ISSE 在安全系统设计中的应用*)

谭兴烈[1] 周明天[2] 沈昌祥[3]

(四川大学数学学院 成都610064,成都卫士通信息产业股份有限公司 成都610041)[1]

(电子科大卫士通信息安全实验室 610054)[2] (海军计算技术研究所 100841)[3]

The Application of ISSE in Security System Design

TAN Xing-Lie[1] ZHOU Ming-Tian[2] SHEN Chang-Xiang[3]

(Mathematics College of Sichuan University, Chengdu 610064; Chengdu Westone Info Industry, Co. Ltd 610064)[1]

(Computer Sci&Tech College of Electronic Sci&Tech University 610054)[2]

(Navy Computing Institute 100841)[3]

Abstract ISSE is a kind of methodology in information system security designing and security management. In this paper, we first give simple discussions of the main steps and basic functions of ISSE, then we take a large scale network security system as an example to discuss how to use ISSE, and finally, we point out the importance of ISSE in designing security system and in security management.

Keywords System engineering(SE), Information system security engineering(ISSE), Information assurance technical framework(IATF), System review

1 引言

系统工程(SE)过程的原理是将问题与解决方案区分开来,问题代表了需求限制、风险、策略和其它解决问题的约束条件,解决方案代表了要完成的活动和需要创造的用来满足用户需求的产品。但要有一个评估体系来评估解决方案是否可以解决存在的问题,而这些评估是对问题和解决方案做出必要修正的基础。系统工程包括下面五个过程:发掘业务需求;定义系统功能;系统设计;部署系统和有效性评估[1]。

信息系统安全工程(ISSE)涉及到一个综合的系统工程环境中与 INFOSEC 工程实践有关的各个方面,它是这样一个过程:它分析用户的信息保障需求,是系统工程学、系统采购、风险管理、认证和鉴定以及生命周期的支持过程的一部分;是作为系统工程过程的一个自然扩展而给出的。这些过程都具有公共的要素:发现需求、定义系统功能、设计系统元素、开发和安装系统和评估系统有效性。ISSE 活动包括:分析并描述信息保障需求;在早期的系统工程过程中,基于需求而产生信息保障的要求;以一个可接受的信息保障的风险水准来满足要求;建立一个基于要求的功能性的信息保障体系;将信息保护功能分配到一个物理和逻辑的体系之中去;设计系统;部署信息保障体系;以成本、进度和操作的适宜性及有效性等因素,来平衡信息保障风险管理和其它的 ISSE 事项;研究与其它的信息保障和系统工程原则如何进行权衡;将 ISSE 过程与系统工程和采购过程相结合;测试系统以核实信息保障的设计,并验证信息保障要求;在实施完成后进行用户支持,并根据其需求进行调整[2,3]。

ISSE 在安全系统建设中变得十分重要,主要是因为如下几个原因:信息系统在政府、国防、国民经济各部门和私人方面的使用都有迅速的发展;当代信息系统存在的固有安全弱点、偶然或故意的滥用使信息的暴露随着信息访问的增多而增加,使得政府、国防和国民经济各部门、私人的信息和信息系统必须进行安全保护;技术的发展使得信息系统的建设方式正逐渐从建设专用系统转向集成商用/政府现货设备(COTS/GOTS)的新方向转移。在全生命期的每一阶段,运用 ISSE 过程的概念和功能的目的是确保所有信息系统安全(INFOSEC)的要求都得到满足。

本文首先简要介绍了 ISSE 的主要内容,之后结合具体实例分析了 ISSE 在系统安全设计中的应用。我们通过这个具体的实例可以看到,ISSE 在信息系统安全建设中可以发挥巨大的作用。

2 ISSE 的主要内容

2.1 概述

信息系统生命期安全工程包括9个阶段、6个基本功能,可以得到 MNS、ASR 等8个报告,参见图1。

2.2 ISSE 包括的九个主要阶段

·*先期概念阶段* 其目的是确定用户的任务需求,指出开始构建一个信息系统应具备的安全能力。先期概念阶段结束时要提出一份有效的任务能力需求报告(MNS)。MNS 中的内容不一定完全能实现,它只是一个目标。

·*概念阶段* 其目标是对一系列概念层面的信息系统安全方案进行探索,决定哪些方案可能满足任务要求,并从中选出要进一步讨论的方案。

·*要求阶段* 其主要目标是进一步发展上一阶段(即概念阶段)得出的信息系统安全需求和概念,总结出一份正式的信息系统安全需求报告。

在本阶段结束时,与信息系统建设的各个参与者一起,提出一份系统要求评审(即 SRR),它是一份包括系统所有需求

*)本文受973项目035801课题的资助。谭兴烈 博士,高工,主要研究方向为信息安全、电子政务、电子商务。周明天 教授,博导,研究方向为分布式计算、信息安全、中间件计算、移动计算。沈昌祥 研究员,工程院院士,博导,主要研究方向为信息安全、电子政务、电子商务。

指标的草案。

需求阶段要完成一份功能基线草案。正式的功能基线包括了一份初步认可的文件，文件对系统的功能、性能、互操作性、接口要求等做出了描述，还给出了系统是否达到这些要求的检验手段。

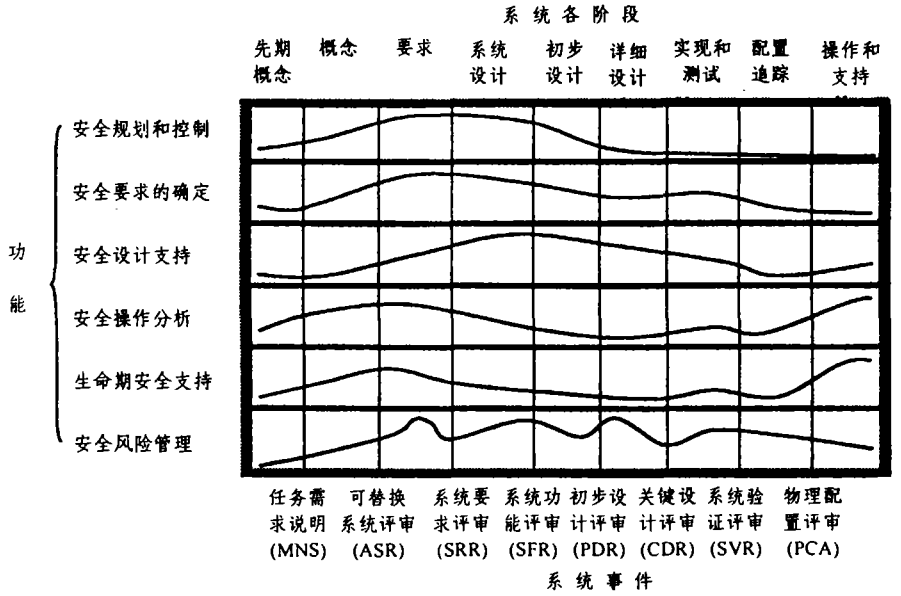

图1 ISSE 的功能、阶段及系统事件

·设计阶段 完成系统的顶层设计，决定组成系统的配置项(即 CIs)，确定系统指标。它是正式的工程活动的开始，是 CI 层面上管理的开始。本阶段以一份系统功能(设计)评审(即 SFR)结束。SFR 包含了正式开发活动开始前所必需的系统指标。系统设计阶段和紧接着的开发阶段都是由系统的开发/集成小组来进行。本阶段也进行与安全有关的活动。

·初步设计阶段 在此阶段，系统层面上的设计要求和指标都被分配到了配置项(CI)层面上了。初步设计评审(即 PDR)包括对每个系统配置项(CI)的硬件和软件的评审，系统各方面的问题都要加以考虑，各问题间的相互关系也应理顺。当成功地进行了 PDR 后，应为绝大多数系统配置项(CIs)建立起分配基线，此时初步设计阶段也就完成了。每个 CI 的分配基线包括了一些初步认可的文件，这些文件描述了 CI 的功能、性能、互操作性，与上层的接口要求，同层间的接口要求，设计限制、新的要求，以及这些限制和要求被解决后的确证手段。

·详细设计阶段 本阶段的任务是完成那些不能买到现成品的配置项的设计。在这一阶段，先要完成整个系统的关键设计评审(即系统的 CDR)。系统的关键设计评审(CDR)包括了构成系统的各配置项的具体设计，这些具体设计通常是一些相关的软件和硬件的设计评审与文件。在开始进行最终系统的实现以及下一步的测试前，系统工程各方面的问题都要加以考虑，各问题之间的关系也应理顺。本阶段也有与安全有关的活动。

·实现和测试阶段 无论是新开发一个系统或是进行系统修改，本阶段的主要目的是准备好手头没有的 CI 成品，组建出所有的开发 CI，将所有的 CI 集成为完整的系统，并且检查确认集成出的系统符合要求。在实现和测试阶段的最后要得到一份系统确认评审(即 SVR)，其中将指出所建的系统与要求一致，能满足任务要求。系统工程各方面的问题都应加以考虑，各问题之间的关系也应理顺。

·配置审计阶段 本阶段中，要进行一次系统层面的评审，把刚建好的系统和前面的系统文件记录相比较(这些文件中记录了系统应达到的指标)。通过系统层面的评审，确保系统的每个 CI 都接受了配置审计，所有大的偏差和问题都被发现了并得到了解决。

·运行和支持阶段 在此阶段，系统开始布署使用。本阶段要一直持续到系统拆除时为止。从系统发挥作用到最终拆除，ISSE 照常发挥作用，确保系统安全得到维护，它包括处理系统在现场运行时的安全问题和采取措施保证系统的安全水平在系统运行期间不会下降。

2.3 ISSE 的八个主要功能

·安全规划与控制 系统和安全项目的管理与规划活动从一个机构做出商业决策来承担特定工程就开始了。规划活动做得好，就能够为把安全要求系统地变换为有效的设计和实现提供坚实的基础。规划和准备活动为建立要求的可跟踪性、基准程序和客户确认提供了平台。

·安全需求的确定 系统特有的要求和定义一般在两个级别上做出：从用户角度给出高级操作要求定义；从系统开发者或集成者的工程观点提出更正式的要求规范的定义。

·安全设计支持 通过安全设计，一个被选择的系统体系结构被形式化，然后转换为稳定的、可生产的和有好的经济效益的系统设计。对信息系统而言，这种转换通常包括软件开发和软件设计，还可能包括信息数据库或知识库的设计。

"安全体系结构"提供了对安全服务，安全机制，安全特性的深刻理解，这些可用于满足系统的要求，能提供整个系统体系结构内什么地方可配置什么安全机制。系统体系结构的安全视图将集中在系统安全服务和高级安全机制，分配与安全有关的功能到系统分配置项、接口和较低级的部件，如有必要的话，还包括确认与安全有关的部件、服务和机制之间的相互依赖性，解决它们之间的冲突。

·安全操作分析 它将影响产品，特别影响过程和系统安全要求的解决方案。通过这一功能的反复应用与安全设计支持功能相组合，将确认"过程"安全解决方案。安全操作概念的分析和定义是系统工程和 ISSE 过程的集成的部分，是对安全认证和认可(C&A：Certification and Accreditation)的关键

输入。

·生命周期安全支持 SPO(系统项目办公室)将监督系统的整个生命期各阶段的计划,包括开发,生产,现场工作,维护,培训和处理。在操作和维护期间,在设计性能级,确认的操作可用详细准备的生命期支持计划及其实现来达到。

·安全风险管理 在系统工程过程中,风险是对达到属于技术性能,成本和进度方面的目的和目标的不确定性的一种量度。风险等级用事件和事件结果的概率来分类。对获取程度,系统在产品和过程方面进行风险评价。风险源包括技术方面的如可行性,可操作性,生产性,测试性和系统的有效性;成本和计划表方面的如预算,目标,里程碑等以及规划方面的如资源、合同。

系统风险管理是一个识别什么会出错,测定和评价有关的风险。对避开或处理被识别出的每个风险的适当手段进行实施或控制的一种有组织的分析过程。在系统定义,系统规范,系统设计,系统实现或系统操作和支持期内的任何时候都要识别出所存在的风险。技术风险管理计划是系统工程管理计划的基本部分。

3 ISSE 在安全设计中的应用

我们从上面对 ISSE 的讨论可以看出,ISSE 过程是作为系统工程过程的一个自然扩展而给出的。这些过程具有如下的公共的要素:发现需求、定义系统功能、设计系统元素、开发和安装系统、评估系统有效性[4~6]。

我们在设计某部委的大型安全系统时,就是按照 ISSE 的思想,充分考虑上述几个公共的元素来对安全系统进行设计、建设和维护的,可以提供全生命期的安全服务。

由于可能涉及到许多用户的秘密和部分技术秘密,在本文的论述中略去了特别具体的部分。

基于 ISSE 的思想,我们与用户一起确定了该系统比较合理的安全需求,定义了安全系统,设计开发并安装好了系统,对系统提供了有效性评估,并能提供相应的服务。具体地说:

在发现需求方面,我们与用户一起仔细分析了系统的网络情况(包括广域网、局域网及原有的内部局域网)和应用系统(各种视频、话音和数据应用,各种具体的业务应用)的情况,并与用户进行了充分的讨论,了解到要完成任务的信息保障需求,需要做下面的工作:需要保护所有在广域网上传输的信息,需要对 LAN 上的重要服务器实施访问控制,需要对重要的局域网进行访问控制,需要对重要信息实施细粒度访问控制(比如基于角色的访问控制),需要对一些重要的机密敏感信息进行应用层的加密保护(加密存储及加密传输),需要部署主动防御系统,能及时发现来自网络中的各种攻击,需要建设一整套病毒防范系统;对于信息管理的威胁方面,需要一套集中的密钥管理体系,并由专人组织管理,在信息保障政策方面,我们需要建设整个安全系统的具体保障政策和制度。

在定义系统功能方面,需要建立什么样的信息保障系统?信息保障系统如何实现良性运行?如何处理好信息保障系统的内/外部接口?我们具体考虑了如下的因素:信息保障目标(实施安全措施后我们要能达到的具体保证功能,即能保证什么);系统内部关联和环境(充分考虑了要建设的系统与现有内部系统,要建设的系统与外部网络系统之间的联系);信息保障要求(用户特别关注的安全要求,和我们依据经验从专家角度认为应该提供的安全要求);功能分析。依据上面我们定义的安全需求和系统需要的功能,我们就可以设计系统中的各种要素。

在设计系统要素方面,我们具体考虑了如下的因素:确保了一套较低水平的要求,使其可以满足系统级的要求(我们设计了一个最基本的要求集和一些依据经费等情况可选择的其它要求事项);支持系统级的架构、CI 和接口定义(依据自顶向下的设计思路,进行由粗到细的设计);依据系统对安全的不同要求,分步实施,支持长期的订/交货时间和早期的采购决定(在系统中我们特别强调分步实施);定义了信息保障核实和验证的程序和策略;考虑了信息保障运作和生命周期的支持问题;持续跟踪和细化信息保障相关的采购和工程管理计划及策略;持续系统细节的信息保障风险检查和评估;支持认证和鉴定过程,对整个设计方案进行了多次专家评审,依据专家意见进行了各方面的完善,并送国家有关部门进行认证和测评。

在开发和安装系统方面,我们具体考虑了:按照计划更新对于系统信息保障威胁的评估,以及对于系统运作状况的评估;核实系统信息保障要求以及实施解决方案的限制;跟踪、参与和应用信息保障担保机制;考查系统运行过程的进展情况,包括生命周期的支持计划;提供一套正式的信息保障评估系统;对于验证和鉴定过程的活动进一步增加内容;参与集体的、多学科的综合检查。具体内容包括采购、建设和测试三个阶段。在整个开发和安装系统方面,我们都进行了严密的组织和策划,充分考虑各种可能出现的情况。

在评估系统有效性方面,我们充分考虑了互操作性、可用性、培训、用户接口及成本等方面的因素。

在上述的几个方面,我们均做了相应的评审(REVIEW),特别是在系统设计完成后,我们组织了多位专家和用户单位的同志进行了多次评审,在系统完成后,严格地进行验收测试,制定一整套生命期服务的规范(制定了非常明确的售后服务计划,特别是建立了应急响应体系)。具体的工程实践告诉我们,只有按照 ISSE 所要求的去做,我们就可以更加科学地建设比较完善的安全系统。

结束语 ISSE 的许多思想目前已被吸纳到 IATF 的体系中[7,8]。目前国内有许多大型的网络系统已经建成或正在建设过程中,这些网络系统都必须建设成一个安全的系统,本人曾参与了多个大型安全工程的设计和建设,深感依据 ISSE 的思想来设计、来实施和来运行这些安全的系统,是十分必要和重要的。它能确保全生命期信息系统的安全,使用户对安全有更大的信心。由它为主线进行信息系统安全工程质量管理也是有重要意义的。

但是,在我国如何真正实现信息系统安全工程还需要信息安全行业的同行共同努力。

参考文献

1 关义章,蒋继洪,方关宝,戴宗坤. 信息系统安全工程学. 金城出版社,2000

2 DoD Directive 5200.40, DoD Information Technology Security Certification and Accreditation Process, (DITSCAP), Nov. 1997

3 Information System Security Policy Guidelinea: [I942-TR-003]. 1994

4 Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.1, CCIMB-99-031, Aug. 1999

5 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 2.1, CCIMB-99-032, Aug. 1999

6 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.1, CCIMB-99-033, Aug. 1999

7 谭兴烈. 信息保障在安全系统设计中的应用. 信息安全与通信保密,2001(10)

8 National Security Agency. Information Assurance Technical Framework