Hardware security: trends and pitfalls of the past decade

Dr Sergei Skorobogatov

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

• Introduction

• Motivations for hardware security
  – parties involved in hardware security
  – economics and psychology of hardware security

• Progress in attacks and defences
  – attack technologies
  – defence technologies

• What went wrong in hardware security
  – myths from manufacturers of secure chips
  – pitfalls in some secure chips

• Trends and projection into the nearest future

• Conclusion
Introduction

• Hardware security of semiconductor chips (all is in silicon)
  – microcontrollers with security protection and smartcards
  – CPLDs and FPGAs with security protection
  – secure memory chips and ASICs

• The talk is based on the hardware security analysis of hundreds of chips from the following manufacturers: Motorola, Microchip, Atmel, Hitachi, NEC, Xilinx, Lattice, Actel, Cypress, Zilog, Dallas, Mitsubishi, Freescale, Renesas, Altera, Texas Instruments, Intel, Scenix, Fujitsu, STMicroelectronics, Winbond, Holtek, Philips, Temic, Cygnal, Toshiba, Samsung, Ubicom, Siemens, Macronix, Elan, National Semiconductor

• Purpose of the talk is to give a general view on a situation and attract attention to problems, so I will refrain from linking a particular vulnerability to a particular product
Introduction

• Security is a part of our everyday life
• Technical progress pushed secure semiconductor chips towards ubiquity
  – consumer electronics (authentication, copy protection)
  – aftermarket control (spare parts, accessories)
  – 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 secure system? (hardware security engineering)
  – How to evaluate protection? (estimate cost of breaking)
  – How to find the best solution? (minimum time and money)
Motivations for hardware security

• Parties involved
  – chip manufacturers (make silicon chips)
  – developers (use chips in their designs)
  – attackers (break chips)
  – evaluators (help to improve things)

• Manufacturers
  – offer security as a feature for extra cost and increase their profit

• Developers
  – want protection of their IP from competitors and malicious people

• Attackers
  – want to benefit from breaking various devices

• Evaluators
  – offer service to help manufacturers and developers
Motivations for developers

• Attack scenarios (reasons to attack their products)
  – theft of service
  – cloning and overbuilding
  – theft of IP and reverse engineering
  – denial of service

• Can cloning represent the biggest threat?

• How to choose secure components for your design?
  – lack of information on hardware security features
  – no independent analysis or reviews
  – no means of comparing security in various chips (maybe just some general labels: insecure, has security, protected, secure, highly secure)
Motivations for developers

• How the cloning can harm?
Motivations for manufacturers

• Attack scenarios
  – theft of IP and reverse engineering
  – denial of business

• Cost reduction methods
  – fables production
  – old technologies, cheaper solutions and less testing
  – security via obscurity
  – low-cost and less robust security features

• Sales increase methods
  – using ‘magic’ words: Security, Military, Encryption, Protection, Unique technology, Authentication, Highly secure, Strong defence against piracy, Cannot be duplicated, Unbreakable, Impossible to attack, Uncompromising security, Buried under 10 metal layers
  – PR (look how good we are) and Black PR (look how bad they are)
Motivations for attackers

• Get profit from exploiting the attacks
  – cloning and overbuilding: make cheaper products
  – theft of service: offer on a black market at lower price
  – theft of IP and reverse engineering: offer better products
  – denial of service: dishonest competition
  – denial of business: maximise profit from vulnerabilities

• Cost reduction methods
  – use second-hand equipment
  – renting equipment
  – try to attack many products in a hope that some will have vulnerabilities
  – outsourcing
  – move to Far East
Motivations for attackers

• How could the denial of business attack work?
  – almost every product has security vulnerabilities
  – what options does the attacker have to profit from finding a bug?
    • disclose to the manufacturer
    • make it public
    • exploit it himself
    • sell on a grey market
    • demonstrate the attack and make the big news out of it
  – what if the attacker is a well organised company with highly educated specialists in economics and market analysis?
    • an average vulnerability can influence a share price at around 0.5-3%
    • hardware bugs are difficult to patch, hence, they cause more damage
    • if the time can be predicted precisely enough the attacker will benefit
    • more serious vulnerability might influence the share price even larger
Motivations for evaluators

• Academics
  – have interest in research and publications
  – evaluation can be done cheaper than in the industry

• Companies
  – offer security evaluation as a service

• Can help chip manufacturers
  – develop secure products through testing
  – find bugs in their chip designs to prevent further exploit

• Can help developers
  – prevent cloning and overbuilding by choosing correct components
  – reduce theft of service by applying correct security policy
  – eliminate theft of IP and increase cost of reverse engineering
  – fight denial of service with correct protocols
Progress in attacks and defences

• New attacks appeared, new countermeasures were introduced, have they balanced each other?
  – side-channel analysis: lower signal and higher frequency compensated by faster and more precision acquisition
  – microprobing: no success without sophisticated equipment, but still there is possibility to outsource or hire equipment time
  – more knowledge is required to perform attacks
  – little progress in semi-invasive attacks area

• Other problems
  – cost affects both the attackers and the defenders
  – time requirements become tougher
  – strong competition from fast growing Asian markets
  – lack of knowledge (properly educated engineers)
Progress in attacks

• We introduced new attack – optical fault injection
  – new attack method was defined in 2002: Semi-invasive attacks
  – shaken the security industry causing development of new countermeasures and amendment of Common Criteria evaluation requirements
Progress in defences

• Fabrication technology
  – was 1.2µm/0.5µm with 1M/3M, now 0.35µm/90nm with 3M/10M
  – reduced power consumption made power analysis harder
  – increased operating frequency made attacks more challenging

• Glitch attacks were mostly defeated
  – internal clock and power supply pumps
  – frequency and voltage monitors

• Other protection techniques
  – temperature sensors and top metal sensor mesh
  – dummy CPU cycles
  – data bus encryption

• Cost of defences
  – chip fabrication became more expensive and was moved to fables
  – evaluation became harder to perform and was outsourced
Myths from manufacturers

• Claim: Flash technology is secure because the state of a cell is not observable
  – What about data remanence?
  – What about influence from neighboring cells?
  – What about sensitivity to fault injection attacks?

• Real situation
  – there is no protection by default as the floating gate controls the floating-gate transistor – no need to determine the charge inside the floating gate
  – as the floating-gate transistor cell only provides the information, it is the responsibility of a memory control logic to grant the access

• EEPROM could be even worse as some technologies are vulnerable to more attacks
Myths from manufacturers

• Claim: Readback protection is highly secure – your design will not be compromised
  – What about factory testing?
  – What about memory access?

• Real situation
  – if there is a memory to access, there is a policy on who can access. If the memory control logic can be attacked, contents of the memory can be easily extracted
  – there is a wide variety of readback protection methods and most of them were successfully compromised due to vulnerabilities:
    • software-only protection (e.g. Motorola microcontrollers)
    • easy-to-find security fuse (e.g. Microchip, Atmel microcontrollers)
    • shared memory and factory settings (e.g. Dallas protected memory)
Myths from manufacturers

• Claim: We employ cryptography and encrypt all the data in our devices, so they are extremely secure
  – Really? Give me the key I will check
  – Does it really matter whether it takes 10’000 trillion years or only 100 million years to break the encryption?
  – Where is the key? How is it managed?

• Real situation
  – cryptography does not provide protection on its own – only to a certain extent
  – the key must be well protected and it must be impossible to guess, brute force or steal it
Myths from manufacturers

- **Claim:** Our devices are protected against all known attacks
  - How do they know that?
  - What about undisclosed attacks?

- **Real situation**
  - It takes some time between the point when a new attack was introduced and when countermeasures were put in place. Example: optical fault injection attacks
  - If there is an incentive in attacking certain devices then very likely they will be attacked
  - The more someone could benefit from breaking a particular device, the more chance that device will be compromised
Myths from manufacturers

- Claim: Our devices are secure and some useful features are available without license fees or royalties for use
  - Sounds too good?
  - Is this really the case?

- Real situation
  - if the security is there it will serve the manufacturer’s needs first
  - remember: free cheese is only found in the mousetrap.
  - Very likely, the manufacturer would charge more for pre-programmed or factory-tested silicon chips and use the security to protect their own IP
  - what if someone would find a way to circumvent the protection and, hence, offer a way of using standard low-cost chips in such applications?
Myths from manufacturers

• Claim: Academics can only pose problems, not solutions
  – How many attacks were discovered by academics?
  – What part of those attacks were unknown to the attackers?

• Real situation
  – do not shoot the messenger
  – does someone really believe that if a certain attack was published by some academics it has not been known to attackers?
  – the level of funding academics have does not allow everything
  – only small fraction of the work done in hardware security area is ever published
    • corporations refrain from publishing about vulnerabilities
    • attackers publish only useless material
    • academics do not publish everything they did
    • some publications are out of date due to restrictions from NDAs
Pitfalls

- Reading out memory (firmware) from smartcards
  - Could be much simpler (e.g. Hitachi 16-bit smartcard)
    - CPU instruction set vulnerability: only single modification is needed
    - Operating frequency is in wide range (from 150kHz to 8MHz)
    - Power supply voltage can vary (from 2.8V to 5.8V)
Pitfalls

- Certification has little to do with the actual security
  - Common Criteria only assures against compliance with some rules, but not their completeness
  - Does the manufacturer provide any form of guarantee or insurance on their secure chips?
  - If a certain secure chip is broken, will the manufacturer be responsible for any damage caused?
  - How one can be sure that there is no backdoors or embedded trojans inside the silicon chip?
Pitfalls

• Security upgrade (add security features to insecure chip)
  – allows quick introduction of a new member to the market
  – offers easier access to information and inherits vulnerabilities

• Lack of security analysis expertise with modern fables manufacturing
  – flaws in memory design and memory control logic
  – some known attacks could still work

• Availability of samples and tools is crucial for the attacker
  – easy access to device samples makes attack more feasible
  – documentation is essential as well as development tools

• Design outsourcing – less control

• Fables manufacturing – less involvement
## Trends

- **Constant pressure on cost reduction:**
  - attacks: cutting equipment cost, developing low-cost methods
  - defences: fables production, reducing evaluation cost, employing low-cost solutions, security via obscurity approach, adding security patches rather than redesigning the chip

- **Increasing number of devices with security features**
  - attacks: harder to find a suitable target and to get any profit
  - defences: shorter life cycle, harder to choose proper solution

- **Many devices were reported as being insecure**
  - not only microcontrollers, FPGAs and some old smartcards
  - secure memory chips (DS2432, AT88SC, KeeLoq, Mifare)
Trends

• Increased demand for security evaluation in the last years as chip fabrication technology became more advanced

• Cost of attacks has dropped significantly and data extraction from some chips is offered in Far East at prices under $100 (mainly microcontrollers and secure memory)

• Is it always bad if your product is compromised?
  – entertainment industry: sales go up (DVD players, game consoles)
Projection into the nearest future

• Many devices were already reported as being insecure
  – the situation will only deteriorate with the ongoing economic slowdown as more attention will be paid to cutting on costs
  – more devices will be reported as being insecure due to worsening situation with investment into hardware security research

• How to compare security of different products?
  – maybe it worth introducing something similar to MTBF used for electronic equipment, for example, MTBC (mean time before cracked), however, that could be expensive

• New low-cost attacks will be introduced posing more challenges to chip manufacturers and developers
Conclusion

• There is no such a thing as absolute protection – given enough time and resources any protection can be broken
• If you have not heard about your product being compromised it does not mean that it has not been broken yet
• Many vulnerabilities were found in various secure chips and more are to be found, thus posing more challenges to hardware security engineers
• With the economic downturn, less expensive and more powerful attacks are very likely to appear and that would create even bigger problems
• Not all lessons were learned – things can go wrong, things do go wrong and they will go wrong – who cares?