攻击模型的分析与研究*

陈春霞[1]，黄　皓[1,2]

(1.南京大学 计算机科学与技术系；2.南京大学 软件新技术国家重点实验室,江苏 南京 210093)

摘　要：保护网络安全必须对网络攻击技术进行深入研究,攻击模型能对攻击过程进行结构化描述和有效分析,有助于安全知识的共享以及提高攻击检测和安全预警的效率。对目前常用的几种攻击模型进行了分析与对比,并对攻击模型研究的发展作了展望。

关键词：攻击模型；攻击树；攻击网

中图法分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1001-3695(2005)07-0115-04

Analysis and Research of Attack Model

CHEN Chun-xia[1], HUANG Hao[1,2]

(1. Dept. of Computer Science & Technology, Nanjing University, Nanjing Jiangsu 210093, China; 2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing Jiangsu 210093, China)

Abstract: It needs to further investigate technology of network attack to protect the network security. Attack models can help in describing and analyzing the course of attack structurely and effectively, further more, they can help in sharing the security knowledge and improving the efficiency of attack detection and security prediction. This article analyzes and compares several attack models in common use at present, and then prospects the future directions of attack model research in the end.

Key words: Attack Model; Attack Tree; Attack Net

1　引言

飞速发展的互联网技术促进了社会信息化和信息网络化,许多经济关键领域中的重要应用越来越依赖于计算机网络。相应地,针对网络的各种恶意攻击发生的频率和复杂度都在不断增长,并向大规模、自动和协同方向发展,影响范围和造成的损失越来越大,网络安全技术的研究显得越发重要。

攻击和防御是网络安全的两个密切相关的侧面,不深入研究攻击理论和技术就不能做到知己知彼,也就无法有效保护网络信息系统的安全。网络攻击研究的一个关键问题是对攻击的认识和描述。一次完整的攻击过程通常会包括一系列单独的攻击行为,每个攻击行为是对某个系统漏洞的一次利用。攻击行为可以通过简单地定义攻击的前提、动作和后果来描述。而攻击过程由多种攻击行为组成,达到攻击目标前的每个阶段都可能采用不同的攻击行为,难以使用简单的方法描述。由于攻击过程本身的复杂和多样性,要在已知攻击行为中间找出关联并总结出规律非常艰难。而且目前攻击检测技术的理论基础并不完备,一般情况下带有经验和假设的成分,因此存在一定的不确定性。攻击模型能对整个攻击过程进行结构化和形式化的描述,有助于分析和充分利用已有的攻击行为研究成果,进一步提高攻击检测和安全预警的效率。

2　相关技术进展

目前许多安全站点对网络攻击所利用的各种系统和应用程序的漏洞进行了详细分类和描述,但这并不足以描述整个攻击过程,因此不能代替对攻击模型的研究。

攻击模型的研究是个较新的领域,目前常用的几种攻击模型基本上都处于理论研究阶段。根据主要功能的不同可以将攻击模型分为两种,即适用于安全知识共享的模型和适用于攻击检测和安全预警的模型。

适用于安全知识共享的模型为专家们交换、共享专业知识提供一种方法。为制定出能有效阻止攻击的对策,必须了解系统可能被攻击的途径以及漏洞产生的机制。各领域的专家,如系统设计者、开发者、管理员以及安全专家之间借助适用于安全知识共享的攻击模型协同合作,实现专业知识最大程度的共享,可以发现更多的系统漏洞和入侵途径从而制定出更有针对性的防护措施。目前适用于知识共享的攻击模型主要有 Attack Tree 和 Attack Net 模型。适用于攻击检测和安全预警的模型能提高攻击检测和安全预警的效率,一方面能详尽地描述各种攻击行为,可以更好地满足攻击检测的要求;另一方面能够根据系统的安全需求定义多个系统状态,并对系统状态的变化趋势以及导致状态变化的可能的攻击行为进行较准确的描述,从而满足安全预警的要求。目前适用于攻击检测和安全预警的攻击模型主要有基于系统状态集合的攻击模型。

3　常用攻击模型

目前常用的几种攻击模型都有各自的主要用途和优缺点,本文将逐一介绍几个常用的攻击模型。

3.1　Attack Tree 模型

Attack Tree 模型最早为 Bruce Scheier 提出,是一种结构

收稿日期：2004-07-04；修返日期：2004-09-07

基金项目：国家“863”计划资助项目(2001AA142010)

化、可复用的将攻击过程文档化的方法。

Attack Tree 模型使用树来表示攻击行为及步骤之间的相互依赖关系,树的每个节点代表一个攻击行为或子目标,根节点表示攻击的最终目标。子节点表示在实现父节点目标之前需要成功执行的攻击行为,同一父节点下的子节点具有 AND 或 OR 的关系。AND 关系表示攻击者完成了子节点的全部攻击行为或子目标才可实现父节点的目标。OR 关系表示完成任一个子节点的攻击行为或子目标就可实现父节点的目标。Attack Tree 就是由这些 AND 和 OR 关系组合而成。我们可以使用深度优先方式从攻击树中推导出实现终极目标的攻击路径。图 1 为一个 Attack Tree 的例子。图 1 中 G1, G2 和 G3, G6 和 G7 之间为 OR 关系, G4 和 G5, G8 和 G9 之间为 AND 关系。从图 1 中可以推导出要实现最终目标 G0,存在攻击路径: < G4, G5 > , < G2 > , < G6 > , < G8, G9 > 。可以看到,中间节点在攻击路径中并不出现,因为它们已由底层节点描述。

对于复杂的 Attack Tree,图形化表示将会变得笨拙,因此通常还可使用文本方式表示。一般加入新的 OR 关系会产生新的攻击路径,加入新的 AND 关系则使已存在的攻击路径延长。还可以根据攻击行为发生的概率或代价为树节点补充权重,以找出最佳攻击路径。但对于一般攻击来说,权重过于具体,要在协同环境中找出精确的攻击概率也是不现实的。

Attack Tree 模型的优点在于直观、易于理解,有助于以图形化、数学化方式描述攻击,以及用可重用的方式收集安全知识。利用 Attack Tree 模型可以进行风险分析,设计实现防范攻击的对策并进行测试。

3.2 基于 Petri Net 的 Attack Net 攻击模型

基于 Petri Net 的 Attack Net 模型最早由 McDermott 提出,该模型的提出是为了更好地共享安全知识。

3.2.1 Petri Net 简介

Petri Net 是对离散并行系统的数学表示,是一种网状图形表示的系统建模方法。

Petri Net 由四种不同元素组成: 区域(Place) 用 “○ ”表示; 转换(Transition) 用 “| ”表示; 连接 Place 和 Transition 的有向弧(Arcs) 又分为输入和输出有向弧,输入 Arcs 从 Place 指向 Transition,输出 Arcs 从 Transition 指向 Place; 位于 Place 中的令牌(Token) 用 “ ”表示。Place 表示系统状态的逻辑描述,可拥有任意数量的令牌,令牌数量标志系统当前状态。Transition 表示系统中事件或行为的产生过程。如果每个输入区域都拥有令牌,转换即被允许。发生转换时输入区域的令牌被消耗,同时为输出区域产生令牌。图 2 为一个 Petri Net 的例子。

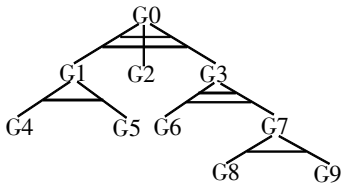

图 1 Attack Tree

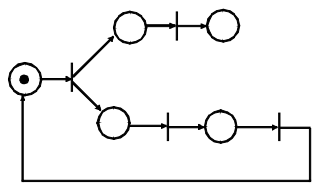
图 2 Petri Net

3.2.2 Attack Net 攻击模型

Attack Net 攻击模型是基于 Petri Net 的模型,使用 Petri Net 的 Place 表示攻击的阶段, Transition 表示攻击行为,攻击过程由 Petri Net 中的路径表示,如图 3 所示。

Attack Net 相比 Attack Tree 易于扩展,增加节点可以不改变原有结构。在图 3 的例子中,要将社交工程作为攻击者获取密码的一个选择(OR - 条件) ,可以添加一个新的 Transition 到 Knowledge of Password 节点。AND - 条件则可通过将新的 Place 附加到一个 Transition 上, 如添加一个新节点 Hashes in / etc / password 到 Brute-force Guess Password 这个 Transition 上。在最基本的 Petri Net 中,令牌之间不可区分,在更复杂 Petri Net 中增加了令牌着色,进一步增强了 Attack Net 的描述能力。

由于 Petri Net 是一个强有力的数学建模工具,适于在大型、复杂系统的模型应用中描述和分析异步、并发和资源竞争等问题,具有强大的建模能力。因此基于 Petri Net 的 Attack Net 模型成为目前最适合描述协同攻击的模型。

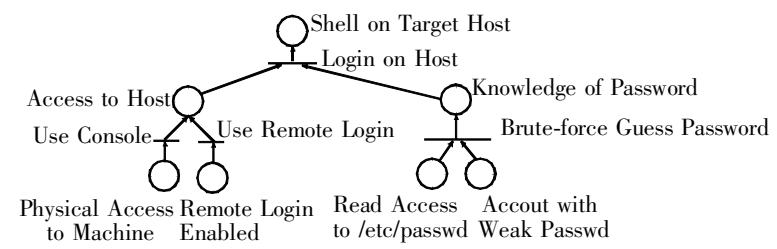

图 3 一个 Attack Net 的例子

3.2.3 基于 Wiki Web 的 Attack Net 攻击模型

Attack Net 适于描述协同攻击,基于 Wiki Web 的攻击模型是对它的一种扩展实现。

(1) Wiki Web 简介

Wiki Web 是一种超文本系统,与普通网页的区别在于: 拥有权限的用户通过浏览器就可任意浏览、创建、更改 Wiki 网页,发布的代价也远比 HTML 文本要小。每个 Wiki 页面都被唯一的 Wiki Name 所标志,系统自动将 Wiki Name 描述成超链接。

(2) 基于 Wiki Web 的 Attack Net 攻击模型

基于 Wiki Web 的 Attack Net 攻击模型将 Wiki Web 技术与 Attack Net 结合,引入前提、后果和上下文的概念。该模型的两个主要元素是条件(Condition) 和转换(Transition) 。Condition 与 Attack Net 中的 Place 对应,描述系统属性或攻击者的能力。Transition 由前提(Precondition) 和后果(Postcondition) 定义,与 Attack Net 中的 Transition 对应,语义是一致的,描述使一组前提集合向指定后果集合的转换,即只有前提集合中的所有前提都满足了,向后果集合的转换才能进行。模型中 Condition 和 Transition 都由特定的 Wiki 页面实现, Attack Net 中的 Arcs 则用 Wiki 页面间的超链接实现。

将 Wiki 页面与 Condition 和 Transition 结合的好处在于: Wiki 页面可包含结构自由地描述,包括详细的背景信息、代码例子或其他有价值的信息。每个 Condition 和 Transition 可用 Wiki Name 标志或引用,这样, Condition 和 Transition 可以从网络内部、从普通 Wiki 页面甚至 Wiki Web 外部被超链接连接起来。

为使模型在适用于大范围环境的同时也能适用于特定系统,又引入了上下文(Context) 的概念,意义在于: 有助于信息分类和过滤无关信息。Condition 和 Transition 不是所有情况下都有意义,所以应该置于特定上下文中。模型中的 Context 概念是基于多继承机制的。Context 使用特定类型的 Wiki 页面表示,内容包括对 Context 自身的描述和对所继承 Context 的引用。此处继承的语义是,与一个 Context 相关的页面也与继承它的 Context 相关。继承机制的引入使得不同抽象级别的信息能够联系起来。

如下是图 3 例子中一个 Transition (Brute-force Guess Password) 在基于 Wiki Web 的 Attack Net 模型中的表示。其中 [- > . . .] 表示模型中的超链接:

Name: Brute-force guess password

Preconditions: [- > read access to /etc/passwd] , [- > account with weak password]

Postconditions: [- > knowledge of password]

Context: [- > UNIX-like system] , [- > Linux system] : most modern Linux systems use shadow passwords, so /etc/passwd does not contain password hashes.

Descriptions: A password can be guessed if it is included in a reasonably small search space, such as all combinations of lowercase letters or lists of English words or names. See [- > account with weak password] for more cases of weak passwords.

If the hash value of the password is known, an attacker can do the password guessing off-line by generating a hash value of each candidate in the search space and comparing it with the known hash .

3.3　基于系统状态集合的攻击模型

设计攻击模型的最终目的是进行攻击检测和安全预警。攻击检测和安全预警要求将攻击行为和对系统状态所造成的影响区分开来。另外, 安全预警与系统的安全需求紧密相关。基于系统状态集合的攻击模型是针对攻击检测和安全预警的要求提出的。

3.3.1　基于系统状态集合的攻击模型

基于系统状态集合的攻击模型侧重于描述攻击的整个过程而不是其中的某个行为。

攻击行为都有一个共同特点: 行为发生前系统处于某种状态, 发生后系统状态必定会发生变化。如果系统状态没有发生变化, 就意味着系统未受任何影响。实际上, 对系统没有影响的行为是不需要关心, 也是难以甚至不能检测的。基于系统状态集合的攻击模型是建立在攻击行为造成系统状态改变的前提之上的。

将系统状态定义为 s(host, describe, risk) 。其中, Host 为系统状态涉及的主机集合; Describe 为系统状态的文字描述; Risk 为表示系统状态危险等级的数字, 取决于系统状态本身对安全的危害程度和系统对安全的需求。根据状态本身的危险程度, 给每个系统状态的 Risk 赋一个缺省值 d。系统状态与安全需求无关时 $s.\ \text{risk} = d$, 否则由安全需求 r 决定系统状态的危险等级 $s.\ \text{risk} = \max(r_1, r_2, \ldots, r_m)\ (r_1 + r_2 + \ldots + r_m \neq 0)$ 。

实际环境中系统往往不只处于一种状态, 系统危险等级应是所有状态危险等级的最大值。从预警角度可将系统抽象为系统状态集合和系统危险等级的二元组: sys(S, sys_risk) 。其中, S 为系统状态集合; sys_risk 为系统危险等级, 定义为 max ($s_1.\ \text{risk}, s_2.\ \text{risk}, \ldots, s_n.\ \text{risk}$) 。

攻击行为的发生必须满足一定前提条件: ①系统静态配置, 因为攻击行为一般是对特定系统特定版本的漏洞的利用; ②系统当前所处状态, 如果系统当前状态不满足攻击行为的要求则攻击行为不能发生。将攻击行为定义如下: Attack(PRE, S_0, S_{end}) 。其中, PRE 为系统静态配置; S_0 为攻击行为的初始状态集合, 只有 $\text{Attack}.S_0 \subseteq \text{sys}.S$ 时, 即系统当前状态满足攻击行为要求的初始状态时, 攻击行为才可能发生; S_{end} 为攻击行为完成的状态集合, 要求 $S_0 < S_{end}$, 这意味着不考虑对系统状态不产生影响的行为。此外, 对系统状态影响相同的攻击行为会被描述为同一种攻击行为, 因为它们具有相同的初始和完成状态。这两个特点使得基于系统状态集合的攻击模型能对纷繁复杂的攻击行为作适当归约。

可以看出, 攻击行为和系统状态集合间存在如下关系: $\text{sys}_i.S = \text{sys}_{i-1}.S + \text{attack}_i.S_{end}\ (1 \leq i \leq n)$ 。attack_i 是第 i 个攻击行为, sys_0 是初始系统, sys_i 是 attack_i 发生后的系统。

最后将攻击过程定义为如下序列: track (attack_1, attack_2, attack_3, . . . , attack_n) 。其中, $\text{attack}_i.S_0 \subseteq \text{sys}_{i-1}.S\ (1 \leq i \leq n)$, attack_i 是第 i 个攻击行为, sys_i 是 attack_i 发生后的系统, sys_0 是初始系统。攻击目的不同, 攻击过程可能包含不同的攻击行为; 同一攻击目的也可使用不同的攻击行为; 不同攻击行为可能具有相同起始状态和完成状态。正是由于攻击行为间的复杂关系导致了攻击过程的复杂多变。

3.3.2　在攻击检测和安全预警中的应用

常见入侵检测系统(IDS) 多是对具体攻击行为进行检测, 没有考虑攻击行为间的关联。应用基于系统状态集合的攻击模型的攻击检测将 IDS 检测到的攻击行为序列作为输入, 与攻击模型中的已知攻击行为序列相比较, 如果匹配成功, 说明该攻击过程正在进行, 从而实现攻击检测。进一步地根据模型中已知攻击过程和攻击者在该攻击过程中所处阶段, 可以预测攻击者下一步可能采取的行为从而实现安全预警。

4　几种攻击模型的比较

以上介绍的攻击模型都有各自的优势和适用领域, 也或多或少存在着不足。

Attack Tree 模型的优点是直观、易于理解, 具有实用性。但仍存在许多问题, 如攻击行为和结果都用节点表示, 不进行区分, 容易造成混乱; AND/OR 节点不适于频繁修改和扩展; 缺乏标准化描述语言; 另外, 根据 Attack Tree 可以进行怎样的分析, Attack Tree 应细化到什么程度, 都需要通过进一步研究将其规范化。相比 Attack Tree 模型, 基于 Petri Net 的 Attack Net 模型对攻击行为和结果进行了区分, 且更易于扩展, 增加节点可以不改变原有结构。Attack Net 的 Transition 同样能很好地表达 Attack Tree 中 AND/OR 节点所能表达的逻辑联系。而且 Petri Net 的图表示更适于直观地展现漏洞及其产生原因, 复杂 Petri 网中增加令牌着色后更增强了模型的描述能力。由于 Petri Net 强大的建模能力, 基于 Petri Net 的 Attack Net 模型成为目前最适合描述协同攻击的模型。然而, Attack Net 图表示很容易增长到无法在纸张上显示的大小。

基于 Wiki Web 的攻击模型是对 Attack Net 的一种扩展, 该模型的提出是为了更好地共享安全知识。Wiki 因使用方便及开放的特点, 适于在一个社群内共享某领域的知识, 这为专家和普通用户分享安全知识, 一起致力于建立和完善攻击模型提供了便利。模型的 Attack Net 层次结构有助于信息的组织和文档化, Condition 和 Context 有助于摈除无关信息, 使相关信息联系紧密。通过对漏洞进行归纳并转换为基本 Condition 和 Transition, 还可对漏洞及其产生机制有精确的了解。然而 Wiki 页面可能会遭到恶意破坏, 不过大量公共 Wiki Web 系统的运行证明了 Wiki Web 的可行性, 可以通过在技术和运行规则上做一些规范(如 IP 禁止、制定编辑规则等) 来维持系统正确性。当基于 Wiki Web 的攻击模型付诸应用时应该制定更严格

的约束规则以保证内容结构的完整一致。

Attack Tree 和 Attack Net 都侧重于描述攻击过程所包含的各种攻击行为之间的联系,没有将攻击行为和对系统状态所造成的影响区分开,也没有将攻击的危害与系统的安全要求结合起来,而安全预警是与具体系统的安全需求紧密相关的。因此 Attack Tree 和 Attack Net 不能直接应用于攻击检测和预警系统,需与其他技术相结合。基于系统状态集合的攻击模型则是针对攻击检测和安全预警的要求设计的,用系统状态集合改变的序列来表示攻击过程,有足够的能力描述攻击。通过上节的分析可知,当 IDS 检测到攻击行为后,利用基于系统状态集合的攻击模型,可以预测将会发生的攻击行为。同时,模型中系统状态的取值将系统安全需求考虑在内,为实现准确的安全预警提供了可能。

5 结束语

攻击模型帮助我们结构化描述攻击过程,利用已有的攻击行为研究结果,指导我们分析、识别攻击,进一步进行攻击过程检测和安全预警。

攻击模型的研究是一个较新的领域,本文介绍的几个现有攻击模型大多也处在理论研究阶段或试验阶段,还远未达到成熟和实用化的程度。一方面要继续研究新的攻击模型,另一方面要将已有模型标准化、应用化和工程化,并与其他技术相结合,如神经网络、遗传算法、模糊技术、专家系统等,以向自动化、智能化方向发展。尽管在技术上有许多未克服的难题,但正如攻击技术不断发展一样,攻击模型的研究也将会不断完善成熟。

参考文献:

[1] leg Sheyner, Somesh Jha, Joshua Haines, *et al*. Tools for Generating and Analyzing Attack Graphs [C]. Oakland, CA: Proceedings of the IEEE Symposium on Security and Privacy, 2002.

[2] T Tidwell, *et al*. Modeling Internet Attacks [C]. West Point, NY: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, 2001. 5-6.

[3] Andrew P Moore, Robert J Ellison, Richard C Linger. Attack Modeling for Information Security and Survivability[R]. CMU/SEI-2001-TN-001, Software Engineering Institute, 2001.

[4] Jan Steffan, Markus Schumacher. Collaborative Attack Modeling [C]. New York, USA: ACM Press, Proceedings of the 2002 ACM Symposium on Applied Computing (SAC), Madrid, Spain, 2002. 253-259.

作者简介:

陈春霞(1979-),女,硕士,主要研究方向为计算机网络安全;黄皓,教授,博士生导师,主要研究方向为安全信息系统。

(上接第 110 页)

企业的自评估活动是一个动态的过程,随着企业的发展,需要不断地进行自评估,以此来满足企业的安全需求。当再次进行自评估的时候,评估人员应该以先前评估的结果作为本次评估的起始点,这些结果具有重要的参考价值,可以提高下次评估的效率。

3.2 该流程的评价

在第 3.1 节里,我们对该流程具体实施的一些要点进行了分析。与他评估相比,企业的信息安全风险的自评估在具体的应用过程中增加了一些额外的实施内容,如评估时机的选择、评估人员的确定等。同时,考虑到企业自身评估能力的欠缺,在某些步骤如资产、威胁、脆弱点的评估上进行了简化,提高了评估的效率,但是,这并不会过分地降低评估的效果。这些都充分地考虑了企业自评估的实际情况,为该流程的实际应用打下了坚实的基础。而且该流程符合通常的评估习惯,步骤比较清晰,容易被企业接受,内部人员能够较快地理解该流程,进而尽早地入手评估工作。

4 结束语

风险评估作为企业信息安全管理的第一步,它的评估结果直接影响着整个安全管理的质量。由于评估的各个要素又是处于不断变化之中,所以及时了解企业的安全状态是十分必要的,而定期的自评估是达到目的的必不可少的手段。本文首先分析企业信息安全风险评估的两种模式,即自评估和他评估,指出了它们的优缺点;然后讨论企业自评估的评估要素和评估原则;最后为企业自评估设计了一个实施流程,对该流程的各个环节进行了较为深入的分析,并对该流程进行评价,希望对读者和相关人员有所帮助。当然,风险评估本身存在一些问题,如评估方法的选择、风险计算采用的方式、资产价值的估算等在自评估中仍然会存在,这些都需要我们进行进一步的分析与研究。

参考文献:

[1] ode of Practice for Information Security Management[S]. ISO/IEC 17799, 2000.

[2] Information Technology-Guidelines for the Management of IT Security [S]. ISO/IEC 13335, 1997.

[3] Information Security Risk Assessment-Practices of Leading Organizations[R]. U. S. General Accounting Office, 1999.

[4] Christopher Alberts, Audrey Dorofee. Managing Information Security Risks: The OCTAVE Approach[M]. Addison Wesley Inc., 2002.

[5] Thomas R Pelitier. Information Security Risk Analysis[M]. Rothstein Associates Inc., 2001.

[6] Yacov Y Haimes. Risk Modeling, Assessment and Management[M]. Wiley & Sons Inc., 2002.

[7] Gary Stoneburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems[R]. NIST SP800-30, 2001.

[8] Mariane Wanson. Security Self-Assessment Guide for Information Technology System[R]. NIST SP800-26, 2001.

[9] 科飞管理咨询公司. 信息安全管理概论——BS7799 理解与实施[M]. 北京: 机械工业出版社, 2002.

作者简介:

许诚(1979-),男,安徽宿州人,硕士研究生,主要研究方向为网络管理与安全、信息安全;张玉清(1966-),男,副研究员,主要研究方向为信息与网络安全;雷震甲(1944-),男,副教授,主要研究方向为网络管理与安全。