Real world AES key extraction

Sergei Skorobogatov

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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Introduction

- AES is widely used for authentication and data protection
  - algorithm is cryptographically secure
  - infeasible to break it by brute force attacks
- Implementation of the AES algorithm might not be secure
  - AES key might be extracted from embedded memory
  - fault attacks might work against algorithm implementation
  - AES key might be leaked via side channels
  - intermediate data might be leaked via side channels
- Secure chips are used in real world applications
  - authentication and access control
  - firmware update and encrypted code execution
- Tasks for hardware security expert
  - evaluate the strength of AES key protection
  - estimate the cost and time for AES key extraction

Challenges

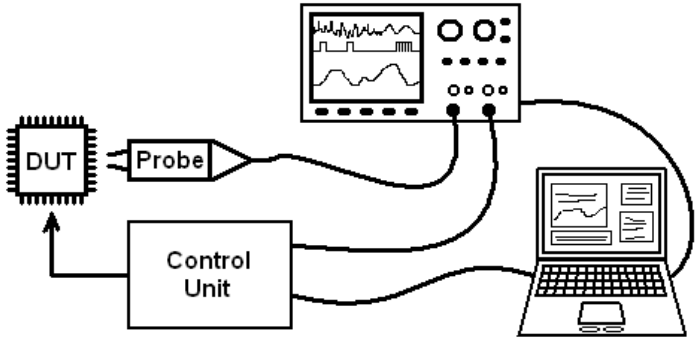
- Secure chips with hardware crypto-engines for IP protection
  - secure key storage (no readback access to the key)
  - no ways of simple software reverse engineering
- Fault analysis is not possible
  - no access to the output of crypto-engine
- No tamper evidence to be left
  - non-invasive approach, e.g. side-channel attacks
- Limited budget: maximum $10,000
  - the attacks are more likely to pose a significant threat
- Limited attack time: maximum 1 second on real device
  - does not raise any suspicion
  - offers real-time extraction
  - take your time for evaluation, but do it quickly on a real device

Why only 1 second?

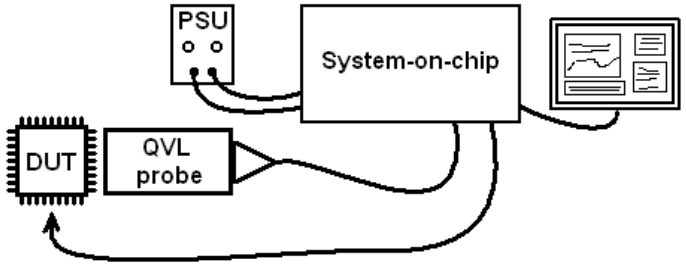
- Just the right time in many aspects
  - innocent look at the device while establishing wired connection
  - passing the device from one person to another
  - usual distraction time needed for deception trick
- Will 0.1 second make any better?
  - it takes about 0.2 seconds to put an average chip into a test socket
  - it will raise more concerns about effectiveness of countermeasures
- Will 10 second suffice?
  - can be spotted by a suspicious victim
  - could be ineffective if the key is changed frequently

Is it possible to attack in 1 second?

- Standard side-channel analysis setup



- New more efficient setup



- Plus another 9 problems to address and fix in order to get an average of 1'000'000 times improvement
  - in reality from 1'000 to 1'000'000'000'000 times improvement

To tell or not to tell

- Devices to be used for testing and demonstration of attack
  - standard secure chips with hardware AES crypto-engine
  - secure and widely used chips which manufacturers believe to be highly secure and developers believe they are unbreakable
- Special sensor is being developed under license by industrial sponsor with all details being under strict NDA
  - collaboration is limited to chip manufacturers and large companies
  - I will be first in academia to evaluate the new technology
- Forthcoming publications about the attack
  - subject to restrictions by IP, license and patent holders
  - similar to the way done by industry, i.e. with minimum information
- Aim of the proposed research
  - develop new evaluation technology for side-channel analysis
  - demonstrate its effectiveness on real world devices

When to expect the results?

- Initial set of experiments was carried out with some promising results
- September–October 2010 for the first set of experiments to finalise the requirements
- November–December 2010 for reaching 1-second barrier
- 2011–2012 new experiments and further improvements
- It is going to be a good analysis tool for chip manufacturers
  - better comparison of hardware countermeasures
  - faster and more reliable result
- For latest updates visit:

  http://www.cl.cam.ac.uk/~sps32/qvl_proj.html