基于概率推理的入侵意图识别研究

彭 武[1] 姚淑萍[2]
(北京理工大学机电学院 北京 100081)[1] (北京理工大学软件学院 北京 100081)[2]

摘 要 攻击者的入侵行为背后往往蕴含着攻击者的目标和意图,据此提出了入侵意图识别的层次化模型。为了处理网络环境中的不确定性信息,提出了基于概率推理的入侵意图识别算法,并在此基础上预测攻击者的后续攻击规划和目标,从而起到提前预警的作用。根据网络安全事件、目标和意图之间的因果关系建立的贝叶斯网络能够描述和处理并发意图识别问题。试验证明了该方法的可行性和有效性。

关键词 意图识别,有效意图,概率推理,贝叶斯网络
中图法分类号 TP393 **文献标识码** A

Study on Intrusion Intention Recognition Based on the Probabilistic Inference

PENG Wu[1] YAO Shu-ping[2]
(School of Mechanics and Electronics, Beijing Institute of Technology, Beijing 100081, China)[1]
(School of Software, Beijing Institute of Technology, Beijing 100081, China)[2]

Abstract Intrusive behaviors of attackers always imply their objects and intentions, hereby a hierarchical model of intrusion intention recognition was proposed. In order to handle the uncertain message in the circumstance of computer networks, intrusion intention recognition algorithm based on probabilistic inference was presented. On this basis the future plans and goals of the attackers can be predicted in order to take actions in advance. Bayesian networks were constructed to cope with the concurrent intention recognition problems according to the relationship of network security events, goals and intentions. Feasibility and validity of this method were proved from the experiments.

Keywords Intention recognition, Valid intention, Probabilistic inference, Bayesian networks

入侵意图识别是对大量底层报警信息进行分析,来解释和判断入侵者所要达到的目的、设想和打算,其本质上是实现对大量攻击数据给出合理解释的过程。对入侵者的意图识别能够判断入侵者的真实意图和预测入侵者的后续行为,是威胁分析和决策响应的前提和基础,是网络安全态势感知的重要组成部分,已经成为网络安全领域的研究热点。

目前,国内外学者从不同的角度开展了入侵意图识别的研究,取得了一定的成果。Honeywell 实验室的 Geib 等[1]将人工智能领域的规划识别引入到网络安全领域中来,并指出网络安全领域中的规划识别与传统的规划识别不同,是一种对抗式的规划识别。攻击者总是采取欺骗、隐蔽等手段掩盖自己的行为和意图。Geib 将主体所有的可能攻击行为作为扩展集,当攻击发生时,删除已经发生的行为,添加可能的攻击行为,构成新的扩展集。扩展集中概率最大的行为就是主体最可能的攻击规划。该方法能够利用观察到的数据推测攻击者的目标和正在执行的规划,但存在一些不足:很难构建完备的规划库;为了更新扩展集需要搜索主体所有可能的行为,可能引发搜索空间爆炸。诸葛建伟等[2]在规划识别基础上结合网络攻防对抗的特点提出了基于扩展目标规划图的网络攻击规划识别方法。将观察到的具体动作转化为抽象动作,根据抽象动作之间的关联识别背后蕴藏的攻击者意图和规划。观察到的数据来自于入侵报警信息,但这些信息因为多种原因往往是不完整的和不精确的,对这种不确定信息的处理应该作更深层次的研究。

Cuppens 等[3]在 MIRADOR 项目中通过报警关联分析来提炼攻击者的入侵意图。对攻击行为的前提、后果进行建模,根据后续行为的前提与先前行为的后果是否匹配来对两个行为进行关联。当检测到攻击行为时,搜索满足匹配条件的攻击路径来构造攻击者的规划。当有多条攻击路径对应着不同的攻击目标时,选择最短的攻击路径对应的攻击目标作为攻击者的入侵意图。随着事件数量的增多,关联搜索空间急剧增大,不适合大规模的在线处理。而且,当攻击者的行为对应着多个攻击目标时,选择最短路径显然不能达到最佳的效果。Qin 等[4]将攻击树转化为因果网络,并关联孤立的攻击场景,利用专家知识给出因果网络的先验概率分布,推理攻击者的意图和后续的攻击行为。但该方法不能发现新的攻击,不能识别攻击者的欺骗行为,也不能识别多人协作发动的攻击。Ning 等[5]提出了通过报警关联自动生成攻击策略的模型来间接获取攻击者的入侵意图。攻击策略通过攻击策略图(有向无环图)来描述,节点代表攻击行为,边代表攻击的时间顺序。边与节点的约束将攻击行为关联起来构成一个完整的攻击策略。通过对报警的泛化来消除形式改变而本质不变的攻

到稿日期:2009-03-02 返修日期:2009-05-01
彭 武(1979—),男,博士生,主要研究方向为网络安全,E-mail:pw_bit@126.com;姚淑萍(1972—),女,讲师,主要研究方向为信息安全。

击行为对攻击策略分析的影响。该方法还通过攻击策略间的相似性分析来发现未检测到的攻击行为。在实际应用中，可供比较的攻击策略图是很难找到的，即使存在并且相似性满足要求也不能确定该攻击行为一定发生了。

Huang 等[6]借鉴军事战场的意图识别方法开展了网络攻防对抗下的入侵意图识别和入侵策略的研究。攻击手段的灵活多变使得通过低层次的系统事件或网络事件分析入侵者的攻击策略变得非常困难，而高层次的意图识别能够提供独立于具体攻击手段的高水平的分析平台。在意图分析的层面上，入侵检测就变成使用各个异构的 IDS 协同工作去证实或者否定事先定义的各种意图假设。鲍旭华等[7]在此基础之上提出了基于入侵意图的复合攻击检测和预测算法。但是，这种方法没有考虑网络环境中的不确定性因素给意图识别带来的影响，算法还不尽完善。

本文提出了层次化的入侵意图识别模型，从攻击者的行为发现背后蕴藏的攻击目标，根据目标之间的因果关联识别攻击者的入侵意图，预测攻击者的后续目标。考虑到网络环境的不确定性，本文提出了贝叶斯网络等概率推理方法来推理攻击者的意图，为管理员的决策提供支持。

1 入侵意图识别模型

1.1 入侵意图识别过程

定义 1 事件是观察到的攻击者的行为描述。通过对安全设备的报警分析可以获取由攻击者的攻击行为触发的事件。一个事件可以用一个四元组来表示：Event〈name，time，prerequisite，consequence〉。name，time，prerequisite 和 consequence 分别代表事件的名称、事件发生的时间、事件发生的前提条件集和事件引起的后果集。

定义 2 规划是攻击者为达到某个目标而实施的一组行为的描述，以所期望的形式导向目标。规划表示为：Plan〈$SubPlan_1$，$SubPlan_2$，…，$SubPlan_n$〉，其中 $SubPlan_i$ 是规划中的一个子规划。

定义 3 目标是攻击者愿望的描述，它体现为给网络系统造成什么样的后果或自身达到什么样的目的。在多步攻击中，攻击者的入侵过程实质就是一个目标序列的实现过程。一个攻击目标可以用五元组来表示：Goal〈name，time，prerequisite，consequence，weight〉。name，time，prerequisite，consequence，weight 分别表示目标名称、目标时间、目标的前提条件集、目标的后果集、目标的权重。

定义 4 意图是攻击者希望达到某种目的的心理或想法。意图用一个二元组描述：Intention〈name，criticality〉。name，criticality 分别是意图的描述和危险程度。意图的危险程度通过对该意图的流行度、难易度、后果和已完成的进度比重等因素综合衡量获得。意图的危险程度分析可以使管理员重点关注危险程度高的意图，识别攻击者迷惑管理员的虚假意图。

意图识别是意图实现的逆过程，如图 1 所示。首先，网络安全设备观察到安全事件。然后，通过观察到的安全事件识别攻击者的规划和目标。最后，对攻击者的目标序列进行分析抽象，结合具体的网络环境推理其意图[8]。在网络安全领域，入侵意图与攻击者的最终目标往往是一致的。在实际应用中，为了在线分析和提前预警，需要在攻击者实现最终目标之前判断其意图。对于最终目标还没有实现或难以判断的情况，需要通过对已经实施的攻击目标来推断攻击者的意图。

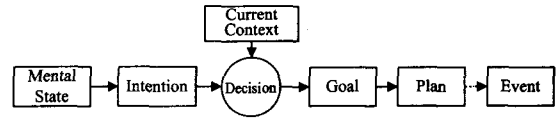

图 1 入侵意图的实现过程

定义 5 事件的隶属度。描述事件隶属于某一目标的程度，根据事件引发的后果与攻击者希望达成的目标进行相似性比较。设 E_i，G_j 分别为事件和目标，则事件 E_i 隶属于目标 G_j 的隶属度为：

$$S(E_i,G_j)=\sum_{k=1}^{m}\alpha_k\cdot\delta_k/m$$

其中，δ_k 为事件 E_i 和目标 G_j 的第 k 个属性的相似程度，α_k 为各个属性的权值，m 为属性个数。属性主要选取事件的后果集和目标的后果集中的元素，权值根据属性的重要性凭经验给定。给定一个阈值 S_0，当 $S(E_i,G_j)\geqslant S_0$ 时，认为事件 E_i 隶属于目标 G_j。

攻击者为达到同一目标可采取的攻击手段很多，这增加了意图识别的难度。通过调整阈值 S_0 的大小，可以在目标的层面上识别攻击者的意图，忽略攻击者的攻击细节信息。在实际攻击过程中，攻击者可能重复多次某个攻击步骤，也可能尝试不同的攻击手段实现同一个目标，通过事件的隶属度分析可以将隶属于同一目标的事件合并，这样对意图识别没有影响，但减小了计算量和处理难度。

定义 6（目标链） 假如 G_i，G_j 是时间片 i，j 时的目标，$i<j$，当且仅当：$\exists p\,|\,prerequisite(G_j,p)\wedge effect(G_i,p)$，即 G_j 的前提条件集中的某一元素 p 为 G_i 的后果集中的元素，记作：$G_i\rightarrow G_j$。

定义 7（有效意图） 意图 $I=\langle G,O,L\rangle$，其中 G 是一个目标链，O 是一组时序关系，L 是目标之间的因果关系，则称意图 I 为有效意图，即满足时序约束的目标链是一个有效意图。

通过对攻击者有效意图的分析可以对其未来的攻击目标进行预测。预测攻击者的目标与预测攻击者的行为相比，不影响威胁分析和决策响应，而且还有一些优点：预测攻击者的目标可以减小搜索空间，提高计算效率；预测攻击者的目标可以避免备选太多，概率过于分散。

定义 8（并发意图） 即根据攻击者已经实施和正在实施的目标搜索出多个目标序列均为有效意图。如图 2 所示，已经识别攻击者的目标序列{host_identify，recon，break_in}，搜索目标空间，可以得到两个有效意图：故意破坏（vandalism）和盗取信息（theft）。

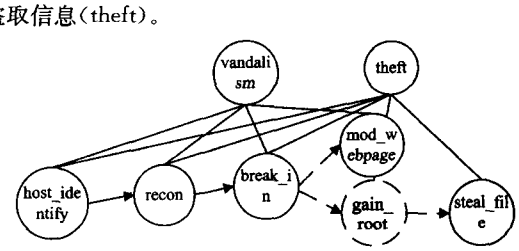

图 2 并发意图示例

1.2 入侵意图识别的层次化模型

在人工智能领域的人机交互（Human-Computer Interaction）研究中，通过观察人的行为来识别其意图[9]，这与入侵

意图识别在本质上是一致的。本文将人工智能领域中的层次化的目标识别模型[10]引入到网络安全领域，提出了入侵意图识别的层次化模型。

从大量底层的安全事件中识别攻击者的意图和规划，其本质上就是要在网络攻防这一复杂的应用领域中研究和实现能够对这些攻击事件给出合理解释的专家系统。通过对意图识别过程的分析，其可以分为事件层、状态层和目标/意图层3个层次。在事件层，攻击者的攻击行为触发安全事件，是入侵意图识别的底层数据来源。状态层包括攻击者状态和系统状态。攻击者状态是指攻击者在针对网络系统实施攻击过程中具备的状态，包括攻击者对网络系统的认知和攻击者具备的能力、资源等。攻击者通过不断试探、攻击等行为获取网络的信息和扩展自身的资源，逐步改变自身的状态。网络系统状态是指受监控系统中与安全相关的信息对象。根据系统状态是否能被攻击者的行为所改变分为不变系统状态和可变系统状态。不变系统状态包括计算机系统的软硬件配置信息、漏洞信息等。可变系统状态是攻击者的行为导致系统状态改变的系统安全状态，包括访问权限、保密性、可用性、完整性等。通过监控系统状态的变化可以间接发现攻击者的攻击行为和规划，为意图识别提供证据支持。在目标/意图层，攻击者的目标和意图往往是分步骤和分层次的，前一目标是后一目标的前提和基础，顶层目标是底层目标的提炼和抽象。图3是攻击者对IIS服务器发动DoS攻击的层次化意图识别示例。

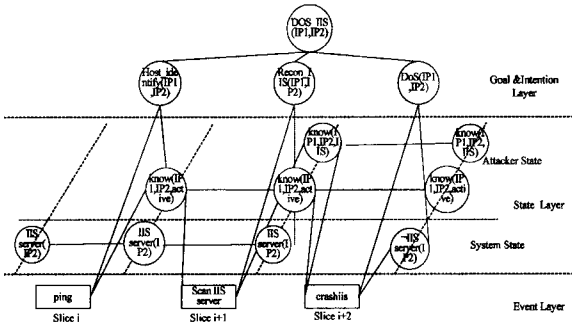

图3 层次化的入侵意图识别示例

2 入侵意图识别算法

攻击者的入侵意图识别可以分三个阶段：第一阶段根据网络安全设备观察到的安全事件识别攻击者的目标；第二阶段根据已经识别的目标序列提炼有效意图；第三阶段通过意图分析识别攻击者的入侵意图并预测攻击者未来的攻击目标。

2.1 目标识别

通过网络安全设备观察到的安全事件，遍历目标库中的目标，计算该事件隶属于目标的程度，如果大于事先定义的阈值，则搜索完毕。在一定的时间区间内观察到多个重复的事件或相似的事件，则归并到同一个目标。通过图4所示的目标识别算法，可以从观察到的多个安全事件中识别攻击者的一个或多个攻击目标，组成目标序列。

```
Input: event E_i , threshold S_0
For every G_j of the set of Goal
Compute: S(E_i,G_j)
If S(E_i,G_j) > S_0
Then  G_j is the goal of E_i
End
```

图4 目标识别算法

2.2 有效意图识别

攻击者的入侵过程实质上就是攻击者的目标逐一实现的过程，因此攻击者的目标之间是存在因果关系的。在观察到的目标序列中，根据目标之间的因果关系构造满足时序关系的目标链，并去掉冗余的目标链即得到有效意图。具体计算流程如图5所示。

```
Input: Goal series{G_1,G_2,…,G_n}
For h=1:n
Valid intention I_h= <G_h,O_h,L_h>
For i=h:n  and  j>i
If <{G_i,G_j},O_i,L_i> is satisfied
Then add G_j in I_h
Return valid intention I_h= {G_h,G_j}
End
End
If I_h is one of the subset of {I_1,…,I_h-1}
Delete I_h
End
```

图5 有效意图识别算法

2.3 入侵意图识别

入侵意图识别是在攻击者还没有完成所有攻击之前识别其最终目标的过程，因此需要在攻击者完成部分攻击行为的基础上进行分析、推理和预测。在网络攻防对抗这一复杂领域，对攻击者意图的识别实质上属于不确定性推理，因此采用贝叶斯网络[11]等不确定性推理方法是合理和科学的。

有效意图 $I=\langle G,O,L\rangle$，$G=\{G_1,G_2,\cdots,G_r\}$ 是网络安全设备间接观察到的满足时序约束和因果关系的一个目标链。在目标库中搜索满足时序关系和因果关系的目标组成新的目标链。如图6所示，目标 G_s 是满足时序要求和因果关系的一个目标，P_s 是在目标 G_r 实现的前提下攻击者发动攻击目标 G_s 的概率，由专家给出或历史数据统计获取。将目标 G_s 加入到目标链中，重新开始新的搜索，直到没有新的目标出现。搜索到的最终目标即为攻击者的入侵意图，发生的概率由目标链中目标之间的先验概率推理得到。

```
Input: Goal series{G_1,G_2,…,G_t}
For every G_s in Goal Base
If  G_r→G_s:P_s
Add G_s in Goal series {G_1,G_2,…,G_r}
End
```

图6 入侵意图识别算法

对于同一个有效意图中的目标链，按照图6所示的算法可能搜索出多条满足时序约束和因果关系的因果链，这就是第1节定义的并发意图。在多步攻击中，攻击者的意图往往是并发的，主要原因有：1)攻击者的攻击策略比较灵活，在攻击的过程中可能视攻击对象的反应不同而改变攻击策略和入侵意图；2)从检测的角度来看，一个安全事件可能是实现多个攻击意图的共同环节。

并发意图的识别采用贝叶斯网络能够取得比较好的效果。贝叶斯网络也称为因果网络，是当前进行不确定性知识表示和推理的主要工具。贝叶斯网络所具有的突出特点有：(1)有比较完备的数学基础；(2)是一种将先验知识和数据进行综合的理想表达方式；(3)能够处理不完全的数据集。

利用贝叶斯网络识别攻击者的并发意图具体实施步骤如下：

1)根据事件与事件、事件与目标、目标与意图之间的关联关系生成贝叶斯网络，并根据专家知识或历史统计数据生成先验概率；

2)根据贝叶斯公式计算各个变量的后验概率；

3)新的事件到来时，完成贝叶斯网络中变量置信度的更新。

3 试验与分析

3.1 基于 DARPA 2000 数据集的试验

为了验证算法的有效性，选取 2000 年 DARPA[12] 的入侵检测评估数据 LLDOS1.0 进行试验分析。该入侵样本中包含了攻击者发动 DDoS 攻击所采取的步骤，这些攻击信息可以分成 5 个阶段：IP 探测，端口扫描发现漏洞，获取 root 权限，安装用于拒绝服务攻击的组件和发动攻击。将分布式入侵检测系统检测到的报警进行融合求精后得到描述攻击者攻击行为的安全事件。因为攻击行为是攻击目标的外在表现，所以可以通过事件分析发现攻击者的目标。LLDOS1.0 中事件与攻击者的目标的关系如图 7 所示。

	Target	Event	Goal
1	172.16.112.0/24	IMAP_PING_SWEEP	IP_SWEEP
2	172.16.112.0/24	SADMIND_PORT_SCAN	PROBE_OF_SADMIND_DAEMON_ON_SOLARIS
3	172.16.112.10	SADMIND_OVER_ATTEMPT	GET_ROOT_PRIVILEGE_VIA_SADMIND_VULNERABILITY
4	172.16.112.50	SADMIND_OVER_ATTEMPT	GET_ROOT_PRIVILEGE_VIA_SADMIND_VULNERABILITY
5	172.16.115.20	SADMIND_OVER_ATTEMPT	GET_ROOT_PRIVILEGE_VIA_SADMIND_VULNERABILITY
6	172.16.112.10	DDOS_AGENT_INSTALL	INSTALL_TROJAN_MSTREAM_DDOS_SOFTWARE
7	172.16.112.50	DDOS_HANDLER_INSTALL	INSTALL_TROJAN_MSTREAM_DDOS_SOFTWARE
8	172.16.115.20	DDOS_AGENT_INSTALL	INSTALL_TROJAN_MSTREAM_DDOS_SOFTWARE
9	131.84.1.31	DDOS	LAUNCH_DDOS_ATTACK_AGAINST_AN_SERVER

图 7　LLDOS1.0 的事件与目标

根据目标之间的因果关系可以得到如图 8 所示的一个有效意图。攻击者的目标依次可以描述为：IP_SWEEP，PROBE_OF_SADMIND，GET _ ROOT _ PRIVILEGE，INSTALL _ DDOS_ SOFTWARE 和 LAUNCH_DDOS。攻击者的意图就是攻击者的最终目标：发动 DDoS 攻击。

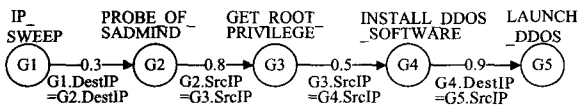

图 8　攻击者的一个有效意图

在实际的网络攻防对抗中，攻击者的目标往往是灵活多变的，而且攻击手段不断推陈出新，因此建立一个完备的目标库是比较困难的。但是通过概率推理来识别攻击者的入侵意图和预测攻击目标是可行和科学的。先验的概率如图 8 所示，由专家知识或历史数据统计得出。网络安全设备观察到的安全事件作为意图识别的证据输入，随着证据的增多，攻击者的意图也越来越明朗。

如图 9 所示，随着观察到的安全事件的增多，攻击者发动 DDoS 攻击的概率就越大。管理员根据系统防护的需要，事先给定一个阈值，当某意图的概率大于给定的阈值时，则认为意图识别成功，并预测攻击者的下一步目标，这样就可以在攻击者的攻击步骤没有完全实施以前发现其意图，为作好防范赢得时间。例如，设定阈值为 0.4，则攻击者发动 SADMIND 缓冲区溢出攻击时，可以认为攻击者的意图是发动 DDoS 攻击，下一步目标是安装后门软件和 DDoS 攻击软件。

	Event	Goal	Intention	Probability
1	IMAP_PING_SWEEP	IP_SWEEP	LAUNCH_DDOS	0.108
2	SADMIND_PORT_SCAN	PROBE_OF_SADMIND	LAUNCH_DDOS	0.36
3	SADMIND_OVER_ATTEMPT	GET_ROOT_PRIVILEGE	LAUNCH_DDOS	0.45
4	DDOS_AGENT_INSTALL	INSTALL_DDOS_SOFTWARE	LAUNCH_DDOS	0.9
5	DDOS	LAUNCH_DDOS	LAUNCH_DDOS	1.0

图 9　入侵意图识别过程

3.2　并发意图识别仿真

在简化计算又不影响试验效果的前提下，假设识别出攻击者有 3 个有效意图：为炫耀而发动的攻击(Brag)、窃取信息(Theft)和拒绝服务攻击(DoS)，分别用 i_1，i_2，i_3 表示，如图 10 所示。为了实现这些入侵意图，攻击者有 4 个攻击目标：侦查(Probe)、获取 root 用户权限(Get_root_privilige)、窃取传输数据(Steal_and_export_ data)和发动 DoS 攻击(DoS_attack)，分别用 g_1，g_2，g_3，g_4 表示。最下层是一组事件序列，由网络安全设备观察得到，分别用 e_1，e_2，…，e_7 表示。

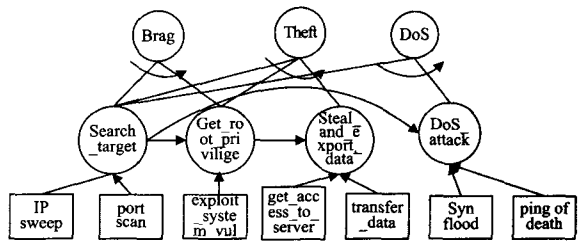

图 10　并发意图识别举例

根据事件、目标和意图之间的因果关系，构造贝叶斯网络如图 11 所示。部分先验概率已在图上标出。每一个结点只有两种属性，真(1)或假(0)。使用联合概率分布推理变量的后验概率。对于 n 个离散二值随机变量，要确定它们的联合概率分布，需要给出 2^n-1 个条件概率值，当 n 较大时，通过各个条件概率来计算联合概率往往是难以处理的。如果贝叶斯网络中的结点满足 d 分离条件(d-separation condition)，则贝叶斯网络满足独立性假设，可以简化计算。计算结果如表 1 所列。

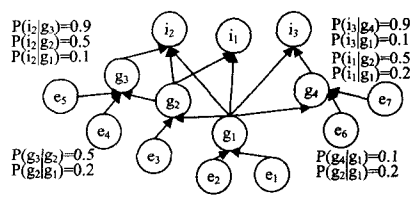

图 11　示例的贝叶斯网络

并发意图的识别得到的一组用概率描述的入侵意图如表 1 所列，再结合意图的危险程度以及系统的防护策略就可以忽略攻击者为了迷惑管理员而发动的虚假意图和威胁程度较小的意图，为管理员的决策提供强有力的支持。

表 1　在各证据集下的入侵意图概率

Evidence sets	P(i1=1|evidence)	P(i2=1|evidence)	P(i3=1|evidence)
e1	0.243	0.235	0.154
e1，e2	0.285	0.190	0.181
e1，e2，e3	0.595	0.468	0.181
e1，e2，e3，e4	0.595	0.818	0.181
e1，e2，e3，e4，e5	0.595	0.868	0.181
e1，e2，e6	0.285	0.190	0.861

结束语　本文在人工智领域中的目标识别和意图识别的基础上，提出了层次化的入侵意图识别模型，采用了概率推理的理论与方法来表示和处理网络中的不确定和不完整信息，详细描述了意图识别的过程和算法。试验证明了该模型和算法的可行性和有效性。对于攻击者采取更隐蔽的手段发动的攻击的意图识别还需要进一步的研究；贝叶斯网络的构造以及算法的效率还有待研究和提高。

参 考 文 献

[1]　Geib C W, Goldman R P. Plan Recognition in Intrusion Detection Systems[J]. IEEE, 2001: 46-55

(下转第 157 页)

1st Workshop on Architectural and System Support for Improving Software Dependability. 2006

[19] Clause J, Li W, Orso A. Dytan: A Generic Dynamic Taint Analysis Framework[C]// Proceedings of the International Symposium on Software Testing and Analysis. 2007

[20] Chen S, Xu J, Nakka N, et al. Defeating memory corruption attacks via pointer taintedness detection[C]// IEEE International Conference on Dependable Systems and Networks(DSN). 2005

[21] Chen S, Pattabiraman K, Kalbarczyk Z, et al. Formal Reasoning of Various Categories of Widely Exploited Security Vulnerabilities Using Pointer Taintedness Semantics[C]// 19th IFIP International Information Security Conference(SEC2004). 2004

[22] Cavallaro L, Saxena P, Sekar R. On the Limits of Information Flow Techniques for Malware Analysis and Containment[C]// Proceedings of the GI SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA). 2008

[23] Ruwase O, Lam M. A practical dynamic buffer overflow detector [C]// Proceedings of the Network and Distributed System Security Symposium. 2004

[24] Avots D, Dalton M, Livshits B, et al. Improving Software Security with a C Pointer Analysis[C]// Proceedings of the 27th International Conference on Software Engineering. 2005

[25] Egele M, Kruegel C, Kirda E. Dynamic Spyware Analysis[C]// Proceedings of the 2007 USENIX Annual Conference(Usenix'07). 2007

[26] Moser A, Kruegel C, Kirda E. Exploiting multiple execution paths for malware analysis[C]// Proceedings of the 2007 IEEE Symposium on Security and Privacy(Oakland'07). 2007

[27] Vogt P, Nentwich F, Jovanovic N, et al. Cross - Site Scripting Prevention with Dynamic Data Tainting and Static Analysis[C]// Proceedings of the Network and Distributed System Security Symposium(NDSS'07). 2007

[28] Akritidi P, Cadar C, Raiciu C, et al. Preventing memory error exploits with WIT[C]// Proceedings of 2008 IEEE Symposium on Security and Privacy(Oakland'08). 2008

[29] Clause J, Doudails I, Orso A, et al. Effective Memory protection Using Dynamic Tainting[C]// International Conference on Automated Software Engineering. 2007

[30] Nethercote N, Seward J. Valgrind: A framework for heavy - weight dynamic binary instrumentation[C]// Proceedings of ACM SIGPLAN 2007 Conference on Programming Language Design and Implementation(PLDI'07). 2007

[31] Seward J, Nethercote N. Using Valgrind to detect undefined value errors with bit-precision[C]// ATEC'05: Proceedings of the USENIX Annual Technical Conference 2005 on USENIX Annual Technical Conference. 2005

[32] Cowan C, Beattie S, Johansen J, et al. PointerGuard: Protecting Pointers From Buffer Overflow Vulnerabilities[C]// Proceedings of the 12th USENIX Security Symposium. 2003

[33] Suh G, Lee J, Zhang D, et al. Secure Program Execution via Dynamic Information Flow Tracking[C]// Proceedings of the 11th Conference on Architectural Support for Programming Languages and Operating Systems. 2004

[34] Lam L, Chiueh T. A general dynamic information flow tracking framework for security applications[C]// Proceedings of the 22nd Annual Computer Security Applications Conference. 2006

[35] Dalton M, Kannan H, Kozyrakis C. Real-World Buffer Overflow Protection for User and Kernel Space[C]// Proceedings of the 17th USENIX Security Symposium. 2008

[36] Haalfond W, Orso A, Manolios P. Using Positive Tainting and Syntax-aware Evaluation to Counter SQL Injection Attacks[C]// Proceedings of the 14th ACM SIGSOFT International Symposium on Foundations of Software Engineering. 2006

[37] Hind M, Pioli A. Which pointer analysis should I use? [C]// Proceedings of the International Symposium Testing and Analysis. 2000

[38] Hind M. Pointer Analysis: Haven't We Solved This Problem Yet? [C]// Proceedings of the 2001 ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering. 2001

[39] Vachharajani N, Bridges M, Chang J, et al. RIFLE: An Architectural Framework for User-Centric Information-Flow Security [C]// Proceedings of the 37th Annual IEEE/ACM International Symposium on Microarchitecture. 2004

[40] Lu S, Li Z, Qin F, et al. Bugbench: Benchmarks for evaluating bug detection tools[C]// Proceedings of the workshop on the Evaluation of Software Defect Detection tools. 2005

(上接第 82 页)

[2] 诸葛建伟,韩心慧,叶志远,等. 基于扩展目标规划图的网络攻击规划识别算法[J]. 计算机学报,2006,29(8):1356-1366

[3] Cuppens F, Autrel F, Miege A, et al. Recognizing Malicious Intention in an Intrusion Detection Process[C]// Second International Conference on Hybrid Intelligent Systems. Santiago, 2002

[4] Qin X, Lee W. Attack Plan Recognition and Prediction Using Causal Networks[C]// Proceedings of the 20th Annual Computer Security Applications Conference. 2004: 370-378

[5] Ning P, Xu D. Learning Attack Strategies from Intrusion Alerts [C]// Proceedings of the 10th ACM conference on computer and communications security. Washington D. C., USA, 2003: 200-209

[6] Huang MY, Wicks TM. A large-scale distributed intrusion detection framework based on attack strategy analysis[J]. Computer Netwroks, 1999: 2465-2475

[7] 鲍旭华,戴英侠,冯萍慧,等. 基于入侵意图的复合攻击检测和预测算法[J]. 软件学报,2005,16(12):2132-2138

[8] Youn S, Oh K. Intention Recognition using a Graph Representation[C]// Proceedings of World Academy of Science and Technology. 2007(21): 13-18

[9] Breazeal C. Social interactions in HRI: the robot view[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2004, 34(2): 181-186

[10] Blaylock N, Allen J. Fast Hierarchical Goal Schema Recognition [C]// Proceedings of AAAI. 2006: 8-15

[11] Pearl J. Probabilistic Reasoning in Intelligent Systems : Networks of Plausible Inference[M]. San Mateo, CA, Morgan Kaufmann, 1988

[12] http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000/LLS_DDOS_1.0.html