系统化的信息安全评估方法

马 兰[1,2] 杨义先[3]

(天津大学系统工程研究所 天津 300072)[1] (中国民航大学空中交通管理学院 天津 300300)[2]

(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)[3]

摘 要 信息安全评估是保证信息安全保障长效机制的关键。以动态系统控制理论为基础,针对信息系统的信息安全评估问题进行了研究,设计了系统化信息安全保障框架模型,提出了信息安全系统化的评估模型,给出了系统化评估的方法和流程,以为信息系统的信息安全评估打下基础。

关键词 信息安全,信息安全保障,评价指标体系,系统化

中图法分类号 TP309 **文献标识码** A

Systemic Approach of Evaluating Information Security

MA Lan[1,2] YANG Yi-xian[3]

(Institute of Systems Engineering, Tianjin University, Tianjin 300072, China)[1]

(Air Traffic Management School, Civil Aviation University of China, Tianjin 300300, China)[2]

(Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)[3]

Abstract Information security evaluation is the guarantee to the effective long-term information security protection. Based on the theory of dynamic system control, this paper emphasized on the system approach of Information security evaluation, presented a framework model for information assurance, and proposed a evaluation model for system approach of information security, dedcribed the procedures of system approach of information security, and provided the hardens to the protect system of information security.

Keywords Information security, Information assurance, Indicator system, Systematization

1 前言

金融、电信、证券、保险、民航、铁路、税收和海关8个系统,以及电信网络、广电网络和互联网络3个基础网络是我国信息安全保障的重中之重。目前,中国信息化水平与国际先进水平还有较大差距,信息安全保障尚存在很多问题亟待解决[1]。我国信息安全保障的发展经历了3个阶段:第一阶段为单机版的杀病毒和防病毒软件;第二个阶段为从单一的防火墙产品逐渐向信息安全系列产品发展;第三个阶段为信息安全保障体系的建设[2]。信息安全保障的内容和深度不断得到扩展和加深,但依然存在着"头痛医头,脚痛医脚"的片面性,没有从系统工程的角度来考虑和对待信息安全保障问题[3,4]。

信息安全保障问题的解决既不能只依靠纯粹的技术,也不能靠简单的安全产品的堆砌,它要依赖于复杂的系统工程——信息安全工程SSE(System Security Engineering)。信息安全工程是采用工程的概念、原理、技术和方法,来研究、开发、实施与维护信息系统安全的过程,是将经过时间考验证明是正确的工程实施流程、管理技术和当前能够得到的最好的技术方法相结合的过程[5]。

由于国家8个重点信息系统和3个重点基础网络本身均为复杂的大型信息系统,因此必须采用系统化方法对其信息安全保障的效果和长效性进行评估。

2 相关工作

目前,国际上系统的信息安全评价方法主要是美国国家安全局提出的系统安全工程能力成熟模型SSE-CMM(System Security Engineering-Capability Maturity Model)和《信息保障技术框架》IATF(Information Assurance Technical Framework)[5,6]。

系统安全工程能力成熟模型(SSE-CMM)的开发源于1993年5月美国国家安全局发起的研究工作。SSE-CMM确定了一个评价安全工程实施的综合框架,提供了度量与改善安全工程学科应用情况的方法。也就是说,对合格的安全工程实施者的可信性,是建立在对一个工程组的安全实施与过程的成熟性评估之上的。SSE-CMM项目的目标是将安全工

到稿日期:2010-10-11 返修日期:2011-01-27 本文受国家自然科学基金委员会与中国民用航空总局联合项目(60776808),天津市应用基础及前沿技术研究计划项目(09JCYBJC00400)资助。

马 兰(1966—),女,副教授,主要研究方向为空中交通管理和信息安全,E-mail:malan66@263.net;杨义先(1961—),男,博士,教授,主要研究方向为信息安全。

程发展为一整套有定义的、成熟的、可度量的学科。目前，SSE-CMM已经成为西方发达国家政府、军队和要害部门组织和实施安全工程的通用方法，是系统安全工程领域里成熟的方法体系，在理论研究和实际应用方面具有举足轻重的作用[5]。

美国国家安全局IATF(《信息保障技术框架》)对信息安全工程进行了深入研究，以为保护美国政府和工业界的信息与信息技术设施提供技术指南。IATF从整体、过程的角度看待信息安全问题，其代表理论为"深度防护战略(Defense-in-Depth)"。IATF强调人、技术、操作这3个核心原则，关注4个信息安全保障领域：保护网络和基础设施、保护边界、保护计算环境、支撑基础设施。最终将信息安全工程的重点放在了发掘信息保护的需求上，即"保护需求的导出PNE"，详细说明了信息安全系统工程ISSE(Information Security System Engineering)中第一个、也是最重要的一个活动[6]。

在国内学术研究方面，北京邮电大学信息安全中心的杨义先教授及其课题组在采用模糊层次分析法Fuzzy-AHP进行网络攻击效果评估[7]方面取得了一定的成果；清华大学的段海新教授提出了一种实体安全体系结构[8]；国防科技大学的黄遵国研究员在网络可生存技术及其实现框架方面取得了成果[9]；国家信息中心的吕欣研究了网络信息系统的信息安全保障[10]；在信息安全评价框架、模型和算法研究方面，北京大学计算机科学技术研究所信息安全实验室的徐辉等研究了基于动态贝叶斯规划图的状态安全报警关联[11]；海军工程大学的吴晓平教授等提出了基于贝叶斯网络的信息安全风险评估方法[12]；成都三零盛安信息技术有限公司的魏忠研究了从定性到定量的系统性信息安全综合集成评估体系[13]；山东大学的黄丽民和王华教授提出了网络安全多级模糊综合评价方法[14]；华中科技大学的肖道举和杨素娟教授进行了网络安全评估模型研究[15]；还有很多其他研究人员在人为因素和管理等方面都做了大量的工作，提出了许多很好的安全评估方法[16]。

目前，有关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[7]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。

3 系统化信息安全评估模型

系统化信息安全评估是为确保实施长效机制的信息安全保障工程，对信息安全保障建设过程进行监督和指导。其内容包括：(1)涉及分布于整个信息安全保障工程生命周期中各个环节的工程活动，包括概念定义、需求分析、设计、开发、集成、安装、运行、维护及更新；(2)为信息安全产品开发者、安全系统开发者和集成者提供信息安全保障指导，以及提供信息安全服务和信息安全工程的组织；(3)适用于各种类型和规模的信息安全保障工程组织，例如行业、商业、政府和研究机构[5]。

3.1 信息安全保障框架模型

信息保障系统在结构上具有分布式、层次化的特点，在功能上具有动态、多样化的特点。现代信息保障体系包含战略、管理、技术和工程体系3大要素；拥有预警、保护、检测、反应、恢复和反击6大能力。信息保障评价过程跨越了信息和信息系统的规划、设计、实施、运维和废弃5个基本阶段。因此，评价一个信息保障系统保障能力的大小，需要从不同的维度进行度量，既要考虑现有的安全措施是否满足抵御威胁的要求，又要考虑实际的运行效果是否满足设计要求[17]。

本文将信息安全保障系统看作为具有多输入、多输出的系统结构。安全保障措施(战略、管理、技术和工程措施)作为系统的输入量，是在一个统一的保障框架下去达到系统所期望的保障效果。多输入、多输出的信息安全保障框架模型如图1所示。其中，信息安全保障系统用函数 $F(N,Y)$ 表示，$N=l+p+q+r$ 代表所有战略 S、管理 M、技术 T 和工程 E 的措施总和；战略表示为 $S=(s_1,s_2,\cdots,s_{l-1},s_l)$，其中 $s_1,s_2,\cdots,s_{l-1},s_l$ 表示每个具体的战略措施；管理表示为 $M=(m_1,m_2,\cdots,m_{p-1},m_p)$，其中，$m_1,m_2,\cdots,m_{p-1},m_p$ 表示每个具体的管理措施；技术表示为 $T=(t_1,t_2,\cdots,t_{q-1},t_q)$，其中 $t_1,t_2,\cdots,t_{q-1},t_q$ 表示每个具体的技术措施；工程表示为 $E=(e_1,e_2,\cdots,e_{r-1},e_r)$，其中 $e_1,e_2,\cdots,e_{r-1},e_r$ 表示每个具体的工程措施；$I=(i_1,i_2,\cdots,i_{y-1},i_y)$ 代表所有的静态(信息安全保障设计措施)、动态(信息安全保障实际运行情况)和状态(信息安全保障实际效果)评价指标的总和[18]，其总数为 Y。$F(N,M)=(f_1,f_2,\cdots,f_{i-1},f_i)$，其中 $(f_1,f_2,\cdots,f_{i-1},f_i)$ 分别表示信息安全保障系统的各个组成系统，例如互联网安全运行系统SOC(Security Operational Center) f_1 和网络信息中心NIC(Network Information Center) f_2 等。由于对信息系统的信息安全评价是一个根据实际安全评价结果(静态、动态和状态评价指标)不断调整安全保障措施，以达到最佳安全性的动态反馈过程，因此必须在 $F(N,Y)$ 中引入动态反馈函数 f_{t_k}，其中 t_k 表示动态调整时刻。如果 $t_k=0$，则属于静态评价。信息安全保障措施和信息安全评价指标之间的关系为 $I=f(t_k)\cdot S\cdot M\cdot T\cdot E\cdot F(N,Y)$。

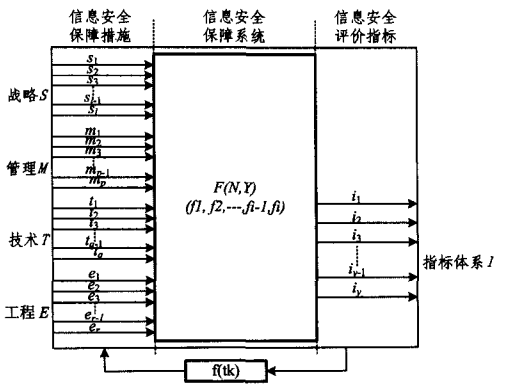

图1 信息保障框架模型

依据上述对保障模型的分析，可以看出保障措施和保障效果的好坏存在因果关系，即保障措施是因，保障效果是果。

保障措施越不力，保障效果就越差，发生安全事件的可能性就越大，反之也成立[19]。但是安全事件的发生除了与保障措施设置不当有关以外，在很大程度上受到偶然性的影响。因而，评价保障措施指标从而预测保障效果和实际运行效果之间存在一定程度的相关关系，它们从不同侧面、不同阶段反映了系统整体的安全保障水平，二者互为补充。这两种指标结合，既考查了系统在一定时期内实际安全保障成绩，又考查了系统要素及其组合中因措施不力而造成的安全隐患，避免了评价过程的片面性，能够比较全面而客观地反映信息保障的整体安全态势。

3.2 基于状态观测器的信息安全综合评价模型

本文根据现代控制理论和状态控制理论，在信息安全保障框架模型（见图 1）的基础上，建立了一个基于状态观测器的信息保障综合评价模型[18,20]，如图 2 所示。

该模型具有 2 个反馈环路。通过状态变量的计算，安全属性值按照一定的反馈控制律反馈输入端，也就是调整安全保障措施，使信息保障的保障能力动态调整，不断地适应安全需求。具体到模型中，反馈控制的变量为保障措施，例如入侵检测、传输加密和防火墙等。保障措施设置不当，体现在某个保障措施的某个具体参数不适当，例如加密算法的密钥长度、防火墙的过滤规则等。假如在整体保障能力中有某项安全属性要求的情况下，依据子系统权重递减的顺序，先分析重要性最高的子系统。如果该子系统能满足属性需求，则考虑次重要子系统。否则，分析该子系统中的基础指标集合，同样依据基础指标的权重，从最重要的基础指标的安全措施调整，调整力度为提高一个序化等级，然后再次进行整体属性计算，直到能够满足所有的安全属性保障需求为止。

图 2 所示的信息保障评价模型，主要包含保障措施集合、保障效果集合、状态观测器、状态反馈控制律、实际效果反馈等组成要素。

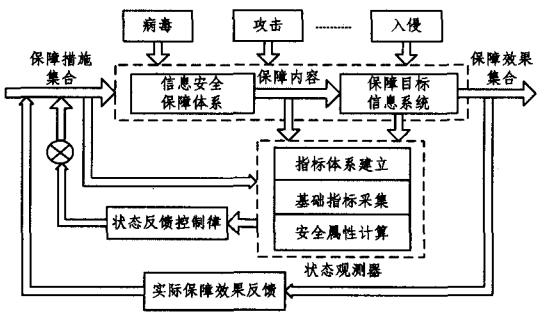

图 2 基于状态观测器的信息保障综合评价模型

在控制理论中，状态观测又叫状态重构，其实质就是对物理上无法直接观测的状态变量进行估计的过程。在本文所设计的基于状态观测器的信息保障评价模型中，状态变量选取的是信息安全属性指标，显然这些指标不具备物理可观测性。因此必须构造适当的状态观测器，对信息安全属性进行测算。

在信息保障评价模型中，状态观测的过程就是通过对目标保障系统建立适当的指标体系，采集指标，然后进行信息安全属性量化计算的过程。目前，对信息安全属性的定义往往是叙述性的描述。若要对其进行量化计算，就需要首先解决两个问题：一个是信息安全属性的量化定义；一个是信息安全属性的量化算法。在现代控制论中，状态变量能够完全反映系统的运动状态。在信息保障评价模型中，状态变量——信息安全属性的计算结果，全面反映着信息保障体系的保障能力，是进行信息保障评价的最终目标之一。因此，状态变量的计算或者说状态观测器的设计就显得尤为重要。

如系统控制理论所说，状态反馈是将系统的每一个状态变量乘以相应的反馈系数，然后反馈到输入端，参考输入相加，形成控制律，作为受控系统的控制输入。因此，反馈控制律的设计是反馈控制的核心。在本文设计的评价模型中，状态反馈发生在信息安全按属性计算之后，通过比较每一个信息安全属性的计算结果和安全需求的差值来判断反馈过程。如果发现某一个安全属性的计算结果大于安全需求区间，则判定为该属性过度保障，需要降低保障措施的保障级别。反之，如果小于安全需求区间，则判定为该属性保障不足，需要提高保障措施的保障级别。

信息安全是一个全面的概念，包含信息系统安全、信息安全和运行安全 3 大层次的内容。信息保障措施依据其保障对象也可以分为信息系统保障措施、信息安全保障措施和运行安全保障措施 3 大类[3,4,21]。

(1)信息系统保障措施保障的是信息系统的抗毁性、生存性和有效性，属于物理安全。面临的主要威胁是人为的或自然的物理破坏，例如地震、火灾、施工破坏、设备自然老化等。保障的目的是信息系统抵御物理破坏的能力或者物理破坏发生后的生存能力。主要的保障措施有重要设备访问控制、机房建筑防火抗震、通信线路合理布置和可靠供电系统等。

(2)信息安全保障措施保障的是信息自身的机密性、完整性、真实性、可鉴别性和不可抵赖性。面临的主要威胁是信息窃取、篡改、仿冒和抵赖等。威胁的表现形式有黑客攻击、病毒、蠕虫和诈骗等。技术保障措施有身份认证、防病毒体系、访问控制、加密技术、安全协议和安全操作系统等。

(3)运行保障措施保障的是系统运行的可控性、可用性、可确认性，保证系统在满足服务需求的水平上稳定运行。主要面临的威胁有非法控制系统、拒绝服务攻击等。主要的技术保障措施有防火墙、入侵检测系统、安全审计技术等。

随着信息保障技术的不断发展，有一些保障技术设备拥有了多种保障能力。例如，有些防火墙设备集中了包过滤、防病毒、入侵检测和加密传输等多种功能。因此，难以从物理形态上对这些保障措施进行区分。所以，本文提出的信息保障评价模型输入量的保障措施为逻辑上的概念，是一定的保障功能和技术参数的集合，并非指的是物理设备。例如，定义防火墙就是一种执行网络过滤功能的保障措施，其技术参数有并发连接数、网络数据包处理速度、最大规则数、时延和包过滤算法等。

为了实现对保障措施自适应的反馈调整，需要对保障措施的保障能力进行度量。度量参考的指标就是每个保障措施自身的技术参数。度量方法可以采用序化度量的方式[17]。序化度量的思想就是采用一系列值，这些值表明由大到小或由小到大的顺序，并不是反映实际的大小或者实际的大小没有意义。例如，加密技术中按照密钥长度进行序化度量，可以分为 128 位、256 位、1024 位等几个级别。这样，当保障措施需要调整时，可以按照需要按升序或降序调整保障措施的具体参数。

就国家而言，保障的核心信息系统的重要性是有层次性和差异性的；就企事业单位而言，支撑其业务正常流转的各类信息、信息系统重要性也有差异。因此，构建信息安全保障体系需要针对信息和信息系统面临的威胁、信息的重要性、信息

系统的重要性和系统遭到攻击破坏后造成的危害程度等，依据国家制定的等级保护标准设定其保护等级，细化安全需求。只有通过科学分析，合理确定安全需求，才能真正实现科学合理的适度保障，既能避免保障不足造成的损失，又不会由于过度保障引起不必要的浪费。安全需求的量化描述就是依据信息安全属性的量化定义，各组织机构依据实际需求，给出所有信息安全属性的量化的需求底线。假设以概率方法定义信息安全属性，以机密性为例是：信息在操作过程中不会被捕获或捕获不被解密的概率，此时某组织对信息保障机密性的要求为95%，其含义就是信息保障系统要保障重要信息不被捕获或者捕获之后不被破解的概率不能低于95%[21]。

在图2所示的评价模型中，实际保障效果作为评价模型的输出量而存在，说明了保障措施和实际保障效果之间存在正相关性。简单来说，就是保障措施设置越到位，在一定时期内安全事件发生的次数就越少，安全事件造成的损失也越小。反之，如果实际保障效果不能满足组织对信息保障的要求，也就说明保障措施的设置存在缺陷，需要有针对性地调整。通过状态观测器测量的属性结果是一种带有预计性的保障能力评价，与实际的保障效果可能有偏差。因此，需要依据一定时期内统计的实际保障效果，有针对性地调整保障措施。实际效果反馈的是一种“亡羊补牢”的思想，信息保障体系在实际运行一定时期后，由于安全形势发生了改变，或者出现新的安全威胁等原因，需要对保障体系进行重新规划和设计[20]。

4 系统化评估方法

系统化的评估方法就是从战略、管理、工程和技术4个方面对信息系统的信息安全进行全面的评估。信息安全评价包括3个过程：静态评估、动态检测和状态监控。本文提出的信息系统信息安全评价方法如图3所示[18,22]。

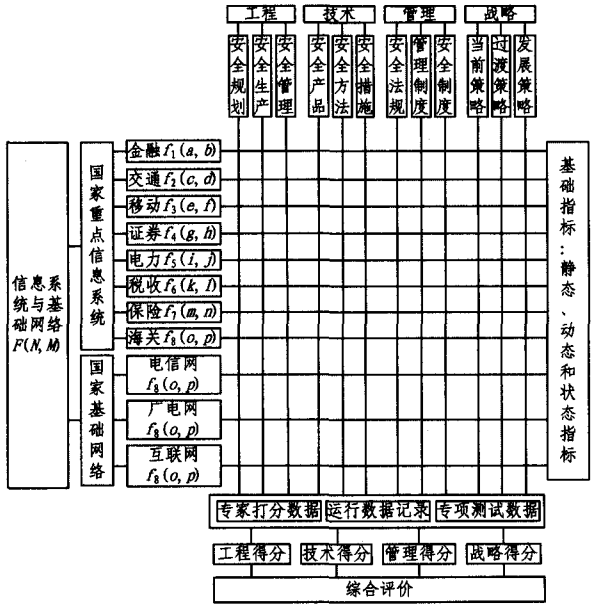

图3 信息系统信息安全评价方案

由上述思想，按照静态、动态和状态3种评价指标提取[22]，最终可以得到评价指标矩阵：

$$X=(x_{ij})_{mn}=\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix}$$

矩阵中的每一列都代表了某一指标 j 的 m 个数据。设 $\overline{X}_j$ 为第 j 个指标的平均值：

$$\overline{X}_j=\frac{[\sum_{i=1}^{m}x_{ij}]}{m},(j=1,2,\cdots,n)$$

权重矩阵：$W=[W_1,W_2,\cdots,W_i]^{\mathrm{T}}$。

各个指标对信息系统的影响不同。为体现各指标的重要性，需对各指标赋予不同的权值，以体现综合评价的合理性。

从上述看出，信息系统信息安全评价首先要建立系统化信息安全的评价指标体系，如图4所示[18,21]。

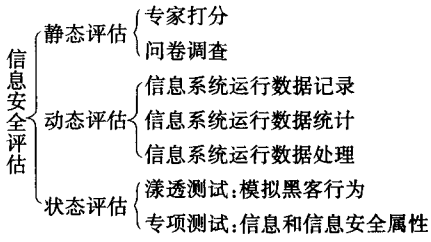

图4 系统化信息安全的评价指标体系

系统化信息安全的评价指标体系中，静态评估是通过专家打分和问卷调查得到的；动态评估是记录信息系统实际的运行数据，并对其进行统计和处理；状态评估是通过模仿黑客行为进行信息安全渗透测试，以及针对信息和信息系统的安全属性进行专项测试。

由于信息系统中因素繁多、复杂，并且许多因素之间相互关联，使判决产生了模糊，因此引入模糊判断矩阵：

$$U=\begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{m1} & \cdots & u_{mn} \end{pmatrix}$$

为了解决模糊问题，基于灰色理论中关联空间和光滑离散函数等概念，定义灰导数和灰微分方程，用离散数据列建立微分方程型的动态模型，即灰色模型GM(Grey Model)。它是本征系统的基本模型，而且模型非唯一。利用多级关联度分析法GRA即可解决信息系统中多层次之间、同层次中各个因素之间的模糊关联问题。

运用图3所示的评价方法进行信息保障评价的具体流程如图5所示[20]。

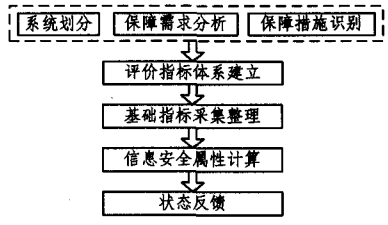

图5 信息保障评价模型工作流程

信息保障评价模型工作流程需要经过系统划分、保障需求分析、保障措施识别、指标体系建立、基础指标采集整理、信息安全属性运算和状态反馈等几个主要环节。其中，系统划分、保障需求分析、保障措施识别是评价准备阶段，为信息安全属性的计算提供基础数据。

结束语 系统化信息安全评价的思想是为确定一个评价信息安全工程实施的综合框架，提供评价度量与改善信息安全工程学科应用情况的方法。系统化评价模型及其评价方法可达到的目的：(1)确定信息安全保障工程的保障能力和目标；(2)完成信息安全保障工程的设计和建设；(2)决定信息安

全保障工程的投资决策;(3)建立信息安全保障工程的长效机制。系统化信息安全评价的方法适用于所有形式的信息安全保障工程,涵盖信息安全保障工程的3个方面:安全状态改善、防护能力评估和保障效果评价。

建立健全的信息系统的信息安全保障评估方法体系,是实施中国信息安全战略的重要保证。借助信息安全保障评价体系对我国的重点信息系统和核心业务系统进行统一分析和纵横比较,将有助于对我国信息安全防御态势做出量化的结论,为国家提供决策支持,对我国重点信息安全建设的规划、信息安全建设的投入,乃至信息安全管理政策的制定、信息安全技术的研究与发展都具有重要意义。因此,建立健全的国家信息安全保障评价体系是一项带有战略意义的任务。

参 考 文 献

[1] 国务院办公厅. 2006-2020年国家信息化发展战略[R]. 中共中央办公厅,2006:1-28

[2] 国家信息化领导小组. 加强信息安全保障工作的意见[R]. 2003:1-17

[3] 杨晨. 六大要素支撑我国信息安全保障体系—访信息安全专家曲成义[J]. 信息网络安全,2005,(3):11-12

[4] 曲成义,构建国家信息安全保障体系的思考[J]. 信息安全与通信保密,2004(5):20-21

[5] Systems Security Engineering Capability Maturity Model(SSE-CMM®): Model Description Document Version 3.0[R]. Carnegie Mellon University. June 2003

[6] 美国国家安全局信息保障解决方案技术处. 信息保障技术框架[M]. 北京:北京中软电子出版社,ISBN:7900057099,2002

[7] 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)

[8] 段海新,吴建平. 计算机网络的一种实体安全体系结构[J]. 计算机学报,2001(8)

[9] 黄遵国,卢锡城,王怀民. 可生存技术及其实现框架研究[J]. 国防科技大学学报,2002(2)

[10] Lu Xin, Ma Zhi. Information Assurance Evaluation for Network Information Systems[C]// 2006 International Conference on Computational Intelligence and Security. 2006,2:1528-1531

[11] 徐辉,冯晋雯,叶志远. 基于动态贝耶斯规划图的状态安全报警关联[J]. 北京大学学报:自然科学版,2006(1)

[12] 付钰,吴晓平,严承华. 基于贝叶斯网络的信息安全风险评估方法[J]. 武汉大学学报:理学版,2006(5)

[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)

[14] 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(10)

[15] 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)

[16] 孙旋,牛秦洲,等. 基于贝叶斯网络的人因可靠性评价[J]. 中国安全科学学报,2006(8)

[17] 赵文. 信息安全保障综合度量及综合评价研究[D]. 成都:四川大学数学学院,2000

[18] 吴志军,杨义先. 信息安全保障评价指标体系的研究[J]. 计算机科学,2010,37(7)

[19] 虞晓芬,傅玳. 多指标综合评价方法综述[J]. 统计与决策,2004(11):76-79

[20] 高伟. 基于状态观测的信息系统安全保障体系[D]. 中国民航大学,2010

[21] 方滨兴. 五个层面解读国家信息安全保障体系[EB/OL]. http://news.cnfol.com/090601/101,1587,5959421,00.shtml

[22] 国家信息中心. 信息安全保障评价指标体系[R]. 2005

(上接第44页)

$$c_1^* = h = g^t$$

$$c_2^* = h^r = (g^t)^r = (g^r)^t = R^t$$

$$c_3^* = m_b Z e(g,h)^a = m_b e(g_{n+1},h) e(g,h)^a$$

$$= m_b e(g^{a^{i+1}}, g^t) e(g,g^t)^a$$

$$= m_b e(g,g^t)^{a+a^{i+1}} = m_b A^t$$

因此,(c_1^*, c_2^*, c_3^*)是良定义的密文。从而$\mathcal{B}$以与$\mathcal{A}$相同的优势解决了判定性n-BDHE问题。

时间复杂度分析:在模拟过程中,$\mathcal{B}$的负担主要是计算$f(ID_j)$和$(\sigma_{i,j}, R_i, A_i)$。计算$f(ID_j)$需要$O(n)$个G中的指数运算,计算R_i需要$O(n)$个G中的指数运算,计算$\sigma_{i,j}$需要$O(n^2)$个G中的指数运算,计算A_i需要$O(n)$个G_T中的指数运算。因此算法$\mathcal{B}$的时间复杂度为$\tau' = \tau + O(n^2\tau_{exp})$,其中$\tau_{exp}$为$G$或$G_T$中的一个指数运算的时间复杂度。

结束语 基于多签名体制,提出了一个叛逆者可追踪的非对称密钥协商协议ASGKAwTT,从可证明安全性角度给出了协议在数学上的严格证明,从而保证了协议的安全性。本协议除了能满足基本的安全性要求外,还能有效实现叛逆者的追踪,有效解决了伍前红等人在2009年欧密会上提出的问题。ASGKAwTT协议只能抵抗被动攻击,可以利用KY编译器[9]将它们转换为抗主动攻击的密钥协商协议。

参 考 文 献

[1] Wu Qian-hong, Mu Yi, Susilo W, et al. Asymmetric Group Key Agreement[C]// Proc. of EUROCRYPT 2009. LNCS 5479, Berlin: Springer-Heidelberg, 2009:153-170

[2] 秦波. 基于对的群体密码学研究[D]. 西安:西安电子科技大学,2008

[3] Colin B, Manuel G N J. Round-optimal Contributory Conference Key Agreement[C]// Proc. of PKC 2003. LNCS 2567. Berlin: Springer-Verlag, 2002:161-174

[4] Mchoudary G, Colin B, Manuel G N J, et al. Generic One Round Group Key Exchange in the Standard Model[EB/OL]. http://eprint.iacr.org/2009/514

[5] Mchoudary G, Boyd C, Manuel G N J. One Round Group Key Exchange with Forward Security in the Standard Model[EB/OL]. http://eprint.iacr.org/2010/083

[6] Zhang Lei, Wu Qian-hong, Qin Bo, et al. Identity-based Authenticated Asymmetric Group Key Agreement Protocol[EB/OL]. http://eprint.iacr.org/2010/209.pdf, 2010

[7] Lu S, Ostrovsky R, Sahai A, et al. Sequential Aggregate Signatures and Multisignatures Without Random Oracles[C]// Proc. of EUROCRYPT 2006. LNCS 4004. Berlin: Springer-Heidelberg, 2006:465-585

[8] Brent W. Efficient Identity-based Ecnryption without Random Oracles[C]// Proc. of EUROCRYPT 2005. LNCS 3493. Berlin: Springer-Heidelberg, 2005:114-127

[9] Jonathan K, Yung M. Scalable Protocols for Authenticated Group Key Exchange[J]. Journal of Cryptology, 2007, 20:85-113