Texplained

HARDWARE SECURITY INSIGHT

IC REVERSE ENGINEERING & DATA EXTRACTION

Who Am I

- Olivier Thomas:
  - Studied analog micro-electronics design.
  - Worked 8 years in the PayTv field.
    - RE Secure Elements to extract their firmware / data
    - Acquire knowledge used to
      - strengthen new designs
      - use the most efficient counter-measures
  - Founder & CTO of Texplained.
    - Reverse-Engineer motivated by finding new techniques and strategy to uncover secrets from ICs while looking at the constant, mind-blowing evolution of semiconductor and packaging technology.
    - Make IC RE visible and more affordable through better tooling.

INTRODUCTION

Integrated Circuit Reverse-Engineering Use-Cases

- Integrated Circuits are EVERYWHERE
- They handle sensitive / critical operations
- They store and use our personal data
- They should be considered as strategic assets
  - Chip global shortage
  - China’s wanted independence
  - Taiwanese unsafe situation

=> A number of risks can be identified from this point!!..

Integrated Circuit Reverse Engineering & Data Extraction

Integrated Circuit Reverse-Engineering Use-Cases

STORAGE DEVICES HAVE BECOME MORE & MORE ENCRYPTED AND PROTECTED

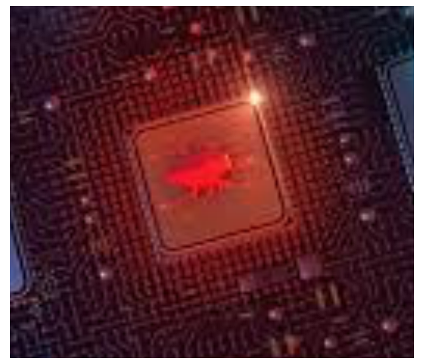
→ **DIGITAL FORENSICS** →

DIGITAL EVIDENCE HAVE BECOME EXTREMELY DIFFICULT TO EXTRACT

MANY UNDOCUMENTED ELECTRONIC DEVICES ARE NO LONGER AVAILABLE

→ **OBSOLESCENCE Mngt** →

A REPLACEMENT INVOLVES A GLOBAL CHANGE OF THE SYSTEM WHICH IS TOO EXPENSIVE



MOST OF COMPONENTS ARE MANUFACTURED IN FOREIGN COUNTRIES

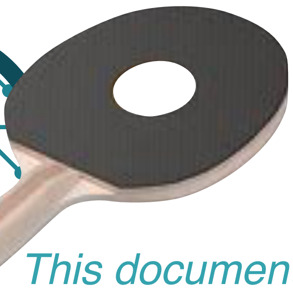
→ **HARDWARE BACKDOORS** →

MALICIOUS GROUPS MAY HAVE INTEGRATED TROJANS DURING MANUFACTURING FOR A LATER REMOTE ATTACK

OFFENSIVE & DEFENSIVE TRADE SECRETS & IPs ANALYSES REQUIRE A HIGH LEVEL OF EXPERTISE

→ **AGGRESSIVE COMPETITION** →

ANALYZING THE COMPETITORS ICs CAN BE DONE ONLY BY EXPERTS

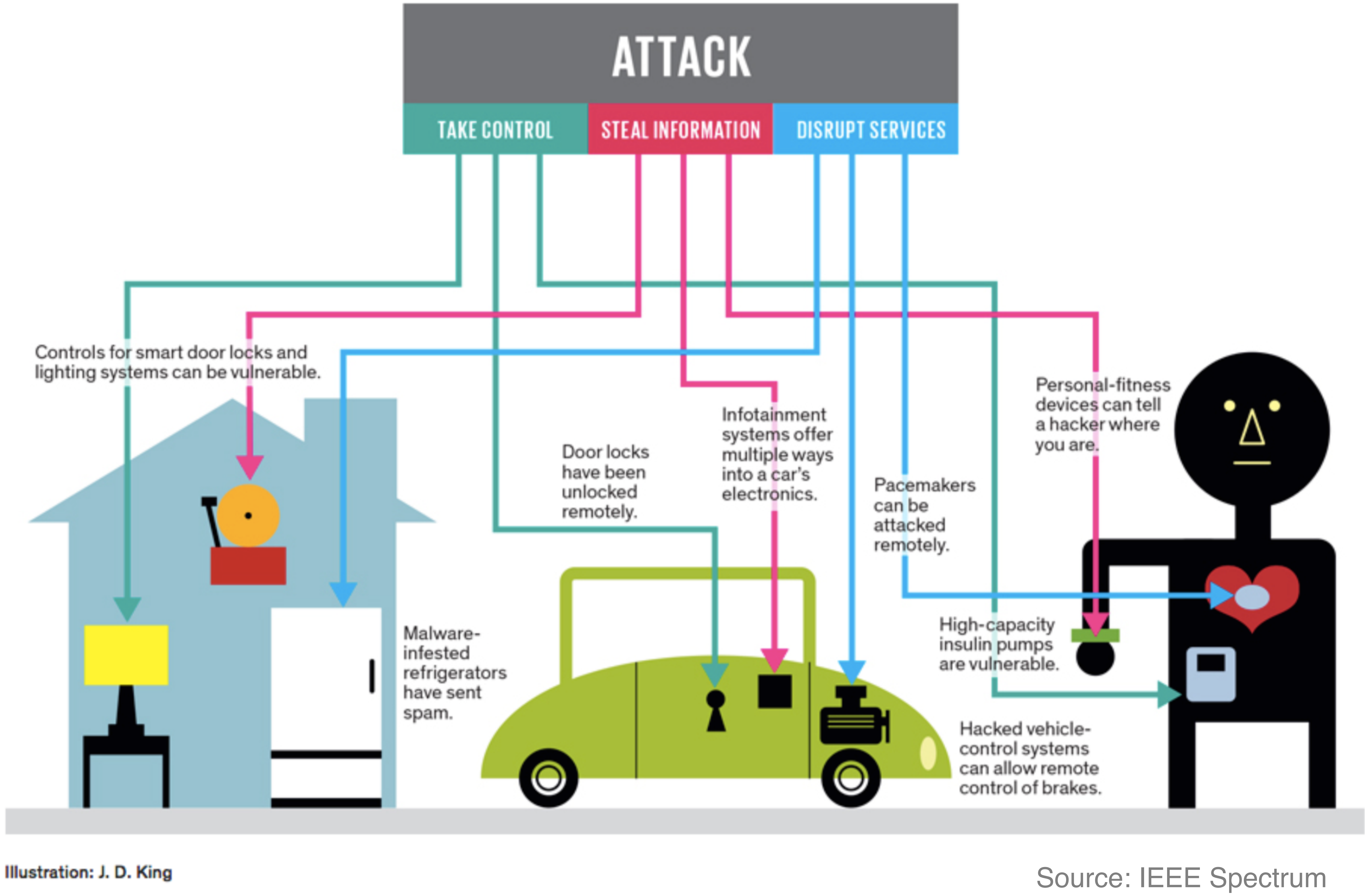


PIRACY PACE IS FASTER THAN SECURITY EVALUATION SCHEMES

→ **SECURITY EVALUATION** →

HARDWARE SECURITY EVALUATION DOES NOT COVER A SUFFICIENT SPECTRUM

Security as a Main Concern for the Semiconductor Industry


ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Personal-fitness devices can tell a hacker where you are.
Pacemakers can be attacked remotely.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.
Illustration: J. D. King

Source: IEEE Spectrum

Hardware piracy consists in different types of Abuses:

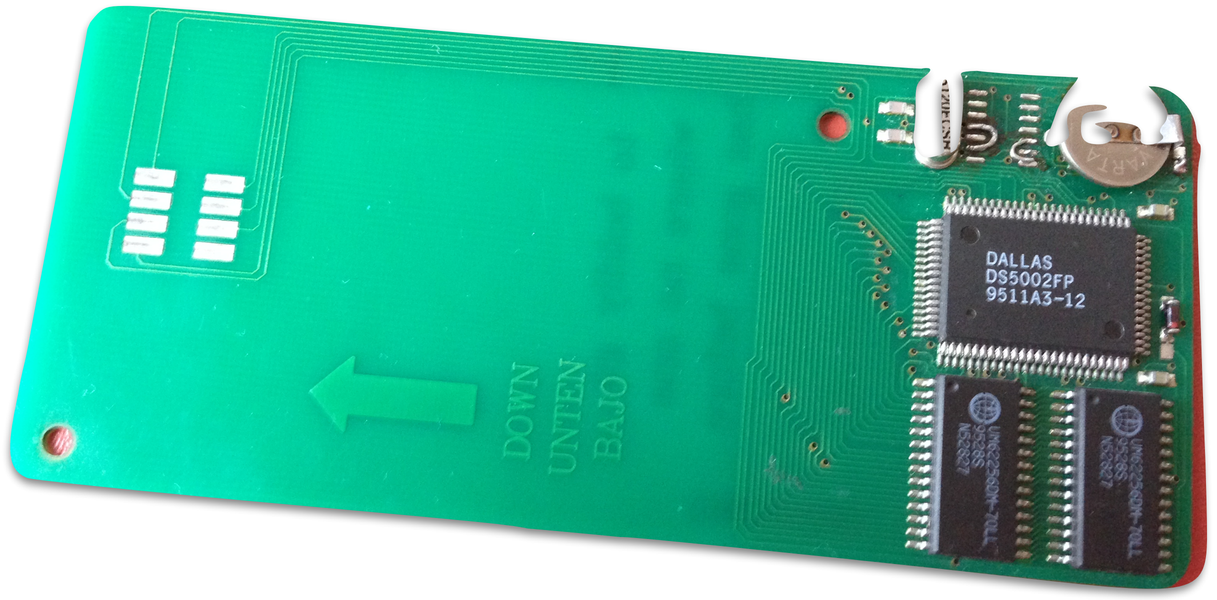
- Counterfeiting
- Intellectual Property Theft
- Mask, Chip and Circuits theft
- Illegal Copy and Cloning
- Illegal Renovation
- Functionalities modification (unlocking, DRM)
- Trojans Implementation

Context

Devices on the spot

Most known examples of hardware pirated devices includes :

- Pay-Tv
- Video games (cartridges, controllers..)
- Printer Ink Cartridges



Pay-Tv Pirate Card - Battery Card

Video Game Console & Peripheral

Printer Cartridges

Devices on the spot

Gaming console - hardware hacking

- The security of a console as a platform requires that only authorized code be executed on the console.
- Consoles are complex systems and hardware vulnerabilities in the overall architecture are often used to compromise the device.
- The goals for an attacker often include identifying vulnerabilities in low level boot loaders
- Since low level boot loaders may be realized as mask ROMs they cannot be patched
- Although there are “valid” uses, such as homebrew software, piracy is one of the primary drivers on the black market

Microsoft XBox

Devices on the spot

Texplained

Gaming console - hardware hacking

- Many Modchips existed for the original Xbox.
- The initial hacks are described extensively in bunnie's "Hacking the Xbox".
- This included using an FPGA to eavesdrop on the device's HyperTransport bus.
- Allowed users to replace the 8GB hard drives with much larger drives.
- Eventually mod chips utilized the LPC bus to replace the Xbox firmware.
- Microsoft released several PCB revisions to prevent users from installing mod chips

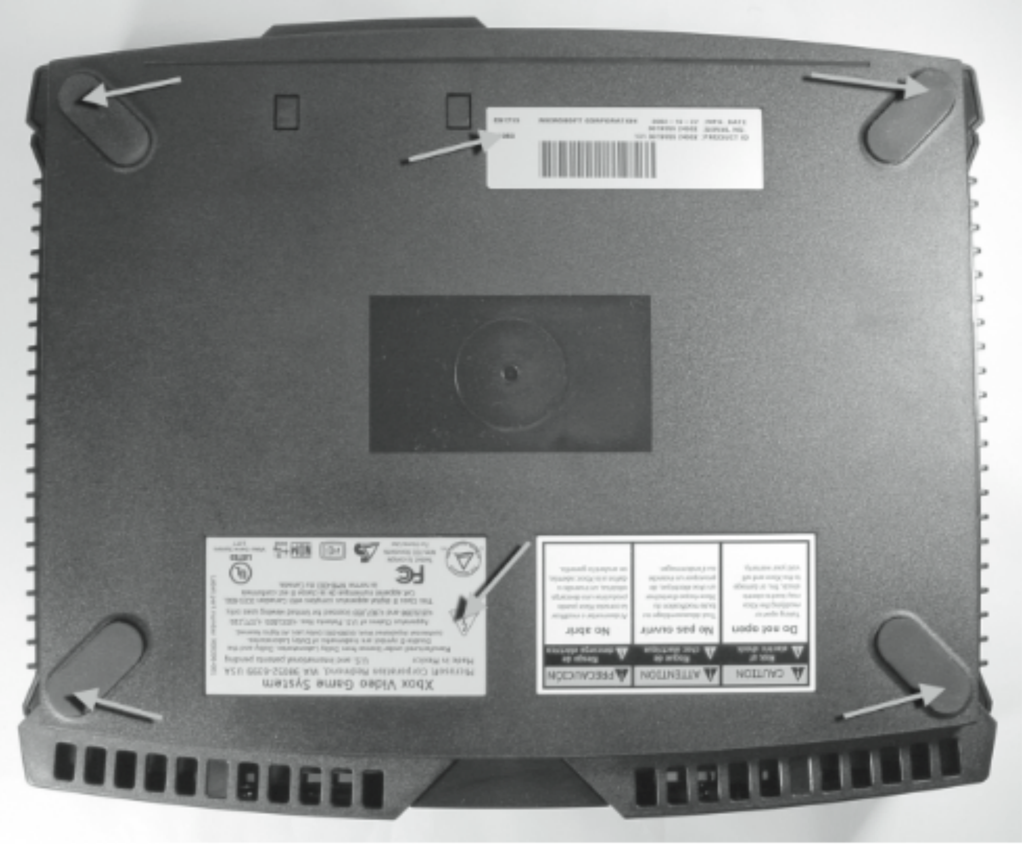


Figure 1-2: Location of the Xbox case screws. This is a view of the bottom of the Xbox.

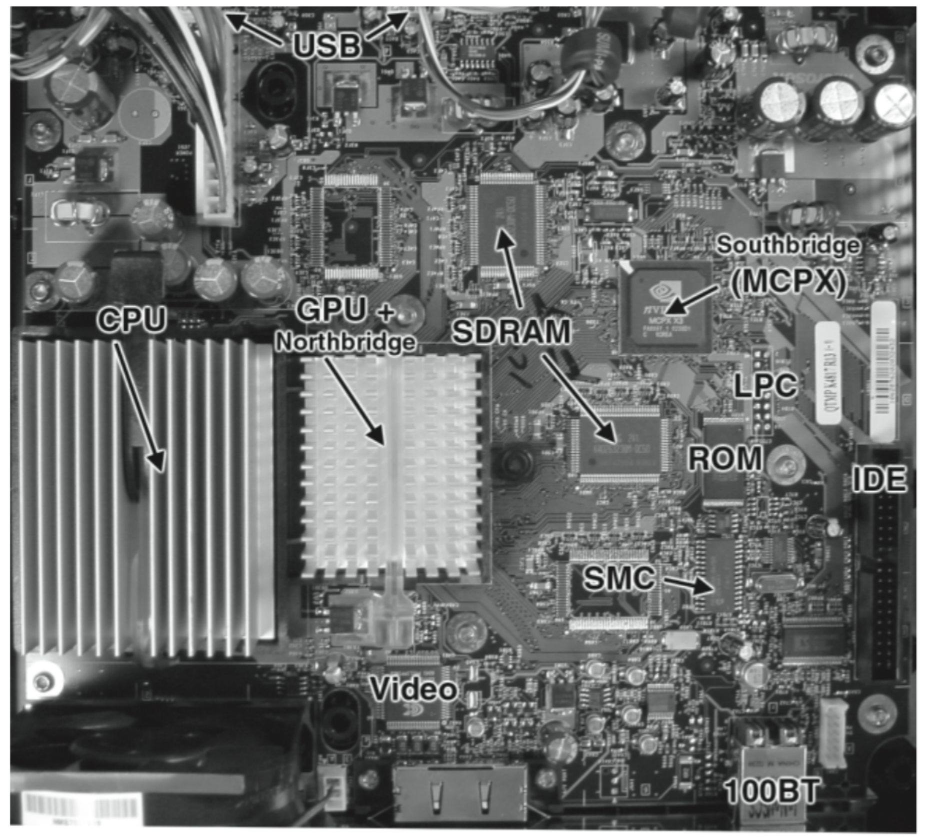


Figure 2-6: Photograph of an Xbox motherboard with the major components labelled.

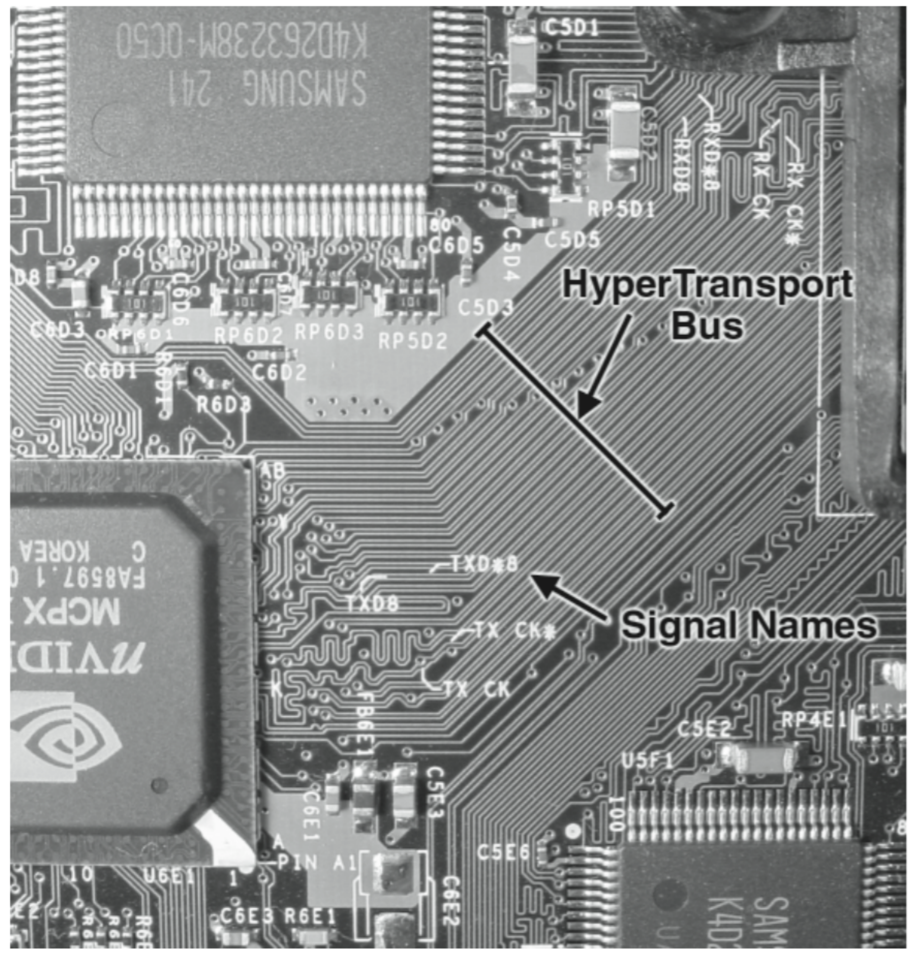


Figure 8-1: HyperTransport bus traces as laid out on an Xbox motherboard.

Context

Secure Microcontrollers

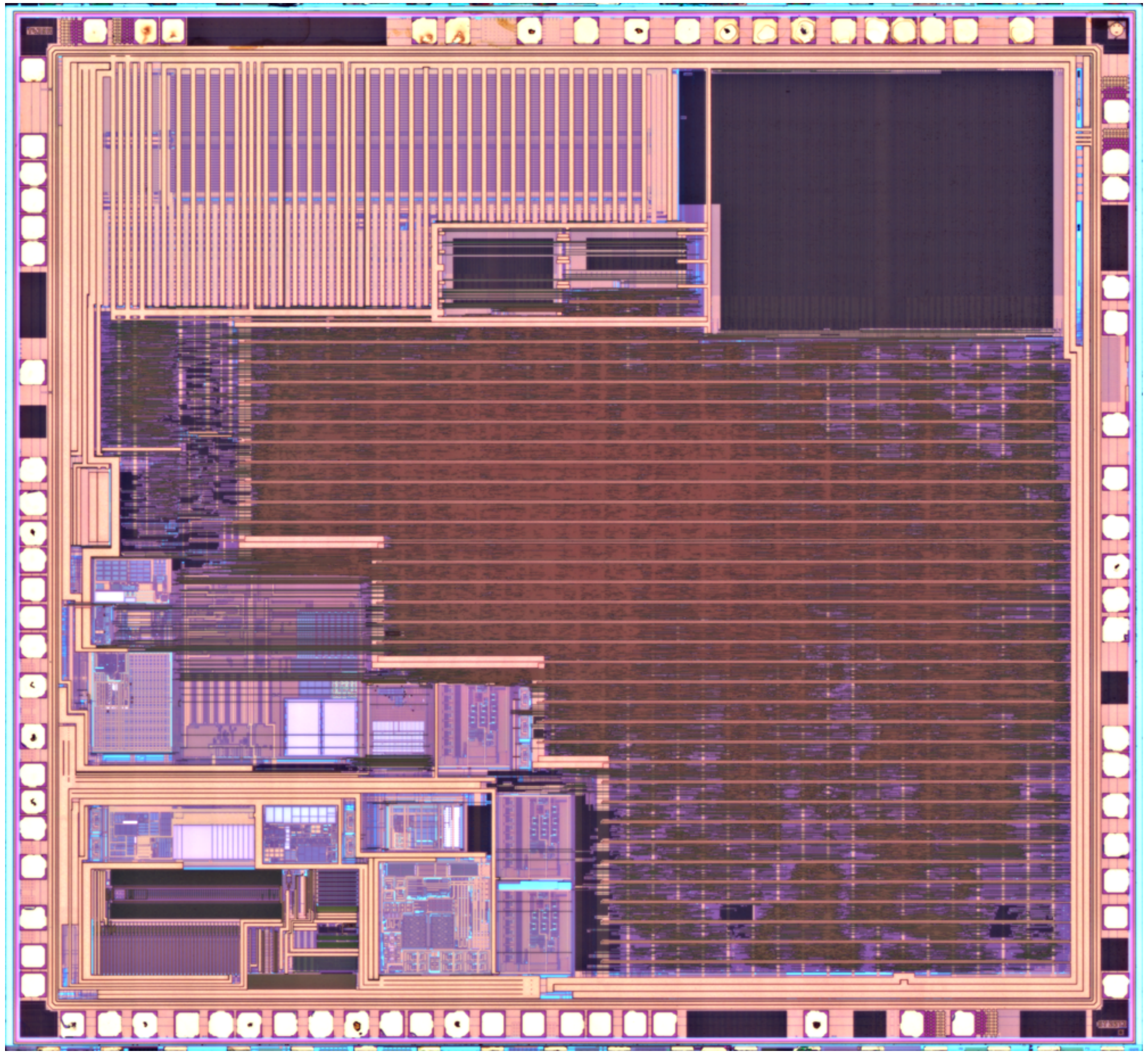
- Although we will cover SoCs as well, secure micro controllers are often the target of attacks in the wild.

- They are self contained systems consisting of a single IC.

- Secure micro controllers integrate a CPU, program memory and storage for sensitive data.

- Secure micro-controllers are available in different form-factors

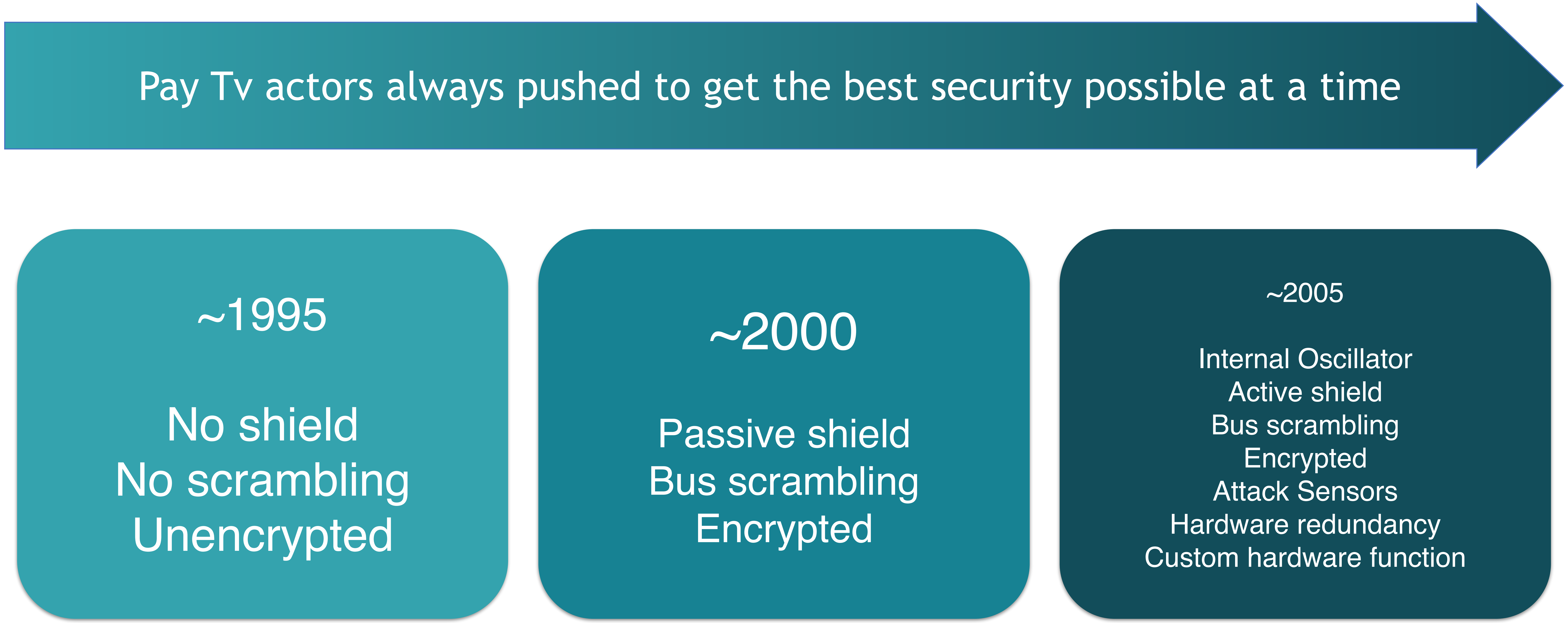
- Members of a particular product family will share device characteristics.



STM_STM32-F3_STM32f302k8u6_top_10x

Devices on the spot

Pay-Tv : Integrated Circuits (IC) Hacking



Pay Tv actors always pushed to get the best security possible at a time

~1995

No shield
No scrambling
Unencrypted

~2000

Passive shield
Bus scrambling
Encrypted

~2005

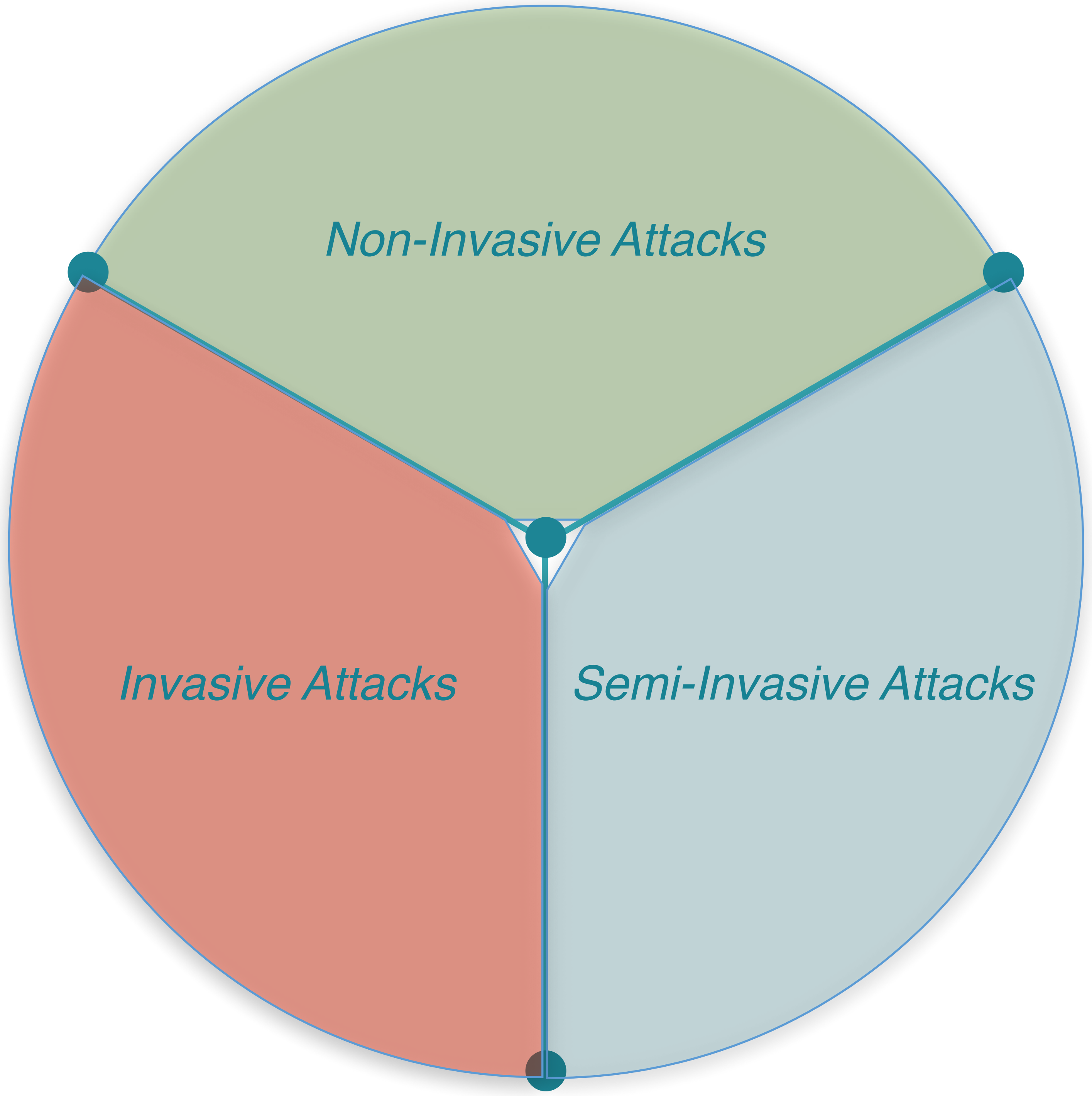
Internal Oscillator
Active shield
Bus scrambling
Encrypted
Attack Sensors
Hardware redundancy
Custom hardware function

Attack Landscape

3 Major Attack Classes

Non Invasive Attacks

- No direct chip access
- Only use external signals
  - Manipulate signal
    - VCC / Clk glitch
  - Listen to signals : Side Channel
    - SPA / DPA



Invasive Attacks

- Access to the chip
- Physical modification allowed
  - Microprobing
  - Reverse-Engineering
  - Counter-Measure bypass
  - …

Semi-Invasive Attacks

- Access to the chip
- No physical modification
  - LFI
  - EM Attacks
  - …

The Training

Goal

- IC RE is not impossible and in many cases fairly straightforward
  - Understand digital electronics
  - Understand analysis mindset
  - Understand the time and resources required
  - Understand the equipment:
    - Sample preparation
    - High-Res (Scanning Electron Microscope)
    - Automated analysis techniques

I want to give you an almost exhaustive view on hardware reverse engineering techniques and capabilities

- so you can decide if that is a domain you want to investigate more
- to raise awareness about the associated threats

COURSE SYLABUS

- INTRODUCTION
- RECOMMENDED READING
- INTEGRATED CIRCUIT
  - Target Identification
  - Some IC Packages
  - Bonding Wires
  - Structure of an IC
- TRANSISTORS
  - Physical Construction
  - Mode of Operation
  - Usage
  - CMOS Logic
  - Abusing Transistors
- DIGITAL ELECTRONICS
  - COMBINATORIAL LOGIC
    - The Inverter
    - Building Truth Tables and Finding the Function
      - ◉ Assignment 1 : Build the Truth Table - Basic
      - ◉ Assignment 2 : Build the Truth Table - Basic
    - Simplifying Boolean Equations
      - ◉ Assignment 3 : Build the Truth Table - Find the Standard Cell Function
    - Sequential Logic Building Blocs
      - ◉ Assignment 4 : Draw Complex Standard Cells - Find the Standard Cell Function
      - ◉ Assignment 5 : Draw Complex Standard Cell from its Function
    - Building Functions
      - ◉ Assignment 6 : Half Adder
      - ◉ Assignment 7 : Full Adder
    - Cascading
    - Datagram
      - ◉ Assignment 8 : Build Timing Diagrams
  - SEQUENTIAL LOGIC
    - CPU Architecture Basics
    - Registering Data
    - Register Transfer Layer
      - ◉ Assignment 9 : Find the Critical Path
  - MEMORIES
    - CPU Architecture Basics
    - Memories Architecture
      - ◉ Assignment 10 : Build an Address Decoder

COURSE SYLABUS

- Memory Types
  - ◉ Assignment 11 : Extract the ROM bits
  - ◉ Assignment 12 : Extract the Scrambled ROM

- MANUFACTURING PROCESS
  - Manufacturing Steps
  - Planarization
  - Main Processes
  - Layout
  - Stick Diagrams
    - ◉ Assignment 13 : Draw Stick Diagrams
  - Finding the Digital Circuit

- FAILURE ANALYSIS
  - Regular Use of FA Equipments
  - FA for Reverse-Engineering
  - The RE Process

  - DEPROCESSING / DELAYERING
    - Depackaging
    - Cross-sections

    - PRINCIPLE
      - Tilt setup
      - Naming Convention
      - Deprocessing Theory

    - WET CHEMICALS

    - DRY CHEMICALS

    - CMP

  - IMAGERY
    - Optical Imagery
    - SEM Imagery

  - CIRCUIT MODIFICATION
    - Repackaging
    - FIB Circuit Edit
    - Micro-Probing

- INVASIVE ATTACKS
  - FIRST STEP
    - ◉ Assignment 14 : Process Definition
    - Overview Analysis
      - ◉ Assignment 15 : Overview Analysis
      - ◉ Assignment 16 : Overview Analysis

  - READING ROM

COURSE SYLABUS

- READING FLASH
  - LINEAR CODE EXTRACTION
    - CPU Architecture Basics
    - LCE Principle
    - Simple LCE
      - Assignment 17 : Find Area of Interest
      - Assignment 18 : Picture Analysis
      - Assignment 19 : Define the Attack Strategy
    - Using Charge Pump for Reliability
    - Controlled LCE

- INVASIVE ATTACKS INVOLVING REVERSE ENGINEERING
  - REVERSE-ENGINEERING STANDARD CELLS
    - Creating an Attack Scenario - Game
      - Assignment 20 : Find a memory extraction spot
      - Assignment 20.1 : RE a standard cell and adapt the attack strategy : SC_1
      - Assignment 20.2 : RE a standard cell and adapt the attack strategy : SC_2
      - Assignment 20.3 : RE a standard cell and adapt the attack strategy : SC_3
      - Assignment 20.4 : RE a standard cell and adapt the attack strategy : SC_4
      - Assignment 20.5 : RE a standard cell and adapt the attack strategy : SC_5
      - Assignment 20.6 : RE a standard cell and adapt the attack strategy : SC_6
      - Assignment 20.7 : RE a standard cell and adapt the attack strategy : SC_7
      - Assignment 21 : Finding weaknesses inside a Standard Cell
      - Assignment 21.1 : RE a standard cell and adapt the attack strategy : SC_7'
      - Assignment 22 : Is the RAM encrypted?

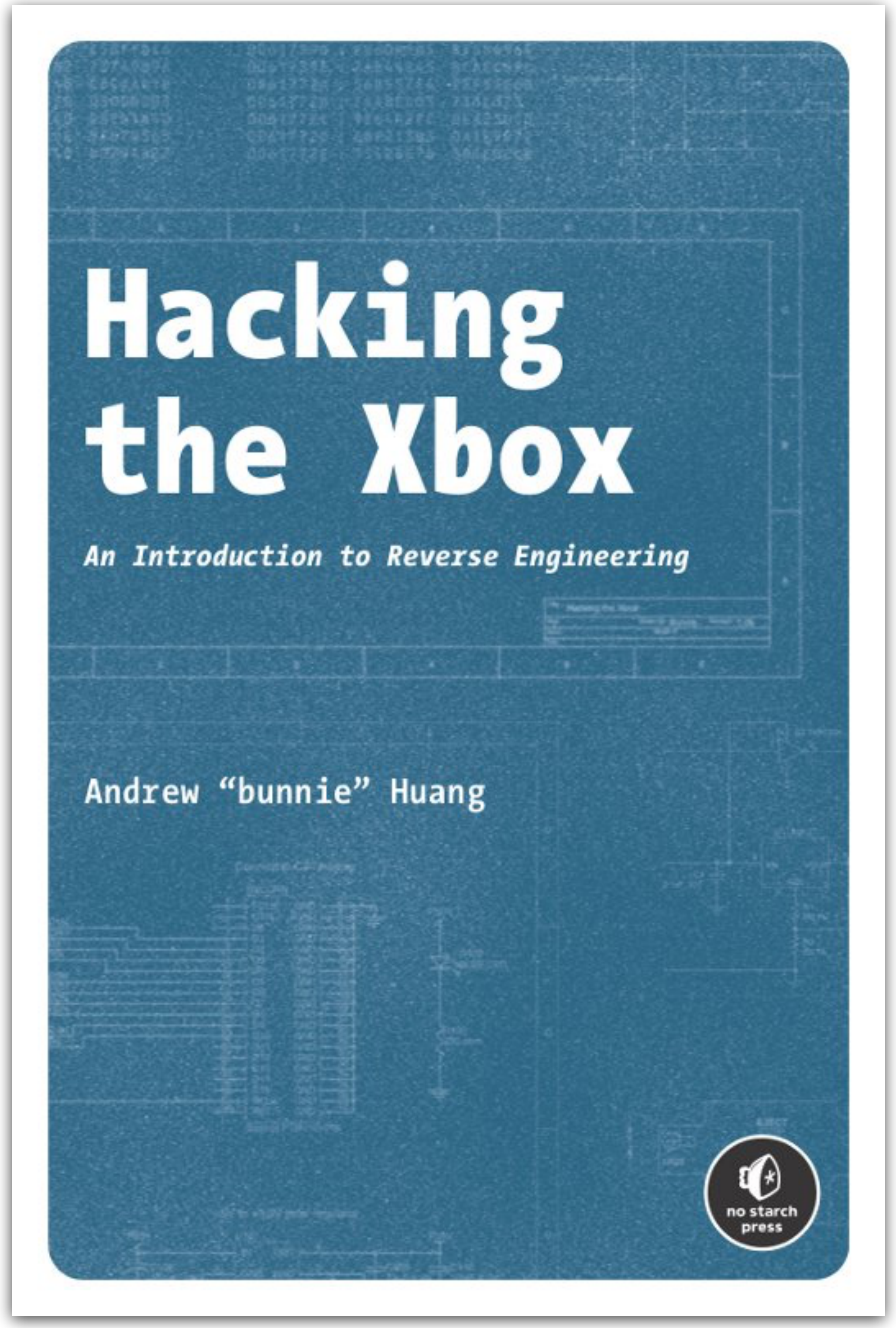
- SHIELD / MESH

- AUTOMATING THE REVERSE ENGINEERING
  - Example
  - Impact on Common Criteria

RECOMMENDED READING

Recommended Reading

Hacking the Xbox



Hacking the Xbox

An Introduction to Reverse Engineering

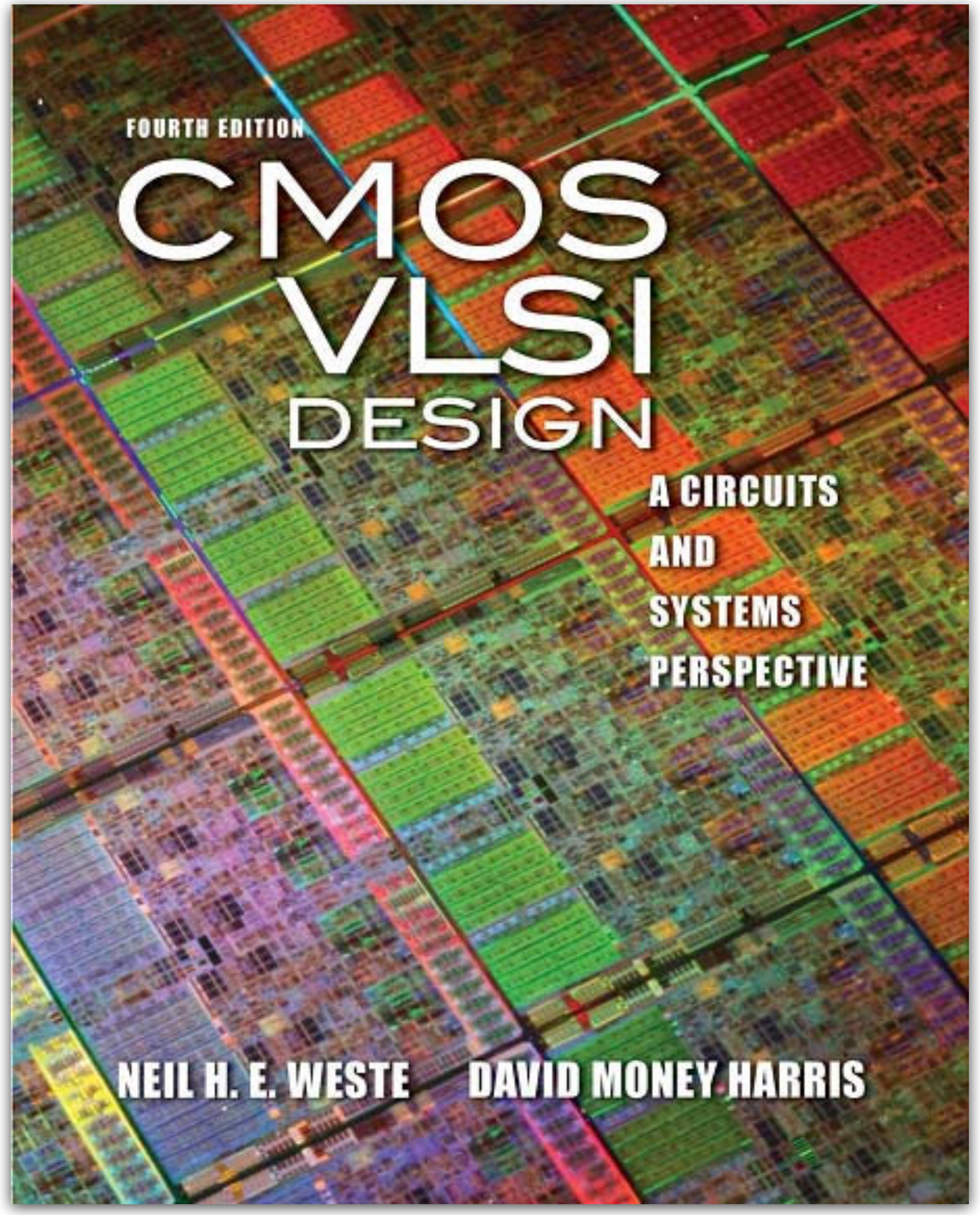
Andrew “bunnie” Huang

no starch press

- Author: Andrew “bunnie” Huang
- Publisher: No Starch Press
- Explains in detail how the Microsoft Xbox was compromised.
- Describes how to build tools to dump the data from a high-speed interconnect on the Xbox.
- Also a great introduction to hardware hacking in general.
- Available for free as a PDF.

Recommended Reading

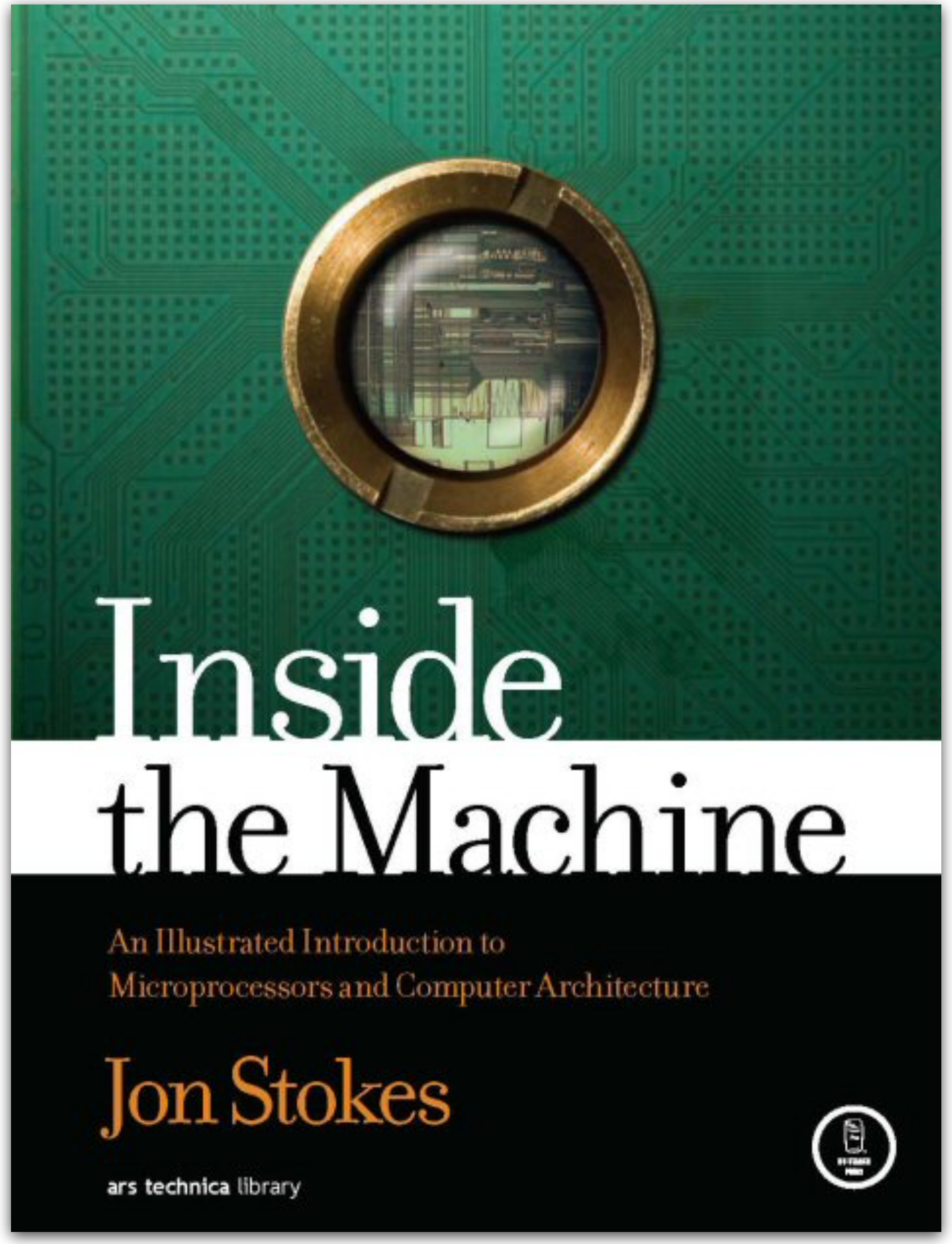
CMOS VLSI Design



- Authors: Neil H.E. Weste & David Money Harris
- Publisher: Addison-Wiley
- Popular in U.S. engineering programs
- Very good overview of basics as well as advanced concepts
- Thorough example of the construction of MIPS CPU

Recommended Reading

Inside the Machine


Inside the Machine
An Illustrated Introduction to Microprocessors and Computer Architecture
Jon Stokes
ars technica library

- Author: Jon Stokes

- Publisher: No Starch Press

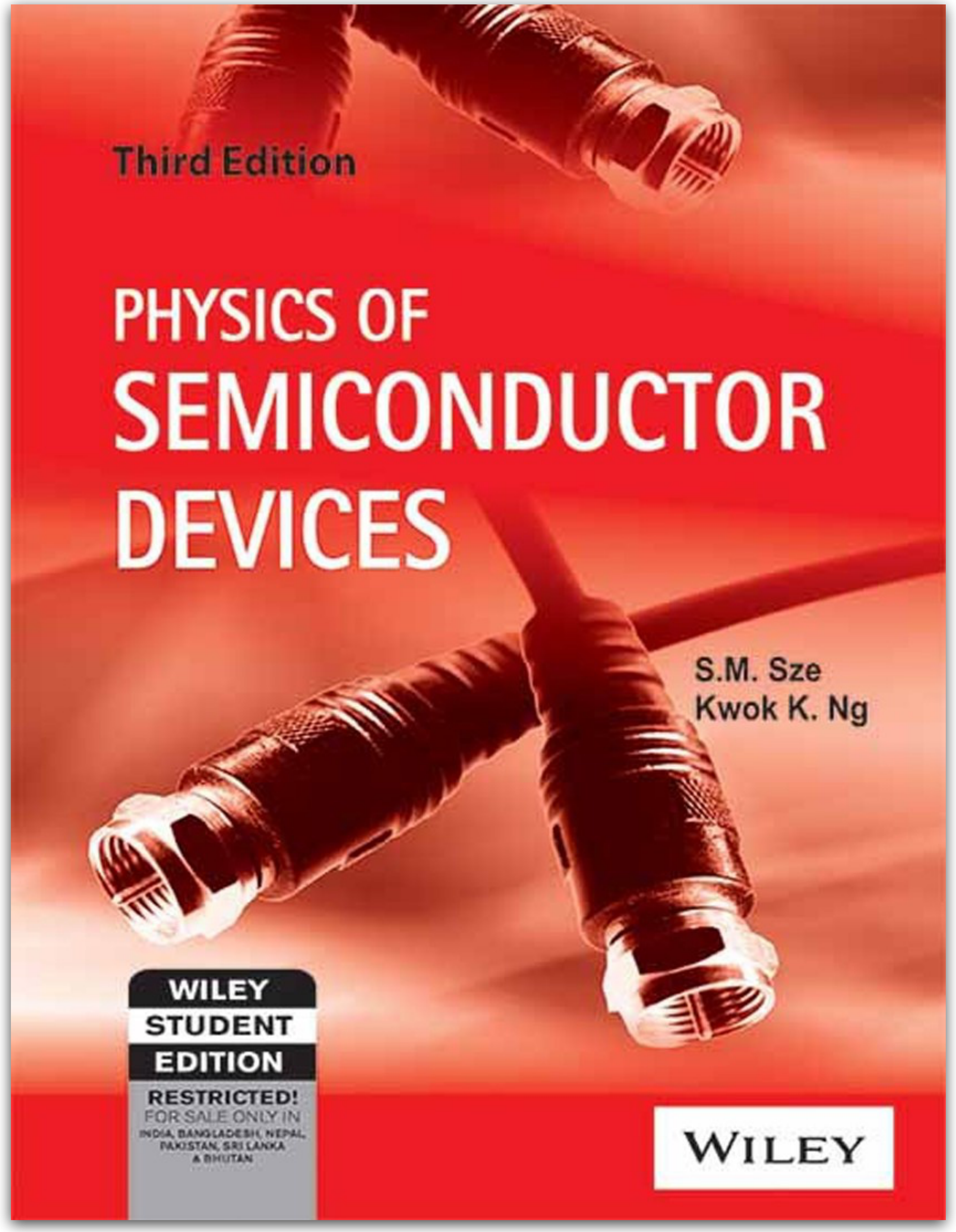
- The first 3 chapters cover CPU Basics:

1. Basic Computing Concepts
2. The Mechanics of Program Execution
3. Pipelined Execution

- And lots of info about modern CPU architectures (PowerPC 970, x86-64, …)

Recommended Reading

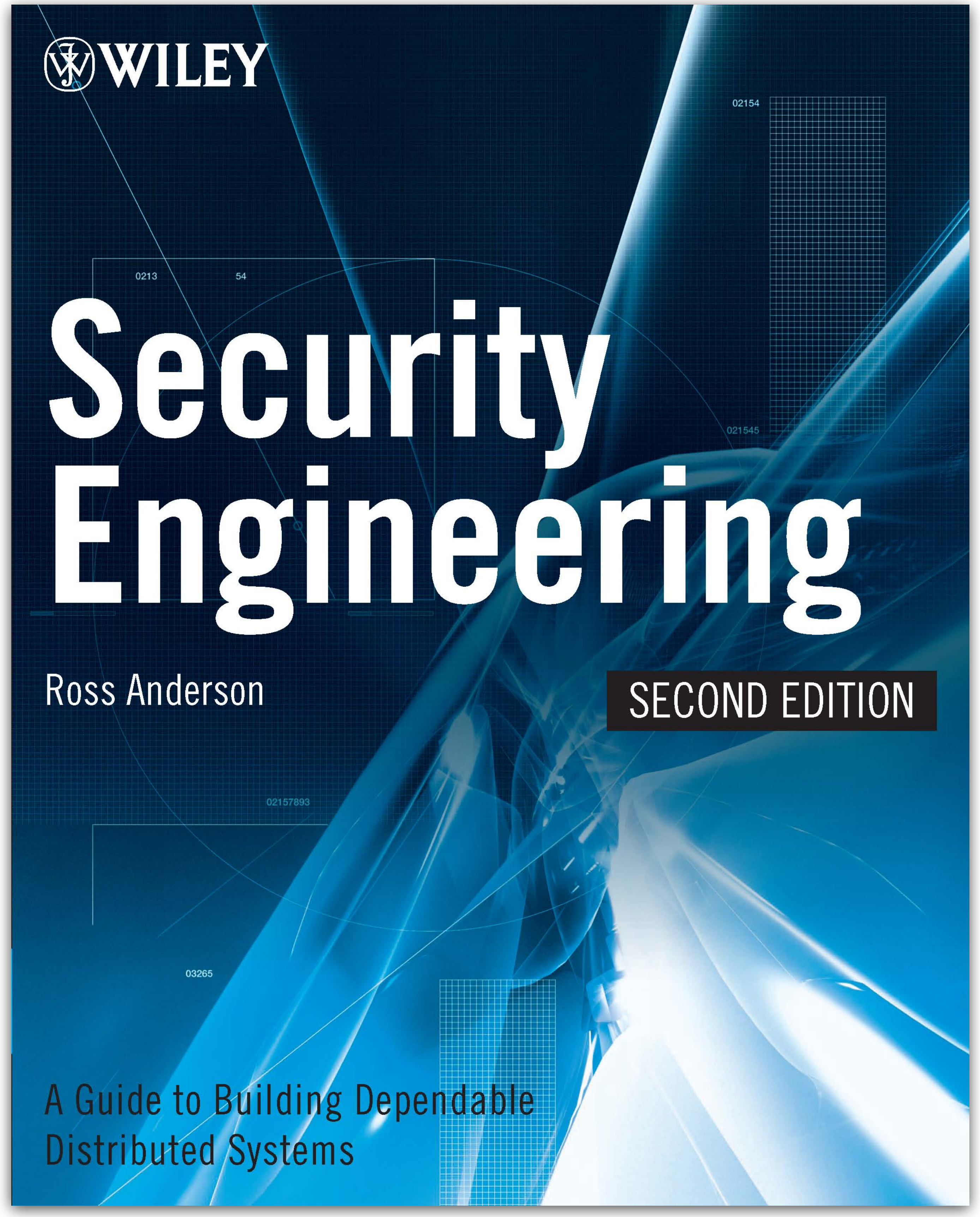
Physics of Semiconductor Devices


Third Edition
PHYSICS OF SEMICONDUCTOR DEVICES
S.M. Sze
Kwok K. Ng
WILEY STUDENT EDITION
RESTRICTED! FOR SALE ONLY IN INDIA, BANGLADESH, NEPAL, PAKISTAN, SRI LANKA & BHUTAN
WILEY

- Authors: Sze, Ng
- Publisher: Wiley
- Third edition
- One of the most popular university textbooks for semiconductor physics.
- Explains everything starting from basic transistor theory to photonic emissions
- Good reference for floating gate technologies

Recommended Reading

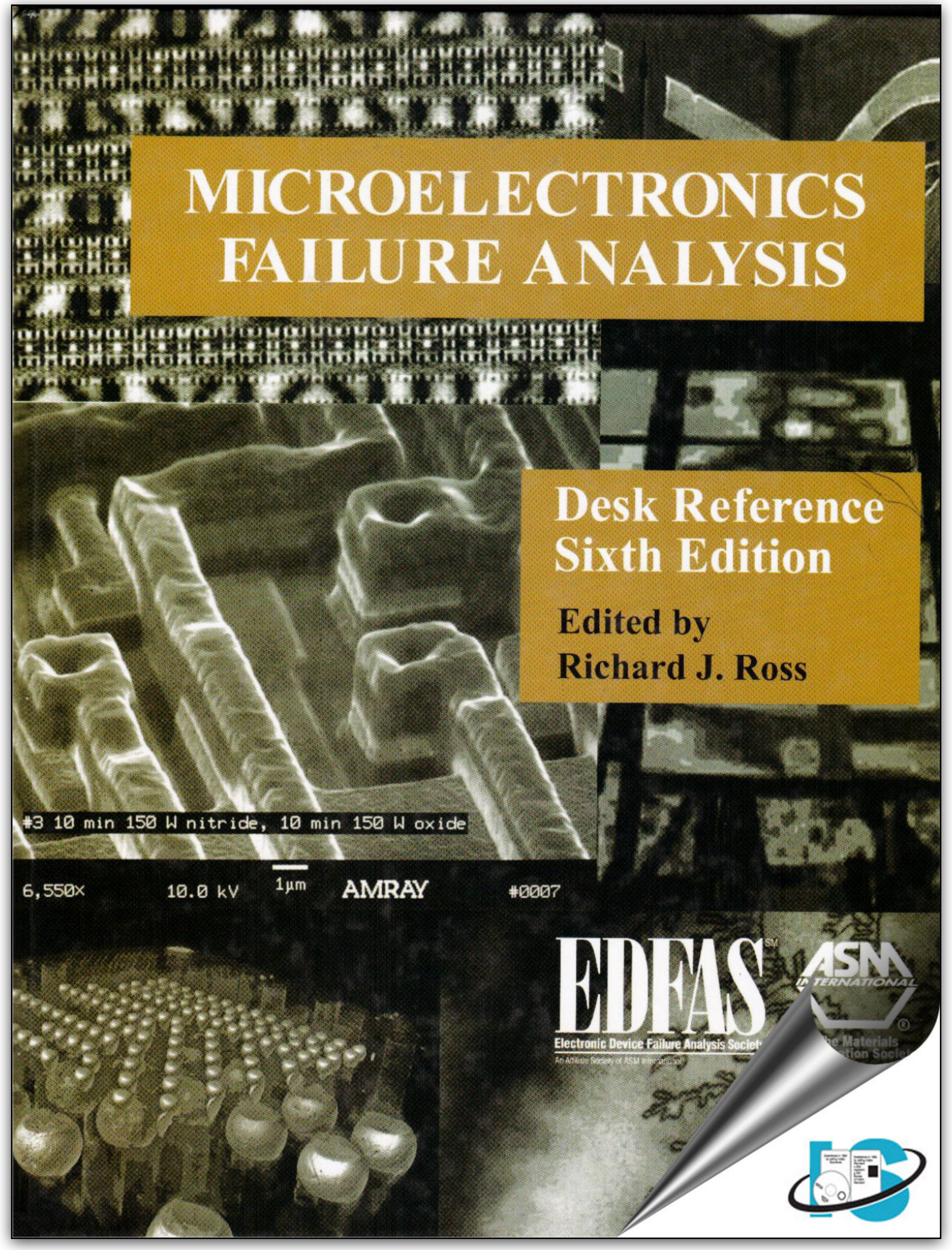
Security Engineering



- Author: Ross Anderson
- Publisher: ASM International
- Second Edition
- Free to download
- Read just the following chapters:
  - Chapter 16 “Physical Tamper Resistance”
  - Chapter 17 “Emission Security”

Recommended Reading

Microelectronics Failure Analysis



- Editor: Richard J. Ross
- Publisher: ASM International
- Sixth Edition
- Good reference for advanced failure analysis (FA) and sample preparation techniques
- A collection of academic papers