系统安全工程中信任度评估模型和方法*)

The Assurance Appraisal Model and Method in Systems Security Engineering

蔡皖东

(西北工业大学计算机科学与工程系　西安710072)

Abstract The assurance appraisal is import part of compose of security product validate, it can be assessed by both finally products-oriented method and engineering process-oriented method. The engineering process-oriented method uses the Systems Security Engineering Capability Maturity Model (SSE-CMM), it establishes assurance of security products developed in the organization by assessing security engineering capability maturity of an organization, the assess result bas continuity, repeatability and validity. It can simplifies the validate practice. In this paper, the SSE-CMM and its appraisal method are discussed.

Keywords Systems Security Engineering, Assurance Appraisal, Systems Security Engineering Capability Maturity Model (SSE-CMM)

1 引言

随着Internet的普及,人们在享受网络所带来方便和效益的同时,面临着信息安全方面的巨大挑战、计算机病毒、黑客攻击、信息非法获取等对网络信息系统安全带来严重威胁,并造成了巨大经济损失。因此,网络信息安全问题已引起包括我国在内的世界各国政府的普遍关注,并投入巨资开发安全产品,以保护网络信息系统的安全。

网络信息系统安全涉及诸多领域和学科,必须按照系统工程的方法来解决。系统安全工程旨在分析企业存在的安全风险,建立相平衡的安全需求,通过融合各种工程学科将安全需求转换为贯穿系统整个生命周期的工程实施指南。系统安全工程活动的生命周期包括概念定义、需求分析、系统设计、开发、集成、安装、操作、维护,甚至系统退役,将涉及众多安全方面的问题,如计算机安全、网络安全、通讯安全、信息安全、操作安全、管理安全、物理安全、辐射安全和人员安全等。系统安全工程还需要证实安全机制的正确性和有效性,证明系统安全的信任度能够达到用户的要求,或系统遗留的安全脆弱性及风险是在用户所容许的范围之内。

通常,一个组织或企业开发的安全产品必须通过严格的测评认证后才能进入市场,被用户所接受。在安全产品测评时,除了要对产品的安全功能进行测评外,还要对产品的安全信任度(Assurance)进行评估,所谓的信任度是指用户对一个安全产品正确执行其安全功能的信任程度或信心大小,这显然不是一个能直接加以测量的物理量。目前,安全产品信任度评估方法主要有两种:面向最终产品的方法和面向工程过程的方法。

面向最终产品的评估方法主要通过对产品及其所有文档的严格分析和测试来建立信任度指标。这种方法缺少继承性,被测产品的安全信任度与同一组织以前所开发产品的安全信任度并无直接关系,每个产品的评测都要从头做起,评测过程相对复杂和冗长,增大评测的开销。

面向工程过程的评估方法采用系统安全工程能力成熟度模型(Systems Security Engineering Capability Maturity Model,SSE-CMM)来评估一个组织或企业从事安全工程的能力,该模型定义一组关键工作过程作为过程能力,通过执行这些过程来评估一个组织的能力成熟度,其执行结果的质量变化范围越小,说明该组织的工程能力越成熟,其产品质量的一致性就越高,而工程风险就越小;反之亦然。通过对一个组织的能力成熟度的评估,建立对该组织所开发安全产品的信任度,可以大大简化对安全产品的认证实践。然而,这种方法并不能完全取代对最终产品的测评和认证。如果将两种方法有机结合起来,则会加快安全产品的评测过程,节省大量的开销。本文主要论述SSE-CMM模型及其评估方法。

*)国防基础研究基金资助项目,蔡皖东　教授,博士,主要研究方向:计算机网络、网络信息安全和多媒体通信等。

2 SSE-CMM 模型

一个组织或企业从事工程的能力将直接关系到工程和产品的质量。国际上通常采用能力成熟度(Capability Maturity Model,CMM)模型来评估一个组织的工程能力,CMM 模型是建立在统计过程控制理论基础上的,统计过程控制理论发现,所有成功企业都有共同特点:具有一组定义严格、管理完善、可测控的工作过程。CMM 模型认为,高能力成熟度的企业持续生产高质量产品的可能性很大,而工程风险则很小。

为了将 CMM 模型引入到系统安全工程领域,1994年4月美国国家安全局、美国国防部、加拿大通信安全局以及60多个著名公司共同启动了面向系统安全工程的能力成熟度模型(SSE-CMM)项目,该项目力求在原有 CMM 模型的基础上,通过对安全工程进行管理的途径将系统安全工程转变为一个具有良好定义的、成熟的、可测量的先进工程学科。1996年10月,SSE-CMM 模型的第一个版本问世。项目主管单位选择了5家公司对该模型进行了长达一年的试用,并依据试用中积累的经验对模型进行了多次修改。SSE-CMM 2.0版本于1998年10月公布,并提交给国际标准化组织申请作为国际标准。

2.1 基本概念

SSE-CMM 模型将各种各样的系统安全工程任务抽象为11个有明显特征的子任务,而完成一个子任务所需要实施的一组工程实践称为一个过程域。SSE-CMM 模型为每个过程域定义了一组确定的基本实践(Basic Practice),并规定每一个基本实践都是完成该子任务所不可缺少的。

一个组织每次执行同一个过程时,其执行结果的质量可能是不同的。SSE-CMM 模型将这个变化范围定义为一个组织的过程能力。对于"成熟"的组织,每次执行同一任务结果的质量变化范围比"不成熟"的组织要小。为了衡量一个组织的能力成熟度,其过程完成的质量必须是可度量的。为此,SSE-CMM 模型定义了5个过程能力级别,每个级别用一组共同特性来标识,每个共同特性则通过一组确定的通用实践来描述。

这里的组织是指执行过程或接受过程能力评估的一个组织机构。一个组织可以是整个企业、企业的一个部门,或者是一个项目组。

SSE-CMM 模型是 CMM 模型在系统安全工程领域中具体应用而派生的一个变种。SSE-CMM 模型在系统安全工程领域中抽取了一组"良好"工作实践,定义了11个"良好"安全工程过程域,这11个过程域可能出现在安全系统生命周期的各个阶段,为此 SSE-CMM 模型并没有规定它们之间的顺序,SSE-CMM 模型所设置的5个能力成熟度级别都是由一组能反映过程能力变化的通用特征来定义的,这些通用特征适用于所有过程域。

总之,SSE-CMM 模型定义了一个两维的框架结构,横轴上有11个安全工程过程域,纵轴上有5个能力级别,如果对每个过程域都进行能力级别评分,则可以得到一个两维图形,参见图1。

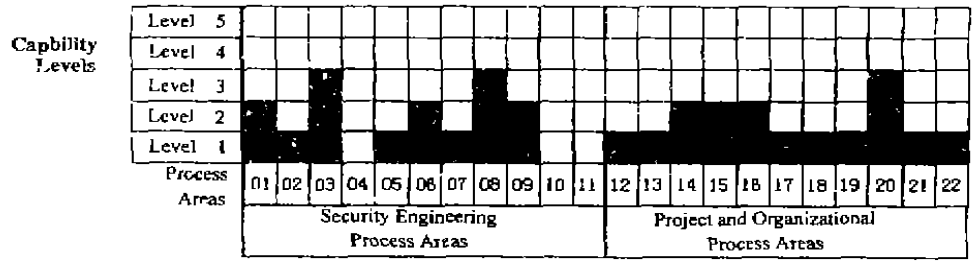

图1 SSE-CMM 模型的两维框架结构

图1形象地反映了一个组织整体上的系统安全工程能力成熟度,也间接地反映了这个组织工作结果的质量及其工作结果在安全上的信任度。

2.2 过程域

系统安全工程涉及到:安全工程、项目(Project)和组织三种过程域。后两个过程域并不直接与系统安全相关,故不是该模型的一部分,而是在系统工程能力成熟度模型(SE-CMM)中定义。SE-CMM 模型也是 CMM 模型的一个变种,同样定义了11个过程域,通常与 SSE-CMM 模型的11个过程域一起用来共同量度一个组织的过程能力成熟度。这些过程域如下:

(1)SSE-CMM 过程域

- PA01:管理安全控制
- PA02:评估影响
- PA03:评估安全风险
- PA04:评估威胁
- PA05:评估脆弱性
- PA06:构造信任度论据

·PA07:协调安全
·PA08:监督安全态势
PA09:提供安全输入
·PA10:说明安全需求
·PA11:校验和验证安全
(2)SE-CMM 过程域
·PA12:保证质量
·PA13:管理配置
·PA14:管理工程风险
·PA15:监督和控制技术成就
·PA16:监督和控制技术成就
·PA17:定义组织的系统工程过程
·PA18:改进组织的系统工程过程
·PA19:管理产品线进展
·PA20:管理系统工程支持环境
·PA21:提供正进行的技能和知识
·PA22:协调和补充

SSE-CMM 模型将系统安全工程过程分为三类:风险过程、工程过程和信任度过程。

风险是发生了某种不希望的事件并对系统造成影响的可能性。根据模型,能够成为风险的事件有三个组成部分:威胁、系统脆弱性和事件造成的影响。一般而言,这三种因素必须全部存在才足以构成风险(使风险值大于零)。例如,不安全的系统但无威胁存在、不幸事件发生但没有造成影响等都不视为是风险。系统风险分析建立在对威胁、系统脆弱性和事件影响分析的基础上。而通过系统中的安全机制可将系统遗留的风险控制在可接受的程度内。模型中定义了4个风险过程:评估影响(PA02),评估安全风险(PA03),评估威胁(PA04)和评估脆弱性(PA05)。

安全工程不是一个独立的实体,而是系统工程的一个组成部分。例如,安全系统集成通常是系统集成的一个组成部分。SSE-CMM 模型强调系统安全工程与其它工程学科的合作和协调,并定义了专门的安全协调过程域(PA07)。在一个工程项目的初始阶段,承担工程的组织必须根据风险分析结果、有关系统需求、可应用的法律法规和方针政策等信息,与客户一起共同定义系统的安全需求,这一过程称为说明安全需求过程域(PA10)。在综合考虑了包括成本、性能、技术风险及使用难易程度等各种因素后,提出解决问题的方案,这一过程称为安全输入过程域(PA09)。然后,该组织必须保证其安全机制的正确配置和正常运行,这一过程称为管理安全控制过程域(PA01)。同时,对系统进行连续的监测,以保证新风险不会增大到不可接受的程度,这一过程称为监督安全态势过程域(PA08)。

在信任度问题上,SSE-CMM 模型强调对执行安全工程过程结果质量的可重复性信任度,信任度过程不增加额外的系统安全机制,只是通过校验和验证现有系统安全机制的正确性和有效性来实现,这一过程称为校验和验证安全过程域(PA11)。并且允许借鉴其它各个过程域的工作产品来构造系统安全信任度论据,这一过程称为构造信任度论据过程域(PA06)。

SSE-CMM 模型并没有规定各个过程域在系统安全工程生命周期中出现的顺序,某些过程域甚至可能重复出现在生命周期中的几个阶段。实际上,过程域是依照过程域名的英文字母顺序来编号的。

2.3 过程能力

过程能力由一组通用实践(GP)来评估。通用实践是对所有过程都通用的工程实践。通用实践按其具有的共同特性及能力级别构成三级结构:通用实践;共同特性;能力级别。注意,过程能力是用来度量每个过程域的,而不是用来度量整个组织的。SSE-CMM 模型定义了如下5个能力级别:

·Level 1:非正式执行的过程。它仅仅要求一个过程域的所有基本实践都被执行,而对执行的结果并无明确的要求。

·Level 2:计划并跟踪的过程。它强调过程执行前的计划和执行中的检查。这使得一个组织可以根据最终结果的质量来管理其实践活动。

·Level 3:良好定义的过程。它要求过程域所包括的所有基本实践都必须依照一组良好定义的操作规范来进行。这组规范是一个组织依据长期工作经验制订出来的,其合理性是经过验证的。

·Level 4:定量控制的过程。它能够对一个组织的表现进行定量的度量和预测,使过程管理成为客观的和准确的实践活动。

·Level 5:持续改善的过程。它为过程行为的高效化和实用化建立定量的目标,可以准确地度量过程的持续改善所收到的效果。

SSE-CMM 模型围绕这5个能力级别定义了12个共同特性。对共同特性的评测可以清楚地反映出过程能力的成熟度是否发生了实质性的变化。

当一个组织不能执行一个过程域中的基本实践时,该过程域的过程能力是0级。0级不是一种真正意义上的能力级别,不包含任何通用实践,也不需要测量。

2.4 过程能力评估方法

运用 SSE-CMM 模型评估一个组织的过程能力可采用两种方法:自我评估和第三方评估。

一个组织可以运用 SSE-CMM 模型自我评估每个过程域的能力级别,评测结果可作为改善其过程能力的理论依据和目标。

(下转第105页)

PDU 进行解密处理[5]：

```
statusInformation=
    ——处理结果指示成功或失败
decryptData(
        IN decryptKey
            ——用户加密密钥
        IN privParameters
            ——加密协议相关参数
        IN encryptedData
            ——加密数据
        OUT decryptedData
                ——解密以后的数据
)
```

若加密模块出现错误，则消息不能进一步处理，usmStatsDecryptionErrors 计数器增一，返回解密失败错误指示及该计数器的 OID/value 给调用模块；若处理成功，则将解密得到的数据返回给调用模块；

b)若安全级别指示消息没有经过加密处理，则直接将消息返回给调用者；

(9)计算响应消息允许的 PDU 最大长度；

(10)根据消息中的用户名字段从基于用户的安全模型的用户信息表中读取用户的安全名(securityName)；

(11)将与该消息相关的安全数据缓存下来，以供响应消息处理时使用。与对应的请求消息相同的安全参数，要缓存如下信息：msgUserName，usmUserAuthProtocol，usmUserAuthKey，usmUserPrivProtocol，usmUserPrivKeysecurity，EngineID，和 securityLevel；

(12)处理结束，返回调用子系统处理成功信息和消息中的 PDU 部分。

结束语 SNMPv1-2都采用了基于共同体名串的简单安全模型，其安全性能很差。虽然在 S-SNMP，SNMPv2P 和 SNMPv2u 分别提出了基于参加者(party)和基于用户的安全模型，但由于其操作复杂臃肿，与 SNMP 强调简单性的设计思想背道而驰，故没有在工业界得到实现和广泛支持。SNMPv3的提出既保证了安全性又保持了操作的简单性，弥补了 SNMP 版本的不足，可以预见它将很快成为业界流行的支持标准。本文的研究成果将指导我们完成863重点研究项目：计算机网络管理与安全系统。

参 考 文 献

1 夏云，等. SNMPv1-2协议的安全性分析 通信工程学院学报，1999，13(2)
2 RFC 2271-1998 An Architecture for Describing SNMP Management Frameworks
3 RFC 2272-1998 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
4 RFC2273-1998 SNMPv3 Applications
5 RFC2274-1998 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
6 RFC 2275 - View-based Access Control Model (VACM) for SNMPv3
7 RFC1910-1996 User-based Security Model for SNMPV2
8 Stalling W. SNMPV3. A Security Enhancement for SNMP. IEEE Communications Surveys，1998，1(1)
9 Stalling W. SNMP，SNMPv2，SNMPv3，and RMON 1 and 2. Third Edition. Prentice Hall PTR，1999
10 Zeltserman D. Brookline and Massachusetts Practical Guide to SNMPv3 and Network Management，First Edition. Prentice Hall PTR：1999
11 Stalling W. Security Comes to SNMP：The New SNMPv3 Proposed Internet Standards. Internet Protocol Journal，1998，1(3). Cisco News Publication Group，Cisco Systems
12 RFC 2104-1997 HMAC：Keyed-Hashing for Message Authentication

---

(上接第111页)

在运用 SSE-CMM 模型评估一个组织的过程能力成熟度之前，应首先使用这一模型评估该组织在以往工程项目中的表现。

由于每个能力级别都定义了一个或多个共同特性，只有当所有共同特性都得到满足时，才达到了对应的能力级别。如果一个过程域只满足了 n+1级或 n+2级上所定义的部分共同特性，但满足了 n 级上所定义的全部共同特性，其过程能力应当评为 n 级。

在执行具体项目时，一个组织可以根据系统安全工程项目的实际需求有选择地执行某些过程域，而不是全部。此外，一个组织也可能需要执行安全工程过程域之外的关键过程。SSE-CMM 模型推荐了 SSE-CMM 模型的11个过程域，它们可用于组织和项目本身的管理，可以与 SSE-CMM 过程域配合使用。

为了支持理论模型，保障过程能力评估结果的一致性，SSE-CMM 项目组编写了 SSE-CMM 模型评估方法指南。评估方法指南详细地规定了评估机构的组成、人员责任的区分、日程的安排、评估过程中所使用的一些表格格式及内容等。评估过程包括持续一周的与被评组织直接接触的调研活动。指南建议的评估时间是：自我评估为500人小时左右，第三方评估为大约1000人小时左右。评估活动本身并不复杂，主要是确认 SSE-CMM 模型中定义的基本实践和通用实践是否存在。被评组织必须提交证据以支持自己的论点。

参 考 文 献

1 SSE-CMM Model Description Document Version 2.0. April 16，1999
2 SSE-CMM Appraisal Method Version 2.0. April 16，1999
3 http:\\www.sse-cmm.org.
4 http:\\www.sse-cmm.org/library/