Fast and Memory-Efficient Key Recovery in Side-Channel Attacks - DTU Orbit (09/11/2017)

Fast and Memory-Efficient Key Recovery in Side-Channel Attacks

Side-channel attacks are powerful techniques to attack implementations of cryptographic algorithms by observing its physical parameters such as power consumption and electromagnetic radiation that are modulated by the secret state. Most side-channel attacks are of divide-and-conquer nature, that is, they yield a ranked list of secret key chunks, e.g., the subkey bytes in AES. The problem of the key recovery is then to find the correct combined key.

An optimal key enumeration algorithm (OKEA) was proposed by Charvillon et al. at SAC'12. Given the ranked key chunks together with their probabilities, this algorithm outputs the full combined keys in the optimal order – from more likely to less likely ones. OKEA uses plenty of memory by its nature though, which limits its practical efficiency. Especially in the cases where the side-channel traces are noisy, the memory and running time requirements to find the right key can be prohibitively high.

To tackle this problem, we propose a score-based key enumeration algorithm (SKEA). Though it is suboptimal in terms of the output order of candidate combined keys, SKEA's memory and running time requirements are more practical than those of OKEA. We verify the advantage at the example of a DPA attack on an 8-bit embedded software implementation of AES-128. We vary the number of traces available to the adversary and report a significant increase in the success rate of the key recovery due to SKEA when compared to OKEA, within practical limitations on time and memory. We also compare SKEA to the probabilistic key enumeration algorithm (PKEA) by Meier and Staffelbach and show its practical superiority in this case.

SKEA is efficiently parallelizable. We propose a high-performance solution for the entire conquer stage of side-channel attacks that includes SKEA and the subsequent full key testing, using AES-NI on Haswell Intel CPUs.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , Riscure, Technical University of Denmark, Aalto University
Authors: Bogdanov, A. (Intern), Kizhvatov, I. (Ekstern), Manzoor, K. (Ekstern), Tischhauser, E. W. (Intern), Witteman, M. (Ekstern)
Pages: 310-327
Publication date: 2016

Host publication information

Title of host publication: 22nd International Conference on Selected Areas in Cryptography (SAC 2015) : Revised Selected Papers
Publisher: Springer
Editors: Dunkelman, O., Keliher, L.
ISBN (Print): 978-3-319-31300-9
ISBN (Electronic): 978-3-319-31301-6

Series: Lecture Notes in Computer Science
Volume: 9566
ISSN: 0302-9743
BFI conference series: Selected Areas in Cryptography (5000230)
Main Research Area: Technical/natural sciences
Conference: 22nd International Conference on Selected Areas in Cryptography, Sackville, Canada, 12/08/2015 - 12/08/2015
DOIs:
10.1007/978-3-319-31301-6_19
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016