1.2 软件面临的安全威胁

本书将软件面临的安全威胁分为三大类：软件自身的安全（软件漏洞）、恶意代码及软件侵权。本节将概

1.3.2 用信息安全的基本属性理解软件安全

软件已经成为现代社会生活中的关键组成，因而可以参照信息安全的基本属性来对软件安全的属性进行定义和描述。软件安全除了应具备最基本的信息安全三大基本属性CIA——保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），还应当包括可认证性、授权、可审计性、抗抵赖性、可控性和可存活性等多种安全属性。

1.4.2 软件安全的主要方法和技术

1.软件安全防护的基本方法

漏洞是引发信息安全事件产生的根源，软件漏洞尤其如此。恶意代码通常也是针对漏洞而编写出来的，软件侵权的成功往往跟软件漏洞也有密切的关系。因此，软件安全防护围绕漏洞消除展开，目前有两种基本方法。

1）采用多种检测、分析及挖掘技术对安全错误或是安全漏洞进行发现、分析与评价，然后采取多种安全控制措施进行错误修复和风险控制，如传统的打补丁、防病毒、防火墙、入侵检测和应急响应等。

这种将安全保障措施置于软件发布运行之时是当前普遍采用的方法。历史经验证明，该方法在时间和经济上投入产出比低，信息系统的安全状况很难得到有效改善。本章前面对于当前软件安全问题的现状分析表明了这点。

2）分析软件安全错误发生的原因，将安全错误的修正嵌入到软件开发生命周期的整个阶段。通过对需求分析、设计、实现、测试、发布及运维等各阶段相关的软件安全错误的分析与控制，以期大大减少软件产品的漏洞数量，使软件产品的安全性得到有效提高。

少产生漏洞.

该方法是将安全保障的实施开始于软件发布之前，尤其强调从软件生命周期的早期阶段开始安全考虑，从而减少软件生命周期的后期系统运行过程中安全运维的工作量，提高安全保障效果。实践经验表明，从系统开发需求阶段就引入安全要素要比在系统维护阶段才考虑安全问题所花费的错误修复成本要低很多。

2.软件安全防护的主要技术

现有关于软件安全的技术主要包含软件安全属性认知、信息系统安全工程及软件安全开发三个方面。

（1）软件安全属性的认知 三个基本安全要素

安全是一个整体性的概念。根据国家标准《软件工程 产品质量 第1部分 质量模型》（GB/T 16260.1—2006），软件安全既离不开它所存储、传输、处理的数据的安全，也离不开相关文档的安全，因此软件安全应涵盖数据及其信息处理过程本身的三个基本安全要素：保密性、完整性和可用性；同时软件需要接收外界信息输入才能实现预期的功能产生输出结果，信息来源的安全性必然成为软件安全重要的组成部分。基于这些分析，本书将保密性、完整性、可用性、认证性、授权和可审计性作为软件安全的核心属性；而软件自身的实现质量，即软件产品包含的漏洞情况也应该是软件安全性的主要内容，因为这些漏洞会直接导致安全性问题，这也是传统的软件安全关注的问题；此外，站在不同的管理者视角，抗抵赖性、可信性、可控性、可靠性及软件弹性等也成为软件被关注的其他安全属性。

（2）系统安全工程

系统安全工程是一项复杂的系统工程，需要运用系统工程的思想和方法，系统地分析信息系统存在的安全漏洞、风险、事件、损失、控制方法及效果之间复杂的对应关系，对信息系统的安全性进行分析与评价，以期建立一个有效的安全防御体系，而不是简单的安全产品堆砌。

确切地说，系统安全工程是系统的安全性问题而不仅是软件产品的安全性问题，是一种普适性的信息系统安全工程理论与实践方法，可以用于构建各种系统安全防御体系。系统安全工程可以在系统生命周期的不同阶段对安全问题提供指导，例如，对于已经发布运行的软件，可以采用系统测试、风险评估与控制等方法构建安全防御体系；而对于尚待开发的系统，也可以应用系统安全工程的思想方法来提高目标系统的安全性。这是一项具有挑战性的工作，也是本书的出发点。

（3）软件安全开发

漏洞是引发信息安全事件的根源，而软件漏洞又是在软件开发的整个生命周期中引入的。软件生命周期包括需求分析、可行性分析、总体描述、系统设计、编码、调试和测试、验收与运行、维护升级、废弃等多个阶段，每个阶段都要定义、审查并形成文档以供交流或备查，以此来提高软件的质量。虽然此类流程严格规范，但是由于开发过程中人员经验不足、开发平台客观条件等方面的原因，依然会引入各种类别的安全漏洞。因此，在软件开发的各个环节中进行漏洞的预防和分析，能够快速、高效地发现软件中的安全问题，减少其在后期带来更大的危害。

SDL

一些软件开发相关的机构和企业意识到了这一情况，纷纷在软件开发过程的各个阶段采取各种措施对开发的软件进行漏洞分析。微软、思科等公司推出的安全开发生命周期（Security Development Lifecycle，SDL）就是一套对软件开发过程进行安全保障的方案，旨在尽量减少设计、代码和文档中与安全相关的漏洞的数量。微软的实践证明，从需求分析阶段开始就考虑安全问题，可以大大减少软件产品漏洞的数量，而不会增加成本。

软件安全开发关注的是如何运用系统安全工程的思想，以软件的安全性为核心，将安全要素嵌入软件开发生命周期的全过程，有效减少软件产品潜在的漏洞数量或控制在一个风险可接受的水平内，提高软件系统的整体安全性。

软件安全开发方法抛弃了传统的先构建系统，再将安全手段应用于系统的构建模式，而是保留了采用风险管理、身份认证、访问控制、数据加密保护和入侵检测等传统安全方法，将安全作为功能需求的必要组成部分，在系统开发的需求阶段就引入安全要素，同时对软件开发全过程的每一个阶段实施风险管理，以期减少每一个开发步骤中可能出现的安全问题，最终提高软件产品的本质安全性。

根据软件开发生命周期的阶段划分，软件安全开发涉及以下几个方面的内容。

●软件安全需求分析。

●软件安全设计。

●软件安全编码。

●软件安全测试。

●软件安全部署。

本书将在后续章节中展开介绍以上技术。

✍ 小结

本节概述了保障软件安全的主要方法和技术，它们各有侧重和不同。对于软件安全性的测试和评估主要基于产品的视角，描述产品是什么，它的安全性怎么样；而系统安全工程与软件安全开发是基于过程的视角，回答软件的安全性是如何构建的，软件安全开发是系统安全工程应用的最高阶段，也是解决信息安全问题的最根本途径。