可信安全体系实施的工程化途径

沈玲玲, 盛荷花, 钱 钢

(南京师范大学 管理科学与工程系, 江苏 南京, 210097)

[摘要] 对建立可信安全体系所面临的问题进行了分析, 给出必须在可信安全体系全生命周期中引入工程化、体系化方法的理由. 在此基础上提出了基于过程的可信安全工程化模型以及该模型指导下的可信安全基线实施途径, 对可信安全工程化进行了有益的探讨.

[关键词] 可信安全, 可信安全工程化模型, 实施途径

[中图分类号] TP309 [文献标识码] A [文章编号] 1672-1292(2010)03-0069-05

Engineering Approaches to Implementation of Trusted Security System

Shen Lingling, Sheng Hehua, Qian Gang

(Department of Management Science and Engineering, Nanjing Normal University, Nanjing 210097, China)

Abstract This paper analyzes the problems of how to establish trusted security system, and gives the reasons of leading engineering and systematic method into the full life-cycle of trusted security system. On this basis, we propose a process-based model for trusted security system and approaches to implementation trusted security baseline under the guidance of the model. Trusted security engineering approach is usefully discussed at last.

Key words trusted security; trusted security engineering model; implementation approach

随着信息化建设的全面展开, 可信安全体系的开发和运行环境已从静态封闭转化为动态开放. 在开放多变的环境中, 安全体系的可信度变得越来越低. 针对可信机制与环境问题, 国内外从硬件、软件和网络等层面进行了广泛的研究. 文献[1]采用可信安全技术构建一种基于硬件的保护机制, 以解决移动代理系统中恶意主机的问题. 文献[2]提出了一种现场可编程门阵列(FPGA)的可信平台硬件配置信息的测量方法. 文献[3]着重在可信计算机制中应用了一种安全系统属性的逻辑结构. 文献[4]提出了一种面向可信计算应用的兼容模型. 文献[5]对可信计算的研究动态进行了调研, 对该领域的相关技术进行了归类及介绍. 文献[6]结合动力系统的基本思想探讨了软件系统在动态开放环境下的可信特性.

从技术上看, 目前国内对可信安全的研究和应用才刚刚起步, 缺乏有效的技术实现与工程管理措施, 尤其是缺乏适合中国国情的可信安全体系的指导. 从市场上看, 安全产品品种繁杂, 功能和可信度相差很大. 由于设备资源特别是安全设备资源的配置不当, 可信安全的整体性得不到保证. 从方法上看, 评估系统的安全性主要是依靠建成后的整体测试, 而不是采用过程中的可信安全控制. 这样某些隐患随着系统的建成将无法弥补.

建立基于结构化 TCB的安全技术体系需要对安全产品的开发、评价、实施以及安全服务的过程进行管理, 使之成为一个具备完好定义的、成熟的、可测量的过程, 执行此类过程的组织开发实施的产品或系统以及提供的服务, 才具有较高安全可信度和可重复性. 由于可信安全涉及面广、性质复杂, 整个活动贯穿于信息化建设的全部生命周期, 因而是一个复杂的系统工程、社会工程.

1 基于过程的可信安全工程化模型

可信安全体系的实施是多层次的. 它包括可信安全产品构造与验证、可信安全体系实施过程和维持可

收稿日期: 2010-06-28
基金项目: 铁道部信息技术中心专项基金(Y-2009-004).
通讯联系人: 沈玲玲, 讲师, 研究方向: 可信安全. E-mail: llshen509@163.com

信安全状态的运行管理等层次. 可信安全体系的建立是动态的, 它随信息技术发展而呈现一个周期性的控制过程. 由于可信安全体系的多层次性和动态性, 因而是一个基于过程的系统工程性问题. 因此希望能够通过一种过程性控制来保证可信安全其可信度的稳定性. 这种控制包括可信安全产品构造与验证的安全保证、可信安全体系实施过程的安全保证和维持可信安全状态的运行管理的安全保证. 为此, 通过引入基于过程的、动态控制的可信安全工程化模型, 作为可信安全体系实施途径的理论依据, 用于指导建立可信安全体系的具体管理工作.

可信安全的工程化是一个复杂且至关重要的问题, 需要采取科学的、脚踏实地的系统化方法去解决. 实际上, 对可信安全产品的研究开发或选择应用都只是可信安全实践活动中的一部分, 只是实现可信安全需求的手段而已. 可信安全更广泛的内容还包括制定完备的可信安全度量标准、建立行之有效的工程化途径等等. 只有这样, 才能在采用可信的过程控制机制的基础上根据需求开发或选择安全技术产品, 并按照既定的安全策略和流程规范来实施、维护和评价可信安全控制措施, 从而保证可信安全目标的实现. 就实现可信安全目标的作用方面, 可信安全工程化的实践价值远大于它的理论价值. 缺少或未采用这类过程的产品研制和系统实施, 不能称之为是可信安全产品或系统, 任何一个环节缺乏或弱化都将降低其最终的可信度, 造成与期望目标的偏差.

基于过程的可信安全工程化模型建立在统计过程控制理论基础之上. 统计过程控制理论发现, 所有成功的管理, 其共同特点都是具有一组定义严格、管理完善、可测可控而高度有效的工作过程, 因而这些控制过程具有连续性、可重复性和有效性. 可信安全工程化模型从中抽取“关键的”工作过程并定义过程的“能力”. 一个过程的能力是指通过执行这一过程所可能得到结果的质量变化范围. 其变化范围越小, 过程的能力越“可信”; 反之则越“不可信”. 可信安全工程化模型运用了上述的概念, 它力图通过对系统可信安全进行过程管理的途径将可信安全体系转变为一个完好的、可测量的先进学科.

可信安全体系的实施之所以难以直接测控, 除安全的渗透性使可信安全系统建设成为一项复杂的系统工程外, 另一原因是可信安全系统的评定不仅要求对系统可信安全功能加以评测, 也要求对系统的安全可信度进行评测. 为此模型将可信安全工程化途径分为 3个相互联系的部分: 可信安全产品构造与验证工程化、可信安全体系实施过程工程化和可信安全运行管理工程化. 模型针对这 3个部分定义若干项关键过程(KPA), 并为每个过程定义了一组完成该过程必不可少的确定的基本实践. 同时模型还定义了 5个可信能力等级, 每个等级的判定反映为一组共同特性. 只有某一级别的所有共同特性都得到满足时, 该过程的能力才达到对应的可信能力级别. 从整体上看, 可信安全工程定义了一个“二维”架构(如图 1所示), 横轴是若干个建立可信安全所需的关键过程域, 纵轴是 5个可信能力等级. 如果给每个过程域赋予一个能力等级的评定, 所得到的“二维”图形便形象地反映了可信安全工程化中某一部分其可信能力的高低, 也间接地反映了可信安全工程的质量, 而且为可信能力提高指出了方向.

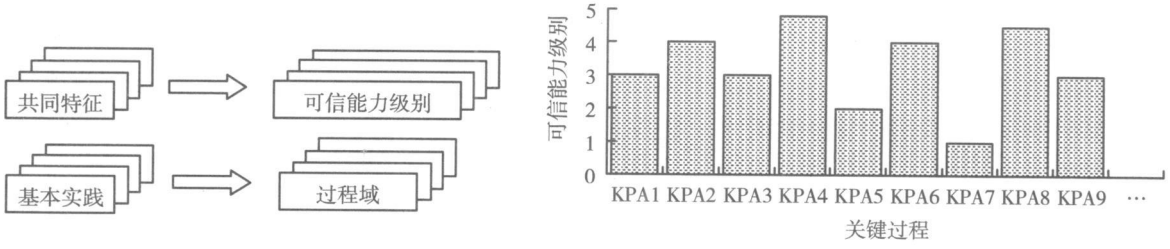

图 1　可信安全工程化模型

Fig.1　Trusted security engineering model

由此可见, 可信安全工程化模型本身并不是安全技术模型, 但它给出了可信安全工程化需考虑的关键过程域, 可指导可信安全从单一的安全设备配置转向系统地解决整个体系的产品研发、验证、安全目标、策略形成、安全方案、实施、评估和生存周期控制等问题, 从而可以将复杂的可信安全体系转变为严格的具有可操作性的、可依赖的工程体系.

面向可信安全全生命周期的可信安全工程化过程包含 3方面内容:

(1) 保证 TCB功能正确性和可靠性的可信安全产品构造与验证工程化. 可信安全产品要遵循相同的

行业标准, 降低可信的复杂性, 并获得指定认证机构的认可. 构造与验证可信安全产品 (软件、硬件、网络) 过程中应采用系统工程方法, 尤其在可信安全产品的建模、构造方法与生成技术、可信需求规约在设计中的精化方法、基于不可信构件构建可信安全系统的方法和技术等关键方面.

(2) 保证 TCB 来源真实性、功能与策略符合性的可信安全实施过程工程化. 通过一体化的管理和技术, 实现在标准框架下的各类技术融合和协同工作, 建立对 TCB的真实性、TCB 功能的正确性和可靠性的信心.

(3) 保证目标系统一直处于期望可信安全状态的运行管理工程化. 可信安全运行管理工程化, 以保证目标系统一直处于可信安全状态. 由于计算技术的发展与组织的变动, 不可能保持一个绝对安全而可信的计算环境, 也不可能避免安全事件的发生. 一个有效的可信安全体系应该做到把安全事件所造成的影响限制在最小, 而且具备对组织变化和安全事件的快速反应能力.

2 可信安全工程化模型的实施途径

从可实施性出发, 可以规定一个用于过程管理的可信安全基线, 并尽量提高其精确度. 可信安全基线是一个系统至少需要满足的安全目标. 此外还可以通过基线库状态对系统进行不间断的监控, 以保证安全风险不至于增大到不能接受的程度.

在可信安全工程化中可信安全基线的制定是核心, 不同性质和安全需求的信息系统其安全基线是不同的 (如图 2所示). 在此给出可信安全工程实施阶段安全基线的 6条制定原则作为应用参考.

图 2 可信安全工程化途径

Fig.2 Trusted security engineering approach

2 1 可信安全需求基线

其目标是明确指出与可信安全相关的需求. 该需求基线是系统的可信安全基础, 应同时满足所有合法的、政策的、组织的可信安全需求. 它是根据系统运行背景、当前的系统环境和已定义的可信安全目标来制定的, 其目标在于:

(1) 收集所有必需的信息来理解用户的可信安全需求;

(2) 收集影响系统可信安全的所有法律、政策和商业标准等外部影响;

(3) 定义一套说明, 这些说明描述了系统中要实现的保护. 确保每个可信安全需求与政策、法律、标准以及系统限制一致;

(4) 使用户需求 (包括非技术手段的需求) 在可信安全方面形成一致.

2 2 可信安全输入基线

其目标是给实施者或用户提供所需要的可信安全信息, 包括可信安全架构、设计和可选的实现方案以及可信安全指南, 可细分为:

(1) 给实施者和用户提供所需要的可信安全信息和标准定义;

(2) 针对可信安全目标和限制, 做出工程选择;

(3) 确定相关工程问题的可能的解决方案;

(4) 确定所选择的可信安全工序的优先次序;

(5) 给其他相关工程提供相关可信安全指南, 包括安全架构、保护原则、设计标准、验证标准;

(6) 给系统用户和管理者提供相关可信安全指南, 包括管理者手册、用户手册、安全描述、系统配置指导.

2 3 协同可信安全基线

其目标是为了保证可信安全工程是整个信息化工程的一个完整部分. 因为可信安全工程不可能在孤立的情况下取得成功. 这种协同包括与所有相关工程的开放性交流, 可细分为:

(1) 定义可信安全工作组与其他工作组之间的协同目标和关系, 定义会议议程、目标、行动主题;

(2) 确认可信安全工程与其他相关工程的协同机制, 以确保交流计划、会议报告、消息、备忘录、文本、

决定和建议的形式标准化;

(3) 实现可信安全工程与其他相关工程协同实施,确定不同工程实体解决冲突的有效办法;

(4) 使用规范的确认机制来协同与可信安全相关的其他工程.

2.4 可信安全管理基线

其目标是为了保证被整合在系统中的可信安全机制能够在系统的执行中有效地工作,可细分为:

(1) 确定和文档化安全控制的责任并传达到相关的每一个人;

(2) 定义可信安全控制的有关软硬件配置管理;

(3) 对所有用户和管理人员进行培训、教育,以提高他们的可信安全意识;

(4) 对可信安全服务和控制机制进行定期维护和审核.

2.5 可信安全保证参数基线

其目标是为了提供满足相关标准的参数,表明用户的可信安全需求已被满足,可细分为:

(1) 确定可信安全保证目标;

(2) 定义可信安全保证策略,确定策略足以应付影响可信安全的风险;

(3) 保存可信安全保证证据(如工程记录、运行记录、测试结果、证据日志);

(4) 可信安全保证证据的分析.

2.6 监视可信安全态势基线

其目标是确保能够识别与报告潜在的导致对可信安全的破坏、破坏企图和过失.因此与系统可信安全相关的事件均要得到检测与跟踪,突发事件须得到响应.为了保证可信安全目标,须识别与处理系统运行中的可信安全态势的变化,可细分为:

(1) 周期性监视内外部环境的变化;

(2) 定义、识别与可信安全相关的事件;

(3) 分析事件记录来决定事件的起因、事件的进展与未来可能的事件,以识别必要的可信安全变化;

(4) 周期性检查可信安全设备的性能与功能的有效性;

(5) 管理可信安全应急响应计划,包括应急响应的测试与维护;

(6) 确保与可信安全事件相关的所有记录得到适当的保存.

2.7 实施可信安全基线的收益

通过实施上述可信安全基线,可获得以下收益:

(1) 通过可信安全体系实施的工程化,由于构建了大量的流程文档,为组织开展各项与可信安全相关的活动提供了明确的目标和操作指引;

(2) 通过可信安全体系实施的工程化,进一步明确分工,使安全风险和责任意识从传统的 IT部门扩展到组织每个员工,提高了可信安全的整体效果;

(3) 通过可信安全体系实施的工程化,组织的 IT部门能够有效控制成本,提高可信安全水平和用户的满意度;

(4) 通过构建静态的组织保障体系和实施动态的对整个体系进行调整、改善过程,使可信安全实施从“静态、被动、散乱”向“动态、主动、系统”的过程转变.

3 结语

采用工程化途径实施可信安全体系,是可信安全产业化的关键.该方法通过全过程、全方位地控制安全事件,同时又与信息系统的常规建设过程相结合,从而有针对性地解决了可信安全的动态性和广泛性.它从宏观上将可信安全融入到整个组织的政策中以加强可信安全的现实性,同时它也引入了业务持续性管理、符合性等措施,将可信安全与组织的业务紧密联系在一起.下一步必须加强对可信安全工程化实现的研究,因为可信安全工程化模型只是一个理论指导模型,如何根据不同性质的信息系统,采取不同的具体实施方案,值得进一步探讨.

[参考文献] (References)

[1] Datta A, Franklin J, Garg D, et al. A logic of secure systems and its application to trusted computing[J]. Security and Privacy, IEEE Symposium, 2009, 30: 221-236.

[2] Munoz A, Mana A, Serrano D. The role of trusted computing in secure agent migration[C]// Research Challenges in Information Science, Third International Conference: Fez, 2009: 255-264.

[3] Glas B, Klimm A, Muller-Glaser K D, et al. Configuration measurement for FPGA-based trusted platforms[C]// Proceedings of the 2009 IEEE/IFIP International Symposium on Rapid System Prototyping. Washington DC: IEEE Computer Society, 2009: 123-129.

[4] Zhu Lu, Yu Sheng, Zhang Xing, et al. Formal compatibility model for trusted computing applications[J]. Wuhan University Journal of Natural Sciences, 2009, 14(5): 388-392.

[5] 龚敏明, 石志国. 可信计算及其安全性应用研究综述[J]. 江西师范大学学报: 自然科学版, 2009, 33(3): 348-352.
Gong Minming, Shi Zhiguo. The research survey of trusted computing and its application of security[J]. Journal of Jiangxi Normal University: Natural Science Edition, 2009, 33(3): 348-352. (in Chinese)

[6] 郑志明, 马世龙, 李未, 等. 软件可信性动力学特征以其演化复杂性[J]. 中国科学 (F辑): 信息科学, 2009, 39(9): 946-950.
Zheng Zhiming, Ma Shilong, Li Wei, et al. Kinetics characteristic and complexity of evolution of software trustworthiness[J]. Science in China(F): Information Science Edition, 2009, 39(9): 946-950. (in Chinese)

[责任编辑: 严海琳]

(上接第 59页)

[2] Skowron A. Extracting laws from decision tables: A Rough set approach[J]. Computational Intelligence, 1995, 11(47): 371-388.

[3] 王锡淮, 张腾飞, 肖健梅. 基于二进制可辨矩阵的决策规则约简算法[J]. 计算机工程与应用, 2007, 43(27): 178-180.
Wang Xihuai, Zhang Tengfei, Xiao Jianmei. Algorithm for decision rules based on binary discernibility matrix[J]. Computer Engineering and Application, 2007, 43(27): 178-180. (in Chinese)

[4] 桂现才. 简化的二进制差别矩阵属性约简算法的改进[J]. 计算机工程与设计, 2007, 28(16): 3971-3973.
Gui Xiancai. Improved algorithm for attribute reduction based on simple binary discernibility matrix[J]. Computer Engineering and Design, 2007, 28(16): 3971-3973. (in Chinese)

[5] 程京, 朱靖, 张帆. 一个基于差别矩阵的属性约简改进算法[J]. 湖南大学学报: 自然科学版, 2009, 36(4): 85-88.
Cheng Jing, Zhu Jing, Zhang Fan. An updated algorithm for attribute reduction based on discernibility matrix[J]. Journal of Hunan University: Natural Science Edition, 2009, 36(4): 85-88. (in Chinese)

[责任编辑: 严海琳]