Hardware Security:
Present challenges and Future directions

Dr Sergei Skorobogatov

http://www.cl.cam.ac.uk/~sps32 email: sps32@cam.ac.uk
Outline

• Introduction
• History of powerful physical attacks
• Knowledge and predictability of attacks
• Challenges to hardware engineers
• Attacking modern devices
• Future directions
• Conclusion
Introduction

• Senior Research Associate at the University of Cambridge
  – Hardware Security research (attack technologies) since 1995
  – Test microcontrollers, smartcards, FPGAs and SoCs for security
  – Knowledge: chemistry, electronics, physics (MSc), computers (PhD)
  – PhD in Hardware Security from the University of Cambridge (2005)

• Strong track record of new and “impossible” attack methods
  – 1996: clock glitching attacks on security in MC68HC05 and MC68HC11 MCUs
  – 1999: power glitching attacks on security in PIC16F62x/8x and AT90SCxx MCUs
  – 2002: discovery of optical fault injection attacks shook the industry
  – 2005: prove of data remanence in EEPROM and Flash memory
  – 2006: use for combined attacks of fault injection with power analysis
  – 2009: use of optical emission analysis to complement power analysis
  – 2010: bumping attacks that can extract AES key and data from Flash memory
  – 2012: hardware acceleration to power analysis for finding backdoors
  – 2016: demonstration of “impossible” NAND mirroring attack on iPhone 5c
  – 2016: direct SEM imaging of EEPROM and Flash memory contents
  – 2017: data extraction from encrypted data bus using microprobing attack
  – 2018: live decapsulation carried on a battery powered chip
Introduction

• Hardware security is becoming an important trend
  – if the hardware has a vulnerability then defences at software level are unlikely to help
  – in real world systems there is a trend towards systems-on-chip (SoC) and reconfigurable hardware

• Secure systems are being attacked
  – theft of service – attacks on service providers: satellite TV, IoT, electronic meters, access cards, software protection dongles
  – access to information: information recovery and extraction, gaining trade secrets (IP piracy), ID theft, Firmware extraction
  – cloning and overbuilding: copying for making profit without investment in development, low-cost mass production by subcontractors
  – denial of service: dishonest competition, electronic warfare

• Attack technologies are being constantly improved
  – so should the defence technologies
Introduction

• There is growing demand for secure chips
  – car industry, service providers, chip manufacturers, IoT
  – banking industry and military applications

• Technical progress pushed secure semiconductor chips towards ubiquity
  – consumer electronics (authentication, copy protection)
  – aftermarket control (spare parts, accessories, consumables)
  – access control (RF tags, cards, tokens and protection dongles)
  – service control (mobile phones, satellite TV, license dongles)
  – intellectual property (IP) protection (software, algorithms, design)

• Challenges
  – How to design a secure system? (hardware security engineering)
  – How to evaluate the protection? (estimate the cost of breaking)
  – How to find the best solution? (minimum time and money)
History of attacks

• Direct data extraction from embedded memory: Mask ROM
  – before 1990s: encoded in transistor mask, poly, M1 or M2 layer, vias
  – since 1990s: information is encoded with doping level
  – impossible to see under optical microscope or SEM
  – Failure Analysis helps with defects etching
    • O. Kömmerling, M. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. USENIX 1999
  – countermeasures at silicon level or obfuscation/encryption
  – Was this outcome predictable?
    • chip manufacturers are well aware about fabrication process and Failure Analysis methods
History of attacks

- Power analysis reveals deep secrets
  - leakage from switching CMOS transistors is correlated with processed data
    - can break passwords and crypto keys
    - countermeasures are very sophisticated
  - Was this outcome predictable?
    - chip manufacturers use standard tools to calculate power dissipation
History of attacks

- Optical fault injection
  - CMOS transistors and memory cells can be controlled with a laser beam
    - S. Skorobogatov, R. Anderson: Optical Fault Induction Attacks. CHES 2002
  - confirmed down to 28nm devices
  - countermeasures at silicon level
  - Was this outcome predictable?
    - chip manufacturers new that radiation causes circuits to malfunction
History of attacks

- Data remanence in Flash/EEPROM
  - residual information present after memory Erase operation
    - S. Skorobogatov: Data Remanence in Flash Memory Devices. CHES 2005
    - could lead to recovery of sensitive data
    - once learned can be easily defeated
    - Was this outcome predictable?
      - was known for magnetic media
History of attacks

• Combined attacks
  – Power analysis + Fault injection
    • S. Skorobogatov: Optically Enhanced Position-Locked Power Analysis. CHES 2006
  – more powerful and localised
  – countermeasures are hard to implement
  – Was this outcome predictable?
    • attacks were not considered because simpler attacks did exist

read memory location (laser Off/On)
write memory location (laser Off/On)
read memory location (laser Off/On)
contents of memory changed by laser
History of attacks

- **Optical emission analysis**
  - switching CMOS transistors emit photons
  - can be detected with CCD cameras (2D) and photomultiplier tubes (time resolved)
    - S. Skorobogatov: Using Optical Emission Analysis for Estimating Contribution to Power Analysis. FDTC'09
  - countermeasures are hard to implement
  - Was this outcome predictable?
    - was known for many years that semiconductor devices emit photons
History of attacks

- **Bumping attacks**
  - memory 'Bumping attacks' is a new class of fault injection attacks aimed at the on-chip internal integrity check procedure
    - Sergei Skorobogatov: Flash Memory 'Bumping' Attacks. CHES 2010
  - simple 'bumping' is aimed at blocks of data down to bus width
  - 'selective bumping' is aimed at individual bits within the data bus
  - countermeasures can be implemented at silicon design level
  - Was this outcome predictable?
    - can be simulated with chip design tools
History of attacks

• Finding backdoor in secure FPGA
  – Pipeline Emission Analysis (PEA) technique improves side-channel analysis
    • S. Skorobogatov, C. Woods: Breakthrough silicon scanning discovers backdoor in military chip. CHES’12
  – dedicated hardware rather than off-the-shelf equipment
  – lower noise, higher precision, low latency, fast processing
  – countermeasures are the same as for DPA
  – Was this outcome predictable?
    • could be as there were fast hardware approaches to tasks of breaking ciphers
History of attacks

• NAND mirroring attack on iPhone 5c
  – resetting passcode attempt counter by rewriting Flash storage
    • Sergei Skorobogatov: The bumpy road towards iPhone 5c NAND mirroring. arXiv 2016
  – FBI Director claimed that making a copy of the phone’s chip to get around the passcode "doesn’t work" and aimed at "software-based"
  – hardware approach was not straightforward
    • the iPhone 5c sample was taken apart
    • NAND Flash chip was desoldered and placed on a socket
    • proprietary NAND protocol was learned using logic analyser
    • special tool was built to clone the NAND Flash chips
    • the cloned NAND chip allowed the passcode to be entered again 6 times without any delay
  – Was this outcome predictable?
    • could be tested without problem by government labs
History of attacks

- Flash/EEPROM imaging under SEM
  - more efficient and faster than Scanning Probe Microscopy (SPM)
  - destructive to memory cells
  - physical limits for detectable charge
  - countermeasures are hard to implement
  - Was this outcome predictable?
    - was not considered until latest SEMs with PVC

0.35µm Flash in Atmel microcontroller
0.21µm EEPROM in Atmel smartcard
0.35µm Flash in TI microcontroller
History of attacks

• Bypassing data bus encryption with microprobing
  – injecting data into encrypted data bus between CPU and memory
    • Sergei Skorobogatov: How microprobing can attack encrypted memory. Euromicro DSD, AHSA 2017
  – injecting code into data bus until CPU executes required command
  – execute Trojan code to gain access to the memory
  – countermeasures can be implemented at hardware level
  – Was this outcome predictable?
    • was used before in systems with encrypted external memory
History of attacks

• Gaining access to the chip surface on battery backed chips
  – using chemical decapsulation on live circuits
    • Sergei Skorobogatov: Is Hardware Security prepared for unexpected discoveries? IPFA 2018
  – Vasco Digipass 270 authentication token
    • battery-backed SRAM storage for keys
    • the device stops working on losing power or if Reset is applied
  – sample preparation
    • insulated and protected the PCB with tape
    • created stencil using aluminium tape
    • applied hot 100% Nitric Acid via stencil
    • washed and cleaned with Acetone
  – countermeasures could involve surface sensors
  – Was this outcome predictable?
    • was expectable for low-cost mass produced devices
Challenges

• Embedded memory in ICs
  – Mask ROM: bootloader, firmware, algorithms
  – EEPROM: variables, keys, passwords
  – Flash: bootloader, firmware, algorithms, keys, passwords

• Memory extraction is the crucial step in attacks
  – access to firmware for reverse engineering
  – extraction of crucial algorithms
  – access to sensitive data, keys and passwords
  – rely on Failure Analysis methods for advanced attacks
Challenges

• Data extraction from mechanically damaged devices
  – restore challenging packages (QFN, BGA)
  – recovering information from shattered dies

• Data extraction from electrically damaged devices
  – recovering information from chips with burned I/O
  – recovering information if logic is burned

• More efficient methods have to be developed
  – SPM methods are very slow and damaging
  – SEM methods have limitations and damaging
Challenges

• Hardware security in EEPROM and Flash memory
  – EEPROM and Flash memory store information in the form of electrical charge on a floating gate of memory cell transistor
  – floating gates leave no physical imprint on the silicon
    • Virage Logic: Reverse engineering Techniques in CMOS Based NVM, 2009
  – conventional deprocessing methods destroy charge and data
    • Actel: Design Security in Nonvolatile Flash and Antifuse FPGAs, 2003
  – highly resistant against non-invasive and invasive attacks

• Previous attack methods are inefficient and expensive
  – SPM methods
    • Scanning Capacitance Microscopy (SCM)
    • Scanning Kelvin Probe Microscopy (SKPM)
  – require special sample preparation and multiple samples
  – require expensive equipment and also time consuming
  – likely to damage samples during preparation, handling or scanning

• SEM attack methods are more efficient and affordable
  – SEM methods: Passive Voltage Contrast (PVC) with TLD/SE2
  – simpler sampler preparation and widely available microscopes
Is Flash/EEPROM secure enough?

• Is there really a problem with silicon hardware?
  – How fast and reliable could Flash and EEPROM be extracted?
  – Can their contents be extracted at a very low cost in the future?
  – Could lead to affordable reverse engineering of firmware

• Secure devices are everywhere
  – Banking cards, car keys, access cards, smart batteries, printer cartridges, smart meters, smartphones

• Secrets are usually combined
  – Reverse engineering is needed to extract algorithm
  – Data extraction gives encrypted values
  – Key extraction combined with algorithm give plaintext data

• Data secrecy rely on data extraction challenges
  – Common wisdom of Flash/EEPROM being the most secure
  – High cost and low success rate of existing methods (e^- are too small, leave no impact and hard to detect)
How secure is Embedded memory?

- **Mask ROM**
  - invasive extraction based on Failure Analysis methods

- **EEPROM**
  - large memory cells, small memory size
  - both SPM and SEM methods work well
  - new methods being developed for smaller fabrication processes

- **Flash**
  - small memory cells, especially for NAND types
  - large memory size, especially for NAND types
  - only SEM methods are practical
  - new methods being developed for smaller fabrication processes

- **SRAM**
  - sophisticated Failure Analysis methods using lasers
  - ongoing research into innovative invasive methods
Flash/EEPROM: Speed, Size, Process

• It is all about the cost and state-of-the-art is commercially developed
  – publicised achievements: 250nm, 48kB 1T Flash, 5hrs, 7 errors
    • Sergei Skorobogatov: Deep dip teardown of tubeless insulin pump. arXiv 2017
  – consulting: 130nm, 400kB 1T Flash + 64kB 2T EEPROM, 7hrs, 5 errors
  – in development: 65nm, 200kB 1T Flash
• Modern Flash: 14nm/16nm NAND and 28nm/40nm NOR (embedded)
• SEM PVC have limits, but methods under development will aim at 16nm
• Automation can bring extraction speed to 1MB/hour or 1GB/day (MSEM)
• Size is limited by sample preparation – no limit with proper tools: >1GB
Have we learned everything?

• Successful attacks do take place
  – access cards, banking cards
  – IP piracy is well established with cloning and overbuilding
  – denial of service ran by dishonest competitors
• Does defence technology go ahead of attack technology?
• There is growing demand for secure chips
  – How are they tested?
• Industry depends on limited manufacturers and designs
  – Where most chips are designed?
  – Who fabricates the silicon?
• Hardware assurance: Do you get exactly what you wanted?
  – Are there enough of trustworthy manufacturers?
  – How to perform silicon testing for trojans and backdoors?
Attack categories

- **Side-channel attacks**
  - techniques that allow the attacker to monitor the analog characteristics of power supply and interface connections and any electromagnetic radiation

- **Software attacks**
  - use the normal communication interface and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation

- **Fault generation**
  - use abnormal environmental conditions to generate malfunctions in the system that provide additional access

- **Microprobing**
  - can be used to access the chip surface directly, so we can observe, manipulate, and interfere with the device

- **Reverse engineering**
  - used to understand the inner structure of the device and learn or emulate its functionality; requires the use of the same technology available to semiconductor manufacturers and gives similar capabilities to the attacker
**Attack methods**

- **Non-invasive attacks (low-cost)**
  - observe or manipulate the device without physical harm to it
  - require only moderately sophisticated equipment and knowledge to implement

- **Invasive attacks (expensive)**
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - normally require expensive equipment, knowledgeable attackers and time

- **Semi-invasive attacks (affordable)**
  - semiconductor chip is depackaged but the internal structure of it remains intact
  - fill the gap between non-invasive and invasive types, being both inexpensive and easily repeatable
Non-invasive attacks challenges

- Non-penetrative to the attacked device and low-cost
- Types of non-invasive attacks
  - side-channel attacks: timing, power and emission analysis
  - fault injection: glitching, bumping
  - data remanence
  - brute forcing
- Challenges for side-channel attacks
  - higher operating frequency and noise: faster equipment needed
  - power supply is reduced from 5V to 1V: lower signal, more noise
  - 8-bit data vs 32-bit data: harder to distinguish single-bit change
  - more complex circuits: higher noise from other parts, hence, more signal averaging and digital signal processing are required
  - effective countermeasures for many cryptographic algorithms
Non-invasive attacks challenges

• Challenges for fault injection attacks
  – internal clock sources, clock conditioning and PLL circuits
  – internal charge pumps and voltage regulators
  – lower power supply requires more precise control over the glitch
  – checksums (CRC, SHA-1) and encryption
  – asynchronous design
  – effective countermeasures are in place: clock and supply monitors

• Other considerations
  – attack methods are normally independent from the silicon process
  – devices with flash memory are more sensitive to attacks
  – devices with higher operating frequency are harder to attack
  – devices with wider data bus are harder to attack
Semi-invasive attacks challenges

• Less damaging to target device and affordable cost

• Types of semi-invasive attacks
  – **imaging**: optical and laser techniques
  – **fault injection**: UV attack, photon injection, local heating, masking
  – **side-channel attacks**: optical emission analysis, induced leakage

• Challenges for fault injection attacks
  – internal clock sources, clock conditioning and PLL circuits
  – internal charge pumps and voltage regulators
  – checksums (CRC, SHA-1) and encryption
  – asynchronous design
Semi-invasive attacks challenges

• Challenges for side-channel attacks
  – higher operating frequency and noise: faster equipment needed
  – power supply is reduced from 5V to 1V: lower signal, more noise
  – 8-bit data vs 32-bit data: harder to distinguish single-bit change
  – more complex circuits: higher noise from other parts, hence, more signal averaging and digital signal processing are required
  – effective countermeasures for many cryptographic algorithms

• Other considerations
  – attack methods are highly sensitive to the silicon process
  – backside approach is required for 0.35µm or smaller process chips
  – BGA and pin-less packages are harder to deal with
  – limited resolution of low-cost imaging solutions
  – devices with flash memory are more sensitive to attacks
  – devices with higher operating frequency are harder to attack
  – devices with wider data bus are harder to attack
Invasive attacks challenges

- Damaging to target device and very expensive
- Types of invasive attacks
  - **imaging**: optical, laser techniques and SEM
  - **fault injection**: microprobing, chip modification
  - **side-channel attacks**: microprobing
  - **reverse engineering**
- Challenges
  - attack methods are highly sensitive to the silicon process
  - backside approach is required for 130nm or smaller process chips
  - very high cost imaging solutions for 180nm or smaller process chips
  - BGA and pin-less packages are harder to deal with
  - devices with higher operating frequency are harder to attack
  - devices with wider data bus are harder to attack
  - countermeasures are in place: active mesh sensors, CRC, crypto
Future work

• Improving semi-invasive attacks
  – some chips down to 65nm were tested
  – preparation for testing 40nm and 28nm chips is under way

• Seeking collaboration with industry
  – evaluation of products against new attacks
  – developing new attack methods and techniques
  – desire to establish hardware security research centre

• New challenges
  – synchronisation techniques for side-channel attacks
  – improving side-channel attacks with new techniques
  – advanced data extraction methods from Flash and SRAM

• Developing new countermeasures
  – if it takes a few seconds to extract crypto-key or password then
    existing countermeasures may fail to protect from adversaries
Future work

• Is it possible to predict new attacks?
  – need for hardware security educated engineers
  – desire for open minded design reviewers

• Unexpected attacks: bad or good
  – it helps in understanding the nature
  – what is bad for chip manufacturers might be good for technological progress
  – new materials could be created
  – new processes could be developed
  – new solutions to existing problems could be found
Conclusion

• There is no such thing as absolute protection
  – given enough time and resources any protection can be broken

• Attack technologies are constantly evolving
  – do not underestimate capabilities of the attackers
  – technical progress reduces cost of already known attacks
  – most attacks are based on well known facts and phenomena

• Defence should be ahead of attack technologies
  – Hardware Security engineers must be familiar with existing attack technologies to develop adequate protection
  – many chips unavoidably have backdoors as a part of fabrication and testing process, but they must be made as secure as possible to prevent attacks

• Many vulnerabilities were found in various secure chips and more are to be found posing more challenges to hardware security engineers
Thank You!