

《FPGA安全性设计指南》

图书基本信息

书名：《FPGA安全性设计指南》

13位ISBN编号：9787111457838

出版时间：2014-5-23

作者：（美）Ted Huffmire

页数：163

译者：房亮

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《FPGA安全性设计指南》

内容概要

现场可编程门阵列(FPGA)已经成为嵌入式系统设计的主要应用技术之一。可重构器件由于融合了硬件和软件的特性,能够在专用集成电路的高性能和CPU的可编程性之间找到自己的应用空间,产生更好的应用效果。与此同时,FPGA安全性设计的问题也日益突出。目前,关于FPGA安全性设计的专门著述较少,FPGA设计者很难针对具体应用进行系统的安全性分析和设计。

本书通过理论阐述并结合实用设计的方式,通过举例说明FPGA安全性设计的问题如何进行解决。作者从如何编写顶层设计的形式化说明开始,逐步涉及低层硬件电路的各项强化机制,并分为多个层面对FPGA安全性问题和解决方案进行了全面的阐述。作者结合近年来在计算机安全性理论、编程语言、编译器和硬件设计等领域中的最新进展,与FPGA设计中的安全性问题作为一个整体予以阐述,创建了一整套静态和动态分析互相配合的多样化设计技术,使得使用商业芯片构建的FPGA系统有可能成为一个稳定、可靠和安全的强健系统。

本书旨在为EDA(电子设计自动化)和FPGA领域工作的研究者和实践者们提供一整套FPGA安全性设计的管理实用方法。本书适合在公司、工厂和政府研究实验室工作,从事FPGA设计的工程师和学术界人士阅读。尤其是对FPGA安全性要求较高的领域。同时也适合致力于FPGA安全性设计研究的人士,用以提高专业技能。

书籍目录

原书前言

作者简介

第1章概述

1.1对FPGA日益增加的依赖

1.1.1航空航天用FPGA

1.1.2超级计算用FPGA

1.1.3用FPGA分析视频

1.1.4高吞吐量加密用FPGA

1.1.5入侵检测及防范用FPGA

1.2FPGA体系结构

1.2.1可重构硬件的吸引力

1.2.2FPGA的内部结构

1.2.3设计流程

1.3FPGA安全问题的复杂性

1.3.1安全是一个难题

1.3.2复杂度以及抽象

1.3.3烘烤和修补的比较

1.3.4FPGA核的隔离

1.4本书结构

参考文献

第2章高保障软件的经验与技术

2.1背景

2.2恶意软件

2.2.1特洛伊木马

2.2.2后门

2.3保障度

2.4相称的保护

2.4.1威胁模型

2.5安全策略的执行

2.5.1安全策略类型

2.5.2策略执行机制

2.5.3可信任部件的组合

2.6保障度管理策略的执行

2.6.1生命周期支持

2.6.2配置管理

2.6.3独立评估

2.6.4动态程序分析

2.6.5可信任发售

2.6.6可信任恢复

2.6.7静态分析

参考文献

第3章硬件安全的难点

3.1恶意硬件

3.1.1恶意硬件的分类

3.1.2晶圆代工厂的可信度

3.1.3物理攻击

3.2隐蔽信道定义

- 3.2.1 进程抽象
- 3.2.2 等价类
- 3.2.3 形式定义
- 3.2.4 同步
- 3.2.5 共享资源
- 3.2.6 要求
- 3.2.7 旁路
- 3.3 制约隐蔽信道和侧信道攻击的现有方法
 - 3.3.1 共享资源矩阵法
 - 3.3.2 缓存干扰
 - 3.3.3 FPGA掩码的保护方法
- 3.4 FPGA隐蔽信道攻击的探测及应对
 - 3.4.1 设计流程
 - 3.4.2 空间隔离
 - 3.4.3 存储保护
- 3.5 作为隐蔽存储信道的策略状态
 - 3.5.1 状态策略
 - 3.5.2 隐蔽信道机制
 - 3.5.3 编码方案
 - 3.5.4 隐蔽存储信道探测
 - 3.5.5 减轻隐蔽信道可能造成的危险
- 参考文献
- 第4章 FPGA更新及可编程性
 - 4.1 概述
 - 4.2 比特流加密和认证
 - 4.2.1 密钥管理
 - 4.2.2 战胜比特流加密
 - 4.3 远程更新
 - 4.3.1 认证
 - 4.3.2 可信恢复
 - 4.4 部分可重构
 - 4.4.1 部分可重构的应用
 - 4.4.2 热置换和停机置换的比较
 - 4.4.3 内部配置访问端口
 - 4.4.4 动态安全性和复杂度
 - 4.4.5 客体复用
 - 4.4.6 完整性验证
- 参考文献
- 第5章 FPGA的存储保护
 - 5.1 概述
 - 5.2 FPGA上的存储保护
 - 5.3 策略描述与综合
 - 5.3.1 存储访问策略
 - 5.3.2 硬件综合
 - 5.4 高级描述语言
 - 5.5 示例策略
 - 5.5.1 受控共享
 - 5.5.2 访问列表
 - 5.5.3 中国墙

- 5.5.4 Bell与LaPadula保密模型
- 5.5.5 高水位线
- 5.5.6 Biba完整性模型
- 5.5.7 编辑
- 5.6 系统架构
- 5.7 评估
- 5.8 使用策略编译器
- 5.9 从数学角度构建严格的策略
 - 5.9.1 交叉乘积法
 - 5.9.2 实例
 - 5.9.3 单一的策略变化
 - 5.9.4 混合策略的形式化要素
- 5.10 总结
- 参考文献
- 第6章采用壕沟技术的空间隔离
 - 6.1 概述
 - 6.2 隔离
 - 6.3 采用壕沟技术的物理隔离
 - 6.4 构建壕沟
 - 6.4.1 间隔法
 - 6.4.2 检查法
 - 6.4.3 间隔法与检查法的比较
 - 6.5 使用吊桥的安全互连
 - 6.5.1 直连的吊桥技术
 - 6.5.2 局部重构的路线跟踪
 - 6.5.3 共享总线架构的吊桥技术
 - 6.6 采用壕沟技术来保护引用监视器
- 参考文献
- 第7章综合运用：设计实例
 - 7.1 多核可重构嵌入式系统
 - 7.2 片上外围总线
 - 7.3 AES核
 - 7.4 逻辑隔离区
 - 7.5 引用监视器
 - 7.6 状态性策略
 - 7.7 安全的互连可扩展性
 - 7.8 隐蔽信道
 - 7.9 壕沟技术与吊桥技术的合并
 - 7.10 实施与评估
 - 7.11 软件界面
 - 7.12 安全可用性
 - 7.13 更多的安全架构示例
 - 7.13.1 设计的种类
 - 7.13.2 拓扑结构
 - 7.14 总结
- 参考文献
- 第8章前瞻性问题的
 - 8.1 可信的工具
 - 8.2 安全系统的形式验证

- 8.3安全可用性
- 8.4硬件可信性
- 8.5语言
- 8.6配置管理
- 8.7供应链的安全防护
- 8.8针对FPGA的物理攻击
- 8.9设计盗窃与故障分析
- 8.10局部重构与动态安全
- 8.11结论

参考文献

附录A计算机体系结构的基本原理

- A.1计算机架构师的日常工作是什么？
- A.2CPU、FPGA与ASIC之间的折中方案
- A.3计算机体系结构与计算机科学
- A.4程序分析
 - A.4.1处理器仿真科学
 - A.4.2片上分析引擎
 - A.4.3二进制测试设备
 - A.4.4相位分类
- A.5新型计算机结构
 - A.5.1DIVA结构
 - A.5.2原生微处理器
 - A.5.3WaveScalar结构
 - A.5.4应用于医学领域的结构
- A.6存储器
- A.7超标量处理器
- A.8多线程

《FPGA安全性设计指南》

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:www.tushu000.com