信息安全保障评价指标体系的研究

吴志军[1] 杨义先[2]
(中国民航大学电子信息工程学院 天津 300300)[1]
(北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)[2]

摘 要 信息安全保障与信息系统本身一样是一个复杂的系统。为了能够很好反映信息安全保障系统的功效,需要用可量化的参数作为衡量指标。从中国信息安全保障的国家战略、管理策略、工程规范和技术措施方面出发,提出了以"安全基线政策"(Security Baseline Policy)为核心的信息安全评价指标体系(Indicator);研究了具有双重反馈的评价思想和流程。利用信息安全保障评价指标体系有助于建立信息系统安全保障的长效机制,增强信息系统的安全性。

关键词 评价指标体系,信息安全保障,安全基线政策,评价
中图法分类号 TP309 **文献标识码** A

Research of Indicator for Information Assurance Evaluation

WU Zhi-jun[1] YANG Yi-xian[2]
(School of Electronics & Information Engineering, Civil Aviation University of China, Tianjin 300300, China)[1]
(Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)[2]

Abstract Both information system and information assurance are complex systems. To demonstrate the efficiency of information assurance better, it needs the quantitative parameters which are used as the indicators for the purpose of security evaluation. This paper presented the indicators for information assurance based on the core of security baseline policy, which is extracted from the juristic documents of national stratagem, management policy, engineering criterion, and technique measurements. The evaluate methods and procedures with double feedbacks were given in this paper. The indicators will help to improve the efficient and persistent of information assurance, and make the information system more secure.

Keywords Indicator, Information assurance, Security baseline policy, Evaluation

1 前言

为了更好地保障我国的信息安全,中央办公厅下发了《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)。27号文明确了加强信息安全保障工作的总体要求和主要原则,对加强信息安全保障工作做出了全面部署,提出了5年内建成国家信息安全保障体系IA(Information Assurance)的构想。目前,关系国家安全、经济命脉和社会稳定等方面的3大基础信息网络(电信网络、广电网络和互联网络)和8个重要信息系统行业(金融、电信、证券、保险、民航、铁路、税收和海关)的信息安全保障系统逐渐建成,并投入使用。

信息化是信息技术系统与社会系统相互作用、紧密耦合,且有大量人的行为参与其中的综合发展进程。然而安全因素和系统因素相互制约,使得信息安全具有很大的综合性、复杂性和不确定性[1-3]。同时,信息安全保障会伴随信息化的发展而不断变化。为了保证国家基础网络设施和重要信息系统等关键部门所建设的信息安全保障体系的长效机制,迫切需要针对不同重要行业、业务系统研究建立科学的、可度量的、可操作的信息安全保障评价指标体系(Indicator)[1-3],对其信息安全保障的整体状态进行科学的、客观的评价与描述,从而确定所建设的信息安全保障体系的保障水平、保障实效和保障周期等问题。因此,信息安全保障评价指标体系就是用一组科学的、可度量的指标作对信息安全保障系统的保障功能、保障效果和保障周期进行综合的考核和评价。

2 相关工作

现有的安全评估方式可以大致归结为4类:安全审计、风险分析、安全测评和系统安全工程能力成熟度模型SSE-CMM(Systems Security Engineering Capability Maturity Model)等。大部分通用的信息安全标准,如ISO 17799,ISO 13335等,其核心思想都是基于风险的安全理念[4-6]。信息技

到稿日期:2009-08-28 返修日期:2009-11-01 本文受国家973项目(No. 2007CB311203),国家863计划(No. 2009AA012439),国家自然科学基金委员会与中国民用航空总局联合资助项目(No. 60776808)和天津市应用基础及前沿技术研究计划项目(No. 09JCYBJC00400)资助。
吴志军(1965-),男,博士,教授,博士生导师,主要研究方向为通信网络和信息安全,E-mail:zhijun-wu@163.com;杨义先(1961-),男,博士,教授,博士生导师,主要研究方向为信息安全。

术先进的国家，例如美国、俄罗斯和日本等在信息安全保障评价指标体系方面已经率先开展了研究工作。特别是美国，利用卡内基梅隆大学系统安全工程能力成熟度模型 SSE-CMM[4]较早地建立了信息安全保障评价指标体系[5,6]。Rayford B. Vaughn[7]和 Nabil Seddigh[8]等人研究了信息安全保障评价的概念和范畴，给出了信息安全保障评价的框架。在国内，国家信息中心[9,10]研究了网络信息系统的信息安全保障理论和评价指标体系；更多的研究针对网络安全的评价指标体系[11]。在评估方面，魏忠[12]提出了从定性到定量的系统性信息安全综合集成评估体系；肖道举等[13]进行了网络安全评估模型的研究；黄丽民等[14]提出了网络安全多级模糊综合评价方法；李雄伟等[15]在采用模糊层次分析法 Fuzzy-AHP 评估网络攻击效果方面取得了一定的成果。有些研究已经应用到具体的行业中[16-18]。最近，中国工业与信息产业部推出了“中国信息安全产品评测指标体系”[19]。

目前，有关网络信息系统的安全评价虽然存在着多种多样的具体实践方式，但在世界上还没有形成系统化和形式化的评价理论和方法。评价模型基本是基于灰色理论(Gray Theory)或者模糊(Fuzzy)数学，而评价方法基本上用层次分析法 AHP(Analytic Hierarchy Process)或模糊层次分析法 Fuzzy-AHP，将定性因素与定量参数结合，建立了安全评价体系，并运用隶属函数和隶属度确定待评对象的安全状况。

上述各种安全评估思想都是从信息系统安全的某一个方面出发，如技术、管理、过程、人员等，着重于评估网络系统安全某一方面的实践规范，在操作上主观随意性较强，其评估过程主要依靠测试者的技术水平和对网络系统的了解程度，缺乏统一的、系统化的安全评估框架，很多评估准则和指标没有与被评价对象的实际运行情况和信息安全保障的效果结合起来。在目前的评估方法中，基础指标(技术、管理、工程和战略)是相互独立的，技术、管理、工程和战略措施是并行的，评价指标之间相互独立，从而导致评价精度下降和评价准确性出现偏差。

本文从中国信息安全保障的国家战略、管理策略、工程规范和技术措施方面出发，提出以“安全基线政策”(Security Baseline Policy)为核心的信息安全评价指标体系(Indicator)。

3 基于安全基线政策的信息安全保障评价指标体系

研究信息安全保障评价指标体系的主要目的是保证信息安全保障体系的战略完备性、管理先进性、工程成熟性和技术有效性。如何对这 4 个方面进行评价，则需要参照相关标准规定，即安全基线政策(Security Baseline Policy)。

3.1 安全基线政策的定义和含义

安全基线政策是为了保障互联网的信息安全，国家政府职权部门、行政管理部门和技术支撑单位从宏观、中观和微观 3 个角度，在国家、企事业和用户 3 个层次上，根据战略、管理、工程和技术 4 个方面制定的法律依据、标准规范、实施手段和技术方法的具体内容的统称。

安全基线政策制定了保障和维护国家信息安全的办法。它实际上规定了信息系统安全的边界，是个封闭的、不可逾越的警示线。信息系统的信息安全保障系统基线政策核心如图 1 所示。

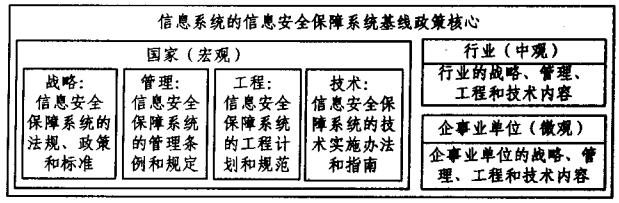

图 1 信息系统的信息安全保障系统基线政策核心

国家(宏观)的政策是从上而下贯穿到底的，它是行业(中观)和企事业单位(微观)必须坚决执行的。也就是，行业(中观)和企事业单位(微观)制定的发展战略、行政管理、规划工程和实施技术必须以国家(宏观)的相关政策为基础、以此为目标的。其中，

(1)战略保障为信息安全保障提供法律依据，包括法规、政策和标准。即根据信息社会发展的需要界定法律边界、规划发展蓝图和指明策略方向，例如《全国人大常委会关于维护互联网安全的决定》，以及国家和各相关部委的标准和规定等；

(2)管理保障为信息安全保障提供制度保证，包括条例和规范。即根据中国国情制定实施规范，颁布具体条例和说明执行程序，例如国家公安部、工业和信息部颁发的标准和规范等；

(3)工程保障为信息安全保障提供实施方法，包括实施和运行。即根据具体的保障情况要求实施质量监督和状态监控，例如国家对信息化工程实施指南的细则；

(4)技术保障为信息安全保障提供具体措施，包括需求、设计和方法。即根据美国安全工程能力成熟度模型(SSE-CMM)分析系统的功能需求，设计系统的整体方案，建立系统的协同机制，进行系统的安全运行管理，完成系统的安全时间审计和实施系统的安全态势监视，例如国家计算机安全管理中心和国家病毒中心推出的具体措施。

由安全基线政策的定义和含义可以得出安全基线(Security Baseline)的定义为：从安全基线政策中抽取具体的量化值，用以具体表示安全基线政策，安全基线就是在安全基线政策的“圈”上通过抽样选取的具有代表性的点。

3.2 信息安全保障评价框架和流程

随着信息化的快速发展，面临着许多安全威胁，比如病毒侵入、恶意入侵和蓄意攻击等。为了保证信息化快速健康地发展，必须建立长效机制的信息安全保障系统。为了保证和检验信息系统的信息安全保障系统的有效性和长久性，建立信息安全保障评价指标体系，用于对信息安全保障系统进行综合性评价。

信息安全保障系统必须是在达到安全基线政策的要求下，根据中办发[2003]27 号文的精神，结合实际信息系统而设计的。它是在针对安全威胁(病毒、入侵和攻击等)进行风险评估，判断现在的安全形势的基础上，研究安全策略，制定具体的安全措施，形成系统的安全保障，达到一定的安全保障效果(安全属性：安全性、机密性和不可抵赖性等)。因此，可以得出信息安全保障体系由 3 部分组成：

(1)信息安全保障措施，包括战略、管理、工程和技术措施；

(2)信息安全保障系统框架，是将信息安全保障措施综合集成为系统的保障体系，应用到实际信息系统的保障中；

(3)安全属性,是信息安全保障效果最终的体现,具体反映出信息安全保障体系在信息和信息系统的安全属性方面的效果。

根据信息安全保障系统的组成,可以得到信息安全保障评价的3个角度。

(1)保障角度:根据具体信息系统的应用功能,以及面临的安全威胁分析,确定相应的信息安全保障策略和方法;

(2)运行角度:根据保证信息系统正常运行的要求,进行必要的数据统计和监控手段;

(3)效果角度:根据信息系统安全保障的重点,针对具体的保障内容进行保障效果的检验。

通过以上所述,可以得到信息安全保障评价框架,如图2所示。从系统的角度来说,信息安全保障的目的就是使整个信息系统保持动态平衡(安全)的状态。

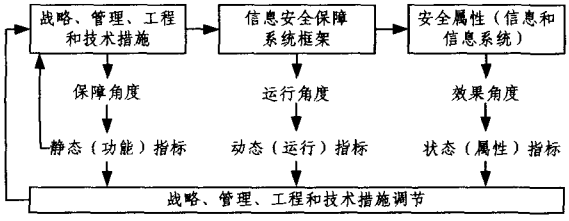

图2 信息安全保障评价框架示意图

从图2可以看出,完整的信息安全保障评价流程包括3个过程:静态评估、动态评估、状态评估。

(1)静态评估:评价纸面上的东西,即评价信息安全保障设计的方案文档、制定的安全措施档案和安全管理的标准规范等。主要评价内容为安全方案的合理性、安全措施的正确性和标准规范的科学性。

静态评估的主要手段有两种。第一种为专家打分:要求一定数目的专家组成员独立针对每项安全方案、措施和规范的设计和内容进行评分,采用层次分析法(AHP)或者模糊层次分析法(F-AHP)将评分进行综合,得到评价结果;第二种为问卷调查:专家组成员根据具体信息系统的应用功能,事先有针对性地准备好一些问题,让被评估单位的专业人员进行回答,然后评估专家根据问卷的得分,对评估对象给出评价结论。

(2)动态评估:是对信息系统和信息安全保障系统的运行情况做出判断。该过程需要统计信息系统和安全保障系统日常运行的记录数据,包括信息安全值班的所有记录和安全审计的日志等,例如网络流量、网络带宽、协议,以及入侵检测、防病毒、防火墙和安全审计等原始记录数据和统计显示数据。对记录数据进行统计和处理,以得到信息安全的评价结论。

(3)状态评估:是检验信息安全保障的效果。主要表现在对信息和信息系统的安全属性(保密性、完整性、真实性、可用性、不可抵赖性、抗毁性、生存型和有效性)进行测试和检验。主要手段包括两种:第一种为渗透测试,模拟黑客攻击的渗透测试技术,有助于查找信息系统的脆弱点和检验信息安全保障系统的效果;第二种为专项测试,针对信息和信息系统的某个安全属性,采用专业技术进行单项测试,检验信息安全保障在某个功能上的保障效果。

针对上述3个评估过程可以得到3种信息安全评价指标:静态(功能)指标、动态(运行)指标和状态(属性)指标。

图2中的3个评估过程是通过2个反馈关联起来的。其中,第一个反馈是内反馈,它将静态(功能)指标的评价结果反馈到信息系统的安全方案设计、安全措施实施和安全管理标准规范制定这个环节上,以对相关的文档进行修改,通过调整达到静态(功能)指标的要求;第二个反馈是外反馈,它是将动态(运行)指标和状态(属性)指标的评价结果送入到战略、管理、工程和技术调节单元中,把相关的调整变化也反馈到安全方案设计、安全措施实施和安全管理标准规范制定这个环节上,以保证从源头开始,满足信息系统的信息安全保障的要求。

通过3个评估过程和2个反馈,从系统化的角度,信息系统和信息安全保障系统形成一个动态平衡的系统,即在一定时间内保持相对安全的系统(安全是相对的,它在某一时段是安全的,而在另外一个时段就可能不安全了)。该系统可以根据安全威胁的变化,通过调节安全策略和措施,使整个系统长期达到动态的平衡状态,即安全状态。

3.3 信息安全保障评价指标体系

由信息安全保障评价框架和流程可以得知,信息安全保障评价指标的核心为静态(功能)指标、动态(运行)指标和状态(属性)指标。信息安全保障评价指标体系如图3所示[20]。

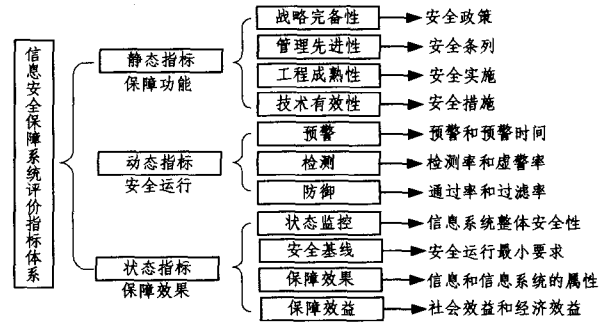

图3 信息安全保障评价指标体系

由图3可得信息安全保障评价指标体系分为4级:

(1)总体指标

总体指标为信息安全保障评价指标,表示信息安全保障整体的安全态势、保障效果、经济和社会效益。

(2)Ⅰ级指标

分别采用静态评估、动态评估和状态评估3种手段对信息安全保障系统进行评价,得到3个Ⅰ级指标,即静态、动态和状态指标。

(2)Ⅱ级指标

由3个Ⅰ级指标延伸出如下11个Ⅱ级指标:

a)静态指标包括战略完备性、管理先进性、工程成熟性和技术有效性;

b)过程指标包括预警、检测和防御;

c)效果指标包括状态监控、安全基线、保障效果和保障效益。

(3)Ⅲ级指标

Ⅲ级指标为基础指标,它是在信息系统上通过技术手段和管理手段可以直接或者间接采集或者统计得到的数据和信息,即为底层的信息安全保障运行数据。

基础指标的组成如下:

a)静态指标包括安全政策、安全条例、安全实施和安全措施;

b)过程指标包括预警、检测和防御；

c)效果指标包括整体安全性、安全运行最小要求、信息和信息系统的安全属性以及社会效益和经济效益。

4 比较分析

本文提出的基于安全基线政策的信息安全保障评价指标体系与常用的信息安全评估方法存在以下区别：

(1)目前的评估方法都是采用专家打分，利用层次分析法(AHP)进行评估。这个方法的缺点十分明显：

a)评价结果的指标单一，不能形成一个指标体系，所以评估的结果片面性较强；

b)评价对象相对比较独立，而且结构形式不能太复杂，对于复杂的计算机网络则不太适合。

因此，本文提出评价指标体系的思想，采用一组多级的评价指标，构成对信息安全保障系统评价的指标体系，采用关联判定和综合评估的方法对复杂的信息安全保障系统进行综合评价。

(2)现有的评估方法都是将保障系统中的功能模块进行划分，单独评估，最大的问题在于没有考虑每个模块之间的关系，或者将每个模块之间的关系简单化，导致评估的结果精确度下降。而之所以采用模块划分的评估方法，是因为没有一个统一的评估流程模型可以综合评估过程中的众多因数。

因此，本文在系统控制理论的基础上，从安全性评估的角度，利用反馈技术，提出一个基于反馈控制系统的信息安全保障系统安全性评估流程模型。

(3)现有的评估方式是在系统设计完成后再进行评估，而不是对每个环节都加以考虑，这样使评估的效果不好，修改空间和可能性很小，导致系统存在安全性设计缺陷。

本文提出的评价指标体系是在系统设计、实施和运行的每个阶段均进行评估，采用 SSE-CMM 模型 6 个方面的问题来进行综合评估，保证了信息系统及其信息保障体系在建设、使用和更新等各个过程中的安全。

(4)目前的系统安全性评估往往与系统可靠性评估联系起来，利用可靠性指标代替安全性评价。

本文提出的思想，是在保证信息系统的可靠性前提下，针对信息和信息数据的安全方面问题提出评估的指标和方法。

(5)现有的信息安全评估框架，没有给出具体的评估流程，重要的是没有与信息系统的业务关联，没有明确面向业务流程的评估方法，可操作性较差。

本文提出的评价指标体是将信息系统的各种业务和业务流程联系起来，根据具体业务的传输和应用，提取不同的信息安全评价指标，具有操作方便的特点。

结束语 本文从战略、管理、工程和技术 4 个方面，在宏观、中观和微观层面建立了互联网信息安全保障系统的评价指标体系，提出了综合评价的思想，给出了评价的具体流程，并与现有的评估方法进行了比较。

本文的主要工作集中在以下两点：

(1)研究了信息安全保障安全基线政策，在此基础上提取了安全基线指标。

战略、管理、工程和技术的基线指标提取是基于安全系统工程成熟度模型 SSE-CMM 的安全基线制定的 6 条原则。

① 战略基线

战略基线包括安全需求基线和安全输入基线。

② 管理基线

管理基线包括协同安全基线和安全管理基线。

③工程基线

工程基线包括安全实施基线和质量管理基线。

④ 技术基线

技术基线包括安全保证参数基线和监视安全态势基线。

(2)建立了信息安全保障系统的评价指标体系。

① 研究思路总结

a)从一个实体的 3 个角度评价

功能角度——评价采用的技术、管理和战略措施的水平(战略完备性、管理先进性、工程成熟性和技术有效性)；

运行角度——保障系统的功能完善和强大(预警、保护、检测、反应、恢复、反击)和能力(6 个能力指标)；

效果角度——属性(信息：保密性、完整性、真实性、可用性和不可抵赖性；信息系统：抗毁性、生存性和有效性)和目的(8 个属性指标)。

b)两个反馈支路

大反馈支路：在针对信息系统实验战略、管理、工程和技术上的信息安全保障措施后，根据体现在被保护对象上的具体效果情况，进行反馈调节，使信息系统的运行状态达到动态平衡(安全)状态。

小反馈支路：用于调节战略、管理、工程和技术措施之间的平衡。

② 评价指标体系建立

保障对象的系统层次划分-涉安定级；

根据信息系统的层次划分，针对相应的保障措施提取评价指标。

信息安全保障评价指标体系能够全面、综合地反映信息安全保障的有效性、可用性和持续性，为我国信息安全保障的建设提供了有力的保证，有助于我国信息安全保障的良好发展。

参 考 文 献

[1] Network Evaluation and Benchmarking Standard Service Level Agreement (SLA)[R]. University of Michigan, Information Technology, 2004: 1-47

[2] Executive office of the president Washington dc national science and technology council. Federal Plan for Cyber Security and Information Assurance Research and Development[R]. 2006: 1-140

[3] Evans D W, Chatmon C L. Increasing minority participation in information assurance[C]// Proc. of Information Technology Based Higher Education and Training, 6th ITHET International Conference. 2005: 12 -15

[4] Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document Version 3. 0[R]. Carnegie Mellon University, 2003: 1-150

[5] Peltier T R. Information Security Risk Analysis[M]. Boca Raton, Florida: CRC Press LLC, 2001

[6] Butler S A. Security Attribute Evaluation Method: A Cost-benefit Approach[C]// 24th International Conference on Software Engineering. ACM, 2002: 230-240

(下转第 82 页)

理论分析相符。iHEED 在多跳情况下，可能出现“分簇父节点丢失”现象，导致网络断裂，聚合数据无法传送回 sink 节点，在 5 组仿真情况下，其分簇后网络连通的成功率最高只有 80%。通过仿真实验，证明了“分簇父节点丢失”现象的存在。

结束语 本文通过理论分析和实验仿真说明了 iHEED 协议中可能出现的“分簇父节点丢失”现象，提出了改进协议 iHEED-CHLevel。iHEED-CHLevel 采用分层成簇算法，保证了簇间在多跳情况下的连通，并通过在 TOSSIM 上模拟运行，验证了 iHEED-CHLevel 算法的可靠性。本文所实现的 iHEED-CHLevel 协议可集成于 TinyOS 下其他多跳路由协议中，对实际工程应用具有一定的指导意义。

参 考 文 献

[1] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless sensor networks: a survey [J]. Computer Networks, 2002: 393-422

[2] 任丰原，林闯. 无线传感器网络[J]. 软件学报，2003，14(07)：1282-1291

[3] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks [C]//Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Maui, HI, 2000: 1-10

[4] Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks[J]. IEEE Transactions on Mobile Computing, 2004, 3(4): 660-669

[5] Younis O, Fahmy S. Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-efficient Approach[C]// Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. INFOCOM, 2004: 629-640

[6] Lindsey S, Raghavendra C, Sivalingam K M. Data gathering algorithms in sensor networks using energy metrics [J]. IEEE Transactions on Parallel and Dist ributed Systems, 2002, 13(9): 924-935

[7] Heinzelman W, Chandrakasan A, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks [J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670

[8] 陈静，沈鸿. MELEACH 一个高效节能的 WSN 路由协议[J]. 传感技术学报，2007(12)：2089-2094

[9] Chang Ruay-shiung, Kuo Chia-jou. An Energy Efficient Routing Mechanism for Wireless Sensor Networks[C]// Proceedings of the 20th International Conference on Advanced Information Networking and Applications. 2006: 308-312

[10] Younis O, Fahmy S. An experimental study of routing and data aggregation in sensor networks[C]//Proceedings of the International Workshop on Localized Communication and Topology Protocols for Ad hoc Networks. Washington, DC, 2005: 49-57

[11] Levis P, Madden S, Polastre J, et al. TinyOS: An operating system for wireless sensor networks[C]// Ambient Intelligence. New York, NY: Springer-Verlag, 2005(12): 115-148

[12] 颜庭苇，孙利民. TinyOS 路由协议原理及性能评估[J]. 计算机工程，2007(1)：112-114

[13] Gay D, Levis P, Behren R, et al. The nesC language: A holistic approach to networked embedded systems[C]// Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation. New York, USA: ACM Press, 2003: 1-11

[14] Levis P, Lee N, Welsh M, et al. TOSSIM: Accurate and scalable simulation of entire tinyos applications [C] // Proc. of the 1st International Conference on Embedded Networked Sensor System. ACM Press, 2003: 126-137

(上接第 10 页)

[7] Vaughn R B Jr, Henning R, Siraj A. Information Assurance Measures and Metrics-State of Practice and Proposed Taxonomy [C]// Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03). Big Island: Hawaii, 2003

[8] Seddigh N, Pieda P. Current Trends and Advances in Information Assurance Metrics[C]// Proceedings of the Second Annual Conference on Privacy, Security and Trust. Privacy, Security, and Trust, 2004: 197-205

[9] Lu Xin, Ma Zhi. Information Assurance Evaluation for Network Information Systems[C]// Computational Intelligence and Security. Guangzhou, China: Springer, 2006: 869-877

[10] 吕欣. 信息系统安全保障理论与评价指标体系[J]. 微电子学与计算机，2006，23(10)：10-12

[11] 郭振民，胡学龙，姜会亮. 网络与信息系统安全性评估及其指标体系的研究[J]. 现代电子技术，2003(9)：9-11

[12] 魏忠. 从定性到定量的系统性信息安全综合集成评估体系[J]. 系统工程理论方法应用，2004，13(5)：478-479

[13] 肖道举，杨素娟. 网络安全评估模型研究[J]. 华中科技大学学报，2002，30(4)：37-39

[14] 黄丽民，王华. 网络安全多级模糊综合评价方法[J]. 辽宁工程技术大学学报，2004，23(4)：510-513

[15] 李雄伟，杨义先，等. Fuzzy-AHP 法在网络攻击效果评估中的应用[J]. 北京邮电大学学报，2006，29(1)：124-127

[16] 章文辉，杜百川，杨盈昀. 模糊层次分析法在广播电视信息安全保障评价指标体系中的应用研究[J]. 电子学报，2008(10)：2060-2064

[17] 程学东. 电信网网络安全评估指标体系研究[J]. 现代电信科技，2005(8)：10-13

[18] 王剑，彭越，吴志军. 航空信息系统安全评价指标体系[J]. 信息安全与保密通信，2008(1)：24-26

[19] 中国工业和信息部. 中国信息安全产品评测指标体系，技术标准[S]. 深圳：工业和信息化部旗下中国软件评测中心，2008：1-4

[20] 国家信息中心. 信息安全保障评价指标体系[R]. 2005：1-20