高等学校网络空间安全专业“十三五”规划教材

# 硬件安全威胁与防范

主 编 胡 伟 王馨慕

西安电子科技大学出版社
http://www.xduph.com

高等学校网络空间安全专业“十三五”规划教材

# 硬件安全威胁与防范

主　编　胡　伟　王馨慕
参　编　毛保磊　张慧翔　邰　瑜



西安电子科技大学出版社

## 内 容 简 介

本书主要针对近年来日趋严峻的硬件安全威胁和日益增多的硬件安全攻击事件，介绍在信息系统普遍互联和集成电路供应链不断全球化背景下计算机硬件所面临的安全威胁与挑战。本书涉及硬件安全领域新的攻击手段和防范措施，从安全威胁与防护两个方面介绍领域内最新的发展动态，具有较强的时效性、前沿性和一定的技术深度。

本书可作为高年级本科生或研究生信息安全课程的教材，亦可作为硬件安全领域科研和开发工作者的参考书。

**图书在版编目(CIP)数据**

**硬件安全威胁与防范** / 胡伟，王馨慕主编. —西安：西安电子科技大学出版社，2019.8
ISBN 978-7-5606-5303-7

Ⅰ. ① 硬… Ⅱ. ① 胡… ② 王… Ⅲ. ① 硬件—计算机安全 Ⅳ. ① TP303

**中国版本图书馆 CIP 数据核字(2019)第 078595 号**

策划编辑 陈 婷
责任编辑 张 倩 陈 婷
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西日报社
版 次 2019 年 8 月第 1 版 2019 年 8 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印张 12.5
字 数 286 千字
印 数 1～3000 册
定 价 30.00 元
ISBN 978-7-5606-5303-7/TP
**XDUP 5605001-1**

# 高等学校网络空间安全专业“十三五”规划教材
# 编审专家委员名单

# 作者简介

胡伟，男，西北工业大学网络空间安全学院副教授、硕士生导师(学校教师主页http://jszy.nwpu.edu.cn/weihu)，主要从事硬件安全、形式化安全验证方法、硬件安全度量和可重构计算等方面的研究。在国内外期刊和会议上发表论文50余篇，其中CCF认定的A、B类刊物及会议论文20余篇。代表性成果包括IEEE Transactions on Information Forensics & Security长文1篇，IEEE Transactions on Computer-Aided Design of Integrated Circuits and System长文2篇，ACM Transactions on Design Automation of Electronic Systems长文1篇，计算机辅助设计领域三大权威会议ACM/EDAC/IEEE Design Automation Conference论文3篇，IEEE/ACM International Conference on Computer Aided Design论文6篇，Design，Automation & Test in Europe Conference & Exhibition论文4篇，出版学术专著1部(科学出版社)，主持国家自然科学基金青年基金项目1项。

王馨慕，女，西北工业大学网络空间安全学院助理教授，主要从事硬件安全、硬件木马设计与检测、片上系统可信性设计等方面的研究。在国内外期刊和会议上发表论文15篇，其中CCF认定的A、B、C类刊物及会议论文7篇。代表性成果包括IEEE Transactions on Computers长文1篇，计算机辅助设计领域高水平会议ACM/EDAC/IEEE Design Automation Conference论文1篇，IEEE International Conference on Computer Design论文1篇，Design，Automation & Test in Europe Conference & Exhibition论文1篇。

# 前　言

传统的集成电路硬件设计流程主要注重设计的功能正确性和性能指标，忽视了设计的安全性需求，甚至将安全性与功能正确性或稳定性等价起来，而软件安全工程师们则通常假设底层硬件是安全、可信的。这种假设在计算机硬件与外界只有有限的交互能力时，似乎能够成立。然而，随着计算机硬件的智能化及与外界交互能力的不断增强，如可穿戴医疗设备——心脏起搏器和胰岛素泵都提供了无线通信接口，智能汽车的通信范围已经不再局限于车内的 CAN (Control Area Network，总线网络)，已经具备了与基础设施接入点进行数据交互的能力。在此背景下，关于底层硬件安全性的假设就越来越难以成立，且越来越多的安全攻击事件都利用了硬件相关的漏洞。

回顾一下代表性的硬件安全事件：打印机病毒芯片使得海湾战争中伊拉克的防空系统彻底瘫痪；叙利亚的军事雷达中可能被植入了“切断开关(Kill Switch)”，对以色列的非隐形战机视而不见；“震网”病毒使得伊朗核电站上千台离心机报废；军用级 FPGA 芯片上发现了硬件后门，攻击者可以利用它监视和改变芯片上的数据；Boeing 787 的飞行控制网络被成功入侵，黑客能够控制飞机的飞行姿态；手机芯片生产商 Qualcomm 的移动处理器中存在安全漏洞，攻击者可以利用它来破解 Android 设备的全盘加密功能；Intel 处理器于 2018 年 1 月爆出了 Meltdown(熔断)和 Spectre(幽灵)安全漏洞，会导致敏感信息泄露。硬件安全已经触及了个人计算设备、高可靠系统和军用武器系统。计算机硬件已经成为非常具有吸引力的攻击面。

然而，研究者和设计师们更多地关注软件和网络层面的安全问题，而忽视了来自底层硬件的安全威胁。但是，一个大家普遍接受的事实是：系统的整体安全性由安全性最低的环节来决定，即便上层软件协议再安全，如果底层硬件平台中存在安全缺陷，整个系统仍然是存在安全隐患的。大量的硬件安全事件表明：在硬件层面上，攻击者能够直接访问和操控许多软件层面不可见的关键资源，具有更强的攻击和破坏能

力。如果底层硬件被成功入侵，即便上层软件防护措施再安全也都将形同虚设。因此，非常有必要让未来的信息安全从业者和硬件设计师们深入地了解硬件安全在信息安全中所处的地位和计算机硬件所面临的日趋严峻的安全威胁，并致力于硬件安全相关的教学、研究和开发工作。

本书的写作目的是让读者系统地了解计算机硬件所面临的安全威胁和常用的安全防护措施，并掌握一些简单的硬件安全攻击和防护手段，为相关专业课程的学习和日后工作打下一定的基础。

本书在前人的研究基础上，结合编者十余年的硬件安全研究经验编写而成，主要介绍在计算机系统日趋智能化和网络化的背景下，计算机硬件所面临的各种安全威胁，包括硬件旁路信道分析、故障注入攻击、硬件木马、集成电路供应链安全、硬件安全漏洞等，以及常用的硬件安全防护措施，包括密码算法、隔离技术、随机化和掩码算法、木马检测方法、硬件安全测试与验证技术等。全书共9章，其中胡伟编写了第一章、第二章和第九章，王馨慕编写了第四章和第八章硬件木马方面的内容，毛保磊编写了第三章和第七章，张慧翔编写了第五章，邰瑜参与编写了第六章。

本书的章节安排如下：第一章主要阐述硬件安全的相关概念、本书写作的背景以及常见的硬件安全威胁类型及防护技术；第二章介绍由设计缺陷导致的安全威胁，主要包括未定义功能(如状态机中未占用状态和无关输入)、电磁干扰(如新型DRAM器件存储单元之间的干扰)、冗余路径、调试接口和由性能优化所导致的安全漏洞等；第三章讨论由旁路信道引发的信息泄漏问题及相应的攻击方法；第四章讨论硬件木马设计原理与工作机制；第五章主要介绍密码技术与认证技术，主要探讨几种代表性的密码算法、随机数发生器和物理不可克隆函数，以及可信平台模块；第六章主要介绍安全隔离技术以及ARM Trust Zone和Intel SGX的基本原理；第七章探讨常用的旁路信道保护技术，主要包括随机化技术和掩码技术；第八章重点阐述硬件木马防御技术；第九章主要介绍硬件信息流分析技术，主要包括信息流分析、信息安全验证与漏洞检测技术。

期望本书的出版能够起到抛砖引玉的作用，促进相关学科的教师和研究工作者密切关注硬件安全问题，并在教学和科研工作中提高未来信息安全从业者在硬件安全方面的理论素养和实践能力。

本书的出版得到中央高校基本科研业务费(3102017OQD094)的资

助，在此深表谢意；感谢加州大学圣迭戈分校(University of California, San Diego)的 Ryan Kastner 教授、西北工业大学的戴冠中教授和慕德俊教授，他们为本书编者的研究工作和本书的编写提出了许多宝贵的指导意见；感谢西北工业大学的张璐和朱嘉诚等研究生，他们在本书写作过程中做了大量的辅助工作。

鉴于编者能力和水平有限，书中难免会存在疏漏之处，恳请读者批评指正。

编　者

2019 年 4 月 27 日于西安

# 目　录

# 第一章 绪 论

随着物联网、信息物理系统和云计算等新技术领域的兴起，越来越多的计算设备配备了与外界通信的接口。这些通信接口一方面提高了设备的交换能力和智能化水平，另一方面也使得这些设备暴露于局部或者公开的网络环境之中，从而为黑客提供了入侵和控制这些硬件设备的攻击界面。本章简要探讨硬件安全的相关概念和范畴，并通过一些典型的硬件安全事件来揭示计算硬件所面临的安全威胁，最后，简要介绍常用的硬件安全防护技术。

## 1.1 硬件安全概述

### 1.1.1 硬件的范畴

计算机系统通常可以划分为软件(Software)、硬件(Hardware)和固件(Firmware)三个组成部分。

(1) 软件是一系列按照特定顺序组织的计算机数据和指令的集合。在计算机系统中，操作系统、应用程序、与程序相关的文档都属于软件。

(2) 硬件是指计算机系统中由电子、机械和光电元件等组成的各种物理装置的总称。例如，CPU、存储器、总线控制器、传感器部件等。

(3) 固件是指硬件内部保存的设备“驱动程序”，通常担负着计算机系统最基础和最底层的工作，如完成系统初始化并负责加载系统软件。在计算机系统中，基本输入/输出系统(BIOS，Basic Input/Output System)是固件最为典型的例子。此外，一些存储于 EEPROM 或者 Flash 存储器中的设备配置程序也通常被认为是固件。

本书主要讨论由电子元件所组成的硬件的安全性问题，重点关注由半导体器件所组成的数字和模拟电路所面临的安全威胁，以及常用的防护技术。我们以逻辑和数据安全(信息安全)为主要分析目标，仅在必要时对物理安全作简要探讨。

### 1.1.2 硬件设计的描述形式

当前的数字电路设计从抽象层次上，可分成以下 4 个层次。

(1) 算法级设计：利用高级语言(如 C 语言)及其他一些系统设计工具(如 Xilinx Vivado、Altera OpenCL和 Mentor Graphics Catapult HLS 等)从算法层面对硬件设计进行描述。算法级不需要包含精确的时序信息。

(2) 寄存器传输级设计：用数据流在寄存器间传输的模式来对设计进行描述。寄存器传输级(RTL，Register Transfer Level)硬件设计已经包含了周期精确的时序信息。

(3) 门级：用门级的与、或、非等基本逻辑门及其连接关系对设计进行描述。

(4) 开关级：用晶体管、寄存器及它们之间的连线关系来对设计进行描述。晶体管是逻辑门的基本组成单元，例如与非门由四个晶体管组成，非门由两个晶体管组成等。

硬件的生命周期可划分为设计说明、开发、测试、部署等多个阶段，硬件在各个阶段有不同的描述形式。本书主要关注硬件在开发、测试和部署阶段的安全问题，硬件在这些阶段的描述形式主要有代码级硬件设计、逻辑网表和物理(FPGA 可编程逻辑或 ASIC 芯片)实现三种，如图 1-1 所示。

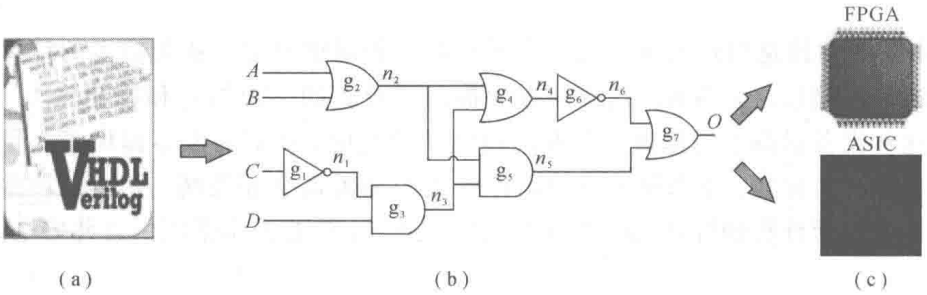


图 1-1 硬件设计的描述形式

(a) 代码级硬件设计；(b) 逻辑网表；(c) FPGA 可编程逻辑或 ASIC 芯片实现

(1) 代码级硬件设计：代码级硬件设计包含算法级设计和 RTL 级设计两个层次，一般采用高层综合语言(如 HLS C)、系统建模语言(如 System Verilog)或者硬件描述语言(HDL，Hardware Description Language)对硬件设计所实现的逻辑功能进行建模和描述。代码级硬件设计是高层综合工具和逻辑综合工具的输入。

(2) 逻辑网表：代码级硬件设计在输入高层综合或者逻辑综合工具之后，将被转换为逻辑网表，逻辑网表由工艺库中定义的基本宏单元及其连接关系构成。逻辑网表可进一步细分为门级和开关级两种。

(3) 物理实现：硬件电路通常有两种物理实现形式，一种是下载和配置现场可编程逻辑门阵列(FPGA，Field Programmable Gate Array)，另一种是通过流片和封装转换为专用集成电路(ASIC，Application Specific Integrated Circuit)芯片。

图 1-2 显示了自顶向下的硬件设计流程和不同抽象层次所处的位置。硬件设计通过高

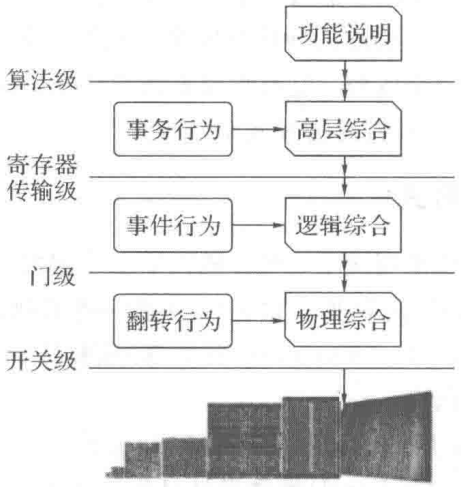


图 1-2 自顶向下的硬件设计流程和不同抽象层次所处的位置

层综合(HLS, High-Level Synthesis)实现从算法到 RTL 级设计的转换，通过逻辑综合实现从 RTL 代码到门级网表的转换，然后，通过物理综合实现从门级网表到物理网表的转换。

### 1.1.3 硬件安全

人类关于信息安全的需求由来已久，密码技术由战争催生，最早诞生于公元前 405 年的古希腊，即斯巴达密码。第二次世界大战期间，密码及其破译技术由于保密通信的需求而迅猛发展。一般认为，信息安全问题被系统地提出并受到关注，起源于 1949 年 Claude Elwood Shannon 发表的《保密系统的通信理论(Communication Theory of Secrecy Systems)》一文，该文奠定了信息安全学科的理论基础，如信息源、密钥、加解密和密码分析的数学原理。1976 年，Whitfield Diffie 和 Martin Edward Hellman 发表了一篇具有开创性的论文《密码学的新方向(New Directions in Cryptography)》，这篇论文首次引入了公共密钥加密协议与数字签名的概念，这两者构成了现代互联网中广泛使用的加密协议的基石。

1996 年和 1998 年，Cryptography Research 公司的首席科学家 Paul Carl Kocher 发表了关于时间和能量信道攻击方面的文章；1997 年，斯坦福大学的 Dan Boneh 发现智能卡上密码算法执行过程可能会受到干扰，产生错误输出，攻击者可以利用其成功恢复算法密钥；2000 年，比利时的 Jean-Jacques Quisquater 和 David Samyde 发现密码算法运行过程中存在电磁辐射，该辐射同样可用于密钥破解。上述事件正式揭开了硬件攻击研究的序幕。

直至 2007 年，硬件安全(Hardware Security)才被作为一个独立的概念提出，正式成为一个相对独立的领域。这是由于硬件攻击往往需要专门的设备，并且要求能够与硬件设备近距离接触以完成必要的测量。在相当长的一段时间里，硬件攻击的条件还不够成熟(低效的攻击设备或者缺少实施攻击的界面/接口)，因此，传统的软件安全应用和研究通常假设底层硬件是安全、可信的，然而，这种假设已经难以成立，越来越多的攻击事件都利用了与硬件相关的安全漏洞。通过硬件电路中的设计缺陷、旁路信道、后门程序和硬件木马发起攻击，往往能够更有效地突破软件安全防护措施，以较低计算代价破解算法密钥，越过访问控制机制或使系统彻底失效。日益增多的攻击事件表明：计算机硬件正面临日趋严峻的安全威胁，已成为新的攻击热点。

## 1.2 硬件安全事件

大多的硬件安全事件都是利用了硬件设计中的安全漏洞或者预置的后门，并通过软件攻击的形式来实施的。虽然也有完全基于硬件的攻击方式，例如某些错误注入攻击，通过调节硬件的工作电压或者工作频率使得电路产生错误的输出等，但是，通过软件途径发起的攻击能更有效地利用硬件中的安全漏洞来获取敏感信息或者直接操控系统。下面介绍一些代表性的硬件安全事件。

### 1.2.1 伊拉克打印机病毒芯片

海湾战争爆发之前，伊拉克军方转道约旦，从法国购买了一种用于防空系统的新型电脑打印机，准备通过约旦首都安曼偷运到巴格达。这个信息被美国情报部门迅速截获。美

军随即派遣间谍潜入约旦，通过某些渠道接触到了这些打印设备，偷偷把一套带有病毒的同类芯片换装到这种打印机里。据称，病毒芯片是由位于美国马里兰州米德堡的国家安全局设计的，病毒名为 Afgl。随后，这些被做过手脚的打印机就被运进了伊拉克，并被伊拉克军方毫无防范地连接到了电脑上。

当美国领导的多国部队发动“沙漠风暴”行动，空袭伊拉克时，美军利用无线遥控设备激活了打印机中的病毒芯片，这些芯片中存储的电脑病毒便传到了与之连线的电脑上，然后，经由一台电脑传播给了与之联网的其他电脑，没过多少时间，整个伊拉克防空体系的电脑设备都停止了运行，伊拉克的防空体系全面瘫痪。在这种情况下，即使当时美军没有隐形战机 F117，而是直接对其进行大规模的空袭，伊拉克也会毫无办法，只能眼看着对方的空军对自己的要害部门狂轰滥炸。这些携带了病毒和后门程序的打印机正是导致战争迅速朝着不利于伊拉克方向发展的重要原因。

### 1.2.2 叙利亚军事雷达“切断开关”

2007 年，为扼杀叙利亚核计划，以色列进行了“果园行动” 空袭，即非隐形战机深入战略纵深地带摧毁预定目标并全身而退。整个行动中，叙军先进的防空系统没有做出任何反应。第二年，《IEEE 波谱杂志(IEEE Spectrum Magazine)》的一篇报道追踪到的消息显示，一家法国芯片公司提供给叙利亚的雷达防御设备中包含一个“切断开关(Kill Switch)”。另外，根据美国国防部供应商匿名提供的情况，一个“欧洲芯片制造商”在叙军防空武器系统的微处理器中加入了可以远程访问的“切断开关”。攻击者可以利用这个“切断开关”远程侵入雷达防御设备并使其完全失效，从而导致叙利亚无法监测到以色列轰炸机正在执行的袭击活动，即便行动中采用的是非隐形战机。

虽然上述内容未经叙利亚方面证实，但是，它足以为我们敲响警钟，即来自第三方的芯片设计中可能存在人为设置的后门或者恶意代码，攻击者能够利用这些在技术文档中未说明的功能来操控整个系统，或者使系统在关键时刻完全失效。

### 1.2.3 伊朗核电站“震网”病毒

2010 年 9 月，伊朗核设施突遭来源不明的网络病毒攻击，西方学者称该病毒为“震网”。由于“震网”的袭击，导致纳坦兹离心浓缩厂的上千台离心机报废，事件所造成的严重后果令世人震惊。

“震网”病毒是一种蠕虫病毒，主要利用 Windows 系统漏洞，通过移动存储介质和网络进行传播，它攻击西门子公司控制系统的数据采集与监视控制系统(SCADA，Supervisory Control And Data Acquisition)。美国科学与国际安全研究所最新公布的研究报告认为，“震网”病毒于 2009 年经网络传至伊朗纳坦兹离心浓缩厂工作人员的个人计算机，再由移动存储介质侵入纳坦兹离心浓缩厂的控制系统，最后病毒发作导致离心机的转速时快时慢。具体过程是：首先在 15 分钟内使离心机的转速提高 30%，达到离心机材料的极限强度并造成材料内伤，然后回到正常转速；27 天后，在 50 分钟内又以每分钟 2 Hz 的降速使频率下降 100 Hz，致使离心机因震动变形而损伤。如此，每月重复一次，离心机伤而不炸，直到最终永久性损坏。在病毒发作的过程中，纳坦兹离心浓缩厂的安全控制与警报系统从未报警，等到发现异常时至少 1000 台离心机已报废。

攻击伊朗核设施的“震网”病毒主要由两部分组成：第一部分使伊朗离心机的运转速度失控，直至机器瘫痪；第二部分让电脑程序秘密录制浓缩厂离心机正常运转时的状况，当离心机失控后，程序会自动播放录像带，向监控设备发送“正常数据”，制造正常运作的假象。这种“频率变而不显，机器损而不炸”的诡异绝招致使伊朗在发现异常问题时束手无策。

### 1.2.4 军用级 FPGA 的硬件后门

2012 年，英国剑桥大学的 Sergei Skorobogatov 和伦敦库欧·瓦迪斯实验室的 Christopher Woods 发表论文指出，他们发现美高森美公司(Microsemi)研制的军用级 FPGA 芯片ProASIC3 A3P250 中存在硬件后门，攻击者可以利用该后门监视和改变芯片上的数据。同年 6 月 1 日，他们在发布会上声称，“利用差分功耗分析(DPA，Differential Power Analysis)技术，AES[①] 的密钥可以在几分钟内被提取出来；而利用管道排放分析(PEA，Pipeline Emission Analysis)技术则只需花不到一秒钟的时间。破解密码的话，利用差分功耗分析技术，需要好几年；但利用管道排放分析技术，就只需几个小时的时间”。该漏洞会使得黑客未经授权就能访问 FPGA 的内部结构，会带来知识产权被侵害的风险。此外，芯片内的运算和数据也可能被恶意更改。

两位研究者的工作促使我们去思考一个更重大的问题：这个漏洞最初是怎么出现在 FPGA 芯片设计中的？这个后门可能是在有人主使下恶意植入的，也有可能完全出于疏忽。也许有人在芯片设计阶段借由这个后门做了一些测试，在后期没有移除或者禁止这个测试接口。显然，设计者们没有意识到它会被发现并可能会被恶意利用。

作为回应，美高森美公司说：“由于那些研究员没能向美高森美公司展示他们研究过程中那些必要的技术细节，更没有让美高森美公司对其得到的结论进行必要的验证，所以美高森美公司一直无法证实，也无法否认他们的言论。此外，美高森美公司可以确定的一点是：我们公司设计的产品没有哪里的设计是会导致客户的安全受到威胁的。”

美高森美公司承认，确实有一种特殊的内部测试机制，通常用于芯片出厂前的测试和故障分析，但表示该功能在产品封装好出厂后都是被禁用的。

在回应中，美高森美公司也声明，研究员们发布的声明增加了外部差分功耗分析，但正因为以前我们考虑过这个原因，所以几年前在应对即将发布的下一代可编程逻辑器件时，美高森美公司也得到了密码学研究公司(Cryptography Research，Inc)对其进行反攻的许可。

### 1.2.5 Boeing 787 娱乐网络入侵事件

2015 年 2 月，来自安全情报公司——同一个世界实验室(One World Labs)的著名安全研究员 Chris Roberts 声称自己入侵了十几架美国联合航空公司飞机的空中娱乐系统(IFE，In-Flight Entertainment)，而且在一次入侵后还劫持了飞机的推力管理计算机，并在短时间内改变了飞机航道。Roberts 在 4 月份的一份 FBI(Federal Bureau of Investigation，美国联邦调查局)调查报告中表示他使其中一架飞机引擎爬升导致飞机在飞行过程中作出横向

① FPGA 一般采用 AES 算法对配置比特流(Configuration Bitstream)进行加密，以保护设计实现细节和知识产权核，防止针对配置比特流的逆向工程。