<<可信链度量与测评>>

图书基本信息

书名：<<可信链度量与测评>>

13位ISBN编号：9787560626949

10位ISBN编号：7560626947

出版时间：2011-12

出版时间：西安电子科技大学出版社

作者：张帆，徐明迪，杨r　著

页数：122

<<可信链度量与测评>>

内容概要

可信计算是一种信息系统安全新技术，它关注于终端安全，从硬件和软件底层入手，针对信息系统综合采取措施，以增强系统的安全性。
目前，可信计算已经成为国内外信息安全领域的一个新热点，并已取得了令人鼓舞的成绩。
可信计算具有三大基本功能：完整性度量、完整性存储和完整性报告。
其中，完整性度量功能又是完整性存储功能和完整性报告功能的基础。
为了实现完整性度量功能，可信计算组织TCG定义了可信链技术。
能否实现完整、安全的可信链，直接关系到整个可信计算平台能否正常运行。
目前，研究人员从不同角度对可信链进行了深入研究，但仍有不少开放问题有待解决。
《可信链度量与测评》重点针对可信链的两个重要组成部分——完整性度量和安全性测评，从理论和实践两方面作了介绍。
全书共分五章：第一章，可信计算；第二章，可信启动完整性度量；第三章，应用程序完整性度量；第四章，可信链测评；第五章，总结与展望。
《可信链度量与测评》可以作为高年级本科生、研究生的教材，也可以作为可信计算研究人员和工程技术人员的参考书。

<<可信链度量与测评>>

书籍目录

第一章　可信计算
1.1　可信计算简介
1.1.1　可信计算的基本概念
1.1.2　国外可信计算的发展
1.1.3　国内可信计算的发展
1.2　可信链
1.3　可信计算机
1.3.1　可信计算机体系结构
1.3.2　嵌入式安全模块ESM
1.4　本章小结
参考文献
第二章　可信启动完整性度量
2.1　可信启动完整性度量分析
2.1.1　Linux启动流程分析
2.1.2　Linux启动流程的完整性度量因素
2.1.3　Linux启动流程需要度量的内容
2.2　基于PMBR的SBA设计
2.3　基于PMBR的SBA实现
2.3.1　BIOS安全增强与MP驱动
2.3.2　PMBR详细设计与实现
2.3.3　从绝对路径文件名到磁盘扇区地址的转换
2.3.4　PMBR安全性证明与形式化开发
2.4　实验
2.4.1　EXT3文件系统实验
Z．4.2　SBA实验
2.4.3　性能分析
2.5　本章小结
参考文献
第三章　应用程序完整性度量
3.1　应用程序静态完整性度量
3.1.1　轻量级应用程序静态完整性度量架构
3.1.2　轻量级应用程序静态完整性度量实现
3.1.3　实验示例
3.2　应用程序动态完整性度量
3.2.1　国内外研究动态
3.2.2　软件动态行为建模
3.2.3　完整性条件下传递无干扰模型
3.2.4　软件动态行为可信性分析
3.2.5　-种软件动态行为可信度量系统实现方案
3.3　本章小结
参考文献
第四章　可信链测评
4.1　安全模型简介
4.1.1　基于语言的安全模型
4.1.2　安全进程代数

4.1.3 基于语义的安全属性
4.1.4 安全属性的可复合性
4.2 可信链交互模型
4.2.1 可信链规范说明
4.2.2 可信链接口模型
4.3 可信链接口安全模型
4.3.1 不可演绎模型
4.3.2 可信链复合模型
4.3.3 进一步的分析
4.4 一致性测试和安全性测试
4.4.1 一致性测试
4.4.2 安全性测试
4.5 可信链PC规范一致性测试
4.5.1 标记变迁系统(LTS)
4.5.2 可信链规范说明状态集
4.5.3 可信链规范实现测试集
4.5.4 测试流程
4.6 可信链规范安全性分析
4.6.1 可信链接口安全等级
4.6.2 可信链接口安全测试
4.7 可信链测试评估系统
4.7.1 可信链测评对象
4.7.2 可信链测评实例
4.7.3 可信链测评总结
4.8 本章小结
参考文献
第五章 总结与展望
5.1 可信链完整性度量
5.2 可信链测评
参考文献
附件A 基于B方法的PMBR的形式化开发
附录B 可信链LTS(s)标记变迁关系
附录C 可信链接口安全等级划分

章节摘录

版权页：插图：可信链是可信计算的关键技术之一，直接关系到整个可信计算平台的可信性，因此，对可信链展开研究，并进而实现完整、安全的可信链，具有重要的理论和现实意义。
前已说明，实现可信链是一项系统性的工作，它涉及可信度量根核、相关证书、TPM/TCM驱动、完整性度量、完整性度量结果存储与集成、可信链恢复、可信链安全性测评等多个环节的工作。
其中任何一个环节出了问题，都可能导致可信链存在安全缺陷，并进而危害到整个可信计算平台的可信性。
在本书中。
我们选择了上述环节中的两个重要方面——完整性度量和安全性测评展开了研究。
可信链完整性度量关注于可信计算平台资源实体的完整性，其通过对资源实体的完整性进行度量，来确保整个可信计算平台运行在一个未被篡改的或者说可知、可控的状态下，从而为用户建立一个基础的可信计算环境，保证应用程序的安全执行和对外服务的可靠运行；可信链安全性测评则研究了可信链的具体实现与可信计算规范之间的一致性，研究了可信链实现是否存在安全漏洞和隐患，以及这些安全漏洞和隐患是否可能被攻击者所利用等。
本书的第二、三章以及第四章分别对可信链完整性度量和可信链安全性测评问题进行了研究。
在本章中，我们将对上述工作做一个总结与展望。
5.1 可信链完整性度量可信链的完整性度量分为静态（完整性）度量和动态（完整性）度量两部分。
其中，TCG定义的完整性度量主要关注的是静态度量。
静态度量的思想比较简单，也不存在大的理论障碍或者技术门槛。
以IBM在2004年提出的完整性度量架构IMA为代表，静态度量问题已经基本解决得比较完善了。
目前，研究人员更加关注的是动态度量问题。
动态度量需要判定某个软件在运行的过程当中，是否发生了危害计算环境可信性的恶意操作，换句话说，需要判定软件在运行时的动态行为是否可信。
由于软件的动态行为是很复杂的，同时，攻击者的攻击手段也是多种多样的，因此这方面的研究目前还处于初步阶段，还有很多问题需要深入研究。
针对软件动态完整性度量问题，第三章提出了一种基于系统调用和无干扰理论的软件动态行为完整性度量框架。

<<可信链度量与测评>>

编辑推荐

《可信链度量与测评》为“十二五”重点图书。

<<可信链度量与测评>>

版权说明