Hints from Hardware Security for solving real-world challenges

Dr Sergei Skorobogatov

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

• Introduction to Hardware Security
• What can be done during challenging time of the lockdown
  – direct help: making life better
  – indirect help: encouragement and ideas
• Facing challenges and coming up with workarounds
• Future work
• Conclusion
Introduction

• Hardware Security is important
  – data and IP protection
  – cyber security and preventing attacks on services
  – countermeasures against all known attacks
  – educate hardware engineers

• Hardware Security is about finding flaws and fixing them
  – evaluation of implemented security features and improving them

• Hardware Security challenges
  – new attack technologies
  – modern fabrication processes (7nm, 10nm, 14nm, 28nm, 32nm, 40nm)
  – develop countermeasures through understanding of flaws
  – predict new attack methods

• What could we possibly learn from Hardware Security?
  – innovative approaches to virtually impossible tasks
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), computer science (PhD)
• 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 AT90Sxxx 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
What can be done during challenging time

- Hardware Security research does not run very well in the lockdown
  - physical devices are not always small
  - sample preparation is sometime a messy process (chemicals, machinery)
  - experimental setup could be bulky or require special environment

- Hardware Security could still help with solving challenges
  - authentication against unauthorised counterfeiting (supply chain security)
  - temporary solutions for authorised authentication (supply chain disruption)
  - build compatible products if normal supply is struggling

- Hardware Security could encourage research in other areas
  - find workarounds if obstacles are encountered
  - bring innovations to new approaches and “impossible” methods
  - come up with new “crazy” ideas

- What could we possibly learn from Hardware Security?
  - innovative approaches to virtually impossible tasks
Direct methods

• Authentication of devices
  – Defence: prevent counterfeit products by improving hardware security
  – Attack: allow legitimate ways of bypassing protection in disrupted supply

• Invasive attacks (high cost and long setup time)
  – silicon deprocessing and reverse engineering
  – microprobing and chip modification

• Semi-invasive attacks (medium cost and setup time)
  – optical imaging and emission analysis
  – optical fault injection

• Non-invasive attacks (low-cost and short setup time)
  – brute forcing
  – side-channel: eavesdropping, timing, power and electromagnetic analysis
  – power glitching and electromagnetic fault injection
  – data remanence
Indirect methods

• Bringing ideas and innovative thinking rather than actual solutions
• Challenge: bypass code/data protection in microcontrollers
  – detection and analysis of counterfeit products
  – compatibility purposes: develop alternative solution
  – teaching and training
• Solution
  – fault injection using power glitching
  – was used since early 90s
  – improved with bipolar glitching in late 90s
  – demonstrated on data remanence in 2018
• Lesson
  – undocumented feature (or bug) in SRAM and flip-flops
  – data remanence time could be reduced by several orders of magnitude

Indirect methods

- **Challenge:** disrupt normal devices operation
  - inject faults into cryptographic operations
  - take control over device operation
  - bypass security protection mechanisms

- **Solution**
  - optical fault injection using laser beam
  - was successfully used since early 2000s

- **Lesson**
  - exploiting unusual features of MOSFET transistors (light sensitivity)

Indirect methods

• Challenge: recover data from erased memory
  – information recovery
  – forensic analysis of devices

• Solution
  – residual information present in memory cells after memory Erase operation
  – possibility of data recovery was demonstrated in 2005

• Lesson
  – undocumented features of memory transistors (incomplete erasure)

Indirect methods

- **Challenge:** learn about device operation and recover data
  - information recovery and partial reverse engineering
  - extraction of cryptographic keys

- **Solution**
  - combining optical fault injection and power analysis
  - were introduced in 2006

- **Lesson**
  - more powerful attacks could be created by combining several methods


![Graphs showing memory location changes](#)

- read memory location (laser Off/On)
- write memory location (laser Off/On)
- contents of memory changed by laser
Indirect methods

- **Challenge:** bypass ‘no readback’ protection in devices
  - information and keys recovery
  - forensic analysis of devices

- **Solution**
  - memory 'Bumping attacks' as a new class of fault injection attacks aimed at the on-chip internal integrity check procedure
  - were introduced in 2010

- **Lesson**
  - leakage of information through a single Yes/No status

Indirect methods

• Challenge: bypass passcode protection in iPhone
  – increase the number of passcode entering attempts
  – forensic analysis of devices

• Solution
  – 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“ solutions
  – NAND Mirroring attack on iPhone 5C: resetting passcode counter by rewriting Flash
  – was demonstrated in 2016

• Lesson
  – workarounds could sometime work

Sergei Skorobogatov: The bumpy road towards iPhone 5c NAND mirroring. arXiv:1609.04327, September 2016
Indirect methods

- **Challenge:** recover data from Flash and EEPROM memory
  - information and keys recovery
  - forensic analysis of devices

- **Solution**
  - PVC imaging under SEM
  - more efficient and faster than Scanning Probe Microscopy (SPM)
  - was demonstrated in 2016

- **Lesson**
  - old techniques could be revisited for new capabilities

Indirect methods

• **Challenge:** recover data from battery backed embedded SRAM
  – information recovery
  – forensic analysis of devices

• **Solution**
  – decapsulation with 100% Nitric Acid
  – was demonstrated in 2018

• **Lesson**
  – “crazy” ideas might just work

Sample preparation challenges

• Physical samples are essential for Hardware Security research
  – semi-invasive methods require access to die surface

• Challenges during the lockdown
  – sample preparation is sometime a messy process (chemicals, large machinery)
  – optical fault injection requires optical tables

• Some semi-invasive methods could still work
  – UV attacks only require access to the die surface, but the chip must be operational

• Partial chip decapsulation opens up the package just above the die
  – usually decapsulation starts with shallow mechanical milling to create a cavity
  – the sample is placed on a hotplate at 60°C…70°C under fume cupboard
  – then a drop of fuming nitric acid (>95%) is applied to the sample
  – after several seconds the sample is thoroughly washed with acetone
  – the process is repeated again from the acid step until the die is fully exposed
  – then the sample is cleaned with acetone in ultrasonic bath
  – finally the sample is dried with compressed air
  – incompatible with copper bonding wires widely used in modern ICs
Sample preparation challenges

- **Is it possible to perform decapsulation without any chemicals?**
  - mechanical milling with precision CNC machine
  - laser ablation followed by microwave induced plasma (MIP) etching

- **Is it possible to do decapsulation without large and expensive tools?**
  - suitable for home use (no dangerous chemicals, compact size)
  - affordable price
  - easy to perform

- **8-bit PIC16F1938 microcontroller was chosen as a target**
  - old fabrication process (~250nm) which is sensitive to UV light
  - easy to order and fully documented
  - easy to check the results by reading Flash, EEPROM and fuses contents

- **Pure mechanical approach was used**
  - no chemicals involved apart from organic solvents
  - the most expensive tool is a simple polishing machine (~2k USD)
  - safe for copper bonding wires
Mechanical decapsulation

• Start grinding the package from the front side of the die (package top)
  – use sandpaper with large grit (P400 or P600) until bonding wires are exposed
  – continue with medium grit sandpaper (P1000 or P1500) until the die is close
  – finish with fine sandpaper (P2500 or P4000) until the die is exposed

• What about the bonding wires?
  – they will be gone by now, but don’t worry
  – bonding pads could be polished away and passivation layer scratched, but it’s OK
Mechanical decapsulation

- Is it possible to restore bonding wires?
- Wire bonding machines can do the job
  - bonding pads on the die must be clean and not damaged
  - external frame must be available to which bond the wire
  - expensive and bulky machines
- What else can be used to restore the bonding wires?
  - it is not possible to solder to the remaining bits – they are too small (~20µm)
  - maybe some kind of a conductive glue can be used
Mechanical decapsulation

• Restoring the bonding wires
  – conductive epoxy did not stick well (too low viscosity)
  – PCB trace repair paste was too thick (low viscosity)
  – conductive paint was just right

• Bonding wire restore process
  – find desired wires and bonding pads (e.g. power supply and ground pins)
  – create a template on the chip surface using masking tape
  – fill carefully the gaps with conductive paint connecting the pad with exposed wire
  – let it dry and remove the template
Mechanical decapsulation

• Bonding wire restore process
  – find desired wires and bonding pads (MCLR, PGD, PGC)
  – apply new template on the chip surface using masking tape
  – fill carefully the gaps with conductive paint connecting the pad with exposed wire
  – let it dry and remove the template
Mechanical decapsulation

• Bonding wires can be restored without any dangerous chemicals
  – affordable price
  – can be safely carried out at home
  – fully functional chip despite to scratched passivation layer and polished away pads
  – robust solution
  – worked even with the die polished at a slight angle
Limitations and improvements

• Packages
  – type and material of the package: BGA/LGA are challenging
  – size of the package: small packages are particularly hard to do
  – number of pins: large number of pins result in smaller gaps

• Programming and debugging do not require many pins
  – SWI: 1 pin
  – SWD, ICSP, SMB: 2 pins
  – JTAG, SPI: 4 pins

• Mechanical stability is also important
  – can be improved with using adhesives and fillers
Future Work

• Addressing real-world problems
  – counterfeit detection: research into secure authentication devices
  – supply chain disruption: help with developing compatible solutions

• Equipment access challenges
  – develop affordable imaging solutions (aim at $100 confocal microscope)
  – develop affordable measurement solutions (aim at $100 interferometer)
  – solution: innovation, improvisation, out-of-the-box thinking and hard work

• Collaboration with industry is essential
  – bring new ideas and test new methods
  – funding is important especially if aiming to go beyond state-of-the-art

• New horizons
  – Hardware Security ← fabrication of semiconductors ← Chemistry
  – some real-world problems: energy, diseases, ecology
  – batteries ← Chemistry → capacity, charging time, safety
  – diseases → live cells ← Chemistry ← new boundaries
Conclusion

• Hardware Security relies on innovative approach and out-of-the-box thinking
• Hardware Security can help with counterfeit detection in supply chain
• Hardware Security can help in making compatible products if supply chain is disrupted
• Real world problems could be solved in innovative and out-of-the-box thinking way with some hints from Hardware Security
• Lockdown gives time to stop and look back with scrupulous analysis
• New approaches and methods are essential in fighting modern challenges and are likely to be developed
• Can Hardware Security solve more important problems?
  – probably not directly
  – but it sometime relies on Chemistry tricks to make some “impossible” things
  – Chemistry is likely to offer solutions to many challenges
Thank you!

URL:  http://www.cst.cam.ac.uk/~sps32
      email:  sps32@cam.ac.uk