Open Science Index, Electrical and Computer Engineering Vol:9, No:08, 2015 publications.waset.org/abstracts/17652.pdf

A Survey on Countermeasures of Cache-Timing Attack on AES Systems

Authors : Settana M. Abdulh, Naila A. Sadalla, Yaseen H. Taha, Howaida Elshoush

Abstract : Side channel attacks are based on side channel information, which is information that is leaked from encryption systems. This includes timing information, power consumption as well as electromagnetic or even sound leaking which can exploited by an attacker. Implementing side channel attacks are possible if and only if an attacker has access to a cryptosystem. In this case, the attacker can exploit bad implementation in software or hardware which is not controlled by encryption implementer. Thus, he/she will represent a real threat to the security system. Several countermeasures have been proposed to eliminate side channel information vulnerability.Cache timing attack is a special type of side channel attack. Here, timing information is collected and analyzed by an attacker to guess sensitive information such as encryption key or plaintext. This paper reviews the technique applied in this attack and surveys the countermeasures against it, evaluating the feasibility and usability of each. Based on this evaluation, finally we pose several recommendations about using these countermeasures.

Keywords : AES algorithm, side channel attack, cache timing attack, cache timing countermeasure
Conference Title : ICSM 2015 : International Conference on Security and Management
Conference Location : London, United Kingdom
Conference Dates : August 20-21, 2015