Fault Injection Attacks: Attack Methodologies, Injection Techniques and Protection Mechanisms

Bhasin, Shivam; Mukhopadhyay, Debdeep

2016

Bhasin, S., & Mukhopadhyay, D. (2016). Fault Injection Attacks: Attack Methodologies, Injection Techniques and Protection Mechanisms. 2016 International Conference on Security, Privacy, and Applied Cryptography Engineering, 415-418.

https://hdl.handle.net/10356/82845

https://doi.org/10.1007/978-3-319-49445-6_24

Fault Injection Attacks: Attack Methodologies, Injection Techniques and Protection Mechanisms

A Tutorial

Shivam Bhasin[1,3] and Debdeep Mukhopadhyay[2,3]

[1]Physical Analysis and Cryptographic Engineering, Temasek Laboratories
Nanyang Technological University, Singapore
[2]Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur, India.
[3]Embedding Security and Privacy Pvt Ltd. (ESP-Research)
Email: sbhasin@ntu.edu.sg; debdeep@cse.iitkgp.ernet.in

Abstract. Fault Injection Attacks are a powerful form of active attack mechanism which can threaten even the strongest of cryptographic algorithms. This attack vector has become more pertinent with the growing popularity of the Internet of things (IoT), which is based on small omnipresent embedded systems interacting with sensitive data of personal or critical nature. This tutorial addresses this issue of fault attacks, covering a wide range of topics which has accumulated through years of research. The first part of the talk will cover fault attacks and its application to attack standard cryptosystems. Different popular forms of fault attacks, namely Differential Fault Attacks (DFA) and Differential Fault Intensity Attacks (DFIA) are presented. It is followed subsequently by a discussion on the underlying injection techniques. Finally, protection mechanism will be discussed highlighting on information redundancy based reactive countermeasures and sensor-based protection mechanisms as two alternative strategies for security against the menacing fault attacks.

KeyWords: fault injection attacks, differential fault analysis, parity, sensors

1 Overview

Fault analysis of cryptographic primitives was first reported by Boneh et. al. [3] in 1996 to attack an RSA cryptosystem. After this seminal work, a new research direction was triggered to conduct study of fault analysis with respect to all popular cryptosystems, including symmetric key cryptosystems, public key cryptosystems and hash function. Fault attacks involve injecting faults into an implementation of a cryptographic algorithm, followed by analysis under different fault models to recover the key. Such attacks have rendered even mathematically robust and classically secured cryptosystems vulnerable. With fault attacks now being an established threat to cryptosystems, sound countermeasures are needed to protect them. Designing countermeasures against fault attacks is a

non-trivial task in the present scenario, given the multitude of fault models and fault injection techniques that an adversary has at her disposal. Finally, it is also important to design suitable metrics to quantify the vulnerability of a given crypto primitive against a particular fault model, as well as to compare multiple cryptosystems in terms of their security against fault attacks. The tutorial at hand presents a comprehensive coverage of the state-of-the-art in each of these aspects, and also points out future research directions.

In this talk, we first present the concept of fault analysis and its relation to cryptography. Subsequently, we discuss on Differential Fault Analysis (DFA) [2] of the world-wide standard block cipher, namely the Advanced Encryption Standard (AES). A detailed case study of DFA on AES-128 is presented to show how a single well formed fault can lead to a drastic reduction of the key-space, and eventually its leakage [8, 14]. The optimality of this attack is subsequently discussed. Thereafter, we extend these attacks to multiple byte faults, using a new fault model based on the diagonals of the AES state matrix. This fault attack, commonly called as the Diagonal Fault Attack shows that the cipher can be attacked if one, two or three diagonals are affected needing 2, 2 or 4 faulty cipher-texts respectively to uniquely obtain the key [13]. In order to thwart such powerful attacks, fault tolerance is introduced in block ciphers through either detection or infective schemes. However, there is a gap!; While conventional fault tolerance offers large amount of reliability under the assumption that all faults are equally likely, an attacker is equipped with a biased fault injection mechanism, which can threaten most existing fault tolerant architectures. We formalize the notion of bias of a fault model using the variance of the fault distribution. Subsequently, we discuss that the bias in the fault injection increases the probability of fault collisions which can lead to attacks against popular detection schemes [10]. In this context, we further discuss a different flavour of fault attacks, called Differential Fault Intensity Analysis (DFIA), that combines principles of differential power analysis with fault attacks [4].

The second part of the tutorial will cover practical aspects of fault attacks. Research on fault injection techniques has advanced over the last two decades. From global and inexpensive methods like power glitch [1] which troubled the pay television industry for several years, to sophisticated and local methods employing techniques like laser [11] or electromagnetic injections [12] which can penetrate with precision even the latest technology nodes. A comparative analysis of techniques involved, their extent, limitations and applications are discussed. The study of injection techniques is naturally followed by protection mechanisms. These protection can be applied either at the physical level [15, 7] to detect injection attempts or at the information level [6, 5] to detect data modification. Physical level countermeasures are based on sensors which detect any change in environmental condition that may result in faults. On the other hand, information level countermeasures profits from concurrent error detection mechanisms to detect data change by faults. However, the biasness of the fault injection techniques makes many classic fault tolerant techniques weak and can be still subjected to fault analysis [10]. Finally, we conclude with the novel idea

of Fault Space Transformation (FST) as a novel proposition to counter such biased fault attacks [9].

References

1. Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C.: The sorcerer's apprentice guide to fault attacks. Proceedings of the IEEE 94(2), 370–382 (2006)
2. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Annual International Cryptology Conference. pp. 513–525. Springer (1997)
3. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 37–51. Springer (1997)
4. Ghalaty, N.F., Yuce, B., Taha, M.M.I., Schaumont, P.: Differential fault intensity analysis. In: Tria, A., Choi, D. (eds.) 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014, Busan, South Korea, September 23, 2014. pp. 49–58. IEEE Computer Society (2014), http://dx.doi.org/10.1109/FDTC.2014.15
5. He, W., Breier, J., Bhasin, S., Chattopadhyay, A.: Bypassing parity protected cryptography using laser fault injection in cyber-physical system. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security. pp. 15–21. ACM (2016)
6. Karri, R., Wu, K., Mishra, P., Kim, Y.: Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers. IEEE Transactions on computer-aided design of integrated circuits and systems 21(12), 1509–1517 (2002)
7. Miura, N., Najm, Z., He, W., Bhasin, S., Ngo, X.T., Nagata, M., Danger, J.L.: Pll to the rescue: a novel em fault countermeasure. In: Proceedings of the 53rd Annual Design Automation Conference. p. 90. ACM (2016)
8. Mukhopadhyay, D.: An improved fault based attack of the advanced encryption standard. In: Preneel, B. (ed.) Progress in Cryptology - AFRICACRYPT 2009, Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5580, pp. 421–434. Springer (2009), http://dx.doi.org/10.1007/978-3-642-02384-2_26
9. Patranabis, S., Chakraborty, A., Mukhopadhyay, D., Chakrabarti, P.P.: Using state space encoding to counter biased fault attacks on AES countermeasures. IACR Cryptology ePrint Archive 2015, 806 (2015), http://eprint.iacr.org/2015/806
10. Patranabis, S., Chakraborty, A., Nguyen, P.H., Mukhopadhyay, D.: A biased fault attack on the time redundancy countermeasure for AES. In: Mangard, S., Poschmann, A.Y. (eds.) Constructive Side-Channel Analysis and Secure Design - 6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers. Lecture Notes in Computer Science, vol. 9064, pp. 189–203. Springer (2015), http://dx.doi.org/10.1007/978-3-319-21476-4_13
11. Pouget, V., Douin, A., Lewis, D., Fouillat, P., Foucard, G., Peronnard, P., Maingot, V., Ferron, J., Anghel, L., Leveugle, R., Velazco, R.: Tools and methodology development for pulsed laser fault injection in SRAM-based FPGAs. In: 8th LATW'07). p. Session 8. IEEE Computer Society, Cuzco, Peru (2007)
12. Quisquater, J.J., Samyde, D.: Eddy current for magnetic analysis with active sensor. In: Esmart 2002, Nice, France (2002)

13. Saha, D., Mukhopadhyay, D., Chowdhury, D.R.: A diagonal fault attack on the advanced encryption standard. IACR Cryptology ePrint Archive 2009, 581 (2009), http://eprint.iacr.org/2009/581
14. Tunstall, M., Mukhopadhyay, D., Ali, S.: Differential fault analysis of the advanced encryption standard using a single fault. In: IFIP International Workshop on Information Security Theory and Practices. pp. 224–233. Springer (2011)
15. Zussa, L., Dehbaoui, A., Tobich, K., Dutertre, J.M., Maurine, P., Guillaume-Sage, L., Clediere, J., Tria, A.: Efficiency of a glitch detector against electromagnetic fault injection. In: Proceedings of the conference on Design, Automation & Test in Europe. p. 203. European Design and Automation Association (2014)