虚拟网络攻防分析模型

郭春霞[1],刘增良[2],陶 源[1],张智南[1]
GUO Chun-xia[1],LIU Zeng-liang[2],TAO Yuan[1],ZHANG Zhi-nan[1]

1.北京科技大学 信息工程学院,北京 100083
2.国防大学 信息安全实验室,北京 100091
1.College of Information Engineering,University of Science and Technology Beijing,Beijing 100083,China
2.Information Security Laboratory of National Defense Academy,Beijing 100091,China
E-mail:gcxmq@yahoo.com.cn

GUO Chun-xia,LIU Zeng-liang,TAO Yuan,et al.Virtual Internet offensive and defensive analysis model.Computer Engineering and Applications,2008,44(25):100-103.

Abstract: Virtual network attack and defense training platform is an effective means of training for information security personnel.The article deals with the design on components thinking,with which kinds of simulators,structure components and mission control components are modeled.This paper also presents an interactive mode in support of the synergy between component models.The training practice verifies that the model can provide a better method for information security education.
Key words: information security education;offensive and defensive analysis model;simulator component

摘 要:虚拟网络攻防训练平台是进行信息安全人员训练的有效手段,在进行攻防过程分析研究的基础上,提出网络攻防过程分析模型,采用构件化思想进行攻防对象模拟器构件的设计,并对攻防结构构件和攻防任务控制构件进行建模,保证构件在交互模式支持下完成构件模型的协同特性,最后对模型进行了实践验证。
关键词:信息安全教育;攻防分析模型;模拟器构件
DOI:10.3778/j.issn.1002-8331.2008.25.031 **文章编号:**1002-8331(2008)25-0100-04 **文献标识码:**A **中图分类号:**TP393

信息安全面临的严峻形势催生了人才培训需求,但由于网络技术发展周期不断缩短,而安全训练不但需要与外界不断进行交互,而且需要规律的数据采集和随机安全干预,加上训练过程本身带有破坏性,一旦训练与技术发展脱节,效果会变得很差。针对军队、信息安全应急响应组织等特殊需求单位的需要,国内外安全研究单位和教育机构已经进行了努力,从实际调查和文献调研的结果分析,目前存在少量的模拟环境和实战训练方式[1,4-5],但由于训练设备正常运行所需的后续资金、人员、知识投入的不足,在规模和成效上都存在难以为继的问题。

根据我国的实际情况,国防大学信息安全实验室研制了虚拟网络攻防训练平台,本文着重对其中的基于构件化的虚拟网络攻防过程分析模型进行阐述。模型对网络攻击和防御技术进行虚拟构件化处理,这有利于将攻防知识从训练平台实现中分离出来,方便系统建模和软件设计,从整体上加速模型演化和系统实现。此外,网络攻防技术的构件化处理形成了一系列的类模拟器和个体模拟器,通过规范攻防构件模拟器之间的交互行为特征,为攻防过程提供灵活的粒度变化,根据攻防复杂程度的区别建立粒度大小不一的模拟器构件链,达到对网络攻防的过程进行分析、显示和逆向重组的目的。

本文的组织结构如下:首先介绍了一些相关的工作,指出网络攻防过程分析模型的意义; 然后描述虚拟攻防过程分析模型,包括构件化的建模方法、攻防对象系统的描述和攻防过程分析模式和实践应用, 最后对全文进行总结并给出下一步的工作。

1 相关工作

计算机网络攻防训练问题,实质上是一个如何把网上数字化智能对抗过程和攻防中的一切推理判断、思维和表述,转化为参训人员所能理解的知识来实现,也就是抽象并建立一个与现实等价对应的网络攻防知识系统。信息安全领域知识爆炸性增长的特点暴露了传统信息安全教育的低效,而社会约束力不允许把训练课堂搬到互联网上。因此,如何把网络攻防过程进行分析模拟是实现有效训练的关键技术问题之一。

在网络攻防对抗领域中最引人注目的研究是针对网络攻击所进行的,从互联网推广应用的那一天起,美国就陆续发展了一批官方和民间的组织,比如联邦调查局属下的 NIPC、CIAC(计算机事故咨询小组)、CERT(计算机应急响应小组)和 COAST(计算机操作、审计和安全技术组),他们负责网络攻击

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60572162)。
作者简介:郭春霞(1974-),女,博士研究生,工程师,主要研究领域为信息安全,知识管理;刘增良(1958-),男,博士生导师,主要研究领域为人工智能,信息对抗;陶源,博士研究生,主要研究领域为仿真技术;张智南,博士研究生,主要研究领域为仿真技术。
收稿日期:2008-03-19 **修回日期:**2008-06-20

方法的研究并跟踪研究最新攻击技术，国际上每年举行一次FIRST(安全事故与响应小组论坛)会议,进行黑客攻击方法的最新进展研究和探讨。

与之对应的网络防御研究主要包括网络攻防体系、模型,信息隐藏与检测[2],信息分析与监控[3],应急响应,以及其他行业技术在攻防技术中的应用等。该方向的发展总体还处于初级阶段，各类理论与技术的研究基本上都还处于百家争鸣的状态。与之相似的建设在20世纪70年代和80年代的美军单一系统建设中曾经出现过[7-8],各自独立的系统在飞速发展的信息技术面前很快过时,造成巨大浪费。虽然各国都希望吸取教训,但技术发展自身的节奏和各方利益均衡使得浪费似乎不可避免,所以,在网络安全建设中,雷同的局面不断出现就不足为奇了。

现实世界中的网络攻防系统,其构成一般由各种不同的子系统、属性及其相互关系构成,对这些要素的理解程度决定了网络攻防知识系统的性能。本文提出的虚拟网络攻防过程分析模型的原型开发借鉴了梅宏等人基于体系结构的构件开发方法的优点,在平台知识的组织上采纳了刘增良教授的因素神经网络框架思想[9],将现实世界中的网络攻防行为抽象为一个虚拟网络攻防训练平台,并进行攻防对象构件化模拟处理,在平台训练真实感的同时保证了模拟器开发的独立性、复用性和平台模拟内容的可拓展性,从而保障了训练的与时俱进。

2　基于构件化的虚拟网络攻防分析模型

2.1　虚拟攻防系统的形式化描述

设 U 为所考虑的论域,SA 是所考虑的虚拟攻防系统,与现实世界中的网络攻防系统一样,虚拟攻防系统也由一些不同种类的子系统、属性及其相互关系所构成,依据所认知与描述的角度不同,其表达方式会有所变化,一般性地,可用($SA=\{ds, as, fs, ys | ds\in D, as\in A, fs\in F, ys\in Y, s\in S\}<s>$)来表达虚拟攻防系统 SA,其中 $S=\{s\}$为各种认知与描述观点的集合,s 为一种认知或描述观点;$A=\{as\}$为系统行为事物构件集合,as 为系统中可认知的行为事物构件,它包括各类可感知事物,各类功能行为体以及各类软硬件行为等;$D=\{ds\}$为系统的结构构件集合,它表达的是系统中各类行为事物之间的关系模式。包括时空状态关系模式，行为模式、状态转换关系模式及约束条件等;$F=\{fs\}$为系统认知与描述因素集合;$Y=\{ys\}$为系统的各种功能状态。

为了认知并表达虚拟网络攻防系统 SA,需要对 SA 进行各种归纳与抽象,比如,将一系列具有相同特征,服从和遵守相同规则的具体行为事物抽象成一个认知“对象”。将类似实体所具有的某些具体特性抽象成一个共同的描述因素,并将具体网络攻防行为事物在描述因素方面的表现看作是描述因素的一种状态。这些对象在技术上映射就是颗粒度大小不一的构件,描述因素状态的变化映射为构件的接口参数变化。

在平台内容规划上,需要根据某种观点对系统的行为事物进行分类,表现在论域 U 内,就是选定一种认知(或描述)观点 s 并依据 s 将 as 依据一种“等价关系”进行归类划分。

定义 1　设 A 是一个事物构件集合,R 是 A 上的一个关系,称在 s 观点下 R 为 A 上的一个等价关系,若在 s 观点下,对 $x, y, z\in A$,$R(s)$满足

(1)自反性:$xR(s)x$;

(2)对称性:若 $xR(s)y$,则 $yR(x)x$;

(3)传递性:若 $xR(s)y, yR(x)z$,则 $xR(s)z$。在 s 观点下,A 上的等价关系 $R(s)$通常记为$(x)R(s)(y)$或$(x)\frac{R(s)}{}(y)$,$(x, y\in A)$。

定义 2　称 o 为 A 中在等价关系 $R(s)$下的一个等价类,若 $a\in A$,$o=\{y|(y)R(s)(a)\}$。

定义 3　若 o 为 A 中在等价关系 $R(s)$下的一个等价类,则称 o 为系统 SA 在 s 观点下的一个抽象对象。令 $O=\{o|o$ 为 SA 在 s 观点下的对象$\}$。则 O 为系统 SA 在 s 观点下的对象集合。

定义 4　设 A_i 是 A 的子集,若有 $A=\cup A_i$,则$\{A_i\}$称为 A 的一个划分层次;若还有 $A_\alpha\cap A_\beta=\Phi(\alpha\neq\beta, A_\alpha, A_\beta\in A)$,则$\{A_i\}$称为 A 的一个确定性划分。

系统中对象的划分反映了人对事物的一种认知与描述观点。这种观点根据所考虑问题的层次与角度对对象进行粒度粗细不同程度划分。

定义 5　设 $R(s_1), R(s_2)$为集合 A 上的两种不同对象划分的等价关系,若有$(x)R(s_1)(y)\rightarrow(x)R(s_2)(y)$,则称 $R(s_1)$比 $R(s_2)$细,记作 $R(s_1)<<R(s_2)$。

根据 SA 中对象划分程度的不同,各对象构件之间的相互关系、构件协同方式以及构件执行后系统状态也会发生相应的变化。采用颗粒度大小不等的构件组合的目的,主要为了根据对攻防训练研究和分析问题角度和目的不同找到最佳的功能组合和表现形式,生成各种不同的认知与描述模型。由于这些认知和描述模型反映的是同一个训练系统,所以它们之间一定存在着某些共同的特性,我们希望这些颗粒度大小不同的构件间存在以下关系:

(1)这些构件模型具有某种层次关系。

(2)在同层次上由不同侧面所获得的各个模型可以合并成一个综合模型。

(3)不同层次模型间的性质具有某种保持性。比如,若原系统为拓扑结构，则其拓扑性质在不同层次模型中应保持不变,若原系统为偏序结构,则其各个模型也应具有此偏序性。

定义 6　称 $M=<<O, G>, F, X>$为 SA 在 s 观点下的一个认知或描述模型。

若 $O=\{o\}$<称为 M 中的对象构件集合>

O 为 SA 中行为事物在 s 观点下等价聚类的对象构件

$G=\{g\}$<称为 M 的交互模式>

g 为 SA 中行为事物关系 d 在 s 观点下的等价转换

$F=\{f\}$<称为 M 中的认知或描述因素集合>

f 为 SA 在 S 观点下,以 f_o 为基础选用的认知与描述因素

$X=\{x\}$<称为的因素表达状态集合>

x 为 SA 在 s 观点下选用 F 做表达因素时反映出来的系统状态

定义 7　设 $SA=(<A, D>, f_o, Y)$是一个虚拟攻防系统,对 A',A 具有性质 H。若在 s 观点下,由 SA 所获得的系统模型 $M=<<O, G>, F, X>$,使 $s: A'\rightarrow s(A')\in M$，$s(A')$也具有性质 H,则称 M 为 SA 的保有性质 H 的模型。

定义 8　设 s_1, s_2 为两种不同的认知与描述观点，对于系统 SA,分别抽象出认知与描述模型 $M_1=<<O_1, G_1>, F_1, X_1>$及 $M_2=<<O_2, G_2>, F_2, X_2>$,若令 $s_3=s_1\odot s_2$ 为 s_1, s_2 的综合,则 $M_3=M_1\odot M_2=<<O_3, G_3>, F_3, X_3>=<<O_1\odot O_2, G_1\odot G_2>F_1\odot F_2, X_1\odot X_2>$称 M_1, M_2 为的综合。这里,$\odot$表示综合运算,它确定一种等价关系 R,对 $\forall x, y\in A$,$(x)R(s_1\odot s_2)(y)\leftrightarrow(x)R(s_3)(y)$。

2.2 攻防模拟器构件的定义和描述

在网络攻防过程分析模型中,模拟器构件作为是一个被调用和执行的单元,其效能和准确性只能在特定应用模型运行时才能确定,与面向对象方法将控制流直接从一个对象传递给另一个对象的方法调用不同的是,构件集成的正确性取决于应用的设计能力。在网络攻防训练过程中,将模拟器构件间的交互抽象为根据不同应用效果需要的任务认知模型,提供构件的联系和交互模式,其形式化描述可表达为 $M=<<O,G>,F,X>$,$G=<In,C,Func,Out>$。

C 为攻击和防御模拟器构件的集合,是个可以在特定环境下自行运行和检验的独立单元,其有效性和效果的表现取决于外部状态(端口,背景)和内部参数的设定,它不需要引用其他构件来定义自身的活动,但可以与其它构件联动。在形式上,一个模拟器构件是一个效果模型集合的子集或独立元素,其形式化描述可表达为 $C=<P,TP,D,R>$,C 为构件集合,P 代表端口集合,T 为类型标识集合,D 表示网络攻击的危害或防御的有效程度集合标识,R 为预定响应标识集合。端口描述 P_C 包含了构件的运行有效性条件如系统、协议和漏洞,TP_C 定义了模拟器构件的类型标识,比如攻击技术的远程控制类,或是防御工具的协议过滤类等,D_C 根据 B 类安全标准设置攻击危害程度和防御的有效程度标识,R_C 定义了构件功能执行的各类结果标识。之所以在构件形式化描述中采用标示集合而非事实描述,其作用在于保持构件可以依托虚拟系统知识库进行知识更新,使得在信息安全技术产生条件和响应时变性条件下保证每一个模拟器构件的应用有效性。每一个独立的构件单元内部都包含了独立的输入($P_{c_{in}}$)/输出端口($P_{c_{out}}$),输入条件和构件参数选择决定输出端口的反应。端口值由交互环境更新,构件只更新参数部分。

$Func$ 为任务调度函数集合{$func$},$func$ 可以采用任意编程语言实现,可以看作调度构件或构件集合,其任务是根据需求 In_t 和效果搜索出适合条件的构件形成构件组,运行结果 Out_t 和终止受虚拟训练平台用户控制。需求集和结果集在本虚拟平台中以数据表形式存在,可以同时为多个用户所调用。

2.3 攻防对抗任务设计模式定义和描述

攻防对抗任务设计模式用于描述系统中的不同元素之间如何协同完成一类或一个对抗训练任务。在虚拟攻防训练平台中,针对特定环境下某个问题的解决策略,给定攻击战术所必须采用的技术和防御战术技术,进行双方对抗,这种训练方式不但策略可以反复应用,而且各种虚拟训练场景和技术也可以反复被多人同时应用,这是构件化虚拟训练平台的最大优势。在模拟器构件形式下,一类构件间的重要行为特征,比如攻防时序特征和空间转移行为依赖于构件间的交互特性,即某类构件相对于系统中其他构件透明的外部接口表现,把这种交互行为规范定义为任务设计模式,满足对抗任务模型对不同构件粒度的控制特性,从而保证对抗过程需求控制的有效性,以及一组构件特性集成映射为攻防时序流特性的可行性。

任务设计模式规定构件运行环境转换、构件交互权限控制和使用通道。从参训者角度,设计模式为他们提供了一类攻防任务所需构件的前提条件、参考策略和任务目标,任务的完成情况由下面的过程分析模型给出,参训者的任务执行能力视个人对任务的理解程度、技术娴熟程度而定。形式上,虚拟攻防训练平台中的一个任务设计模式 TM 是一个转换系统 $TM=(\Sigma,\Lambda,\Gamma,\Omega)$,$\Omega$ 是模式初始状态的集合;Σ 是任务设计模式的状态集合;Λ 是任务设计模式的权限控制集合;$\Gamma=(\sigma_1,\lambda,\sigma_2)$代表构件的特征状态过程集合。

2.4 攻防分析模型

攻防过程分析模型的作用在于把任务模型在不同任务设计模式下形成的交互构件网络进行时序事件提取、分析和综合,使得教师可以通过分析模型了解参训者的训练表现和技能掌握程度,为后续的训练思路提供帮助。分析过程包括了虚拟数据捕获、分析和结果总结三个阶段。一般来讲,攻击过程分析模型的主要任务如下:

(1)捕获可以构成一个攻击或防御工作环境的对象及其认知与表达,以及对象状态转换的交换模式与功能状态;

(2)搜集信息处理知识,从任务模型和交换模式中搜索能进行特定信息控制与转换活动的规则,并指定冲突解决方法;

(3)按一定的结构构件控制策略执行基于规则的推理活动,搜索或生成过程分析的部分或全部解答;

(4)根据攻防过程的事件表达进行问题归约,根据时序确定事件执行顺序和逻辑关系;

(5)执行攻防过程还原回放操作。

任务认知模型 M 的行为控制分总体控制与本体控制两部分。总体控制决定根据任务分配执行策略进行构件协同,以推进任务目标的求解和协调各构件的相互关系。而本体控制的任务设计模式以完成个体构件所分配的任务为主要目的。个体构件在任务模型中所起的作用主要有下述几种:

(1)检测是否满足自身激活条件,以决定是否激活参数设置和功能状态变化;

(2)检测交互模式信息以决定是否执行相关功能活动;

(3)指示构件单元选用的交互模式(包括正向、逆向等);

(4)指示构件单元选用的协同规则,并指定子任务调度策略;

(5)提供构件调度控制的过程信息等。

为了进一步说明上述过程,设想一个多层次攻击构件组合体的运行过程。以总的对象构件为基础,以命题形式来描述有关构件和构件间的关联关系。其形式为$<C,F,Xo(F)>$,以关系模式$(RM,XM,<C,F,Xo(f)>)$来表达构件的过程控制行为等。关系模式通常可显式地表达为一组模块化的断言集合 $e:-c_1:r_1;-c_2:r_2;\cdots-c_m:r_m;-\text{otherwise}:r_{m+1}$。这里 $c_i=\{c_{i1},c_{i2},\cdots,c_{ik}\}$,其说明性解释为

如果条件 $c_1,\cdots,c_{i-1}$ 都不满足,c_i 满足,则 e 等于 r_i;

如果 $c_1,\cdots,c_m$ 都不满足 e 等于(或就是)r_{m+1}。其过程性可解释为:

如果条件 $c_1,\cdots,c_{i-1}$ 都不满足,c_i 满足,则 e 的执行归结为方法 r_i 的执行;

如果 $c_1,\cdots,c_m$ 都不满足,则 e 的执行归结为 r_{m+1} 的执行。

根据上述构件化的攻防分析模型,其攻防行为执行过程可以叙述如下:

第一步:根据对攻击的认知和观点产生意图集合,预测可能的攻击目标集合及攻击期望效果;

第二步:从目标集合任选单个目标,拟定攻击方案;

第三步:根据掌握的单个目标信息,进行攻击目标的分解;

第四步:如果一个攻击操作已经完成,则生成以该目标为

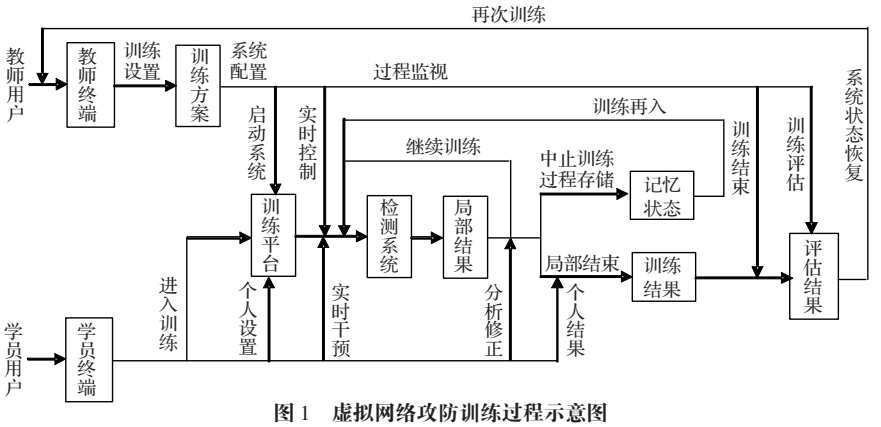

图 1　虚拟网络攻防训练过程示意图

基础的攻击任务;

第五步:如果单个目标无法一次性实现,则进行目标再分解,直至实现所有子目标的任务;

第六步:子目标合并,形成目标攻击任务;

第七步:返回第二步,直至所有攻击目标集合执行完毕;

第八步:整体攻击任务输出。

3　实验验证

根据网络攻防过程分析模型,在实验室开发的虚拟网络攻防训练系统原型上,利用 2 000 个漏洞、55 个经典攻防模拟器、7 种操作系统和 15 个漏洞修复模拟为基础进行了实验验证,利用攻防想定对 3 批共 64 名学习安全专业的人员进行训练,训练过程如图 1 所示。

从实验结果看,这种攻防过程分析模型可以清晰地显示和分析每个学员的训练过程, 并且可以对整个过程实行回放,对于学员的准确能力定位和个性化训练内容调整效果很好,在个体与技能一对一训练中成效比较大。但在进行协同攻防过程中,粒度大小不一的模拟器构件链的组成与攻防想定理解定位上存在误差,主要问题在于语义理解和模拟器重组标识之间还没有实现模糊匹配,这是下一步待改进的地方。

4　结论

本文探讨了一种把网上数字化智能对抗过程转化为参训人员所能理解的可见训练平台的研究方法,强调采用构件化思想设计出攻防对象模拟器构件、攻防结构构件和攻防任务控制构件的建模方法,保证构件间交互局部化,并在交互模式支持下完成构件模型的协同特性。我们已经在模型的基础上实现了一个虚拟网络攻防训练原型系统,并在几个单位进行了实践验证,反馈的信息表明把构件化建模设计方法、数据库技术和攻防知识相结合具有可行性、灵活性和拓展性。在此基础上,我们继续研究把知识增长机理与构件组织模型相关联,以期形成可以进行个性化定制的复杂虚拟训练方式。

参考文献:

[1] Ragsdale D J,Surdu J R,Carver C A.Information assurance education through active learning[R].The IWAR Laboratory,2002.

[2] de Vivo M,de Vivo G O,Isern G.Internet security attacks at the basic levels[J].Operating Systems Review,2002,32(2).

[3] Teo L,Zheng Y,Ahn G.Intrusion detection force:an infrastructure for internet-scale intrusion detection[C]//Proceedings of the First IEEE International Workshop on Information Assurance (IWIA'03),Darmstadt,Germany,2003:73-91.

[4] 李志勇,刘锋,孙晓燕.网络对抗实验平台构建[J].实验技术与管理,2004,21(5).

[5] 裴斐,郑秋生,郭基凤,等.网络攻防训练平台设计[J].中原工学院学报,2004(1).

[6] 梅宏,陈锋,冯耀东,等.ABC:基于软件体系结构、面向构件的软件开发方法[J].软件学报,2003,14(4).

[7] 冯忠国,赵小松.美军网络中心战[M].北京:国防大学出版社,2004.

[8] 郑连清,刘增良,吴耀光.战场网络战[M].北京:军事科学出版社,2002.

[9] 刘增良,刘有才.因素神经网络理论及实现策略研究[M].北京:北京师范大学出版社,1992.

(上接 99 页)

[3] 王永才,赵千川,郑大钟.传感器网络自身定位方法的设计与实现[J].计算机工程与应用,2005,41(13):4-6.

[4] Cheng Xiuzhen,Thaeler,Xue Guoliang,et al.TPS:a time-based positioning scheme for outdoor wireless sensor networks[C]//IEEE INFOCOM'2004.Hong Kong,China,2004:2685-2696.

[5] He Tian,Huang Chengdu,Blum B M,et al.Range-free localization schemes in large scale sensor networks[C]//Proceedings of the 9th Annual International Conference on Mobile Computing and Networking,San Diego,California,USA.ACM Press,2003:81-95.

[6] Liu Chong,Wu Kui.Performance evaluation of range-free localization methods for wireless sensor metworks[D].Computer Science Dept,University of Victoria BC,Canada,2005.

[7] 蒋小兰.无需测距的 WSN 节点自定位算法研究[D].成都:西南交通大学,2007.

[8] 邓平,李莉,范平志.一种 TDOA/TOA 混合定位算法及其性能分析[J].电波科学学报,2002,17(6).