基于智能规划的多步攻击场景识别算法

胡 亮[1,4],解男男[1],努尔布力[2],刘志宇[3],柴 胜[1,4]
(1.吉林大学 计算机科学与技术学院,吉林长春,130012;2.新疆大学信息科学与工程学院,新疆乌鲁木齐,830046;
3.公安部第一研究所,北京,100048;4.吉林大学符号计算与知识工程教育部重点实验室,吉林长春 130012)

摘 要: 多步攻击的识别过程与智能规划的求解过程具有一定的对应性.提出了一种基于智能规划的多步攻击识别模型,将智能规划的方法应用于多步攻击识别的领域,并以此为基础实现相应的识别算法.采用DARPA数据集进行实验,这种算法在多步攻击识别领域,具有较好的有效性和可行性,能够达到可接受的准确率和完备率.

关键词: 多步攻击; 智能规划; 攻击场景识别
中图分类号: TP393.0 **文献标识码:** A **文章编号:** 0372-2112 (2013) 09-1753-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.09.013

A Multi-Stage Attack Scenario Recognition Algorithm Based on Intelligent Planning

HU Liang[1,4], XIE Nan-nan[1], Nurbol[2], LIU Zhi-yu[3], CHAI Sheng[1,4]
(1. *Computer Science and Technology College, Jilin University, Changchun, Jilin* 130012, *China*; 2. *Information Science and Engineering College, Xinjiang University, Urumqi, Xinjiang* 830046, *China*; 3. *The First Research Institute of the Ministry of Public Security of PRC, Beijing* 100048, *China*; 4. *Key Laboratory for Symbol Computation and Knowledge Engineering (Jilin University), Ministry of Education Changchun, Jilin* 130012, *China*)

Abstract: Multi-stage attacks recognize process have similar relationship with solving intelligent planning problems. Intelligent planning is used in multi-stage attacks recognition, in order to achieve the attack scenarios recognition. A multi-stage attack recognition model based on intelligent planning is proposed, and based on this, a multi-stage attack scenario recognition algorithm is realized. Experiments on DARPA datasets shows this algorithm have acceptable accuracy and completeness rate in multi-stage recognition.

Key words: multi-stage attack; intelligent planning; attack scenario recognition

1 引言

当前网络防御能力日益提升,仅仅依靠单步攻击即可完成入侵目的已经几乎不可能实现,多步攻击则成为目前网络攻击主要手段之一.据CNCERT/CC国家互联网应急中心2011年关于互联网的安全报告[1],将关于网络安全的攻击事件依照攻击类型分类,占总数90%以上属于多步攻击的范畴,一个完备的网络攻击计划往往是由一系列典型的单步攻击手段组合而成.针对政府及大中型企事业的多阶段、协作式攻击事件频繁发生,对网络安全造成巨大的威胁.高级持续威胁(Advanced Persistent Threat, APT)是近年来广泛被关注的一种典型复杂网络攻击,是针对特定目标的渗透性攻击手段,由多种攻击方式结合,通过多阶段、长时间的针对性攻击达到破坏的目的.因此通过单一的防护手段往往不能有效的进行检测和防御[2].

多步攻击过程一般是由多个相互关联的攻击步骤组成的,其中前一个步骤往往是后一个步骤发生的条件,因此更加难以检测.针对多步攻击难以检测的现状,研究者们提出了入侵警报关联和攻击场景构建等方法.目前,入侵检测领域存在的主要问题有警报数据缺乏一致性表示、各警报数据之间关联性较差、以及检测多步攻击的能力较差等方面.

智能规划最初是对行动路径的研究,比如机器人的行动路径,它始于20世纪60年代,并在七、八十年代获得了快速的发展[3].智能规划所应用的场合多为解决领域问题,其中规划域的概念就是针对不同的领域以不同的专家知识库作为指导.智能规划系统的运行方法在于

收稿日期:2013-01-14;修回日期:2013-03-22;责任编辑:梅志强
基金项目:国家重点基础研究发展计划(No.2009CB320706);国家高技术研究发展计划(No.2011AA010101);国家自然科学基金(No.61073009,No.61163052);新疆大学博士启动基金(No.BS110126)

通过专家知识库所提供的匹配规则,进行推理计算,找出使得状态得以转变的操作序列.

本文的工作将智能规划应用于与多步攻击场景识别领域,提出了一种基于智能规划的多步攻击识别模型,从流程化的角度对多步攻击场景识别进行建模,进而实现一种基于智能规划的多步攻击场景识别算法.本文工作是将智能规划方法应用于网络攻击入侵检测领域的探索,重点关注所提模型和算法的有效性与可行性,试验基于 DARPA 2000 数据,能够达到可接受的准确率和完备率.

2 多步攻击与智能规划

2.1 多步攻击

警报关联研究开始于 20 世纪 90 年代初,是主要研究针对多步攻击的解决方案.基于入侵检测系统的警报关联方法,从繁杂冗余的警报数据中抽丝剥茧,目标是提炼出入侵者的本质目标与动机所在.Jakobson 等提出了一种基于专家知识库的关联方法,然后将其用于网络安全事件管理的研究[4,5].Peng Ning 等提出了基于前因后果的警报关联方法,利用攻击间的依赖关系,是具有代表性的工作之一,但是需要大量的先验知识来确定攻击间的关系,并且依赖专家定义的关联规则[6].Xinzhou Qin 等提出基于统计的警报关联方法,利用时间序列模型,计算警报事件序列变量之间的 GCI 指数,对先验知识的需求较少,但对参数较多[7].梅海彬等基于动态规划的思想,提出了基于警报序列聚类的多步攻击模式发现方法,对先验知识的依赖少,需要设置的参数少[8].

现有的多步攻击呈现出了以下主要特性:

(1)攻击者所采取的手段多样化[9].例如,攻击者要获取主机的 root 权限,则可以通过包括利用数据库注入、主机相关服务漏洞、以及缓冲区溢出等多种方法达到目的.

(2)多个攻击步骤间相似度较低.攻击者由于要躲避入侵检测系统、防火墙等的防御工具,需要制定有计划性的攻击步骤,而由于每一步的目标不同,因此步骤间的相似度就较低.例如,攻击者先通过大范围的搜索网络锁定一台主机,接下来从网络中广泛搜集该主机的信息,通过这些信息进一步锁定与其关联的一系列主机,完成目标定位后,使用相关工具查找该目标的弱点及漏洞,最后利用这些缺陷施行具体攻击行为.

(3)攻击步骤间具有一定的顺序性.在一次完整的多步攻击中,各个攻击步骤目标明确,承前启后.各攻击步骤对应不同的攻击行为,在时间顺序上有先后性,也就是前一个攻击步骤的完结往往意味着下一个攻击步骤的开始.同时,有些攻击需在有限的时间段内完成,否则可能意味着结果的无效性甚至被有被发现的危险.

2.2 多步攻击建模和场景识别

多步攻击模型的建立是为了从关键性多步攻击行为角度出发,更真实的刻画出网络攻击的场景.目前的研究中,根据侧重点及角度的不同,有两类典型的建模方法,其一是基于状态的建模方法,其二是基于漏洞的建模方法[10~12].

(1)基于状态的多步攻击建模方法

这种方法的理论基础是确定有限状态自动机 DFA (Deterministic Finite Automation).DFA 表述系统每个状态,即正常安全状态、攻击开始状态、攻击进行中状态、攻击完成状态等,并给出各状态间完整详细的转换条件.这种方法通常定义一个包含状态集合、状态转换函数集合、状态转换中边集合、系统目标状态和系统初始状态的五元组,设定状态间的转换概率是确定.这种模型的优点在于确定了系统状态及转换函数后,描述系统各行为动作是明确清晰的[9].

(2)基于漏洞的多步攻击建模方法

无论是系统软件还是应用程序,漏洞与缺陷都是不可避免的.而这些由系统或者程序漏洞所暴露出的脆弱性,吸引着攻击者在此处实施多种入侵攻击行为.因此以漏洞为基础,建立多步攻击的模型也是一种典型的方法.这种模型常用攻击图描述,所谓攻击图是一种包含节点集和边集的有向图,其中,单个节点所表示的是系统的某个状态;每条边表示一个漏洞使得系统的状态发生了相应转变,如通过漏洞,攻击者实施对目标网络配置、访问权限等的修改.更进一步,节点集及边集在不同场合所描述的内容及能力可更改.

以上两种方法的描述能力都明确清晰,但是缺乏灵活性,随着网络攻击技术的发展进步,新的系统程序和应用软件的漏洞也会不断的出现,状态集合及相应转换条件也在不断变化,因此模型需要不停更新,因此后期的维护工作量较大.

Zhang Zonghua 等针对企业网络中的多步共谋攻击,提出了一种用于理解分析的模型 Janus[13].赖海光等提出了一种基于系统状态集合的攻击模型,对系统的安全状况进行抽象,用以评价系统的安全状态,并对可能发生的攻击行为进行预警[14].黄光球等基于双枝模糊决策和模糊 Petri 网为理论基础,定义了一种网络攻击模型 BBFPAN,直观的表示网络攻击的演变情况[15].

现有的 IDS 往往不具有必要的关联能力,警报信息层次相对较低,仅能检测单步的攻击或者攻击片段,难以发现复杂的多步攻击.对多步攻击步骤进行关联,从中提出对应的多步攻击场景,对攻击目的预测以及安全应急响应都有重要的意义.田志宏等提出了一种基

于全能转换模型的实时告警信息相关性分析的方法,从大量的低级入侵告警信息中构建高层次的攻击场景[16].郭山清等首先利用贝叶斯规则对报警信息进行过滤,在此基础上,根据可信的报警事件集完成攻击场景的重构,并且实现了报警事件的在线分析功能[17].孙雷等在分析基于因果关系关联方法的基础上,提出了一种攻击场景构建方法,基于系统漏洞和报警相关度,能够减少误报和漏报[18].Ahmadinejad SH 等提出了一种混合的警报关联模型,其中包含用于处理已知的攻击和未知攻击的两部分,同时更新攻击图[19].Liu zhijie 等提出了一种多步攻击警报关联和攻击场景构建的方法,是以攻击模式的模型为基础,通过 DARPA 数据集证明了算法的有效性[20].

2.3　多步攻击和智能规划

智能规划研究的往往是特定领域问题,由领域内专家将该领域所含知识描述成规划推理所用到的知识库即规划域,另一方面需向规划推理器输入在对应规划域上待求解的规划问题.因此,智能规划所需要具备的条件是规划域和规划问题,而多步攻击的识别的过程中,所需要具备的条件是知识库和攻击警报数据,其中,知识库的构建与规划域相对应,攻击警报数据与规划问题相对应,表 1 从阶段性、因果关系、序列化三个角度对比智能规划问题求解和多步攻击步骤识别的过程.

如表 1 中所示,智能规划问题的求解过程与多步攻击步骤的识别过程具有相似之处,因此,本文以智能规划的方法为基础,进行多步攻击场景的识别.

表 1　智能规划与多步攻击的对比

相同点	智能规划问题的求解	多步攻击步骤的识别
阶段性	规划问题通常通过将整个问题的求解划分成多个阶段,逐个击破,最终完成整体问题的求解	多步攻击本身既具有阶段性的特点,每步通过很多细节来实现该步攻击的目标,从而得到阶段性成果
因果关系	操作序列间的因果关系在于先求出的操作往往提供了下一步操作查找的一些必要条件	诸多攻击只有当前一步攻击完成后,才能占有足够的信息和资源,为下一步攻击提供准备
序列化	智能规划的解绝大多数都是依次执行的串行的操作序列	多步攻击的攻击步骤间为序列关系

3　基于智能规划的多步攻击模型

基于智能规划的多步攻击场景识别模型,如图 1 所示.

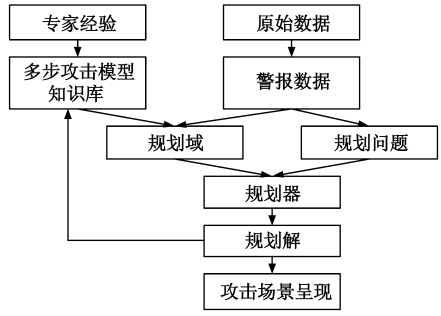


图1　识别模型框架图

在上述模型中,主要部分在于多步攻击规划域和规划问题的建立.对于规划域,先对多步攻击进行建模形成知识库,进而形成多步攻击规划域;对于规划问题部分,将原始警报数据采用中间警报数据格式进行处理,同时形成规划问题描述.模型主要分为以下部分:

(1)原始数据:通过入侵检测系统、审计等产生的警报记录,这些数据是初级的警报,不包含警报之间的联系.

(2)警报数据:经过预处理后的警报数据,由不同的入侵检测系统产生的警报数据,格式也是不同的,因此,初始的警报数据,需要经过规范化等处理,变成统一的数据格式.

(3)多步攻击模型知识库:针对不同的多步攻击,攻击过程都是明显不同,例如 DDoS 攻击,有不同的表现形式,这些不同的攻击过程需要分别建立对应的模型知识库,在模型中,当求出规划解后,可以据此更新或者优化知识库.

(4)规划域:参考多步攻击模型知识库和警报数据,采用规范化的描述语言,例如 PDDL,将多步攻击的过程进行知识表示,形成规划器使用的知识库.

(5)问题域:即规划问题,是待求解的问题描述,与规划域相对应,如果所描述的规划问题,在规划域中没有涉及,那么是无法求解的.

(6)规划器:是利用智能规划进行多步攻击识别的关联的核心,以规划域和问题域为核心,通过核心的智能方法,进行计算推理.

(7)规划解:规划器通过推理得出的结论,通常规划解是一些操作序列,求得的规划接通过评估,当规划域和模型知识库不完整时,可能出现不能得出规划解的情况,或者规划解并不好,此时需要对规划域和知识库进行优化.

(8)场景重现:由于规划解本身可能并不便于理解,因此需要对结果进行初步的处理,成为需要的呈现,针对多步攻击,就可以以场景呈现的方式.

4 多步攻击场景识别算法 MARP

4.1 算法描述

以上文的多步攻击识别模型为基础,提出基于智能规划的多步攻击场景识别算法 MARP(Multi-stage Attack Recognize Algorithm Based on Intelligent Planning).定义攻击模型知识库表示为 Knowledge_ M,原始数据为 Sourse_ D,警报数据 Alert_ D,规划域 Domain_ D,问题域集合 $P=\{P_1,P_2\cdots\cdots P_k\}$,其中 P_k 表示当前规划警报的问题 k,算法描述如下.

输入:经统一格式转换的警报数据.

输出:多步攻击场景识别序列.

Step1 根据专家经验将 Sourse_ D 进行冗余处理,生成 Alert_ D;

Step2 根据 Step1 产生的 Alert_ D,提取生成问题域集合 $P=\{P_1,P_2\cdots\cdots P_k\}$;

Step3 利用 Alert_ D 和选取的专家知识库攻击模型 Knowledge_ Mi,生成与当前攻击模型对应的规划域 Domain_ D;

Step4 选取 Step2 生成问题域集合 P 中的一个 P_i ($i=0\cdots\cdots k$)和 Domain_ D 输入到具体规划器,使用先前已内置的规划算法进行智能规划求解;

Step5 如果 Step4 中有解,则跳转到 Step6,否则跳转到 Step4 继续选取问题集合,如果问题域集合所有集合都已经取完,则跳转到 Step3,重新生成新的规划域继续计算.

Step6 输出多步攻击场景识别结果序列;

Step7 完成退出.

Step2 和 Step2 是将智能规划理论应用于多步攻击场景识别的关键所在,包含规划问题的生成过程及规划域的编写.Step4 到 Step6 则是应用智能规划实现多步攻击场景识别的流程.

4.2 实验环境

(1)规划器:规划器 FF v2.3

FF 规划器即 Fast Forward 规划器.它在 IPC-2000 的比赛中脱颖而出,求解用时短且更易于求出最优解.它结合启发式与图规划两种方法,同时作用于规划器的计算推理中.其首选采用加强型爬山算法进行问题的求解,计算速度较快但未必能得最终解.若未能完成求解,则采取最佳优先搜索算法,求解速度较慢但能保证求解的完备性.

(2)评估指标

评估入侵检测系统的指标众多,本文采用了入侵检测领域常用的两类指标,即准确率和完备率.有如下假设:测试数据集中的攻击事件总数为 A,利用本文识别算法确认为攻击的为 B,已确认攻击中真正包含在测试数据集的为 R.由此对于上述两类指标定义如下:

A:准确率:即描述方法的正确性,Accurate Rate = R/B.

B:完备率:即描述方法的完备性,Completeness Rate = R/A.

4.3 数据集

入侵检测领域中广为人知的 DARPA 数据集来自 MIT 下林肯实验室的信息系统技术小组 CSTG(Cyber Systems and Technology Group).是在美国空军研究实验室 AFRL 和先进防御研究项目机构的联合资助下,收集并发布的第一个用以评估网络入侵检测系统的标准数据集.DARPA 2000 数据集是在 DARPA 98 与 DARPA 99 基础上,加入多步攻击方面的内容形成的.其早已成为网络入侵检测领域事实上的标准测试数据集.DARPA 数据集在采集测试时的网络组成如表 2.

表 2 DARPA 数据集的网络组成

Network Type	Host	OS Type
Outside	14	Redhat, Solaris, SunOS, MacOS
DMZ	6	Redhat, Solaris
Inside	40	Redhat, Solaris, SunOS, MacOS, Windows

Darpa 数据集 LLDOS1.0 中多步攻击类型为拒绝服务攻击.攻击者主机 IP 为 202.77.162.213,通过探测 172.16.112.0/24、172.16.113.0/24、172.16.114.0/24 和 172.16.115.0/24 四个目标地址,搜寻在线主机,并定位已安装 Sadmind 远程管理工具的主机,利用此管理工具的漏洞来获取对应主机 root 权限,从而在其上安装攻击软件的服务器端及主控制端,并最终向目标主机 131.84.1.31 发动拒绝服务攻击,网络拓扑和攻击过程如图 2 和图 3.

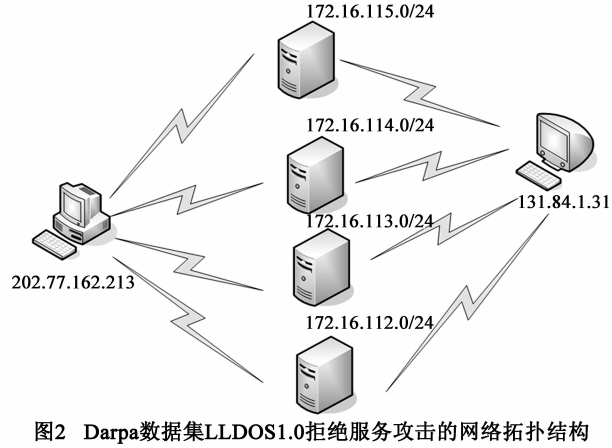


图2 Darpa数据集LLDOS1.0拒绝服务攻击的网络拓扑结构

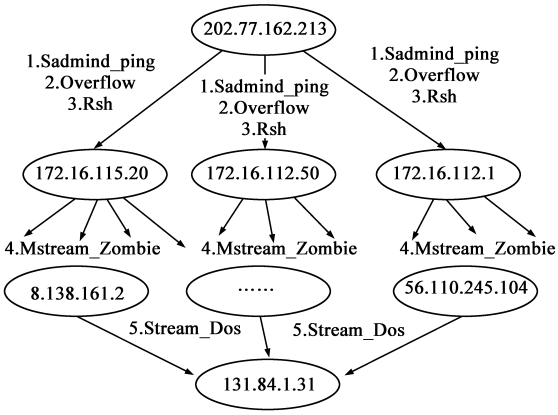


图3　LLDOS1.0攻击过程

4.4　结果分析

(1)算法有效性和性能测试

LLDOS1.0 中的多步攻击是由 3 条独立路径所组成,分为 5 个攻击阶段,如图 3 中所示.最终的攻击目标只有主机 131.84.1.131.图 4 列出了使用本文 MARP 方法得出的各阶段数据与原始 Darpa 数据集中各阶段实际数据的对比显示.我们在之前工作发表的文献"A Description Model of Multi-step Attack Planning Domain based on Knowledge Representation"中,运用相同数据集和方法来证明当时规划域描述模型的有效性.本文的实验结果强调算法和模型的有效性.

图 4 中是经过本文提供的方法与 DARPA2000 中多步攻击实际步骤的对比,在阶段 1 中,实际数据中有三条数据,本文方法能够关联出三条数据,而在第 4 阶段,本文方法未能全部关联.可知 MARP 方法还存在一些不足,此方法可能将原数据集中一些重复性的数据丢失,但最终的识别效果是有效并且可用的.根据上述实验结果,得出 MARP 方法准确率及完备率,如表 3 和图 5.

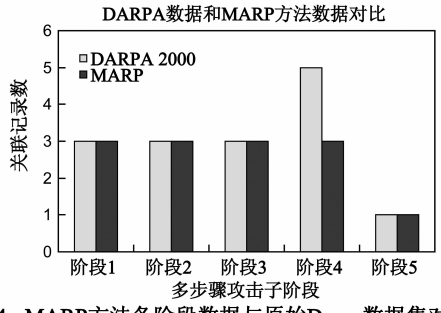


图4　MARP方法各阶段数据与原始Darpa数据集对比

表 3　MAPR 方法的准确率及完备率

评估指标	阶段 1	阶段 2	阶段 3	阶段 4	阶段 5	总计
准确率	100%	100%	100%	100%	100%	100%
完备率	100%	100%	100%	60%	100%	92%

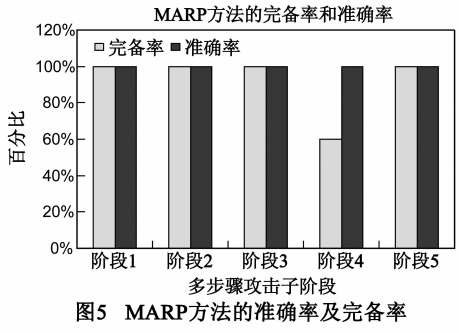


图5　MARP方法的准确率及完备率

综合以上实验,无论从应用 MARP 方法识别出的多步攻击各阶段的攻击数及各攻击间的关联关系,还是该方法本身的准确率及完备率,本文提出的 MARP 方法都具有较好性能.

(2)与同类工作比较

TIAA 作为一款应用于入侵检测领域的数据关联工具,核心方法是基于贝叶斯网络,即基于概率的算法.将 Peng Ning 等人的实验结果[21,22]与上述应用 MARP 方法得出的实验结果进行对比,得出如下对比如图 6.

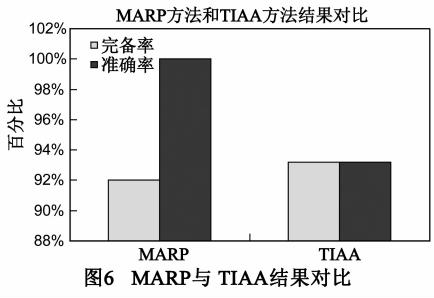


图6　MARP与 TIAA结果对比

从使用 DARPA 数据集进行测试的实验结果到与 TIAA 工具的对比结果,可看出本文提出的 MARP 方法在进行多步攻击场景识别问题的求解方面虽然与 TIAA 有不同,但方法具有可行性.

5　结束语

网络在企业、政府的日常办公中占据了越来越重要的位置,互联网已经改变了人们的沟通方式和资源共享方式.入侵检测作为网络防护系统能够及时发现一些网络攻击事件.但是随着网络结构日益复杂化,以及网络规模的不断扩大,数据流量与日俱增,网络攻击形式的多样化,网络攻击过程的复杂化和隐蔽化,导致网络攻击的检测越来越难.攻击场景的识别作为入侵检测系统中常用的方法,也成为入侵检测领域一直以来的热点.

本文基于智能规划方法和入侵检测的领域问题,提出了多步攻击场景识别算法 MARP,对算法的框架和实现方法进行了介绍,通过领域内的权威数据 DARPA2000 进行了实验验证,并与 TIAA 工具的关联效

果进行对比,在准确率和完备率方面都达到了可接受的效果.在未来工作中,将关注其他更加优秀的规划方法,通过对众多规划方法的区分,引入更适合多步攻击关联识别的智能规划技术作为支撑,提高攻击场景识别方法的效果.在研究小组发表的与本文相关的另外两篇文章中,讨论了多步攻击规划域与规划问题的描述,与本文的工作一样,主要研究将智能规划方法应用于网络多步攻击识别的可行性.未来工作中,将进一步探索适合网络多步攻击的智能规划方法,从而提高识别的效果.

参考文献

[1] 国家互联网应急中心.中国互联网网络安全报告[EB/OL]. http://www.cert.org.cn/publish/main/46/2012/20120523085533341215471/20120523085533341215471_.html,2012

[2] Baize Eric. Developing secure products in the age of advanced persistent threats[J]. IEEE Security & Privacy, 2012, 10(3): 88 – 92.

[3] 丁德路,姜云飞.智能规划及其应用研究[A].2001 年中国智能自动化会议论文集(下册)[C].北京:中国自动化学会,2001.837 – 844
Ding Delu, Jiang Yunfei. Intelligent planning and its application [A]. CIAC'2001[C]. Beijing: Chinese Association of Automation, 2001.837 – 844. (in Chinese)

[4] Jakobson G, Lemmon A, Weissman M. Knowledge-based Gui for network surveillance and fault analysis[A]. Network Operations and Management Symposium[C]. Washington DC: IEEE Computer Society, 1994.846 – 855.

[5] Jakobson G, Weissman M, Brenner L, et al. GRACE: Building next generation event correlation services[A]. Network Operations and Management Symposium[C]. Washington DC: IEEE Computer Society, 2000.701 – 714.

[6] NING P, XU D. Learning attack strategies from intrusion alerts [A]. Proceedings of the 10th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2003.200 – 209.

[7] Qin X, LEE W. Discovering novel attack strategies form INFOSEC alerts[A]. Proceddings of 9th European Symposium on Research in Computer Security[C]. US: Springer, 2004.439 – 456.

[8] 梅海彬,龚俭,张明华.基于警报序列聚类的多步攻击模式发现研究[J].通信学报,2011,32(5):63 – 69.
Mei Haibin, Gong Jian, Zhang Minghua. Research on discovering multi-step attack patterns based on clustering IDS alert sequences[J]. Journal on Communications, 2011, 32(5): 63 – 69. (in Chinese)

[9] 何金山.基于智能规划的多步攻击识别方法的研究[D].长春:吉林大学计算机科学与技术学院,2012.
He Jinshan. Research on Multi-Stage Attack Recognition Method Based on AI Planning[D]. Changchun: Computer Science and Technology College of Jilin University, 2012. (in Chinese)

[10] 王英梅,程湘云,刘增良.基于有限状态机的多阶段网络攻击方法研究[J].空军工程大学学报(自然科学版),2006,7(1):31 – 34
Wang Yingmei, Cheng Xiangyun, Liu Zengliang. The research for multi-stage attacks based on FSM[J]. Journal of Air Force Engineering University (Natural Science Edition), 2006, 7(1): 31 – 34. (in Chinese)

[11] 王永杰,鲜明,刘进,王国玉.基于攻击图模型的网络安全评估研究[J].通信学报,2007,28(3):29 – 34.
Wang Yongjie, Xian Ming, Liu Jin, Wang Guoyu. Study of network security evaluation based on attack graph model[J]. Journal on Communications, 2007, 28(3): 29 – 34. (in Chinese)

[12] 张永,陆余良.多阶段网络攻击建模[J].网络安全技术与应用,2002,(4):16 – 21.
Zhang Yong, Lu Yuliang. Multi-stage network attack modeling [J]. Network Security Technology & Application, 2002, (4): 16 – 21. (in Chinese)

[13] Zhang ZH, Ho PH. Janus: A dual-purpose analytical model for understanding, characterizing and counterming multi-stage collusive attacks in enterprise networks[J]. Journal of network and computer applications, 2009, 32(3): 710 – 720.

[14] 赖海光,黄皓,谢俊元.基于系统状态集合的攻击模型及其应用[J].计算机应用,2005,25(7):1535 – 1539.
Lai Haiguang, Huang Hao, Xie Junyuan. Attack model and its application based on system states aggregation[J]. Computer Applications, 2005, 25(7): 1535 – 1539. (in Chinese)

[15] 黄光球,任大勇.基于双枝模糊决策与模糊 Petri 网的攻击模型[J].计算机应用,2007,27(11):2689 – 2693.
Huang Guangqiu, Ren Dayong. Attack model based on both-branch fuzzy decision-making and fuzzy petri net[J]. Journal of Computer Applications, 2007, 27(11): 2689 – 2693. (in Chinese)

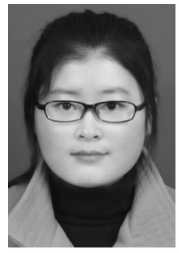
[16] 田志宏,张伟哲,张永铮,等.基于权能转换模型的攻击场景推理、假设与预测[J].通信学报,2007,28(12):78 – 84.
Tian Zhihong, Zhang Weizhe, Zhang Yongzheng, et al. Attack scenarios reasoning, hypothesizing and predicting based on capability transition model [J]. Journal of Communications, 2007, 28(12): 78 – 84. (in Chinese)

[17] 郭山清,曾英佩,谢立.基于可信报警事件的在线攻击场景重构算法[J].计算机科学,2006,33(8):100 – 105.
Guo Shanqing, Zeng Yingpei, Xie Li. An online attack scenarios construction algorithms based on delievable alarms[J].

Computer Science,2006,33(8):100 – 105.(in Chinese)
[18] 孙雷,姜淑娟,曾英佩,郭山清.基于系统漏洞的多步攻击场景构建[J].计算机工程,2007,33(20):150 – 152.
Sun Lei, Jiang Shujuan, Zeng Yingpei, Guo Shanqing. Attack scenarios construction based on system vulnerabilities[J]. Computer Engineering,2007,33(20):150 – 152.(in Chinese)
[19] Ahmadinejad SH, Jalili S, Abadi M. A Hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. Computer networks, 2011, 55(9): 2221 – 2240.
[20] Liu Zhijie, Wang Chongjun, Chen Shifu. Correlating multi-step attack and constructing attack scenarios based on pattern modeling[A]. Proceedings of the second international conference on information security and assurance[C]. Washington DC: IEEE Computer Society,2008.214 – 219.
[21] Peng Ning, Yun Cui, Douglas S Reeves. Constructing attack scenarios through correlation of intrusion alerts[A]. Proceedings of the 9th ACM Conference on Computer and Communications Security[C]. New York: ACM,2002.245 – 254.
[22] Peng Ning, Yun Cui, Douglas S Reeves, DingBang Xu. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security,2004,7(2):274 – 318.

作者简介

胡　亮　男,1968 年生于吉林长春,教授,博士生导师,1999 年在吉林大学计算机学院获得博士学位,现任教于吉林大学计算机科学与技术学院.主要研究方向为网格计算、分布式系统、信息安全等.
E-mail:hul@jlu.edu.cn



解男男　女,1987 年出生于黑龙江省哈尔滨市,现为吉林大学计算机科学与技术学院在读博士生.研究方向为计算机网络、信息安全.

柴　胜(通信作者)　男,1976 年出生于吉林省,现为吉林大学计算机学院讲师.研究方向为网络安全.
E-mail:chaisheng@jlu.edu.cn