

网络攻击语言是最早的对网络攻击行为进行描述的建模方法。其原理是通过一种形式化的描述语言对网络攻击行为进行形式化的描述, 包括 NASL, STATL, LAMBDA, BRO, ADELE, N-code 等, 能够直接地对一个或一类攻击行为进行语言化的描述, 适合工程化应用; 但不适合描述阶段性的攻击行为。

攻击树用一个树形结构来描述对系统的攻击, 把攻击要达到的总目标作为树的根节点, 达到总目标的子目标作为子结点, 逐步细分, 最后树的末端的叶节点就是具体的攻击方法。该方法比较适合于宏观上的分析, 可应用于威胁分析、风险分析。在对系统做安全分析时, 以其易于理解的表示方法、附带的多种评估参数而具有很高的实用价值。但它仅限于描述、形式化分析, 主观性比较强, 不适合于复杂度高的大型网络系统建模。

攻击网由位置、变迁、弧和令牌构成, 位置与攻击图中的节点相对应, 攻击行为通过令牌在位置间变迁的转换来描述。攻击网有强大的 Petri 网理论做背景, 可以较好地表示攻击所处的状态、攻击的动作以及攻击的进展, 在自动控制方面具有独到之处。但是攻击模型没有考虑到网络的拓扑结构, 因此对网络信息的利用不全面。

状态转移图以有限状态机模型为技术基础表示入侵过程。入侵者的渗透过程都可以看作从有限特权开始, 利用系统存在的漏洞和配置错误等不断提升用户权限的过程。但是在模型中系统状态不具备认识实际含义, 仅仅是一个标记, 其状态的含义不甚明确, 应用面较窄。

网络攻击图就是一组攻击者能够使目标计算机网络系统的特定安全属性遭受破坏的攻击预案集合。网络攻击图将网络拓扑信息考虑在网络的建模工作中, 并可自动化生成模型, 使建模和评估工作减少了人为的主观因素的影响, 更加科学化。因此, 利用攻击图对复杂的组合网络攻击进行建模较为合适。

2 网络攻击图的定义

攻击图是研究人员综合攻击、漏洞、目标、主机和网络连接关系等因素, 为发现网络中复杂的攻击路径或者引起系统状态变迁的渗透序列而提出的一种描述网络安全状态的表示方法。

攻击图可用来表示在攻击者试图入侵计算机网络时, 能否从初始状态到达目的状态。攻击者可以利用已经取得权限的主机作为跳板再次发起攻击, 直到达到最终的攻击目的。一个完整的攻击图可以表示所有可能达到目的的操作序列[18]。

3 典型的网络攻击图的生成方法

计算机网络攻击图历经最初的手动生成到自动生成,从有几个主机的简单网络到大规模网络的攻击图生成过程。下面重点分析几种典型的攻击图生成方法。

3.1 基于攻击模板的攻击图生成方法

为了在安全分析中把网络拓扑信息也考虑在内,1998年Swiler等提出了一种攻击图生成方法[3]。在该模型中,攻击图的节点代表可能的攻击状态,节点内容包括主机、用户权限、攻击的效能等。边代表由攻击者的单一行为或不知情的辅助工具的行为引起的状态转换,行为执行者可能是攻击者、普通用户、后门程序等。该方法的输入由三部分组成:配置文件、攻击者简档和攻击模板。配置文件包括操作系统信息、网络类型、网络拓扑结构以及路由器配置等。攻击者简档表示攻击者的能力信息。攻击模板表示一致攻击的步骤,攻击模板也表示已知攻击的步骤,其节点表示系统的状态,包括用户权限、脆弱性、攻击者的能力、状态等,边表示攻击动作。从节点 u 到节点 v 的边中,节点 u 称为边尾,节点 v 称为边头。

通过已有的攻击模板,从目标状态反向生成系统的攻击图。首先,从目标节点开始,遍历攻击模板库,寻找含有与目标节点相同的边头的攻击模板;对每个相匹配的模板,如果目标节点与模板中的节点相匹配,同时满足所有的约束条件,则生成边尾节点 N_i,并把该节点从队列中移除。N_i 同时为新边的边头,通过递归运算,直到达到攻击者的初始节点。同时,通过边权重可以表示攻击成功概率等。

该算法的复杂性与攻击模板及攻击图的深度有关,设攻击模板的数目为 N,攻击图的深度为 m,则该算法的计算复杂性为 $O(N^m)$。但是该算法的难点在于攻击模板库的建立,在最初提出时,只能手动生成不超过20个攻击模板的攻击图。

3.2 基于模型检测的攻击图生成方法

攻击图可用一个5元组 $G=(S,\tau,S_0,S_s,D)$ 来表示[20]。其中 S 是状态的集合,$\tau\subseteq S\times S$ 表示变迁关系,$S_0\subseteq S$ 是初始状态的集合,$S_s\subseteq S$ 是成功状态的集合,$D: S\rightarrow 2^{AP}$ 是对状态的标记(AP 表示原子命题集合),在该状态上为一些命题为真的集合。

模型检测方法为攻击图建模提供了自动生成的工具。模型检测的描述规范由两部分组成:一是模型,这是一个由变量、变量的初始值、变量的值发生变化的条件描述所定义的状态机;二是关于状态和执行路径上时序逻辑约束。模型检测器访问所有可到达的状态,检验在每条可能的路径上时序逻辑属性是否得到满足。如果属性没有得到满足,模型检测器输出一条状态的轨迹或序列形式的反例,而这个反例在攻击图模型中正是一个攻击路径。这就是模型检验方法的攻击图自动生成原理。

3.2.1 基于符号模型检测的攻击图生成算法

Jha和Wing提出了采用符号模型检测算法来计算攻击预案图。首先构建二分决策图,将网络攻击事件模型转化为符号模型检验的输入,然后确定由初始状态出发所能到达的状态的集合 S_{reach}。通过符号模型检验方法计算有路径通向不安全状态的状态集合 S_{unsafe}。令 τ 为模型的变迁关系,也即 $(s,s')\in\tau$ 当且仅当存在一条从状态 s 到 s' 的变迁。通过限制到集合 S_{unsafe} 的变迁的集合 τ 的范围,得到一个变迁关系的集合 τ',τ' 封装了攻击图的边。于是,攻击图是 $G_p=(S_{unsafe},\tau',S_0^p,S_s^p,D)$,其中 S_{unsafe} 和 τ' 分别代表了攻击图的节点集合和边集合。$S_0^p=S_0\cap S_{unsafe}$ 是初始状态的集合,终止状态的集合为 $S_s^p=\{s\mid s\in S_{unsafe}\wedge unsafe\in L(s)\}$。

在该生成算法中,状态变量之间的复杂交互使构建的二分决策图的大小不可控,即使有合适的变量次序,在有600个可达状态时,模型建立也需要2h[20]。在此基础上Sheyner提出了基于显示状态模型检测的攻击图生成算法[20]。

3.2.2 基于显式状态模型检测的攻击图生成算法

在基于符号模型的基础上,首先计算两个自动机的交,$M=(S,\tau_m,S_m^0,S_a,S_f,D)$ 为网络攻击事件

的B chi 模型, $N_p = (S_p, \tau_p, S_p^0, S_p^a, S_p^f, \cong)$ 为非正确属性 B chi 模型, 则这两个自动机的交表示当自动机的所有状态为可接受的和最终态时是有效的, $M_s = M \cap N_p = (S \times S_p, \tau, S_m^0 \times S_p^0, S \times S_p^a, S \times S_p^f, D)$。接下来采用Tarjan 经典算法计算 M_s 的强连通组件(SCC) 图, 在转换 SCC 图和记录结果预案图的组件的基础上, 计算结果自动机。

实际上, 计算 SCC 图可与其他步骤并行进行, 而在整个过程中可以使用深度优先来遍历可达的状态空间。因此该算法渐进运行时间为 $T(E) = S(E)O(E)$, 其中 E 是图中边的个数, $S(E)$ 是搜索算法的运行时间。

3.3 基于抽象模型的攻击图生成方法

生成攻击图方法的瓶颈之一为大型网络的可测性, 而影响攻击图复杂性的主要因素为原子攻击的数量和模型中计算机的数目。为了减少原子攻击的数目, Melissa Danforth 提出了一种抽象类模型[9], 同时通过对同一网段的标识主机进行聚类来减少机器的数目。

在预处理阶段, 把基于网络信息文件的攻击转换成抽象模型, 包括把基于权能的攻击映射成抽象权能, 把基于端口的攻击映射成抽象端口, 对于大多数映射来说为一对一映射。但是, 有时需要多对一映射。

在聚类阶段, 首先根据权能把所有机器聚合成基本簇, 然后再依次考虑各个簇并根据网络段进行细分。为权能创建一个字符串, 该字符串为哈希表中的键。通过顺序扫描主机把拥有相同字符串的机器放进相同的哈希表槽中。如果槽中只有一台机器则输出网络信息文件, 否则通过防火墙规则来区分是否在同一网段中。细分以后对每一个聚合进行命名。

抽象类模型的性能优于基于攻击的模型[9], 平均抽象类模型的运行时间为基于攻击模型的一半。聚类算法可以急剧降低运行时间、初始化变量的数目以及计算的边数, 如拥有 1000 台主机的网络的攻击图可以在 2~ 3h 内生成(标准的 Pentium 4 系统), 此外聚类方法还可以减少可视化的复杂性。

3.4 以主机为中心的攻击图生成方法

从理论上讲, 以状态为节点的攻击图由于空间爆炸将难以管理, 为了保障计算机网络的安全, Ronald W. Ritchey 提出基于主机而不是攻击程序或脆弱性的攻击图[11]。把网络中的每一个主机作为访问图的节点, 基于网络规则和配置的信任关系对两个主机之间的访问进行初始化。两个主机间的通信可能有几种方式, 由于对目标主机拥有较高权限意味着可以完成更强大的攻击, 该模型只保留拥有最高访问权限的边而不是添加多个边。

生成以主机为中心的攻击图模型需要两步: 初始化过程和最大化访问权限过程。

初始化的目的是在应用任何攻击之前确立主机间初始的信任关系。顺序访问层次为 *none*, *connectivity*, *pass-through*, *user* 和 *admin*。访问图中每条边的初始访问权限为 *none*, 网络中两个主机间的信任关系可能有多个, 这时应保留最高权限。对信任关系进行更新时, 为了减少计算复杂性, 如果已经达到 *admin* 权限, 则停止。

通过攻击程序来获得网络中所有主机间的最大访问权限。如果两个主机间通过某个合适的端口有充足的连通性, 同时满足攻击需要的所有前提条件, 从源主机到目的主机间可增加边。边的标识包括路由 ID、源主机、目的主机、边生成的方法、获取的访问权限、漏洞 ID 以及用来识别是否为一系列攻击的链 ID 标志。算法通过直接攻击和间接攻击来提升访问权限, 同时应用著名的 Floyd-Warshall 算法来解决所有主机节点之间的最短路径问题。

初始化过程是利用一系列信任关系 T 来计算网络初始访问权限, 网络中有 n 台主机, 分析每两个主机间的关系得到 n^2。最大化访问权限过程在算法中利用攻击程序来决定最大访问权限, 需要较高的计算成本。第一部分为检测直接连接边, 在最差情况下需要 XVn^2。其中 X 为所有主机的攻击程序数目, V 为网络中当前所有漏洞的总数目, n 为主机数。第二部分检测间接边可达到 n^3。该算法的计算复杂性为 $O(n^2 + XVn^2 + n^3)$。

该方法可以在大规模网络中生成攻击图, 缺点是不能识别每一个攻击序列。

3.5 其他

以上为典型的攻击图生成算法,同时研究人员还提出了需求/产出模型、特权提升图、基于逻辑的建模方法来描述和生成攻击图。

Templeton 和 Levitt 提出了需求/产出模型(Requires/Provides)[21],把计算机网络攻击看作一组抽象的攻击"概念"的结合体。"能力"和"概念"是该模型的主要组成部分,"能力"为攻击能够发生的前提条件和信息,"概念"是特定攻击中子任务的抽象表示。该模型通过对"能力"和"概念"的需求/产出关系进行匹配来发现或产生攻击序列。

Dacier 和 Ortalo[22] 等提出使用特权提升图来进行网络脆弱性分析。对于攻击者来说,利用目标系统的脆弱性实施攻击是特权提升的过程。哈尔滨工业大学的汪立东等[23-24]在此基础上提出了特权图、特权提升、特权集等概念,并给出了相应的定义。

Xinming Ou 提出了基于 Prolog 逻辑的建模方法——MulVAL 建模方法[25]。首先对网络配置信息、主机信息和安全策略进行形式化描述,并且把形式化描述的原子攻击行动作为推理规则,然后利用 MulVAL 推理机询问该安全策略能否保证,如果不能,则给出所有攻击路径。

3.6 典型网络攻击图生成方法的比较

由表1分析得知,典型的攻击图生成主要有两大类,一类为状态的变迁,通过算法可生成完整的攻击图,但应用在大规模商业网络中时常引发"状态空间爆炸";另一类以主机为中心,可应用在大规模网络中,但缺点是不能列出所有的攻击路径。在以后的研究中,应该在复杂性和完整性中间达到平衡,以便很好地应用在网络攻击和网络安全中。

表1 典型网络攻击图生成方法比较

Tab.1 Comparison of the represented method of generating network attack graph

		结点	边	主要特点	主要应用
基于攻击模板的攻击图生成方法		攻击状态	引起状态转换的行为	攻击模板	脆弱性分析
基于模型检测的攻击图生成方法	符号模型检测显示状态模型检测	原子攻击对主机造成的影响	攻击者实施的原子攻击	符号模型检测 深度优先遍历可达状态空间 追溯搜索模式	网络安全
基于抽象模型的攻击图生成方法		攻击对主机造成的影响	攻击者实施的攻击	抽象类模型 聚类技术	风险评估
以主机为中心的攻击图生成方法		网络中的主机	访问权限	把主机作为攻击图的结点	安全分析

4 网络攻击图的应用

随着计算机网络入侵技术的不断发展,网络攻击行为表现出不确定性、复杂性和多样性等特点,攻击向大规模、协同化和多层次方向发展,基于攻击图的计算机网络攻击建模应运而生,网络攻击图的自动生成赋予了其广阔的应用前景,主要表现在网络安全分析、入侵检测、安全防御、风险评估等领域。

4.1 网络安全分析

随着网络系统逐渐复杂和庞大,特别是网络攻击和破坏行为的日益普遍和多样性,网络安全性面临着严峻的挑战。网络攻击图可用于分析网络安全,确定从一个特定位置是否可以获得目标的特殊权限[26];网络攻击图可用来测量脆弱性网络的重要资源的安全性,同时从不完全输入数据得到网络安全测量的准确结果[27]。

4.2 入侵检测

入侵检测技术作为动态安全系统核心的技术之一, 在网络纵深防御体系中起着极为重要的作用, 它是静态防护转化为动态防护的关键, 也是强制执行安全策略的有力工具。攻击图可用于对 IDS 产生的大量告警进行分组[28-29], 首先对拥有 IDS 防护的计算机网络系统构建攻击图, 预示着攻击者通过攻击路径成功进行攻击的告警顺序到来。通过对告警进行分组, 为安全分析员提供更高层次的告警。

4.3 安全防御

动态安全防御技术是一种基于安全信息管理的技术, 系统安全稳定是通过对安全信息的监控、融合、反馈、动态调整安全策略来实现的[30]。网络防御者利用攻击图来阐明攻击者用来获取目标网络的访问权限的攻击路径, 在此基础上对网络的脆弱性和配置错误进行修复[31]。同时可通过攻击图进行攻击预测, 对网络系统进行安全防御[32]。

4.4 风险评估

攻击图可用于对计算机体系结构进行安全风险分析[33], 它可以获取攻击者达到攻击目标的路径。在系统设计时对风险进行分析, 使设计者和分析者减轻这些风险时达到平衡, 直到风险可以接受为止。

5 结论和展望

基于攻击图的计算机网络攻击建模研究是随着计算机网络技术的发展逐步深入的, 建模的对象从只含有几个主机的简单网络发展到了大规模网络, 建模的手段从最初的手动向自动化的方向发展。本文在综合论述计算机网络攻击建模的研究概况的基础上, 剖析网络攻击图的定义, 讨论现有的网络攻击图的主要生成方法并对其进行复杂性分析, 归纳总结了目前网络攻击图的应用。

基于攻击图的计算机网络攻击建模已获得较广泛的应用。但是, 还存在着以下几个问题, 揭示了未来的发展方向:

(1) 大型网络的可测性

虽然已提出抽象类模型、以主机为中心的模型等攻击图生成方法, 但对于大规模网络的攻击图建模方法, 应根据建模目的合理调整建模方法, 以减小时间、空间复杂性。

(2) 通过攻击图给出网络安全性建议

网络管理员可以利用攻击图发现网络中存在的潜在危险, 在不影响网络中主机正常运作的情况下消除网络中重要的危险, 为决策提供更多包括安全投入/收益平衡以及安全措施优化等的辅助信息。

(3) 攻击规划

攻击者通过社会工程、扫描、入侵等攻击技术可得到被攻击网络的信息, 根据这些信息建立简略攻击图, 从中找出最佳攻击路径, 达到攻击权益的最大化。

参 考 文 献:

[1] Cunningham W H. Optimal Attack and Reinforcement of a Network [J]. Journal of the ACM (JACM), 1985, 32(3): 549-561.

[2] Kuang R B. Rule Based Security Checking[R]. Technical Report, MIT Lab for Computer Science, 1994.

[3] Swiler L P, Phillips C, Gaylor T. A Graph Based Network Vulnerability Analysis System, SAND97-3010/1[R]. Sandia National Laboratories, Albuquerque, New Mexico and Livermore, California, 1998.

[4] Ritchey R W, Ammann P. Using Model Checking to Analyze Network Vulnerabilities[C]// Proceedings of the IEEE Computer Society Symposium on Security and Privacy(S&P 2000), Oakland, California, 2000: 156-165.

[5] Jha S, Sheyner O, Wing J. Two Formal Analyses of Attack Graphs[C]// Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW'15), Cape Breton, Nova Scotia, Canada, 2002: 49-63.

[6] Sheyner O, Haines J, Jha S, et al. Automated Generation and Analysis of Attack Graphs[C]// Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&P 2002), Oakland, California, 2002: 254-265.

[7] Ammann P, Wijesekera D, Kaushik S. Scalable, Graph-based Network Vulnerability Analysis[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02), Washington DC, ACM, 2002: 217-224.

[8] Zhang T, Hu M Z, Li D, et al. An Effective Method to Generate Attack Graph [J]. Machine Learning and Cybernetics, 2005: 3926-3931.

[9] Danforth M. Models for Threat Assessment in Networks [D]. University of California-davis, 2006.

[10] Ingols K, Lippmann R, Keith P. Practical Attack Graph Generation for Network Defense [C]// Computer Security Applications Conference, ACSAC apos, 06.22nd Annual Volume, Issue, Dec. 2006: 121- 130.

[11] Ritchy R W. Efficient Network Attack Graph Generation [D]. George Mason University, 2007.

[12] Man D P, Zhang B, Yang W, et al. A Method for Global Attack Graph Generation[C]// IEEE International Conference on Networking, Sensing and Control, 2008: 236- 241.

[13] Moderg F. Security Analysis of an Information System Using an Attack Tree Based Methodology [D]. Chalmers University of Technology, 2000.

[14] Tidwell T, Larson R, Fitch K. Modeling Internet Attacks [C]// Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 2001: 54- 59.

[15] McDermott J P. Attack Net Penetration Testing [C]//The 2000 New Security Paradigms Workshop, ACM SIGSAC, ACM Press, 2000: 15- 22.

[16] Steffan J, Schumacher M. Collaborative Attack Modeling [C]// Proc. of the 2002 ACM Symposium on Applied Computing Madrid, Spain, 2002: 253- 259.

[17] Ritchey R W, Ammann P. Using Model Checking to Analyze Network Vulnerability [C]// IEEE Symposium on Security and Privacy, 2000: 156- 165.

[18] Lippmann R P, Ingols KW. An Annotated Review of Past Papers on Attack Graphs[R]. Lincoln Laboratory, 2005.

[19] Sheyner O. Automated Generation and Analysis of Attack Graphs [C]// Proceedings of the IEEE Symposium on Security and Privacy, 2002: 273- 284.

[20] Sheyner O M. Scenario Graphs and Attack Graphs [R]. CMU- CS- 04- 122, 2004.

[21] Templeton S T. A Requires/Provides Model for Computer Attacks[C]// Proceedings of the New Security Paradigms Workshop, Cork Ireland, 2000: 31- 38.

[22] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security [J]. IEEE Transactions on Software Engineering, 1999, 25(5): 633- 650.

[23] 汪立东. 一种量化的计算机系统和网络安全风险评估方法[D]. 哈尔滨: 哈尔滨工业大学, 2002.

[24] 张永铮, 云晓春, 胡铭曾. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报, 2004, 25(7): 107- 114.

[25] Ou X M, 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, 2006: 336- 345.

[26] Jajodia S. Topological Analysis of Network Attack Vulnerability[C]// ASIACCS' 07, Singapore, March 20- 23, 2007: 2.

[27] Chen F, Su J S. A Flexible Approach to Measuring Network Security Using Attack Graphs[C]// Proceedings of the International Symposium on Electronic Commerce and Security, Guangzhou, China, 2008: 426- 431.

[28] Cuppens F. Alert Correlation in a Cooperative Intrusion Detection Framework[C]// Proceedings of the 2002 IEEE Symposium on Security and Privacy, Washington, DC, IEEE Computer Society, 2002.

[29] Ning P, Xu D. Learning Attack Strategies from Intrusion Alerts[C]// Proceedings of the 10th ACM Conference on Computer and Communications Security, New York: ACM Press, 2003: 200- 209.

[30] Arbaugh W. Active Systems Management: The Evolution of Firewalls [EB] . http:// citeseer. nj. nec. com/ 560818. html.

[31] Ingols K, Lippmann R, Piwowarski K. Practical Attack Graph Generation for Network Defense [R]. ACSAC, 2006: 121- 130.

[32] Lei J, Li Z T. Using Network Attack Graph to Predict the Future Attacks [J]. Communications and Networking in China, 2007: 403- 407.

[33] Gupta S, Winstead J. Using Attack Graphs to Design Systems [J]. Security & Privacy, IEEE, 2007, 5(4): 80- 83.