

基于因果知识发现的攻击场景重构研究

樊迪¹, 刘静^{1,2,3}, 庄俊奎^{1,2,3}, 赖英旭^{1,2,3}

(1. 北京工业大学信息学部, 北京 100124;

2. 北京工业大学可信计算北京市重点实验室, 北京 100124;

3. 北京工业大学信息安全等级保护关键技术国家工程实验室, 北京 100124)

摘要: 为了从分散的告警日志中发现攻击模式、构建攻击场景, 通过分析现有攻击场景重构方法, 针对现有方法因果知识复杂难懂且难以自动获取的问题, 提出一种基于因果知识发现的攻击场景重构方法。所提方法首先按照知识发现的过程, 通过告警日志间 IP 属性的相关程度, 构建攻击场景的序列集合; 然后, 采用时间序列建模的方式去除误告警, 以精简攻击场景序列; 最后, 利用概率统计方法发现各告警类型间的关联关系。在 DARPA 2000 数据集上对方法进行了实验验证, 结果表明, 该方法能有效识别多步攻击模式。

关键词: 入侵检测; 告警关联; 时间序列建模; 攻击场景重构

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00148

Research on attack scenario reconstruction method based on causal knowledge discovery

FAN Di¹, LIU Jing^{1,2,3}, ZHUANG Jun-xi^{1,2,3}, LAI Ying-xu^{1,2,3}

(1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China;

2. Beijing Key Laboratory of Trusted Computing, Beijing University of Technology, Beijing 100124, China;

3. National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing University of Technology, Beijing 100124, China)

Abstract: In order to discover the attack pattern from the distributed alert data and construct the attack scene, a method of finding the attack scene from the alert data generated by intrusion detection system was studied. Current research suffer from the problem that causal knowledge is complex and difficult to understand and it is difficult to automatically acquire the problem. An attack scenario reconstruction method based on causal knowledge discovery was proposed. According to the process of KDD, the sequence set of attack scenes was constructed by the correlation degree of IP attributes among alert data. Time series modeling was adopted to eliminate the false positives to reduce the attack scene sequence. Finally, causal relationship between the alert data was found by using probability statistics. Experiments on the DARPA2000 intrusion scenario specific data sets show that the method can effectively identify the multi-step attack mode.

Key words: intrusion detection, alert correlation, time series modeling, attack scenario reconstruction

1 引言

2015 年, 国家计算机网络应急技术处理协调

中心 (CNCERT/CC) 成功处理的网络安全事件共 125 815 起, 其中, 网页假冒占 59.7%, 漏洞占 20.2%, 网页篡改占 9.8%, 网站后门占 3.2%, 恶

收稿日期: 2016-12-09; 修回日期: 2017-03-06。通信作者: 樊迪, 1428590394@qq.com

基金项目: 北京市自然科学基金资助项目 (No.4162006)

Foundation Item: Beijing Municipal Natural Science Foundation (No.4162006)

意程序占 2.9%，恶意代码占 2.6%，网页挂马占 0.8%，其他占 0.8%。另外，影响范围较大或涉及政府部门、重要信息系统的恶意程序、网站后门、网页挂马、拒绝服务攻击等事件也是 2015 年 CNCERT/CC 事件处理工作的重点^[1]。上述网络安全事件大部分都不是攻击者一步就可以完成的，而是需要有目的、有计划、有步骤地一步步完成，如拒绝服务攻击。发现攻击者实施多步攻击的模式，进行攻击场景重构，可以剖析出攻击者常使用的攻击方式及攻击意图，从而为安全管理员构建更安全的防护体系提供依据，进而保证网络空间的安全。

攻击过程中，攻击者按照其每阶段的目的，采用不同的攻击方式，逐步完成自己的攻击目标。攻击者如果采用同样的攻击策略（或攻击工具）进行攻击，那么他（它）们的攻击行为在一定程度上具有相似性，即在不同攻击步骤之间存在一定的模式。入侵检测系统（IDS, intrusion detection system）存在的目的是对防火墙补充，实时监控计算机系统的安全违规迹象，在发现安全威胁时触发告警或采取相应的行动主动保护网络安全。攻击者发起攻击时，会在 IDS 告警中留下痕迹，这样，攻击者在攻击行为上的这种相似性就可以通过 IDS 产生的告警显示出来。因此，需要将告警信息关联起来，从中发现复杂的多步攻击模式，从而达到构建攻击场景掌握入侵全貌的目的，进而为实时检测网络中正发生的多步攻击提供依据。

然而，IDS 所获取和分析信息具有局限性，这是由其工作原理、所处的网络层次导致的。IDS 产生的告警大部分是分散的、低层次的、针对单个漏洞攻击的，而对描述相对较为复杂的多步攻击的特征比较困难。现有的告警分析方法，虽然可以从告警信息中识别出多步攻击，但大多需要大量预先定义的先验知识^[2,3]，或需要大量未知参数的辅助，存在参数确定困难的问题^[4]。文献[5]采用多步攻击模式识别时未考虑 IDS 产生告警存在误报问题。面对现有方法依赖先验知识、告警关联自动获取难的情况，本文提出一种基于因果知识发现的攻击场景重构方法，该方法不需要大量的先验知识，难以配置参数较少，且在知识发现的数据与处理过程中利用时间序列建模去除周

期性误告警，提高了因果知识的正确性，缓解了基于原始告警进行关联分析所带来的因果知识复杂难懂的状况。实验结果表明，该方法能在 IDS 告警数据中对多步攻击模式做出有效识别，构建较为准确的攻击场景。

2 相关工作

2.1 安全事件关联分析方法

攻击场景重构就是通过对 IDS 等安全设备产生的原始安全事件进行关联分析，还原出攻击者对整个网络空间的攻击、渗透过程，然后将这种高层次的场景信息反馈给管理员^[6]。由上可知，攻击场景重构中最重要的一点就是告警间关联的发现与分析。

2000 年，Templeton 等^[7]提出通过一种灵活可扩展的计算机攻击模型，利用特定的模型语言，分析攻击间的因果关系识别出多步攻击。之后，Ning 等^[8]于 2002 年在 TIAA 项目中，依据 Templeton 等^[7]因果关系的思想，进一步进行深层次的研究，提出通过定义攻击步骤之间的先决和可能产生的后果来关联报警构建攻击场景。2002 年，Cuppens^[9-11]领导的 MIRADOR 项目，在基于因果关系利用 Lambda 语言描述攻击后，脱机相关过程会分析这些攻击说明，以自动生成一组相关规则；然后，在线相关过程将这些相关规则应用于由 IDS 生成的警报，以识别更多的全局攻击情形。文献[12]将职能规划用于多步攻击识别，但该方法依然需要依赖专家知识库中的匹配规则。此类方法都是事先定义攻击的关联规则，过分依赖规则定义人员的知识储备，而且不能处理未知攻击。

Qin 等^[13,14]利用系统和网络的安全状态与时间序列和统计分析方法这 2 个互补机制来挖掘攻击场景片段，并使其连接成为完整的攻击场景。Morin 等^[15]也利用时序模式识别的方法来识别攻击场景。但是这种通过时序算法挖掘产生攻击知识模板的方法需要大量的计算，且需要配置的参数比较多。

Zhang 等^[16]提出采用时间窗口对告警序列进行分段，在每个时间窗口的控制下发现多步攻击模式，但这种方法时间窗口较难确定。这是由于

时间窗口的定义者无法确定攻击者的攻击行为所持续的时间。此外,该方法未考虑时间属性以外的其他信息对告警划分产生的影响,如IP地址等,这会影响挖掘的正确性。同样,文献[17]也存在滑动时间窗口确定困难的问题。2014年,冯学伟等^[5]提出一种面向原始告警数据的因果知识挖掘方法,该方法考虑利用IP地址的相关性对告警日志进行划分,利用马尔可夫性质挖掘告警间的关联关系。虽然方法不需要大量的先验知识,也无需配置未知参数,但该方法面向原始数据流,这可能会导致挖掘到的因果知识过于繁杂,且该方法未考虑IDS产生告警时的误报或漏报情况,这也会影响因果知识的正确性。

2.2 安全事件误报或漏报处理方法

文献[18,19]研究了IDS产生告警时的误报或漏报情况。Pietraszek等^[18]提出基于机器学习的方法ALAC,正确识别与攻击相关的IDS警报。ALAC告警处理方法提高了自动性,但在利用机器学习进行训练时需要对告警进行真伪性的区分,明确标明哪些告警是真实告警,哪些是误告警。因为无法将IDS在实际环境中产生的告警明确地分为真实告警还是误告警,所以这种方法更适用于分析DARPA等数据集。同样,2009年,田志宏等^[19]所提出的对误告警进行自动鉴别的方法也存在同样的问题。

由上可知,在告警事件关联分析过程中,数据挖掘方式对先验知识的依赖小,也具有识别未知攻击的能力,但现有方法依然存在以下问题:

1)告警划分及误告警自动鉴别困难;2)未知参数多;3)因果知识复杂难懂。针对以上问题,本文提出一种基于因果知识发现的攻击场景重构方法。本文所提方法基于知识发现的过程不需要大量先验知识,难以配置的未知参数较少,并且借鉴周期性的告警是误告警的思想^[20],利用时间序列建模去除周期性误告警,保证了因果知识的正确性和简洁性。而且,在误告警去除过程中,不需要明确标明告警属于真实告警还是属于误告警,更适用于实际网络环境。

3 攻击场景识别方法

3.1 本文方法描述

本文方法按照知识发现的过程,在数据准备阶段,首先确定要处理的对象为告警日志,对告警日志的格式统一化,接着判断IDS告警日志间的IP属性是否相关,构建攻击场景的序列集合;然后对攻击场景序列中的告警事件进行预处理,采用时间序列建模的方式,将具有周期性的误告警数据去除,达到精简攻击场景序列的目的。在数据挖掘阶段,通过计算每个攻击场景序列中攻击类型之间的转移条件概率,自动发现告警日志间的相关可能性,生成攻击模式构建攻击场景。在结果解释阶段,对挖掘到的因果知识进行结果的形式化表达。方法总体过程如图1所示。

3.2 构建攻击场景序列集合

由分步攻击的特性^[21]可知,多步攻击有多个

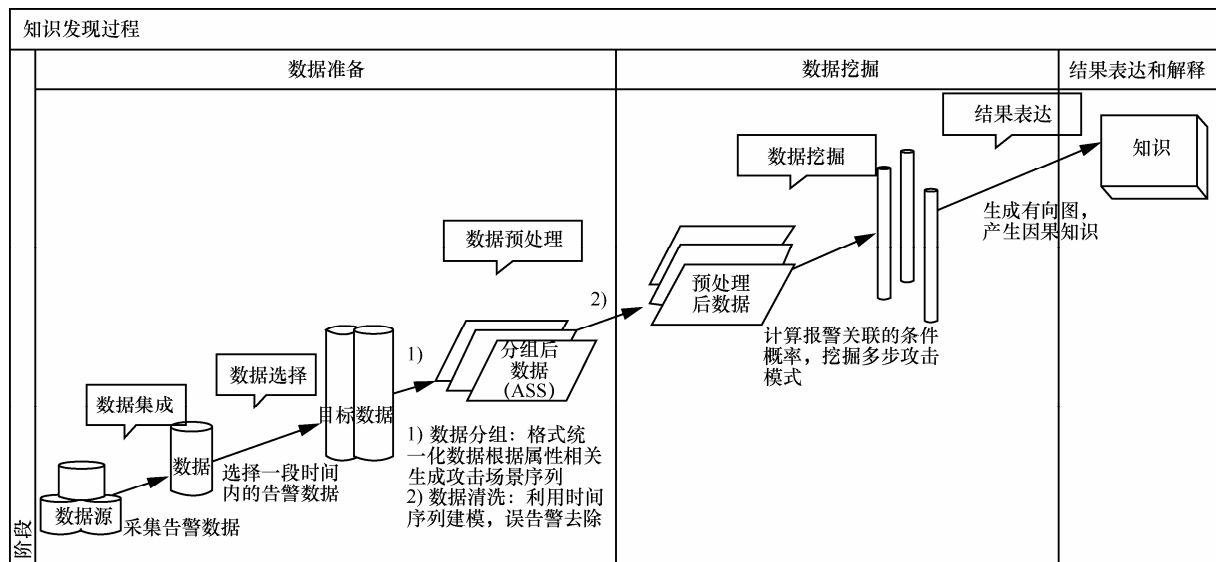


图1 方法总体过程

不同的攻击步骤，每个步骤都有一个目的，达到该目的后继续进行下个步骤，这些不同的攻击步骤可以通过 IDS 告警日志体现出来。为了从 IDS 告警日志中发现多步攻击的模式，本文首先对原始的 IDS 告警进行处理，规范日志的格式，并将告警数据进行聚类，转换为可能包含攻击场景的告警集合。

为了更好地说明本部分内容，涉及概念如下。

定义 1 告警事件。告警事件是一个 n 元组 $(a_1, a_2, \dots, a_n)$ ，其中， $a_k (1 \leq k \leq n)$ 表示告警事件的第 k 个属性 (attribute)，记告警事件 $e = (a_1, a_2, \dots, a_n)$ 。

定义 2 告警序列 (AS, alarm sequence)。一组按时间顺序排列的告警事件集合称为告警序列，记为 $AS, AS = \langle e_1, e_2, \dots, e_m \rangle$ ，满足 $e_i.timestamp < e_j.timestamp (1 \leq i < j \leq m)$ 。

定义 3 攻击场景序列 (ASS, attack scene sequence)。攻击者完成一次多步攻击活动时触发 IDS 产生的告警序列称为攻击场景序列，记为 $ASS, ASS = \langle e_1, e_2, \dots, e_k \rangle$ ，其中， $e_i (1 \leq i \leq j \leq k)$ 表示第 i 个告警，且满足 $e_i.timestamp < e_j.timestamp (1 \leq i < j \leq k)$ 。

本文将告警事件设计成一个 7 元组， $e_i = (timestamp, attType, srcIP, srcPort, dstIP, dstPort, priority)$ ，其中， $timestamp$ 表示 IDS 告警的时间戳， $attType$ 表示攻击的类型， $srcIP$ 和 $srcPort$ 表示 IDS 告警源 IP 地址和源端口， $dstIP$ 和 $dstPort$ 分别表示 IDS 告警的目的 IP 地址和目的端口， $priority$ 表示告警的优先级。

构建攻击场景序列的一个重点就是确定告警事件之间的关联关系。即从告警序列 AS 中找出相关性较大的一组告警事件，构成一个 ASS 。基于 IP 属性相关性来构建攻击场景序列的方法基于如下假设：若告警事件 e_1 和 e_2 的 IP 属性相关，那么 e_1 的 IP 地址中至少有一个与 e_2 的 IP 地址相同^[5]。这是因为同一多步攻击过程中所触发的 IDS 告警事件在地址分布上具有相关性^[5]。在告警序列 AS 中，若相邻 2 个告警事件之间是 IP 属性相关的，则划分到同一攻击场景序列中；若新告警的 IP 存在于某攻击场景序列 (如 ASS_i) 的 IP 集合中，但与 ASS_i 中最后的告警事件 IP 不相关，则在 ASS_i 中找出与新告警事件 IP 直接相关的告警，取该告警事件前的告警重新创建一个由 ASS_i 衍生出来的新攻击场景序列，

直到遍历完 AS 中全部的告警事件。如算法 1 所示。

算法 1 基于 IP 地址相关构建 ASS 集合

输入：告警序列 $AS = \langle e_1, e_2, \dots, e_m \rangle$

输出：攻击场景序列的集合

$CASS = \{ASS_1, ASS_2, \dots, ASS_n\}$

```

1) Create  $CASS = \text{null}$ ; /*  $CASS$  用于存放  $ASS_1, ASS_2, \dots, ASS_n$  */
2) While( $AS$  is not  $\emptyset$ )
3)    $temp = AS.first$  and delete  $AS.first$ 
4)   If( $CASS$  is null) Then
5)     Create  $ASS_0$ ;
6)     add  $temp$  to  $ASS_0$  and add  $temp.IP$  to  $ASS_0.IPSet$ ;
7)      $CASS = CASS \cup ASS_0$ ;
8)   Else
9)     For  $ASS_i$  in  $CASS$ 
10)      If ( $temp.IP$  is in  $ASS_i.IPSet$ ) Then
11)         $index = f(temp.IP, ASS_i)$ ; /* 该函数用于查找  $ASS_i$  中 IP 等于  $temp.IP$  的最后一个告警事件的索引 */
12)        If ( $index == ASS_i.size - 1$ )
13)          add  $temp$  to  $ASS_i$ ;
14)          If ( $temp.IP$  has a new IP address which not in  $ASS_i.IPSet$ )
15)            add  $temp.IP_{new}$  to  $ASS_i.IPSet$ ;
16)          GoTo 2);
17)        Else
18)          Create  $ASS_{new}$ ;
19)          Create  $ASS_{new}.IPSet$ ; /* 取  $ASS_i$  中 0- $index$  项，新建由  $ASS_i$  衍生出来的攻击场景序列  $ASS_{new}$  */
20)          add  $temp$  to  $ASS_{new}$ ;
21)           $CASS = CASS \cup ASS_{new}$ ;
22)          GoTo 2);
23)        Create  $ASS_{new}$ ;
24)        add  $temp$  to  $ASS_{new}$  and create  $ASS_{new}.IPSet$ ;
25)       $CASS = CASS \cup ASS_{new}$ ;
26) Return  $CASS$ 

```

3.3 误告警去除

在实际的网络环境中，IDS 通常会产生大量

的告警数据。在这些大量的告警数据中，有一部分是误告警和无关告警。本文将由正常的或非恶意的网络活动引发的IDS告警称为误告警。将由攻击者发起恶意网络活动所引发的、但不属于同一攻击者或同一多步攻击的IDS告警事件称为无关告警。文献[20]指出，IDS产生的误告和无关告警最多可能占告警总数的99%以上。这些误告警和无关告警的存在严重影响了知识挖掘的准确性。算法1将IP属性相关的告警聚合到一起，最大限度地保证了每个ASS中的告警事件都是由一次攻击活动产生。若尽可能去除每个ASS中的误告警，因果知识挖掘正确性将大大提高。

定义4 误告警去除规则(RD, rule to delete)。误告警去除规则是一个3元组($attType$, IP , $IPFlag$)，其中， $attType$ 表示攻击的类型， IP 表示需要去除的IDS告警事件的IP地址， $IPFlag$ 表示IP地址的类型是源IP地址还是目的IP地址。记误告警去除规则为RD， $RD=(attType, IP, IPFlag)$ 。

误告警去除规则可以分为两类：一类是在对攻击场景序列集合CASS中的每个攻击场景序列ASS进行时间序列建模之前，基于告警的重尾分布特点^[21]，通过统计分析得到产生告警数量最多的三元组，称为待检误告警去除规则(RD_dubious)；一类是时间序列建模后经过周期性检验的真实的误告警去除规则(RD_real)。待检误告警去除规则的产生过程如下。

基于告警的重尾分布特点，首先选择CASS中的一个ASS，确定该ASS中 $attType$ 阈值 $attType_threshold$ 和IP阈值 $ip_threshold$ ；然后计算该ASS中 $attType$ 类型的告警事件占总告警数的比重，若超过 $attType_threshold$ ，再统计该类型的告警事件中哪些IP所占的比例超过 $ip_threshold$ ，并输出相应的RD_dubious，具体过程见算法2。

算法2 待检误告警去除规则生成算法

输入： $ASS=<e_1, e_2, \dots, e_k>$, $attType_threshold$, $ip_threshold$

输出： RD_dubious 集合，记为 RD_dubious_Set = {RD_dubious₁, RD_dubious₂, ..., RD_dubious_n}

1) Create $N=ASS.size$ and $RD_dubious_Set=null$; /* N is the Number of elements in ASS*/

2) Foreach $e_i.attType$ in ASS

3) Create $attTypeSet=fattType(e_i.attType)$; /*获取ASS中该攻击类型产生的告警集合*/

4) $n=attTypeSet.size$;

5) If ($\frac{n}{N} > attType_threshold$) Then /*

$attTypeSet$ 中所有告警对应的src IP和dst IP构成的IP集合分别记S和D*/

6) Foreach $srcIP$ in S

7) If(The proportion of $srcIP$ in S $> ip_threshold$) Then

8) add ($attType, srcIP, srcIPFlag$) to $RD_dubious_Set$

9) Foreach $dstIP$ in D

10) If (The proportion of $dstIP$ in D $> ip_threshold$) Then

11) add ($attType, dstIP, dstIPFlag$) to $RD_dubious_Set$

12) Return $RD_dubious_Set$

定义5 告警时间序列(TS, time series)。对一个攻击场景序列 $ASS=<e_1, e_2, \dots, e_k>$ 来说，设其持续攻击的时间为T，即 $T=e_k.timestamp-e_1.timestamp$ ，将时间等分成N个间隔，每个时间间隔记为 ΔT 。统计某个AS在每个 ΔT 中发生的个数x，这一系列的统计数字定义为告警事件序列，记为TS， $TS=<x_1, x_2, \dots, x_N>$ 。

$TS=<x_1, x_2, \dots, x_N>$ 的产生过程如下。

步骤1 AS经过算法1生成CASS。

步骤2 计算每个ASS的持续攻击时间T，设置时间间隔 ΔT 。每个CASS中的ASS利用算法2做统计分析，产生RD_dubious。

步骤3 取其中一条RD_dubious规则，统计该ASS中在每个 ΔT 中满足该规则的告警个数，生成TS。

通过上述过程将对告警的分析转换成对告警产生的时间序列的分析，利用文献[20]中的周期分析过程，首先对时间序列进行自相关分析以加强原始时间序列的周期性；再对产生的自相关序列进行离散傅里叶变换，求出周期性时间序列的周期；最后利用其构造的F分布模型检验周期的真伪，将算法2形成的待检误告警去除规则中的规则进行筛选，保留真实的告警去除规则。假设

算法2中的2个阈值参数分别为 x_1 、 x_2 ，则算法2的时间复杂度为 $O(n \cdot x_1 \cdot n \cdot x_2 \cdot n) = O(n^3)$ 。周期分析过程的时间复杂度为 $O(n \log(n))$ 。误告警去除算法的基本思想与文献[20]的思路类似，均基于时间序列分析理论，但文献[20]是将采集的全部告警事件作为分析对象，目的是从中找出满足周期性的误告警，而本文的研究对象是攻击场景序列中的告警事件，该告警事件已经做过一系列预处理，基本属于同一攻击场景。本文方法将一组存在内在联系的告警数据作为周期性误告警分析的研究对象，其意义在于能将属于攻击场景中的周期性数据去除。

3.4 因果知识发现

由于精简后的每个攻击场景序列中隐藏了攻击者的攻击行为，而攻击行为有这样的特点：如果攻击步骤A是攻击步骤B的前提，那么攻击步骤A一定发生在攻击步骤B之前，且攻击步骤A引发的IDS告警一定比攻击步骤B引发的IDS告警产生的时间早。这种行为特点与条件概率的计算思想一致，故本文采用概率统计的方法发现攻击告警序列中各IDS告警类型间的统计关联关系，最终形成因果知识。报警关联的条件概率 $P(nT|fT)$ 表示在发生 fT 类型告警的条件下紧接着发生 nT 类型告警的概率。

定义6 因果知识。每个ASS中都可能隐含一个多步攻击的模式，描述ASS中隐含的各攻击类型间内在因果关系的有向图称为因果知识。因果知识有向图的形式可表示为 $G = \langle V, E, P \rangle$ 。其中， $V = \{e_i.attType | e_i \in ASS\}$ ， $E = \{ \langle e_i.attType, e_j.attType \rangle | e_i \in ASS \text{ 且 } e_j \in ASS \}$ ， $P = \{ \text{报警关联的条件概率 } P(nT|fT) \text{ 的集合} \}$ 。

算法实现过程中用二维矩阵表示因果知识，其对应关系如图2所示。

遍历去除周期性误告警后ASS中的每个告警事件，创建条件概率矩阵 M ， $M_{fT, nT}$ 用于统计攻击类型 fT 后面直接跟 nT 的个数，如果出现新的攻击类型，则添加一行一列到条件概率矩阵中，直到遍历完该ASS中的全部告警事件。此时矩阵中每个数据统计的是该行所代表攻击类型下一步跟着发生该列所代表的攻击类型的次数，则索引 i 对应攻击类型发生的条件下，

下一步攻击为索引 j 所对应攻击类型的概率 $P_{ij} =$

$$\frac{M_{ij}}{\sum_{n=0}^{columnNum} M(i, n)}, \text{ 其中, } M(i, n) \text{ 表示矩阵 } M \text{ 中第 } i \text{ 行第 } n \text{ 列元素。}$$

因果知识发现过程的具体算法如算法3所示。

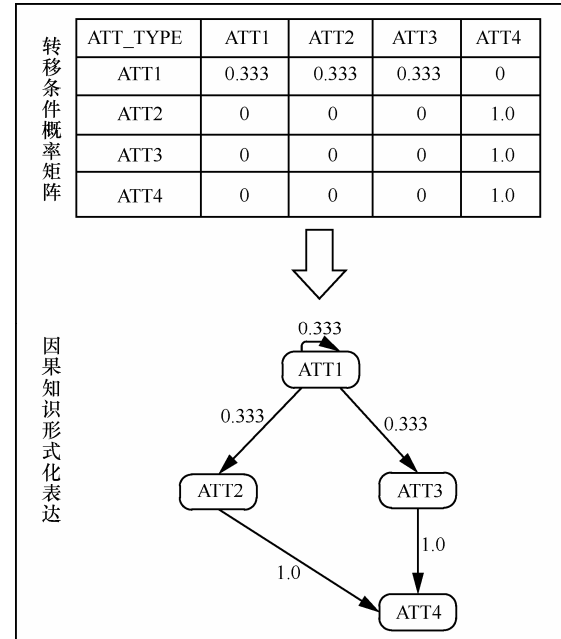


图2 条件概率矩阵表示因果知识对应关系

算法3 因果知识发现过程

输入：误告警去除后具有IP地址相关性的攻击场景重构序列集合 $ASS = \langle e_1, e_2, \dots, e_k \rangle$

输出：条件概率二维矩阵

1) Create V ;

2) Foreach e_i : ASS

3) If (V is empty) Then

4) $fT = e_0.type$ and $nT = e_1.type$;

5) Add fT and nT to V ;

6) Create a matrix M according to the V ;

7) The $V.attType$ map to $M.index$;

8) $M_{fT, nT}++$; /* $M_{fT, nT}$ 用于统计攻击类型 fT 后面直接跟 nT 的个数 */

9) Else

10) $fT = a_i.type$ and $nT = a_{i+1}.type$;

11) If (! $V.contains(nT)$) Then

12) add nT to V and add new row and column to M ;

```
13) The  $nT$  map to  $M.index$ ;  
14)  $M_{fT,nT}++$ ;  
15) Else  
16)  $M_{fT,nT}++$ ;  
17) For(int  $i=0;i<M.rowNum;i++$ )/计算条件  
    概率*/  
18) For(int  $j=0;j<M.columnNum;j++$ )  
19)  $P_{ij} = \frac{M_{ij}}{\sum_{n=0}^{columnNum} M(i,n)} M(i,n)$ ;  
20) Return  $P$ 
```

4 实验分析

4.1 实验说明

本文采用 DARPA 2000 数据集^[22]来验证方法的可用性。DARPA 2000 数据集是美国麻省理工学院林肯实验室提供有较强代表性的入侵场景关联数据集。数据集模拟的网络环境包括 3 个部分：Inside、Outside 以及 DMZ，其涉及网段详细信息如表 1 所示，网络拓扑如图 3 所示。

DARPA 2000 包含 2 个典型的攻击场景 DARPA 2000 LLDOS1.0 和 DARPA 2000 LLDOS2.0.2。本

表 1 DARPA 2000 网络环境详细信息

名称	主机个数/台	操作系统
Outside	14（包括 1 台路由器，1 台外部网关，1 台外部 Web 服务器）	Solaris、Linux Redhat、SunOS、MacOS
DMZ	6（包括 1 台路由器，1 台防火墙）	Solaris、Linux Redhat
Inside	40（包括 3 台防火墙）	Solaris、Linux Redhat、Windows、SunOS

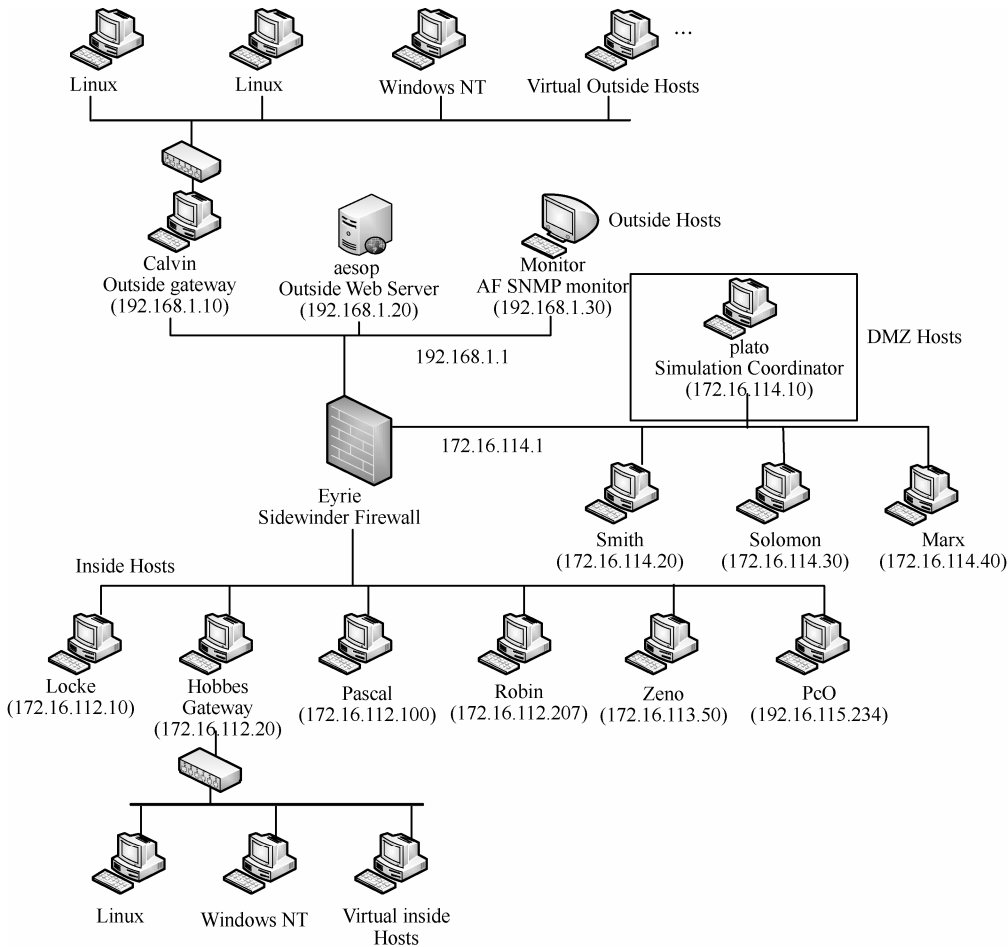


图 3 实验环境网络拓扑

文选用第一个攻击场景，在 Linux 系统下利用 Tcpreplay 工具向 Snort 监测的网段重放数据。重放过程中，Snort 产生的告警日志作为本方法的原始日志数据。

DARPA 2000 LLDOS1.0 包含如下场景。

- 1) 从远程站点采用 IPSweep 方式进行 IP 扫描。
- 2) 对活动 IP 进行探测以查询运行在 Solaris 主机上的进程 sadmind。
- 3) 尝试 sadmind 缓冲区溢出攻击，并且尝试 telnet 到主机，获取 root 权限。
- 4) 攻击者远程登录跳板机，安装 mstream 守护程序，为 DDoS 攻击做准备。
- 5) 发起 DDoS。

进行数据重放时涉及对 Snort 配置，下面做几点说明。首先，由于数据集的限制，将 Snort 的监控网段设置为数据集中 IP 地址的地址段，即将 Snort 配置文件 snort.conf 中的 HOME_NET 属性设置为 172.16.0.0/16；其次，说明 Snort 生成告

警日志时开启的告警规则为其本身默认规则；最后，播放原始数据时，以 DARPA 1999 提供的训练数据集中不含攻击的正常数据流为背景流量。

4.2 实验结果

表 2 给出了未加入背景流量时，数据集 5 个攻击阶段的告警数量及相关信息。

加入 DARPA 1999 中的正常流量作背景流量后，共收集 snort 告警 17 966 条。将原始告警格式统一后，利用算法 1 构建攻击场景序列集合 CASS，生成 ASS 共 14 种 ($ASS_0 \sim ASS_{13}$)。对每个 ASS 中的告警类型及 IP 地址进行分析，发现符合重尾分布^[20]的特性（以 ASS_1 为例，其告警类型情况如图 4 所示）。所以，利用算法 2 统计每个 ASS 中所占比例较大的告警类型和告警 IP 生成待检误告警规则 $RD_dubious$ ，然后对符合规则的告警事件建立告警时间序列进行周期发现和确定，最终生成真实误告去除规则 RD_real ，这样的方法去除攻击场景序列中的误告警是比较有效的。误告警去除效果由式(1)评估，其中，alarms

表 2 Snort 产生的日志情况（无背景流量情况下）

dump 文件	DMZ		Inside	
	数据分组/个	告警/个	数据分组/个	告警/个
phase-1-dump	785	767	40	20
phase-2-dump	148	134	158	79
phase-3-dump	530	138	226	57
phase-4-dump	526	3	521	3
phase-5-dump	34 214	0	73 925	263

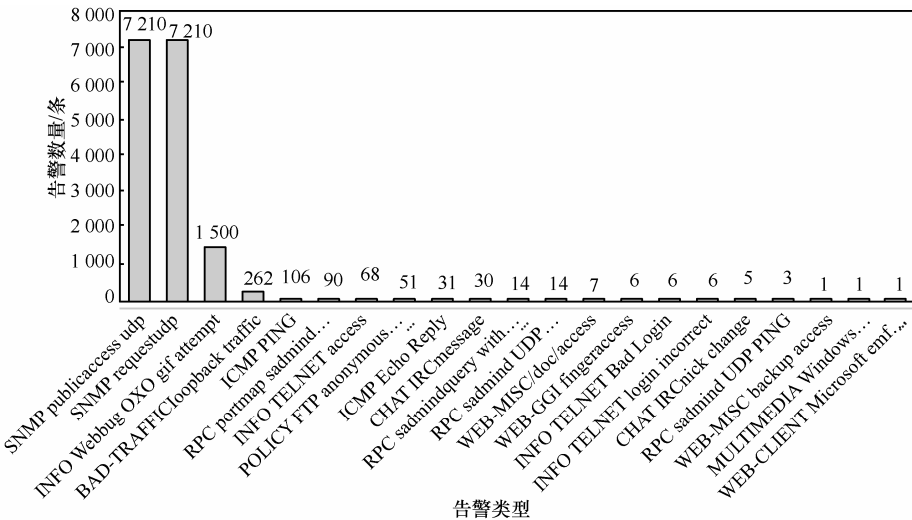


图4 告警类型重尾分布特性

$_Delete_Number$ 表示 ASS 中利用告警规则去除的告警数, $alarms_Total_Number$ 表示 ASS 中总的告警数。

$$\text{告警去除率} = \frac{alarms_Delete_Number}{alarms_Total_Number} \quad (1)$$

当参数选取 $attType_threshold=0.15$, $ip_threshold=0.15$, $\Delta T=15 \text{ min}$ 时, ASS_1 经过算法 2 后生成待检误告警去除规则 $RD_dubious$ 共 242 条, 其中经过 F 分布检验周期性真伪后, 产生真实误告警去除规则 212 条, 误告警去除率 = $\frac{16\,622 - 3\,049}{16\,622} = 81\%$ 。在此组参数下, 误告警去除

算法较准确有效。在利用误告警去除算法精简后的攻击场景序列集合 $CASS$ 中, $ASS_1 \sim ASS_6$ 存在关

联概率矩阵是有效的攻击场景序列, 其中, $ASS_2 \sim ASS_5$ 是由 ASS_1 衍生出来的告警序列; ASS_0 及 $ASS_7 \sim ASS_{13}$ 中的告警事件的数量及种类少, 属于无效攻击场景序列。

在有效 ASS 中, ASS_2 描述的攻击场景与 DARPA 2000 LLDOS1.0 符合度最高。 ASS_2 的关联概率矩阵及因果知识如图 5(a) 所示, 其告警类型的对应编号见表 3。在图 5(a) 中, 给出攻击的前 4 个阶段; 节点表示攻击模式中的一个攻击步骤; 节点中的文字是告警事件类型; 连接 2 个节点的有向箭头为步骤发生的先后顺序; 有向箭头上的数字表示从一个攻击步骤到另一个攻击步骤的可能性。

ASS_2 是由 ASS_1 衍生出的 5 个攻击场景序列中的一个。分析发现, 其他几个由 ASS_1 衍生出来的

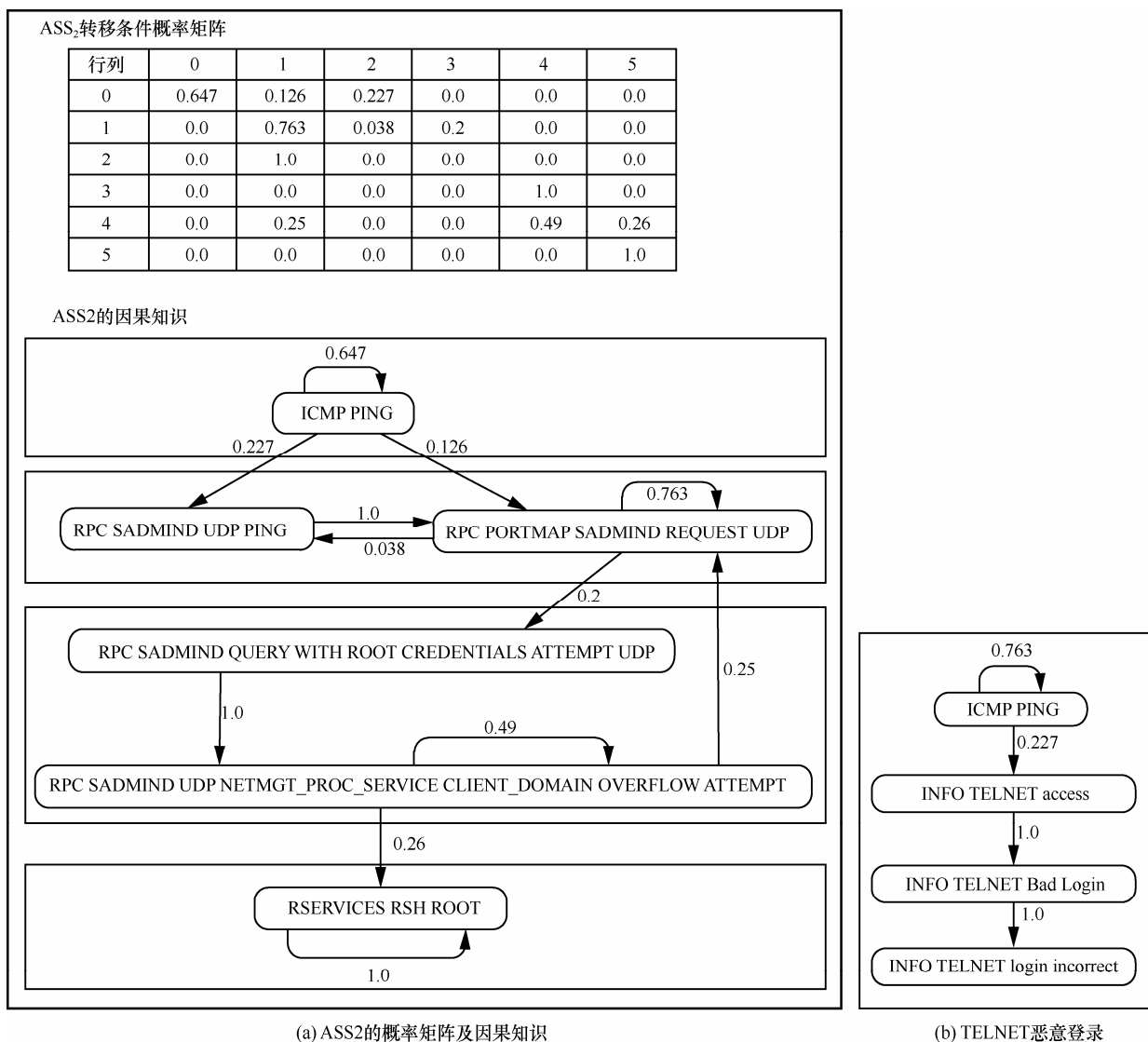


图5 CASS 中部分 ASS 的概率矩阵及因果知识

攻击场景挖掘得到的因果知识描述的是攻击者在实施攻击的各个阶段采取的其他一些尝试性攻击手段,图 5(b)描述的是 ASS_3 的因果知识,它显示攻击者在尝试通过 TELNET 恶意登录,这些尝试性的攻击手段,都是为了达到最终的攻击目的。

表 3 ASS_2 中告警类型及其编号

编号	告警类型
0	ICMP PING
1	RPC PORTMAP SADMIND REQUEST UDP
2	RPC SADMIND UDP PING
3	RPC SADMIND QUERY WITH ROOT CREDENTIALS ATTEMPT UDP
4	RPC SADMIND UDP NETMGT_PROC_SERVICE CLIENT_DOMAIN OVERFLOW ATTEMPT
5	RSERVICES RSH ROOT

本文提出的实验结果表明,本文提出的方法能够有效地精简 IDS 告警日志,并且能在日志中比较准确地发现因果知识,挖掘出告警间的内在因果关联,识别出多步攻击的模式。由于本文提出的方法考虑了告警日志中的 IP 属性,来衡量告警信息处于同一攻击场景的可能性,从而弥补了文献[16]中只考虑告警的时间属性所带来的不利影响,使攻击场景序列更符合攻击者实施多步攻击行为时的实际情况,从一定程度上保证了因果知识的准确性。此外,考虑 IDS 产生的告警本身可能存在误报,方法参考文献[20]提出的思想,利用时间序列建模的方式对每个攻击场景序列中的告警日志进行了周期性分析,将符合周期性的误告警去除,减少了误告警对因果知识发现的影响,进一步保证了所获取的因果知识的正确性。

5 结束语

本文提出的方法按照知识发现的过程,首先,明确业务对象是 IDS 中的告警日志,目的是分析多步攻击模式,重建攻击场景;其次,规范数据格式,通过告警日志中 IP 属性的相关性,构建攻击场景的序列集合,并且给出了产生误告去除规则,达到精简攻击场景序列的目的;再次,在因果知识挖掘时,采用概率统计的方法发现攻击告警序列中各个事件类型间的统计关联关系,并给出了相应算法;最后,给出了因果知识的图像化

表示。由于方法不需要依赖大量的先验经验,也不需要配置大量的参数,且在进行告警间因果关系挖掘之前对告警进行了 IP 相关分析及误告的去除,提高了所发现因果知识的准确性。通过在经典入侵场景关联数据集 DARPA 2000 上进行实验,验证该方法的有效性和可用性。

由于每个攻击场景序列中挖掘到的因果知识可能是局部的,尤其是算法 1 中衍生的攻击场景序列,所以,下一步的工作重点是对生成的因果知识进行融合,使其能够更加全面地反映攻击者的攻击步骤。

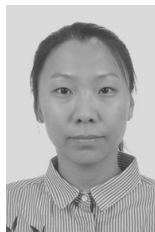
参考文献:

- [1] 国家计算机网络应急技术处理协调中心. 2015 年中国互联网网络安全报告[R]. 2016.
National Computer Network Emergency Response Coordination Center. The Chinese Internet network security report[R]. 2016.
- [2] NING P, CUI Y, REEVES D S. Techniques and tools for analyzing intrusion alerts[J]. ACM Trans on Information and System Security, 2004, 7(2): 274-318.
- [3] QIN X, LEE W. Statistical causality analysis of INFOSEC alert data[C]//The 6th International Symposium on Recent Advances in Intrusion Detection. 2003: 591-627.
- [4] MAGGI F, ZANERO S. On the use of different statistical tests for alert correlation: short paper[C]//The 10th International Conference on Recent Advances in Intrusion Detection. 2007: 167-177.
- [5] 冯学伟, 王东霞, 黄敏恒, 等. 一种基于马尔可夫性质的因果知识挖掘方法[J]. 计算机研究与发展, 2014, 51(11): 2493-2504.
FENG X W, WANG D X, HUANG M H, et al. A mining approach for causal knowledge in alert correlating based on the Markov property[J]. Journal of Computer Research and Development, 2014, 51(11): 2493-2504.
- [6] FENG X, WANG D, ZENG J, et al. Analyzing and correlating security events using state machine[C]//IEEE International Conference on Computer and Information Technology. 2010: 2849-2854.
- [7] TEMPLETON S J, LEVITT K. A requires/provides model for computer attacks[C]//The 2000 Workshop on New Security Paradigms. 2000: 31-38.
- [8] NING P, CUI Y, REEVES D S. Constructing attack scenarios through correlation of intrusion alerts[C]//The 9th ACM Conference on Computer and Communications Security. 2002: 245-254.
- [9] CUPPENS F, MIEGE A. Alert correlation in a cooperative intrusion detection framework[C]//The 2002 IEEE Symposium on Security and Privacy. 2002: 202-215.
- [10] CUPPENS F. Managing alerts in a multi-intrusion detection environment[C]//The 17th Annual Computer Security Applications Conference. 2001: 22-31.
- [11] CUPPENS F, AUTREL F, MIEGE A, et al. Correlation in an intrusion detection process[C]//The SEC102 Workshop. 2002: 153-171.
- [12] 胡亮, 解男男, 努尔布力, 等. 基于智能规划的多步攻击场景识

- 别算法[J]. 电子学报, 2013, 41(9): 1753-1759.
- HU L, XIE N N, NU E B L, et al. A multi-stage attack scenario recognition algorithm based on intelligent planning[J]. Acta Electronica Sinica, 2013, 41(9): 1753-1759
- [13] QIN X, LEE W. Discovering novel attack strategies from INFOSEC alerts[C]//The 9th European Symposium on Research in Computer Security. 2004: 439-456.
- [14] QIN X, LEE W. Causal discovery-based alert correlation[C]//The 21st Annual Computer Security Application Conference, 2005: 33-40.
- [15] MORIN B, DEBAR H. Correlation of intrusion symptoms: an application of chronicles[J]. Lecture Notes in Computer Science, 2003, 2820:94-112.
- [16] ZHANG AF, LI Z, LI D, et al. Discovering novel multistage attack patterns in alert streams[C]//The International Conference on Networking, Architecture, and Storage. 2007. 115-121.
- [17] 王泽芳, 袁平, 黄晓芳. 一种新的多步攻击场景重构技术研究[J]. 西南科技大学学报, 2016, 31(1): 55-60.
- WANG Z F, YUAN P, HUANG X F. Research of a novel attack scenario constructing method[J]. Journal of Southwest University and Technology, 2016, 31(1): 55-60.
- [18] PIETRASZEKT, TANNER A. Data mining and machine learning-towards reducing false positives in intrusion[J]. Information Security Technical Report, 2005, 10: 169-183.
- [19] 田志宏, 张永铮, 张伟哲, 等. 基于模式挖掘和聚类分析的自适应告警关联[J]. 计算机研究与发展, 2009, 46(8):1304-1315.
- TIAN Z H, ZHANG Y Z, ZHANG W Z, et al. An adaptive alert correlation method based on pattern mining and clustering analysis[J]. Journal of Computer Research and Development, 2009, 46(8):1304-1315.
- [20] 李冬, 李之棠, 雷杰. 周期性误告警去除方法研究[J]. 小型微型计算机系统, 2009, 30(7):1336-1340.
- LI D, LI Z T, LEI J. Research on the method of reducing false positives with periodicity[J]. Journal of Chinese Computer Systems, 2009, 30(7):1336-1340.
- [21] 王莉. 网络多步攻击识别方法研究[D]. 武汉: 华中科技大学, 2007.
- WANG L. Study on method of network multi-stage attack plan recognition[D]. Wuhan: Huazhong University of Science and Technology, 2007.
- [22] MIT Lincoln Lab. 2000 DARPA intrusion detection scenario spe-

cific data sets [EB/OL]. <http://www.ll.mit.edu/ideval/data/2000data.html>.

作者简介:



樊迪 (1992-), 女, 山东惠民人, 北京工业大学硕士生, 主要研究方向为网络安全、日志分析。



刘静 (1978-), 女, 北京人, 北京工业大学讲师, 主要研究方向为网络安全、可信计算。



庄俊玺 (1981-), 女, 河南新乡人, 北京工业大学讲师, 主要研究方向为网络安全、可信计算。



赖英旭 (1973-), 女, 辽宁抚顺人, 博士, 北京工业大学教授, 主要研究方向为网络接入控制、病毒防御技术、网络安全工程、可信计算理论及其应用。