信度向量正交投影分解的网络安全风险评估方法

刘 刚* 李千目 张 宏
(南京理工大学计算机科学与技术学院 南京 210094)

摘 要：传统安全风险评估方法大都存在着主观性和片面性问题，该文针对网络节点的漏洞和攻击层面的风险分析需求，提出了漏洞信度和攻击信度的概念，设计了一种信度向量正交投影分解的网络安全风险评估方法。该方法首先将攻击所依赖的漏洞信息和节点本身漏洞信息相关联，结合网络中各节点自身的权重，量化从节点至全网的安全风险分析；其次，在漏洞信度计算时，为了排除漏洞扫描工具自身的不确定因素和数据源的单一性，将多个扫描工具的检测结果融合，构成数据源；最后，基于欧式空间向量投影的思想提出了一个信度向量投影分解算法。实验结果验证了该文方法的有效性。

关键词：网络安全；安全风险评估；信度向量正交投影分解
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2012)08-1934-05
DOI: 10.3724/SP.J.1146.2011.01387

Reliability Vector Orthogonal Projection Decomposition Method of Network Security Risk Assessment

Liu Gang Li Qian-mu Zhang Hong
(*School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing* 210094, *China*)

Abstract: Most traditional security risk assessment methods have the shortcomings of subjectivity and one-sidedness. Considering the risk analysis demand of vulnerabilities and attacks of network nodes, this paper proposes the concept of vulnerability reliability and attack reliability, and designs a reliability vector orthogonal projection decomposition method of network security risk assessment. First, this method associates vulnerability information which attacks relying on with vulnerability information of the node itself, and quantifies the security risk analysis from the node to the whole network, with the own weight of each node in the network. Second, in order to exclude the own uncertainties of vulnerability scanning tools and the unity of the data source, this method fuses several test results of scan tool, and constitutes the data source when calculating the vulnerability reliability. Finally, based on the idea of Euclidean space vector projection, the method puts forward an algorithm of reliability vector projection decomposition. The result of the experiment of the network security risk evaluation procedure is given to verify the proposed evaluate method.

Key words: Network security; Security risk assessment; Reliability vector orthogonal projection decomposition

1 引言

随着物联网和云计算的发展与普及，诸如电子商务、电子政务等众多网络信息系统都朝着物联、云联的方向发展。一旦这些网络信息系统发生安全问题，将会对国家的经济和安全带来巨大的损失和灾难性的后果[1−3]。因此，如何准确、全面地评估网络的安全风险具有重要的现实意义。本领域作为新兴研究热点，诸多研究人员近期开展了大量的研究，目前代表性的研究成果主要有：

文献[4]利用入侵检测系统收集海量报警信息和网络性能指标，结合服务、主机自身的权重及网络系统的组织结构，提出一种服务、主机、网络系统的层次化安全威胁态势定量评估模型及量化方法，但该方法的数据来源较为单一，而且在量化算法中多处采用加权分析，具有较大的主观性。文献[5]提出将目标主机基本信息、目标主机可能存在的漏洞、各漏洞的可利用性影响因素通过证据理论融合起来，得到主机的总体安全量化值，该方法未考虑证据之间可能存在冲突，当信息源数量增大时，融合计算复杂度会呈指数上升。文献[6]基于网络性能度量指标，评估分析网络攻击对系统安全的影响，此

2011-12-27 收到，2012-04-13 改回
国家自然科学基金(60903027)，江苏省自然科学重大研究项目(BK2011023)和江苏省自然科学基金(BK2011370)资助课题
*通信作者：刘刚 liugang_nj@163.com

方法仅适用于分析拒绝服务类攻击，不能评估其他类别的攻击对系统安全的威胁。文献[7]设计了一种基于 Markov 博弈分析的网络安全态势感知方法，通过对威胁、管理员和普通用户的行为进行博弈分析，建立三方参与的 Markov 博弈模型，进而评估网络安全态势。但该方法的不足在于，当资产数据增加时，博弈模型的状态空间呈指数增加，使得评估效率急速下降。

结合已有的研究成果，本文将节点漏洞信息和成功攻击时所依赖的漏洞关联起来，提出了一种信度向量正交投影分解的网络安全风险评估方法。该方法从网络节点的漏洞和攻击角度出发，将攻击所依赖的漏洞信息和节点本身漏洞信息相关联，提出漏洞信度、攻击信度的概念，结合网络中各节点自身的权重，使得网络节点和整个网络的安全风险得以量化。

2　安全风险评估框架

本文在文献[8]和文献[9]证据理论中对信度定义的基础上，给出以下定义：

定义 1　漏洞信度。节点中单个漏洞存在的支持度，记作 f_{v_i}。

定义 2　攻击信度。节点中单个攻击成功发生的支持度，记作 f_{a_j}。

定义 3　漏洞危害度：节点中单个漏洞对其的危害程度，记作 e_{v_i}。

定义 4　攻击危害度：节点中单个攻击成功发生后对其的危害程度，记作 e_{a_j}。

定义 5　漏洞安全风险 R_{v_i}，某节点中单个漏洞存在时所致的风险大小，用漏洞信度和漏洞危害度的乘积表示。

$$R_{v_i} = f_{v_i} e_{v_i} \tag{1}$$

其中 f_{v_i} 为漏洞 v_i 存在的信度，e_{v_i} 为漏洞 v_i 对其节点的危害程度。

定义 6　攻击安全风险 R_{a_j}，外部攻击利用网络节点的漏洞成功发生时所致的风险大小，用攻击信度和攻击危害度的乘积表示。

$$R_{a_j} = f_{a_j} e_{a_j} \tag{2}$$

其中 f_{a_j} 为攻击 a_j 成功发生的信度，e_{a_j} 为攻击 a_j 成功发生后对其节点的危害程度。

定义 7　节点安全风险 R_{H_k}，单个节点的安全风险由其所有的漏洞安全风险和攻击安全风险两部分组成。

$$R_{H_k} = \sum_{i=1}^{m} R_{v_i} + \sum_{j=1}^{n} R_{a_j} \tag{3}$$

其中 m 为节点 H_k 中所存在的漏洞总数，n 为节点 H_k 中成功发生的攻击总数，R_{v_i} 为式(1)计算出来的漏洞安全风险，R_{a_j} 为式(2)计算出来的攻击安全风险。

定义 8　网络安全风险 R_{N}，外部攻击通过各网络节点对其造成的损失，用节点安全风险的加权和来表示。

$$R_{\mathrm{N}} = \sum_{k=1}^{p} \omega_k R_{H_k} \tag{4}$$

其中 p 为网络中节点的总数，ω_k 为节点 H_k 占网络的权重，R_{H_k} 为式(3)计算出来的单个节点安全风险。

本文根据网络系统的层次结构以及攻击和漏洞的逻辑关系，设计了如图 1 所示的安全风险评估框架。

该框架自下而上，首先通过多种漏洞扫描工具确定节点中存在的漏洞集，进一步计算出节点的漏洞信度向量和攻击信度向量，结合每种漏洞危害和攻击危害，推算出节点的漏洞安全风险和攻击安全风险，进而评估单个节点的安全风险值，最后根据网络各节点所占网络的权重，给出整个网络系统的安全风险结果。

3　安全风险量化算法

根据图 1 的评估框架评估整个网络系统的安全风险值，首先要计算出漏洞安全风险值 R_{v_i} 和攻击安

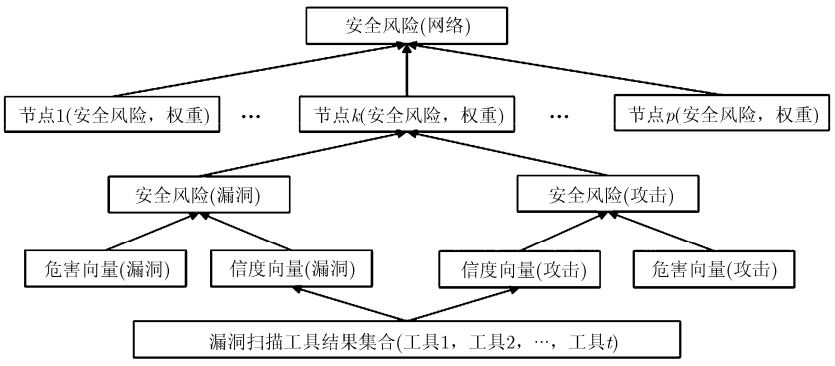

图 1　安全风险评估框架

全风险值 R_{a_j}。而漏洞安全风险值 R_{v_i} 和攻击安全风险值 R_{a_j} 的计算又要先确定各漏洞信度 f_{v_i}，漏洞危害度 e_{v_i}，攻击信度 f_{a_j} 和攻击危害度 e_{a_j}。

3.1 漏洞信度

由于漏洞扫描工具本身具有不确定性，错报率和漏报率较高，为了得到单个漏洞的信度，本文以多种漏洞扫描工具的结果为数据源，提出了一种信度向量正交投影分解算法，来计算单个漏洞的信度。将单个漏洞扫描工具的准确率作为可信度，扫描结果集看作一个信度向量，对每个信度向量进行正交投影分解，进而得到单个漏洞的信度。下面以 t 种漏洞扫描工具对单个节点 H_k 扫描为例，其步骤见表 1 的算法 1。

算法 1 中漏洞扫描工具种数 t 的选取，管理员可根据网络的规模、评估的实际需要和以往的经验来选择。但 t 值过大导致评估成本和计算的时间过长，t 值过小使得漏报率和错报率过高。因此，根据经验，其取值一般 3–4 较为合适。

表 1 漏洞信度算法

算法 1　漏洞信度算法

输入：每种扫描工具的漏洞集合

输出：节点 H_k 中每个漏洞的信度

(1)利用 t 种漏洞扫描工具对节点 H_k 进行漏洞扫描，得到每种工具对节点 H_k 的漏洞扫描结果集合，记作 $V_s, s=1,2,\cdots,t$。将所有扫描工具对 H_k 的漏洞扫描结果集合相并，作为节点 H_k 的漏洞信度向量空间，记为 $\Omega=\bigcup_{s=1}^{t} V_s=\{x_1,x_2,\cdots,x_m\}$。由于 Ω 中的元素两两互不包含，将其中的元素看作是两两互相垂直的坐标轴，Ω 即为包含 m 个坐标轴的坐标系。

(2)将每种扫描工具的结果集 V_s，看作 Ω 中的一个信度向量 $\boldsymbol{v}_s$，将每种扫描工具的准确率归一化后作为信度向量 $\boldsymbol{v}_s$ 的模，记为 $\|\boldsymbol{v}_s\|=r_s$。

(3)设信度向量 $\boldsymbol{v}_s$ 与坐标轴 $x_i, i=1,2,\cdots,m$ 的方向角为 $\alpha_{\boldsymbol{v}_s x_i}$，计算信度向量 $\boldsymbol{v}_s$ 与空间中各坐标轴 x_i 的方向余弦 $\cos\alpha_{\boldsymbol{v}_s x_i}$。$\forall x_i\in\Omega$，若 $x_i\notin V_s$，则 $\cos\boldsymbol{v}_s x_i=0$；若 $x_i\in V_s$，则 $\boldsymbol{v}_s$ 与这些坐标轴的方向余弦相等。令信度向量 $\boldsymbol{v}_s=\{x_1,x_2,\cdots,x_u\}, s=1,2,\cdots,t$，信度向量空间 $\Omega=\{x_1,x_2,\cdots,x_u,x_{u+1},\cdots,x_m\}$，$\cos\alpha_{\boldsymbol{v}_s x_i}=1/\sqrt{u}$。

(4)计算信度向量 $\boldsymbol{v}_s$ 在各坐标轴 $x_i, i=1,2,\cdots,m$ 上的正交投影分解值，即

$$r_s\cos\alpha_{\boldsymbol{v}_s x_i} \tag{5}$$

(5)将每个信度向量 $\boldsymbol{v}_s$ 向同一个坐标轴上的正交投影分解值累加求和，

$$f_{x_i}=\sum_{s=1}^{t} r_s\cdot\cos\alpha_{\boldsymbol{v}_s x_i} \tag{6}$$

将所有 $f_{x_i}, i=1,2,\cdots,m$ 归一化，得

$$\overline{f}_{x_i}=f_{x_i}\Big/\sum_{i=1}^{m} f_{x_i} \tag{7}$$

$\overline{f}_{x_i}$ 即为节点 H_k 中单个漏洞存在的信度。$\overline{f}_{x_i}$ 所构成的集合为节点 H_k 中的漏洞信度向量。

3.2 攻击信度

节点所遭受的攻击是利用网络节点存在的安全漏洞而实施的，攻击的成功与否主要取决于其所依赖的漏洞，因此节点上存在攻击所依赖的漏洞越多，攻击成功的可能性就越大。本文用已发生的攻击所依赖的漏洞和节点中存在的漏洞的匹配程度来衡量其信度。其算法流程描述如表 2 算法 2 所示。

表 2 攻击信度

算法 2　攻击信度

输入：t 种漏洞扫描工具对节点 H_k 的漏洞扫描结果集合 $V_s, s=1,2,\cdots,t$；攻击 a_j 所依赖的漏洞集合 $\{v_1,v_2,\cdots,v_w\}$

输出：攻击信度 f_{a_j}

(1)set $f_{a_j}=0$；

(2)将所有扫描工具对 H_k 的漏洞扫描结果集合相并，得到节点 H_k 的漏洞空间，记为 $\Omega=\cup V_s=\{v_1,v_2,\cdots,v_m\}, s=1,2,\cdots,t$；

(3)if($\{v_1,v_2,\cdots,v_w\}$ of an attack $\subseteq\{v_1,v_2,\cdots,v_m\}$ of a node){

(4)　$f_{a_j}=1$；

(5)　return f_{a_j}；

(6)}

(7)for each vulnerability v_i in $\{v_1,v_2,\cdots,v_w\}$ of an attack {

(8)　if (v_i in $\{v_1,v_2,\cdots,v_m\}$ of a node) $f_{a_j}+=f_{v_i}$；

(9)}

(10)return f_{a_j}。

算法 2 描述了单个攻击的可信度计算，针对节点中所发生的攻击种类，只要重复多次使用算法 2，就可确定节点中的攻击信度向量。

3.3 漏洞危害度、攻击危害度和权重分配

3.3.1 漏洞危害度　漏洞的危害程度是该漏洞严重性的直接表现，因此可以用漏洞的严重程度来衡量其危害度。美国国家漏洞数据库(National Vulnerability Database Version 2.2)是目前最为权威的漏洞信息数据库之一。该数据库从漏洞的利用方式、利用复杂度、目标认证次数以及对信息机密性、完整性和可用性的影响大小等几个方面给出了漏洞的严重性度量[10]，其值介于 0 至 10 之间。可以根据通用漏洞披露(Common Vulnerabilities and Exposures, CVE)的标识，从美国国家漏洞数据库中查询其对应的严重度，作为漏洞的危害度。

3.3.2 攻击危害度　参考中国反入侵反病毒研究中心(National Anti-Intrusion & Anti-Virus Research Center)对攻击的危害度的界定，以及美国林肯实验室的入侵检测攻击数据库中对攻击种类的划分，本文将攻击的危害指数 r_{a_j} 划分为以下 4 个等级：

超高：如缓冲区溢出攻击，权限提升攻击等。危害指数 4；

高：如远程过程调用攻击，ftp 攻击等，危害指数 3；

中：如拒绝服务攻击等，危害指数 2；

低：如网络连接扫描，端口扫描等。危害指数 1。

由于一个超高级攻击可能要比多个中、低级攻击的危害度更大，因此在计算攻击危害度时，参照文献[4]对攻击事件威胁指数的修正，攻击危害度的计算如下：

$$e_{a_j} = C_{a_j} \cdot 10^{r_{a_j}} \tag{8}$$

其中 C_{a_j} 是攻击 a_j 发生的次数，可对攻击日志数据库进行统计得到；r_{a_j} 是攻击危害指数。

3.3.3 权重分配　本文权重分配是由系统管理员根据节点中服务的重要程度、节点的拓扑连接、服务的访问次数等因素给出网络中各节点的地位 I_k，并对其进行归一化处理得到。在实际操作过程中，可根据系统的不同做相应的调整。

4　实验与分析

为了说明本方法的具体应用，本文设计了如图 2 所示的网络拓扑结构来验证本方法的有效性。网络中有 3 台服务器，分别为一台公共 Web 服务器，

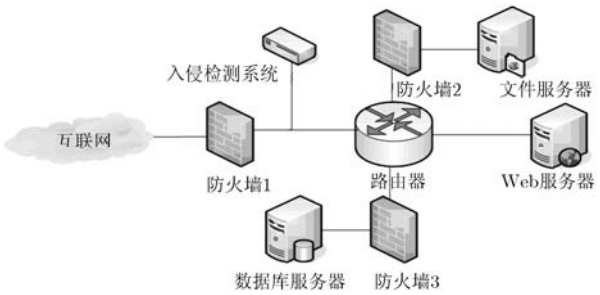

图 2 网络拓扑图

其上运行 Web 服务、邮件服务、远程管理控制服务和 FTP 服务；一台文件服务器，用于重要文件和数据的备份；一台数据库服务器，为 Web 服务器提供数据库服务。

利用 Nessus, ISS 互联网扫描器和 SARA 3 种漏洞扫描工具，对网络中 3 个服务器节点进行扫描，扫描结果如表 3 所示，括号内的数值表示该漏洞的危害度。

模拟黑客，按照 7:00 至 11:00, 11:00 至 15:00，15:00 至 19:00 3 个时段，对 Web 服务器、文件服务器和数据库服务器发起 DoS(Denial of Service)攻击、ftp 缓冲区溢出攻击和超级管理员(Root)权限提升攻击。每种攻击所依赖的漏洞如表 4 所示。

表 3 漏洞扫描结果

工具	节点		
	Web Server	File Server	Database Server
Nessus	CVE-2010-4562 (4.3) CVE-2011-1871 (7.8) CVE-2007-0066 (7.1)	CVE-2004-2111 (8.5) CVE-2011-4800 (9.0)	CVE-2002-0060 (7.5) CVE-2000-0800 (10)
ISS	CVE-2011-1871 (7.8)	CVE-2004-2111 (8.5)	CVE-2002-0060 (7.5) CVE-2000-0800 (10)
SARA	CVE-2010-4562 (4.3) CVE-2011-1871 (7.8)	CVE-2009-1439 (7.8) CVE-2012-0450 (2.1)	CVE-2002-0060 (7.5) CVE-2000-0800 (10)

第 1 时段：8:00 至 11:00 期间，对 Web 服务器发起 DoS 攻击，由 Intrusion Detection System (IDS) 的日志分析得到攻击检测结果如表 5 所示。

表 4 攻击信息

攻击	依赖漏洞	危害指数
ftp缓冲区溢出	CVE-2004-2111, CVE-2011-4800	4
Root权限提升	CVE-2002-0060, CVE-2000-0800	4
DoS	CVE-2010-4562, CVE-2011-1871, CVE-2007-0066	2

表 5 第 1 时段攻击检测结果

攻击\节点	Web服务器(次)	文件服务器(次)	数据库服务器(次)
ftp缓冲区溢出	0	0	0
超级管理员权限提升	0	0	0
DoS	5	0	0

根据算法 1 可得漏洞 CVE-2010-4562, CVE-2011-1871 和 CVE-2007-0066 的所构成的信度向量为(0.30851, 0.55038, 0.14111)。同理，可得文件服

务器中漏洞 CVE-2004-2111, CVE-2011-4800, CVE-2009-1439, CVE-2012-0450 所构成的信度向量为 (0.45, 0.187, 0.1815, 0.1815)；数据库服务器中漏洞 CVE-2002-0060, CVE-2000-0800 所构成的信度向量为(0.5, 0.5)。根据算法 2 可得 DoS 的攻击信度为 1。进而可得 Web 服务器、文件服务器和数据库服务器的风险分别为 506.621438, 7.30485, 8.75，根据管理员对 Web 服务器、文件服务器和数据库服务器权重的分配，假设为 0.25, 0.35, 0.4，可计算第 1 时段网络的安全风险为 132.712。

第 2 时段：12:00 至 15:00 期间，继续加强对 Web 服务器的 DoS 攻击，同时向文件服务器发起 ftp 缓冲区溢出攻击，IDS 检测到的攻击如表 6 所示。

表 6 第 2 时段攻击检测结果

攻击\节点	Web服务器 (次)	文件服务器 (次)	数据库 服务器(次)
ftp缓冲区溢出	0	1	0
超级管理员权限提升	0	0	0
DoS	10	0	0

按照上述同样的计算方法，可得第 2 时段网络的安全风险为 3756.861。

第 3 时段：17:00 至 20:00 期间，继续对文件服务器发起 ftp 缓冲区溢出攻击，同时向数据库服务器发起超级管理员权限提升攻击，但停止对 Web 服务器的 DoS 攻击，IDS 检测到的攻击如表 7 所示。

表 7 第 3 时段攻击检测结果

攻击\节点	Web服务器 (次)	文件服务器 (次)	数据库 服务器(次)
ftp缓冲区溢出	0	1	0
超级管理员权限提升	0	0	1
DoS	0	0	0

同理，第 3 时段网络的安全风险为 7507.712。

由上述实验可以看出，第 1 时段的风险最低，第 2 时段居中，第 3 时段的风险最高。和第 1 时段相比，第 2 时段由于攻击次数的增加，该时段风险值要比第 1 时段的高，特别是增加了一次危害指数为 4 级的 ftp 缓冲区溢出攻击后，其网络的风险有了显著的增加。第 3 时段，虽然停止了 DoS 的攻击，攻击次数有了明显降低，但所发生的攻击危害指数较大，因此第 3 时段的风险反而有了更进一步的增大，进一步验证了一个超高级攻击要比多个中、低级攻击的危害大得多。在选取适当的时间窗口之后，周期性地采用本文提出的评估方法能够有效地、合理地评估整个网络的安全风险。

5 结束语

本文提出了一种信度向量正交投影分解的网络安全风险评估方法，该方法从网络节点的漏洞和攻击角度出发，将节点漏洞信息和成功攻击时所依赖的漏洞关联起来，用漏洞信度、漏洞危害度、攻击信度和攻击危害度来表示节点风险。结合网络中各节点自身的权重，进而量化整个网络的安全风险。最后，利用本文提出的评估方法，在一天的不同时段，通过对一个小型局域网络的风险评估，更进一步的说明了本方法的具体应用。实验表明该方法的评估结果和实际情况相符，能正确的评估网络的安全风险，并能直观地给出量化风险值。

参 考 文 献

[1] Grobauer B, Walloschek T, and Stocker E. Understanding Cloud computing Vulnerabilities[J]. *IEEE Security & Privacy*, 2011, 9(2): 50–57.

[2] Chen Jun and Tu Xiong-gang. Network security risk assessment based on support vector machine[C]. 2011 IEEE 3rd International Conference on, Communication Software and Network(ICCSN), Xi'an, China, May 27–29, 2011, 9: 184–187.

[3] Anderson E E. Firm objectives, IT alignment, and information security[J]. *IBM Journal of Research and Development*, 2010, 54(3): 5:1–5:7.

[4] 陈秀珍, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885–897.
Chen Xiu-zhen, Zheng Qing-hua, Guan Xiao-hong, *et al.*. Quantitative hierarchical threat evaluation model for network security[J]. *Journal of Software*, 2006, 17(4): 885–897.

[5] 陆余良, 夏阳. 主机网络安全量化融合模型研究[J]. 计算机学报, 2005, 28(5): 914–920.
Lu Yu-liang and Xia Yang. Research on target-computer secure quantitative fusion model[J]. *Chinese Journal of Computers*, 2005, 28(5): 914–920.

[6] Hariri S, Qu G Z, Dharmagadda T, *et al.*. Impact analysis of faults and attacks in large-scale networks[J]. *IEEE Security & Privacy*, 2003, 1(5): 49–54.

[7] 张勇, 谭小彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495–508.
Zhang Yong, Tan Xiao-bin, Cui Xiao-lin, *et al.*. Network security situation awareness approach based on Markov game model[J]. *Journal of Software*, 2011, 22(3): 495–508.

[8] Shafer G A. Mathematical Theory of Evidence [M]. Princeton: Princeton University Press, 1976: 25–38.

[9] Dempster A P. Upper and lower probabilities induced by a multivalued mapping[J]. *The Annals of Mathematical Statistics*, 1967, 38(2): 325–339.

[10] Mell P, Scarforne K, and Romanosky S. A complete guide to the common vulnerability scoring system version 2.0[OL]. http:// www.first.org/cvss/cvss-guide.html#i2.1, 2007, 6.

刘 刚： 男，1985 年生，博士生，研究方向为信息安全.
李千目： 男，1979 年生，副教授，研究方向为信息安全、无线传感网.
张 宏： 男，1956 年生，教授，博士生导师，研究方向为网络安全、可信计算.