一种基于AHP的信息安全威胁评估模型研究

李 杨 韦 伟 刘永忠 张为群

(西南大学计算机与信息科学学院 重庆 400715) (重庆市智能软件与软件工程重点实验室 重庆 400715)

摘 要 对信息化发展过程中信息系统所面临的各种威胁进行有效的评估预测,并根据评估结果部署相应的措施,可减少威胁带来的负面影响。提出了一种基于AHP的信息安全威胁评估模型,它将AHP方法与模糊综合评价法相结合,建立了威胁评估指标,通过资产识别、威胁识别、威胁分析的方法拟得到评估结果。通过实践验证了模型的有效性和可行性。

关键词 威胁评估,AHP,资产识别,威胁识别

Research on Information Threaten Assessment Model Based on AHP

LI Yang WEI Wei LIU Yong-zhong ZHANG Wei-qun

(Faculty of Computer and Information Science, Southwest University, Chongqing 400715, China)

(Chongqing Intelligent Software and Software Engineering Laboratory, Chongqing 400715, China)

Abstract The measures deployed by the assessment results can reduce the negative impacts of the threats of information systems that we assess and predict in informatization development process. Proposed an model of information security threaten assessment based on AHP, which combining AHP with Fuzzy Comrehensive Evaluation, establishes threat assessment indicators, and plans to get the assessment result through the methods of assets identify, threats identify, threats analysis. The results of experiment verify the feasibility and validity of the model.

Keywords Threaten assessment, AHP, Assets identify, Threats identify

1 引言

伴随着信息技术的飞速发展,以信息技术为基础的信息产业已经成为世界经济的重要支柱产业。如何对信息化发展过程中形成的关系国家政治、经济、文化等方面的重要信息系统所面临的各种威胁进行评估、预测,是国家信息安全保障体系中的重要基础工作之一。这就要求对其进行信息安全风险评估,而信息安全威胁评估是风险评估的重要部分。所谓威胁,是指对信息系统或组织产生危害的事故的潜在起因,有效的信息安全威胁评估可降低潜在问题发生的可能性,部署的措施可减少威胁带来的负面影响。

众多研究者对信息安全评估进行了不同角度、不同方面的研究,如风险评估[1]、资产评估[2]、脆弱性评估。H. Ke等基于攻击路径,从成本效益角度建立了面向对象的威胁建模方法[3];C. Qingming等从主动型和被动型两方面研究了评估工具及其应用[4];C. Lin等人提出了基于攻击路径图的威胁评估方法[5]。但是已有的方法还存在以下一些问题:(1)未考虑历史记录中威胁发生频率和资产暴露因子相结合而影响威胁发生的可能性计算结果。(2)考虑单个资产、单个威胁值、综合威胁值之间的关系还不够全面。针对以上问题,本文提出了一种基于AHP的威胁评估模型AHPTAM,用于对信息系统进行威胁评估。通过建立威胁评估指标,根据威胁发生频率,采用AHP算法,考虑单个信息资产的威胁值和威胁综合值,结合模糊综合评价得到最终结果,达到有效评估信息系统面临的直接或间接威胁,从而提出改进措施,控制其安全状态。

2 相关定义

定义1(资产集合A) 指组织中具有价值的信息或资源的集合,是安全策略要保护的所有对象。$A=\{a_i \mid 1\leqslant i\leqslant n\}$,其中$a_i$表示第$i$个资产,$n$表示资产的数量。

定义2(资产价值集合AV) 表示关键资产的重要程度或敏感程度,是资产的属性集合。$AV=\{av_i \mid 1\leqslant i\leqslant n\}$,$f: a_i \rightarrow f(a_i)=av_i=\left\{\begin{matrix}1\\2\\3\end{matrix}\right\}$,1表示资产一般重要,2表示资产比较重要,3表示资产很重要。

定义3(资产暴露因子集合AE) AE是指由于外界因素或每个资产本身存在的弱点而增加威胁发生的程度所构成的集合。$AE=\{ae_i \mid 1\leqslant i\leqslant n\}$,$g: a_i \rightarrow g(a_i)=ae_i=\left\{\begin{matrix}1\\2\\3\end{matrix}\right\}$,1表示

到稿日期:2011-04-03 返修日期:2011-06-25 本文受重庆市信息产业发展资金项目(200921011)资助。

李 杨(1987—),女,硕士生,主要研究方向为软件工程、信息安全等,E-mail:sjww@swu.edu.cn;韦 伟(1983—),男,硕士生,主要研究方向为信息安全等;刘永忠(1986—),男,硕士生,主要研究方向为信息安全等;张为群(1950—),男,教授,硕士生导师,主要研究方向为软件工程、形式语言、软件测试等。

没有暴露，2 表示一般暴露，3 表示严重暴露。

定义 4(威胁评估指标集 TU) $TU=\{TU_1, TU_2, TU_3, TU_4\}$。其中 TU_1 代表网络威胁，TU_2 代表物理威胁，TU_3 代表系统威胁，TU_4 代表环境威胁。用 t_i 表示威胁，则有威胁集 $T=\{t_i \mid 1\leqslant i\leqslant m\}$。详细描述见表 1。

表 1 威胁评估指标

指标类别	编号	威胁名称
网络威胁	t_1	篡改
	t_2	伪造
	t_3	截取
	t_4	中断
物理威胁	t_5	硬件故障
	t_6	软件故障
	t_7	通讯故障
系统威胁	t_8	蓄意破坏
	t_9	无意行为
环境威胁	t_{10}	自然灾害
	t_{11}	基础设施

定义 5(威胁发生的可能性 p) 用 p_i 表示某种威胁发生的可能性大小，所构成的集合为 $P, p_i\in P, 1\leqslant i\leqslant m$。假设 $q_i\in Q, 1\leqslant i\leqslant m, q_i$ 是指某威胁事件发生的频率，所构成的集合用 Q 表示。则有 $P=F(Q,AE)$，即通过 q_i 和 ae_i 确定出 p_i。

定义 6(判断矩阵 R) 假设层次结构中以某元素为准则，其所支配的下一层元素为 $\{r_1, r_2, \cdots, r_i, \cdots, r_n\}$。请 c 个专家依据威胁发生的可能性和历史威胁等级，采用 1～9 比例标度法对元素的相对重要性进行比较并赋值，得到 n 个元素之间的判断矩阵 R：

$$R=(r_{ij})_{n\times n}=\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{12} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix}$$

式中，r_{ij} 就相当于 r_i 和 r_j 相对于准则元素的重要性比例。并且 R 满足：$r_{ij}>0$，$r_{ij}\cdot r_{ji}=1$，$r_{ii}=1$。

定义 7(层次结构模型) 将威胁评估问题分解成若干部分，构成若干元素，各个元素又按属性归为不同组，形成不同的层次。同一层次的元素作为准则对下一层的某些元素起支配作用，同时它又受上面层次元素的支配。本文确定的模型分为目标层 G(问题的最终目标——单资产威胁分析)、准则层 TU(影响目标实现的准则——4 类威胁)、方法层 T(促使目标实现的具体方法——具体的威胁)。

根据本文提出的威胁评估指标，可建立信息安全威胁评估层次结构模型，如图 1 所示。

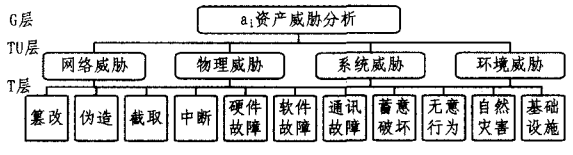

图 1 信息安全威胁评估层次结构模型

3 AHPTAM 威胁评估模型

AHP(Analytical Hierarchy Process)[6] 法善于把研究对象作为一个系统进行处理，它按照分解、比较、判断、综合的方式进行决策，通过对统计数据的学习，得到系统中各个因素的相应权重。但实际影响各指标的重要性程度的因素有很多，仅用 AHP 方法不能全面解决问题。模糊综合评价法善于解决不精确的、模糊的问题，能够模拟人的综合判断推理能力，在定性与定量分析之间建立联系，而且有较强的综合判断能力。但仅用模糊综合评价法，还不能通过学习获得威胁评估模型各指标的权重。因此，本文将 AHP 方法与模糊综合评价法相结合来构造信息安全威胁评估模型，以取长补短，使模型的评估效果更具科学性。

AHPTAM 威胁评估模型主要包括 3 部分：资产识别、威胁识别、威胁分析，最后根据威胁分析结果对信息系统的安全状态进行评估，并提出相应的改进措施[7,8]。

3.1 资产识别

资产识别是根据历史威胁数据库和相关负责人提供资料的方式识别出评估对象的信息资产，形成资产列表，并确立资产价值和资产暴露因子。本文用一个三元组 D 来表示，即 $D=(A, AV, AE)$。

3.2 威胁识别

威胁识别对评估对象存在的历史威胁和潜在威胁进行识别，得到威胁列表，并输出威胁发生的频率列表。本文用一个三元组 H 来表示，即 $H=(T, Q, \overline{W^2})$，其中 $\overline{W^2}$ 为历史威胁对资产的影响集。

3.3 单资产威胁后果分析的 AHP 算法

根据资产列表和威胁列表进行计算，得到威胁分析预处理列表，用三元组 $E=(T, A, P)$ 表示，代表资产 A 可能发生的威胁事件 T 及其发生可能性。根据定义 7 的描述构建每一个资产的层次结构模型，通过定义 6 和 E 确定 R，然后进行层次单排序并进行一致性检验，最后进行层次总排序，得到单资产威胁分析结果。

求解层次单排序算法的步骤如下。

输入：R'，平均随机一致性指标 RI

输出：权重排序向量 W

Step1 初始化 R'。

Step2 构造 R。

Step3 计算同一层次某一准则下的 d 个元素的排序向量 $w_i=\frac{1}{d}\sum_{j=1}^{d}\left(\frac{r_{ij}}{\sum_{k=1}^{d} r_{kj}}\right)$，其中 $i=1,2,\cdots,d$，得到 $W=(w_1, w_2, \cdots, w_d)^{\mathrm{T}}$。

Step4 计算判断矩阵的最大特征值 $\lambda_{\max}=\frac{1}{d}\sum_{i=1}^{d}\frac{\sum_{j=1}^{d}(r_{ij}w_j)}{w_i}$。

Step5 若 $r_{ik}=r_{ij}\times r_{jk}$，其中 $i,j,k=1,2,\cdots,d$，则转至 Step7。

Step6 计算判断矩阵一致性指标 $CI=\frac{\lambda_{\max}-d}{d-1}$ 和一致性比例 $CR=\frac{CI}{RI}$。如果 $CR\geqslant 0.1$，判断矩阵不满足一致性，转至 Step2。

Step7 输出 W。

由上述算法得到的各 W，分别用 W^1 和 W_j^2 保存。W^1 表示为第一层元素相对于目标元素的排序向量，$W^1=(w_1^1, w_2^1, \cdots, w_i^1)^{\mathrm{T}}$；$W_j^2$ 表示第二层元素在第一层准则元素 j 下的排序向量，$W_j^2=(w_{1j}^2, w_{2j}^2, \cdots, w_{4j}^2)^{\mathrm{T}}$，其中 $j=1,2,\cdots,d$。然后进行层次总排序。具体算法步骤如下。

输入：W^1 和 W_j^2

输出：$\overline{W^2}$

Step1 初始化 $\overline{W^2}$。

Step2 计算层次总排序向量 $\overline{w_k^2}=\sum_{k=1}^{d}(w_{kj}^2)w_i^1$，$\overline{W^2}=W_j^2W^1=(\overline{w_1^2}, \overline{w_2^2}, \cdots, \overline{w_d^2})^{\mathrm{T}}$。

Step3　输出$\overline{W^2}$。

3.4　单资产的模糊综合威胁等级分析

假设威胁分析评价集为V，本文从安全事件发生对声誉、经济、业务3方面受到的影响程度，将其分为5个等级，通过V来确定评估对象的各资产面临的威胁等级。$V=\{v_1,v_2,v_3,v_4,v_5\}=$｛影响很小，影响不大，有一定影响，影响很大，影响极大｝$=\{0\sim20,20\sim40,40\sim60,60\sim80,80\sim100\}$。

每一个等级对应一个模糊子集，给出一个模糊映射(即隶属度函数)$f:TU\to F(V)$，$F(V)$是V上的模糊集全体，m_i表示其中一个元素，即$m_i\in F(V)$。$m_i=(\frac{c_{i1}}{c},\frac{c_{i2}}{c},\cdots,\frac{c_{ij}}{c},\cdots,\frac{c_{iy}}{c})$，$f$表示威胁因素$t_i$对评价集中各评语的支持程度，其中$c_{ij}$表示$c$位专家中评价某一资产面临的威胁因素$t_i$为等级$v_j$的人数。通过模糊集的隶属度函数确定出因素集的模糊评判矩阵M：

$$M=\begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1y} \\ m_{12} & m_{22} & \cdots & m_{2y} \\ \vdots & \vdots & \cdots & \vdots \\ m_{s1} & m_{s2} & \cdots & m_{sy} \end{pmatrix}_{s\times y}$$

式中，s表示因素集中元素个数，y表示威胁等级的元素个数。然后计算出单资产的综合威胁值并确定威胁等级。具体算法步骤如下。

输入：TU,V

输出：综合威胁等级集$AW=\{aw_1,aw_2,aw_3,aw_4,\cdots,aw_n\}$

Step1　根据$V=\{v_1,v_2,v_3,v_4,v_5\}$，$m_{ij}=\frac{c_{ij}}{c}$，其中$1\leqslant i\leqslant s$，$1\leqslant j\leqslant y$，求出$M$。

Step2　通过AHP算法计算出的$\overline{W^2}$，归一化后与M进行模糊变换计算，得到单资产的综合威胁值b_j及其集合B。$B=\overline{W^2}\circ M$，$b_j=\sum_{i=1}^{5}(\overline{w_i^2}m_{ij})$，其中$1\leqslant j\leqslant 5$。

Step3　得到$B=\{b_1,b_2,b_3,b_4,b_5\}$。

Step4　计算单资产的综合威胁等级$aw_i=\sum_{j=1}^{5}(b_jv_j)$。如果$1\leqslant i\leqslant n$，转至Step1。

Step5　输出AW。

3.5　信息安全威胁分析结果评估

通过3.4节所确定的信息资产威胁等级集AW，结合信息资产价值集AV，评估信息系统的综合威胁情况。用ZW表示不太乐观的状态集，$ZW=(aw_i\geqslant 3\wedge av_i\geqslant 2)$，应加强安全防范，以确保信息系统安全。

综上所述，本文提出的AHPTAM流程如图2所示。

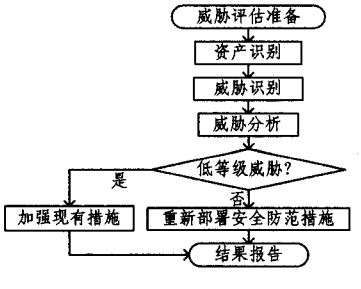

图2　信息安全威胁评估模型流程

4　实践

本文对某市招生录取系统进行信息安全威胁评估实践。首先根据相关部门提供的资料进行资产识别，得到资产列表，如表2所列。

表2　资产列表

A	a1	a2	a3	a4	a5	a6	a7
	数据	软件	硬件	服务	人员	文档	其它
AV	av1	av2	av3	av4	av5	av6	av7
	3	3	3	2	2	2	1
AE	ae1	ae2	ae3	ae4	ae5	ae6	ae7
	2	2	2	1	1	1	1

由于没有历史威胁数据，则根据威胁评估指标，结合专家经验知识，以数据资产为例进行预处理计算，产生威胁分析预处理列表，如表3所列。

表3　数据资产预处理列表

T	t1	t2	t3	t4	t5	t6
P	0.85	0.23	0.05	0.10	0.02	0.03
T	t7	t8	t9	t10	t11	
P	0.15	0.02	0.62	0.20	0.33	

由3.3节所述方法，根据威胁评估层次结构模型分别构造各个层次的判断矩阵。下面是TU层相对于G层的R：

$$R=\begin{pmatrix} 1 & 7 & 3 & 5 \\ 1/7 & 1 & 1/5 & 1/4 \\ 1/3 & 5 & 1 & 1/3 \\ 1/5 & 4 & 3 & 1 \end{pmatrix}$$

求得$W=(0.5461,0.0525,0.1706,0.2308)^T$。然后计算$R$的最大特征根和$CR$：$\lambda_{max}=4.0645$，$CR=0.0241<0.1$，可知$R$满足一致性，得到的权重比较合理。再通过构造$T$层各元素相对于$TU$层各元素的$R$，最后得到$T$层相对于$G$层的$\overline{W^2}=(0.3926,0.0918,0.0167,0.0368,0.0117,0.0264,0.0467,0.0117,0.1735,0.0725,0.1178)^T$。

接着对数据资产进行模糊综合威胁等级分析。本次实验有10位专家参与评价，首先得到模糊评判矩阵M：

$$M=\begin{pmatrix} 0 & 1/10 & 1/10 & 3/10 & 5/10 \\ 0 & 2/10 & 4/10 & 2/10 & 2/10 \\ 4/10 & 2/10 & 2/10 & 2/10 & 0 \\ 2/10 & 4/10 & 3/10 & 1/10 & 0 \\ 6/10 & 2/10 & 1/10 & 1/10 & 0 \\ 4/10 & 1/10 & 5/10 & 0 & 0 \\ 5/10 & 2/10 & 2/10 & 1/10 & 0 \\ 1/10 & 2/10 & 2/10 & 1/10 & 4/10 \\ 2/10 & 5/10 & 3/10 & 0 & 0 \\ 2/10 & 3/10 & 5/10 & 0 & 0 \\ 3/10 & 4/10 & 3/10 & 0 & 0 \end{pmatrix}$$

经线性变换计算后，得到$B=\{0.1410,0.2478,0.2406,0.1504,0.2193\}$。根据$aw_i=\sum_{j=1}^{5}(b_jv_j)$可以求出$aw_i=61.1654$，可知数据资产的威胁等级为$v_4$。以此类推，可以得到其它6个资产的威胁值和对应的威胁等级，从而得到$AW=\{v_4,v_2,v_3,v_1,v_2,v_2,v_1\}$。最后，将威胁等级集与各资产的价值相结合，得出结论：此招生录取系统部分符合要求，其面临的总体威胁影响不大，其中数据资产、硬件资产相对严重，应加强安全防范。

实践结果与第三方评测机构所测试的结果[9]是一致的，均为部分符合要求。由此可以看出，本文提出的基于AHP

的信息安全威胁评估模型是可行的，并且符合评估标准。

结束语 本文针对信息安全威胁评估问题，将模糊综合评价法和AHP方法相结合，识别出关键信息资产。建立层次模型后，考虑不同威胁发生的可能性，分别对每一层指标因素进行评估，从单资产威胁开始分析，再对综合威胁进行模糊综合评价，最后得到威胁评估结果。实验表明，本方法能够对信息系统面临的直接或间接的威胁进行有效评估，为科学管理提供了有力依据。但信息安全威胁存在动态复杂性，可采取预防、阻止、转移、检测和恢复来处理安全事件。为了有效地控制信息安全威胁，可采取5种方法来提高安全性：加密、软件控制、硬件控制、策略和过程、物理控制。不管采用何种安全措施，都要按照以下4大原则进行考虑：最易渗透原则、最弱环节原则、适度保护原则、有效性保护原则。

参考文献

[1] 赵冬梅，刘金星，马建峰. 基于改进小波神经网络的信息安全风险评估[J]. 计算机科学，2010，37(2)：90-93

[2] 宫亚峰，赵波，徐金伟. 再论信息安全资产的识别与评估[J]. 计算机安全，2010，2：5-10

[3] 何可，李晓红，冯志勇. 面向对象的威胁建模方法[J]. 计算机工程，2011，37(4)：21-23

[4] 陈清明，张俊彦. 信息安全风险评估工具及其应用分析[J]. 信息安全与通信保密，2010，1：93-95

[5] 蔡林，刘学忠. 基于攻击路径图的威胁评估方法[J]. 计算机应用，2009，6(29)：74-76

[6] Saaty T L. How to Make a Decision: The Analytic Hierarchy Process[J]. Interfaces, 1994, 24(6): 19-43

[7] Ashenden D. Information security management: A human challenge[J]. Information Security Technical Report, 2008(13): 195-201

[8] Garcia-Alfaro J, Barbeau M, Kranakis E. Analysis of Threats to the Security of EPC Networks[C]// Communication Networks and Services Research Conference. 2008

[9] OPR13等级测评报告[R]. 50000843002-10-5001-01. 2009：111

[10] 易昆南，晏玉梅. 改进的DS/AHP方法及应用[J]. 重庆理工大学学报：自然科学版，2011，25(5)：121-126

(上接第18页)

以访问并使用的在线代码缺陷分析集成服务云。在整体介绍CODAS之后，本文详细叙述了CODAS在可扩展性方面的设计和实现。为了解决缺陷检测能力的扩展性问题，CODAS设计了一个统一的“独立缺陷分析工具”服务化的封装接口。为了解决数据存储能力的扩展性问题，基于分布式文件式系统Hadoop，搭建了一个可扩展的数据存取服务并将其独立部署，以供CODAS集中方便地进行数据(受检程序，中间分析结果、历史缺陷分析报告等)存储。除此之外，我们也对数据库服务和Windows文件资源存取服务进行了独立部署，以满足CODAS的其他数据访问需求。为了解决缺陷报告的合理汇总和排序问题，我们基于机器学习的方式对开源软件的缺陷修复历史进行挖掘学习，从而自动化地识别出最有可能引起程序员修复行为的缺陷报告并将其优先报告[11]。为解决运算性能问题，我们尽可能将系统中的各个功能模块化进而独立部署，以提高整个系统的响应时间和并发访问量。本文还通过实验，分别评估了CODAS的有效性。通过实验，发现CODAS的缺陷报告能使得Lucene，ANT，Spring等受检项目的前22，19，7条缺陷报告的准确度始终高于90%。实验说明CODAS能够有效预测出准确且能够优先引起程序员修复动作的缺陷报告并将其优先报出。

在未来工作中，将围绕CODAS的可用性和有效性方面的不足继续完善本在线缺陷分析集成系统。我们可以通过提供同一受检项目不同版本的缺陷分析报告的比较功能，帮助程序员快速定位新版本引入的缺陷报告，以提高其排错效率。除此之外，还可以通过探索更好的在线缺陷报告反馈功能，高效地收集程序员对于缺陷分析报告的权威评价，从而进一步优化缺陷分析报告的排序效果。

参考文献

[1] Copeland T. PMD applied[M]. Centennial Books, 2005

[2] Ayewah N, Hovemeyer D, Morgenthaler J D, et al. Experiences using static analysis to find bugs[J]. IEEE Software, 2008, 25(5): 22-29

[3] Nanda M G, Gupta M, Chandra S, et al. Making Defect-finding Tools Work for You[C]// Proceedings of the International Conference on Software Engineering (ICSE). 2010: 99-108

[4] Nielson F, Nielson H R, Hankin C. Principles of Program Analysis(Corrected 2nd printing)[M]. Springer, 2005

[5] Boyer R S, Elspas B, Levitt K N. SELECT—a formal system for testing and debugging programs by symbolic execution[C]// Proceedings of the International Conference on Reliable Software. 1975: 234-245

[6] Clarke E M, Grumberg J O, Peled D A. Model Checking[M]. MIT Press, 2000

[7] Cousot P, Cousot R. Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints[C]// Proceedings of the 4th ACM Symposium on Principles of Programming Languages (POPL). 1977: 238-252

[8] Lint4J[EB/OL]. http://www.jutils.com/

[9] Hallem S, Chelf B, Xie Y, et al. A System and Language for Building System-Specific, Static Analyses[C]// Proceedings of the ACM SIGPLAN 2002 Conference on Programming Language Design and Implementation(PLDI). 2002: 69-82

[10] Wagner S, Jrjens J, Koller C, et al. Comparing bug finding tools with reviews and tests[C]// Proceedings of the 17th International Conference on Testing of Communicating Systems. volume 3502 of Lecture Notes in Computer Science, June 2005: 40-55

[11] Liang Guang-tai, Wu Ling, Wu Qian, et al. Automatic Construction of an Effective Training Set for Prioritizing Static Analysis Warnings[C]// Proceedings of the 25th IEEE/ACM International Conference on Automated Software Engineering. 2010: 93-102

[12] Hovemeyer D, Pugh W. Finding Bugs is Easy[C]// Companion to the 19th annual ACM SIGPLAN Conference on Object-oriented Programming Systems, Languages and Applications (OOPSLA). 2004: 92-106

[13] Jlint[EB/OL]. http://artho.com/jlint