Thesis Title

Royal Holloway

Luke Atherton (100905113)

1st March 2019

Abstract

This is my abstract

Dedication

This is my dedication

Declaration

This is my declaration

Acknowledgements

Thanks everyone!

Contents

Chapter 1

Introduction

Welcome to my introduction

1.1 Introduction

Introduction

Ideas:

"Virtual Binding of Hardware to Software of Embedded Systems through 2-Way Remote Attestation"

Use remote attestation of static and control flow to keep device in running state.

2 - way: Server sends remote attestation request, device responds with hash of completed signal path somehow along with static hash of software. Device requests current hash or something like that from server and compares to local value. If fails it stops function of software and reverts to simple operating mechanism (such as timed traffic lights).

Chapter 2

Introduction

2.1 Introduction

2.2 Smart Card Attacks

2.2.1 Introduction

2.2.2 Invasive Attacks

Page 196. Invasive attacks: microprocessor removed, and attacked directly through physical methods. In theory any microprocessor can be attacked in this way. Requires expensive equipment and large investment in time. Examples of attack: Probing bus lines between blocks on a chip (with a hole being made in a chip's passivation layer). Secret information is derived by observing information sent from one block on to another. Extreme example: Use focused ion beam to destroy or create tracks on the chip's surface. This could be used to reconnect disconnected fuses (think fuse used to deactivate PUF derivation). Use of fuses can also be to turn off test mode which is used to read/write to memory addresses during manufacture. This vulnerabiltiy has now been removed as test circuit is axtually removed from when the chip is cut from the die. [1] [2]

2.2.3 Semi-Invasive Attacks

Semi-invasive attacks: surface of chip needs to be exposed, security is compromised without directly modifying the chip. Examples: Observing electomagnetic eminations using a suitable probe [3], [4], injecting faults using laser [5] or white light [6]. Numerous more [7].

Fault Injection

Variations in supply voltage [1],[8]: may cause processor to misinterpret or skip instructions. Variations in external clock [1],[9],[2]: Data can be misread (data is attempted to be read before memory has time to latch-out correct value). Instruction miss. Extremes of temperature [10],[11]: unpredictable effects in microprocessor. Two effects obtained [5]: random modification of RAM cells due to overheating, read and write temperature thresholds in most NVM do not coincide. If temperature is set to level where write ops work by read do not a number of attacks can be mounted. Laser light (French!!(15), [12], Frechn!!(39)): Light arriving on metal surface induces a current, if intense enough could induce fault in a circuit. White light [1]: Proposed as alternative to laser [6], but not directional so may be a challenge to apply to particular portions of microprocessor. Electromagnetic flux [13]: change values in RAM, strong eddy currents can affect microprocceors - only observed in insecure microprocessors.

Effects: Reset data: force data to blank state Data randomisation: Change data to new random value. Modifying opcodes: Change intstructions executed on chip's cpu [1]. Often same effect as previous effects. Additionally removal of functions and breaking of loops.

Countermeasures given in [5]

2.2.4 Non-Invasive Attacks

Non-invasive attacks: Derive information without modification. Derive information through information that leaks during computation of given command, or attempt to inject faults in manner other than light. Examples: Observe power consumption [14], [15], inject faults by glitching power supply [1], [5]

Appendix A

Appendix Title

This is my appendix

Bibliography

[1] R. Anderson and M. Kuhn, "Tamper Resistance — a Cautionary Note," pp. 1–11, 1996. [Online]. Available: http://www.cl.cam.ac.uk/%7B~%7Drja14/Papers/tamper.pdf.

[2] O. Kömmerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," *USENIX Workshop on Smartcard Technology*, pp. 9–20, 1999.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," pp. 251–261, 2007. DOI: 10.1007/3-540-44709-1_21.

[4] J. Quisquater, "ElectroMagnetic Analysis : Measures and Countermeasures for Smart Cards," pp. 200–210, 2001.

[5] H. Bar-el and H. Choukri, "The Sorcerer ' s Apprenctice ' s Guide to Fault Attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, 2006. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/1580506/%7B%5C%7D0Ahttp://www.hbarel.com/media/blogs/hagai-on-security/Sorcerers%7B%5C_%7DApprentice%7B%5C_%7DGuide.pdf.

[6] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," pp. 2–12, 2007. DOI: 10.1007/3-540-36400-5_2.

[7] S. P. Skorobogatov, "Semi-invasive attacks-a new approach to hardware security analysis," *Technical report, University of Cambridge, Computer Laboratory*, no. 630, p. 144, 2005, ISSN: 1476-2986. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.228.2204%7B%5C&%7Drep=rep1%7B%5C&%7Dtype=pdf.

[8] J. Blömer and J.-P. Seifert, "Fault Based Cryptanalysis of the Advanced Encryption Standard (AES)," in, 2003, pp. 162–181. DOI: 10.1007/978-3-540-45126-6_12. [Online]. Available: http://link.springer.com/10.1007/978-3-540-45126-6%7B%5C_%7D12.

[9] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices," in, 1998, pp. 125–136. DOI: 10.1007/BFb0028165. [Online]. Available: http://link.springer.com/10.1007/BFb0028165.

[10] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Eliminating Errors in Cryptographic Computations," *Journal of Cryptology*, vol. 14, no. 2, pp. 101–119, Mar. 2001, ISSN: 0933-2790. DOI: 10.1007/s001450010016. [Online]. Available: http://link.springer.com/10.1007/s001450010016.

[11] S. Govindavajhala and A. W. Appel, "Using memory errors to attack a virtual machine," *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2003-January, pp. 154–165, 2003, ISSN: 10816011. DOI: 10.1109/SECPRI.2003.1199334.

[12] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *IEEE Transactions on Nuclear Science*, vol. 12, no. 5, pp. 91–100, 1965, ISSN: 15581578. DOI: 10.1109/TNS.1965.4323904.

[13] D. Samyde, S. Skorobogatov, R. Anderson, and J. J. Quisquater, "On a new way to read data from memory," *Proceedings - 1st International IEEE Security in Storage Workshop, SISW 2002*, pp. 65–69, 2003. DOI: 10.1109/SISW.2002.1183512.

[14] U. Maurer, "Differential Power Analysis," *Advances in Cryptology — CRYPTO' 99*, vol. 1666, p. 785, 1999, ISSN: 0302-9743. DOI: 10.1007/3-540-48405-1. [Online]. Available: http://www.springerlink.com/content/cdp6u8xpenkkx08m.

[15] S. Mangard, *Power analysis attacks : revealing the secrets of smart cards*. New York: Springer, 2007, ISBN: 0387308571.