基于条件随机场的改进型BLP访问控制模型

马 萌[1,2] 唐 卓[1,2,3] 李仁发[1,2] 熊燎特[1,2]

(湖南大学信息科学与工程学院 长沙 410081)[1] (嵌入式与网络计算湖南省重点实验室 长沙 410081)[2]

(武汉大学软件工程国家重点实验室 武汉 430072)[3]

摘 要 针对大多访问控制模型缺乏对系统安全状态和风险的动态感知能力这一问题,通过将基于条件随机场的机器学习方法引入BLP模型的规则优化中,提出一种动态BLP模型——CRFs-BLP。该模型首先通过对历史访问日志进行预处理与标注,来提取特征值。然后用CRF++工具包对其学习和训练,使模型规则能够根据当前系统的安全状态及安全事件进行动态调整,还可以动态地限制敏感客体的读写范围。最后,通过实验表明了模型在实际环境中的有效性和准确性。

关键词 访问控制,条件随机场,机器学习,BLP模型

中图法分类号 TP301 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.030

Improved BLP Model Based on CRFs

MA Meng[1,2] TANG Zhuo[1,2,3] LI Ren-fa[1,2] XIONG Liao-te[1,2]

(College of Computer Science and Electronic Engineering, Hunan University, Changsha 410081, China)[1]

(Key Laboratory for Embedded and Network Computing of Hunan Province, Changsha 410081, China)[2]

(State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China)[3]

Abstract As most access control models are short of the ability to perceive the system security status and risks in a dynamic way, the paper introduced a machine learning method CRFs into the rule optimization of BLP model, and proposed a dynamic BLP model, CRFs-BLP. After preprocessing and tagging the history access log, it will extract the feature set, then CRF++ toolkit will be taken to finish the study and training of these datasets, so the model can be adjusted dynamically according to the current secure state and events in system, and the read-write scope for sensitive objects will be limited dynamically. Finally, the experiment shows the availability and accuracy of the model in a real environment.

Keywords Access control, CRFs, Machine learning, BLP model

1 引言

计算机安全是计算机与网络领域信息安全的一个分支。随着计算机的普及和网络的发展,计算机安全已成为一个重大问题。目前计算机攻击已非常普遍和多样化,如不请自来的欺骗用户、获取用户信息的电子邮件,又如擦除系统数据及关闭计算机系统的危险病毒等。

访问控制[1-3]机制是保护数据安全的重要途径,通过使用某种途径明确地对访问进行许可或限制,以此来约束用户对特定资源的访问,从而避免非法用户的访问或者因合法用户的失误操作而导致的安全问题。但现有访问控制模型大多缺乏对系统安全状态和风险的动态感知能力,访问控制策略及规则一旦确定,在整个系统的执行及状态变迁过程中就不会变化,这将给系统的攻击者带来发现漏洞的可能,从而给系统带来风险。

对于安全性需求较高的系统,如政府、军事部门或银行系统,资源多以不同密级的形式进行划分,整个系统则采用严格的强制访问策略保护数据机密性和完整性。Bell-LaPadula模型[4,5]是David Bell和Leonard La Padula于1973年创立的模拟军事安全策略的计算机安全模型,其本质是对具有密级划分信息的访问控制,是最早、最广泛的一种计算机多级安全策略模型。模型的基本思想是给每一个数据对象定义一个安全级来表示它所包含信息的敏感性;同时给每一个用户定义一个安全级用于表示它能访问的数据对象。每个安全级由密级和范围的集合组成。BLP模型定义了系统、系统状态、状态间的转换规则,制定了一组安全特性,对系统状态和状态转换规则进行约束。如果系统的初始状态是安全的,经过一系列规则转换之后仍是安全的,那么该系统就是安全的。图1给出了BLP模型所定义的系统。其中X表示请求序列集,Y表示结果序列集,Z表示状态序列集,下标t表示离散时刻集。

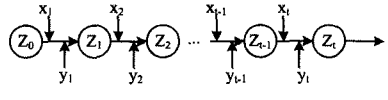

图1 BLP系统

到稿日期:2014-08-04 返修日期:2014-11-28 本文受国家自然基金项目(61103047),863计划(2012AA01A301-01),武汉大学软件工程国家重点实验室开放基金(SKLSE2012-09-18)资助。

马 萌(1990-),女,硕士生,CCF学生会员,主要研究方向为访问控制、机器学习,E-mail:horsemengyyy@126.com;唐 卓(1981-),男,博士,讲师,主要研究方向为分布式计算、云计算。

在分布式环境下，任意时刻用户的请求是随机的；而系统对请求 x 做出的决策 $y \in Y$ 是固定的，任何时刻系统状态的取值都可以是 Z 中的任意一个，所以 Z 也是随机的。由于请求的多样性，BLP 现有的安全公理和规则不能很好地适应系统的变化，以至于会出现以下情况：

第一，传统 BLP 模型的安全性基于平稳性原则。平稳性原则要求主体和客体一旦被创建，它们的密级在整个生命周期都不发生改变。尽管平稳性原则的执行保证了模型的安全性，但是，在实际应用中发现，这样做往往造成对主体行为限制过强，严重影响了系统的可用性。也就是说，“向下读，向上写”这一策略限制了高级别主体产生的公开信息向低级别流动，以及高密级主体向非敏感客体写数据的合理要求。为了提高模型的可用性，Bell 引入了可信主体，允许具有可信范围的主体在受控范围内违反 SS-性质和 *-性质。由于这些可信主体不受任何访问控制规则的限制，导致可信主体的权限过大，违背了最小特权原则。

第二，在现有的 BLP 应用场景中，读写敏感客体的主体范围往往是确定的，“向上写”使安全等级较低的用户可以对高于其安全等级的客体任意添加信息，使得系统的完整性没有任何保证。在实际情况下，某些敏感客体在其生存周期中不应该总是被高于其安全级的主体读，也不应该总是被低于其安全级的主体写，而是动态判断该客体是否允许跨级访问。

另一方面，传统的安全软件需要大量的人力来识别威胁，从威胁中提取特征并将这些特征编码为软件以检测威胁，这个人力密集的过程可以有效地运用机器学习算法来缓解。机器学习是人工智能的核心，是使计算机具有自我学习能力的一种有效途径。机器学习算法是一类从数据中自动分析获得规律，并利用规律对未知数据进行预测的算法。目前有多种比较成熟的算法，如贝叶斯分类、近邻法、决策树、神经网络、支持向量机、隐马尔科夫模型和条件随机场等。本文利用机器学习方法对历史数据进行训练，以修正 BLP 模型规则中存在的缺陷。

综上所述，现有应用中的 BLP 模型缺乏对系统安全状态和风险的动态感知能力。本文采用条件随机场理论对 BLP 模型重新建模，提出了一种基于条件随机场的改进型 BLP 访问控制模型——CRFs-BLP(Conditional Random Fields based Bell-LaPadula Model)，对现有的系统访问日志进行分析与标注，然后采用机器学习的方法建模，对经验数据进行学习，使模型规则能够根据现在系统的安全状态及安全事件进行动态调整，包括高安全级的非密级信息可以流向低安全级和动态限制敏感客体的读写范围。

2 相关工作和进展

BLP(Bell-La Padula)模型问世至今，已经在各种安全需求较高的系统中得到了广泛的研究和应用。然而，随着安全理论的不断发展，BLP 模型也逐渐暴露出自身的局限性。针对 BLP 模型的缺陷，国内外学者提出了针对 BLP 模型的一系列改进方案。

在完整性方面，Shen[6] 等人基于 Lattice 理论对 BLP 进行分析并提出 BLP-I 模型，该模型具有较好的完整性及机密性。文献[7]提出了一个可动态调节主体安全标记(即主体敏感级)的改进的 BLP 模型。文献[8]利用保密性标识和可信度标识共同构成主客体的访问标识，以此来改善 BLP 模型的完整性，但它只对“添加”进行约束，完整性策略限制不够严格。文献[9]对上行信息流增加了必要的限制，但它只是缩小了“上写”的范围，并未从根本上保护信息的完整性。

在可用性方面，Lee[10] 认为可信主体在特定情况下才是可信的，提出了部分可信主体的概念，并将可信主体的行为限定在一定范围内。在开发 GEMSOS[11] 时，Schell 等人也提出了类似的多级主体的概念以限制可信主体的特权，但 Lee 和 Schell 没有明确给出主体安全标记的调整方案。文献[12]给出了可信度判定规则，用可信度调节主体的访问权限，但可信度的定义并不明确。文献[13]在 BLP 模型中增加主客体的可信度标记和可信度评估函数，建立了对可信主体的约束机制，但没有证明模型的安全性，难以确定调整后的系统是否安全。

基于机器学习的计算机安全应用是近年来计算机安全领域里的一个应用分支，伴随着计算机安全问题的日益严峻和复杂化，基于机器学习的计算机安全应用已经出现了很多研究成果。Yamaguchi 等人使用主成分分析(Principal Component Analysis)和文本挖掘技术挖掘源代码中的缺陷[14]。该方法将代码嵌入到向量空间并利用机器学习自动化地检测 API 使用模式；Bozorgi 等人提出了训练支持向量机[15](SVM)，并用它预测一个漏洞是否及在多久之后有可能被利用[16]，该支持向量机工作在高维特征向量上，是从文本字段、时间戳、交叉引用和现有的漏洞披露报告的其他条目中提取出来的；谭小彬[17] 等建立了一个计算机系统运行情况的隐 Markov(HMM)模型，然后在此模型上提出了一个实时、准确和高效的异常检测算法。此外，人工神经网络、决策树、朴素贝叶斯、最大熵模型和条件随机场等机器学习方法也被广泛地应用于恶意网页和恶意代码检测、入侵检测领域[18-21]。其中条件随机场是一种用于结构数据分类的无向图模型。通常使用训练数据得到模型，然后给定输入序列，使输出序列的条件概率最大化。CRFs 由于克服了隐马尔科夫模型 HMM 严格的独立性假设和最大熵模型 MEMs 的标记偏置问题(Label bias problem)的缺点，因此被广泛地应用于各种机器学习和自然语言处理任务中，例如汉语分词、词性标注、命名实体识别等。

3 CRFs-BLP 的基本模型

3.1 基本概念和定义

设某信息系统参数如下：$S=\{s_1, s_2, \cdots, s_n\}$ 是主体的集合；$O=\{o_1, o_2, \cdots, o_n\}$ 是客体的集合；$C=\{c_1, c_2, \cdots, c_n\}$ 是密级集合，其中 $c_1 \leqslant c_2 \leqslant \cdots \leqslant c_n$，如一般≤秘密≤机密≤绝密；$K=\{k_1, k_2, \cdots, k_n\}$ 是部门或类别集合；$A=\{r, w, e, a, c\}$ 是访问权限集，分别表示读、写、执行、追加和控制访问权限。

BLP 模型是一种状态机模型，状态是系统中元素的表示形式，状态 $v \in V$ 由一个有序三元组 (b, M, f) 表示，其中：

(1)$b \subseteq (S, O, A)$ 表示在某个特定的状态下，哪些主体以何种访问属性访问哪些客体，其中 S 是主体的集合，O 是客体的集合，A 是访问属性集。

(2)M 为访问控制矩阵，表示系统中所有主体对所有客体所拥有的访问权限，其中元素 $m_{ij} \in A$，表示主体 s_i 对客体 o_j 的访问权限。

(3)f 是访问类函数，表示当前时刻所有主体和客体的密级和部门集。$f\in F$，记作 $f=(f_1,f_2,f_3,f_4)$。本文用 $L(s)$ 表示主体的安全级函数(包括主体的密级 $f_1(s)$ 和部门集 $f_3(s)$)，$L(o)$ 表示客体的安全级函数(包括客体的密级 $f_2(o)$ 和部门集 $f_4(o)$)。它们之间的支配关系用$\geqslant$或$\leqslant$表示。

系统用 $\sum:R\times D\times V\times V=\{(R_k,D_m,v^*,v)\mid R_k\in R,D_m\in D,v^*,v\in V\}$ 表示。有序四元组 (R_k,D_m,v^*,v) 中：

(1)R 是请求集，$R=S^*\times RA\times S^*\times O\times X$，其中，$S^*=S\cup\{\emptyset\}$，$X=A\cup\{\emptyset\}\cup F$，$R$ 中的元素是一个五元组 $\{\sigma_1,\gamma,\sigma_2,o_j,x\}$，其中 $\sigma_1,\sigma_2\in S*$ 分别是主体 1、主体 2；$\gamma\in RA$ 表示某一请求元素，$RA=\{g,r,c,d\}$；$o_j\in O$ 表示某一客体；$x\in X$ 指访问权限或空集或主客体的安全级。

(2)D 是判定集或结果集，是指对请求所作出的响应结果。$D=\{$yes,no,error,?$\}$，yes 表示请求被执行，no 表示请求被拒绝，error 表示系统出错，?表示请求出错。

(3)V 是状态集，v 表示当前状态，v^* 表示通过请求之后的状态。

BLP 模型定义了系统、系统状态及状态间的转换规则，制定了一组安全特性，对系统状态、状态转换规则进行约束。这些安全公理是构成 BLP 模型的基础，即在系统 $\sum$ 中系统状态 v 是安全状态当且仅当状态 v 满足以下 3 个安全特性：

(1)自主安全性，简称 ds-特性。状态 $v=(b,M,f)$ 满足 ds-特性，iff $(s_i,o_j,x)\in b\Rightarrow x\in M_{ij}$。

(2)简单安全性，简称 SS-特性。状态 $v=(b,M,f)$ 满足 SS-特性，对所有的 $(s,o,x)\in b$ iff

(i)$x=e$ or $x=a$ or $x=c$

(ii)$(x=r$ or $x=w)$ and $L(s)\geqslant L(o)$

(3)*-性质。状态 $v=(b,M,f)$ 满足 *-性质，iff 对所有的 $S'\in S$：

$$s\in S'\Rightarrow\left\{\begin{array}{l}o\in b(S:a)\Rightarrow L(o)\geqslant L(s)\\o\in b(S:w)\Rightarrow L(o)=L(s)\\o\in b(S:r)\Rightarrow L(o)\leqslant L(s)\end{array}\right\}$$

其中，符号 $b(S:x_1,x_2)$ 表示 b 中主体 S 对其具有访问特权 x_1 或 x_2 的所有客体的集合。

SS-性质和 *-性质说明了 BLP 模型的“上写下读”策略，其示意图如图 2 所示。

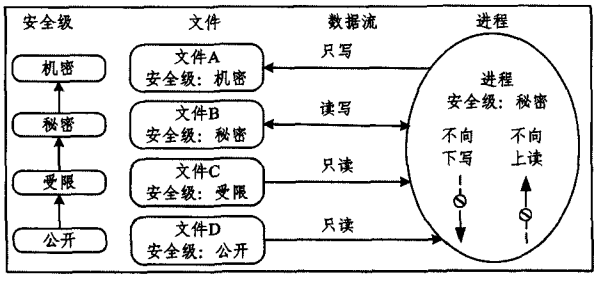

图 2 “上写下读”示意图

BLP 模型的基本安全定理：如果系统的初始状态是安全的，经过一系列规则转换后都还是安全的，那么可以证明该系统是安全的。

BLP 模型的形式化描述给出了模型的推理过程。系统从一个安全的初始状态开始，随着主体对客体的访问操作而进行状态转换。在此过程中，如果每次状态转换后系统的新状态是安全的(即符合 BLP 模型的安全公理)，则可以证明整个系统是安全的。

3.2 系统状态转换规则

系统状态间的转换是由一组规则定义的，规则为函数，它说明对任意状态，输入(请求)所产生的下一状态及输出(判定)。

给定一个请求和状态，规则 ρ 决定系统对请求产生的响应和下一状态。规则是安全策略的表现形式，CRFs-BLP 的基本思想就是给出一个能感知当前系统安全状况的规则智能调整框架。在 CRFs-BLP 模型中，首先将 BLP 中的状态转移规则形式化，如式(1)－式(10)所示。

$$\rho_1(R_k,v)=\left\{\begin{array}{ll}(?,v), & \text{if } R_k\notin(\emptyset,g,s_i,o_j,r)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,g,s_i,o_j,r)\&\\ & r\in M_{ij},L(s_i)\geqslant L(o_j)\&\\ & o\in b(s_i:w,a),L(o_j)\leqslant L(o)\\(\text{no},v), & \text{otherwise}\end{array}\right. \tag{1}$$

规则(1)表示主体 s_i 请求得到对客体 o_j 的 r 访问权。其中 $v^*=\{b\cup\{s_i,o_j,r\},M,f\}$。$\sigma_1=\emptyset,\gamma=g,p=r,\sigma_2\neq\emptyset$ 是用于验证请求的定义域是否为 $(\emptyset,g,s_i,o_j,r)$；$r\in M_{ij}$ 和 $L(s_i)\geqslant L(o_j)$ 是用于验证是否符合 BLP 模型的自主安全性公理和简单安全性公理，即主体 s_i 在访问矩阵 M 中是否对客体 o_j 有 r 权限以及主体的安全级是否支配客体的安全级；$o\in b(s_i:w,a),L(o_j)\leqslant L(o)$，是用于验证是否符合 BLP 模型的 *-性质公理，即高安全级的信息不能流向低安全级。$b\cup\{s_i,o_j,r\}$ 中符号“$\cup$”代表在当前主体 s_i 对客体 o_j 的访问权限的基础上增加 r 权限。

$$\rho_2(R_k,v)=\left\{\begin{array}{ll}(?,v), & \text{if } R_k\notin(\emptyset,g,s_i,o_j,a)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,g,s_i,o_j,a)\&\\ & a\in M_{ij}\ \&\ o\in b(s_i:r,w),\\ & L(o_j)\geqslant L_2(o)\\(\text{no},v), & \text{otherwise}\end{array}\right. \tag{2}$$

规则(2)表示主体 s_i 请求得到对客体 o_j 的 a 访问权。其中 $v^*=\{b\cup\{s_i,o_j,a\},M,f\}$。$\sigma_1=\emptyset,\gamma=g,p=a,\sigma_2\neq\emptyset$ 是用于验证请求的定义域是否为 $(\emptyset,g,s_i,o_j,a)$；$a\in M_{ij}$ 和 $o\in b(s_i:w,a),L(o_j)\geqslant L(o)$ 是用于验证是否符合 BLP 模型的自主安全性公理和 *-性质公理。注意，当 s_i 请求以 append 方式访问 o_j 时无需做简单安全性检查。

$$\rho_3(R_k,v)=\left\{\begin{array}{ll}(?,v), & \text{if } R_k\notin(\emptyset,g,s_i,o_j,e)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,g,s_i,o_j,e)\&\\ & e\in M_{ij}\\(\text{no},v), & \text{otherwise}\end{array}\right. \tag{3}$$

规则(3)表示主体 s_i 请求得到对客体 o_j 的 e 访问权。其中 $v^*=\{b\cup\{s_i,o_j,e\},M,f\}$。不需要作简单安全性和 *-性质的检查。

$$\rho_4(R_k,v)=\left\{\begin{array}{ll}(?,v), & \text{if } R_k\notin(\emptyset,g,s_i,o_j,w)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,g,s_i,o_j,w)\&\\ & w\in M_{ij},L(s_i)\geqslant L(o_j)\&\\ & \{[o\in b(s_i:r),L(o_j)\geqslant L(o)]\text{or}\\ & [o\in b(s_i:a),L(o_j)\leqslant L(o)]\text{ or}\\ & [o\in b(s_i:w),L(o_j)=L(o)]\}\\(\text{no},v), & \text{otherwise}\end{array}\right. \tag{4}$$

规则(4)表示主体 s_i 请求得到对客体 o_j 的 w 访问权。其中 $v^*=\{b\cup\{s_i,o_j,w\},M,f\}$。规则(4)的安全性检查类似于规则(1),分别需要做定义域、自主安全性、简单安全性和 *-性质的检查。

规则(1)-(4)适用于主体请求对某客体的访问权的情况。

$$\rho_5(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,r,s_i,o_j,x)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,r,s_i,o_j,x)\\(\text{no},v), & \text{otherwise}\end{cases}\quad(5)$$

规则(5)表示主体 s_i 请求释放对客体 o_j 的 x 访问权。其中 $v^*=\{b\cup\{s_i,o_j,x\},M,f\}$,$x$ 的取值为 r,w,a,e。$b-\{(s_i,o_j,x)\}$ 中符号"-"代表在当前主体 s_i 对客体 o_j 的访问权限的基础上删除 x 权限。

规则(5)适用于主体释放它对某客体的访问权的情况。

$$\rho_6(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(s_\lambda,r,s_i,o_j,x)\\(\text{yes},v^*), & \text{if } R_k\in(s_\lambda,r,s_i,o_j,x)\&\\ & p\in M_{\lambda j},c\in M_{\lambda j}\\(\text{no},v), & \text{otherwise}\end{cases}\quad(6)$$

规则(6)表示主体 s_λ 请求授予主体 s_i 对客体 o_j 的 x 访问权,x 的取值为 r,w,a,e。其中 $v^*=\{b,M\oplus[x_{ij}],f\}$,$M\oplus[p_{ij}]$代表在主体 s_i 对客体 o_j 的访问权限矩阵 M 中增加权限 p。在规则(6)中,当一个主体请求授予另一主体对客体的访问权限时,无需更改当前访问集 b,只需要更改权限矩阵即可。

$$\rho_7(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,r,s_i,o_j,x)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,r,s_i,o_j,x)\&\\ & p\in M_{\lambda j},c\in M_{\lambda j}\\(\text{no},v), & \text{otherwise}\end{cases}\quad(7)$$

规则(7)表示主体 s_λ 请求撤销主体 s_i 对客体 o_j 的 x 访问权,x 的取值为 r,w,a,e。其中 $v^*=\{b-\{(s_i,o_j,x)\},M\odot[x_{ij}],f\}$,$M\odot[p_{ij}]$代表在主体 s_i 对客体 o_j 的访问权限矩阵 M 中撤销权限 p。当一个主体请求撤销另一主体对客体的访问权限时,需要同时更改当前访问集 b 和权限矩阵 M。

规则(6)和规则(7)适用于主体授予和撤销另一主体对客体的访问权的情况。

$$\rho_8(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,c,\emptyset,o_j,F)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,c,\emptyset,o_j,F)\&\\ & f_1^*=f_1,f_3^*=f_3\&\\ & \forall j\in A(m),f_2^*(o_j)=f_2(o_j),f_4^*(o_j)=f_4(o_j)\\(\text{no},v), & \text{otherwise}\end{cases}\quad(8)$$

规则(8)表示主体对客体安全级的改变,其中 $v^*=\{b,M,f^*\}$。$f_1^*=f_1,f_3^*=f_3$,表示主体的安全级是不能改变的,f_1 和 f_3 表示 $t-1$ 时刻主体的密级和部门级,f_1^* 和 f_3^* 表示 t 时刻主体的密级和部门级;$f_2^*(o_j)=f_2(o_j),f_4^*(o_j)=f_4(o_j)$,for any $j\in A(m)$表示活动客体的安全级是不能改变的,f_2 和 f_4 表示 $t-1$ 时刻客体的密级和部门级,f_2^* 和 f_4^* 表示 t 时刻客体的密级和部门级,$A(m)$表示活动客体的下标集合并且 $A(m)=\{j\mid 1\leqslant j\leqslant m,\exists i,\text{使 } M_{ij}\neq\emptyset\}$。

原 BLP 模型中的相应规则在改变客体安全级时存在以下缺陷:首先,任何主体都可以改变客体的安全级,无论主体和客体安全级之间是否存在支配关系;其次,该规则只能用于改变静止客体的安全级。本文将该规则改进如下:

$$\rho_8^*(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,c,s_i,o_j,F)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,c,s_i,o_j,F)\&\\ & L(s_i)\geqslant L(o_{new})\geqslant L(o_j)\&\\ & s\in b(o_j:r,w),L(s)\geqslant L(o_j)\&\\ & \{[b(s_\lambda,o_j,a),L(o_{new})\geqslant L(s_\lambda)]\text{or}\\ & [b(s_\lambda,o_j,w),L(o_{new})=L(s_\lambda)]\text{ or}\\ & [b(s_\lambda,o_j,r),L(o_{new})\leqslant L(s_\lambda)]\}\\(\text{no},v), & \text{otherwise}\end{cases}\quad(8')$$

式(8′)首先指定了改变客体安全级的主体(这里客体的新安全级本文用 $L(o_{new})$表示);其次,主体的安全级必须大于 $L(o_{new})$,$L(o_{new})$的安全级必须大于原客体的安全级;再次,所有对 o_j 有 r 或 w 权限的主体 s,其安全级必须支配客体的安全级;最后,客体的新安全级对于系统内其它主体也需要满足 *-性质。因此,$v^*=\{b,M,f^*\}$。

$$\rho_9(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,c,s_i,o_j,\emptyset/e)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,c,s_i,o_j,\emptyset/e)\&\\ & j\notin A(m)\\(\text{no},v), & \text{otherwise}\end{cases}$$

$$\rho_9^*(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,c,s_i,o_j,\emptyset/e)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,c,s_i,o_j,\emptyset/e)\\(\text{no},v), & \text{otherwise}\end{cases}\quad(9)$$

规则(9)表示主体 s_i 请求创建一个新客体 o_j,其中 $v^*=\{b,M\oplus[x]_{ij},f\}$,$x$ 的取值为$\{r,w,a,e,c\}$或者$\{r,w,a,c\}$。$j\notin A(m)$表示要创建的客体 o_j 的下标不属于活动客体下标 $A(m)$,即客体 o_j 在被创建之前是不存在的。但是发现该规则在创建新客体的时候,并没有给新客体赋予安全级,因此本文对规则(9)进行了改进:新客体的安全级别和创建者的安全级相同。

$$\rho_{10}^*(R_k,v)=\begin{cases}(?,v), & \text{if } R_k\notin(\emptyset,d,s_i,o_j,\emptyset)\\(\text{yes},v^*), & \text{if } R_k\in(\emptyset,d,s_i,o_j,\emptyset)\&\\ & c\in M_{ij}\\(\text{no},v), & \text{otherwise}\end{cases}\quad(10)$$

规则(10)表示主体 s_i 请求删除客体 o_j,原 BLP 模型中的相应规则在删除客体时,并没有删除客体的安全级以及当前访问集中与 o_j 相关的访问。在 CRFs-BLP 模型中,本文将该规则改进如下:在删除一个客体时,同时删除当前访问集 b、权限矩阵 M 和安全级函数 f 中与 o_j 有关的信息,因此 $v^*=\{b-\{(s_i,o_j,x)\},M\odot[x]_{ij},1\leqslant i\leqslant n,f\odot L(o_j)\}$。

规则 ρ 保持安全状态当且仅当 $\rho(R_k,V)=(D_m,V^*)$,v 是安全状态时,有 v^* 是安全状态。

3.3 基于条件随机场的状态转移过程

条件随机场(Conditional Random Fields,CRFs)最早由 Lafferty 等人于 2001 年提出,其模型思想的主要来源是最大熵模型。其是一种用于标记和分割关系数据的概率框架,用于结构数据分类的无向图模型,通常使用训练数据得到模型,

然后给定输入序列，使输出序列的条件概率最大化。一阶链式 CRFs 是最为常用的一种结构：设 X 与 Y 是随机变量，$P(Y|X)$是在给定 X 的条件下 Y 的条件概率分布。若随机变量 Y 构成一个由无向图 $G=(V,E)$ 表示的马尔科夫随机场，即 $P(Y_v|X,Y_w,w\neq v)=P(Y_v|X,Y_w,w\sim v)$ 对任意节点 v 成立，则称条件概率分布 $P(Y|X)$ 为条件随机场。式中 $w\sim v$ 表示无向图 G 中与节点 V 有边连接的所有节点 W，$w\neq v$ 表示除节点 V 以外的所有节点。有边连接的物理意义是指顶点 v 在状态 Y_v 的概率只依赖顶点 v 的最近临节点，并且顶点 v 对图中的其他任何节点是条件独立的，反之亦然。对给定的 CRFs 模型，根据 Hammersley-Clifford 定理，CRFs 的参数化形式可以表示为：

$$p(y|x)=\frac{1}{Z(x)}\exp\left(\sum_{i,k}\lambda_k t_k(y_{i-1},y_i,x,i)+\sum_{i,l}\mu_l s_l(y_i,x,i)\right)$$

其中，$Z(x)=\sum\exp\left(\sum_{i,k}\lambda_k t_k(y_{i-1},y_i,x,i)+\sum_{i,l}\mu_l s_l(y_i,x,i)\right)$，求和是在所有可能的输出序列上进行的。$t_k$ 和 s_l 是特征函数，λ_k 和 μ_l 是对应的权值。$Z(x)$是规范化因子，用于保证 $p(y|x)$满足经典概率规则 $\sum_y p(y|x)=1$。其中 t_k 是定义在边上的特征函数，称为转移特征，其值依赖于当前和前一个位置；s_l 是定义在节点上的特征函数，称为状态特征，其值依赖于当前位置。通常特征函数的值取 0 或 1。条件随机场完全由特征函数 t_k，s_l 和对应的权值 λ_k，μ_l 确定。

CRFs 由于克服了隐马尔科夫模型 HMM 严格的独立性假设和最大熵模型 MEMs 的标记偏置问题(label bias problem)的缺点，并且还可以表达长距离依赖性和交叠性特征，被广泛地应用于各种机器学习和自然语言处理任务中。本文采用条件随机场理论来描述 CRFs-BLP 模型中系统每一步状态转换的转移概率，来对系统请求的安全性进行预测。

在 BLP 模型中，系统决策集 Y 属于一个大小为 N 的有限状态集，任何时刻系统决策的取值 y 都可以是 Y 中的任意一个，所以系统决策 y 是一个随机变量，本文将随机变量 Y 表示成 CRFs 的输出序列集，并且 $Y=y_1y_2\cdots y_t\cdots$。其次，由于在分布式环境下，在任一时刻客户的请求也是随机的，因此客户的请求序列 X 也是一个随机变量，所以可以将随机变量 X 表示成 CRFs 的输入序列集，并且 $X=x_1x_2\cdots x_t\cdots$。

因此，CRFs-BLP 模型的建模过程如下：将 BLP 模型的请求序列作为 CRFs 的输入序列。在 BLP 模型中，输入序列是用户的请求集 R；将 BLP 模型的决策序列作为 CRFs 的输出序列。根据系统访问日志得到数据集，提取数据集的相关特征，建立特征模版，结合 CRF++工具建立模型，以实现动态感知的 CRFs-BLP 模型。

4 CRFs-BLP 数据集标注

本节的基本思路是通过对我院内部办公系统的访问日志进行整理和分析，提取特征函数，构建符合 CRF++的原始数据集。其次进行人工标注，针对提取的特征函数构建特征模版，采用 CRF++提供的相关命令建立 CRFs-BLP 模型，再用该模型对测试集进行预测。

4.1 数据集

CRFs 中的原始数据集为系统的历史访问日志，本文首先将其预处理为可作为模型输入的记录格式，主要包括当前时刻系统状态、用户所做的操作以及系统对用户请求所做出的响应。需要提取请求和当前状态作为 CRFs 数据集的特征向量。其中“请求”特征向量的值由一个五元组$\{\sigma_1,\gamma,\sigma_2,o_j,x\}$组成，各个元组的取值情况如表 1 所列。

表 1 请求特征定义

元素	取值	意义
主体 σ_1	0	0 表示取空值
	S_i	非 0 表示一个具体的主体 s
请求元素 γ	g/r/c/d	可以取 RA 集合里面的任意值
主体 σ_2	0	0 表示取空值
	S_i	非 0 代表具体主体 s
客体 o_j	0	0 表示取空值
	O_j	非 0 代表具体客体 o
x	r/w/e/a/c	访问属性集里面任意值
	0	0 表示取空值
	F	表示主客体的安全级

以本文模型中的规则(1)为例，规则(1)表示主体 s_i 请求得到对客体 o_j 的 r 访问权，那么该规则能够接受的请求元组为$(\emptyset,g,s_i,o_j,r)$，采用表 1 定义的方法请求元组的取值为$(0,g,s_1,o_1,r)$。其中 σ_1 非空的情况只应用于规则(6)和规则(7)，也就是一个主体请求授予/撤销另一个主体对客体的访问权，因此规则(1)中 σ_1 取空值 0；请求得到某种权限时请求元素 γ 的取值为 g；σ_2 和 o_j 对应规则中的主体 s_i 和客体 o_j；x 取 r 值表示请求得到读访问权。

另外，系统的当前状态是一个包含(b,M,f)的三元组，各个元素的定义如表 2 所列。

表 2 当前状态特征定义

元素	意义
b	给出系统中当前状态下的访问集，例如(S1,O2,rwe)
M	系统权限矩阵，将二维矩阵用一维存储
f	系统中所有主体和客体的密级与安全级

对于某条系统日志，预处理后可表示为以下数据，即 B: s3o2e 0 0 0 0 M: s1o1r s2o3rc s1o3rc s2o2werca s3o10 s1o2wea s2o1rc s3o3rc s3o2e F: o110 s12310 o23310 o313 s233210 s343210 R:0 g s1 o1 r Decision:yes。这条数据分成 5 个部分，第一部分是系统当前访问集 b，总共有 5 列，其中 s3o2e 表示主体 s_3 对客体 o_2 当前具有 e 访问权，后面的 0 用于补足当前数据集列数。第二部分是系统权限矩阵 M，这部分日志数据总共取了 3 个主体与 3 个客体，因此权限矩阵 M 总共有 9 列。第三部分中的 6 列是安全级函数 F，包括 3 个主体和 3 个客体，其中 s12310 表示主体 s_1 的密级为 2，部门集为{3,1,0}。第四个部分代表系统请求 R，共 5 列，表示主体 s_1 请求得到对客体 o_1 的 r 访问权限。最后是 CRFs-BLP 模型中需要标记的内容：决策集 Decision，即标记对一个输入系统做的决策，包括：yes、no、? 和 error 4 种。规则(1)中训练数据标记为 yes 的前提是：请求必须合法(第四部分)，主体的安全级必须支配客体的安全级(第三部分)，请求的权限必须属于权限矩阵(第二部分)，需要满足 *-性质(第一部分和第三部分)。因此这条数据总共有 25 个特征。

针对可信主体权限过大的问题，本文引入了可信客体的概念。

定义 1(可信客体) 一段时间内客体 O 是可信客体，表示所有主体在这段时间内对该客体有读写权限，不管主体的

安全级是否支配或被支配客体的安全级。

不同于可信主体在整个系统运行期间可以任意读写所有客体，可信客体是在指定时间段内所有主体可以读写的客体，而不是对所有客体执行操作，这样可限制系统危险操作的范围。此外，只有那种高安全级的非密级信息才能标注为可信客体。

鉴于此，本文在 CRF 的数据集里面加上一列可信客体的特征，若该列取值为 0，表示请求 R 中的客体不可信；取值为 1 表示客体可信。访问记录 B：s2o2wr s2o1r s3o2e s2o5r 0 0 M：s2o3c s2o2wrca s3o10 s2o1rc s3o3c s3o2we s3o5wrca s2o5wa F：o110 o23310 s233210 s343210 o323 o543210 R：0 g s2 o5 r Decision：no 表示主体 s_2 请求对客体 o_5 的读权限。由于 o_5 的安全级支配 s_2 的安全级，信息不能从高往低流，违反了 SS-性质，因此系统拒绝该请求。若将 o_5 标注为可信客体，则该请求应该绕过 SS-性质检查，并执行该请求，如图 3 所示。

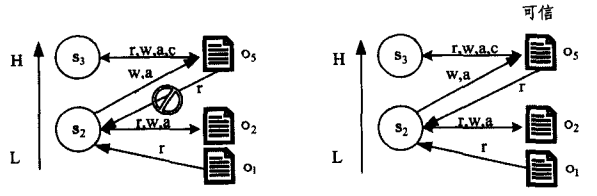

图 3　高安全级非密级信息的读写

针对敏感客体是否允许跨级读写问题，本文加入了一个跨级读写特征，值为 1 表示不能跨级读写，值为 0 表示可以跨级读写。

如图 4 所示，左图中 s_1、s_2、s_3 都可以对客体 o_5 进行写操作，同时，本模型用一个标志位来表示实际过程中敏感客体不能够被跨级读写的语义。在右图中 o_5 已被标识为不允许跨级读写，故此情况下，s_1 和 s_2 对 o_5 的操作都将会被拒绝。

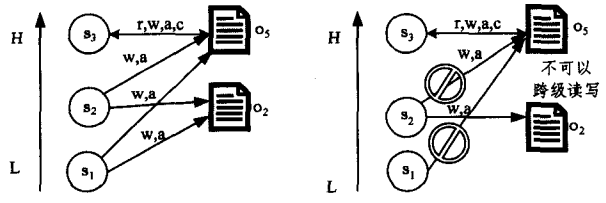

图 4　高安全级读写限制

综上所述，CRFs-BLP 模型的数据集格式如表 3 所列。

表 3　CRFs-BLP 模型的数据集格式

特征名称	取值范围
当前访问集	(s_i,o_j,x) …
可信客体	0/1
跨级读写	0/1
权限矩阵	(s_i,o_j,x)…
安全级	s_i/o_j:(C,K)
请求	$\{\sigma_1,\gamma,\sigma_2,o_j,x\}$
决策	{yes,error,no,?}

4.2　特征模板定义

在条件随机场模型中，一个非常重要的问题是如何针对特定的任务为模型选择合适的特征集。特征选择就是针对特定的任务为模型选择合适的特征集，定义模型中的特征函数。特征函数是对状态转移 $y_{t-1}\rightarrow y_t$，观察序列 X 和序列中第 t 个位置各方面属性特征的一个衡量。由于特征的数量非常庞大，直接从训练语料中手工选取是不现实的，一般的做法是选择特征模板，再通过特征模板在训练语料中实例化的方式获取特征，采用特征的形式来表示已有知识。特征模板的选取是条件随机场模型中最为关键的部分，它决定了识别正确率，一般要求所选取的特征尽可能地体现所识别对象的特点。

CRF 特征模板需要被设计成尽可能多地包含各种相关信息。对于一个文本，可以提取到很多属性，如字、词、拼音、词长、词在句中的位置等，一类属性便可以成为一类特征。对于一条系统访问记录，需要提取请求、当前访问集、权限矩阵和安全级函数 4 类特征。

本文选择两类特征，一类是基本特征，另一类是组合特征。基本特征又叫原子特征，原子特征模板只考虑影响分词的一类因素，它实际上是当前字段的上下文的函数。组合特征就是基本特征相结合所组成的新的特征。一般有两种组合方式，一种是同一类特征的上下文组合，另一种是不同类特征之间的组合。

为了结合上下文进行测试，将上下文窗口取 2。针对本文设计对应的特征模板，用 R_i 表示请求特征，B_i 表示当前访问集特征，M_i 表示权限矩阵特征，F_i 表示安全级特征，i 表示窗口的长度。本文的特征模板见表 4。

表 4　“2+1”窗口特征模板

编号	类型	特征符号	特征意义
1	原子特征	R_{-1}	前一个请求
2		R_0	当前请求
3		R_1	后一个请求
4		B_{-1}	上一状态下的访问集
5		B_0	当前状态下的访问集
6		B_1	下一状态下的访问集
7		M_{-1}	上一状态下的权限矩阵
8		M_0	当前状态下的权限矩阵
9		M_1	下一状态下的权限矩阵
10		F_{-1}	上一状态下的安全级
11		F_0	当前状态下的安全级
12		F_1	下一状态下的安全级
13	同类组合特征	B_{-1} B_0	上一状态和当前状态下的访问集
14		M_{-1} M_0	上一状态和当前状态下的权限矩阵
15		F_{-1} F_0	上一状态和当前状态下的安全级
16	不同类组合特征	B_{-1} M_{-1} F_{-1}	系统前一个状态
17		B_0 M_0 F_0	系统当前状态
18		R_{-1} B_{-1} M_{-1} F_{-1}	系统前一个状态下的请求
19		R_0 B_0 M_0 F_0	系统当前状态下的请求

5　实验结果及分析

5.1　实验条件和方法

本文采用 CRF++软件实现了通过特征模板选取特征的方法，特征模板定义了特征在训练语料中实例化的方式。特征模板有如 U%X[i,j]的形式，其中 i,$j\geqslant 0$，分别表示实例化时观察值对当前位置的偏移量(假设当前位置为[0,0])。

首先需要将表 4 中的特征组合表示成 CRF++中的特征模板。如 B_{-1} 表示为 U%X[−1,0]/ %X[−1,1] / %X[−1,2] / %X[−1,3] / %X[−1,4]，B_0 M_0 F_0 表示为 U%X[0,0]/ %X[0,1] / %X[0,2] / %X[0,3] / %X[0,4] / %X[0,5] / %X[0,6] / %X[0,7] / %X[0,8] / %X[0,9] / %X[0,10] / %X[0,11] / %X[0,12] / %X[0,13] / %X[0,14] / %X[0,15] / %X[0,16] / %X[0,17] / %X[0,18] /

%X[0,19] / %X[0,20] / %X[0,21] / %X[0,22] / %X[0,23] / %X[0,24]。

4.1 节详细描述了实验数据集的构造过程。采用CRF++工具包进行实验，数据集总共有 1963 条数据，也就是 1963 个特征向量。数据集的标注总共有 3 类：yes，no 和 ?。表 5 列出了各类标注结果所占的比例，可以看出标注为 no 的数据集最多，?的最少。为了更好地评估实验结果，分别采用 Repeated Random Sub-Sampling（RRSS）和 P-fold 交叉验证技术对数据集进行训练和测试。表 6 列出了两种交叉验证技术所采用的训练集和测试集数据。

表 5 决策分布情况

总数	yes	no	?
1963	553	1091	319

表 6 两种交叉验证技术的数据集分布情况

交叉验证	Tag	Training set	Testing set
RRSS	yes	369	184
	no	727	364
	?	213	106
	(Sum)	1309/66.7%	654/33.3%
P-fold	yes	498	55
	no	982	109
	?	287	32
	(Sum)	1767/90%	196/10%

同时采用 RRSS 和 10-fold 交叉验证技术进行数据集的训练与测试。RRSS 技术将数据集随机分成 3 份，1309(2/3)个特征向量用于训练，654(1/3)个特征向量用于测试，将该过程重复 3 次，再取平均值。

而 P-fold 交叉验证技术则是将输入集随机分成 10 份，其中 9 份作为训练集，1 份作为测试集。该过程重复 P 次，通常取 $P=10$，然后求平均值。

5.2 实验结果分析

两种交叉验证技术的结果如表 7 和表 8 所列。表 9 列出了两种交叉验证结果的综合情况。从表 7 和表 8 可以看出，CRFs-BLP 模型能够对系统请求做出比较准确的决策，其准确率都能达到 97%以上，并且还能够对已有的历史访问日志的规则进行动态调整，从而对新请求做出正确的判断。从预测结果中可以看到，主体 s_3 在 t 时刻创建了客体 o_4，此时主体 s_1 读取 o_4 的请求因为违反了 SS-性质而被拒绝，而因为之后某个时刻 o_4 被标注为可信客体，自此主体 s_1 可以顺利地读取客体 o_4；主体 s_3 在 m 时刻创建了客体 o_5，并将其标注为“不可以跨级读写”。可以看到，在 o_5 的生命周期中只有 s_3 可以对其进行读写操作，其余任何主体对它的操作都被拒绝，因为只有 o_5 和 s_3 的安全级相同。

表 7 RRSS 交叉验证结果

数据集	决策	准确率	召回率	F1 值	平均值
数据集 1	yes	100%	78.88%	88.14%	94.04%
	no	90.29%	100%	94.90%	
	?	100%	100%	100%	
数据集 2	yes	100%	99.46%	99.73%	99.85%
	no	99.73%	100%	99.86%	
	?	100%	100%	100%	
数据集 3	yes	100%	94.05%	96.93%	98.32%
	no	97.05%	100%	98.51%	
	?	100%	100%	100%	

表 8 P-fold 交叉验证结果

数据集	决策	准确率	召回率	F1 值	平均值
数据集 1	yes	100%	92.73%	96.23%	97.97%
	no	96.46%	100%	98.20%	
	?	100%	100%	100%	
数据集 2	yes	100%	100%	100%	100%
	no	100%	100%	100%	
	?	100%	100%	100%	
数据集 3	yes	100%	66.07%	79.57%	90.36%
	no	85.16%	100%	91.98%	
	?	100%	100%	100%	
数据集 4	yes	100%	98.21%	99.01%	99.49%
	no	99.01%	100%	99.54%	
	?	100%	100%	100%	
数据集 5	yes	100%	85.71%	92.31%	95.94%
	no	93.16%	100%	96.46%	
	?	100%	100%	100%	
数据集 6	yes	100%	98.21%	99.10%	99.49%
	no	99.10%	100%	99.54%	
	?	100%	100%	100%	
数据集 7	yes	96.55%	100%	98.25%	98.98%
	no	100%	98.17%	99.07%	
	?	100%	100%	100%	
数据集 8	yes	100%	98.21%	99.10%	99.49%
	no	99.10%	100%	99.54%	
	?	100%	100%	100%	
数据集 9	yes	100%	89.29%	94.34%	96.95%
	no	94.78%	100%	97.32%	
	?	100%	100%	100%	
数据集 10	yes	93.33%	100%	96.55%	97.97%
	no	100%	96.33%	98.13%	
	?	100%	100%	100%	

表 9 两种交叉验证的综合结果

交叉验证技术	评价指标(%)		
	准确率	召回率	F1 值
RRSS	97.40%	97.40%	97.40%
P-fold	97.66%	97.66%	97.66%

结束语 本文所提出的 CRFs-BLP 模型的主要目标是解决现有安全模型在系统安全状态感知和自优化方面的局限性。首先对历史访问记录进行预处理与人工标注，结合实际系统分析和提取特征向量，定义特征模版。然后基于该特征模型进行学习和训练，使之能够根据经验数据修正现有 BLP 模型规则的缺陷，以增加其可用性。最后通过实验对该模型的准确率、召回率和 F1 值等关键性指标进行评测，结果表明：对于具有机器学习功能的 BLP 访问控制模型，其规则能够根据当前系统的安全状态及安全事件进行动态调整，具有较好的实用价值和应用前景。

参 考 文 献

[1] Sandhu R S, Samarati P. Access control: principle and practice [J]. Communications Magazine, IEEE, 1994, 32(9): 40-48

[2] Yang Kan, Jia X H. Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(7): 1735-1744

[3] Lan Zhou, Varadharajan V, Hitchens M. Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1947-1960

（下转第 151 页）

services for wireless networks: challenges, approaches, and prospects[J]. IEEE Communications Magazine, 2013, 51(2): 142-150

[9] He D, Chen C, Chan S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53

[10] He D, Bu J, Chan S, et al. Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks [J]. IEEE Transactions on Computers, 2013, 62(3): 616-622

[11] Jing Q, Zhang Y, Fu A, et al. A privacy preserving handover authentication scheme for EAP-based wireless networks [C] // IEEE Global Telecommunications Conference. Houston, 2011: 1-6

[12] He D, Chen C, Chan S, et al. Analysis and improvement of a secure and efficient handover authentication for wireless networks [J]. IEEE Communications Letters, 2012, 16(8): 1270-1273

[13] Fu A, Lan S, Huang B, et al. A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks[J]. IEEE Communications Letters, 2012, 16(11): 1744-1747

[14] Lai C, Li H, Lu R, et al. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks [J]. Computer Networks, 2013, 57(17): 3492-3510

[15] Lee C, Lai Y M. Toward a secure batch verification with group testing for VANET[J]. Wireless networks, 2013, 19(6): 1441-1449

[16] Chen C, He D, Chan S, et al. Lightweight and provably secure user authentication with anonymity for the global mobility network [J]. International Journal of Communication Systems, 2011, 24(3): 347-362

[17] The NS-3 Consortium. NS3 tutorial[OL]. http://www.nsnam.org

[18] Baldo N, Requena-Esteso M, Miozzo M, et al. An open source model for the simulation of LTE handover scenarios and algorithms in ns-3 [C] // Proceedings of 16th ACM International Conference on Modeling, Analysis & Simulation of Wireless and Mobile Systems. Barcelona, 2013: 289-298

(上接第 144 页)

[4] Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations: ESD-TR-73-278, I(AD)770768[R]. Bedford, UK: MITRE Corporation, 1973

[5] Bell D E, LaPadula L J. Secure Computer System: A Mathematical Model [R]. Bedford, MA: Electronic Systems Division, Air Force System Command, Hanscom AFB, 1973

[6] Shen Ying, Xiong L R. Lattic based BLP extended model [C]// Proc of the 2nd International Conference on Future Information Technology and Management Engineering. 2009: 309-312

[7] Liang H L, Sun Y F, Zhao Q S, et al. Design and implementation of a security label common framework [J]. Journal of Software, 2003, 14(3): 547-552

[8] 蔡谊, 郑志蓉, 沈昌祥. 基于多级安全策略的二维标识模型[J]. 计算机学报, 2004, 27(5): 619-624
Cai Yi, Zheng Zhi-rong, Shen Chang-xiang. A Planar Attributes Model Based on Multi Level Security Policy [J]. Chinese Journal of Computers, 2004, 27(5): 619-624

[9] 刘彦明, 董庆宽, 李小平. BLP 模型的完整性增强研究[J]. 通信学报, 2010, 31(2): 100-106
Liu Yan-ming, Dong Qing-kuan, Li Xiao-ping. Study on enhancing integrity for BLP model[J]. Journal on Communications, 2010, 31(2): 100-106

[10] Lee T M P. Using mandatory integrity to enforce "commercial" security[C]// Proc of IEEE Conference on Security and Privacy. Washington DC: IEEE Computer Society, 1998: 140-146

[11] Schell R, Tao T F, Heckmn M. Designing the GEMSOS security kernel for security and performance[C]// Proc of the 8th National Computer Security Conference. 1985: 108-119

[12] 聂晓伟, 冯登国. 基于动态可信度的可调节安全模型[J]. 通信学报, 2008, 29(10): 37-44
Nie Xiao-wei, Feng Deng-guo. Modified security model based on dynamic trusted degree [J]. Journal on Communications, 2008, 29(10): 37-44

[13] 谭智勇, 刘铎, 司天歌, 等. 一种具有可信度特征的多级安全模型[J]. 电子学报, 2008, 36(8): 1637-1641
Tan Zhi-yong, Liu Duo, Si Tian-ge, et al. Multilevel Security Model with Credibility Characteristics [J]. Acta Electronica Sinica, 2008, 36(8): 1637-1641

[14] Yamaguchi F, Lindner F, Rieck K. Vulnerability extrapolation: Assisted discovery of vulnerabilities using machine learning[C]// Proceedings of the 5th USENIX Conference on offensive Technologies. USENIX Association, 2011: 13-13

[15] 顾亚祥, 丁世飞. 支持向量机研究进展[J]. 计算机科学, 2011, 38(2): 14-17
Gu Ya-xiang, Ding Shi-fei. Advances of Support Vector Machines [J]. Computer Science, 2011, 38(2): 14-17

[16] Bozorgi M, Saul L K, Savage S, et al. Beyond heuristics: learning to classify vulnerabilities and predict exploits[C]// Proc. of 16th Int. Conf. on Knowledge discovery and Data Mining. ACM, 2010: 105-144

[17] 谭小彬, 王卫平, 奚宏生, 等. 计算机系统入侵检测的隐马尔可夫模型[J]. 计算机研究与发展, 2003, 40(2): 245-250
Tan Xiao-bin, Wang Wei-ping, Xi Hong-sheng, et al. A Hidden Markov Model Used in Intrusion Detection [J]. Journal of Computer Research and Development, 2003, 40(2): 245-250

[18] Tjhai G C, Furnell S M, PaPadaki M, et al. A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm [J]. Computers & Security, 2010, 29(6): 712-723

[19] 王辉, 陈泓予, 刘淑芬, 等. 基于改进朴素贝叶斯算法的入侵检测系统[J]. 计算机科学, 2014, 41(4): 111-115, 119
Wang Hui, Chen Hong-yu, Liu Shu-fen, et al. Intrusion Detection System Based on Improved Naïve Bayesian Algorithm[J]. Computer Science, 2014, 41(4): 111-115, 119

[20] Seifert C, Welch I, Komisarczuk P. Identification of malicious Web pages with static heuristics[C]// Proc. of Telecommunication Networks and Applications Conference. 2008: 91-96

[21] 张健, 陈松乔. 一种基于最大熵原理系统异常检测模型研究[J]. 小型微型计算机系统, 2008, 29(4): 643-648
Zhang Jian, Chen Song-qiao. Research on an Abnormal Detect Model for System Call Sequence Using Maximum Entropy Principle [J]. Journal of Chinese Computer System, 2008, 29(4): 643-648