第一图书网, tushu007.com

<<计算机固件安全技术>>

图书基本信息

书名：<<计算机固件安全技术>>

13位ISBN编号：9787302301110

10位ISBN编号：7302301115

出版时间：2012-12

出版时间：清华大学出版社

作者：周振柳

页数：184

字数：269000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

<<计算机固件安全技术>>

内容概要

《计算机固件安全技术》内容涵盖作者在计算机固件安全领域多年的研究成果，是国内第一部公开出版的计算机固件安全领域的学术著作。

全书内容包括：计算机固件概念和功能、国内外固件产品和技术研究发展历程、固件开发基础技术与规范、固件安全研究历史与现状、传统固件BIOS安全技术研究开发实例、BIOS安全漏洞及其威胁、BIOS安全检测方法与实现、可信固件开发的安全策略和模型、可信固件中可信度量基础与方法、可信固件的开发实现。

《计算机固件安全技术》可作为高等学校网络安全、信息安全专业教材，或相关专业人员的参考研究书籍。

第一图书网, tushu007.com

作者简介

周振柳，1971年生，湖北黄梅人；毕业于中国科学院研究生院，获得博士学位。
长期从事计算机网络与信息安全教学和科研工作，获得中共中央办公厅科学技术一等奖和二等奖各1项，国家技术发明专利2项，公开发表学术论文30余篇。

第一图书网, tushu007.com

<<计算机固件安全技术>>

书籍目录

第一图书网, tushu007.com

第一图书网, tushu007.com

章节摘录

版权页： 插图： 3.系统芯片组初始化 早期主板上，各种组件之间的连接与协调电路极为复杂，动辄使用到上百块各类型的IC、电容，不但占用主板面积，也造成了除错上的麻烦与无谓的成本。
随着半导体科技的进步，主板上的许多线路，已使用几个大型IC芯片来取代，可以简化设计与除错时间、减少成本，这些专攻主板简化设计的芯片，就称为系统芯片组。
一般主板上会有几个大型的芯片，每一个芯片有着特定的功能，这其中最重要的就是南北桥芯片组。
以Intel D9459nt主板为例，离CPU最近的芯片是Intel 82945G芯片，称之为北桥芯片（North bridge），主要负责内存和显示控制；另一个是Intel 82801G芯片，称之为南桥芯片（South bridge），主要负责外围的输入／输出控制。
系统芯片组初始化是极其复杂的一项工作，往往需要芯片组厂商提供详细的Data Sheet甚至初始化代码来完成。
芯片组厂商对于新系统芯片组的这部分资料往往要作为商业秘密，只在密切相关的小范围内授权公开，这也是造成30年来固件B10S技术高度垄断的一个重要原因。
2.3.2 总线接口规范 任何一个微处理器都要与一定数量的部件和外围设备连接，但如果将各部件和每一种外围设备都分别用一组线路与CPU直接连接，那么连线将会错综复杂，甚至难以实现。
为了简化硬件电路设计、简化系统结构，常用一组线路，配置以适当的接口电路，与各部件和外围设备连接，这组共用的连接线路被称为总线。
采用总线结构便于部件和设备的扩充，尤其制定了统一的总线标准使不同设备间容易实现互连。
微机中总线一般有内部总线、系统总线和外部总线。
内部总线是微机内部各外围芯片与处理器之间的总线，用于芯片一级的互连；系统总线是微机中各插件板与系统板之间的总线，用于插件板一级的互连；外部总线则是微机和外部设备之间的总线，它用于设备一级的互连。
计算机固件要通过这些总线发现和访问主板上连接的芯片和设备，对这些芯片或设备的控制器（Controller）进行配置，并负责把设备初始化配置、数据结构、驱动ROM等信息传递给操作系统。
固件开发者必须清楚如何操控这些总线去完成芯片和设备的发现和初始化工作。
本节对同计算机固件开发密切相关的几种总线作一简单介绍。

第一图书网, tushu007.com

编辑推荐

《计算机固件安全技术》可作为高等学校网络安全、信息安全专业教材，或相关专业人员的参考研究书籍。

第一图书网, tushu007.com

<<计算机固件安全技术>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com