PCCSCCF

信息与网络安全研究新进展

全国计算机安全学术交流会论文集

第二十二卷

主办单位

中国计算机学会计算机安全专业委员会

中国电子学会计算机工程与应用学会计算机安全保密学组

中国科学技术大学出版社

PCCSCCF

信息与网络安全研究新进展

全国计算机安全学术交流会论文集

第二十二卷

主办单位

中国计算机学会计算机安全专业委员会

中国电子学会计算机工程与应用学会计算机安全保密学组

中国科学技术大学出版社

·合肥·

图书在版编目（CIP）数据

信息与网络安全研究新进展：全国计算机安全学术交流会论文集.第22卷/中国计算机学会计算机安全专业委员会，中国电子学会计算机工程与应用学会计算机安全保密学组编. —合肥：中国科学技术大学出版社，2007.7

ISBN 978-7-312-02159-6

Ⅰ.信… Ⅱ. ①中… ②中… Ⅲ. 电子计算机—安全技术—学术会议—文集 Ⅳ.TP309-53

中国版本图书馆CIP数据核字（2007）第101038号

中国科学技术大学出版社出版发行

（安徽省合肥市金寨路96号，230026）

中国科学技术大学印刷厂印刷

全国新华书店经销

开本：889×1194/16 印张：22.75 字数：649千

2007年7月第1版 2007年7月第1次印刷

印数：1—1000册

定价：150.00元

前　言

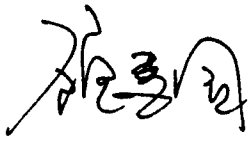
第二十二次全国计算机安全学术交流会，在美丽的张家界市举行。我们将征集到的全体同仁一年来辛勤工作的结晶——学术论文，细心筛选了 83 篇论文，汇编成《全国计算机安全学术交流会论文集（第二十二卷）》呈现给大家。《全国计算机安全学术交流会论文集（第二十二卷）》由中国科技大学出版社出版发行。

2007 年我们国家的信息安全工作，将以科学发展观为指导，认真贯彻加强信息安全保障工作的意见和国家信息安全“十一五”规划，着眼于提高信息网络保障水平和信息安全防护的能力，全面推进信息系统安全等级保护工作，全面加强互联网安全管理。我们希望《全国计算机安全学术交流会论文集（第二十二卷）》能对各位同仁有所帮助。

我们感谢第二十二次全国计算机安全学术交流会的承办方——中国人民解放军空军电子技术研究所对会议和论文集所做的努力！

期望会议圆满成功！

中国计算机学会计算机安全专业委员会主任



二〇〇七年六月

目　录

基于多要素融合的风险评估模型的设计

海 然 谢小权
中国航天科工集团706所

摘 要：本文在分析现有风险评估模型存在不足的基础上，设计了基于多要素融合的风险评估模型MFDM。MFDM模型考虑了当前风险评估模型中没有考虑资产间关联关系及脆弱性间关联关系的不足，通过将影响风险的要素进行关联、分析、计算，最后得出风险评估结论。

关键词：风险评估 模型 信息安全

一、概述

信息安全风险评估是当前信息安全领域研究的热点之一，目前国家也在大力倡导开展信息安全风险评估工作。信息安全风险评估技术可以使人们了解信息系统目前与未来的安全状况，明确信息系统存在的风险，以便更好的采取相应的安全措施，将风险降低到可接受水平。

目前国内外对信息安全风险评估研究主要包括信息安全风险评估相关标准的制定、自动化风险评估工具的研制、风险评估模型的研究等。其中，风险评估模型在风险评估过程中发挥着重要的作用：风险评估需要依靠风险评估模型完成相应的评估功能、确保风险评估结果的准确性、全面性、可信性。虽然目前对风险评估模型的研究已取得了一定的成果，但现有的风险评估模型对影响风险的主要因素之间的关系进行抽象时基本都采取了资产面临威胁、威胁利用脆弱性的要素关联关系，忽略了资产之间的相互影响关系、脆弱性之间的相互影响关系，而这种影响关系又是衡量系统安全性的重要指标，直接影响了系统安全状态。

本文针对现有风险评估模型存在的上述问题，设计基于多要素融合的风险评估模型，解决影响信息系统安全的关键因素之间存在的相互影响关系。本文首先分析总结了现有风险评估模型存在的不足，然后设计了多要素融合模型MFDM，其中重点对模型的结构进行了详细设计，最后对设计的MFDM模型进行总结。

二、信息安全风险评估模型现状

风险评估模型对信息系统进行风险评估具有指导作用，对风险评估模型的研究一直是信息安全风险评估技术的研究热点之一。根据不同的研究目的，国外建立了各种风险评估模型，这些模型大致可以分为风险概念模型、风险评估过程模型、风险计算模型[1]。

风险概念模型主要描述了风险评估的相关要素，以及各个要素之间的相互关系。其中应用比较广泛的风险概念模型包括ISO 13355中提出的风险要素相互作用模型、BS 7799中提出的风险要素模型等。风险评估过程模型描述了风险评估操作的总体流程，可用来指导风险评估的进行。其中比较典型的风险过程模型包括OCTAVE模型等。风险计算模型主要描述了风险的计算方法。其中比较典型的风险计算模型包括美国标准局发布的《自动的数据处理风险分析指南》中提出的使用年损失期望（ALE）计算风险。

上述模型比较具有代表性，目前风险评估模型大多是在这些模型的基础上，根据评估需求，对上述模型进行细化或裁减，满足不同的评估要求。但是这些

模型也存在一定的不足，主要有以下3个方面：

（1）没有考虑资产之间的关系对风险的影响

目前利用风险评估模型对信息系统的资产进行风险评估，只是针对单个资产进行分析，没有考虑资产之间的相互关系。信息系统中单个资产的安全不足以保证资产交互后整个信息系统是安全的，一个资产面临风险，可能导致与其存在关联的资产面临风险，进而导致整个网络面临的风险增加[2]。

（2）没有建立脆弱性之间的关联关系

资产存在的脆弱性之间也存在一定的相互关系，从攻击者的角度看，网络攻击与脆弱性的关系，应当认为攻击者挖掘脆弱性不是孤立的，而是组合各脆弱性进行挖掘[3]。一个脆弱性可以被攻击者利用进行攻击，也可以作为另一个脆弱性被利用的条件，增加另一个脆弱性被利用的可能性，从而导致资产面临的风险增加。

（3）缺少对信息系统提供的应用服务的安全性的分析

信息系统中的资产是信息系统安全性关注的一个方面，除此之外，信息系统的安全性还体现在所提供的应用服务的安全性等方面。但是现有的风险评估模型中没有提出衡量应用服务安全的要素。

通过上面的分析可以看出，现实世界中影响信息系统安全性各个要素之间的关系是错综复杂的、互相影响的，只有准确反映信息系统安全要素关系的评估模型，才能保证评估结果的准确性。本文主要针对问题（1）、（2），设计风险评估模型，提高风险计算的精确度。下文将对模型进行详细描述。

三、多要素融合模型的设计

本章将设计风险评估模型——多要素融合模型（Multi-factors Dissolve Model，简写为：MFDM）。首先设计MFDM模型的总体结构，然后对MFDM模型的风险评估要素、风险评估要素关联关系、模型的处理过程进行详细设计，最后确定模型的应用过程。

1. MFDM模型的设计

（1）模型的总体结构

MFDM模型包括风险评估要素、风险评估要素关联关系、模型的处理过程三个部分。MFDM模型描述为：

MFDM模型=$\{F,C,D\}$

F表示MFDM模型的风险评估要素，指在风险评估过程中必须考虑的风险的组成部分、影响因素和相关因素，确定了评估模型所能实现的评估功能。

C表示MFDM模型的风险评估要素关联关系，指各个要素在风险评估过程中相互之间的因果关系。

D表示MFDM模型的处理过程，指模型通过分析、计算，得出资产的风险值。

（2）风险评估要素的设计

基于风险概念模型中提出的影响风险的主要因素，MFDM模型采用其中的<资产、威胁、脆弱性>作为模型的风险评估要素。

风险评估要素由如下集合表示：$\{A,T,V\}$。

A表示被测信息系统的资产集合，$A=\{a_i \mid value\}$，资产a_i由$value$描述，$value$表示a_i的价值。

T表示被测信息系统面临的威胁集合，$T=\{t_i \mid fren\}$，威胁t_i由$fren$描述，$fren$表示t_i的发生频率。

V表示被测信息系统资产存在的脆弱性集合，$V=\{v_i \mid serious, diff\}$，脆弱性$v_i$由$serious, diff$两个属性描述，$serious$表示$v_i$的严重程度，$diff$表示$v_i$被利用的难易程度。

（3）风险评估要素关联关系的设计

MFDM模型采用风险概念模型中提出的资产、威胁、脆弱性间的主要关联关系：资产面临威胁，威胁利用脆弱性。除了以上关联关系，MFDM模型还将资产之间的关联关系和脆弱性之间的关联关系作为模型的风险评估要素关联关系。

1）资产-威胁-脆弱性之间的关联关系

●资产面临威胁

资产面临威胁，表示为：$C_1=AT\subseteq A\times T$，其中$AT(a_i,t_j)$表示资产$a_i$面临威胁$t_j$。

一个资产通常会面临多个威胁，表示为：$a\rightarrow\{t_1,t_2,\cdots,t_j\}$，其中$\{t_1,t_2,\cdots,t_j\}$表示资产$a$面临的威胁集合。一个威胁可能会影响多个资产，表示为：$t\rightarrow\{a_1,a_2,\cdots,a_i\}$，其中$\{a_1,a_2,\cdots,a_i\}$表示威胁

t 所影响的资产的集合。

●威胁利用脆弱性

威胁利用脆弱性，表示为：$C_2 = AT \subseteq A \times T$，其中 TV（t_i, v_i,）表示威胁 t_i 可以利用脆弱性 V_i。

一个威胁可利用多个脆弱性，表示为：$t \to \{v_1, v_2, \cdots, v_i\}$，其中 $\{v_1, v_2, \cdots, v_i\}$ 表示威胁 t 可利用的脆弱性集合。一个脆弱性可被多个威胁利用，表示为：$v \to \{t_1, t_2, \cdots, t_j\}$，其中 $\{t_1, t_2, \cdots, t_j\}$ 表示可利用同一个脆弱性 v 的威胁集合。

2）资产间安全依赖关系

定义 1：资产间安全依赖关系 ASDR（Asset Security Dependency Relation）

被测信息系统中的资产 A 和资产 B，如果资产 A 上的应用程序或提供的服务面临风险，从而导致与其存在访问关系的资产 B 面临风险，则称资产 A 和资产 B 之间存在安全依赖关系，记为：$ASDR_{AB}$，称资产 A 为关联资产，资产 B 为被关联资产。

资产间安全依赖关系表示为：$C_3 = AA \subseteq A \times A$，其中 $AA(a_m, a_n)$ 表示资产 a_m 与资产 a_n 之间存在的安全依赖关系。

一个资产可能会和多个资产存在安全依赖关系，表示为：$a \to \{a_1, a_2, \cdots, a_k\}$，其中 $\{a_1, a_2, \cdots, a_k\}$ 表示和资产 a 存在安全依赖关系的资产集合。

MFDM 模型中资产间的安全依赖关系由一个 5 元组描述：

$$(A, s, B, u, P)$$

其中：s,u 分别表示资产 A 和资产 B 提供的应用程序或服务，P 为资产 A 和资产 B 之间存在安全依赖关系的概率，$P \in (0,1)$。

3）脆弱性间相互影响关系

定义 2：脆弱性间相互影响关系 VIR（Vulnerability Interaction Relation）

资产 A 存在的脆弱性 $\{v_1, v_2, ..., v_j\}$，如果由于脆弱性 v_i 的存在导致增加了脆弱性 v_k 被攻击者利用的可能性，则称脆弱性 v_i 与脆弱性 v_k 之间存在相互影响关系，记为：$VIR_{vi:vk}$。

脆弱性间相互影响关系表示为：$C_4 = VV \subseteq V \times V$，其中 $VV(v_m, v_n)$ 表示脆弱性 v_m 与脆弱性 v_n 之间存在的相互影响关系。

一个脆弱性可能会和多个脆弱性存在关联关系，表示为：$v \to \{v_1, v_2, \cdots, v_j\}$，其中 $\{v_1, v_2, \cdots, v_j\}$ 表示和脆弱性 v 存在相互影响关系的脆弱性的集合。

MFDM 模型中利用攻击树分析脆弱性间相互影响关系。攻击树有两种基本的结构：AND 结构和 OR 结构[5]。

●AND 结构表示为：$< V_1 \& V_2, \cdots, \& V_n, V >$。

●OR 结构表示为：$< V_1 | V_2, \cdots, | V_n, V >$。

（4）模型的处理过程的设计

模型的处理过程主要通过分析资产之间的安全依赖关系、脆弱性之间的相互影响关系，计算资产的风险值。

MFDM 模型的处理过程分两步进行，第一步根据资产-威胁-脆弱性以及脆弱性之间的相互影响关系计算资产的风险值，第二步根据资产之间的安全依赖关系计算资产的风险值。如果资产之间不存在安全依赖关系，则只进行第一步计算。

第一步：考虑资产-威胁-脆弱性以及脆弱性之间的相互影响关系时计算资产的风险值。

风险是一种潜在可能性，是指某个威胁利用某个资产的脆弱性导致风险事件发生的可能性及其造成的损失。MFDM 模型中风险事件发生的可能性由威胁发生频率和脆弱性被利用难易程度决定，风险事件造成的损失由资产价值和脆弱性严重程度决定。MFDM 模型中资产的风险计算公式为：

$$R_1 = f(G(T_{fren}, P(v_i)), L(A_{value}, V_{serious}))$$

其中：R_1 表示资产的风险值。

A_{value} 表示资产价值。

T_{fren} 表示威胁发生频率。

$V_{serious}$ 表示脆弱性严重程度。

$P(v_i)$ 表示脆弱性被利用的难易程度。

G 表示风险事件发生可能性的计算函数。

L 表示风险事件所造成的损失的计算函数。

f 表示资产风险值的计算函数。

下面分别通过确定风险事件发生可能性以及风险事件造成的损失的计算方法，计算资产的风险值。

1）计算风险事件发生的可能性

定义集合 A={被测信息系统中的所有资产}=$\{A_1, A_2, \cdots, A_m\}$。

定义集合 B ={被测信息系统资产存在的脆弱性}={$B_1,B_2,\cdots,B_n$}，其中 $B_i,(i=1\cdots n)$ 表示资产 i 存在的脆弱性的集合，$B_i=\{B_{i1},B_{i2},\cdots,B_{ij}\}$，其中 $b_{ik},(k=1\cdots j)$ 表示资产 i 存在的脆弱性。

定义集合 C ={所有进行完脆弱性关联关系判断的资产}。

Step 1：判断集合 A 是否为空，如果 A 不为空，进行下一步；

Step 2：从集合 A 中选择一个没有进行过标记的资产 A_i；

Step 3：从集合 B 中选出资产 A_i 存在的所有脆弱性 b_{ik}，根据脆弱性之间相互影响关系的定义进行分析，确定该资产存在的脆弱性之间是否存在相互影响关系；

Step 4：如果该资产存在的脆弱性之间存在相互影响关系 $VV(v_m,v_n)$，进行下一步，否则，根据分析确定的资产-威胁-脆弱性之间的关联关系：$AT(a_i,t_j)$ 和 $TV(t_i,v_i)$，按照公式：风险事件发生的可能性 = $G(T_{fren},P(v_i))$，计算风险事件发生的可能性。

Step 5：由于考虑了脆弱性间的关联关系，某些脆弱性被利用的难易程度将发生改变，根据攻击树中的两种结构：AND 结构和 OR 结构分别计算脆弱性被利用的难易程度：

对于 AND 结构，其被利用的难易程度等于该节点各子树被利用的难易程度的乘积，即：$P(v)=P(v_1)\times P(v_2)\times\cdots\times P(v_n)$，其中：$v_1,v_2,\cdots,v_n$ 代表 v 节点的子树，$P(v)$ 代表 v 节点被利用的难易程度，$P(v_n)$ 代表子树被利用的难易程度。

对于 OR 结构，其被利用的难易程度等于该节点各子树被利用的难易程度的最大值，即：$P(v)=\max\{P(v_1),P(v_2),\cdots,P(v_n)\}$。

Step 6：根据上一步进算得出的脆弱性被利用的难易程度，按照公式：风险事件发生的可能性= $G(T_{fren},P(v_i))$，计算风险事件发生的可能性。

Step 7：对分析过的资产进行标记，并将该资产从集合 A 放到集合 C 中。

2）计算风险事件发生后的损失

根据资产价值和脆弱性严重程度，按照公式：风险事件发生后的损失= $L(A_{value},V_{serious})$，计算风险事件发生后的损失。

3）计算资产的风险值

根据计算得出的风险事件发生可能性和风险事件造成的损失，按照公式：

$R_1=f(G(T_{fren},P(v_i)),L(A_{value},V_{serious}))$，计算资产的风险值。

第二步：考虑资产之间安全依赖关系时计算资产的风险值。

定义集合 Q={所有需要分析是否具有安全依赖关系的资产}={$A_1,A_2,\cdots,A_m$}。

定义集合 AF={所有进行完安全依赖关系分析的资产}。

初始化：Q={需要判断是否具有安全依赖关系的资产}，AF={}。

Step 1：判断集合 Q 是否为空，如果 Q 不为空，进行下一步；

Step 2：从集合 Q 中选择需要判断安全依赖关系的资产 A_i；

Step 3：找出所有和资产 A_i 存在安全依赖关系的资产，如果存在 $AA(a_m,a_n)$，进行下一步，否则，转到 Step 2；

Step 4：对于每一个安全依赖关系，假设存在如下的安全依赖关系：$(A_i,s,A_j,u,P)A_j:uA_i:s$，如果资产 A_i 上的 s 存在的脆弱性导致资产 A_i 面临风险，按照以下公式计算资产 A_j（被关联资产）的风险值：

$$R_2=f(R_1,P)$$

其中：R_1 表示关联资产 A_i 的风险值（通过第一步计算得出），R_2 表示被关联资产 A_j 的风险值，P 表示资产 A 和资产 B 存在安全依赖关系的概率；

Step 5：将 $A_j:u$ 放到集合 Q 中；

Step 6：将 $A_i:s$ 从集合 Q 移入集合 AF 中。

2. MFDM 模型的应用

MFDM 模型的应用分为 4 个步骤：资产评估，威胁评估，脆弱性评估，风险计算。下面对这 4 个部分所完成的评估功能进行详细描述。

（1）资产评估

资产评估主要根据资产调查结果，确定被测信息系统中的资产类型，即确定集合 A 中的每个元素 a_i；根据安全调查结果获取的决定资产价值的相关属性，计算每个资产价值，即确定 $\{a_i|value\}$。

（2）威胁评估

威胁评估主要根据IDS检测结果和问卷调查结果，确定被测信息系统面临的威胁，即确定集合 T 中的每个元素 t_i；计算威胁发生频率，即确定 $\{t_i \mid fren\}$；分析资产面临的威胁，即确定 $AT(a_i,t_j)$。

（3）脆弱性评估

脆弱性评估主要根据漏洞扫描结果、BIOS 安全检测结果、WLAN 检测结果、设备有效性检测结果，确定被测信息系统存在的脆弱性，即确定集合 V 中的每个元素 v_i；确定每个脆弱性的严重程度和被利用难易程度，即确定 $\{v_i \mid serious, diff\}$；分析威胁可利用的脆弱性，即确定 $TV(t_i,v_i)$。

（4）风险计算

风险计算主要分析脆弱性间相互影响关系，即确定 $VV(v_m,v_n)$；分析资产间安全依赖关系，即确定 $AA(a_m,a_n)$；根据模型的处理过程确定的资产风险计算方法，计算资产的风险值。

四、结束语

本文在分析现有风险评估模型存在的问题的基础上，设计了多要素融合 MFDM 模型。MFDM 模型考虑了影响信息系统安全的主要因素，反映了信息系统安全因素之间的关键因素关系，确定了资产风险的计算方法。MFDM 模型简洁，具有通用性，为风险评估系统的设计奠定了基础。

参考文献

[1] 唐慧林.基于模糊处理的系统风险评估方法研究[D].郑州：中国人民解放军信息工程大学硕士论文，2005.

[2] Yong-Zheng Zhang, Bin-Xing Fang, Xiao-Chun Yun. A Risk Assessment Approach for Network Information System[D]. IEEE, 2004.

[3] Skaggs B, Blackburn B, Manes G, Shenoi S. Network vulnerability analysis[D]. IEEE, Computer Society Press, 2002.

[4] B. Schneier. Attack Trees[D]. Dr. Dobb's Journal, December, 1999:21-29.

信息安全等级保护和风险评估的关系研究

吴　贤
北京网络行业协会信息系统等级保护测评中心

一、等级保护和风险评估的宏观联系

信息安全等级保护制度作为我国信息安全保障体系建设的一项基本制度，它的总体目标是为了统一信息安全保护工作，提高我国信息安全建设的整体水平；通过充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到对信息和信息系统重点保护和有效保护的目的。等级保护工作的核心是对信息安全分等级，按标准进行建设、管理和监督。

风险评估是基于传统的风险管理经验通过对信息系统的资产、威胁、弱点和风险等要素进行评估分析的过程。信息系统的用户常常借助风险评估方法来分析自己的安全现状，评估自身安全需求和安全现状的差距，从而进行安全整改。

等级保护制度从一定意识上讲是信息安全保障工作中国家意志的体现，体现了国家对相应系统建设和使用单位在信息安全建设的基本要求。风险评估作为信息安全工作的一种重要技术手段，在实施信息安全等级过程中发挥着重要作用。

在落实信息安全等级保护工作中，信息系统运营使用单位可以结合本单位信息系统应用及行业特点，自主开展系统风险评估，为系统的安全整改和自查等工作提供重要参考依据。

二、风险评估在等级保护周期中的作用

信息安全等级保护制度在建设中要涉及一系列技术和管理问题。对于不同系统的各个安全域，用什么样强度的安全保护措施、措施的有效性是否能够达成、如何调整措施以满足系统的安全需求等，都可通过一些手段和方法来进行判断与分析。风险评估作为用户自主的一种技术手段可以运用到等级保护周期的系统定级、安全实施和安全运维三阶段：

1. 系统定级

由于信息系统具有自身的行业和业务特点，且所受到的安全威胁均有所不同，因此，可以依据信息安全风险评估国家标准对所评估资产的重要性、客观威胁发生的频率以及系统自身脆弱性的严重程度进行识别和关联分析，判断信息系统应采取什么强度的安全措施，然后将安全事件一旦发生后可能造成的影响控制在可接受的范围内。即将风险评估的结果作为确定信息系统安全措施的保护级别的一个参考依据。

2. 安全实施

安全实施是根据信息安全等级保护国家标准的要求，从管理与技术两个方面选择不同强度的安全措施，来确保建设的安全措施满足相应的等级要求。

风险评估在安全实施阶段就可以直接发挥作用，那就是对现有系统进行评估和加固，然后再进行安全设备部署等。

在安全实施过程中也会发生事件并可能带来长期的安全隐患，如安全集成过程中设置的超级用户和口令没有完全移交给用户、防火墙部署后长时间保持透明策略等都会带来严重的问题，风险评估能够及早发现并解决这些问题。

3. 安全运维

安全运维是指按照系统等级进行安全实施后开展运行维护的安全工作。

安全运维包括两方面：一是维护现有安全措施等级的有效性。可依据国家有关等级划分准则对信息系统所采取的安全措施是否满足要求进行检验，

以保证所采取的安全措施的强度持续有效。二是根据客观情况的变化以及系统内部建设的实际需要，等级要进行定期调整，以防止过度保护或保护不足。再定级的过程可参见系统定级部分的内容。

等级保护的三个阶段和风险评估的关系如图 1 所示。

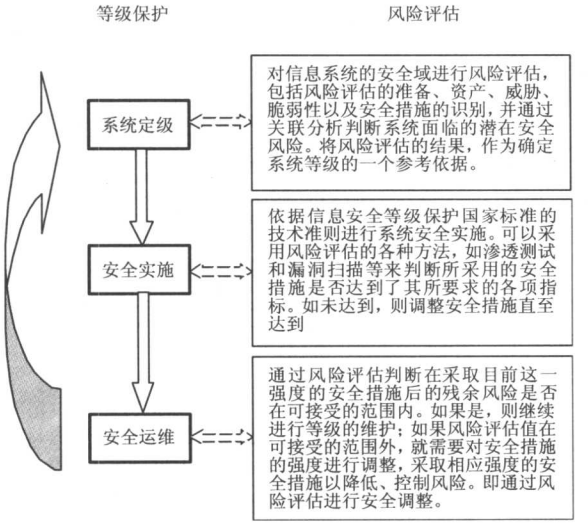


图 1　等级保护的三个阶段和风险评估的关系影射图

从图 1 可以看出，在等级保护的三个环节中，风险评估的作用分别为：在系统定级阶段用于参考帮助确定系统的安全等级，在安全实施阶段可以作为评估系统是否达到必需的安全等级的重要依据，在安全运维阶段开展定期和不定期风险评估以便帮助确认它保持的安全等级是否发生变化。

三、风险评估在等级保护层次中的应用

风险评估不但在等级保护周期的某些阶段发挥着重要的作用，在等级保护的各层次中也不可或缺。

下面仅就风险评估的技术手段（如系统审计、漏洞扫描和渗透测试等）在等级保护的各层次中发挥的作用进行说明。

漏洞扫描可以大致分为如下四类：主机漏洞扫描，网络漏洞扫描，数据库漏洞扫描，应用漏洞扫描。它们分别可以应用在主机安全、网络安全、数据库安全、应用安全的技术要求部分，如图 2 所示。

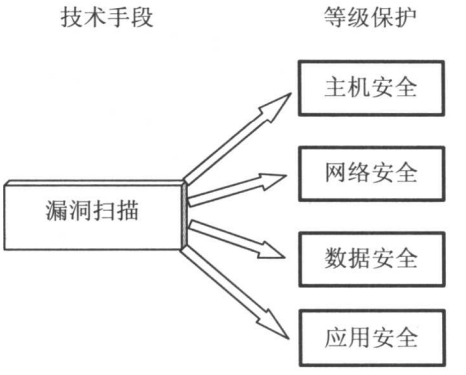


图 2

系统审计可以应用在等级保护中的网络安全审计、主机安全审计、数据库安全审计、应用安全审计的技术要求部分，如图 3 所示。

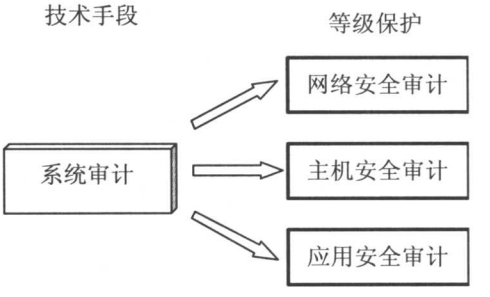


图 3

渗透测试可以应用在等级保护中的安全方案实施和安全运维两个阶段，并在网络安全、主机安全、应用安全、数据安全等技术要求部分起着辅助作用，如图 4 所示。

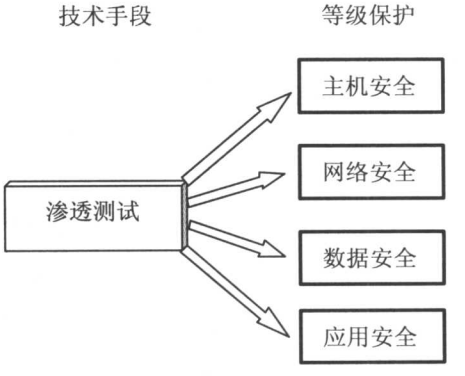


图 4

四、渗透测试在等级保护测评中的应用例子

在国家等级保护测评要求中大量使用了渗透测试，原因是客观上我国测评机构难以拿到国外厂家操作系统和数据库管理系统等的设计文档及源代码等，没有办法进行深度测试。具体说明如表 1 所示。

表 1

技术层	技术类	技术要求
主机系统安全	身份鉴别	应渗透测试服务器操作系统，可通过使用口令破解工具等，对服务器操作系统进行用户口令强度检测，查看能否破解用户口令，破解口令后能否登录进入系统。
		应渗透测试服务器操作系统，测试是否存在绕过认证方式进行系统登录的方法，例如，认证程序存在的安全漏洞，社会工程或其他手段等。
	访问控制	应渗透测试服务器操作系统和数据库管理系统，可通过非法终止强制访问模块，非法修改强制访问相关规则，使用假冒身份等方式，测试强制访问控制是否安全、可靠。
应用安全	身份鉴别	应渗透测试主要应用系统，测试身份鉴别信息是否不易被冒用（如通过暴力破解或其他手段进入系统，对 WEB 系统可采用 SQL 注入等绕过身份鉴别的方法）。
	访问控制	应渗透测试应用系统，测试自主访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作（如试图绕过系统访问控制机制等操作）； 应渗透测试应用系统，通过试图对系统进行绕过访问控制的操作，查看系统自主访问控制是否不存在缺陷。

五、风险评估结果在等级保护的定级阶段的应用举例

在等级保护的系统定级阶段引入风险评估的结果是结合国家等级保护标准和系统实际风险的过程，下面举一个等级保护试点的例子来说明风险评估在定级阶段的巨大作用。

在该试点中，对系统定级工作流程进行了如图 5 所示的定义。

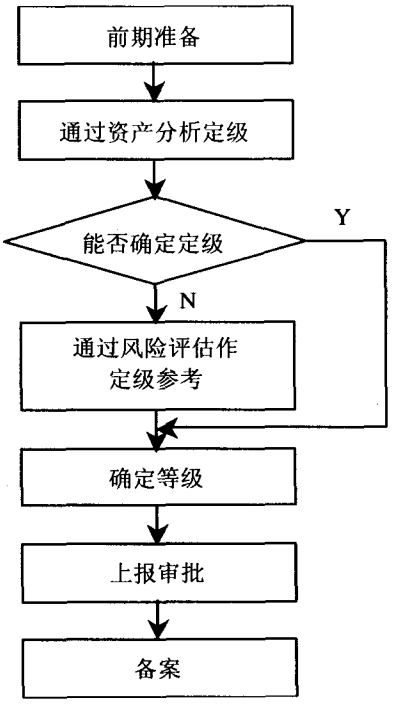


图 5　系统安全定级过程

①前期准备：为开展定级工作进行必要的准备。如准备待定级系统建设方案、安全解决方案、安全措施等相关材料。

②通过信息资产分析定级：按照等级保护相关标准，采用资产分析定级方法，评定其系统安全保护等级。

③通过风险评估作定级参考：当在金融、通信等非政府行业开展定级工作时，通过信息资产分析往往不能准确定级，则需要结合风险评估结果以引入风险调节因子作为重要参考来评定系统等级。

④确定等级：根据等级评定结果，确定本单位系统的安全等级。

⑤上报审查：将结果报同级信息化主管部门审查，同级信息化主管部门出具审查意见。

⑥备案：确定安全等级后，报信息化主管部门备案。

⑦已确定安全等级并已备案的系统，如果进行

改扩建，需依据等级保护相关标准并结合系统需求重新确定系统等级。

1. 通过资产分析定级

由系统资产价值来确定系统安全等级。

在定级要素中，信息资产价值对等级的划分起着决定性的作用。对于指定的系统必须首先进行资产识别与分析，明确被保护的信息资产，对每一项资产进行确认和评估。在对资产进行识别分析时，根据系统遭受破坏后，对保密性、完整性和可用性造成的影响来决定信息资产的价值。

2. 通过风险评估定级

在资产分析方法难以准确定级时，需要进一步采用风险评估方法得到系统面临的风险，作为风险调节因子，参考确定系统安全等级。

风险评估定级流程如图 6 所示。

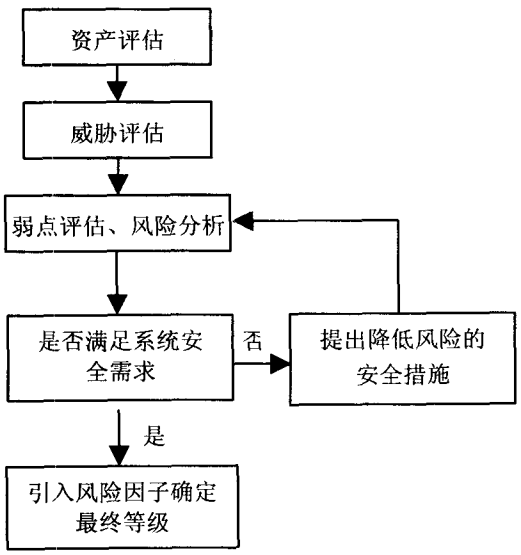


图 6 风险评估定级流程

①资产评估：在适当的粒度上识别、评估被保护资产，列出与资产清单，确定清单内每一项资产的价值。对资产进行评估时，要着重考虑资产对系统业务、机构整体利益以及国家安全的价值。

②威胁评估：对需要保护的信息资产进行威胁分析，确定系统面临的威胁。

③弱点评估、风险分析：评估系统脆弱性，采集有关统计数据，判断威胁发生的可能性，根据信息资产价值判断威胁发生时所造成的影响。

④如果系统的安全需求不能得到满足，根据风险分析结果提出降低风险的安全措施要求，并对采取这些措施的系统再次进行风险分析、判断，直到系统的安全需求可以满足。

⑤引入风险因子来参考调节系统等级。

五、结束语

目前国家关于等级保护和风险评估方面的具体工作要求、技术标准、管理办法等还在进一步完善中。本文基于对国家有关等级保护、风险评估要求及内容的理解，结合一些工作实践，形成了对两者相互之间关系的一些基本判断，可以看出等级保护是指导我国信息安全保障体系建设的一项基本制度，风险评估是在等级保护制度下，对信息及信息系统安全性评价方面特定的、有所区分但又有所联系的研究和分析方法，是等级保护（不同等级不同安全需求）的重要参考和技术手段，必将成为提升整个国家信息安全保障能力和水平,推进我国的国民经济和信息化进程的重要保障。

对信息安全等级结构的思考

赵利军
北方交通大学计算所

摘　要：本文针对当前信息安全等级建设中的一些情况提出了等级建设应当注意的问题，指出了一些问题产生的原因。但是，由于信息安全等级建设比较复杂，涉及面比较多，文中只讨论了技术层面上反映的情况。文中提出的一些观点仅供学术研究参考。

信息安全的等级结构往往是在信息安全保障体系之下确立的。因此，在讨论信息安全等级结构时，让我们先来看一下信息安全保障体系所应涉及的内容是有益的。

信息安全保障体系是考虑在复杂信息空间范围内建立信息安全防护结构，并根据其结构建立法规、标准、管理、人员配置等一系列配套措施，形成整体。所谓复杂的信息空间，是指具有不同系统平台，不同网络，不同信息存储、加密，不同系统接口，不同管理模式、运行时间，不同客户应用等的，既有分布，又有交错融合的环境。在这种环境下，人员管理、身份认证、信息监控、安全操作程序等许多环节上也是不统一和复杂的。

为解决上述问题，信息安全保障体系通常要包含法律法规、建设标准、组织结构、技术措施、实施管理等许多方面的内容。在这许多措施和内容中，本文只讨论信息安全的等级结构问题。那么什么是本文强调的信息安全等级结构呢？我们所说的等级结构是信息安全保障体系需要的技术框架，它是构建信息安全保障体系的基本技术模型和基础。因此，本文在讨论信息安全等级结构时，不涉及法律、法规和管理等问题。

等级结构怎样建立，我们认为首先应当考虑的是信息安全的基本需求。等级因需求而增减。例如，信息安全需要区分什么样的使用范围，需要采用怎样的技术来支持等级的建立，需要什么样的结构建立关系等。在不同的范围内，信息的处理方式不同，导致各个范围之间传递关系不同。基本结构的讨论就是要指导建立各种相对安全可靠的关系和结构，以便在实际信息安全体系建设中，规范各个等级结构设计，规划控制和传递，减少可能出现的结构性问题。

一、等级结构的关系和存在问题

按照目前的情况，我们将一些相对纯净的等级结构关系和存在的问题以图示形式描述，如图 1 所示。

根据图 1，我们所说的相对纯净是指在一个体系内：①在一种系统结构下；②各层结构明确，层次分明；③不存在交叉域、相同域和包含域。

在图 1 中，A、B、C、D、E 分成 5 个层次，分别代表 5 个域。由于域的不同，形成的等级也不同。每个域的边缘表示域的边界。我们用五角星代表采用的技术种类和设备（我们在此不考虑其类型）。在这种状态下可以产生不同的关系，而这种关系要靠边界、接口和传递来建立。在图 1 中的连线说明了这种关系。

等级关系的分别含义有层、域、技术种类、接口、边界和传递几个方面。

分层：有等级就要分层。有许多模型分物理层、系统层、应用层等，自下向上从技术层面上分层。或者其中附加一些中间层和控制层等。这样的好处是上下比较连贯，技术实现相对容易，兼容性好些，系统与物理设备配套，技术应用与系统配套。缺点