信息系统安全需求分析方法研究*)

曹 阳 张维明
(国防科技大学管理科学与工程系 长沙410073)

Approaches for Security Requirements Analysis of Information Systems

· CAO Yang ZHANG Wei-Ming
(Department of Managing Science and Engineering, National University of Defence Technology, Changsha 410073)

Abstract Security requirements analysis is a precondition to provide effective and appropriate safeguard for information systems. Based on the existing theories and approaches, this paper discusses the categories and analysis procedure of security requirements in information systems. And according to the basic steps of security requirements analysis, the security hazard analysis model and the security risk analysis model are presented here. At the end, the methods of security requirements specification and the corresponding improvements are also introduced.

Keywords Security requirements analysis, Security functional requirements, Security assurance requirements, Security hazard analysis, Security risk analysis

1 引言

在人类社会的发展和生存越来越依赖于信息的今天，信息系统已成为人们用于产生、传送、使用、管理信息的主要工具和手段。然而，随着计算机和通信网络技术的飞速发展，信息系统的安全保密问题也日益突出和复杂化。怎么才能确保信息系统的有效性和安全性，已经成为社会普遍关注的重点问题。为此，在新信息系统的构建以及旧信息系统的维护和扩展中，建立一个安全子系统以确保信息系统的安全已成为许多系统设计者的首选方案，安全子系统(下文简称为安全系统)的开发也将成为信息系统开发过程中的一个重要部分[1]。然而，开发一个新的安全系统，需要解决的问题常常是极为复杂的。系统的安全目标是什么，系统应该提供什么样的安全服务，工作将受什么条件约束等等，这些都是安全系统的开发人员必须研究的问题，而这些问题往往是通过安全需求分析而得以解决的。

安全需求分析就是为了在安全系统的开发人员和提出需求的人员(这里统称为用户)之间建立一种理解和沟通的机制，以确定安全系统"做什么"而非"怎么做"(即如何实现)的问题。安全需求以一种清晰、简洁、一致且无二义性的方式，对一个待开发的安全系统中各个有意义的方面进行了陈述，它必须包含有足够多的信息，以使开发人员编制一个能使用户满意的安全系统。

当前针对安全需求的研究有很多[2~9]，美国的DOC组织(The Department of Commerce)1999年财政年度的Small Business Innovation Research计划中第一阶段审批通过的40个项目中就有"Security Requirements Analysis, Methods and Tools"一项[9]。CERIAS主办的国际会议"Symposium on Requirements Engineering for Information Security"，2002年也将举办第二届。这些研究主要讨论了安全需求的分析[3,6]、描述和验证[2,4,5,7,8]等方面的内容，研究出来的理论和方法在各自的领域中均有所建树，但就整个安全需求工程而言，尚未形成一套完整、成熟的理论方法体系。

为此，在现有的理论和方法的基础上，本文就安全需求工程中的两个重要问题：安全需求的分类和安全需求的分析过程进行了讨论，给出了安全需求分析过程中的安全危险性分析模型和安全风险分析模型，最后对安全需求描述中可以用到的各种方法进行了比较，给出了相应的改进措施。

2 安全需求的分类

用户对安全方面的需求有很多，涉及待开发系统的功能、性能和约束等各个方面的内容。"信息技术安全性认证通用标准"(Common Criteria for Information Technology Security Evaluation, CC标准)[5]中将安全需求划分成安全功能需求(Security functional requirements)和安全保障需求(Security assurance requirements)两个独立的范畴来定义，前者描述的是安全系统应该提供的安全功能；后者描述的是系统的安全可信度及为获取一定的可信度而应该采取的措施。为了规范化安全需求，CC标准中定义了11种安全功能需求类和7种安全保障类，并给出了一套评价系统安全可信度的指标——安全保障级别(EAL)。EAL通过安全系统在构造管理、发行与操作、开发、指南文档、生命周期支持、测试和脆弱性评估等方面所采取的措施来确定系统的安全可信度。

CC标准提供安全保障的原则是基于对系统安全可信度的评价。然而，除了EAL这一定性的评价指标外，可以用于评价系统安全保障程度的指标还有很多[10~14]，尤其是其中的一些定量化指标(例如系统的病毒感染率和平均失效时间MTTF等)，对用户来说更加直观，更加易于理解。CC标准中并没有排斥也没有评论这些指标，当这些指标的计算和评价方法进一步成熟之后，用户对这些定量指标的要求将被纳入到对系统的安全保障需求中去。

在现有的这些评价安全保障程度的定量化指标中，安全

*)国家自然科学基金(NO. 60003013)资助项目。曹 阳 博士研究生，主要从事信息系统分析与建模，信息系统安全体系结构等方面的研究。张维明 教授，主要从事信息系统与软件工程等方面的研究。

风险值是当前较为流行，也是比较成熟的一种指标[13,14]。用户对系统安全风险值的要求也应该是安全保障需求中的一部分。此外，在CC标准和信息保障技术框架(Information Assurance Technical Framework，IATF)[1]中，信息系统的安全风险也是确定安全需求的一个重要依据，所以安全风险分析是安全需求分析过程中的一个重要步骤，它的模型将在4.2节中进行详细的介绍。

3 安全需求分析过程

信息系统安全需求的分析过程，由于作者不同，说法也不尽相同，但总的来说主要有以下几个基本的步骤[15,16]：

1、系统调查。了解信息系统所处的安全环境(存在于系统边界之外并对系统的安全具有潜在的或直接影响的所有因素)及其它与安全相关的信息，例如用户、组成部件、运行机制及与其它系统的连接情况等等。在此基础上确定需要保护的资产，其中可能包括硬件、软件、数据、文档和计算机服务等等，并评价各个资产的相对价值。

2、定性地分析系统的脆弱点和可能遭受的安全威胁。这一步骤比第一步更加困难，因为它需要一定程度的想象，以预测资产可能受到的损害及损害来自何方。系统脆弱点和安全威胁是两个互相依存的概念：没有威胁，就无所谓脆弱点；没有脆弱点，威胁也就不称其为"威胁"。所以当系统的脆弱点被确定后，就需要针对每个脆弱点分析由此可能引发的安全威胁及其对资产可能造成损害的程度。

3、脆弱点和安全威胁的定量分析。这一步骤的目标是确定系统暴露各种脆弱点及面临安全威胁的可能性。这种可能性与当前采用的安全措施和所处的安全环境有关。对脆弱点和安全威胁的可能性进行估算是非常困难的，主要采用的是概率统计的方法，分析凭借的数据主要是操作日志，局部犯罪的统计和用户的投诉等等，由此得到的结果可以进一步计算出系统承受的安全风险值。

4、需求的确定。需求分析的最后一个阶段将定性分析和定量分析的结果结合起来以定义信息系统的安全需求，然后开发人员由此确定相应的安全措施，以达到为信息系统提供有效而且合理的安全保障的目的。

安全需求分析的过程并不是一蹴而就的。由于数据的不确定性和环境的不断变化，安全需求的内容需要不断地进行修正，因此安全需求的管理工作也将一直进行下去，以最终指导信息系统安全保障措施的实施。

4 安全需求分析方法

4.1 安全危险性分析模型

安全需求的获取实际上是一个对用户意图不断进行揭示和判断的过程。当用户在对信息系统自身的状况和可能遇到的安全危险并不太了解的情况下，只能提出一些较为抽象的安全需求。安全危险性分析的目标就是对各种危险信息进行全面的收集和充分的分析，以使用户能够进一步地明确系统的脆弱点和可能遭受的安全威胁，从而能够提出详细、准确的安全需求。

当前分析安全危险性的方法有很多，例如软件故障树分析(SFTA)方法[3,4,17]，危险性与可操作性分析(HAZOP)方法，故障模式、影响和危险度分析(FMECA)方法[4,17]等等。这些方法大都是从可靠性工程中引入的。其中，SFTA以一种逆推的方式对一个已知的入侵行为进行建模分析；HAZOP将系统、设备或过程细分为一系列组件来进行故障分析；FMECA应用演绎逻辑对系统或过程进行故障分析，确定子部件的失效对整个系统操作的影响，并根据它们的严重程度划分潜在的危险性。结合正向推导的方法(例如HAZOP和FMECA)以发掘系统潜在的脆弱点和安全威胁，再用逆向推导的方法(例如SFTA)以确定这些安全危险的可信性，是一种行之有效的安全危险性分析模型。但是上述这些方法也存在不足的地方。它们将注意力主要集中在系统自身的组成和运行机制上，而忽略了系统所处的安全环境和与外界之间的交互关系。然而统计数据表明，系统资产可能受到的损害很大一部分是来自与系统交互的某些人员和外界系统的行为。

文[6]中给出了一种用UML中的用例图(Use case diagram)及其扩展——不当用例图(Abuse case diagram)进行安全危险性分析的方法，正好弥补了上述方法的缺陷。在这种方法中，用例图描述了由于正常的工作需要，系统提供的用例与角色之间的交互关系。这里，角色指的是与系统进行交互的人或外界系统，用例是系统提供功能(即系统的具体用法)的描述。对于那些可能危及系统或其他角色利益和安全的恶意或误用行为，用不当用例图来进行建模。这里，一个完整的不当用例(abuse case)定义了一个对系统或某一角色有害的交互行为。对不当用例进行建模的最终目的在于通过分析系统与外界环境之间的交互行为来达到寻找遗漏的安全需求、设计漏洞和实现漏洞的目的。在实际操作中，一般先建立描述角色与系统正常交互关系的用例图，再利用其中的部件构建不当用例图。

除了用例图和不当用例图，UML中可以用于建模分析的工具还有许多[18]，例如活动图(Activity diagram)、类图(Class diagram)、状态转换图(State Transition diagram)和交互图(Interaction diagram)。在安全危险性分析中，这些图并不一定都要一一画出，安全分析人员可以根据自己的需要有选择地绘制。

这样，将UML方法与上述几种方法结合起来使用，既可以分析出系统自身内部机制中存在的危险性因素，又可以发现系统与外界环境交互中的不正常并有害的行为，从而完成系统脆弱点和安全威胁的定性分析，并由此确定了系统中可能受到损害的资产。

4.2 安全风险分析模型

安全风险是由于某种不希望事件的发生，从而对系统造成影响的可能性。根据系统安全工程能力成熟模型(SSE-CMM)[19]中的理论，能够成为风险的事件有三个重要的组成部分：安全威胁、系统脆弱点和事件造成的影响。一般而言，这三个因素必须同时存在才能构成安全风险(使风险值大于0)。

信息系统面临的安全风险值是确定系统安全需求的一个重要依据，也是评价系统安全可信度的一个重要的定量化指标。按照上一节给出的方法，确定了可能受到损害的资产，并分析出相应的脆弱点和安全威胁后，就可以通过安全风险分析确定系统资产目前与未来的风险所在，再采用适当的、有成本效益的安全措施将信息系统遗留的安全风险控制在可接受的程度之内。图1给出了安全风险分析的全过程。

对于一个具有破坏性的安全事件(例如恶意攻击事件、自然灾害或不可预见的错误)来说，系统脆弱点和安全威胁两者都是必不可少的。所以这一安全事件的发生概率是系统脆弱点和安全威胁两者概率的函数。根据联合概率的计算公式可以推出安全事件 I 的发生概率 $L_I=V_I\times T_I$[20]，其中 V_I 是引

发安全事件 I 的系统脆弱点出现的概率，T_i 是相应安全威胁出现的概率。这些概率值往往是非常难以确定的，文[16]中给出了计算这些概率平均值的方法。

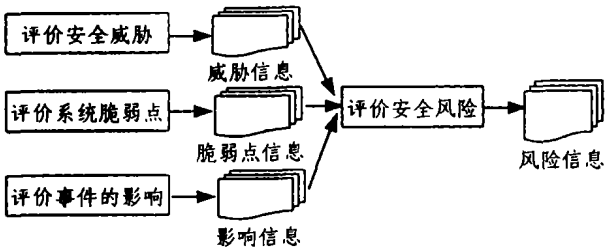

图1 安全风险分析过程

当安全事件发生后，由于安全威胁的程度不同，不同资产受到的影响程度也是不同的，而这些影响是通过对资产的各安全属性(机密性、完整性、可用性、可控性和不可否认性)的损害程度来体现的。这里用影响因子 δ_{IX} 来表示安全事件 I 对资产 X 的影响程度，它的值可以通过安全事件对资产各安全属性的损失度加权平均来获得。

这里，影响因子 δ_{IX} 是一个无量纲的系数，表示资产损失的百分比，所以资产真正的损失金额还与资产自身的价值有关。因此，有必要对可能受到威胁的资产进行价值评估。不过许多资产的价值或重要性是很难用金钱来衡量的。为了对所有资产的价值以可比的方式进行描述，可以给每个资产赋予一个相对的权重 W_X(例如文[1]中定义的 V1～V5或文[21]中定义的1～10)，取值越大表示该资产越重要，保护措施不当的话可能遭受的损失越大。

有了上面计算的几个参数后，资产 X 面临的安全风险 R_X 就不难计算出来了：

$$R_X=\sum_{I\in\Omega}\delta_{IX}\times W_X\times L_I$$

其中 Ω 为对信息系统具有破坏性作用的所有安全事件的集合。

对于面临不同安全风险的资产应该采取不同的安全措施和安全策略。例如简单地将安全风险划分为高、中、低三个等级，对于安全风险高的资产，应当采取严格措施进行保护，或者进行物理隔绝，这时需要实现的安全功能和安全保障措施可能不计较成本效益；安全风险为中的资产，实现适当的符合成本效益的安全功能和保障措施对其进行保护即可；安全风险低的资产视情况而定，有的资产完全置于目前的安全措施之下即可。

由于在安全风险的计算中，一些参数值是很难确定的，例如某一安全事件在明年的发生概率或某个特定部件的使用频率，因此安全风险的计算结果往往带有很大的不确定性，而这一不确定性的大小主要依赖于掌握数据的数量和质量。因此仅依赖一次性的计算结果往往是不够的，安全风险值将随着收集和掌握数据的数量的扩大和精确度的提高而不断地得到修正。

4.3 安全需求的描述方法

信息系统安全需求分析中的两大难题主要是：获取实际系统的安全需求；选用合适的表达方式对安全需求进行描述，既要便于用户理解，也要便于开发者使用。前者在上两节已经讨论过了，而第二个难题涉及安全需求的描述问题。

目前很多人往往需要用自然语言来描述安全需求。自然语言唯一的好处是直观易懂、交流方便，但它由于本质上的原因而隐藏了可能导致误解的模糊成分。特别是对于需要精确、简洁描述的安全需求来说，自然语言的二义性可能导致开发人员对用户需求的误解，隐藏的模糊成分可能导致安全系统某些功能的自相矛盾。

文[22]给出了几种软件工程中使用的形式化、非形式化和基于知识表示的需求规格说明方法，它们各有优缺点，但由于其缺乏对安全领域知识的描述能力，因此在描述安全需求方面存在着某些不足。文[2,4]给出了几种形式化的安全需求描述方法。形式化方法虽然能够非常严密、精确地描述和分析安全需求，但是由于其往往复杂而难以掌握，不易于被非专家级的人员理解，从而不便于和用户沟通。目前应用仍存在一定的局限性。

被国际标准化组织认可的 CC 标准中给出了一套安全需求的定义方法，供安全系统的开发人员、用户和评价人员参照使用。在 CC 标准中，安全需求以类(Class)、族(Family)、组件(Component)的形式进行定义，其中类和族反映的是分类方法，具体的安全需求由组件来体现。例如，对加密支持方面的需求归为一个类；这个类中，对密钥管理方面的需求归为一个族；这个族中，对密钥产生方面的需求构成一个组件。

通常，一个安全系统总是融多项安全需求于一身，需要用多个需求组件以一定的组织方式组合起来进行表示。CC 标准定义了三种类型的组织结构用于描述系统的安全需求：安全组件包(package)、保护框架定义书(Protection Profile，简记为 PP)和安全对象定义书(Security Target，简记为 ST)。

采用 CC 标准中的描述方法，不仅可以产生标准化的需求规格说明，而且便于采用 CC 标准中的评价准则对由此产生的安全系统进行有效的安全评估。当然这种方法也有不足的地方：一、由于描述语言的形式化程度不高，从而不便于对安全需求进行一致性和完备性的验证；二、缺乏对定量化的安全保障需求的描述。

为了克服这些缺点，较为现实的方法是结合使用其它的描述方法，将 CC 标准的需求规格说明方法进行扩展。其中，安全专家使用的形式化方法可以用于具体安全需求组件的说明，例如在密钥发布组件的说明中附加精确的形式化模型来描述其协议规范，从而可以大大减少一致性和完备性验证的工作量。

此外，在4.1节中采用的 UML 方法同样也可用于安全需求的描述。它可以在 PP 或 ST 中描述安全环境；也可以在需求确定前，对安全需求组件进行建模，以便于与用户交流。

至于定量化的安全保障需求，用户可以选择可接受的安全风险值或其它安全度量指标来表示，并在 PP 或 ST 的相应位置加以定义。

结论 由于安全需求对后续开发工作所起的指导性作用以及对安全系统的最终交付使用所起的评价、审定、鉴定性作用，其分析过程在整个安全系统开发过程中的地位日益突出，并受到越来越多的重视。进行充分的安全需求分析能够保证开发出的安全系统为信息系统提供充足、有效的安全保障，从而使开发人员的工作价值得以完全体现，所以可以说准确、完备的安全需求分析是安全系统得以正确、高效实现的前提。

文中的内容对安全需求的有关问题进行了讨论，其中包括安全需求的分类，安全需求的分析过程及其中可能使用到的模型和方法。事实上，安全需求工程中涉及的问题还有很多，例如需求模型的检证和实现等等，这些都是需要重点研究

的内容。

参考文献

1 National Security Agency. Information Assurance Technical Framework (IATF), Version 3.0. http://www.iatf.net, 2000
2 Rushby J. Security Requirements Specifications: How and What. Symposium on Requirements Engineering for Information Security (SREIS), 2001
3 Helmer G, et al. A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System. Symposium on Requirements Engineering for Information Security (SREIS), 2001
4 Lutz R R. Software Engineering for Safety: A Roadmap. Future of Software Engineering(FoSE) at ICSE'00, 2000
5 The International Organization for Standardization. Common Criteria for Information Technology Security Evaluation. ISO/IEC15408:1999(E), 1999
6 McDermott J, Fox C. Using Abuse Case Models for Security Requirements Analysis. In: Proc. of the 15th Annual Computer Security Applications Conf. 1998
7 Leiwo J, Zheng Yuliang. A Formal model to aid documenting and harmonizing of information security requirements. In: Proc. of the IFIP TC11 13th Intl. Conf. on Information Security (SEC'97), 1997. 25～38
8 Leiwo J, Gamage G, Zheng Yuliang. Harmonizer- A Tool for Processing Information Security Requirements in Organizations. In: Proc. of the Third Nordic Workshop on Secure IT Systems (NORDSEC'98), 1998
9 U.S. DEPARTMENT OF COMMERCE. Small Business Innovation Research Program, ABSTRACTS OF AWARDS FOR FISCAL YEAR 1999. http: // www.rdc.noaa.gov/～ amd/abstracts1999.pdf
10 Payne S C. A Guide to Security Metrics. http://www.sans.org/infosecFAQ/audit/metrics.htm, 2001
11 Nielsen F. Approaches to Security Metrics. A Report of the Workshop Held at the National Institute of Standards and Technology (NIST) In conjunction with the Computer System Security and Privacy Advisory Board (CSSPAB) Meeting, 2000
12 Bodeau D J. Information Assurance Assessment: Lessons-Learned and Challenges. http: // philby.ucsd.edu/～ cse291_IDVA/papers/rating-position/Bodeau.pdf, 2001
13 Jelen G F, Williams J R. A Practical Approach to Measuring Assurance. 14th Annual Computer Security Applications Conf. Dec. 1998
14 Williams J R, Jelen G F. A Framework for Reasoning about Assurance. National Institute for Standards and Technology, DRAFT, 1995
15 Eames D P, Moffett J. The Integration of Safety and Security Requirements. Safecomp'99, 1999. 27～29
16 Pfleeger C P. Security in Computing. Second Edition. London: Prentice Hall PTR, 1997. 462～471
17 Lutz R R, Shaw H-Y. Applying Adaptive Safety Analysis Techniques. In: Proc. of the Tenth Intl. Symposium on Software Reliability Engineering, 1999
18 蒋慧，吴礼发，陈卫卫. UML设计核心技术. 北京：北京希望电子出版社，2001. 9～21
19 SSO. The Systems Security Engineering Capability Maturity Model (SSE-CMM). http: // www.sse-cmm.org/model.htm, 1999
20 Williams J R, Jelen G F. A Framework for Reasoning about Assurance [R]. Document Number ATR 97043, Arca Systems, Inc., 1998
21 何全胜，姚国祥. 网络安全需求分析及安全策略研究. 计算机工程，2000, 26(6): 56～58
22 周之英. 现代软件过程(中)－基本方法篇. 北京：科学出版社，2000. 1～26

(上接第117页)

在我们自行设计的高性能嵌入式微处理器银河TS-1[9]中，通过测试可以获得如图6所示的数据。

		非向量版本	向量版本	加速比
指令条数		13	8	
执行周期数	VLR=4	294	132	2.23
	VLR=8	578	210	2.75
	VLR=16	1146	360	3.18
	VLR=32	2282	666	3.43
	VLR=64	4554	1272	3.58

图6 向量化性能测试结果

由此可见，向量化之后对程序的执行性能提高是极有好处的。

结束语 如果在微处理器设计中，在微处理器内部设置相关的向量部件，并且在编译过程中对程序进行向量化，可以提高程序在微处理器上的执行性能。本文提出的单重循环向量化方法实验结果表明，可以在二进制代码兼容的条件下达到优化程序的执行性能。将此向量化方法运用在我们自行设计的银河TS-1高性能嵌入式微处理器[9]中，结合硬件的向量处理功能，取得了良好的效果[10]。

同时，由于在处理器中引入了向量处理部件，将增大访存单元的负担。特别是算法所需要的支持非连续存储器单元访问的功能(LDV、SDV)，是实现这一算法的难点。但是，由于执行代码的向量化，可以使得访存单元能够提前得到有关数据地址的信息，有利于连续读入/写入相关的数据。另外，由于向量部件可以在较长的时间内充分利用功能部件，因此可以在硬件上实现更多的存储单元访问操作。

本文所考虑的情况是基于硬件资源不受限的单重循环向量化，如何开发多重循环的向量化成分，如何在向量处理部件资源受限的条件下，在向量化过程中进行资源的分配也是我们在今后的工作中将要着重研究的问题。

参考文献

1 李晓梅，蒋增荣，等. 并行算法. 湖南科学技术出版社，1992
2 张丽君，金绥更. 向量算法与并行算法. 国防工业出版社，1993
3 Lopez D, Valero M, et al. Increasing Memory Bandwidth with Width Bus: Compiler, Hardware and Performance Trade-offs. ACM, 1997
4 Burger D, et al. Memory Bandwidth Limitations of Future Microprocessors. ACM, 1996
5 Saulsbury A, et al. Missing the Memory Wall: The Case for Processor/Memory Integration. ACM, 1996
6 Quintana F, Espasa R, Valero M. Performance Advantages of Merging Instruction- And Data-Level Parallelism (Extended Version)
7 Espasa R, Valero M. Exploiting Instruction and Data Level Parallelism in Future High Performance Processors
8 Wall D W. Limits of Instruction-Level Parallelism: [David W. Wall, WRL Technical Note TN-15]. Western Research Laboratory, Dec. 1990
9 陆洪毅，赵学秘，王蕾，戴葵，王志英. 一种高性能的嵌入式微处理器：银河TS-1. 电子学报，2002. 10
10 宋辉，戴葵，王志英. 基于银河TS-1的高性能量子计算. 电子学报，2002. 10