# NIDS报警信息关联分析进展研究*)

刘雪飞[1,2] 马恒太[2,3] 张秉权[1] 吴伯桥[4] 蒋建春[2,3] 文伟平[2,3]

(南京理工大学计算机系 南京210096)[1] (中科院信息安全技术工程研究中心 北京100080)[2]

(中科院软件所 北京100080)[3] (湖南信息技术职业学院计算机系 长沙610200)[4]

**摘 要** 入侵检测技术是当前网络安全领域的一个研究热点,报警关联分析是其中一个重要部分。通过报警信息的关联分析,可以显著地降低入侵检测系统的误警率,提高它的检测率和可用性,帮助网络管理员更好地掌握当前网络的安全状况。本文对当前国际上报警关联分析技术的研究现状进行了综合分析,并对现有方法进行了分类和比较。

**关键词** 入侵检测,报警信息关联分析

## Progress Research of Association Analysis of Alarm Information of NIDS

LIU Xue-Fei[1,2] MA Heng-Tai[2,3] ZHANG Bing-Quan[1] WU Bai-Qiao[4] JIANG Jian-Chun[2,3] WEN Wei-Ping[2,3]

(Computer Department, Nanjing University of Science and Technology, Nanjing 210096)[1]

(Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing 100080, China)[2]

(Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)[3]

(Computer Department, Hunan Vocational Institute of Information Technology, Changsha 610200)[4]

**Abstract** Intrusion detection is a research hot point of present network security domain, association analysis of alarm information is an important part of it. Through association analysis of alarm information, rate of false alarms of intrusion detection is increasingly reduced, rate of detection and usability of it are increased, it can help administrator hold present security states of network. The paper analyzes present international research state of association analysis technology of alarm information, classifies and compares existing methods.

**Keywords** Intrusion detection, Association analysis of alarm information

## 1 前言

随着互联网的普及,网络安全问题变得越来越重要。目前,黑客网络攻击事件呈现出爆炸式的增长趋势。因此,入侵检测系统(Intrusion Detection System, IDS)[1]受到了各国政府、军队和企业等的关注,并逐渐成为安全敏感部门网络的标准配置,以监视网络、主机、文件等关键资源的安全状况。然而,入侵检测技术的实用性在业界高层是存在争议的,一些用户也对其效果存在怀疑。究其原因,在于入侵检测技术本身的局限性。目前IDS主要采用误用检测和异常检测两种方法[1],它们都不可避免地会产生漏报警和大量误报警,重复报警多,可读性差,管理员很难从中真正了解当前系统的安全状况。异常检测方法[1]是通过建立系统或用户的正常(或异常)行为轮廓,如果发现观察值偏离(或符合)程度超过预定的阈值就会产生报警。事实上,异常行为并不总是意味着攻击,所以会发生误报警;同时,攻击者如果意识到检测系统的存在,可以有意识地诱导系统以适应其行为,从而导致漏报警。误用检测方法[1]是通过定义和匹配攻击模式实现,实际上,穷尽定义攻击模式是一件不可能的事,因此,误用检测也不可避免地会出现漏报警;当然,不考虑目标系统状态的检测模式也不可避免产生误报警。

针对这些问题,研究者们在不断改进检测算法、完善攻击模式库的同时,开始考虑利用攻击事件之间的关联来提高检测的准确性和可用性,这方面的研究主要有两个分支:一是在检测时实时地对网络事件进行关联;二是对报警信息进行关联分析。二者都基于同样的思想,即攻击者要实现其目的通常是通过一系列攻击步骤来完成的,而不是通过单个攻击行为。因此,通过关联分析技术可以减少误报警,提高检测率,大大提高报警信息的可用性。

本文对当前IDS报警信息关联方法的研究现状进行了分类和总结,分析了这些方法的优缺点。第2节介绍概率关联方法;第3节介绍基于数据挖掘关联分析方法;第4节介绍基于因果关系的混合方法;最后是结束语。

## 2 概率关联方法

### 2.1 基于特征相似的概率关联方法

为了融合不同IDS的优点,往往在不同网络域配置不同类型的IDS。对来自不同类型IDS的报警信息进行综合关联分析,可以有效地识别真正的攻击事件,对减少重复报警和误报警有很大作用。目前,不同类型IDS产品的开发没有采用统一标准,报警数据格式和内容不统一,判断是否是对同一事件的报警相当困难。

文[2]提出利用报警信息特征的相似性来解决该问题,其方法描述如下:(1)定义特征相似函数。对报警信息的共有特

*)本文资助项目:国家自然科学基金:60083007;国家重点基础研究发展规划(973):G1999035810.高技术研究发展计划(863):2003AA144030.中科院软件所基础课题研究基金:CXK45634.刘雪飞 博士生,研究方向:信息安全,数据挖掘;马恒太 博士,研究方向:信息安全;张秉权 博士生,研究方向:信息安全;文伟平 博士生,研究方向:信息安全.

征(如攻击源、攻击目标、攻击类型、时间戳)分别定义相似函数。(2)定义特征相似期望。相似期望是关联的必要非充分条件,它表达了对报警信息特征相似的先验期望,这个相似期望大小的定义依赖于特定上下文。因为不同的特征对于报警信息是否整体相似的作用是不一样的,所以采用不同特征的相似度加权值来计算整体相似度。(3)定义特征最小相似度。如果某特征的相似度小于最小相似度,则两条报警信息的该特征不具有相似性,即取值为0。(4)定义报警相似度阈值域。如果两条报警信息的相似度不包含在相似度阈值域,则两条报警不相似。(5)计算报警相似度。其计算公式为:$sim(X,Y)=\sum_j E_j sim(X_j,Y_j)/\sum_j E_j$,其中 $X$ 表示候选元报警,$Y$ 表示新的报警,$j$ 是报警消息的特征索引,$E_j$ 是对第 $j$ 个特征的相似期望,它代表特征的权值,$X_j$ 和 $Y_j$ 分别表示报警消息 $X$ 和 $Y$ 的第个 $j$ 特征的值。文[2]给出的实验结果表明,通过该关联分析,可减少1/2到2/3的报警数据,其缺点是所分析比较的报警信息必须具有共有特征,另外,它也不能发现报警消息之间的因果关系。

### 2.2 基于攻击场景构建的概率关联方法

通过对攻击过程的研究发现,一次完整的攻击过程通常经历五个步骤,即:目标系统信息收集、目标漏洞探测、权限提升、实施破坏、攻击痕迹清除。因此,可对同属一个攻击场景的报警信息进行关联。

文[3,4]采用原子模型方法:每从IDS接收到一个报警信息,就与已构建的攻击场景进行概率关联,即计算该报警属于已知攻击场景的概率,把该报警归为概率最大的攻击场景,如果所有的关联概率都低于预先给定的阈值,则创建新的攻击场景。一旦报警归为一个攻击场景,就不再改变。概率计算可采用手工编码方法、启发式方法或数据挖掘方法,下面简单介绍启发式方法,其它方法可参见文[4]。

报警消息是否属于给定攻击场景的计算公式为:$sim(X,Y)=l_{ij}\cdot\sigma_{ij}(\Delta t)\cdot R_{ij}(r)$。其中 $X$ 表示待处理的报警消息;$Y$ 表示攻击场景中最新的报警消息;$l_{ij}$ 表示两个报警消息之间的联系;$\sigma_{ij}(\Delta t)$ 表示两条报警消息之间的时间间隔;$R_{ij}(r)$ 表示两个报警消息的源 $IP$ 地址范围。$l_{ij}$、$\sigma_{ij}(\Delta t)$、$R_{ij}(r)$ 的取值范围均为[0,1],因此 $sim(X,Y)$ 的取值也是[0,1]。$l_{ij}$、$\sigma_{ij}(\Delta t)$、$R_{ij}(r)$ 的具体含义如下:$l_{ij}$ 表示来自第 $j$ 个攻击阶段的报警消息紧跟来自第 $i$ 个攻击阶段的报警消息的概率。如,扫描之后发生权限提升的概率要大于实施破坏之后发生权限提升的概率,这是因为,攻击者往往要通过扫描才有可能得到访问系统的权限,而一个没有相当权限的攻击者不太容易实施破坏。$\sigma_{ij}(\Delta t)$ 是 $sigmoid$ 函数,定义为 $\sigma_{ij}(\Delta t)=1/(1+e^{\alpha+\beta\Delta t})$。$R_{ij}(r)$ 是两条报警消息源IP地址的相似程度,它是 $r$ 的函数,其取值依赖于报警消息所处的攻击阶段。$r$ 表示两个IP地址的相同二进制位数,其取值范围为[0,32],$r=32$ 说明两个IP地址完全一样,$r=0$ 说明两个IP地址不可能属于同一个子网。在五个过渡类型阶段,$r$ 取值为 $r=0,8,16,24,32$,$r$ 的其他取值由 $R_{ij}(r)$ 的线性插值决定,如 $DoS$ 对攻击中的所有的 $r$ 都有 $i=j=DoS$,则 $R_{ij}(r)$ 可有一个相对很大的值,这样就能够识别使用假IP地址进行的攻击。该方法的优点是:能够发现利用假冒源IP地址和潜伏期很长的攻击场景;关联速度快,在不到2秒内,可对16000个报警分配攻击场景[4]。其缺点是:由于场景的分配基于原子模型,一旦一个攻击场景出错,就会影响到后续报警信息的关联,因此该方法需要在减少错误场景创建上进行改进。

## 3 基于数据挖掘的关联分析方法

数据挖掘[5]是一门对过去、历史的学习掌握规律从而把握未来的技术。其中的聚类分析、序列分析、关联分析技术已成功应用于入侵检测系统。如,Barbara[6,7]采用增量式数据挖掘方法实时检测异常网络流量模式;Lee 和 Stolfo[8]利用数据挖掘技术自动构建检测特征和对检测入侵的分类器进行训练,希望构建的IDS更加系统化,同时克服现有IDS的局限性;Barbara 和 Jajodia[9]出版了一本专著,对数据挖掘在计算机安全中的应用进行了讨论。

### 3.1 聚类分析

聚类分析是根据特征对对象进行分类的一种多元分析技术,把特征相近的个体归为一类,使得同一类中的个体具有高度的相似性,不同类之间的个体具有高度的相异性。

*3.1.1 基于攻击场景的启发式聚类* 攻击场景是指具有共同特征的事件集合。报警信息中的特征都可作为聚合属性,目前一般采用三个聚合属性:攻击源、攻击目标、攻击类型。场景定义为:(攻击源,攻击目标,报警类型,严重级别)。

文[11]根据攻击者采取的攻击方法定义了七种攻击场景:(1)具有相同攻击源、攻击目标、攻击类型,如攻击者对Web服务器发动一系列的Web攻击;(2)具有相同攻击源、攻击目标,如攻击者对目标的不同服务发动攻击;(3)具有相同攻击目标、攻击类型,如攻击者共同协作以对同一目标实行分布式攻击,使之拒绝服务;(4)具有相同攻击源、攻击类型,如攻击者对不同的域名服务器发动攻击;(5)具有相同攻击源,如攻击者对不同目标发动不同攻击;(6)具有相同攻击目标,如分布式攻击,不同攻击者针对系统不同漏洞发动攻击;(7)具有相同攻击类型,如不同攻击者针对同一漏洞发动攻击。该方法的优点是方法简单,容易实现,开销小。其缺点是需要事先知道相应的攻击场景,不能发现新的攻击场景。

*3.1.2 面向属性归纳的概念聚类方法* 面向属性归纳AOI(Attribute-Oriented Induction)是数据概化的一种方法,它由 Cai, Cercone 和 Han[12]于1991年首次提出。概念聚类[5,13,14]依据对象的概念描述形成聚类簇,一般分两步进行:首先发现合适的簇;其次形成对每个簇的描述。

概念聚类主要优点是:(1)通过聚类簇的可理解性描述,方便了聚类解释;(2)概念聚类擅长处理类别属性特征数据,如IP地址、端口号和报警类型等。AOI首先是作为一种数据总结技术被提出,后来建立起与概念聚类之间的联系[15,16],成为概念聚类的工具。下面是根据AOI算法进行修改的面向属性的聚类算法。

输入:报警信息集合 $L$,一个聚类的最小报警信息数 $min\_size$,组成报警信息的各个特征的概念层次表 $T_1,\cdots,T_n$。

输出:概化的报警信息。

算法:

```
O:=L;
while(true){
    对O中每一个报警信息α{
      C:=报警消息α覆盖的报警消息x的个数;
      如果 C>min_size,则终止并返回报警信息α;}
    根据启发性知识选择报警信息的一个特征 A_i,i∈
    {1,…,n};
```

对每一个报警 $\alpha$，$\alpha[A_i]:=\text{parent}(\alpha[A_i],T_i)\}$；

概化属性的选择：对于 $A_i$，设 $f_i$ 表示一个报警信息覆盖其他报警信息的最大个数，存在一个报警信息 $\alpha^* \in O$，$\alpha^*$ 所覆盖的报警信息是最多的，如果 $f_i$ 小于 $\min\_size$，则需要对 $A_i$ 进行概化，因此选择 $A_i$ 概化。

概化的结果使报警信息可读性更强。

### 3.2 序列模式挖掘方法

序列模式挖掘[17]是指挖掘相对时间或其他模式出现频率高的模式—频繁场景。通过序列模式的挖掘[13,14]，从理论上发现了报警信息之间有价值的关联模式：(1)发现攻击工具的特征—场景：如，一个攻击场景中，来自同一攻击源的报警消息，如果攻击目标不同且报警序列相同，通常这样的攻击场景表明攻击者使用同一攻击工具对不同目标进行了攻击。(2)发现场景规则：通过已发生的攻击可以对攻击者的行为进行预测，并可采取适当措施对抗。(3)发现隐含报警(复合报警)：有些报警可能包含或隐含其他报警。如 IDS 报警消息“TCP FIN Host Sweep”隐含报警信息“Orphaned FIN Packet”，反之则不然。(4)对合法系统操作引起的报警进行过滤：异常并不一定意味着入侵，因此，对非入侵行为所造成的报警消息进行预先过滤处理，可以减少分析的负担。

该方法的缺点是：自动化程度较低，仅有1%的报警数据可被自动处理；产生的攻击场景难以理解，定位操作很耗时，需要寻找更实用的报警序列模式挖掘算法。如序列挖掘算法[18]已成功应用于特权进程序列的挖掘中，我们认为该算法可以进行拓展，用于报警信息关联分析。

### 3.3 关联方法

关联方法[5,19,20]由 Agrawal 等人于1996年提出，它是寻找给定数据集中项之间的有价值联系的方法。关联规则的挖掘分两步：(1)找出所有的频繁项集；(2)由频繁项集产生强关联规则。

关联方法的典型应用实例是购物篮分析。同样，该方法可用于 IDS 报警信息关联分析[19,20]，如 IBM 提供了遍布全球的客户实时入侵检测服务，在客户网络中配置 NetRanger、CiscoSystems 等商用 IDS 产品，所有的报警信息通过 Internet 送到 IBM 的网络操作中心。因此，如何有效管理不同客户的报警信息成为其面对的一个难题，由于每一个 IDS 有独立的历史报警数据，它们在报警类型、报警速率、一天内或一周内的报警分布等方面是不同的，因此，需要构建不同 IDS 的正常(或异常)轮廓。具体方法是：用频繁项集来刻画每一个 IDS 的正常报警。首先，把来自同一客户的连续报警流分为单个报警脉冲，一个报警脉冲对应于关联分析中的一次交易，其中一个报警消息称为项。然后应用 IBM 的 Intelligent Miner for Data toolkit 来发现频繁报警集合，最后产生关联规则用来过滤报警信息。

关联方法没有考虑报警信息之间的时间顺序，在有些情况下，报警序列(即时间因素)是很重要的，因此要采取序列模式分析作为补充；同时该方法没有考虑丢失相关报警信息所带来的风险。

## 4 基于因果关系的混合方法

攻击的先决条件是攻击成功的必要条件。如服务存在漏洞是进行远程缓冲区溢出攻击的先决条件。通过攻击，攻击者还可取得实施进一步攻击的条件，如发现服务漏洞、安装木马程序等。因此可根据攻击的前提和结果进行关联[21,23,24,26,27]，依据其因果关系的表达方式，分为 Requires/Provides 模型方法和关联规则方法。

### 4.1 Requires/Provides 模型方法

文[21]采用 Requires/Provides 模型描述攻击场景，在该模型中，引入能力(capabilities)和概念(concepts)两个术语。能力是攻击发生所需要的条件(如 telnet 需要合法的用户名和口令及开放 telnet 服务)，更正式地，它是一个封装了语义类型属性的语义对象，该对象描述特定的能力实例和与其他能力关联的方法。概念是形成攻击场景子任务的抽象情况。根据攻击的抽象组件概念定义攻击场景，每一个概念是单独描述的，概念需要能力来支撑，能力之间能互相提供能力。

该模型的核心是攻击描述语言 JIGSAW[22]，它可以表达和描述复杂的攻击场景。一般攻击描述是根据攻击所利用的漏洞或事件序列给出，但这些方法无法刻画复杂攻击场景或概括未知攻击。该模型中，攻击描述为一系列的能力集，而不是事件序列。能力提供对抽象攻击概念的支持，反过来概念又提供新的能力。

虽然作者提到可以应用该模型进行报警信息关联分析，但是 JIGSAW 很难成为一个实际可行的报警信息关联技术，这是因为，该方法要求所有的攻击前提都必须满足才考虑攻击的结果，如果 IDS 发生漏报警，则不能关联检测到的攻击事件。该方法目前只是理论讨论，并未进行实验和测试。

### 4.2 关联规则方法

该方法用关联规则表示攻击场景，它以谓词为基本构建块对每种类型攻击进行编码，描述攻击的前提和结果。如用 $UDPVulnerableToBOF(VictimIP, VictivmPort)$ 表示通过扫描攻击发现 UDP 服务漏洞以确定是否进行了缓冲区溢出攻击。

攻击发生所必须具备的条件称为攻击的先决条件，实施攻击步骤后所取得的效果称为攻击的结果。对攻击的结果与后续攻击的先决条件进行比较，可重构攻击序列。Ning[23,24]和 Cuppens[26,27]所作的工作都是基于关联规则的，但具体实现稍有不同，下面分别介绍。

Ning 用概念 hyper-alert type 表示报警类型的前提和结果，它是一个三元组(fact，prerequisite，consequence)，其中 fact 是属性名称集合，prerequisite 表示谓词之间的逻辑连接，谓词中的自由变量就是 fact 中的元素，consequence 是谓词集合，它的所有自由变量属于 fact。hyper-alert type 的实例为超报警(hyper-alert)。超报警之间的关系用图形表示，即形成超报警关联图，该图清晰地表示了隐藏在攻击背后的攻击策略。系统的实现由五大部分组成：(1)知识库。存放 hyper-alert type 的一些必要信息以及谓词之间的隐含关系，这些信息都由 XML 文件存贮，报警关联初始化时从 XML 文件读取相关信息并将其转换存储于知识库中。(2)报警预处理器。根据知识库中的信息从原始报警信息中分离出超报警及辅助数据信息。(3)关联引擎。根据超报警和辅助信息执行实际的关联任务。(4)超报警关联图产生器。从数据库中抽取关联报警，产生关联文件。(5)可视化。利用 GraphViz 可视化超报警之间的关联。该方法的优点是：不依赖预定义攻击场景以发现相关攻击序列，能够识别攻击企图，关联范围没有限制，只要有联系的报警消息都能进行关联，即使是一些相关的失败攻击或被 IDS 忽略的信息。此外它提供了超报警关联图机制以显示通过关联分析构建的攻击场景，通过超报警关联图能够更好地理解攻击者的攻击意图。缺点是：(1)由于依赖于 IDS 的报警信息，因此，如果发生漏报警，丢掉了攻击序列中的关键报警消息，则一个攻击场景就被分为了多个部分，会降低甚至丧失

关联的意义;(2)盲目攻击的报警信息得不到关联,当然,该情况可通过诸如概率关联方法加以补充;(3)方法的性能依赖于攻击模型。

同样,Cuppens 采用关联规则关联报警信息,其实验系统包含五大模块:(1)报警管理模块。采用 XML 技术,把来自不同 IDS 的报警消息统一到关系数据库中,该模块采用 prolog 语言实现,即把报警消息转化为 prolog 事实库,再把事实转化为关系集合,方便分析和比较。(2)聚类模块。对报警信息进行分组,同组信息可以来自同一 IDS,也可来自不同 IDS,根据相似关系进行聚类,相似关系用专家规则来表示,系统定义了基于攻击类型、时间、源和目标的相似规则。(3)合并模块。对每个聚类进行合并,产生全局报警,合并内容包括攻击类型、时间、源和目标信息,这样的报警更全局、更精确。(4)关联模块。把来自同一攻击者的攻击事件进行关联,以识别攻击者的攻击意图。误用检测报警消息(事件之间的关联关系可以明确给出的事件)采用显关联的方式,关联规则由手工给出;异常检测报警消息采用半显式关联方式,关联规则根据攻击的前提和结果离线产生,该方法基于 LAMBDA[25]对攻击进行描述。(5)意图识别模块。为了明确应该采用何种响应和反击措施,以阻止攻击者的进一步入侵,首先要识别入侵意图,包括对攻击者过去、现在和未来行为的判断。

**结束语** 入侵检测系统报警信息关联分析是近几年才开展起来的研究工作,大多处在理论探讨和实验测试阶段,其面临的问题主要有:攻击场景准确描述、关联规则自动提取、攻击意图识别、关联分析的效率、关联结果的可读性和可视化等,这些问题都有待进一步研究与解决。

## 参 考 文 献


1 Denning D E. An intrusion-detection model. IEEE Trans. Softw. Eng. ,1987,SE-13:222～232
2 Valdes A, Skimmer K. Probabilistic Alert Correlation. In: 4th Workshop on Recent Advances in Intrusion Detection (RAID), LNCS, Springer Verlag,2001. 54～68
3 Dain O,Cunningham R. Building Scenarios from a Heterogeneous Alert Stream. In:Proc. of the 2001 IEEE
4 Dain O,Cunningham R. Fusing a heterogeneous alert stream into scenarios. In: Proc. of the 2001 ACM Workshop on Data Mining for Security Applications,2001. 1～13
5 Jwhan,Micheline K. Data mining concepts and techniques. China Machine Press,2001
6 Barbara D,Couto J,Jajodia S,Popyack L,Wu N. ADAM: Detecting Intrusions by Data Mining. In: IEEE workshop on Information Assurance and Security, 2001
7 Barbara D,Wu N,Jajodia S. Detecting Novel Network Intrusion Using Bayes Estimators. In: First SIAM Int'l Conf. On Data Mining(SDM'01), 2001
8 Lee W,Stolfo S J. A Framework for Constructing Features and Models for Intrusion Detection Systems. ACM Transactions on Information and System Security,2000,3(4):227～261
9 Barbara D,Jajodia S. Applications of Data Mining in Computer Security. Kluwer Academic Publisher,Boston,2002
10 Fawcett T, Provost F. Adaptive Fraud Detection. Data. Mining and Knowledge Discovery,1997,1:291～316
11 Debar H,Wespi A. Aggregation and correlation of intrusion-detection alerts. Recernt Advances in Intrusion Detection. LNCS 2212, 2001. 85～103
12 Cai Y,Cercone N,Han J. Attribute-Oriented induction in relational database. In: G. Piatetsky-Shapiro and W. J. Frawley, eds. Knowledge Discovery in Database,Cambridge, MA:AAAI/MIT Press,1991. 213～328
13 Julisch K. Mining Alarm Clusters to Improve Alarm Handling efficiency. In:17th Annual Computer Security Applications Conf. (ACSAC),Dec. 2001. 12～21
14 Julisch K,Dacier M. Mining intrusion detection alarms for actionable knowledge.
15 Han J,Fu Y. Exploration of the power of attribute-oriented induction in data mining. In: U. M. Fayyad, G. Piatetsky-Shapiro, P. Smyth, and R. Uthrusamy,eds. Advances in Knowledge Discovery and Data Mining. AAAI Press/MIT Press,1996
16 Heinonen O,Mannila H. Attribute-Oriented induction and conceptual clustering:[Technical Report Report-C-1996-2]. University of Helsinki, 1996
17 Mannila H, Toivonen H, Verkamo A I. Discovering frequent episodes in sequences. In:proc. of the 1st intl. conf. on knowledge discovery in databases and data mining, Montreal, Canada, Aug. 1995
18 Wespi A,Dacier M. An intrusion-detection system based on the Teiresias pattern-discovery algorithm. EICAR In:Proc. 1999
19 Manganaris S,Christensen M,Zerkle D,Hermiz K. A Data Mining Analysis of RTID Alarms. Computer Networks,2000,34(4)
20 Zerkle D. A Data-Mining Analysis of RTID. In: Second Intl. Workshop on the Recent Advances in Intrusion Detection (RAID'99),Purdue,USA,Oct. 1999
21 Templeton S,Levit K. A requires/provides model for computer attacks. In: Proc. of New Security Paradigms Workshop, ACM Press,2000. 31～28
22 http://seclab. cs. ucdavis. edu/global-guard/meetings/stevendarpa/
23 Ning P,Cui Y. An intrusion alert correlator based on prerequisites of intrusions:[Technical Report TR-2002-01]. North Carolina State University, Department of Computer Science,2002
24 Ning P,Reeves D S. Correlating alerts using perquisites of intrusions:[Technical Report TR-2001-13]. North Carolina State University, Department of Computer Science,2001
25 Cuppens F, Ortalo R. LAMBDA: A Language to Model a Database for Detection of Attacks. In: Proc. of the Third Intl. Workshop on the Recent Advances in Intrusion Detection (RAID'2000),Toulouse,France,Oct. 2000
26 Cuppens F. Managing alerts in a multi-intrusion detection envronment. In:17th Annual Computer Security Applications Conf. (ACSAC). New-orleans,Dec. 2001
27 Cuppens F,Miege A. Alert correlation in a cooperative intrusion detection framework. In: Proc. of the 2002 IEEE Symposium on Security and Privacy,2002


(上接第54页)

(5)$k$ :分配3比特,即001,值为1,映射成1。

(6) $P_{II}$:分配10比特,即0110111011,值为0.763,映射成1.645。

(7)$x_{0.II}$:分配11比特,即00111100010,值为-0.471。

(8)$U_{II}$:不分配,取固定值0。

(9)$T_{max}$:分配10比特,即10100111000,值为1336,映射成2336。

于是得到系统密钥参数 Key=(0.295,0.330,0.5,6,1,1.645,-0.471,0,2336)。

**结束语** 本文对文[1]中的多级混沌加密系统进行了安全性分析,包括密钥空间、密文对密钥的敏感性、抗攻击能力等方面,分析结果表明该系统具有良好的密码学特性。同时给出了如何将用户口令映射为系统加密参数的关键技术,这对工程应用具有一定指导作用。

我们注意到,混沌加密系统还有别于传统加密系统,主要是缺少一个评估加密算法安全性以及性能的标准,目前只能依靠有限的数值仿真算法来进行检验,这方面的工作需要进一步加强。

## 参 考 文 献


1 彭军,张伟,廖晓峰,吴中福.一种改进的多级混沌加密系统.计算机科学,2002,29(9):137～139,145
2 Li Shujun, Mou Xuanqin,Cai Yuanlong. Improving security of a chaotic encryption approach, Phys. Lett. A, 2001, 290 (3-4): 127～133
3 Alvarez G,Montoya F,Romera M,Pastor G. Cryptanalysis of a chaotic encryption system. Phys. Lett. A, 2000, 276 (1-4): 191～196
4 Alvarez E,Fernández A,García P,Jiménez J,Marcano A. New approach to chaotic encryption. Phys. Lett. A, 1999, 263 (4-6): 373～375
5 Shannon C E. Communication theory of secrecy system. The Bell System Technical Journal, 1949, 28(4): 656～715
6 Kocarev L. Chaos-based cryptography: A brief overview. IEEE Trans. on CAS-I, 2001, 1(3): 6～21
7 Stallings W[美]著,杨明,胥光辉,齐望东,等译.密码编码学与网络安全:原理与实践(第二版).北京:电子工业出版社,2001