信息系统安全度量与评估模型

闫 强,陈 钟,段云所,王立福
(北京大学 计算机科学技术系,北京 100871)

摘 要: 信息技术安全评估标准 GB17859 定义了信息系统安全评估的安全要素集,并以等级的形式表示信息系统的安全度量. 为区分各个安全要素在信息系统安全度量评估过程中表现出的不同特性,提出了组合独立性安全要素、组合互补性安全要素及组合关联性安全要素的概念,通过定义访问路径、规范路径及组件之间的相互关系,给出了信息系统安全度量的形式化评估模型及其实现.

关键词: 安全度量; 评估; 组合独立性安全要素; 组合互补性安全要素; 组合关联性安全要素; 访问路径
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2003) 09-1351-05

Information System Security Metrics and Evaluation Model

YAN Qiang, CHEN Zhong, DUAN Yun-suo, WANG Li-fu
(Dept. of Computer Science & Technology, Peking University, Beijing 100871, China)

Abstract: Information technology security evaluation criteria GB 17859 represents the security metrics of information systems as different ratings and defines the security elements set for the security metrics evaluation. The concepts of composition independent security element, composition complementary security element and composition correlated security element are introduced to discriminate between the various characters of the security elements presented in the process of security metrics assessment. The formal evaluation model for information system security metrics and its implementation are also introduced based on the definitions of access path, regular path and the relationship between components.

Key words: security metrics; evaluation; composition independent security element; composition complementary security element; composition correlated security element; access path

1 引言

2000 年 7 月,美国 NIST (National Institute of Standards and Technology) 和 CSSPAB (Computer System Security and Privacy Advisory Board) 联合举办了一个针对安全度量 (security metrics) 的讨论会. 会议指出,通用准则 (CC)[1] 虽然是指导安全评估的一个非常好的标准,但它并没有全面解决安全度量的问题,在这方面还有很多需要进一步研究的内容[2],如:

- 安全度量目前存在哪些不同的定义?
- 信息系统的安全度量是什么?
- 针对特定安全威胁的安全度量是什么?
- 定性的安全度量是什么?
- 大规模网络中的实时安全度量是什么?
- 如何解释安全度量、保证等级、风险管理等内容,从而使人们对安全保护能有一个正确的理解?

2001 年 5 月,ACSA (Applied Computer Security Associates) 与 MITRE Corporation 联合组织了对安全度量的讨论,并对其作出如下定义[3]:

信息系统安全度量是通过一些评估过程从一个偏序集中选择的一个值,它表示了信息系统的信息安全相关的质量,它提供或用于产生一种关于信任程度的描述、预言或比较.

一般来说,信息安全相关的质量涉及信息的机密性 (confidentiality)、完整性 (integrity) 和可用性 (availability) 等三方面. 但是从网络和信息系统的应用环境来看,这些内容并不是一成不变的,例如在军事组织和商业组织中,信息系统的信息安全相关的质量所涉及的内容显然是不一样的[4]. 从涉及的范围看,信息系统安全度量包括技术性安全度量、组织性安全度量、操作性安全度量以及物理性安全度量等.

本文将围绕信息系统的技术性安全度量,介绍安全要素集中的组合独立性安全要素、组合互补性安全要素、组合关联性安全要素,并在此基础上对信息系统安全度量评估模型进行探讨.

2 信息系统安全要素集

计算机信息系统是由计算机及其相关的和配套的设备、设施 (含网络) 构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统[5].

收稿日期:2003-01-16;修回日期:2003-04-10
基金项目:国家自然科学基金 (No. 69973004, 60003015)

本文以安全要素表示系统信息安全相关的质量所涉及的内容,并定义安全要素集 E:

$$E = \{ e_1, e_2, \cdots, e_n \}$$

各种安全评估标准为信息系统安全评估提供了一个确定安全要素集的框架,并在此基础上以等级的形式表示安全度量,安全度量之间存在偏序关系"$\geq$",这种偏序关系表示"安全性大于等于",安全度量的集合构成一个偏序集. 若以 S 表示信息系统,以 $f_e(S)$ 表示在安全要素 e 上信息系统 S 的安全性到安全度量偏序集上的映射,以 $f_E(S)$ 表示信息系统 S 整体安全性到安全度量偏序集的映射,则对两个信息系统 S, S',若 $\forall e \in E, f_e(S) \geq f_e(S')$,则有 $f_E(S) \geq f_E(S')$.

例如 TCSEC[6]在安全策略方面定义的安全要素包括自主访问控制(DAC)、客体重用(Object Reuse)、标记(Labels)及强制访问控制(MAC)等,并将安全度量定义为七个等级,从 D 级到 A 级,每个安全要素的要求逐级增强,系统的安全性也逐级增强.

$$E_{TCSEC} = \{ DAC, Object\ Reuse, Labels, MAC \}$$

通用准则 CC 通过定义安全功能类和安全保证类,提供了一个确定安全要素集的框架,并将安全度量定义为 7 个评估保证级别. 如 CC 在安全审计类(FAU)中定义了安全审计自动响应(FAU_ARP)、安全审计数据产生(AU_GEN)、安全审计分析(FAU_SAA)、安全审计查阅(FAU_SAR)、安全审计事件选择(FAU_SEL)、安全审计事件存储(FAU_STG)等族. 这些族构成了安全审计类上的安全要素集.

$$E_{FAU} = \{ FAU\_ARP, FAU\_GEN, FAU\_SAA, FAU\_SAR, FAU\_SEL, FAU\_STG \}$$

我国《计算机信息系统安全保护等级划分准则》(GB 17859)中定义了 10 个安全要素:自主访问控制、身份鉴别、数据完整性、客体重用、审计、标记、强制访问控制、隐蔽信道分析、可信路径及可信恢复等,并将安全度量定义为五个等级,从第一级到第五级,每个安全要素的要求逐级增强,系统的安全性也逐级增强.

安全评估准则同时还规定了信息系统整体安全度量与其在各个安全要素上的安全度量之间的关系,如 CC 中给出的评估保证级别和保证组件之间的交叉索引关系. 因此只要得到了信息系统在每个安全要素上的安全度量,就可以依据评估准则得到系统整体的安全度量.

不失一般性,本文将在安全要素集 E 上讨论信息系统安全度量的评估模型.

3 信息系统安全度量评估模型

本文提出的信息系统安全度量评估模型建立在以下假设基础上:

假设 1 攻击者能力最大化假设,即攻击者对系统存在的脆弱性有充分的了解,并具有利用这些脆弱性进行攻击的能力.

假设 2 攻击者能够选择系统中最薄弱的环节进行攻击.

假设 3 潜在的攻击可能来自系统外部,也可能来自系统内部.

假设 4 组件安全度量已知.

一个信息系统可以和其他系统/组件组合成更大的信息系统,在本文中,当指整体中的一个部分时以组件表示,当指整体时以系统表示. 当组件的安全度量已知时,系统安全评估的重点是组件组合后系统整体的信息安全相关的质量. 组件间的组合在系统中表现为访问路径.

定义 1 访问路径 p:在信息系统中,响应一种用户请求(如信息采集、加工、存储、传输、检索)所涉及到的所有软件、硬件构成一条访问路径,简称为路径,记为 p,系统中所有访问路径的集合记为 p.

系统评估过程将分析各个安全要素在每条访问路径中的实现情况,在此基础上得到系统的安全度量.

以 C 表示组件的集合, $C = \{ c_1, c_2, \cdots, c_n \}$. 以 $f_e(c)$ 表示在安全要素 e 上产品 c 本身的安全性到安全度量偏序集上的映射,以 $f_e(p)$ 表示在安全要素 e 上访问路径 p 的安全性到安全度量偏序集上的映射,其中 $e \in E$.

当系统 S 由组件 $c_1, c_2, \cdots, c_n$ 组合而成时,记为 $S = \cup(c_1, c_2, \cdots, c_n) = \bigcup_{i=1}^{n} c_i = \cup C$

定义 2 系统、访问路径、组件之间的包含关系 $\triangleright$

(1)对 $p \in P, p \triangleright S$,表示系统 S 包含访问路径 p,或者说 p 属于 S;

(2)对 $p \in P, c \in C, c \triangleright p$ 表示访问路径 p 包含组件 c,或者说 c 属于 p.

若 $c \triangleright p$,则 c 在访问路径 p 中的安全性到安全度量偏序集上的映射记为 $f_e^p(c)$.

组件度量是在组件评估假设环境下通过评估过程得到的,当集成到一个系统中时,组件的运行环境与其评估时的假设环境可能不一致. 组件评估环境是静态的,而系统评估环境是动态的,在系统运行时,每条访问路径中的各个组件之间存在交互. 评估环境的改变导致 $f_e^p(c)$ 不一定等于 $f_e(c)$.

定义 3 组合独立性安全要素

对 $e \in E$,如果有:

(1)对 $\forall S, p, c, p \in P$ 且 $p \triangleright S, c \in C$ 且 $c \triangleright p$,有 $f_e^p(c) = f_e(c)$;

(2)对系统 S 和 S',设其所包含的组件和访问路径集合分别为 C, P 与 C', P',对 $\forall c, c', p, p', c \in C, c' \in C', p \in P, p' \in P'$,且 $c \triangleright p, c' \triangleright p'$,若 $f_e^p(c) = f_e^{p'}(c')$,则有 $f_e(S) = f_e(S')$.

则称安全要素 e 为组合独立性安全要素,组合独立性安全要素的集合记为 E.

组合独立性安全要素的定义中,条件 1 表示在安全要素 e 上,任意一个系统中的任意一个组件在其所属的每条访问路径中的安全度量等于该组件本身的安全度量,条件 2 表示在安全要素 e 上,系统的安全度量只和系统中组件在其所属的每条访问路径中的安全度量本身有关. 如果两个系统中的所有组件在其所属的每条访问路径中的安全度量相同,则这两个系统的安全度量也相同.

组合独立性安全要素的一个例子如 CC 中的"剩余信息保护(*FDP_RIP*)",*FDP_RIP* 要求评估对象安全功能(TSF)应确保在分配给客体的资源或在客体释放的资源中没有可用剩余信息.由于不同组件对客体资源的分配与回收是独立进行的,所以对 *FDP_RIP* 而言,组件在系统中的安全度量等于该组件本身的安全度量,同时,系统整体在 *FDP_RIP* 上的安全度量也只取决于组件在系统中的度量本身.所以 *FDP_RIP* 属于组合独立性安全要素.

定义 4　组合互补性安全要素

对 $e \in E$,若 $\exists S, p, c, p \in P$ 且 $p \triangleright S, c \in C$ 且 $c \triangleright p$,使得 $f_e^p(c) \neq f_e(c)$,则称安全要素 e 为组合互补性安全要素.组合互补性安全要素的集合记为 $\overrightarrow{E}$.

组合互补性安全要素的一个例子如 CC 中的"存储数据完整性(*FDP_SDI*)",*FDP_SDI* 提供了对 TSF 控制范围内存储的用户数据的保护要求.由于完整性错误可能会影响存储在内存或其他存储设备中的数据,而对那些不直接控制内存和其他存储设备的组件,其在系统中的安全度量必然受其他直接控制内存和其他存储设备的组件的影响,也即前者的安全度量在其集成到系统中时将发生改变.因此,*FDP_SDI* 属于组合互补性安全要素.

定义 5　组合关联性安全要素

对 $e \in E$,若 $\exists S, S'$,其所包含的组件和访问路径集合分别为 C, P 与 C', P',对 $\forall c, c', p, p', c \in C, c' \in C', p \in P, p' \in P'$,且 $c \triangleright p, c' \triangleright p'$,当 $f_e^p(c) = f_e^{p'}(c')$ 时,有 $f_e(S) \neq f_e(S')$,则称安全要素 e 为组合关联性安全要素.组合关联性安全要素的集合记为 $\overleftrightarrow{E}$.

组合关联性安全要素的一个例子如 CC 中的"安全审计数据产生(*FAU_GEN*)",*FAU_GEN* 定义了对 TSF 控制下的安全相关事件的审计记录要求.由于各个组件记录的只是组件 TSF 控制下的安全相关事件的信息,因此为在系统范围内形成安全相关事件的完整信息,组件的审计记录必须通过某种标识关联起来.这种关联要求是系统 TSF 附加于组件安全审计功能之上的,因此,信息系统在安全审计上的度量不仅仅取决于组件本身的安全度量,还取决于对这种附加的关联要求的度量.所以 *FAU_GEN* 属于组合关联性安全要素.

组合互补性安全要素不满足组合独立性安全要素定义的条件 1.组合关联性安全要素不满足组合独立性安全要素定义的条件 2.

显然,E、$\overrightarrow{E}$、$\overleftrightarrow{E}$ 及 $\not{E}$ 之间满足以下关系:

$$\not{E} \subseteq E, \overrightarrow{E} \subseteq E, \overleftrightarrow{E} \subseteq E,$$

$$\not{E} \cap \overrightarrow{E} = \varnothing, \not{E} \cap \overleftrightarrow{E} = \varnothing, \overrightarrow{E} \cap \overleftrightarrow{E} \neq \varnothing,$$

$$\not{E} \cup \overrightarrow{E} \cup \overleftrightarrow{E} = E$$

定义 6　组件间的依赖关系

对 $e \in \overrightarrow{E}, c_1, c_2 \in C, p \in P$ 且 $c_1, c_2 \triangleright p$,如果 c_1 在与 c_2 的交互过程中,c_1 对安全要素 e 的实现受 c_2 的约束,则称 c_1 在安全要素 e 上依赖于 c_2,记为 $c_1 \xrightarrow{e} c_2$.

组件间依赖关系具有以下性质:

对 $e \in \overrightarrow{E}, a, b, c \in C, p \in P, a, b, c \triangleright p$,

(1)非对称性:若 $a \xrightarrow{e} b$,则 $\neg(b \xrightarrow{e} a)$;

(2)传递性:若 $a \xrightarrow{e} b \wedge b \xrightarrow{e} c$,则 $a \xrightarrow{e} c$;

(3)若 $a \xrightarrow{e} b$,则 $f_e^p(a) = f_e^p(b)$;

(4)若 $\neg(\exists d \in C, d \triangleright p \wedge a \xrightarrow{e} d)$,则 $f_e^p(a) = f_e(a)$.

下面分析在一条路径中以下几种依赖关系是否合理:

图 1 中组件 a, b, c, d, e 组成一条路径,以实线连接表示,虚线表示组件之间在安全要素 e 上的依赖关系.对路径 (a),$b \xrightarrow{e} c, c \xrightarrow{e} d$,合理,但存在冗余,根据依赖关系的传递性,可知 $b \xrightarrow{e} d$,路径 (a) 可以转化为路径 (d).对路径 (b),$b \xrightarrow{e} c, c \xrightarrow{e} d$,根据依赖关系的传递性,可知 $b \xrightarrow{e} d$,又 $d \xrightarrow{e} b$,与依赖关系的非对称性矛盾,所以路径 (b) 所示情况不合理.对路径 (c),$b \xrightarrow{e} c, b \xrightarrow{e} d$,合理,但存在冗余,$f_e^p(b) = \max(f_e(c), f_e(d))$.路径 (d) 合理.

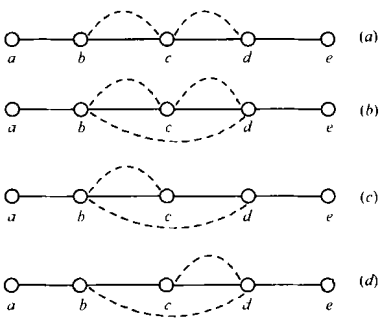

图 1　路径中组件间的依赖关系

通过消除路径 p 中的冗余依赖关系,p 可以转化为规范路径 p^*.

定义 7　规范路径 p^*

$\forall c_i \triangleright p, e \in \overrightarrow{E}$,如果有:

$$\exists c_j \triangleright p, c_i \xrightarrow{e} c_j \Rightarrow \neg(\exists c_k \triangleright p, c_j \neq c_k \wedge c_i \xrightarrow{e} c_k) \wedge \neg(\exists c_l \triangleright p, c_l \xrightarrow{e} c_i)$$

则称路径 p 为规范路径,记为 p^*,规范路径的集合记为 p^*.

定义 8　组件间的关联关系

$\forall c_i \triangleright p, e \in \overleftrightarrow{E}$,如果 c_i 在路径 p 中遵从信息系统关于 e 的统一安全策略,则称路径 p 中的组件满足 e 上的关联关系.

若路径 p 中所包含的组件集合为 $C = \{c_1, c_2, \cdots, c_n\}$,则对安全要素 e,以 $f_e^p(\overleftrightarrow{C})$ 或 $f_e^p\left(\overleftrightarrow{(c_1, c_2, \cdots, c_n)}\right)$ 表示 p 中组件间关联关系的安全性到安全度量偏序集上的映射.

规则 1　访问路径安全度量在安全要素集 E 上的评估规则:

对 $C = \{c_1, c_2, \cdots, c_n\}, p^* \in P^*, p^* \triangleright S, c_1, c_2, \cdots, c_n \triangleright p^*$,有:

(1) $\forall e \in \not{E}, f_e(p^*) = \min(f_e(c_1), f_e(c_2), \cdots, f_e(c_n))$;

(2) $\forall e \in \overrightarrow{E} \wedge e \notin \overleftrightarrow{E}, f_e(p^*) = \min(f_e(c_1^*), f_e(c_2^*), \cdots, f_e(c_k^*))$,

其中,对 $\forall i \in \{1, 2, \cdots, k\}, c_i^* \in C$,

有 $\neg(\exists c_j \in C, c_i^* \xrightarrow{e} c_j)$;

(3) $\forall e \in \overleftrightarrow{E} \wedge e \notin \overrightarrow{E}$, $f_e(p^*) = \min(f_e(c_1), f_e(c_2), \cdots, f_e(c_n), f_e^{p^*}(\overleftarrow{c_1, c_2, \cdots, c_n}))$;

(4) $\forall e \in \overrightarrow{E} \wedge e \in \overleftrightarrow{E}$, $f_e(p^*) = \min(f_e(c_1^*), f_e(c_2^*), \cdots, f_e(c_k^*), f_e^{p^*}(\overrightarrow{c_1^*, c_2^*, \cdots, c_k^*}))$;

其中,对 $\forall i \in \{1,2,\cdots,k\}$, $c_i^* \in C$,

有 $\neg(\exists c_j \in C, c_i^* \xrightarrow{e} c_j)$.

证明:

(1) 已知 $e \in E$,由 E 定义的条件 2 知,在安全要素 e 上,路径 p^* 的安全度量只取决于其所包含的组件在该路径中的安全度量,e 在各组件间的实现是独立的,组件组合后,组件之间不存在 e 上的关联关系,又由假设 2,得:

$f_e(p^*) = \min(f_e^{p^*}(c_1), f_e^{p^*}(c_2), \cdots, f_e^{p^*}(c_n))$

由 E 定义的条件 1 得:

$\forall c_i \triangleright p^*, f_e^{p^*}(c_i) = f_e(c_i)$

所以, $f_e(p^*) = \min(f_e(c_1), f_e(c_2), \cdots, f_e(c_n))$;

(2) 由 $e \notin \overleftrightarrow{E}$ 知,在安全要素 e 上,路径 p^* 的安全度量只取决于其所包含的组件在该路径中的安全度量,e 在各组件间的实现是独立的,组件组合后,组件之间不存在 e 上的关联关系,再由假设 2 得:

$f_e(p^*) = \min(f_e^{p^*}(c_1), f_e^{p^*}(c_2), \cdots, f_e^{p^*}(c_n))$

又 $e \in \overrightarrow{E}$,所以对 $c_x, c_y \in C$,如果 $c_x \xrightarrow{e} c_y$,由组件间依赖关系的性质 3,可得:

$f_e^{p^*}(c_x) = f_e^{p^*}(c_y)$

如果 $\exists c_z \in C$,使得 $c_y \xrightarrow{e} c_z$,则与规范路径的定义矛盾,所以 $\neg(\exists c_z \in C, c_y \xrightarrow{e} c_z)$.

由组件间依赖关系的性质 4,得:

$f_e^{p^*}(c_y) = f_e(c_y)$

所以, $f_e(p^*) = \min(f_e(c_1^*), f_e(c_2^*), \cdots, f_e(^*c_k))$

其中,对 $\forall i \in \{1,2,\cdots,k\}$, $c_i^* \in C$,有 $\neg(\exists c_j \in C, c_i^* \xrightarrow{e} c_j)$;

(3) 由 $e \notin \overrightarrow{E}$ 知,组件在其所属路径中的安全度量等于该组件本身的安全度量,即:

$\forall c_i \triangleright p^*, f_e^{p^*}(c_i) = f_e(c_i)$,

又由 $e \in \overleftrightarrow{E}$ 知 p 的安全度量除取决于各个组件本身外,还需考虑组件之间关联关系的度量,再由假设 2 得:

$f_e(p^*) = \min(f_e^{p^*}(c_1), f_e^{p^*}(c_2), \cdots, f_e^{p^*}(c_n), f_e^{p^*}(\overleftarrow{c_1, c_2, \cdots, c_n}))$

$= \min(f_e(c_1), f_e(c_2), \cdots, f_e(c_n), f_e^{p^*}(\overleftarrow{c_1, c_2, \cdots, c_n}))$;

(4) 由 $e \in \overleftrightarrow{E}$ 知 p 的安全度量除取决于各个组件本身外,还需考虑组件之间关联关系的度量,再由假设 2 得:

$f_e(p^*) = \min(f_e^{p^*}(c_1), f_e^{p^*}(c_2), \cdots, f_e^{p^*}(c_n), f_e^{p^*}(\overleftarrow{c_1, c_2, \cdots, c_n}))$

又 $e \in \overrightarrow{E}$,所以对 $c_x, c_y \in C$,如果 $c_x \xrightarrow{e} c_y$,由组件间依赖关系的性质 3,可得:

$f_e^{p^*}(c_x) = f_e^{p^*}(c_y)$

如果 $\exists c_z \in C$,使得 $c_y \xrightarrow{e} c_z$,则与规范路径的定义矛盾,所以 $(\exists c_z \in C, c_y \xrightarrow{e} c_z)$.

$\neg$ 由组件间依赖关系的性质 4,得:

$f_e^{p^*}(c_y) = f_e(c_y)$

所以, $\forall e \in \overrightarrow{E} \wedge e \in \overleftrightarrow{E}$, $f_e(p^*) = \min(f_e(c_1^*), f_e(c_2^*), \cdots, f_e(c_k^*), f_e^{p^*}(\overrightarrow{c_1^*, c_2^*, \cdots, c_k^*}))$,

其中,对 $\forall i \in \{1,2,\cdots,k\}$, $c_i^* \in C$,有 $\neg(\exists c_j \in C, c_i^* \xrightarrow{e} c_j)$.

证毕.

规则 2 信息系统安全度量在安全要素集 E 上的评估规则:

对系统 S,安全要素 $e \in E$,若 S 包含的规范路径集为 $P^* = (p_1^*, p_2^*, \cdots, p_m^*)$,则 $f_e(S) = \min(f_e(p_1^*), f_e(p_2^*), \cdots, f_e(p_m^*))$.

证明:(略).

根据安全评估准则规定的信息系统安全度量与其在各个安全要素上的安全度量之间的关系,可由 $f_e(S)$ 得出整个信息系统的安全度量.

4 实现

作者在承担国家计委高科技产业项目过程中提出文中介绍的有关概念和模型,并将该思想运用到了信息系统安全保护等级评估工具研制过程中. 这套评估工具以 GB 17859 为依据,采用自动拓扑分析及问卷调查相结合的方式,确保检测覆盖系统中所有访问路径;同时采用设计分析、功能验证及穿透测试相结合的方法,对系统访问路径中组件间的依赖关系和关联关系进行检测,结合组件评估数据,得出被测系统在组合独立性安全要素、组合互补性安全要素以及组合关联性安全要素上所能够达到的安全等级. 在此基础上,结合系统组织性、操作性以及物理性安全度量,得出被测系统达到的安全保护等级.

5 结束语

本文介绍了信息系统安全度量以及安全要素集,提出了组合独立性安全要素、组合互补性安全要素、组合关联性安全要素及规范路径的概念,并建立了一种信息系统安全度量评估模型.

本文没有涉及具体的检测技术,在作者所承担的信息系统安全保护等级评估工作中,我们采用了问卷调查、设计分析、功能验证及穿透测试相结合的方法,我们将在今后的工作中进一步验证该方法的有效性. 另外,关于特定威胁的度量、安全度量与保证等级、风险管理的关系等问题都值得进一步研究.

表 1 是 WISSSR 对美国目前正在开展的信息安全度量及

评估项目的一个数量统计.

从这个统计数据可以看出,目前关于信息系统的安全度量成为研究的重点,对安全的定度量量还存在一定困难,定性及定性与定量相结合的方式仍是目前的主要度量形式.

表 1　信息安全度量及评估项目统计数据

度量形式	评估对象					合计
	系统	产品	组织计划	组织过程	环境因素	
定　性	5	2	6	1	1	15
定　量	4	2	2	1	0	9
定性+定量	7	1	4	3	1	16
合　计	16	5	12	5	2	40

参考文献:

[1] ISO/IEC 15408, Information Technology-Security Techniques-Evaluation Criteria For IT Security[S].

[2] Fran Nielsen. Approaches to Security Metrics[R]. Gaithersburg: NIST, 2000.

[3] ACSA and MITRE Corp. Information system security attribution quantification or ordering[A]. 2001 1ST Workshop on Information System Security Scoring and Ranking Proceedings[C]. Virginia: ACSA and MITRE Corp, 2001. 1-70.

[4] Bennet S Yee. Security metrology and the monty hall problem[EB/OL]. http://www.cs.ucsd.edu/~bsy/pub/metrology.pdf, 2001-04-02.

[5] GB 17859-1999, 计算机信息系统安全保护等级划分准则[S].

[6] DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria[S].

作者简介:

闫　强　男,1972 年 7 月生于山西临汾,现为北京大学计算机科学技术系博士研究生,主要从事网络与信息系统安全评估、安全风险管理及安全策略等方面的研究工作.

陈　钟　男,1963 年生于江苏徐州,博士生导师,研究领域包括网络与信息安全、嵌入式系统技术及软件工程等方向.