信息系统安全度量理论和方法研究*)

吕 欣
(国家信息中心 北京 100045)

摘 要 随着国家信息化工作的纵深推进,信息安全问题日益突出,政府、重要行业和企业对信息安全的依赖性越来越大,投入逐步增加,并越来越意识到"度量"在信息安全工作中的重要地位。介绍了信息安全度量的基本原理,分析了信息安全度量的核心要素和建模方法。综合考虑信息安全能力、信息安全费用和信息安全措施等因素,给出了基于"基线"的信息安全度量模型,并研究了信息安全模糊综合度量方法。

关键词 信息安全,风险管理,安全度量,指标体系

Information System Security Metrics: Theoretics and Methodology

LU Xin
(State Information Center, Beijing 100045, China)

Abstract As information security lost continues to rise, public and private organizations contend that metrics initiatives will become critical to managing and understanding the impact of information security programs. Information security metrics theory was introduced and the several key steps to implement metrics program were defined. Considering the security capabilities, security cost and security countermeasures, we addressed a baseline-based information security metrics model and applied the fuzzy synthetic techniques to information security metrics.

Keywords Information security, Risk management, Security metrics, Evaluation indices

1 引言

随着国民经济和社会信息化进程的推进,网络与信息系统的基础性、全局性作用日益增强,国民经济和社会发展对网络和信息系统的依赖性越来越大,信息安全已经成为国家非传统安全的一个重要领域[1-3]。党的十六届四中全会,将信息安全提到与国家政治安全、经济安全、文化安全并重的高度。2006年3月,中共中央办公厅、国务院办公厅联合颁布了《2006-2020年国家信息化发展战略》,把建设信息安全保障体系纳入国家信息化发展战略,加快信息安全保障体系建设成为推进经济社会信息化的重要内容。科学判断和掌控我国信息安全态势,加强信息安全度量理论和方法研究,提升国家信息安全决策和管理水平成为新世纪、新阶段信息安全工作的重要任务。

度量(Metrics)和测量(Measure)之间有着本质的不同。测量是通过计数提供对离散因素的精确描述[4-6]。度量是通过收集、分析、报告与性能相关的数据以协助决策、提高性能和明确责任的过程。度量的目的是为了监控被测对象的状态,并能根据度量结果,采取相关措施,以提高被测对象的性能。

安全度量提供了一个信息系统安全管理体制,并能维持组织信息安全状况的持续改进。目前国内外研究较多的信息安全度量是关于信息技术或产品的安全度量、信息安全风险分析等相关理论和方法,并已形成相应的标准与规范,如ISO/IEC 17799[7],ISO/IEC 13335-1[8],ISO/IEC 15408[9]等。这些标准对信息技术的安全性评估方法、系统或资产的风险分析要素等进行了系统的描述。

本文重点研究信息系统安全度量的一般原理和方法,为组织信息安全决策提供理论和实践支持。本文认为,信息安全度量至少应包括以下几方面内容:

- 信息系统的脆弱性;
- 呈现出的安全威胁;
- 信息系统配置的符合性,检查系统的软硬件配置是否符合相关标准和规范;
- 安全策略的实施,人员和管理流程等是否满足组织的安全策略;
- 安全风险评估;
- 补救(Remediation),通过安全测度,给出信息系统中哪些设备和主机需要修复,哪些系统需要升级,并对已经损害的系统和设备进行恢复。

信息安全度量是业界公认的一个难题[1,3]。信息安全度量一般需要回答两个问题:信息系统安全不安全?信息系统的安全程度是多少?通常情况下,常常通过分析某个信息系统在一段时期内发生安全事件的多少来分析一个系统是否安全。然而,一段时期信息安全事件(如网页遭受篡改)的数量少于以前,其原因可能是多方面的:一种可能是系统增加了安全防护措施,系统变得安全了;第二种可能是外部攻击少了,即外部环境发生了变化;第三种可能是信息系统所承载的信息的吸引力降低了,致使黑客的视线被吸引到其它地方。因此,实施信息安全度量至少需要考察三个方面的因素:防护措施和能力的变化、外部安全环境的变化和信息自身价值的变化。因此,诸多不确定因素的存在增加了信息安全度量的复

*)本研究得到国家博士后科学基金(No. 20060400048),国家社会科学基金(No. 07CTQ010)资助。吕 欣 博士后,副研究员,研究方向为电子政务、信息安全。

杂性，也决定了对信息安全的度量是多维的，而且各个维之间还存在着非线性的复杂关联。

信息安全度量需要注意的另一个概念就是安全的相对性。说“一个对象（如密码算法或系统）是安全的”隐含着两层含义，一是该对象针对谁（即什么水平的攻击者）是安全的，在多长时间内是安全的。这是因为很多安全的概念都是以某些数学假设为基础的，即假设计算设备的计算能力有限，且计算时间有限。

基于以上分析可知，评估至少要对以下因素进行分析：

①信息和信息系统自身价值判断；

②外部安全环境变化，即对手的攻击强度；

③时间因素的分析；

④保障措施的强度和费用等。

2 信息安全度量的基本原理

科学的信息安全度量一般包括目标定义、需求分析、建立度量模型、设定安全基线、信息系统改进和安全控制等内容。

（1）明确度量目标

度量目标就是一个组织实施信息安全度量的动机，它影响着度量所采用的指标以及相应的安全基线。信息安全度量的目标可以分为长期目标和短期目标。信息安全度量的长期目标包括：分析和判断信息安全态势、信息安全控制的有效性、为组织的信息安全管理和决策提供支持等。信息安全度量的短期目标包括：了解对某一项安全项目投入的效益、为调整近期的安全策略提供决策依据等。

（2）定义信息安全需求

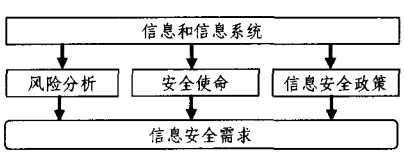


图1 信息系统安全需求分析

面对复杂的网络信息系统，全面、准确地分析其安全需求是实施度量的基础。本文建议通过以下步骤分析信息系统的安全需求。

1）界定研究对象，明确本系统信息安全的使命、目标和功能，分析系统在国家安全、社会稳定和经济发展中的地位和作用。

2）给出信息系统业务描述，包括本信息系统主要业务应用、业务流程和信息流程。

3）针对本系统信息安全建设的使命、信息的重要程度、信息系统承载业务的重要程度、风险分析的结果、系统遭到攻击破坏后造成的危害程度等因素，确定本信息系统的安全的总体需求。

4）进一步明确系统对信息和信息系统的保密性、完整性、可用性、真实性和不可否认性等安全属性的需求程度。

（3）确定度量指标

根据组织的度量目标和信息系统的安全需求确定度量指标。度量指标的选取要遵循两个原则：定性与定量相结合原则和可操作性原则。在信息安全度量过程中会涉及到诸多不确定性因素，有些度量指标可以量化，而有些则无法进行直接量化。因此，需要坚持定性与定量相结合的原则。同时，信息安全度量所建立的模型，应满足量化计算的可行性，否则，会导致无法计算而得不到最终的评估结果。

选取度量指标要以产生可计量的数据为导向，以便于比较。例如可以采用公式以便于分析，或选择参考点以追踪变化。百分比和平均数也是度量中常用的方法，有时也可以使用绝对数，这都取决于被考察对象的性质。

（4）建立度量模型

建立度量模型有两个任务：一是分析各度量指标所占的权重；二是将各度量指标通过数学模型进行合成，且要保证模型的科学性。

（5）设定信息安全基线

“基线”对应的英文是 Baseline，其含义是 a standard measurement or fact against which other measurements or facts are compared，它是一种用于度量或在度量中用于比较的基准。“基线”的概念已经应用于信息安全标准或规范当中，如美国联邦信息处理标准 FIPS199。本文把信息安全基线定义为特定条件下实现其安全使命和功能的基本安全需求。

信息安全基线是为了度量不同时段的安全状况所开发出的一套指标集，它将信息系统当前的安全状况与基线进行度量比较，可以了解当前的安全状态。基线会随着组织及其信息系统结构的变化而变化。如果一个组织增加了 50 名新员工，或新配置了无线局域网办公环境，组织系统的正常运行会发生新的变化。这时，就需要为系统更新或添加新的安全基线指标。

（6）制定信息安全度量制度

建立了信息安全度量模型和基线，就可以对组织的信息系统实施安全度量了。但是，确定信息安全度量周期、建立专职队伍、实施人员培训、将安全度量纳入组织的日常管理等等，则需要建立一套与度量目标相一致的度量制度。

3 信息安全度量的理论模型设计

安全基线为建立信息安全度量指标体系提供了参考和标准，同时信息安全度量的结果又反作用于基线，并能对保障基线进行动态调整（如图 2 所示）。基线控制流程可表述为：

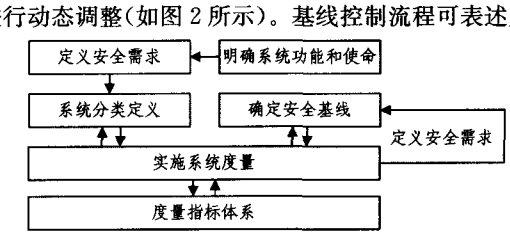


图2 信息安全基线控制流程

安全基线方法为组织信息安全管理提供了一种经济的解决方案，组织不需要花费力气制定各自的安全解决方案，它们可以根据基线目录来选取安全措施，以满足其需求。

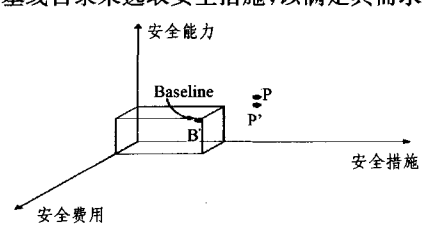


图3 信息安全基线度量模型

在信息安全基线度量模型中（见图 3），记信息安全能力

为 IA、信息安全费用为 CST、信息安全措施为 C、时间计为 T。对某信息系统 A 的安全度量可表述为 IA，CST，C 和 T 的函数：

$$S=(IA,CST,C,T) \tag{1}$$

(1) 信息安全措施

信息安全措施是指为实现信息和信息系统的保密性、完整性、可用性、真实性和不可否认性等所采取的技术和管理手段。如加密、认证、PKI、信息隐藏和灾难备份技术等。

(2) 信息安全能力

信息安全能力(IA 能力)度量用于考察网络系统的预警能力、安全防护能力、隐患发现能力、应急处置能力和追踪反制能力。IA 能力度量的数据主要来自某个时段的历史数据和试验数据。

1)系统预警能力

主要由预警时间和预警空间两个指标进行度量。预警时间指标可以从漏洞信息发布到利用此漏洞实施攻击实际发生的时间差，以及某种攻击方式的出现到某大规模蔓延之间的时间差统计得到。预警空间指标可以用预警信息发布时，被度量对象已经遭受该类型攻击或脆弱性被利用以实施攻击的空间范围来做出评价，为统计值。

2)安全防护能力

指使用技术和管理的手段来保证信息和信息系统的保密性、完整性、真实性、可用性、可控性和不可否认性、可靠性等。该指标可以从研究对象单位时间内(如一年)基于某一个(多个)安全属性(如：保密性)的安全事件的数量、事件起因分析、风险级别、造成的损失、潜在威胁估算等实施度量。同时，可运用渗透测试等手段进行实验分析。

3)隐患发现能力

隐患发现能力指数主要由检测技术的有效性(如漏报率和误报率)，检测制度的完备性和检测的实时性等指标合成。

4)反应处置能力

反应处置是对发生的安全事件、破坏行为和过程，能及时做出处理，限制潜在的损失和破坏。可从不同规模(可分为大、中、小三类)安全事件的反应时间、技术手段、管理措施、处理效果等方面进行考评。

5)系统恢复能力

系统恢复能力主要针对系统遭受不同规模的攻击和破坏后，能恢复到正常运行状态的度量，包括对系统灾备能力、容错能力、修复能力等的度量。

6)追踪反制能力

追踪反制能力主要由攻击源追踪能力、攻击路径追踪能力和取证能力等指标构成。

(3)信息安全费用

信息安全费用包括人力资源、时间资源和财务资源等内容。人力资源主要包括人员培训、专职人员等；时间资源包括信息系统的安全建设、安全运营和安全维护等所占用的时间因素；财务资源包括购置一切信息安全软、硬件产业和服务的财务支出。

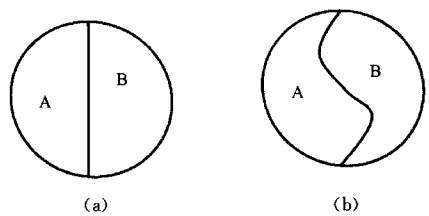
基于以上定义，特定信息系统的安全基线方程可表示为：

$$f_B=F(IA_B,CST_B,C_B) \tag{2}$$

设当前某信息系统 I 的安全保障状态为 P，且满足 $f_P \geqslant f_B$，我们则说当前系统 P 满足信息安全基线要求。否则，系统不满足信息安全基线要求。对于同一信息系统的两个不同安全策略 P 和 P'，如果 $IA_P=IA_{P'}$，$C_P=C_{P'}$，且 $CST_P<CST_{P'}$，则我们称信息安全策略 P 优于信息安全策略 P'。

4 信息系统安全度量方法

在第一部分我们就提到，信息安全度量具有复杂性和相对性。对于信息系统 A，我们很难说它目前的状态是安全的或不安全的。信息安全的概念不是“非此即彼”的概念(如图 4(a)所示)，而是在一定条件下相互转化的关系。信息系统的安全状态随着外部环境的变化和自身价值的变化进行着复杂的演化，因此，对信息系统“安全”的界定就带有很大的“模糊性”。在信息安全度量方法的选择上，本文引入“模糊综合度量法”，其度量过程如下：



(a) (b)

图 4 安全的相对性

(1)按照信息安全度量指标体系，建立度量因素集：

$$U=[u_1,u_2,\cdots,u_n]$$

这一步的目的是建立度量指标体系的层次分析模型，对被度量指标进行逐层分解，直到最基本指标为止，形成度量指标体系的层次结构。

(2)建立度量等级集

$$V=[v_1,v_2,\cdots,v_m]$$

这里，被度量指标对各评语等级的隶属度通过该模糊向量表示出来，体现了度量的模糊性。评语等级的个数 m 的取值范围通常是 $4\leqslant m\leqslant 9$。

(3)建立模糊关系矩阵

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ & \cdots & \cdots & \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix},(0\leqslant r_{ij}\leqslant 1) \tag{3}$$

其中，r_{ij} 为 U 中指标 u_i 对应 V 中等级 v_i 的隶属关系。

(4)确定指标的权重向量

权重反映了本层指标相对于上层指标的重要程度，可采用 AHP[6] 方法获得，权向量可表示为 $\boldsymbol{W}=(w_1,w_2,\cdots,w_n)$，$\boldsymbol{W}$ 是表示指标重要程度的模糊子集。

(5)综合度量

对指标集 U 上的模糊子集 $\boldsymbol{W}$，通过模糊关系 $\boldsymbol{R}$ 变换为评语集 $\boldsymbol{V}$ 上的模糊集 $\boldsymbol{B}$，称为综合度量的等级模糊子集，表示为

$$\boldsymbol{B}=\boldsymbol{W}\cdot\boldsymbol{R}=(b_1,b_2,\cdots,b_m)$$

“$\cdot$”为广义模糊合成算子，可根据实际情况取不同的度量模型，b_j 表示综合度量结果为等级 v_j 的隶属度，可按最大隶属度原则选择与最大的 b_j 所对应的等级 v_j，也可给每一个等级一个等级分值，再求其加权和，得出综合分值。

(6)度量结果向量的归一化处理

对每个度量指标的计算结果都是一个模糊向量，不能直接用于各度量指标间的排序比较，因此，需要对模糊度量结果向量 B 进行归一化处理：

$$b_j'=\frac{b_j}{\sum_{i=1}^{m} b_i} \tag{4}$$

(下转第 198 页)

(1)若 $ND \vdash P_i[XY] \overset{s}{\subseteq} P_j[WZ]$ 和 $ND \vdash P_j: W \xrightarrow{s} Z$ 成立，则 $ND \vdash_{Pi} : X \xrightarrow{s} Y$ 也成立。其中 $X=x_1,\cdots,x_m$，$W=w_1,\cdots,w_m$，$Y=y_1,\cdots,y_n$，$Z=z_1,\cdots,z_n$。

(2)若 $ND \vdash P_i[XY] \overset{s}{\subseteq} P_j[WU]$、$ND \vdash P_i[XZ] \overset{s}{\subseteq} P_j[WV]$、$ND \vdash_{Pj} : W \xrightarrow{s} U$ 成立，则 $ND \vdash P_i[XYZ] \overset{s}{\subseteq} P_j[WUV]$ 也成立。其中 $X=x_1,\cdots,x_m$，$W=w_1,\cdots,w_m$，$Y=y_1,\cdots,y_k$，$U=u_1,\cdots,u_k$，$Z=z_1,\cdots,z_n$，$V=v_1,\cdots,v_n$。

(3)设 $\sum=\{P_i[XY] \overset{s}{\subseteq} P_j[WU], P_i[XZ] \overset{s}{\subseteq} P_j[WU], P_j: W \xrightarrow{s} U\}$。若 $T_i \triangle P_i$，$T_j \triangle P_j$ 满足 $\sum$，$T_{i1} \subseteq T_i$，$T_{i1} \leftrightarrow P_i$，则 $val(N_{i1}(y_b)) \doteq val(N_{i1}(z_b))(b \in [1,n])$。其中 $X=x_1,\cdots,x_m$，$W=w_1,\cdots,w_m$，$Y=y_1,\cdots,y_n$，$U=u_1,\cdots,u_n$，$Z=z_1,\cdots,z_n$。

证明：(1)设 $T_i \triangle P_i$，$T_{i1} \subseteq T_i$，$T_{i1} \leftrightarrow P_i$，$T_{i2} \subseteq T_i$，$T_{i2} \leftrightarrow P_i$ 满足 $val(N_{i1}(x_a)) \div val(N_{i2}(x_a))(a \in [1,m])$。由 $ND \vdash_{Pi} [XY] \overset{s}{\subseteq} P_j[WZ]$，则存在 $T_j \triangle P_j$，$T_{j1} \subseteq T_j$，$T_{j1} \leftrightarrow P_j$，$T_{j2} \subseteq T_j$，$T_{j2} \leftrightarrow P_j$ 满足 $val(N_{j1}(w_a)) \doteq val(N_{i1}(x_a))$，$val(N_{j1}(z_b)) \doteq val(N_{i1}(y_b))$ 和 $val(N_{j2}(w_a)) \doteq val(N_{i2}(x_a))$，$val(N_{j2}(z_b)) \doteq val(N_{i2}(y_b))$ 成立$(b \in [1,n])$。由 $val(N_{i1}(x_a)) \div val(N_{i2}(x_a))$ 得 $val(N_{j2}(w_a)) \div val(N_{j1}(w_a))$，又由 $ND \vdash P_j: W \xrightarrow{s} Z$ 得 $val(N_{j2}(z_b)) \doteq val(N_{j1}(z_b))$，所以 $val(N_{i2}(y_b)) \doteq val(N_{i1}(y_b))$。即若 $T_{i1} \subseteq T_i$，$T_{i1} \leftrightarrow P_i$，$T_{i2} \subseteq T_i$，$T_{i2} \leftrightarrow P_i$ 满足 $val(N_{i1}(x_a)) \div val(N_{i2}(x_a))$，则 $val(N_{i1}(y_b)) \doteq val(N_{i2}(y_b))$，所以 $ND \vdash P_i: X \xrightarrow{s} Y$ 成立。

(2)设 $T_i, T_j \in ND$，$T_i \triangle P_i$，$T_j \triangle P_j$ 满足 $P_i[XY] \overset{s}{\subseteq} P_j[WU]$，$P_i[XZ] \overset{s}{\subseteq} P_j[WV]$，$P_j: W \xrightarrow{s} U$。设 $T_{i1} \subseteq T_i$，$T_{i1} \leftrightarrow P_i$，则有 $T_{j1} \subseteq T_j$，$T_{j1} \leftrightarrow P_j$，$T_{j2} \subseteq T_j$，$T_{j2} \leftrightarrow P_j$ 满足 $val(N_{j1}(w_a)) \doteq val(N_{i1}(x_a))$，$val(N_{j1}(u_b)) \doteq val(N_{i1}(y_b))$ 且 $val(N_{j2}(w_a)) \doteq val(N_{i1}(x_a))$，$val(N_{j2}(v_c)) \doteq val(N_{i1}(z_c))(a \in [1,m], b \in [1,k], c \in [1,n])$。所以 $val(N_{j1}(w_a)) \doteq val(N_{j2}(w_a))$，则 $val(N_{j1}(w_a)) \div val(N_{j2}(w_a))$，由 $P_j: W \xrightarrow{s} U$，则 $val(N_{j1}(u_b)) \doteq val(N_{j2}(u_b))$ 成立。又由 $val(N_{j1}(u_b)) \doteq val(N_{i1}(y_b))$，则 $val(N_{j2}(u_b)) \doteq val(N_{i1}(y_b))$，所以对于每个 $T_{i1} \subseteq T_i$，$T_{i1} \leftrightarrow P_i$，则存在 $T_{j2} \subseteq T_j$，$T_{j2} \leftrightarrow P_j$ 且满足 $val(N_{j2}(w_a u_b v_c)) \doteq val(N_{i1}(x_a y_b z_c))$，所以 $ND \vdash P_i[XYZ] \overset{s}{\subseteq} P_j[WUV]$ 成立。

(3) 设 $T_i, T_j \in ND$，$T_i \triangle P_i$，$T_j \triangle P_j$ 满足 $P_i[XY] \overset{s}{\subseteq} P_j[WU]$，$P_i[XZ] \overset{s}{\subseteq} P_j[WU]$，$P_j: W \xrightarrow{s} U$。设 $T_{i1} \subseteq T_i$，$T_{i1} \leftrightarrow P_i$，则存在 $T_{j1} \subseteq T_j$，$T_{j1} \leftrightarrow P_j$ 和 $T_{j2} \subseteq T_j$，$T_{j2} \leftrightarrow P_j$ 满足 $val(N_{j1}(w_a)) \doteq val(N_{i1}(x_a))$，$val(N_{j1}(u_b)) \doteq val(N_{i1}(y_b))$ 和 $val(N_{j2}(w_a)) \doteq val(N_{i1}(x_a))$，$val(N_{j2}(u_b)) \doteq val(N_{i1}(z_b))(a \in [1,m], b \in [1,n])$ 成立。所以 $val(N_{j1}(w_a)) \doteq val(N_{j2}(w_a))$，则 $val(N_{j1}(w_a)) \div val(N_{j2}(w_a))$，又由 $P_j: W \xrightarrow{s} U$，则 $val(N_{j1}(u_b)) \doteq val(N_{j2}(u_b))$ 成立，所以 $val(N_{i1}(y_b)) \doteq val(N_{i1}(z_b))$ 也成立。证毕。

结束语 本文研究了在不完全信息环境下的 XML 强闭包依赖理论。通过对 XML 强闭包依赖的研究，对 XML 文档中的不确定性数据进行了约束，为研究不完全信息环境下的 XML 数据库的外键奠定了基础。在以后的工作中，将进一步对不完全信息环境下 XML 函数依赖和闭包依赖的范式进行研究。

参 考 文 献

[1] Buneman P, Davidson S, Fan W, et al. Keys for xml. Computer Networks, 2002, 39(5): 473-487

[2] Buneman P, Fan W, Weinstein S. Path constraints on structured and semistructured data// Proc. ACM PODS Conference. 1998: 129-138

[3] Vincent M W, Liu Jixue. Functional Dependencies for XML, APWeb, 2003: 22-34

[4] Vincent M W, Liu Jixue. Multivalued Dependencies in XML, BNCOD, 2003: 4-18

[5] Fan W, Libkin L. On XML integrity constraints in the presence of DTDs. Journal of the ACM, 2002, 49(3): 368-406

[6] Fan W, Simeon J. Integrity constraints for xml. Journal of Computer and System Sciences, 2003, 66(1): 254-291

[7] Vincent M W, Schrefl M, Liu Jixue, et al. Generalized Inclusion Dependencies in XML// APWeb 2004, LNCS 3007: 224-33

[8] 郝忠孝. 空值环境下数据库导论. 北京：机械工业出版社，1996

[9] Levene M, Loizu G. Null Inclusion Dependencies in Relational Databases. Inf. Comput, 1997(136): 67-108

[10] Vincent M W, Liu Jixue, Liu Chengfei. Strong functional dependencies and their application to normal forms in XML. ACM Trans. Database Syst, 2004, 29(3): 445-462

(上接第 44 页)

得到归一化向量：

$$\boldsymbol{B}'=(b_1', b_2', \cdots, b_m') \quad (5)$$

结束语 度量是信息安全管理的一个重要环节。信息安全度量是收集安全证据的过程，它包括度量模型、度量指标、度量基线和度量方法等关键因素。本文系统分析了信息安全度量的概念、原理和方法，给出了一个基于基线的信息安全度量模型，并研究了信息安全模糊综合度量方法。信息安全度量是一个复杂的过程，它在今后信息安全保障体系建设中的地位和作用日益重要。我们下一步的工作将侧重于对信息安全度量的共性技术和工具的研究，以及在信息系统的实践。

参 考 文 献

[1] 吕欣. 我国信息安全现状和趋势. 国家信息中心：中国信息安全年鉴, 2007: 54-68

[2] Zhang K. A theory for system security // Computer Security Foundations Workshop, 1997. Proceedings. 1997: 148-155

[3] Maconachy W V, Schou C D, Ragsdale D, et al. A Model for Information Assurance: An Integrated Approach// Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. United States Military Academy, 2001: 306-310

[4] Lü Xin. Information Security Assurance Evaluation for Network Information Systems// CIS2006: Computational Intelligence and Security. LNAI, Vol 4456. Springer, 2007: 869-877

[5] Fowler K, Schmalzel J. Why do we care about measurement?. Instrumentation & Measurement Magzaine, IEEE, 2004, 7(1): 38-46

[6] 秦寿康，等. 综合评价原理. 北京：电子工业出版社，2003

[7] British Standards Institute. Code of practice for information security management, BS 7799, London, 1999

[8] ISO/IEC 13335-5: 2001. Information technology—Guidelines for the management of IT Security —Part5: Management guidance on network security, 2001

[9] ISO/IEC15408. Information Technology-Security Techniques-Evaluation Criteria for IT Security, 2005